Interaction Administrator

Printed help

PureConnect powered by Customer Interaction Center® (CIC)

2018 R5

Last updated November 09, 2018

Table of Contents

Interaction Administrator 1

Interaction Administrator Help 1

Interface commands 1

Create new entries 1

Modify existing entries 2

Editing lists of configuration entries 2

Using the Apply button 2

Site name 2

License information. 3

About Setup Assistant 3

New features in Interaction Administrator 5

Overview of Interaction Administrator 6

Overview of Interaction Administrator 6

License Management 7

Navigation Controls 7

Telephony Server Configuration 8

User and Workgroup Configuration 8

CIC System Configuration 9

Starting CIC server modules 10

Minimum Hardware and Software Requirements 10

Command-line Options 10

Interaction Administrator Interface 12

System security for IA 30

Collective 35

Collective concepts 35

Collective concepts 36

Home Site 37

Peer Site 38

Assistants 42

Assistants 42

- Add Location Assistant 43
- Managed IP Phone Assistant 46

IC Server 57

- Overview of CIC server configuration 57
- Server Configuration 58
- Lines 82
- Line Groups 177
- Stations 183
- Managed IP Phones 247
- SIP Bridges 324
- Audio Sources 324
- Server Parameters 326
- Structured Parameters 372
- Regionalization 373

License Allocation 389

- Licenses Allocation 389
- License Configuration 390

People 394

- People 394
- Security for people 395
- ACD 428
- Default User 433
- Roles 435
- Users 440
- Workgroups 464
- Password Policies 488
- Schedules 494
- Secure Input Forms 498
- Wrap-up Codes 503
- Wrap-up Categories 506
- CIC Client Buttons 510
- Client Configuration 513

Queue Columns 528

Account Codes 530

Client Templates 535

Response Management 537

Skills 542

Access Control Groups 546

About inheritance of configuration properties 554

Activating configuration changes for users, workgroups, roles, and the default user 555

System Configuration 556

CIC System Configuration 556

System Configuration Pages 556

Interaction Processor 569

Phone Numbers 573

Report Logs 607

Accumulators 637

System Parameters 639

Status Messages 641

Actions 646

Log Retrieval Assistant (LRA) 649

Mail 652

Single Sign-On 675

PureCloud 685

Interaction Process Automation 698

Interaction Feedback Settings 700

Fax Configuration 701

IC Data Sources 707

Contact Data Manager 717

Web Services 725

Recognition 732

Media Servers 746

SIP Proxies 751

MRCP Servers 752

Session Manager Configuration 758

SMS 759

Problem Reporter 768

Layouts 769

Analytics 774

Interaction Tracker 775

About Interaction Tracker 775

Configuring Interaction Tracker 775

Defining Interaction Tracker Entity Types 782

Security 784

Interaction Recorder 785

Interaction Recorder 785

Configuration 786

Policy Editor 791

Who can see and listen to recordings 791

Screen Recording 792

Remote Content Server 794

Interaction Optimizer 795

Interaction Optimizer 795

Interaction Optimizer Configuration 797

Interaction Optimizer 802

Interaction Conference 803

Interaction Conference Configuration 803

Conference Room Configuration 805

Interaction Conference Email Templates 806

Setting Default Conference Options 807

Interaction Analyzer 809

Overview of Interaction Analyzer 809

Keyword concepts 810

Manage keyword sets 831

Manage keywords 838

Report Management 842

Report Management 842
Report Configuration 842
Report Configuration Export 848
Report Configuration Import 849
Report System Settings 850
Configure secure report parameters 851
Glossary 853
ACD term 853
DND 854
CIC Port Number 854
CIC Registry Entries 854
Immediate Mode 854
Initialization Function 854
Wink Mode 855
Diagnosing Problems 855
Solving problems 855
Revisions 856
CIC 2018 R4 856
CIC 2018 R2 857

Interaction Administrator

Interaction Administrator Help

This help contains information about the Interaction Administration application. The application interface consists of a tree view window (the left hand pane) with container names and icons, and a list view window (the right hand pane) displaying columns of pertinent configuration data for the container selected in the tree view.

> **Note**: Anytime you open Interaction Administrator, the top-level container is expanded and displays all sibling containers under it.
>
> **A note about client applications:** Customer Interaction Center (CIC) supports two interaction management client applications. This documentation uses the term "CIC client" to refer to either Interaction Connect or Interaction Desktop. For more information about CIC clients, see the CIC Client Comparison in the PureConnect Documentation Library.

Interface commands

Click on one of the following links for more information on available commands from the Interaction Administrator interface:

- Menu Commands
- Toolbar Commands
- Right-Click Menu Commands
- Selection Commands

Create new entries

To create new configuration entries, select a container in the tree view. Configuration objects in that container (if any are defined) appear in the list view.

In the list view pane:

1. Press the **Insert** key to create a new entry, or

   Right-click and select the **New Insert** command, or

   On the **Edit** menu select the **New Entry Insert** command
2. Type the name of the configuration entry, and then click **OK**.

> Some containers have an associated Configuration object displayed in the list view window (such as Default User Configuration and System Configuration). Double-click the configuration object to modify its properties.
>
> **Note:** The list view does not redraw the list every time you insert, delete, or modify an entry. The list view is refreshed only when you use the Refresh (F5) command, sort the columns, or when you select a new branch in the tree view. Deletes will leave the following item selected. Inserts are added to the bottom of the list.

Modify existing entries

To modify existing configuration entries, do one of the following:

- Double-click on a configuration object in the list view window, or
- Select an entry in the list view and right-click to select the **Properties** menu, or
- On the **Edit** menu, click **Properties**.

> You can display a pop-up menu for some configuration entries. In list view, select the entry, and then right-click the entry. Use the menu options to modify key configuration data, and then click **OK** to save the changes.

Editing lists of configuration entries

Property pages in most configuration entries include two buttons to facilitate making individual changes to each entry quickly.

The « » buttons allow you to display the previous (above) or the next (below) entry's configuration in the list view window, automatically saving changes as you do.

The ☐ Confirm auto-save check box gives you the option to display a dialog box asking you to confirm you want to save any changes. Click here for an explanation of why you may see the "Do you want to save changes?" in the Auto Save dialog box when you didn't change anything.

> **Notes:** Most configuration property changes are recognized by CIC immediately after they are saved. The only exceptions are server parameters and entry fields that include UNC or explicit drive/directory names. These changes are recognized only after restarting CIC.
>
> All property page fields that require a file name for input include a **Browse** button to help you locate and enter the correct path and file name.

Using the Apply button

Use the **Apply** button to save any changes you may have made in a property page without closing the property page, like the OK button. When you create a new object in Interaction Administrator, the Apply button is not available until after you click the OK button and open it the second time. The Apply button is available all the time, but it knows if you have already saved something; it will not write the same saved data again.

Site name

The site name is specified during the IC Server installation procedure and cannot be changed from within Interaction Administrator. The server name is automatically detected during IC Server installation and this name is inserted in Interaction Administrator.

> **Caution:** If you need to change the site, configuration (Production), or server name settings after you install IC Server, use the Setup Assistant. For more information, see the IC Setup Assistant help.
>
> If a PureConnect Customer Care representative gives you specific instructions to edit these settings in the registry, use only DSEdit to make the recommended changes. If you incorrectly change these settings, you could adversely affect the performance of CIC or prevent it from functioning properly.

License information.

The Interaction Administrator screen displays how many days you have to renew your license before expiration in the lower left-hand corner.

A message is shown requesting the system administrator re-register the license file prior to the license anniversary date. If license renewal is due within a specific time period, a message is displayed similar to "Your license is due for its annual re-registration in XX days. Please visit http://license.inin.com to re-register your license."

Other licensing messages are displayed as well. For example, in a non-Switchover environment, you may see "The new license file was successfully published to this server.", or "The new license file failed to apply to this server. Contact PureConnect Customer Care for further assistance."

Related Topics

Overview of how to add users

Auto Save feature

Exporting configuration data

Updating configuration values

11/09/2018
CIC 2018 R4

About Setup Assistant

During installation, the installer uses IC Setup Assistant to configure any or all of the following features for Interaction Administrator:

- CIC administrator and network information
- CIC license
- Dial plan
- Database
- CIC optional components, such as Switchover, Multi-Site RTM, and TFTP server
- Site Information (Interaction Tracker — add-on license)
- Server Group Certificate and Private Key (Switchover)
- Interaction Recorder (add-on license)
- Speech Recognition engine (add-on license)
- Mail provider

- Log Retrieval Assistant
- SIP Lines and Default Registration
- Stations
- Users
- Workgroups
- Roles
- Default hours of operation
- Group call processing
- DCOM security

After the installation is complete, you can re-run IC Setup Assistant to complete the tasks that you cannot complete in Interaction Administrator or anywhere else in CIC.

When you re-run the IC Setup Assistant, a different **Welcome** page appears. From this page, you can make the following changes by re-running IC Setup Assistant:

- Identity
- Optional components
- Dial plan
- Rename DS
- Database
- DCOM
- Certificates

You must make additions or changes to the following configurations in Interaction Administrator:

- Site information
- SIP lines and default registration group
- Interaction Recorder
- Speech recognition
- Mail provider
- Log retrieval assistant
- Stations
- Users
- Workgroups
- Roles

Additions or changes to the following configurations must be made in Interaction Attendant:

- Default hours of operation
- Group call processing

New features in Interaction Administrator

Interaction Administrator version 4.0 contains the following new features to assist you in customizing and configuring Interaction Center. The new features include:

Access Control Groups: Access Control Groups (ACGs) provide a flexible way of defining administrative access rights.

AudioCodes phones: CIC now supports AudioCodes phones.

Concurrent Licensing: This new license option allows licenses to be assigned to more users than there are licenses available.

Crystal Reports: The Report Management container is now used to configure Crystal Reports 2013. You can now configure Crystal Reports run by IC Business Manager to execute without a direct connection to the database server. You can also configure secure parameters to restrict report results with secure parameters.

Enhanced Interaction Administrator Change Notification Log: CIC supports enhanced change audit logging for selected Interaction Administrator containers.

Gmail OAuth support: CIC now supports OAuth 2.0 for Gmail authentication.

Interaction Analyzer: Interaction Analyzer's real-time word and phrase spotting allows for fully-integrated speech analytics with supervisors and agents being informed in real time of interaction scores and spotted keywords and phrases.

Interaction Update: You can now configure the local Interaction Update provider URI in the System Configuration container.

Password policies now contain additional configuration options for enhanced security.

PureCloud for CIC Integration: The new PureCloud container allows you to easily configure the integration between your CIC server and your PureCloud organization.

Remote Content Server: Interaction Recorder Remote Content Server provides multiple efficiencies in recording telephone conversations and screen activity in the Interaction Center environment. The Remote Content Server can take over the certain tasks from the CIC server improving bandwidth.

Security: The new security configuration and management dialog boxes have changed significantly, allowing simplified management of these security settings. With the addition of a search function and the ability to get better insight into the security inheritance model, administration and ongoing system maintenance has become much easier. The new security settings also allow more granular control over existing features.

Server parameters for IC Business Manager views allow you to restrict the number of records that may appear in the IC Business Manager statistics views.

Session Manager Regionalization: An off-server session manager can be assigned to a specific region/location and all the client applications (the CIC clients and IC Business Manager) running in that location use the local off-server session manager.

Single sign-on: When single sign-on is enabled, a user can log in once and then access multiple CIC applications without being prompted to log in again. To simplify the configuration process, activate the Single Sign-on Configuration Utility plug-in by enabling the **EnableSSOConfiguration** server parameter.

SMS: New configuration options are available for SMS messages. These include associating an SMS broker account with a workgroup or user, purging SMS data, and tracking SMS messages with Interaction Tracker.

Advanced syslog tracing options are available for Polycom phones.

Wrap-up Categories: Wrap-up codes can be associated with categories.

Overview of Interaction Administrator

Overview of Interaction Administrator

> **Important:** Interaction Administrator is available in several different editions: Interaction Administrator, Interaction Web Edition, and Interaction Administrator Server Manager Administrator Edition. In this help system, "Interaction Administrator" denotes the specific edition that you are using. The full product name appears at the top of each help topic. The full product name may also be used in a help topic when necessary to distinguish between Interaction Administrator editions.

Interaction Administrator allows the system administrator to configure virtually every aspect of CIC - from the telephony hardware and inbound/outbound phone lines on the server, to the appearance and security levels of each user’s CIC client.

Other configurable features include:

- Fax resources and fax groups
- Dial plan configuration and dialing privileges for the server
- Telephone lines and line groups, including an SMDI interface
- Customizations for T1, ISDN, and other digital line interfaces
- Stations, such as PCs, telephones, internal and external fax resources
- Users, Roles, and Workgroups, including ACD agent and skill configuration
- Account codes for designated types of calls and account billing
- A collective for easy communications across multiple CIC sites
- Administration , security, and user privileges
- CIC report logs and reports for tracking phone system activity
- CIC handlers, parameters, and other system initialization functionality

- Status messages
- DDE actions for invoking third party applications with each call
- Data manager configuration for speed dial lists and directories
- Response Management for creating Agent documents
- Web interaction messages and URLs for the CIC Web server interface

In Interaction Administrator, functionality is organized in containers. For more information, see *Containers list*.

Related topics

Containers list

License Management

Use the License Management dialog box to view and load licenses.

> **Note:** Only users with the master administrator right can access the **License Management** dialog box. This is a display list only. You cannot add to, delete from, or copy or paste into this list. For general licensing information, see the *PureConnect Licensing Technical Reference* in the PureConnect Documentation Library.

For complete instructions on updating your licenses, go to the Activation File Management area of the Customer Care portal dashboard.

Navigation Controls

The following navigation controls are always available in Interaction Administrator:

Lists support quick-key selection. That means you can select an entry inside any list and then press the letter or number key that begins the entry you want to select. The cursor jumps to the first entry in the list that begins with that character. If there are multiple entries that begin with the same character, you can continue to press the same character key to select the next entry that begins with that character.

- In the list view (right pane), once an entry is highlighted, you can press Enter to open the page for that entry.
- When a configuration dialog box is open to a particular page, and there are multiple entries in that configuration container, you can click on the **>>** button at the bottom of the page to view that page in the next entry down the list. If the Confirm Auto-save check box is selected, you can make changes to each page, click the **>>** (or **<<** to go up) button, and the changes are saved automatically.
- Interaction Administrator automatically remembers which container was selected from one session to the next. In addition, it remembers which property page you were on each time you open a page.
- Context sensitive menus are available in the list view (right pane) when you right-click, or when you see the Context menu available on the menu bar. The available menus depend on which container is selected.

Telephony Server Configuration

An IC server contains telephony hardware resources (for example, analog and/or digital voice boards, fax boards, station boards, etc.) that connect incoming telephone lines with your company's PCs, telephones, fax machines, etc. Each IC server has a specific number of configurable resources that are defined in Interaction Administrator containers found under the container named after the IC server (for example, I3Server). These include:

- Report logs and accumulators activated for this server
- Telephone lines that are defined to use a particular phone number, telephony board, port/channel, and other attributes
- Line groups that are named groups of telephone lines used for specific applications
- Stations (for example, PCs, telephones, fax devices and stand-alone fax machines) that have extensions and are associated with specific boards, ports/channels, and so on

> Each IC server also supports server parameters that are similar to macros that contain data (such as drive and path information) unique to that server and that can be used by the IC Interaction Processor as it operates.

Related topics

Add Stations Assistant

Add User Assistant

CIC System Configuration

Configure a SIP Line

Line Group Configuration

Station Group Configuration

User and Workgroup Configuration

User and Workgroup Configuration

Each CIC user has at least one unique attribute (such as an extension number) along with many other attributes that define the user's CIC client interface, status messages, telephone privileges, security controls, workgroup memberships, and so on. Each user inherits default values for some of these attributes from the **Default User** configuration container, which is the logical place to start user configuration. The CIC installation program creates a minimal set of Default User attributes that can be modified.

Each CIC user must have a network user account (for a Windows server) and have a Microsoft Exchange mail account to receive voicemail and faxes. Configuring CIC users is easier if the network and Exchange accounts are already established, but it is not required. Each user can be a member of zero or more CIC workgroups, which are logical groups of users that can (optionally) have a common telephone extension and serve as a queue for ACD calls as well as other attributes. Workgroups also inherit some default attributes from the **Default User** configuration container.

Wherever a user logs in to the CIC network, the Interaction Processor (IP) identifies that user by his or her unique extension number and routes calls to the extension number of his or her current workstation. IP then routes calls and tracks user interactions based on that user's activity.

Related topics

Delete User

CIC System Configuration

Telephony Server Configuration

Overview of how to add users

CIC System Configuration

CIC system resources control specific features and functionality provided in the Interaction Center for the entire configuration, regardless of how many servers or users are installed. System-level configuration includes:

- Interaction Processor (IP) variables and startup handlers
- Phone number identification and pattern matches. All dial plan configuration and phone number classifications are controlled in the Phone Numbers container.
- Report , Report Log , and Accumulator activity for gathering and producing call activity reports
- System-wide parameters that can be referenced by all CIC handlers on each server
- Status messages that can be defined on the server and set on each workstation running a CIC client.
- Action definitions
- Log Retrieval
- Administrative, fax, and voice email account names
- Interaction Process Automation
- Interaction Feedback
- Fax server, Interaction Fax Viewer default attributes and fax groups that are named groups of fax devices used for specific applications.
- Database and data source configuration
- Predefined Web chat messages and URLs for agents taking Web chat sessions
- Voice recognition
- Media Servers
- SIP Proxies

- MRCP Servers
- Session Manager
- SMS

Starting CIC server modules

The CIC server installation procedure sets up the IC Console service, which starts all the CIC server modules automatically as Windows services when the server is rebooted. If the server is restarted for any reason, all CIC services are automatically started. In addition, if any individual module is ever terminated (for example, someone kills a process in Task Manager), it will automatically be restarted when IC Console is running as a service.

In general, we recommend that any future CIC server restarts include a complete power cycle of the server to ensure that the telephony hardware and/or software is completely reset.

> **Warning:** Do NOT manually edit the registry entries in the IC ProcessTree and do NOT use these optional EicService command line arguments without explicit instructions from PureConnect Customer Care representatives. Doing so could cause your system to stop functioning or not start as designed.

Minimum Hardware and Software Requirements

The system requirements for the current release are available on the Product Information site.

Command-line Options

Overview of command line options

When necessary, you can also start Interaction Administrator from a command line. When you do that, you can use optional command line arguments to do the following things:

- Specify another CIC server on the network.
- Run Interaction Administrator as a master administrator.
- Specify the default language (locale) for Interaction Administrator.

Related topics

Specify an alternate CIC server

Start Interaction Administrator as a master administrator

Specify the default language (locale)

Specifying an alternate CIC server

You can specify an alternate CIC server when you start Interaction Administrator from a command line. This allows you to use the same workstation to configure or test with multiple CIC servers.

To specify an alternate CIC server with Interaction Administrator

1. Open a command prompt and type one of the following:

    - IAShellA.exe /notifier=servername

    > Note: If your release of CIC includes the Multi-server Administration license and you are attempting to make configuration changes to a Multi-server Administration slave, a warning message is displayed. The message instructs you to change the /notifier=servername parameter to point to the Multi-server Administration Master.

    - IAShellA.exe /notifier=ipaddress

Substitute the name of another CIC server on the network for servername, or enter that server's IP address if the *servername* is not available on the LAN.

Related topics

Overview of starting options for Interaction Administrator

Start Interaction Administrator as a master administrator

If you accidentally delete all of the user accounts with master administrator privileges, you can start Interaction Administrator from the CIC server console.

> **Note:** You will not be able to start it as master administrator from another computer.

To start Interaction Administrator as a master administrator

1. On the CIC server, open a command prompt and type one of the following:

    - C:> IAShellU.exe

    - C:> IAShellU.exe /notifer=localhost

    Do not use the /user and /password command line arguments in this case. This starts Interaction Administrator as a (undefined) user with master administrator privileges. From there, you can recreate user accounts and assign master administrator privileges to other accounts.

Related topics

Overview of starting options for Interaction Administrator

Specify the default language

You can start Interaction Administrator in a specific locale.

To specify the default language during startup

1. Enter the following at a command line: IAShellA.exe /LANGID=[language code]

Related topics

Overview of starting options for Interaction Administrator

Interaction Administrator Interface

Interaction Administrator Help

This help contains information about the Interaction Administration application. The application interface consists of a tree view window (the left hand pane) with container names and icons, and a list view window (the right hand pane) displaying columns of pertinent configuration data for the container selected in the tree view.

> **Note**: Anytime you open Interaction Administrator, the top-level container is expanded and displays all sibling containers under it.
>
> **A note about client applications:** Customer Interaction Center (CIC) supports two interaction management client applications. This documentation uses the term "CIC client" to refer to either Interaction Connect or Interaction Desktop. For more information about CIC clients, see the CIC Client Comparison in the PureConnect Documentation Library.

Interface commands

Click on one of the following links for more information on available commands from the Interaction Administrator interface:

- Menu Commands
- Toolbar Commands
- Right-Click Menu Commands
- Selection Commands

Create new entries

To create new configuration entries, select a container in the tree view. Configuration objects in that container (if any are defined) appear in the list view.

In the list view pane:

1. Press the **Insert** key to create a new entry, or

   Right-click and select the **New Insert** command, or

   On the **Edit** menu select the **New Entry Insert** command
2. Type the name of the configuration entry, and then click **OK**.

> Some containers have an associated Configuration object displayed in the list view window (such as Default User Configuration and System Configuration). Double-click the configuration object to modify its properties.
>
> **Note:** The list view does not redraw the list every time you insert, delete, or modify an entry. The list view is refreshed only when you use the Refresh (F5) command, sort the columns, or when you select a new branch in the tree view. Deletes will leave the following item selected. Inserts are added to the bottom of the list.

Modify existing entries

To modify existing configuration entries, do one of the following:

- Double-click on a configuration object in the list view window, or
- Select an entry in the list view and right-click to select the **Properties** menu, or
- On the **Edit** menu, click **Properties**.

> You can display a pop-up menu for some configuration entries. In list view, select the entry, and then right-click the entry. Use the menu options to modify key configuration data, and then click **OK** to save the changes.

Editing lists of configuration entries

Property pages in most configuration entries include two buttons to facilitate making individual changes to each entry quickly.

The «» buttons allow you to display the previous (above) or the next (below) entry's configuration in the list view window, automatically saving changes as you do.

The □ Confirm auto-save check box gives you the option to display a dialog box asking you to confirm you want to save any changes. Click here for an explanation of why you may see the "Do you want to save changes?" in the Auto Save dialog box when you didn't change anything.

> **Notes:** Most configuration property changes are recognized by CIC immediately after they are saved. The only exceptions are server parameters and entry fields that include UNC or explicit drive/directory names. These changes are recognized only after restarting CIC.
>
> All property page fields that require a file name for input include a **Browse** button to help you locate and enter the correct path and file name.

Using the Apply button

Use the **Apply** button to save any changes you may have made in a property page without closing the property page, like the OK button. When you create a new object in Interaction Administrator, the Apply button is not available until after you click the OK button and open it the second time. The Apply button is available all the time, but it knows if you have already saved something; it will not write the same saved data again.

Site name

The site name is specified during the IC Server installation procedure and cannot be changed from within Interaction Administrator. The server name is automatically detected during IC Server installation and this name is inserted in Interaction Administrator.

> **Caution:** If you need to change the site, configuration (Production), or server name settings after you install IC Server, use the Setup Assistant. For more information, see the IC Setup Assistant help.
>
> If a PureConnect Customer Care representative gives you specific instructions to edit these settings in the registry, use only DSEdit to make the recommended changes. If you incorrectly change these settings, you could adversely affect the performance of CIC or prevent it from functioning properly.

License information.

The Interaction Administrator screen displays how many days you have to renew your license before expiration in the lower left-hand corner.

A message is shown requesting the system administrator re-register the license file prior to the license anniversary date. If license renewal is due within a specific time period, a message is displayed similar to "Your license is due for its annual re-registration in XX days. Please visit http://license.inin.com to re-register your license."

Other licensing messages are displayed as well. For example, in a non-Switchover environment, you may see "The new license file was successfully published to this server.", or "The new license file failed to apply to this server. Contact PureConnect Customer Care for further assistance."

Related Topics

Overview of how to add users

Auto Save feature

Exporting configuration data

Updating configuration values

11/09/2018
CIC 2018 R4

Containers list

The following table describes the containers and subcontainers in Interaction Administrator.

If a listed container does not appear in your copy of Interaction Administrator, it may mean that you have not installed the release of CIC or functionality that requires that container, or it may mean that you do not have rights to the container.

Configuration Container	Description
Collective	If you have installed Interaction Multi-Site, this is the container in which you can configure several Multi-Site behaviors.
Collective: **Home Site**	Configures the site identifier and password for this CIC server.
Collective:**Peer Sites**	Identifies other CIC servers in the collective and allows you to check connectivity and synchronize with those sites.
Server (your CIC server Name)	Configures the handlers, report logs, accumulators, and several other settings to run on this server. **Note**: When Interaction Administrator is connected to a backup server in a switchover pair, and you are connected to the backup server, the name of the server appears with the label "(Backup)."
Server:**Lines**	Configures digital lines for the server.
Server:**Line Groups**	Defines line groups and dial groups based on configured lines.
Server:**Stations**	Configures workstations, fax stations, stand-alone phones, or any other kind of station information including extension, board number, port number, etc.
Server:Stations: **Templates**	Configures the default behavior of stations by the type of station, such as standalone phone or workstation.
Server:Stations:**Groups**	Creates station groups so that you may transfer a caller to a specific group of stations.
Server:Stations:**Default Station**	Configures default station settings globally, including SIP stations settings.
Server:**Managed IP Phones**	Configures and manages IP phones.

Server:Managed IP Phones:**Templates**	Configures the default behavior when importing or creating new individual managed IP phones.
Server:Managed IP Phones:**Ring Tones**	Configures ring tone behavior for managed IP phones.
Server:Managed IP Phones:**Default IP Phone**	Configures the default IP phone provisioning line.
Server:Managed IP Phones:**Registration Groups**	Configures the settings used when provisioning managed IP phones.
Server: **SIP Bridges**	Configures connectivity paths (SIP bridges) between remote users and the CIC server.
Server: **Audio Sources**	Configures sources that continuously transmit audio and can be listened to simultaneously by multiple calls.
Server:**Server Parameters**	Defines parameters used by handlers and CIC subsystems for this server.
Server:**Structured Parameters**	Defines typed, grouped parameters that are used by handlers and CIC subsystems for this server.
Regionalization	Defines region-specific configuration options, such as locations.
Regionalization: **Locations**	Defines locations and endpoints (lines, stations, and servers) that share a common dial plan and sets the codec mappings for the endpoints.
Regionalization: **Default Regionalization**	Sets the default server location and conference settings.
Regionalization: **Selection Rules**	Configures rules that are used for prioritizing server use, per location.
Licenses Allocation	Displays licenses and their allocations based on users and stations.
People	Contains subcontainers where you configure users, workgroups, roles, and related

	functionality.
People:**Default User**	Controls user options, basic security and access control for all users, workgroup members, and roles. All users, workgroup members, and roles inherit these properties.
People:**Roles**	Defines roles, which are reusable sets of basic security settings and access control settings. You use roles to easily configure standardized security and access control levels for users and workgroups.
People:**Users**	Controls workgroups, options, basic security, ACD features, access control, etc., for each user.
People:**Workgroups**	Controls members, options, basic security, ACD features, and access control for workgroups.
People:**Password Policies**	Configures security policies for use with CIC passwords and apply these policies per role or user.
People:Password Policies:**Policies**	Defines new policies.
People:**Schedules**	Creates and configures schedules used to schedule menus in Interaction Attendant.
People:**Secure Input Forms**	Defines forms that Agents use to collect confidential customer information.
People: **Wrap-up**	Defines categories and codes that indicate the nature of interactions for reporting purposes.
People: **Wrap-up Categories**	Defines groupings of wrap-up codes for reporting and other purposes.
People:Wrap-up:**Wrap-up Codes**	Defines wrap-up codes that Agents associate with interactions to indicate the nature of the interaction.
People:**Client Buttons**	Configures buttons to appear in the CIC clients that open an application or invoke a custom handler.

People:**Client Configuration**	Defines templates that specify the CIC client configuration and apply these templates to users.
People:Client Configuration:**Templates**	Defines new templates.
People: **Queue Columns**	Configures which fields can be displayed in Interaction Client's **My Interactions** page.
People:**Account Codes Configuration**	Enables the account code feature for tracking incoming and outgoing calls.
People:Account Codes Configuration:**Account Codes**	Creates and configures account codes optionally used for incoming and outgoing calls.
People:**Client Templates**	Defines templates that determine how the CIC clients should look and behave. The templates can be assigned to multiple agents to simplify the installation and configuration of their stations.
People:**Response Management**	Creates a library of predefined responses that agents can use in chat sessions, email messages, and callbacks.
People:Response Management:**Import Documents**	Imports previously exported response management documents into the library of responses.
People:**Skills**	Defines ACD skills to assign to users or workgroups.
People:**Access Control Groups**	Provides a flexible way to group CIC objects in order to assign administrative access rights to users and workgroups.
System Configuration	Controls default mailbox accounts, languages, and host server configuration.
System Configuration:**Interaction Processor**	Configures handlers in Interaction Processor.
System Configuration:Interaction Processor:**Handlers**	Lists handlers active on the server.
System Configuration:Interaction	Lists initialization functions used by CIC

Processor:**Initialization Functions**	handlers (**do not modify these functions**).
System Configuration:Interaction Processor:**Tables**	Enables you to create in-memory tabular databases for fast lookups on static data by handlers
System Configuration:**Phone Numbers**	Defines dial plans, dialing classifications, and phone number processing.
System Configuration:**Report Logs**	Defines report logs that capture all call data. Several standard logs are bundled with CIC.
System Configuration:**Accumulators**	Defines accumulators used to hold numbers of system events for tracking and monitoring system performance.
System Configuration:**System Parameters**	Defines parameters that are used by handlers and CIC subsystems on all servers across the system.
System Configuration:**Status Messages**	Defines status messages and their attributes that appear in the CIC clients in the Status box (e.g., At Lunch, Available, etc.).
System Configuration:**Actions**	Defines DDE actions and commands that can be invoked when a call connects or disconnects.
System Configuration:**Log Retrieval Assistant**	Configures how logs are retrieved through Log Retrieval Assistant.
System Configuration:**Mail**	Defines multiple mail storage sources.
System Configuration: **Single Sign-On**	Enables users to securely log in to CIC applications through third-party authentication providers.
System Configuration: Single Sign-On: **Secure Token Server**	Configures the Secure Token Server, which grants authenticated users access to specific CIC applications.
System Configuration: Single Sign-On: **Identity Providers**	Configures the Identity Providers, which authenticate login requests from users.
System Configuration: **Interaction Process**	Activates and deactivates published Interaction

Automation	Process Automation processes.
System Configuration: Interaction Process Automation:**Security Specifications**	Controls access to process-level variables in an Interaction Process Automation process.
System Configuration: **Interaction Feedback**	Configures settings for survey recordings.
System Configuration:**Fax**	Controls the fax appearance, cover page, and other options.
System Configuration:Fax Configuration:**Fax Groups**	Defines fax groups when multiple fax resources are available to be dedicated to specific purposes (e.g., inbound, outbound, etc.)
System Configuration:**IC Data Sources**	Defines external data sources CIC uses for report logs, contact databases, etc.
System Configuration:**Contact Data Manager**	Controls general resources used by the Contact List Sources.
System Configuration:Contact Data Manager:**Contact List Sources**	Specifies CIC data sources to use for creating contact lists that integrate with CIC clients.
System Configuration:**Web Services**	(Available with Web add-on license, IC Web Services installed.) No configuration dialog exists for Web Services. You can, however, configure five parameters using the Parameters folder in the Web Services container.
System Configuration:Web Services:**Web Services Parameters**	(Available with Web add-on license, IC Web Services installed.) Lets you configure parameters including the join and leave messages for Chats, the CIC server name displayed for the agent's side of Chats (you might put your company's name here), the Web Services port number, and the time that visitor's URLs will remain in the Web Sessions tab after they have left the website.
System Configuration:**Recognition**	Configures the behavior of all speech recognition servers.
System Configuration:Recognition:**Loquendo**	Configures the behavior of all Loquendo speech recognition servers.
System	Configure the behavior of each individual

Configuration:Recognition:**Loquendo:Servers**	Loquendo speech recognition server.
System Configuration:Recognition:**Interaction Speech Recognition**	Configures the behavior of all Interaction Speech Recognition servers.
System Configuration:Recognition:**MRCP**	Configures the behavior of all MRCP speech recognition servers.
System Configuration:Recognition:MRCP:**Servers**	Configures the behavior of each individual MRCP speech recognition server.
System Configuration:Recognition:**Nuance Recognizer**	Configures the behavior of all Nuance speech recognition servers.
System Configuration:Recognition:Nuance Recognizer:**Servers**	Configures the behavior of each individual Nuance speech recognition server.
System Configuration:**Media Servers**	Configures stand-alone media servers to record and monitor calls on media server devices, as well as play on-hold music to callers connected with a media server device.
System Configuration:Media Servers:**Servers**	Sets the location and other server-specific details for each media server.
System Configuration:**SIP Proxies**	Configures the settings for each SIP proxy.
System Configuration:**MRCP Servers**	Configures options for all MRCP servers including the protocol and network adapter
System Configuration:MRCP Servers:**Servers**	Configures the SIP address, location, priority, and capabilities of each MRCP server.
System Configuration:**Session Managers**	Configures the settings for all Session Manager servers.
System Configuration:Session Managers:**Servers**	Configures the settings for each Session Manager server. These settings include the FQDN, the acceptable connections, and the server location.
System Configuration:**SMS**	Configures behavior of Short Message Service messages.

System Configuration:SMS:**Brokers**	Defines connection with a broker.
System Configuration:**Problem Reporter**	Enables an authorized user to report a problem with a CIC client to the user's support representative.
System Configuration: **Problem Reporter**	Enables an authorized user to report a problem with a CIC client to the user's support representative.
System Configuration: **Layouts**	Identifies station locations on floor plan images.
Interaction Tracker	Configures Interaction Tracker behavior that displays views of interaction history.
Interaction Tracker:**Individual Types**	Defines individual types such as Marketing Director.
Interaction Tracker:**Organization Types**	Defines organization types such as Marketing.
Interaction Tracker:**iAddress Types**	Defines iAddress types such as Home or Mobile.
Interaction Tracker:**iAddress Subtypes**	Defines iAddress sub-types to extend iAddress type such as Home 1 and Home 2.
Interaction Tracker:**Tracker Attribute Types**	Defines attribute types for individuals, locations and organizations to extend these types.
Interaction Tracker:**Tracker Address Types**	Defines address types such as billing or shipping.
Interaction Tracker:**Titles**	Defines titles such as Mr. or Mrs.
Interaction Tracker:**Read-only Data Sources**	Designates read-only data sources, so that Data Manager does not modify them.
Interaction Recorder	Configures what interactions are recorded and how interactions are recorded.
Interaction Recorder:**Policy Editor**	Creates policies that manage recordings.
Interaction Recorder:**Screen Recording**	Configures Interaction Screen Recorder.
Interaction Recorder:**Remote Content Server**	

Interaction Optimizer	Configures Activity Types, Day Classifications, and Scheduling Units to prepare Forecasts and Schedules for Real-time Adherence.
Interaction Analyzer	Defines the keywords that Interaction Analyzer uses to monitor conversations between agents and customers.
Interaction Analyzer:**Keyword Sets**	Organizes keywords into logical groups.
Report Management	Configures custom reports that are run in Interaction Reporter in IC Business Manager.
Report Management:**Report Configuration**	Manages report metadata.
Report Management:**Report Configuration Export**	Exports report configuration metadata to an XML format file.
Report Management:**Report Configuration Import**	Imports report configuration metadata from an XML format file.
Report Management:**Report System Settings**	Configures the first day of a customer's work week and sets the report timeout value.

Menu Commands

The menu bar includes commands on each of the **File**, **Edit**, **View**, **Context**, and **Help** menus. The following information describes the most important menu bar commands. Available commands vary according to the selected container.

File

The **File** menu includes the **Export**, **License Management**, and **Exit** commands.

Export dumps the existing CIC configuration data into a `.csv` file, which can then be opened with Excel.

License Management To update CIC licenses, click this command to display the **License Management** dialog.

The **Exit** command closes Interaction Administrator.

Edit

The **Edit** menu includes the **Copy** (Ctrl+C) and **Paste** (Ctrl+V) commands to copy and paste (with a new name) configuration entries. Copy and Paste work for all entries except Skills and Report Logs.

The menu also includes the following standard **New Entry (Insert)**, **Delete Entry (Delete)**, and **Properties (Enter)** commands:

Command	Description
New Entry (Insert)	Requires that you select a configuration container in the tree view. Newly inserted items are added to the bottom of the list.
Delete Entry (Delete)	Requires that you select one or more configuration entries in the list view. A Delete leaves the previous item in the list selected.
Properties (Enter)	Requires that you select only one configuration entry in the list view.

View

The **View** menu includes the following commands:

Filter Bar (F3)

Jump to/from filter Bar (Shift+F3)

Clear Filter Bar (Alt+F3)

Expand Tree

Select this command to expand the tree and to show all branches.

Initial Tree

Select this command to revert the initial tree view that is displayed when you start Interaction Administrator. The initial tree view displays the top-level (Production) as expanded and displays all sibling containers under Production.

Collapse Whole Tree

This command collapses the entire tree showing only Site.

Refresh (F5)

This command causes Interaction Administrator to read the directory services data and to refresh the entries in the list view. The list view does not redraw the list after every time you insert, delete, or modify an entry. The list view is refreshed only when you use the **Refresh (F5)** command, sort the columns, or when you select a new branch in the tree view.

Toolbar

This command controls (toggles) the appearance of the toolbar icons near the top of the Interaction Administrator window.

Status Bar

This command controls (toggles) the appearance of the status bar at the bottom of the window.

The **Status Bar** and **Toolbar** commands control (toggle) the appearance of the status bar at the bottom of the Interaction Administrator window, and the toolbar icons near the top of the window.

Context

The **Context** menu displays different commands, depending on whether Lines , Stations, or Users entries are displayed in the list view.

Help

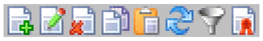
Use the Help menu to display Help topics for Interaction Administrator and information for your CIC release.

Selection Commands

In the list view window, as well as most list boxes in the configuration pages, you can select one or more entries in the list using the standard Windows control keys. This allows you to delete multiple entries, or perform some context sensitive actions on a group of entries. Use the standard Windows GUI commands to select multiple rows (for example, hold the Shift or Ctrl key while selecting rows with the mouse.)

Toolbar Commands

Interaction Administrator includes an optional toolbar, which you can control from the View menu’s Toolbar command. The toolbar provides the following icon commands:



New Entry (Insert)

Properties (Enter)

Delete Entry (Delete)

Copy

Paste

Refresh

Filter

License Management

Right-Click Menu Commands

In the list view window, right-click displays a context sensitive menu to perform basic editing operations. This menu is populated with three static entries - New (Insert), Delete (Delete) and Properties (Enter). These commands are also available on the Edit menu and the Toolbar icons. A few types of configuration data support additional right-click menu commands in the list view. These include:

Lines

Line objects have three additional entries in the context sensitive menu. These commands work on multiple entries.

Command	Description
New	Create a new SIP line.
Delete	Remove the selected line or lines.
Set Active	Can be On or Off to activate or deactivate the selected lines. The line can not be deactivated if there are any active calls on the line. Some changes to SIP lines require deactivation and reactivation in order for changes to take affect.

Stations

Station objects have one additional entry in the context sensitive menu. This action can be performed on multiple entries.

Command	Description
Set Active	Can be Yes or No to activate or deactivate the selected stations.
Set to Template	Sets the station to a specific station template values.
Set Preferred Language	Select the preferred language for the prompts for the selected station(s). The default setting is <System Default>.
Auto Extensions	Changes the extensions of the selected station(s).
Rename Station	Renames the selected station.
Change Station Type	Changes the station type of a selected station (workstation, stand-alone phone, or stand-alone Fax).
Station Assistant	Opens the Station Assistant.
Change Station Columns to View	Opens a dialog box to select the columns to view.
Managed IP Phone Properties	Opens the properties of a managed IP phone.

Users

Users' entries have one additional item in the context sensitive menu. This action can be performed for multiple entries.

> **Note:** If you enabled the Enhanced Interaction Administrator Change log, then all of your changes made through these menu items are tracked in that log. For more information, see *About the Enhanced Interaction Administrator Change Log*.

Command	Description
Set Status	Select a status from the sub-menu (for example, **At Lunch**.) for the selected user(s). **Note**: In Interaction Administrator, you can change an agent's current status to another status only if the current status is persistent.
Set Password...	Set passwords for Exchange or LotusNotes user(s) and set password options.
Set Auto-Answer ACD Calls	Select Yes or No to change the auto-answer ACD calls setting. This also can be set (checked or unchecked) on the ACD tab under Options.
Set Auto-Answer non-ACD Calls	Select Yes or No to change the auto-answer non-ACD calls setting.
Set Unified Messaging Destination	Select the server destination for messages when using SIP diversion. **Note**: For more information on configuring CIC to use UM, see *Unified Messaging Integration with CIC Technical Reference* in the PureConnect Documentation Library on the CIC server.
Set Preferred Language	Select the preferred language for the prompts for the selected user(s). The default setting is <System Default>.
Set Time Zone...	Sets the Time Zone... for the selected users.
Set Location	Sets the location of the selected users.
Set User's NT Domain Name	Click this option and type the name of the domain used to connect their user to the CIC server, (i.e., i3 domain), and then click OK.
Reset Failed Login Count	Click this option to reset the count to 0, so that the user is no longer locked out of the system.

Managed IP Phones

The following commands may be performed from the right-click menu in the managed IP phones list:

Command	Description
Change Multiple IP Phones	Change options on multiple IP phones.
Reload Now	Reloads the selected managed IP phone(s) now.
Reload at a Scheduled Time	Reloads the selected managed IP phone(s) at a scheduled time .
Cancel Scheduled Reload	Cancels a scheduled reload of managed IP phone(s) and reverts phone to it's previous status.
Reload All (Reload Required) Now	Reloads the managed IP phone(s) now that require a reload.
Unprovision	Unprovisions the managed IP phone(s) so that the phone can not be used. For example, you might want to unprovision a managed IP phone if an employee leaves the company, and a new employee is going to use the phone. Unprovision it and it will be waiting to be provisioned for the next person. **Notes**: Clearing the MAC or computer name will also cause the phone to become unprovisioned.
Set Active	Can be Yes or No to activate or deactivate the selected stations.
Set Preferred Language	Sets the language for all prompts for this managed IP phone. Can be set to <System Default> or any other languages that have been installed.
Set Custom Attributes	Define Custom Attributes for the selected IP phones.
Set Time Zone...	Sets the Time Zone... for the selected IP phones. *This option is reserved for a future release.*
Set Location	Sets the location of the managed IP phone.
Set to Template	Sets the managed IP phone options to a specific station

	template's values .
Managed IP Phone Assistant	Opens the Managed IP Phone Assistant .

Media Servers

The following command may be performed from the right-click menu in the Media Servers list:

Command	Description
Set Location	Sets the location of the media server.

SIP Proxies

The following command may be performed from the right-click menu in the SIP Proxies list:

Command	Description
Set Location	Sets the location of the media server.

MRCP Servers

The following command may be performed from the right-click menu in the MRCP Servers list:

Command	Description
Set Location	Sets the location of the media server.

About Interaction Administrator

Click the **About Interaction Administrator** button to display information about the CIC release. In addition, you can display details about Customer Interaction Center's environment and the environment of your computer.

Auto Save feature

Most of the time, using the » (next) and « (previous) browse buttons to view configuration data in a list (for example, the list of CIC users) displays the next or previous dialog immediately, unless you made changes to the settings. However, in a certain situation, CIC may display the Auto Save dialog box and ask, "Do you want to save changes?" even if you did not make any changes. This can occur if a new release of CIC is installed and new attributes are supported in the registry.

> For example, if a new field is added to the Line object in a new release of CIC, the next time a line entry is opened and the »button is clicked, the Auto Save dialog box appears and asks "Do you want to save changes?" even though nothing was changed on the dialog.

This happens because Interaction Administrator looks at all fields currently in Directory Services (that is, the registry). When Interaction Administrator decides whether or not to save the configuration data for that page, it checks all fields that can be written against what is currently in the registry. Since a new field was added to Interaction Administrator in the patch release, it detects a difference and assumes the user changed something. As a result, the Auto Save dialog asks, "Do you want to save changes?" If you select "Yes," Interaction Administrator will not display the dialog for that property page again, unless you make a change.

System security for IA

System security for CIC

CIC is a Windows Server-based communication system that takes advantage of NT Advanced Server (NTAS) security features built into the operating system. CIC also uses encrypted passwords, implicit and explicit login procedures, and it provides other mechanisms to prevent the abuse of CIC accounts and toll fraud practices. Toll fraud is a common abuse of phone system privileges where employees and external thieves use corporate resources for long distance phone charges. To control telephone access, CIC allows you to define patterns or groups of phone numbers for any number of dialing destinations (for example, Local Calls, Emergency Calls, In State, International, etc.), called "classifications." It also allows you to assign zero or more of these classifications to all users, individual users, all members of a workgroup, or any station (for example, stand-alone telephone) defined in CIC an organization or organizational group . This approach gives CIC administrators complete control over which users and stations are allowed to dial certain numbers.

Using Interaction Administrator, CIC administrators can control which parts of the CIC clients appear on each agent’s computer, and which telephone features each agent may use. A CIC Master Administrator can also give limited CIC administration controls to trusted users who have access to Interaction Administrator.

The following sections provide an overview of several security considerations. For more information about CIC security considerations that may affect your environment, see the *Interaction Center Security Features Technical Reference* in the Documentation Library.

Basic Precautions

To minimize opportunities for toll fraud or sabotage to the CIC server, follow these basic precautions in any CIC installation.

- CIC client users should log out each day or evening before going home. To be safe, CIC users should lock their desktops or completely log out of the operating system to prevent unauthorized users from starting the CIC clients and gaining dialing privileges. As long as a CIC client user’s workstation is logged in to the CIC server, that workstation’s telephone can be used to make any kind of call that user has privileges to make, even if the user’s computer is password protected.
- Configure each CIC user account with that user’s NT domain account (see the User Configuration page in Interaction Administrator) to enable NTAS account/password security. See the *CIC Account Authentication* section below for details on how this works.
- Unless it is absolutely necessary, do not modify the IC DialPlan handler to require all users to dial a single digit (for example, 9) to dial an external number. This scheme is prone to the bogus "test your line" phone scam where a caller falsely representing the phone company asks an unsuspecting operator to press the keys 9, 0, and # and then hang up in order to conduct a line

test. Doing so gives the caller access to that line. CIC can intelligently select the appropriate lines (that is, dial groups) for external calls; CIC does not require a prefix digit to "get an outside line."

- Control access to the corporate toll free line, and follow the precautions described in the Toll Fraud Prevention topic to prevent remote callers from abusing CIC’s powerful remote access capabilities.
- To enhance security and simplify the process updating CIC, ensure that each CIC user account name identically matches the user's corresponding NT domain account name. This name convention is not a requirement, but it will enable you to take advantage of improved security features.

Fraud, authentication, and passwords

Toll Fraud

See the Toll Fraud Prevention topic for a detailed discussion on preventing toll fraud by employees who may choose to abuse CIC’s powerful remote access features.

CIC Account Authentication

Each CIC user account generally corresponds to a network domain account established on a Windows server. This network account usually has an email account on a mail server (for example, Microsoft Exchange Server) on the network. CIC user accounts can exist apart from a network account, but those CIC users will not have access to CIC’s unified messaging features, and they must explicitly log in to CIC with a CIC password each time they connect to the IC server. The most efficient, and recommended, way for CIC users to connect to CIC is via an implicit login using a valid network account. CIC performs implicit or explicit account validation the first time a CIC user starts a client application (for example, the CIC client, voice mail form, Interaction Fax Viewer, and so on.) The implicit login process uses NTAS to verify the CIC user has a valid NT domain account, and is thereby automatically authenticated to the CIC server.

Login Authentication Cache

During the initial account authentication process, that account’s login information is cached on the local client workstation, if the login was successful. CIC applications started after that they do not require manual validation because they use the cached login information by default. For example, if you successfully start Interaction Client Fax Viewer and then later choose to start Interaction Fax Viewer or use the MAPI voicemail form, those CIC client applications will not need to be authenticated by the CIC server because the user’s login information is cached on the client workstation.

You can manually start some CIC applications with /User= and /Password= command line arguments, which override the cached login names. When an CIC user logs out of the operating system, or restarts the computer, the login account cache is destroyed. Just logging out of CIC does not destroy the user cache. If a user encounters a problem logging in to CIC, you can manually clear the client workstation’s login cache by closing the process named I3aca.exe on that workstation.

Implicit Login

Implicit login allows properly configured CIC users to be authenticated on the CIC server via the user’s NT domain account. When someone logs in to a network domain, that person is authenticated on the network via NTAS. CIC Client applications can take the domain/account name used to log in to a workstation and compare it with a list of domain/account names entered in the CIC user’s configuration in Interaction Administrator. If a match is found, the IC Client application is automatically authenticated.

This works only if the Domain User field is properly completed in Interaction Administrator for the users starting CIC applications. If it does not find an exact match between the client's domain/user name and the user configuration data on the CIC server, the login is denied and the client application can prompt the user to manually log in. Click here for more details.

Implicit login requires that each CIC user's Configuration page has the NT Domain User field correctly filled in with the text:

DOMAIN/UserName

The DOMAIN portion is the name of the network domain the CIC server is on, and the CIC user accounts have access to (for example, I3Domain). The UserName portion is the network user's account name (for example, KevinK). If the NT Domain User field is not filled in (for example, I3domain/Kevink), users must log in to CIC manually.

Explicit Login

CIC client applications can manually log in to the CIC server in two ways.

- Some CIC client applications can use /User and /Pass command line arguments
- If implicit login fails, CIC client applications present the Login dialog

Some applications, like snteraction Fax Viewer and Fax Monitor cannot be started with user name and password arguments. However, the CIC clients, Interaction Administrator, Interaction Designer, and several other CIC client applications can be started from a command prompt with command line arguments that specify the CIC user name and password. For example:

```
C:> clienta /user=sonyam /password=123 /notifier=I3server
```

If CIC finds a CIC user named "sonyam" with a CIC password of "123" defined on the CIC server, the login is successful and the login data is cached on client workstation for subsequent connections. However, if the user name or password is not authenticated (for example, the wrong password is entered), CIC displays a login dialog to prompt the user, as shown below:

In the Login dialog box, enter a valid CIC user and server configuration data:

- **IC Username** A valid CIC account name (such as, milanv)
- **Password** The CIC password for this account (such as, 1234)
- **Server** The name or IP address of the CIC server (such as, I3Server)

Password Encryption

While passwords entered on a command line are visible, and therefore vulnerable, at that point, passwords are concealed on the Login dialog box. In both cases, passwords are immediately encrypted before they are passed across the network; they are not passed as clear text. Passwords are stored in an encrypted format in the registry on the CIC server and are therefore not readable by editing the registry. If a CIC user forgets his or her unique password, the CIC administrator must enter a new password for that user in the User Configuration page in Interaction Administrator.

Related topics

Overview of security for people

Client Admin Components Login Details

Toll Fraud Prevention

Toll Fraud Prevention

Toll fraud is the theft of long distance service. A common type of toll fraud involves employees who use company phones in an unauthorized manner to make personal long distance calls. Because CIC is capable of performing many different telephone operations, CIC administrators should know that under certain conditions employees could use CIC features to commit toll fraud.

This topic addresses ways that CIC features could be used to commit toll fraud, and ways that CIC could be configured to prevent such abuses. This does *not* cover possible toll fraud activities that only a system administrator could commit (for example publishing rogue handlers), or toll fraud activities that could be performed on an ordinary telephone system (for example using stolen phone access codes).

> **Note:** All the toll fraud activities described in this topic occur in the context of an employee calling into the company's phone system on a corporate toll-free number.

Reply to a voice mail from a long distance caller

Description

An employee calls into the CIC's auto attendant system via a corporate toll-free number. The employee listens to a personal voice mail message from a long distance caller. Upon playing the message, the CIC auto attendant system allows the employee to reply back to the message, which the employee chooses to do. CIC dials the long distance number, the call connects, and it is charged to the company bill.

Prevention

You can prevent this type of toll fraud by blocking the employee from initiating all long distance calls, including the ability to reply to long distance calls. In Interaction Administrator you can set Basic Security rights so that the employee does not have the option to initiate Long Distance, International, or 900 Service calls. These rights can be set for an individual user, a workgroup, or the entire company. For more information, see the Configuration Property Inheritance and User Rights.

Set the forward number to a long distance number

Description

An employee sets the user status to **Available, Forward**. However, the forward number the employee enters is the long distance number of a friend that the employee wants to call. Later, the employee calls his/her own extension via a corporate toll-free number. CIC automatically forwards the call to the friend's long distance phone, the call connects, and it is charged to the company bill. For more information, see the help for the CIC clients.

Prevention

Again, the key to preventing this type of toll fraud is to block the employee from initiating long distance calls, which includes forwarding a call to a long distance number. Interaction Administrator allows you to set Basic Security rights so that the employee does not have the option to initiate Long Distance, International, or 900 Service calls. These rights can be set for an individual user, a workgroup, or the entire company. For more information, see the Configuration Property Inheritance and User Rights help.

Set the forward number to a local number and call from long distance

Description

An employee sets the user status to **Available, Forward**. However, the forward number the employee enters is a friend's local phone number. Then, from a long distance number (for example while on vacation in another state) the employee calls his/her own extension using a corporate toll-free number. CIC automatically forwards the call to the friend's local number and the call connects. For more information, see the *Forward Calls* help topic in Interaction Client.

This scenario is similar to the previous one. However, instead of CIC forwarding a call from a local number to a long distance number, now CIC is forwarding a call from a long distance number to a local number. In either case, the result is the same—the employee has used a company phone line to make an unauthorized long distance call.

Prevention

Preventing this type of toll fraud activity requires you to block the employee from setting the forward number to a local external number. There are several ways to do this:

- Block the employee's ability to configure the Interaction Client

  One simple way to prevent this type of toll fraud is to block the employee from making ***any*** configuration changes to the Interaction Client, including the ability to set a forward number. In the Interaction Administrator you can set the Basic Security rights so that the employee does not have the rights to view and modify the Configuration Page on Interaction Client. You can set these rights for an individual user, a workgroup, or the entire company. For more information, see the Configuration Property Inheritance and User Rights help topics.

- Remove the "Available, Forward" status

  Another simple way to prevent this type of toll fraud is to completely remove the **Available, Forward** status. In Interaction Administrator's **Status Messages** container, you can delete this status. This solution is more extreme because removing a status can be performed only on a *global* level. In other words, if you remove this status for one employee, it will also be removed for the entire company. For more information, see the User Configuration help topic.

- Configure CIC so that it forwards calls only to internal numbers

  A final way to prevent this type of toll fraud is to configure CIC so that ***all*** employees—both those in and out of the office—must set their forward numbers to internal extensions. Again, this prevents the forward number feature from being abused, while still allowing it to be used for work related purposes. To configure CIC so that it requires all employees to set their forward numbers to internal extensions, insert a lookup step in the **SystemIVRRemoteEmployee** handler. The lookup step should check to see if the forward number is a valid extension. If it is valid, the handler would allow the employee to set personal attributes; if it is not valid, the handler could play an "Invalid Number" message and permit the employee to reenter the forward number. For more information on this handler, see the *SystemIVRRemoteEmployee* help topic in Interaction Designer.

Related topics

System security for CIC

Client Admin Components Login Details

The first time a CIC client application is started (without explicitly passing a CIC user name and password) after logging in to the network domain, the application calls the EICAuth COM object on the CIC server. The EICAuth program attempts to authenticate the network domain user who started the application. At this point, the Notifier compares the NT Domain User field values (see the User Configuration property page in Interaction Administrator) stored on the CIC server with the domain/account name in use on the client workstation. If it finds an exact match, the CIC client connection succeeds and the login authentication information for that user is cached on the client workstation for subsequent logins (during the remainder of the current Windows session). If the Notifier does not find an exact match between the client's domain/user name and the user configuration data on the CIC server, the login is denied and the client application can prompt the user to manually log in.

Related topics

System security for CIC

Collective

Collective concepts

A collective is a group of CIC servers that communicate with each other and that share resources. In a collective, CIC servers act as **home sites** and **peer sites**.

The **home site** for a user depends on the user's configuration. By default, a user's home site is the site that the user is logged on to. However, you can configure a "permanent" home site for a user, if necessary.

The collective for a user looks different on each of the CIC sites that the user logs on to. For example, suppose that CIC servers in Indianapolis, Indiana, Deerfield Beach, Florida, and Aix, France, all communicate with one another. For example, if a user logs on in Indianapolis, then Indianapolis is the user's home site and Deerfield Beach and Aix are peer sites.

A user in a collective can log on to any of the collective's sites. For example, a user in Indianapolis can see whether or not another user in Deerfield is on the phone. If a user visits Indianapolis, someone dialing that user's extension from any of the other sites is automatically connected to the phone that person is currently logged on to in Indianapolis. When new users are added in any of these cities, the users automatically appear in the company directory, which is viewable from all of the other cities.

A user can be shared between the collective site and workgroups that span the collective. User data is replicated between collective sites, but not all users are replicated. Only users that are members of spanning workgroups are replicated.

All calls or workgroup-related activity for the user are routed to the last CIC site the user logged on to.

For more information, see the *Multi-Site Technical Reference* document in the PureConnect Documentation Library on your CIC server.

Overview of the process to set up a collective

To set up a collective, in the **Collective** container, use the **Home Site** subcontainer to configure the home site. Then use the **Peer Sites** container to add one or more peer sites.

Related topics

Home site concepts

Configure a home site

Peer site concepts

Add a peer site

Configure a peer site

Configure trusted access for a peer site

User extensions that span peer sites

Collective concepts

A collective is a group of CIC servers that communicate with each other and that share resources. In a collective, CIC servers act as **home sites** and **peer sites**.

The **home site** for a user depends on the user's configuration. By default, a user's home site is the site that the user is logged on to. However, you can configure a "permanent" home site for a user, if necessary.

The collective for a user looks different on each of the CIC sites that the user logs on to. For example, suppose that CIC servers in Indianapolis, Indiana, Deerfield Beach, Florida, and Aix, France, all communicate with one another. For example, if a user logs on in Indianapolis, then Indianapolis is the user's home site and Deerfield Beach and Aix are peer sites.

A user in a collective can log on to any of the collective’s sites. For example, a user in Indianapolis can see whether or not another user in Deerfield is on the phone. If a user visits Indianapolis, someone dialing that user’s extension from any of the other sites is automatically connected to the phone that person is currently logged on to in Indianapolis. When new users are added in any of these cities, the users automatically appear in the company directory, which is viewable from all of the other cities.

A user can be shared between the collective site and workgroups that span the collective. User data is replicated between collective sites, but not all users are replicated. Only users that are members of spanning workgroups are replicated.

All calls or workgroup-related activity for the user are routed to the last CIC site the user logged on to.

For more information, see the *Multi-Site Technical Reference* document in the PureConnect Documentation Library on your CIC server.

Overview of the process to set up a collective

To set up a collective, in the **Collective** container, use the **Home Site** subcontainer to configure the home site. Then use the **Peer Sites** container to add one or more peer sites.

Related topics

Home site concepts

Configure a home site

Peer site concepts

Add a peer site

Configure a peer site

Configure trusted access for a peer site

User extensions that span peer sites

Home Site

Home site concepts

Use the **Home Site Configuration** tab to define the specific characteristics of a CIC server that is participating in a collective as a home site.

If you have multiple CIC servers at different sites that need to send the output of their report logs to a single database server via a LAN, WAN, or some other remote connection, configure a unique site identifier for each site in the **Home Site** container. All CIC report logs include a SiteID column to identify the site for each row of data in the logs.

For example, suppose a company has three call center offices. Each site uses CIC. The headquarters office has a central SQL Server machine that hosts all of the call center report logs. To uniquely identify each call center in the report log data, assign a unique site identifier to each site. Also, configure the data source for each CIC server to point to the central database server that hosts the CIC SQL Server database.

To ensure that all report log data is captured correctly, implement and test this part of the site configuration before you start the CIC server.

> **Note:** For a multi-site reporting system, configure the CIC data source for each of the CIC servers on the network to point to the same SQL server. Then populate the **ServerReportLogDataDestination** CIC server parameter with the following value:
>
> PMQ:<The name of the IA data source that points to the SQL server>

Related topics

Configure a home site

Collective concepts

Configure a home site

To configure a home site

1. In the **Collective** container, double-click the **Home Site** container.
2. In the list view window, right-click **Configuration**.
   The **Home Site Configuration** dialog box appears.
3. In the **Site Identifier** box, type a number that uniquely identifies this site. This number appears in all CIC report logs and can be used to create custom queries that isolate data for this site. The default value is 0 (zero). For the purposes of reports, a 0 means that a single CIC server is writing data to the report logs.
4. In the **Password** box, type a password for the site. Passwords are case-sensitive and can be any length or character. The next time that you open this dialog box, the **Password** and **Confirm** boxes will display 16 asterisk (*) characters, regardless of the length of the password that you type now.

   > **Tip**: You can change the password whenever you open the **Site Configuration** dialog box.

5. In the **Confirm** box, re-type the password.
6. In the **Note ID Dial String Digits** box, type a two-digit value. This value identifies a multi-site call when it is sent to a peer site through an established tie-line connection. For example, *90.
7. Do one of the following:
   - If you have a switchover environment, complete steps 8 and 9.
   - Otherwise, skip to step 10.
8. In the **Switchover Server Configuration** section, in the **Switchover Server A** and **Switchover Server B** lists, select the locations of the switchover servers. For example, you may have switchover servers in different geographic locations. This location is not the computer name. This location of a switchover server allows you to change the codecs that is associated with the server.
9. Type the server names.
10. To activate the site as a home site in a collective, select the **Activate this site to participate in a multi-site configuration** check box.
11. Click **OK**.

Related topics

Home site concepts

Collective concepts

Peer Site

Peer site concepts

You can add one or more **Peer Sites** to a collective. Each site can have its own configuration.

Related topics

Add a peer site

Configure a peer site

Configure trusted access for a peer site

Collective concepts

Add a peer site

To add a peer site to a collective

1. In the **Collective** container, double-click the **Peer Sites** container.
2. In the list view window, right-click and then click **New**.
   The **Entry Name** dialog box appears.
3. Type the name of the peer site.

> **Note:** The name of the peer site must match an existing site name.

4. Click **OK**.
   The **Peer Site Configuration** dialog box appears.
5. Configure the peer site. For more information, see *Configure a peer site*.

Related topics

Configure a peer site

Configure trusted access for a peer site

Peer site concepts

Collective concepts

Configure a peer site

These instructions assume that you have added a peer site to the collective and want to edit its configuration.

If you are in the process of adding a peer site, start with step 3.

To configure a peer site

1. In the **Collective** container, double-click the **Peer Sites** container.
2. In the list view window, right-click the name of the peer site that you want to configure.
   The **Peer Site Configuration** dialog box appears.
3. In the **Site Identifier** box, type a number or a set of numbers that identifies the peer site. The site identifier (site ID) allows peer sites to connect to one another. The default value is 0 (zero). You cannot use a host name.

4. In the **Phone Number** box, type the telephone number of the peer site. CIC uses this telephone number to route calls to a user who is logged on to the peer site.
5. In the **Password** box, type the password of the peer site. Passwords are case-sensitive. Use the password you set when you configured the site as a home site. For more information, see *Configure a home site*.
6. Do one of the following:
    - If you have a Multi-Server Administration license, complete steps 7 and 8.
    - Otherwise, skip to step 9.
7. In the **Site Address** box, type the IP address or host name for this peer site.
8. In the **Location** list, select a location. For more information, see *Locations*.
9. Sometimes peer sites are connected via tie lines as well as via PSTN. When a tie line has been established between two sites CIC has a **Tie Line Optimization** feature that allows it to process multi-site calls more efficiently. Do you want to use the Tie Line Optimization feature?
    - If yes, select the **Use Note ID Dial String** check box.
    - Otherwise, skip to the next step.
10. Press **Check Site** to verify that the peer site be reached with the site identifier and that the password for the peer site is correct.
11. Press **Synchronize** to force the local site and the peer site to synchronize.

> **Note:** If you change the peer site name or the site ID, you must press **Synchronize** in order to save the change.

12. Click **OK**.

Related topics

Add a peer site

Configure a home site

Locations

Configure trusted access for a peer site

Peer site concepts

Collective concepts

Trusted access concepts

Trusted access refers to the ability of selected users to publish and manage handlers or to act as master administrators, when they are logged on to a peer site.

> **Note:** Trusted access applies only to users who the appropriate security right(s) and access right. Fore more information, see **Security**.

When trusted access is configured, a user must have the appropriate security right(s) in order to perform the tasks:

- An Interaction Designer user must have the **Publish** right in order to update production handlers or publish new handlers on the CIC server.
- An Interaction Designer user must have the **Manager** right in order to add or remove production handlers from the CIC server.
- A user must have **Master Administrator** access in to act as a master administrator.

For information on assigning the security rights, see *Security*.

Related topics

Security

Configure trusted access for a peer site

Peer site concepts

Configure a peer site

Collective concepts

Configure trusted access for a peer site

For more information on trusted access, see Trusted access concepts.

To configure trusted access for a peer site

1. In the **Collective** container, double-click the **Peer Sites** container.
2. In the list view window, right-click the name of the peer site that you want to configure.
   The **Peer Site Configuration** dialog box appears.
3. Click the **Trusted Access** tab.
4. To allow users who have the **Publish** right for handlers to update production handlers or publish new handlers on the CIC server while they are logged on to this peer site, select the **Publish Handlers** check box.
5. To allow users who have the **Manage** right for handlers to add handlers to or remove handlers from the CIC server while they are logged on to this peer site, select the **Manage Handlers** check box.
6. To allow users who are master administrators to perform their master administrator responsibilities from this peer site, select the **Master Administrator** check box.
7. Click **OK**.

Related topics

Trusted access concepts

Peer site concepts

Configure a peer site

Collective concepts

User extensions that span peer sites

It is always important to plan for growth when you create user extensions in Interaction Administrator. Consider both the growth of your current site and the growth of other sites or other CIC systems.

> **Note:** Avoid duplicate user extensions.

When multiple CIC sites form a collective, CIC replicates user information throughout the collective. A user who spans sites (a “spanner”) on a CIC server that is part of a collective cannot have the same user extension as another spanner on another CIC server in the collective.

For example, suppose User A on Server 1 is part of a workgroup that spans sites. User A has an extension of 8001. User B on Server 2 is part of a workgroup that spans sites. User B also has an extension of 8001. When their user data is replicated throughout the collective, they will have a problem getting calls and other services.

Use careful planning if you change user extensions. The extensions must be unique if a user is added to a workgroup that spans sites. Here are some suggested approaches:

- Change the user extension altogether. For example, if User A on Server 1 had an extension of 8001, change the extension to 8801.
- Add a digit to the beginning of the user’s extension. For example, if User A on Server 1 has an extension of 8001, then change the extension to 18001. This extension means "Server 1, User A extension 8001." Likewise, if User B on Server 2 has an extension of 8001, then change it to 28001. This extension means Server 2, User B extension 8001.

Related topics

Collective concepts

Configure a peer site

Assistants

Assistants

This section contains help about the Assistants available in Interaction Administrator:

Add Stations Assistant

Add User Assistant

Add Location Assistant

Managed IP Phone Assistant

Add Location Assistant

Add Location Assistant

The Location Assistant steps you through the location configuration tasks in a linear fashion, so there is no need to manually open each related container or sub-container to complete the new location configuration.

Related topics

- Overview
- Assign Stations
- Add Gateway
- Call Routing
- Select Media Server

Location Assistant Overview

This page lists each location configuration task and provides a summary of each task. The check box next to each task indicates if the task needs to be completed (☑gray checkmark), has been completed (☑green checkmark), is optional (no checkmark), or cannot be completed without other prerequisite configuration (✘ red "X"). You can also choose a task listed on the left to further configure or examine this location's behavior.

Click **Next** to go to Assign Stations.

Related Topics:

Assign Stations

Add Gateway

Call Routing

Select Media Server

Regionalization

Assign Stations

Use this page to assign stations to this location. What the Assign Stations page displays depends on whether the prerequisite station line group SIP Station Transport configuration exists.

Station Support Exists

If station support exists, a summary of what stations are assigned to this location is displayed. Click **Add or remove stations** to modify the station members that are in the station line group assigned to this location.

No Station Support Exists

If no station support exists, you are prompted to create a station line group in the first task, Add Station Support. After adding station support, you can return to this task by selecting **Assign Stations** on the left, or clicking **Back.** Once station support exists, you can click **Add or remove stations** to modify the station members that are in the station line group assigned to this location.

Click **Next** to go to Add Gateway.

Related Topics:

Location Assistant Overview

Add Gateway

Call Routing

Select Media Server

Regionalization

Add Gateway

This page allows you to use line objects to create a SIP gateway associated with this location. Click **Add or remove gateway lines…** to open the **Assign Endpoints** dialog box. From this dialog box, you can click **Add Lines** to add lines as endpoints or to change the line endpoint memberships for this location. You can also click **Create a new line...** to create a new SIP line.

Once you add lines to the location, click **Next** to go to **Call Routing** and make sure that the dial plan is configured properly.

Related topics

Location assistant overview

Assign stations

Call routing

Select media server

Regionalization

Call Routing

This page displays a table of this location's gateway usage within the dial plan. The table displays each line, its dial group, and indicates whether it's used in the dial plan. This task helps the user set up dial plan entries to help route calls for the gateways associated with a location. If no gateways have been added, you're prompted to return to the Add Gateway task.

Click **Update the dial plan for these gateways...** to open the first page of the Dial Plan Call Routing Wizard, Select a Gateway Line and it's Dial Group. The wizard allows you to configure dial groups and specific dial plan entries.

Click **Review the current dial plan...** to open the Regional Dial Plan page in the Phone Numbers sub-container listed under the System Configuration container. The Regional Dial Plan page displays the associated attributes of the dial plan.

After updating the dial plan for the gateways, or reviewing the current dial plan, click **Next** to go to Select Media Server.

Related Topics:

Location Assistant Overview

Assign Stations

Add Gateway

Select Media Server

Regionalization

Select Media Server

Use this page to associate a media server with this location.

Add or remove media servers...

Click this link to add or remove a media server associated with this location. Select **Add** or **Remove** from the **Assign Endpoints** page.

Click **OK** to save the media server changes. Click **Close** to save all the changes made to this location and to close the Location Assistant.

Related Topics:

Location Assistant Overview

Assign Stations

Add Gateway

Call Routing

Select Media Server

Regionalization

Managed IP Phone Assistant

Managed IP Phone Assistant

The Managed IP Phone Assistant allows you to create new managed IP phones and the associated SIP stations by importing.

The advantage of managed IP phones and SIP stations is ease of configuration. All configuration is done in Interaction Administrator. The IC ProvisionServer subsystem take cares of "serving" the phone its configuration and manufacturer-specific firmware through a registration group. Using Interaction Administrator to manage IP phones also eliminates the need going forward to maintain SIP phone configuration (.cfg) files.

Importing CSV Lists

Use the .CSV **import** option if you want to create multiple new managed IP phones and the associated SIP stations.

For example, you have purchased 50 Interaction SIP Station or Polycom phones, and you want to create new managed IP phones and the associated SIP stations for all 50 of the phones at the same time, each having different names and extensions.

Prerequisites for import:

- Create one or more managed IP phone templates based on managed IP phone type, manufacturer, model, location, language, audio protocol, station appearance, etc.
- Create one or more CSV Managed IP Phone Lists.

Migrating: You can use the migrate option if you already have SIP stations in Interaction Administrator and you want to migrate these station appearances into managed IP phones. For example, you are updating CIC and you have 100 existing Polycom SIP stations already configured in Interaction Administrator. You want to migrate all 100 stations to managed IP phones at the same time.

You must know the location and format of the SIP configuration (.cfg) files when importing. Also, see the SIP Phone Information Update server parameter for help during the migration process.

> **Notes**: The Managed IP Phone Assistant after business hours because the procedure requires significant server resources.
>
> After running the Managed IP Phone Assistant, the managed IP phones must be provisioned. For more information, see *CIC Managed IP Phones Administrator's Guide* and *CSV List Import Technical Reference* in the PureConnect Documentation Library.

Add Managed IP Phones

Add Managed IP Phones

To create new managed IP phones, import new SIP stations from a CSV file or migrate existing SIP stations based on the manufacturer.

To add managed IP phones

1. Do one of the following:
    - Select the **Create Managed IP Phones From a CSV File** option. Then do the following:
        - Select the .csv file
        - Review .csv file import results
        - Correct errors if detected and reload the .csv file
        - Commit changes
    - Select the **Create Managed IP Phones By Migrating Existing Stations to Phones on a Per Manufacture Basis** option. Then do the following:
        - Select the manufacturer
        - Specify the format strings for the phone names
        - Enter the directory location that contains the IP phone configuration (*.cfg) files
        - Select items to migrate
        - Build migration items
        - Review current state of migration items
        - Correct errors or make changes to name, model, or type
        - Back up directory services
        - Convert migration items into phones
        - Display migration results
2. Click **Next**.

Related topics

Create managed IP phones From a CSV File

Create managed IP phones by migrating existing stations to phones on a per manufacture basis

Create Managed IP Phones From a CSV File

Create Managed IP Phones From a CSV File

Create managed IP phones based on:

- Template containing name, template, proxy group, extension, identification address, label, and address information for the appropriate IP phones in your CIC system, and/or...

- Type, Manufacturer, and Model containing name, type, model, manufacturer, proxy group, extension, identification address, label, and address information for the appropriate IP phones in your CIC system.

> **Note:** The CSV file must be in UTF-8 format. For more information, see CSV files with non-English column headings

1. Click **Browse** to select the CSV file that contains the managed IP phones that you want to create and their additional information.

   To see sample data, click **Example**. Two sample Managed IP Phones CSV lists corresponding to the two types of CSV lists are available to download from the Product Information site:

- CSV Managed IP Phone List-Template.csv and CSV Managed IP Phone List-Template.xlsx
- CSV Managed IP Phone List-TMM.csv and CSV Managed IP Phone List-TMM.xlsx

The managed IP phones CSV files are formatted in two sections; a header section, and a data section. The header is the first row in the file and contains the names of all columns to import. The two sample lists are described below.

CSV Managed IP phone-Template list supports the following columns:

Name (Required): This is the IP phone name.

Template (Required): Type the managed IP phone template for this IP phone. The template name must be identical to one of the templates you have created.

Proxy Group: Type the Registration (Proxy) Group to be used with the managed IP phone template for this IP phone. If this value is left blank, Managed IP Phone Assistant will fill in the Registration Group defined in the template.

Extension: Type the primary appearance extension number for this IP phone.

Identification Address: If you know the IP address for this IP phone ahead of time, type the SIP connection address in the form of sip:xxx@[IPaddress]:[portnumber], e.g., sip:320@172.17.238.68:5060.

If you do not know the IP address, leave this value blank. It will be filled in when the phone registers with the CIC server following provisioning.

Label: (Polycom only) Type the label that will be used for the primary appearance of this IP phone and the associated SIP station. Typical values for “label” are the station extension or the user’s extension (in the case where one user will almost always be using the station).

When this value is left blank, Managed IP Phone Assistant will fill in the Name attribute (IP phone name).

Address: If you know the address for this IP phone ahead of time, type:

- **For Polycom phones:** The MAC address of the IP phone.
- **For SIP Soft Phones:** The full computer name for the IP phone. To make sure you get the full computer name, navigate to My Computer….Properties….Computer Name and note the **Full Computer Name**. For example: PattyJ.acme.com.

- **For Interaction SIP Station phones:** The MAC address of the IP phone. Interaction SIP Station MAC addresses always start with 00.26.fd.

If you do not know the address ahead of time, you will need to manually provision the Polycom phone or SIP Soft Phone using the provisioning IVR. (Interaction SIP Station phones cannot be manually provisioned.)

CSV Managed IP Phone - TMM list supports the following columns:

Name (Required): Type the name of the IP phone.

Type (Required): Type the type of IP phone – Workstation or Stand-alone Phone. For Interaction SIP Station phones: Type Workstation. (Stand-alone Phone is not supported).

Manufacturer (Required): Type the IP phone manufacturer. Currently, the supported manufacturers are Polycom and ININ (Genesys).

Model (Required): Type the phone model based on the manufacturer. If the manufacturer is Polycom: Type the Polycom phone model. If the manufacturer is ININ: If the manufacturer is ININ, type Soft Phone or Interaction SIP Station.

Proxy Group: Type the Registration (Proxy) Group to be used with the managed IP phone template for this IP phone. If this value is left blank, Managed IP Phone Assistant will fill in the Registration Group defined in the template.

Extension: Type the primary appearance extension number for this IP phone.

Identification Address: If you know the IP address for this IP phone ahead of time, type the SIP connection address in the form of sip:xxx@[IPaddress]:[portnumber], e.g., sip:320@172.17.238.68:5060. If you do not know the IP address, leave this value blank. It will be filled in when the phone registers with the CIC server following provisioning.

Label (Polycom only): Type the label that will be used for the primary appearance of this IP phone and the associated SIP station. Typical values for “label” are the station extension or the user’s extension (in the case where one user will almost always be using the station). When this value is left blank, Managed IP Phone Assistant will fill in the Name attribute (IP phone name).

Address: If you know the address for this IP phone ahead of time, type:

- For Polycom phones: The MAC address of the IP phone.
- For SIP Soft Phones: The full computer name for the IP phone. To make sure you get the full computer name, navigate to My Computer….Properties….Computer Name and note the Full Computer Name. For example: PattyJ.acme.com.
- For Interaction SIP Station phones: The MAC address of the IP phone. Interaction SIP Station MAC addresses always start with 00.26.fd.

If you do not know the address ahead of time, you will need to manually provision the Polycom phone or SIP Soft Phone using the provisioning IVR. (Interaction SIP Station phones cannot be manually provisioned.)

2. Click **Yes** to continue to Saving Managed IP Phones. If the assistant encounters errors while parsing the CSV file a message is displayed. Click Errors to view the status of the errors and a description:

- Warning error - Managed IP Phone Assistant cannot verify one or more values. You can continue with the import, but some of those values will not be imported.
- Severe error - Managed IP Phone Assistant detects no columns or the file could not be opened. You cannot continue with the import.

Saving Managed IP Phones

If you are ready to save the import results, click on **Commit Changes**. Click **Back** to make changes.

It may take several hours to import all the IP phones, depending on the number of IP phones and station appearances being created for each phone. On average, expect the import to take 1 to 2 seconds per IP phone with a single station appearance.

If you imported a CSV list based on type, manufacturer, and model (CSV Managed IP Phone TMM List)**,** clicking **Commit Changes** takes you to the following pages:

- Access Control
- Station Appearance Licenses
- **License Allocation Results**

If you imported a CSV list based on template (CSV Managed IP Phone Template List), clicking **Commit Changes** takes you to the **License Allocation Results** page**.**

Access control

This page may appear when you run the Add Stations Assistant or the Managed IP Phones Assistant.

> **Note for the Add Stations Assistant**: If you created a dial plan in IC Setup Assistant, select the dial plan classifications for the new stations. If you did *not* create a dial plan in IC Setup Assistant, no Available classifications appear. After you create the dial plan in Interaction Administrator after installation, run the Add Stations Assistant in Interaction Administrator and specify the outbound dialing privileges for your stations.

Use the Access control page to select the dial plan classifications for new stations. These classifications determine the outbound dialing privileges for the new stations.

Select one or more classification names from the list of **Available** classifications and add them to the **Currently Selected** list to give the selected dialing privileges to this station.

If someone attempts to place a call from a station and the dialed phone number is not supported in one of the phone number classifications for the station, CIC plays a prompt that says that the station does not have sufficient dialing privileges to place the call.

Stations Appearance Licenses

Use this page to assign licenses to the station appearance.

Basic Station License

This license represents an audio path between CIC and a station. This license is not required, but without it the audio for station will not play. A non-audio station may be used or for non-audio interactions.

Remote Stations must be assigned a Basic Station license. If a user logs into a remote station it will also need to acquire a Client Access license, which delivers the previously defined price list functionality of a "Business User". If a TUI login is performed against dynamic remote stations, no Client Access license is acquired.

Client Access License

Assigning this license to the station allows the client functionality of the CIC clients. Without this license assignment, the CIC clients will not run on this station.

ACD Access License

Select this check box if this workstation is an ACD station, then select the type of ACD license. These are the available types of ACD licenses:

- Media 1 - This license allows 1 interaction type at a given time.
- Media 2 - This license allows 2 interaction types at a given time.
- Media 3 Plus - This license allows 3 or more interaction types at a given time.

> **Note:** Failure to have a ACD Access License assigned to the station will prevent that station from being ACD active.

Interaction Process Automation License

Select the **Interaction Process Automation** check box if this user is an Interaction Process Automation user, and then select the type of license to assign to that user.

These are the available types of Interaction Process Automation licenses:

- **Direct Routed Work Items** (I3_ACCESS_IPA_USER) license: Enables you to launch any process to which you have rights. It also enables you to receive Work Items that are directly routed to you.
- **Group Routed Work Items** (I3_ACCESS_IPA_USER_ACD) license: Enables you to receive Work Items that are either routed to you directly or as a member of a workgroup (similar to an ACD queue).
- **Process Monitor** (I3_ACCESS_IPA_MONITOR) license: Enables you to view process status and details in the Process Monitor or to use Process Reporting in IC Business Manager Applications.
- **Process Designer** (I3_ACCESS_IPA_DESIGNER) license: Enables you to use the Process Designer to create and modify Interaction Process Automation processes.

> **Note**: Each license in this list enables you to **use the Interaction Process Automation features included in all the previous licenses in the list**. That is, the Group Routed Work Items license includes the Direct Routed Work Items license. The Process Monitor license includes both of the Routed Work Items licenses. The Process Designer license includes all the other licenses.
>
> For more information about designing processes, refer to the *Interaction Process Automation Technical Reference* and the Process Designer help.

License List

This list displays additional licenses that are available. Select the licenses you wish to assign to this station.

> **Note:** For specific license information on each type of license, see *PureConnect Licensing Overview Technical Reference* in the PureConnect Documentation Library.

Click **Next**.

☎ License Allocation Results

Use this page to view license allocation results. License errors can occur if the total license count is exceeded. If this occurs, or if different licenses need to be specified, use the license allocation page to make changes.

Click on **Review** to display any licensing errors.

☎ Complete the Managed IP Phone Assistant

The Managed IP Phone Assistant process is now complete. Click **Finish** to exit the assistant.

In the **Managed IP Phone** container, notice the new managed IP phones listed in the right-hand pane:

- The new managed IP phones will have a Status of "Not registered". Their status will become “Up-to-date” on the phones’ next SIP registration.
- If you did not supply the Address attribute for one or more managed IP phones in your CSV Managed IP Phone list, they will have a status of “Not provisioned”. Their status will become “Up-to-date” once you provision them using the Polycom phone or SIP Soft Phone provisioning IVR.

In the **Stations** container, notice the SIP station appearances associated with the new IP phones:

The SIP stations associated with managed IP phones are of the type **Managed Workstation** or **Managed Stand-alone Phone**.

> **Tip**: To make sure the list of managed IP phones is up-to-date at any time, click **F5** to refresh the screen.

Information on migration

Created Managed IP Phones by Migrating

☎ Select Manufacturer

If you select **Create Managed IP Phones By Migrating Existing Stations to Phones on a Per Manufacture Basis**, you will need to choose the manufacturer of the stations you wish to migrate.

Select **Polycom** and click **Next** to go to the Select Default Model page.

☎ Select Default Model

Use this page to select the default phone model that should be used if the model cannot be derived from the stations on the phones being migrated.

For example, SIP stations associated with a Polycom configuration file may not have a manufacturer or model set in Interaction Administrator. By selecting a default model, the Managed IP Phone Assistant knows what settings to use for the migration.

The Polycom models available are:

- IP300
- IP301
- IP320
- IP321
- IP330
- IP331
- IP335
- IP4000
- IP430
- IP450
- IP500
- IP501
- IP550
- IP560
- IP600
- IP6000
- IP601
- IP650
- IP670
- IP7000
- SL8440
- SL8450
- TRIO8500
- TRIO8800
- VVX101
- VVX201
- VVX300

- VVX310
- VVX400
- VVX500
- VVX600

Select the default model on the pull-down menu, and click **Next** to go to the New Phone Naming page.

New Phone Naming

Use this page to specify a format string that specifies the name for the assistant to use for the migration item. The assistant also creates an associated SIP station with the same name. There are two different substitution strings that can also be used with a name format to create phone names.

Phone Name Format

This is the name of the first private station display name that is added to the migration item. Use a format string to define the phone's name when created. Use one or more substitution strings with a format string, so that every phone created will have meaningful and unique name.

There are two different substitution strings:

- $FirstPrivateStation$ - This is the name of the first private station display name as defined in the reg.x.displayName attribute found in the SIP phone's .cfg file.) that is added to the migration item. (For more information on .cfg file attributes, click here.)
- MAC - This is the MAC address of the phone being migrated.

By default, the assistant uses the $FirstPrivateStation$ substitution string. A substitution string can be used separately, in combination with the other substitution string, in combination with a format string, or a format string can be used alone. For example:

- $FirstPrivateStation$
- MAC
- $FirstPrivateStation$-MAC-SecondFloor
- SecondFloorPhone – Using just text, the assistant appends the text with _1, _2, and so on after naming the first IP phone and associated SIP station.

If a single format string of ManagedPhone is used without a substitution string, then all new phone names created would be named "ManagedPhone_1", "ManagedPhone_2", etc. If the substitution string MAC is used together with the format string of ManagedPhone, such as ManagedPhone - MAC, then the MAC address for each phone would be substituted in the new name, i.e., "ManagedPhone - 0004f2008100".

> **Note**: The substitution strings are case-sensitive manner. For example, if Phone - mac is specified, mac will not resolve to the MAC address. The string must be entered as Phone -MAC for proper MAC address resolution.

Sample Phone Name

The sample phone name field shows how the phone name format field will resolve.

Click **Show Available Substitution Strings** to view the substitution strings.

Click **Next** to go to the Phone Configuration File Directory page.

Phone Configuration File Directory

Enter the directory or click **Browse** to select the directory where the existing IP phone configuration (.cfg) files are located. The Managed IP Phone Assistant searches this directory for .cfg files and displays a list of files found in the next page, **Select the Items to Migrate**. The assistant uses the settings in the selected .cfg files to create managed IP phone objects.

> **Note**: For the assistant to recognize a phone configuration file, the file must:
>
> - Be in the XXXXXXXXXXXX.cfg format, where XXXXXXXXXXXX is a 12 character alpha-numeric MAC address
>
> - Contain an APPLICATION XML element at the root that has a CONFIG_FILES XML attribute that specifies the other phone configuration files
>
> Each .cfg file that meets this criteria will be displayed as a selectable item to migrate. The assistant must have read access to the phone configuration directory specified. See Frequently Asked Questions for more information on .cfg files and the Managed IP Phone Assistant.

About the Managed IP Phone Assistant's Migration of Polycom Configuration Files

The assistant reviews the data in the .cfg files, and bases the migration items that it will build on the settings that are known in Interaction Administrator. The assistant displays migration item details, including any errors, in migration information. For the best and most error-free migration process, it is recommended to use the IP Phone Configurator utility to generate the SIP stations and SIP phone configuration files. (See *CIC Managed IP Phones Administrator's Guide* in the **Technical Reference Documents** section in the PureConnect Documentation Library on the CIC server.)

Not all settings, such as custom settings in Polycom configuration files (and where the configuration files have been set up manually instead of using the IP Phone Configurator), may be recognized by the assistant. Settings that are not recognized may not be written to the new managed IP phone's configuration file when provisioning.

> **Note**: If there is a needed setting that is not recognized by the assistant, it is possible to use "custom override attributes." For more information, see the *IC Managed IP Phones Administrator’s Guide* in the CIC Documentation Library.

Select the Items to Migrate

Use this page to select the items to migrate by moving the items from the **Available** list to the **Selected** list. The items displayed in the **Available** list are the Polycom configuration files that the assistant found in the directory specified in the previous page, Phone Configuration File Directory.

Select the items to migrate, and click **Next** to go to the Build Migration Items page. At least one item must be selected to continue.

Build Migration Items

This page shows that the migration process is going to begin building migration items, and it lists the number of migration items that will be included in the process.

Click **Next** to begin the process of building migration items, and to go to the next page, Current State of Migration Items.

Current State of Migration Items

Use this page to view summary information of the migration items that have built. The page displays items with errors, items with warnings, and items with no errors or warnings.

- Items with errors: The assistant can *not* create a managed IP phone from these items.
- Items with warnings: These items are candidates for migration at the current state, and the assistant *may* be able to create a managed IP phone from these items.
- Items with no errors or warnings: These items are good candidates for migration at the current state, and the assistant will most likely be able to create a managed IP phone from these items.

> **Note**: *Please review the migration item details*. The assistant may have detected warnings while building the migration items, but some warnings may not impact whether an item is a candidate for migration and creation of a managed IP phone. For example:
>
> A Polycom configuration file selected for migration has two registrations specified in it. The assistant matches the first registration to a SIP station in Interaction Administrator, but does not match the second registration to a SIP station or shared appearance. In this migration item's current state, the assistant can still create a managed IP phone from it, because it does recognize the one station (first registration) which would be the private station, and therefore there are not any true errors.

It is strongly recommended to review migration item details by clicking **Show Item Details** to display the migration information. Item details show what happened during the building of the migration items, and shows why an item may have a warning or an error.

After reviewing the item details, click **OK** to go to the next page, Backup Directory Services.

> **Note**: After clicking **OK**, the assistant displays a prompt that it will not create managed IP phones from migration items with errors. Clicking **Continue** will go to the next step in the migration process: Backup Directory Services.

Backup Directory Services

It is strongly recommended to perform a Directory Services backup. This is the final step in the migration process before the Managed IP Phone Assistant begins creating the managed IP phones based on the migration items.

Click **Backup Directory Services** to perform the backup. The Directory Services backup may take several minutes. There is a timeout set at 40 minutes. If the timeout is reached, the assistant displays "The Interaction Center server was unable to perform a backup of Directory Services." Either click **Try Again** to attempt another backup, or click **Continue** without making a backup.

> **Note**: It is strongly recommended to make a backup of directory services. In the event that a restoration of directory services is necessary, click here for instructions.

When the backup is complete, the dialog will show the location of the backup file. Please note the location.

Click **Next** to begin the migration and go to the next page, Migration Results. The migration process begins, and the assistant creates IP phones from the migration items. This process may take several minutes.

For detailed information in the migration process, click here.

Migration Results

This page shows the number of IP phones that have been created in the migration process, and shows the number of IP phones that have not been created.

Click **Show Detailed Migration Results** to view each step that was taken during the migration.

Complete the Managed IP Phone Assistant

The Managed IP Phone Assistant process is now complete. Click **Finish** to exit the assistant.

In the **Managed IP Phone** container, notice the new managed IP phones listed in the right-hand pane:

- The new managed IP phones will have a Status of "Not registered". Their status will become “Up-to-date” on the phones’ next SIP registration.
- If you did not supply the Address attribute for one or more managed IP phones in your CSV Managed IP Phone list, they will have a status of “Not provisioned”. Their status will become “Up-to-date” once you provision them using the Polycom phone or SIP Soft Phone provisioning IVR.

In the **Stations** container, notice the SIP station appearances associated with the new IP phones:

The SIP stations associated with managed IP phones are of the type **Managed Workstation** or **Managed Stand-alone Phone**.

> **Tip**: To make sure the list of managed IP phones is up-to-date at any time, click **F5** to refresh the screen.

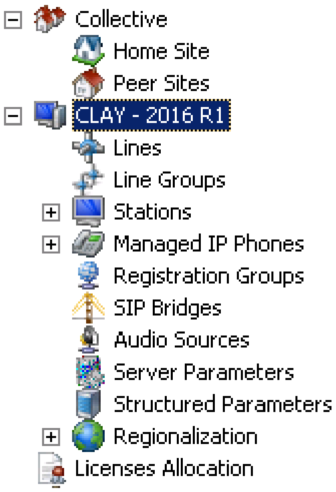
Information on migration

IC Server

Overview of CIC server configuration

Each CIC server requires a specific configuration to support the hardware and software resources that are associated with it.

You configure your server in the server configuration container, which displays the name of your CIC server.



Collective
Home Site
Peer Sites
CLAY - 2016 R1
Lines
Line Groups
Stations
Managed IP Phones
Registration Groups
SIP Bridges
Audio Sources
Server Parameters
Structured Parameters
Regionalization
Licenses Allocation

Related topics

Configure your CIC server

SIP lines concepts

Configure line groups

Configure stations

Configure managed IP phones

Configure registration groups

Configure SIP bridges

Configure audio sources

Configure server parameters

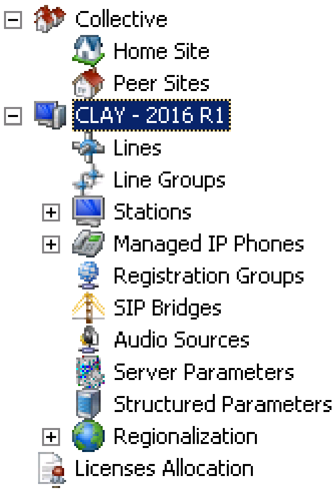
Configure structured parameters

Server Configuration

Overview of CIC server configuration

Each CIC server requires a specific configuration to support the hardware and software resources that are associated with it.

You configure your server in the server configuration container, which displays the name of your CIC server.



- Collective
  - Home Site
  - Peer Sites
- CLAY - 2016 R1
  - Lines
  - Line Groups
  - Stations
  - Managed IP Phones
  - Registration Groups
  - SIP Bridges
  - Audio Sources
  - Server Parameters
  - Structured Parameters
  - Regionalization
- Licenses Allocation

Related topics

Configure your CIC server

SIP lines concepts

Configure line groups

Configure stations

Configure managed IP phones

Configure registration groups

Configure SIP bridges

Configure audio sources

Configure server parameters

Configure structured parameters

Review the IP configuration of your CIC server

To review the IP configuration of your CIC server

1. In the ***<IC Server>*** container, in the list view window, double-click **Configuration**.
   The **Server Configuration** dialog box appears. The boxes on the **IP Configuration** tab are automatically completed for you. For more information, see *IP configuration options*.

> **WARNING:** Do **not** modify the boxes on this tab unless you know what changes need to be made, or you have been instructed to modify the settings by a PureConnect Customer Care representative.
>
> If you get an event log message stating that some handlers did not run immediately because the thread pool limit was reached, contact PureConnect Customer Care or your support representative. A representative will advise you if it is necessary to increase the number of available threads.

Related topics

IP configuration options

Overview of CIC server configuration

Configure your CIC server

IP configuration options

The following table describes the options on the **IP Configuration** tab.

Option	Description	Default
Starting Number of Threads in Thread Pool	Each handler runs in a separate thread. This box shows how many threads are available. If this box is set to **0**, then there are 100 starting threads in the thread pool. To gain a small amount of efficiency when IP starts, increase the value to a number closer to the **Maximum Number of Threads in Thread Pool**. **Note:** The maximum number of threads is 5,000.	0
Maximum Number of Threads in Thread Pool	This number indicates the maximum number of threads that you want your system to create to run handlers. If this box is set to **0**, then a maximum of 5,000 threads will be created to run handlers.	0

	Note: The maximum number of threads is 5,000.	

Related options

Review the IP configuration of your CIC server

Overview of CIC server configuration

Configure your CIC server

Configure your CIC server

<*IC Server*> > Configuration > Server Configuration

Configure your server using the tabs in this dialog box. For complete instructions, click the links below.

Related topics

Server configuration concepts

Review the IP configuration of your CIC server

Handlers concepts

Select the handlers for your CIC server

Monitor handlers concepts

Select the monitor handlers for your CIC server

Accumulators concepts

Select the accumulators for your CIC server

CPU load detection concepts

Configure CPU load detection for your CIC server

Report log purging concepts

Configure report log purging for your CIC server

Configure reports concepts

Configure reports for your CIC server

Audio compression concepts

Configure audio compression for your CIC server

Telephony parameters concepts

Configure general telephony parameters for your CIC server

General telephony parameters reference

Configure SIP telephony parameters for your CIC server

SIP telephony parameters reference

Recording beep tones concepts

Configure recording beep tones for your CIC server

Define a recording beep tone

Handlers

Overview of handlers

A handler is a process that runs in response to an event. In CIC, handlers complete numerous functions.

Interaction Designer users create and publish handlers. Published handlers are available to all CIC servers. In Interaction Administrator, you select the handlers to run on your CIC server by activating them and deactivating them. Interaction Processor uses the activated handlers to complete CIC functions.

> **Note:** As the system administrator, you must also assign the necessary security right to the users who create and publish handlers in Interaction Designer.

For more information on handlers, see the Interaction Designer Help.

Related topics

Select the handlers for your CIC server

Security

Configure your CIC server

Select the handlers for your CIC server

***<IC Server>* > Configuration > Server Configuration** > **Handlers**

The handlers that are listed in the **Active Handlers** list run on your CIC server. Do one of the following:

- To activate handlers, select them in the **Inactive Handlers** list and then click **Add**.
- To deactivate handlers, select them in the **Active Handlers** list and then click **Remove**.

> **Note**: When an Interaction Designer user modifies and re-publishes an active handler, Interaction Processor automatically detects the new version of the handler. It uses the new handler for all new interactions that require it. Any interaction that is uses the older version of the handler finishes its processing with the old version of the handler.

Related topics

Overview of handlers

Configure your CIC server

Monitor handlers

Overview of monitor handlers

A monitor handler is a process that monitors specific interactions in CIC and gathers data for reporting.

Interaction Designer users create and publish the monitor handlers. Published monitor handlers are available to all CIC servers. In Interaction Administrator, you select the monitor handlers to run on your specific CIC server by activating and deactivating them. Interaction Processor uses the activated monitor handlers to monitor numerous functions in CIC.

> **Note:** As the system administrator, you must also assign the necessary security right to the Interaction Designer users who create and publish monitor handlers in Interaction Designer.

For more information on monitor handlers, see the Interaction Designer Help.

Related topics

Select the monitor handlers for your CIC server

Configure your CIC server

Security

Select the monitor handlers for your CIC server

<IC Server> **> Configuration > Server Configuration** > **Monitor Handlers**

The monitor handlers that are listed in the **Active Monitor Handlers** list run on your CIC server. Do one of the following:

- To activate monitor handlers, select them in the **Inactive Handlers** list and then click **Add**.
- To deactivate monitor handlers, select them in the **Active Monitor Handlers** list and then click **Remove**.

> **Note**: When an Interaction Designer user modifies and republishes an active monitor handler, Interaction Processor automatically detects the new version of the monitor handler. It uses the new monitor handler for all new interactions that require it. Any interaction that is uses the older version of the monitor handler finishes its processing with the old version of the monitor handler.

Related topics

Overview of monitor handlers

Configure your CIC server

Accumulators

Overview of accumulators

Accumulators are similar to global variables. They hold a value outside of a handler. Accumulator tools within handlers can assign, increment, and retrieve the values stored in accumulators. The types of values that you can store in accumulators are String, Integer, Numeric, Boolean, and DateTime values.

In Interaction Administrator, you select the accumulators that can be set on your CIC server by activating them and deactivating them.

> **Notes:** To see the definition of an accumulator or to configure an accumulator, use the **Accumulators** subcontainer of the **System Configuration** container.
>
> When a new instance of an accumulator is created in the **Accumulators** subcontainer, you must deactivate it and then reactivate it for your CIC server. If you do not do this, a warning message appears when an accumulator tool attempts to use the accumulator.

Related topics

Select the accumulators for your CIC server

Accumulator configuration

Handlers concepts

Select the accumulators for your CIC server

<IC Server> **> Configuration > Server Configuration** > **Accumulators**

The accumulators that are listed in the **Currently Selected Accumulators** list run on your CIC server. Do one of the following:

- To activate accumulators, select them in the **Available Accumulators** list and then click **Add**.
- To deactivate accumulators, select them in the **Currently Selected Accumulators** list and then click **Remove**.

Related topics

[Overview of accumulators]

[Configure your CIC server]

CPU load detection

Overview of CPU load detection

You can monitor the CPU load on your CIC server in order to determine if IC Server's **Notifier** and **Queue Manager** subsystems are overloaded.

To configure CPU load detection, you set a high watermark value, a low watermark, and the sample period. IC Server calculates the time it takes to send two back-to-back ping messages to **Queue Manager** during a sample period. It then divides this resulting number by two to get the average time. The average time indicates how quickly **Notifier** is passing messages, and if **Queue Manager** is keeping up with queue transitions or attribute changes.

IC Server then compares the average time against the high watermark and the low watermark values:

- If the average time of the ping messages take longer than the **high watermark**, then IC Server sends a message to the CIC subsystems. This message states that the CIC system is experiencing high load conditions. When this occurs, e-mails are no longer queued, Interaction Dialer stops placing campaign calls, and other subsystems take action to reduce the load on the system.
- IC Server continues to send ping messages. When the ping messages result in an average time that is less than the **low watermark**, IC Server sends a message to the CIC subsystems. This message states that the CIC system has returned to normal. The CIC subsystems then return to normal as well.

> **Note:** In multiprocessor systems, the average ping time is measured across all CPUs. For example, if you have two CPUs and one is 50% busy and the other is 100% busy, the CPU utilization is 75%.

Related topics

[Configure CPU load detection for your CIC server]

[Configure your CIC server]

Configure CPU load detection for your CIC server

***<IC Server>* > Configuration > Server Configuration > CPU Load Detection**

1. In the **High Watermark** field, select the number of milliseconds that indicates high load conditions. The default value is 200.
2. In the **Low Watermark** field, select the number of milliseconds that indicates normal (or low) load conditions. The default value is 200.

3. In the **Sample Period(s)**, select the period of time over which the CIC system determines the average time of a test ping. The default value is 5 seconds.
4. Click O**K**.

Related topics

Overview of CPU load detection

Configure your CIC server

Report log purging

Overview of report log purging

You can configure when the CIC system deletes expired report log records from the log databases. Report log records are expired when they exceed their retention times. You configure retention time for each report log in the **Report Logs** subcontainer, which is found in the **System Configuration** container.

Related topics

Configure report log purging for your CIC server

Configure your CIC server

Report log retention

Configure report log purging for your CIC server

> **Note:** Data in the Enhanced Interaction Administrator change log is purged based automatically on the setting of this field. For more information, see *About the Enhanced Interaction Administrator change log*.

<*IC Server*> > Configuration > Server Configuration > Report Log Purging

1. Use the **Reference Time** fields to select the hour, minute, and second when you want expired logs to be purged.
2. Use the **Run Every** fields to select the days, hours, and minutes between each purge.
3. Click **OK**.
   The **Purge will occur at** list displays the dates and times when the purge will occur.

Note: Report log purging for large databases might require using an optional server parameter to prevent a five-minute timeout. For more information, see the *PureConnect Reporting Technical Reference*.

Related topics

Overview of report log purging

Configure your CIC server

About the Enhanced Interaction Administrator Change Notification Log

Reports configuration

Overview of report configuration

You can configure the following report options for your CIC server:

- Generation of DNIS reporting data, which allows you to run the DNIS reports
- Reporting by media type
  If you activate this feature, then CIC logs interaction types in log 90, log 91, and log 92. By default, CIC logs interaction types only in log 10.

> **Notes**
> If you run Interaction Optimizer, then you automatically have the ability to run reports by media type.
>
> If you activate reporting by media type, then you must restart the Stat Server if you activate media type report data for the change to take effect. Also, you will notice an increased amount of logged data.

- Inclusion of the detailed report version information on each report that is run the Interaction Reporting application
- The number of minutes during which CIC collects data in each reporting interval
- The interval period for the line and line group data in the report logs

Related topics

Configure reports for your CIC server

Configure your CIC server

Configure reports for your CIC server

***<IC Server>* > Configuration > Server Configuration** > **Report Configuration**

Options

- To activate DNIS reporting data in the Queue Period Statistics data, select the **Generate DNIS reporting data** check box. When this feature is activated, the report group for calls is DNIS-{Dnis} and all calls are put into a statistics group called DNIS. You can generate the DNIS reports that are included with CIC.

- To activate reporting by media type, select the **Generate media type reporting data**... check box.
- The **Display report version in reports** check box is not currently used.

Reporting intervals

- To change the interval during which CIC collects report data, in the **Queue/IVR reporting interval (min)** field, use the up and down arrow keys to set the number of minutes to collect data in a reporting interval. The default value is 30 minutes.

> - **Note:** The minimum allowable interval is 15 minutes. If you specify an smaller interval, then CIC automatically uses 15 minutes.

- To change the report log interval period for the line and line group data, in the **Line reporting interval (min)** field, use the up and down arrow keys to set the length in minutes of the report log interval. The default value is 30 minutes.

Proxy enabled reporting

The values in this section allow you to set limits on the amount of time your users wait for Internet enabled reports before they time-out.

> **Note:** The default settings are appropriate for most customers. Do not change these values unless your access to reports is critical, or you run a significant number of reports. These settings are per session manager.

- **Maximum Reporting Proxy Client Connections**: This is the highest number of IC clients that can simultaneously access reports through the proxy.
- **Maximum Proxied Report Run Time (min)**: This is the highest run time (in minutes) allowed for a report running through the proxy.
- **Reporting Proxy Client Timeout (sec)**: This is the amount of time (in seconds) that a report running through the proxy can be inactive.

For information about running Internet-based reports, see Report Connection Configuration and the *PureConnect Reporting Technical Reference* in the PureConnect Documentation Library.

Related topics

Overview of report configuration

Configure your CIC server

Audio compression

Overview of audio compression

You can configure the audio compression options for the **Audio Compression Manager** that runs on your CIC server.

> **Note:** If you do not configure the audio compression settings, then the **Audio Compression Manager** sets them to the appropriate values.

Related topics

Configure audio compression for your CIC server

Configure your CIC server

Configure audio compression for your CIC sever

***<IC Server>* > Configuration > Server Configuration** > **Audio Compression**

1. In the **Total Number of Compression Threads** field, enter the number of compression threads for audio compression. By default the system uses 3 compression threads.
2. In the **Local Compression Thread Priority** field, select **Below Normal**, **Normal**, or **Above Normal**. This value represents the thread priority of compression threads running on the CIC server.
3. Click **OK**.

Related topics

Overview of audio compression

Configure your CIC server

Telephony parameters

Overview of Telephony parameters

You can configure the resources that connect incoming telephone lines with your company's computers, telephones, fax machines, and so on.

Related topics

Configure general telephony parameters for your CIC server

General telephony parameters

Configure SIP telephony parameters for your CIC server

SIP telephony parameters

Configure your CIC server

Configure general telephony parameters for your CIC server

***<IC Server>* > Configuration > Server Configuration > Telephony Parameters**

1. In the list, select **General**.
   The general telephony parameter options appear in the right side of the tab.
2. Select the check boxes for the parameters that you want to enable. For information, see *General telephony parameters*.
3. As necessary, specify any additional values.
4. Click **OK**.

Related topics

General telephony parameters

Overview of telephony parameters

Configure your CIC server

General telephony parameters

The following table describes the general telephony parameters. For information on how to set these parameters, see *Configure general telephony parameters for your CIC server*.

Parameter	Description
Allow Recording of External Transfers	Determines whether a call can be recorded when an agent transfers it to an external number. If you do not select this option, a call is not recorded if it is transferred to an external party and parties are involved. If you do select this option, the call recording continues after the transfer
Append SIP Call-ID to CallLog	Determines whether the call log includes the SIP call ID.
Auto Disconnect Last Party	Determines whether the CIC system automatically disconnects the last party in a conference.
Block All External Transfers	Blocks all consult and blind transfers to external parties and remote numbers. This option work **Disconnect Conferences with Only External Parties** option to help prevent toll fraud.
Board Event Window Limit	Specifies the maximum number of allowable digital board events. Excessive board events can generate in-sync/out-of-sync errors from a bad board or a bad digit option prevents bad equipment (such as T-1, ISDN, and other digital lines) from causing excessi slowing down CIC.

	Note: If board events are disabled on a board, the board remains registered as active. However, events are disabled for the amount of time specified for the **Event Recovery Time** If more than this number of digital events is counted during the **Board Event Window Time**, th events are disabled on the board. The minimum number of events is 5.
Board Event Window Time (ms)	Specifies the number of consecutive milliseconds during which digital board events are countec minimum number is 10000 ms (10 seconds). **Note:** If 20 events occur within 60 seconds, CIC disables the board that generated the events See also **Board Event Window Limit**.
Call Analysis Diagnostic Record	Enables diagnostic call recordings for call analysis. Diagnostic records are 8k, mono, 8bit unsigned PCM. **Note:** If Media Servers are not used for advanced operations, diagnostic recordings are placed in the default Recordings directory and have the following naming convention: DR_<callid>.pcm. If Media Servers are used for advanced operations, diagnostic recordings are stored on each Media Server with the following naming convention: %inin_trace_root%\<date>\diagnostics\<lastTwoDigitsOfCallId>\<callId>_<16RandomCharac Diagnostic recordings stored on Media Servers are automatically deleted after seven days.
Keyword Spotting Diagnostic Recording	Enables diagnostic recordings for keyword spotting. Interaction Analyzer uses diagnostic recordings to help determine accuracy in keyword spottinç information, see *Interaction Analyzer Technical Reference* in the PureConnect Documentation L CIC server.
Fetch Diagnostic Recordings from Media Server	Retrieves all diagnostic recordings from the Media Server and from the [drive]:[IC installation folder]/logs/diagnostics.
Confirm Station Connection	Sends an **eCallEvent_StationConnectionConfirmation** event. This event can be intercepted anc the ConfirmStationConnection initiator and the StationConnectionConfirmation tool step. This user to intercept a remote client connection call and change the behavior via a handler.
Diagnostic Recording Extension Time (sec)	Sets the time (in seconds) that a diagnostic recording will be extended beyond the completion analysis operation. Support Services may increase this period to troubleshoot call analysis resu order to thoroughly analyze the audio. The acceptable values are 3 through 30.
Disconnect	Disconnects conferences in which the only members are external parties and remote numbers.

Conferences with Only External Parties	If all internal parties leave a conference, and only external parties remain on the call, the confe disconnected. This option works with the **Block all External Transfers** parameter to help preven
Enable Call Analysis for Conference Add Party	Enables the ability to add a party to a conference immediately or to perform call analysis befor party to the conference.
Enable Secure Input feature	Activates the **Secure Input** feature, which separates and encrypts data to protect it from theft When this parameter is elected, you can create and configure secure input forms in the **Secure** container. You can then assign individual secure input forms to different workgroups in the **Wo** container.
Extension Dialing Analysis Type	Used with extension dialing. When CIC uses extension dialing to place a call, and the number di a /xxx where xxx is an IVR entry or extension number, CIC attempts to detect if the dialed num answered by a human voice or an answering machine or an IVR script. The acceptable values are: • **Voice**: CIC waits for the dialed number to answer and then automatically sends the DTI the extension. This has the advantage that you can always be certain that the DTMF wi disadvantage is that when a human answers the call, the DTMF will play in that person • **Answering Machine**: CIC attempts to recognize an IVR or automated voice before senc tones. If it does not detect an automated voice, it assumes a human voice answered ar send the DTMF extension digits. This kind of detection is less reliable than voice detect
Global No Connection Timeout (min)	Sets a timer on all calls made on the CIC system. The CIC system disconnects a call if the call do connected state before the expiration of this timer.
Held Call Timeout (seconds)	Specifies the number of seconds a call can remain on hold. When the timer elapses, the call flo a menu to present the caller with options. This menu is generated by the System_HeldInteracti handler. You can modify the call flow behavior in the CustomHeldInteractionTimer handler. The default value is **900 seconds (15 minutes)**.The minimum value is 2 seconds. **Note:** If you change this parameter, you do not need to restart CIC in order for it to take effe
Honor No Answer Timeout	Sets CIC to honor the no answer value presented to it by the caller, which is usually the client o step.
Inband Dial Delay (ms)	Sets the time in milliseconds that the system waits before dialing in-band digits to the external In-band dial digits are most commonly used for extension dialing and account code dialing.
Intercom Calls ASR	Allows a user to toggle permissions for allowing ASR enabled intercom calls on the system, as v

Enabled	threshold for concurrent intercom ASR enabled sessions. The acceptable values are: • **On** • **Off** • **0**
Line Event Window Limit	Disables line events if a digital line starts generating abnormal numbers of events and degrade performance. Such events can generate in-sync/out-of-sync errors from a bad board or bad digital line. This s mechanism prevents bad equipment (such as T-1, ISDN, and other digital lines) from causing ex and dragging down CIC. The event and shutdown threshold is configurable with three paramete **Window Limit**, **Line Event Window Time**, and **Event Recovery Time**. Enter the maximum number of digital line events to detect within the **Line Event Window Tim** before disabling digital events on the excessive board. If a digital line exceeds this limit, CIC disa from that line for the specified **Event Recovery Time**. The minimum event limit is 5. The board remains registered as active, but events are disabled f specified time. **Note:** Not all lines implement this option.
Line Event Window Time	Specifies the number of consecutive milliseconds during which digital line events are counted. window is 10000 ms (10 seconds). **Notes:** If 20 events occur within 60 seconds, CIC disables the line that generated the events. Not all lines implement this options
Maximum ASR Session Limit	Sets a maximum value of resources that are expected to be used concurrently at any given tim system for ASR sessions. Specify any integer. **Note:** CIC derives a proper value if you do not provide one.
Maximum Number of Calls per Station	Sets the maximum number of outgoing calls originating from a single station that are allowed t When an outgoing call is made, TsServer checks a map of Call IDs to Station IDs and, if the stati specified number of outgoing calls still active, the new call attempt will fail. If not, an entry sho in the map. When the call disconnects, the entry is removed from the map.
Minimum ASR Session Limit	Sets a minimum value of resources that are expected to be available to the system for any ASR minimum level of resources that should not be fixed to any line, and therefore available to all s The acceptable values are:

	- **0**: Indicates that no minimum level is required - Any integer
Optimize Audio for Conferences	This option applies only to conferences. If you select this option, CIC automatically identifies th speaker and mutes all of the other calls on the conference. Conference calls hosted by Interaction Media Server include features such as dominant speake with echo cancellation (muting errant noises from other callers), automatic level control (volum for Interactive Voice Response (IVR) input, and other optimizations. **Note:** This parameter globally controls dominant speaker detection with echo cancellation fo calls. If you experience audio issues when this parameter is enabled, you can enter the **ConferenceTypeDominantSpeakerDiagnosticRecording** property through the Media Servers Interaction Administrator and set the value to **true**. This property creates diagnostic recordi can send to a PureConnect Customer Care representative for analysis.
Perform Call Analysis	Contact your authorized PureConnect Customer Care representative for information on this se For more information, see the *Interaction Media Server Technical Reference* document in the P Documentation Library.
Play Digits Tone Specification	Sets the number duration of the on or off time between DTMF tones. By default Telephony Services uses DTMF tones of 100ms in duration with 50ms off time betwe vendor-specific levels. In some circumstances it may be necessary to adjust the duration on or that the receiving system can correctly detect different tones. This parameter applies to all DTMF played using the Play Digits tool step. The acceptable values where X=on time (ms) and Y=off time (ms).
Recording Silence Time	Sets the duration (milliseconds) of silence that is required to disconnect a call that is in voice m This parameter is valid only for calls that are on the system, such as station-to-station calls, as o physical external lines. External lines have the same configuration option, which is available on configuration page in Interaction Administrator.
Remote Station Timeout Override	This parameter should be modified only with the direction of a PureConnect Customer Care rep Any modifications to the value can have a significant impact on the accuracy of call progress an those changes will be noted in the appropriate log files. Modifying this parameter without expl from a PureConnect Customer Care representative could result in a billable support incident to functionality.
Ringback Silence Detection Time	**Dialogic and Aculab:** Adjusts the maximum period of silence allowed before call analysis will de ringback. If unspecified, TS defaults to 11 seconds for connection calls (calls to a remote statio

	seconds for all other outbound calls. The minimum value allowed is 8 seconds. **Note:** This setting has no effect if Media Servers are used for advanced operations.
Ringback File	Specifies the .wav file that is played to the caller during alerting to the destination user or stati are located in the resource directory: Ringback.wav?playlocation=mediaserver **Caution:** If you replace the **RingBack.wav** file in the Resources directory with your own custom this file will be overwritten when you update to a newer release. If you have replaced this file i Resources directory, back up your customized file before you begin the update process. Then r after the upgrade is complete. This applies to the files on IC servers and on Media Servers.
Telephony Supported IP Versions	This parameter is available if the appropriate server parameter is selected. Specifies the type of protocol address family that is supported by the CIC server. For more information, see *SIP Line Transport* and *SIP Station Transport*. **Note:** If this parameter is set to IPv4, then all lines and stations that specify the Address Fami the Media Address Family as IPv6, are unusable and shown as "Unusable" in the Status colun If this parameter is set to IPv6, then all lines and stations that specify the Address Family as I Media Address Family as IPv4, are unusable and shown as "Unusable" in the Status column. For more information, contact your authorized PureConnect Customer Care representative.
Ts Consult Transfer To Intercom Move All Queues Active	Specifies that when a call is consult transferred to an intercom call, the transferring call is place queues of the replaced intercom call.
Waiting Call Indication	Enables call waiting. If this parameter is not selected, call waiting is globally disabled for all aler
Use Voice Buffer Input	Specifies whether the voice buffer input is activated. If you enable this parameter, it decreases the usage of voice and conference resources. If you c this parameter, there is no timeout.
Timeout (seconds)	Sets the number of seconds to wait before freeing up the resource after a play switches to the VoiceBufferInput role. Acceptable values are 5-20000 seconds.
Warm Down Time (ms)	Specifies the duration in milliseconds that the audio remains in Interaction Center after a user
Zone Page Delay	Sets the maximum time in milliseconds that the CIC server should wait for the stations being pa

	respond to a page request. Stations that take longer than this timeout to respond are be includ If all stations respond before this timeout is reached, the page begins to load immediately.

Related topics

[Configure general telephony parameters for your CIC server]

[Secure input]

[SIP line transport]

[Overview of telephony parameters]

[Configure your CIC server]

Configure SIP telephony parameters for your CIC server

***<IC Server>* > Configuration > Server Configuration > Telephony Parameters**

1. In the list, select **SIP**.
   The SIP telephony parameter options appear in the right side of the tab.
2. Specify the values for the parameters that you want to enable. For more information, see *SIP telephony parameters*.
3. Click **OK**.

Related topics

[SIP telephony parameters]

[Overview of telephony parameters]

[Configure your CIC server]

SIP telephony parameters

The following table describes the SIP telephony parameters. For information on how to set these parameters, see *Configure SIP telephony parameters for your CIC server*.

Parameter	Description	Default
Broken RTP Disconnect Time	Determines the amount of time (in seconds) that a VoIP call remains active after audio has been disrupted before the call is automatically disconnected. Audio is considered disrupted if no RTP, no RTCP, and no comfort noise packet is received from the remote device. • **0** - Disables this feature. Calls will not be monitored or disconnected. • **1** - Number of seconds before a	30 seconds

	disrupted call is disconnected **Note:** By default, CIC disconnects a call when both endpoints are in the idle state (no RTP packets). If you want CIC to disconnect calls where only one endpoint has entered the idle state, see the **TreatEndpointIdleAsFullIdle** server parameter. For more information, see the *Media Server Technical Reference* in the PureConnect Documentation Library.	
Default Display String	Sets the SIP display string in the FROM header when calls are made to persistent SIP managed **stations** and to any SIP managed station when the CIC client **MakeCall** button is pressed. This display string appears on the **From** field on the phone TUI display. Any string value is acceptable.	Interaction Center
Managed Phone Shortcut	Specifies the main IVR number that is given to managed phones. This number is typically an "*." Configure your network to route calls that are generated by managed phones to use this number to reach the Interaction Center. The acceptable values are: • SIP • None • Any number	None
Message Button	Specifies the number to retrieve voice mail over the IP phone when the user presses the **Message** button. Configure the voice mail button of the phone to call this number when it is pressed. Do not enter spaces. The acceptable values are: • None • Any number. Spaces are not allowed. **Note**: When this option is not set, the	None

	message button dials "stationname" when it connects to voice mail.	
Voicemail Direct	Sends calls directly to voice mail for unmanaged phones. Voice mail for managed phones is already handled. Configure your network to send calls that are destined for voice mail to this number. The acceptable values are: • None • Any number	None
Lineside Transcode Preference	If a transcode is necessary, this parameter indicates which side (the line or the station) to tap first. Since recordings tap the line side, transcoding should, too. This parameter is rarely used.	Yes
Initial Contact Expiration	Specifies the time that is used to expire a station contact address on system startup. • This parameter is used only if all of the following are true: • The station allows registrations to update its contact address. • The station sent a REGISTER message that had not expired before the CIC reboot. • The station has NOT sent a REGISTER message after the CIC reboot. For example, a station is registered with a CIC server. The CIC server is rebooted. If the contact address that the phone sent before the reboot was suppose to expire before **Initial Contact Expiration** seconds after the reboot, it will not expire.	86400

Related topics

Configure SIP telephony parameters for your CIC server

TreatEndpointIdleAsFullIdle server parameter

Overview of telephony parameters

Configure your CIC server

Recording beep tones

Overview of recording beep tones

You can configure beep tones for the **Beeps During Recordings** feature. A beep tone allows participants to be aware that a conversation is being recorded, which may be required for regulatory compliance.

For a beep tone, you can configure the length of beeps, the interval between beeps, and how the beeps sound.

You can apply beep tones to a workgroup.

CIC includes a default beep tone that you cannot edit or remove.

Related topics

Configure recording beep tones for your CIC server

Recording beep tone options

Configure your CIC server

Workgroup configuration

Configure recording beep tones for your CIC server

***<IC Server>* > Configuration > Server Configuration** > **Recording Beep Tones**

1. Do one of the following:
    - To add a recording beep tone, click **Add**.
      The **Add Recording Beep Tone** dialog box appears.
    - To edit a recording beep tone, select the tone and then click **Edit**.
      The **Edit Recording Beep Tone** dialog box appears.
    - To delete a recording beep tone, select the tone and then click **Remove**.
2. Complete the options on the dialog box. For more information, see *Recording beep tone options*.
3. Click **OK**.

Related topics

Recording beep tone options

Overview of recording beep tones

Configure your CIC server

Recording beep tone options

The following table describes the options for recording beep tones. For information on how to set these options, see *Configure recording beep tones for your CIC server*.

Option	Description	Default
Name	A meaningful name for the beep tone.	New Beep Tone
Duration (ms)	The time in milliseconds that the actual beep sound lasts.	200 ms
Interval	The time in seconds between the beeps. This is the time between the start of one beep and the start of the next beep.	12 seconds
Tone Type	The type of tone for the beep. You can set the beep as a single tone, or dual tone (having two tones). If you select **Dual** as the type, the **Frequency 2 (Hz)** and **Amplitude 2 (dB)** fields are available.	Single
Frequency (Hz)	The beep tone frequency in Hertz.	1400Hz
Amplitude (dB)	The beep tone volume in decibels.	-24dB
Frequency 2 (Hz)	The frequency of the second part of the tone and is available when the beep tone type is dual.	1400Hz

Amplitude 2 (dB)	the amplitude of the second part of the tone and is available when the beep tone type is dual. The acceptable range is -33dB is through 0.	-24dB

Related topics

Configure recording beep tones for your CIC server

Overview of recording beep tones

Configure your CIC server

History

This page provides a way to manually document configuration changes and when they occurred. Changes made in Interaction Administrator are also automatically logged in the Interaction Administrator Change Notification Log (Log ID 7). Later, authorized users can run reports against this log to summarize all configuration changes.

> **Note:** If you enabled the Enhanced Interaction Administrator Change log, then all of your changes to the History page in the User Configuration dialog box and the Workgroup Configuration dialog box dialog box are tracked in that log. For more information, see *About the Enhanced Interaction Administrator Change Log*.

Last Modified

This date is automatically updated each time you click the **OK** button, presumably after you make changes to the configuration. To avoid updating this date, exit the page by clicking the **Cancel** button.

> **Note:** If you click **Cancel**, none of the changes made to this page will be preserved.

In addition, the history is updated when changes are made to the record elsewhere in Interaction Administrator. For example, when a user change his or her password, the **Last Modified** date is updated.

> **Note:** Changes to the licenses for a user or a station do not update the Last Modified date.

Date Created

This date is automatically set when the user creates the initial configuration for this page. If the page was initially created during setup, the date could be blank.

Notes

Type notes about configuration settings and changes. If you change the configuration page and click **OK**, the **Last Modified** date is updated.

You must manually enter the date beside each entry in the **Notes** field to identify the date of each note.

To create a new line in the **Notes** field, press Enter.

Lines

SIP lines concepts

You use Interaction Administrator to configure your SIP interface. CIC enables SIP by default; you do not need to set any server parameters in order to use the SIP-related features. However, you must configure each SIP line you want to use with CIC.

You can associate a SIP line with one, many, or all stations that are connected to the CIC server. For example, you can associate a SIP line with a workstation, fax machine, stand-alone phone, and so on. A single SIP line can handle multiple calls.

> **Note:** You configure stations in the **Stations** container.

CIC uses SIP lines and their associated stations for inbound and outbound calls. SIP lines allow the CIC server to communicate with the SIP boards.

> **Note**: IC Setup Assistant automatically creates three permanent SIP station lines for different transport protocols: < Stations-TCP>, <Stations-UDP>, and < Stations-TLS>. These lines are used for station-to-station calls. You cannot delete them.

Many of the configuration options for a SIP station that is associated with a SIP line are similar to the configuration options for SIP lines. The settings for a SIP **station** configuration always override the settings for the same configuration options for the SIP **line** configuration.

In general, when you set or change the configuration of a SIP line, your settings take effect immediately. No restart is required.

> **Note:** If you change the transport protocol for a line, you must deactivate the line and then reactivate it in order for the change to take effect.

Related topics

Overview of creating SIP lines

Configure a SIP line

Stations

Line groups

Line group configuration

Add and remove lines from a line group

SIP lines concepts

You use Interaction Administrator to configure your SIP interface. CIC enables SIP by default; you do not need to set any server parameters in order to use the SIP-related features. However, you must configure each SIP line you want to use with CIC.

You can associate a SIP line with one, many, or all stations that are connected to the CIC server. For example, you can associate a SIP line with a workstation, fax machine, stand-alone phone, and so on. A single SIP line can handle multiple calls.

> **Note:** You configure stations in the **Stations** container.

CIC uses SIP lines and their associated stations for inbound and outbound calls. SIP lines allow the CIC server to communicate with the SIP boards.

> **Note**: IC Setup Assistant automatically creates three permanent SIP station lines for different transport protocols: < Stations-TCP>, <Stations-UDP>, and < Stations-TLS>. These lines are used for station-to-station calls. You cannot delete them.

Many of the configuration options for a SIP station that is associated with a SIP line are similar to the configuration options for SIP lines. The settings for a SIP **station** configuration always override the settings for the same configuration options for the SIP **line** configuration.

In general, when you set or change the configuration of a SIP line, your settings take effect immediately. No restart is required.

> **Note:** If you change the transport protocol for a line, you must deactivate the line and then reactivate it in order for the change to take effect.

Related topics

Overview of creating SIP lines

Configure a SIP line

Stations

Line groups

Line group configuration

Add and remove lines from a line group

Overview of adding and configuring SIP lines

The process of setting up SIP lines involves multiple containers in Interaction Administrator:

1. In the **Lines** container, add a SIP line.
2. Configure the SIP line. For more information, see *Configure a SIP line*.
3. In the **Server** container, define the global configuration for SIP stations.
4. Configure the SIP workstations.

Related topics

SIP lines concepts

Configure a SIP line

Add a SIP line

To add a SIP line

1. In the ***<IC_Server>*** container, double-click the **Lines** container.
2. In the list view window, right-click and then click **New**.
   The **Entry Name** dialog box appears.
3. Type the line name and then click **OK**.
4. Configure the SIP line.

Related topics

Configure a SIP line

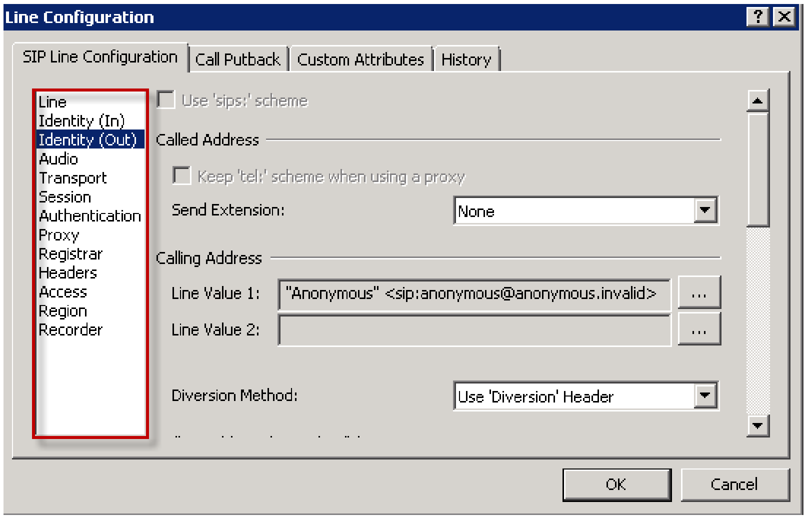
Configure a SIP line

Configure a SIP line

To configure a SIP line

1. In the ***<IC_Server>*** container, double-click the **Lines** container.
2. In the list view window, double-click a line.

3. In the list of options, click **Identity (Out)**.



□ Use 'sips:' scheme

Called Address

□ Keep 'tel:' scheme when using a proxy

Send Extension: None

Calling Address

Line Value 1: "Anonymous" <sip:anonymous@anonymous.invalid>

Line Value 2:

Diversion Method: Use 'Diversion' Header

4. Specify the **Outbound Identity** of the line.

5. In the list of options, click **Access**.

6. Verify that the access type does not conflict with other SIP lines in the same port.

7. As necessary, click the other options in the list and the other tabs in the **Line Configuration** dialog box to specify additional configuration details. For more information on these options, use the links under **Related topics**.

8. Click **OK**.

Related topics

SIP line options

SIP line identity (In) options

SIP line identity (Out) options

SIP line audio options

SIP line transport options

SIP line session options

SIP line authentication options

SIP line proxy options

SIP line registrar options

SIP line headers options

SIP line access options

SIP line region options

SIP line recorder options

SIP Line TLS Security options *(only if the line's transport protocol is TLS)*

Call putback options

Custom attributes

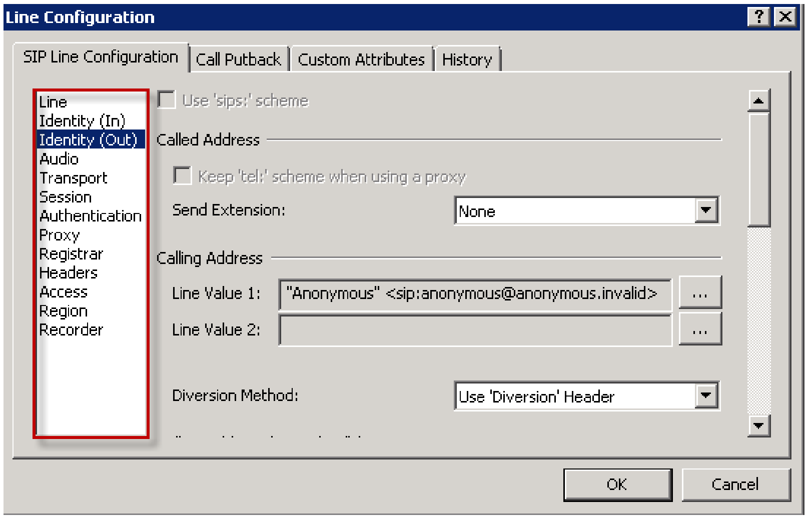
History

Lines concepts

Configure a SIP line

To configure a SIP line

1. In the ***<IC_Server>*** container, double-click the **Lines** container.
2. In the list view window, double-click a line.
3. In the list of options, click **Identity (Out)**.



☐ Use 'sips:' scheme

Called Address

☐ Keep 'tel:' scheme when using a proxy

Send Extension: None

Calling Address

Line Value 1: "Anonymous" <sip:anonymous@anonymous.invalid>

Line Value 2:

Diversion Method: Use 'Diversion' Header

4. Specify the **Outbound Identity** of the line.
5. In the list of options, click **Access**.
6. Verify that the access type does not conflict with other SIP lines in the same port.
7. As necessary, click the other options in the list and the other tabs in the **Line Configuration** dialog box to specify additional configuration details. For more information on these options, use the links under **Related topics**.
8. Click **OK**.

Related topics

SIP line options

SIP line identity (In) options

SIP line identity (Out) options

SIP line audio options

SIP line transport options

SIP line session options

SIP line authentication options

SIP line proxy options

SIP line registrar options

SIP line headers options

SIP line access options

SIP line region options

SIP line recorder options

SIP Line TLS Security options *(only if the line's transport protocol is TLS)*

Call putback options

Custom attributes

History

Lines concepts

Custom attributes

The Custom Attributes page allows you to add customized attributes so that you can reference your own variables and settings through the IceLib interface.

> **Note:** If you enabled the Enhanced Interaction Administrator Change log, then all of your changes to the Custom attributes page in the User Configuration dialog box and the Workgroup Configuration dialog box dialog box are tracked in that log. For more information, see *About the Enhanced Interaction Administrator Change Log*.

The page contains a list for the attributes and displays a **Name** and a **Value** column, and has the following buttons:

Add

Click **Add** and select an existing custom attribute from the pull-down list, enter a new custom attribute. If creating a new attribute, use a unique name, otherwise the existing attribute will be overwritten.

Edit

Click **Edit** to change the value of an existing custom attribute.

Delete

Click **Delete** to delete an existing custom attribute.

Manage Attributes

Click **Manage Attributes** to open a dialog box that displays a list of custom attributes. Click **Add** or **Delete** to manage the appearance of the custom attributes in the pull-down list.

The custom attributes are saved in the path of the root container. This **Path** is displayed at the bottom of the dialog box.

> **Note**: For more information on the Interaction Center Extension Library (IceLib), see The **System APIs section** in the PureConnect Documentation Library on the CIC server.

History

This page provides a way to manually document configuration changes and when they occurred. Changes made in Interaction Administrator are also automatically logged in the Interaction Administrator Change Notification Log (Log ID 7). Later, authorized users can run reports against this log to summarize all configuration changes.

> **Note:** If you enabled the Enhanced Interaction Administrator Change log, then all of your changes to the History page in the User Configuration dialog box and the Workgroup Configuration dialog box dialog box are tracked in that log. For more information, see *About the Enhanced Interaction Administrator Change Log*.

Last Modified

This date is automatically updated each time you click the **OK** button, presumably after you make changes to the configuration. To avoid updating this date, exit the page by clicking the **Cancel** button.

> **Note:** If you click **Cancel**, none of the changes made to this page will be preserved.

In addition, the history is updated when changes are made to the record elsewhere in Interaction Administrator. For example, when a user change his or her password, the **Last Modified** date is updated.

> **Note:** Changes to the licenses for a user or a station do not update the Last Modified date.

Date Created

This date is automatically set when the user creates the initial configuration for this page. If the page was initially created during setup, the date could be blank.

Notes

Type notes about configuration settings and changes. If you change the configuration page and click **OK**, the **Last Modified** date is updated.

You must manually enter the date beside each entry in the **Notes** field to identify the date of each note.

To create a new line in the **Notes** field, press Enter.

Line

SIP line options

The following table describes the general options that you can use to configure a SIP line. For information on how to access these options, see *Configure a SIP line*.

Changes to any of the options on this dialog box take effect immediately.

Option	Description	Default
Active	Activates or deactivates the line in the CIC system. You can not deactivate a line if any calls are on the line. If you change line configuration parameters or to perform other line maintenance, you may have to deactivate a line and then reactivate it in order for the changes to take effect. For example, if you change the SIP line transport protocol. **Note:** Genesys only counts active lines to determine whether you are in compliance with your license agreement.	Active
Line Usage	Designates the usage of the line. The options are: • **General Purpose** • **Microsoft Lync** • **Station Connections**	General Purpose
Domain Name	Specifies the domain name that is used to formulate SIP-URLs for CIC users and phone numbers. This domain name is automatically appended to all REGISTER requests that are sent by CIC. This value is used in the "From" header in outbound SIP calls. **Note:** You can set additional identity settings by click **Identity (In)** and **Identity (Out)** in the options list.	Varies depending on your configuration

Maximum Number of Calls	Designates the maximum limit number of calls that the SIP line processes. When the number of calls is reached, this line processes no more calls. The options are **Combined** or **Inbound/Outbound**: • **Combined** means that the maximum number is the sum of both inbound calls and outbound calls. • **Inbound/Outbound** means that the values specified for each type of call count towards the maximum number of calls. The **No Limit** check box indicates whether there is a maximum limit. If **No Limit** is *not* selected, then you must set a maximum number of calls.	No limit
Fax Protocol	Indicates the fax protocol to use. The options are: • **T30 only** • **T38 only** • **T38 then T30**: If you select this option, CIC tries the T38 fax protocol first. If the recipient endpoint does not support this protocol, then CIC tries the T30 fax protocol.	T38 only
Enable Fax Detection	Indicates whether fax tones are detected when the **Allow Deferred Answer** check box is selected. To determine whether to play the fax detection prompt or not, the system evaluates this check box: • If this check box is selected, then the system overrides the user's setting. • If this option is not selected, then	Selected

	the system uses the user's setting. If you select a **Fax Protocol**, then this check box is also automatically selected. If the Fax Protocol check box is set to **None**, then this check box is not available.	
Maximum Number of Faxes	Designates the maximum limit number of faxes that the SIP line processes. When the number of faxes is reached, this line processes no more faxes. The options are **Combined** or **Inbound/Outbound**: • **Combined** means that the maximum number is the sum of both inbound faxes and outbound faxes. • **Inbound/Outbound** means that the values specified for each type of fax count towards the maximum number of faxes . The **No Limit** check box indicates whether there is a maximum limit. If **No Limit** is *not* selected, then you must set a maximum number of faxes.	No limit
Auto Disconnect when Silence Detected in Voice Mail	Designates whether CIC automatically disconnects a call that is in voice mail after a certain number of seconds of silence. This option is important if your CO (public exchange switch) does not send a disconnect signal (a forward disconnect notice) when a caller disconnects a call. If this check box is selected, when a call is left in voice mail, CIC waits for the number of seconds of silence that you specify in the **Silence Time (ms)** box, and then it automatically disconnects the call. If the CO does not send a disconnect signal, and if this check box is not selected, then the voice mail will continue to record silence.	Selected; The default silence time is 10,000 milliseconds (10 seconds).

Call Analysis Type	Indicates the call analysis type for this SIP line. The options are: ▪ **Media Server**: The Media server listens to the RTP stream and performs call analysis. Use this option with a third-party gateway. ▪ **Interaction Gateway (Gen2 only; *not recommended for new deployments*)**: The CIC server defers to the Interaction Gateway, which listens to the TDM (ISDN) lines and returns the results via SIP messages. Do not use this option with Interaction Gateway. ▪ **Media Server to Interaction Gateway**: Interaction Gateway and Media Server are both used; the Media Server performs call analysis. This is the preferred setting to use with Interaction Gateway and Interaction Gateway Gen2. Do not use this option with any third-party gateway.	Media Server
Allow Deferred Answer	Indicates whether to delay answering an incoming call until an agent is reached or an IVR system is entered. This gives callers time to disconnect the call without being charged by their telecommunications provider. **Note**: Deferred answer is not used with ACD calls. If a call is placed to the DID of an ACD workgroup, interactions are immediately answered before alerting occurs. **Note**: Use the **Allow Multiple Calls to Station On Deferred Answer Line** server parameter to disable the alert to a station for an additional call when **Allow Deferred Answer** is selected.	Not selected
Playback	Indicates whether to use early media	Not selected

Early Media to Inbound Calls	(when the remote party sends SDP before the call is answered in a 183 response) instead of ringback on an inbound call. This option does not apply to ACD calls on this line. **Note**: This option works only if *either* of the following conditions exist: *The CIC server receives an `INVITE` with SDP. *The CIC server receives an `INVITE` with no SDP but with `100rel` in the `Supported:` header. Additionally, this option requires both of the following conditions: *CIC must get an SDP from the remote. *The CIC server must have the `INVITE` and a `PRACK` to get an SDP *before answering.* (`PRACK` requires `100rel`).	
Enable SIP Prack/Update for Early Media Support	This option indicates whether the system tells the SIP line to enable PRACK in the outbound and inbound registration.	Not selected
Max Probation Time (s)	This is the maximum time in seconds for probation on a failed line. To improve query times, the query for line selection ignores lines that are on probation.	600 seconds

Related topics

Configure a SIP line

SIP lines concepts

SIP line Identity (In) options

SIP line identity (Out) options

Transport protocol

Media Server Fax

Fax configuration

SIP line proxy options

SIP line registrar options

SIP line options

The following table describes the general options that you can use to configure a SIP line. For information on how to access these options, see *Configure a SIP line*.

Changes to any of the options on this dialog box take effect immediately.

Option	Description	Default
Active	Activates or deactivates the line in the CIC system. You can not deactivate a line if any calls are on the line. If you change line configuration parameters or to perform other line maintenance, you may have to deactivate a line and then reactivate it in order for the changes to take effect. For example, if you change the SIP line transport protocol. **Note:** Genesys only counts active lines to determine whether you are in compliance with your license agreement.	Active
Line Usage	Designates the usage of the line. The options are: • **General Purpose** • **Microsoft Lync** • **Station Connections**	General Purpose
Domain Name	Specifies the domain name that is used to formulate SIP-URLs for CIC users and phone numbers. This domain name is automatically appended to all REGISTER	Varies depending on your configuration

	requests that are sent by CIC. This value is used in the "From" header in outbound SIP calls. **Note:** You can set additional identity settings by click **Identity (In)** and **Identity (Out)** in the options list.	
Maximum Number of Calls	Designates the maximum limit number of calls that the SIP line processes. When the number of calls is reached, this line processes no more calls. The options are **Combined** or **Inbound/Outbound**: • **Combined** means that the maximum number is the sum of both inbound calls and outbound calls. • **Inbound/Outbound** means that the values specified for each type of call count towards the maximum number of calls. The **No Limit** check box indicates whether there is a maximum limit. If **No Limit** is *not* selected, then you must set a maximum number of calls.	No limit
Fax Protocol	Indicates the fax protocol to use. The options are: • **T30 only** • **T38 only** • **T38 then T30**: If you select this option, CIC tries the T38 fax protocol first. If the recipient endpoint does not support this protocol, then CIC tries the T30 fax protocol.	T38 only
Enable Fax Detection	Indicates whether fax tones are detected when the **Allow Deferred Answer** check box is selected.	Selected

	To determine whether to play the fax detection prompt or not, the system evaluates this check box: • If this check box is selected, then the system overrides the user's setting. • If this option is not selected, then the system uses the user's setting. If you select a **Fax Protocol**, then this check box is also automatically selected. If the Fax Protocol check box is set to **None**, then this check box is not available.	
Maximum Number of Faxes	Designates the maximum limit number of faxes that the SIP line processes. When the number of faxes is reached, this line processes no more faxes. The options are **Combined** or **Inbound/Outbound**: • **Combined** means that the maximum number is the sum of both inbound faxes and outbound faxes. • **Inbound/Outbound** means that the values specified for each type of fax count towards the maximum number of faxes . The **No Limit** check box indicates whether there is a maximum limit. If **No Limit** is *not* selected, then you must set a maximum number of faxes.	No limit
Auto Disconnect when Silence Detected in Voice Mail	Designates whether CIC automatically disconnects a call that is in voice mail after a certain number of seconds of silence. This option is important if your CO (public exchange switch) does not send a disconnect signal (a forward disconnect notice) when a caller disconnects a call. If this check box is selected, when a call is left in voice mail, CIC waits for the number	Selected; The default silence time is 10,000 milliseconds (10 seconds).

	of seconds of silence that you specify in the **Silence Time (ms)** box, and then it automatically disconnects the call. If the CO does not send a disconnect signal, and if this check box is not selected, then the voice mail will continue to record silence.	
Call Analysis Type	Indicates the call analysis type for this SIP line. The options are: ▪ **Media Server**: The Media server listens to the RTP stream and performs call analysis. Use this option with a third-party gateway. ▪ **Interaction Gateway (Gen2 only; *not recommended for new deployments*)**: The CIC server defers to the Interaction Gateway, which listens to the TDM (ISDN) lines and returns the results via SIP messages. Do not use this option with Interaction Gateway. ▪ **Media Server to Interaction Gateway**: Interaction Gateway and Media Server are both used; the Media Server performs call analysis. This is the preferred setting to use with Interaction Gateway and Interaction Gateway Gen2. Do not use this option with any third-party gateway.	Media Server
Allow Deferred Answer	Indicates whether to delay answering an incoming call until an agent is reached or an IVR system is entered. This gives callers time to disconnect the call without being charged by their telecommunications provider. **Note**: Deferred answer is not used with ACD calls. If a call is placed to the DID of an ACD workgroup, interactions are immediately	Not selected

	answered before alerting occurs. **Note**: Use the **Allow Multiple Calls to Station On Deferred Answer Line** server parameter to disable the alert to a station for an additional call when **Allow Deferred Answer** is selected.	
Playback Early Media to Inbound Calls	Indicates whether to use early media (when the remote party sends SDP before the call is answered in a 183 response) instead of ringback on an inbound call. This option does not apply to ACD calls on this line. **Note**: This option works only if *either* of the following conditions exist: *The CIC server receives an `INVITE` with SDP. *The CIC server receives an `INVITE` with no SDP but with `100rel` in the `Supported:` header. Additionally, this option requires both of the following conditions: *CIC must get an SDP from the remote. *The CIC server must have the `INVITE` and a `PRACK` to get an SDP *before answering.* (`PRACK` requires `100rel`).	Not selected
Enable SIP Prack/Update for Early Media Support	This option indicates whether the system tells the SIP line to enable PRACK in the outbound and inbound registration.	Not selected
Max Probation Time (s)	This is the maximum time in seconds for probation on a failed line. To improve query times, the query for line selection ignores lines that are on probation.	600 seconds

Related topics

Configure a SIP line

SIP lines concepts

SIP line Identity (In) options

SIP line identity (Out) options

Transport protocol

Media Server Fax

Fax configuration

SIP line proxy options

SIP line registrar options

Identity In

SIP line identity (in) concepts

You can configure line identity options for inbound SIP interactions. Inbound SIP line behavior includes how CIC passes SIP line extensions in SIP messages, what CIC considers a diverted call and what information it passes, and how CIC routes an inbound call.

> **Note**: All **Inbound Identity** settings affect the values of the **Eic_RemoteAddress** and **Eic_RemoteId** call attributes.

Related topics

SIP line identity (In) options

Configure a SIP line

Lines concepts

SIP line identity (in) options

The following table describes the options that you can use to configure inbound identity options for a SIP line. For information on how to access these options, see *Configure a SIP line*.

Changes to all of the options on this dialog box take effect immediately.

Option	Description	Default
Use only numeric portion	Determines whether only the numeric portion of the caller ID is displayed. If this option is selected, then all other information is removed.	Selected

	For example: • If this check box is selected, the caller ID appears as **3178723000**. • If this check box is not selected, the caller ID appears as **sip:3178723000@123.45.67.89**. **Notes**: **If you do not select this check box**, then CIC's telephony services do not change the inbound address and extension before the dial plan standardizes the address. The address appears in this format: sip:8723000;ext=999@inin.com. **If you do select this check box,** then CIC's telephony services changes the inbound address and extension before the dial plan standardizes the address. The address appears in this format: (317) 872-3000 ^ 999. **If you do select this check box, and if the user portion of the SIP address is *not* numeric,** then the entire SIP address is used as the caller ID.	
Called Address	Designates the *local* selection method. The options are: ▪ **Use Request URI:** displays the destination address in the form <sip:counsel@acme.com>. ▪ **Use 'To' header:** displays the "To" field in the SIP header as the called address (the destination address). ▪ If the field contains both a URI and a display name, then both of these items are displayed. For example, "Patty Johnson" <sip:counsel@acme.com>. ▪ If the field contains only a display name, then it is displayed alone. For example, "Patty Johnson."	Use Request URI
Use this diversion info if present	Displays the diversion information, such as the original or most recent line value. This information is contained in the URI address field in the SIP message. When this option is enabled, you can select the following values:	Not selected

	• **Use most recent** • **Use original**	
Calling Address	Designates the remote selection method. P-Asserted-Identity is a header field in a SIP message that contains a URI and display name (optional). For example, "Patty Johnson" <sip:counsel@acme.com>. The options are: • **Use 'From' header only:** displays only the "From" field in the SIP header as the calling address (the origination address). • If the field contains both a URI and a display name, then both of these items are displayed. For example, "Patty Johnson" <sip:counsel@acme.com>. • If the field contains only a display name, then it is displayed alone. For example, "Patty Johnson." • **Use 'P-Asserted-Identity' header only:** displays only the authenticated sender origination information from the SIP message. If the "P-Asserted-Identity" header information is not available and no value is set in the header, then the number appears as “Private number,” and the name appears as “Unknown Name.” • **Use 'P-Asserted-Identity' header then 'From' header" (default)**: displays the authenticated sender information from the SIP message. • If the "P-Asserted-Identity" header is known, then that value is used and then the "From" header information is used. • If the "P-Asserted-Identity" header is unknown, then only the "From" header information is used.	Use 'P-Asserted-Identity' header then 'From' header
Ignore address if user portion is not numeric	if the address is not numeric (for example, <sip:counsel@acme.com>), then this option sets the **From** field to "Unknown."	Not selected

	You can optionally use this option with the **Use only numeric portion** check box. Either way, the CIC client displays the call as "Private Number.”	

Related topics

Configure a SIP line

Dial plan

Line options reference

SIP line identity (in) concepts

Lines concepts

Identity Out

SIP line identity (Out) concepts

You can configure line identity options for outbound SIP interactions. Outbound SIP line behavior includes how CIC passes SIP line extensions in SIP messages, what CIC considers a diverted call and what information it passes, and how CIC routes an outbound call.

Related topics

SIP line identity (out) options

Configure a SIP line

Lines concepts

SIP line identity (out) options

The following table describes the options that you can use to configure outbound identity options for a SIP line. For information on how to access these options, see *Configure a SIP line*.

Changes to all of the options on this dialog box take effect immediately.

Option	Description	Default
Use 'sips:' scheme	**Note:** This option is applicable only to TLS lines. Converts the SIP address in the "From" header to use SIPS	Not selected

	instead of SIP. SIPS is a secure transmission that uses the URI format. For example: <sips:+13178723000@ICServer:5061>. If you do not select this option, CIC converts all SIPS to SIP.	
Called Address: **Keep 'tel:' scheme when using a proxy**	**Note**: This option is available only if one or more proxy addresses are configured. It is available for all three line protocols. Determines whether CIC uses the telephone format (tel:NNNNNNNNNN) for the remote address. If you do not select this option, CIC converts the phone and phone number to the SIP format (SIP:NNNNNNN@ipaddress).	Not selected
Called Address: **Send Extension**	Determines whether CIC dials an extension if one is passed. If this option is selected, then CIC dials it after "/." The options are: • **None**: CIC does not include the extension in the SIP message. • **Use** 'ext=' • **Post Connect**: After the call connects, CIC sends the extension as DTMF tones.	Post Connect
Calling Address: **Line Value 1**	Sets the first calling address. After you set the value here, you can select it for the **Calling Address** options below. For more information, see *SIP Line Options* and *Configure a line value.*	Not specified
Calling Address: **Line Value 2**	Sets the second calling address. After you set the value here, you can select it for the **Calling Address** options below. For more information, see *SIP Line Options* and *Configure a line value.*	Not specified
Calling Address: Diversion Method	Sets how an outbound call on this line is indicated to the network. The **Use 'Diversion' Header** setting causes the line to use a	Use 'Diversion' Header

	header with diversion information, such as the origination address or the most recent address.	
Calling Address (Normal Calls): **From Header Address**	Sets the value that appears as the local address in an outbound SIP interaction that is not diverted or redirected. The options are: ▪ **Use line value 1**: displays the value in the **Line Value 1** field. ▪ **Use line value 2**: displays the value in the **Line Value 2** field. ▪ **Use passed value if present**: displays the CIC user's outbound ANI. For example, "Name if present" <sip:+13178723000@ICServer.ININ.com>.	Use passed value if present
Calling Address (Normal Calls): **From Header Name**	Sets the value that appears as the local name in an outbound SIP interaction that is not diverted or redirected. The options are: ▪ **Use line value 1**: displays the value in the **Line Value 1** field. ▪ **Use line value 2**: displays the value in the **Line Value 2** field. ▪ **Use passed value if present**: displays the name value that the handlers pass. If the handlers do not pass a value, and if the CIC user's outbound ANI is configured, then CIC uses the CIC user's display name. For example, "CIC User's Display Name" <sip:+13178723000@ICServer.ININ.com>. ▪ **None:** displays only the address value.	Use passed value if present
Calling Address (Normal Calls): **'P-Asserted-Identity' Header Address**	Sets the value that appears as the authenticated local address in the outbound SIP interaction that is not diverted or redirected. The options are:	None

	▪ **Use line value 1**: displays the value in the **Line Value 1** field. ▪ **Use line value 2**: displays the value in the **Line Value 2** field. ▪ **Use passed value if present**: displays the address value that the handlers pass. If the handlers do not pass a value, then CIC displays the CIC user's outbound ANI. For example, "Name if present" <sip:+13178723000@ICServer.ININ.com>. ▪ **None:** displays neither the address nor the name.	
Calling Address (Normal Calls): **'P-Asserted-Identity' Header Name**	Sets the value that appears as the authenticated local name in the outbound SIP interaction that is not diverted or redirected. The options are: ▪ **Use line value 1**: displays the value in the **Line Value 1** field. ▪ **Use line value 2**: displays the value in the **Line Value 2** field. ▪ **Use passed value if present**: displays the name value that the handlers pass. If the handlers do not pass a value, and if the CIC user's outbound ANI is configured, then CIC displays the CIC user's display name. For example, "CIC User's Display Name" <sip:+13178723000@ICServer.ININ.com>. ▪ **None:** displays neither the address nor the name. **Note**: This option is not available if **'P-Asserted-Identity' Header Address** is set to **None**.	None
Calling Address (Normal Calls)**: Diverted Header Address**	Sets the value that appears as the destination address in the diversion header for the outbound SIP interaction. The options are: ▪ **Use line value 1**: displays the value in the **Line Value 1** field.	None

	▪ **Use line value 2**: displays the value in the **Line Value 2** field. ▪ **Use passed value if present**: displays the address value that the handlers pass. If the handlers do not pass a value then CIC uses the CIC user's outbound ANI. For example, "Name if Present" <tel:+13178723000>. ▪ **None:** displays neither the address nor the name.	
Calling Address (Normal Calls): **Diverted Header Name**	Sets the value that appears as the destination name in the diversion header for an outbound SIP interaction. The options are: ▪ **Use line value 1**: displays the value in the **Line Value 1** field. ▪ **Use line value 2**: displays the value in the **Line Value 2** field. ▪ **Use passed value if present**: displays the name value that the handlers pass. If the handlers do not pass a value, and if the CIC user's outbound ANI is configured, then CIC displays the CIC user's display name. For example, "CIC User's Display Name" <tel:+13178723000>. ▪ **None:** displays neither the address nor the name. **Note**: This setting is not available if **Diversion Header Address** is set to **None**.	None
Calling Address (Diverted Calls): **'From' Header Address**	Sets the value that appears as the local address in an outbound SIP interaction that is redirected. This is typically a follow-me or forwarded interaction. The options are: ▪ **Use line value 1**: displays the value in the **Line Value 1** field. ▪ **Use line value 2**: displays the value in the **Line Value 2** field. ▪ **Use passed value if present**: displays the CIC *calling* user 1 outbound ANI. For example, "User 1 Name if Present" <sip:+13178723000@ICServer.ININ.com>. For external to follow-me interactions and forwarded	Use passed value if present

	interactions, CIC displays the **From** address of the external device. ▪ **Use diverted value**: displays the CIC user 2 outbound ANI. For example, "User 2 Name if Present" <sip:+13178723000@ICServer.ININ.com>.	
Calling Address (Diverted Calls): **'From' Header Name**	Sets the value that appears as the local name in an outbound SIP interaction that is redirected. This is typically a follow-me or forwarded interaction. The options are: ▪ **Use line value 1**: displays the value in the **Line Value 1** field. ▪ **Use line value 2**: displays the value in the **Line Value 2** field. ▪ **Use passed value if present**: displays the CIC *calling* user 1 display name, if the user's outbound ANI is configured. For example, "CIC User 1 display name" <sip:+13178723000@ICServer.ININ.com>. For external to follow-me interactions and forwarded interactions, CIC displays the **From** name of the external device. ▪ **Use diverted value**: displays the CIC user 2 display name if the user's outbound ANI is configured. For example, "CIC User 2 display name" <sip:+13178723000@ICServer.ININ.com>. ▪ **None:** displays the address only.	Use passed value if present
Calling Address (Diverted Calls): **'P-Asserted-Identity' Address**	Sets the value that appears as the authenticated local address in an outbound SIP interaction that is redirected. This is typically a follow-me interaction or a forwarded interaction. The options are: ▪ **Use line value 1**: displays the value in the **Line Value 1** field. ▪ **Use line value 2**: displays the value in the **Line Value 2** field. ▪ **Use passed value if present**: displays the CIC *calling* user 1 outbound ANI. For example, "User 1 Name if Present" <sip:+13178723000@ICServer.ININ.com>. For external to follow-me interactions or forwarded	None

	interactions, CIC displays the authenticated **From** address of the external device. ▪ **Use diverted value**: displays the CIC user 2 outbound ANI. For example, "User 2 Name if present" <sip:+13178723000@ICServer.ININ.com>. ▪ **None:** displays neither the address nor the name.	
Calling Address (Diverted Calls): **'P-Asserted-Identity' Name**	Sets the value that appears as the authenticated local name in an outbound SIP interaction that is redirected. This is typically a follow-me interaction or a forwarded interaction. The options are: ▪ **Use line value 1**: displays the value in the **Line Value 1** field. ▪ **Use line value 2**: displays the value in the **Line Value 2** field. ▪ **Use passed value if present**: displays the name value that the handlers pass. If the handlers do not pass a value, then CIC displays the user's outbound ANI, if it is configured. For example, "CIC user's Outbound ANI" <sip:+13178723000@ICServer.ININ.com>. For external to follow-me interactions or forward interactions, CIC displays the authenticated **From** name of the external device. ▪ **Use diverted value**: displays the CIC user 1 display name if the user's outbound ANI is configured. For example, "CIC User 1 display name" <sip:+13178723000@ICServer.ININ.com>. ▪ **None**: displays the address only. **Note**: This option is unavailable if **'P-Asserted-Identity' Address** is set to **None**.	None
Calling Address (Diverted Calls): **Diverted Header Address**	Sets the value that appears as the destination address in the diversion header for an outbound SIP interaction that is redirected. This is typically a follow-me interaction or forwarded interaction. The options are: ▪ **Use line value 1**: displays the value in the **Line Value 1** field.	Use diverted value

	▪ **Use line value 2**: displays the value in the **Line Value 2** field. ▪ **Use passed value if present**: displays the address value that the handlers pass. If the handlers do not pass a value then CIC displays the CIC user 1 outbound ANI, if it is configured. For example, "CIC User 1 Outbound ANI" <sip:+13178723000@ICServer.ININ.com>. ▪ **Use diverted value:** displays the CIC user 1 outbound ANI, if it is configured. For example, "CIC User 1 Outbound ANI" <tel:+13178723000>. ▪ **None**: displays neither the address nor the name.	
Calling Address (Diverted Calls): **Diverted Header Name**	Sets the value that appears as the destination name in the diversion header for an outbound SIP interaction that is redirected. This is typically a follow-me or forwarded interaction. The options are: ▪ **Use line value 1**: displays the value in the **Line Value 1** field. ▪ **Use line value 2**: displays the value in the **Line Value 2** field. ▪ **Select "Use passed value if present**: displays the name value that the handlers pass. If the handlers do not pass a value then CIC displays the CIC user 1 display name, if the user's outbound ANI is configured. For example, "CIC User 1 display name" <sip:+13178723000@ICServer.ININ.com>. ▪ **Use diverted value**: displays the CIC user 1 display name if the user's outbound ANI is configured. For example, "CIC User 1 display name" <sip:+13178723000@ICServer.ININ.com>. ▪ **None**: displays neither the address nor the name. **Note**: This setting is unavailable if **Diversion Header Address** is set to **None**.	Use diverted value

Related topics

SIP line identity (out) concepts

Configure a SIP line

Configure a line value

User outbound ANI configuration

Lines concepts

Configure a SIP line value

You can configure the appearance of an outbound SIP line. You then select a line appearance (value) for each **Calling Address** option when you configure the identity (out) options for a SIP line.

For more information on configuring the outbound identity of a SIP line, see *Configure a line* and *Identity (out) options*.

To configure a line value

1. In the <IC_Server> container, double-click the Lines container.
2. Do one of the following:

- To add a new line, in the list view window, right-click and then click **New**.
  The **Entry Name** dialog box appears.
  Type the line name and then click **OK**.
- To edit an existing line, in the list view window, double-click a line

3. In the **Line Configuration** dialog box, in the list of options, click **Identity (Out)**.

4. In the **Calling Address** section, next to the **Line Value 1** field or the **Line Value 2** field, click **...**
The **Configure Line Value** dialog box appears.

5. To display non-specific information for the outbound line identification, select the **Use Anonymous** values check box.
This option displays: Address = "sip:anonymous@anonymous.invalid," Name = "Anonymous.”

6. In the **Name** box, type the SIP phone name (or line name). CIC automatically displays this information. Additionally, this information appears in the **From** header in outbound SIP calls.
If you select **Use Anonymous**, then "Anonymous" appears in the **From** header. Alternatively, a handler can set a name value.

7. In the **Address** box, type the SIP phone number (or line number). CIC automatically displays this information. Additionally, this information appears in the **From** header in outbound SIP calls.
If you select **Use Anonymous**, then "sip:anonymous@anonymous.invalid" appears in the **From** header. Alternatively, a handler can set an address value.

8. The **Display** value box displays the actual value as it appears in CIC.

9. Click **OK**.

Related topics

Identity (out) options

Configure a SIP line

Lines concepts

Audio

SIP line audio options

The following table describes the options that you can use to configure audio options for a SIP line. For information on how to access these options, see *Configure a SIP line*.

Changes to all of the options on this dialog box take effect immediately.

Option	Description	Default
Audio Path	For information on the available options, see the following resources on the Product Information site: • *SIP Application Note* • *Telephony Applications Note* • *Interaction Media Server document*	Dynamic
DTMF Type	Sets the Dual Tone Multi-Frequency (DTMF) type for the station. The options are: • Do not use RFC2833 inband only • **RFC2833 if supported, otherwise inband** (default) • **RFC2833 only**.	RFC2833 if supported, otherwise inband
DTMF Payload	Sets the value that is used for the DTMF Real-time Transport Protocol (RTP) payload value. The acceptable values are 96-127. The vendor-specific values are:100, 102-105. Vendor-specific values should not be used for AudioCodes stations.	101
Voice Activation Detection (VAD)	Determines whether packets are sent for silence.	18 (24, 011000) CS53
	When **Voice Activation Detection** is selected, no packets are sent for silence. This option saves bandwidth on your network. However, like compression, there is some loss of voice quality.	Not selected

Echo Cancellation	Determines whether echo cancellation is used. Echo cancellation removes echoes from voice communication to improve the sound quality.	Selected
Allow Multiple Codecs in Outbound SDP Offer	This option indicates whether CIC delivers all of the available Codecs to the recipient endpoint when a user makes an outbound call. The recipient endpoint can then select which Codec it recognizes. You set up Codecs in the **Locations** container.	Not Selected

Related topics

Configure a SIP line

Lines concepts

SIP line audio options

The following table describes the options that you can use to configure audio options for a SIP line. For information on how to access these options, see *Configure a SIP line*.

Changes to all of the options on this dialog box take effect immediately.

Option	Description	Default
Audio Path	For information on the available options, see the following resources on the Product Information site: • *SIP Application Note* • *Telephony Applications Note* • *Interaction Media Server document*	Dynamic
DTMF Type	Sets the Dual Tone Multi-Frequency (DTMF) type for the station. The options are: • Do not use RFC2833 inband only • **RFC2833 if supported, otherwise inband** (default) • **RFC2833 only**.	RFC2833 if supported, otherwise inband

DTMF Payload	Sets the value that is used for the DTMF Real-time Transport Protocol (RTP) payload value. The acceptable values are 96-127. The vendor-specific values are:100, 102-105. Vendor-specific values should not be used for AudioCodes stations.	101
Voice Activation Detection (VAD)	Determines whether packets are sent for silence. When **Voice Activation Detection** is selected, no packets are sent for silence. This option saves bandwidth on your network. However, like compression, there is some loss of voice quality.	18 (24, 011000) CS53 Not selected
Echo Cancellation	Determines whether echo cancellation is used. Echo cancellation removes echoes from voice communication to improve the sound quality.	Selected
Allow Multiple Codecs in Outbound SDP Offer	This option indicates whether CIC delivers all of the available Codecs to the recipient endpoint when a user makes an outbound call. The recipient endpoint can then select which Codec it recognizes. You set up Codecs in the **Locations** container.	Not Selected

Related topics

Configure a SIP line

Lines concepts

Transport

SIP line transport options

The following table describes the options that you can use to configure transport options for a SIP line. For information on how to access these options, see *Configure a SIP line*.

Changes to *most* of the options on this dialog box take effect immediately.

Note: The protocol and port settings on this page are static. You must restart the CIC server in order for changes to these settings to take effect.

Option	Description	Default
Transport Protocol	Sets the transport protocol. Your selection depends on the protocols that are supported by your SIP-enabled devices (gateway, phones, and so on). The options are: • **TCP** (Transmission Control Protocol). The **TCP** station line is available if needed. Most new IP phones support TCP. • **TLS** (Transport Layer Security or SSL). This option requires the **Advanced Security** feature license. After you select it, the TLS Security configuration option appears. • **UDP** (User Datagram Protocol). Nearly all IP phones support UDP. **Note**: If you change the transport protocol, you must deactivate and reactivate the line in order for the change to take effect. The line cannot be deactivated if any calls are active on it. When a line is deactivated, no calls can be taken. Therefore, after you deactivate the	UDP

	line, reactivate it and then verify that it can take calls. The other available options on this dialog box depend on the transport protocol that you select.	
Audio Protocol	Indicates whether the audio stream is unencrypted or encrypted. The options are: • **RTP** (Real Time Protocol): The audio stream is unencrypted. • **SRTP** (Secure RTP): The audio stream is encrypted. This option is available only if you select the **TLS** transport protocol. Select **SRTP** only if the endpoint(s) on this line support SRTP. If you select **SRTP**, the **Security** option is also available. Calls between devices that transmit and receive SIP TLS messages and SRTP audio are completely secure.	RTP (unencrypted)
Security	The **Security** setting determines, in part, whether the security lock icon appears in the CIC clients when a user places or receives an insecure call on this SIP line. The **Security** option is	Depends on your selection for the transport protocol

	available only when you select the **SRTP** audio protocol. In a CIC system environment, some devices may be configured to use SRTP while others do not. When two devices that use SRTP connect directly, both Interaction Clients display the lock icon to indicate that the call is secure from "end to end." The display of this lock icon is automatic and is not configurable. If one device uses SRTP and another device does not, then at least one segment of a call between these devices is insecure. The audio between these devices needs to be transcrypted (converted) between SRTP and RTP via an intermediate device such as the media server. If a SIP line handles insecure calls, you can configure the display of an open-lock icon to inform CIC client users that the call is not secure. The options are: • **Minimal:** hides the display of the open-lock icon on non-secure calls. If you select this option, completely secure calls always show the lock icon and all other calls show no lock icon. If a secure call creates a conference that includes a non-	

	secure call, the lock icon disappears to indicate that the call is no longer secure. • **End-to-Edge:** displays the open-lock icon when a call, or at least one segment of a call in the CIC system domain is or becomes non-secure. End-to-edge means from one end of the call in the CIC system up to the edge of the CIC system (a gateway connected to the PSTN). It does not indicate security conditions on the PSTN or service provider outside of the CIC domain. If you select this option, secure calls always show the lock icon and all other calls that are non-secure show the open-lock icon. If a secure call creates a conference that includes a non-secure call, all parties in the conference see the lock icon turn into an open-lock icon. Conversely, if a non-secure conference call becomes secure from all of the end points to the edge of the CIC system, the open-lock icons	

	change to lock icons.	
Adapter Name	Determines the local server IP address. The name of the adapter appears below the list. This setting was formerly **Address to Use**.	The actual name of your network adapter. This value is typically *Local Area Connection* because that is the default network adapter name that Windows uses.
Usable Addresses	CIC displays the list of IP addresses assigned for the chosen adaptor. This option is available only if the **EnableIPv6** server parameter is set to 1 (true).	Not specified.
Address Family	Sets the family of addresses to which CIC listens. CIC listens to all IP address assigned to each family. This option is available only if the **EnableIPv6** server parameter is set to 1 (true). The options are: • **IPv4** • **IPv6** • **Telephony Default (IPv4 and IPv6)**. The host name resolves to both IPv4 and IPv6.	The default setting uses the order returned from a DNS query. If there are multiple IP addresses, CIC uses the first IP address in that range.
Media Address Family	Specifies the media address family to which CIC should listen. This option is available only if the **EnableIPv6** server parameter is set to 1 (true). The options are • **IPv4**	

	- **IPv6** - **Telephony Default (IPv4 and IPv6)**. The host name resolves to both IPv4 and IPv6. This option is typically used when CIC offers media, but it also helps to determine an answer when CIC receives identical media types and transport protocols for IPv4 and IPv6 information in the session description protocol (SDP).	
Receive Port	**UDP, TCP, and TLS**: This option sets the port number for which the CIC SIP engine services requests. The valid values are 1024 to 65535. TLS runs on top of TCP. There is a conflict if TCP is set on the same port or the same protocol. A new SIP line cannot have the same port **and** the same protocol as an existing SIP line. However, a new line may use the same port of an existing line if it uses a different protocol. For more information, see *PureConnect Security Features* in the PureConnect Documentation Library.	The default is **5060.** For TLS, this is set to 5061.
Connect Timer	**TCP and TLS only:** Sets the timer value in milliseconds	2000

	for TCP connections on the SIP Line. The valid values are 500 to 20000 (milliseconds).	
T1 Timer (ms)	**UDP only**: Sets the timer value in milliseconds that represents the initial incremental delay between packet retransmission. The valid values are 500 to T2 (milliseconds).	500
T2 Timer (ms)	**UDP only**: Sets the timer value in milliseconds that represents the maximum incremental delay between packet retransmissions. The valid values are any values greater than or equal to 1000 (milliseconds).	1000
Maximum Packet Retry	**UDP only**: Sets the maximum number of packet retry attempts for requests. Valid values are from 0 to 10.	4
Maximum Invite Retry	**UDP only**: Sets the maximum number of packet retry attempts for INVITE and ACK requests. Valid values are from 0 to 6.	3
Reinvite Delay (ms)	**UDP only**: Sets the reinvite delay in milliseconds.	50
Retryable Reason Codes	Defines the list of valid SIP reason codes. If this line is part of a line group, and an outbound call that is made on this line returns a valid SIP reason code, then CIC retries	480, 500-599

	the call on the next line in the line group. Separate reason codes or ranges of reason codes with commas. For example: "500-599" Or... "401, 480, 490-495, 500-599" **Note**: "480" is not available on lines that are enabled for Microsoft Lync.	
Retryable Cause Codes	Defines a list of SIP cause codes. Cause codes take precedence over SIP response codes for retry attempts. If dial attempts are exhausted, the disconnect is treated as the most recent cause code if a cause code was present on any of the dial attempts. All dial attempts are traced at the note level when multiple retries are not treated as a 'no available lines' error. Separate cause codes with commas. For example: "503, 507, 550"	The default value is 1-5,25,27,28,31,34,38,41,42,44,46,62,63,79,91,96,97,99,100,103
SIP DSCP Value	Sets the Differentiated Services Code Point (DSCP) value of Quality of Service (QoS) in transmitted SIP packets. The values are shown in both hex (00..3F) and related decimal (0..63) formats. Some values are also identified by the binary format, CS6. The range of valid values is	18 (24, 011000) CS3

	00 (0, 000000) through 3F (63, 111111).	
Inbound Progress Timer (ms)	Sets the number of milliseconds to wait before sending the 180 RINGING message. If the call is answered before this time expires, the 180 RINGING message is not sent. Acceptable values are 1000 through 60,000 milliseconds	5000
No Inbound Progress Timer	Determines whether the 180 RINGING message is never sent on this SIP line.	Not selected
SIP Answer Delay (ms)	Sets the number of milliseconds of delay to insert before a call is answered. This setting is useful when there is some audio loss during call setup. The acceptable values are from 0 through 8,000 milliseconds. If the value is greater than or equal to 1000 milliseconds, an 180 Ringing SIP signal is sent before delay is inserted. Regardless of the value, the delay is always inserted after 200 OK is sent back.	500 milliseconds

Related topics

Configure a SIP line

PureConnect Customer Care

SIP line transport concepts

SIP lines concepts

SIP line transport concepts

You can configure the SIP line transport options to specify secure protocols to encrypt SIP messages and audio streams, define security indicator behavior for the CIC clients, and specify encryption cipher suites and authentication certificates for each SIP line.

You can also set some of these configuration options at the station level. Station-level settings override the corresponding line-level settings.

The transport protocol corresponds to Layer 4 in the Open Systems Interconnection (OSI) reference model. The protocol that you use depends on the features that your devices support.

Related topics

SIP line transport options

Configure a SIP line

Lines concepts

SIP line transport options

The following table describes the options that you can use to configure transport options for a SIP line. For information on how to access these options, see *Configure a SIP line*.

Changes to *most* of the options on this dialog box take effect immediately.

> **Note:** The protocol and port settings on this page are static. You must restart the CIC server in order for changes to these settings to take effect.

Option	Description	Default
Transport Protocol	Sets the transport protocol. Your selection depends on the protocols that are supported by your SIP-enabled devices (gateway, phones, and so on). The options are: • **TCP** (Transmission Control Protocol). The **TCP** station line is available if needed. Most new IP phones support TCP.	UDP

	• **TLS** (Transport Layer Security or SSL). This option requires the **Advanced Security** feature license. After you select it, the TLS Security configuration option appears. • **UDP** (User Datagram Protocol). Nearly all IP phones support UDP. **Note**: If you change the transport protocol, you must deactivate and reactivate the line in order for the change to take effect. The line cannot be deactivated if any calls are active on it. When a line is deactivated, no calls can be taken. Therefore, after you deactivate the line, reactivate it and then verify that it can take calls. The other available options on this dialog box depend on the transport protocol that you select.	
Audio Protocol	Indicates whether the audio stream is unencrypted or encrypted. The options are: • **RTP** (Real Time Protocol): The audio stream is unencrypted. • **SRTP** (Secure RTP):	RTP (unencrypted)

	The audio stream is encrypted. This option is available only if you select the **TLS** transport protocol. Select **SRTP** only if the endpoint(s) on this line support SRTP. If you select **SRTP**, the **Security** option is also available. Calls between devices that transmit and receive SIP TLS messages and SRTP audio are completely secure.	
Security	The **Security** setting determines, in part, whether the security lock icon appears in the CIC clients when a user places or receives an insecure call on this SIP line. The **Security** option is available only when you select the **SRTP** audio protocol. In a CIC system environment, some devices may be configured to use SRTP while others do not. When two devices that use SRTP connect directly, both Interaction Clients display the lock icon to indicate that the call is secure from "end to end." The display of this lock icon is automatic and is not configurable. If one device uses SRTP and another device does not, then at least one segment of a call between these devices is insecure. The audio	Depends on your selection for the transport protocol

	between these devices needs to be transcrypted (converted) between SRTP and RTP via an intermediate device such as the media server. If a SIP line handles insecure calls, you can configure the display of an open-lock icon to inform CIC client users that the call is not secure. The options are: • **Minimal:** hides the display of the open-lock icon on non-secure calls. If you select this option, completely secure calls always show the lock icon and all other calls show no lock icon. If a secure call creates a conference that includes a non-secure call, the lock icon disappears to indicate that the call is no longer secure. • **End-to-Edge:** displays the open-lock icon when a call, or at least one segment of a call in the CIC system domain is or becomes non-secure. End-to-edge means from one end of the call in the CIC system up to the edge of the CIC system (a gateway connected to the PSTN). It does not indicate security	

	conditions on the PSTN or service provider outside of the CIC domain. If you select this option, secure calls always show the lock icon and all other calls that are non-secure show the open-lock icon. If a secure call creates a conference that includes a non-secure call, all parties in the conference see the lock icon turn into an open-lock icon. Conversely, if a non-secure conference call becomes secure from all of the end points to the edge of the CIC system, the open-lock icons change to lock icons.	
Adapter Name	Determines the local server IP address. The name of the adapter appears below the list. This setting was formerly **Address to Use**.	The actual name of your network adapter. This value is typically *Local Area Connection* because that is the default network adapter name that Windows uses.
Usable Addresses	CIC displays the list of IP addresses assigned for the chosen adaptor. This option is available only if the **EnableIPv6** server parameter is set to 1 (true).	Not specified.
Address Family	Sets the family of addresses to which CIC listens. CIC listens to all IP address	The default setting uses the order returned from a DNS query. If there are multiple IP addresses, CIC uses the first IP address in that range.

	assigned to each family. This option is available only if the **EnableIPv6** server parameter is set to 1 (true). The options are: • **IPv4** • **IPv6** • **Telephony Default (IPv4 and IPv6)**. The host name resolves to both IPv4 and IPv6.	
Media Address Family	Specifies the media address family to which CIC should listen. This option is available only if the **EnableIPv6** server parameter is set to 1 (true). The options are • **IPv4** • **IPv6** • **Telephony Default (IPv4 and IPv6)**. The host name resolves to both IPv4 and IPv6. This option is typically used when CIC offers media, but it also helps to determine an answer when CIC receives identical media types and transport protocols for IPv4 and IPv6 information in the session description protocol (SDP).	
Receive	**UDP, TCP, and TLS**: This option sets the port number	The default is **5060.**

Port	for which the CIC SIP engine services requests. The valid values are 1024 to 65535. TLS runs on top of TCP. There is a conflict if TCP is set on the same port or the same protocol. A new SIP line cannot have the same port **and** the same protocol as an existing SIP line. However, a new line may use the same port of an existing line if it uses a different protocol. For more information, see *PureConnect Security Features* in the PureConnect Documentation Library.	For TLS, this is set to 5061.
Connect Timer	**TCP and TLS only:** Sets the timer value in milliseconds for TCP connections on the SIP Line. The valid values are 500 to 20000 (milliseconds).	2000
T1 Timer (ms)	**UDP only**: Sets the timer value in milliseconds that represents the initial incremental delay between packet retransmission. The valid values are 500 to T2 (milliseconds).	500
T2 Timer (ms)	**UDP only**: Sets the timer value in milliseconds that represents the maximum incremental delay between packet retransmissions. The valid values are any values greater than or equal	1000

	to 1000 (milliseconds).	
Maximum Packet Retry	**UDP only**: Sets the maximum number of packet retry attempts for requests. Valid values are from 0 to 10.	4
Maximum Invite Retry	**UDP only**: Sets the maximum number of packet retry attempts for INVITE and ACK requests. Valid values are from 0 to 6.	3
Reinvite Delay (ms)	**UDP only**: Sets the reinvite delay in milliseconds.	50
Retryable Reason Codes	Defines the list of valid SIP reason codes. If this line is part of a line group, and an outbound call that is made on this line returns a valid SIP reason code, then CIC retries the call on the next line in the line group. Separate reason codes or ranges of reason codes with commas. For example: "500-599" Or... "401, 480, 490-495, 500-599" **Note**: "480" is not available on lines that are enabled for Microsoft Lync.	480, 500-599
Retryable Cause Codes	Defines a list of SIP cause codes. Cause codes take precedence over SIP response codes for retry attempts. If dial attempts are exhausted, the disconnect is	The default value is 1-5,25,27,28,31,34,38,41,42,44,46,62,63,79,91,96,97,99,100,103

	treated as the most recent cause code if a cause code was present on any of the dial attempts. All dial attempts are traced at the note level when multiple retries are not treated as a 'no available lines' error. Separate cause codes with commas. For example: "503, 507, 550"	
SIP DSCP Value	Sets the Differentiated Services Code Point (DSCP) value of Quality of Service (QoS) in transmitted SIP packets. The values are shown in both hex (00..3F) and related decimal (0..63) formats. Some values are also identified by the binary format, CS6. The range of valid values is 00 (0, 000000) through 3F (63, 111111).	18 (24, 011000) CS3
Inbound Progress Timer (ms)	Sets the number of milliseconds to wait before sending the 180 RINGING message. If the call is answered before this time expires, the 180 RINGING message is not sent. Acceptable values are 1000 through 60,000 milliseconds	5000
No Inbound Progress Timer	Determines whether the 180 RINGING message is never sent on this SIP line.	Not selected
SIP Answer	Sets the number of milliseconds of delay to	500 milliseconds

Delay (ms)	insert before a call is answered. This setting is useful when there is some audio loss during call setup. The acceptable values are from 0 through 8,000 milliseconds. If the value is greater than or equal to 1000 milliseconds, an 180 Ringing SIP signal is sent before delay is inserted. Regardless of the value, the delay is always inserted after 200 OK is sent back.	

Related topics

Configure a SIP line

PureConnect Customer Care

SIP line transport concepts

SIP lines concepts

Session

SIP line session options

The following table describes the options that you can use to configure session options for a SIP line. For information on how to access these options, see *Configure a SIP line*.

Changes to any options on this dialog box take effect immediately.

Option	Description	Default
Use SIP Session Timer	Determines whether a recurring OPTIONS message is sent to the remote device. If the remote device does not respond to the OPTIONS message, the call is disconnected.	Not selected
SIP Session Timeout	The recurrence interval of the OPTIONS message that is sent when the **Use SIP Session Timer** check box is selected.	60 seconds
Disconnect on Broken RTP	Determines if a VoIP call remains active if the audio is disrupted. Audio is considered disrupted if no RTP, RTCP, and no comfort noise packet is received from the remote device.	Not selected

Media Timing	The options are: - **Normal** - **Delayed**	Normal
Media reINVITE Timing	Specifies if the media attempts to add media streams to the session immediately or if the timing is delayed when it receives a reINVITE. The options are: - **Normal** - **Delayed**	Normal
Terminate Analysis on Connect	Terminates the call analysis procedure when a SIP connection indication from the network is received. For example, Interaction Center makes its PSTN call via SIP calls through a SIP/ISDN gateway. In this example, the SIP/ISDN gateway sends only a SIP connect message back to Interaction Center after the remote party answers the call. If call analysis is used, you would want to select **Terminate Analysis On Connect**, so that call analysis terminates when the SIP connect message is received. For example, Interaction Center makes its PSTN call via SIP calls through a SIP/Analog gateway. In this example, the SIP/Analog gateway always sends a SIP connect message back to Interaction Center prematurely, before the remote party answers the call. If call analysis is used, you would want to deselect **Terminate Analysis On Connect**, so that call analysis continues after the SIP connect message is received. If the connection is to a station, the **Terminate Analysis On Connect** configured in the station is used. **Notes**: Beginning in IC 4.0 SU3, CIC terminates call analysis when it connects to **remote stations**. This decreases the time it takes to connect the caller to the agent at the remote station. If you want to restore the previous functionality of using call analysis when connecting to remote stations, create the Remote Station Call Analysis Answer Supervision Interaction Center server parameter, and set it to **False**.	Not selected

	You should always enable the **Terminate Analysis on Connect** option for a standalone fax station. Otherwise outbound faxing could fail.	
Disable Media Server Passthru	Determines whether the media server rewrites the SSRC header.	Not selected
ASR Enabled	Determines whether ASR (Automatic Speech Recognition) resources are allocated for this SIP line.	Selected

Related topics

Configure a SIP line

PureConnect Customer Care site

Optional general server parameters

Media server general configuration

Lines concepts

SIP line session options

The following table describes the options that you can use to configure session options for a SIP line. For information on how to access these options, see *Configure a SIP line*.

Changes to any options on this dialog box take effect immediately.

Option	Description	Default
Use SIP Session Timer	Determines whether a recurring OPTIONS message is sent to the remote device. If the remote device does not respond to the OPTIONS message, the call is disconnected.	Not selected
SIP Session Timeout	The recurrence interval of the OPTIONS message that is sent when the **Use SIP Session Timer** check box is selected.	60 seconds
Disconnect on Broken RTP	Determines if a VoIP call remains active if the audio is disrupted. Audio is considered disrupted if no RTP, RTCP, and no comfort noise packet is received from the remote device.	Not selected
Media Timing	The options are:	Normal

	- **Normal** - **Delayed**	
Media reINVITE Timing	Specifies if the media attempts to add media streams to the session immediately or if the timing is delayed when it receives a reINVITE. The options are: - **Normal** - **Delayed**	Normal
Terminate Analysis on Connect	Terminates the call analysis procedure when a SIP connection indication from the network is received. For example, Interaction Center makes its PSTN call via SIP calls through a SIP/ISDN gateway. In this example, the SIP/ISDN gateway sends only a SIP connect message back to Interaction Center after the remote party answers the call. If call analysis is used, you would want to select **Terminate Analysis On Connect**, so that call analysis terminates when the SIP connect message is received. For example, Interaction Center makes its PSTN call via SIP calls through a SIP/Analog gateway. In this example, the SIP/Analog gateway always sends a SIP connect message back to Interaction Center prematurely, before the remote party answers the call. If call analysis is used, you would want to deselect **Terminate Analysis On Connect**, so that call analysis continues after the SIP connect message is received. If the connection is to a station, the **Terminate Analysis On Connect** configured in the station is used. **Notes**: Beginning in IC 4.0 SU3, CIC terminates call analysis when it connects to **remote stations**. This decreases the time it takes to connect the caller to the agent at the remote station. If you want to restore the previous functionality of using call analysis when connecting to remote stations, create the Remote Station Call Analysis Answer Supervision Interaction Center server parameter, and set it to **False**. You should always enable the **Terminate Analysis on Connect** option for a standalone fax station. Otherwise	Not selected

	outbound faxing could fail.	
Disable Media Server Passthru	Determines whether the media server rewrites the SSRC header.	Not selected
ASR Enabled	Determines whether ASR (Automatic Speech Recognition) resources are allocated for this SIP line.	Selected

Related topics

Configure a SIP line

PureConnect Customer Care site

Optional general server parameters

Media server general configuration

Lines concepts

Authentication

SIP line authentication options

The following table describes the options that you can use to configure authentication options for a SIP line. For information on how to access these options, see *Configure a SIP line*.

Changes to all options on this dialog box take effect immediately.

Option	Description	Default
Authentication	Determines whether authentication is enabled for this SIP line.	Not selected
User Name	Specifies the **User Name** that is used in the authentication process. If you enable authentication for the SIP line, you must specify a user name.	Not specified
Password	Specifies the **Password** that is used in the authentication process.	Not specified
Confirm	Confirms the **Password** that is used in the authentication	Not

Password	process.	specified

Related topics

SIP line authentication concepts

Configure a SIP line

Lines concepts

SIP line authentication concepts

Authentication credentials on the SIP line apply only to outbound calls that are made from the Interaction Center.

SIP line authentication is only used when a proxy “challenges” an outbound call.

A SIP line is typically used to send a call to an external party through a SIP gateway or proxy. If the gateway or proxy challenges the call with a 401 or 407 response code, then the **User Name** and **Password** that are defined in the **Authentication** options in the **SIP Line Configuration** dialog box on the are used to authenticate the call.

The digest access algorithm is used as defined in RFC 2617 HTTP Authentication: Basic and Digest Access Authentication.

Related topics

SIP line authentication options

Configure a SIP line

Lines concepts

SIP line authentication options

The following table describes the options that you can use to configure authentication options for a SIP line. For information on how to access these options, see *Configure a SIP line*.

Changes to all options on this dialog box take effect immediately.

Option	Description	Default
Authentication	Determines whether authentication is enabled for this SIP line.	Not selected

User Name	Specifies the **User Name** that is used in the authentication process. If you enable authentication for the SIP line, you must specify a user name.	Not specified
Password	Specifies the **Password** that is used in the authentication process.	Not specified
Confirm Password	Confirms the **Password** that is used in the authentication process.	Not specified

Related topics

SIP line authentication concepts

Configure a SIP line

Lines concepts

Proxy

SIP line proxy options

The following table describes the options that you can use to configure proxy options for a SIP line. For more information, see *SIP line proxy concepts* and *Configure proxy addresses.*

Changes to most of the options on this dialog box take effect immediately.

> **Note:** If you change the port number of a proxy address, then you must restart the CIC server in order for the change to take effect.

Option	Description	Default
Prioritized list of Proxy addresses	Displays the a prioritized list of outbound proxy addresses that are available to CIC. All messages are sent to the **first** proxy address in this list. The remaining proxy addresses are used only if the first proxy address is not operational. "Not operational" means that CIC did not receive any response from the proxy and the request timed out. For each IP address, specify the port number at which the proxy services requests.	The default proxy port number for a line that uses TLS is 5061. The default proxy port number for all other

	Valid port numbers are 1024 to 65535.	protocols (TCP and UDP) is 5060.
DNS SRV	Dynamically requests a list of proxy servers from a DNS server.	Not selected

Related topics

Configure proxy addresses

SIP line proxy concepts

Configure a SIP line

Line group configuration

Lines concepts

SIP line proxy concepts

If you configure an outbound proxy, then all SIP messages are sent to it for transmission. For each proxy you can specify one or more proxy addresses.

The list of proxy addresses indicates the order in which they are tried. All messages are sent to the **first** proxy address in this list. The remaining proxy addresses are used only if the first proxy address is not operational. "Not operational" means that CIC did not receive any response from the proxy and the request timed out.

If any response is received from the proxy then the proxy selection operation is considered complete, regardless of the response value.

This proxy list is intended to be used only when the proxies are considered to be "cold-standbys" of each other, meaning that only one is operational at a time.

If you intend to use the proxies as "hot-standbys" or N+1 configurations, then use SIP lines and line groups instead.

For example:

1. Assign one proxy per SIP line. Assign multiple SIP lines into one line group. This method orders proxies alphanumerically by line name. It enables the use of different hunt selection methods.

2. Assign one proxy per SIP line. Assign one SIP line into one line group. You can then arrange the line group list in Dial Plan Dial Group List. This method allows the selection of one proxy as the main proxy regardless of the line name.

Each SIP line contains a configurable list of response codes that can be retried. The response codes can be used to determine when or if the next SIP line or line group is attempted.

Related topics

Configure proxy addresses

SIP line proxy options

Configure a SIP line

Lines concepts

SIP line proxy options

The following table describes the options that you can use to configure proxy options for a SIP line. For more information, see *SIP line proxy concepts* and *Configure proxy addresses.*

Changes to most of the options on this dialog box take effect immediately.

> **Note:** If you change the port number of a proxy address, then you must restart the CIC server in order for the change to take effect.

Option	Description	Default
Prioritized list of Proxy addresses	Displays the a prioritized list of outbound proxy addresses that are available to CIC. All messages are sent to the **first** proxy address in this list. The remaining proxy addresses are used only if the first proxy address is not operational. "Not operational" means that CIC did not receive any response from the proxy and the request timed out. For each IP address, specify the port number at which the proxy services requests.	The default proxy port number for a line that uses TLS is 5061. The default proxy port number for all other protocols

	Valid port numbers are 1024 to 65535.	(TCP and UDP) is 5060.
DNS SRV	Dynamically requests a list of proxy servers from a DNS server.	Not selected

Related topics

[Configure proxy addresses]

[SIP line proxy concepts]

[Configure a SIP line]

[Line group configuration]

[Lines concepts]

Configure proxy addresses

To configure proxy addresses

1. Open the **Proxy** tab of the **Line Configuration** dialog box.
2. In the list of options, click **Proxy**.
3. To request a list of proxy servers from a DNS server, select the **DNS SRV** check box. You can then add an occurrence of a proxy server into the prioritized list.
4. To add a proxy address, click **Add**. Specify the proxy address and port number. Click **OK**.
5. To edit a proxy address, select the address. Click **Edit**. Make your changes. Click **OK**.

> **Note:** If you change the port number of a proxy address, then you must restart the CIC server in order for the change to take effect.

6. To delete a proxy address, select the address. Click **Delete**.
7. To change the priority order of a proxy address, select the address. Then use the **Up** and **Down** buttons to change its position in the list.
8. To save your changes, click **OK**.

Related topics

SIP line proxy concepts

SIP line proxy options

Configure a SIP line

Lines concepts

Registrar

SIP line registrar options

The following table describes the options that you can use to configure registrar options for a SIP line. For information on how to access these options, see *Configure a SIP line*.

Changes to all of the options on this dialog box take effect immediately.

Option	Description	Default
External List of Telephone Numbers	This is a list of **External Phone Numbers** that are not configured in CIC but that need to be directed to the CIC server when they are encountered. Therefore, CIC (via TS) must register these external phone numbers with the registrar. Typically, these are numbers that are provisioned on the PSTN interface but that are not provisioned in the CIC system, such as a 1-800 number.	Not specified
Prioritized List of Registrar addresses	This is a list of registrars in order of priority that are available for contact registration by CIC. If a registrar is configured, then all CIC contacts are sent to it in a SIP REGISTER message by TS. The SIP engine attempts to register the given telephone numbers to every host in the registrar list. Each entry in the list must be either an IP address in the IPv4 dotted-notation or a fully qualified domain name. For each IP address there should be a port. The port number identifies the port at which the registrar will be servicing requests. Valid port values are from 1024 to 65535. For each IP address, you must also specify the registration time in seconds. The value for the registration time must be an integer between 0 and 360000 (100 hours) inclusive.	The default for a line that uses TLS is 5061. The default for all other protocols (TCP and UDP) is 5060.

Related topics

Configure a SIP line

SIP line registrar concepts

Lines concepts

SIP line registrar concepts

In SIP, a registrar is a logical entity that stores information about where to contact a user when someone dials that user's number. In CIC, a registrar represents a SIP carrier. Before service is granted, the SIP carrier usually requires CIC to register the SIP line, which is done by TS sending a SIP REGISTER message to the carrier. The registration tells the SIP carrier that if it receives calls for CIC's DID (Direct Inward Dial)s, then those calls should be sent to CIC.

Related topics

SIP line registrar options

Configure a SIP line

Lines concepts

SIP line registrar options

The following table describes the options that you can use to configure registrar options for a SIP line. For information on how to access these options, see *Configure a SIP line*.

Changes to all of the options on this dialog box take effect immediately.

Option	Description	Default
External List of Telephone Numbers	This is a list of **External Phone Numbers** that are not configured in CIC but that need to be directed to the CIC server when they are encountered. Therefore, CIC (via TS) must register these external phone numbers with the registrar. Typically, these are numbers that are provisioned on the PSTN interface but that are not provisioned in the CIC system, such as a 1-800 number.	Not specified
Prioritized List of Registrar	This is a list of registrars in order of priority that are available for contact registration by CIC. If a registrar is configured, then all CIC contacts are sent to it in a SIP REGISTER message by TS. The	The default for a line that uses

addresses	SIP engine attempts to register the given telephone numbers to every host in the registrar list. Each entry in the list must be either an IP address in the IPv4 dotted-notation or a fully qualified domain name. For each IP address there should be a port. The port number identifies the port at which the registrar will be servicing requests. Valid port values are from 1024 to 65535. For each IP address, you must also specify the registration time in seconds. The value for the registration time must be an integer between 0 and 360000 (100 hours) inclusive.	TLS is 5061. The default for all other protocols (TCP and UDP) is 5060.

Related topics

Configure a SIP line

SIP line registrar concepts

Lines concepts

Headers

SIP line headers options

The following table describes the options that you can use to configure header options for a SIP line. For information on how to access these options, see *Configure a SIP line*.

Changes to all of the options on this dialog box take effect immediately.

Option	Description	Default

Transferred Headers	Specifies the headers that are collected from the initial inbound INVITE message and transferred to the outbound INVITE message to the partner or connection call. Define the header for use by both the inbound line and the outbound line. Valid entries in the list must contain a string of the following characters: ▪ lowercase "a" through "z" ▪ uppercase "A" through "Z" ▪ digits "0" through "9" ▪ "-" ▪ "." ▪ "!" ▪ "%" ▪ "*" ▪ "_" ▪ "+" ▪ "`" ▪ "'" ▪ "~"	Not specified

Call Attribute Headers	Specifies the headers that are collected on inbound SIP messages. These headers are converted into CIC attributes for use by the CIC subsystems. Each entry in the list must contain a string of the following characters: ▪ lowercase "a" through "z" ▪ uppercase "A" through "Z" ▪ digits "0" through "9" ▪ "-" ▪ "." ▪ "!" ▪ "%" ▪ "*" ▪ "_" ▪ "+" ▪ "`" ▪ "'" ▪ "~"	Not specified
User-to-User Settings	Determines the exchange of user-to-user information (UUI) data when a SIP session is initiated.	
Header	Selects the type of UUI header information. The options are: • **X-UserToUser**: This parameter format is the Audiocodes proprietary header. It does not use the protocol discriminator (PD). The length limit of the data is 129 bytes	X-UserToUser

	(129*2 hex digits). - **User-to-User**: This is the general parameter that includes the PD in the format User-to-User: XXhexdata;encoding=hex, where the XX is the PD. The length limit is 129 bytes including the PD (129*2 hex digits). - **User-to-User PD Attribute**: This is the parameter that some gateways use where the PD is specified separately in the format User-to-User: hexdata;pd=XX;encoding=hex .	
Protocol Discriminator	Describes the user protocol message being transferred. You can specify any integers, lowercase letters from a-f, and uppercase letters from A-F. If the X-UserToUser header is used, this option is not applicable.	00
Attribute Format	Selects the encoding format for the header. The options are: - **Hex** - **Ascii** - **Extended Ascii**	Hex

Related topics

Configure a SIP line

Optional general server parameters

SIP line headers concepts

Lines concepts

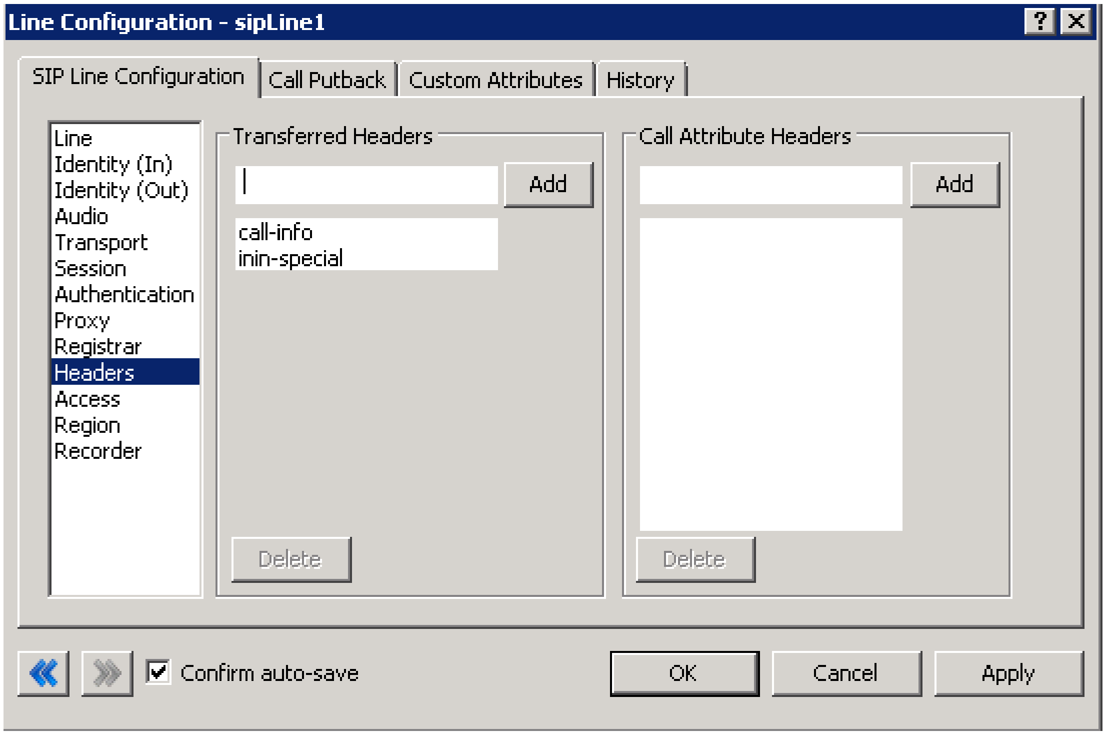
SIP line headers concepts

On a SIP line, headers are collected on inbound SIP messages. Based on header type, the header information is sent to stations or converted into CIC attributes. The header information is not always transferred: the phone receiving the partner call may not have a use for the header.

Example

An external call to GeorgeB is inbound on DID number 317.555.1212. The call, referred to as **0001**, comes into CIC through the gateway, and is assigned to line **SIP_ININ_GW**.

The **Transferred Headers** for this line have been configured for **call-info** and **inin-special**.



Transferred Headers:
call-info
inin-special

☑ Confirm auto-save

CIC retains these headers for call **0001**. The information may or may not be needed.

GeorgeB's station is 8182, so another call, **0002**, is created to contact his station. This 'connection' call **0002** is now a partner with call **0001**, since they need to collaborate.

The outbound call **0002** is assigned line **Stations-TCP**, which has **inin-special** defined as a **transferred header.** Call **0002** now has the **inin-special** header information, but not the **call-info** header information from call **0001**, and it is passed to GeorgeB's station **8182**.

In this case, only the transferred headers at the intersection of the inbound line **SIP_ININ_GW** and the outbound line **Station-TCP** defines what information is transferred.

Related topics

Optional general server parameters

SIP line headers options

Configure a SIP line

Lines concepts

SIP line headers options

The following table describes the options that you can use to configure header options for a SIP line. For information on how to access these options, see *Configure a SIP line*.

Changes to all of the options on this dialog box take effect immediately.

Option	Description	Default
Transferred Headers	Specifies the headers that are collected from the initial inbound INVITE message and transferred to the outbound INVITE message to the partner or connection call. Define the header for use by both the inbound line and the outbound line. Valid entries in the list must contain a string of the following characters: ▪ lowercase "a" through "z" ▪ uppercase "A" through "Z" ▪ digits "0" through "9" ▪ "-" ▪ "." ▪ "!" ▪ "%" ▪ "*" ▪ "_" ▪ "+"	Not specified

	▪ "`" ▪ "'" ▪ "~"	
Call Attribute Headers	Specifies the headers that are collected on inbound SIP messages. These headers are converted into CIC attributes for use by the CIC subsystems. Each entry in the list must contain a string of the following characters: ▪ lowercase "a" through "z" ▪ uppercase "A" through "Z" ▪ digits "0" through "9" ▪ "-" ▪ "." ▪ "!" ▪ "%" ▪ "*" ▪ "_" ▪ "+" ▪ "`" ▪ "'"	Not specified

	▪ "~"	
User-to-User Settings	Determines the exchange of user-to-user information (UUI) data when a SIP session is initiated.	
Header	Selects the type of UUI header information. The options are: • **X-UserToUser**: This parameter format is the Audiocodes proprietary header. It does not use the protocol discriminator (PD). The length limit of the data is 129 bytes (129*2 hex digits). • **User-to-User**: This is the general parameter that includes the PD in the format User-to-User: XXhexdata;encoding=hex, where the XX is the PD. The length limit is 129 bytes including the PD (129*2 hex digits). • **User-to-User PD Attribute**: This is the parameter that some gateways use where the	X-UserToUser

	PD is specified separately in the format User-to-User: hexdata;pd=XX;encoding=hex	
Protocol Discriminator	Describes the user protocol message being transferred. You can specify any integers, lowercase letters from a-f, and uppercase letters from A-F. If the X-UserToUser header is used, this option is not applicable.	00
Attribute Format	Selects the encoding format for the header. The options are: • **Hex** • **Ascii** • **Extended Ascii**	Hex

Related topics

Configure a SIP line

Optional general server parameters

SIP line headers concepts

Lines concepts

Access

SIP line access options

The following table describes the options that you can use to configure access options for a SIP line. For more information, see *Configure a SIP line* and *Configure exceptions to the default SIP line access level*.

Changes to all of the options on this dialog box take effect immediately.

Option	Description	Default
All computers will be: **Granted Access** **Denied Access**	Indicates the default access level for all computers.	Granted Access
Exceptions	Lists the computers that are exceptions to the default access level.	Not specified

Related topics

Configure a SIP line

Configure exceptions to the default SIP line access level

Lines concepts

SIP line access concepts

You can protect the SIP line against denial of server (DoS) attacks. A DoS attack occurs when a website or other resource is overwhelmed is intentionally overwhelmed with bogus requests for service. As a result, legitimate customers are deprived of the services that the resource provides.

To protect the SIP line, you enter the SIP address restrictions by doing either of the following:

- **Grant Access** to all computers and then enter the exceptions for the computers to which you want to deny access.
- **Deny Access** to all computers, and then enter the exceptions for the computers to which you want to grant access.

Related topics

SIP line access options

Configure exceptions to the default SIP line access level

Configure a SIP line

Lines concepts

SIP line access options

The following table describes the options that you can use to configure access options for a SIP line. For more information, see *Configure a SIP line* and *Configure exceptions to the default SIP line access level*.

Changes to all of the options on this dialog box take effect immediately.

Option	Description	Default
All computers will be: **Granted Access** **Denied Access**	Indicates the default access level for all computers.	Granted Access
Exceptions	Lists the computers that are exceptions to the default access level.	Not specified

Related topics

Configure a SIP line

Configure exceptions to the default SIP line access level

Lines concepts

Configure exceptions to the default SIP line access level

To configure exceptions to the default SIP line access level

1. Open the **SIP Line Configuration** tab of the **Line Configuration** dialog box.
2. Do any of the following:
   - To add an exception, click **Add**.
     The **Grant <Exception Type> On** dialog box appears.
   - To edit an exception, select it in the **Exceptions** list and then click **Edit**.
     The **Grant <Exception Type> On** dialog box appears.
   - To delete an, select it in the **Exceptions** list and then click **Delete**.
2. In the **Type** group, select **Single Computer** or **Group of Computers**.
3. In the **Validate access using** list, select which IP address is checked against the access list of a sip line. Select one of the following:
   - Select **Last hop's IP Address**
   - Select **Originator's IP Address**
4. Complete the **Address** field:
   - If you selected **Single Computer**, do one of the following:
   - Enter an address string using IPv4 dotted notation (for example, 172.16.1.25).

- Enter an address string using IPv6 dotted notation.
- Click the **DNS Lookup...** button. Then type a fully qualified domain name and click **OK**.
- If you selected **Group of Computers**, enter the beginning IP address for the range of addresses in the **Network ID field**. Then in the **Subnet prefix length** box, type the ending IP address for the range of addresses. If you use the IPv4 dotted notation, the **Subnet mask length:** defaults to 24. If you select IPv6 protocol, the **Subnet mask length:** defaults to 48.

> Note: Only one SIP line per port per protocol can grant all access. IP address entries must be unique per port per protocol.

5. Do one of the following:

- Click **OK** to close the dialog box.
- Click **Apply** to save your changes and continue with the configuration process.

Related topics

SIP line access concepts

SIP line access options

Configure a SIP line

Lines concepts

Region

SIP line region options

The following table describes the options that you can use to configure region options for a SIP line. For information on how to access these options, see *Configure a SIP line*.

Changes to all of the options on this dialog box take effect immediately.

Option	Description	Default
Location	Sets a location for this SIP line. **Note:** The locations that appear in the **Location** list are defined in the **Regionalization** container.	Default Location

Related topics

Configure a SIP line

SIP line region concepts

Regionalization

Lines concepts

SIP line region concepts

A region defines areas where SIP stations and lines are physically interconnected. Within a region, a specific dial plan may be required depending on the central office or switching mechanism to which it is connected. CIC uses locations to define the bandwidth requirements and endpoints (stations and lines) for a region.

A location represents the area where devices are considered to be in the same physical place. This location defines a set of endpoints that can share a common dial plan. The stations and lines that are members of a location are utilized by the dial plan entries that apply to the locale in which they are operating. The location also defines the codec communications and the ability to communicate between devices and locations.

Related topics

SIP line region options

Configure a SIP line

Lines concepts

SIP line region options

The following table describes the options that you can use to configure region options for a SIP line. For information on how to access these options, see *Configure a SIP line*.

Changes to all of the options on this dialog box take effect immediately.

Option	Description	Default
Location	Sets a location for this SIP line. **Note:** The locations that appear in the **Location** list are defined in the **Regionalization** container.	Default Location

Related topics

Configure a SIP line

SIP line region concepts

Regionalization

Lines concepts

Recorder

SIP line recorder options

The following table describes the options that you can use to configure Interaction Recorder options for a SIP line. For information on how to access these options, see *Configure a SIP line*.

Changes to all of the options on this dialog box take effect immediately.

Option	Description	Default
Use Proactive Recording	Determines whether CIC starts recording as soon as audio starts on a call and continues that recording until the call disconnects. **Note:** Not all proactive recordings are stored. CIC retains proactive recordings only when all of the following occur: * The recording is run through Recorder Policies. * Tracker data is stored.	Not selected
Encrypt Recordings	Determines whether the recordings are encrypted. This option is available only if the **Use Proactive Recording** option is selected. **Note**: This setting overrides the **Encrypt the Recording** setting in an initiation policy. For example, if **Encrypt the Recordings** setting is *not* selected in an initiation policy, and both the **Use Proactive Recording** and **Encrypt Recordings** settings are selected here, then the recording is encrypted.	Not selected

	If **Encrypt the Recording** setting is selected in an initiation policy, and the **Use Proactive Recording** setting is selected, but the **Encrypt Recordings** setting is *not* selected here, then the recording is *not* encrypted. In the event of a conflicting record call request, a Configuration Error warning message is logged in the Application log.	
Include Hold Music	Determines whether the recordings include hold music. This option is available only if the **Use Proactive Recording** option is selected.	Not selected
Include Early Audio (IVR and ACD Wait)	Determines whether the recordings include IVR and ACD Wait audio. **Note:** This check box is available only if you have the appropriate license. This option is available only if the **Use Proactive Recording** option is selected. **Note**: The default compression format for a new SIP line with Proactive Recording selected is "µ-law." The compression format can be changed for this SIP line by configuring Interaction Recorder's recording processing.	Not selected

Related topics

Configure a SIP line

Configure Interaction Recorder's recording processing

Lines concepts

SIP line recorder options

The following table describes the options that you can use to configure Interaction Recorder options for a SIP line. For information on how to access these options, see *Configure a SIP line*.

Changes to all of the options on this dialog box take effect immediately.

Option	Description	Default
Use Proactive Recording	Determines whether CIC starts recording as soon as audio starts on a call and continues that recording until the call disconnects. **Note:** Not all proactive recordings are stored. CIC retains proactive recordings only when all of the following occur: * The recording is run through Recorder Policies. * Tracker data is stored.	Not selected
Encrypt Recordings	Determines whether the recordings are encrypted. This option is available only if the **Use Proactive Recording** option is selected. **Note**: This setting overrides the **Encrypt the Recording** setting in an initiation policy. For example, if **Encrypt the Recordings** setting is *not* selected in an initiation policy, and both the **Use Proactive Recording** and **Encrypt Recordings** settings are selected here, then the recording is encrypted.	Not selected

	If **Encrypt the Recording** setting is selected in an initiation policy, and the **Use Proactive Recording** setting is selected, but the **Encrypt Recordings** setting is *not* selected here, then the recording is *not* encrypted. In the event of a conflicting record call request, a Configuration Error warning message is logged in the Application log.	
Include Hold Music	Determines whether the recordings include hold music. This option is available only if the **Use Proactive Recording** option is selected.	Not selected
Include Early Audio (IVR and ACD Wait)	Determines whether the recordings include IVR and ACD Wait audio. **Note:** This check box is available only if you have the appropriate license. This option is available only if the **Use Proactive Recording** option is selected. **Note**: The default compression format for a new SIP line with Proactive Recording selected is "µ-law." The compression format can be changed for this SIP line by configuring Interaction Recorder's recording processing.	Not selected

Related topics

Configure a SIP line

Configure Interaction Recorder's recording processing

Lines concepts

TLS Security

SIP line TLS security options

The following table describes the options that you can use to configure TLS security options for a SIP line. The behavior of TLS communication depends on the capabilities of the devices that use this SIP line.

For information on how to access these options, see *Configure a SIP line*.

> **Note:** The **TLS Security** options are available only if you select TLS as the transport protocol on the **Transport** dialog box.

Changes to any of the options on this dialog box take effect immediately.

Option	Description	Default
TLS Options		
Require mutual authentication	Determines whether the CIC server requests a certificate from the SIP device and authenticates it. **Note:** This option works if the devices that use the SIP line support the capability to perform a mutual authentication. The SIP device then requests a certificate from the CIC server, validates it, and establishes a secure TLS connection. This one-way authentication of the server is sufficient to ensure the SIP device is connecting to the proper CIC server. By default, a SIP device using TLS to connect to the CIC server must contain the CIC line certificate authority (CA) certificate in order to authenticate the CIC server when it connects.	Not selected
Certificates	Displays the list of authority certificates that are selected for this SIP line. You can select additional authority certificates if you plan to	<Default Line Authority Certificate>

	use an external third-party certificate authority to sign line certificates. For more information, see *Select certificate authorities for a SIP line*. Click **Configure certificates and port mappings...** to open the **SIP/TLS Configuration** dialog box. **Note**: For more information, see *PureConnect Security Features* in the **Technical Reference Documents** section of the PureConnect Documentation Library.	

Related topics

Configure a SIP line

Modify TLS cipher suites

Select certificate authorities for a SIP line

SIP line transport options

Configure a SIP line

SIP lines concepts

TLS security concepts

If a SIP device (that is, some AudioCodes Mediant gateways) using this line does not support the stronger AES (Advanced Encryption Standard) cipher suites used by default in CIC, click the Modify Cipher Suites button to select one or more additional cipher suites to add to the list of TLS Cipher Suites to use. The cipher suites are listed in order of strongest to weakest. CIC will negotiate with each SIP device and agree to use the strongest cipher suite common between the device and the CIC server.

Related topics

TLS line certificate concepts

Configure TLS line certificates

TLS authority certificate concepts

Configure TLS authority certificates

TLS port-to-certificate mapping concepts

Configure TLS port-to-certificate mappings

Third-party certificate signing concepts

Sign third-party certificates

Import a certificate

Configure a SIP line

SIP lines concepts

SIP line TLS security options

The following table describes the options that you can use to configure TLS security options for a SIP line. The behavior of TLS communication depends on the capabilities of the devices that use this SIP line.

For information on how to access these options, see *Configure a SIP line*.

> **Note:** The **TLS Security** options are available only if you select TLS as the transport protocol on the **Transport** dialog box.

Changes to any of the options on this dialog box take effect immediately.

Option	Description	Default
TLS Options		
Require mutual authentication	Determines whether the CIC server requests a certificate from the SIP device and authenticates it. **Note:** This option works if the devices that use the SIP line support the capability to perform a mutual authentication. The SIP device then requests a certificate from the CIC server, validates it, and establishes a secure TLS connection. This one-way authentication of the server is sufficient to ensure the SIP device is connecting to the proper CIC server.	Not selected

	By default, a SIP device using TLS to connect to the CIC server must contain the CIC line certificate authority (CA) certificate in order to authenticate the CIC server when it connects.	
Certificates	Displays the list of authority certificates that are selected for this SIP line. You can select additional authority certificates if you plan to use an external third-party certificate authority to sign line certificates. For more information, see *Select certificate authorities for a SIP line*. Click **Configure certificates and port mappings…** to open the **SIP/TLS Configuration** dialog box. **Note**: For more information, see *PureConnect Security Features* in the **Technical Reference Documents** section of the PureConnect Documentation Library.	<Default Line Authority Certificate>

Related topics

Configure a SIP line

Modify TLS cipher suites

Select certificate authorities for a SIP line

SIP line transport options

Configure a SIP line

SIP lines concepts

Modify TLS cipher suites

You can specify which cipher suites to use for encrypting SIP messages when using TLS on the SIP lines. The CIC server uses the activated TLS cipher suites in the order in which they appear.

The following weaker cipher suites do not comply with PCI standards and no longer appear in the list for you to activate:

- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_DES_EDE_CBC_SHA
- TLS_RSA_WITH_RC4_128_SHA
- TLS_RSA_EXPORT_WITH_DES40_CBC_SHA

If you previously activated any of these weaker cipher suites, they still appear in the list as activated. Once you deactivate any of these weaker cipher suites, the cipher suite is no longer available in the list.

To modify the TLS cipher suites

1. Open the **TLS Security** tab of the **Line Configuration** dialog box.

   > **Note:** In order to access the **TLS Security** tab, you just first select **TLS** as the transport protocol on the **Transport** tab.

2. Click **Modify Cipher Suites**.
   The **TLS Cipher Suites** dialog box appears.
3. Do any of the following:
   - To activate a cipher suite, select its check box.
   - To deactivate a cipher suite, deselect its check box.
   - Use the **Move Up** and **Move Down** buttons to change the order of the cipher suites.
   - Click **Default** to restore the default cipher suites settings.
4. Click **OK**.

Related topics

SIP line TLS security options

Select certificate authorities for a SIP line

Configure a SIP line

Select certificate authorities for a SIP line

CIC provides a default line authority certificate for use with every SIP line. You can select additional certificate authorities if you plan to use an external third-party certificate authority to sign line certificates.

The third-party certificate authority files must be generated and copied to the CIC server before you can select them for a SIP line.

To select certificate authorities for a SIP line

1. Open the **TLS Security tab** of the **Line Configuration** dialog box.

> **Note:** In order to access the **TLS Security** tab, you just first select **TLS** as the transport protocol on the **Transport** tab.

2. Click **Modify**.
   The Select the certificate authorities for this line dialog box appears.
3. To select a certificate authority, select it in the **Available** list and then click **Add**.
4. To deselect a certificate authority, select it in the **Currently Selected** list and then click **Remove**.
5. Click **OK**.

Related topics

SIP line TLS security options

Modify TLS cipher suites

TLS security concepts

Configure a SIP line

Configure certificates and port mappings

TLS security concepts

If a SIP device (that is, some AudioCodes Mediant gateways) using this line does not support the stronger AES (Advanced Encryption Standard) cipher suites used by default in CIC, click the Modify Cipher Suites button to select one or more additional cipher suites to add to the list of TLS Cipher Suites to use. The cipher suites are listed in order of strongest to weakest. CIC will negotiate with each SIP device and agree to use the strongest cipher suite common between the device and the CIC server.

Related topics

TLS line certificate concepts

Configure TLS line certificates

TLS authority certificate concepts

Configure TLS authority certificates

TLS port-to-certificate mapping concepts

Configure TLS port-to-certificate mappings

Third-party certificate signing concepts

Sign third-party certificates

Import a certificate

Configure a SIP line

SIP lines concepts

TLS security concepts

If a SIP device (that is, some AudioCodes Mediant gateways) using this line does not support the stronger AES (Advanced Encryption Standard) cipher suites used by default in CIC, click the Modify Cipher Suites button to select one or more additional cipher suites to add to the list of TLS Cipher Suites to use. The cipher suites are listed in order of strongest to weakest. CIC will negotiate with each SIP device and agree to use the strongest cipher suite common between the device and the CIC server.

Related topics

TLS line certificate concepts

Configure TLS line certificates

TLS authority certificate concepts

Configure TLS authority certificates

TLS port-to-certificate mapping concepts

Configure TLS port-to-certificate mappings

Third-party certificate signing concepts

Sign third-party certificates

Import a certificate

Configure a SIP line

SIP lines concepts

TLS line certificate concepts

You can configure the certificates that enable secure connections over SIP TLS lines.

TLS line certificates are signed by the CIC server's root certificate authority (CA) or a third-party CA. They are used to identify the CIC server when it connects to remote SIP devices via TLS.

In a switchover pair environment, you must import, on each switchover server, a special certificate that contains the domain name and a DHCP service record (SRV) so Polycom phones can be authenticated against both CIC servers. This special certificate is created by Setup Assistant and stored in the \server\ic\certificates\Lines folder.

A <Default Line Certificate> is automatically installed for you. The <Default Line Certificate> is signed by the CIC <Default Line Authority> CA. By default, this line certificate is used on single CIC servers that use the CIC certificate authority.

> **Note:** You can optionally include a third-party certificate in a Windows certificate store in order to enable Windows to recognize that the certificate is trusted. If you do not include the certificate in a Windows certificate store, the certificate status in CIC indicates that the certificate is not trusted by Windows. However, this status does not affect the security of the CIC system.

Related topics

Configure TLS line certificates

TLS security concepts

Configure TLS line certificates

To configure TLS line certificates

1. Use one of these paths:

    - **System Configuration > Configuration > Certificate Management > SIP/TLS Certificates Configuration > Modify > Line Certificates**

    - **IC Server > Lines > Line Configuration > TLS Security > Configure certificates and port mappings > Line Certificates**

    > **Note:** In order to access the **TLS Security** tab, you just first select **TLS** as the transport protocol on the **Transport** tab.

2. To load line certificates to use with a third-party certificate authority, click **Import**.
3. To view the general and detailed information about the issuer, valid dates, and descriptive details for a certificate in the list, select it and then click **View**.
4. To delete a certificate, select it and then click **Delete**.
5. Click **Close**.

Related topics

Import a certificate

TLS line certificate concepts

SIP lines concepts

Configure a SIP line

TLS authority certificate concepts

You can configure the certificate authority files that are used to validate devices connecting to the CIC server over SIP TLS lines. This is typically used when mutual authentication is required.

A <Default Line Authority Certificate> is automatically installed for you. The <Default Line Authority Certificate> is equivalent to the root certificate authority for lines. It is responsible for signing the default CIC line certificates.

In a switchover pair environment, the <Default Line Authority> certificate file is automatically replicated on the backup server as soon as the primary CIC server and the resident switchover service is started. If you import any new authority certificates on this tab, they are automatically replicated to the backup switchover server, if one is available.

> **Note:** You can optionally include a third-party authority certificate in a Windows certificate store in order to enable Windows to recognize that the certificate is trusted. If you do not include the certificate in a Windows certificate store, the certificate status in CIC indicates that the certificate is not trusted by Windows. However, this status does not affect the security of the CIC system.

Related topics

Configure TLS line certificates

TLS security concepts

Configure TLS authority certificates

To configure TLS authority certificates

1. Use one of these paths:
    - **System Configuration > Configuration > Certificate Management > SIP/TLS Certificates Configuration > Modify > Authority Certificates**
    - **IC Server > Lines > Line Configuration > TLS Security > Configure certificates and port mappings > Authority Certificates**

    > **Note:** In order to access the **TLS Security** tab, you just first select **TLS** as the transport protocol on the **Transport** tab.
2. To load authority certificates, click **Import**.
3. To view information about the issuer, valid dates, and descriptive details for an authority certificate, select it and then click **View**.
4. To delete an authority certificate, select it and then click **Delete**.
5. Click **Close**.

Related topics

TLS authority certificate concepts

TLS security concepts

Import a certificate

SIP lines concepts

Configure a SIP line

TLS port-to-certificate mapping concepts

SIP/TLS lines can use only one line certificate per port. Therefore, if you have multiple SIP/TLS lines and one of the lines requires a different certificate for its connection (for example, to a gateway, SIP Proxy server, and so on), you must map a port number to the line certificate to use for that connection. The port for each line is specified on the SIP line's **Transport** tab, in the **Receive Port** box.

By default, when only the default line certificate is being used, all TLS line ports maps to that certificate and no mappings appear or are required in the **Port-To-Certificate Mappings** tab.

When you use a pair of switchover servers, you must assign a port number to the domain certificate in the **Line Certificate** list and then add it to the **Port-To-Certificate Mappings** list. The default port number for all SIP/TLS lines is 5062. Port 8062 is recommended for the SIP/TLS line and certificate map to the domain certificate.

Related topics

Configure TLS port-to-certificate mappings

TLS security concepts

SIP line transport options

Configure TLS port-to-certificate mappings

To configure TLS port-to-certificate mappings

1. Use one of these paths:

    - **System Configuration > Configuration > Certificate Management > SIP/TLS Certificates Configuration > Modify > Port-To-Certifcate Mappings**
    - **IC Server > Lines > Line Configuration > TLS Security > Configure certificates and port mappings > Port-To-Certifcate Mappings**

    > **Note:** In order to access the **TLS Security** tab, you just first select **TLS** as the transport protocol on the **Transport** tab.

2. To add a mapping, do the following:

    - in the **Line Certificate** list, select the certificate that you want to map to a port number.

        > **Note:** To import an existing certificate that does not appear in this list, click the **Import New Line Certificate…** link.

    - In the **Port** field, select the port number. The port number must match the receive port number on the SIP/TLS line that you want to use with the certificate.
    - Click **Add**.

3. To remove a mapping, select it in the **Port-To-Certificate Mappings** list and then click **Remove**.
4. Click **Close**.

Related topics

TLS authority certificate concepts

TLS security concepts

SIP lines concepts

Configure a SIP line

Third-party certificate signing concepts

You can sign a certificate from a third-party device (for example an Audiocodes Mediant gateway) that uses the CIC authority certificate.

This is necessary when you configure a SIP line that uses TLS to connect to a third-party device that supports TLS. The connection between the CIC server and the third-party device needs to be authenticated when it establishes a connection that uses mutually authenticated certificates. If the device's certificate is not signed by the CIC line authority certificate, the connection will not be authenticated.

> **Note**: Use the **Third Party Certificate Signing** tab only if you use the CIC line authority certificates. Do not use it if you have your own third-party certificate authority.
> If you use your own third-party certificate authority and line certificates, then you must use your own certificate signing utility to sign the third-party device certificate.

Related topics

Sign third-party certificates

TLS security concepts

Sign third-party certificates

To sign a third-party certificate

1. On the remote device to which you want to connect, generate the text for a Certificate Signing Request (CSR). Copy that text to the clipboard on the CIC server or copy it in a text file that you can access on the CIC server.
2. Use one of these paths:
    - **System Configuration > Configuration > Certificate Management > SIP/TLS Certificates Configuration > Modify > Third Party Certificate Signing**
    - **IC Server > Lines > Line Configuration > TLS Security > Configure certificates and port mappings > Third Party Certificate Signing**

    > **Note:** In order to access the **TLS Security** tab, you just first select **TLS** as the transport protocol on the **Transport** tab.
3. For the **Digest Algorithm** option, select either **SHA-1** or **SHA-256** as your preferred secure hash algorithm.
4. Paste the CSR text from step 1 into the **Certificate Request To Sign** box.
5. Click **Sign** button. The signed certificate and the signing authority certificate are generated. They appear in the **Generated Certificates** fields on the tab.
6. Under the field that displays the signed certificate, click **Save As**.
7. Specify the directory and file name for this certificate.

> **Tip:** Include the name of the third-party device in the name.

8. Under the field that displays the signing authority certificate, click **Save As**.
9. Specify the directory and file name for this certificate.

> **Tip:** Use a name that distinguishes this certificate from the signed certificate.
>
> **Note**: Some third-party interfaces may let you paste the signed certificate or signed authority certificate data directly in to their interface, or you may wish to copy and paste this certificate text into your own file. In this case, use the Clipboard button to select and copy the signed certificate text to the clipboard for pasting into another application.

10. Copy the saved signed certificate and the saved CIC default line authority certificate to a USB flash drive. Then import them on the third-party device and continue the configuration there.

Related topics

SIP lines concepts

Configure a SIP line

Import a certificate

Identify the location and format of your own corporate (or third-party) line certificate and line private key or a line authority certificate you wish to use on this IC server. You do not normally need to use this dialog if you use the CIC Default line authority and CIC Default Line certificates provided with Interaction Center.

This dialog is also used in Setup Assistant to import your own server group certificate and private key on a pair of switchover IC servers. See the IC Setup Assistant help for more information about server group certificates.

Using your own line certificate, private key and authority certificate

If your company has already established its own root certificate authority and manages its own certificates, you can choose to use your own authority certificate, line certificate and private key for the IC server instead of the default IC-generated certificate authority and line certificates.

If you are using your own certificates, you must also specify the **Type** and **Format** information, and whether the private key is password protected.

Switchover server pair considerations

In the case where you have two IC servers in a switchover pair, certificate authority files (e.g., *YourLinesAuthorityCertificate.cer*) are automatically replicated to the backup switchover server as soon as both servers are running and the switchover service is enabled. This is to ensure that the same certificate authority file and public key is always resident on both servers. The private key is not copied over the network, to avoid a potential security breach.

Each switchover server must have its own unique line certificate and private key, which are generated for each server by your root certificate authority (CA). Once the line certificates are generated, you can manually copy the line certificates via a USB flash drive to install the line certificates on each IC server, then use the Import dialog on the Line Certificates page to import the certificates. See Transferring certificate files for a recommended secure procedure for transferring certificates via a USB flash drive.

> **Note**: Even though it is technically possible to use the Import dialog to browse and directly import a certificate over the network, we strongly recommend against this. If the network is already compromised and a network packet sniffer is in use, the certificate and its private key could be intercepted, which defeats the purpose of enabling security on the lines.

Name:

Enter a descriptive name for this line or authority certificate. This name appears in the Line Certificates or Authority Certificates page. It also appears on the Line Configuration page.

Certificate Path

Browse to the directory location of the certificate (e.g., *YourLineCertificate.cer* or *YourCertificateAuthority.cer*) you wish to use for this IC server.

Certificate Type

> **Note**: This field is applicable if you are using *your own* line certificate/private key or certificate authority. Otherwise, use the default selection.

Select one of the following CIC-supported certificate file format storage types:

- **X.509**: Standard specification for public key certificates, in either DER or PEM format.
- **PKCS 7**: Contains one or more certificates in either DER or PEM format.
- **PKCS 12**: Defines a file format to store keys *and* certificates in either DER or PEM format.

Certificate Format

> **Note**: This field is applicable if you are using *your own* line certificate/private key or certificate authority. Otherwise, use the default selection.

Select one of the following CIC-supported certificate file encoding formats:

- **DER** – Binary encoding
- **PEM** – Base64 encoding

Private Key Path

Browse to the directory location of the line certificate private key file (e.g., *YourLinesPrivateKey.bin*) you wish to use.

Private Key Format

> **Note**: This field is applicable if you are using *your own* line certificate private key certificate. Otherwise, use the default selection.

Select one of the following IC-supported key file encoding formats:

- **DER** – Binary encoding
- **PEM** – Base64 encoding

My private key is password protected

> **Note**: This field is applicable if you are using *your own* certificate/private key. Otherwise, use the default selection.

Select this check box if a password is attached to the private key file.

Password

Enter the private key password.

Transferring certificate files

When transferring a line certificate from one server to another, use the following procedure.

1. Insert a USB flash drive in the source server, where the certificate was generated.
2. Browse to the directory on the source server that contains the original certificate to be transferred.
3. Copy the Line Certificate file (e.g., ICSrvOneLineCertificate.cer) and its Private Key file (e.g., ICSrvOneLinePrivateKey.bin) to the USB drive.
4. Eject the USB drive from the source server.
5. Insert the USB drive in the destination IC server, where you want to copy the certificate.
6. From the SIP/TLS Line Certificates Configuration page in Interaction Administrator, click the Import… button to open the Import Certificate dialog.
7. In the Import Certificate dialog on the destination server, browse to the locations of the certificate and private key files on the USB drive in the Certificate Path and Private Key Path fields, for example, F:\ICSrvOneLineCertificate.cer and F:\ICSrvOneLinePrivateKey.bin.
8. Click OK and you will see the newly generated certificate listed on the SIP/TLS Line Certificates Configuration page.
9. Delete the certificate and private key files on the USB drive.
10. Eject the USB drive from the destination server.
11. Repeat this process for any additional IC servers, using a uniquely generated line certificate for each IC server.
12. (Recommended) As an additional security procedure, re-format the USB drive:

- Open My Computer on the desktop
- Right-click USB Drive and select Format...
- In the Format USB Drive dialog, select Start.

Call putback

Call putback options

The following table describes the options that you can use to configure call putback options for a SIP line. For information on how to access these options, see *Configure a SIP line*.

Changes to all of the options on this dialog box take effect immediately.

Option	Description	Default
Enable sending SIP REFER messages	Determines whether CIC can do the following items without tying up two CIC lines (one for the original call and one for the call to the destination): 1. Receive a call from the PSTN or a PBX. 2. Perform some processing on the call. 3. Transfer the call to a non-CIC destination (a PBX station or a remote number).	Not selected
Enable sending SIP REFER messages to Lines in other Lines Groups	Determines whether CIC can send SIP REFER messages to lines in other line groups. This option is available only if **Enable sending SIP REFER messages** is selected.	Not selected
Enable Processing of Received SIP REFER Messages	Determines whether CIC allows the party sending the REFER to be notified of the outcome of the received request. This option is typically set on lines going to internal gateways or CIC servers. **Notes**: Because this option can be used to enable other applications including call transfer, it can create additional calls and carrier charges.	Not selected

Related topics

SIP lines concepts

Configure a SIP line

Call putback options

The following table describes the options that you can use to configure call putback options for a SIP line. For information on how to access these options, see *Configure a SIP line*.

Changes to all of the options on this dialog box take effect immediately.

Option	Description	Default

Enable sending SIP REFER messages	Determines whether CIC can do the following items without tying up two CIC lines (one for the original call and one for the call to the destination): 1. Receive a call from the PSTN or a PBX. 2. Perform some processing on the call. 3. Transfer the call to a non-CIC destination (a PBX station or a remote number).	Not selected
Enable sending SIP REFER messages to Lines in other Lines Groups	Determines whether CIC can send SIP REFER messages to lines in other line groups. This option is available only if **Enable sending SIP REFER messages** is selected.	Not selected
Enable Processing of Received SIP REFER Messages	Determines whether CIC allows the party sending the REFER to be notified of the outcome of the received request. This option is typically set on lines going to internal gateways or CIC servers. **Notes**: Because this option can be used to enable other applications including call transfer, it can create additional calls and carrier charges.	Not selected

Related topics

SIP lines concepts

Configure a SIP line

Line Groups

Overview of line groups

The **Line Groups** container allows you to create line groups and specify membership.

Purpose

A line group identifies a group of one or more lines that are reserved for specific uses, such as long distance calls, local calls, and so on. A line group can also reserve a group of lines for calls for an individual user or a workgroup. The DialPlanEx handler determines if an outgoing call uses the next available line (default behavior), or a specific line group.

Call selection sequence

CIC's Telephony Services subsystem attempts to minimize line conflicts between inbound and outbound calls. Specifically when the DialPlanEx handler sends Telephony Services a line group to use for an outbound call, Telephony Services sorts the lines in the line group in alphabetical order. When a call is placed, Telephony Services selects the next line in the line group.

Eligible lines

Any SIP line can be part of a line group. You can include individual lines in multiple line groups.

Reporting considerations

> **Note:** To ensure accuracy in reporting, do not generate reports on line groups that contain the same lines.

Related topics

Line Group Configuration

Line Group Members

Overview of line groups

The **Line Groups** container allows you to create line groups and specify membership.

Purpose

A line group identifies a group of one or more lines that are reserved for specific uses, such as long distance calls, local calls, and so on. A line group can also reserve a group of lines for calls for an individual user or a workgroup. The DialPlanEx handler determines if an outgoing call uses the next available line (default behavior), or a specific line group.

Call selection sequence

CIC's Telephony Services subsystem attempts to minimize line conflicts between inbound and outbound calls. Specifically when the DialPlanEx handler sends Telephony Services a line group to use for an outbound call, Telephony Services sorts the lines in the line group in alphabetical order. When a call is placed, Telephony Services selects the next line in the line group.

Eligible lines

Any SIP line can be part of a line group. You can include individual lines in multiple line groups.

Reporting considerations

> **Note:** To ensure accuracy in reporting, do not generate reports on line groups that contain the same lines.

Related topics

Line Group Configuration

Line Group Members

Add a line group

To add a line group

1. In the ***<IC server>*** container, click the **Line Groups** subcontainer.
2. In the list view, right-click and then click **New**.
3. In the **Entry Name** box, type the line group name and click **OK**.
4. Complete the **Line Group Configuration** tab and the **Line Group Members** tab. For more information, click the links under *Related topics*.

Related topics

Line Group Configuration

Line Group Members

Configure a line group

To configure a line group

1. In the ***<IC server>*** container, click the **Line Groups** subcontainer.
2. In the list view, right-click the line group you want to configure and then click **Properties**.
3. In the **Description** box, type a descriptive name or sentence that describes the purpose of the line group. For example, "Line Group 1 Long Distance" or "This line group is reserved for long distance calls" could be used for a description of a group of lines reserved for long distance calls.
4. To cause CIC to generate trunk group usage statistics for reporting on the lines in this group, select the **Use for Reporting** check box. To keep the statistics clean and the line group reports useful, you must not select this check box on more than one line group that contains the same lines. If you do, Interaction Administrator warns you about the need to have unique lines in each line group that is used for reporting. You may chose to ignore the warning, but the statistics generated for the line group reports will not be reliable. When this check box is clear, CIC does not generate line group usage statistics for the lines in this line group.
5. To use this line group as a dial group when you configure dial plans, select the Use as **Dial Group** check box. Dial plans allow you to automate how certain kinds of calls are routed. For more information, see *Overview of regional dial plans* and *Overview of old dial plans*. The lines you include in a dial group should have a direction of outbound rather than inbound or both.

6. To use the dial group for a private line assignment, select the **Use for Private Line Assignment** check box. This option is available only when you first select the **Use as Dial Group** check box. For more information, see *Overview of private line assignment*.

7. Under **Hunt Selection Method**, select how CIC selects the line to ring. After you configure the line group, you use the **Members** tab to add lines to it.

- Choose **Descending Sequential** to ring lines one at a time, beginning from bottom of the list on the **Members** tab.
- Choose **Ascending Sequential** to ring lines one at a time, beginning from the top of the list on the **Members** tab. If no a call is not answered, the prompt "No one is available to take your call at this time" is played, and the call is routed back to the IVR System. Lines are distinguished by their name.
- Choose **Round-robin** to have CIC remember the last user who was sent a call. Round Robin works in a loop, repeating the process down through the list, and then the process starts over with the next call.

For example, a line group has three lines (Line1 - Line3), all available for calls and are listed Line1, Line2, Line3, in that order. If Line1 was alerted, then Line2 was alerted, even though both are now available, the next alerting call will go to Line3. Round-robin knows which line has been alerted and goes to the next available line in the list.

8. Click **OK**.

Related topics

Add a line group

Add and remove lines from a line group

Overview of dial groups

Overview of regional dial plans

Overview of old dial plans

Add and remove lines from a line group

Line groups define a group of one or more lines that can be reserved for specific uses, such as long distance and local calls. A line group can also reserve a group of lines for calls for an individual user or a workgroup. You can include individual lines in more than one line group, but be careful to not use line groups (containing the same lines) for reporting.

> **Notes:** If you combine two or more different types of lines (for example, analog lines and digital channels) in a single line group, be sure to specify the appropriate prefix numbers for the lines.

To add lines to a line group

1. In Interaction Administrator, under the server name, select the **Line Groups** container.

2. Double-click one of the line group names in the **Line Group** column. The **Line Group Configuration** window appears.
3. Select a line name in the **Available Lines** box, and then click **Add**.
4. Click **OK**.

To remove lines from a line group

1. In the **Currently Selected Lines** box, select a line name and then click **Remove**.
2. Click **OK**.

Related topics

Add a line group

Configure a SIP line

Configure a dial group entry

Line selection order

CIC's Telephony Services subsystem attempts to minimize line conflicts between inbound and outbound calls. Specifically when the DialPlanEx handler sends Telephony Services a line group to use for an outbound call, Telephony Services sorts the lines in the line group in alphabetical order. When a call is placed, Telephony Services selects the next line in the line group.

Delete a line group

> **Note:** Before you can delete a line group that is also a dial group, you must first remove the dial group.
>
> Before you can delete a line group that is used in a regional dial plan, you must first remove the line group from the regional dial plan.

To delete a line group

1. In the ***<IC server>*** container, click the **Line Groups** subcontainer.
2. In the list view, right-click the line group you want to delete and then click **Delete**.

Related topics

Overview of line groups

Overview of dial groups

A dial group is a group of lines or channels that CIC uses for outbound calls. You define dial groups in the **Line Groups** container.

> **Note:** The lines included in a dial group should have a direction of outbound or both rather than inbound to avoid line contention when dialing.

You can use dial groups in your regional dial plan to direct certain kinds of outbound calls (for example, classifications of calls) to specific lines. As an example, international calls may be directed to one dial group and local outbound calls may be directed to another dial group.

Related topics

Add a line group

Configure a dial group entry

Custom attributes

The Custom Attributes page allows you to add customized attributes so that you can reference your own variables and settings through the IceLib interface.

> **Note:** If you enabled the Enhanced Interaction Administrator Change log, then all of your changes to the Custom attributes page in the User Configuration dialog box and the Workgroup Configuration dialog box dialog box are tracked in that log. For more information, see *About the Enhanced Interaction Administrator Change Log*.

The page contains a list for the attributes and displays a **Name** and a **Value** column, and has the following buttons:

Add

Click **Add** and select an existing custom attribute from the pull-down list, enter a new custom attribute. If creating a new attribute, use a unique name, otherwise the existing attribute will be overwritten.

Edit

Click **Edit** to change the value of an existing custom attribute.

Delete

Click **Delete** to delete an existing custom attribute.

Manage Attributes

Click **Manage Attributes** to open a dialog box that displays a list of custom attributes. Click **Add** or **Delete** to manage the appearance of the custom attributes in the pull-down list.

The custom attributes are saved in the path of the root container. This **Path** is displayed at the bottom of the dialog box.

> **Note**: For more information on the Interaction Center Extension Library (IceLib), see The **System APIs section** in the PureConnect Documentation Library on the CIC server.

History

This page provides a way to manually document configuration changes and when they occurred. Changes made in Interaction Administrator are also automatically logged in the Interaction Administrator Change Notification Log (Log ID 7). Later, authorized users can run reports against this log to summarize all configuration changes.

> **Note:** If you enabled the Enhanced Interaction Administrator Change log, then all of your changes to the History page in the User Configuration dialog box and the Workgroup Configuration dialog box dialog box are tracked in that log. For more information, see *About the Enhanced Interaction Administrator Change Log*.

Last Modified

This date is automatically updated each time you click the **OK** button, presumably after you make changes to the configuration. To avoid updating this date, exit the page by clicking the **Cancel** button.

> **Note:** If you click **Cancel**, none of the changes made to this page will be preserved.

In addition, the history is updated when changes are made to the record elsewhere in Interaction Administrator. For example, when a user change his or her password, the **Last Modified** date is updated.

> **Note:** Changes to the licenses for a user or a station do not update the Last Modified date.

Date Created

This date is automatically set when the user creates the initial configuration for this page. If the page was initially created during setup, the date could be blank.

Notes

Type notes about configuration settings and changes. If you change the configuration page and click **OK**, the **Last Modified** date is updated.

You must manually enter the date beside each entry in the **Notes** field to identify the date of each note.

To create a new line in the **Notes** field, press Enter.

Stations

Overview of stations

A station represents a workstation, remote station, stand-alone fax, stand-alone phone, or unified messaging entity that is not managed by PureConnect's managed IP phone feature. You configure each station so that CIC can recognize the station and deliver messages to and from it.

> **Note:** For Switch hook stations: If a user is logged into a station, then that user's rights apply and override the station rights. If no user is logged in, the system uses the station rights.

Related topics

Overview of how to add stations

Configure a station

Overview of the default station

Overview of station templates

Overview of station groups

Add stations

Overview of how to add stations

There are several ways that you can add stations. You can use:

- The **Add Stations Assistant** to be guided through the process of quickly adding station records.
- The **Station Configuration** dialog box to add a single user record.

Related topics

Add stations with the Add Stations Assistant

Add a station with the Station Configuration dialog box

Add a station

To add a station

1. In the ***<IC_Server>*** container, double-click the **Stations** container.
2. In the list view window, right-click and then click **New**.
   The **Entry Name** dialog box appears.
3. Do one of the following:

- In the box, type the station name.
- Click ... to browse for the station.

4. Select the station type and then click **Next**.
5. Complete the configuration options. Depending on the type of station you are creating the configuration options vary.

> **Note:** If you are using a station template, some values may already be completed for you.

Related topics

Station types

Configure a station

4.

Station name

Type the name of a station connected to the network with the CIC server. A station can be one of the following kinds of devices:

- Workstation (a PC on the network, such as SUPPORT1PC)
- A phone not directly connected to the CIC (such as a remote employee working at home)
- Fax machine (a stand-alone fax machine, such as HPOfficeJet1)

Browse

Click Browse to select a station from the network. The Browse location defaults to the last open domain.

> **Hint:** Type a descriptive station name to more easily identify the kind of station, its location, the user, or another key attribute that uniquely identifies the station (such as Conference_Room_Phone, Mktg_Fax_Machine, and so on).

Related topics

Add a station

Station types

You can create several types of stations:

Station Type	Description
Workstation	A PC (with a phone) on the network in the same domain as the CIC server.
Stand-Alone Phone	A telephone that is NOT associated with a PC, but that has an extension number on the Interaction Center server.
Stand-Alone Fax	An independent fax machine with its own phone line (for example, HP OfficeJet).

Remote Station	A station assigned to a user or agent who runs a CIC client outside of the network domain of the CIC server.
Unified Messaging	This station type defines the station as a Third Party Unified Messaging provider. This station type is only available when a SIP or a Third Party Unified Messaging license is present.

> Once a station entry is complete, the only way to change that station's name is to create a new entry with the new name and configuration attributes and then delete the original station.
>
> **Note:** All stations have dialing Access Controls that determine what kinds (for example, classifications) of phone numbers each station is permitted to dial. This provides a level of dialing security to prevent toll fraud.

Add Stations Assistant

Add Stations with the Add Stations Assistant

To simplify the process of creating SIP stations, the **Add Stations Assistant** walks you through the necessary station configuration steps.

To add a station with the Add Stations Assistant

1. Under ***<IC Server>*** container, click the **Stations** Container.
2. Right-click in the right pane.
3. Select **Station Assistant**
4. Complete the pages in the wizard.
5. Click the help button on each page for instructions on how to complete the fields.

Related topics

Import SIP stations from a CSV list

Review created stations

Set access control

Save SIP station data

Import SIP Stations from a CSV List

Use this page to select the CSV file that contains SIP stations and any additional information such as name, type, extension or address.

> **Note:** The CSV file must be in UTF-8 format. For more information, see CSV files with non-English column headings

Click **Browse** to the location of the CSV file.

> **Note**: If you plan to implement managed IP phones, please note that managed IP phones/stations are imported from the Managed IP Phones Assistant in Interaction Administrator, following the CIC installation. Use Add Stations Assistant to create non-managed SIP stations only.

Click **Example** to view a sample CSV file.

A Microsoft Excel document (CSV SIP Station List.xls) and a sample CSV file (CSV SIP Station List.csv) are available on the CIC products disc in Additional Files...CSV Lists.

The SIP stations CSV file is formatted in two sections; a header section, and a data section. The header is the first row in the file and contains the names of all columns to import. Open a copy of CSV SIP Station List.xls in Excel, and enter the information in the appropriate columns for the SIP stations you wish to create. The following columns are supported:

Name (Required): This is the station name.

Type: The type must be workstation, phone, or fax.

Extension: Enter a unique extension number for the SIP station.

Identification Address: Enter the SIP identification address.

Connection Address: Enter the connection address of the SIP station. If specified, this column will create a static SIP station. If left blank the station will be dynamic.

Manufacturer: Enter Generic, Cisco, Polycom, etc.

Model: Enter the specific type of phone model made by the phone manufacturer.

- If Cisco is the manufacturer, use 7905, 7912, 7940, or 7960.
- If Polycom is the manufacturer, use SoundPoint IP 300, SoundPoint IP 500, or SoundPoint IP 600.

MAC Address: Enter the MAC address of the SIP station.

Machine Name: Maps a machine to this station for licensing.

When your additions are complete, save the document as a .CSV file type and download it to a secure location on the CIC server. You can open the new .CSV file in any text editor.

For more information, including station attribute descriptions and instructions for importing the CSV SIP Station list in Add Stations Assistant, see *CSV List Import Technical Reference* in the PureConnect Documentation Library.

Review Imported SIP Stations

Use this page to review the stations that you imported from a CSV file.

If this information is not correct, click **Back** to make changes. Otherwise click **Next**.

Access control

This page may appear when you run the Add Stations Assistant or the Managed IP Phones Assistant.

> **Note for the Add Stations Assistant**: If you created a dial plan in IC Setup Assistant, select the dial plan classifications for the new stations. If you did *not* create a dial plan in IC Setup Assistant, no Available classifications appear. After you create the dial plan in Interaction Administrator after installation, run the Add Stations Assistant in Interaction Administrator and specify the outbound dialing privileges for your stations.

Use the Access control page to select the dial plan classifications for new stations. These classifications determine the outbound dialing privileges for the new stations.

Select one or more classification names from the list of **Available** classifications and add them to the **Currently Selected** list to give the selected dialing privileges to this station.

If someone attempts to place a call from a station and the dialed phone number is not supported in one of the phone number classifications for the station, CIC plays a prompt that says that the station does not have sufficient dialing privileges to place the call.

Saving SIP Station Data

If you have reviewed your SIP station data and are ready to commit the new station creation, click on the **Commit Changes** button. After clicking **Commit Changes**, there is a progress indicator displayed while saving the SIP stations and station configurations that you have created. Depending on how many stations you created, this may take several moments.

Station Licenses

Use this page to assign licenses to the stations you are creating. This page applies to workstations or remote stations.

Basic Station License

This license represents an audio path between CIC and a station. This license is not required, but without it the audio for station does not play. A non-audio station may be used or for non-audio interactions.

Remote stations must be assigned a Basic Station license. If a user logs into a remote station, it also needs a Client Access license. (In previous versions, this was a Business User license.) If a TUI login is performed against dynamic remote stations, no Client Access license is acquired.

Client Access License

To allow the station to run a CIC client, assign this license to the station.

> **Note:** If the user has this license, the user can run any of the CIC clients.

ACD Access License

Select this check box if this workstation is an ACD station. Then select one of the following ACD licenses for the station:

- Media 1 - This license allows 1 interaction type at a given time.
- Media 2 - This license allows 2 interaction types at a given time.
- Media 3 Plus - This license allows 3 or more interaction types at a given time.

> **Note:** A station can receive ACD interactions only if it has the ACD Access License.

Interaction Process Automation License

Select the **Interaction Process Automation** check box if this user is an Interaction Process Automation user. Then select one of the following Interaction Process Automation licenses for the user:

- **Direct Routed Work Items** (I3_ACCESS_IPA_USER) license: Enables the user to launch any process to which the user has rights. It also enables the user to receive work items that are directly routed to the user.
- **Group Routed Work Items** (I3_ACCESS_IPA_USER_ACD) license: Enables the user to receive work items that are either routed to the user directly or as a member of a workgroup (similar to an ACD queue).
- **Process Monitor** (I3_ACCESS_IPA_MONITOR) license: Enables the user to view process status and details in the Process Monitor or to use Process Reporting in IC Business Manager Applications.
- **Process Designer** (I3_ACCESS_IPA_DESIGNER) license: Enables the user to use the Process Designer to create and modify Interaction Process Automation processes.

> **Note**: Each license in this list enables the user to **use the Interaction Process Automation features included in all the previous licenses in the list**. That is, the Group Routed Work Items license includes the Direct Routed Work Items license. The Process Monitor license includes both of the Routed Work Items licenses. The Process Designer license includes all the other licenses.
>
> For more information about designing processes, refer to the *Interaction Process Automation Technical Reference* and the Process Designer Help.

License List

Select any additional licenses to assign to this station.

> **Note:** For specific license information on each type of license, see the *PureConnect Licensing Overview Technical Reference* in the PureConnect Documentation Library.

Complete the Add Stations Assistant

You have successfully completed the **Add Stations Assistant**. Click **Finish** to save your changes or newly created stations. Select **I want to add additional stations** then click **Next** to run the Add Stations Assistant again.

Configure a station

Configure a station

To configure a station

1. In the ***<IC_Server>*** container, double-click the **Stations** container.
2. Do one of the following:
3. In the list view window, right-click and then click **New**.
   The **Entry Name** dialog box appears.

- To add a station, in the list view window, right-click and then click **New**.
  The **Entry Name** dialog box appears.
  Type the station name and then click **OK**.

- To edit an existing station, in the list view window, double-click a station.

4. Enter the station name and then click **OK**.
   The **Station Type** dialog box appears.

5. Select the station type and complete the other fields on the screen.

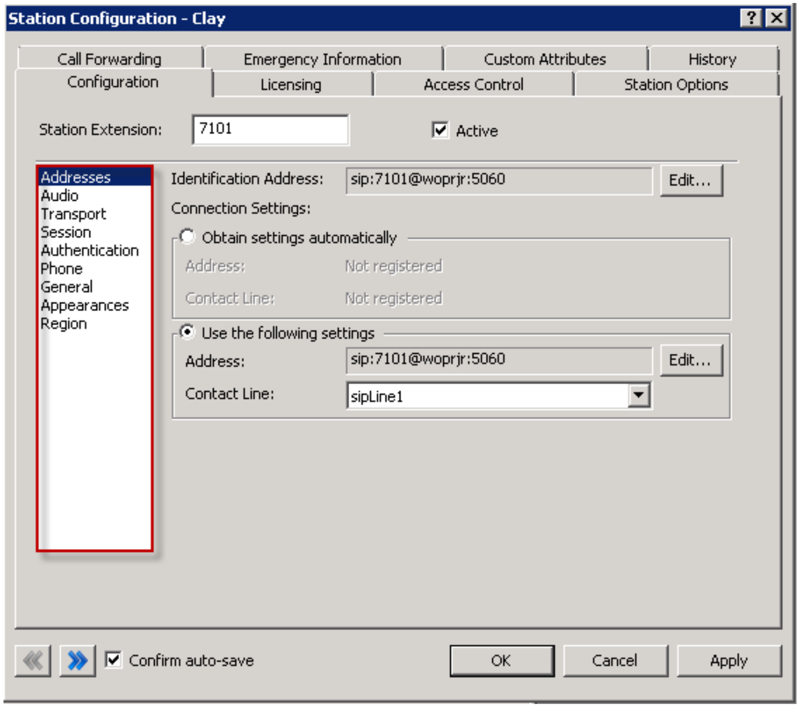
6. To use a template to create the station, in the **Station Template** list, select the template.

7. Click **Next**.
   The **Station Configuration** dialog box appears.

8. In the **Station Extension** field, type a unique extension for the station.

9. Complete any other fields that appear in the top portion of the page. For an explanation of these fields, click the links under *Related topics*.

10. If a list of headings appears along the left side of the page, click each heading and complete the required fields. The headings that appear depend on the station type. For an explanation of these fields, click the links under *Related topics*.



Station Extension: 7101 ☑ Active

Identification Address: sip:7101@woprjr:5060

Connection Settings:

○ Obtain settings automatically

Address: Not registered

Contact Line: Not registered

● Use the following settings

Address: sip:7101@woprjr:5060

Contact Line: sipLine1

☑ Confirm auto-save

11. As necessary, click the other tabs in the **Station Configuration** dialog box to specify additional configuration details. The tabs and options that appear depend on the station type. For more information on these options, use the links under **Related topics**.

12. Click **OK**.

Related topics

Addresses

Audio

Transport

Session

Authentication

Phone

General

Appearances

Region

Licensing

Licenses for standalone fax and phone stations

Access control

Options

Call forwarding

Emergency information

SIP station addresses settings

Use this page to configure your SIP station addresses. Depending on whether you are configuring a default Global SIP Station, or a stand-alone fax or phone as a station, some of these options are not available.

Station Extension (Station configuration only)

Type a unique extension number for this SIP workstation phone. During the installation of the CIC clients, the Station Extension is created based on the user's input. You can enter any extension number you like (as long as it does not conflict with existing numbers), but it is helpful to preserve a visible relationship between a user's logical extension and his or her default workstation extension.

> **Note**: If the Enable Regional Dialing option is selected in Regionalization - Location, and a change to a station extension creates an extension conflict, a message is displayed listing duplicate extensions. For later reference when resolving conflicts, click **Copy to Clipboard** to copy the listing, and then paste the content to a program that supports CSV (like Microsoft Excel).

Connection Type (Station configuration only)

This option is grayed-out and is set to SIP because you have previously selected to create a SIP workstation. Click **Back** to select a different type of workstation if this is not correct.

Active (Station configuration only)

Select this check box to activate the station. This enables the station to place and receive calls. Clear the check box to deactivate the station, preventing calls from coming in to or going out from the station.

Auto Conference (Station, if stand-alone phone, configuration only)

If this check box is selected, and if a call is already connected or held at the station, a conference is created between the new incoming call and the existing call(s). An announcement of the new call is played to the existing call(s) before the conference is established.

PIN (Station, if stand-alone phone, configuration only)

If you enabled auto conference you must enter the Personal Identification Number.

Identification Address (Station configuration only)

Click **Edit** to choose a predefined format or use an alternate format for the identification address for this SIP station.

Connection Settings

Select **Obtain Settings Automatically** or **Use the Following Settings**.

Obtain Settings Automatically (Station configuration only)

This setting allows the station's **Address** and **Contact Line** information to be dynamically updated where the contact address and the new contact line are set automatically when an IP phone registers (SIP INVITE message or REGISTER message). This option is very useful if SIP stations use DHCP and can change IP addresses frequently.

Use the Following Settings (Station configuration only)

This setting is static where you have to manually specify the contact address and contact line.

Address: Enter the User Portion, Host, and Port manually.

Contact Line: **(Global SIP Station and Station configuration)**

Select an existing SIP line from the pull-down menu to use that line's settings for registration information. In a new CIC installation, the contact line for the Global SIP Station is <Stations-UDP>.

> **Note**: If you are configuring a new station and you select "Use Global SIP Station" for the contact line on static (Use the Following Settings) SIP stations, you still need to set a contact line on the default Global SIP Station. Setup Assistant populates the contact line on the Global SIP Station with the default <Stations-UDP> setting.

Other (Station configuration only)

To enter other connection address Click **Edit** to choose a predefined format or use an alternate format.

SIP audio settings

The following table describes the SIP audio settings for the global SIP station, managed IP phones, and managed IP phones templates.

Setting	Description	Default

Use Global SIP Station Audio Settings (Station Configuration Only)	This option specifies whether stations inherit the values that are defined for the global SIP station.	
Audio Path	See the latest version of *SIP Application Note* on the Product Information site.	Dynamic
DTMF Type	The options are: • Do not use RFC2833 inband only • RFC2833 if supported, otherwise inband • **RFC2833 only**	RFC2833 if supported, otherwise inband
DTMF Payload	This option sets the value that is used for the DTMF RTP payload type. The acceptable values are 96-127. The vendor-specific values are: 100 and 102-105. **Note:** The values 100, 102-105 should not be used for AudioCodes.	101
RTP DSCP Value	This option sets the Differentiated Services Code Point (DSCP) value of Quality of Service (QoS) in transmitted RTP packets. The values are shown in both hex (00..3F) and related decimal (0..63) formats. Some values are also identified by the binary format, CS6. The range of acceptable values is 00 (0, 000000) through 3F (63, 111111). **Note**: If this is a Polycom, SIP Soft Phone, or Interaction SIP Station managed IP phone, the default value is 2E (46, 101110) EF.	18 (24, 011000) CS53
Voice Activation	This option indicates whether Voice	Not selected

Detection (VAD)	Activation Detection is enabled on your network. When Voice Activation Detection is used, no packets are sent for silence and bandwidth is saved. However, like compression, there is some loss of voice quality.	
Echo Cancellation	This option indicates whether echoes are removed from voice communications to improve the sound quality.	Selected
Allow Multiple Codecs in Outbound SDP Offer	This option indicates whether CIC delivers all of the available Codecs to the recipient endpoint when a user makes an outbound call. The recipient endpoint can then select which Codec it recognizes. You set up Codecs in the **Locations** container.	Not selected

Related topics

Configure advanced options for managed IP phones and templates

Codecs

SIP transport settings

The following table describes the SIP transport settings for the global SIP station, managed IP phones, and managed IP phone templates.

Setting	Description	Default
Use Global SIP Station Transport Settings	This option specifies whether stations inherit the values that are defined for the global SIP station. This option is available for station configurations only.	Selected
Use Proxy for Station Connections	This option indicates that the proxy list configured in the line configuration in Interaction Administrator should be used to connect stations. **Tip**: If this option is not selected, CIC	Not selected

	contacts the stations directly.	
Audio Protocol (does not apply to managed IP phones)	The audio stream on this SIP station can be unencrypted using RTP (Real Time Protocol) or encrypted using Secure RTP (SRTP). You must choose TLS as the Transport Protocol to use SRTP. Choose SRTP only if the endpoint(s) on this line support SRTP. If you select SRTP, it enables the Security option (below). Calls between devices transmitting and receiving SIP TLS messages and SRTP audio are completely secure.	
Security (does not apply to managed IP phones)	The Security list box is available only when you select SRTP as the Audio Protocol. The Security setting determines, in part, the visibility of the security icons on calls that appear in the CIC clients when placing or receiving calls via this SIP station. In an CIC system environment, some devices may support and be configured to use SRTP while other devices do not support SRTP or are not configured to use it. When two devices (e.g., two stations) that support and are configured to use SRTP connect directly, both CIC clients will always display the lock icon because the call uses SRTP from one end to the other and is therefore secure. This secure icon display is automatic and not configurable. If one device supports and is configured to use SRTP and another device does not support or use SRTP, then at least one segment of a call between these devices is not secure. That means audio between these devices needs to be transcrypted (i.e., converted) between SRTP and RTP and vice versa via an intermediate device such as the Interaction Media Server. SIP stations that handle calls that are not secure from one end to the other can use the Security list box to control the display of an open-lock icon to inform CIC client users that the call is not secure.	

	In the Security list box select Minimal to hide the display of the open-lock icon on non-secure calls. In this case, completely secure calls will always show the lock icon and all other calls will show no lock icon. If a secure call creates a conference and includes a non-secure call, the lock icon will disappear, indicating the call is no longer secure. Select **End-to-Edge** to display the open-lock icon when a call, or at least one segment of a call in the CIC system domain is or becomes non-secure. End-to-edge means from one end of the call in the CIC system up to the edge of the CIC system (e.g., a gateway connected to the PSTN). It does not indicate security conditions on the PSTN or service provider outside of the CIC domain. In this case, secure calls will always show the lock icon and all other calls that are non-secure will show the open-lock icon. If a secure call creates a conference and includes a non-secure call, all parties in the conference will see the lock icon turn into an open-lock icon. Conversely, if a non-secure conference call becomes secure from all the end points to the edge of the CIC system, the open-lock icons will change to lock icons.	
Fax Protocol	Indicates the fax protocol to use. The options are: • **T30 only** • **T38 only** • **T38 then T30**: If you select this option, CIC tries the T38 fax protocol first. If the recipient endpoint does not support this protocol, then CIC tries the T30 fax protocol.	T38 only
SIP DSCP Value	This option indicates is the Differentiated Services Code Point (DSCP) value of Quality	18 (24, 011000) CS53

	of Service (QoS) in transmitted SIP packets. The available values appear in hex (00..3F) and related decimal (0..63) formats. Some values are also identified by the binary format, CS6. The range of values available is 00 (0, 000000) through 3F (63, 111111).	

Related topics

Configure advanced options for managed IP phones and templates

PureConnect Customer Care

SIP session settings

The following table describes the SIP session settings for the global station, managed IP phones, and managed IP phone templates.

Setting	Description	Default
Use Global SIP Station Session Settings	This option specifies whether stations inherit the values that are defined for the global SIP station. This option is available for station configurations only.	
Use SIP Session Timer and SIP Session Timeout	This setting indicates whether an OPTIONS messages is sent to the remote device when a SIP session times out. By default, a timeout occurs after 60 seconds. If the remote device does not respond to the OPTIONS message, the call is disconnected.	Selected
SIP Register Interval	This setting specifies the amount of time in days, hours, minutes or seconds.	1 day
Disconnect on Broken RTP	This setting determines if a VoIP call remains active after audio has been disrupted. Audio is considered disrupted if	Selected

	no RTP, RTCP and no comfort noise packet is received from the remote device. By default, this parameter is turned on (checked).	
Media Timing	This setting specifies the timing on an INVITE request that contains a new media description in the SIP message body in the existing signaling session. The available options are: • **Normal** • **Delayed**	Delayed
Media reINVITE Timing	This setting indicates the type of timing on a re-INVITE request that contains a new media description in the SIP message body in the existing signaling session. The available options are: • **Normal** • **Delayed**	Delayed
Terminate Analysis on Connect	This setting indicates whether the call analysis procedure terminates when a SIP connection indication from the network is received. **Example:** CIC makes its PSTN call via SIP calls through a SIP/ISDN gateway. This particular SIP/ISDN gateway only sends a SIP connect message back to Interaction Center after the remote party answers the call. If call analysis is used, select this setting so that call analysis terminates when the SIP connect message is received. **Example:** CIC makes its PSTN call via SIP calls through a SIP/analog gateway. This particular SIP/Analog gateway always sends a SIP connect message back to CIC prematurely, before the remote party answers the call. If call analysis is used, deselect this setting so that call analysis continues after the SIP connect message is received.	Selected

	Tip: If the connection is to a station, the configuration of this option for the station determines the call analysis behavior.	
Disable Media Server Passthru	This setting stops the media server from rewriting the SSRC header.	Not selected
Station Connections are Persistent	This setting determines whether a persistent voice connection to the CIC server is maintained. If so, then the audio path does not disconnect until the station initiates the disconnection. If this setting is not selected, when CIC determines that the audio path to the station is no longer needed, CIC initiates the disconnection. Recommended settings: • **Operators—Selected**: If you want to handle more calls than the phone is capable of handling, select this setting. For example an operator wants to handle up to 20 simultaneous calls. • **Call Center Agents—Selected**: If call center agents use an IP phone with a headset and also uses the CIC clients, select this setting.	Not selected
Connection Call Warm Down Time	This value represents the number of seconds a connection call should remain connected after the regular call is disconnected. Once this timeout is expired, the connection call will be disconnected. **Note:** This option is not used for persistent connection calls.	5 seconds **Note**: Decreasing the default value (5 seconds) can cause stability issues and is not recommended.
Call Appearances	Select the number of call appearances the phone can handle. CIC will send up to the configured number of calls to the phone. The default value for this option is 1. **Note:** If **Persistent** is selected, the number of call appearances defaults to	

	1 and is grayed-out. Recommended settings: - **General**: This value should be over 1 for experienced phone users only. - **Cisco**: The Cisco IP phone 7960 can have up to 6 line appearances (each line appearance is equivalent to a station). Each line appearance has a unique SIP address. *Line* appearances are different than *call* appearances. Each *line* appearance handles 2 *call* appearances. Configure the phone to one line appearance and then this station configuration to 1 or 2 call appearances. - **Pingtel**: Pingtel Expressa IP phone has one line appearance that handles 4 call appearances. Set station configuration to 1, 2, 3, or 4 call appearances. This option does not apply to managed IP phones.	
Enable AutoAnswer	If selected, this option sets the phone's "Enable Talk Event" attribute to yes. This attribute allows the phone to automatically receive phone calls. If this option is not selected, the agent will not be able to pick up calls from the CIC clients or from the toast message.	Selected

Related topics

Media Server General Configuration

Configure advanced options for managed IP phones and templates

SIP station shared appearances

SIP authentication settings

The following table describes the SIP audio settings for the global SIP station, managed IP phones, and managed IP phones templates.

Enabling authentication causes the phone to exchange credentials with the CIC server before the CIC server processes its requests. SIP station authentication prevents access to Interaction Center resources from unauthorized SIP devices. If authentication fails, then the station will not be able to make outbound calls.

Setting	Description	Default
Use Global SIP Station Authentication Settings	This setting specifies whether stations inherit the values that are defined for the global SIP station. This setting is available for station configurations only.	
Authentication	This setting activates or deactivates the authentication process for this SIP station. **Note**: In the Managed IP Phone container, only the **Authentication** setting appears because the user name and password are automatically generated. When **Authentication** is selected for a managed IP phone, authentication is encrypted.	Selected
User Name	This setting is the **User Name** to be used in the authentication process. This name should match the user name configured in the SIP device being authenticated. This setting is available for station configurations only. **Note**: If you modify the user name for a global SIP station, the system checks all SIP stations that are CE Phone enabled (that have a data source and a user association). If a match is found, the data source Desired Values and the Active Directory entries are updated with the new values. For more information, see *CE Phone Administration*.	
Password	This setting is the **Password** to be used in the authentication process. This password	

	should match the password configured in the SIP device being authenticated. This setting is available for station configurations only. **Note**: If you modify the password for a global SIP station, the system checks all SIP stations that are CE Phone enabled (that have a data source and a user association). If a match is found, the data source Desired Values and the Active Directory entries are updated with the new values. For more information, see *CE Phone Administration*.	
Confirm Password	This setting is confirms the **Password**. This setting is available for station configurations only.	

Note: The **Use SIP Station Authentication Defaults** setting appears on the **Station Configuration** dialog box when the **SIP Station Authentication** setting is selected on the **Server Configuration** dialog box. Select this setting to inherit the defaults selected under **Authentication** on the **Sip Station Authentication** page of the **Server Configuration** dialog box. SIP station defaults are inherited by all SIP stations and can be overridden for a specific individual station.

Related topics

Configure advanced options for managed IP phones and templates

Genesys Support

CE Phone Administration

SIP station phone settings

Use this page to configure your SIP station manufacturer and model.

Use Global SIP Station Phone Information Settings (Station Configuration Only)

Select this check box to inherit the values defined at the Global SIP Station level.

Manufacturer

Select the manufacturer of the phone for this SIP station. Possible values are **Polycom** (default for Global SIP Station), Cisco**,** Generic**,** Aastra**,** Microsoft Lync, or free-text entry.

Model

Enter the SIP phone model.

For more information on configuring SIP stations for Zone Paging, see *Configuration of CIC Phone Features for Polycom Phones* Technical Reference in the PureConnect Documentation Library.

SIP station appearances settings

This page is not available when setting options for a Global SIP Station.

CIC's shared appearances feature allows SIP stations to use boss-assistant (primary-secondary) settings and group extensions settings to define relationships between the stations. By configuring stations to use a shared appearance, users have the following abilities:

- All members of a shared appearance group are alerted when a call alerts for the primary number.
- All members of a shared appearance group can determine that the primary number is in use.
- Users of secondary appearances can answer calls as if they are using the primary number.
- Users of secondary appearances can place calls as if they are using the primary number.

> **Notes**: This feature applies to Polycom phone models IP301, IP430, IP501, IP550, IP601, IP650 only. Similar functionality is available via the features of the CIC clients.
> For more information on configuring SIP Station shared appearances, see Managed IP Phone Configuration - General.
>
> Also see *Configuration of CIC Phone Features for Polycom Phones Technical Reference* in the PureConnect Documentation Library.

Use this page to add appearances to SIP stations. A station can have one or more shared appearance entries, where each shared appearance has:

- The name of the other station on which the **Primary Station** is appearing
- A **Number of Call Appearances** setting (similar to the existing SIP station, but is a separate setting for the shared line appearance itself)
- An **Identification Address** setting (similar to the existing SIP station, but it is a separate setting for the shared line appearance itself)
- A **Connection Address** setting (similar to the existing SIP station, but it is a separate setting for the shared line appearance itself)

> **Note:** You can create a maximum of 20 appearances per station.

The page contains two lists, **Appearance For:** and **Appearance On:**. The **Appearance For** list contains the stations that will appear on the current station being edited. The **Appearance On** list contains the stations on which the current station will appear.

Select the list in which you wish to add an entry and click **Add**.

Buttons

Use the **Up** and **Down** buttons to arrange the order of the entries in the **Appearances For** list. This order specifies the way shared line appearance buttons appear in Interaction Client.

Click **Modify** to edit settings for an existing entry or click **Delete** to remove an entry.

SIP station region settings

A region defines areas where SIP stations and lines are physically interconnected and within this region a specific dial plan may be required based on the central office or switching fabric it may be connected to.

CIC uses locations to define the bandwidth requirements and endpoints (stations and lines) for a region.

Use this page to set a location for this SIP station. *This page is not available when setting options for a Global SIP Station.*

Location

Choose the **Location** from the pull-down menu for this SIP station.

The location represents an area where devices are considered to be in the same physical place. This location defines a set of endpoints that can share a common dial plan. The stations and lines that are members of a Location are utilized by the dial plan entries that are applicable to a locale they are operating in. The location also defines the codec communications and the ability to communicate between devices and locations.

> **Note**: Location options available from the pull-down menu are defined in the Regionalization container.

Station licensing settings

Use this page to assign licenses to the station or station template. This page applies to Workstations or Remote Stations.

> **Note:** If you enabled the Enhanced Interaction Administrator Change log, then changes to station licenses are tracked in that log. For more information, see *About the Enhanced Interaction Administrator Change Log*.

Licensed Machine Name

You can associate a station with a specific machine. Typically the **Licensed Machine Name** is the station name, but you can select the check box to override this setting. Click **...** to select the machine name.

The machine name cannot be a duplicate of an already **Licensed Machine Name**. This is a required field used for licensing only, and it cannot be blank.

When you log in to ICBM, use the machine name that is associated with the station. You will not be logged off the client to which you are currently logged on.

If a module requires station audio, the module will check to see if there is a logged in station that supports audio. If there is not a station that supports audio, the audio functionality will be disabled.

Basic Station License

This license represents an audio path between CIC and a station. This license is not required, but without it the audio for station will not play, and there will be no dial tone. A non-audio station may be used or for non-audio interactions.

Remote Stations must be assigned a Basic Station license.

Client Access License

Assigning this license to the station allows the client functionality of the CIC clients. Without this license assignment, no CIC client will not run on this station.

ACD Access License

Select this check box if this workstation is an ACD station, then select the type of ACD license. These are the available types of ACD licenses:

- Media 1 - This license allows 1 interaction type at a given time.
- Media 2 - This license allows 2 interaction types at a given time.
- Media 3 Plus - This license allows 3 or more interaction types at a given time.

If **Media 1** or **Media 2** type of ACD licenses is selected, you can click **Interaction Types** and select the type of interaction from the list to apply to the license. **Interaction Types** is grayed-out and not available if **Media 3 Plus** is selected.

> **Notes:** Failure to have a ACD Access License assigned to the station will prevent that station from being ACD active.
>
> If the station (Station A) is assigned a Basic Station license and two different users (User A and User B) each have all other necessary rights (i.e., Client Access) assigned to them, then both users can simultaneously login to that station, (User A and User B can both be logged into Station A at the same time). If the second user to login does not have the necessary licenses assigned, then the second user login will fail.

Interaction Process Automation License

Select the **Interaction Process Automation** check box if this station is an Interaction Process Automation station, and then select the type of license to assign to that station.

These are the available types of Interaction Process Automation licenses:

- **Direct Routed Work Items** (I3_ACCESS_IPA_USER) license: Enables you to launch any process to which you have rights. It also enables you to receive Work Items that are directly routed to you.
- **Group Routed Work Items** (I3_ACCESS_IPA_USER_ACD) license: Enables you to receive Work Items that are either routed to you directly or as a member of a workgroup (similar to an ACD queue).

> **Note**: The Group Routed Work Items license includes the Direct Routed Work Items license.
>
> For more information about designing processes, refer to the *Interaction Process Automation Technical Reference* and the Process Designer online help.

License List

This list displays additional licenses that are available. Select the licenses you wish to assign to this station.

Enable Licenses

Select this check box to set the license settings to Active. If unchecked, the licenses settings on this page are ignored by the system. This is a way to turn off licensing for a station, but keep the license settings.

Click OK to save your changes. These license assignments are immediately reflected in the license counts in the Licenses Allocation container list.

> **Note:** For specific license information on each type of license, see the *PureConnect Licensing Overview Technical Reference* in the PureConnect Documentation Library.

Related topics

Overview of the default station

About Remote Stations

Licensing

Other Station Licenses

Licenses for stand-alone fax and stand-alone phone stations

> **Note:** If you enabled the Enhanced Interaction Administrator Change log, then changes to station licenses are tracked in that log. For more information, see *About the Enhanced Interaction Administrator Change Log*.

Use this page to assign licenses to the station or station template. This page applies to Stand-alone Fax and Stand-alone Phone station types.

Basic Station License

This license represents an audio path between CIC and a station. This license is not required, but without it the audio for station will not play. A non-audio station may be used or for non-audio interactions.

A Standalone Fax and Standalone Phone should always be assigned a Basic Station License. A Bus Device Fax station does not use a Basic Station License.

> **Note**: If the station (Station A) is assigned a Basic Station license and two different users (User A and User B) each have all other necessary rights (i.e., Client Access) assigned to them, then both users can simultaneously login to that station,   (User A and User B can both be logged into Station A at the same time). If the second user to login does not have the necessary licenses assigned, then the second user login will fail.

Recorder Access License

Assign this license to enable the ability to record on this station.

Enable Licenses

Select this check box to set the license settings to Active. If unchecked, the licenses settings on this page are ignored by the system. This is a way to turn off licensing for a station, but keep the license settings.

Click OK to save your changes. These license assignments are immediately reflected in the license counts in the Licenses Allocation container list.

> **Note:** For specific license information on each type of license, see the *PureConnect Licensing Technical Reference* in the PureConnect Documentation Library.

Related topics

Overview of the default station

Station access control settings

Station Access Control enables you to specify the outbound dialing privileges for a station, if any.

Select one or more classification names from the list of Available classifications and add them to the Currently Selected list to give the selected dialing privileges to this station. If someone attempts to place a call from this station and the dialed phone number is not supported in one of the phone number classifications for this station, CIC plays a prompt saying that the station does not have sufficient dialing privileges to place the call.

To give this station all dialing privileges, automatically including new classifications added in the future, select the **[All*]** entry, and then click **Add.**

> To prevent a CIC station (such as a stand-alone phone) from having any dialing privileges, leave the Currently Selected list of classifications blank. If someone attempts to place a call from a disabled station, CIC plays a prompt saying that the station does not have sufficient dialing privileges to place the call.

Phone number classifications are defined in the Classifications page and used in the Dial Plan page in the Phone Numbers container.

Related topics

Overview of the default station

Station options settings

Use this page to set station options.

Timeout for Incoming Interactions

This setting determines the number of seconds an incoming interaction rings at the CIC client station before the interaction quits alerting and proceeds to the next step in the handler (for example, goes to voicemail or changes an ACD agent’s status to ACD-Agent not answering and offers the interaction to another agent). The default value is 15 seconds; entering 0 (zero) also means 15 seconds. The minimum value is 7 seconds, which allows at least one full ring cycle. For North America, the standard ring duration for one ring is six seconds, which includes two seconds of ring and four seconds of pause time.

Use IC Follow Me *(applies only to Exchange - Unified Messaging users)*

Select this option to rely on the CIC server instead of the UM platform to perform this function.

Require Forced Authorization Code

Select **Require Forced Authorization Code** to require users to enter an extension and a password for certain phone classifications assigned to this station. The phone classifications have been previously set up by the server parameter "Toll Call Classifications." This setting does not apply to UM station types.

Station has MWI message light (*this option is not available on a managed workstation*)

Select **Station has MWI message light** so the system will turn on the message light (on Caller ID and ADSI telephones) whenever a caller leaves a voice message. When the message is picked up, the light is automatically turned off.

> **Note:** To fully enable the MWI feature, you must activate MWI at the default station level, the station level, and the user level.

Outbound ANI

Enter the ANI/Caller ID for the system to send when making an outbound call from this station.

> **Notes**: If a user is logged into the station and makes a call, the user's configuration for the Outbound ANI overrides this setting.
>
> This Outbound ANI option does not override a call placed with a specific Calling Party Number and Calling Party Name. Call Forwarding and Follow-me numbers placed as outbound calls use the Forwarded Parties ANI and Name where allowed.

Related topics

Overview of the default station

Activate MWI for the default station

Activate MWI for a user

User's configuration for the Outbound ANI

Station emergency information settings

Use this page to set station location options that are used in the event of an emergency.

Description

Enter the description of the location of this station. This description is displayed in station group directories in the CIC clients. For example, a description might be "Conference Room 1."

Emergency Access

Use this section to enter emergency access information for this station for emergency support.

Calling Party Number

Enter the outbound ANI (10 digit numeric) to use for emergency calls from this station. The Automatic Location Identification (ALI) record field is CPN and in "emergency" terminology it is Emergency Location Identification Number (ELIN).

Location

Enter the location information (60 digit alpha-numeric) for emergency personnel dispatched (i.e., Building 1, floor 3, north wing, office #26, next to elevator). The ALI record field is LOC.

Customer Name

Enter the name (32 character alpha-numeric) to provide for this station (i.e., John Smith). The ALI record field is NAM.

Related topics

Overview of the default station

Emergency classification

Custom attributes

The Custom Attributes page allows you to add customized attributes so that you can reference your own variables and settings through the IceLib interface.

> **Note:** If you enabled the Enhanced Interaction Administrator Change log, then all of your changes to the Custom attributes page in the User Configuration dialog box and the Workgroup Configuration dialog box dialog box are tracked in that log. For more information, see *About the Enhanced Interaction Administrator Change Log*.

The page contains a list for the attributes and displays a **Name** and a **Value** column, and has the following buttons:

Add

Click **Add** and select an existing custom attribute from the pull-down list, enter a new custom attribute. If creating a new attribute, use a unique name, otherwise the existing attribute will be overwritten.

Edit

Click **Edit** to change the value of an existing custom attribute.

Delete

Click **Delete** to delete an existing custom attribute.

Manage Attributes

Click **Manage Attributes** to open a dialog box that displays a list of custom attributes. Click **Add** or **Delete** to manage the appearance of the custom attributes in the pull-down list.

The custom attributes are saved in the path of the root container. This **Path** is displayed at the bottom of the dialog box.

> **Note**: For more information on the Interaction Center Extension Library (IceLib), see The **System APIs section** in the PureConnect Documentation Library on the CIC server.

History

This page provides a way to manually document configuration changes and when they occurred. Changes made in Interaction Administrator are also automatically logged in the Interaction Administrator Change Notification Log (Log ID 7). Later, authorized users can run reports against this log to summarize all configuration changes.

> **Note:** If you enabled the Enhanced Interaction Administrator Change log, then all of your changes to the History page in the User Configuration dialog box and the Workgroup Configuration dialog box dialog box are tracked in that log. For more information, see *About the Enhanced Interaction Administrator Change Log*.

Last Modified

This date is automatically updated each time you click the **OK** button, presumably after you make changes to the configuration. To avoid updating this date, exit the page by clicking the **Cancel** button.

> **Note:** If you click **Cancel**, none of the changes made to this page will be preserved.

In addition, the history is updated when changes are made to the record elsewhere in Interaction Administrator. For example, when a user change his or her password, the **Last Modified** date is updated.

> **Note:** Changes to the licenses for a user or a station do not update the Last Modified date.

Date Created

This date is automatically set when the user creates the initial configuration for this page. If the page was initially created during setup, the date could be blank.

Notes

Type notes about configuration settings and changes. If you change the configuration page and click **OK**, the **Last Modified** date is updated.

You must manually enter the date beside each entry in the **Notes** field to identify the date of each note.

To create a new line in the **Notes** field, press Enter.

Station templates

Overview of station templates

Station templates allow you to configure the behavior of stations by the type of station, such as standalone phone or workstation.

This feature allows you to create stations of type easily because default behavior is already defined.

By default, Interaction Administrator provides standard template types. These types are **Stand-alone Fax Machine**, **Remote Station**, **Stand-alone Phone, SIP**, and **Workstation, SIP**. These templates cannot be deleted.

Depending on the type of template you select, configuration options vary. For example, you cannot change the grayed-out options on default templates, but you can change other (not grayed-out) options.

Click on the station template type below for specific configuration information:

- Remote Station
- Stand-alone Fax Machine, SIP
- Workstation, SIP

Add a station template

To add a station template

1. In the ***<IC_Server>*** container, click the **Stations** container.
2. Click the **Templates** subcontainer.
3. In the list view window, right-click and then click **New**.
   The **Entry Name** dialog box appears.
4. Type the template name and then click **OK**.
   The **Station Type** dialog box appears.
5. Select the station type and then click **Next**.
   The **Information** dialog box appears.
6. In the **Description** box, type a meaningful description and then click **Next**.
   The configuration dialog box appears. The configuration options that appear depend on the station type that you selected. Click **Next** to view additional dialog boxes of configuration options.
7. Complete the configuration. See the links under *Related topics* for more information.

Related topics

Information

Addresses

Audio

Transport

Session

Authentication

Phone

General

Appearances

Region

Licenses

Licenses for standalone fax and phone stations

Access control

Options

Call forwarding

Emergency information

Remote station configuration template settings

To configure a remote station template, complete the information on the **Remote Station Configuration** page. For more information on the other pages in this dialog box, click the links under *Related topics*.

Ring Always

Select this check box if you want the station telephone to always ring when the user receives a call, even if the CIC client is not running or if the Ring Telephone check box is not selected.

Clear this check box to allow the state of the Ring Always check box to determine if a user's default workstation telephone rings when a new interaction arrives for a user.

Use Global Remote Station Settings

Select this check box to use the **Station Connections are Persistent** and **Connection Call Warm Down Time** settings as defined in the Default Station configuration for Remote Stations.

- **Station Connections are Persistent**

  Select this check box to maintain a persistent voice connection to the CIC server. The audio path will not disconnect until the station initiates the disconnect.

  Clear this check box to indicate when CIC determines that the audio path to the station is no longer needed, and CIC will initiate the disconnection.

- **Connection Timeout (min)**

  If a station connection is persistent, you can configure the timeout in minutes. If you leave a remote station connected, it will stay connected until it is manually disconnected, which could result in additional billing. By setting this parameter to a value in minutes greater than 0, the connection will timeout at the set number of minutes. By default, this setting is 0, meaning it is disabled and the connection will not time out.

  This option can be configured here, or in the remote station configuration.

- **Connection Call Warm Down Time**

  This value represents the number of seconds a connection call should remain connected after the regular call is disconnected. Once this timeout expired, the connection call will be disconnected. The default value for this option is 5 seconds.

> **Note**: This option is not used for persistent connection calls.

Related topics

Overview of station templates

Information

Licensing

Access control

Station Options

Custom Attributes

History

Stand-alone fax template settings

To configure a stand-alone fax template, complete the information on the **Stand-alone Fax Configuration** page. For more information on the configuration options, click the links under *Related topics*.

Related topics

Overview of station templates

Addresses

Audio

Transport

Session

Authentication

Phone

General

Region

Information

Licensing

Access control

Station Options

Custom Attributes

History

Stand-alone SIP phone template settings

To configure a stand-alone SIP phone template, complete the information on the **Stand-alone Phone Configuration** page. For more information on the configuration options, click the links under *Related topics*.

Preferred Language

Select the preferred language for the prompts for this station. The default setting is <System Default>.

Auto Conference

If this check box is selected, and if a call is already connected or held at the station, a conference is created between the new incoming call and the existing call(s). An announcement of the new call is played to the existing call(s) before the conference is established.

PIN

If you enabled auto Conference you must enter a **Personal Identification Number**.

Related topics

Overview of station templates

Addresses

Audio

Transport

Session

Authentication

Phone

General

Region

Information

Licensing

Access control

Station Options

Custom Attributes

History

Workstation template settings

To configure a stand-alone workstation template, complete the information on the **Configuration** page. For more information on the configuration options, click the links under *Related topics*.

Related topics

Overview of station templates

Addresses

Audio

Transport

Session

Authentication

Phone

General

Region

Information

Licensing

Access control

Station Options

Custom Attributes

History

Station groups

Overview of station groups

Create station groups to transfer a caller to a specific group of stations. In a station group, a user does not have to be logged on to a CIC client in order for the station to ring. For example, you might want to set up a station group for certain phones to ring after normal business hours (night transfer).

Related topics

Add a station group

Add a station group

To add a station group

1. In the ***<IC_Server>*** container, click the **Stations** container.
2. Click the **Groups** subcontainer.
3. In the list view window, right-click and then click **New**.
   The **Entry Name** dialog box appears.
4. Type the group name and then click **OK**.
   The **Station Group Configuration** dialog box appears.
5. Complete the configuration. See the links under *Related topics* for more information.

Related topics

Configure a station group

Configure a station group

Configure a station group

To configure a station group

1. In the ***<IC_Server>*** container, click the **Stations** container.
2. Click the **Groups** subcontainer.
3. Double-click the station group that you want to configure.
   The **Station Group Configuration** dialog box appears. Complete fields on the tabs. See the links under **Related topics** for complete information.

Related topics

Configuration

Members

Custom Attributes

History

Configuration

Use this page to select the configuration options for a station group.

Extension

Type a unique extension for the station group.

> **Notes**: See DID/DNIS Routing for information on mapping DID/DNIS to station groups.
>
> If the **Enable Regional Dialing** option is selected in **Regionalization - Location**, and a change to a station group extension creates an extension conflict, a message is displayed listing duplicate extensions. For later reference when resolving conflicts, click **Copy to Clipboard** to copy the listing, and then paste the content to a program that supports CSV (like Microsoft Excel).

Type

There are several types of station groups: **Group Ring, Sequential**, and **Round-robin**.

Type	Description
Group	Simultaneously alerts the members of a Workgroup that a call is available in the queue for that Workgroup. Selecting **Group Ring** disables the Agent Utilization, ACD Skills, and ACD Actions functions (the items on those tabs will not be available). The length of the **Group Ring** is determined by the Workgroup Offering Call Timeout setting. **Note:** There can be a maximum of 20 members (stations or users) in a workgroup that uses group ring.
Sequential	Alerts individual members of a Workgroup that a new call is available in the queue for that Workgroup. Members are alerted to the call in the order specified in **Workgroup Configuration** properties>**Members** page >under **Currently Selected Users**. For more information on alerting users in Workgroup queues, see Maintain Order in Workgroup Members Help. Selecting **Sequential** disables the Agent Utilization, ACD Skills, and ACD Actions functions (the items on those tabs will not be available).The length of the **Sequential Ring** is determined by the Workgroup Offering Call Timeout setting.
Round Robin	Similar to linear hunt groups, CIC's Round Robin remembers the last user who was sent a call. Round Robin works in a loop, repeating the process down the through list, and then

	the process starts over with the next call. For example, a workgroup has three users (User1 - User3), all available for workgroup calls and are listed User1, User2, User3, in that order . If User1 received the last call but is available, the next alerting call will go to User2 if available. If User2 is not available, the call will go to User3. The next alerting call after that will go back to User1 if that user is available. If you select the Maintain Order option (in Workgroup Configuration properties --> Members --> Currently Selected Users), members are alerted to the call in the order specified in the list. For more information on alerting users in Workgroup queues, see Maintain Order in Workgroup Members Help. Selecting Round Robin disables the Agent Utilization, ACD Skills, and ACD Actions functions (the items on those tabs will not be available).

- Choose **Group Ring** to simultaneously ring the stations in the group. All phones ring until the call times out after 1 minute. At that time, the prompt, "No one is available to take your call at this time" is played. The call is then routed back to the IVR system**.**
- Choose **Sequential** to ring stations one at a time, in the order specified in Station Group Configuration dialog, in the Currently Selected Stations box on the Members page. In the sequential **Retries** box, type the number of retries for calling each station before timing out. The default is 1. If the number of retries is reached and no one answers, the prompt, "No one is available to take your call at this time" is played and the call is routed back to the IVR System.
- **C**hoose **Round-robin** to have CIC remember the last user who was sent a call. Round Robin works in a loop, repeating the process down through the list, and then the process starts over with the next call.

For example, a station group has three stations (Station1 - Station3), all available for workgroup calls and are listed Station1, Station2, Station3, in that order . If Station1 was alerted, then Station2 was alerted, even though both are now available, the next alerting call will go to Station3. Round-robin knows which station has been alerted and goes to the next available station in the list.

Selecting Round-robin disables the Agent Utilization, ACD Skills, and ACD Actions functions (the items on those tabs will not be available).The length of the Round-robin ring is determined by the Workgroup Offering Call Timeout setting.

> **Note:** If you select the Maintain Order option for the workgroup members, then the members are alerted to the call in the order specified in the list. For more information on alerting users in workgroup queues, see *Workgroup Members*.

Station Timeout (sec)

This is the amount of time in seconds that each individual station will alert using any of the alert types. The default value is 15 seconds.

Must Answer

Select **Must Answer**, for Group Ring or Sequential, for the call to continue ringing. Also, **Must Answer** will only work if stations in the station group are available to be alerted. Selecting this option causes Round-robin and Sequential to try the members of the station group 3000 times.

> **Enhanced call routing to station phones**
>
> Station groups can contain station devices only. If a user is logged into a station group phone, a call to the station group will also appear in My Interactions in the user's CIC client, in the same way as regular calls. Users should always see a call to a station that they are logged into.

Related topics

DID/DNIS Routing

Workgroup members

Members

Use this page to add stations to a station group.

Available Stations

In the **Available Stations** box, select the stations to include in the station group, and click **Add**.

> **Note:** Stations can be stand-alone phone stations, workstations, or stand-alone fax stations.

Station groups can contain station devices only. If a user is logged into a station group phone, a call to the station group will also appear in My Interactions in the user's CIC client, in the same way as regular calls. Users should always see a call to a station that they are logged into.

Currently Selected Stations

This box displays the stations you have included in the Station Group. To remove a station, select is and click **Remove**.

> **Note:** If you have selected sequential ring, stations ring in the order listed in this box.

For more information on adding SIP stations to a station group for Zone Paging, see *Configuration of CIC Phone Features for Polycom Phones Technical Reference* in the PureConnect Documentation Library.

Custom attributes

The Custom Attributes page allows you to add customized attributes so that you can reference your own variables and settings through the IceLib interface.

> **Note:** If you enabled the Enhanced Interaction Administrator Change log, then all of your changes to the Custom attributes page in the User Configuration dialog box and the Workgroup Configuration dialog box dialog box are tracked in that log. For more information, see About the Enhanced Interaction Administrator Change Log.

The page contains a list for the attributes and displays a **Name** and a **Value** column, and has the following buttons:

Add

Click **Add** and select an existing custom attribute from the pull-down list, enter a new custom attribute. If creating a new attribute, use a unique name, otherwise the existing attribute will be overwritten.

Edit

Click **Edit** to change the value of an existing custom attribute.

Delete

Click **Delete** to delete an existing custom attribute.

Manage Attributes

Click **Manage Attributes** to open a dialog box that displays a list of custom attributes. Click **Add** or **Delete** to manage the appearance of the custom attributes in the pull-down list.

The custom attributes are saved in the path of the root container. This **Path** is displayed at the bottom of the dialog box.

> **Note**: For more information on the Interaction Center Extension Library (IceLib), see The **System APIs section** in the PureConnect Documentation Library on the CIC server.

History

This page provides a way to manually document configuration changes and when they occurred. Changes made in Interaction Administrator are also automatically logged in the Interaction Administrator Change Notification Log (Log ID 7). Later, authorized users can run reports against this log to summarize all configuration changes.

> **Note:** If you enabled the Enhanced Interaction Administrator Change log, then all of your changes to the History page in the User Configuration dialog box and the Workgroup Configuration dialog box dialog box are tracked in that log. For more information, see About the Enhanced Interaction Administrator Change Log.

Last Modified

This date is automatically updated each time you click the **OK** button, presumably after you make changes to the configuration. To avoid updating this date, exit the page by clicking the **Cancel** button.

> **Note:** If you click **Cancel**, none of the changes made to this page will be preserved.

In addition, the history is updated when changes are made to the record elsewhere in Interaction Administrator. For example, when a user change his or her password, the **Last Modified** date is updated.

> **Note:** Changes to the licenses for a user or a station do not update the Last Modified date.

Date Created

This date is automatically set when the user creates the initial configuration for this page. If the page was initially created during setup, the date could be blank.

Notes

Type notes about configuration settings and changes. If you change the configuration page and click **OK**, the **Last Modified** date is updated.

You must manually enter the date beside each entry in the **Notes** field to identify the date of each note.

To create a new line in the **Notes** field, press Enter.

Default Station

Overview of the default station

The default station represents the set of configuration options that apply to all stations.

Related topics

Configure the default station

Options for the default station

Options for the global SIP station

Configure options for remote stations

Configure auto extensions

Configure the default station

To configure the default station

1. In the ***<IC_Server>*** container, double-click the **Stations** container.
2. Click the **Default Station** container.
3. In the list view window, double-click **Configuration**.
4. In the **Default Station Configuration** dialog box, complete the tabs. For more information about the configuration options on those tabs, click the links under *Related topics*.

Related topics

Station Options

Global SIP Station

Remote Stations

Stations Auto Extensions

Options for the default station

Use this page to configure settings that affect all stations.

> **Notes**: The settings on this page are not inherited when you add a SIP station. A new SIP station inherits only the settings in the Global SIP Station.
>
> To fully enable the MWI feature, you must activate MWI for the default station, for the station that user uses, and for the user.

MWI

Use these check boxes to configure Message Waiting Indicator (MWI) behavior for this default station.

Message Light

Select this check box to activate message light logic in the Interaction Center for this default station. Disable it to turn this option off.

Message Light Persistent

Select this check box to set the message light on the phone associated with this default station to persistent in the on state while any unread voicemails exist.

If you enable Message Light and disable Message Light Persistent it causes the message light on the phone to turn off after the first unread voicemail is read.

Related topics

Global SIP Station

Activate MWI for a user

Activate MWI for a station

Global SIP Station

Options for the global SIP station

For information about the configuration options for the global SIP station, click the links under *Related topics*.

Related topics

Addresses

Audio

Transport

Session

Authentication

Phone

SIP station addresses settings

Use this page to configure your SIP station addresses. Depending on whether you are configuring a default Global SIP Station, or a stand-alone fax or phone as a station, some of these options are not available.

Station Extension *(Station configuration only)*

Type a unique extension number for this SIP workstation phone. During the installation of the CIC clients, the Station Extension is created based on the user's input. You can enter any extension number you like (as long as it does not conflict with existing numbers), but it is helpful to preserve a visible relationship between a user's logical extension and his or her default workstation extension.

> **Note**: If the Enable Regional Dialing option is selected in Regionalization - Location, and a change to a station extension creates an extension conflict, a message is displayed listing duplicate extensions. For later reference when resolving conflicts, click **Copy to Clipboard** to copy the listing, and then paste the content to a program that supports CSV (like Microsoft Excel).

Connection Type *(Station configuration only)*

This option is grayed-out and is set to SIP because you have previously selected to create a SIP workstation. Click **Back** to select a different type of workstation if this is not correct.

Active *(Station configuration only)*

Select this check box to activate the station. This enables the station to place and receive calls. Clear the check box to deactivate the station, preventing calls from coming in to or going out from the station.

Auto Conference *(Station, if stand-alone phone, configuration only)*

If this check box is selected, and if a call is already connected or held at the station, a conference is created between the new incoming call and the existing call(s). An announcement of the new call is played to the existing call(s) before the conference is established.

PIN *(Station, if stand-alone phone, configuration only)*

If you enabled auto conference you must enter the Personal Identification Number.

Identification Address *(Station configuration only)*

Click **Edit** to choose a predefined format or use an alternate format for the identification address for this SIP station.

Connection Settings

Select **Obtain Settings Automatically** or **Use the Following Settings**.

Obtain Settings Automatically (Station configuration only)

This setting allows the station's **Address** and **Contact Line** information to be dynamically updated where the contact address and the new contact line are set automatically when an IP phone registers (SIP INVITE message or REGISTER message). This option is very useful if SIP stations use DHCP and can change IP addresses frequently.

Use the Following Settings (Station configuration only)

This setting is static where you have to manually specify the contact address and contact line.

Address: Enter the User Portion, Host, and Port manually.

Contact Line: **(Global SIP Station and Station configuration)**

Select an existing SIP line from the pull-down menu to use that line's settings for registration information. In a new CIC installation, the contact line for the Global SIP Station is <Stations-UDP>.

> **Note**: If you are configuring a new station and you select "Use Global SIP Station" for the contact line on static (Use the Following Settings) SIP stations, you still need to set a contact line on the default Global SIP Station. Setup Assistant populates the contact line on the Global SIP Station with the default <Stations-UDP> setting.

Other (Station configuration only)

To enter other connection address Click **Edit** to choose a predefined format or use an alternate format.

SIP audio settings

The following table describes the SIP audio settings for the global SIP station, managed IP phones, and managed IP phones templates.

Setting	Description	Default
Use Global SIP Station Audio Settings (Station Configuration Only)	This option specifies whether stations inherit the values that are defined for the global SIP station.	
Audio Path	See the latest version of *SIP Application Note* on the Product Information site.	Dynamic
DTMF Type	The options are: • Do not use RFC2833 inband only	RFC2833 if supported, otherwise inband

	• RFC2833 if supported, otherwise inband • **RFC2833 only**	
DTMF Payload	This option sets the value that is used for the DTMF RTP payload type. The acceptable values are 96-127. The vendor-specific values are: 100 and 102-105. **Note:** The values 100, 102-105 should not be used for AudioCodes.	101
RTP DSCP Value	This option sets the Differentiated Services Code Point (DSCP) value of Quality of Service (QoS) in transmitted RTP packets. The values are shown in both hex (00..3F) and related decimal (0..63) formats. Some values are also identified by the binary format, CS6. The range of acceptable values is 00 (0, 000000) through 3F (63, 111111). **Note**: If this is a Polycom, SIP Soft Phone, or Interaction SIP Station managed IP phone, the default value is 2E (46, 101110) EF.	18 (24, 011000) CS53
Voice Activation Detection (VAD)	This option indicates whether Voice Activation Detection is enabled on your network. When Voice Activation Detection is used, no packets are sent for silence and bandwidth is saved. However, like compression, there is some loss of voice quality.	Not selected
Echo Cancellation	This option indicates whether echoes are removed from voice communications to improve the sound quality.	Selected
Allow Multiple Codecs in Outbound SDP	This option indicates whether CIC delivers all of the available Codecs to the recipient endpoint when a user makes an outbound	Not selected

Offer	call. The recipient endpoint can then select which Codec it recognizes. You set up Codecs in the **Locations** container.	

Related topics

Configure advanced options for managed IP phones and templates

Codecs

SIP transport settings

The following table describes the SIP transport settings for the global SIP station, managed IP phones, and managed IP phone templates.

Setting	Description	Default
Use Global SIP Station Transport Settings	This option specifies whether stations inherit the values that are defined for the global SIP station. This option is available for station configurations only.	Selected
Use Proxy for Station Connections	This option indicates that the proxy list configured in the line configuration in Interaction Administrator should be used to connect stations. **Tip**: If this option is not selected, CIC contacts the stations directly.	Not selected
Audio Protocol (does not apply to managed IP phones)	The audio stream on this SIP station can be unencrypted using RTP (Real Time Protocol) or encrypted using Secure RTP (SRTP). You must choose TLS as the Transport Protocol to use SRTP. Choose SRTP only if the endpoint(s) on this line support SRTP. If you select SRTP, it enables the Security option (below). Calls between devices transmitting and receiving SIP TLS messages and SRTP audio are completely secure.	

Security (does not apply to managed IP phones)	The Security list box is available only when you select SRTP as the Audio Protocol. The Security setting determines, in part, the visibility of the security icons on calls that appear in the CIC clients when placing or receiving calls via this SIP station. In an CIC system environment, some devices may support and be configured to use SRTP while other devices do not support SRTP or are not configured to use it. When two devices (e.g., two stations) that support and are configured to use SRTP connect directly, both CIC clients will always display the lock icon because the call uses SRTP from one end to the other and is therefore secure. This secure icon display is automatic and not configurable. If one device supports and is configured to use SRTP and another device does not support or use SRTP, then at least one segment of a call between these devices is not secure. That means audio between these devices needs to be transcrypted (i.e., converted) between SRTP and RTP and vice versa via an intermediate device such as the Interaction Media Server. SIP stations that handle calls that are not secure from one end to the other can use the Security list box to control the display of an open-lock icon to inform CIC client users that the call is not secure. In the Security list box select Minimal to hide the display of the open-lock icon on non-secure calls. In this case, completely secure calls will always show the lock icon and all other calls will show no lock icon. If a secure call creates a conference and includes a non-secure call, the lock icon will disappear, indicating the call is no longer secure. Select **End-to-Edge** to display the open-lock icon when a call, or at least one segment of a call in the CIC system domain is or becomes non-secure. End-to-edge means from one end of the call in the CIC	

	system up to the edge of the CIC system (e.g., a gateway connected to the PSTN). It does not indicate security conditions on the PSTN or service provider outside of the CIC domain. In this case, secure calls will always show the lock icon and all other calls that are non-secure will show the open-lock icon. If a secure call creates a conference and includes a non-secure call, all parties in the conference will see the lock icon turn into an open-lock icon. Conversely, if a non-secure conference call becomes secure from all the end points to the edge of the CIC system, the open-lock icons will change to lock icons.	
Fax Protocol	Indicates the fax protocol to use. The options are: • **T30 only** • **T38 only** • **T38 then T30**: If you select this option, CIC tries the T38 fax protocol first. If the recipient endpoint does not support this protocol, then CIC tries the T30 fax protocol.	T38 only
SIP DSCP Value	This option indicates is the Differentiated Services Code Point (DSCP) value of Quality of Service (QoS) in transmitted SIP packets. The available values appear in hex (00..3F) and related decimal (0..63) formats. Some values are also identified by the binary format, CS6. The range of values available is 00 (0, 000000) through 3F (63, 111111).	18 (24, 011000) CS53

Related topics

Configure advanced options for managed IP phones and templates

PureConnect Customer Care

SIP session settings

The following table describes the SIP session settings for the global station, managed IP phones, and managed IP phone templates.

Setting	Description	Default
Use Global SIP Station Session Settings	This option specifies whether stations inherit the values that are defined for the global SIP station. This option is available for station configurations only.	
Use SIP Session Timer and SIP Session Timeout	This setting indicates whether an OPTIONS messages is sent to the remote device when a SIP session times out. By default, a timeout occurs after 60 seconds. If the remote device does not respond to the OPTIONS message, the call is disconnected.	Selected
SIP Register Interval	This setting specifies the amount of time in days, hours, minutes or seconds.	1 day
Disconnect on Broken RTP	This setting determines if a VoIP call remains active after audio has been disrupted. Audio is considered disrupted if no RTP, RTCP and no comfort noise packet is received from the remote device. By default, this parameter is turned on (checked).	Selected
Media Timing	This setting specifies the timing on an INVITE request that contains a new media description in the SIP message body in the existing signaling session. The available options are: • **Normal** • **Delayed**	Delayed

Media reINVITE Timing	This setting indicates the type of timing on a re-INVITE request that contains a new media description in the SIP message body in the existing signaling session. The available options are: • **Normal** • **Delayed**	Delayed
Terminate Analysis on Connect	This setting indicates whether the call analysis procedure terminates when a SIP connection indication from the network is received. **Example:** CIC makes its PSTN call via SIP calls through a SIP/ISDN gateway. This particular SIP/ISDN gateway only sends a SIP connect message back to Interaction Center after the remote party answers the call. If call analysis is used, select this setting so that call analysis terminates when the SIP connect message is received. **Example:** CIC makes its PSTN call via SIP calls through a SIP/analog gateway. This particular SIP/Analog gateway always sends a SIP connect message back to CIC prematurely, before the remote party answers the call. If call analysis is used, deselect this setting so that call analysis continues after the SIP connect message is received. **Tip**: If the connection is to a station, the configuration of this option for the station determines the call analysis behavior.	Selected
Disable Media Server Passthru	This setting stops the media server from rewriting the SSRC header.	Not selected
Station Connections are Persistent	This setting determines whether a persistent voice connection to the CIC server is maintained. If so, then the audio path does not disconnect until the station initiates the disconnection.	Not selected

	If this setting is not selected, when CIC determines that the audio path to the station is no longer needed, CIC initiates the disconnection. Recommended settings: • **Operators—Selected**: If you want to handle more calls than the phone is capable of handling, select this setting. For example an operator wants to handle up to 20 simultaneous calls. • **Call Center Agents—Selected**: If call center agents use an IP phone with a headset and also uses the CIC clients, select this setting.	
Connection Call Warm Down Time	This value represents the number of seconds a connection call should remain connected after the regular call is disconnected. Once this timeout is expired, the connection call will be disconnected. **Note:** This option is not used for persistent connection calls.	5 seconds **Note**: Decreasing the default value (5 seconds) can cause stability issues and is not recommended.
Call Appearances	Select the number of call appearances the phone can handle. CIC will send up to the configured number of calls to the phone. The default value for this option is 1. **Note:** If **Persistent** is selected, the number of call appearances defaults to 1 and is grayed-out. Recommended settings: • **General**: This value should be over 1 for experienced phone users only. • **Cisco**: The Cisco IP phone 7960 can have up to 6 line appearances (each line appearance is equivalent to a station). Each line appearance has a unique SIP address. *Line* appearances are different than *call* appearances. Each *line* appearance handles 2 *call* appearances.	

	Configure the phone to one line appearance and then this station configuration to 1 or 2 call appearances. - **Pingtel**: Pingtel Expressa IP phone has one line appearance that handles 4 call appearances. Set station configuration to 1, 2, 3, or 4 call appearances. This option does not apply to managed IP phones.	
Enable AutoAnswer	If selected, this option sets the phone's "Enable Talk Event" attribute to yes. This attribute allows the phone to automatically receive phone calls. If this option is not selected, the agent will not be able to pick up calls from the CIC clients or from the toast message.	Selected

Related topics

Media Server General Configuration

Configure advanced options for managed IP phones and templates

SIP station shared appearances

SIP authentication settings

The following table describes the SIP audio settings for the global SIP station, managed IP phones, and managed IP phones templates.

Enabling authentication causes the phone to exchange credentials with the CIC server before the CIC server processes its requests. SIP station authentication prevents access to Interaction Center resources from unauthorized SIP devices. If authentication fails, then the station will not be able to make outbound calls.

Setting	Description	Default
Use Global SIP Station Authentication Settings	This setting specifies whether stations inherit the values that are defined for the global SIP station. This setting is available for station configurations only.	

Authentication	This setting activates or deactivates the authentication process for this SIP station. **Note**: In the Managed IP Phone container, only the **Authentication** setting appears because the user name and password are automatically generated. When **Authentication** is selected for a managed IP phone, authentication is encrypted.	Selected
User Name	This setting is the **User Name** to be used in the authentication process. This name should match the user name configured in the SIP device being authenticated. This setting is available for station configurations only. **Note**: If you modify the user name for a global SIP station, the system checks all SIP stations that are CE Phone enabled (that have a data source and a user association). If a match is found, the data source Desired Values and the Active Directory entries are updated with the new values. For more information, see *CE Phone Administration*.	
Password	This setting is the **Password** to be used in the authentication process. This password should match the password configured in the SIP device being authenticated. This setting is available for station configurations only. **Note**: If you modify the password for a global SIP station, the system checks all SIP stations that are CE Phone enabled (that have a data source and a user association). If a match is found, the data source Desired Values and the Active Directory entries are updated with the new values. For more information, see *CE Phone*	

	Administration.	
Confirm Password	This setting is confirms the **Password**. This setting is available for station configurations only.	

Note: The **Use SIP Station Authentication Defaults** setting appears on the **Station Configuration** dialog box when the **SIP Station Authentication** setting is selected on the **Server Configuration** dialog box. Select this setting to inherit the defaults selected under **Authentication** on the **Sip Station Authentication** page of the **Server Configuration** dialog box. SIP station defaults are inherited by all SIP stations and can be overridden for a specific individual station.

Related topics

Configure advanced options for managed IP phones and templates

Genesys Support

CE Phone Administration

SIP station phone settings

Use this page to configure your SIP station manufacturer and model.

Use Global SIP Station Phone Information Settings (Station Configuration Only)

Select this check box to inherit the values defined at the Global SIP Station level.

Manufacturer

Select the manufacturer of the phone for this SIP station. Possible values are **Polycom** (default for Global SIP Station), Cisco**,** Generic**,** Aastra**,** Microsoft Lync, or free-text entry.

Model

Enter the SIP phone model.

For more information on configuring SIP stations for Zone Paging, see *Configuration of CIC Phone Features for Polycom Phones* Technical Reference in the PureConnect Documentation Library.

Configure remote station options

CIC supports remote agents who run CIC clients outside of the network domain of the CIC server. Most commonly, these agents have a PC at home with two phone lines (or ISDN, etc.), and access to the CIC server via the Internet. These agents can connect CIC clients to the CIC server and have incoming company calls routed to them at home. This Remote Station Configuration page allows you to specify a line group to carry calls routed to remote agents.

> **Note:** You must create the line group in the Line Group container before you can assign it to carry calls to remote stations.

Line Group

Select the (predefined) line group from the drop-down list. When the program routes an incoming call to a remote agent connected to CIC, that call is forwarded to the remote agent using a line in the specified line group. This setting affects agents logged into remote stations and agents logged into remote numbers.

Disable Automatic Connect on no-ringback / no-answer

Select this check box to prevent false connections with long PBX delays.

Station Connections are Persistent

Select this check box to maintain a persistent voice connection to the CIC server. The audio path will not disconnect until the station initiates the disconnection.

Clear this check box to indicate when CIC determines that the audio path to the station is no longer needed, and CIC will initiate the disconnection.

Connection Timeout (min)

If a station connection is persistent, you can configure the timeout in minutes. If you leave a remote station connected, it will stay connected until it is manually disconnected, which could result in additional billing. By setting this parameter to a value in minutes greater than 0, the connection will timeout at the set number of minutes. By default, this setting is 0, meaning it is disabled and the connection will not time out.

This option can be configured here, or in the default remote station configuration.

Connection Call Warm Down Time

This value represents the number of seconds a connection call should remain connected after the regular call is disconnected. Once this timeout is expired, the connection call will be disconnected. The default value for this option is 5 seconds.

> **Note**: This option is not used for persistent connection calls.

Configure how extensions are automatically assigned

Use this page to set the default values for the Automatic Extensions feature.

Each CIC station requires a unique extension. And extension is recommend to be 3 to 6 digits. A station extension cannot start with the digit '0'.

Starting Extension

Enter the starting extension number. The default setting is 100.

Overwrite existing extensions

Select this check box to change already existing extensions with the new extension numbers. By default, this option is not enabled.

Next Station Extension

The next station extension is always the starting extension.

Custom attributes

The Custom Attributes page allows you to add customized attributes so that you can reference your own variables and settings through the IceLib interface.

> **Note:** If you enabled the Enhanced Interaction Administrator Change log, then all of your changes to the Custom attributes page in the User Configuration dialog box and the Workgroup Configuration dialog box dialog box are tracked in that log. For more information, see *About the Enhanced Interaction Administrator Change Log*.

The page contains a list for the attributes and displays a **Name** and a **Value** column, and has the following buttons:

Add

Click **Add** and select an existing custom attribute from the pull-down list, enter a new custom attribute. If creating a new attribute, use a unique name, otherwise the existing attribute will be overwritten.

Edit

Click **Edit** to change the value of an existing custom attribute.

Delete

Click **Delete** to delete an existing custom attribute.

Manage Attributes

Click **Manage Attributes** to open a dialog box that displays a list of custom attributes. Click **Add** or **Delete** to manage the appearance of the custom attributes in the pull-down list.

The custom attributes are saved in the path of the root container. This **Path** is displayed at the bottom of the dialog box.

> **Note**: For more information on the Interaction Center Extension Library (IceLib), see The **System APIs section** in the PureConnect Documentation Library on the CIC server.

History

This page provides a way to manually document configuration changes and when they occurred. Changes made in Interaction Administrator are also automatically logged in the Interaction Administrator Change Notification Log (Log ID 7). Later, authorized users can run reports against this log to summarize all configuration changes.

> **Note:** If you enabled the Enhanced Interaction Administrator Change log, then all of your changes to the History page in the User Configuration dialog box and the Workgroup Configuration dialog box dialog box are tracked in that log. For more information, see *About the Enhanced Interaction Administrator Change Log*.

Last Modified

This date is automatically updated each time you click the **OK** button, presumably after you make changes to the configuration. To avoid updating this date, exit the page by clicking the **Cancel** button.

> **Note:** If you click **Cancel**, none of the changes made to this page will be preserved.

In addition, the history is updated when changes are made to the record elsewhere in Interaction Administrator. For example, when a user change his or her password, the **Last Modified** date is updated.

> **Note:** Changes to the licenses for a user or a station do not update the Last Modified date.

Date Created

This date is automatically set when the user creates the initial configuration for this page. If the page was initially created during setup, the date could be blank.

Notes

Type notes about configuration settings and changes. If you change the configuration page and click **OK**, the **Last Modified** date is updated.

You must manually enter the date beside each entry in the **Notes** field to identify the date of each note.

To create a new line in the **Notes** field, press Enter.

Station configuration

Use this page to enter a physical extension for the station and complete the configuration options that are specific to the type of station that you are creating.

Station Extension

Type a unique extension number for this workstation's analog (or PC) phone. During the installation of the CIC clients, the Station Extension is created based on the user's input. You can enter any extension number you like (as long as it does not conflict with existing numbers), but it is helpful to preserve a visible relationship between a user's logical extension and his or her default workstation extension.

The extension can be dialed directly to ring the analog phone at this workstation, regardless of who is logged in to the network at this workstation. The analog phone at this extension also rings if:

A call is sent to a user's queue on his or her default workstation, that user does not have a DND status, and the Ring Always check box is selected. It doesn't matter if a CIC client is running or not when the Ring Always check box is selected.

> **Note**: If the **Enable Regional Dialing** option is selected in **Regionalization - Location**, and a change to a user extension creates an extension conflict, a message appears with the duplicate extensions. To streamline the process of resolving the duplicate extensions, click **Copy to Clipboard**. Then paste the content to a program that supports CSV (like Microsoft Excel).

Active

Select this check box to activate the station. This enables the station to place and receive calls. Clear the check box to deactivate the station, preventing calls from coming in to or going out from

the station.

Preferred Language

Select the preferred language for the prompts for this station. The default setting is <System Default>.

Auto Conference

If this check box is selected, and if a call is already connected or held at the station, a conference is created between the new incoming call and the existing call(s). An announcement of the new call is played to the existing call(s) before the conference is established.

PIN

If you enabled **Auto Conference** you must enter the Personal Identification Number**.**

Related topics

Overview of the default station

Addresses

Audio

Transport

Session

Authentication

Phone

General

Appearances

Region

Licensing

Licenses for standalone fax and phone stations

Access control

Options

Call forwarding

Emergency information

Remote Station Configuration

Use this page to configure the remote station.

Active

Select this check box to activate the station. This enables the station to place and receive calls. Clear the check box to deactivate the station, preventing calls from coming in to or going out from the station.

Connection

Enter the phone number or SIP address for this connection.

Ring Always

This check box controls whether or not the telephone associated with a workstation rings when incoming calls alert on that station. The Ring Always check box always overrides the setting in the CIC client. If the station configuration in Interaction Administrator has Ring Always selected, on the Client Configuration page, the "Ring telephone for calls" option is selected and grayed out by default and the user can not override it.

Select this check box if you want the station telephone to always ring when the user receives a call, even if the CIC client is not running or if the Ring Telephone check box is not selected. Clear this check box to allow the state of the Ring telephone for calls check box to determine if a user's default workstation telephone rings when a new interaction arrives for a user.

> **Notes**: Selecting Ring Always prevents the agent/user from controlling the telephone ringing - this setting always overrides the CIC client option.
>
> This option must be selected to properly enabled a default workstation for a user.

Use Global Remote Station Settings

Select this check box to use the **Station Connections are Persistent, Connection Timeout**, and **Connection Call Warm Down Time** settings as defined in the Default Station Configuration for Remote Stations.

Station Connections are Persistent

Select this check box to maintain a persistent voice connection to the CIC server. The audio path will not disconnect until the station initiates the disconnection.

Clear this check box to indicate when CIC determines that the audio path to the station is no longer needed, and CIC will initiate the disconnection.

Connection Timeout (min)

If a station connection is persistent, you can configure the timeout in minutes. If you leave a remote station connected, it will stay connected until it is manually disconnected, which could result in additional billing. By setting this parameter to a value in minutes greater than 0, the connection will timeout at the set number of minutes. By default, this setting is 0, meaning it is disabled.

This option can be configured here, or in the remote station configuration.

Connection Call Warm Down Time

This value represents the number of seconds a connection call should remain connected after the regular call is disconnected. Once this timeout is expired, the connection call will be disconnected. The default value for this option is 5 seconds.

> **Note**: This option is not used for persistent connection calls.

Related topics

Overview of the default station

Multi-Server Site

The Multi-Server Site page appears if the following conditions apply:

- This station is a workstation, a stand-alone phone or a stand-alone fax
- Your release of CIC includes the Multi-Server Administration license

Use this page to select the multi-server site settings.

Home Site

Select the **Home Site** using the ... button which allows the selection of site IDs as defined by the peer sites.

Current Site

This is the **Current Site** for this station, and is read-only.

Muti-Server Home Site Allocation option

Also available from the right-click menu in the stations container, is the **Multi-Server Home Site Allocation** option. Select this option to open the Site Allocation dialog box and apply random site IDs or specific site IDs to stations. The site ID(s) can be applied to all selected stations, all stations, or all stations without an existing site ID.

> **Note**: Site IDs can be applied to Workstation, Stand-alone Phone, or Stand-alone Fax station types only.

Related topics

Overview of the default station

Station Licensing

Station licensing settings

Use this page to assign licenses to the station or station template. This page applies to Workstations or Remote Stations.

> **Note:** If you enabled the Enhanced Interaction Administrator Change log, then changes to station licenses are tracked in that log. For more information, see *About the Enhanced Interaction Administrator Change Log*.

Licensed Machine Name

You can associate a station with a specific machine. Typically the **Licensed Machine Name** is the station name, but you can select the check box to override this setting. Click **...** to select the machine name.

The machine name cannot be a duplicate of an already **Licensed Machine Name**. This is a required field used for licensing only, and it cannot be blank.

When you log in to ICBM, use the machine name that is associated with the station. You will not be logged off the client to which you are currently logged on.

If a module requires station audio, the module will check to see if there is a logged in station that supports audio. If there is not a station that supports audio, the audio functionality will be disabled.

Basic Station License

This license represents an audio path between CIC and a station. This license is not required, but without it the audio for station will not play, and there will be no dial tone. A non-audio station may be used or for non-audio interactions.

Remote Stations must be assigned a Basic Station license.

Client Access License

Assigning this license to the station allows the client functionality of the CIC clients. Without this license assignment, no CIC client will not run on this station.

ACD Access License

Select this check box if this workstation is an ACD station, then select the type of ACD license. These are the available types of ACD licenses:

- Media 1 - This license allows 1 interaction type at a given time.
- Media 2 - This license allows 2 interaction types at a given time.
- Media 3 Plus - This license allows 3 or more interaction types at a given time.

If **Media 1** or **Media 2** type of ACD licenses is selected, you can click **Interaction Types** and select the type of interaction from the list to apply to the license. **Interaction Types** is grayed-out and not available if **Media 3 Plus** is selected.

> **Notes:** Failure to have a ACD Access License assigned to the station will prevent that station from being ACD active.
>
> If the station (Station A) is assigned a Basic Station license and two different users (User A and User B) each have all other necessary rights (i.e., Client Access) assigned to them, then both users can simultaneously login to that station, (User A and User B can both be logged into Station A at the same time). If the second user to login does not have the necessary licenses assigned, then the second user login will fail.

Interaction Process Automation License

Select the **Interaction Process Automation** check box if this station is an Interaction Process Automation station, and then select the type of license to assign to that station.

These are the available types of Interaction Process Automation licenses:

- **Direct Routed Work Items** (I3_ACCESS_IPA_USER) license: Enables you to launch any process to which you have rights. It also enables you to receive Work Items that are directly routed to you.
- **Group Routed Work Items** (I3_ACCESS_IPA_USER_ACD) license: Enables you to receive Work Items that are either routed to you directly or as a member of a workgroup (similar to an ACD queue).

> **Note**: The Group Routed Work Items license includes the Direct Routed Work Items license.
>
> For more information about designing processes, refer to the *Interaction Process Automation Technical Reference* and the Process Designer online help.

License List

This list displays additional licenses that are available. Select the licenses you wish to assign to this station.

Enable Licenses

Select this check box to set the license settings to Active. If unchecked, the licenses settings on this page are ignored by the system. This is a way to turn off licensing for a station, but keep the license settings.

Click OK to save your changes. These license assignments are immediately reflected in the license counts in the Licenses Allocation container list.

> **Note:** For specific license information on each type of license, see the *PureConnect Licensing Overview Technical Reference* in the PureConnect Documentation Library.

Related topics

Overview of the default station

About Remote Stations

Licensing

Other Station Licenses

Licenses for stand-alone fax and stand-alone phone stations

> **Note:** If you enabled the Enhanced Interaction Administrator Change log, then changes to station licenses are tracked in that log. For more information, see *About the Enhanced Interaction Administrator Change Log*.

Use this page to assign licenses to the station or station template. This page applies to Stand-alone Fax and Stand-alone Phone station types.

Basic Station License

This license represents an audio path between CIC and a station. This license is not required, but without it the audio for station will not play. A non-audio station may be used or for non-audio interactions.

A Standalone Fax and Standalone Phone should always be assigned a Basic Station License. A Bus Device Fax station does not use a Basic Station License.

> **Note**: If the station (Station A) is assigned a Basic Station license and two different users (User A and User B) each have all other necessary rights (i.e., Client Access) assigned to them, then both users can simultaneously login to that station,   (User A and User B can both be logged into Station A at the same time). If the second user to login does not have the necessary licenses assigned, then the second user login will fail.

Recorder Access License

Assign this license to enable the ability to record on this station.

Enable Licenses

Select this check box to set the license settings to Active. If unchecked, the licenses settings on this page are ignored by the system. This is a way to turn off licensing for a station, but keep the license settings.

Click OK to save your changes. These license assignments are immediately reflected in the license counts in the Licenses Allocation container list.

> **Note:** For specific license information on each type of license, see the *PureConnect Licensing Technical Reference* in the PureConnect Documentation Library.

Related topics

Overview of the default station

Station access control settings

Station Access Control enables you to specify the outbound dialing privileges for a station, if any.

Select one or more classification names from the list of Available classifications and add them to the Currently Selected list to give the selected dialing privileges to this station. If someone attempts to place a call from this station and the dialed phone number is not supported in one of the phone number classifications for this station, CIC plays a prompt saying that the station does not have sufficient dialing privileges to place the call.

To give this station all dialing privileges, automatically including new classifications added in the future, select the **[All*]** entry, and then click **Add.**

> To prevent a CIC station (such as a stand-alone phone) from having any dialing privileges, leave the Currently Selected list of classifications blank. If someone attempts to place a call from a disabled station, CIC plays a prompt saying that the station does not have sufficient dialing privileges to place the call.

Phone number classifications are defined in the Classifications page and used in the Dial Plan page in the Phone Numbers container.

Related topics

Overview of the default station

Station options settings

Use this page to set station options.

Timeout for Incoming Interactions

This setting determines the number of seconds an incoming interaction rings at the CIC client station before the interaction quits alerting and proceeds to the next step in the handler (for example, goes to voicemail or changes an ACD agent's status to ACD-Agent not answering and offers the interaction to another agent). The default value is 15 seconds; entering 0 (zero) also means 15 seconds. The minimum value is 7 seconds, which allows at least one full ring cycle. For North America, the standard ring duration for one ring is six seconds, which includes two seconds of ring and four seconds of pause time.

Use IC Follow Me *(applies only to Exchange - Unified Messaging users)*

Select this option to rely on the CIC server instead of the UM platform to perform this function.

Require Forced Authorization Code

Select **Require Forced Authorization Code** to require users to enter an extension and a password for certain phone classifications assigned to this station. The phone classifications have been previously set up by the server parameter "Toll Call Classifications." This setting does not apply to UM station types.

Station has MWI message light (*this option is not available on a managed workstation*)

Select **Station has MWI message light** so the system will turn on the message light (on Caller ID and ADSI telephones) whenever a caller leaves a voice message. When the message is picked up, the light is automatically turned off.

> **Note:** To fully enable the MWI feature, you must activate MWI at the default station level, the station level, and the user level.

Outbound ANI

Enter the ANI/Caller ID for the system to send when making an outbound call from this station.

> **Notes**: If a user is logged into the station and makes a call, the user's configuration for the Outbound ANI overrides this setting.
>
> This Outbound ANI option does not override a call placed with a specific Calling Party Number and Calling Party Name. Call Forwarding and Follow-me numbers placed as outbound calls use the Forwarded Parties ANI and Name where allowed.

Related topics

Overview of the default station

Activate MWI for the default station

Activate MWI for a user

User's configuration for the Outbound ANI

Station call forwarding options

You can configure this station to forward calls if it is busy or there is no answer.

Forward calls to this extension

Type the extension to forward calls to in the box.

When this station has an active call, forward these calls:

Select this box to forward calls when the station is in use. To select which calls to forward when the line is busy, click the drop-down arrow and:

Select	To
Internal	Forward all internal calls.
External	Forward all external calls.
Unknown	Forward all calls that cannot be determined if they are internal or external.
All	Forward internal and external calls.

When calls go unanswered, forward these calls:

Select this box to forward calls that are not answered. To select which calls to forward when the phone rings and there is no answer, click the drop-down arrow and:

Select	To
Internal	Forward all internal calls.

External	Forward all external calls.
Unknown	Forward all calls that cannot be determined if they are internal or external.
All	Forward internal and external calls.

> **Note:** You can also configure Client templates to enable additional Call Forwarding and Follow Me features. For more information on client templates, see *Call Coverage* and *Follow Me*.

Related topics

Overview of the default station

Call Coverage

Follow Me

Station emergency information settings

Use this page to set station location options that are used in the event of an emergency.

Description

Enter the description of the location of this station. This description is displayed in station group directories in the CIC clients. For example, a description might be "Conference Room 1."

Emergency Access

Use this section to enter emergency access information for this station for emergency support.

Calling Party Number

Enter the outbound ANI (10 digit numeric) to use for emergency calls from this station. The Automatic Location Identification (ALI) record field is CPN and in "emergency" terminology it is Emergency Location Identification Number (ELIN).

Location

Enter the location information (60 digit alpha-numeric) for emergency personnel dispatched (i.e., Building 1, floor 3, north wing, office #26, next to elevator). The ALI record field is LOC.

Customer Name

Enter the name (32 character alpha-numeric) to provide for this station (i.e., John Smith). The ALI record field is NAM.

Related topics

Overview of the default station

Emergency classification

Managed IP Phones

Managed IP phones

CIC systems using SIP can reduce initial IP phone configuration time and ongoing maintenance with managed IP phones. A provisioning subsystem manages the configuration of all IP phones in Interaction Administrator.

Related topics

Managed IP phone template concepts

Add a managed IP phone or template

Configure managed IP phones or templates

Registration Group Configuration

Ring Sets

Default IP Phone

Add a managed IP phone or template

To add a managed IP phone or template

1. In the ***<IC_Server>*** container, do one of the following:
    - To add a managed IP phone, double-click the **Managed IP Phones** container.
    - To add a managed IP phone template, double-click the **Templates** container.
2. In the list view window, right-click and then click **New**.
3. In the **Name** box, type a unique name. To create a managed IP phone template that is based on an existing workstation, click **Browse.**
4. If you are adding a managed IP phone and want to use a template, from the **Template** list, select the template. For more information on templates, see *Managed IP phone template concepts.*
5. In the **Type** list, select the appropriate type for the phone.
6. In the **Manufacturer** list, select the manufacturer.
7. In the **Model** list, select the model of the phone.
8. The **Access Control Group** field appears if one or more access control groups have been added in the **Access Control Groups** subcontainer, which is found in the **People** container.

9. To associate this IP managed phone with an access control group, click **...** and then select the access control group.
10. Click **OK**.
    The **Managed IP Phone Configuration** dialog box appears.
11. Use the tabs in this dialog box to configure the managed IP phone or managed IP template. For complete information on the configuration settings, use the links under **Related topics**.

Related topics

Overview of configuration settings for managed IP phones and templates

Managed IP phone template concepts

Select access control group

Right-Click Menu Commands

Change multiple IP phones

Change Multiple IP Phones allows you to edit multiple IP phones at one time. To access this feature, select two or more IP phones in the Managed IP Phones container, right-click and select the **Change Multiple IP Phones …** from the context menu.

You can change settings in the **General**, **Option Values**, and **Advanced Options** tabs.

> **Note**: The Advanced Options tab appears only if one of the selected IP phones has advanced settings.

To change a setting, click on the pull-down menu and select the desired option. If you do not change a value, a grayed-out “Leave unchanged” message is displayed. Optionally, you can right-click on a row and select "Reset" to removed any changes already made. After clicking **OK**, any changes made are saved and applied to all selected (or highlighted) IP phones. A progress dialog box appears while CIC updates the phones.

You can cancel the application of the new values, but IP phones that have already been modified do not revert to the initial settings. If any errors occur during the process, they are listed on the **Errors** tab on the progress dialog box.

Configure managed IP phones

Overview of configuration settings for managed IP phones and templates

This topic contains links to the configuration settings that are available for managed IP phones and templates.

AudioCodes phones

General settings

Options

Advanced options

Information

Interaction SIP stations

General settings

Options

Advanced options

Information

Polycom phones

General settings

Options

Advanced options

Information

Related topics

Add a managed IP phone or template

Configure managed IP phones or templates

To configure a managed IP phone or template

1. In the ***<IC_Server>*** container, do one of the following:
    - To configure a managed IP phone, double-click the **Managed IP Phones** container.
    - To configure a managed IP phone template, double-click the **Templates** container.
2. In the list view window, click the item that you want to configure.
3. Use the tabs in this dialog box to configure the managed IP phone or managed IP template. For complete information on the configuration settings, use the links under **Related topics**.

Related topics

AudioCodes phones

General settings

Options

Advanced options

Information

Interaction SIP stations

General settings

Options

Advanced options

Information

Polycom phones

General settings

Options

Advanced options

Information

Related topics

Add a managed IP phone or template

AudioCodes phones

AudioCodes settings

General settings

Options

Advanced options

SIP settings

Information

General settings: AudioCodes phones or templates

The following table describes the general settings for AudioCodes phones and templates. For information on how to access these settings, see *Configure managed IP phones or templates*.

Setting	Description	Default
Name	The name of this IP phone must be unique. Click **Browse** to locate an existing station.	Specified when the phone is added
Active	Inactive phones do not receive calls.	Active
MAC Address	The MAC address must be in the format xx:xx:xx:xx:xx:xx. AudioCodes addresses start with 00:90:8f. **Note**: Changing the MAC address will reload a previously registered managed IP phone.	
Registration Group	The default options are: • **Default Registration Group** • **Default Secure Registration Group** You can create other registration groups in the **Registration Groups** container.	Default Registration Group
Location	All station appearances are in this same location. Time zone information is read from the location and used to set the phone time, DST settings, and so on. **Note**: If the Enable Regional Dialing option is selected, and a change to this location creates an extension conflict of a managed IP phone, a message is displayed listing duplicate extensions. For later reference when resolving conflicts, click **Copy to Clipboard** to copy the listing, and then paste the content to a program that supports CSV (like Microsoft Excel).	Default Location

Preferred Language	This option is available only if multiple languages are installed. Select the language for all prompts for this managed IP phone. The available options depend on the installed languages.	System Default
Use Location Time Zone	Determines whether the time zone of the associated location is used to set the date/time. **Note:** You can also configure the time zone on the DHCP server. If you configure the time zone both on the DHCP server and in Interaction Administrator, then the time zone on the DHCP server is used.	Selected
Firmware Version	The available firmware options are listed.	
Audio Protocol	The audio stream on this IP phone can be unencrypted using RTP (Real Time Protocol) or encrypted using Secure RTP (SRTP). • To use SRTP, you must choose TLS as the Transport Protocol. • Choose SRTP only if the endpoint(s) on this line support SRTP. • If you select SRTP, it enables the Security option (below). Calls between devices transmitting and receiving SIP TLS messages and SRTP audio are completely secure.	
Time Zone	The time zones listed are the same as Windows time zones. The managed IP phone will use this time	(UTC-05:00) Eastern Time (US & Canada)

	zone to set the daylight saving time information. **Note:** You can also configure the time zone on the DHCP server. If you configure the time zone both on the DHCP server and in Interaction Administrator, then the time zone on the DHCP server is used.	
Station Appearances	This is a regular station appearance. It is the default appearance of this managed IP phone. AudioCode phones do not support shared line appearances. After you add, edit, or remove station appearances, you must reload the phone.	Not specified

Related topics

Configure managed IP phones or templates

Add Registration

Registration Group

SIP Bridge

SIP Bridges Configuration

Location

Enable Regional Dialing option

Managed IP phone appearance configuration

Options: AudioCodes phones or templates

The following tables describe the options for AudioCodes phones or templates. For information on how to access these settings, see *Configure managed IP phones or templates*.

General

Option	Description	Default
Ring Always	When this setting is enabled, the phone will always ring when the user receives a call, even if a CIC client is not running.	
Inband Call Waiting Tone	When this setting is enabled, the phone will emit a tone on an incoming call when another call is active	
SIP Receive Port	This is the port that the IP phone uses to send and receive SIP signaling packets. **Note:** The Interaction SIP Station and the SIP Soft Phone use this setting regardless of the protocol type.	5060
Media Port Start Range	Use this setting for Polycom and Interaction SIP Station phones that need to use a different port range than the default ports for audio traffic. Set this to a valid port number that begins the new range of ports to use for audio. Reasons to use this include phones that are behind a firewall, or that use port forwarding, or that have another reason to specify a different port range. If Interaction SIP Stations use both RTP and RTCP for the audio stream, a new port number specified in the **Media Port Start Range** (e.g., 6400) will apply to RTP audio, and RTCP audio will automatically use one port number higher (e.g., 6401). The default port number of 4000/4001 on Interaction SIP Stations works well for most situations.	Depends on the device manufacturer
LAN Port Mode	This is the network speed over the Ethernet for the IP phone through the LAN port.	Automatic

	Acceptable values are: - 10 Mbps Full-duplex - 10 Mbps Half-duplex - 100 Mbps Full-duplex - 100 Mbps Half-duplex	
PC Port Mode	This is the network speed over the Ethernet for the IP phone through the PC port. Acceptable values are: - 10 Mbps Full-duplex - 10 Mbps Half-duplex - 100 Mbps Full-duplex - 100 Mbps Half-duplex	Automatic

Interface

Option	Description	Default
Ring Volume (0-9)	This value sets the ring volume heard in the agent’s headset. When the phone configuration is reloaded or the device is rebooted (e.g., the network cable is unplugged and reconnected), the phone resets ring volume to this default value.	5

Emergency Information

Option	Description	Default
Description	The description of the location of this IP phone. This description is displayed in station group directories in the CIC clients. For example, a description might be	Not specified

	"Conference Room 1".	
Location	The location information (60 digit alpha-numeric) that is provided to dispatched emergency personnel (for example, Building 1, floor 3, north wing, office #26, next to elevator). The ALI record field is LOC.	Not specified
Calling Party Number	The outbound ANI (10 digit numeric) to use for emergency calls from this IP phone. The Automatic Location Identification (ALI) record field is CPN and in "emergency" terminology it is Emergency Location Identification Number (ELIN).	Not specified
Customer Name	The name (32 character alpha-numeric) to provide for this IP phone (i.e., John Smith). The ALI record field is NAM.	Not specified

Related topics

Configure managed IP phones or templates

Advanced options: AudioCodes phones or templates

The following tables describe the advanced options for AudioCodes phones or templates. For information on how to access these settings, see *Configure managed IP phones or templates*.

> **Note:** These options are used only for diagnostic and troubleshooting purposes. Do not change them without clear direction from a PureConnect Customer Care representative.

Provisioning

Option	Description	Default
Provisioning Method	This setting supports several methods for determining the provisioning server to which the IP phone should connect. The options are **DHCP Options**, **Disabled**, **Static**	**DHCP Options**

	URL. Depending on which method is selected, the **DHCP Option** or the **Static URL** may be required below.	
DHCP Option	This setting specifies the Dynamic Host Configuration Protocol (DHCP) option number that identifies the vendor and functionality of a DHCP client. **Note:** For AudioCodes, instead of setting this option, set the **DHCP Option Records 002** in the network configuration. For more information, see *CIC Managed IP Phones Administrator's Guide* in the **Technical Reference Documents** section of the PureConnect Documentation Library.	160
Static URL	This setting specifies the CIC server by entering the host name or IP address. All IP addresses in managed phones configuration are pass-through strings to support IPv6. **Note**: If **Provisioning Method** is set to **Disabled**, the AudioCodes phone does not attempt to connect with the provisioning server. Therefore configuration of firmware is not requested, so that configuration information requires updates through the web interface.	blank or <empty>
Enable Configuration Web Page	This setting determines whether the phone's configuration web page appears on the AudioCodes phones. By default, this configuration page is visible to users.	On

Syslog Tracing

The following are all of the Syslog tracing options for AudioCode phones. The available options depend on the model.

Option	Description	Default
Syslog Enabled	This setting enables or disables diagnostic logs for Interaction SIP Stations in the form of Syslog messages. Setting this to **Yes** requires a Syslog Server to be specified. Use this only at the direction of authorized PureConnect Customer Care representatives.	No
Syslog Server	This setting specifies the IP address of a third party Syslog server used to capture diagnostic logs and error messages generated by the Interaction SIP Station. A valid Syslog server IP address is required if **Syslog Enabled** is set to **Yes**. All IP addresses in managed phones configuration are pass-through strings to support IPv6 in a future release.	The default IP address is 0.0.0.0, which is invalid until set to a valid address.
Server Port	This setting defines the UDP port of the Syslog Server. The valid range is from 0 to 65,535.	514
Voip Application	This setting specifies the level at which Syslog messages are generated related to VoIP. Select from the following list: None Emergency Error Warning Notice Info Deb	None
Control Center	This setting specifies the level at which Syslog messages are generated related to Networking	None
LCD Display	This setting specifies the level at which Syslog messages are generated related to	None

	LCD Display and other keypresses.	
Web	This setting specifies the level at which Syslog messages are generated related to phone web server.	None
Watchdog	This setting specifies the level at which Syslog messages are generated related to the watchdog process, which keeps other processes running.	None
802.1x	This setting specifies the level at which Syslog messages are generated related to the security protocol.	None
Kernel	This setting specifies the level at which Syslog messages are generated related to the kernel process of the phone.	None
DSP	This setting specifies the level at which Syslog messages are generated related to the voice engine of the phone.	None

Gain

The microphone settings adjust the volume for the benefit of the caller and the speaker settings adjust the volume for the benefit of the agent. We recommend you talk to authorized PureConnect Customer Care engineers if you have problems with audio volume.

Digital settings adjust volume to the line while the analog settings adjust volume to headset. Select the intended value from the drop-down list.

Option	Description	Default
NB Headset Digital Microphone Gain)	This setting controls the gain of the RTP audio stream sent from the AudioCodes phone to the line (narrow band).	+0 dB
NB Headset Digital Speaker Gain	This setting controls the gain of the RTP audio stream from the line through the AudioCodes phone and to the headset (narrow band).	+4 dB

WB Headset Digital Microphone Gain	This setting controls the gain of the RTP audio stream sent from the AudioCodes phone to the line (wide band).	+0 dB
WB Headset Digital Speaker Gain	This setting controls the gain of the RTP audio stream from the line through the AudioCodes phone and to the headset (wide band).	-4dB

VLAN

Option	Description	Default
VLAN Discovery Mode	This setting specifies the method that this AudioCodes phone uses to find its Virtual Local Area Network (VLAN). This setting controls the use of VLAN tagging (802.1Q) for audio streams over a VLAN: • Automatic (CDP+LLDP) – This (default) option uses CDP (Cisco Discovery Protocol) together with LLDP (Link Layer Discovery Protocol) to automatically obtain the VLAN ID assignment. This option allows for discovery using whichever mode is active, and to use VLANs on different switches without changing configuration of the phone. • Automatic (CDP) - This option uses CDP (Cisco Discovery Protocol) to automatically obtain the VLAN ID assignment. Use this option to strictly limit VLAN discovery to Cisco switches. • Automatic (LLDP) - This option uses LLDP (Link Layer Discovery Protocol) to automatically obtain the VLAN ID assignment. Use this option to strictly limit VLAN	

	discovery to non-Cisco switches. - Disabled – This option disables the use of VLANs which stops VLAN tagging for this AudioCodes phone. If you do not have the standard Voice/Data VLAN set up in your network, using this option skips the VLAN discovery mode which causes the IP phone to start-up faster on a reboot. - Manual – This option requires you to specify a VLAN ID in the Manual VLAN ID field. This option allows the IP phone to generate traffic on the specified VLAN without having either CDP or LLDP protocols enabled on the network.	
Manual VLAN ID	If the **VLAN Discovery Mode** field is set to "Manual", you can specify the VLAN ID for this AudioCodes phone in this field by entering the value it will use. Valid values are 1 through 4094. **Note**: **Important information regarding Manual VLAN ID** If you configure an AudioCodes phone to a **Manual VLAN ID**, the phone will not listen to packets that come into its network port unless the appropriate 802.1q tagging is set in the header. Some network switches have been observed to strip away this header before sending the packets to the ISS in the field. If this occurs, and **Manual VLAN ID** is set on the device, the device will no longer hear any traffic and cannot be accessed. If this occurs, there are only two ways to recover the device: 1.The switch must be changed to not strip the 802.1q header. The simplest way to do this is to configure the switch port as a trunk port. The method for performing this is dependent on your type of switch.	

	2.The device must be reset to factory defaults to reset/clear the **Manual VLAN ID** value. This however is only possible if the phone is already running on the 2.0.0.18 version of firmware.	

LAN

Option	Description	Default
IP Assignment Mode	This setting specifies the method that this AudioCodes phone uses to obtain an IP address: • Automatic (DHCP) – (Default) All network IP settings are provided by the Dynamic Host Control Protocol (DHCP) server in your network. • Static – All network IP settings are specified manually through the remaining fields in the LAN section.	
IP Address	This setting specifies the IP address that this AudioCodes phone will use when it starts. This field is used only if the IP Assignment Mode field is set to Static. All IP addresses in managed phones configuration are pass-through strings to support IPv6.	
Subnet Mask	This setting specifies the appropriate subnet mask for your IP telephony network. The IP address for this AudioCodes phone must fall within the range specified by the subnet mask. All IP addresses in managed phones configuration are pass-through strings to support IPv6.	
Default	This setting specifies the IP address for the network device that controls the routing of	

Gateway	IP packets. This field is used only if the IP Assignment Mode field is set to Static. All IP addresses in managed phones configuration are pass-through strings to support IPv6.	
Primary DNS	This setting specifies the IP address of the primary Domain Name Server (DNS). Do not enter a URL in this field. This field is used only if the IP Assignment Mode field is set to Static. All IP addresses in managed phones configuration are pass-through strings to support IPv6.	
Secondary DNS	This setting specifies the IP address of the secondary DNS. Do not enter a URL in this field. This field is used only if the IP Assignment Mode field is set to Static. All IP addresses in managed phones configuration are pass-through strings to support IPv6. **Note**: The fields for the IP network settings do not reflect the settings that are assigned by the DHCP server to the AudioCodes phone.	

Audio Quality Diagnostics

These settings are designed to help diagnose audio quality problems by capturing recorded audio packets using a network sniffer utility (for example Wireshark) and analyzing the network traffic and audio packets. Change these settings only at the direction of authorized PureConnect Customer Care technical support representatives. Setting these values incorrectly can cause additional audio problems.

Option	Description	Default
Packet Recording Enabled	This option activates the packet recording mechanism.	No
Packet Recording Remote IP Address	This setting specifies the IP address of the remote computer to capture the recorded packets. The recorded packets should be captured by a network sniffer application. The default IP address is **0.0.0.0**. All IP	

	addresses in managed phones configuration are pass-through strings to support IPv6.	
Packet Recording Remote Port	This setting specifies the UDP port on the computer specified in **Packet Recording Remote IP Address**.	5000
RTP Recording Enabled	This option activates the DSP RTP recording.	No
Network Recording (To User) Enabled	This option activates the DSP network recording of outgoing audio traffic.	No
TDM Recording (From User) Enabled	This option activates the DSP TDM recording of incoming audio traffic.	No
Echo Canceller Debug Recording Enabled	This option activates the recording of the echo cancellation activity to debug associated echo problems.	No

Registration

Option	Description	Default
Allow Manual Redundant Proxy Symmetric	CIC sets the redundant_proxy_is_symmetric parameter to true only when proxy type is configured as Line. In some scenarios, this is problematic and as a result the phone cannot be registered. Set this option to **Yes** to allow CIC to set the redundant_proxy_is_symmetric parameter as true if the first and second registration types are manual. For more information about the use of this option, see the *Interaction SIP Proxy Technical Reference*.	No

Related topics

Configure managed IP phones or templates

Support Site special notices

SIP settings overview: AudioCodes phones or templates

SIP settings are organized into categories, as shown under **Related topics**.

For information on how to access the SIP settings, see *Configure advanced options for managed IP phones or templates*.

Related topics

SIP audio settings

SIP transport settings

SIP session settings

SIP authentication settings

Configure advanced options for managed IP phones or templates

Information: AudioCodes phones or templates

The following table describes the information that is shown for AudioCodes phones or templates. This information is automatically updated when the IP phone, or an IP phone that uses the template, is registered.

For information on how to access these settings, see *Configure managed IP phones or templates*.

Detail	Description
Phone	This is the manufacturer and model of the IP phone device.
Type	This is the type of station (workstation or stand-alone phone.

IP Address	This is the IP address of the device. N/A indicates the device is not registered.
Contact Line	This is the SIP line used when the phone registered with the CIC server. This line will be used to send SIP signaling to the phone.
Last Reload	This is the date and time when the phone requested configuration update or the phone was reloaded after a configuration change.
Status	This is the status of the phone from the CIC server perspective (i.e., Not registered, Up-to-date, Reloading, Reload required.
Max. Line Keys	This is the maximum number of line keys associated with this device. An AudioCodes phone has 1 line key.
Max. Appearances	This is the maximum number of shared line appearances for this device. An AudioCodes phone has 1 appearance.
Notes	These are any comments CIC administrators add about this device or the associated template.

Related topics

Configure managed IP phones or templates

Interaction SIP stations

Interaction SIP stations settings

General settings

Options

Advanced options

SIP settings

Information

General settings: Interaction SIP stations or templates

The following table describes the general settings for Interaction SIP stations or templates. For information on how to access these settings, see *Configure managed IP phones or templates.*

Setting	Description	Default
Name	The name of this IP phone must be unique. Click **Browse** to locate an existing station.	Specified when the phone is added
Active	Inactive phones do not receive calls.	Active
MAC Address	The MAC address must be in the format xx:xx:xx:xx:xx:xx. Interaction SIP station MAC addresses start with 00:26:fd. **Note**: Changing the MAC address will reload a previously registered managed IP phone.	
Full Computer Name	The correct full computer name is listed on the SIP soft phone user's computer. Navigate to My Computer --> Properties --> Computer Name and note the **Full Computer Name**. For example: PattyJ.acme.com or... PattyJ This option is available for SIP soft phones only. **Notes**: Changing the Full Computer	

	Name will reload a previously registered managed IP phone. When you add a SIP Soft Phone, CIC automatically trims extra whitespace from the beginning and the end of the Full Computer Name.	
Registration Group	The default options are: • **Default Registration Group** • Default Secure Registration Group You can create other registration groups in the **Registration Groups** container.	Default Registration Group
Location	All station appearances are in this same location. Time zone information is read from the location and used to set the phone time, DST settings, and so on. **Note**: If the Enable Regional Dialing option is selected, and a change to this location creates an extension conflict of a managed IP phone, a message is displayed listing duplicate extensions. For later reference when resolving conflicts, click **Copy to Clipboard** to copy the listing, and then paste the content to a program that supports CSV (like Microsoft Excel).	Default Location
Preferred Language	This option is available only if multiple languages are installed. Select the language for all prompts for this managed IP phone. The available options depend on the installed languages.	System Default
Audio Protocol	The audio stream on this IP phone can be unencrypted using RTP (Real Time Protocol) or encrypted using Secure RTP (SRTP). • To use SRTP, you must choose TLS	RTP

	as the Transport Protocol • Choose SRTP only if the endpoint(s) on this line support SRTP. • If you select SRTP, it enables the **Security** option (below). Calls between devices transmitting and receiving SIP TLS messages and SRTP audio are completely secure. **Note**: Interaction SIP Station phone models IP300, IP301, IP500, IP501, IP600, and IP601 do not support this audio protocol option, therefore this field is not displayed for these models.	
Use Location Time Zone	Determines whether the time zone of the associated location is used to set the date/time. **Note:** You can also configure the time zone on the DHCP server. If you configure the time zone both on the DHCP server and in Interaction Administrator, then the time zone on the DHCP server is used.	Selected
Firmware Version	The available firmware options are listed.	
Time Zone	The time zones listed are the same as Windows time zones. The managed IP phone will use this time zone to set the daylight saving time information. **Note:** You can also configure the time zone on the DHCP server. If you configure the time zone both on the DHCP server and in Interaction	(UTC-05:00) Eastern Time (US & Canada)

	Administrator, then the time zone on the DHCP server is used. *The SIP Soft Phone does not support this time zone option.*	
Station Appearances	There are three types of station appearances (or an existing station may be selected). Not all types of appearances apply to all phones: • **Station Appearance** - This is a regular station appearance. For example, ManagedIPPhone105 has a regular station appearance by default labeled ManagedIPPhone105 on this station. (The label can be edited.) Interaction SIP Station uses only one station appearance. • **Shared Station Appearance** - This is an appearance that is assigned to another SIP station. If the key that is associated with this appearance is pressed, an incoming call can be picked up from the other SIP station. **Note**: This option does not apply to Interaction SIP Station or a managed IP phone using a SIP bridge. • **External Registration** - The IP phone obtains its registration outside the IC server or the managed proxy system. For example, one station appearance for the IP phone connects to the IC server, and another appearance connects to an outside SIP server. **Note**: This option does not apply to a managed IP phone using a SIP bridge.	Not specified

	After you add, edit, or remove station appearances, you must reload the phone.	

Related topics

Configure managed IP phones or templates

Support Site special notices

Add Registration

Registration Group

SIP Bridge

SIP Bridges Configuration

Location

Enable Regional Dialing option

Managed IP phone appearance configuration

Options: Interaction SIP stations or templates

The following tables describe the options for Interaction SIP stations or templates. For information on how to access these settings, see *Configure managed IP phones or templates***.**

General

Option	Description	Default
Ring Always	When this setting is enabled, the phone will always ring when the user receives a call, even if a CIC client is not running.	Not selected
Inband Call Waiting Tone	When this setting is enabled, the phone will emit a tone on an incoming call when another call is active	Not selected
SIP Receive Port	This is the port that the IP phone uses to send and receive SIP signaling packets using the TCP and UDP transport protocols.	5060
SIP TLS Receive Port	This is the port that the IP phone uses to send and receive SIP signaling packets using the TLS transport protocol.	5061
Media Port	Use this setting for Polycom and Interaction SIP Station phones that need to	Depends on the device

Start Range	use a different port range than the default ports for audio traffic. Set this to a valid port number that begins the new range of ports to use for audio. Reasons to use this include phones that are behind a firewall, or that use port forwarding, or that have another reason to specify a different port range. If Interaction SIP Stations use both RTP and RTCP for the audio stream, a new port number specified in the **Media Port Start Range** (e.g., 6400) will apply to RTP audio, and RTCP audio will automatically use one port number higher (e.g., 6401). The default port number of 4000/4001 on Interaction SIP Stations works well for most situations.	manufacturer
LAN Port Mode	This is the network speed over the Ethernet for the IP phone through the LAN port. Acceptable values are: • 1 Gbps Full-duplex • 10 Mbps Full-duplex • 10 Mbps Half-duplex • 100 Mbps Full-duplex • 100 Mbps Half-duplex	Automatic
PC Port Mode	This is the network speed over the Ethernet for the IP phone through the PC port. Acceptable values are: • 1 Gbps Full-duplex • 10 Mbps Full-duplex • 10 Mbps Half-duplex	Automatic

	- 100 Mbps Full-duplex - 100 Mbps Half-duplex	
Ringing Tone Name	This option allows you to select a custom ring tone for SIP100, SIP200, and 420HD phones. The ININDefault.wav file contains the ring tone that is included with CIC. You can replace this file with your custom ring tone provided that it meets these requirements: - The ring tone file must be a WAV file (A/Mu-Law, 8-kHz audio sample rate and 8-bit audio sample size or PMC 16-kHz audio sample rate and 16-bit audio sample size, Intel PCM encoding. - You must name your ring tone file **ININDefault.wav**. - You must place your ringtone file in \i3\ic\resources on the CIC server.	ININDefault.wav

Interface

Option	Description	Default
Ring Volume (0-9)	This value sets the ring volume heard in the agent's headset. When the phone configuration is reloaded or the device is rebooted (e.g., the network cable is unplugged and reconnected), the phone resets ring volume to this default value.	5

Emergency Information

Option	Description	Default
Description	The description of the location of this IP phone. This description is displayed in station group directories in the CIC clients.	Not specified

	For example, a description might be "Conference Room 1".	
Location	The location information (60 digit alpha-numeric) that is provided to dispatched emergency personnel (for example, Building 1, floor 3, north wing, office #26, next to elevator). The ALI record field is LOC.	Not specified
Calling Party Number	The outbound ANI (10 digit numeric) to use for emergency calls from this IP phone. The Automatic Location Identification (ALI) record field is CPN and in "emergency" terminology it is Emergency Location Identification Number (ELIN).	Not specified
Customer Name	The name (32 character alpha-numeric) to provide for this IP phone (i.e., John Smith). The ALI record field is NAM.	Not specified

Related topics

Configure managed IP phones or templates

Advanced options: Interaction SIP stations or templates

The following tables describe the advanced options for Interaction SIP Station phones or templates. For information on how to access these settings, see *Configure managed IP phones or templates*.

> **Note:** These options are used only for diagnostic and troubleshooting purposes. Do not change them without clear direction from a PureConnect Customer Care representative.

Provisioning

Option	Description	Default
Provisioning Method	This setting supports several methods for determining the provisioning server to which the IP phone should connect. The options are **DHCP Options**, **Disabled**, **Static URL**. Depending on which method is selected, the **DHCP Option** or the **Static**	**DHCP Options**

	URL may be required below.	
DHCP Option	This option specifies the Dynamic Host Configuration Protocol (DHCP) option number that identifies the vendor and functionality of a DHCP client.	160
Static URL	Specify the CIC server by entering the host name or IP address. All IP addresses in managed phones configuration are pass-through strings to support IPv6. **Note**: If **Provisioning Method** is set to **Disabled**, the Interaction SIP Station does not attempt to connect with the provisioning server. Therefore configuration of firmware is not requested, so that configuration information requires updates through the web interface.	blank or <empty>

Syslog Tracing

The following are all of the Syslog tracing options for Interaction SIP stations. The available options depend on the model.

Option	Description	Default
Syslog Enabled	This setting enables or disables diagnostic logs for Interaction SIP Stations in the form of Syslog messages. Setting this to **Yes** requires a Syslog Server to be specified. Use this only at the direction of an authorized PureConnect Customer Care engineer.	No
Syslog Server	This setting specifies the IP address of a third party Syslog server used to capture diagnostic logs and error messages generated by the Interaction SIP Station. A valid Syslog server IP address is required if **Syslog Enabled** is set to **Yes**. All IP addresses in managed phones configuration are pass-through strings to	The default IP address is 0.0.0.0, which is invalid until set to a valid address.

	support IPv6 in a future release.	
Server Port	This setting defines the UDP port of the Syslog Server. The valid range is from 0 to 65,535.	514
Voip Application	This setting specifies the level at which Syslog messages are generated related to VoIP. Select from the following list: None Emergency Error Warning Notice Info Deb	None
Control Center	This setting specifies the level at which Syslog messages are generated related to Networking	None
LCD Display	This setting specifies the level at which Syslog messages are generated related to LCD Display and other keypresses.	None
Web	This setting specifies the level at which Syslog messages are generated related to phone web server.	None
Watchdog	This setting specifies the level at which Syslog messages are generated related to the watchdog process, which keeps other processes running.	None
802.1x	This setting specifies the level at which Syslog messages are generated related to the security protocol.	None
Kernel	This setting specifies the level at which Syslog messages are generated related to the kernel process of the phone.	None

DSP	This setting specifies the level at which Syslog messages are generated related to the voice engine of the phone.	None

Gain

The microphone settings adjust the volume for the benefit of the caller and the speaker settings adjust the volume for the benefit of the agent. We recommend you talk to authorized PureConnect Customer Care engineers if you have problems with audio volume.

Digital settings adjust volume to the line while the analog settings adjust volume to headset. Select the intended value from the drop-down list.

Option	Description	Default
Headset Digital Microphone Gain (default +0 dB)	This setting controls the gain of the RTP audio stream sent from the Interaction SIP Station device to the line.	+0 dB
Headset Digital Speaker Gain (default +0 dB)	This setting controls the gain of the RTP audio stream from the line through the Interaction SIP Station device and to the headset.	+0 dB
Headset Analog Microphone Gain (default +39 dB)	This setting controls the audio signal gain from the analog headset microphone into the Interaction SIP Station device.	+39 dB
Headset Analog Speaker Gain (default -12 dB)	This setting controls the audio signal gain from the Interaction SIP Station device to the analog headset.	-12 dB
Headset Analog Sidetone Gain (default - 12 dB)	This setting controls the sidetone audio signal gain from the Interaction SIP Station device to the analog headset. The sidetone controls the agents ability to hear their own voice in the headset as they speak.	-12 dB

VLAN

Option	Description	Default
VLAN Discovery Mode	This setting specifies the method that this Interaction SIP Station uses to find its Virtual Local Area Network (VLAN). This setting controls the use of VLAN tagging (802.1Q) for audio streams over a VLAN: • Automatic (CDP+LLDP) – This (default) option uses CDP (Cisco Discovery Protocol) together with LLDP (Link Layer Discovery Protocol) to automatically obtain the VLAN ID assignment. This option allows for discovery using whichever mode is active, and to use VLANs on different switches without changing configuration of the phone. • Automatic (CDP) - This option uses CDP (Cisco Discovery Protocol) to automatically obtain the VLAN ID assignment. Use this option to strictly limit VLAN discovery to Cisco switches. • Automatic (LLDP) - This option uses LLDP (Link Layer Discovery Protocol) to automatically obtain the VLAN ID assignment. Use this option to strictly limit VLAN discovery to non-Cisco switches. • Disabled – This option disables the use of VLANs which stops VLAN tagging for this Interaction SIP Station. If you do not have the standard Voice/Data VLAN set up in your network, using this option skips the VLAN discovery mode which causes the IP phone to start-up faster on a reboot. • Manual – This option requires you to specify a VLAN ID in the Manual VLAN ID field. This option allows the IP phone to generate traffic on	

	the specified VLAN without having either CDP or LLDP protocols enabled on the network.	
Manual VLAN ID	If the **VLAN Discovery Mode** field is set to "Manual", you can specify the VLAN ID for this Interaction SIP Station in this field by entering the value it will use. Valid values are 1 through 4094. **Note**: **Important information regarding Manual VLAN ID** If you configure an Interaction SIP Station (ISS) to a **Manual VLAN ID**, the phone will not listen to packets that come into its network port unless the appropriate 802.1q tagging is set in the header. Some network switches have been observed to strip away this header before sending the packets to the ISS in the field. If this occurs, and **Manual VLAN ID** is set on the device, the device will no longer hear any traffic and cannot be accessed. If this occurs, there are only two ways to recover the device: 1.The switch must be changed to not strip the 802.1q header. The simplest way to do this is to configure the switch port as a trunk port. The method for performing this is dependent on your type of switch. 2.The device must be reset to factory defaults to reset/clear the **Manual VLAN ID** value. This however is only possible if the phone is already running on the 1.2.2 version of firmware. **WARNING** Because of this danger of causing the device to be inaccessible, systems running on firmware versions prior to 1.2.2 will not honor the **Manual VLAN ID** value until you set a safety server parameter. The server parameter is "**Provision ISS Manual VLAN ID**	

	Enabled" and needs to be set to "Yes" to enable it. Make sure you test one single phone to ensure your switch is not stripping the 802.1q VLAN tagging before you set any more phones! If you choose to set the VLAN ID manually on an ISS and they are on pre-1.2.2 firmware, you will have to set your network switch ports to trunk ports in the case that they are stripping the 802.1q headers. If the ISS is on post 1.2.2 firmware, you will have to either configure the network switch ports as trunk ports, or perform the factory reset sequence on the device that is added in the 1.2.2 firmware. Be sure to check the support site for special notices.	

LAN

Option	Description	Default
IP Assignment Mode	This setting specifies the method that this Interaction SIP Station uses to obtain an IP address: • Automatic (DHCP) – (Default) All network IP settings are provided by the Dynamic Host Control Protocol (DHCP) server in your network. • Static – All network IP settings are specified manually through the remaining fields in the LAN section.	
IP Address	This setting specifies the IP address that this Interaction SIP Station will use when it starts. This field is used only if the IP Assignment Mode field is set to Static. All IP addresses in managed phones configuration are pass-through strings to	

	support IPv6.	
Subnet Mask	This setting specifies the appropriate subnet mask for your IP telephony network. The IP address for this Interaction SIP Station must fall within the range specified by the subnet mask. All IP addresses in managed phones configuration are pass-through strings to support IPv6.	
Default Gateway	This setting specifies the IP address for the network device that controls the routing of IP packets. This field is used only if the IP Assignment Mode field is set to Static. All IP addresses in managed phones configuration are pass-through strings to support IPv6.	
Primary DNS	This setting specifies the IP address of the primary Domain Name Server (DNS). Do not enter a URL in this field. This field is used only if the IP Assignment Mode field is set to Static. All IP addresses in managed phones configuration are pass-through strings to support IPv6.	
Secondary DNS	This setting specifies the IP address of the secondary DNS. Do not enter a URL in this field. This field is used only if the IP Assignment Mode field is set to Static. All IP addresses in managed phones configuration are pass-through strings to support IPV6. **Note**: The fields for the IP network settings do not reflect the settings that are assigned by the DHCP server to the Interaction SIP Station.	

Audio Quality Diagnostics

These settings are designed to help diagnose audio quality problems by capturing recorded audio packets using a network sniffer utility (for example Wireshark) and analyzing the network traffic and audio packets. Change these settings only at the direction of authorized PureConnect Customer Care technical support representatives. Setting these values incorrectly can cause additional audio problems.

Option	Description	Default
Packet Recording Enabled	This setting activates the packet recording mechanism.	No
Packet Recording Remote IP Address	This setting specifies the IP address of the remote computer to capture the recorded packets. The recorded packets should be captured by a network sniffer application. The default IP address is **0.0.0.0**. All IP addresses in managed phones configuration are pass-through strings to support IPv6.	
Packet Recording Remote Port	This setting specifies the UDP port on the computer specified in **Packet Recording Remote IP Address**.	5000
RTP Recording Enabled	This setting activates the DSP RTP recording.	No
Network Recording (To User) Enabled	This setting activates the DSP network recording of outgoing audio traffic.	No
TDM Recording (From User) Enabled	This setting activates the DSP TDM recording of incoming audio traffic.	No
Echo Canceller Debug Recording Enabled	This setting activates recording of the echo cancellation activity to debug associated echo problems.	No
Port Mirroring	This setting activates port mirroring.	No
SRTP Audit Events	This setting activates auditing of SRTP events.	No
Noise Reduction Debug Recording	This setting activates noise reduction debug recording.	No

Registration

Option	Description	Default
Allow Manual Redundant Proxy Symmetric	CIC sets the redundant_proxy_is_symmetric parameter to true only when proxy type is configured as Line. In some scenarios, this is problematic and as a result the phone cannot be registered. Set this option to **Yes** to allow CIC to set the redundant_proxy_is_symmetric parameter as true if the first and second registration types are manual. For more information about the use of this option, see the *Interaction SIP Proxy Technical Reference*.	No

Related topics

Configure managed IP phones or templates

Support Site special notices

SIP settings overview: Interaction SIP stations or templates

SIP settings are organized into categories, as shown under **Related topics**.

For information on how to access the SIP settings, see *Configure advanced options for managed IP phones or templates*.

Related topics

SIP audio settings

SIP transport settings

SIP session settings

SIP authentication settings

Configure advanced options for managed IP phones or templates

Information: Interaction SIP stations or templates

The following table describes the information that is shown for Interaction SIP stations or templates. This information is automatically updated when the IP phone, or an IP phone that uses the template, is registered.

For information on how to access these settings, see *Configure managed IP phones or templates*.

Detail	Description
Phone	This is the manufacturer and model of the IP phone device.
Type	This is the type of station (workstation or stand-alone phone.
IP Address	This is the IP address of the device. N/A indicates the device is not registered.
Contact Line	This is the SIP line used when the phone registered with the CIC server. This line will be used to send SIP signaling to the phone.
Last Reload	This is the date and time when the phone requested configuration update or the phone was reloaded after a configuration change.
Status	This is the status of the phone from the CIC server perspective (i.e., Not registered, Up-to-date, Reloading, Reload required.
Max. Line Keys	This is the maximum number of line keys associated with this device. Interaction SIP Station and SIP Soft Phone both have 1 line key.
Max. Appearances	This is the maximum number of shared line appearances for this device. Interaction SIP Station and SIP Soft Phone both have 1

	appearance.
Notes	These are any comments CIC administrators add about this device or the associated template.

Related topics

Configure managed IP phones or templates

Polycom phones

Polycom phone settings

General settings

Options

Advanced options

SIP settings

Information

General settings: Polycom phones or templates

The following table describes the general settings for Polycom phones or templates. For information on how to access these settings, see *Configure managed IP phones or templates*.

Setting	Description	Default
Name	The name of this IP phone must be unique. Click **Browse** to locate an existing station.	Specified when the phone is added
Active	Inactive phones do not receive calls.	Active
MAC Address	The MAC address must be in the format	

	xx:xx:xx:xx:xx:xx. Polycom MAC addresses start with 00:04:f2. **Note**: Changing the MAC address will reload a previously registered managed IP phone.	
Registration	The available options are: • **Registration Group** • SIP Bridge If you choose SIP Bridge, and there are more than one SIP bridges available, then select the name of the bridge in the list. If no bridge exists, CIC prompts you to create one. To modify an existing SIP bridge, select the bridge and click **Configure**. **Note:** If you select a SIP Bridge registration, then you must complete the **MAC Address** field.	Default Registration Group
Location	All station appearances are in this same location. Time zone information is read from the location and used to set the phone time, DST settings, and so on. **Note**: If the Enable Regional Dialing option is selected, and a change to this location creates an extension conflict of a managed IP phone, a message is displayed listing duplicate extensions. For later reference when resolving conflicts, click **Copy to Clipboard** to copy the listing, and then paste the content to a program that supports CSV (like Microsoft Excel).	Default Location
Firmware Version	Older firmware versions previously installed on this system may also appear in the drop down list. In certain scenarios,	Latest

	you may wish to select older approved firmware for this Polycom IP phone model, for example, to control the rollout of new firmware to a managed IP phone or group of managed IP phones during an SU update. You can change this setting on multiple IP Phones if each phone selected supports this feature. **Note**: This option will not appear if the selected Polycom IP phone model does not support the selectable firmware feature.	
Preferred Language	This option is available only if multiple languages are installed. Select the language for all prompts for this managed IP phone. The available options depend on the installed languages.	System Default
Audio Protocol	The audio stream on this IP phone can be unencrypted using RTP (Real Time Protocol) or encrypted using Secure RTP (SRTP). • To use SRTP, you must choose TLS as the Transport Protocol. • Choose SRTP only if the endpoint(s) on this line support SRTP. • If you select SRTP, it enables the **Security** option (below). Calls between devices transmitting and receiving SIP TLS messages and SRTP audio are completely secure.	RTP
Use Location Time Zone	Determines whether the time zone of the associated location is used to set the date/time.	Selected

	Note: You can also configure the time zone on the DHCP server. If you configure the time zone both on the DHCP server and in Interaction Administrator, then the time zone on the DHCP server is used.	
Time Zone	The time zones listed are the same as Windows time zones. The managed IP phone will use this time zone to set the daylight saving time information. **Note:** You can also configure the time zone on the DHCP server. If you configure the time zone both on the DHCP server and in Interaction Administrator, then the time zone on the DHCP server is used.	(UTC-05:00) Eastern Time (US & Canada)
Expansion Modules	In the first list, select the number of expansion modules you want. If a second list appears, select the type of expansion modules you want. **Note:** If you select multiple expansion modules, they must all be of the same type. IA automatically adds the appropriate number of line keys for the type of expansion module that you select.	
Station Appearances	There are three types of station appearances (or an existing station may be selected). Not all types of appearances apply to all phones: • **Station Appearance** - This is a regular station appearance. For example, ManagedIPPhone105 has a regular station appearance by default labeled ManagedIPPhone105 on this	Not specified

	station. (The label can be edited.) Interaction SIP Station uses only one station appearance. - **Shared Station Appearance** - This is an appearance that is assigned to another SIP station. If the key that is associated with this appearance is pressed, an incoming call can be picked up from the other SIP station. **Note**: This option does not apply to a managed IP phone using a SIP bridge. - **External Registration -** The IP phone obtains its registration outside the CIC server or the managed proxy system. For example, one station appearance for the IP phone connects to the CIC server, and another appearance connects to an outside SIP server. **Note**: This option does not apply to a managed IP phone using a SIP bridge. After you add, edit, or remove station appearances, you must reload the phone.	

Related topics

Configure managed IP phones or templates

Options

Information

Advanced options

Add Registration

Registration Group

SIP Bridge

SIP Bridges Configuration

Location

Enable Regional Dialing option

Managed IP phone appearance configuration

Options: Polycom phones or templates

The following tables describe the options for Polycom phones or templates. For information on how to access these settings, see *Configure managed IP phones or templates*.

General

Option	Description	Default
Enable MWI	When this setting is enabled, the phone will flash a message-waiting indicator (MWI) LED when instant messages and voice messages are waiting.	Yes
Ring Always	When this setting is enabled, the phone will always ring when the user receives a call, even if a CIC client is not running.	No
Inband Call Waiting Tone	When this setting is enabled, the phone will emit a tone on an incoming call when another call is active	No
SIP Receive Port	This is the port that the IP phone uses to send and receive SIP signaling packets using the TCP and UDP transport protocols.	5060
SIP TLS Receive Port	This is the port that the IP phone uses to send and receive SIP signaling packets using the TLS transport protocol.	5061
Media Port Start Range	Use this setting for Polycom phones that need to use a different port range than the default ports for audio traffic. Set this to a valid port number that begins the new range of ports to use for audio. Reasons to use this include phones that are behind a firewall, or that use port forwarding, or that have another reason to	Depends on the device manufacturer

	specify a different port range.	

Polycom Interface

Option	Description	Default
Language	This is the internal language used by the Polycom interface. The language is specified in <language-region> format. **Notes**: The supported languages for this IP phone depend on your Polycom firmware version and your CIC version. Please check the firmware release notes for information on your firmware version at VoIP SIP Software Release Matrix. It is recommended to select "internal" for the Polycom IP430 phone to conserve memory resources.	English-United States
Regional Tone Set	Use this setting to change the language of most call progress tones. The tone set can be specified separately from the **Language**, but the value defaults to "Language Default", which is the country based on the value of the **Language** setting. The IP phone requires a reload after changing this setting. Valid languages for the regional tone set include: Canada, China, Denmark, France, Germany, Italy, Japan, Korea, Netherlands, Norway, Poland, Portugal, Russia, Slovenia, Spain, Sweden, United Kingdom, United States. **Notes**: The regional tone set does not affect busy tones, ringback tones, or reorder tones. If the tone set is not providing the desired tones, contact a PureConnect Customer Care representative for assistance in making	Language Default

	configuration changes.	
Use 24 Hour Clock	Use this setting to display the time in 24 hour format (for example, 21:43:12). The options are: • **Yes** • **Language Default** • **No**	Language Default
Use Long Date Format	Use this setting to display the date in the long date format (for example, January 14, 2010). The options are: • **Yes** • **Language Default** • **No**	Language Default
Show Date Before Time	Use this setting to display the date before the time. If the date and time are on the same line, then the date will be displayed on the left. If the date and time are on separate lines, then the date is displayed above the time. The options are: • **Yes** • **Language Default** • **No**	Language Default
Date Format	Use this setting to display the day of week, day, and month in a specific order. The options are: • **Thursday, 21 January**	Language Default

	- **Thursday, January 21** - **21 January, Thursday** - **January 21, Thursday** - **MM-DD-YY** (for example, 07-03-10) - **DD-MM-YY** (for example, 03-07-10) **Note:** For **Use 24 Hour Clock**, **Use Long Date Format**, **Show Date before Time**, and **Date Format** parameters, the “Language Default” value uses the **Language** field above.	
Headset Mode	When this setting is enabled, the headset is selected as the preferred mode after its first use until the headset key is pressed again. If this setting is not enabled, hands-free (speaker phone) mode is the preferred mode.	No
One Touch Voicemail	When this setting is enabled, the voice mail summary display is bypassed, and voice mail is dialed directly.	No
Polycom Call Waiting	Use this setting to change the call waiting behavior on Polycom IP phones. The options are: - Beep - **Silent** (for no sound indicator for a call that is waiting)	Beep
Persist Headset Volume	When this setting is enabled, the receive volume between calls is remembered. If not enabled, the receive volume is reset to nominal at the start of each call.	No
Persist Handset Volume	When this setting is enabled, the receive volume between calls is remembered. If not enabled, the receive volume is reset to	No

	nominal at the start of each call.	
Persist Handsfree Volume	When this setting is enabled, the receive volume between calls is remembered. If not enabled, the receive volume is reset to nominal at the start of each call. The default value is Yes (enabled).	Yes
Enable Handsfree	When this setting is enabled, the speakerphone can be used to dial. If not enabled, the handsfree mode is disabled and the speakerphone cannot be used to dial.	Yes
Line 2 Key Function	This applies to Polycom IP 330/IP 320 only. Use this setting to change the function of the Line 2 hard key. The options are: • Line 2 • Messages • Do Not Disturb	Line 2
DND Key Function	Select **Phone only** to enable DND functions on this IP phone. Select **Status Synchronized** to synchronize the user's status with the user's CIC client configuration status when he/she is logged into the station.	Disabled
Forward Key Function	Select **Phone only** to enable forwarding functions on this IP phone. When setting this option to **Phone only**, this phone's status changes to "Reload Required." After rebooting, a forward softkey is shown on the IP phone.	Disabled
Number First in Caller ID	This setting specifies the order of name and number in the caller ID.	No

	The options are: - **No**: The caller's name appears first. - Yes: The phone number appears first.	

Polycom Local Dialplan

Option	Description	Default
Emergency Registration Group	Select the registration group from the pull-down list to use when routing calls made to emergency numbers (as listed in the **Emergency Numbers** option below).	Not specified
Emergency Numbers	This setting lists the numbers that should be monitored. If one of these numbers is detected as having been dialed by a user, the call will automatically be directed to the defined **Emergency Registration Group**. Separate multiple numbers by a comma.	911

Emergency Information

Option	Description	Default
Description	The description of the location of this IP phone. This description is displayed in station group directories in the CIC clients. For example, a description might be "Conference Room 1".	Not specified
Location	The location information (60 digit alpha-numeric) that is provided to dispatched emergency personnel (for example, Building 1, floor 3, north wing, office #26, next to elevator). The ALI record field is LOC.	Not specified

Calling Party Number	The outbound ANI (10 digit numeric) to use for emergency calls from this IP phone. The Automatic Location Identification (ALI) record field is CPN and in "emergency" terminology it is Emergency Location Identification Number (ELIN).	Not specified
Customer Name	The name (32 character alpha-numeric) to provide for this IP phone (i.e., John Smith). The ALI record field is NAM.	Not specified

Related topics

Configure managed IP phones or templates

Advanced options: Polycom phones or templates

The following tables describe the advanced options for Polycom phones or templates. For information on how to access these settings, see *Configure managed IP phones or templates*.

> **Note:** These options are used only for diagnostic and troubleshooting purposes. Do not change them without clear direction from a PureConnect Customer Care representative.

Polycom General

Option	Description	Default
Call Offering Timeout		
Call Ringback Timeout	This option specifies the time in seconds to allow an outgoing call to remain in the ringback state before dropping the call.	0
Call Dialtone Timeout	This option specifies the time in seconds to allow the dialtone to be played before dropping the call. If set to 0, the call is not dropped. If set to <NULL> (or no value), the	15

	call is dropped after 60 seconds.	
Configuration Time Zone Overrides DHCP	This option determines whether the time zone that is set for the location that is associated with the IP phone overrides the DHCP time zone settings.	No
Configuration NTP Server Overrides DHCP	This option determines whether the SNTP server settings that are associated with the IP phone override the DHCP server settings.	No
DTMF On Time	This option sets the length of time (in milliseconds) that the tones are generated when a sequence of DTMF tones is played automatically. This option also sets the minimum time the tone is played when an agent dials manually, regardless of the duration of the key press.	80
DTMF Off Time	This option sets the length of time (in milliseconds) that the IP phone pauses between digits when a sequence of DTMF tones is played automatically. This option also sets the minimum inter-digit time when an agent dials manually.	80
Phone Limits Calls Per Line Key	This option indicates whether the number of calls per line key is limited by the specific model of Polycom IP phone settings.	No
Always Reboot on Reload	This option indicates whether the phone is automatically rebooted when a user clicks **Reload Now**. **Note:** When you enable this option, another port/service is open on the phone. Consider the security implications before you enable this	No

	option.	
Enable Configuration Web Page	This option allows you to enable or disable the webpage on Polycom phones.	Off
Phone Offer Cryptosuites	This option determines which cryptosuite(s) the phone offers in SDP. The choices are: • AES_CM_128_HMAC_SHA1_32 only • AES_CM_128_MHAC_SHA1_80 only • Both **Note:** If you do not set this option, the phone automatically offers both cryptosuites.	Both
Phone Require Secure Media	This option indicates whether the phone is allowed to use only secure media streams. • If set to "No,"the phone can accept non-secure media streams. • If set to "Yes,"the phone accepts only secure media streams. • Any offered SIP INVITEs must include a secure media description in the SDP or the call is rejected. • For outgoing calls, only a secure media stream description is included in the SDP of the SIP INVITE. The non-secure media description is not included.	No
Enable Power Saving	Select this option to enable power saving mode. When the phone is in power saving mode, the phone's LCD display is automatically turned off after 1 minute. This option is available for Polycom VVX	Off

	models only: • By default, this option is disabled on the VVX 300, 301, 310, 311, 400, 401, 410 and 411 models. • By default, this option is enabled on the VVX 500, 501, 600 and 601 models.	
Use 486 For Reject	This option indicates whether CIC sends a busy signal as the rejection reason to a SIP request.	No
Phone Warning Level	This option determines when the phone’s warning icon and warning pop-message appear on the Polycom phones. The choices are: • All warnings • Critical warnings • None The default value is All warnings. You must opt-in for settings other than the default value. **Note:** The warning, “Default admin password is in use. Please contact your administrator,” reminds you to change the default administrator password on the phone. Genesys recommends that you change this password. Alternatively, you can change the Phone Warning Level to 1 and the warning will no longer appear. However, changing the phone warning level **does not** actually fix the root problem involving the default admin password. On the phone, the warnings always appear under Settings>Status>Diagnostics>Warnings.	
TCP Session Timeout	This option sets the number of seconds CIC waits before it attempts a TCP connection.	<Null> or 0 (The IP phone's default settings are used.)

(seconds)	CIC attempts to connect until it meets the TCP session retries count. To control the timeout behavior in the event of a TCP connection failure, set this parameter and the **TCP Session Retries** parameter.	
TCP Session Retries	This option sets the number of times CIC attempts to make a TCP connection. If it cannot connect within this number of times, CIC moves to the next server. A retry is made if the session reaches in seconds the timeout as set in the **TCP Session Timeout** (above). To control the timeout behavior in the event of a TCP connection failure, change this parameter and the **TCP Session Timeout** parameter.	<Null> or 0 (The IP phone's default settings are used.)
Boot Server Type	This option determines whether the phone controls boot server options by the menu or the provisioning server controls boot server options. If controlled by the phone, the CIC provisioning subsystem does not write configuration for boot server options. If controlled by the provisioning server, the server writes configuration to the provisioning files. **Note**: If the **Boot Server Option**, **Boot Server Option Type**, or **Provisioning URL** contain incorrect values, the provisioning server does not write the configuration for boot server options. If incorrect values exist, the provisioning logs contain errors such as: • Boot Server Option not in range of 128-254. • Provisioning URL is not a compliant RFC 2396/RFC 3986 URI. This option is available for Polycom phones	Phone

	capable of 4.0 or newer firmware. Select: **Phone** to use the phone menu to control boot server options. **Custom** to use the DHCP option you set by using the Boot Server Option option and the Boot Server Option Type option. **Custom + Opt.66** to use the DHCP option you set by using the **Boot Server Option** option and **Boot Server Option Type** option. If the phone cannot determine the information from the Boot Server Option option, the phone uses DHCP option 66. **Opt.66** to use DHCP option 66 to determine boot server parameters. **Static** to use the Provisioning URL option to determine the boot server.	
Boot Server Option	This option is the DHCP option that the phone uses when trying to determine the boot server parameters. Set this option if you selected **Custom** or **Custom + Opt.66** in the **Boot Server Type** option. Valid entries include empty string or an integer in range from 128 to 254. This option is available for Polycom phones capable of 4.0 or newer firmware.	
Boot Server Option Type	This option indicates the DHCP option type to use with the **Boot Server Option** option. You can select **IP Address** or **String.** Set this option if you selected **Custom** or **Custom+Opt.66** in the **Boot Server Type** option**.** This option is available for Polycom phones capable of 4.0 or newer firmware.	String
Provisioning URL	This option indicates the URL that the phone points to. Set this option if you selected **Static** in the **Boot Server Type** option. Enter a compliant RFC 2396/RFC 3986 URI and use a scheme of FTP/TFTP/FTPS/HTTP/HTTPS. If you do not enter the scheme, the phone uses HTTP. If	

	you do not enter the port, the phone uses the default value for the scheme. For HTTP provisioning, the URL must specify port 8088 since the Provisioning subsystem on the CIC server listens on port 8088 and not port 80. Polycom phones assume port 80 for an HTTP URL. Example: http://provision.mydomain.com:8088 This option is available for Polycom phones capable of 4.0 or newer firmware.	

Polycom Features

Option	Description	Default
Presence	This option is related to the Presence feature of Microsoft Windows Messenger 5.1 on the IP phone. **Note**: The **Presence** feature is reserved for custom integrations outside of CIC. Enabling this option in Interaction Administrator has no effect in the CIC system.	No
Messaging	This option is related to the Instant Messaging feature of Microsoft Windows Messenger 5.1 on the IP phone. **Note**: The **Messaging** option is reserved for custom integrations outside of CIC. Enabling these features in Interaction Administrator has no effect in the CIC system.	No
Directory	This option specifies whether the user can edit the local contacts.	Yes
All Call Lists	This option specifies whether the user can view all call lists, including the Received Call List, the Placed Call List, and the Missed Call List.	Yes

Received Call List	This option specifies whether the user can view the list of received calls.	Yes
Placed Call List	This option specifies whether the user can view the list of placed calls.	Yes
Missed Call List	This option specifies whether the user can view the list of missed calls.	No
URL Dialing	This option specifies whether URL/name dialing is available from a private line. (This feature is never available from a shared line.)	No
Call Park	This option specifies whether active calls can be parked and retrieved.	Yes
Group Call Pickup	This option specifies whether calls to another phone within a predefined group can be picked up without dialing the extension of the other phone.	Yes
VVX D60 Profile	This option indicates whether to enable the VVX D60 feature.	No

Polycom Interface

Option	Description	Default
Idle Screen Logo	This option sets the background image that the Polycom IP phone displays when the phone is not on a call. Enter the name of the file excluding the extension. For example, if logo_ip600.bmp is the complete file name, enter the value of "logo_ip600." Supported formats for VVX phones are PNG, JPG, and BMP. Supported formats for	

SoundPoint IP phones are JPG and BMP.

Note: If you do not specify an extension, CIC assumes that BMP is the extension.

Place the source image file in the \\ic\provision\polycom directory on the CIC server.

If you leave this value, which is the default setting, the system looks for the following file names, based on the model:

Model(s)	File name
IP320, IP330	IP_330
IP430	IP_430
IP450	IP_450
IP501	IP_501
IP550, IP560, IP600, IP601, IP650, IP670	IP_600
IP4000	IP_4000
IP6000	IP_6000
IP7000	IP_7000
TRIO8500	TRIO_8500
TRIO8800	TRIO_8800

Note: The resolution is dependent on the model. JPG, PNG, and BMP images may require special file format

	parameters. See the "Adding a Background Logo" section in the *Polycom Administration Guide* for information on resolutions.	
Idle Screen Background Color	This option sets a custom background color for the Polycom IP670 phone. This option is used to improve the appearance of the **Idle Screen Logo** for the IP670. Enter the color in either hexidecimal (for example, "0x0077FF" - must being with "0x"), or decimal value.	Not specified
Headset Echo/Noise Suppression	This option indicates whether echo and noise suppression is used with the agents' headsets. **Note**: When you enable the **Headset Echo/Noise Suppression** option, there is a short transmit delay of 30 milliseconds.	No
Headset Microphone Gain	This option specifies the gain value for the headset microphone: • IP330 group (320, 321, 330, 331, 335)=21, and acceptable values are 0 to 21 • IP430=21, and acceptable values are 0 to 39 • IP450=21, and acceptable values are 0 to 21 • IP550 and IP560=21, and acceptable values are 0 to 21 • IP650 and 670=21, and acceptable values are 0 to 21	
Headset Speaker Gain	This option specifies the gain value for the headset speaker: • IP330 group (320, 321, 330, 331, 335)=4, and acceptable values are 0 to 25 • IP430 and IP450=1, and acceptable	

	values are 0 to 25 • IP550 and IP560=1, and acceptable values are 0 to 25 • IP650 and IP670=1, and acceptable values are 0 to 25	
Headset Sidetone Gain	This option specifies the gain value for the headset sidetone: • IP330 group (320, 321, 330, 331, 335)=-3, and acceptable values are -25 to -3 • IP430 and IP450=-3, and acceptable values are -25 to -3 • IP550 and IP560=-3, and acceptable values are -25 to -3 • IP650 and IP670=-3, and acceptable values are -25 to -3	
Electronic Hookswitch Mode	This option indicates whether optional external hardware is available for use with a headset attached to the IP phone's analog headset jack. The options are: • Regular (None) • Jabra (DHSG) • Plantronics	Regular (None)
Auto Dial on Off-hook	This option indicates whether contacts can be automatically dialed when the phone is off-hook. Contacts must be configured with the **Auto Dial on Off-hook Number** option.	No
Auto Dial on Off-hook Number	This option specifies a number to auto dial when the **Auto Dial on Off-hook Number** option is enabled.	

VVX D60 Allowing Paring	This option indicates whether a user can pair or unpair a VVX D60 base station with a VVX business media phone. You can select: • **None -** To not allow users to pair or unpair a base station from the VVX phone. • **Pairing -** To allow users to pair the base station with the VVX phone, but not allow users to unpair a base station. • **Unpairing -** To allow users to unpair the base station from the VVX phone, but not allow users to pairing a base station. • **Both** - To allow users to pair and unpair the base station with the VVX phone.	None

Polycom Local Dialplan

Option	Description	Default
Digitmap	This option allows you to edit digitmap properties. The digitmap feature eliminates the need for using the Dial or Send soft key when making outgoing calls when a matching digit pattern is detected. As soon as a digit pattern match is found, the call setup process completes automatically. Acceptable values are strings compatible with the digit map feature of MGCP described in 2.1.5 of RFC 3435. String is limited to 768 characters and 30 segments; a comma is also allowed; when reached in the digit map, a comma will turn dial tone back on;’+’ is allowed as a valid digit;	x.T|*T|*905|*90[1-4]x.T

	extension letter ‘R’ is used. For complete information, see the *Polycom Technical Bulletin 11572* and Polycom's *Administrator’s Guide for the SoundPoint® IP/SoundStation® IP Family.*	
Digitmap Timeout	This option sets the timeout in seconds for each segment of the digitmap. **Note**: If there are more digitmaps than timeout values, the default value of 3 is used. If there are more timeout values than digitmaps, the extra timeout values are ignored.	3|1|3|3

Polycom Network Address Translation (NAT)

Option	Description	Default
NAT IP Address	This option sets the IP address to use in NAT traversal. **Note:** This setting only changes the IP address that is displayed in SIP signaling. *All IP addresses in managed phones configuration are pass-through strings to support IPv6.*	Not specified
NAT Signal Port (1024-65535)	This option sets the signal port to use in NAT traversal. This setting changes the port setting used by the IP phone.	Not specified
NAT Audio Port Start (1024-65535)	This option sets the audio port to start in NAT traversal. This setting changes the RTP port that is initially allocated to the IP phone.	Not specified
NAT Keep Alive Interval (0-3600 seconds)	This option sets the interval time in seconds in which IP phones send a keep-alive packet to the NAT device to keep the communication port open so that NAT can continue to function as initially configured.	Not specified

Polycom Flash Parameters

Option	Description	Default
Admin Password	This setting changes the phone's local administrator password. Any string is an acceptable value. **Note**: When this password is changed, the value is passed to the phone one time, and then is removed from DS (Directory Services). The Polycom phone remembers the password change, and the provisioning server does not send this value to the phone configuration in any subsequent phone reboots.	Not specified
802.1Q VLAN Identifier	This setting is used by the IP phone to set the phone's 802.1Q VLAN identifier if VLAN ID is not obtained by CDP or DHCP. Acceptable values are 0 to 4094	Not specified (no VLAN tagging)
LAN Port Mode	This option sets the network speed over the Ethernet for the IP phone through the LAN port. Acceptable values are: • Auto • 10 Full Duplex • 10 Half Duplex • 100 Full Duplex • 100 Half Duplex	Auto

Polycom Syslog Tracing

Option	Description	Default
Syslog Server	This option sets the syslog server IP	Not specified (syslogging is enabled, and the log file no

	address or host name. When a **Syslog Server** is specified, the **Syslog Transport** and **Syslog Render Level** settings are used. When a **Syslog Server** is *no*t specified, the **Syslog Transport** and **Syslog Render Level** settings are ignored. All IP addresses in managed phones configuration are pass-through strings to support IPv6. **Note**: When you specify a Syslog Server value, the IP phone's application log which is sent to the provisioning server, is no longer used, or disabled. This means the log file no longer appears in the IC, and all information is present in the syslog instead, which protects Polycom's flash memory abilities.	longer appears in the CIC system)
Syslog Transport	This option sets the syslog transport protocol. Acceptable values include TCP and TLS.	UDP
Syslog Render Level	This option sets the lowest class of event that will be rendered to the syslog. The acceptable range of values is 0 through 6.	0
Disable App Logs When Using Syslog	When **Syslog Tracing** is enabled, application logs are disabled (set to **Yes**) by default. Change this setting to **No**, to enable the creation of application logs by Polycom phones. The information generated and collected in the application log (which is stored in the phones folder in the IC server's logging directory, usually \\IC\Logs\[date]\..., is the same information as the information	

	generated and collected in the system log. Tracing bandwidth can be reduced by turning off the application log collection when the system log collection is enabled.	
Application	This option sets the tracing level for the Application syslog topic. **Note:** When you increase the tracing level, phone performance may be adversely affected. This is especially true if you increase multiple tracing levels simultaneously Be sure to reduce the tracing level when you no longer need it. For more information, see Logging levels.	4
Browser	This option sets the tracing level for the Browser syslog topic. **Note:** When you increase the tracing level, phone performance may be adversely affected. This is especially true if you increase multiple tracing levels simultaneously Be sure to reduce the tracing level as soon as possible. For more information, see Logging levels.	4
Configuration	This option sets the tracing level for the Configuration syslog topic. Note: When you increase the tracing level, phone performance may be adversely affected. This is especially true if you increase multiple tracing levels simultaneously Be sure to reduce the tracing level as soon as possible. For more information, see Tracing levels for the Polycom Syslog.	4
Copy Utilities	This option sets the tracing level for the Copy Utilities syslog topic. **Note:** When you increase the tracing level, phone performance may be	4

	adversely affected. This is especially true if you increase multiple tracing levels simultaneously Be sure to reduce the tracing level as soon as possible. For more information, see Tracing levels for the Polycom Syslog.	
CURL	This option sets the tracing level for the CURL syslog topic. **Note:** When you increase the tracing level, phone performance may be adversely affected. This is especially true if you increase multiple tracing levels simultaneously Be sure to reduce the tracing level as soon as possible. For more information, see Tracing levels for the Polycom Syslog.	4
Key Observer	This option sets the tracing level for the Key Observer syslog topic. **Note:** When you increase the tracing level, phone performance may be adversely affected. This is especially true if you increase multiple tracing levels simultaneously Be sure to reduce the tracing level as soon as possible. For more information, see Tracing levels for the Polycom Syslog.	4
SIP	This option sets the tracing level for the SIP syslog topic. **Note:** When you increase the tracing level, phone performance may be adversely affected. This is especially true if you increase multiple tracing levels simultaneously Be sure to reduce the tracing level as soon as possible. For more information, see Tracing levels	4

	for the Polycom Syslog.	
Support Objects	This option sets the tracing level for the Support Objects syslog topic. **Note:** When you increase the tracing level, phone performance may be adversely affected. This is especially true if you increase multiple tracing levels simultaneously Be sure to reduce the tracing level as soon as possible. For more information, see Tracing levels for the Polycom Syslog.	4
TLS	This option sets the tracing level for the TLS syslog topic. **Note:** When you increase the tracing level, phone performance may be adversely affected. This is especially true if you increase multiple tracing levels simultaneously Be sure to reduce the tracing level as soon as possible. For more information, see Tracing levels for the Polycom Syslog.	4
Wapp Mgr	This option sets the tracing level for the Wapp Mgr syslog topic. **Note:** When you increase the tracing level, phone performance may be adversely affected. This is especially true if you increase multiple tracing levels simultaneously Be sure to reduce the tracing level as soon as possible. For more information, see Tracing levels for the Polycom Syslog.	4

Polycom Voice Quality Monitoring

Note: The Polycom Voice Quality Monitoring feature requires a license.

Option	Description	Default
Enable RTCP-XR Reports	This setting indicates whether Polycom phones to generate reports in RTCP XR packet metrics on listening and conversational quality.	No
Enable Collector Session Reports	This setting indicates whether Polycom phones to create session type reports, which are generated at the end of a call.	No
Enable Collector Periodic Reports	This setting indicates whether Polycom phones to create periodic type reports, which are generated throughout a call.	No
Report Collector Address	This option sets the IP address or host name of the SIP server (report collector) that accepts voice quality reports contained in SIP PUBLISH messages. All IP addresses in managed phones configuration are pass-through strings to support IPv6.	
Report Collector Port	This option sets the port of the SIP server (report collector) that accepts voice quality reports contained in SIP PUBLISH messages. If port is 0 or <Null>, port 5060 will be used.	
Collector Period (5 to 20)	This option sets the time interval between successive periodic quality reports.	20

Polycom Voice Quality Monitoring Alerts

Option	Description	Default
Enable Triggered Collector Periodic Reports	This option indicates whether the generation of periodic quality reports triggered by alert states. The options are: • **Critical**: periodic reports will be	Disabled

	generated when an alert state is critical - **Warning or Critical**: periodic reports will be generated when an alert state is either warning or critical	
MOS-LQ Warning Threshold (15 to 40)	This option sets the threshold value of listening MOS score that causes the IP phone to send a warning alert quality report. Acceptable values are 15 to 40.	Not specified (warning alerts are not generated)
MOS-LQ Critical Threshold (15 to 40)	This option sets the threshold value of listening MOS score that causes the IP phone to send a critical alert quality report. Acceptable values are 15 to 40.	Not specified (warning alerts are not generated)
Delay Warning Threshold (10 to 2000)	This option sets the threshold value of one way delay (in ms) that causes the IP phone to send a warning alert quality report. Acceptable values are 10 to 2000.	Not specified (warning alerts are not generated due to one way delay; includes both network and end system delays)
Delay Critical Threshold (10 to 2000)	This option sets the threshold value of one way delay (in ms) that causes the IP phone to send a critical alert quality report. Acceptable values are 10 to 2000.	Not specified (critical alerts are not generated due to one way delay; includes both network and end system delays)

Polycom SIP Security

Option	Description	Default
Inbound SIP Security	This option sets the level of security the Polycom IP phone uses to validate the SIP	None (the phone does not take any steps to authenticate

Challenge	inbound (to the phone versus inbound to CIC) traffic. The possible values are: - **Source**: The IP phone checks the source IP address of the SIP request against the IP addresses of its SIP Registrations. If addresses do not match, the SIP request is rejected. If there is a match, the request is accepted. - **Digest**: The IP phone sends a 401 Unauthorized challenge when a SIP request comes in, and the sender of the request must respond with the proper credentials for the SIP transaction to proceed. - **Source and Digest**: The IP phone first applies the **Source** method, then the **Digest** method.	inbound SIP traffic)
Phone side only SRTP (Offloading)	This setting has the same effect as the as the audio protocol setting in the general configuration, however it only changes the phone setting.	No

Related topics

Configure managed IP phones or templates

Location

SNTP server

Audio protocol

SIP settings: Polycom phones or templates

SIP settings are organized into categories, as shown under **Related topics**.

For information on how to access the SIP option settings, see *Configure advanced options for managed IP phones or templates*.

Related topics

SIP audio settings

SIP transport settings

SIP transport settings

SIP session settings

SIP authentication settings

Configure advanced options for managed IP phones or templates

Information: Polycom phones or templates

The following table describes the information that is shown for Polycom phones or templates. This information is automatically updated when the IP phone, or an IP phone that uses the template, is registered.

For information on how to access these settings, see *Configure managed IP phones or templates*.

Detail	Description
Phone	This is the manufacturer and model of the IP phone device.
Type	This is the type of station (workstation or stand-alone phone.
IP Address	This is the IP address of the device. N/A indicates the device is not registered.
Contact Line	This is the SIP line used when the phone registered with the CIC server. This line will be used to send SIP signaling to the phone.
Last Reload	This is the date and time when the phone requested configuration update or the phone was reloaded after a configuration change.
Status	This is the status of the phone from the CIC server perspective (i.e., Not registered, Up-

	to-date, Reloading, Reload required.
Max. Line Keys	This is the maximum number of line keys associated with this device.
Max. Appearances	This is the maximum number of shared line appearances for this device.
Notes	These are any comments CIC administrators add about this device or the associated template.

Related topics

Configure managed IP phones or templates

Registration Groups

Registration Group Configuration

You must specify a registration group for every managed IP phone. The registration group controls how and where the phone is registered with CIC. It determines which phone is associated with which user, and it controls the user's contact information.

When you add a registration group, you designate it as either regular or external. See Add Registration for more information.

Each registration group is comprised of a list of registration entries:

- To add an entry to a regular registration group, you can select an existing line, you can specify an entry manually, you can designate a proxy, or you can designate a DNS server. You can specify only one line in a regular registration group.
- To add an entry to an external registration group, you can specify an entry manually, or you can designate a DNS server.

The entries in a registration group are ordered. When CIC attempts to place a call to the registration group, it tries to connect to the first entry in the list. If it connects to that entry, then it attempts to connect to the next entry in the list, and so on. You can change the order of entries in a registration group by using the up and down arrow keys.

> **Notes:**
> A registration group can have multiple entries. The first entry in the list is the only device that has full SIP functionality. Therefore, if you add a line registration, you must add it as the first entry. Or, if you add a DNS SRV registration, you must add it as the first entry. You cannot add both a line registration and a DNS SRV registration to the same registration group.
>
> A single Polycom phone can have up to 3 devices in a registration group. Polycom registers all

> entries in the registration group, even if the phone is not actively sending outbound calls to the server.
>
> A registration group can have a maximum of 4 registration entries.

Default Registration Groups

By default, in a new CIC installation, CIC creates two permanent default registration groups:

- **<Default Registration Group>**: line type of <Stations-UDP> See SIP Line Transport for more information.
- **<Default Secure Registration Group>**: secure line type of <Stations-TLS> The certificate is set to the domain certificate. See SIP Line TLS Security and SIP Line Transport for more information.

Interaction SIP Station does not currently support TLS, so you can choose to use the permanent <**Default Registration Group**>, or create a custom registration group in the **Registration Groups** in the **Managed IP Phones** container.

> **Note**: See *CIC Managed IP Phones Administrator's Guide* in the **Technical Reference Documents** section of the PureConnect Documentation Library on the CIC server.

Registration Types

Line - Select an existing line from the pull-down list for the registration. This is currently the only type of registration allowed for Interaction SIP Station.

Manual - Manually enter the address, port, and protocol for the registration.

DNS SRV - Enter the domain name and protocol for the registration.

> **Note**: If you change a line that is used in a registration group, all managed IP phones using it will immediately need to be reloaded. Any phones not reloaded will stop functioning when the line is changed.

Field Definitions

Name

This is the name of the registration group. The default registration groups are read-only and can not be renamed.

Registrations

This section displays the registration types and registration details.

Click Add to add a new registration entry to the registration group.

Add Registration

Use this page to select the type of registration and enter the settings. The options that are available depend on the registration group type.

If the registration group is "External," then you must define the registration settings manually or obtain them from DNS SRV. You cannot obtain the registration settings automatically from a line or from a proxy.

If Polycom phones connect to both a primary CIC server and to another SIP server, then you can create an external group and add an external station appearance to the phones.

> **Switchover Systems**
>
> If you are configuring a Switchover pair on an IP phone network for managed Polycom phones, select **Obtain registration settings automatically using DNS SRV** on this page to obtain registration settings from the DNS SRV records created when you configured the network for Polycom phones.
>
> For more information, see the *CIC Managed IP Phones Technical Reference* in the **Technical Reference Documents** section of the PureConnect Documentation Library.

Obtain registration settings automatically from this line

This option does not currently apply to an external registration group.

Use this option for Interaction SIP stations.

From the list, select the line from which settings are to be read. By default, the line setting is <Stations-UDP>. The settings used from the line are the network adapter, transport, protocol, and port. In this case, switchover is handled by the provisioning server.

CIC allows only one line registration per registration group. If there were multiple line registrations per registration group, phones could register to the same server twice.

> **Note**: CIC creates two default line type registration groups.

Use the following registration settings

This option does not currently apply to Interaction SIP stations.

Address: Enter an IP address or host name. and the protocol (default: UDP) address. IP addresses are pass-through strings to support IPv6.

Port: Enter the port to be used. The default is 5060.

Transport Protocol: Select the type of transport protocol. The options are **UDP**, **TCP,** and **TLS**. The default is **UDP**.

Obtain registration settings automatically from this proxy

This option does not currently apply to Interaction SIP stations, nor does it apply to an external registration group.

SIP Proxy: The SIP proxy that is trusted and available appears here.

Alternate Address: Type the alternate SIP proxy address in the format where the proxy is appended to the address, like "1|Proxy|proxy1|TCP|10.10.10.10." If you leave this field blank, the value is location-based.

Transport Protocol: Select the type of transport protocol for the proxy. The options are **UDP**, **TCP,** and **TLS**. The default is **UDP**.

Obtain registration settings automatically using DNS SRV

CIC allows only one DNS SRV registration per registration group, otherwise phones could register to the same server twice.

Domain: Type the DNS domain name.

Transport Protocol: Select the type of transport protocol. The options are **UDP**, **TCP,** and **TLS**. The default is **UDP**.

> **Note**: Shared appearances do not attempt to register with managed SIP proxies. If a registration group has multiple entries, one of which is a managed SIP proxy, shared appearances using that registration group will attempt to register with all other entries, but not with a managed SIP proxy. Other (non-shared) appearances register as usual.

Related topics

SIP proxies

SIP line proxy

SIP proxy configuration - general

Endpoints

Registration groups

Managed IP Phone configuration - general

Registration Group Options

Use this page to select the DNS cache option and a custom certificate authority for managed IP phones.

Use Polycom Static DNS Cache

Select this check box to use cache file's preloaded resource information which is obtain when the DNS service is started.

Certificate Authority

Select the certificate from the pull-down list to use for managed IP phones for this registration group.

> **Note**: You must first import the certificate authority in Certificate Authorities. This option is available only if the registration transport protocol is TLS, which requires the Advanced Security Feature license.

Default IP Phone Configuration

Use the this page to select the menu line. This page does not apply to Interaction SIP Station.

> **Note**: Interaction SIP Station devices do not currently support auto-provisioning. In addition, the Use digest authentication option must be disabled to use Interaction SIP Stations on the server.

Auto-Provisioning

This line is used to provide the provisioning IVR you hear when you plug in an unprovisioned IP phone. The protocol and security settings of this line are used on the IP phone.

For example, if you have the advanced security feature license, then you can use a TLS line with SRTP enabled. Using a TLS line makes sure the DTMF can not be captured while entering your setup password.

Menu Line

Select the menu line for the default IP phone. The options are:

- Stations - TCP
- Stations - TLS
- Stations - UDP (default)
- An existing SIP line

Line Label

Type the name (or string) to display for the line on IP phones. This is a free-form field and the default value is "Setup".

Configuration Requests

Use this section to set the request options for the default IP phone configuration.

Use Digest Authentication

Select this check box to enable digest authentication. Digest authentication is a protocol used with web browsers for authenticating users browsing the Internet, and also a general protocol used for authentication, and by using SASL, provides increased protection. If this option is enabled, enter the **User Name** and **Password**, and **Confirm Password** to use as the authentication credentials. By default, this option is not enabled.

Use HTTPS Always

Select this check box to always have HTTP requests redirected to the HTTPS Port. Selecting this option requires mutual authentication. By default, this option is not enabled.

> Note: To install client certificates through configuration and provide mutual authentication, select the **Use HTTPS Always** check box and set the Provision HTTPS Mutual Authentication server parameter to "Yes. Also, the client certificates must be signed by the Default Lines Certificate Authority. For more information, See the ***CIC Managed IP Phones Administrator's Guide*** document in the **Technical Reference Documents** section of the PureCloud Documentation Library on the CIC server.

Support Insecure Legacy Phones

Select this check box to support legacy phones that do not support HTTPS protocol, which means FTP/HTTP protocol is required. By default, this option is not enabled.

> **Note**: If **Support Insecure Legacy Phones** *and* **Use HTTPS Always** options are both selected, then the HTTP protocol channel is available only for legacy phones. All other requests are redirected to HTTPS. Therefore, later model Polycom phones used as managed IP phones, should use HTTP directly.

Ring Set Configuration

A ring set contains details of the type of ring that occurs on incoming internal (user to user), external (through the main IVR or workgroup) and direct inward dial (DID) calls on a Polycom phone. By default, there is ring set <Default-Polycom> already configured for Polycom phones. The ring sets are assigned to stations/station appearances.

Use this page to configure additional ring sets or change the behavior of the default ring set.

Name

Type a descriptive name of the ring set. The category, ring type and details are displayed below the ring set name. Highlight the category to display the options for each setting. Select one option per internal, external, or DID setting. The options include settings for **Cadence**, **Wave File**, **Wave URL**, and **Visual**:

Cadence - Select one of the built-in ring types (based on the IP phone manufacturer):

- LowTrill
- LowDoubleTrill
- MediumTrill
- MediumDoubleTrill
- HighTrill
- HighDoubleTrill
- HighestTrill
- HighestDoubleTrill
- Beeble
- Triplet

Wave File - Select a wave file to play for a call. The wave file location must be in \\ic}\resources\....

Wave URL - Select a valid URL for a wave file to play for a call.

Visual - Select this option to change the behavior of an incoming call, such that when a call is alerting and the user picks up the handset, the IP phone assumes that a new call is being placed. This protects against accidentally being connected to an alerting call.

Related Topic:

Managed IP Phone Appearances Configuration

SIP Bridges

SIP Bridges

A SIP bridge provides connectivity between an IP phone located at a user's home (remotely) and the CIC server (office). It allows remote users to use IP phones with a VPN connection, without requiring separate hardware. It serves as a relay for all RTP, SIP, HTTP, and DHCP Options communications to and from the IP phone.

This section includes:

New SIP Bridge Name

SIP Bridges Configuration: General

New SIP Bridge Name

Type a meaningful and unique name that represents this new SIP bridge. This name is displayed in various dialog boxes in CIC.

SIP Bridges Configuration: General

Use this page to configure a SIP bridge by associating a registration group to it.

Before you configure SIP bridges and associated managed IP phones:

- Determine a unique name for each bridge.
- Get the MAC addresses of IP phones you are going to configure as managed IP phones used a SIP bridge.

Registration Group

the options are <Default Registration Group> (default) and <Default Secure Registration Group>.

SIP Bridge Details

The information displayed here shows details of this SIP bridge.

> **Note**: Managed IP phones using a SIP bridge do not support shared appearances and external registrations.

Audio Sources

Audio Sources Introduction

Audio Sources is a feature that provides “named” audio sources that continuously transmit audio and can be listened to simultaneously by multiple calls. A common use of Audio Sources is for hold music, either for system-wide calls on-hold or in-queue waiting for an agent, but there is no restriction on the use of this feature.

CIC currently supports voice resources that continuously play an audio file.

ACD workgroup on-hold music

To implement ACD workgroup on-hold music using an Audio Source:

1. Create a name for an audio source in the Audio Source Entry Name dialog box.
2. Configure the WAV file audio source in the Audio Source Configuration dialog box.
3. Navigate to the Workgroups container.
4. Right-click on the workgroup you want to hear the audio source and select **Properties**.
5. In the Files tab, type “Audio:*AudioSourceName*” in the **On-Hold Music** field.
6. Repeat steps 4 and 5 for other workgroups.

Custom implementations

Use the “Audio:*AudioSourceName*” call attribute name in a Play Audio File tool step to create custom handlers for other Audio Source implementations.

There is also an optional timeout setting in seconds, that can be used with the "Audio:*AudioSourceName*" parameter, For example:

audio:*audiosourcename*:#seconds

The "#seconds" is a timeout value that TS uses to play the audio source for that number of seconds, and then stops playing the audio.

> **Note**: This optional timeout setting is not normally used. See the **Interaction Designer** online help for more information.

Audio Source Entry Name

Type a name to represent an audio source.

Audio Source Configuration

Use this page to configure the audio source.

Audio source for a WAV file

If you plan to create a WAV file, a safe format to use (which is also optimal in many configurations) is 8 kHz mono mu-law PCM. Store it in the \\IC\Resources directory. The default WAV files are also located in the \\IC\Resources directory.

If you have not already done so, create an audio source in the Audio Source Entry Name dialog box.

1. In the **Audio Source** tab in the Audio Sources Configuration dialog, select **WAV File**.
2. Set **Filename** to the address of the WAV file in the \\IC\Resources directory or use the Browse button to locate the locate WAV file in that directory.
3. Implement the audio source using the "Audio:*AudioSourceName*" call attribute in one of the following ways:

- For system-wide on-hold music, in the OnHoldAudioRandomizerMonitor handler.
- For ACD workgroup on-hold music , in the Workgroup Configuration…Files dialog.
- To create a custom handler, in the Play Audio File tool step.

Server Parameters

Server Parameter Configuration

Type a value for the parameter.

Parameters are like macro names that can be included as a variable in a handler step, a path to a report, and so on. When the handler runs or the report is generated, the parameter is expanded and its value is used in the process.

> **Note**: Parameters can have a server-level scope which is known as a server parameter, a system-wide (for example, enterprise) scope which is known as a system parameter. Their names and configuration are otherwise identical. Server parameters are available only on a particular CIC server and system parameters are available on all CIC servers on a network.
>
> For example, server parameter values could include a valid directory path, a DLL file name, a database name, and so on. A system parameter might contain a corporate phone number or some other enterprise-wide value referenced by handlers on multiple servers.
>
> Certain chat parameters are used for Web Services.

Using Parameters

If you use multiple references to the content of a particular directory whose location may change, or if you use multiple references to some other value that may change, you should probably define a server or system parameter. Using a parameter in such cases allows you to change the value in one location (where the parameter is defined) instead of looking for and changing all locations of the value.

> For example, suppose a few handlers and a configuration attribute need to reference the directory containing report files. Create a server parameter named ReportsPath whose value is, for example, D:\EIC\Reports\. Then, wherever you need to refer to the contents of that directory, specify the name ${ReportsPath} instead of the physical directory name. Such references work in Interaction Administrator fields.
>
> **Note:** Parameters containing directory paths (for example, ServerReportLogOutputPath) are not updated, nor are they recognized immediately, when you change a path. To update these values, you must restart CIC.

Packaged Server Parameters

CIC includes several pre-configured server parameters that are used in the default handlers and by various modules on the CIC server. In addition, there are several optional server parameters that modify the default behavior of the email tools and the CIC and Exchange interface.

> **Note:** Parameters containing directory paths (for example, ServerReportLogOutputPath) are not updated, nor are they recognized immediately, when you change a path. To update these values, you must restart CIC.

Packaged Server Parameters	Description
AdminServerMonitorPath	This server parameter monitors paths and replaces trailing bac value: ${SERVER}\Parameters\Attendant Audio Path\Value;${SERVER Path\Value;${SERVER}\Parameters\Attendant Fax path\Value;${SERVER}\Parameters\CustomMirrorDir\Value;${S Path\Value;${SERVER}\Parameters\Rx Document Path\Value;$ Path\value;${SERVER}\Parameters\Temp Path\value;${SERVER Path\value;${SERVER}\Parameters\IconPath\Value
Allow Voicemail Operator Escape	Use this parameter to enable or disable the (silent) option to e pressing '0' during voicemail. Acceptable values are Y, Yes, T, T parameter. Any other value is treated as false which disables th
Attendant Audio Path	This is the default path where Interaction Attendant's stores its is usually \\IC\Resources\InteractionAttendantWaves, which is AttendantWaves directory. This value is set during installation, and you should not change
Attendant Fax Path	This is the path where Interaction Attendant's fax files are stor usually \\IC\Resources\InteractionAttendantFaxes, which is sha directory. This value is set during installation, and you should not change
Collective Support	When this server parameter has a value of 1, it tells CIC that M has a value of 0, Multi-Site is not installed.
CreateICNotifierIdentityProvider	To reset the IC Notifier Identity Provider entries to set this server parameter to “1.” The first time the IC Secure Token Server (STS) st

	sets the IC Notifier Identity Provider Directory Ser STS also creates the CreateICNotifierIdentityProvic and sets it to “1” (true). The IC STS automatically resets the value of this s each time it resets the IC Notifier Identify Provider settings to their default values to prevent it from r
CustomMirrorDir	Specifies one or more directories on the active server to be mi in addition to the default mirrored directories. Any time a file modified in one of these directories, the change is mirrored in on the backup server. Each directory in the list is separated fro If you want the directory mirrored recursively (including direct place a + in front of the directory name. For example: +D:\server\ic\ImportantDir Please refer to the Automated Switchover technical reference directories.
Default Hold Music File	The default value used by TS is "SystemDefaultMusicOnHold.wav?playlocation=mediaserver" **Note**: Handlers may override the hold music for any call by sett call attribute. CIC adds the ?playlocation=mediaserver by default. CIC uses th check boxes are selected on the Media Server General Configu Configuration.
DID Voicemail Workgroup	Use this server parameter to set workgroups members having call is placed to the DID number, callers hear the name prompt voicemail. Type the name of the workgroup to set this behavio
Director Support	You use Setup Assistant to configure a server as a Director Sup monitored server support, you can set this parameter to **0** and
DirectoryGrammarFileCall	Use this parameter to set the resource directory for Call gramn D:\I3\IC\Resources\CallDirectory.
DirectoryGrammarFileCompany	Use this parameter to set the resource directory for Company D:\I3\IC\Resources\CompanyDirectory.

DirectoryGrammarFileForward	Use this parameter to set the resource directory for Forward g D:\I3\IC\Resources\DirectoryForward.
DirectoryGrammarFileMessage	Use this parameter to set the resource directory for Message g D:\I3\IC\Resources\MessageDirectory.
DirectoryGrammarFileMO	Use this parameter to set the resource directory for Mobile Of example, D:\I3\IC\Resources\MODirectory.
e-FAQ Support	Set this parameter to 1 or True to enable the e-FAQ controls in default, this parameter is set to 0.
EnableDynamicStatusIconUpdates	This parameter protects network bandwidth by limiting when (icon after you change it. By default, all CIC clients will display the new status icon after t Set this parameter to Yes to enabled all logged-in CIC clients to status icon.
EnableSupervisoryRecordAndMonitor	Allows an administrator to turn on the hidden supervisory reco If the server parameter is set to Yes on the server, the CIC clien of Workgroup Queue Supervisor Monitoring or Recording. When this parameter is added or modified, all CIC clients need to become effective. By default, this parameter is set to No. **Note**: If you change the setting of this server parameter, Sessio to recognize the change. The change will not affect any interac progress until an update occurs for them. For more information, see Who can see and listen to recording
External Priority Voicemail	Set this parameter to Yes for an external caller to set the priori this parameter is set to No.
Generate CBO Statistics	**This parameter applies to CIC subsystems that use an Oracle c** **parameter will have no effect on CIC subsystems that use an S**

	Set this parameter to a value in the format 'HH:MM' with the t collection should run. Removing the parameter or clearing the running. On a large database, this can be a time consuming prc scheduled in off-time if possible.
Handler Path	Specifies the active handler storage directory on the CIC server
Held Call Timeout **(This server parameter is now a setting in IC server Telephony Parameters - General configuration.)**	**Obsolete as server parameter.** Specifies the number of second before TsServer signals an event. The minimum setting is two s setting is 900 seconds (15 min). By default CIC uses this event t the held call after 15 minutes. By default CIC uses this event to present the caller with an IVR allowing the caller to stay on hold, go to voice mail or re-alert t selected, the call will automatically be disconnected after the t Also, the call must be placed on hold by the user, not by the sy Agent is not a valid on hold state in this instance) .
I3Tables Path	Specifies the path for the location of table data used by CIC har data without this parameter. The default location on the CIC se \\ic\Common\I3Tables
IconPath	This value is set and used during IC server installation to deterr to create the shortcuts to CIC help files and applications. Do not change this value.
Ignore Dial String Leading Plus Sign	Set this parameter to True for CIC to ignore the "+" beginning a parameter is set to False.
Ignore Dial String Leading Slash	Set this parameter to False for CIC to acknowledge the "\" begi this parameter is set to True.
InitialMirrorDir	Specifies one or more directories on the active server to be mi when the CIC server starts, in addition to the default mirrored the list is separated from the next by a semicolon (;). If you want the directory mirrored recursively (including direct place a + in front of the directory name. For example: +D:\server\ic\ImportantDir Please refer to the *CIC Automated Switchover Technical Refere* mirrored directories.

Interaction Limit (Chats)	This is the maximum number of chat interactions that are allov given time. The default is 4000. This server parameter is dynamic, meaning that any change to If there are chat interactions in the queue when you set a new number is less than the previous maximum number, then the c currently in the queue will remain there. However, no new cha the queue until the number of chat interactions in the queue fa
Interaction Limit (Emails)	This is the maximum number of email interactions that are allo given time. The default is 10000. This server parameter is dynamic, meaning that any change to If there are email interactions in the queue when you set a nev maximum number is less than the previous maximum number, that are currently in the queue will remain there. However, no added to the queue until the number of email interactions in tl limit.
Internal Call Classifications	The default name of the phone number classification for calls v example, station-to-station calls) is Intercom. That classificatio Internal and work identically. CIC handlers look for the name(s) determine the name of the classification to use for dialing inter example, translate) the name of the Intercom classification, yo server parameter. This parameter is a comma delimited list of classifications that calls. The default value of this parameter is `Intercom,Inte` server install. Customers can add any classification, which has l Phone Number > Classifications configuration, to this list. (Our with `Intercom` as the internal call classification.) Any Classific will be treated as an internal call by the handlers that process r
Keep Internal Regional Calls On Server	Set this server parameter to Enable, E, Disable, D, Same Region can be completed as intercom calls rather than "out and back i PSTN.
Last Known Good Backup	D:\I3\IC\Backup\RegistryBackup_18-8-2011-825171
Mirror Exceptions	Specifies the extensions of any files that you do not want to mi

	extensions with a semicolon, for example: txt;gif;myext.
Mobile Office DID	This parameter adds capability to direct dial into Mobile Office When the user calls the DID, the ANI is recognized as a number prompted for the voicemail password for Mobile Office. By def Set>.
PlayUserPrompts	When this parameter is set to false, internal calls and transferr name and extension that is being called. PlayUserPrompts = True Prompts will be heard for all calls. PlayUserPrompts = False User prompts will not be heard on internal calls and calls trans just hear the phone ring. The default value for this server parameter is **false**.
Mobile Office ANI Pattern	Patterns are defined in the "Mobile Office ANI Pattern" server for digits along with any other characters as literals, so the patt would format 3178723000 as "+1 (317) 872 - 3000". Because the ANI may not be stored in the user's settings in the received, the tool will try to use the following patterns (in orde Any pattern specified using the "Mobile Office ANI Pattern" ser followed by: XXXXXXXXXX XXX-XXX-XXXX (XXX)XXX-XXXX (XXX) XXX-XXXX 1-XXX-XXX-XXXX 1-(XXX)-XXX-XXXX For this server parameter, the format should be a pipe | delimi pattern, X is the next available digit of the ANI, and any other c example, if the ANI is 3178723000, and the pattern is ABC-XXX- used for the search would be ABC-317-123-872-3000.
NewVMPollingInterval	This parameter determines the interval in time in seconds that

	server for unread voicemails for users. The default value is 240
OutofBandReportDataTransfer	This parameter enables Interaction Reporter reports that run c data from the database using a secure communication layer.
Play Queue Announcements	Set this parameter to External for user and extension prompts callers. Set this parameter to No for no prompts to be played.
Reco Call Type	This parameter should only be used by the direction of an Inter representative.
Recording Path	A packaged server parameter, pre-configured, which specifies t used to store uncompressed manually recorded calls. The path server installation. Interaction Recorder uses its own setting to **Location**. If you used IC Setup Assistant during IC Sever installation to con **Recorder Compressed Files Location**, the directory you specifie **Default Storage Location** Retention Policy. The **Default Storage Location** Retention Policy for compressed be modified using Interaction Recorder Policy Editor. For more *Recorder and Interaction Quality Manager Technical Reference* Documentation Library.
RecordServer	Enter the name of the recording server.
ReportComponentsInstalled	Used by various CIC systems to determine which type of report this value. Reporting is considered active when REPORTS is fou parameter. All references to the Report tab in the CIC clients ar considered inactive (when REPORTS is not found in the string o
ReportFilePath	Specifies the path to the report templates used to generate rep default value is \\${ServerName}\IC_Reports.
ResetCalledIDOnExternalTransfer	If the call is in the IVR and the call is blind transfered to a non-N Number/Queue then CIC will reassign the Cisco TAPI Call Attrib redirecting it to. This works well when CIC is acting as a front e Example: 1.) Call come into Main IVR (CalledID = 3000) 2.) CIC performs a blind transfer to another PBX at 3010. 3.) When the PBX gets the call. (CalledID = 3010)
ResetCalledIDOnTransferToUser	This reassigns the Cisco TAPI Call Attribute “CalledID” value to t

	any time a call is sent to a user through the alert tool step. Example: 1.) Call comes into Main IVR (CalledID = 3000) 2.) IC blind transfers the call to User logged into Station 7001. (3.) User then blind transfers to User logged into Station 7075. (
Resource Path	Specifies the directory on the CIC server used to store CIC reso cover pages, etc. The path is specified during the IC server insta

Rx Document Path	Response management document path on the server. Defaults `C:\server\IC\I3RxDocs` where C: is the install drive.
	Paths to create on the server:
	${Rx Document Path}
	${Rx Document Path}\users
	For example, if Rx Document Path = `C:\server\IC\serve` directories must be created:
	`C:\server\IC\server\i3rxdoc`
	`C:\server\IC\server\i3rxdoc\users`

Server Path	Specifies the home directory of the CIC system software. The p server installation.
ServerReportLogAutoN	Auto logging refers to the ability of statserver to receive its ow notification and then log the statistics to the database. Turn of handlers to catch this information and log it to the database. **T administrator use only.**
ServerReportLogDataDestination	This parameter replaces the ServerReportLogMSMQPath parar for CSV, RTM, and other transport types.
SNMPTrapEnterprise	This parameter tells the I3 SNMP Trap Monitor what SNMP tra values are **All**, **I3**, **ININ**, **Microsoft** (default), and **None**. The Trap these traps to Handlers.
Station Event Window Time	Station Event Window Time is the number of consecutive millis maximum number of station events (set in "Station Event Winc 60000 ms (60 seconds), with a minimum window of 10000 ms events occur within 60 seconds, CIC disables the station device

SupressAdsiCallDetailLogging	ADSI calls are not normally seen on the queues, and cannot be if they should some how end up on the queues. After you install this optional parameter, you may use it to con Set the parameter to T, TRUE, Y, YES, or 1 to suppress logging A Set the parameter to F, FALSE, N, No, or 0 (Zero) to log ADSI ca The default setting for this feature is Yes. You should not chang
SwitchAddress	If the Switchover system uses a Dataprobe device with an Ethe parameter specifies the IP address.
SwitchComPort	If the Switchover system uses a Dataprobe device with a serial parameter specifies the COM port. **Note:** This server parameter is installed by default, but is not r
SwitchMACAddress	This parameter specifies the MAC address of the Ethernet cont device.
Switchover UDP Initial Ping Delay	Specifies the time in seconds that Switchover on the backup se to listen for datagrams from the active server. Acceptable valu seconds. The default value is 5 seconds.
SwitchoverServer A	The name of the Switchover server designated as the initial act come up as active first and will remain so until the first Switcho system uses a Dataprobe device to switch lines, this is the serv **Note:** This server parameter is installed by default, but is not r
SwitchoverServer B	The name of the Switchover server designated as the initial bac come up as backup first and will remain so until the first Switch system uses a Dataprobe device to switch lines, this is the serv **Note:** This server parameter is installed by default, but is not r
SwitchType	The type of switch control used between the two Switchover se If the Switchover system does NOT use a Dataprobe device to s None. (SIP/AudioCodes, and Cisco TAPI systems do not use a D If the Switchover system uses a Dataprobe device, set one of th on the type of control card: SerialCP8, SerialK16, EthernetEPAL the Automated Switchover technical reference for information control cards.
Temp Path	Specifies the temporary file storage location on the CIC server.

Toll Call Classifications	This server parameter is used for setting Forced Authorization installation with these values: Long Distance;International;Unk Additional phone classifications can be added as values, or the **Tip**: See How Do I Set Up Forced Authorization Codes?
Unified Messaging	This server parameter is set to 1 during the IC server installatio messaging options was selected (such as Microsoft Exchange o Interaction Administrator can configure all mailboxes for user, unified messaging option was selected during installation, this zero. In this case, Interaction Administrator will not attempt to Domino server, and the Mailboxes dialogs will not work for use
Use Enhanced Regional Dial Plan	Contact a PureConnect Customer Care representative for infor parameter.
Use ICMS for AdHoc Conferences	Set this server parameter to Yes for Interaction Conference Me conferences instead of a Media Server. By default, the parame
Use Outbound Base Call For Connection	This parameter should only be used at the direction of a PureConnect
Use Network Echo	The CIC client's listen feature allows authorized users to listen listener can hear both the agent and the external caller via tele cases, the listener may be able to hear the agent but not the e change the value of Use Network Echo to 1, which dynamically the network to listen to the remote party.
Voicemail Maximum Duration	Set this parameter (in minutes) to pass the value to the Record the default values. The default length of voicemail recordings in the shipping hanc minutes), and the default length of the voicemail recordings by 600 seconds (10 minutes). You may want to set an arbitrary va settings, for this duration. For more information on the Record Audio toolstep, see the In
Web Event Image Path	/i3webimages/
Work Path	Specifies the location of a working directory used by the fax an

	store intermediate copies of faxes and voicemail.

Related topics

Automated Switchover System Server Parameters

Dialer Server Parameter

e-FAQ Server Parameters

Optional Server Parameters

Packaged System Parameters

Text To Speech Server Parameters

Optional General Server Parameters

The following general server parameters are optional.

To set these server parameters, add the parameters in the **Server Parameters** container. Then set the values as necessary.

Optional Server Parameter	Description
ACDAgentLockTimeout	This parameter determines how long the agent will l toolsteps are not called for the agent. Without this parameter the ACD agent lockout time
ACDAvailableOnNon-ACD	Use this parameter so that agents are available for A unavailable, the agents must set their status to a no Yes, 1, true,etc., to enable it. Without this parameter, or if there is no value enter when on non-ACD interactions. For similar email-specific actions, see the ACDAvaila
ACDAvailableOnNon-ACDEmail	Use this parameter so that agents are available for A creating a new email from Interaction Desktop, or re must set their status to a non-ACD status. Set the pa enable it. Without this parameter, or if there is no value enter when on non-ACD email.

	This parameter is similar to the ACDAvailableOnNon
ACDConsiderSingleTypeForEWTAvailable	Use this parameter for ACD Queue Statistics to comp interaction type. Possible values are: • call • chat • callback • web collaboration • instant question • sms message • email • generic Note: Enter only one interaction type. This parameter is useful if you want to route a partic unavailable due to being on other interaction types forces a single type of interaction to agents when ot interaction.
ACDDisableOnHold ProcessingForCalls	A non-blank value turns off "on hold" processing for Agent's utilization "score."
ACDDoNotDelete ObjectsUntil Deallocation	Currently, ACD skills are lost when calls are transferr until the call is deallocated from the system before c ACDDoNotDeleteObjectsUntilDeallocation=1
ACDInteractionLockTimeout	This server parameter determines how long the interaction will be locked if the "Select agent" or "Re interaction. Without this parameter the ACD interaction lockout
ACD Recorded Workgroups	This is an optional parameter that was added for EIC modifying handlers. This parameter will work with C workgroup names (not the fully qualified queue id, c workgroups existed Marketing, Support and Sales th automatic recording on for those two workgroups. T Automatic recording is off by default for workgroups workgroup’s Configuration tab in IA. This does not a
Additional Redaction Expression	This parameter allows you to either append text to t

	default filter expression. To append text to the default filter expression: Add the Redact Using Default Expression server para Add the Additional Redaction Expression server para To replace the default filter expression: If you added a Redact Using Default Expression para Add the Additional Redaction Expression and specify
Allow Multiple Calls to Station On Deferred Answer Line	If the **Allow Deferred Answer** SIP line option is enab whether an additional call alerts the station. To enable the alert, set this parameter to **T**, **True**, **Y**, additional call, an additional call alerts the station ev To disable the alert, set this parameter to a value ot additional call does not alert the station.
Allow Full Custom Headers	Use this server parameter to allow the use of custon headers). If you do not set this parameter to "Yes", y this parameter is not present, so you must create it a
AllowScripterToBypassStatusCheck	To allow Scripter to be exempt from status change a If you do not add this server parameter, then errors arises: The agent's status in the User container indicates th The user's has the View access control rights for the The agent goes on break but leaves his or her status Scripter cannot set the agent's status to "Do Not Dis
Allow Voicemail Save As	Use this server parameter to conditionally show or h CIC clients. By default, the menu option is available (
Allow SNMP Process Restarts	If you use SNMP monitoring/management tools to m stop/restart processes via SNMP, create this server p parameter is disabled (is not listed in the server para

Attendant System Profile	Attendant System Profile designates which Interacti the star (*) key after going off hook. See the Interact
AutoAddUsernameCategory	This server parameter adds a category to each user 0: Feature is turned off. 1: Feature is turned on adding a suffix of "-auto" to t <any other value>: Feature is turned on adding a suf For example, if set to "1", user JeffS would result in a would result in a category of JeffS-Director. Blank or <null> values are not supported. This param changes are not dynamically updated in ACD Server, parameter, requires a restart of the ACD Server.
AutoSortWorkgroupOverview	To enhance performance, IC Business Manager no lo that view, add the AutoSortWorkgroupOverview ser
BatchSaveSalesforceCallLogs	Use this parameter to configure the way the Salesfo Salesforce saves attributes in an iterative method, o • Set the parameter to 1 to save all custom pa • Set the parameter to 0 (which is the default) Notes: Setting this parameter to 1 to save all parameters at saves will fail. Otherwise, if there is no errors, the sa log in again to Salesforce to save the change in beha
BridgeHostTrustedSites	Use this parameter to provide BridgeHost with a list located almost anywhere, including outside of the fi By default Session Manager only trusts connections connections in a 3 second span from clients on a diff connections. Enter values in the following pipe-delimited format: <IPAddress>|<IPAddress>|....
Call Analysis Language	CIC can provide language specific call analysis based parameter and the value is not specified here, call an Enter the language value such as "en-US". The value name located in the [drive]:[install folder]\IC\Resour language folder "bg-BG" or "de-DE". For more information on Call Analysis, see Media Se

Call Forward Analysis Mode	This server parameter affects the "SystemIVRFollow The possible parameters values are: •DEFAULT (default settings) •CA_DISABLE (disable Call Analysis) •VM_DISABLE (disable VM Analysis) •FULL_DISABLE (set both to false) If you set this parameter to "FULL_DISABLE," then CI agents who have selected either the Follow-me statu immediately.
Call History Max Size	Use this parameter to set the number of calls per us default value is 300.
Call History Max Time	Use this parameter to set the time in hours to save t clients. The default value is 72, meaning the call hist of calls is reached (See Call History Max Size).
Callback Interaction Recovery Enabled	Create this parameter and assign a non-zero value to server parameter is available in IC 4.0 SU3 and later
Chat Interaction Recovery Enabled	Create this parameter and assign a non-zero value to server parameter is available in IC 4.0 SU3 and later
ClientDirectoryPageSize	Use this parameter to specify the number of directo interface is being used. The default value is 25.
Confirm Station Connection	Enabling this sever parameter sends an `eCallEve` can be intercepted and handled by the ConfirmStati tool step. This allows the User to intercept a remote handler. Valid values are: `true`, `yes`, `false`, and `no`.
ConnectionCache.ODBC.Timeout	This server parameter provides a way to explicitly se You can use this parameter to fine tune the perform seconds.
Continue to Monitor Calls After Transfer	This server parameter provides the option for an Int the call is transferred away from the monitored ager away from the agent. To enable this option, set the p about continuous monitoring, see "Monitor Agent, S Supervisor Help.

CustomOnHookNotification	
DefaultSpeedDialPageSize	If MaxSpeedDialPageSize is not defined, CIC uses thi directory records to display in a Speed Dial view. For
DialByNameExten sionLength	Defines how many characters can be used in searchi Companies with large directories can extend the def search results.
DID Ringback Only	If you do not like the current voice prompt that plays the change, create this server parameter with one o case sensitive. To use a custom .wav, set the value t 'DID_CustomRingback.wav' located in the Resources Note If you use this server parameter some Fax syst other indication of answer before sending a fax tone
DirectoriestoCacheOnSMStartup	Lists the directories that Session Manager will cache Directory are cached upon the first request.
Disable Related Interactions	In case of system degradation due to rapid multiple mechanism was put into place. In order to shut off a interactions emergency shut off server parameter, a As long as this server parameter exists with the spec from any clients. This will NOT disable the interactio Note: The related interactions feature is only availab check during the Tracker plug-in initialization to see Oracle database is detected, the related interactions interaction history are available for Oracle as well as
DiscardFailedFax	Note: This server parameter is not used when Media - Fax Server. Use this server parameter to disable delivery of part faxes are discarded. The value is 0 by default, and pa
Don't Allow Users To Delete Recordings	Enter this parameter to turn off the ability for users of this parameter turns off the ability to delete recor
EmailEditor	This parameter determines which editor agents use appears as a toolbar of formatting options. • To use the Telerik editor, set this parameter • To use the MSHTML editor, set this paramet

	- To display the CEF (Chromium Embedded Fr For more information on how agents use the editor, Documentation Library. Note: This parameter affects all users of Interactio other. In Interaction Desktop, the MSHTML editor available for the Email Preview view and Editor vie Help. Important: If you configure the CIC clients to use the unavailable. If users had the Email Editor or Email Pr closed. In order to get these views back you would h this is done the user can re-add these views or you c
Email Admin User	When listening to voicemail messages remotely or th number to a Display Name in the system, then reads then the system reads the phone number that the call is from. If the call is from an external number, th Use this parameter to show the external number (re .Set the value to a CIC user name or the display nam
Email Stream	This parameter allows a voicemail opened from Exch rather than copy the entire contents of the message CIC server might be in one location and the Exchang turn on this parameter.
Enable CaaS Speech Billing	For PureConnect Cloud customers only. This parameter determines whether the system pro Speech (ASR/TTS). If this parameter is set to True, th PureConnect Cloud billing system, IC billing The default value is false.
EnableEnhancedTTS	Interaction Text to Speech (ITTS) supports enhanced better caller experience. These models, trained with Germany), en-AU (English, Australia), en-US (English (Dutch, Netherlands), and ja-JP (Japanese, Japan). Starting with CIC 2018 R2, Media Servers use enhanc models. If a Media Server connects to multiple CIC s environments for example), calls on all environment updated with CIC 2018 R2. DNN models slightly increase processing and memor heavy use of text-to-speech, or you have Media Serv to use GMM models instead. In a future release, the

	The EnableEnhancedTTS server parameter is not cre DNN models to use older GMM models. To use GMM 1. On each CIC server that connects with your I EnableEnhancedTTS server parameter. 2. Set the value of the parameter False. After t you do not need restart the Media Server. If you change your mind, you can switch back to DNI True on each CIC server. When opting in, you must r
Enable Media Server Call Analysis	When this setting is enabled (set to "1" or "true"), ar box is selected, call analysis is turned on. when turne Type drop-down list on the SIP Line Configuration pa option will disappear and the Interaction Media Serv
EnableSSOConfiguration	To activate the Single Sign-on Configuration Utility p default value is False. The Single Sign-on Configuration Utility plug-in simp mechanism for your Interaction Center Server. For m Utility plug-in, see the Identity Providers Technical R
ErrorOutIfT38ReinviteIsNotSupported	Create this parameter and set to "true", to help prev For more information, contact your PureConnect Cu
External Pick Access Codes	(Value = a list of any strings, separated by a semicolo converted to their key pad equivalent so it can be co attribute is set, then external callers must enter this outside call. External callers can pickup held, parked be used in a scenario where a user can use a cell pho meeting and Sarah came and said she parked a call o and pickup the call.
Fax Header "From" String	Set this parameter to the appropriate replacement f
Fax Header "To" String	Set this parameter to the appropriate replacement f
Force 200 Response For Delayed Media Remote Initiated Unhold	This server parameter applies to customers using ph connections and that are connected to a CUCM. The remote stations cannot resume the persistent conne regular ongoing call. The calls are dropped instead. To remedy this problem, create this server paramete
Force Message Button Password Only	Set this parameter to Y, Yes, T, True or 1 for users to voicemail access code when using the message butto

	station or have the station set as the default worksta
Generic Parameter with Replaces	Cisco Series 7960 Customers: To make the Call Reco this parameter to True. The default value is False.
Global Remote Message Limit	This parameter limits the number of messages enum value is given, it overrides other email settings and is to zero, it will return all messages. NOTE: Beginning in 2.3, the message limit is set glob server parameter for backward compatibility issues, container instead. The Mail setting takes precedenc
HDSI Switchover	This server parameter informs TsServer that the HDS be set to: true, yes, no, or false. The default value is
Honor User Language	Set this parameter to Yes or True to recognize the us Interaction Administrator. For example, a CIC server may have users in multiple presented in UK English, while a German user's voice Based on this server parameter, CIC sets the languag server parameter is not enabled, the default behavi
ICRenderServerHost	After you run the IC Render Server setup, create a se and type the name of the computer running IC Rend
Immediate Socket Operations	This is an optional general system parameter for TLS or TLS connections during times of high call volume, TCP connections and disconnections. The default val
Include Fax With Notification	Set this parameter to Yes, for all users that are setup attachment to the fax notification email. The default
Include VM with Notification	SystemNotificationsProcessor uses this parameter to voicemail notification. It only affects the client config
INDEPENDENT_STATION_TIMEOUT	If you select the Prevent station logout on navigation you can set this parameter to a number of minutes. Salesforce Integration when CIC does not detect any information,see the PureConnect for Salesforce Inte Note: To enforce a timeout, CIC requires both this pa setting. This parameter does not affect Interaction C 2017 R3 Patch 8 or later.

Interaction Conference Support	This server parameter is created by the Interaction C presence of this parameter signifies that the Interact
INTERNAL_USER_PIC_URL	This parameter enables the Company Directory shor for each user. Set the value to http://intranet.yourco example value with actual valid URI pointing to imag currently selected user's ID into the URL string.
INTERNAL_USER_LOCATION_PIC_URL	This parameter enables the "Office Location" feature in the Company Directory. When selecting Office Loc value to http://intranet.yourcompany.com/offices/{ valid URI pointing to images. The string formatting p into the URL string.
IR Disable Social Snippets When Recording	Snippets for social interactions are always enabled b "True", snippets will be disabled for social interactio
IR Search Unique Tracker Joins	This optional server parameter controls the number search is run that includes the search attributes Date When this server parameter is set to 1, in addition to recordings are also returned for participants whose
ISDN Inband Dial Enabled	Add this parameter and set the value to True to ena code to be dialed inband.
IWPCallMonitoringOperationTimeouts	Add this parameter to specify timeout values in milli operations, type the value in milliseconds. For exam different types of call operations, use a pipe | delimi eSTART_MONITORING|eSTOP_MONITORING|eDISC Note: If you do not set this parameter, then the defa
IwpLdapSyncFrequency	Add this parameter to control how frequently IC syn order for the parameter to take effect. The default is Notes: In earlier CIC releases, the LDAP sync frequency defa version, CIC will continue to use the sync value you s configuration are automatically created with a 5 sec
IVRReportingTransactionBatchCount	Add this parameter to designate the batch count for Prior to 2015 R3, all IVR tracing transactions were se and reduced throughput. When this parameter is en

	batch has the number of transactions defined by thi To disable transaction batching, set this parameter t The default value is 100.
IVRReportingTransactionDelayMilliseconds	Add this parameter to designate the delay in millise results in a throttling of transactions when the numb To prevent this delay from being used, set this paran The default value is 5000.
IVRReportingTransactionDelayThresholdSeconds	Add this parameter to designate the threshold in sec tracing transaction. If the transactions exceed this threshold three conse IVRReportingTransactionDelayMilliseconds paramete If subsequent transactions are under this threshold f IVRReportingTransactionDelayMilliseconds paramet To disable the automatic throttling mechanism, set t occur every time. The default value is 10.
Leave Dynamic Calls Connected on Shutdown	Add this parameter and set it to True to keep dynam value is True. Note: For development and test machines, set this p
Mail Interaction Recovery Enabled	Create this parameter and assign a non-zero value to server parameter is available in IC 4.0 SU3 and later
Mail Maximum Interactions	Add this parameter to specify the maximum number one time. This is not a typical situation, but for exam
Max T.38 Datagram Size	This parameter allows you to configure the max data If the server parameter is undefined or set to -1, the You can specify any positive value up to the maximu for all fax sessions. The recommended value is 150.
Max Cover Page Size	This parameter determines the maximum size of a c is 10,000 KB. If the cover page for a fax exceeds the
MaxDirectoryStatusWatches	Add this parameter and set the value to a number to before the interface changes to a paged interface.

MaxQualitySearchResultsICWS	Use this parameter to specify the maximum number Connect My Quality Results view. If you do not define MaxQualitySearchResultsICWS,
MaxSpeedDialPageSize	Use this parameter to specify the maximum number parameter works in conjunction with DefaultSpeedD • If you do not define DefaultSpeedDialPageSi greater than MaxSpeedDialPageSize, the nu • If you define only DefaultSpeedDialPageSize DefaultSpeedDialPageSize. • If you define both MaxSpeedDialPageSize ar contacts is less than or equal to MaxSpeedD returned. If greater than MaxSpeedDialPage returned. • If you do not define either MaxSpeedDialPag contacts returned is less than or equal to 25
Maximum Ringing Calls per Second	Add this parameter to limit the number of station ca Note: If you are using workgroups that are configure stability. By default, there is no limit.
MaximumHttpSessions	Add this parameter to specify the maximum number the maximum threshold is reached, any subsequent under the limit. Note: This limit is per Session Manager and not the The default value is 1000.
Non-silence Timeout	When using Media Server, set this parameter to spe no silence is detected. If this parameter doesn't exis The value of this parameter should be greater than t parameter, otherwise, the timeout occurs before sil
OnPhoneDoes NotChangeTime InStatus	Set this server parameter to prevent users' "Time in not want their status to change). To enable, set the value to true. To return to the previous behavior, set the value to
Outlook Data Source	This server parameter is used by handlers for Data M Mobile Office. The name of the parameter is the san

	Source Configuration. Parameter value: <the data source name for outlook
PAS_usev2	Set this parameter to True, Yes, or 1 to use Process A Automation Server version 1 by default. This parameter was deprecated in 2018 R1.
PAS_blockLaunchDuringRestore	Set this parameter to True, Yes, or 1 to have Process until it finishes restoring previously-existing flows.
PAS_HandlerResponseTimeout	Use this parameter to specify the number of second Handler action if it does not execute successfully. If t seconds. If the server parameter's value is 0, then th Note: Only processes migrated from Interaction Proc Interaction Process Automation 4.0, you can configu
PAS Maximum Monitored Flows	This server parameter determines the maximum nur workspace in IC Server Manager. You can use it to re much data. Set this parameter to any value to overri allowable value is 100.
PAS_UseOldDroplist	When enabled, this parameter allows users to quick
Play Queue Announcements	This server parameter applies to non-DID calls (value • Neither (N) - Neither internal or external cal • Internal (I) - only internal (intercom) calls wi • External (E) - only external calls hear queue not set or set with an invalid value) • Both (B) - both internal and external calls he Note DID calls: Queue announcements are different number is called (only accessible from an external, in Queue Announcementsfor more information.
Prevent Multiple Proactive Recordings	Set this server parameter to True to prevent multipl
ProblemReporterPath	Use this server parameter to specify the local path to <ICservername>\I3\IC\ProblemReporter\<CIC client Reporter.

ProcessIVREvents	Set this server parameter to True to enable IVR tool
Provision Auto-Provisioning Enabled	Set this parameter to No to disable the auto-provisio displays a Setup label. It allows the phone to be asso of the need for the MAC Address to be entered into the provisioning server is required to make this setti
Provision FTP Enabled	This parameter allows you to enable FTP on the prov If the value is anything other than "Yes"(case in-sens present, the default behavior is FTP enabled. Note: The provision server must be restarted after a effect.
Provision HTTPS Mutual Authentication	Set this parameter to Yes and enable Use HTTPS Alw authenticates the IP phone, and the IP phone authen signed by the Default Lines Certificate Authority A re take affect. For more information, See IC Managed I Documentation Library.
Provision ISS Manual VLAN ID Enabled	For more information, see Managed IP Phone Advar
QPSReportingTransactionBatchCount	Add this parameter to control the batching of the qu Stat Server at every interval. To reduce the StatServer CPU usage, reduce the bat large PMQ files could become backed up on the hard To increase the StatServer CPU usage, increase the b processing and reduces PMQ file backups if they bec The default value is 100.
Redact Using Default Expression	This parameter allows you to filter most credit card email messages. These numbers are replaced with m information. By default, masked numbers appear as “########## See also the Additional Redaction Expression and Re
Redaction Replacement Text	This parameter allows you to specify the how maske Optionally use this server parameter with the Redac Additional Redaction Expression server parameter.
Reject T38 If Multiple Media In INVITE	Some SIP carriers offer SIP INVITE messages with mu

	(voice) and T.38 (fax). When this server parameter i portion of these INVITE messages while acknowledg Note: This server parameter does not affect SIP REINVITE r
Remote Station Call Analysis Answer Supervision Interaction Center	Call analysis should terminate as soon as a call conn beginning in IC 4.0 SU3. To revert to the previous be
RemoteEmailFormLimit	This server parameter limits the number of email for includes the Email Window for Incoming Messages a parameter applies only to CIC clients in a Citrix or Te disable the limit, set this parameter to -1.
ResetCalledIDOnExternalTransfer	This server parameter is a feature for customers tha for voice mail. When this parameter is set to 1 or Yes (enabled), if a (EXTERNAL) CIC Directory Number/Queue, then CIC value it's redirecting it to. This works well when CIC Example: 1.) Call come into Main IVR (CalledID = 3000) 2.) CIC Blindtransfers to another PBX at 3010. 3.) When the PBX gets the call. (CalledID = 3010)
ResetCalledIDOnTransferToUser	This server parameter is a feature for customers tha for voice mail. When this parameter is set to 1 or Yes (enabled), the "CalledID" value to the destination Directory Numbe step. Example: 1.) Call come into Main IVR (CalledID = 3000) 2.) CIC Blindtransfers the call to User logged into Sta 3.) User then Blindtransfers to User logged into Stati
Rx Tree Init Collapsed	This server parameter gives users the option (on the Management nodes open or closed when accessing Set the value to 1 for the nodes to be collapsed initia

SAPI DSCP Value	If the PureConnect QoS driver is not installed, Intera through VoIP calls. Enter "0x0" to represent the Diff inserted in RTP packets of VoIP interactions. The DSC there is a specific need to do so.
Screen Record Delta Frame Count	This optional server parameter controls the number Recording. Increasing this value effectively decrease For more information, see Interaction Recorder and PureConnect Documentation Library.
Seize Deactivated Lines	This parameter applies to analog lines. When present and set to a value of "true" or "yes", t not configured as active in Interaction Administrator lines to receive a busy signal. Note Values are not case sensitive.
Send FBMC Call Recordings To Notification Address	Set this server parameter to Y, Yes, T, True or 1 to ha fax notification email address as configured in CIC cli False, or disabled.
Send MWI to PBX	Set this parameter to Yes to send MWI to non-CIC st
Send Status Forward Notification	Set this parameter to Internal, External, All or None an email notification if the user is in a forwarding sta
Server A Address	Specifies the alternate IP address of SwitchoverServe
Server B Address	Specifies the alternate IP address of SwitchoverServe
Show Legacy Res Mgt	Legacy response management containers (Interactio displayed unless they contain legacy information. Use this parameter to display the legacy containers (Set the value to "1" to display the legacy containers. "No", then the legacy response management contai information.
Single-Sided Monitor	This parameter allows you to listen to both sides of a sides. If the server parameter is set to 1, monitoring will on you are short on conference resources, but in genera parameter to 1 is you save conference resources. In

	monitored call.
SIP Phone Information Update	Enter this parameter and set the value to "1", "yes", and Model information, and MAC address for Polyc registration process. This server parameter is helpfu
Split E-1 Support	A value of 1 tells TS to turn on Split E-1 support. You Configuration dialog when creating a new line. Your choices will include: <Not Split> E & M FXS Loopstart
Split T-1 Support	A value of 1 tells TS to turn on Split T-1 support. You Configuration dialog when creating a new line. Your choices will include: <Not Split> E & M FXS Loopstart
StatServer_AlwaysTrackACWForLastACDInteraction	After an interaction is disconnected for an agent, the (After Call Work). By default, Stat Server only adds a statuses within the first two minutes post-disconnec workgroups, add this server parameter and set it to Interaction data (created by the Tracker subsystem) manual status that was started during the two minu
StatServer_CombineConsecutiveAcwStatus Changes	If set to True, CIC combines consecutive ACW status
StatServer_SendQPSNotification	You can create the StatServer_SendQPSNotification the Queue Period Initiator handler to generate a not amount of user or workgroup data, the notification some cases, the Notifier service terminates. For this
StatServer_UseTotalInteractionCountForServiceLevelCalculations	When enabled, Stat Server calculates the service lev the default calculation is Target Answered / Total Ar
Station Pickup User Validation	(Value = Yes) - If this attribute is set, users must ente other than their own. Users only have access to the This parameter requires that the user identify thems logged into.

Stop Recording T38	Use this parameter to automatically stop the proact IC Server automatically enables the proactive record time when the call is switched to a T.38 fax call, you parameter is not enabled, inbound and outbound fa By default, this parameter is disabled.
Stutter Tone	If you create this server parameter and give it any no contains unheard voicemails. If you want to change the tone, it can be edited in Sy
SupervisorViewSuspendDelay	Use this parameter to tell Supervisor how long (in se are suspended. This parameter is queried at startup. Supervisor must be restarted to apply the change.
SupervisorMaxActiveInvisibleViews	Use this parameter to tell Supervisor how many invis parameter is queried at startup. If the parameter val restarted to apply the change.
SuppressForwardingAnnouncement	Currently, for "available, forward" calls, the prompt hold music) is played. If you do not want this promp the call is being forwarded and connected. To suppress the prompt, add this server parameter v case sensitive).
Switchover NetTest A	For use with Switchover in WAN environments. Appl Switchover NetTest A specifies the name or IP addre SwitchoverServer B. It is used by the Switchover pro backup server. Whenever a failure condition is detected, Switchove this IP endpoint found on the same network segmen endpoint, it will assume the active server is still oper Important: Since Switchover no longer has a networ an error to the event log and shut down processing. monitoring and replication to resume. Recommendation: The value for Switchover NetTest to SwitchoverServer B from SwitchoverServer A.
Switchover NetTest B	For use with Switchover in WAN environments. Appl Specifies the name or IP address of a machine on the by the Switchover process on SwitchoverServer B wh Recommendation: The value for Switchover NetTest

	to SwitchoverServer A from SwitchoverServer B.
Switchover NetTest Timeout	For use with Switchover in WAN environments. Appl Used with Switchover NetTest A and Switchover Net seconds) that Switchover should wait for the ICMP e
Switchover Monitoring	For use in Interaction Director Switchover systems. A Director configurations, instead of Telephony Service parameter to "IP".
Switchover IP Retry Delay	For use in Interaction Director Switchover systems. V effect as Switchover TS Failure Retry Delay.
Switchover IP Timeout	For use in Interaction Director Switchover systems. V effect as Switchover TS Timeout.
Switchover UDP Monitor	Allows UDP (hearbeat) monitoring to be disabled. Cr a failure occurs, file replication is in an unknown stat Switchover monitoring and replication to resume.
Switchover UDP Maximum Ping Delay	Specifies the number of failures (failure count increa on the backup server will tolerate before initiating a Switch The default value is 5 seconds.
Switchover TS Timeout	Specifies the number of seconds that Switchover wil active server before signallng a TS failure. The value seconds.
Switchover TS Failure Retry Delay	Specifies the number of seconds Switchover will wai Services (TS) ping before retrying a TS ping. A second greater than 0 seconds. The default is 1 second.
SwitchMACAddress	Specifies the MAC address of the Ethernet control ca
Switchover Ping on Aux Connection	Set this parameter to Yes or 1 to move the TS ping fr Note: To enable QoS on the ping on the auxilary con the Switchover Ping on Aux Connection and the Swit on ping if only Switchover Use Qos For Ping paramet
Switchover Use Qos For Ping	This parameter allows customized use of QoS for the of ping (echo request and echo reply) packets. Set th

	Further customization can be made using Switchove QoS Value 8021, each described below. Note: To enable QoS on the ping on the auxilary con the Switchover Ping on Aux Connection and the Swit on ping if only Switchover Use Qos For Ping paramet
Switchover QoS DSCP	When Switchover Use Qos For Ping is enabled, set this parameter to set the value in the QoS byte. I significant bits of a packet. You can use DSCP to prio Note: To enable QoS on the ping on the auxilary con Connection and the Switchover Use QoS For Ping pa Use Qos For Ping parameter is enabled.
Switchover QoS Token Rate	When Switchover Use Qos For Ping is enabled, set th switchover. Note: To enable QoS on the ping on the auxilary con Connection and the Switchover Use QoS For Ping pa Use Qos For Ping parameter is enabled.
Switchover QoS Value 8021	When Switchover Use Qos For Ping is enabled, set th (priority levels in both RTP and RTCP packets) for the Note: To enable QoS on the ping on the auxilary con Connection and the Switchover Use QoS For Ping pa Use Qos For Ping parameter is enabled.
Tone Location	Use this server parameter to set the global signaling by handlers. Entering a value does not change the si and users will hear during calls so the tones are mor User and station settings can be changed by configu Possible values: Belgium France Germany Israel Italy Japan Norway Singapore

	SouthKorea Sweden Switzerland Taiwan TheNetherlands UnitedKingdom UnitedStates Notes: Internal alerts are controlled by the global se internal alerting since the context of the tone is tied controlled by the server parameter setting only. Ringback for outbound calls to delayed answer devic ringback, set 'Ringback File' in Telephony Parameter calls on a SIP line that is configured to use Delayed M
Track Abandoned Dialer Interactions in InteractionSummary	Beginning in 2016 R1, Interaction Dialer calls with a summary table. To re-enable this behavior, add this After you enable or re-enable this parameter, Intera you must do one of the following: • Modify an item under Items tracked in Intera Items Tracked configuration (Interaction Tra changes. You then can re-check (enable) tha Or... • Restart Interaction Tracker - we recommenc
TreatEndpointIdleAsFullIdle	By default, CIC disconnects a call when both endpoir on Disconnect Time. If you want CIC to disconnect ca create this parameter and set to "On", "True", or "Ye in the PureConnect Documentation Library on the Cl
TS Remove From Workgroup Conference Logic Active	This server parameter was added to make conferenc for transfers. The default is set to TRUE. If you set the value to FALSE, the function will be res where a workgroup call transferred from a three-par transfer, and the call stays on the workgroup (even v the system).
UseDNISStringComparison	This server parameter determines how the DNIS of a • Set this value to 0 to evaluate the DNS numb

	• Set this value to 1 to evaluate the DNIS num ○ The DNIS starts with leading 0's (for ○ The value of the DNIS is greater thar When the DNIS is evaluated as a stri 000153 is used instead of 53. In the because any value greater than 2^3 Note: Changes to this parameter do not take effect u
UseExternalTranProviderForPurging	Use this parameter to avoid a five-minute timeout tl To prevent restarting the PureConnect service when Microsoft SQL Server command line tools or the Ora
UUI Headers Copied in REFER	UUI information is sent via a BlindTransfer or a Cons duplicated the UUI information in the transferee's R from CIC 2016 R1. If you want to duplicate the UUI information in the t true. Note: The standard technique of forwarding UUI info the Refer-To address URI. The default value is false.
Waiting Call Indication	Call waiting is enabled out-of-the-box. The default fo Use the Waiting Call Indication parameter to globally to disable call waiting with one of the following valu
Workgroup Alert Users On Calls	Set this parameter to T (true) to alert users on calls f alerts. The default value is F (false).
Workgroup Distribution List Behavior	Set this parameter to True, Yes, or 1 to make a work members. When this server parameter is enabled, voicemail m the workgroup members. The workgroup can not ha feature to work correctly. See “Set Up Voice Mail Dis help for more information.

Related topics

Packaged Server Parameters

Automated Switchover System Server Parameters

Dialer Server Parameters

E-FAQ Server Parameters

Server parameters for IC Business Manager Views

Text To Speech Server Parameters

Automated Switchover System Server Parameters

The server parameters for the Automated Switchover System affect how interactions are handled when a switchover occurs. The following table lists the *optional* Switchover System server parameters that you can set. For information about the required Switchover System server parameters, see *Packaged Server Parameters*. For more information about the Automated Switchover System, see the *Automated Switchover System Technical Reference* in the PureConnect Documentation Library on the CIC server.

Automated Switchover System Server Parameter	Description
Callback Interaction Recovery Enabled	To enable switchover support for callback interactions, add this parameter and assign it a non-zero integer. This server parameter is available in IC 4.0 SU3 and higher releases. By default, this parameter is set to "0" or "Off."
Chat Interaction Recovery Enabled	To enable switchover support for chat interactions, add this parameter and set it to "Yes" or "1." This server parameter is available in IC 4.0 SU3 and higher releases. **Note:** CIC does not support SMS resiliency when the Chat destination option is selected. By default, this parameter is set to "0" or "Off."
Custom Upgrade Attribute Exceptions	For information about this server parameter, see the *Automated Switchover System Technical Reference* in the PureConnect Documentation Library.
Custom Upgrade File Synchronization Directories	For information about this server parameter, see the *Automated Switchover System Technical Reference* in the PureConnect Documentation Library.
Custom Upgrade File Synchronization	For information about this server parameter, see the

Exceptions	*Automated Switchover System Technical Reference* in the PureConnect Documentation Library.
Custom Upgrade Synchronization Directories	For information about this server parameter, see the *Automated Switchover System Technical Reference* in the PureConnect Documentation Library.
ForceSwitchoverFQDNs	This parameter enables the Switchover system to override the system-generated names for the switchover pair, which it automatically resolves. When this parameter is set to "Yes" or "1," the Switchover system instead uses the names that the system administrator specifies in the SwitchoverServerFQDN A and SwitchoverServerFQDN B server parameters. **Note**: If this server parameter is missing or disabled, then Switchover will try to automatically resolve the FQDNs from the NetBIOS.
Mail Interaction Recovery Enabled	To enable switchover support for email interactions, create this parameter and assign it a non-zero value. This server parameter is available in IC 4.0 SU 3 and later releases. By default, this parameter is set to "0" or "Off."
Server A Address	To specify the IP address of the dedicated Switchover NIC on SwitchoverServer A in a dual or multiple NIC configuration, add this parameter. When Server A Address and Server B Address are set, the Switchover system uses these addresses exclusively to direct its traffic.
Server B Address	To specify the IP address of the dedicated Switchover NIC on SwitchoverServer B in a dual or multiple NIC configuration, add this parameter. When Server A Address and Server B Address are set, the Switchover system uses these addresses exclusively to direct its traffic.
SMS Interaction Recovery Enabled	To enable switchover support for SMS interactions, add this parameter and set it to "Yes" or "1." This server parameter is available in CIC 2016 R4 and higher releases. By default, this parameter is set to "0" or "Off."
StatServer_DisableQPSLoggingOnBackup	To disable the backup server from sending its log data to

	the CSV file, add this parameter and set its value to Yes.
Switchover Disable Gateway Ping	To enable the gateway ping, set this server parameter to “No” or “0.” To disable the gateway ping set the parameter to “Yes” or “1.” For more information about using this server parameter, see the *Automated Switchover System Technical Reference* in the PureConnect Documentation Library.
Switchover DS Request Timeout	To specify the timeout length (in seconds) for DS requests that are sent by the backup server to the primary server, add this parameter. The requests can be sent during either the initial startup of the backup server or the resynchronization with the primary server. When you enable the WAN Optimizations for DS Synchronization parameter, the minimum value for the Switchover DS Request Timeout parameter is 120 seconds. In this case, the 120-second timeout is used only as a temporary value. The Switchover DS Request Timeout parameter is not changed from its user-defined setting.
Switchover File Monitor Health Check Interval	Set this parameter to the number of seconds between each health check request that is sent from the backup server to the File Monitor on the primary server. To turn off the health check request, set this parameter to "0." If no value is specified, the default value is 60 seconds.
Switchover File Monitor Health Check Timeout	Set this parameter to the number of seconds that the backup server gives File Monitor to respond to the health check request before it times out and traces the failure. If no value is set, the default value is 10 seconds.
Switchover IP Retry Delay	Add this parameter, if necessary, for use with Interaction Director Switchover systems. When monitoring IP, this server parameter has the same effect as Switchover TS Failure Retry Delay. The Interaction Director server install automatically creates this server parameter. Genesys recommends that you review this server parameter in Interaction Administrator on the Interaction Director server to confirm the setting.
Switchover IP Timeout	Add this parameter, if necessary, for use with Interaction Director Switchover systems. When monitoring IP, this server parameter has the same effect as Switchover TS Timeout. The Interaction Director server install automatically creates this server parameter. **Note**: Confirm the setting of this server parameter in

	Interaction Administrator on the Interaction Director server.
Switchover Max Restarts	To specify the maximum number of times in a restart period that a new process ID can be returned in the TS ping notification before a restart occurs, add this parameter. By default, this value is 2.
Switchover Max Restarts Period	To specify the time period (in seconds) during which the Switchover system counts TS ping notifications that contain new process IDs, add this parameter. By default, this value is 300 (5 minutes).
Switchover Max Sequential Restarts	To specify the maximum number of sequential times that a new process ID can be returned in the TS ping notification before a switch occurs, add this parameter. By default, this value is 2.
Switchover Max TS Failures	To specify the number of TS ping failures the Switchover system on the backup server tolerates before starting a switchover, add this parameter. **Note**: Set this value greater than 0. The default value is 2 **Note**: The failure count is reset each time the Switchover system successfully receives a response from TS on the primary server.
Switchover Monitoring	Add this parameter, if necessary, for use with Interaction Director Switchover systems. The Interaction Director server install automatically creates this server parameter. It sets up an IP ping process in Interaction Director configurations, which are similar to the TS ping process in CIC configurations. The default value is TsServer. **Note**: Confirm the setting of this server parameter in Interaction Administrator on the Interaction Director server.
Switchover NetTest A	Add this parameter, if necessary, for switchover in WAN environments. It applies to "Pure SIP" configurations only. Switchover NetTest A specifies the name or IP address of a computer on the same network segment as SwitchoverServer B. The Switchover system uses the IP address on SwitchoverServer A when SwitchoverServer A is the backup server. Whenever a failure condition is detected, the Switchover system on the backup server uses ICMP echo to ping this IP endpoint. It must find the IP endpoint on the same network segment as the active server. If the Switchover system cannot ping this endpoint, it assumes that the active server is still operable and doesn't switch because there a WAN failure. **Important**: Since the Switchover system no longer has a network connection (and thus cannot replicate changes), it logs an error to the event log and shuts down processing. Restart the backup server, so that the Switchover system can resume its monitoring and replication. **Recommendation**: The value for Switchover NetTest A is the closest "pingable" (ICMP echo) IP address to SwitchoverServer B from SwitchoverServer A.
Switchover NetTest B	Add this parameter, if necessary, for switchover in WAN

	environments. It applies to "Pure SIP" configurations only. This parameter specifies the name or IP address of a computer on the same network segment as SwitchoverServer A. The Switchover process on SwitchoverServer B uses the IP address when SwitchoverServer B is the backup server. **Recommendation**: The value for Switchover NetTest B is the closest "pingable" (ICMP echo) IP address to SwitchoverServer A from SwitchoverServer B.
Switchover NetTest Timeout	Add this parameter, if necessary, for use with Switchover in WAN environments. It applies to "Pure SIP" configurations only and is used with Switchover NetTest A and Switchover NetTest B. This parameter specifies the amount of time (in seconds) Switchover waits for the ICMP echo to return. By default, this value is 1 second.
Switchover Notifier Reconnect Delay	Specifies the interval in seconds that the Notifier connections will wait to re-establish a new connection after a loss. Lower values can improve reconnection response during short periods of connection los with the primary monitor. The default value is 5. The minimum value is 5. The maximum value is 60.
Switchover Ping on Aux Connection	This parameter moves the TS ping from the main data connection to the auxiliary connection. By default, this parameter is set to 1, which means it is enabled. **Note**: To enable QoS on the ping on the auxiliary connection (not the main connection), enable both the Switchover Ping on Aux Connection and the Switchover Use QoS For Ping parameters. If only the Switchover Use QoS For Ping parameter is enabled, QoS is not used on the ping.
Switchover Primary Monitor Ping Delay	Specifies the delay in seconds between the primary monitor pings to the notifier on the primary monitor. The default value is 0. The maximum value is 300.
Switchover Primary Monitor Retry Ping Delay	Specifies the delay in seconds between pings when the primary monitor is in retry mode. The default value is 0. The minimum value is 0. The maximum value is 300.
Switchover Primary Monitor Retry Count	Specifies the number of times the primary monitor will send retry pings before it begins diagnosing the connection issues. The default value is 2. The minimum value is 1. The maximum value is 50.
Switchover Primary Monitor Timeout	Specifies the timeout value in seconds for a ping from the primary monitor on the backup to the notifier on the primary. If a ping is not received in this time frame, the primary monitor will then begin its retry mode. The default value is 0, which indicates that the value will be one half of the monitored module timeout whose default value is 10

	seconds. The maximum value is 300.
Switchover QoS DSCP	When Switchover Use QoS For Ping parameter is enabled, add this parameter to set the value in the QoS byte. Differentiated Services Code Point (DSCP) is the 6 most significant bits of a packet. You can use DSCP to prioritize QoS traffic on Switchover. **Note**: To enable QoS on the auxiliary connection ping, enable both the Switchover Ping on Aux Connection and the Switchover Use QoS For Ping parameters. If only the Switchover Use QoS For Ping parameter is enabled, QoS is not used on the ping.
Switchover Reconnect Delay	Add this parameter to specify the number of seconds that the Switchover system waits after the main connection goes down before it attempts to reconnect to the primary server. When this parameter is set, a switchover does not occur as a result of the auxiliary connection going down until after the delay period. You can use this parameter to prevent switchovers from occurring on networks where the connection occasionally drops for a short, consistent amount of time. The default value is 90 seconds.
Switchover Reconnect Timeout	Specifies the duration in seconds that switchover on the backup will attempt to reconnect with the primary. This timeout begins once the primary monitor has diagnosed the connection and signaled the appropriate event to the switchover state machine. Therefore, the actual duration from the time connections issues were first detected to the time the backup gives up and switches over will be longer than this because there is the interval where the retry pings are sent and then the network checks all made by the primary monitor. This can take around 15 seconds if the backup is not connected to the network or 70 seconds if the primary is not connected to the network. A value of 0 indicates an immediate switchover when a connection is lost. A value greater than 0 indicates the number of seconds that the timer will be set to expire. The default value is 30. The minimum value is 0. There is no maximum value.
Switchover TS Failure Retry Delay	To specify the number of seconds that the Switchover system waits, after marking a TS failure, before sending the second ping, add this parameter. The system switches once the failure count exceeds the value stored in the Switchover Max TS Failures parameter, which defaults to 2. **Note**: Set this value to greater than 0 seconds. The default is 1 second.
Switchover TS Timeout	To specify the number of seconds that the Switchover system waits from the time the ping is sent until it is marked as a TS failure, add this parameter. This parameter also specifies the number of seconds that the Switchover system waits after a TS success before it sends another ping. Set this value between 5 - 60 seconds. The default is 10 seconds.

Switchover Unreachable Primary Ping Count	Specifies the number of times that a ping set is sent to the primary before switching over. A ping set consists of one or more pings sent during a single attempt to detect the primary's system on the network. Pings will be sent until the primary responds or the maximum number of ping attempts is reached. This count is not the number of pings sent in a single set when trying to contact the primary but the maximum number of sets before a switchover will occur. The delay between sending ping sets is defined by the **Switchover Unreachable Primary Ping Delay** parameter. A value of 0 results in an immediate switchover. No further attempts are made to detect the primary after it is considered unreachable. This is the default value if the parameter is not defined. A value of -1 results in unlimited attempts until the primary is reachable. In this case, if the connection issue has been determined to be an unreachable primary, switchover will not occur since the backup will keep waiting for the primary to be reachable again. This value should only be used if a switchover should never occur as long as the primary is unreachable. The default value is 0. The minimum value is -1. There is no maximum value.
Switchover Unreachable Primary Ping Delay	Specifies the interval in seconds between sending ping sets to the primary monitor when it is unreachable. See the **Switchover Unreachable Primary Ping Count** parameter for the definition of a ping set. The default value is 10. The minimum value is 1. The maximum value is 300.
Switchover Use QoS for Ping	To customize QoS for the TS ping on the auxiliary connection, add this parameter and set it to Yes or 1 to enable it. Use this parameter to set the priority of ping (echo request and echo reply) packets. You can make further customizations by using the Switchover QoS DSCP parameter. When enabling DSCP tagging, AF41 (DSCP 34) is tagged by default. To change the value, set it to any of the tagging classes. **Note**: To enable QoS on the ping on the auxiliary connection (not the main connection), enable both the Switchover Ping on Aux Connection and the Switchover Use QoS For Ping parameters. If only the Switchover Use QoS For Ping parameter is enabled, QoS is not used on ping.
SwitchoverServerFQDN A	When the **ForceSwitchoverFQDNs** server parameter is enabled, then the **SwitchoverServerFQDN A** server parameter contains the fully qualified domain name of the Switchover Server A. For more information, see **ForceSwitchoverFQDNs**.
SwitchoverServerFQDN B	When the **ForceSwitchoverFQDNs** server parameter is enabled, then the **SwitchoverServerFQDN B** server parameter contains the fully qualified domain name of the Switchover Server B. For more information, see **ForceSwitchoverFQDNs**.

Related topics

Dialer Server Parameter

The optional server parameter for the Dialer check box is:

Dialer Server Parameter	Description	Module
Dialer Support	Set the value of this server parameter to 1 to enable the "Dialer" check box in Interaction Administrators User configuration. This server parameter, along with the appropriate feature license is required for expose Interaction Dialer in Interaction Administrator.	Interaction Dialer

e-FAQ Server Parameters

The optional server parameters available for e-FAQ support are:

e-FAQ Server Parameter	Description	Module
e-FAQ Support	This server parameter enables the e-FAQ Interaction Administrator plug-in to register e-FAQ servers for use with the CIC clients. A value of 1 means e-FAQ is installed, and a value of 0 means e-FAQ is not installed.	e-FAQ
Hide e-FAQ	This server parameter removes the e-FAQ tab from the CIC clients. If the e-FAQ Support server parameter is 1 and Hide e-FAQ server parameter is 0, the e-FAQ tab will be displayed as well as the options menu. If the e-FAQ Support server parameter is 0 and Hide e-FAQ server parameter is 0, the e-FAQ tab will show a "commercial" for e-FAQ and the e-FAQ Options menu item will be gray and not available. If the Hide e-FAQ server parameter is 1, neither the e-FAQ tab nor the e-FAQ Options menu item will be	e-FAQ

	displayed regardless of the value for e-FAQ Support.	

Server parameters for IC Business Manager Views

You can set the following server parameters to restrict the number of records that may appear in the IC Business Manager statistics views.

To set these server parameters, add the parameters in the **Server Parameters** container. Then set the values as necessary.

> **Note:** When performing scalability tests for 5000+ agents and 500+ supervisors, we were able to allow each supervisor to observe up to 720 agent statistics and 720 workgroup statistics simultaneously. Exceeding the tested number of simultaneous statistics watches could cause CIC server scalability issues.

Parameter Name	Description
MaximumAgentsInAgentGraphView	Set this parameter to limit the number of agents shown in the Agent Graph view. The default value is 20.
MaximumAgentsInAgentOverviewView	Set this parameter to limit the number of agents shown in the Agent Overview view. The default value is 20.
MaximumStatisticsInAgentGraph	Set this parameter to limit the number of statistics shown in the Agent Graph

	view. The default value is 40.
MaximumStatisticsInWorkgroupGraph	Set this parameter to limit the number of statistics shown in the Workgroup Graph view. The default value is 40.
MaximumStatisticsInWorkgroupOverviewView	Set this parameter to limit the number of statistics shown in the Workgroup Overview view. The default value is 180.
MaximumWorkgroupsInWorkgroupOverviewView	Set this parameter to limit the number of statistics shown in the Workgroup Overview view. The default value is 20.
MaximumWorkgroupsInWorkgroupGraphView	Set this parameter to limit the number of workgroups shown in the

	Workgroup Graph view. The default value is 20.

Server parameters to suppress logging of sensitive data

Trace logs, particularly the IP trace log, can potentially contain sensitive data. Logging of sensitive data can occur when Interaction Attributes are used to store sensitive values. The value of an attribute is traced when the attribute is set, retrieved, or processed. For this reason, sensitive data may be traced and logged by multiple processes, not just by IP. Logging can also occur when traced output from SOAP tools contains an XML blob with sensitive data in it, or when an IceLib function is traced.

Examples of sensitive data include:

- Data that could be useful for hacking or identity theft. Common examples are birth date, social security number, home address, credit card or ID numbers,
- Data that must be protected for legislative reasons.
- Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership.
- Data concerning a person's health, sex life, or sexual orientation.
- Genetic or biometric data.
- Salary information.
- Data relating to criminal offenses and convictions.
- Any other attributes that your business wants to remain confidential.

Not all data is sensitive. Examples of non-sensitive data include:

- Data stored about configured users of the IC server.
- Calling name data for telephone calls (internal or external).
- Email addresses.
- Telephone numbers.
- IP addresses.

Starting with PureConnect CIC 2018 R2, customers can suppress tracing of potentially sensitive data, by setting 2 server parameters.

Parameter	Description
SuppressSensitiveDataTracing	If this server parameter is not present, or it is set to a case-insensitive value of "TRUE", "YES", or "1", then "##Suppressed## is written to trace log entries instead of the value traced.
SensitiveAttributes	This parameter identifies which attributes will be suppressed. Set its value to a delimited list of Interaction Attributes whose value should not be traced. Attribute names are automatically trimmed of leading or trailing spaces. You may delimit items

	using semicolons or new lines. For example, if you assign a value of `CC_SOCIAL_SECURITY;CC_AMOUNT_DUE` then `##Suppressed##` will be written to logs instead of the actual values of those custom attributes. When this parameter is empty, no tracing of Interaction Attributes is suppressed. But if SuppressSensitiveDataTracing is enabled, the system will suppress tracing of potentially sensitive data from SOAP Tools XML and when IceLib function is traced.

Notes:

- Both server parameters are dynamic. Changes go into effect immediately.
- For new installations, SuppressSensitiveDataTracing is TRUE by default and SensitiveAttributes is set to an empty string.
- These parameters are not supported prior to CIC 2017 R2, and will not be back ported.

Text To Speech Server Parameters

The optional server parameters for the CIC's Telephony tools for text-to-speech (TTS) conversion can change the default behavior of the TTS tools and the way CIC interfaces with the TTS engine on the CIC server. If the server parameter is not set (that is, it does not appear in the Server Parameters container in Interaction Administrator), the default values are in effect for each condition.

The most common optional TTS server parameters are listed in the following table. Other server parameters can be set as needed, under the direction of qualified PureConnect Customer Care staff.

TTS Server Parameters	Description	Module
TTS Audio File Directory	Specifies the path to a .wav file created with the Record String tool if the path was not specified in the tool step. (For more information, see the Record String tool in Interaction Designer's online help.)	TTS
TTS Speech Pitch	An integer that specifies the number of hertz used to determine the voice pitch of the TTS engine reading a user's email or other text.	TTS
TTS Speech Rate	An integer that specifies the rate (words per minute) at which the TTS engine reads a user's email or other text.	TTS

Set up forced authorization codes

To require users to enter an extension and a password in order to make a call, you can configure forced authorization codes.

There are many reasons you might want to use forced authorization codes. If you have a phone station in a reception area, you might set it up so an authorization code would have to be used to make a call. You might set codes so users, placing long distance calls from an associate's office, would have to enter their own extension and password to make a call.

The first step in setting forced authorization codes is including a phone classification in the server parameter "Toll Call Classification." Then, set the forced authorization codes by the Default User, users, members of roles and workgroups, or by stations.

Set up the Toll Call Classification server parameter

The server parameter "Toll Call Classification" is created during installation and includes the following classifications: Long Distance; International; and Unknown. You can add additional classifications or remove existing ones. To configure this server parameter:

1. In the list view of the Server Parameter container, double-click **Toll Call Classification**.
2. To add a phone classification, type the name exactly as it appears on the Classifications page in the Phone Number Configuration dialog. Use a semi-colon (;) between classifications. You can also delete classifications from the server parameter.

Next, set the Forced Authorization Codes to be required by Default User, User, members of Roles and Workgroups, or by stations.

Set up the default user

1. Double-click **Configuration** in the Default User container.
2. On the **User Rights** page, select **Required Forced Authorization Code**.

Set up a user

1. In the list view of the **Users** container, double-click on a user name.
2. On the **User Rights** page, select **Required Forced Authorization Code**.

Set up a member of a role or workgroup

1. In the list view of the **Roles** or **Workgroups** container, double-click on a name.
2. On the **User Rights** page, select **Required Forced Authorization Code**.

Configure a station

1. In the list view of the **Stations** container, double-click on a station.
2. On the **Station Rights** page, select **Required Forced Authorization Code**.

The extension and password defined in the User Configuration dialog is used for forced authorization code access.

> **Note:** If a user is dialing an external (long distance) number through the switch hook and the forced authorization codes are in effect for that user, then the user has to enter an authorization code.

Structured Parameters

Structured Parameters

The Structured Parameter container allows you to add typed parameters grouped together (like server parameters). Single strings, multi-strings and passwords are supported. The passwords are stored in an encrypted fashion. These parameters are accessible by the handlers through a tool step.

For example, you may want to use the LDAP tools to access an LDAP directory. In the structured parameter container you can store the LDAP server name, the login account and the required password. Use the **Get Structured Parameters** and **Put Structured Parameters** tools under **System** in Interaction Designer to access the parameters.

Related topics

Add a Structured Parameter

Packaged Structured Parameters

Add a Structured Parameter

To add a parameter click **Add** and enter the **Name**, **Type**, and **Value**.

Name

Type the name of the parameter.

Type

Select the type of parameter from the list. Options are String, Multi-string and Secrets.

Value

Enter the value of the parameter.

To edit a parameter entry, select it and then click **Edit**.

To delete a parameter entry, select it and then click **Delete**.

Packaged Structured Parameters

CIC includes a pre-configured structured parameter that is accessible through the **Get Structured Parameters** and **Put Structured Parameters** tools under **System** in Interaction Designer.

The pre-configured structured parameters are:

Packaged Server Parameter	Description	Module
Additional Client About Statement	Use this parameter to create an additional statement to be displayed in the CIC client interface in the	CIC clients

	"About" box. Create name-value pairs associated with your required language (i.e., en-US = "Hello", es = "Hola", or fr-FR = "Bon Jour"), or use a default (i.e., Default = "Hello").	

Related Topics:

Structured Parameters

Add a Structured Parameter

Regionalization

Regionalization

CIC's Regionalization allows the use of high-bandwidth Codecs across LANs and low-bandwidth Codecs across WANs to increase call quality and reduce traffic across LAN/WAN links.

The Regionalization container provides a view of location configuration. This view can be used to modify existing locations, but cannot be used to add or delete locations (which must be performed in the Locations sub-container. The information displayed in each cell is based on your CIC licenses.

A region defines areas where SIP stations and lines (or servers) are physically interconnected, and within this region a specific dial plan may be required based on the central office or switching fabric it may be connected to. To use this functionality, you must define and add the following information:

- Define a Location
- Add stations, lines, or servers as Endpoints to a Location

  Or...

- Define the Codec Communications between Locations
- Define a single-table Dial Plan with input patterns for specific regions and assign to a Location(s)

> **Note**: For more on Regionalization, see *IC Regionalization and Dial Plan* in the PureConnect Documentation Library.

Create Location

Create Location

Create a location to allow incoming calls to be routed to stations and perform dial plan operations on remote gateways for emergency calls and/or toll bypass.

To create a new location perform the following steps:

- Name the Location
- Select Location Communications
- Select Codecs

- Save the Location and Launch the Location Assistant (*Optional)*

Related topics

Regionalization

Location Name

Use this page to name the new location and enter a description.

Location Name

Enter a name for the location, i.e., "HQ".

Description

Enter a description for the location, i.e., "Indianapolis Headquarters".

Time Zone

Select time zone for this location from the pull-down menu. The time zones listed are the same as Windows time zones. The managed IP phones in this location use the time zone to set the daylight saving time information.

SNTP Server

Managed IP phones in this location use this server to request the time. Select **Use IC server** to use the CIC server as the SNTP server or select **Other** and enter the SNTP server IP address.

Enable Regional Dialing

Select this check box to allow dialing of short extensions within the same location. When selected, the **Significant Digits** setting is enabled. By default, this option is not enabled.

Example:

- Station A in Location "Indianapolis" has an extension of 1500
- Station B in Location "Indianapolis" has an extension of 1600

If the Enable Regional Dialing check box is selected in the Location "Indianapolis" the Significant Digits are set to "3", Station A can reach Station B by dialing 600, and Station B can reach Station A by dialing 500.

This feature is not limited to stations. All objects that can be assigned an extension, including users (through the default workstation for the user) and IP phones, as well as stations, are included in the scope of this feature.

Significant Digits

When the Enable Regional Dialing option is selected, the Significant Digits option can be set. By default, the value is 4 digits. A value of 0 means that no number of (or zero) digits are significant, therefore regional dialing is not truly enabled. Set the value to 3 to make the last three digits of an extension significant, set the value to 2 to make the last two digits significant, etc. See the example above.

> **Note**: If changing the significant digit setting on a location creates an extension conflict, i.e., using the example above and setting the significant digits to "2", a conflict would exist between Station A (00) and Station B (00). If the system detects a conflict, a message is displayed listing duplicate extensions. For later reference to help with conflict resolution, click **Copy to Clipboard** to copy the listing, and then paste the content to a program that supports CSV (comma-separated value) format (like Microsoft Excel).

Related topics

Select Location Communications

Select Codecs

Save the Location

Location Assistant

Select Location Communications

Use this page to indicate which locations are allowed to communicate with devices in each other location. The location you are creating is listed as "This Location" at the top of the list, and the <Default Location> and other configured locations are listed below it. Select a location(s) by clicking the check box next to the location.

Click **Next** to go to Select Codecs for Each Location Mapping

Related topics

Regionalization

Location Name

Select Codecs

Save the Location

Location Assistant

Select Codecs

Use this page to specify the Codecs used to communicate within that location and from that location to each of the other previously selected locations. The first location listed is the new location you are creating. The default Codecs for each location is displayed. Click **Modify Codecs...** to change the default Codec selection for a location.

Click **Next** to go to Save the Location.

Related topics

Regionalization

Location Name

Select Location Communications

Save the Location

Location Assistant

Save the Location

This page allows you to review the new location and the location communications. Click **Finish** to save the location. You can optionally select the **Launch the Location Assistant after the new location is saved** check box to step through the Location Assistant. The assistant steps you through the location configuration tasks in a linear fashion, so there is no need to manually open each related container or sub-container to complete the new location configuration.

Related topics

Regionalization

Location Name

Select Location Communications

Select Codecs

Location Assistant

Location Settings

Location

A location represents an area where things are considered to be in the same physical place. This location defines a set of endpoints (lines, stations, and servers) that share a common dial plan, and it defines Codec communications for the endpoints. A Codec mapping defines the list of Codecs for two locations to communicate with each other sharing a common set of bandwidth requirements. The stations and lines that are members of a Location define the dial plan entries that are applicable to a locale they are operating in.

Use the **Location** container to configure the following:

- Location Name
- Configuration
- Selection Rules
- Communications
- Endpoints
- Custom Attributes
- History

How CIC prioritizes multiple locations

In IA, you can select locations for the following items:

- Users
- Stations
- Lines

When a user initiates or transfers a call, CIC determines which servers to use in the following ways:

- When a user makes an outbound call while logged in to a workstation, CIC uses the servers in the station's region.
- When a users makes an outbound call while logged in to a remote station or remote number, CIC uses the servers in the user's region.
- If a user transfers an inbound call to an external number with the forward, follow me, or TUI transfer feature, CIC uses stations in the region of the line on which the inbound call arrived.

Related topics

SIP Line Region

SIP Station Region

Regional Dial Plan

Home Site Configuration

Location Assistant

Peer Site Configuration

User Configuration

Managed IP Phone Configuration - General

Location

A location represents an area where things are considered to be in the same physical place. This location defines a set of endpoints (lines, stations, and servers) that share a common dial plan, and it defines Codec communications for the endpoints. A Codec mapping defines the list of Codecs for two locations to communicate with each other sharing a common set of bandwidth requirements. The stations and lines that are members of a Location define the dial plan entries that are applicable to a locale they are operating in.

Use the **Location** container to configure the following:

- Location Name
- Configuration
- Selection Rules
- Communications

- Endpoints
- Custom Attributes
- History

How CIC prioritizes multiple locations

In IA, you can select locations for the following items:

- Users
- Stations
- Lines

When a user initiates or transfers a call, CIC determines which servers to use in the following ways:

- When a user makes an outbound call while logged in to a workstation, CIC uses the servers in the station's region.
- When a users makes an outbound call while logged in to a remote station or remote number, CIC uses the servers in the user's region.
- If a user transfers an inbound call to an external number with the forward, follow me, or TUI transfer feature, CIC uses stations in the region of the line on which the inbound call arrived.

Related topics

SIP Line Region

SIP Station Region

Regional Dial Plan

Home Site Configuration

Location Assistant

Peer Site Configuration

User Configuration

Managed IP Phone Configuration - General

Selection rules for a location

CIC uses selection rules to determine the following things:

- Which media servers CIC uses to handle audio communications for an interaction
- Which session managers CIC uses to handle connections between users and stations
- Which content servers CIC uses to manage recordings for a location
- Which ASR servers CIC uses to handle automatic speech recognition
- Which MRCP servers CIC uses to handle text to speech and in-line audio (MoH)

CIC has a default selection rule for each of these types of objects. You can define additional selection rules in the **Selection Rules** container. For each location, you can configure the selection rule(s) that you want CIC to use.

Related topics

Selection Rules

Location Configuration

Use this page to add a description for this location. If this is the **Default Location** which CIC automatically creates, these fields are read-only and cannot be edited.

Description

Enter the description for this location.

Time zone

Select the tome zone for this location.

SNTP Server

Managed IP phones in this location use this server to request the time. Select **Use IC server** to use the CIC server as the SNTP server or select **Other** and enter the SNTP server IP address.

This IC server is in this location (Default Location)

Use this check box to indicate if this CIC server is in this specific location. This is applicable when the server acts as an endpoint. By default this check box is selected (enabled).

This Location accepts hub conferences

The default value should be selected for locations containing a CIC server and false/unchecked otherwise.

By default, CIC enables hub conferences for locations containing a CIC server, and defines latency values of 10. For locations outside current location, hub conferences are not enabled by default, although if you enable it, the latency defaults to 100. These default actions ensure functionality of the distributed conferencing feature through the Interaction Center network.

> **Note**: Use these default settings for the distributed conferencing feature. Extensive modification of hub connector locations and latency values could result in unforeseen or unintended consequences, such as usage of expensive network connections and the inability of Interaction Media Server to connect regional conference calls. Other variables, such as allowed codecs, can increase the possibility of not being able to connect regional conference calls. For more information on the Distributed Conferencing feature, see the *Interaction Conference Media Server Technical Reference* document in the PureConnect Documentation Library on the CIC server.

The Switchover Server A (server name) is in this location

Select this check box if you have a switchover environment, and Switchover Server A is located in this geographic location. By default, this check box is not selected. The location of a switchover server allows you to change codecs associated with the server.

The Switchover Server B (server name) is in this location

Select this check box if you have a switchover environment, and Switchover Server B is located in this geographic location. By default, this check box is not selected. The location of a switchover server allows you to change codecs associated with the server.

Enable keyword spotting in this location

Select this check box to use Interaction Analyzer's Keyword Spotting for this location. For more information about keyword spotting, see *Interaction Analyzer Technical Reference* in the CIC Documentation Library.

Enable Regional Dialing

Select this check box to allow dialing of short extensions within the same location. When selected, the **Significant Digits** setting is enabled. By default, this option is not enabled.

Example:

- Station A in Location "Indianapolis" has an extension of 1500
- Station B in Location "Indianapolis" has an extension of 1600

If the Enable Regional Dialing check box is selected in the Location "Indianapolis," and the Significant Digits are set to "3," Station A can reach Station B by dialing 600, and Station B can reach Station A by dialing 500.

This feature is not limited to stations. All objects that can be assigned an extension, including users (through the default workstation for the user) and IP phones, as well as stations, are included in the scope of this feature.

Significant Extension Digits

When the **Enable Regional Dialing** option is selected, you can set the Significant Digits option. By default, the value is 4 digits. A value of 0 means that no number of digits are significant, therefore regional dialing is not truly enabled. Set the value to 3 to make the last three digits of an extension significant, set the value to 2 to make the last two digits significant, etc. See the example above.

> **Note**: If changing the significant digit setting on a location creates an extension conflict, i.e., using the example above and setting the significant digits to "2," a conflict would exist between Station A (00) and Station B (00). If the system detects a conflict, a message is displayed listing duplicate extensions. For later reference, click **Copy to Clipboard** to copy the listing, and then paste the content to a program that supports CSV (like Microsoft Excel).

Related topics

Communication

Endpoints

SIP line region options

SIP Station Region

Regional Dial Plan

Home Site Concepts

Location Assistant

Configure a Peer Site

Users

Use this page to select users that belong in this physical location. Click **Add** to open the **Select Users** page, and use this page to identify the users in this location. Click **Delete** to remove a user from this location.

Related Topics

Location

Communications

Endpoints

SIP Line Region

SIP Station Region

Regional Dial Plan

Home Site Configuration

Location Assistant

Peer Site Configuration

Communication

Use this page to define a set of Codec communications for the endpoints (lines, stations, and servers). Communication between devices require a mapping between locations.

Click **Modify** to display the list of prioritized Codecs. Select the Codecs to map to the endpoints. By default, no Codecs are selected. You must select one Codec for the mapping to be valid. The **Up** and **Down** buttons set the preferred order of Codecs to use.

Click **Set Parameters** to modify the **Frame Size** (in milliseconds) and the **Frames per Packet** of a Codec. This option is available only for G.711 Codecs.

Us the up and down arrows to set the **Inter-conference latency** in milliseconds. You assign latency values to connections between locations. By specifying the latency values, you create a method of indicating which connections CIC should prefer when it joins regional conference calls through hub servers.

By default, the latency value for communications within a location is 10. The default latency value for communications to other locations is 100. Acceptable latency values range from -1 to 3000. You can adjust the latency values to specify which location Interaction Center should first attempt to use in establishing connections between regional servers and hub servers.

As an example, if the cost of bandwidth usage to one location is much more expensive than another location, you could give a higher latency value to the first location. Interaction Center would try to join conference calls through a hub server in the second location. Only if no hub servers in the second location had enough resources to facilitate the conference calls would Interaction Center then try to use a hub server in the first location.

You can use any criteria you prefer to determine the latency values that you will assign to connections between locations. The criteria could include bandwidth costs, bandwidth limits, network quality, and so on.

Notes

Latency: For distributed conference calls in the Interaction Center environment, *latency* does not implicitly refer to the delay in the relaying of transmissions on a network. Instead, *latency* is a value that an administrator specifies to indicate which locations Interaction Center should first use to find a hub server for joining regional conference calls together.

Multiple Codecs: To enable the use of multiple codecs, contact your PureConnect Customer Care support representative.

No Codecs Defined: If two devices each have a Codec defined, but there are no Codecs defined in the communications between them, then they are not allowed to communicate directly to each other. This can be used to intentionally block traffic between some Codecs.

G.726: G.726 is only available with AudioCodes.

Packet and Frame size: Summary on packet size and frequency from the www.erlang.com website: "The frequency at which the voice packets are transmitted have a significant bearing on the bandwidth required. The selection of the packet duration (and therefore the packet frequency) is a compromise between bandwidth and quality. Lower durations require more bandwidth. However, if the duration is increased, the delay of the system increases, and it becomes more susceptible to packet loss; 20ms is a typical figure." So, the more of the voice you put in a single packet (i.e., 60ms versus 20ms), the more of the voice you lose if that packet is lost.

MOS: The quality of transmitted speech is a subjective response of the listener. A common benchmark used to determine the quality of sound produced by specific Codecs is the mean opinion score (MOS). With MOS, a wide range of listeners judge the quality of a voice sample (corresponding to a particular Codec) on a scale of 1 (bad) to 5 (excellent). The scores are averaged to provide the MOS for that sample.

Tip: For the most current list of Codecs, see the latest version of *SIP Application Note* on the Product Information site.

Related Topics:

Location Configuration

Endpoints

SIP Line Region

SIP Station Region

Regional Dial Plan

Home Site Configuration

Location Assistant

Peer Site Configuration

Endpoints

Use this page to configure endpoints for the location. An endpoint is one end of a SIP connection. An endpoint can be a line, a station, or a server.

Line and Station Endpoints

When you select a line as an endpoint, and a proxy is configured on this line, then the proxy is in this region. When you select a line as an endpoint and a proxy is not configured on this line, then any SIP device that uses this line also uses this region. Typically, this is any device (station or line proxy) that is not configured already in CIC.

> **Notes**: A line or station can only belong to one location.

Server Endpoints

The purpose of server endpoints is to define the Codec communications between the server and other endpoints (i.e., lines or stations) recognized by CIC. The following objects are valid server endpoints:

- Lines
- Managed IP phones
- Media servers
- MRCP servers
- Recognition servers (ASR servers)
- Session manager servers
- SIP proxies
- Unmanaged stations

Example

An example of a server and a station as endpoints is if a call is made from a station into an IVR menu. In this case, the station is one endpoint, and the server playing the IVR menu is the other endpoint.

Adding Endpoints

To add endpoints:

1. In the **Endpoint type** list, select the type of endpoint you want to add.
2. In the **Available endpoints** list, select the endpoints you want for this location and click the arrow to move them to the **Selected endpoints** list.
3. Click **OK**.

> **Note:** Interaction Administrator prevents you from adding unmanaged stations and managed IP phones with duplicate extensions.

Removing Endpoints

> **Note:** You cannot remove endpoints from the default location.

To remove endpoints:

1. In the **Endpoint type** list, select the type of endpoint you want to remove.
2. In the **Selected endpoints** list, select the endpoints you want to remove from this location and click the arrow to move them to the **Available endpoints** list.
3. Click **OK**.

Related topics

Location Configuration

Communications

SIP Line Region

SIP Station Region

Regional Dial Plan

Home Site Configuration

Location Assistant

Peer Site Configuration

Custom attributes

The Custom Attributes page allows you to add customized attributes so that you can reference your own variables and settings through the IceLib interface.

> **Note:** If you enabled the Enhanced Interaction Administrator Change log, then all of your changes to the Custom attributes page in the User Configuration dialog box and the Workgroup Configuration dialog box dialog box are tracked in that log. For more information, see *About the Enhanced Interaction Administrator Change Log*.

The page contains a list for the attributes and displays a **Name** and a **Value** column, and has the following buttons:

Add

Click **Add** and select an existing custom attribute from the pull-down list, enter a new custom attribute. If creating a new attribute, use a unique name, otherwise the existing attribute will be overwritten.

Edit

Click **Edit** to change the value of an existing custom attribute.

Delete

Click **Delete** to delete an existing custom attribute.

Manage Attributes

Click **Manage Attributes** to open a dialog box that displays a list of custom attributes. Click **Add** or **Delete** to manage the appearance of the custom attributes in the pull-down list.

The custom attributes are saved in the path of the root container. This **Path** is displayed at the bottom of the dialog box.

> **Note**: For more information on the Interaction Center Extension Library (IceLib), see The **System APIs section** in the PureConnect Documentation Library on the CIC server.

History

This page provides a way to manually document configuration changes and when they occurred. Changes made in Interaction Administrator are also automatically logged in the Interaction Administrator Change Notification Log (Log ID 7). Later, authorized users can run reports against this log to summarize all configuration changes.

> **Note:** If you enabled the Enhanced Interaction Administrator Change log, then all of your changes to the History page in the User Configuration dialog box and the Workgroup Configuration dialog box dialog box are tracked in that log. For more information, see *About the Enhanced Interaction Administrator Change Log*.

Last Modified

This date is automatically updated each time you click the **OK** button, presumably after you make changes to the configuration. To avoid updating this date, exit the page by clicking the **Cancel** button.

> **Note:** If you click **Cancel**, none of the changes made to this page will be preserved.

In addition, the history is updated when changes are made to the record elsewhere in Interaction Administrator. For example, when a user change his or her password, the **Last Modified** date is updated.

> **Note:** Changes to the licenses for a user or a station do not update the Last Modified date.

Date Created

This date is automatically set when the user creates the initial configuration for this page. If the page was initially created during setup, the date could be blank.

Notes

Type notes about configuration settings and changes. If you change the configuration page and click **OK**, the **Last Modified** date is updated.

You must manually enter the date beside each entry in the **Notes** field to identify the date of each note.

To create a new line in the **Notes** field, press Enter.

Default Regionalization

Default Regionalization Options

CIC's Regionalization allows the use of high-bandwidth Codecs across LANs and low-bandwidth Codecs across WANs to increase call quality and reduce traffic across LAN/WAN links. This is the default configuration for regionalization.

Options

Select the **CIC server** location from the pull-down menu. This location represents an area where things are considered to be in the same physical place. This is the CIC server's default location that defines the location configuration.

See the Regionalization topic for detailed configuration information. Also, see C*IC Regionalization and Dial Plan* in the **Technical Reference Documents** section of the PureConnect Documentation Library on the CIC server.

Related Topics

Regionalization

Location Configuration

Location

Default Regionalization Conferences

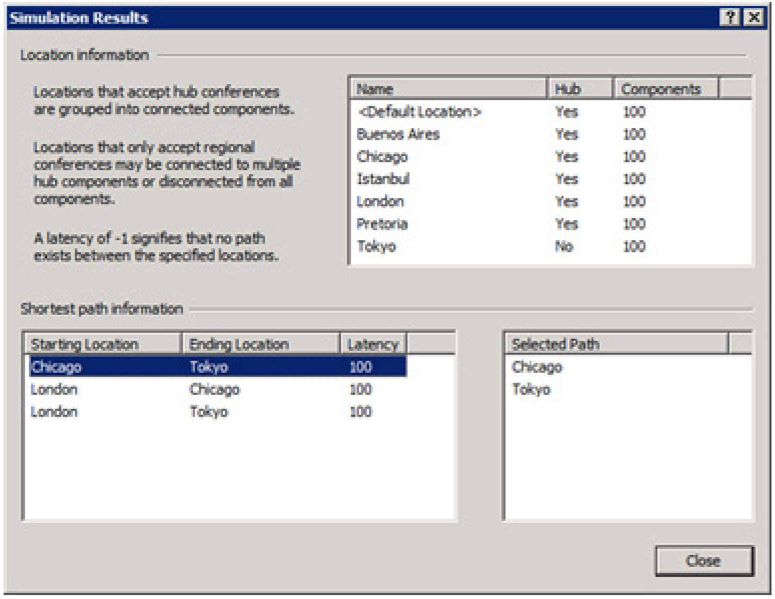
Starting Location

Configuration Simulation

1. In the **Configuration simulation** area, select one of the following options:

- **Include only locations with active media servers** (default)
- **Specify a custom list of locations**
    a. Click the **Configure** button to open the **Select Locations** dialog box and select locations to include.
    b. Click **OK**.

2. Click the **Simulate** button. The **Simulation Results** dialog box is displayed.



Location information

Locations that accept hub conferences are grouped into connected components.

Locations that only accept regional conferences may be connected to multiple hub components or disconnected from all components.

A latency of -1 signifies that no path exists between the specified locations.

Name	Hub	Components
<Default Location>	Yes	100
Buenos Aires	Yes	100
Chicago	Yes	100
Istanbul	Yes	100
London	Yes	100
Pretoria	Yes	100
Tokyo	No	100

Shortest path information

Starting Location	Ending Location	Latency
Chicago	Tokyo	100
London	Chicago	100
London	Tokyo	100

Selected Path
Chicago
Tokyo

If you selected more than two locations, CIC calculates the path between each combination of locations.

3. In the list box on the left side of the dialog box, select an item.

The list box on the right side of the dialog box displays a list of locations through which CIC would connect a distributed conference call. To view the path of the other location combinations, select each item in the list box on the left side of the dialog box.

> **Note**: If an item in the list box on the left side of the **Simulation Results** dialog box displays **-1**, Interaction Center would not be able to connect a distributed conference call between the two locations. This problem is caused by a location that is configured to not accept hub connections. To fix this problem, enable the location to allow hub connections.

4. When you are finished, select the **Close** button.

Selection Rules

CIC uses selection rules for other servers such as media and session manager servers. Use this page to create prioritized lists of locations to select media servers and session manager servers. By default, CIC has a default <Default Media Server Selection Rule> configuration, and a default <Default Session Manager Selection Rule> configuration.

About media servers and selection rules

CIC uses Interaction Media Server to process audio communications for an interaction between two or more endpoints, such as a telephone call. To select a media server, CIC uses **Selection Rules**.

This feature enables you to create prioritized lists of locations in **Selection Rules** configuration. You can select media server to service an interaction. (You can also select a session manager server to service an interaction.)

Within a location, CIC selects a media server, if more than one exists, based on the following criteria:

- Available CPU resources
- Number of resources in use

When an interaction that requires audio processing starts, CIC searches, in order, each location in a selection rules configuration. If a location does not have a media server or all media servers in that location are busy, CIC searches the next location in the **Selection Rules** configuration. This process continues until CIC finds an available media server.

> **Notes**: By default, CIC has only one location: <Default Location>. When you create a device in CIC, it is assigned to the <Default Location> location. To use the selection rules effectively, define additional locations and assign devices, such as stations, SIP lines, and media servers, to those locations.
>
> When you configure RCS server selection rules, you cannot make an RCS server a member of a location. Instead, you configure each RCS server to service one, multiple, or no locations. For more information, see the *Interaction Recorder Remote Content Service Installation and Configuration Guide* in the PureConnect Documentation Library on the CIC server.

For more information, see *Interaction Media Server Technical Reference* in the PureConnect Documentation Library on the CIC server.

About session manager servers and selection rules

Selection rules allow connections for users and stations associated with a particular location, to use certain session manager servers.

A location also uses selection rules to define which session manager locations should be used first, similar to the way media server selection rules are processed: When CIC needs a session manager for processing, CIC searches, in order, each session manager location in a selection rules configuration. If a location does not have a session manager server or all session manager servers in that location are busy, CIC searches the next location in the selection rules configuration. This process continues until CIC finds an available session manager server.

About Interaction Recorder Remote Content Service and selection rules

For more information, see the *Interaction Recorder Remote Content Service Installation and Configuration Guide* in the PureConnect Documentation Library on the CIC server.

Default Selection Rules

CIC provides the following default selection rules:

- <Default ASR Selection Rule>
- <Default Media Server Selection Rule>
- <Default MRCP Selection Rule>
- <Default Session Manager Selection Rule>

Prioritized Location list

Add: Click this button to add a static or variable location to the **Prioritized Location** list box.

Remove: Click this button to remove the highlighted location from the **Prioritized Location** list box.

Move up: Click this button to move the highlighted location to higher position in the **Prioritized Location** list box.

Move down: Click this button to move the highlighted location to a lower position in the **Prioritized Location** list box.

Group selected: Click this button to group the highlighted locations together for distributed call audio processing.

> **Tip**: To select multiple locations, press and hold the Ctrl key while clicking each location in the box.

Ungroup selected: Select this button to remove the highlighted location from an existing call audio processing group.

Excluded Location list

Do not use any other Locations: Select this option to restrict Interaction Center from selecting any other location than those specified in the Prioritized Location list box.

Use any Location, except the following: Select this option to allow Interaction Center to select any available location after it cannot locate an available media or session manager server in the Prioritized Location list box. Interaction Center will exclude any server location specified in the Excluded Location list box.

Add: Click this button to add a location to the Excluded Location list box.

Remove: Click this button to remove the highlighted location from the Excluded Location list box.

Restore: Click this button to reset this configuration to the default settings.

License Allocation

Licenses Allocation

The Licenses Allocation container displays a list of all licenses known by CIC License Manager. These numbers coincide with the numbers in **License Management**. For each license the following information is shown:

- **Name** – This is the license name, such as "ACD Media 2".
- **Assignable Allowed** - This is the number of licenses purchased or the license 'threshold'.
- **Assignable Configured** - This is the number of licenses that are configured or in use by users or stations.
- **Concurrent Allowed** - This is the number of purchased licenses that users can use dynamically, or as needed, through a network connection. For example, a user can acquire a license to access an application, and release the license when logging out of the application. CIC maintains a list

of users and licenses available and in use, similar to a library loaning limited resources to members.

- **Concurrent Configured** - - This is the number of concurrent licenses that are assigned.
- **Concurrent in Use** - - This is the number of concurrent licenses that are currently in use.
- **Notes** – This column shows text if the count exceeds the number of licenses.

> The Interaction Administrator screen displays how many days you have to renew your license before expiration in the lower left-hand corner. If license renewal is due within a specific time period, a message is displayed similar to "Your license is due for its annual re-registration in XX days. Please visit http://license.inin.com to re-register your license."

Right-click the license you want to configure and select Properties. This launches the **License Configuration** page.

Related topics

License Management

License Configuration

License Configuration

The **License Configuration** dialog box allows you to add and remove users, workgroups, and stations allocated to a license as needed, while keeping within the license threshold. This dialog box is especially useful when allocating an Access license because of the overview it provides of users, workgroups, and stations at the same time. Access to this information can save time when determining availability of licenses for new staff or departmental changes, and in setting up newly purchased licenses that must be configured. Large numbers of items such as the CIC clients, or ACD and media level, can be granted the license to a user, workgroup, or station quickly.

The **License Configuration** dialog box has two tabs; **Assignable** and **Concurrent**.

> **Note:** If you enabled the Enhanced Interaction Administrator Change log, then changes to user licenses and station licenses are tracked in that log. For more information, see *About the Enhanced Interaction Administrator Change Log*.

Assignable

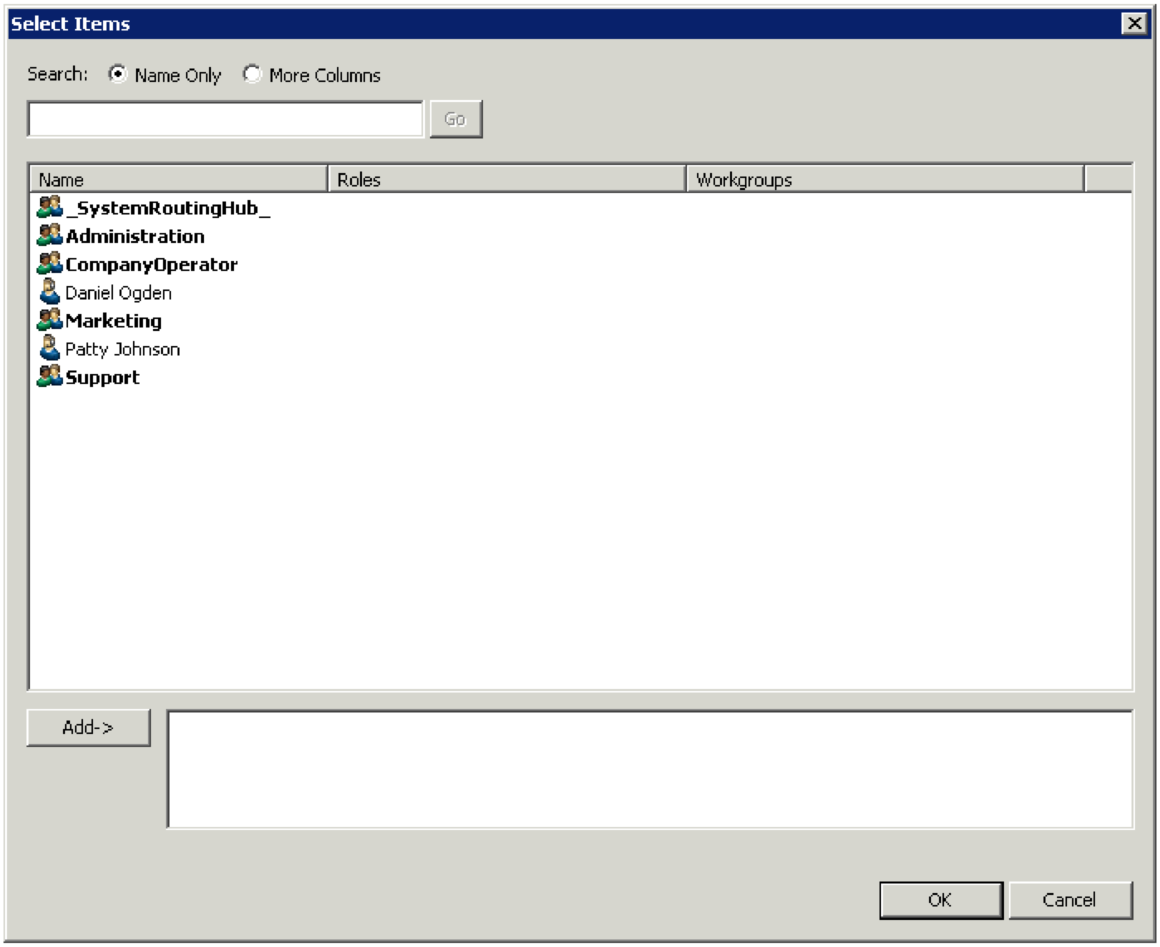
The **Assignable** tab provides a way to allocate licenses to users, workgroups and stations, with the exception of a Basic Station license. The Basic Station license can only be allocated to stations.

There are two counters shown at the bottom of each page. These counters are the **Number of licenses** and the **Total Configured (which is the number of licenses assigned and enabled)** :

- **Number of licenses** - This is the total number of licenses available.
- **Total Configured** - This is a count of the total number of users, workgroups and stations that are granted and *have the enabled* the current license based on the contents of this page. If this number exceeds the **License Threshold,** warning text is displayed at the bottom of the page.

To allocate a license to a user or workgroup (making this user or workgroup a licensed user or workgroup):

1. Click the **Add** button to the right of the user or workgroup list to display the **Select Items** dialog box.



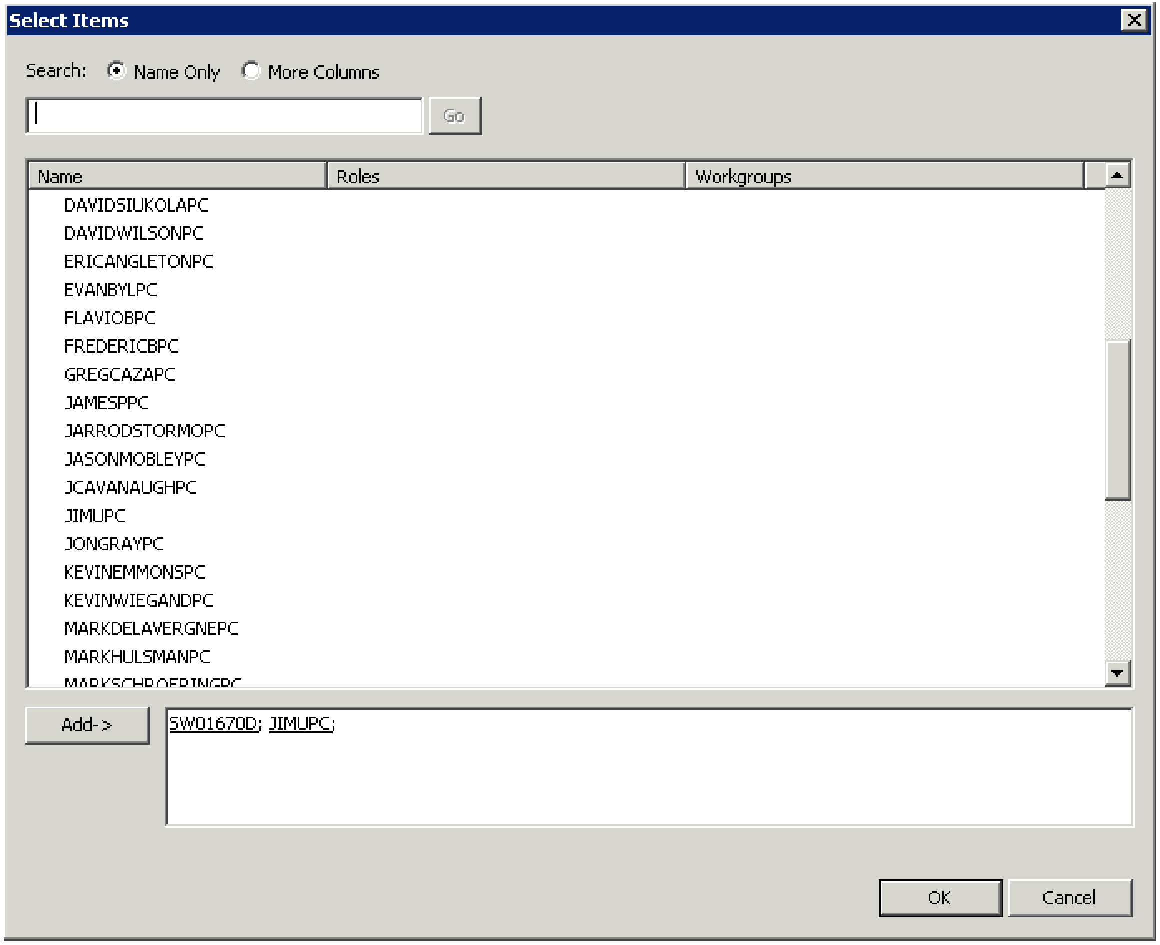
2. Add users or workgroups to be assigned the license:

- Double-click the user or workgroup, *or*
- Select the user or workgroup and click **Add**. To add a group of users or workgroups, highlight each, then click **Add**.

3. Optionally search for **Name Only** or display **More Columns**.
4. Click **OK** to return to the **License Configuration** dialog box.

To allocate this license to a station (making this station a licensed station):

1. Click the **Add** button to the right of the station list to display the **Select Items** dialog box.



DAVIDSIUKOLAPC
DAVIDWILSONPC
ERICANGLETONPC
EVANBYLPC
FLAVIOBPC
FREDERICBPC
GREGCAZAPC
JAMESPPC
JARRODSTORMOPC
JASONMOBLEYPC
JCAVANAUGHPC
JIMUPC
JONGRAYPC
KEVINEMMONSPC
KEVINWIEGANDPC
MARKDELAVERGNEPC
MARKHULSMANPC
MARKSCHROERINGPC

SW01670D; JIMUPC;

2. Add stations to be assigned the license:

- Double-click the station, *or*
- Select the station and click **Add**. To add a group of stations, highlight each station, then click **Add**.

3. Optionally search for **Name Only** or display **More Columns**.
4. Click **OK** to return to the **License Configuration** dialog box.

To de-allocate this license to a user, workgroup, or station (making this user, workgroup, or station not licensed):

1. Highlight the user, workgroup or station and click the **Delete** button to the right. To de-allocate a group of user, workgroups, or stations, highlight each, then click **Delete**.
2. Click **OK** to save the changes.

Concurrent

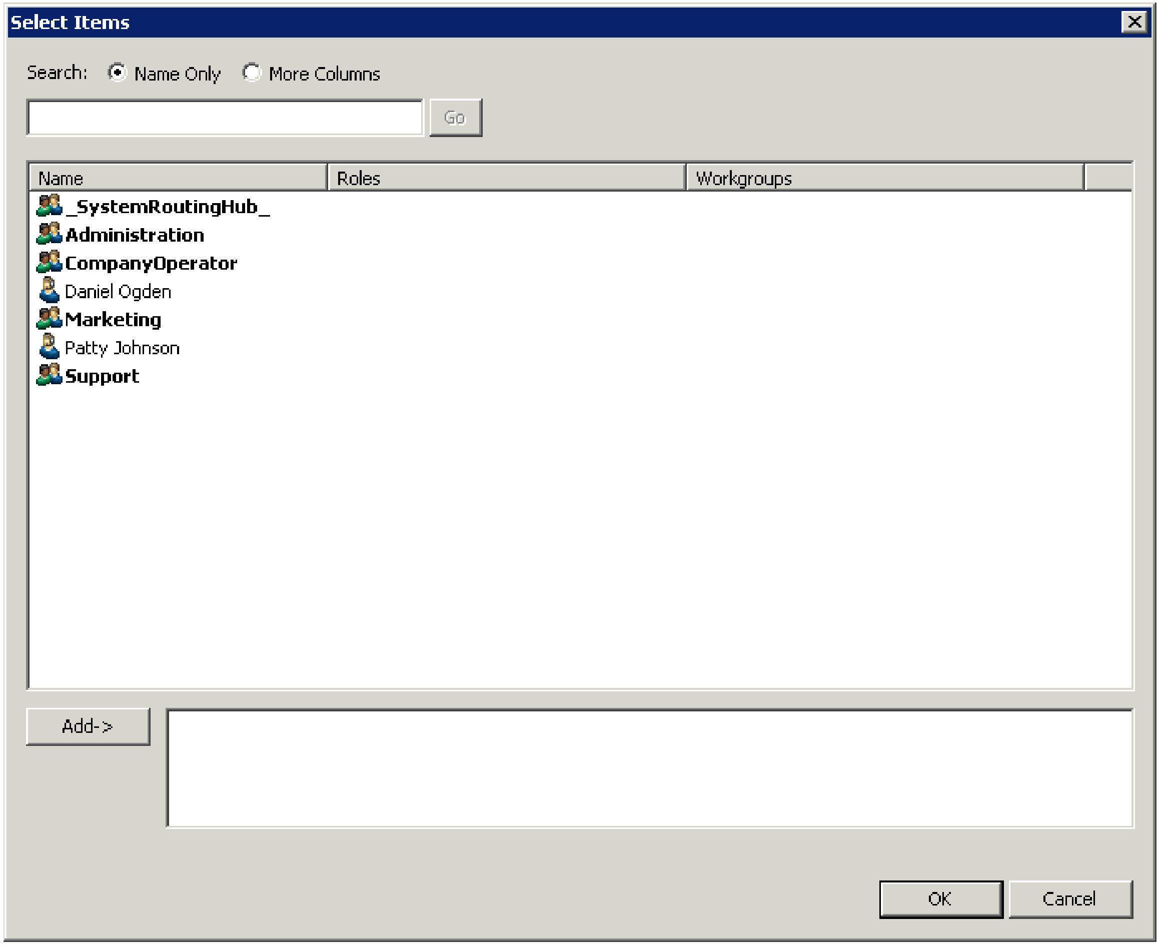
The **Concurrent** tab provides a way to allocate licenses to users only and is based on the number of simultaneous users accessing a feature or function. This license method allows users to acquire available licenses during logon instead of based on configuration. With the concurrent license method, the license is not allocated until the user logs in to the application. CIC maintains a list of users, and licenses available and in use.

There are two counters shown at the bottom of each page. These counters are the **Number of licenses** and the **Total Configured**:

- **Number of licenses** - This is the total number of licenses available.
- **Total Configured** - This is a count of the total number of users and stations that are granted the current license based on the contents of this page. If this number exceeds the **License Threshold,** warning text is displayed at the bottom of the page. If a user or station was granted the license but does not have licenses enabled, then the user or station is not included in the Total Configured count. Instead, the assigned but disabled license appears in a **dynamic** count next to the Total Configured count.

To allocate a concurrent license to a user:

1. Click the **Add** button to the right of the user list to display the **Select Items** dialog box.



Select Items

Search: ● Name Only ○ More Columns

Name	Roles	Workgroups
SystemRoutingHub		
Administration		
CompanyOperator		
Daniel Ogden		
Marketing		
Patty Johnson		
Support		

2. Add users to be assigned the license:

- Double-click the user, *or*
- Select the user and click **Add**. To add a group of users, highlight each, then click **Add**.

3. Optionally search for **Name Only** or display **More Columns**.
4. Click **OK** to return to the **License Configuration** dialog box.

> **Note:** Clicking OK on the License Configuration dialog box updates the total license values for the users or stations by updating the station and user configuration directly. The list for this license in the Licenses Allocation container is updated to reflect the user and station allocations. Also, the **Total Configured** count changes based on the selections on each page.

Related Topics

Licensing

Station Licenses

Other Station Licenses

License Allocation

People

People

You use the **People** container to configure the following options for your CIC users:

- Default User
- Roles
- Users
- Workgroups
- Password Policies
- Schedules
- Secure Input Forms
- Wrap-up Codes
- Wrap-up Categories
- Client Buttons
- Client Configuration
- Queue Columns
- Account Codes
- Client Templates

- Response Management
- Skills
- Access Control Groups

Related topics

About inheritance of configuration properties

Security for people

Overview of security for people

You can configure security for the default user, for roles, for a user, or for a workgroup.

Because users inherit one or more properties from the default user, roles and workgroup, the Security page is available from each of these containers. See *Configuration Property Inheritance* for an explanation of how these properties are related in each container.

> **Note:** If you enabled the Enhanced Interaction Administrator Change log, then all of your changes related to user security are tracked in that log. For more information, see *About the Enhanced Interaction Administrator Change Log*.

For more information on the types of security available for people, see the links under *Related topics*.

Related topics

Overview of the master administrator rights

Overview of administrator access rights

Overview of access control rights

Overview of security rights

Configuration property inheritance

Master administrator rights

Overview of the master administrator rights

Users with master administrator rights have permission to add, remove or change all security rights. Anyone having master administrator rights can view and change everything in Interaction Administrator, and assign or remove all levels of rights for any other CIC account, including others with master administrator rights. All security pages (especially Administrator Access and Access Control) for the Default User, User, Workgroup, and Role containers are visible to master administrators. This is not the case for other accounts without master administrator rights.

Master administrators can grant individual users a range of access rights, which enable them to manage other CIC configuration resources. These rights can be very minimal, such as a user allowed to run Interaction Administrator to change only their own user and station configuration, or perhaps the user and station configurations for the members of a workgroup. In contrast, a master administrator can grant another user rights to create, modify, or delete any other CIC configuration resource in Interaction

Administrator, including giving other users a subset of their own administration rights. Master administrators also control the appearance of the Access Control and Administrator Access pages for select users (other users do not have the option to control these pages).

Authorized Master Administrator network accounts

When CIC is first installed, only the designated CIC Administrator account and the account used to run the CIC server Setup program have master administrator rights in Interaction Administrator. The CIC Administrator account is specified during the IC server installation. When you are logged in to the network as either the CIC Administrator or with the account used to run the IC Server Setup program (typically, the network system administrator account), you have Master Administrator rights when you start Interaction Administrator. All other users who start Interaction Administrator will not see the configuration containers in the left window pane unless they are given rights to view and or modify specific configuration entries

Related topics

Assign the master administrator rights

Overview of security for people

Assign the master administrator rights

> **Note:** If you enabled the Enhanced Interaction Administrator Change log, then all of your changes on this page are tracked in that log. For more information, see *About the Enhanced Interaction Administrator Change Log*.

To assign the master administrator right

1. On the **Security** page, select any combination of the following options:
    - To allow the user to modify anything in CIC, select the **Master Administrator** check box. If you select this option, the other options are unavailable, because they represent a subset of the functionality provided by the Master Administrator right.
    - To allow the user the right to edit all Administrative Access items, select the **Allow Administrative Access editing** check box**.**
    - To allow the user the right to edit all Access Control items, select the **Allow Access Control editing** check box.
2. Click **OK**.

Related topics

Overview of the master administrator rights

Administrator access rights

Overview of administrator access rights

Administrator access options allow access to a subset of rights that are available with the **Master Administrator** right. These rights control what objects are shown and what objects can be edited in Interaction Administrator. You can set access at the default user, role, user, or workgroup level.

Related topics

Overview of security for people

Admin Access Categories

Assign administrator access rights

Admin access categories

These are the available categories in the **Category** list in the **Administrator Access** page:

- Account Codes
- Accumulators
- Actions
- Audio Sources
- Client Buttons
- Client Configuration
- Client Configuration Templates
- Collective
- Contact Data Manager
- Contact List Sources
- Default IP Phone
- Default Location
- Default Station
- Default User
- e-FAQ
- Fax Configuration
- Fax Groups
- Handlers
- IC Data Sources
- Initialization Functions

- Interaction Conference: Allows user access to configure the Interaction Conference global settings.
- Interaction Conference Rooms: Allows user access to configure individual conference rooms.
- Interaction Feedback
- Interaction Files
- Interaction Messages
- Interaction Recorder
- Interaction Tracker
- Interaction URLs
- Interfaces
- IP Phone Registration Groups
- IP Phone Ring Sets
- IP Phone Templates
- IP Phones
- Licenses Allocation
- Line Groups
- Lines
- Locations
- Log Retrieval Assistant
- Mail Configuration
- Media Servers
- MRCP
- MRCP Servers
- Optimizer Advanced Configuration
- Optimizer Agents
- Password Policies
- Password Policies Configuration
- Peer Sites
- Phone Numbers
- Recorder Categories
- Recorder Questionnaires
- Report Logs

- Reports
- Response Management
- Roles
- Schedules
- Server Parameters
- Servers
- SIP Proxies
- Skills
- SMDI Ports
- SMS Broker
- SMS Configuration
- Speech Recognition
- Station Groups
- Station Templates
- Stations
- Status Messages
- Structured Parameters
- System Configuration
- System Parameters
- Tables
- Telephony Resources
- Users
- Voice Modules
- Web Services Parameters
- Widgets

> **Note**: Unlike other Admin Access Categories which refer to objects you can edit in Interaction Administrator, this category controls whether the assigned user can display the Widgets view in Interaction Connect.

- Workgroups
- Wrap-up Codes

Assign administrator access rights

Administrator access allows a user to modify configuration options in Interaction Administrator containers. You can assign administrator access to any role, workgroup, user, or the default user.

> **Note:** If you enabled the Enhanced Interaction Administrator Change log, then all of your changes on this page are tracked in that log. For more information, see *About the Enhanced Interaction Administrator Change Log*.

To assign administrator access rights

1. In the **Security** page, click **Administrator Access.**
   The **Administrator Access** dialog box appears.

   By default (<All>) categories are displayed. You can select a specific category of access rights or you can locate rights by using the **Search** box.

2. Select the rights to assign. You can assign specific access rights within a group (or container), or assign *[All] access rights in a group.

3. Click **Close**.
   The **Administrator Access** page appears.

4. Click **Apply.**
   Your configuration changes are saved.

To allow an administrator to assign (edit) all of the actions in the Actions container

1. From the **Category** list, select **System**.
2. Under **Actions**, select the ***[All]** check box.
3. Click **Close**.

Related topics

Analyzer category

Attendant category

Collective category

Conference category

Dialer category

Integrations category

Optimizer category

People category

Recorder category

Resource category

Server category

Survey category

System category

Access control rights

Overview of access control rights

Access control rights determine which items each user, workgroup, or role can view and which items they can modify in CIC. "Modify" means to perform CIC client functions such as pick up calls, listen in on calls, place calls on hold, change (valid) status, and so on. You can assign access control rights to roles, workgroups, the default user and users.

You cannot remove access control rights that a user, workgroup, or role has inherited. You must remove rights at the level where they are set. See *Configuration property inheritance* for more information.

Related topics

Overview of security for people

Assign access control rights

Configuration property inheritance

Assign access control rights

> **Note:** If you enabled the Enhanced Interaction Administrator Change log, then all of your changes on this page are tracked in that log. For more information, see *About the Enhanced Interaction Administrator Change Log*.

To assign access control rights

1. In the **Security** page, click **Access Control.**
   The **Access Control** dialog box appears. The categories of rights that appear depend on the CIC products that you have installed. You can locate rights by selecting a category or by using the **Search** box.

2. Select the rights to assign. You can assign specific rights within a group, or assign *[All] rights in a group. The following tables show the available access control groups, the rights, and the associated descriptions, by category.

Application Category		
Group	**Name**	**Description**
Feedback Surveys	View	Determines which Interaction Feedback surveys and survey results the user can view.

	Modify	Determines which Interaction Feedback survey definitions can be modified. **Note:** Select this right for the user if the user needs to be able to enable the survey.
Recorder Questionnaires	View	Determines which questionnaire directories are available from the drop-down list in the **Interaction Recorder Questionnaire** container. If available from the list, a recording can be scored with that questionnaire.
	Modify	Determines which questionnaire directories can be modified. Users can create and delete questionnaires within the directory.
Attendant Profiles Category		
Group	**Name**	**Description**
Email Profiles	View	Determines which Interaction Attendant email profiles can be viewed.
	Search	Determines which Interaction Attendant email profiles are available in the **Transfer to** dialog box.
	Modify	Determines which Interaction Attendant email profiles can be modified. Users who can modify a profile can acquire a lock and edit or publish it.
Inbound Profiles	View	Determines which Interaction Attendant inbound profiles can be viewed.
	Search	Determines which Interaction Attendant inbound profiles are available in the **Transfer to** dialog box.
	Modify	Determines which Interaction Attendant inbound profiles can be modified. Users who can modify a profile can acquire a lock and edit or publish it.
Operator Profiles	View	Determines which Interaction Attendant operator profiles can be viewed.
	Search	Determines which Interaction Attendant operator profiles are available in the **Transfer to** dialog box.

	Modify	Determines which Interaction Attendant operator profiles can be modified. Users who can modify a profile can acquire a lock and edit or publish it.
Outbound Profiles	View	Determines which Interaction Attendant outbound profiles can be viewed.
	Search	Determines which Interaction Attendant outbound profiles are available in the **Transfer to** dialog box.
	Modify	Determines which Interaction Attendant outbound profiles can be modified. Users who can modify a profile can acquire a lock and edit or publish it.

Interaction Conference Category		
Group	**Name**	**Description**
Conference Rooms	Restrict	Determines if a conference room is available for creating conferences. A conference room is a set of telephone phone numbers or stations that are designated as a conference room in Interaction Conference. If you assign the Restricted right to a conference room, then users cannot make new conferences that use the conference room. Users can still call into the conference room if they have a PIN. By default, every user who has access to Interaction Conference can use every conference room that is defined in CIC.

Interaction Dialer Category		
Group	**Name**	**Description**
Campaigns	View	Determines which campaigns can be viewed in Interaction Dialer Manager.
	Modify	Determines which campaigns can be managed in Interaction Dialer Manager.

Interaction Optimizer Category		
Group	**Name**	**Description**

Agent Groups	View	Determines which agent groups in Interaction Center Business Manager (ICBM) can be viewed.
	Modify	Determines which agent groups in ICBM can be modified.
	Create	Determines if user can create agent groups in ICBM.
	Delete	Determines if user can delete agent groups in ICBM.
Forecasts	View	Determines which forecasts in Interaction Center Business Manager (ICBM) can be viewed.
	Modify	Determines which forecasts in Interaction Center Business Manager (ICBM) can be modified.
	Create	Determines which forecasts in Interaction Center Business Manager (ICBM) can be created.
	Delete	Determines which forecasts in Interaction Center Business Manager (ICBM) can be deleted.
Interaction Optimizer Master Administrator	Has Right	Allows access to all Interaction Optimizer-related activities in IC Business Manager. Requires the RTA view right.
Intraday Monitoring	View	Allows access to view Intraday Monitoring configuration in ICBM.
Real-time Adherence (RTA)	View	Allows access to view RTA configuration in ICBM. Required for the Interaction Optimizer Master Administrator right.
	Modify	Allows access to modify RTA configuration in ICBM.
Schedule Preferences	View	Allows access to the Schedule Preferences configuration in ICBM.
Schedules	View	Allows access to view schedules in ICBM. This includes weekly schedules and schedule bids.
	Modify	Allows access to modify schedules in ICBM. This includes weekly schedules and schedule bids.

	Create	Allows access to create schedules in ICBM. This includes weekly schedules and schedule bids.
	Delete	Allows access to delete schedules in ICBM. This includes weekly schedules and schedule bids.
Scheduling Unit Configuration	View	Allows access to view scheduling units.
	Modify	Allows access to modify scheduling units. See Security Rights for rights to create or delete scheduling units.
Shift Rotations	View	Allows access to view shift rotations.
	Modify	Allows access to modify shift rotations.
	Create	Allows access to create shift rotations.
	Delete	Allows access to delete shift rotations.
Shifts	View	Allows access to view shifts in ICBM.
	Modify	Allows access to modify shifts in ICBM.
	Create	Allows access to create shifts in ICBM.
	Delete	Allows access to delete shifts in ICBM.
Time off requests	View	Allows access to view time-off requests.
	Modify	Allows access to modify time-off requests.
	Delete	Allows access to delete time-off requests.
	Create	Allows access to create time-off requests.
Interaction Process Automation Category		
Group	**Name**	**Description**
Processes	View	Determines what processes in Process Monitor and the CIC clients can be searched for and viewed.

	Manage	Determines which processed can be searched, canceled, and retried in Process Monitor.
	Launch	Determines which processes can be launched from the CIC clients. **Note**: A process must be published before it can be launched.
People Category		
Group	**Name**	**Description**
Account Codes	View	Determines which account codes the user can view in the CIC client dialog boxes. To assign account codes to incoming and outgoing calls the Account Code Verification security right must be assigned in addition to this access control right.
Client Buttons	View	Determines which custom buttons can be used on the Queue Control toolbar in the CIC clients.
Directory Status Columns	View	Determines which status columns the user can add to a directory view. These status columns include: Activated, Forward Number, Logged In, Notes, On Phone, Status, Status Summary, Time in Status, and Until.
Queue Columns	View	Determines which queue columns the user can view in user, station, orbit, or workgroup queues. For more information, see Who can see and listen to recordings.
	Substitute	Determines which interaction attributes the user can use in a response macro. For more information, see the help for the CIC clients.
Skills	View	Determines which skills the user to can use design processes that transfer interactions to workgroups. For more information, see the Interaction Process Automation help.
Workgroups	View	Determines how the user can work with workgroups in the CIC clients.
	Statistics	CIC clients: View workgroups in the Workgroup Statistics view. Interaction Supervisor: View and select workgroup statistics.

Queues Category(see note)		
Group	**Name**	**Description**
Line Queues	Modify	Allows pickup, transfer, and disconnect of call interactions on a line queue.(see note)
	Monitor	Allows coach, join, listen, and record of call interactions on a line queue.(see note)
	View	Determines which line queues can be viewed.
Station Queues	Modify	Allows disconnect, hold, mute, Pickup, or transfer of call interactions on a station queue. (see note)
	Monitor	Allows coach, join, listen, or record of call interactions on a station queue.(see note)
	View	Determines which station queues can be viewed.
	Search	Determines which station queues can be transfer targets in the **Transfer** dialog box.
User Queues	Modify	Allows disconnect, hold, mute, pickup, or transfer of interactions on a user queue.(see note)
	Monitor	Allows coach, join, listen, or record of interactions in a user queue.(see note)
	View	Determines which user queues can be viewed. See also Configure the visibility of user data in reports
	Statistics	Determines which user queues' statistics can be viewed.
Workgroup Queues	Modify	Allows disconnect, hold, mute, pickup, or transfer of interactions on a workgroup queue.(see note)
	Monitor	Allows coach, join, listen, or record of interactions on a workgroup queue.(see note)
	View	Determines which workgroup queues can be viewed. **Note:** The View Workgroup Queue rights filter which

		workgroups are exposed to a user when the user is using the Telephone User Interface (TUI) to send or forward voice mail and email messages.
	Search	Determines which workgroup queues can be transfer targets in the **Transfer** dialog box.

> **Note**: The **Advanced Access Details** button is enabled when you select a line, station, user, or workgroup queue. Click this button to select or de-select a subset of queue rights or individual rights.
>
> Example 1: For a person, you can select the ability to preview interactions.
>
> Example 2: For a queue, you can give a user the ability to snip other users' interactions. For more information on snipping interactions, see the *Interaction Recorder and Interaction Quality Manager Technical Reference* in the PureConnect Documentation Library and Recording Generation.

Server Category		
Group	**Name**	**Description**
Station Groups	View	Determines which station groups can be viewed.
	Search	Determines which station groups can be transfer targets in the **Transfer** dialog box.

Station Logon Category		
Group	**Name**	**Description**
Stations	Login	Determines which stations can be logged in.

System Category		
Group	**Name**	**Description**
General Directories	View	Determines which general directories can viewed.
IC Data Sources	View	Determines which data sources the user can configure and reference in database actions in Interaction Process Automation.

Interaction Reporter Reports	View	Determines which Interaction Reporter reports can be generated.
Layouts	View	Determines which layouts the user can view.
Misc Items	View	Allows a user to log in on behalf of another user.
Phone Number - Classifications	View	Determines which phone number classifications can be accessed, such as blocked or long distance.
	Follow-me	Determines which phone number classifications can be used as follow-me numbers.
	Forward	Determines which phone number classifications can be used as forwarding numbers.
	TUI	Determines which phone number classifications can be used as forward numbers available through the menu when logged into voice mail. This access right prevents toll-fraud through the TUI.
Positions	View	Determines which floor plan images (positions) the user can use in Interaction Supervisor iPAD Edition.
Plugins	View	Determines which plug-ins can be added.
Response Management	View	Allows access to chat features.
Status Messages	View	Determines which statuses can be selected from the **My Status** list or from the **Set Status** list when changing another user's status.
e-FAQ's	View	Determines which eFAQs and eFAQ controls agents can see.

	User Category	
Group	**Name**	**Description**
Users	View History	Determines whose interactions can appear in the Interaction Tracker Related Items view in the CIC clients.

	Change Status	Determines which users' status can be changed..

3. Click **Close** to return to the **Security** page
4. Click **Apply** to save changes to the configuration.

Example

If an administrator user needs access control rights to view all general directories, do the following:

1. From the **Category** list, select **System**.
2. Under the **General Directories** access control, select the ***[All]** check box in the **View** column.
3. Click **Close**.

To assign the same rights to the default user, role, or workgroup, follow the same procedure.

> **Caution**: It is strongly recommend not to select the *[All] check box for the default user, since it would give every user access control to these categories minimizing phone system security. This could also significantly impact system performance on sites with large numbers of users (that is, more than 1,000 users). It is further recommend to limit the number of users who have access control to *[All] user and station queues, as those items generate the most traffic in large implementations.

Related topics

Administrator access

Assign scurity rights

Security rights

Overview of security rights

Security rights determine the functionality a user can work with in the CIC clients. For example, whether the buttons for recording, listening, and coaching appear.

You cannot remove security rights that a user, workgroup, or role has inherited. You must remove rights at the level where they are set. See *Configuration property inheritance* for more information.

Related topics

Overview of security for people

Assign Security rights

Configuration property inheritance

Assign security rights

> **Note:** If you enabled the Enhanced Interaction Administrator Change log, then all of your changes on this page are tracked in that log. For more information, see *About the Enhanced Interaction Administrator Change Log*.

To assign security rights

1. In the **Security** page, click **Security Rights** to display the **Security Rights** dialog box.
   There are two categories of security rights; Application and User. The categories are further divided into groups of related rights. By default, <All> categories is selected to display security rights in both categories. You can optionally locate rights by typing information in **Search**.
2. Select the rights to assign. The following tables show the available security rights groups, the rights, and the associated descriptions, by category:

1.

Application Category		
Group	**Name**	**Description**
Alerting Rights	Email Alerts	This security right allows the user to add e alerts that are automatically triggered wh Interaction Supervisor statistic is within a range.
	Handler Alerts	This security right allows the user to add h that are automatically triggered when an Interaction Supervisor statistic is within a range.
	Memo Alerts	This security right allows the user to add r alerts that are automatically triggered wh Interaction Supervisor statistic is within a range.
Attendant	Allow the User to Create Email Profiles	Allows users to create profiles used to pro interactions. This security right gives users modify access right to email profiles they
	Allow the User to Create Inbound Profiles	Allows users to create profiles used to pro incoming interactions. This security right g the modify access right to inbound profile create.
	Allow the User to Create Operator Profiles	Allows users to create profiles used to pro incoming interactions to the operator. Thi right gives users the modify access right to profiles they create.

	Allow the User to Create Outbound Profiles	Allows users to create profiles used to pro transferred interactions. This security righ users the modify access right to outbound they create.
Interaction Conference Policy	Create and Modify All Conferences	Allows users to create conferences and to conferences regardless of creator.
	Create and Modify Conferences	Allows users to create conferences, but to only those conferences they created.
Interaction Process Automation	Publish	Allows the user to publish from the Intera Process Automation designer in the IC Ser Manager application.
Interaction Dialer	Logon Campaign	Allows the Interaction Scripter user, at log select campaigns to participate in. Agents have this right are logged into all campaig automatically. See the *Interaction Scripter User Guide*.
	Manually Transition to a Campaign Group	When using the Advanced Campaign Man feature and monitoring a campaign in the Campaign Sequence Details view in IC Bus Manager, this right allows a user to be abl manually transition from the currently act campaign group to any campaign group ir sequence. Without this right, users can only monitor transitions.
	Modify Configuration General	View and modify two specific settings on t **General** tab of the **Global Configuration S** dialog box in Interaction Dialer Manager. T settings are: • Delay in seconds before auto-disposit disconnect interaction • Pause a campaign when the database failure rate exceeds
	Modify Preview Call Behavior	Modify specific preview call settings on th tab of the **Global Configuration Settings** d in Interaction Dialer Manager. The setting

		- If a Preview call fails to connect, p file to the agent - If a Preview call encounters a busy play this file to the agent
	Run Contact List Predefined Actions	This right allows the user to perform the P Actions from the **Data Query** section of a List. The actions are: - Bulk Edit - Delete - Make Callable - Make Uncallable - Reset Attempts - Schedule Calls The View/Modify Contact List Data Query required to use the Run Contact List Prede Actions right.
	View Configuration General	View, but not modify, two specific setting **General** tab of the **Global Configuration S** dialog box in Interaction Dialer Manager. settings are: - Delay in seconds before auto-disposit disconnect interaction - Pause a campaign when the database failure rate exceeds
	View Preview Call Behavior	View specific preview call settings on the tab of the **Global Configuration Settings** d in Interaction Dialer Manager. The setting - If a Preview call fails to connect, p file to the agent - If a Preview call encounters a busy play this file to the agent
	View/Modify Contact List Data Query	Determines whether or not the Data Quer Contact List object is visible or not. The Da tab queries the contact list to display a list in a data grid. Query results can be saved

		Users may also apply actions to records di the grid, and commit changes back to the
Interaction Dialer - Campaigns	Create/Modify Dialer Campaign Group	When using the Advanced Campaign Man feature, this right allows a user to be able new and modify existing campaign groups Campaign Sequence tab in the Campaigns Without this right, users can only view exi campaign groups.
	Modify Campaign Group Sequence	When using the Advanced Campaign Man feature, this right allows a user to be able new and modify existing campaign sequer the Campaign Sequence tab in the Campa Without this right, users can only view exi campaign sequences.
	View/Modify Agentless Calling Type	Determines whether users can select Age dialing mode when setting the Calling mod Campaign.
	View/Modify Automatic Zone Mapping	Grants right to select the "Automatically r zones and all child options" option for a C object. Without this right, these options a unavailable.
	View/Modify Line Settings	Enables settings in the Dialer Line Informa group box for a Campaign. Options in this configure Dialer to adhere strictly to CIC's or to use one specific line group for camp
	View/Modify Maximum Lines	Maximum Lines per Campaign setting on t Configuration tab of a Campaign is enable
	View/Modify Status	Enables the Campaign Execution Panel for campaign entry. Users who have this right control the running state of a campaign, w runs in accordance with a schedule, or in a operated state. Users can also recycle the list, recycle the campaign, and test to ensu campaign settings are valid. When not gra these controls are unavailable.
Interaction	Modify Change Auditing	Grants right to modify Configuration Chan

Dialer - Global Dialer Settings		Auditing settings under Global Dialer Setti When enabled, auditing tracks configurati changes made.
	Modify HTTP Server	Grants right to modify HTTP Server setting Global Dialer Settings. These settings are u stream data in and out of a contact list tal
	Modify Outbound Dialer Servers	Grants right to modify settings on the Out Dialer Servers tab under Global Dialer Set user can designate an ODS server to send notifications and e-mails when errors or o occur, and can set threshold values for inc ODS servers, including Maximum Calls and Maximum Call Rate.
	Modify Phone Number Types	Grants right to modify Phone Number Typ Global Dialer Settings. Types are user-defi strings that can be associated with contac to identify a type of telephone number. Ex phone number types might be "Work", "H "Cell".
	View Change Auditing	Grants right to view Configuration Change settings under Global Dialer Settings. Thes are disabled if the user does not have this Configuration Change Auditing feature tra configuration changes made using Dialer I or an API such as IceLib.Configuration.Dia
	View HTTP Server	Grants right to view HTTP Server settings Global Dialer Settings. These settings are u stream data in and out of a contact list tal Options on the HTTP Server tab are disabl this right is not granted.
	View Outbound Dialer Servers	Grants right to view the Outbound Dialer tab under Global Dialer Settings. The user which ODS server has been selected to se notifications and e-mails when errors or o occur. When this right is not granted, opti tab are disabled
	View Phone Number Types	Grants right to view the Phone Number Ty under Global Dialer Settings. Types are us strings that can be associated with contac to identify a type of telephone number. Ex

		phone number types might be "Work", "H "Cell". When this right is not granted, opti the tab are disabled.
	View/Modify Data Connections	Grants right to view and modify Database Connections in Dialer Manager. When this not granted, Database Connection option disabled.
	View/Modify DNC Sources	Grants right to view and modify the DNC S view in Dialer Manger. A DNC Source prov of telephone numbers that should not be When this right is not granted, DNC optio disabled
	View/Modify Time Zone Map Data	Grants right to view and modify the Timez Data view in Dialer Manger. A time zone r file that associates the initial digits of a ph number (area code and exchange in North for example) with a time zone. When this not granted, options on the view are disal
Interaction Dialer - Policy/Rule Sets	Lock Policy Sets	Determines whether or not a user can check the "Locked" check box a Dialer policy object, preventing it from being modified, removed, o by anyone who does not have Master Administrator rights. Once a policy is locked, users who are not Master Administrators car policy, but they cannot remove or edit it until a Master Administrato the lock. Locked policies can be assigned to a campaign, but they car removed from a campaign without Master Administrator rights.
	View/Modify Custom Handler Actions	Grants right to run the Dialer_RuleActionEvent handler by setting up Action or Policy Behavior. A user who does not have this right canno settings that configure a Run Handler rule action.
	View/Modify Event Log	Grants right to configure Rule Set Actions or Policy Set Behaviors tha event log entry.
Interaction Optimizer	Agent can bid on schedules	Allows users to bid on preferred schedules in Interaction Desktop.
	Agent can see rank	Allows agents to view their ranking of potential schedules in order of least-desired. Agents can view the details about how the bid was ran Bid Information section in Interaction Desktop. When enabled, agent the initial part of their rank string, such as “Your rank is 22 for this bi

	Agent can see relative rank	Allows agents to view their ranking of potential schedules compared agents' rankings. Agents can view the details about how their bids we compared to other agents' bids in the Bid Information section in Inte Desktop. When enabled, agents can see the second part of their ranl such as “Your rank is 22 out of 45 for this bid.” vs. "Your rank is 22 fo
	Agent can specify schedule preferences	Allows users to set schedule preferences in Interaction Desktop.
	Agent can submit time off	Allows users to submit requests for time off.
	Can create activity codes	Allows users to add activity codes.
	Can create day classifications	Allows users to add day classifications.
	Can create scheduling units	Allows users to create scheduling units.
	Can delete activity codes	Allows users to delete activity codes.
	Can delete day classifications	Allows users to delete day classifications.
	Can delete scheduling units	Allows users to delete scheduling units.
	Can create scheduling units	Allows users to create scheduling units.
	Can modify activity codes	Allows users to edit activity codes.
	Can modify activity type mapping	Allows users to edit activity type mappings.
	Can modify day classifications	Allows users to edit day classifications.
	Can view activity codes	Allows users to view activity codes.

	Can view activity type mapping	Allows users to view activity type mappin
	Can view day classifications	Allows users to view day classifications.
Interaction Reporter	Interaction Report Administrator	Allows users to configure all features and in Interaction Reporter.
Recorder Policy	Create/Delete Questionnaire Directories	Create, modify, or delete Interaction Qua Manager Questionnaires directories and Questionnaire rankings.
	Interaction Recorder Policy Editor	Access the Interaction Recorder Policy Edi configure and update Interaction Recorde The Interaction Recorder policies determi interactions are recorded, and where the are stored and archived. The Interaction R policies also determine how long recordin retained, and who can access, modify, an actions for recordings within the system.
	Master Key Password Administrator	Create, change, or deactivate the Master Password that is used to protect the Mast and securely encrypt master key data. Thi right requires the Master Key Password li (I3_FEATURE_RECORDER_MASTER_KEY_P) to be included in the IC Server license. T Key Password function is available on the Interaction Recorder Key Generation page **Important Note:** PureConnect Customer cannot recover encrypted recordings if a key password is lost.
	Override Finished Scorecards	Make additional answer and scoring chan Interaction Quality Manager Questionnai Scorecards that have already been finishe system. **Note**: Overriding a finished scorecard can reports.
Tracker Policy	Add Individuals	Allows users to add individuals in Interac Tracker.
	Add Organizations	Allows users to add organizations in Inter

		Tracker.
	Delete Individuals	Allows users to delete individuals in Intera Tracker.
	Delete Organization	Allows users to delete organizations in Int Tracker.
	Have Private Contacts	Allows users to designate an Interaction T contact as private and prevent other user viewing or using information for this conta
	Modify Individuals	Allows users to change or update individu Interaction Tracker.
	Modify Interactions	Allows users to change or update interact Interaction Tracker.
	Modify Organizations	Allows users to change or update organiza Interaction Tracker.
	Related Interactions Page	Allows users to view the page that shows interactions in Interaction Tracker.
	Interaction Tracker Administrator	Gives users the rights to access all pages i Interaction Tracker.
	View Other People's Private Interactions	Allows users to view other users' private interactions in the Related Items view anc these interactions included in search resu Find Interaction dialog box. Users can indi an interaction is "Private" to prevent othe from recording or listening to it.

2.

User Category		
Group	**Name**	**Description**
Alerting Rights	Email Alerts	Allows users to add alerts to email type actions in Interaction Supervisor. Users must also have the Alert Programming user

		right to add any type of alert.
	Handler Alerts	Allows users to add alerts to handler type actions in Interaction Supervisor. Users must also have the Alert Programming user right to add any type of alert.
	Memo Alerts	Allows users to add alerts to memo type actions in Interaction Supervisor. Users must also have the Alert Programming user right to add any type of alert.
Client Rights (in CIC clients)	Account Code Verification	Allows users to assign account codes to incoming and outgoing interactions. See also the View Account Codes access control right.
	Can Create Speed Dials	Allows users to create speed dial views.
	Conference Calls	Allows users to create conference calls. See also the Conference Rooms access control right.
	Customize Client	Allows users to customize configuration settings in the CIC clients. It also allows users to add view, however, the ability to display certain views may require additional access control rights.
	Force User Logout	Allows a user to log off another user. From the Workgroup Details view or the Workgroup Directory view in IC Business Manager/Interaction Supervisor, a user with this security right can log off another user from all CIC applications except for Interaction Administrator, Interaction Recorder Screen Capture Client, and Interaction Recorder Policy Editor. For example, if a user left for the day and forgot to log off, a supervisor with this security right can log off another user to release the licenses the user was consuming.
	Manage Client Templates	Allows users to create and edit configuration templates in Interaction

		Desktop and IC Business Manager.
	Mini-Mode	Allows users to run the Mini-Mode add-on to Interaction Desktop. Mini-mode provides a compact view and basic control of your interactions.
	Monitor Columns	Allows users to add the Lstns column and Recs column to a queue view. The Lstns column shows a speaker icon when someone is listening to the conversation. The Recs column shows a red dot icon to indicate that the conversation is being recorded. For more information, see Who can see and listen to recordings.
	Multiple Calls	Determines whether or not users are alerted when a new call arrives in the queue when already on a call. This only occurs on calls into lines that are marked "Allow Deferred Answer." If users do not have this right, or are already on a call and do not have call coverage set to forward calls when busy, then they are not alerted to the new call and it rolls to voicemail. This setting does not actually prevent multiple calls from being on a queue at the same time. It merely controls whether users are alerted or not. This setting applies only to My Interactions, not to calls to a logged-in station or default workstation.
	Orbit Queue	This security right allows a user to park a call on an orbit queue. An orbit queue is a numbered queue that holds a call until another user picks it up.
	Persistent Connections	Allows users the option of keeping remote telephone connected until you log off. Allows users to select Allow Persistent Connection when using a dynamic remote client connection with Interaction Connect or Interaction Desktop.

	Personal Rules	Allows users to set up Personal Rules or create a Quick Call rule. These rules automatically perform specific actions when triggered by certain interactions
	Problem Reporter	Allows users to use the **Report a Problem** option from the **File** menu in Interaction Desktop. This option allows users to send an email message containing problem information to a specified email recipient.
	Receive Voice mail	If users have this right, callers are sent to voice mail when in a DND status (Gone Home, Out of the Office, or some other "not available" status) or when not answering phone. If users don't have this right, callers are returned to the Interaction Attendant main menu.
	Response Management	Allows users to use Response Management to incorporate a stored response such as a standard greeting or their company's support website address in e-mail messages, chats, callback requests, or text message.
	Status Notes	Allows users to create a Status Note when they set Status details for themselves or other users. Status Notes provide additional details about status, for example, the date an agent expects to return after vacation.
	User-defined Telephone Number on Remote Login	Allows users to enter a new Remote Number when logging in to Interaction Connect or Interaction Desktop.
	Workgroup Queue Statistics	This security right allows a user to use the **Workgroup Statistics** view in the CIC clients.
	Workgroups/Profiles Tab	Allows users to display the Workgroup and Profiles view. This view lists workgroups and Attendant Profiles by name.

Handler Rights	Debug	Allows users to debug handlers published to the CIC server. This applies only to users who have the Interaction Designer program and who are authorized to update production handlers or create new handlers on the CIC server. If this check box is not selected, users who attempt to debug handlers from Interaction Designer will see an appropriate error message.
	Manage	Allows users to add or remove handlers published to the CIC server. A handler's status can be managed by someone running the Interaction Designer program on a workstation and using the Manage Handlers command on the Tools menu. If this option is not selected, users who attempt to manage handlers from Interaction Designer will see an appropriate error message.
	Publish	Allows users to publish new or updated handlers on the CIC server. This applies only to users who have the Interaction Designer program and who are authorized to update production handlers or create new handlers on the CIC telephony server. If this check box is not selected, users who attempt to publish handlers from Interaction Designer will see an appropriate error message.
Interaction Command Rights - (Restricts which commands are visible in the CIC clients) Note: These rights control the buttons in	Assistance	Displays the Assistance button.
	Coach	Displays the Coach button.
	Disconnect	Displays the Disconnect button.
	Hold	Displays the Hold button.
	Join	Displays the Join button.
	Listen	Displays the Listen button.
	Mute	Displays the Mute button.

the CIC clients.	Park	Displays the Park button.
	Pause	Displays the Pause button.
	Pickup	Displays the Pickup button.
	Private	Displays the Private button.
	Record	Displays the Record button.
	Secure Input	Displays the Secure Input button.
	Secure Recording Pause	Displays the Secure Record button.
	Snip	Displays the Snip button. For more information, see the *Interaction Recorder and Interaction Quality Manager Technical Reference* in the PureConnect Documentation Library and Recording Generation.
	Transfer	Displays the Transfer button.
	Voicemail	Displays the Voicemail button.
My Interaction Rights	Coach Interactions	Allows users to coach interactions by adding themselves to other agents' interactions.
	Disconnect Interactions	Allows users to disconnect interactions using the CIC clients instead of hanging up the telephone.
	Initiate Secure Input Interactions	Allows users to initiate Secure Input to collect confidential information from a customer.
	Join Interactions	Allows users to join interactions, thus creating a conference call.
	Listen in on Interactions	Allows users to listen to calls. Both sides of a call can be heard.

	Mute Interactions	Allows users to disable the microphone on the telephone so that the other party or parties cannot hear what is being said during a call. It also enables users to reactivate the microphone.
	Park Interactions	Allows users to park calls on orbit. Note: Can only park calls appearing in My Interactions.
	Pause Interactions	Allows users to use the Pause button to control a recording session. The button can be clicked to pause the recording session. It can be clicked again to resume the recording session.
	Pickup Interactions	Allows users to pick up interactions.
	Private Interactions	Allows users to prevent other CIC client users from recording or listening to their conversation.
	Put Interactions on Hold	Allows users to place selected interactions on hold.
	Record Interactions	Allows users to record interactions. The recordings are stored in files.
	Request Assistance from Supervisors	Allows users to request assistance from supervisors.
	Secure Recording Pause Interactions	Allows users to Secure Pause a Recording to avoid recording sensitive information, such as Social Security numbers or credit card numbers, when recording interactions.
	Snip Interactions	Allows users to create snippet recordings of their own interactions. **Note:** If a user needs to create snippet recordings of another user's interactions, you must assign the appropriate access control rights. For more information, see Assign access

		control rights. For more information, see the *Interaction Recorder and Interaction Quality Manager Technical Reference* in the PureConnect Documentation Library and Recording Generation.
	Transfer Interactions	Allows users to transfer interactions.
	Transfer Interactions to Voicemail	Allows users to transfer calls to voicemail.
Remote Access Rights	Email Access via TUI	Allow users to participate in e-mail interactions through the Telephone User Interface (TUI).
	Fax Access via TUI	Allows users to participate in fax interactions through the Telephone User Interface (TUI).
	Mobile Office User	Allows users access to the Mobile Office feature.
	Outlook TUI User (Requires Mobile Office User)	Allows users access to Microsoft Outlook through the Telephone User Interface (TUI).
	Voicemail Access via TUI	Allows users to participate in voicemail interactions through the Telephone User Interface (TUI).
User Rights	Alert Programming	This right controls whether or not users can add, edit and remove alerts. When this right is assigned, context menus over statistic-based values in Supervisor provide the ability to add, edit and remove alerts. Without this right, users can only view alerts.
	Directory Administrator	Allows users to edit public directories that were created by other users.
	Follow Me	Allows users to call-forward multiple numbers, long distance numbers, and international numbers.

	Intercom Chat	Allows users to have intercom chats between other users on the same CIC server.
	IP Phone Provisioning Administrator	Allows users to provision IP phones in the Managed IP Phones container.
	Remote Control	Allows users to remotely run applications and utilities that are Notifier clients, for example, IC System Manager and Switchover Control Panel.
	Require Forced Authorization Code	Requires users logged into station phones to enter a code that authorizes toll number calls.
	TIFF Faxes	Allows users to use TIFF (Tag Image File Format) for faxes.
	Trace Configuration	Allows users to configure tracing using IC System Manager or IC Trace utility.
	Video	Reserved for future use.
	View Interaction Details	Allows users to use Interaction Details view in the Interaction Tracker category. This view allows Interaction Supervisor users to search for interactions and examine the details.
Widgets	Widgets Configuration Master	Allows users to create widget and configure every widget property in the Interaction Connect Widgets view.

3. Click **Close** to return to the Security page
4. Click **Apply** to save changes to the configuration.

Example

If a user needs security rights to join interactions creating conference calls, do the following:

1. Select "User" from the **Category** drop-down list.
2. Under the "Interaction Command" security rights, select the check box in the **Has Right** column for **Join** to display/enable the **Join** button in Interaction Connect and Interaction Desktop.

3. Under "My Interactions" security rights, select the check box in the **Has Right** column for **Join Interactions.**
4. Click **Close**.

To assign the same rights to the default user, role, or workgroup, follow the same procedure.

Related topics

Administrator Access

Access Control

Overview of security

Configuration property inheritance

ACD

ACD configuration

For ACD applications that use skills based call routing, you must configure each ACD agent with skills and attributes. Each skill associated with an agent is described in terms of that user's proficiency in that skill and his or her desire to use that skill. Agents can inherit skills defined from each Workgroup of which they are members. If an agent inherits skills assigned in the **Workgroup ACD** configuration page, you can override the proficiency and desire to use levels of the inherited skills on this **User ACD** configuration page.

In addition to skills, each agent has attributes that are used to help calculate the score of an agent when CIC is evaluating how to match a call with an agent or an agent with a call. The first attribute is the Cost of an agent and the other three attributes are customizable (and not used unless values are entered for each). Cost is a value that reflects an agent's expense to the company; the higher the cost value, the more it costs the company to use that agent. For example, a senior technical support agent has a higher cost (a larger number) than a junior technical support agent.

Handlers that define skills-based routing evaluate these skills and attributes, and their various weights, to route calls to the appropriate agent. Weights are assigned in the handler tool steps (for example, ACDProcessCall).

> **Tip**: For complete information on ACD processing and how these settings are used in CIC, see the *CIC ACD Processing Technical Reference* in the PureConnect Documentation Library.

The options in the list box on the left include Utilization, Skills, Options, Options2, and Statistics. Depending which ACD category you choose, the options displayed in the page are different.

Click on the following options for specific configuration information:

- Utilization
- Skills
- Options
- Options2
- Statistics

Related topics

Workgroup ACD

Utilization

You can set these utilization options at the workgroup or user level (user settings override workgroup settings). Agents can handle multiple phone calls and other interactions simultaneously and in any combination. Using the ACD Utilization settings, you can configure how much of an agent's attention would be required for each of the interaction types as a percentage.

For example, if, as an administrator, you set the Chat category for an agent to 25%, it would mean that the agent could handle up to four chat events simultaneously. Indicating 100% for an event type would mean that the agent could handle only one such event at a time.

The percentages might vary from agent to agent based on their experience. Agents are available to the extent that the sum of the percentage utilization of all their current interactions is less than 100.

For example, if an agent is configured so that phone calls are set to 100 percent, chats to 25 percent, and email messages to 10 percent, then the agent could, at any given time, process one phone call, or four chats, or two chats and five email messages, or one chat and seven email messages, and so forth.

> **Note**: Once an interaction enters a conference or enters an ACD queue as the consult portion of a consult transfer, utilization is no longer recognized. If an interaction is transferred to an ACD Queue, utilization is only recognized if the transfer is a blind transfer.
>
> **Note:** If you enabled the Enhanced Interaction Administrator Change log, then all of your changes on this page are tracked in that log. For more information, see *About the Enhanced Interaction Administrator Change Log*.

Interaction Type

The **Interaction Type** list displays the interaction types assigned to this workgroup or user, including Call, Callback, Chat, Email, Generic Object, Social Conversation, Social Direct Message, or Work Item.

% Utilization

The **% Utilization** list shows the percentage of an agent's attention required for each interaction type.

When you add an Interaction Type, the percent utilization you assign to that interaction appears in this list. By default, the **% Utilization** is 100%.

> **Tip**: Set the percent utilization for Calls to **51% or more** when either or both of the following conditions apply:
>
> - You have selected **Auto answer** for the agent.
>
> - You have selected **Exempt held interactions** for the agent.

Under the above conditions and at less than 51% utilization, if an agent is on a call and another call comes in, the CIC client puts the first call on hold automatically and connects the incoming call.

Since calls on hold (held interactions) are exempt and do not count against the agent's percent utilization, the CIC client will continue putting active calls on hold automatically and connecting new calls to that agent.

Setting 51% or more utilization ensures that an agent handles only one call at a time. Setting it at 50% allows the CIC client to assign two calls simultaneously to the agent, one active and one on hold (achievable by some agents).

> **Note:** Calls at 50% or less utilization with a maximum assigned of 1 will only allow 1 call.

Max. Assign.

The **Max. Assign.** list displays the maximum number of interactions allowed for this interaction type. By default, the value of **Max. Assign** is "1" for Call interaction type. The default value of **Max. Assign** for all other interaction types is "0".

Edit

Select an interaction type and click **Edit** to see the **Edit** dialog where you can change the percent utilization for a Call, Chat, Email, or other interaction type.

Skills

You can assign skills to each agent in addition to any **Inherited Skills** from the workgroup he or she belongs to. The agent's total skill set is the union of **Inherited Skills** plus the agent skills in this list. You can also override the agent's inherited skill's **Proficiency** and **Desire to use** levels.

> **Note:** If you enabled the Enhanced Interaction Administrator Change log, then all of your changes on this page are tracked in that log. For more information, see *About the Enhanced Interaction Administrator Change Log*.

Proficiency

Type a value of 1 - 100 to indicate the minimum proficiency of skill level that an agent must have in order to receive an ACD call that requires this skill. 100 represents the highest skill level required. You define the skill attributes, which include proficiency level, for an agent on the **ACD configuration** page. The default value is 1. By default, the weight for proficiency is equal to 1, so this value is included in the ACD skills calculation.

Desire to Use

Type a value from 1 - 100 to indicate the minimum desire to use level agents must have in order to receive an ACD call that requires this skill. 100 is the highest possible desire; the higher the number, the more often the user wants to use the skill. Remember, desire to use is different than knowledge or ability. An agent can have a high level of proficiency (ability), but very little desire to use that ability. The default value is 0.

> **Notes:** A user inherits the desire setting for a skill from any workgroup(s) to which the user belongs. However, you can override this with a user-level proficiency setting.
>
> By default, the weight for Desire to Use equals 0, so the value that you specify is evaluated only as a qualifier instead of as the specified Desire to Use range for the ACD interaction. The Desire to Use setting is considered for ACD skill calculations when ACD customization points (such as CustomACDInitiateProcessing) are used. The weight for Desire to Use must be set to a value greater

> than 0 in order for it to be considered in ACD skills calculations. For more information on skills-based routing using the ACD Specify Interaction Skill Tool, see the *ACD Processing Technical Reference* in the PureConnect Documentation Library on the CIC server or the white paper, ACD Processing: CIC's Automatic Communication Distribution in the documentation directory on the CIC server.

Related topics

Utilization

Options

Options2

Statistics

ACD Options

Use this page to set ACD options for the user.

> **Note:** If you enabled the Enhanced Interaction Administrator Change log, then all of your changes on this page are tracked in that log. For more information, see *About the Enhanced Interaction Administrator Change Log*.

Auto-Answer ACD Interactions

Select this check box if you want CIC to automatically connect ACD interactions to an agent's phone. When a interaction alerts on a user's queue, you can use the Alert tool in Interaction Designer to play a tone, a wave file, or both to inform the agent about the incoming interaction. These are called "whisper tones." This is useful if you are using auto-answer but want to warn an agent that another interaction is about to connect to his or her queue. If this box is selected, an agent must be at his or her station to be automatically connected to a interaction.

Clear this check box if you want to alert an agent and not automatically connect the interaction. When the agent's CIC client rings, he or she must manually click the Pickup button or pick up the handset to answer the interaction.

> **Note:** In other CIC applications, the "whisper tones" feature is referred to as "Coach."

Cost

Type a positive number from 1 to 100 to define the cost attribute for this agent. The higher the cost number, the more expensive this agent appears to the ACD processing. If you want to consider employee cost when distributing ACD calls, assign a cost to each ACD agent according to their relative expense in the company or group. Then make analogous changes in the ACDProcessCall tool to increase the weight for Cost. The default value is 0.

Agent Greeting

Select the **Enable** check box to activate the agent's greeting ("smile") prompt played for callers at the beginning of every ACD call to this agent. To select a prompt (.wav) file, click the **Browse** button, navigate to the directory containing the recording, and select a .wav file (for example, \\ICServer\IC\Resources\AgentGreeting_MarkM.wav). See Queue Announcements for more information.

> **Tip:** For more information on ACD processing, see *the white paper ACD Processing: CIC's Automatic Communication Distribution* and the *ACD Processing Technical Reference* in the PureConnect Documentation Library.

Options2

Use this page to set additional ACD options for the user.

> **Note:** If you enabled the Enhanced Interaction Administrator Change log, then all of your changes on this page are tracked in that log. For more information, see *About the Enhanced Interaction Administrator Change Log*.

Attribute1

Any unique agent attribute that can be used to qualify an agent to receive a call. Leave this field blank if the ACD handlers do not use it. Otherwise enter any whole number.

Attribute2

Any unique agent attribute that can be used to qualify an agent to receive a call. Leave this field blank if the ACD handlers do not use it. Otherwise enter any whole number.

Attribute3

Any unique agent attribute that can be used to qualify an agent to receive a call. Leave this field blank if the ACD handlers do not use it. Otherwise enter any whole number.

Whisper Tone Level

Move the slider bar to adjust the 'whisper' tone the agent hears when there is an ACD call to the workgroup. Adjusting the slider bar to the right results in a whisper tone at a higher volume level.

ACD Statistics

You can set ACD statistic shift start options for a user or for a workgroup.

> **Note:** If you enabled the Enhanced Interaction Administrator Change log, then all of your changes on this page are tracked in that log. For more information, see *About the Enhanced Interaction Administrator Change Log*.

Call Statistics

The Call Statistics fields appear only in the workgroup configuration since these fields affect only call statistics for Workgroup (that is, ACD) queues that belong to an ACD Workgroup.

Statistics Period

The is the number of minutes used to define the "current period" and the "previous period" statistics on the Queues page in Interaction Supervisor. The statistics period includes every X number of minutes from midnight to the current time, where X is the number in the field. The default time is 30 minutes, which means the "current period" and "previous period" changes on every half-hour boundary.

Estimated Call Time Interval

The ACD Statistics (Call or Queue) tools in a handler that provides callers with estimated wait time feedback, uses this number of minutes in its wait time calculation. This is a rolling interval, which means the interval is the number of minutes prior to each use of the estimated wait time function as it is invoked on the CIC server. The ACD Statistics tools calculate the estimated wait time for a caller in a queue by taking the average time all callers waited in the queue during the current interval (for example, the previous 30 minutes from the time the ACD Statistics tool in a handler was invoked). The default setting for the interval is 30 minutes.

Statistic Shift Starts

This list of times determines the beginning time and duration of each shift for this user or the members of the current workgroup. These times are used to define (relative to the current time) the "current shift" and the "previous shift" on the Queues page in Interaction Supervisor. The default statistic shift is a 24 hour shift starting at midnight (0:00), meaning the statistics are relative to one day (or 24 hours).

Use the **Add** and **Delete** buttons to add or remove shift times. To change a shift time, first delete it and then add a new time to replace it.

Default User

Default User

When you configure the Default User, you set global options that have an impact on all other CIC users.

Click the following links for specific configuration information:

- About inheritance of configuration properties
- ACD Options
- Options
- Security
- Access Control
- Admin Access

Default User - ACD Options

Use this page to configure default ACD Options for users.

Whisper Tone Level

Move the slider bar to adjust the 'whisper' tone the agent hears when there is an ACD call to the workgroup. Adjusting the slider bar to the right results in a whisper tone at a higher volume level.

Apply to All Users

Click this button to apply the whisper tone level to all new and existing users.

Default User Options

Incoming Faxes

Select the format from the drop-down list, of faxes received in Interaction Connect. The options are <None> (default), PDF or PNG.

Non-ACD Alerting Actions

You can specify different kinds of application actions for ACD calls and non-ACD calls. To configure actions for ACD calls, see the ACD Actions page. For applications to respond to non-ACD calls, specify the following actions.

Alerting Action

Select an action to start each time a non-ACD call enters an alerting state (for example, the station rings) in a user or workgroup queue. Actions in this list are defined in the Actions container. For the complete procedure, click here.

Disconnected Action

Select an action to start each time a call moves from the Connected state to a Disconnected state. Actions in this list are defined in the Actions container in the Interaction Administrator hierarchy.

Parked Interactions

Use this section to set the maximum time that a parked **call**, **chat**, **email**, or **generic object** will wait on silent hold, and to specify the extension that interaction will be transferred to when the time has elapsed.

Timeout (minutes)

Set the maximum time in minutes here that a parked call should wait before transfer to the specified extension.

Extension

Set the destination extension here for a parked call that has reached its timeout.

Tracing...

Tracing allows users to set trace levels for various IceLib (Interaction Center Extension Library) -based client applications through Interaction Administrator. Click Tracing... to display the Tracing Configuration page.

Overview of security for people

You can configure security for the default user, for roles, for a user, or for a workgroup.

Because users inherit one or more properties from the default user, roles and workgroup, the Security page is available from each of these containers. See *Configuration Property Inheritance* for an explanation of how these properties are related in each container.

> **Note:** If you enabled the Enhanced Interaction Administrator Change log, then all of your changes related to user security are tracked in that log. For more information, see *About the Enhanced Interaction Administrator Change Log*.

For more information on the types of security available for people, see the links under *Related topics*.

Related topics

Overview of the master administrator rights

Overview of administrator access rights

Overview of access control rights

Overview of security rights

Configuration property inheritance

Roles

Overview of roles

A role is a way to define a special group of people that require specific CIC client rights or Interaction Administrator access. Users and members of workgroups can be assigned to a role.

Users and members of a workgroup that is assigned to a role inherit the user rights and administrative access controls that are configured for the role. Users and workgroups can be assigned multiple roles.

Default roles

The following roles are created during installation:

- Administrator
- Agent
- Billable-Time User
- Business User
- Mobile Office
- Operator
- Supervisor

These roles have default rights, access, and dialing privileges. You can change the permissions for these roles in the **Roles** subcontainer.

> **Note:** There are no values set for the default user created during setup. If a role is not defined for a user, the default Business User role is added to the user's configuration. Administrator Role is added to the administrator's user configuration.

Related topics

About inheritance of configuration properties

Client Configuration Introduction

Roles

Roles configuration

Add a role

To add a role

1. In the **People** container, click the **Users** subcontainer.
2. In the list view, right-click and then click **New**.
3. In the **Entry Name** box, type the role name and click **OK**. For more information, see *Role name*.
4. In the **Role Configuration** dialog box, complete the tabs. See the links under *Related topics* for complete information.
5. Click **OK**.

Related topics

Role name

Configuration

Client Configuration

Security

Password Policies

Custom Attributes

History

Configuration

Use this tab to assign users and workgroups to the role you are creating.

1. To add a user to this role, in the **Users** list, click **Add User**.
2. To delete a user from this role, select the user and click **Delete**. You can select multiple users at a time.
3. To add a workgroup to this role, in the **Workgroup** list, click **Add Workgroup**.
4. To delete a workgroup from this role, select the workgroup and click **Delete**. You can select multiple workgroups at a time.

> **Note**: Workgroup membership is not inherited by a user assigned to a role. Adding a workgroup to a role, and then assigning the role to a user, does not mean the user automatically is assigned to the workgroup.

Related topics

Overview of roles

CIC Client Configuration

Use this tab to select the template for the role.

1. From the **Client Configuration** list, select the template to assign.

> **Note:** You can also configure templates at the user level. For more information, see *Configure a CIC client* for a user.

Related topics

Overview of roles

Configure a CIC client for a user

Overview of security for people

You can configure security for the default user, for roles, for a user, or for a workgroup.

Because users inherit one or more properties from the default user, roles and workgroup, the Security page is available from each of these containers. See *Configuration Property Inheritance* for an explanation of how these properties are related in each container.

> **Note:** If you enabled the Enhanced Interaction Administrator Change log, then all of your changes related to user security are tracked in that log. For more information, see *About the Enhanced Interaction Administrator Change Log*.

For more information on the types of security available for people, see the links under *Related topics*.

Related topics

Overview of the master administrator rights

Overview of administrator access rights

Overview of access control rights

Overview of security rights

Configuration property inheritance

Password Policies

These password policy options can be set at the user or role level. The default password policy has pre-selected settings and other rights. You can change these values in the Password Policy container. The settings displayed depend on whether you are configuring password policies for user or role.

For more information about password policies, see the *Security Precautions Technical Reference* in the PureConnect Documentation Library on the CIC server.

For Users

Inherited

A password policy is a set of rights. When a password policy is added to a role, the user assigned that role, automatically takes on those rights. The inherited password policies are displayed in this list.

Owned

To assign a password policy to a user, in the **Owned** list click **Add**.

To delete a policy that is assigned in the **Owned** list, select the password policy and click **Delete**. You can select multiple policies to delete.

For Roles

A password policy is a set of rights. When a password policy is added to a role, users assigned that role take on those rights.

The **Available Password Policies** list shows the policies available to assign to the role. Select an available policy and click the **Add** button to assign the policy to this role. It appears in the **Currently Selected Password Policies** list.

To remove a policy from a role, click the **Remove** button. You can select multiple policies to add or remove.

Related Topics

Creating Policies

Password Policies

Custom attributes

The Custom Attributes page allows you to add customized attributes so that you can reference your own variables and settings through the IceLib interface.

> **Note:** If you enabled the Enhanced Interaction Administrator Change log, then all of your changes to the Custom attributes page in the User Configuration dialog box and the Workgroup Configuration dialog box dialog box are tracked in that log. For more information, see *About the Enhanced Interaction Administrator Change Log*.

The page contains a list for the attributes and displays a **Name** and a **Value** column, and has the following buttons:

Add

Click **Add** and select an existing custom attribute from the pull-down list, enter a new custom attribute. If creating a new attribute, use a unique name, otherwise the existing attribute will be overwritten.

Edit

Click **Edit** to change the value of an existing custom attribute.

Delete

Click **Delete** to delete an existing custom attribute.

Manage Attributes

Click **Manage Attributes** to open a dialog box that displays a list of custom attributes. Click **Add** or **Delete** to manage the appearance of the custom attributes in the pull-down list.

The custom attributes are saved in the path of the root container. This **Path** is displayed at the bottom of the dialog box.

> **Note**: For more information on the Interaction Center Extension Library (IceLib), see The **System APIs section** in the PureConnect Documentation Library on the CIC server.

History

This page provides a way to manually document configuration changes and when they occurred. Changes made in Interaction Administrator are also automatically logged in the Interaction Administrator Change Notification Log (Log ID 7). Later, authorized users can run reports against this log to summarize all configuration changes.

> **Note:** If you enabled the Enhanced Interaction Administrator Change log, then all of your changes to the History page in the User Configuration dialog box and the Workgroup Configuration dialog box dialog box are tracked in that log. For more information, see *About the Enhanced Interaction Administrator Change Log*.

Last Modified

This date is automatically updated each time you click the **OK** button, presumably after you make changes to the configuration. To avoid updating this date, exit the page by clicking the **Cancel** button.

> **Note:** If you click **Cancel**, none of the changes made to this page will be preserved.

In addition, the history is updated when changes are made to the record elsewhere in Interaction Administrator. For example, when a user change his or her password, the **Last Modified** date is updated.

> **Note:** Changes to the licenses for a user or a station do not update the Last Modified date.

Date Created

This date is automatically set when the user creates the initial configuration for this page. If the page was initially created during setup, the date could be blank.

Notes

Type notes about configuration settings and changes. If you change the configuration page and click **OK**, the **Last Modified** date is updated.

You must manually enter the date beside each entry in the **Notes** field to identify the date of each note.

To create a new line in the **Notes** field, press Enter.

Users

Users overview

In CIC, a user is someone who has a valid domain user name and an associated mailbox user profile on the network mail server (for example, Exchange Server or Notes server). Each user must have a name that is registered as a valid network account and email user account before the user can receive calls on the CIC system.

In the CIC system users have their own extensions separate from physical station devices. Users may have their own call routing preference separate from phone devices, as well. This allows users to log in to the system from any station or remote location.

> **Note:** The above information does not apply to Interaction Message Store users. Interaction Message Store uses mailboxes that are kept on the CIC server, so network mailboxes are not required.

Related topics

About inheritance of configuration properties

Add users overview

Configure a user

Add users

Overview of how to add users

There are several ways that you can add users. You can use:

- The **Add Users Assistant** to be guided through the process of adding multiple user records.
- The **User Worksheet** to quickly add multiple user records with only the most frequently needed attributes.
- The **User Configuration** dialog box to add a single user record.

Related topics

Add users with the Add Users Assistant

Add users with the User Worksheet

Add a user with the User Configuration dialog box

User name

Interaction Administrator displays a list of valid domain user names associated with each mailbox user profile on the network mail server (for example, Exchange Server or Notes server). Default CIC user names are identical to each network account that has an email user profile.

To specify a user name, you can type a name in the box, or to retrieve a list of existing users for a domain, click the ....

You can type a user name not found in the list of email users, but that name must be registered as a valid network account and email user account before the user can receive calls on the CIC system. This name must contain only valid (alpha-numerical) characters.

> **Notes:**
>
> Do not use these characters: \ / : * < > |
>
> If you copy an existing user and paste to create a new user, any workgroups the original user is a member of are not copied to the new user. The problems with users inheriting rights and memberships are too complicated and require the administrator to deliberately assign workgroup membership to users created this way.
>
> You can choose Interaction Message Store (formerly Voicemail Only or FBMC) to store and track user voice mails and faxes. If you chose Interaction Message Store as your voice mail option, it was installed and configured during Interaction Center installation.
>
> Do not exceed 64 characters.

Related topics

Add a user

Add User Assistant

Add users with the Add Users Assistant

The **Add Users Assistant** wizard guides you through the creation of multiple CIC user accounts. You can import users from the following sources:

- Mail server distribution lists
- Windows
- A CSV user list

You can use the **Add Users Assistant** to assign the extensions and passwords to the CIC user accounts that you import from mail servers or from Windows. Alternatively, you can assign the extensions and passwords in the **User Worksheet**, which is launched when you complete the **Add Users Assistant**.

> **Notes:**
> In order to use the Add Users Assistant, you must have sufficient rights to create new users, roles, and workgroups. Specifically, you must have either the Master Administrator right, or you must have all of the security rights to add, edit, and delete users, workgroups, and roles.
>
> If you enabled the Enhanced Interaction Administrator Change log, then the addition of users is tracked in that log. For more information, see *About the Enhanced Interaction Administrator Change Log*.

To add users with the Add Users Assistant

1. Under **People**, click the **Users** Container.
2. Right-click in the right pane.
3. Select **User Assistant and Worksheet...**
4. On the first page, select **Search for new users**.
5. Complete the pages in the wizard.
6. Click the help button on each page for instructions on how to complete the fields.

Search Options

Search Options

Use this page to determine how you want to locate existing users. The options are:

- **Discover users from a mail server**

  Use this option to search for mail users.

- **Discover Windows users**

  Use this option to select users from Windows

- **Import users from a CSV user list**

  Use this option to import users from a comma-separated value user list.

Discover users from a mail server

Use this page to select how users will be imported for the mail provider's directory. The Add User Assistant searches all enabled mail providers with directory lookup enabled. The options are:

- **Search for all users**

  Add User Assistant will import each user in the address list you pick. The members of the address list and their attributes (email address, address, etc.) serve as the source of information to be replicated into CIC user entries in IC Directory Services. Click **Next** to search for all users.

  If no address lists are defined but you wish to use one, exit the Add User Assistant, define an address list on the email server, and start the Add User Assistant again.

  You can make changes to these users in the User Worksheet after the Add User Assistant completes.

> **Note:** If the Address List is very large (e.g., several thousand accounts), you will notice a significant delay (and potential failure) during installation.

- **Search only for users in a distribution list**

  To further reduce a subset of users, use this option to select a distribution list within the address list. Click **Find** to get distribution lists.

  A distribution list is typically much smaller than the address list; set up for the convenience of users when messages are frequently sent to the same group of individuals, for example, a department.

  If no distribution lists are defined but you wish to use a subset list, quit the Add User Assistant, define a distribution list on the email server, and restart the Add User Assistant again.

  You can make changes to these users in the User Worksheet after the Add User Assistant completes.

Discover users from Windows

Use this page to query for existing Windows users in your current domain. If not in a domain, these will be the users local to the machine. Click **Find** to begin the search.

The results are displayed showing **Windows Users**, **Display Name** and **Comments**. You may select one user or use the **CTRL** key to select multiple users to import. Click **Select All** to select all users for import. Click **Back** if this is not the correct list of users.

Search Results from Windows

Use this page to review the results of your Windows user search.

The results are displayed showing **Windows Users**, **Display Name** and **Comments**. You may select one user or use the **CTRL** key to select multiple users to import. Click **Select All** to select all users for import. Click **Back** if this is not the correct list of users.

Import users from a CSV list

Click **Browse...** to select the CSV User List that contains your CIC users and their attributes. If you receive the User CSV Import Errors dialog box, you should correct the errors shown in the CSV list and run the import again. You may continue without resolving any errors by selecting the **I want to continue on with these warning-only errors**. Click **Next** to continue.

In most cases you should have your CSV User List completed before you run the Add User Assistant.

> **Note:** The CSV file must be in UTF-8 format. For more information, see CSV files with non-English column headings

Example

Click **Example** to view a sample CSV file.

A Microsoft Excel document (CSV User List.xls) and a sample CSV file (CSV User List.csv) are available on the CIC products disc in Additional Files...CSV Lists.

The User CSV file is formatted in two sections; a header section, and a data section. The header is the first row in the file and contains the names of all columns to import. Open a copy of CSV User List.xls in Excel, and enter the information in the appropriate columns for the users you wish to create. The following columns are supported:

User Name (Required): Type a unique user name. That name must be registered as a valid network account and e-mail user account before the user can receive calls on the CIC system.

First Name: Type the user's first name.

Last Name: Type the user's last name.

Display Name: Type the name to display on voicemails and faxes from this user. This information is also used for the Voice-Mail Only messaging account (if Interaction Message Store (Voice Mail Only) was chosen for this CIC server.)

Extension: Type the user’s extension.

DID: Type the user’s Direct Inward Dialing number. This is the number a caller would dial to call this user directly to bypass the autoattendant. Some users may not have a DID.

Password: If you type a user password here, it will be used. If you do not type a user password here, the assistant will automatically generate one that meets the default password policy requirements. You will have an opportunity at the end of the import to view those passwords, and to copy them to a document for distribution. *Caution*: Keep these passwords confidential by keeping track of the password report presented at the completion.

Network ID: Type the unique identifier for the user's computer workstation. Also include the name of the domain. For example: AcmeDomain\RogerDPC.

Mailbox: Type the e-mail address known by the mail provider. For example, use an “SMTP:” prefix for SMTP, like SMTP:ictwin@twin.local. Use a "GMAIL:" prefix for Gmail, like GMAIL:user@gmail.com.

If the mail provider is Interaction Message Store (Voicemail only), no mailbox is needed. Instead, type “FBMC” in this column. The assistant will automatically assign a Voice Mail address.

Roles: Type the role that users should be assigned. It must be one of the following roles:

- Administrator
- Agent
- Billable-Time User
- Business User
- Mobile Office
- Operator
- Supervisor

These roles each have certain associated dialing privileges, such as Long Distance calling and Emergency dialing. See “Default Roles” for more information. IC Setup Assistant automatically assigns the Operator Role to the default Company Operator.

Note: You can add additional roles. IC Setup Assistant will create the role in Directory Services, but no permissions will be assigned to that role. After installation, you can assign the permissions in the Interaction Administrator Roles container.

Workgroups: Type the names of the workgroups the user should belong to. After installation, you can further define the workgroups in the Interaction Administrator Workgroups container. IC Setup Assistant creates a default Company Operator workgroup. All users are automatically assigned to the Company Operator workgroup. You can modify this for each user later in Interaction Administrator.

Station Name: Type the user’s station name. This should be a computer of the user running a CIC client. The assistant uses this information to assign the correct CIC station account (whose name must be identical.)

Example CSV:

```
Client1,Billy,Smith,Billy
Smith,1002,7151002,1234,twinadmin,SMTP:ictwin@twin.local,Agent,MegaSales|MegaMarketing,Guest
01,No
```

When your additions are complete, save the document as a .CSV file type and download it to a secure location on the CIC server. You can open the new .CSV file in any text editor.

For more information, including user attribute descriptions and instructions for importing the CSV User list in Add Users Assistant, see *CSV List Import Technical Reference* in the PureConnect Documentation Library.

Search Results from a CSV List

Use this page to review the results of your user import. The results are displayed showing **User ID**, **Display Name**, **Extension**, **Password** and **Network ID**.

Click **Next** to import all users in the list.

Mail Search Results

Use this page to review the results of your mail search. The results are displayed showing **User Name**, **Display Name**, **First Name** and **Last Name**. Depending on whether you discovered users from an address or distribution list, the **Directory searched**, and the **Distribution list** are displayed, along with the **Number found** of users.

Set extensions for CIC user accounts

Use this page to tell the Add User Assistant how station extensions should be assigned.

I want to skip the automatic assignment of user extensions.

If you select this option, any imported extensions are used.

Automatically assign each user's extension, starting with the specified value

Select this option if you want IC Setup Assistant to automatically generate an extension for each user. You will be able to view the user information once your changes are committed. Enter the **Starting Extension**. The extensions are incremented by 1.

You might choose this option if you are importing users from an email server, or if you have not entered user extensions in the CSV User List.

> **Note**: If the Enable Regional Dialing option is selected in Regionalization - Location, and a newly created user extension creates an extension conflict, a message is displayed listing duplicate extensions. For later reference when resolving conflicts, click **Copy to Clipboard** to copy the listing, and then paste the content to a program that supports CSV (like Microsoft Excel).

Set Passwords for CIC User Accounts

Use this page to tell the Add User Assistant how to create user passwords. Users will use this password to start the CIC clients and also to access the voice mail messaging menu over the telephone. CIC users can change their passwords over the telephone by accessing their personal options through the voice mail retrieval menu.

For more information about passwords, see the *PureConnect Security Precautions Technical Reference* in the PureConnect Documentation Library on the CIC server.

I want to skip the automatic assignment of user passwords

If you select this option, any imported passwords are used. Click **Next**.

> **Note**:
>
> If you select this option, the import process does **not** check that the user passwords in the User Worksheet comply with your password policies.

Assign a single password for each new user account

Select this option to use the same password for every account. You should recommend that users change their password later by dialing into their voicemail retrieval. Enter the **Password** and click **Next.**

The password you enter here must meet the default password policy requirements. If not, the **Add Users Assistant** displays an error message.

> **Notes**:
>
> If you select this option, the import process checks that the selected password complies with your password policies. If the password is not compliant, an error message appears.
>
> It is not advisable to use a simple value such as "1234" for the password for security reasons. It is recommended to use the Set Password feature in Interaction Administrator after completing the current tasks.
>
> If you have master administrator rights, you can use the a command line executable to report on password usage within a CIC organization. Run the PWCheckU executable from a command prompt in the CIC server path using a user log in switch, for example, "C:\ pwchecku -login adminuser 07158609." For more information about this utility, see the Product Information site.

Preview Search Results

Use this page to preview search results of any users found from a mail server search or a Windows users search. If you chose to set extensions or set passwords you can view this information as well. Click **Next** to continue.

Preview Import Results

Use this page to preview import results of any users imported from a CSV list. If you chose to set extensions or set passwords you can view this information as well. Click **Next** to continue.

Completing the Add User Assistant

You have successfully completed the **Add User Assistant**. Click **Finish** to review the information in the User Worksheet before applying the changes. Click **Back** to return to the previous screen.

User Worksheet

Use this page to add users, modify user attributes or delete users. Make changes directly in the worksheet, or select the user attribute then use the shortcut icons below. When you are finished save your changes by selecting **Save and Close** from the **File** menu, Ctrl+S, or click 💾.

The User Worksheet automatically opens after you complete the Add Users Assistant. Alternatively, you can skip the Add Users Assistant and use the User Worksheet to quickly add new users. In the User Worksheet, you can add users and specify only the attributes that are most frequently used.

Starts the Add User Assistant if you want to run it again.

Opens the Mailbox Selection dialog box for the selected user.

Opens the Set Extensions dialog box to assign extensions (if you skipped this process before), or reassign extensions if you want to make changes. You can set extensions for one, all, or only selected users.

Opens the Set Passwords dialog box to assign passwords (if you skipped this process before), or reassign passwords if you want to make changes. You can set passwords for one, all, or only selected users.

Use the Tools menu to select Manage Roles or Manage Workgroups.

The following user attributes can be modified:

User Name

Click on this field to add or modify the user name. This is the name that appears before the @ in an email address. Do not use these characters: \ / : * < > |

First Name

Click on this field to add or modify the user's first name.

Last Name

Click on this field to add or modify the user's last name.

Display Name

Click on this field to add or modify the user's display name. This is the name that displayed to users in the CIC clients.

Extension

Click on this field to add or modify the user's extension.

> **Note**: If the Enable Regional Dialing option is selected in Regionalization - Location, and a newly created user extension creates an extension conflict, an error message is displayed. The conflict must be resolved before saving the worksheet information.

DID

Click on this field to add or modify the user's DID number.

Password

Click on this field to add or modify the user's password.

Network ID

Click on this field to add or modify the user's network ID.

Mailbox

Use the button to open the Mailbox Selection dialog box. Review mailbox attributes or make changes to the mailbox attributes for this user.

Roles

Use the ▾ button to open the Roles selection box. To add roles to this user, select the role and click >>. The role appears in the Selected list. To remove a role from this user select the role and click <<. The role appears in the Available list. Multiple roles can be assigned to a user.

Workgroups

Use the ▾ button to open the Workgroups selection box. To add workgroups to this user, select the workgroup and click >>. The workgroup appears in the Selected list. To remove a workgroup from this user select the workgroup and click <<. The workgroup appears in the Available list. Multiple workgroups can be assigned to a user.

> **Warning:** The system creates a workgroup called "_SystemRoutingHub_" for the routing of calls. This workgroup exists for internal reasons only.

User Workstation

Use the ▾ button to open the list of defined user workstations. Add or modify the workstation assigned to this user.

Station Name

Use the ▾ button to open the list of defined stations. Add or modify the station assigned to this user.

Location

Use the ▾ button to open the list of defined locations. Add or modify the location assigned to this user.

Add users with the User Worksheet

You can bypass the Add Users Assistant and add users directly in the User Worksheet.

> **Notes:**
> In order to use the User Worksheet, you must have sufficient rights to create new users, roles, and workgroups. Specifically, you must have either the Master Administrator right, or you must have all of the security rights to add, edit, and delete users, workgroups, and roles.
>
> If you enabled the Enhanced Interaction Administrator Change log, then the addition of users is tracked in that log. For more information, see *About the Enhanced Interaction Administrator Change Log*.

To add users with the User Worksheet

1. Under People, click the **Users Container**.
2. Right-click in the right pane.
3. Select **User Assistant and Worksheet...**
4. On the first page, select **Skip the search and add or modify user entries within the worksheet**.
5. Add the users and attributes directly in the worksheet.

6. To save your changes, from the **File** menu, click **Save and Close**.

> **Note:** At any time you can click the button to run the **Add Users Assistant**.
>
> The import process checks that any user passwords in the User Worksheet comply with your password policies. If a password is not compliant, an error message appears.

Related topics

User Worksheet

Add a user

> **Note:** If you enabled the Enhanced Interaction Administrator Change log, then the addition of the user is tracked in that log. For more information, see *About the Enhanced Interaction Administrator Change Log*.

*To add a user in the **User Configuration** dialog box*

1. In the **People** container, click the **Users** subcontainer.
2. Right-click the **Users** subcontainer and then click **New**.
3. In the **Entry Name** box, type the user name and click **OK**.

> **Notes:**
>
> Do not use these characters: \ / : * < > |
>
> If you copy an existing user and paste to create a new user, any workgroups the original user is a member of are not copied to the new user. The problems with users inheriting rights and memberships are too complicated and require the administrator to deliberately assign workgroup membership to users created this way.
>
> You can choose Interaction Message Store (formerly Voicemail Only or FBMC) to store and track user voice mails and faxes. If you chose Interaction Message Store as your voice mail option, it was installed and configured during Interaction Center installation.
>
> Do not exceed 64 characters.

4. In the **User Configuration** dialog box, complete the tabs. See the links under *Related topics* for complete information.
5. Click **OK**.

Related topics

User Name

Configuration

Licensing

Personal Info

Workgroups

Roles

Password Policies

ACD (automatic call distribution)

MWI (message waiting indicator)

Client configuration

Phonetic Spellings

Options

Security

Custom Attributes

History

Configure a user

Configure a user

*To configure a user in the **User Configuration** dialog box*

1. In the **People** container, click the **Users** subcontainer.
2. Double-click the user that you want to configure.
   The **User Configuration** dialog box appears. Complete fields on the tabs. See the links under **Related topics** for complete information.
3. Click **OK**.

Related topics

Configuration

Personal Info

Licensing

Workgroups

Roles

Password Policies

Security

ACD

MWI

Client Configuration

Phonetic Spellings

User Configuration

To define a CIC user account or change an existing user account, type or select the appropriate values in this page for the user.

> **Note:** If you enabled the Enhanced Interaction Administrator Change log, then all of your changes on this page are tracked in that log. For more information, see *About the Enhanced Interaction Administrator Change Log*.

Extension

Type a unique (logical) extension number associated with this user. When this user logs on to the network at any CIC client workstation, the CIC system detects that user’s presence (by his or her extension) and routes calls to the workstation where the user logged on. If the user is logged on to more than one workstation at the same time, all connected workstations ring when a call is received for that user, regardless of the workstation’s extension number.

> **Notes:** Be sure the user extension numbers do not begin with a number that conflicts with a workgroup extension or other valid queue extension. Extension numbers can be from two to six digits but should avoid the following numbers (in North America): 1800, 1900, 1411, 1911.
>
> If the **Enable Regional Dialing** option is selected in **Regionalization - Location**, and a change to a user extension creates an extension conflict, a message is displayed listing duplicate extensions. For later reference when resolving conflicts, click **Copy to Clipboard** to copy the listing, and then paste the content to a program that supports CSV (like Microsoft Excel).

Mailbox User

If you are using unified messaging (such as Microsoft Exchange or IMAP email client), select an email account to receive voicemail, faxes, and email sent to this user. If a user does not have an email account, he or she will not receive voice mail. The ... button displays the Mailboxes page that lets you unambiguously specify the mailbox for this user. If this user does not have or require an email account, leave the field blank.

> **Notes:** If you chose Interaction Message Store to store and track user voice mails and faxes, you cannot change the Mailbox User address on this page. When Interaction Message Store is enabled, the name displayed is from information on the Mailbox Info tabbed page. To change Mailbox User information for Interaction Message Store, click the Mailbox Info tab.
>
> User names and addresses must contain only valid (alpha-numerical) characters.

Password

Type a password of any length or any characters (upper and lower case are significant); it is initially displayed as one or more "*" characters. The next time you open the User configuration, the Password and Confirm Password fields will display 16 ‘*’ characters, regardless of the length of the password you entered, as an added security measure. Blank passwords are not allowed. A message appears if you do not enter a password, or if you enter a password that does not satisfy the requirements of the password policy. The default password policy requires that passwords have a minimum of 16 characters.

Keep in mind that remote callers may have to enter this password from a phone key pad. This password is required for some CIC operations, such as remote voicemail retrieval, remote CIC client connections, and Forced Authorization Codes. It is not required for local CIC client use.

> **Note**: If you have master administrator rights, you can use the a command line executable to report on password usage within a CIC organization. Run the PWCheckU executable from a command prompt in the IC server path using a user log in switch, for example, "C:\ pwchecku -login adminuser 07158609." For more information about this utility, see the Product Information site.

For more information about passwords, see the *Security Precautions Technical Reference* in the PureConnect Documentation Library.

Confirm Password

Retype the password exactly as you did in the **Password** box.

Preferred Language

Select the preferred language for the prompts for this user. The default setting is <System Default>.

Default Workstation

From the Default Workstation list, select the name of the workstation primarily associated with the user's account. This field will auto-complete the listing. For example, type in the letter "a" to display a listing of all stations that contain the letter "a".

For example, if **USER1** is the workstation name associated with User 1's account, then **USER1**, or its analog phone, rings on incoming calls even if User One is not logged on to the network unless:

- User 1 has selected a status other than **Available**
  (for example, **Do Not Disturb**.
- Someone other than User 1 is logged on to the workstation. Example, if User 1's default station is Station 1, do not route calls addressed to User 1 to Station 1, as long as another user is logged on to that station (whether Station 1 is the name of the PC or the name specified in the IC command line, it doesn't matter). Otherwise, it causes a security breach.

In either case, incoming calls for User 1 go directly to User 1's voice mail.

> **Notes:** Do not configure as a user's default workstation any workstation intended for regular use by more than one person.
>
> You cannot select a remote station name as the default workstation. Remote users must log on to IC to receive calls.
>
> The workstation needs to have the **Ring Always** setting enabled to properly set the default workstation for the user.

IC Privacy Name

This field is used for creating an alias for agent names in chat and other displays.

NT Domain User

Type the domain qualified user log on name for this CIC user (for example, CorpDomain\SonyaM). Click the **Browse** button to browse domains and users, and to validate. CIC uses this field to automatically authenticate that the CIC user has a valid account in the network domain. With the appropriate value in this field, the CIC user logged in to the domain with this name can start any CIC application and CIC automatically authenticates this user as a form of security. This prevents non-IC users from starting a CIC application (such as a CIC client) and running it on the network.

If this field is blank, IC attempts to validate a CIC user from a cached list of valid CIC accounts created the first time each user logs on to IC. If IC cannot reconcile a CIC user account with a known Windows user account, the log on will fail, or an application may present an IC logon dialog to give the user an opportunity to enter valid IC and account names and passwords.

Outbound ANI

Enter the ANI/Caller ID for the system to send when this user makes an outbound call.

> **Notes**: This option overrides the Outbound ANI setting in Station Options.
>
> This Outbound ANI option does not override a call placed with a specific Calling Party Number and Calling Party Name. Call Forwarding and Follow-me numbers placed as outbound calls use the Forwarded Parties ANI and Name where allowed.

Exclude From Directory

Select this check box to exclude the user from the company directory listing.

Location

Select the physical location for this user. By default, <Default Location> is used.

Time Zone

Select the time zone to associate with this user. The system uses this offset to make date and time announcements for messages such as voicemail and vacation until date status.

Use Location Time Zone

To automatically set the user's time zone based on the user's location, select this check box.

Home Site

Select the **Home Site** using the ... button which allows the selection of site IDs as defined by the peer sites.

Current Site

This is the **Current Site** for this user, and is read-only.

> **Tip**: To create a GIF image photo for this user to appear in a Chat Window during an IC Web Chat session, see the "Agent Photo" section in *Interaction Web Tools Developer's Guide* in the PureConnect Documentation Library.

Related topics

Users overview

Configure a user

Enable Regional Dialing

Forced Authorization Codes

Peer site concepts

Status Messages

Licensing

Use this page to assign licenses to the user.

> **Note:** If you enabled the Enhanced Interaction Administrator Change log, then all of your changes on this page are tracked in that log. For more information, see *About the Enhanced Interaction Administrator Change Log*.

License Allocation Method

Click the type of license allocation to use for this user. By default, **Assignable** method is used.

The **Assignable** method provides a way to allocate licenses to users, workgroups and stations, with the exception of a Basic Station license. The Basic Station license can only be allocated to stations.

The **Concurrent** method provides a way to allocate licenses to users only and is based on the number of simultaneous users accessing a feature or function. This license method allows users to acquire available licenses during logon instead of based on configuration. With the concurrent license method, the license is not allocated until the user logs in to the application. CIC maintains a list of users, and licenses available and in use.

Client Access License

To allow the user to use the CIC clients, assign this license. Without this license assignment, the user cannot run the CIC clients.

ACD Access License

Select this check box if this user is an ACD user, then select the type of ACD license. These are the available types of ACD licenses:

- **Media 1**: This license allows 1 interaction type at a given time.
- **Media 2**: This license allows 2 interaction types at a given time.
- **Media 3 Plus**: This license allows 3 or more interaction types at a given time.

If **Media 1** or **Media 2** type of ACD licenses is selected, you can click **Interaction Types** and select the type of interaction from the list to apply to the license. **Interaction Types** is grayed-out and not available if **Media 3 Plus** is selected.

> **Notes:** Failure to have a ACD Access License assigned to the user will prevent that user from being ACD active.

> If the station (Station A) is assigned a Basic Station license and two different users (User A and User B) each have all other necessary rights (i.e., Client Access) assigned to them, then both users can simultaneously login to that station, (User A and User B can both be logged into Station A at the same time). If the second user to login does not have the necessary licenses assigned, then the second user login will fail.

ACD Social Media

Users with ACD Social Media enabled are eligible to receive routed social media interactions. For more information, see the *PureConnect Social Media Technical Reference*.

IPA License

Select the **IPA License** check box if this user is an Interaction Process Automation user, and then select the type of license to assign to that user.

These are the available types of Interaction Process Automation licenses:

- **Direct Routed Work Items** (I3_ACCESS_IPA_USER) license: Enables you to launch any process to which you have rights. It also enables you to receive Work Items that are directly routed to you.
- **Group Routed Work Items** (I3_ACCESS_IPA_USER_ACD) license: Enables you to receive Work Items that are either routed to you directly or as a member of a workgroup (similar to an ACD queue).
- **Process Monitor** (I3_ACCESS_IPA_MONITOR) license: Enables you to view process status and details in the Process Monitor or to use Process Reporting in IC Business Manager Applications.
- **Process Designer** (I3_ACCESS_IPA_DESIGNER) license: Enables you to use the Process Designer to create and modify Interaction Process Automation processes.

> **Note**: Each license in this list enables you to **use the Interaction Process Automation features included in all the previous licenses in the list**. That is, the Group Routed Work Items license includes the Direct Routed Work Items license. The Process Monitor license includes both of the Routed Work Items licenses. The Process Designer license includes all the other licenses.
>
> For more information about designing processes, refer to the *Interaction Process Automation Technical Reference* and the Process Designer online help.

Enable Licenses

Select this check box to set the license settings to Active. If unchecked, the licenses settings on this page are ignored by the system. This is a way to turn off licensing for a user, but keep the license settings.

Additional Licenses

This list displays additional licenses that are available. Select the licenses you wish to assign to this user.

Click **OK** to save your changes. These license assignments are immediately reflected in the license counts in the Licenses Allocation container list.

Related topics

Configure a user

Personal Info

The **Personal Info** page displays the user's mailbox information.

If the user's mailbox was selected from a directory service (Exchange for example), then the personal information displayed here is populated by that directory service, and is read-only. If the user's mailbox was selected without using a directory service (No Mailbox, Interaction Message Store, or IMAP), then the personal information can be entered manually for display in the Company Directory.

> **Note:** If you enabled the Enhanced Interaction Administrator Change log, then all of your changes on this page are tracked in that log. For more information, see *About the Enhanced Interaction Administrator Change Log*.

To complete the personal information for a user

1. Click the buttons at the top of the Personal Info tab to access all of the pages of personal information fields.

Related topics

Configure a user

User Workgroups

If one or more workgroups are defined in the Workgroups container of Interaction Administrator, they appear in the user’s **Available Workgroups** list. If this user is a member of any workgroup, that workgroup name appears in the **Currently Selected Workgroups** list.

Moving users in and out of workgroups on this page accomplishes the same result as adding and removing users from workgroups in the Workgroups container. In the same way, if a workgroup has a queue, use one of these pages to add or remove users from the workgroup queue.

> **Note:** If you enabled the Enhanced Interaction Administrator Change log, then all of your changes on this page are tracked in that log. For more information, see *About the Enhanced Interaction Administrator Change Log*.

Available Workgroups

Workgroups in this list are defined in the Workgroups container. To add the user to one of the **Available Workgroups**, which is indicated by the workgroup name appearing in the **Currently Selected Workgroups** list, do one of the following:

- Double-click the workgroup name, *or*
- Select a workgroup name and click **Add**.

Currently Selected Workgroups

Workgroups in this list are defined in the Workgroups container. To remove a user from one of the **Currently Selected Workgroups**, which is indicated by the workgroup name appearing in the **Available Workgroups** list, do one of the following:

- Double-click the workgroup name, *or*
- Select the workgroup and click **Remove**.

Related topics

Users overview

Configure a user

Workgroups overview

Roles

You can assign multiple roles to a user or multiple users to a role.

> **Note:** If you enabled the Enhanced Interaction Administrator Change log, then all of your changes on this page are tracked in that log. For more information, see *About the Enhanced Interaction Administrator Change Log*.

Inherited

A role is a set of permissions. When a role is added to a workgroup, the workgroup takes on those permissions. If a user is a member of that workgroup, the user automatically inherits the roles assigned to the workgroup. The inherited roles are displayed in this list.

Owned

To assign a role to this user, in the **Owned** list click **Add**. Again, you must already have defined one or more roles to add a role in this list.

To delete a role that is assigned in the **Owned** list, select the role and click **Delete**. You can select multiple roles to delete.

> **Note:** The only inherited permission that an individual may override is Account Code Required.

Related topics

Configure a user

Users overview

Roles configuration

Password Policies

Security policies can be configured for use with CIC passwords and apply these policies per role or user. These policy configurations are very similar to password security policies of Windows. You can define password policies, control password types, and set password change rules, and so on.

You can disguise passwords by setting a parameter. In this case, asterisks (*) appear instead of the actual password.

You can set the following password attributes:

- Minimum Number of Unique Passwords Before One Can be Reused
- Minimum Age of Password Before User Can Change It (days)
- Maximum password age (days)
- Password Age Warning Period (days before password expires)
- Minimum password length
- Minimum number of unique DTMF digits
- Allow or not allow sequential digits
- Maximum number of failed logins
- Lockout duration (minutes)
- Failed Login Count Reser Time (minutes)
- User Must Change Password At Next Login

> **Note:** If you enabled the Enhanced Interaction Administrator Change log, then all of your changes on this page are tracked in that log. For more information, see *About the Enhanced Interaction Administrator Change Log*.

Related topics

Configure a user

MWI

Use this page to configure the behavior of Message Waiting Indicator (MWI) for a user.

Each PBX phone user must have a CIC user account to receive voice mail.

> **Note:** If you enabled the Enhanced Interaction Administrator Change log, then all of your changes on this page are tracked in that log. For more information, see *About the Enhanced Interaction Administrator Change Log*.

Enable MWI

Select the check box to indicate this user has an MWI-enabled phone and wishes to use the feature. Clear the check box to disable the MWI feature for this user.

If you enable this feature you must select one of the following options:

- **Send to Default or Logged Workstation**: (default) Select this option to send the indicator to the station the user is logged into. If the user is not logged in, it sends the indicator to the user's default workstation.
- **Send to Following Address**: If you select this option, you must also enter the **Address** or directory number.

> **Note:** To fully enable the MWI feature, you must activate MWI for the default station, for the station that user uses, and for the user.

Related topics

Activate MWI for the default station

Activate MWI for a station

Configure a user

Phonetic spellings

You can set phonetic spelling options for users workgroups. Use this page to define alternate (phonetic) spellings of the user name or workgroup name for Text To Speech (TTS) and Automatic Speech Recognition (ASR).

> **Note:** If you enabled the Enhanced Interaction Administrator Change log, then all of your changes on this page are tracked in that log. For more information, see *About the Enhanced Interaction Administrator Change Log*.

Text To Speech

Type the phonetic spelling of the user's or the workgroup's name.

The TTS spelling should be a single-valued attribute. Spell the name like it sounds. For example if you have a user name spelled "Rose," but it is pronounced "Rosy," then enter "Rosy."

Automatic Speech Recognition

Enter the user's or workgroup's phonetic spelling of the name. You can specify multiple spelling entries for ASR. The ASR spelling attribute should be a multi-valued attribute.

The ASR phonetic spelling values are used by the Reco Create Company Directory Grammar. You can specify any valid grammar token, including nicknames or different spellings of a user's name.

For example, assume a user is called "John Smith." This is the first name and last name known to the CIC system, and this spelling entry is used by default for the company directory grammar. To add spelling entries to increase the grammar coverage, add the following alternate spelling entries:

- Johnny Smith
- John Robert Smith
- John R Smith

> **Note:** Be careful not to add too many alternate spelling entries. If the grammar coverage becomes too broad, or if the company directory contains too many similar names, the recognition quality degrades.

You can also include phonetic spelling entries for a specific language. To do this, at the end of the phonetic spelling entry, type **!*language identifier***.

For example, the following spelling entry indicates that it is for the English language.

Johnny Smith !en-us

> **Note:** You can use only one language identifier for each spelling entry. The language identifier must be the last characters of the spelling entry. Any languages that you specify must be installed on all ASR servers, or the company directory grammar will not compile.

Related topics

Configure a user

User Options

Incoming Faxes

If you configure a **user** as fax-capable in Interaction Administrator (**User Configuration-->Options-->Fax Capability**), then callers to that DID hear ring-back while the handler listens for a fax. The handler then places the call on the queue. If you do **not** configure a user as fax-capable, the call goes directly to that user queue.

> **Note**: If you create new users by importing them or by using Setup Assistant, the default **Fax capability** setting for those users is false.
>
> **Tip**: See Tell Me the Difference Between DID Fax and DID Non-fax Users.

Select the Interaction Connect fax format from the **Web Client Fax Format** list. The options are <None> (default), PDF or PNG. This setting is only available if you do not select the **Default** check box (this check box indicates you want to use the default system setting).

> **Note**: For faxes in TIFF format, select TIFF faxes in the list of security rights on the user Security tab.
>
> When a fax is sent specifically to a user, system handlers first check for the TIFF faxes security right. If the security right isn't enabled, the system then checks the user's Web Fax Format setting.

Unified Messaging

Select the server destination from the drop-down list for messages when using SIP diversion, or click Advanced Options to specify to use the CIC user extension (default), or to use other number for Unified Messaging (UM).

> **Note**: For UM users to receive voice mail, faxes, and email, each user will have a uniquely named email account, which you specify in Mailboxes Selection. For more information on configuring CIC to use UM, see *Unified Messaging Integration with Interaction Center* in the PureConnect Documentation Library.

Interaction Alerting

Select the **Auto Answer Non-ACD Interactions** check box if you want CIC to automatically connect non-ACD interactions to an agent's phone. When a interaction alerts on a user's queue, you can use the Alert tool in Interaction Designer to play a tone, a .WAV file, or both, to inform the agent about the incoming interaction. These are called "whisper tones." This is useful if you are using auto-answer but want to warn an agent that another interaction is about to connect to his or her queue. If this box is selected, an agent must be at his or her station to be automatically connected to a interaction.

Clear this check box if you want to alert an agent and not automatically connect the interaction. When the agent's CIC client rings, he or she must manually click the Pickup button or pick up the handset to answer the interaction.

> **Note**: This setting applies to DID/DNIS or ACD calls, but does not apply to non-ACD workgroups calls.

Alerting Action

Select an action to start each time a non-ACD call enters an alerting state (for example, the station rings) in a user or workgroup queue. Actions in this list are defined in the Actions container. For the complete procedure, click here.

Disconnected Action

Select an action to start each time a call moves from the Connected state to a Disconnected state. Actions in this list are defined in the Actions container in the Interaction Administrator hierarchy.

Incoming Interactions

Set the **Timeout** in minutes and/or seconds that an incoming interaction rings at the CIC client station before the interaction quits alerting and proceeds to the next step in the handler (for example, goes to voicemail or changes an ACD agent's status to "ACD-Agent not answering" and offers the interaction to another agent). The **Default** check box indicates the timeout value is the system default of 30 seconds. You can change the value by de-selecting the **Default** check box and using the up and down arrows to adjust the number (7 seconds is the minimum). Use the drop-down list to select Seconds, Days, Hours or Minutes.

Parked Interactions

Use this section to set the maximum time that a parked **call**, **chat**, **email**, or **generic object** will wait on silent hold, and to specify the extension that interaction will be transferred to when the time has elapsed.

Timeout (minutes)

Set the maximum time in minutes here that a parked call should wait before transfer to the specified extension.

Extension

Set the destination extension here for a parked call that has reached its timeout.

Tracing

Tracing allows users to set trace levels for various IceLib (Interaction Center Extension Library) -based client applications through Interaction Administrator. Click Tracing... to display the Tracing Configuration page.

Overview of security for people

You can configure security for the default user, for roles, for a user, or for a workgroup.

Because users inherit one or more properties from the default user, roles and workgroup, the Security page is available from each of these containers. See *Configuration Property Inheritance* for an explanation of how these properties are related in each container.

> **Note:** If you enabled the Enhanced Interaction Administrator Change log, then all of your changes related to user security are tracked in that log. For more information, see *About the Enhanced Interaction Administrator Change Log*.

For more information on the types of security available for people, see the links under *Related topics*.

Related topics

Overview of the master administrator rights

Overview of administrator access rights

Overview of access control rights

Overview of security rights

Configuration property inheritance

Custom attributes

The Custom Attributes page allows you to add customized attributes so that you can reference your own variables and settings through the IceLib interface.

> **Note:** If you enabled the Enhanced Interaction Administrator Change log, then all of your changes to the Custom attributes page in the User Configuration dialog box and the Workgroup Configuration dialog box dialog box are tracked in that log. For more information, see *About the Enhanced Interaction Administrator Change Log*.

The page contains a list for the attributes and displays a **Name** and a **Value** column, and has the following buttons:

Add

Click **Add** and select an existing custom attribute from the pull-down list, enter a new custom attribute. If creating a new attribute, use a unique name, otherwise the existing attribute will be overwritten.

Edit

Click **Edit** to change the value of an existing custom attribute.

Delete

Click **Delete** to delete an existing custom attribute.

Manage Attributes

Click **Manage Attributes** to open a dialog box that displays a list of custom attributes. Click **Add** or **Delete** to manage the appearance of the custom attributes in the pull-down list.

The custom attributes are saved in the path of the root container. This **Path** is displayed at the bottom of the dialog box.

> **Note**: For more information on the Interaction Center Extension Library (IceLib), see The **System APIs section** in the PureConnect Documentation Library on the CIC server.

History

This page provides a way to manually document configuration changes and when they occurred. Changes made in Interaction Administrator are also automatically logged in the Interaction Administrator Change Notification Log (Log ID 7). Later, authorized users can run reports against this log to summarize all configuration changes.

> **Note:** If you enabled the Enhanced Interaction Administrator Change log, then all of your changes to the History page in the User Configuration dialog box and the Workgroup Configuration dialog box dialog box are tracked in that log. For more information, see *About the Enhanced Interaction Administrator Change Log*.

Last Modified

This date is automatically updated each time you click the **OK** button, presumably after you make changes to the configuration. To avoid updating this date, exit the page by clicking the **Cancel** button.

> **Note:** If you click **Cancel**, none of the changes made to this page will be preserved.

In addition, the history is updated when changes are made to the record elsewhere in Interaction Administrator. For example, when a user change his or her password, the **Last Modified** date is updated.

> **Note:** Changes to the licenses for a user or a station do not update the Last Modified date.

Date Created

This date is automatically set when the user creates the initial configuration for this page. If the page was initially created during setup, the date could be blank.

Notes

Type notes about configuration settings and changes. If you change the configuration page and click **OK**, the **Last Modified** date is updated.

You must manually enter the date beside each entry in the **Notes** field to identify the date of each note.

To create a new line in the **Notes** field, press Enter.

Workgroups

Overview of workgroups

Workgroups are logical groups of users (for example, departments) that can function as a group in the CIC system. Workgroups can have extensions and queues that enable all members of a Workgroup to receive calls notifying the Workgroup. In addition, Workgroups can receive regular calls and ACD calls to specific Workgroups and agents. You may also create Workgroups to serve as distribution lists (to the members) for voice mail, email, and faxes from within CIC.

Related topics

About inheritance of configuration properties

Add a workgroup

Add a workgroup

> **Note:** If you enabled the Enhanced Interaction Administrator Change log, then the addition of the workgroup is tracked in that log. For more information, see *About the Enhanced Interaction Administrator Change Log*.

To add a workgroup

1. In the **People** container, click the **Workgroups** subcontainer.
2. Right-click and then select **New**.
3. In the **Entry Name** box, type the workgroup name and click **OK**.

> **Note:** Do not exceed 64 characters.

4. In the **Workgroup Configuration** dialog box, complete the tabs. See the links under **Related topics** for complete information.

Related topics

Configuration

Files

Members

Roles/Supervisors

Wrap-up Codes

ACD (automatic call distribution)

Phonetic Spellings

Secure Input Forms

Options

Security

Custom Attributes

History

Overview of workgroups

Workgroup name

Type a name that describes the purpose and/or nature of the group. For example, if a workgroup queue is solely for ACD calls, use "ACD" as part of the workgroup name, e.g., "ACD - DB Support".

A workgroup name should be no more than 50 characters long (25 characters with a double-byte character set). It must start with an alphabetic character and contain no colon (:) or backslash (\). It may contain spaces.

> **Note**: Profile names in Interaction Attendant should not contain the name of a workgroup to prevent routing errors. See the **Custom Inbound Call Profile Node** help in the Interaction Attendant help for more information.
>
> Do not exceed 64 characters.

Related topics

Add a workgroup

Configure a workgroup

Configure a workgroup

To configure a workgroup

1. In the **People** container, click the **Workgroups** subcontainer.
2. Double-click the workgroup that you want to edit.
   The **Workgroup Configuration** dialog box appears. Complete fields on the tabs. See the links under **Related topics** for complete information.
3. Click **OK**.

Related topics

Configuration

Files

Members

Roles/Supervisors

Wrap-up Codes

ACD (automatic call distribution)

Phonetic Spellings

Secure Input Forms

Options

Security

Custom Attributes

History

Files

Files

Select the voice mail and on hold messages, and the on hold music you want to assign to this workgroup.

Voicemail Message

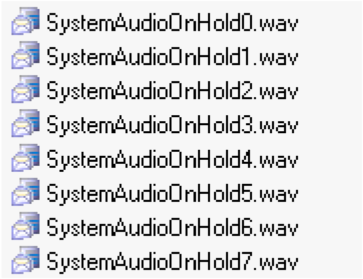
Use this setting to specify the path to a (.wav) file to be played as the voice mail message for the workgroup (ACD or non-ACD).

On Hold Music

CIC plays the named wave (.wav) file each time a call is put on Hold. By default CIC plays the random wave file (SystemDefaultAudioOnHold.wav) file in the \Resources directory. You can also click **Configure** to specify a random wave from Media Server, use a set wave file (optionally from Media Server), or use an audio source.

CIC's On Hold Music selection criteria:

CIC installs eight system audio (.wav) files and stores them on the CIC server in the \\IC\Resources directory:



SystemAudioOnHold0.wav
SystemAudioOnHold1.wav
SystemAudioOnHold2.wav
SystemAudioOnHold3.wav
SystemAudioOnHold4.wav
SystemAudioOnHold5.wav
SystemAudioOnHold6.wav
SystemAudioOnHold7.wav

The .wav file selected to play for external incoming and intercom calls 'held' (not to be confused with the 'ACD wait' state), is determined by the modulus value matching the .wav file name. The handler containing the mod(x,x) function processes the values based on seconds of the current time, returns the modulus, and selects *SystemAudioOnHold***[modulusvalue]***.wav*.

For example, Mod(35,8) returns a modulus of "3". Based on this value, the system selects and plays *SystemAudioOnHold3.wav*. If the modulus was "6", the system would select and play *SystemAudioOnHold6.wav*.

Customers can record their own wave files and replace the files above as long as these two conditions are met:

- The files must be in CCITT mu-law format.
- The file names must be exactly as above.

> **Caution**: If you replace any of the .wav files (including the *SystemAudio[x].wav* or *Ringback[x].wav* files) in the Resources directory with your own customized files, then these files will be overwritten when updating. If you have replaced any of these files in the Resources directory, back up your customized files before updating, then restore the files after the update is complete. This applies to the files on CIC servers and on Media Servers.

On Hold Message

You can specify a recorded message in a sound file to play when a caller is placed on hold. CIC plays the message as long as the call remains on hold in the workgroup queue until the call is routed to an agent for the first time.

Audio Configuration

Use this page to select the on hold audio or in-queue audio (as configured in Media Server) to play to the caller.

> **Note**: The optimal format for .wav files depends on your system configuration. A safe format to use (which is also optimal in many configurations) is 8 kHz mono mu-law PCM.

Use Random Wave File

Select this option to play random wave files from the Resources folder on the CIC server for in-queue audio for this workgroup.

Use Wave File

Type a parameter or the drive, path, and .WAV file name found on the IC server. For example, `C:\I3\IC\server\sounds\support.wav`, where C: is the local drive of the IC server. Use this to specify a unique wave file to play in-queue audio for this workgroup.

Use Audio Source

If you are implementing the Audio Sources feature to identify a single audio stream to be played to calls waiting in the workgroup queue, select an audio source from the drop-down menu. See Audio Sources for complete audio source configuration instructions.

Select **Only play this audio source for ___ seconds**, and enter the number of seconds to limit the length of the audio playing time.

For more information on Media Server, see *Interaction Media Server* in the **Technical Reference Documents** section of the PureConnect Documentation Library on the CIC server.

Workgroup Members

Select the users you wish to belong to this workgroup. You can optionally specify a fixed linear hunt order for alerting Workgroup members when the workgroup has a queue, and it is not an ACD queue.

> **Note:** If you enabled the Enhanced Interaction Administrator Change log, then all of your changes on this page are tracked in that log. For more information, see *About the Enhanced Interaction Administrator Change Log*.

Available Users

Names in the **Available Users** list are registered on the server but are not members of this workgroup. To add one of these users to this workgroup, which is indicated by the user’s name appearing in the **Currently Selected Users** list, do one of the following:

- Double-click a user’s name, *or*
- Select a user's name and click **Add**.

Currently Selected Users

Names in the **Currently Selected Users** list are members of the current workgroup. To remove a user from this workgroup, which is indicated by the user’s name appearing in the **Available Users** list, do one of the following:

- Double-click the user’s name, *or*
- Select the user’s name and click **Remove**.

Maintain Order

Select this check box to preserve the order of the **Currently Selected Users** list. Handlers can optionally use this **Currently Selected Users** list as an ordered (linear) hunt group for alerting users in workgroup queues (not ACD queues). The Alert Workgroup tool includes a check box that allows you to alert all users in a workgroup at the same time, or in a sequential order. If the Alert Workgroup tool specifies a sequential order, and the **Maintain Order** check box is selected, workgroup members will be alerted in the order specified in the **Currently Selected Users** list, starting at the top.

To arrange the order of user selection

1. Click the **Maintain Order** check box at the bottom of the **Currently Selected Users** list to create a fixed order of user selection.
2. Click on the name of the user to be first in order to receive calls in this workgroup queue.
3. Click the **Up** button until that user’s name is at the top of the list.
4. Select the name of the user to be second in order to receive calls in this workgroup queue.
5. Click the **Up** button until that user’s name is second from the top of the list.
6. Select each user’s name and click the **Up** or **Down** button to determine the order in which each user is selected to receive calls that alert on this workgroup queue.
7. Click **OK** to save this order and exit.

For additional information, see **Alert Workgroup tool** in Interaction Designer Help.

Roles/Supervisors

Use this page to assign roles and supervisors to this workgroup. Assigning a role to a workgroup gives the role's permissions to the workgroup members. Assigning a supervisor to a workgroup, associates that supervisor with the supervisor alerts for this workgroup.

> **Note:** If you enabled the Enhanced Interaction Administrator Change log, then all of your changes on this page are tracked in that log. For more information, see *About the Enhanced Interaction Administrator Change Log*.

Roles

To assign a role to this workgroup, in the **Roles** box click **Add**. You must already have defined one or more roles in the Roles container.

To delete a role, select the role and click **Delete**. You can select and delete multiple roles.

Supervisors

If agents need to alert a supervisor, they can type a message and broadcast it to all CIC clients.

To assign a user as a supervisor for this workgroup, in the **Supervisor** box click **Add**. This feature affects the CIC clients.

Related topics

About roles

Wrap-up Codes

> **Note:** If you enabled the Enhanced Interaction Administrator Change log, then all of your changes on this page are tracked in that log. For more information, see *About the Enhanced Interaction Administrator Change Log*.

To configure wrap-up codes for a workgroup

1. To prompt workgroup members to enter a wrap-up code for every interaction, select the **Wrap-up Active** check box.
2. In the **Keypad wait time** box, type the number of seconds that the TUI displays a message to prompt the agent to enter a wrap-up code. When the agent enters the wrap-up code, the TUI removes the prompt. The default is 30 seconds.

> **Note**: The CIC clients also prompt the agent to enter a wrap-up code. The agent can chose whether to use the TUI or the CIC client to enter the wrap-up code. If this is confusing, you can turn off the TUI prompt. To do this, type 0 in the **Keypad wait time** box.

3. In the **Client wait time** box, type the number seconds that the CIC client displays a message to prompt the agent to enter a wrap-up code. When the agent enters the wrap-up code, the CIC client removes the prompt. The default is 30 seconds.
4. In the **Prompt name** box, type the name of the file that instructs the user to enter data.

Related topics

Wrap-up codes overview

ACD

Workgroup ACD

Use this tab to configure ACD settings for the workgroup. Depending what you select in the list on the left, select the related options on the right. The available areas are:

- Utilization
- Skills
- Statistics
- Routing
- Actions
- Wrap-up Codes
- Options

Utilization

You can set these utilization options at the workgroup or user level (user settings override workgroup settings). Agents can handle multiple phone calls and other interactions simultaneously and in any combination. Using the ACD Utilization settings, you can configure how much of an agent's attention would be required for each of the interaction types as a percentage.

For example, if, as an administrator, you set the Chat category for an agent to 25%, it would mean that the agent could handle up to four chat events simultaneously. Indicating 100% for an event type would mean that the agent could handle only one such event at a time.

The percentages might vary from agent to agent based on their experience. Agents are available to the extent that the sum of the percentage utilization of all their current interactions is less than 100.

For example, if an agent is configured so that phone calls are set to 100 percent, chats to 25 percent, and email messages to 10 percent, then the agent could, at any given time, process one phone call, or four chats, or two chats and five email messages, or one chat and seven email messages, and so forth.

> **Note**: Once an interaction enters a conference or enters an ACD queue as the consult portion of a consult transfer, utilization is no longer recognized. If an interaction is transferred to an ACD Queue, utilization is only recognized if the transfer is a blind transfer.
>
> **Note:** If you enabled the Enhanced Interaction Administrator Change log, then all of your changes on this page are tracked in that log. For more information, see *About the Enhanced Interaction Administrator Change Log*.

Interaction Type

The **Interaction Type** list displays the interaction types assigned to this workgroup or user, including Call, Callback, Chat, Email, Generic Object, Social Conversation, Social Direct Message, or Work Item.

% Utilization

The **% Utilization** list shows the percentage of an agent's attention required for each interaction type.

When you add an Interaction Type, the percent utilization you assign to that interaction appears in this list. By default, the **% Utilization** is 100%.

> **Tip**: Set the percent utilization for Calls to **51% or more** when either or both of the following conditions apply:
>
> - You have selected **Auto answer** for the agent.
>
> - You have selected **Exempt held interactions** for the agent.

Under the above conditions and at less than 51% utilization, if an agent is on a call and another call comes in, the CIC client puts the first call on hold automatically and connects the incoming call.

Since calls on hold (held interactions) are exempt and do not count against the agent's percent utilization, the CIC client will continue putting active calls on hold automatically and connecting new calls to that agent.

Setting 51% or more utilization ensures that an agent handles only one call at a time. Setting it at 50% allows the CIC client to assign two calls simultaneously to the agent, one active and one on hold (achievable by some agents).

> **Note:** Calls at 50% or less utilization with a maximum assigned of 1 will only allow 1 call.

Max. Assign.

The **Max. Assign.** list displays the maximum number of interactions allowed for this interaction type. By default, the value of **Max. Assign** is "1" for Call interaction type. The default value of **Max. Assign** for all other interaction types is "0".

Edit

Select an interaction type and click **Edit** to see the **Edit** dialog where you can change the percent utilization for a Call, Chat, Email, or other interaction type.

Workgroup ACD Skills

Workgroup queues can be used to deliver regular calls and ACD calls. Regular calls can appear on a workgroup queue and be answered by any workgroup member monitoring that queue. ACD calls are routed to the appropriate workgroup based on caller input. All members of that workgroup (call agents) are expected to have a core set of skills required to handle any call on that queue. Further ACD processing directs the call to the most appropriate agent who is a member of that workgroup based on each agent's User ACD configuration. This page defines the minimal skill set required by all members of this workgroup who handle ACD calls.

If this workgroup does not have a queue or does not handle skills-based ACD calls, no skills are required.

Skills

This field contains skill names required for members of this workgroup who handle skills-based ACD calls.

To enter a skill for this workgroup:

1. Click **Add** to add a skill requirement.
2. Select a skill name from the list and click **OK**.

> Skill names are created in the Skills section in the People container.

Proficiency

Type a value of 1 - 100 to indicate the minimum proficiency of skill level that an agent must have in order to receive an ACD call that requires this skill. 100 represents the highest skill level required. You define the skill attributes, which include proficiency level, for an agent on the **ACD configuration** page. The default value is 1. By default, the weight for proficiency is equal to 1, so this value is included in the ACD skills calculation.

Desire to Use

Type a value from 0 - 100 to indicate the minimum desire to use level agents must have in order to receive an ACD call that requires this skill. 100 is the highest possible desire; the higher the number, the more often the user wants to use the skill. Remember, desire to use is different than knowledge or ability. An agent can have a high level of proficiency (ability), but very little desire to use that ability. The default value is 0.

> **Notes:** A user inherits the desire setting for a skill from any workgroup(s) to which the user belongs. However, you can override this with a user-level proficiency setting.
>
> By default, the weight for Desire to Use equals 0, so the value that you specify is evaluated only as a qualifier instead of as the specified Desire to Use range for the ACD interaction. The Desire to Use setting is considered for ACD skill calculations when ACD customization points (such as CustomACDInitiateProcessing) are used. The weight for Desire to Use must be set to a value greater than 0 in order for it to be considered in ACD skills calculations. For more information on skills-based routing using the ACD Specify Interaction Skill Tool, see the *ACD Processing Technical Reference* or the white paper, ACD Processing: CIC's Automatic Communication Distribution in the Documentation Library.

Related topics

Skills

Utilization

Statistics

Routing

Actions

Wrap-up

Options

ACD Statistics

You can set ACD statistic shift start options for a user or for a workgroup.

> **Note:** If you enabled the Enhanced Interaction Administrator Change log, then all of your changes on this page are tracked in that log. For more information, see *About the Enhanced Interaction Administrator Change Log*.

Call Statistics

The Call Statistics fields appear only in the workgroup configuration since these fields affect only call statistics for Workgroup (that is, ACD) queues that belong to an ACD Workgroup.

Statistics Period

The is the number of minutes used to define the "current period" and the "previous period" statistics on the Queues page in Interaction Supervisor. The statistics period includes every X number of minutes from midnight to the current time, where X is the number in the field. The default time is 30 minutes, which means the "current period" and "previous period" changes on every half-hour boundary.

Estimated Call Time Interval

The ACD Statistics (Call or Queue) tools in a handler that provides callers with estimated wait time feedback, uses this number of minutes in its wait time calculation. This is a rolling interval, which means the interval is the number of minutes prior to each use of the estimated wait time function as it is invoked on the CIC server. The ACD Statistics tools calculate the estimated wait time for a caller in a queue by taking the average time all callers waited in the queue during the current interval (for example, the previous 30 minutes from the time the ACD Statistics tool in a handler was invoked). The default setting for the interval is 30 minutes.

Statistic Shift Starts

This list of times determines the beginning time and duration of each shift for this user or the members of the current workgroup. These times are used to define (relative to the current time) the "current shift" and the "previous shift" on the Queues page in Interaction Supervisor. The default statistic shift is a 24 hour shift starting at midnight (0:00), meaning the statistics are relative to one day (or 24 hours).

Use the **Add** and **Delete** buttons to add or remove shift times. To change a shift time, first delete it and then add a new time to replace it.

Routing

Routing

You can set routing options at the user or workgroup level. Multiple mailboxes can now be monitored by a single workgroup or user. For each mailbox folder that feeds a queue, Interaction Administrator stores the email address. Because of address lookup, each entry in the list has mailbox, email address, inbound folder, and queued folder. The mailbox and email address uses the same method that is used for associating a user with a workgroup.

> **Tip**: See Set Up Email Routing on ACD Queues.
>
> **Notes**: When searching for a mailbox to select for ACD email routing, distribution lists and public folders are not listed in the search.

> You cannot create an SMTP-monitored mailbox through a workgroup's ACD. If SMTP and IMAP are active, however, you can configure an SMTP/IMAP mailbox through a workgroup's ACD.

ACD Email Routing Active

Use this check box to activate email routing. When activated, CIC uses the same rules for email arriving for the workgroup as it does for calls and faxes.

Mailboxes:

Click Add to open the **ACD Email Routing Mailbox** dialog box.

Save replies to Sent Items folder

When this option is enabled, ACD routed email replies are saved to the Sent Items mailbox associated with the workgroup. This feature is supported for Exchange (EWS) integrations only.

Adding an ACD Email Routing Mailbox

Use this page to add an ACD email routing mailbox.

Mailbox

Click the browse button to open the **Mailbox Selection** dialog box.

Use this mailbox to send outgoing emails

Select this check box to use this mailbox when an agent sends an email message through the CIC clients to a workgroup queue. This outbound email interaction is tracked similar to the way in which an inbound email interaction is tracked in CIC.

Use this mailbox to receive emails

Select this check box to receive workgroup queue emails in this mailbox.

Inbound Folder

Select the folder for routed email from the list. This is the receiving folder in the associated mailbox. CIC polls the inbox every few seconds to see if a new email has entered.

Allow to Receive Encrypted Email

Select this option to support the use of the S/MIME type in email. Selecting this check box enables support of email encryption, but other configuration, such as installing certificates, is necessary. For more information see *CIC Security Concepts* in the **Technical Reference Documents** section of the PureConnect Documentation Library.

Related topics

Mailbox selection

Attendant mailboxes

Email certificates configuration

ACD Actions

These ACD actions options can be can be set at the user or workgroup level. ACD calls directed to an agent's station can initiate DDE, custom screen pop, or web browser screen pop actions when the call rings on an agent's station, is disconnected, or transferred from the agent’s station. For example, when an ACD call alerts the agent's station, a database application can start. When the call is disconnected or transferred, either of those actions can initiate another database application specifically used for completing records or follow up on the call. The Actions property page specifies which actions are used with ACD calls to this workgroup or user. Each workgroup or user may use different actions or no actions at all.

Alerting Action

Select a custom screen pop, web browser screen pop, or DDE action to start on an agent's workstation each time a call enters an alerting state (for example, the station rings) in this workgroup queue. Actions in this list are defined in the Actions container.

Disconnected Action

Select a DDE action to start on an agent's workstation each time a call moves from the Connected state to a Disconnected state (that is, the call terminates) in this workgroup queue. Actions in this list are defined in the Actions container.

No-answer Status

Select a status message from the list to display in an agent's My Status box when an agent is alerted by an ACD interaction and does not answer it. The selected status message should have the "Status is Do Not Disturb" attribute set on the Status Message Configuration page.

> **Note**: The default setting is ACD - Agent Not Answering unless another status has been specified by the workgroup. If a user is a member of multiple workgroups, and just one of those workgroups is configured to change members' status to 'agent not answering' when there is no answer, then the no-answer behavior applies to this user for all workgroup memberships.

Revert to Available After

Set this time interval (in seconds) to automatically return an agent's status to what the status was prior to going to Agent Not Answering. If the status has been changed in the meantime, the agent's status will not be reset. The default value is 0 which does not automatically revert the status.

Transfer Action

Select a DDE action to start on an agent's workstation each time a call is not answered or is transferred by the agent in this workgroup queue. Actions in this list are defined in the Actions container.

If an agent does not pick up an alerting ACD call, the call times out and the agent's status is automatically changed to ACDAgentNotAnswering. The Alerting Action may need to be terminated, or some other action performed if the agent does not pick up the call. When the agent's status is ACDAgentNotAnswering, the agent is not assigned any more calls until he or she changes the status to Available.

If an agent transfers a call using a CIC client, the same Transfer Action may optionally be invoked if the Execute Transfer Action on the User Transfer check box is selected.

Execute Transfer Action on User Transfer

Select this check box to automatically invoke the Transfer Action DDE command when an agent manually transfers a call from his or her station. Leave the check box blank to perform no DDE action when an agent manually transfers a call. If a Transfer Action is defined and this check box is blank, the Transfer Action is invoked only when an ACD call is not picked up at an agent's workstation and then transfers to another agent.

Incoming Transfer Action

Select a DDE action to start on an agent's workstation when that agent receives an ACD call transferred from another agent. This allows an agent who starts an ACD call to transfer that call to another agent and allows the second agent to see the appropriate DDE action when the call alerts.

This action is valid only when the transfer is from one user to another user (not from a user to a workgroup, line, station, or other type of queue).

On Call Status

Select a status message from the list to assign to an agent (and display in an agent's My Status box) while the agent is on an ACD call. After the call disconnects, the agent's status changes to Follow up (or the Wrap Up Status setting) for the designated period before returning to the agent's status before the call (for example, Available).

Wrap-up Status

Use this page to configure the behavior of after call work status for this workgroup.

Status

Select a status message from the list to assign to an agent (and display in the agent's My Status box) while the agent is in the After Call Work (ACW) time. The ACW time begins after an ACD call is terminated; this is when the optional DDE Disconnected Action begins. When the specified ACW period ends, the agent's status message is set to Available again. The selected status message should have the "Status is ACW (After Call Work)" attribute set on the Status Message Configuration page.

> **Note**: If an agent is in an After Call Work (ACW) status at the time a Switchover occurs, the agent's status will not automatically be set to Available after the specified ACW period ends. The agent will need to manually change his status to Available. Supervisors should check for agents who have forgotten to do so after the Switchover event.

Time

Type the number of seconds to allow a CIC client user to finish any After Call Work (ACW) associated with the previous call before becoming available to receive a new call. For example, a value of 180 seconds allows call agents three minutes between the time they end a call and the time they appear on the available list for taking a new call.

If you specify no time, each Workgroup member is considered available to receive calls as soon as the current call is disconnected.

You cannot set a Wrap-Up Time until you select a compatible Status in Wrap-Up Status entry box.

Exempt held interactions

Click this box to allow agents who have ACD interactions on hold to receive new ACD interactions within the parameters listed below. The default CIC client behavior is for the agent with held interactions to be unavailable and for the agent with the highest computed score among those remaining in the workgroup to receive the next ACD interaction.

> This feature does not apply to **direct interactions** that an agent puts on hold**.**

Max number of exempt interactions

Type the maximum number of interactions an agent in a given workgroup can have on hold and still receive another ACD interaction. The default is **1**.

For example, if you set this parameter to **3**, then a workgroup agent could have **three** interactions on hold and still receive an additional ACD interaction. An agent with **four** interactions on hold would **not** receive another interaction until the number of interactions on hold dropped to **three** or fewer.

Grace Period before new interaction

Type the period of pause in seconds before the workgroup agent receives the next interaction. The default is **10** seconds.

Agent score change amount

Type the value you want to add to the computed agent score for each interaction on hold. You might use this to ensure a more even distribution of interactions among the workgroup members. The default is **-10**.

For example, if Agent A has a score of 75 with one interaction on hold and Agent B has a score of 70 with no interactions on hold, applying the Agent Priority change would add -10 (for each held interaction, in this case one call) to Agent A's score, reducing it to 65. Agent B, with no held interactions and a score of 70, would then receive the next ACD interaction.

Direct calls

If Agent C, with a score of 80, receives a **direct** (non-ACD) call and puts the call on hold, the CIC client regards Agent C as unavailable while that direct call is connected because the **Exempt held interactions** feature is not applied to direct calls.

Workgroup ACD Options

Select The **Use Availability Time in Skills Calculation** check box to change the calculation of how skills are configured. By default this check box is selected so skills are calculated on a formula that uses Availability Time, in addition to Desire to Use and Proficiency. Interaction Attendant uses skill settings in the skills-based routing.

Phonetic spellings

You can set phonetic spelling options for users workgroups. Use this page to define alternate (phonetic) spellings of the user name or workgroup name for Text To Speech (TTS) and Automatic Speech Recognition (ASR).

> **Note:** If you enabled the Enhanced Interaction Administrator Change log, then all of your changes on this page are tracked in that log. For more information, see *About the Enhanced Interaction Administrator Change Log*.

Text To Speech

Type the phonetic spelling of the user's or the workgroup's name.

The TTS spelling should be a single-valued attribute. Spell the name like it sounds. For example if you have a user name spelled "Rose," but it is pronounced "Rosy," then enter "Rosy."

Automatic Speech Recognition

Enter the user's or workgroup's phonetic spelling of the name. You can specify multiple spelling entries for ASR. The ASR spelling attribute should be a multi-valued attribute.

The ASR phonetic spelling values are used by the Reco Create Company Directory Grammar. You can specify any valid grammar token, including nicknames or different spellings of a user’s name.

For example, assume a user is called “John Smith.” This is the first name and last name known to the CIC system, and this spelling entry is used by default for the company directory grammar. To add spelling entries to increase the grammar coverage, add the following alternate spelling entries:

- Johnny Smith
- John Robert Smith
- John R Smith

> **Note:** Be careful not to add too many alternate spelling entries. If the grammar coverage becomes too broad, or if the company directory contains too many similar names, the recognition quality degrades.

You can also include phonetic spelling entries for a specific language. To do this, at the end of the phonetic spelling entry, type **!*language identifier***.

For example, the following spelling entry indicates that it is for the English language.

Johnny Smith !en-us

> **Note:** You can use only one language identifier for each spelling entry. The language identifier must be the last characters of the spelling entry. Any languages that you specify must be installed on all ASR servers, or the company directory grammar will not compile.

Related topics

Configure a user

Secure Input Forms: Workgroups

Use this page to make the secure input forms available to a workgroup and give workgroup members access to the form.

Click the form in the **Available Forms** list, and click **Add** (or just double-click the form) to add it to the **Currently Selected Forms** list.

> **Note**: If the dialog box does not include the **Secure Input Forms** tab, verify that you have enabled secure input and defined at least one secure input form. Those two steps add the tab to the dialog box.

Workgroup Options

Incoming Faxes

If you configure a workgroup as fax-capable in Interaction Administrator (**Workgroup Configuration-->Options-->Fax Capability**), callers to that DID hear "Welcome to CIC," then ring-back while the handler listens for a fax. The handler then places the call on the queue. If you do **not** configure a workgroup as fax-capable, the call goes directly to that workgroup queue.

Select **Use TIFF for faxed sent to this workgroup** for received faxes to be in the Tagged Image File Format. You can also select the Interaction Connect received fax format from the **Web Client Fax Format** drop-down list. The options are <None> (default), PDF or PNG. This setting is only available if you do not select the **Default** check box (this check box indicates you want to use the default system setting).

Non-ACD Interactions

Alerting Action

Select an action to start each time a non-ACD call enters an alerting state (for example, the station rings) in a workgroup queue. Actions in this list are defined in the Actions container. For the complete procedure, click here.

Disconnected Action

Select an action to start each time a call moves from the Connected state to a Disconnected state. Actions in this list are defined in the Actions container in the Interaction Administrator hierarchy.

Incoming Interactions

Select the **Warn if chat response time exceeds limit** check box to indicate to a workgroup agent that an ACD-routed chat interaction response time is nearing the limit. When this warning is enabled, you can set the **Response time limit** in seconds that you want to use.

To set the **Operator target**, enter the telephone number or extension to which to send callers that choose zero to exit out of voice mail for this workgroup. See also How Do I Set Up Operator Target?

Set the **Timeout** in minutes and/or seconds that an incoming interaction rings at the CIC client station before the interaction quits alerting and proceeds to the next step in the handler (for example, goes to Voicemail or changes an ACD agent’s status to "ACD-Agent not answering" and offers the interaction to another agent). The **Use Default** check box indicates the timeout value is the system default of 30 seconds. You can change the value by de-selecting the **Use Default** check box and using the up and down arrows to adjust the number (7 seconds is the minimum). Use the drop-down list to select Seconds, Days, Hours or Minutes.

Parked Interactions

Use this section to set the maximum time that a parked **call**, **chat**, **email**, or **generic object** will wait on silent hold, and to specify the extension that interaction will be transferred to when the time has elapsed.

Timeout (minutes)

Set the maximum time in minutes here that a parked call should wait before transfer to the specified extension. The **Use Default** check box indicates the timeout value is the system default of 1 minute. You can change the value by de-selecting the **Use Default** check box and using the up and down arrows to adjust the number (1 minutes is the minimum).

Extension

Set the destination extension here for a parked call that has reached its timeout.

The **Use Default** check box indicates the extension for parked interactions is default workgroup extension as set in workgroup configuration. You can change the value by de-selecting the **Use Default** check box and using the up and down arrows to adjust the extension number (0 is the minimum).

Callbacks

- To enable the use of any attributes that have been set for advanced features, such as Callback Retry, select the **Enable Advanced Callback options in the Interaction Client** option.
- To enable CIC to automatically make callback attempts, select the **Enable callback retries** option.
    - In the **Maximum number of retries** field, select the maximum number of callback attempts that CIC should make for a given interaction.
    - In the **Time between retrying callbacks (min)** field, select the number of minutes between callback attempts.

Tracing...

Tracing allows users to set trace levels for various IceLib (Interaction Center Extension Library) -based client applications through Interaction Administrator. Click Tracing... to display the Tracing Configuration page.

Overview of security for people

You can configure security for the default user, for roles, for a user, or for a workgroup.

Because users inherit one or more properties from the default user, roles and workgroup, the Security page is available from each of these containers. See *Configuration Property Inheritance* for an explanation of how these properties are related in each container.

> **Note:** If you enabled the Enhanced Interaction Administrator Change log, then all of your changes related to user security are tracked in that log. For more information, see *About the Enhanced Interaction Administrator Change Log*.

For more information on the types of security available for people, see the links under *Related topics*.

Related topics

Overview of the master administrator rights

Overview of administrator access rights

Overview of access control rights

Overview of security rights

Configuration property inheritance

Custom attributes

The Custom Attributes page allows you to add customized attributes so that you can reference your own variables and settings through the IceLib interface.

> **Note:** If you enabled the Enhanced Interaction Administrator Change log, then all of your changes to the Custom attributes page in the User Configuration dialog box and the Workgroup Configuration dialog box dialog box are tracked in that log. For more information, see *About the Enhanced Interaction Administrator Change Log*.

The page contains a list for the attributes and displays a **Name** and a **Value** column, and has the following buttons:

Add

Click **Add** and select an existing custom attribute from the pull-down list, enter a new custom attribute. If creating a new attribute, use a unique name, otherwise the existing attribute will be overwritten.

Edit

Click **Edit** to change the value of an existing custom attribute.

Delete

Click **Delete** to delete an existing custom attribute.

Manage Attributes

Click **Manage Attributes** to open a dialog box that displays a list of custom attributes. Click **Add** or **Delete** to manage the appearance of the custom attributes in the pull-down list.

The custom attributes are saved in the path of the root container. This **Path** is displayed at the bottom of the dialog box.

> **Note**: For more information on the Interaction Center Extension Library (IceLib), see The **System APIs section** in the PureConnect Documentation Library on the CIC server.

History

This page provides a way to manually document configuration changes and when they occurred. Changes made in Interaction Administrator are also automatically logged in the Interaction Administrator Change Notification Log (Log ID 7). Later, authorized users can run reports against this log to summarize all configuration changes.

> **Note:** If you enabled the Enhanced Interaction Administrator Change log, then all of your changes to the History page in the User Configuration dialog box and the Workgroup Configuration dialog box dialog box are tracked in that log. For more information, see *About the Enhanced Interaction Administrator Change Log*.

Last Modified

This date is automatically updated each time you click the **OK** button, presumably after you make changes to the configuration. To avoid updating this date, exit the page by clicking the **Cancel** button.

> **Note:** If you click **Cancel**, none of the changes made to this page will be preserved.

In addition, the history is updated when changes are made to the record elsewhere in Interaction Administrator. For example, when a user change his or her password, the **Last Modified** date is updated.

> **Note:** Changes to the licenses for a user or a station do not update the Last Modified date.

Date Created

This date is automatically set when the user creates the initial configuration for this page. If the page was initially created during setup, the date could be blank.

Notes

Type notes about configuration settings and changes. If you change the configuration page and click **OK**, the **Last Modified** date is updated.

You must manually enter the date beside each entry in the **Notes** field to identify the date of each note.

To create a new line in the **Notes** field, press Enter.

Director

Director: Workgroup Configuration

Use this page to manage settings that apply exclusively to Interaction Director post-call routing.

> **Note**: The Director tab and the associated overflow, skills, and error handling options in Workgroup Configuration appear only if Interaction Director is installed and a valid license exists.

The following topics explain Interaction Director options for configuration, skill, overflow, and error handling options in detail.

Related Topics

- Configuration
- Overflow Options
- Skill Options
- Error Handling Options

Director: Configuration Options

Use this page to set Director configuration options.

> **Note**: The Director tab and the associated overflow, skills, and error handling options in Workgroup Configuration appear only if Interaction Director is installed and a valid license exists.

Configuration

When the **Configuration** button is clicked, the following settings related to Enterprise Groups and interactions appear:

Enable Director Processing on this workgroup

This per-workgroup check box enables Director processing for that workgroup. When this box is checked, all calls entering that workgroup will be processed via Director, instead of local ACD.

Enterprise Group

Use this text edit control to specify the Enterprise Group for the workgroup to query. The workgroup does not have to be a member of the Enterprise Group on the Director server.

Enterprise Group browse button

Opens the Browse Enterprise Group dialog box, so that you can select from a list, instead of typing a name manually.

Priority

Per workgroup, specifies an interaction priority which all interactions in this queue will initially inherit. Values can range from 1 to 100. The default priority is 50; higher numbers indicate higher priority.

In Queue Timeout

Specifies the number of seconds that Director will wait for an Agent to pick up the call before performing in-queue timeout actions (running a handler). Director notifies CIC when this time limit passes. CIC can take any action (via a customized handler) such as playing a prompt, transferring the call, and so on.

Related topics

Interaction Director: Workgroup Configuration

Overflow Options

Skill Options

Error Handling Options

Overflow Options

Use this page to set the overflow options for Interaction Director.

> **Note**: The Director tab and the associated overflow, skills, and error handling options in Workgroup Configuration appear only if Interaction Director is installed and a valid license exists.

Overflow

When the **Overflow** button is clicked, a summary of workgroup overflow options appears, listing conditions that will be evaluated when an interaction enters the system via this Queue. These post-call routing rules (conditions) are evaluated in top-down order. A transfer is invoked for the first condition that fails. Overflow rules can be edited or reordered (prioritized) from the summary page.

> **Note**: Overflow conditions specify when an interaction should not be queued, for example, when too many interactions are waiting, when wait time is too high, when an interaction can be serviced immediately, and when there is no viable destination within an enterprise group.

These conditions within the Director system result in some action other than queuing the interaction. The conditions on this tab are evaluated for a newly arrived interaction before it is accepted (i.e. enqueued) by Director. There are five separate conditions: Calls Waiting, Average Wait Time, Longest Wait Time, Immediate Assignment, and No Viable Destination. The first three conditions can be evaluated at any rollup level (Queue, Enterprise Group, Server, System) yielding a great deal of flexibility. For each condition a transfer target can be specified. It indicates where the interaction should go when that condition is triggered. The conditions can be ordered.

Condition

This column lists conditions that will be evaluated when an interaction enters the system via this Queue.

Summary

Displays a logical summary of the configured condition, or "Not Used" if the condition is not enabled.

Edit

This button opens the condition for editing using a dialog box specific to the type of condition:

Overview on Number of Calls Waiting

This dialog sets an overflow condition based on *number of calls waiting*. When this condition is enabled, you can transfer the call to a specific queue or extension when the number of calls waiting in the Queue, Enterprise Group, Server, or system exceeds a configurable limit.

Overview on Average Wait Time

This dialog sets an overflow condition based on *average wait time*. When this condition is enabled, you can transfer the call to a specific queue or extension when the average wait time for the Queue, Enterprise Group, Server, or system exceeds a configurable number of seconds.

Overview on Longest Wait Time

This dialog sets an overflow condition based on *longest wait time*. When this condition is enabled, you can transfer the call to a specific queue or extension when the longest wait time for the Queue, Enterprise Group, Server, or system exceeds a configurable number of seconds.

Overview on no Immediate Assignment Possible

This dialog sets overflow processing that occurs if Director cannot *assign* the call immediately to a monitored server. When this condition is enabled, you can transfer the call to a specific queue or extension.

Overview on no Viable Destination

This dialog sets overflow processing that occurs if there are no viable destinations within an Enterprise Group. "No Viable Destinations" is different from "No Immediate Assignment Possible" in that the latter implies that while there are candidate destinations, all agents might be busy or do not meet the criteria, while the former says there are no candidate destinations at all. This could happen for a variety of reasons, but an example would be that perhaps the Enterprise Group has no members configured, or more likely, all of the member queues are down due to connection loss. In this case, you would not want to make the interaction wait whereas if it is simply a matter of no agents being available you would. When this condition is enabled, you can transfer the call to a specific queue or extension.

Up/Down

Changes the evaluation order of conditions. Topmost conditions are evaluated first.

Related topics

Configuration

Skill Options

Error Handling Options

Skill Options

Use this page to set Director workgroup skills.

> **Note**: The Director tab and the associated overflow, skills, and error handling options in Workgroup Configuration appear only if Interaction Director is installed and a valid license exists.

Skills

When the *Skills* button is clicked, the tab summarizes workgroup skills associated with the Enterprise Group. Skills are evaluated to influence the routing of calls to queues in an Enterprise Group. All interactions that enter the system via this workgroup will initially require the listed skills. The following columns are displayed:

Skill Name

The name of a skill assigned at the workgroup or queue level. Director scores required Skills against the skills of logged in Agents when it determines an interaction's target destination.

Proficiency

This column lists for each skill, *proficiency* values from minimum to maximum, whether or not the bias is positive or negative, and the value of Importance, a weight assigned to this particular skill proficiency.

Desire to Use

This column lists *desire to use* values from minimum to maximum, whether or not the bias is positive or negative, and the value of Importance, a weight assigned to this particular desire.

Add

Click **Add** to open the Enterprise Group Skill Specification dialog box, so that you can define the attributes of a new required skill.

Edit

Click **Edit** to open the selected skill for editing using the Enterprise Group Skill Specification dialog box.

Delete

Click **Delete** to remove the selected skill. You are not asked to confirm this operation.

Related topics

Configuration

Overflow Options

Error Handling Options

Error Handling Options

Use this page to set Director error handling options.

> **Note**: The Director tab and the associated overflow, skills, and error handling options in Workgroup Configuration appear only if Interaction Director is installed and a valid license exists.

Errors

When the **Errors** button is selected, the tab displays options that set flow of control when connectivity between Director and a CIC server is lost while calls are waiting. When the CIC server detects that Director is not reachable, it acts in accordance with the options specified here. The possible actions are wait forever, wait a while and then transfer the call somewhere, or wait a while and let local ACD handle it in place. The following options appear:

Enable Error Handling

This option enables configuration of error processing.

Leave in queue, letting local ACD handle the interaction

This option tells the CIC server not to pass the call to Director or post-call routing. The call will remain in the queue until it is dispatched by local ACD. In short, CIC will transfer the interaction to local ACD in the event of an error.

Transfer to the following target

This option sends the call to the specified workgroup, user name, extension, or external telephone number, or any other transfer type supported by the Extended Blind Transfer (XBT) tool.

Target is passed to a handler. If a Workgroup or User name was specified, the handler passes it to the Extended Blind Transfer tool. If the specified target was not a workgroup, the handler checks to see if it is a user name. If the target was not a workgroup or user name, the entry is passed through dial plan to XBT. If the transfer succeeds, no additional processing occurs. If the transfer fails, the call is transferred to the System queue, where the caller will hear Main Menu prompts again.

Wait time before taking any action

The number of seconds to wait before performing the error recovery action, or 0 to disable delay. In releases before Director 2.3.1, Director would immediately take whatever recovery action was specified when an error occurred. The delay itself was not configurable. In Director 2.3.1 and later, you can configure a time threshold. If the situation rectifies itself within the time allotted, routing resumes where it left off. This can result in less churn in the waiting interaction if a short network glitch occurs.

Related topics

Configuration

Overflow Options

Skill Options

Password Policies

Password Policies

Security policies can be configured for use with CIC passwords and apply these policies per role or user. These policy configurations are very similar to password security policies of Windows. You can define password policies, control password types, and set password change rules, and so on.

You can disguise passwords by setting a parameter. In this case, asterisks (*) appear instead of the actual password.

You can set the following password attributes:

- Minimum Number of Unique Passwords Before One Can be Reused
- Minimum Age of Password Before User Can Change It (days)
- Maximum password age (days)
- Password Age Warning Period (days before password expires)
- Minimum password length
- Minimum number of unique DTMF digits
- Allow or not allow sequential digits
- Maximum number of failed logins
- Lockout duration (minutes)
- Failed Login Count Reser Time (minutes)

- User Must Change Password At Next Login

> **Note:** If you enabled the Enhanced Interaction Administrator Change log, then all of your changes on this page are tracked in that log. For more information, see *About the Enhanced Interaction Administrator Change Log*.

Related topics

Configure a user

Creating Policies

Use this page to create new password policies. Complete the following steps to create new policies or configure the default policy:

1. From Interaction Administrator, select **Policies**.
2. Double-click the **Default Policy** or right-click on the right-hand side of the screen or choose **New** to create a new password policy.
3. Configure the options for the password policy on the following tabs:

Password Policy

1. Enter a description for the password policy in the Description field.
2. Click the check box next to **User must change password next login** if you want the system to prompt the user to change his or her password during the next login.
3. Click **Apply**.

Password

The password tab includes the following options:

- **Minimum Number of Unique Passwords Before One Can Be Reused**:

  Determines the minimum number of unique passwords a user must reach before reusing a password. The default setting is 24.

- **Minimum Age of Password Before User Can Change It (days)**:

  Determines the period of time (in days) that a password must be used before the user can change it. You can set a value between 1 and 999 days, or you can allow changes immediately by setting the number of days to 0. The default setting is 2.

  If the **Maximum Password Age (days)** is more than 0, the **Minimum Password Age** must be less than or equal to the **Maximum Password Age**.

  Configure the minimum password age to be more than 0 if you want the **Password History** policy to be effective. Without a **Minimum Password Age**, users can cycle through passwords repeatedly until they get to an old favorite. Note that if the **Password History** is set to 0, the user does not have to choose a new password. For this reason, **Password History** is set to 1 by default.

- **Maximum Password Age (days)**:

  Determines the period of time that a password can be used before the system requires the user to change it. You can set passwords to expire after a number of days between 1 and 999, or you can specify that passwords never expire by setting the number of days to 0. The default is 180.

- **Password Age Warning Period (days before password expires)**:

  Determines the period of time that reminders will be generated about soon-to-expire passwords. These reminders will be provided in both the CIC clients and through the TUI. This value is ignored if the Maximum Password Age is zero. If this value is greater than or equal to the Maximum Password Age, nagging will occur frequently. You can set this value to zero to suppress warnings. The default is set to 14.

- **Minimum Password Length**:

  Determines the least number of characters that a password may contain. You can set a value of between 1 and 24 characters, or you can set the number of characters to 0 to specify that no password is set for the user, effectively disabling the user account. The default value is 8.

  Note: The **Minimum number of unique DTMF digits** must be less than the **Minimum password length**. If the value of the **Minimum number of unique DTMF digits** is greater than the value of the **Minimum password length**, you will receive a warning message.

- **Minimum Number of Unique DTMF Digits**:

  Determines the minimum number of unique DTMF digits required to be in the password. You can set a value between 1 and 12 digits. The default is 4. While CIC passwords can be composed of digits, punctuation and upper and lower case letters, they are mapped to the 12 standard DTMF digits (0-9, * and #) when entered through the telephone keypad.

  Note: The **Minimum number of unique DTMF digits** must be less than the **Minimum password length**. If the value of the **Minimum number of unique DTMF digits** is greater than the value of the **Minimum password length**, you will receive a warning message.

- **Allow All Sequential Digits**

  This check box allows you to allow or disallow sequential digits in users' passwords. If unchecked, passwords which consist of a sequence (ascending or descending) of consecutive DTMF digits, will not be allowed. This prohibits passwords like "1234" or "9876", but will allow passwords like "1245". While CIC passwords can be composed of digits, punctuation and upper and lower case letters, they are also mapped to the twelve standard DTMF digits (0-9, * and #) when entered through a telephone keypad. This mapped string is used when enforcing the **All Sequential Digits Allowed** policy. The default is set to No, or unchecked.

- **Minimum Number of Uppercase Characters**

  Determines the minimum number of uppercase characters required to be in the password.

- **Minimum Number of Lowercase Characters**

  Determines the minimum number of lowercase characters required to be in the password.

- **Minimum Number of Numeric Characters**

  Determines the minimum number of numeric characters required to be in the password.

- **Minimum Number of Special Characters**

  Determines the minimum number of special characters that are required to be in a user's password. If you complete this box, you must also complete the **Required Special Character Options** box with the special characters that will be counted towards your required minimum number.

- **Required Special Character Options**

  Determines which special characters count towards the required minimum number of special characters. Special characters include: **~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/**
  If you complete this box, you must also complete the **Minimum Number of Special Characters** box.

> **Note:** Users can include other special characters in their passwords. However, only the special characters that you specify in this box count toward the required minimum number of special characters. For example, suppose you require a minimum number of 3 special characters, and you specify the required special characters as !@#*&^. Then a password of JOe@#%1234 is not acceptable because while it contains 3 special characters, it does not contain 3 of the special characters that you require.

Account Lockout

The Account Lockout tab includes the following options:

- **Maximum Number of Failed Login Attempts Before Account is Locked Out**:

  Determines the maximum number of failed login attempts that will be permitted. If this limit is exceeded, an “Account Locked Out” error will be reported until the failed login attempt counter gets reset by an administrator or until the **Account Lockout Duration** has expired. The default setting is 5.

- **Lockout Duration (minutes)**:

  Determines the number of minutes a locked-out account remains locked out before automatically becoming unlocked. The available range is 1 to 99,999 minutes. You can specify that the account will be locked out until an administrator explicitly unlocks it by setting the value to 0. If a **Maximum Number of Failed Login Attempts** is defined, the **Account Lockout Duration** must be greater than or equal to the **Account Lockout Reset Time**. The default setting is 30.

- **Failed Login Count Reset Time (minutes)**:

  Failed Login Count Reset Time defines the minutes since the last failed attempt, that the count gets reset to the Lockout Duration. If the Lockout Duration is not 0, then after whatever time the duration is set to has elapsed since the account was locked out, the account gets "unlocked" and the valid password will work. The default setting is 30.

There are a certain number of failed attempts before the account is locked out as defined by **Maximum number of failed login attempts before account is locked out**. Once you have made that many attempts with incorrect passwords, the account is locked out, and no password will work.

Assuming the account has not been locked out, i.e., the user has not made more than the **Maximum Number of Failed Login Attempts**, once the **Failed Login Count Reset Time** has elapsed since the last attempt with an incorrect password, the count gets reset to 0.

Example: If **Failed Login Count Reset Time** is 1440 minutes (24 hours) and the **Maximum Number of Failed Login Attempts** is 3, the user can try to login with a incorrect password three times before the account is locked out. If he tries three times, then waits 24 hours (the **Failed Login Count Reset Time**), the count goes down to 0 and he gets three more attempts with incorrect passwords before the account gets locked out. The **Failed Login Count Reset Time** is counted from the last login attempt with a incorrect password. If the **Failed Login Count Reset Time** is 0, the count never gets reset automatically. In this example, even if the user waits a day or a week, the fourth time the he tries to login with a incorrect password, the account gets locked out.

Using this same example, if the **Account Lockout Duration** is 1440 minutes (24 hours), once the user tries to login with a incorrect password more than three times, the account gets locked out and he cannot login even with the correct password. After 24 hours from the last login with an incorrect password that triggered the lockout, the account gets unlocked and the user can login with the correct password. He now has 3 chances with incorrect passwords until the account gets locked again. If **Account Lockout Duration** is 0, the account remains locked until an administrator unlocks it from the User container in Interaction Administrator, by right-clicking on the user and choosing **Reset Failed Login Count**. In this case the count is set to 0 as if the time had elapsed. The administrator may reset this count anytime.

Users/Roles

From the Users/Roles tab you can apply policies to users and/or roles. From this page, you can add and delete users, as well as add and delete roles.

History

This page provides a way to manually document configuration changes and when they occurred. Changes made in Interaction Administrator are also automatically logged in the Interaction Administrator Change Notification Log (Log ID 7). Later, authorized users can run reports against this log to summarize all configuration changes.

Last Modified

This date is automatically updated each time the user clicks the OK button, presumably after making changes to the configuration property sheet. To avoid updating this date, exit the page by clicking the Cancel button.

> **Note:** If you click Cancel, none of the changes made to this configuration will be preserved.

Date Created

This date is automatically set when the user creates the initial configuration for this policy. If the policy was initially created by IC Setup Assistant, the date could be blank.

> **Notes**: Type notes about configuration settings and changes. If you change the configuration settimgs and click OK, the Last Modified date is updated.
>
> You must manually enter the date beside each entry in the Notes field to identify the date of each note.
>
> To create a new line in the Notes field, press Ctrl+Enter.

Password Policy Configuration

Use the Policies Configuration page to define new policies. To configure the password policies options, double-click **Configuration** on the right-hand side of the screen. The Password Policies Configuration page appears with the following options:

Combining Policies

Because several password policies can be assigned to a user, through direct assignment or because he or she is assigned to a role which has a policy assigned to it, multiple policies get combined. You must then decide how you want the different policies to be interpreted. This is done through a check box which allows you to choose the most restrictive or least restrictive policy when checking new passwords and when the user has more than one policy. For example:

- Policy A: Password Maximum Age = 10, Minimum Length = 4, Assigned to User A
- Policy B: Password Maximum Age = 20, Minimum Length = 6, Assigned to Role B
- User A is assigned to Role B

Both Policy A and Policy B apply to User A. The values will be combined based on the choice on the **Combining Policies** page.

If **Most Restrictive** is chosen, when a new password is checked for User A, the **Maximum Age** will be 10 days and the **Minimum Length** will be 6. If **Least Restrictive** is chosen, **Maximum Age** will be 20 and **Minimum Length** will be 4.

The example was for just two policies, but any number of policies might apply to a user, and they would all be combined in this way.

1. Click the appropriate check box for the restriction level you want when combining policies for a given user:

- Most restrictive
- Least restrictive

2. Click **Apply**.

History

This page provides a way to manually document configuration changes and when they occurred. Changes made in Interaction Administrator are also automatically logged in the Interaction Administrator Change Notification Log (Log ID 7). Later, authorized users can run reports against this log to summarize all configuration changes.

Last Modified

This date is automatically updated each time the user clicks the OK button, presumably after making changes to the configuration. To avoid updating this date, exit the page by clicking the Cancel button.

Date Created

This date is automatically set when the user creates the initial configuration for this page. If the configuration was initially created by the IC Setup program, the date could be blank.

Notes

Type notes about configuration settings and changes. If you change the configuration page and click **OK,** the **Last Modified** date is updated.

You must manually enter the date beside each entry in the **Notes** field to identify the date of each note. To create a new line in the **Notes** field, press Ctrl+Enter.

Policy Name

Type a unique policy name that will represent a set of attributes and permissions that you want to assign to specified users or a role.

Schedules

About schedules

The **Schedules** container lets you set dates and times to activate *telephone-based menus*. Telephone-based menus (or simply menus) are the set of choices that callers select by pressing buttons on a telephone keypad. In CIC, menus that are configured to run on certain days and at certain times are known as *scheduled menus*.

For example, you can schedule a menu to run on a holiday, every Tuesday, after hours, or during lunch. However before you schedule a menu, you must create the menu using the **Scheduled Menus** feature of Interaction Attendant. For more information, see the Help for Interaction Attendant.

The **Schedules** container is located under the **Peoples** container.

you modify and delete schedules in the right pane of the container.

Note: You cannot delete a schedule that is used Interaction Attendant.

Related topics

Schedule configuration

One time

Link a menu to a schedule

Set dates and times for menus

Schedule Configuration

Use this page to set dates and times to activate **telephone-based menus**. Telephone-based menus (or simply menus) are the set of choices callers select by pressing buttons on a telephone keypad. In CIC, menus that are configured to run on certain days and at certain times are known as *scheduled menus*.

You might schedule a menu to run on a holiday, every Tuesday, after hours, or during lunch. However before you schedule a menu, you must have created the menu using the **Scheduled Menus** feature of Interaction Attendant. For more information on **Scheduled Menus**, see the Interaction Attendant help.

Description

Type information that identifies the menu or type of scheduled event. The description displays in the Interaction Administrator list view window when the **Schedule** container is selected.

Keywords

Type a unique name that categorizes the schedule. For example, if the schedule is one of many schedules for the Support department, you might want to specify "support" as the keyword. Then, all schedules with the keyword "support" are associated. The **Get Schedules** tool uses these keywords for retrieving a list of schedule-specific menus. For more information on the **Get Schedules** tool, see the Interaction Designer help.

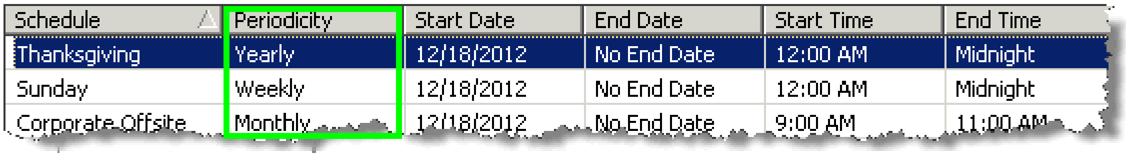
> Use a comma to separate more than one keyword.

Schedule is Active

Select this check box to activate the schedule. When the schedule is active, it is available as a candidate for evaluation by the system. Clear the check box to deactivate the schedule.

Periodicity

Click one of the following tabs to apply the type of schedule (or periodicity). The periodicity tab that is displayed when opening or closing the schedule configuration page, is the type of schedule that is active for the schedule entry. You can also see the type of schedule each entry is by looking at the Periodicity column:



Schedule	Periodicity	Start Date	End Date	Start Time	End Time
Thanksgiving	Yearly	12/18/2012	No End Date	12:00 AM	Midnight
Sunday	Weekly	12/18/2012	No End Date	12:00 AM	Midnight
Corporate Offsite	Monthly	12/18/2012	No End Date	9:00 AM	11:00 AM

- One Time
  Sets a menu to run for the specified time period, which plays the menu as often as needed.

> **Note**: The **One Time** schedule should not be confused with the **Unplanned** schedule type in available in Interaction Attendant. An unplanned schedule allows you to specify an indefinite

> end time, staying active until it is turned off. See *Unplanned Schedules* in the Interaction Attendant help for more information.

- Daily
  Sets a menu to run every day at a specific time for a specified length of time
- Weekly
  Sets a menu to run every week on certain days or every week in a sequence of days
- Monthly
  Sets a menu to run on relative and specific days of the month
- Yearly
  Sets a menu to run on specific and relative days during the year

The type of schedule determines the order in which CIC selects the schedule to play. The order of priority is as follows:

- **Unplanned**: Highest priority (See the note above under **One Time**.)
- One Time
- **Yearly**
- Monthly
- Weekly
- **Daily**: Lowest priority

If there is more than one schedule that matches in priority, then the start and end times are compared. The schedule containing the closest comparable times is the higher priority.

Related Topics

Schedules

Linking a menu to a schedule

One Time

To set dates and times for menus

You can schedule a menu to play at any time, day, week, month, or year. However, before you set the time and date that activates the menu, you must have created the menu using the Schedule feature of Interaction Attendant.

After you have created the menu in Interaction Attendant, follow these steps:

1. In Interaction Administrator, under **People**, select **Schedules**., and right-click and select New. Or click the **Insert** key.
2. Type a name for the schedule, and then click **OK**.
   The Schedule Configuration window appears.

3. In the **Description** box, type information that best describes the scheduled event. The description appears in the Interaction Administrator list view window when the **Schedule** container is selected.

4. In the **Keywords** box, type a unique name that will be used to categorize the schedule. If you have more than one keyword, use commas to separate them. The **Get Schedules** tool uses the keyword to retrieve a list of schedule-specific menus. For information on the **Get Schedules** tool, see the Interaction Designer online Help.

5. Select the button that describes the frequency of event you want to schedule – **One Time**, **Daily**, **Weekly**, **Monthly**, and **Yearly**.

6. Fill in the appropriate fields, and then click **OK**.
   The schedule is added to the Interaction Administrator list view window. From this window, you can modify or delete the schedule.

Related topics

Schedules

Schedule Configuration

One Time

Linking a menu to a schedule

To link a menu to a schedule

Once a menu is created using Interaction Attendant, and a schedule configured using the Schedules container in Interaction Administrator, you will need to establish a link between the menu and the schedule. Follow these steps:

1. Start Interaction Attendant.
   From the **Start** menu, point to **Programs** , and then **PureConnect.** Click **Interaction Attendant**.
   The Interaction Attendant window appears.

2. On the **File** menu, click **Connect to Server**.
   The Logon to Server dialog appears.

3. Type the name of the server, your user ID, and password.

4. Click **OK**.

5. In the tree structure, select the name of an existing profile or schedule form.

6. On the **Insert** menu, click **New Schedule**.

7. Click the **System** tab.

8. In the **System Schedule** list, use the down arrow to find the schedule you want to link to.

9. Click **Show Schedule** to view the schedule in read-only mode.

One Time

You can set a menu to run for the specified time period (required), which plays the menu as often as needed.

> **Note**: The **One Time** schedule should not be confused with the **Unplanned** schedule type in available in Interaction Attendant. An unplanned schedule allows you to specify an indefinite end time, staying active until it is turned off. See *Unplanned Schedules* in the Interaction Attendant help for more information.

Occurs

Sets the menu to run one time during a 24-hour period as follows:

- One time, but not all day.

  Use the Start boxes to select the date and time you want the menu to become active. Use the End boxes to select the date you want the menu to become inactive.

  > **Note:** If you configure both the start time and the end time as 12:00 am, CIC treats the end time as midnight at the end of the specified date (24:00) rather than midnight at the start of the specified date (00:00).

- One time, all day.

  Use the **Start** boxes to select the date and time you want the menu to become active, and then select the **All Day** option.

Secure Input Forms

Overview of secure input forms

You can define secure input forms to allow your customers to enter confidential customer information without divulging that information to agents. During a call, if an agent needs to capture confidential information, the agent can start a secure session. The customer can then use the IVR system to enter confidential information. After the customer has completed the IVR and entered all of the necessary confidential information, the agent can re-engage with the customer to conclude the call.

You manage secure input forms in the **Secure Input Forms** sub-container, which is found under the **People** container.

Before you can use any other secure input features, you must enable the Secure Input feature. You must also do the following things:

- Assign a secure input form to a workgroup.
- Assign the **Secure Input** and **Initiate Secure Input Interactions** security rights to users.

For more information on how to enable the Secure Input feature, see *Enable secure input*. For more information about the Secure Input feature, see the *Secure Input Technical Reference* document in the **Technical Reference Documents** section in the PureConnect Documentation Library.

Related topics

Add a secure input form

Enable secure input

Add a secure input form

> **Note:** Remember to enable the Secure Input feature. For more information, see *Enable secure input*.

To add a secure input form

1.

    1. In the **People** container, click the **Secure Input Forms** subcontainer.
    2. In the list view, right-click and then click **New**.
    3. In the **New Secure Input Form** box, type a meaningful and unique name for the secure input form name.
    4. From the **Form type** list, select one of the following:

    1.

    - **Simple**: Select this type to enable the form to receive text input.
    - **Custom**: Select this type if you have the CIC client add-in to create custom secure input forms. Custom forms receive input with attributes that you specify in your code. For more information, see the *Secure Input Technical Reference* in the PureConnect Documentation Library.

1.

    5. Click **OK**.
    6. In the **Secure Input Form Configuration** dialog box, complete the tabs. See the links under *Related topics* for complete information.

Related topics

Configure general information

Enable secure input

Overview of secure input forms

Configure general information

Use this tab to configure general information about secure input forms.

> **Note:** You must enable the secure input forms feature before any secure input forms are available for agents to use. Secure input is available in Interaction Desktop. For more information, see *Enable secure input*.

To configure general information

1. In the **Dialog title** box, type a title for the secure input form. Agents will see this text in the title bar of the dialog box that contains the secure input form.
2. In the **Description** box, type a description for the secure input dialog box. The CIC clients display the description when an agent selects the secure input form.
3. From the **IVR Handler** list, select a handler to start the secure session. The list includes only published handlers that begin with the Secure Input initiator.
4. To add a form field, next to the **Input fields** list, click **Add**. For more information, see *Add form field*.
5. To edit a form field, select it in the **Input fields** list and then click **Edit**.
6. To remove a form field, select it in the **Input fields** list and then click **Remove**.
7. To change the position of a form field, select it in the **Input fields** list and then use the **Move up** and **Move down** buttons as necessary.

Related topics

Enable secure input

Define a form field

Overview of secure input forms

Enable secure input

You must enable the Secure Input feature in order for agents to use your secure input forms. You can enable secure input in the when you add or edit a secure input form. If you need to create multiple secure input forms, you can wait to enable secure input until all of the forms are available.

> **Note:** Secure input is available in Interaction Desktop.

To enable secure input

1. In the **People** container, click the **Secure Input Forms** subcontainer.
2. Do one of the following:

- Add a new secure input form. For more information, see *Add a secure input form*.
- In the list view, right-click an existing secure input form and then click **Properties**.

3. At the top of the **Secure Input Form Configuration** dialog box, locate the text that indicates that the Secure Input feature is disabled. Click the **click here to enable Secure Input** link.
4. Click **OK**.

> **Note:** You can also enable secure input in the **Telephony Parameters** tab of the **Server Configuration** container.

Related topics

Add a secure input form

Configure general telephony parameters for your CIC server

Custom attributes

The Custom Attributes page allows you to add customized attributes so that you can reference your own variables and settings through the IceLib interface.

> **Note:** If you enabled the Enhanced Interaction Administrator Change log, then all of your changes to the Custom attributes page in the User Configuration dialog box and the Workgroup Configuration dialog box dialog box are tracked in that log. For more information, see *About the Enhanced Interaction Administrator Change Log*.

The page contains a list for the attributes and displays a **Name** and a **Value** column, and has the following buttons:

Add

Click **Add** and select an existing custom attribute from the pull-down list, enter a new custom attribute. If creating a new attribute, use a unique name, otherwise the existing attribute will be overwritten.

Edit

Click **Edit** to change the value of an existing custom attribute.

Delete

Click **Delete** to delete an existing custom attribute.

Manage Attributes

Click **Manage Attributes** to open a dialog box that displays a list of custom attributes. Click **Add** or **Delete** to manage the appearance of the custom attributes in the pull-down list.

The custom attributes are saved in the path of the root container. This **Path** is displayed at the bottom of the dialog box.

> **Note**: For more information on the Interaction Center Extension Library (IceLib), see The **System APIs section** in the PureConnect Documentation Library on the CIC server.

History

This page provides a way to manually document configuration changes and when they occurred. Changes made in Interaction Administrator are also automatically logged in the Interaction Administrator Change Notification Log (Log ID 7). Later, authorized users can run reports against this log to summarize all configuration changes.

> **Note:** If you enabled the Enhanced Interaction Administrator Change log, then all of your changes to the History page in the User Configuration dialog box and the Workgroup Configuration dialog box dialog box are tracked in that log. For more information, see *About the Enhanced Interaction Administrator Change Log*.

Last Modified

This date is automatically updated each time you click the **OK** button, presumably after you make changes to the configuration. To avoid updating this date, exit the page by clicking the **Cancel** button.

> **Note:** If you click **Cancel**, none of the changes made to this page will be preserved.

In addition, the history is updated when changes are made to the record elsewhere in Interaction Administrator. For example, when a user change his or her password, the **Last Modified** date is updated.

> **Note:** Changes to the licenses for a user or a station do not update the Last Modified date.

Date Created

This date is automatically set when the user creates the initial configuration for this page. If the page was initially created during setup, the date could be blank.

Notes

Type notes about configuration settings and changes. If you change the configuration page and click **OK**, the **Last Modified** date is updated.

You must manually enter the date beside each entry in the **Notes** field to identify the date of each note.

To create a new line in the **Notes** field, press Enter.

Disable secure input

To disable secure input

1. In the ***<IC Server>*** container, in the list view window, double-click **Configuration**.
   The **Server Configuration** dialog box appears.
2. Click the **Telephony Parameters** tab.
3. In the list, select **General**.
   The general telephony parameter options appear in the right side of the tab.
4. Clear the check box for the Enable Secure Input option.
5. Click **OK**.

Related topics

Overview of secure input forms

Configure general telephony parameters for your IC server

Wrap-up Codes

Overview of wrap-up codes

You can add wrap-up codes to CIC that can be used to associate the nature of the interaction; for example, Billing Problem, New Order, or Service Request. The wrap-up codes you define are used in reports specific to wrap-up codes. Once wrap-up codes are defined, users can assign wrap-up codes to incoming and outgoing interactions from the Interactions page in the CIC clients.

Phone-only users can use wrap-up codes as well. After a phone-only ACD user completes a call, the CIC server calls that user and plays a prompt requesting he/she enter the appropriate wrap up code. The user keys in the wrap-up code digits (from the wrap-up code definition) and these digits are saved in the report log.

There is a timeout window for all users to enter a wrap-up code. If no wrap-up code value is entered when required, "NS" (for not specified) is entered into the report log instead. Reports can be generated to categorize interaction details by wrap-up codes. Users are not assigned interactions during the wrap-up code timeout, which is defined by either the Client Wait Time or the Keypad Wait Time (for phone-only users).

> **Note:** Phone-only users should not attempt to manage multiple calls while using the wrap-up codes feature. You cannot delete the default wrap-up code.

Related topics

View wrap-up codes

Add a wrap-up code

Configure a wrap-up code

Configure advanced information

View wrap-up codes

The **View Wrap-up Codes** page displays wrap-up codes in a list in the master view, and displays details of the currently selected wrap-up code in the details view. You can take actions on the wrap-up codes in the list view, such as add, delete, and copy and paste, and you can add a new code. You can change the way the list is displayed, such as change visible columns, sort by column, and filter.

To view wrap-up codes

1. Click the **View Wrap-up Codes** action under the **User Management** category or click **View Wrap-up Codes** in the breadcrumbs, if available.
2. The **View Wrap-up Codes** page appears.
3. The details of the selected wrap-up code appear in the details view.

Related topics

Add a wrap-up code

Add a wrap-up code

To add a wrap-up code

1. Right-click in the master view area and select **New o**r click the **New** button in the master view toolbar.
2. Complete the wrap-up code configuration in the details tabs.

Related topics

Configure a wrap-up code

Configure a wrap-up code

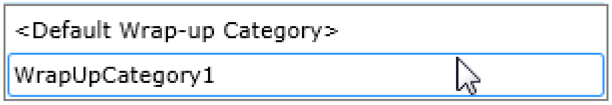
The wrap-up codes details tab contains name, digits, label, category, access control group, and multi-language label information the code. Click the name of the details tab for field descriptions.

To configure a wrap-up code

1. Click the **Configuration** details tab to display the details view.
2. Complete the following information in the first section:

- Type the **Name** of the new code.
- Type the **Code label**. This is label appears in the CIC clients.

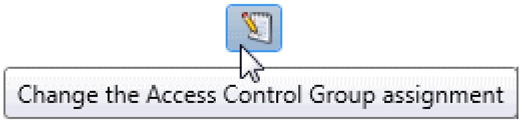
- Select the wrap-up code category to which the new code belongs.



<Default Wrap-up Category>
WrapUpCategory1

The default category is <Default Wrap-up Category>. New categories are defined in Wrap-up Category configuration.

- To display the access control groups membership available, click the icon,



and select the **Access Control Group** from the list to assign to the code.

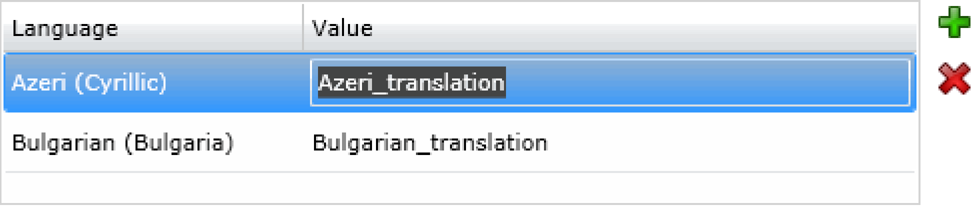
- If the outbound call reaches the intended party, this option is applied to the wrap-up code. Interaction Dialer uses this setting to determine if the intended party was contacted and then includes it in the Right Party Contact calculation.

3. Click the **Multi-language labels** section expander to display (or hide) the language section's contents, and complete the following information:

- Click✚ to open the **Add languages** dialog box.

  Select one or more languages in the **Available** items list, and click **Add** to assign the language to the **Selected** items list. You can also click **Add all** to add all languages. To filter the list of languages, type in the filter field above the list.

- Type in the string value associated with the language selected.



Language	Value
Azeri (Cyrillic)	Azeri_translation
Bulgarian (Bulgaria)	Bulgarian_translation

Note: You must specify a value or the multi-language label is not saved.

4. Save the new code or modified code.

- If necessary, the new code or changes made to an existing code can be reverted.

Related topics

Wrap-up codes: configuration field descriptions

Configure advanced information

The **Advanced** details tab contains the custom attributes and history of the wrap-up code. Click the name of the details tab for field descriptions.

To configure advanced information

1. Click the **Advanced** details tab to display the details view.
2. Click the **Custom Attributes** section expander to display the custom attributes section's contents and then complete the following information:
    - To create a custom attribute, click ✚ and type an attribute name. You must also enter a value for the new attribute.

Fax 5551212

3. Click **History** section expander to display (or hide) the history section's contents, and complete the following information:
    - View the **Created** and **Modified** dates for this wrap-up code.
    - Type or view information in the **Notes** field for the wrap-up code.
4. Save the wrap-up code.

    If necessary, the new wrap-up code or changes made to an existing wrap-up code be reverted.

Related topics

Wrap-up codes: advanced field descriptions

Wrap-up Categories

View wrap-up categories

The **View Wrap-up Categories** page displays wrap-up categories in a list in the master view, and displays details of the currently selected wrap-up category in the details view. You can take actions on the wrap-up categories in the list view, such as add, delete, and copy and paste, and you can add a new category. You can change the way the list is displayed, such as change visible columns, sort by column, and filter.

> **Note:** You cannot delete the default wrap-up category.

To view wrap-up categories

1. Click the **View Wrap-up Codes** action under the **User Management** category or Click **View Wrap-up Categories** in the breadcrumbs, if available.
2. The **View Wrap-up Categories** page appears.
3. The details of the selected wrap-up category appear in the details view.

Related topics

Add a wrap-up category

View wrap-up categories

The **View Wrap-up Categories** page displays wrap-up categories in a list in the master view, and displays details of the currently selected wrap-up category in the details view. You can take actions on the wrap-up categories in the list view, such as add, delete, and copy and paste, and you can add a new category. You can change the way the list is displayed, such as change visible columns, sort by column, and filter.

> **Note:** You cannot delete the default wrap-up category.

To view wrap-up categories

1. Click the **View Wrap-up Codes** action under the **User Management** category or Click **View Wrap-up Categories** in the breadcrumbs, if available.
2. The **View Wrap-up Categories** page appears.
3. The details of the selected wrap-up category appear in the details view.

Related topics

Add a wrap-up category

Add a wrap-up category

To add a wrap-up category

1. Right-click in the master view area and select **New or click** the **New** button in the master view toolbar.
2. Complete the wrap-up category configuration in the details tabs.

Related topics

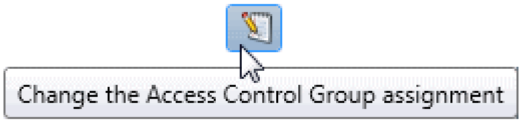
Configure a wrap-up category

Configure a wrap-up category

The wrap-up categories details tab contains name, category label, access control group, record status, phone number status, options, and multi-language label information the category. Click the name of the details tab for field descriptions.

To configure a wrap-up category

1. Click the **Configuration** details tab to display the details view.
2. Complete the following information in the first section:
   - Type the **Name** of the new category.
   - Type the **Category label**. This is label appears in the CIC clients.
   - To display the access control groups membership available, click the icon,

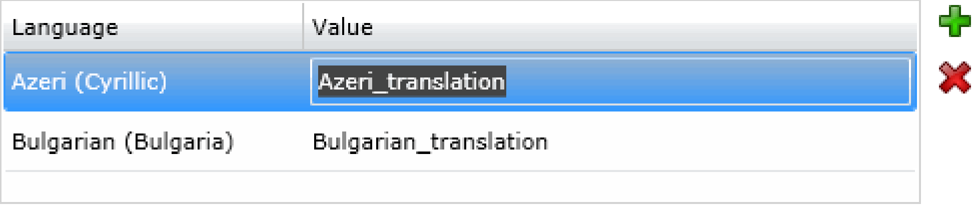
     

     and select the **Access Control Group** from the list to assign to the category.
   - **Record status:** Interaction Dialer uses this setting to determine the status of the record in the contact list.
   - **Phone number status**: Interaction Dialer uses this setting to determine the status of the phone number associated with the record.
   - **The interaction connected to an actual person:** This setting indicates whether the interaction is considered a contact. Interaction Dialer uses this setting to determine if the next contact column should be attempted for the record. If this setting is enabled, then Interaction Dialer will not attempt to dial any other contact columns for the record. If the setting is disabled, Interaction Dialer attempts to dial the next available contact column for the record.
   - **Increment the attempts counter:** Interaction Dialer uses this setting to determine if the interaction is considered an attempt on the record.
   - **The interaction was successful***:* Interaction Dialer uses this setting to determine if the interaction is considered a success. The setting is used for reporting to calculate success rates.
3. Click the **Multi-language labels** section expander to display the language section's contents, and complete the following information:

   1.

   - Click + to open the **Add languages** dialog box

     Select one or more languages in the **Available** items list, and click **Add** to assign the language to the **Selected** items list. You can also click **Add all** to add all languages. To filter the list of languages, type in the filter field above the list. Type in the string value associated with the language selected.



Language	Value
Azeri (Cyrillic)	Azeri_translation
Bulgarian (Bulgaria)	Bulgarian_translation

Note: You must specify a value or the multi-language label is not saved.

4. Save the new category or modified category.

   If necessary, the new category or changes made to an existing category can be reverted.

Related topics

Wrap-up categories configuration field descriptions

Configure advanced information

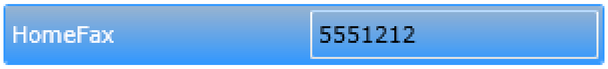
The **Advanced** tab information for custom attributes and history for the wrap-up category. Click the name of the details tab for field descriptions.

To configure advanced information

1. Click the **Advanced** detail tab to display the details view.

2. Click **Custom Attributes** section expander to display (or hide) the custom attributes section's contents, and complete the following information:

   - To create a custom attribute, click ✚ and type an attribute name. You must also enter a value for the new attribute.



HomeFax	5551212

3. Click **History** section expander to display (or hide) the history section's contents, and complete the following information:

   - View the **Created** and **Modified** dates for this category.
   - Type or view information in the **Notes** field for the category.

4. Save the new code or modified category.

   If necessary, the new category or changes made to an existing category can be reverted.

Related topics

Wrap-up categories: advanced field descriptions

CIC Client Buttons

CIC Client Buttons

You can configure the buttons that appear in the CIC clients which open an application, invoke a custom handler, or invoke an add-in.

> **Note**: Custom buttons can appear in both Interaction Desktop and Interaction Connect. Custom buttons that invoke an add-in work only in Interaction Connect. Custom buttons that launch a local application work only in Interaction Desktop. Custom buttons that invoke a handler work in both CIC clients.

CIC Client Button Name

Type a descriptive label for a client button. This is the label for the new button in the CIC clients.

CIC Client Button Configuration

Use this page to configure the behavior and appearance of a button in the CIC clients. Custom buttons can appear on queue control toolbars and interaction form toolbar. You can configure a custom button to apply to an "interaction type" which causes a queue-based custom button to be enabled only when one of the correct interaction types is selected in the queue view.

> Users need the appropriate **Client Buttons: View** Access Control right to see all or selected custom buttons in the CIC client.

Although custom buttons can appear in both Interaction Desktop and Interaction Connect, be aware of the following:

- You can optionally display custom buttons on the appropriate **interaction form toolbars** (for email, chat, call, and so on) only in Interaction Desktop.
- Custom buttons that launch a **local application** work only in Interaction Desktop.
- Custom buttons that invoke an **add-in** work only in Interaction Connect.
- Custom buttons that invoke a **handler** work in both CIC clients.

Active

Select this check box to enable this custom button in the CIC clients.

Description

Enter a description of this CIC client button. This description is used as a tool tip text when CIC client users mouse-over the button.

Icon

You may select an icon to display on the button. Click **Change Icon** to open a file browser to search for a *.ico file.

Availability section

Use the options in this section to define where the custom button is located and when it is enabled.

Enabled

Select when the button is enabled.

- The default option is **Always**. **Always** makes the custom button available in a selected interaction's right-click context menu.

  If you select **Always**, you can optionally select **Deactivate after one use per logon**.

- **Interaction Selected** or **Active Interaction Selected** options affect only the queue toolbar. This is because an interaction form represents only one interaction, which is assumed to be the *selected* interaction, and Interaction Desktop interaction forms cannot be shown for inactive interactions. An active interaction is any interaction that is not in the disconnected state.

  If you select either of these options, you can optionally select **Deactivate after one use per interaction**.

Location

Select where the button should appear from the pull-down menu. The options are Queue (queue toolbar), Interaction Form, or Both.

> **Note**: This setting is ignored by Interaction Connect. Custom buttons automatically show up on Queue views. Interaction Connect does not have interaction forms with buttons.

Interaction Types

Select the check box for each interaction type for which the button should be enabled. Select "All" if the button should be enabled for every interaction (depending on the option chosen for the **Enabled** setting).

> **Note**: Setting **Enabled** to **Always** automatically selects **All** for Interaction Types and selects and disables the check boxes for every interaction type.

In Interaction Desktop, if only certain interaction types are selected, the button is available only on those interaction type forms (if the **Location** is set to "Interaction Form" or "Both"), and it is enabled only when an interaction of the selected types is in the queue (depending on the **Enabled** and **Location** settings).

Deactivate After Use

Select this check box is you wish the button to disable or be grayed out after the first-time use per session.

Action section

Use the options in this section to define what action happens when the custom button is clicked.

Handler Notification

Select this option to send a notification to launch a custom handler. This option passes to the handler the interaction ID of the selected interaction (if any), the ID of the user that pressed the button, and the station from where the request was made. The handler then performs whatever action is required as customized.

Connect Add-In Notification

Select this option to notify add-ins that are installed on the web server. This option passes to the add-in the interaction ID of the selected interaction (if any), the ID of the user who pressed the button, the station from where the request was made, and the queue ID and type if the button was pressed from a queue view. The add-in then performs whatever action is required as customized.

> **Note**: Custom buttons for add-ins are available only for Interaction Connect.

Launch Application

If **Launch Application** is selected, the blind path to the executable application (*.exe) must be defined. Enter the path relative to the local CIC Client workstation (e.g., C:\Program Files\Interactive Intelligence\application.exe), or enter a UNC path (e.g., \\hydra\icapplications\application.exe).

> Note: Custom buttons for launching applications are available only in Interaction Desktop.

When launching an application, you can use the following command line parameters:

- Button ID
- Interaction ID
- Username
- Station

Code Example:

```
Process customApp = new Process();

customApp.StartInfo.FileName = _CustomButton.LocalApplication;

// Use quotes in command string to allow for names with spaces

customApp.StartInfo.Arguments =
String.Format("\"/BUTTON={0}\" \"/OBJECT={1}\" \"/USER={2}\" \"/STATION={3}\"",
ShellEscape(_CustomButton.Id),
interactionId,
ShellEscape(userName),
ShellEscape(stationName));
```

User Notification

Select this check box to display a toast to the user indicating that the custom button was clicked.

Related Topics

Client Button Entry Name

Client Buttons

Client Configuration

Overview of client configuration templates

You can create boilerplates of configuration options that you can then assign to users, workgroups or roles. These client configuration templates streamline the process of configuring large numbers of CIC clients.

> **Note**: The options for queue pages and directories pages are used only by Interaction Desktop.

Configure who can modify values in a template

Each page in a client configuration template contains a **Allow user to modify any of these values** check box. If you select this check box, both the users who are assigned the template and the master administrator can change the settings on that page for the template.

Related topics

Rank client configuration templates and designate the default template

Add a client configuration template

Client configuration template options

☎Rank client configuration templates and designate the default template

The first template in the list is selected when a user inherits multiple templates. When a user does not inherit a template, then the default template is used.

To rank client configuration templates and designate the default template

1. In the **People** container, click the **Client Configuration** subcontainer.
2. In the list view, right-click **Configuration** and then click **Properties**.
3. In the **Templates** list, select a template. Use the **Move Up** and **Move Down** buttons to position it in the list.
4. To designate a template as the default template, click **Set as Default**.
5. Click **OK**.

Related topics

Overview of client configuration templates

Add a client configuration template

Templates

Overview of client configuration templates

You can create boilerplates of configuration options that you can then assign to users, workgroups or roles. These client configuration templates streamline the process of configuring large numbers of CIC clients.

> **Note**: The options for queue pages and directories pages are used only by Interaction Desktop.

Configure who can modify values in a template

Each page in a client configuration template contains a **Allow user to modify any of these values** check box. If you select this check box, both the users who are assigned the template and the master administrator can change the settings on that page for the template.

Related topics

Rank client configuration templates and designate the default template

Add a client configuration template

Client configuration template options

Add a client configuration template

Before you assign a client configuration template to a user, you must first add the template. For more information on CIC client configuration, see the help for the CIC clients.

To add a client configuration template

1. In the **People** container, click the **Client Configuration** subcontainer.
2. Click the **Templates** subcontainer.
3. Right-click and then select **New**.
4. In the **Entry Name** box, type the template name and click **OK**.
5. In the **Client Configuration** dialog box, use the tree structure to navigate through and complete the configuration options. For more information, see the links under *Related topics*.

Related topics

- Alerting
- Voicemail/Fax Paging
- My Interaction Ring Sounds
- Calls
- Follow Me
- Call Coverage

- Personal Prompts
- Emails
- IP Phone
- Monitored Appearances
- Queues Pages
- Directories Pages
- General
- Plugins
- e-FAQ
- Interaction Tracker
- History

Alerting

Alerting

This dialog box displays the alerting configuration options in the **General** section and the **Parked Call** section.

General Alerting

Ring Telephone for Calls

Select this option to make the telephone ring when a call comes to a CIC client. If **Ring Always** setting for the station is enabled, then the **Ring Always** setting overrides this setting. If the station is a remote station, then the **Ring Always** setting overrides this setting.

Ring Computer

Selecting this option causes incoming interactions to ring through the computer's speakers. This feature does not work if the computer does not have a sound card installed. **Ring When On Phone** - When selected, incoming interactions ring on the computer when an agent is already on the phone.

Pop Client

If this option is selected, an incoming interaction causes the CIC client to appear on top of any other applications that are running, but does become the active window. This feature avoids interrupting work in another application.

Pop for Work Items

If this option is selected and a work item (collection of routed forms) is received, the CIC client appears on top of any other applications that are running, but does not become the active window. A work item appears in the 'My Work Items' tab in the CIC client, along with descriptive information.

Auto Select Interactions After Disconnect

CIC allows multiple interactions in the My Interactions queue. However, actions (such as mute, record, and transfer) can only be performed on the currently selected, or highlighted, interaction.

If there are multiple active interactions in the My Interactions queue, choosing this option causes the CIC client to automatically search and select the most recent or next interaction that is not disconnected.

Otherwise, the CIC client automatically selects the interaction that was most recently connected.

By default, if there are no active interactions in the My Interactions queue, when an alerting interaction appears, it is automatically selected.

Timeout for Incoming Calls (in seconds)

Typically, 6 seconds covers one ring and a pause, so 18 seconds should allow three full ring cycles. The default is 30 seconds. Negative numbers are not valid. The Timeout for ACD calls is controlled separately by the Workgroup configuration.

Parked Call Alerting

These options include:

Display Desktop Alert for New Parked Calls

Select this option to display a "pop up" window when calls are on hold (parked) while the agent is on a phone call. This window is displayed on top of all other applications, and pops-up only on new calls parked on the agent's queue.

Play Audio Alert for New Parked Calls

Select this option to play an audio alert when calls are on hold (parked) while the agent is on a phone call, and select one option below:

- **Once** (default): Plays audio alert for parked calls one time only.
- **At regular intervals**: Plays audio alerts for parked calls at specified intervals.

  Minutes between alerts: Specify the minutes between alerts.

Allow User to Modify Any of These Values

Select this check box to allow users assigned to this template and the master administrator to change any of these settings.

Voicemail/Fax Paging

Use this section to configure the following properties.

Alerting Method

Select the way the agent is alerted when a voicemail or fax arrives.

Do Not Send Me Alerts

Select this option when you don't want agents to receive alerts when a voicemail or fax is delivered to their Inbox or phone.

Email Address

Select this option to send an alert notification to an email address when a voicemail or fax is delivered to an Inbox or phone. Enter the full email address (for example: joe.user@inin.com).

Telephone Number

Select this option to send an alert notification to a designated telephone number when a voicemail or fax is delivered to an Inbox or phone. Enter the telephone number using the area code for long distance calls.

Pager Number

Select this option to send a pager notification when a voicemail is delivered to an Inbox or phone. Enter the pager number and ID if applicable. Enter the ID if applicable.

Alerting Reason

Define the criteria for alert notifications by using these options:

I receive a voice mail

Use this option to receive alerts when voicemail messages are delivered to an Inbox or phone.

- **Any voice mail**: Receive alerts for all voicemails.
- **Only urgent voice mails**: Receive alerts for voicemails marked as urgent.

I receive a new fax

Use this option to receive alerts when faxes are delivered to an Inbox or phone.

Alerting Time

Use the following options to restrict when alerts are received.

Any time of day

Receive alerts any time of day.

Only between

Receive alerts only between these times:

- **Start**: Specify the start time for receiving alerts.
- **End**: Specify the end time for receiving alerts.

Allow user to modify any of these values

Select this check box to allow users assigned to this template and the master administrator to change any of these settings.

Related topics

Add a client configuration template

Client configuration template options

My Interaction Ring Sounds

Use this section to configure the following properties. Custom ring sounds are supported in Interaction Desktop.

Calls

Select the location of the .wav file to play when calls ring in the CIC clients.

Chats

Select the location of the .wav file to play when chats arrive in the CIC clients.

Emails

Select the location of the .wav file to play when emails arrive in the CIC clients.

All Other Interactions

Select the location of the .wav file to play when all other interactions arrive in the CIC clients.

Allow user to modify any of these values

Select this check box to allow users assigned to this template and the master administrator to change any of these settings.

Related topics

Add a client configuration template

Client configuration template options

Calls

Calls

Use this section to configure the following properties for calls.

Timeout for external calls (in seconds)

Enter the number of seconds outgoing calls will ring before they are disconnected. This timeout setting will be ignored unless Analyze Outgoing External Calls is selected, and the dialing is from the CIC clients. If outgoing call is manually dialed (using handset), the outgoing call will ignore this setting and will continue ringing until answered. The default value is 45 seconds.

Used advanced dialing options (account code, workgroup)

Select this option to display the Advanced Dialing Options dialog box when calls are made. This dialog box enables assignment of an account code to the call and association of the call with a workgroup.

Analyze outgoing external calls

Select this option to allow the CIC clients to monitor outgoing external interactions. When this option is selected, Telephony Services (TS) monitors whether the outgoing interaction connects to a person or an answering machine. An interaction is listed in the Dialing state after dialing a number from the CIC client Number field or directly on the phone handset. After the remote party picks up the interaction, the state changes to Connected. If an interaction does not connect, then TS will try to diagnose why the attempt to connect failed and display the reason (for example, a connect may fail if the other party fails to answer or if the line is busy).

Enable call waiting

Select this option to turn on the call waiting feature so agents are notified when another call is coming in while they are on the phone.

Mute calls when transferring

Select this option to mute a transferred call so that the caller cannot hear what the agent is saying. (However, the transfer recipient can hear the agent.) Once the call is transferred or the Transfer dialog box is closed, the call is no longer muted.

Connect to Oldest Held Call When I Pick up the Phone (as long as there are no alerting calls)

Select this option for the CIC clients to automatically connect to interactions on hold. When the receiver is picked up and there is one or more interactions on hold, the CIC clients will automatically connect to the call holding the longest in the queue. This option is not available in Cisco TAPI environments.

Show alert dialog when the security of a call falls below the requested security level

Select this option to display an alert to the user if a once secure call is determined to no longer be secure.

Play DTMF sounds when using the dial pad with external stations

When you are using an external station (e.g., a Polycom phone, Interaction SIP station, or a remote station), select this option to play the DTMF tones through the user's PC speakers when pressing the corresponding digits on the CIC clients dial pad. By default, this option is not enabled.

Operator Target Number

Enter the telephone number or extension to which to send callers that choose zero to exit out of voice mail.

Open new window for incoming calls

Select this check box to open a new window for incoming calls, otherwise any incoming call will be opened in the existing window.

Allow user to modify any of these values

Select this check box to allow users assigned to this template and the master administrator to change any of these settings.

Related topics

Add a client configuration template

Client configuration template options

Follow Me

Use this section to configure the following properties for the Follow Me feature.

> **Note:** You can also configure call forwarding for stations. For more information see *Station call forwarding options*.

Phone Number

Enter the telephone number for the CIC clients to call if the agent is not available.

Time Out

Enter the number of seconds for the CIC clients to ring a follow-me routing number before moving to the next number in the list or transferring the call to voicemail. If no number is entered in this field, the CIC client defaults to 15 seconds.

Use Pin

Select this option to force call recipients to enter the CIC password to accept the call.

Screen calls

Select his option for the CIC clients to require callers to record their name. When a CIC client contacts the agent, the callers name will be played before the agent accepts the call.

Allow user to modify any of these values

Select this check box to allow users assigned to this template and the master administrator to change any of these settings.

Related topics

Station call forwarding options

Add a client configuration template

Client configuration template options

Call Coverage

Call coverage allows an agent to forward calls to voice mail, another number, or another agent when the agent changes his or her status to a DND status. When CIC forwards a call to another agent, the original extension information appears with the call so that the agent can see where the call was originally intended to go.

> **Note:** You can also configure call forwarding for stations. For more information see *Station call forwarding options*.

Coverage Options

The Call Coverage section contains the following items:

Forward

Select this option to send all calls, internal calls, external calls, or unknown calls to a Call Coverage number.

If I'm "Do Not Disturb," Forward

Select this option to send all calls, internal calls, external calls, or unknown calls to a Call Coverage number, when status is Do Not Disturb (DND), including not being logged into the CIC clients. This behavior depends on the configuration of DND statuses.

If I'm on the Phone, Forward

Select this option to send all calls, internal calls, external calls, or unknown calls to a Call Coverage number, when an agent is on the phone.

If I Don't Answer, Forward

Select this option to send all calls, internal calls, external calls, or unknown calls to a Call Coverage number, when an agent does not answer.

Coverage Number

The Call Number section contains the following items:

Send My Calls To:

Enter the phone number that interactions are sent to when one of the Coverage Options above in the Coverage Options section is selected. This number must be an internal number or a CIC extension.

If a Caller Leaves Voicemail, Send it to:

Click this drop-down menu to choose to send voice mail messages to the internal telephone number or CIC extension set, or to voice mail. The internal number or extension must have a mailbox assigned. If no mailbox is assigned to this number, then the system will not allow the changes.

For example, when the **My Mailbox** option is selected, any message left by a caller is sent to that agent's voice mail. If the other option (the number you entered in **Send my calls to**) is selected, then this gives ownership of the call (or any voice mail) to that coverage number.

Allow user to modify any of these values

Select this check box to allow users assigned to this template and the master administrator to change any of these settings.

Related topics

Station call forwarding options

Add a client configuration template

Client configuration template options

Personal Prompts

Use this section to configure the following properties.

Activate out of office message

Check this option to activate the **Out of Office** message. Agents should record their **Out of Office** message before they use this option for the first time.

Activate agent greeting

Select this check box to activate the Agent Greeting message. Agents should record their Agent Greeting Message before they use this option for the first time.

Record Out of Office Message

Use this button to record a message played to callers when the agent's status is set to one of the unavailable statuses (i.e. any status other than **Available** or **Available, Forward** or **Available, No ACD**). Also select the **Activate out of office message** option.

Record No Answer Message

Use this button to record a message played to callers when agents do not answer their calls.

Record Follow Me Message

Use this button to record a message to play to callers if agent status is set to Available, Follow Me.

When status is set to Available, Follow Me, the *Follow Me* message plays to callers while the CIC client consecutively calls the agent at a series of numbers that have been set up to find the agent and eventually connects the agent to the caller.

Record Name

Use this button to record agent name. This recording is played anytime someone calls the agent .

Record Agent Greeting

Use this button to record a message to play to callers before the agent answers an ACD call. This greeting, also known as a "smile", is intended for use by call center agents who are members of a workgroup and are receiving ACD calls. This feature is best used with the **Auto Answer Calls** (user/agent attribute set in Interaction Administrator). When used with **Auto Answer Calls** enabled, your **Agent Greeting** plays to the caller as the agent is being alerted. The length of the **Agent Greeting** is limited to 10 seconds, and therefore, is considered an introduction or "smile".

> **Note:** Once recorded, the Agent Greeting will be played to all ACD callers alerting on the agent's queue. To disable this greeting, click **Disable**.

Record Available, Forward message

Use this button to record a message to play to callers when agent status is set to "Available, Forward."

Allow user to modify any of these values

Select this check box to allow users assigned to this template and the master administrator to change any of these settings.

Related topics

Add a client configuration template

Client configuration template options

IP Phone

Use this page to set the default behavior of the Do Not Disturb (DND) button on an IP phone in the CIC clients.

> **Note**: This feature applies to users that are logged into a managed IP phone that supports DND button status synchronization.

When I turn the DND button on, set my status to:

Select a status that is configured as a DND status from the pull-down menu that you want your status to appear as when you enable the DND button on your IP phone. Do Not Disturb is the default DND status.

When I turn the DND button off, set my status to:

Select My Last Available Status (default) to display your status as the last status you had that is configured as an available status, or choose The Following Status and select a status that is configured as an available status from the drop-down menu.

Allow user to modify any of these values

Select this check box to allow users assigned to this template and the master administrator to change any of these settings.

Related topics

Add a client configuration template

Client configuration template options

Emails

Use this section to configure email behavior options in the CIC clients.

Spelling

Select the **Always check spelling before sending email** option to automatically check ACD-routed email messages after clicking send. Once the spell check is complete, the message is sent.

HTML Email

Select this option to automatically download and display any images included in ACD-routed email messages.

Allow user to modify any of these values

Select this check box to allow users assigned to this template and the master administrator to change any of these settings.

Related topics

Add a client configuration template

Client configuration template options

Monitored Appearances

The options in this page allow you to set up monitored appearances to observe the activity of several personnel at the same time. This feature is particularly helpful if a person has a number of personnel for whom he or she manages calls.

For example, receptionists or secretaries can use monitored appearances to continuously observe a manager's queue, control interactions, and perform tasks on his or her behalf, such as picking up or transferring calls and creating conferences.

Add

Click this button to add a user to monitor, then set the following options for the appearance:

Settings

Use this section to set up alerting options for a monitored appearance.

Label

To change the way the name appears in the Monitored Appearances page, in the Label box, type a new name. To list this monitored user on the My Interactions tab, select the **Active** check box.

To remove the user from the list, click to remove the checkmark from the Active check box.

Ring telephone for calls

Select this option to make the phone ring when a monitored user receives a phone call at his or her extension.

Ring Computer

Select this option to receive an audible alert through the computer's speakers when the monitored user receives a telephone call at his or her extension.

> **Note**: If the **Ring when on phone** option is selected, incoming calls for the monitored user ring on the computer when he or she is already on the phone.

Pop Client

Select this option to make the CIC client .appear on top of any other applications that are running when the monitored user receives an incoming interaction.

Display Desktop Alerts

Select this option to display a desktop alert (toast) when a monitored user receives a telephone call.

Call Ring Sound

Use this option to select the sound used by the computer when **Ring Computer** is selected and the monitored user receives a phone call.

> **Tip**: Click the button next to the Call Ring Sound box to test the sound.

Click **Remove** to remove a monitored appearance. To change the order of monitored appearances, select the name of a monitored appearance and click **Move Up** or **Move Down** as needed.

Allow user to modify any of these values

Select this check box to allow users assigned to this template and the master administrator to change any of these settings.

Related topics

Add a client configuration template

Client configuration template options

Queues Pages

Use this page to configure which queue pages appear in the CIC client interface, including station and user queues.

> **Note**: The queue pages options are used only by Interaction Desktop.

Allow User to Modify Any of These Values

Select this check box to allow users assigned to this template and the master administrator to change any of these settings.

Related topics

Add a client configuration template

Client configuration template options

Directories Pages

Use this page to configure which directory and workgroup views appear in the CIC clients.

> **Note**: The directories pages options are used only by Interaction Desktop.

Allow user to modify any of these values

Select this check box to allow users assigned to this template and the master administrator to change any of these settings.

Related topics

Add a client configuration template

Client configuration template options

General

Use this page to show the actual status icon in the system tray, choose whether or not to open a dialog box each time an interaction is dragged from the My Interactions queue to another call in the My Interactions queue, sort account codes by account number, and pop Interaction Tracker for unresolved contacts.

Hide disconnected interactions

Select this check box to remove interactions from the My Interactions page immediately after you disconnect them.

Show actual status icon in system tray

Select this check box to replace the icon of the CIC client with an icon associated with agent status.

Confirm drag and drop operations

Select this check box to confirm drag and drop operations such as dragging and dropping calls on another call to create a conference call.

Confirm single click dialing

Select this check box to display a confirmation dialog box anytime you initiate a call by single-clicking on a number in your Call History, or Company directory. This gives you the opportunity to click Yes or No before the call is dialed.

Sort Account Codes by account number

Select this check box to sort account codes by account number within the CIC client.

Automatically play voice mail interactions

Select this check box to automatically play .wav files that are attached to an email message when that message is opened.

Minimize to the notification area instead of the task bar

Select this check box to remove the icon for Interaction Desktop from the Windows taskbar when the user closes the CIC Client workspace.

> **Note:** This setting has no effect if the user has already pinned the Interaction Client application to the Windows taskbar. If the application is pinned, the task bar icon remains when the user closes Interaction Client.

Allow user to modify any of these values

Select this check box to allow users assigned to this template and the master administrator to change any of these settings.

Related topics

Add a client configuration template

Client configuration template options

Plugins

Use this page to select the check box associated with the plugin that you want to be visible to the user.

> **Note**: When you enable a plugin, some necessary files are downloaded from the CIC server to the CIC clients. Subsequently, plugin availability is determined by comparing information on the CIC server with corresponding information in the CIC clients. Therefore, if a user runs disconnected, or the server connection fails, or if the user changes to another CIC server, previously enabled plugins may not be available or only the plugins that were loaded when the user last closed CIC client may be available.

Allow user to modify any of these values

Select this check box to allow users assigned to this template and the master administrator to change any of these settings.

Related topics

Add a client configuration template

Client configuration template options

e-FAQ

Use this page to configure how e-FAQ search results appear in this client configuration template.

Search Results

Selecting **All** is the least restrictive search configuration where all results found based on the search terms will be returned. **Strict** is the most restrictive search configuration where the search results will only contain the most closely matched entries, similar to keyword matches. Note that relevant entries that contain misspelled words or less common terms may not be included in the search results for **Strict** searches.

Allow user to modify any of these values

Select this check box to allow users assigned to this template and the master administrator to change any of these settings.

Related topics

Add a client configuration template

Client configuration template options

Tracker

Use this page to configure Interaction Tracker related interactions and interaction history behavior in Interaction Desktop.

Show Interactions from the Previous:

Use this option to set the previous timeframe for interactions to appear in Interaction Desktop. The default setting for this option is **Week**. The other options are **Month** and **3 Months**. The interactions tracked are associated with how Interaction Tracker is configured in Interaction Administrator.

Maximum Number of Interactions to Show

Use this option to set the maximum number of interactions to show based on the **Show Interactions from the Previous:** setting above. The default maximum number of interactions to display is **10**. The other options are **50** and **100**.

Allow user to modify any of these values

Select this check box to allow users assigned to this template and the master administrator to change any of these settings.

> **Note**: The **Related Interactions** feature is available only for installations that have the Tracker feature license and that use SQL Server for the Tracker database.

Related topics

Add a client configuration template

Client configuration template options

History

This page allows you to enter information about and changes made to this client configuration template.

Related topics

Add a client configuration template

Client configuration template options

Queue Columns

Queue Columns

The **Queue Columns** container allows you to configure which fields can be displayed in the **My Interactions** page in the CIC clients. The columns displayed can be set in Interaction Desktop by right-clicking the column header.

For descriptions of the columns, see *Queue Columns* in the Interaction Supervisor help, or *Queue Contents* in the Interaction Desktop or Interaction Connect help.

Some of the default columns are:

Column name	Interaction Desktop?	Interaction Connect?	Interaction Supervisor?
Account Code	Yes	Yes	Yes
ACD Wait Reason	Yes	Yes	Yes
Agent Score	No	No	Yes
Associated Process	Yes	Yes	Yes
Attachments	Yes	Yes	Yes
Chat Response Time	Yes	Yes	Yes
Customer Score	No	No	Yes
Details	Yes	Yes	Yes
Duration	Yes	Yes	Yes
Importance	Yes	Yes	Yes
Interaction Id	Yes	Yes	Yes
Interaction Type	Yes	Yes	Yes
Line	Yes	Yes	Yes
Lstns	Yes	Yes	Yes
Name	Yes	Yes	Yes
Number	Yes	Yes	Yes
Process Id	Yes	No	Yes
Queue	Yes	Yes	Yes
Recs	Yes	Yes	Yes
Security	Yes	Yes	Yes
State	Yes	Yes	Yes
Station	Yes	Yes	Yes
Subject	Yes	Yes	Yes

Time in Status	No	No	Yes
Time in Workgroup Queue	No	No	Yes
User	Yes	Yes	Yes
Work Item Category	Yes	No	Yes
Work Item Created On	Yes	No	Yes
Work Item Description	Yes	No	Yes
Work Item Due Date	Yes	No	Yes
Work Item Error	Yes	No	Yes
Wrapup Code	Yes	Yes	Yes

For each column, you can select the interaction attribute and the corresponding attribute type. If you select an interaction attribute that pertains to time, such as Eic_ConnectTime, you can either use **Timestamp** or **Duration** as the attribute type.

To define new columns

1. Right-click and select **New**.
2. Type a unique and meaningful name for the new column, typically a name that reflects the associated attribute.
3. Select an attribute from the list. For the column to populate the information, you must assign an attribute. For information about specific attributes and their meanings, see *Interaction Attributes Technical Reference* in the Technical Reference Help in the PureConnect Documentation Library on the CIC server.
4. Click **OK**.
5. After you add a new column, assign the queue column viewing right to the user. The Queue Columns access control rights in the People category determine which columns are available to the user. Once the user has the appropriate right, the new column is available for display in the CIC clients.

Account Codes

View account codes

You can add special codes to CIC that can be used to associate outgoing and incoming calls. An account code is an identifying set of numbers assigned to an account name. Once users have access to an account code, they can add it to a call so that it can be tracked and reported in standard reports.

Account code authorization can be given to users, and members of a workgroup or role. As an example, suppose you want a specific department to track all outgoing calls placed to a specific customer. Assign the members of that department to a workgroup or role, and give them access to account codes. You can now track the calls made by that department to a specific customer.

Because account code data is stored in call detail and account code mirror tables, your CIC administrator can generate reports that summarize calls by user or by date.

Using Interaction Administrator Web Administrator, you can set up account codes (up to a maximum of 50 digits long) at the system, default user, user, or workgroup level. Once account codes are set up, users can assign them to incoming and outgoing calls.

> **Note:** Because account codes are treated as strings, not numbers, by the database program, account codes with leading zeros will appear first in reports. For example, account numbers 1, 3, 20, 213, 0214, 1234, and 001235 would be sorted as 001235, 0214, 1, 1234, 20, 213, and 3.

The **View Account Codes** page displays account codes in a list in the master view, and displays details of the currently selected account code in the details view. You can take actions on the account codes in the list view, such as add, delete, and copy and paste, and you can add a new account codes. You can change the way the list is displayed, such as change visible columns, sort by column, and filter.

> **Note:** In order for account codes to work, the **Use advanced dialing options (account code, workgroup)** option must be selected in the CIC client.

To view account codes:

1. Click the **View Account Codes** action under the **User Management** category or Click **View Account Codes** in the breadcrumbs if available.
2. The **View Account Codes** page appears.
3. The details of the selected account code are displayed in the details view.

Related topics

Add an account code

Enable account codes

Add an account code

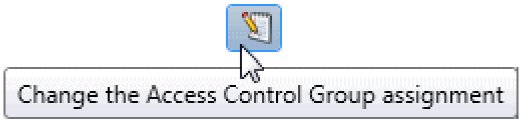
You can add an account code in Interaction Administrator Web Edition. The account codes settings are configured in detail tabs. In the details view, you can click the section expanders to display or hide the sections' contents.

To add an account code:

1. Right-click in the master view area and select **New o**r click the **New** button in the master view toolbar.

   The **New Item** appears in the details view.
2. Complete the following general account code configuration
   - Type the **Code** representing the account code.

- Type a **Description** for the new account code. This information appears in the CIC clients.
- To display the access control groups membership available, click the icon,



Change the Access Control Group assignment

and select the **Access Control Group** from the list to assign to the skill.

3. Click **Custom Attributes** section expander to display the custom attributes section's contents, and complete the following information:
    - To create a custom attribute, click ✚ and type an attribute name. You must also enter a value for the new attribute.

HomeFax 5551212

4. Click **History** section expander to display (or hide) the history section's contents, and complete the following information:
    - View the **Created** and **Modified** dates for this code.
    - Type or view information in the **Notes** field for the code.
5. Save the new account code or modified account code.

   If necessary, you can revert the new account code or the changes that you made to an existing account code.

Notes: To use account codes, they must be enabled at the system level, enabled for each dial plan object, and the user must have access to account codes.

To save a new account code, all required information must be entered. Details tabs containing incomplete or erroneous information, are shown with an error message.

Related topics

Account codes: field descriptions

Account code settings: field descriptions

Enable account codes

Account codes: field descriptions

This topic contains the descriptions for each field in the **Account Codes** details view under the **View Account Codes** page.

Code

This is a set of numbers zero through 9 (up to a maximum of 50 digits) to use as an account code. These numbers are associated with the account name.

> **Note:** Because account codes are treated as strings, not numbers, by the database program, account codes with leading zeros will appear first in reports.
>
> For example, account numbers 1, 3, 20, 213, 0214, 1234, and 001235 would be sorted as 001235, 0214, 1, 1234, 20, 213, and 3.

Description

Type a name for the account code. The name is added next to the account code shown in Interaction Administrator list view.

Access Control Group

An access control group (ACG) is a group of administrative rights. When an ACG is added to the account code, the account code takes on those ACG's rights. The account code can be assigned to only one ACG.

> **Note**: Access Control Groups appear if they have been configured in your environment. If Access Control Groups have not been configured, this field is not displayed.

Custom Attributes

Use customized attributes to reference other variables and settings through the IceLib interface. When adding a new attribute, use a unique name, otherwise an existing attribute with the same name will be overwritten. Click **Edit** to change the value of an existing custom attribute, or **Delete** to delete an existing custom attribute.

History

History provides a way to manually document configuration changes and when they occurred. Changes made in Interaction Administrator are also automatically logged in the Interaction Administrator Change Notification Log (Log ID 7). Later, authorized users can run reports against this log to summarize all configuration changes.

Created

This date is automatically set when the user creates the initial configuration for this account code. If the account code was initially created during setup, the date could be blank.

Modified

This date is automatically updated each time the user clicks the OK button, presumably after making changes to the account code configuration. To avoid updating this date, exit the property sheet by clicking **Revert**.

> **Note:** If you click **Revert**, none of the changes made to this account code since the changes were last saved are preserved.

Notes

Type notes about configuration settings and changes. If you change the configuration and click **Save**, the **Last Modified** date is updated.

You must manually enter the date beside each entry in the **Notes** field to identify the date of each note.

Related topics

Add an account code

Account codes global settings

Enable account codes

You can configure global account code settings in Interaction Administrator Web Edition. To use account codes, they must be enabled here. The account code global settings are configured in the master view. You can click the section expanders to display or hide the sections' contents.

> **Note**: To use account codes, they must also be enabled for each dial plan object, and the user must have access to account codes.

To enable account codes:

1. Select the **Enable Account Codes** check box.
2. Click Custom Attributes section expander to display (or hide) the custom attributes section's contents, and complete the following information:
   - To create a custom attribute, click ✚ and type an attribute name. You must also enter a value for the new attribute.

HomeFax 5551212

3. Click History section expander to display (or hide) the history section's contents, and complete the following information:
   - View the **Created** and **Modified** dates for this code.
   - Type or view information in the **Notes** field for the code.
4. Save the account code configuration.

   If necessary, you can revert your configuration changes.

Related topics

View account codes

Account code settings: field descriptions

This topic contains the descriptions for each field in the **Account Code Settings** master view under the **Account Code Global Settings** page.

Enable Account Codes

This setting activates the account codes feature for the CIC system.

Custom Attributes

Use customized attributes to reference other variables and settings through the IceLib interface. When adding a new attribute, use a unique name, otherwise an existing attribute with the same name will be overwritten. Click **Edit** to change the value of an existing custom attribute, or **Delete** to delete an existing custom attribute.

History

History provides a way to manually document configuration changes and when they occurred. Changes made in Interaction Administrator are also automatically logged in the Interaction Administrator Change Notification Log (Log ID 7). Later, authorized users can run reports against this log to summarize all configuration changes.

Created

This date is automatically set when the user creates the initial configuration for this account code configuration. If the account code configuration was initially created during setup, the date could be blank.

Modified

This date is automatically updated each time the user clicks the OK button, presumably after making changes to the account code configuration. To avoid updating this date, exit the property sheet by clicking **Revert**.

> **Note:** If you click **Revert**, none of the changes made to this account code configuration since the changes were last saved are preserved.

Notes

Type notes about configuration settings and changes. If you change the configuration and click **Save**, the **Last Modified** date is updated.

You must manually enter the date beside each entry in the **Notes** field to identify the date of each note.

Related topics

Add an account code

Client Templates

Overview of client templates

To simplify the configuration of Interaction Desktop clients, CIC provides the Client Templates feature. An authorized CIC client user creates client templates on the CIC server. Then, an administrator assigns the client templates to roles, workgroups, or users by publishing them in the **Client Templates** container.

> Notes:
>
> A user needs the **Manage Client Templates** security right to create or edit templates for other CIC client users. An administrator needs the **Client Templates** administrator access right to use Interaction Administrator to assign these templates to selected CIC client users.
>
> The Client Templates feature is designed to enable the one-time application of a template to a bulk set of users, roles, or workgroups. It is not designed to facilitate incremental, ongoing changes to

> selective users, roles, or workgroups.
>
> If you change a template, you must republish the template in order for the changes to take effect on the CIC clients.

Related topics

Publish a client template

Assign security rights

Publish a client template

You can publish a client template to make it available to roles, workgroups, or user.

To publish a client template to roles, workgroups, or users

1. In the **People** container, open the **Client Templates** subcontainer.
   The **Client Templates** page appears.
2. Under **Select template targets**, do one of the following:
   - Click **Select Users** to select the users who should receive the template.
   - Click **Select Roles** to select the roles that should receive the template. All of the users that have the roles that you select will receive the template.
   - Click **Select Workgroups** to select the workgroups that should receive the template. All of the users in the workgroups that you select will receive the template.
3. Under **Select a template to apply**, click the template that you want to publish. The following predefined templates are available:
   - All Channel Agent. This template provides all available channels to the agent.
   - Basic Chat Agent. This template enables the agent to participate in online chat sessions.
   - Basic Email Agent. This template enables the agent to send and receive emails.
   - Basic Email Agent with preview. This template enables the agent to send and receive emails and to preview incoming calls.
   - Default template. This is the standard template that is automatically assigned to all new users.
   - Default ICM. Not used.
   - Multi-Channel Agent: This template enables the agent to use chats and emails.

   > **Tip:** You can search for templates by name and by application.
4. Click **Apply Template**.
5. Click **Reset**. You can now apply another template if necessary.

Related topics

Overview of client templates

Response Management

Response Management

Response Management is a library of pre-defined responses, such as messages, URLs, and files. The CIC administrator creates and organizes pre-defined responses, and makes them available by granting access control rights to CIC client users. The user can use a stored response during a chat session, in a reply to an ACD-routed email message, or when responding to a callback request. These responses are available to users under administrator-defined folders in the Response Management window in Interaction Desktop and the Response Management view in Interaction Connect.

Response Organization

The organization of responses has three levels:

Library - A library (also called a server document) is the top-level collection of related response items. A library contains individual response items (such as a standard greeting or statement of your typical business hours) which can be organized into categories.

Category - A category is a folder in a response library. Categories are a way to organize individual response items in a library. Categories are optional.

Item - An item is a single response. There are two types of response items:

- Messages: Message items are stored text messages which can contain greetings, closings, and standard responses to common questions. A text message can also contain a working URL hyperlink.
- Files: File items are computer files that you can attach to an email message or send to external chat participants.

How recipients receive responses

When an agent inserts a response file into an email, it appears as an attachment.

When an agent inserts a response file into a chat, it appears as a file that the recipients can download.

To view response management items:

1. Click the **Response Management** sub-container under the **People** container.
2. Click the item you want to view in the master view to display the details of the selected schedule in the details view.

Related Topics

Add a New Response Management Library

Add a Response Management Message

Add a Response Management File

Import a Response Management document

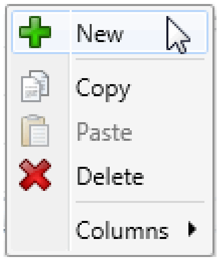
Add a Response Management Library

You can add a response management library that contains response categories and items. The item settings are configured in detail tabs. In the details view, you can click the section expanders to display or hide the sections' contents.

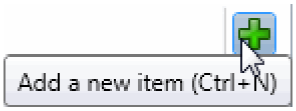
You must create a response management library before creating a category or an item.

To create a library:

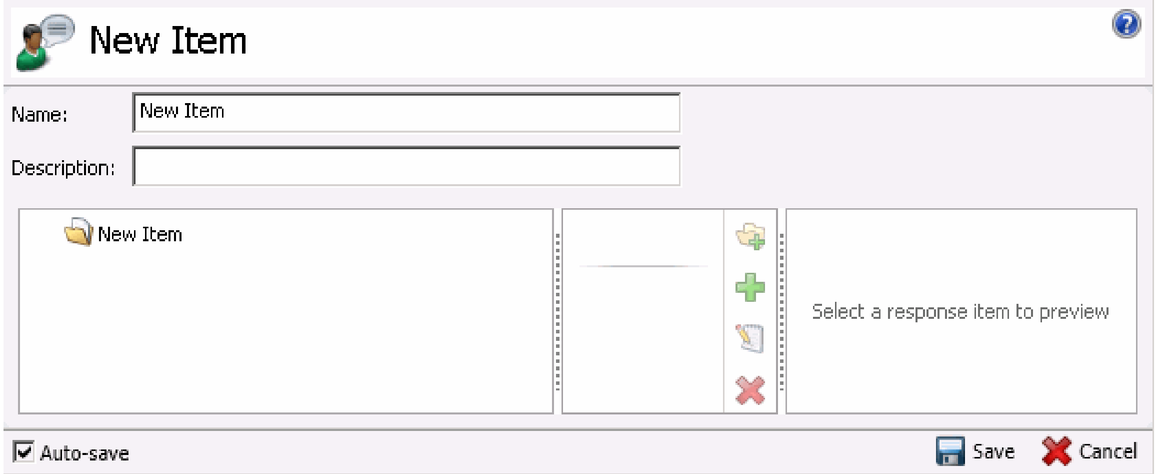
1. Right-click in the master view area and select **New**:



...Or click the **New** button in the master view toolbar:



The **New Item** appears in the details view:



Name: New Item

Description:

☑ Auto-save

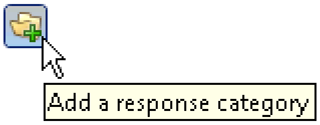
2. Type the **Name** representing the library.

3. Type a **Description** for the new library. This information appears in Interaction Client.

4. Save the library.

To add a category to a library:

1. In the master details view in a library, click the add a response category button.

2. Type a **Name** representing the category. This information appears in Interaction Client.
3. Save the category.

To add items to the library or category, see Add a response management message or Add a response management file.

Related topics

Response Management

Add a Response Management Message

Use a message item to save standard text responses that CIC client users often refer to when interacting with customers. You can add a response management message item to a library or category.

The item settings are configured in detail tabs. In the details view, you can click the section expanders to display or hide the sections' contents.

To create a message response item:

1. In the Response Management library or category details view, click the ➕ to add a response item.
2. In the **Type** section, select **Message**.
3. In the composition area, do one of the following:
   - Import an existing HTML file by clicking the Import HTML toolbar button. In the HTML Editor dialog box, locate an HTML file and click Open.

     Tip: By default, the HTML Editor lists only files with an HTML extension. Use the file type drop-down list to include files with an HTM extension. You can also import plain text files (TXT extension).
4. Optionally, do any of the following in the editor:
   - Format the text: Use any of the text formatting tools.
   - Add a hyperlink: Create a clickable link: Select some text in your message and click the Create Hyperlink tool, then supply a ScreenTip and a URL address.
   - Add an image: Select a place in your message and click the Add Image tool. Use any of the drag handles to resize the image.

- Add a Response Macro: Response macros automatically insert a constant like today's date, an interaction attribute such as the customer's name, or another response item into your response at the time you use it. See the help for the CIC clients for more details.

5. In the **Name** text box, type a name for this stored message.

> **Note**: Response Management provides a full-text search tool that uses the information in Name, Shortcut, and Labels along with the response item's content to find a response.
>
> **Tip**: **Name** identifies the response item, but does not have to be unique. If you do not provide a name, it defaults to the first few characters of the message.

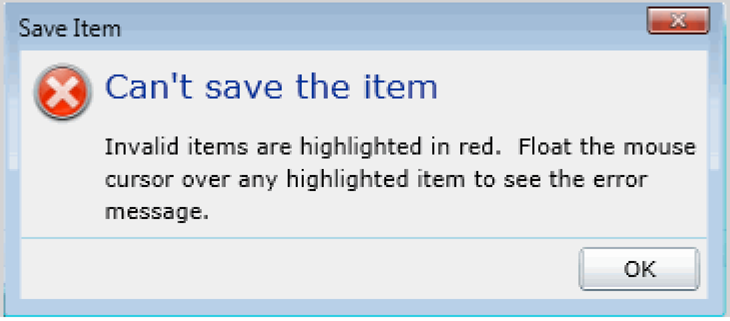
6. In the **Shortcut** text box, type a short name, abbreviation or code for this response.

> Tip: Use this Shortcut to insert a response item where needed by typing the shortcut and then pressing Ctrl+Space. The shortcut does not have to be unique. For example, you could use the shortcut "Hi" for all the variations of your standard greeting.

7. In the **Labels** text box, type a space-separated list of words that identify or classify this response item.

8. Click **Save**.

> **Note**: To save a new item, all required information must be entered. Details tabs containing incomplete or erroneous information, are shown with an error message:



Save Item

Can't save the item

Invalid items are highlighted in red. Float the mouse cursor over any highlighted item to see the error message.

> **Tip:** You can edit or delete multiple files or messages by selecting consecutive items with the Shift key and click, or multiple items with the Control key and click.

Related topics

Section expanders

Response Management

Add a Response Management Library

Add a Response Management File

Add a Response Management File

Use a file item as a pointer to a file on the network that you frequently share with customers. You can add a response management file item to a library or category.

The item settings are configured in detail tabs. In the details view, you can click the section expanders to display or hide the sections' contents.

To create a file response item:

1. In the Response Management library or category details view, click the ✚ to add a response item.
2. In the **Type** section, select **File**.
3. Do one of the following:
   - Click Browse. In the Open dialog box, locate and select the appropriate file and then click Open.
   - Use Windows Explorer to locate and select the appropriate file and then drag and drop the file in the **Drop file here** area.
4. In the **Name** text box, type a name for this file.

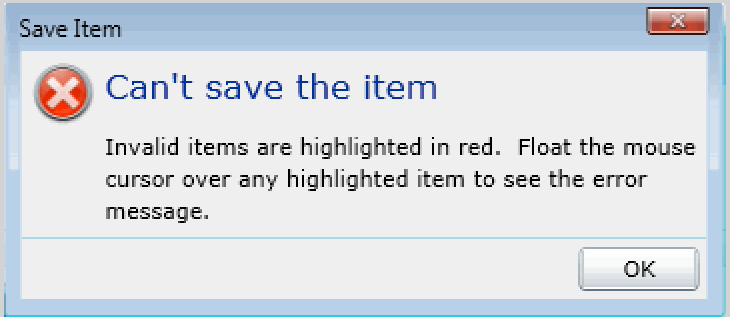
> **Note**: Response Management provides a full-text search tool that uses the information in Name, Shortcut, and Labels, and the response item's content to find a response.
>
> **Tip**: Name identifies the response item, but does not have to be unique. If you do not provide a name, it defaults to the first few characters of the file's directory path.

5. In the **Shortcut** text box, type a short name, abbreviation or code for this response.

> **Tip**: Use this Shortcut to insert a response item where needed by typing the shortcut and then pressing Ctrl+Space. The shortcut does not have to be unique. For example, you could use the shortcut "TS" for all your files containing troubleshooting tips.

6. In the **Labels** text box, type a space-separated list of words that identify or classify this response item.
7. Click **Save**.

> **Note**: To save a new item, all required information must be entered. Details tabs containing incomplete or erroneous information, are shown with an error message:



Can't save the item

Invalid items are highlighted in red. Float the mouse cursor over any highlighted item to see the error message.

> **Tip:** You can edit or delete multiple files or messages by selecting consecutive items with the Shift key and click, or multiple items with the Control key and click.

Related topics

Section expanders

Response Management

Add a Response Management Library

Add a Response Management Message

Import a Response Management Document

You can import response management documents from CIC 3.0 to a later release.

> **Note:** You can import only response management documents that were created with CIC 3.0. Do not use this feature to import XML documents that were created outside of CIC.

1. Under the **Response Management** subcontainer, click the Import Documents subcontainer.
2. To complete the **Response document path** field, click **Browse** to navigate to the document that you want to import.
3. Click **Import.**
4. Optionally click the response management document in the list to preview it.
5. In the **Name** field type a descriptive name that agents will see.
6. Click **Save**.

Skills

Overview of skills

Skills represent the particular characteristic, skill, product, or knowledge that a user or workgroup possesses. Skills are used by ACD (Automatic Communication Distribution) handlers to route interactions to the agents who are best equipped to handle them.

After you create skills in the **Skills** container, you can assign them to agents in the **Skills** container or the **Users** container. You can also assign skills to ACD workgroups in the **Workgroups** container. All agents in a workgroup inherit the skills that you assign to the workgroup.

> **Note:** You cannot assign skills to a non-ACD workgroup or a custom workgroup.
>
> **Prerequisites**: For each skill, you can select the workgroups, users, and access control groups who have it. While you can add these items at any time, it can be more efficient to add them before you configure skills.
> * Define workgroups in the **Workgroups** container. On the Configuration tab, in the **Workgroup has Queue** list, be sure to select **ACD**.
> * Define users in the **Users** container.
> * Define access control groups in the **Access Control Groups** container.

How CIC routes interactions based on skills

CIC uses sophisticated mathematical algorithms to determine how to route interactions to agents. For more information on the ACD routing process, see the *CIC ACD Processing Technical Reference* in the PureConnect Documentation Library.

When you define skills, you set several values that influence the automated routing behavior:

- Proficiency level
- Desire to use

Proficiency level

For each skill, you assign a proficiency level. The proficiency scale is from 1-100, with 100 being the highest value. The proficiency number represents of the ability of the user or workgroup with regards to the skill. Interactions can require minimum proficiency levels for one or more skills.

For example, suppose you have four agents who speak Spanish. Juan is a native speaker, so you assign him a proficiency level of 100. Rebecca studied Spanish in college and can speak and understand conversational Spanish well enough to address most straightforward questions. You assign Rebecca a proficiency level of 60. Barb knows a few basic phrases, so you assign her a proficiency level of 10. Mark does not know Spanish. Therefore, you do not assign the skill to him at all. When an interaction comes in with a requirement of Spanish at 51, CIC can direct it to either Juan or Rebecca.

Depending on the complexity of your combination of skills and agents, you may prefer to identify your criteria for assigning proficiency levels offline before you assign them in CIC.

Desire to use

For each skill, you also set the **Desire to use** level. The desire to use scale is from 1-100, with 100 being the highest value. The desire to use number represents the level of interest the user or workgroup has in applying the skill while they are handling interactions. You can also set this based on your organization's desire for an agent or workgroup to use that skill. The higher you set this number, the greater the likelihood that an agent or workgroup will receive an interaction that requires that skill.

For example, suppose that Rebecca wants to use her Spanish whenever possible. However, since Juan is a native speaker, you would prefer that he answer interactions requiring Spanish ability whenever possible. Therefore, you set Juan's desire to use level to 100 and Rebecca's desire to use level to 80.

Depending on the complexity of your combination of skills and agents, you may prefer to identify your criteria for assigning desire to use levels offline before you assign them in CIC.

Related topics

Add a skill

Add a skill

> **Note:** If you enabled the Enhanced Interaction Administrator Change log, then your addition of a skill is tracked in that log. For more information, see *About the Enhanced Interaction Administrator Change Log*.

To add a skill

1. In the **People** container, click the **Skills** subcontainer.
2. In the master view area, right-click and select **New**, or click the **New** button in the master view toolbar.
3. In the **Name** box, use a word or phrase to identify the skill. You can use blank spaces (for example, Spanish speaker, Database expertise, and so on).
4. Configure general information.
5. Configure advanced information.

Configure general information

Use the **Configuration** tab to configure the access control group, workgroups, and users for a skill.

> **Note**: You can assign skills to workgroups and users in the **Skills** container as described in the following procedure. You can also assign skills to users in the **Users** container and to workgroups in the **Workgroups** container.
>
> **Note:** If you enabled the Enhanced Interaction Administrator Change log, then all of your changes on this tab are tracked in that log. For more information, see *About the Enhanced Interaction Administrator Change Log*.

To configure general information

1. In the details area of the Skills window, click the **Configuration** tab.
2. If the **Access Control Group** box appears, click the icon to select the ACG for the skill.
   An access control group (ACG) is a group of administrative rights. When an ACG is added to the skill, the user that is assigned this skill takes on those ACG's rights. The skill can be assigned to only one ACG.

   > **Note**: Access Control Groups appear if they have been configured in the Access Control Groups container. If Access Control Groups have not been configured, this field is not displayed.

3. To select the workgroups that have the skill, in the **Workgroups** section, click the ✚ button.
4. Select one or more workgroups in the **Available** items list, and click **Add**. Alternatively, click **Add all** to add the skill to all workgroups. To find a specific workgroup, type a simple search in the filter field above the list.

> **Note**: You can select only ACD workgroups. If the workgroup you need does not appear here, go to the **Workgroups** container and edit the workgroup's record. On the **Configuration** tab, select the **Workgroup has Queue** checkbox. Then in the corresponding list, select **ACD**.

5. For each workgroup that has the skill, set the proficiency level. To do this, click under the **Proficiency** heading so that the field is active. Then either type a number or use the controls to select a number. The proficiency number represents the minimum proficiency of skill level workgroup members must have to receive an ACD interaction that requires the skill. The proficiency level is a relative number that you assign based on a scale of 1-100, where 100 is the highest level. For more information, see Proficiency level.

6. For each workgroup that has the skill, set the desire to use level. To do this, click under the **Desire to use** heading so that the field is active. Then either type a number or use the controls to select a number. The desire to use number represents the minimum level of interest users must have in order to receive an ACD interaction that requires this skill. The desire to use level is a relative number that you assign based on a scale of 1-100, where 100 is the highest level. For more information, see Desire to use.

7. To select the users who have the skill, in the **Users** section, click the ➕ button.

8. Select one or more users in the **Available** items list, and click **Add**. Alternatively, click **Add all** to add the skill to all users. To find a specific user, type a simple search in the filter field above the list.

9. For each workgroup that has the skill, set the proficiency level. To do this, click under the **Proficiency** heading so that the field is active. Then either type a number or use the controls to select a number. The proficiency number represents the minimum proficiency of skill level workgroup members must have to receive an ACD interaction that requires the skill. The proficiency level is a relative number that you assign based on a scale of 1-100, where 100 is the highest level. For more information, see Proficiency level.

10. For each workgroup that has the skill, set the desire to use level. To do this, click under the **Desire to use** heading so that the field is active. Then either type a number or use the controls to select a number. The desire to use number represents the minimum level of interest users must have in order to receive an ACD interaction that requires this skill. The desire to use level is a relative number that you assign based on a scale of 1-100, where 100 is the highest level. For more information, see Desire to use.

11. Click **Save**.

Related topics

Overview of skills

Configure advanced information

Configure advanced information

Use the **Advanced** tab information to configure for custom attributes and history.

> **Note:** If you enabled the Enhanced Interaction Administrator Change log, then all of your changes on this tab are tracked in that log. For more information, see *About the Enhanced Interaction Administrator Change Log*.

You can define custom attributes for skills to further assist the ACD routing process in selecting the most appropriate agents. For more information on how to use custom attributes with skills, see the *IC ACD Technical Processing Technical Reference* in the CIC Documentation Library.

To configure advanced information

1. In the Skills window details area, click the **Advanced** tab.
2. To create a custom attribute, under the **Custom Attributes** section, click the ✚ button.
3. In the **Name** box, type the attribute name.
4. In the **Value** box, type the attribute value.
5. To add a history note, under the **History** section, in the **Notes** box, type the information that you wish to capture.
6. Click **Save**.

Related topics

Overview of skills

Configure general information

Access Control Groups

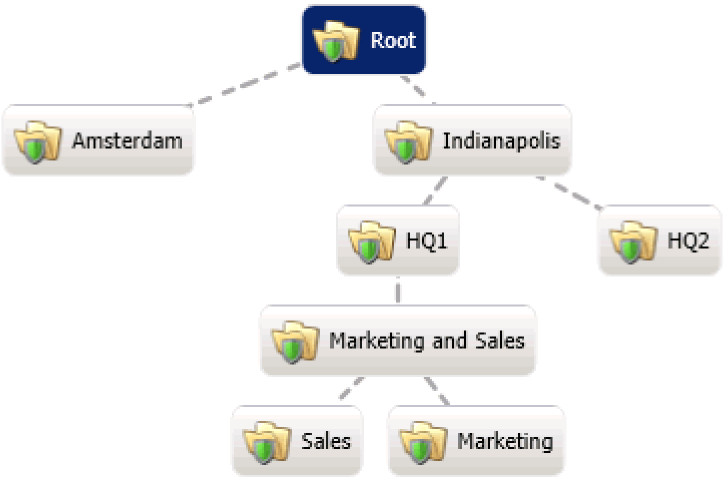
Access control groups

Access control groups (ACGs) provide a flexible way of defining administrative access rights. For example, an ACG can allow an administrator access to manage and modify users and workgroups within a certain part of the organization, without having access to other parts of the organization.

An ACG is similar to Active Directory structure, where the structure is a hierarchical arrangement of information about objects. The ACG allows access rights to be assigned against the hierarchy to define which objects or items (see item list below) a user can access. You can define multiple ACGs containing subsets of objects from the "root" ACG. A user can have access to one ACG or multiple ACGs.

CIC includes a default ACG "Root," which is the parent of the hierarchy.

To create levels in the hierarchy, first create ACGs from the root. Then create a second level of ACGs from, and so on. The maximum levels in a hierarchy is five (5). For example:



An ACG can have only a single parent, and an item can only be a member of a one ACG.

ACGs can contain the following items:

- Account codes
- Analyzer keyword sets
- Client configuration templates
- IP phones
- IP phone proxy groups
- IP phone ring sets
- IP phone templates
- IP tables
- Locations
- Password policies
- Roles
- Schedules
- Skills
- Stations
- Station groups
- Station templates
- Users
- Workgroups
- Wrap-up categories
- Wrap-up codes

Related topics

Access group configuration

Access control groups: members

Access control groups: members field descriptions

Access control groups: advanced

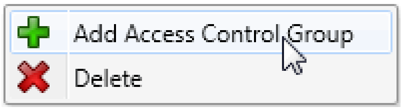
Access control groups: advanced field descriptions

Access group configuration

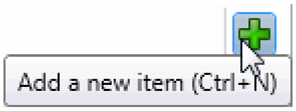
The **Access Control Groups** (ACGs) page displays the ACGs hierarchy in the master view. It displays details of the currently selected ACG in the details view. In the master view, you can add, edit, and delete ACGs. You cannot delete the default root.

To add a new ACG

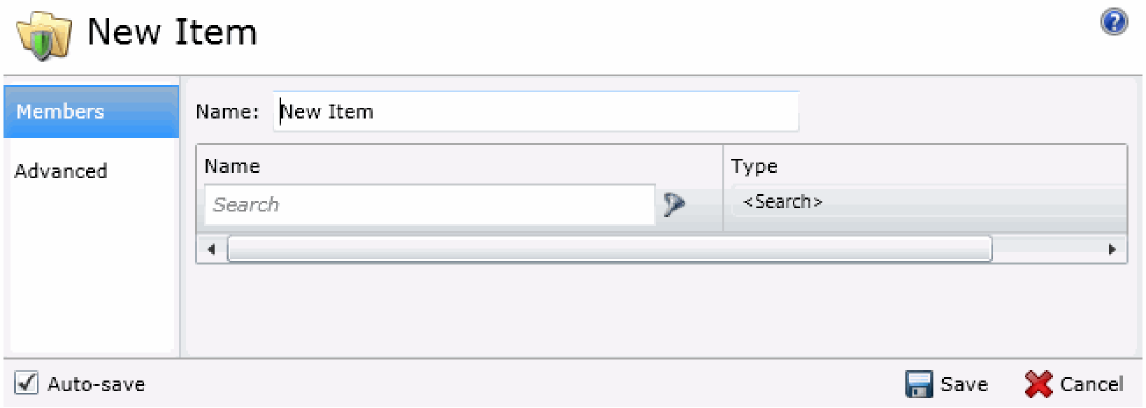
1. Right-click in the master view area and select **Add Access Control Group**:



...Or click the **New** button in the master view toolbar:



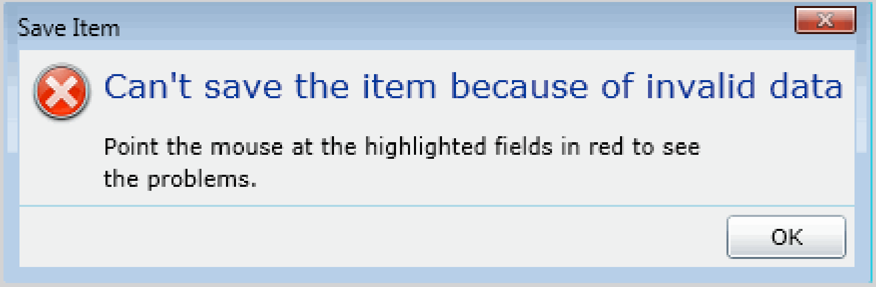
The **New Item** appears in the details view:



Name: New Item

2. Complete the ACG configuration in the two details tabs. The links below open the topics containing procedures for completing each details tabs configuration:

- Members: You can view membership only. Items must be added to ACGs through the specific item configuration.
- Advanced: Complete the optional custom attributes and history information.

> **Note**: To save a new ACG, all required information must be entered. Incomplete or invalid information is shown with a message:
>
> 
>
>
> Can't save the item because of invalid data
>
> Point the mouse at the highlighted fields in red to see the problems.

Related topics

Access control groups: members

Access control groups: members field descriptions

Access control groups: advanced

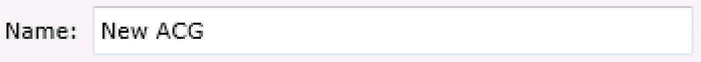
Access control groups: advanced field descriptions

Access control groups: members

The **Members** details tab contains the name of the ACG and the items that belong to the group. Click the name of the details tab for field descriptions.

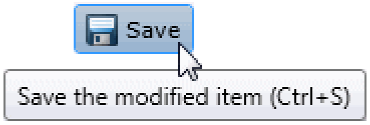
To complete the ACG's general information

1. Click the **Members** details tab to display the details view.
2. Type the ACG Name. The name must be unique.

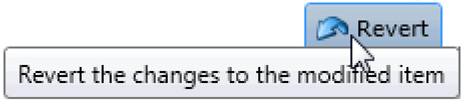
   Name: New ACG

3. Save the new ACG.

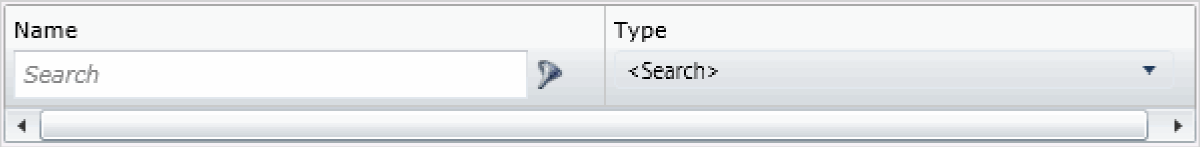
   

   Save the modified item (Ctrl+S)

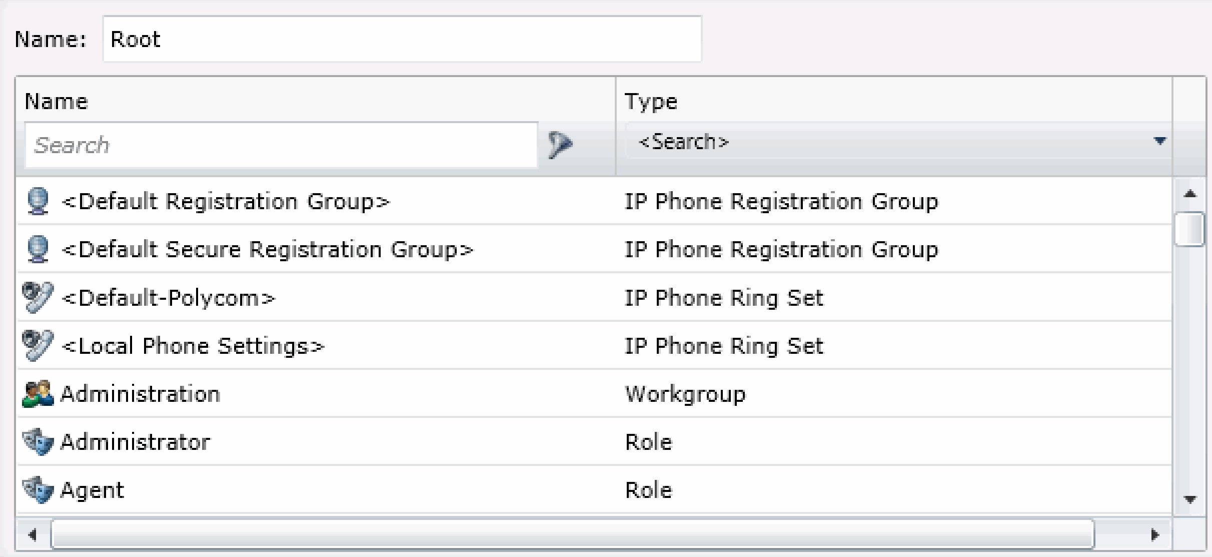
If necessary, the new ACG or changes made to an existing ACG name can be reverted.



Note: The **Name** and **Type** area in the details view is empty.



Items must be added to the ACG through the specific item's configuration. The following image illustrates how an item appears after it is added to the ACG.



Name	Type
<Default Registration Group>	IP Phone Registration Group
<Default Secure Registration Group>	IP Phone Registration Group
<Default-Polycom>	IP Phone Ring Set
<Local Phone Settings>	IP Phone Ring Set
Administration	Workgroup
Administrator	Role
Agent	Role

Related topics

Access group configuration

Access control groups: members field descriptions

Access control groups: advanced

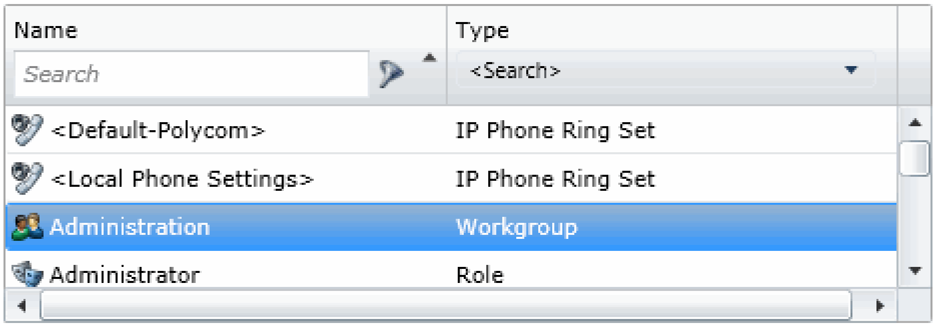
Access control groups: advanced field descriptions

Access control groups: members field descriptions

This topic contains the descriptions for each field in the **Members** details view under the **View Access Control Groups** page.

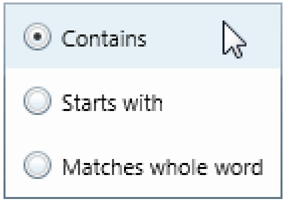
Members

When an item (member) is added to an ACG, the users assigned to the ACG's, take on those rights. The details view here shows the name of the item (Administration) and associated item type (Workgroup):



Name	Type
Search	<Search>
<Default-Polycom>	IP Phone Ring Set
<Local Phone Settings>	IP Phone Ring Set
Administration	Workgroup
Administrator	Role

- To search for a specific item in the list, type a digit or digits and select the filter type to apply:

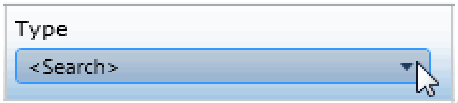


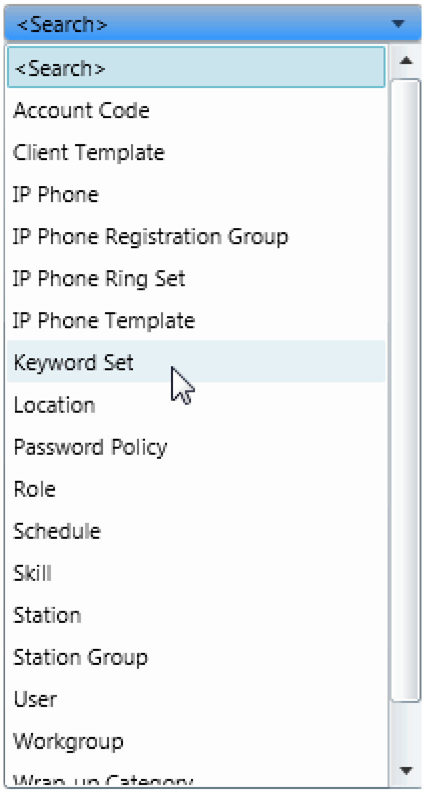
● Contains

○ Starts with

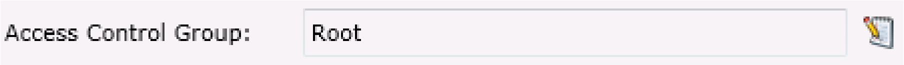
○ Matches whole word

- To search by item type, click , and select the item type from the list:





- All items belonging to an ACG are displayed in this view only list. Items cannot be added to or deleted from this view. Items must be added or deleted from ACGs from the item configuration. For example, a user must be added to an ACG through the **Access Control Group** field in user configuration:



Access Control Group: Root

Related topics

Access group configuration

Access control groups: members

Access control groups: advanced

Access control groups: advanced field descriptions

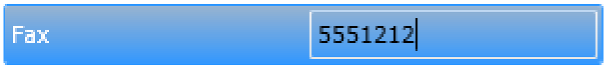
Access control groups: advanced

The **Advanced** details tab contains the custom attributes and history of the ACG. Click the name of the details tab for field descriptions.

To complete the ACG's advanced information

1. Click the **Advanced** details tab.
   The details view appears.
2. Click the **Custom Attributes** section expander to display (or hide) the custom attributes section's contents, and complete the following information:

   - To create a custom attribute, click ✚ and type an attribute name. You must also enter a value for the new attribute.



Fax 5551212

3. Click the **History** section expander to display (or hide) the history section's contents, and complete the following information:

   - View the **Created** and **Modified** dates for this ACG.
   - Type or view information in the Notes field for the ACG.

4. Save the ACG.

> **Note:** If necessary, the new ACG or changes made to an existing ACG can be reverted.

Related topics

Access group configuration

Access control groups: members

Access control groups: members field descriptions

Access control groups: advanced field descriptions

Access control groups: advanced field descriptions

This topic contains the descriptions for each field in the **Advanced** details view under the **View Access Control Groups** master view.

Custom Attributes

Use customized attributes to reference other variables and settings through the IceLib interface. When adding a new attribute, use a unique name, otherwise an existing attribute with the same name will be overwritten. Click **Edit** to change the value of an existing custom attribute, or **Delete** to delete an existing custom attribute.

History

History provides a way to manually document configuration changes and when they occurred. Changes made in Interaction Administrator are also automatically logged in the Interaction Administrator Change Notification Log (Log ID 7). Later, authorized users can run reports against this log to summarize all configuration changes.

Created

This date is automatically set when the user creates the initial configuration for this ACG. If the ACG was initially created during setup, the date could be blank.

Modified

This date is automatically updated each time the user clicks the **OK** button, presumably after making changes to the ACG configuration. To avoid updating this date, exit the details view by clicking Revert.

> **Note:** If you click Revert, none of the changes made to this ACG since the changes were last saved are preserved.

Notes

Type notes about configuration settings and changes. If you change the configuration and click **Save**, the **Last Modified** date is updated.

You must manually enter the date beside each entry in the **Notes** field to identify the date of each note.

Related topics

Access group configuration

Access control groups: members

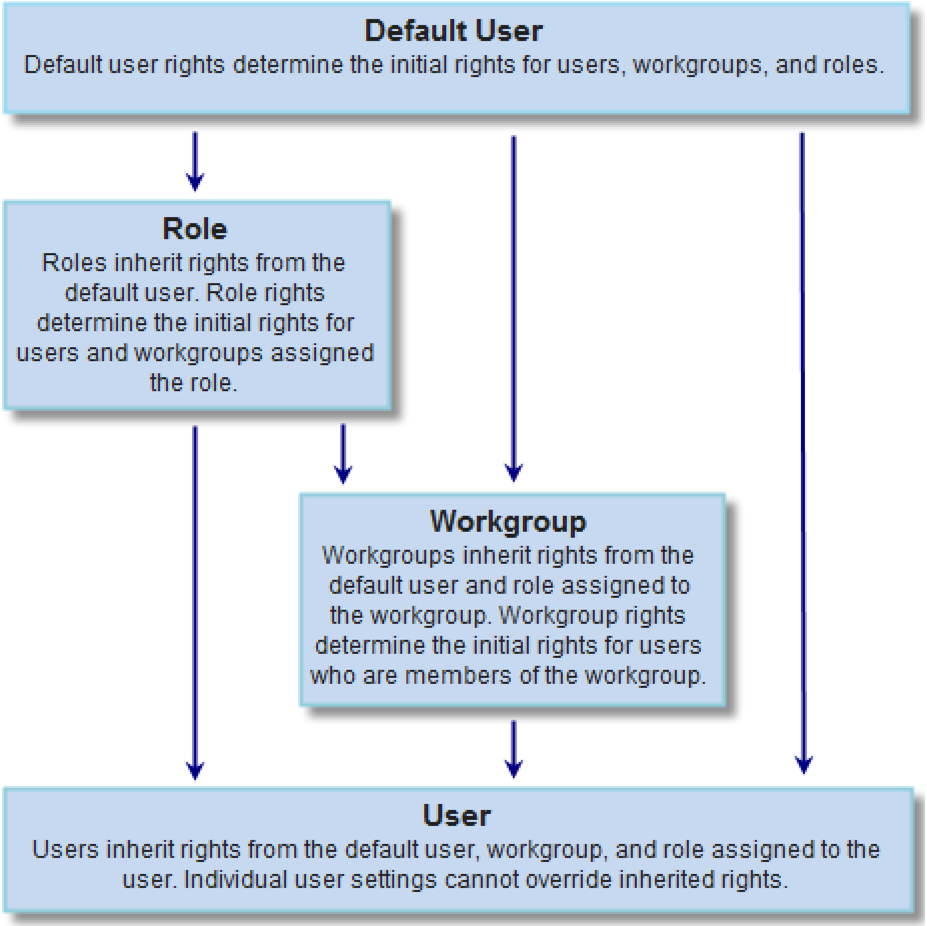
Access control groups: members field descriptions

Access control groups: advanced

About inheritance of configuration properties

To streamline the configuration of people-related records, CIC automatically assigns rights to roles, workgroups, and users based on a system of inheritance.

- All users inherit some initial rights from the default user.
- If you create workgroups, users who are members of a workgroup also inherit rights from that workgroup.
- If you create a role, users who are assigned to the role inherit the rights associated with that role.
- If a user is a member of more than one workgroup, or is assigned more than one role, and if those workgroups and roles include conflicting rights, the user will inherit the union of the rights set in all the workgroups and roles.


Default User
Default user rights determine the initial rights for users, workgroups, and roles.
Role
Roles inherit rights from the default user. Role rights determine the initial rights for users and workgroups assigned the role.
Workgroup
Workgroups inherit rights from the default user and role assigned to the workgroup. Workgroup rights determine the initial rights for users who are members of the workgroup.
User
Users inherit rights from the default user, workgroup, and role assigned to the user. Individual user settings cannot override inherited rights.

Activating configuration changes for users, workgroups, roles, and the default user

Configuration changes made in the configuration pages for users, workgroups, roles, and the default user dynamically update the affected CIC clients while they are actively running.

The following table summarizes how users are affected.

Changes made to:	Update Interaction Client in this way:
Individual User	The user's active CIC client is immediately updated.
Workgroups	Users who are members of that workgroup with active CIC clients are immediately updated.
Roles	Users who have been assigned the role with active CIC clients are immediately updated.
Default User	All users with active CIC clients are immediately updated.

Related topics

Updating configuration values

System Configuration

CIC System Configuration

CIC system resources control specific features and functionality provided in the Interaction Center for the entire configuration, regardless of how many servers or users are installed. System-level configuration includes:

- Interaction Processor (IP) variables and startup handlers
- Phone number identification and pattern matches. All dial plan configuration and phone number classifications are controlled in the Phone Numbers container.
- Report , Report Log , and Accumulator activity for gathering and producing call activity reports
- System-wide parameters that can be referenced by all CIC handlers on each server
- Status messages that can be defined on the server and set on each workstation running a CIC client.
- Action definitions
- Log Retrieval
- Administrative, fax, and voice email account names
- Interaction Process Automation
- Interaction Feedback
- Fax server, Interaction Fax Viewer default attributes and fax groups that are named groups of fax devices used for specific applications.
- Database and data source configuration
- Predefined Web chat messages and URLs for agents taking Web chat sessions
- Voice recognition
- Media Servers
- SIP Proxies
- MRCP Servers
- Session Manager
- SMS

System Configuration Pages

System Configuration Pages

The system configuration pages include:

Connection Security

Certificate Management

Prompt Server

Text to Speech

Display Name Format

Languages/Time Zones

Mailboxes

Host Server

Trace Logs

Site Information

ACD Options

Interaction Client

Connection Security

Use this page to define connection security settings.

Move the slider to select a level of security for connections between subsystems and the server.

High

- Data is only transmitted through server connections using Secure Sockets Layer (SSL)
- All applications use SSL
- Subsystem connections use SSL and certificates

Medium

- Data is encrypted before being transmitted through regular server connections or server connections using Secure Sockets Layer (SSL)
- You have the ability to configure which applications use SSL
- Subsystem connections use SSL and certificates

Low

- Data is transmitted in cleartext through regular server connections or server connections using Secure Sockets Layer (SSL)
- You have the ability to configure which applications use SSL

- Subsystem connections use SSL and certificates

Configure application connection security...

Configure subsystem certificates...

Configure login authentication...

Certificate Management

Use this page to configure which certificates are used on the CIC server.

Subsystem Certificates Configuration

Subsystem certificates are used to allow or deny subsystems from connecting to the server.

Click Modify to manage subsystem certificates.

Email Certificates Configuration

Email certificates are used to securely send and receive email messages and make secure connections to email (IMAP, SMTP, and S\MIME) providers.

Click Modify to manage email certificates.

SIP\TLS Line Certificates Configuration

SIP\TLS line certificates are used to authenticate SIP/TLS connections to and from the server.

Click Modify to manage line certificates.

Prompt Server

Prompt Server

The Prompt Server subsystem is installed on the CIC server, but it is not used by default. You must first assess the capacity and consider the implications of moving most audio play and input operations to the Interaction Media Server before enabling prompt server with the **Use Media Servers for prompt play and input operations** check box on the Media Server Configuration page.

The default values on the Prompt Server Configuration page are reasonable settings for initial use. Depending on the load on your media server and the types of prompts being accessed, you may need to adjust these settings.

Web Server Options

Prompt Server uses an HTTP server hosted on the CIC server to serve audio files to HTTP clients (e.g., Interaction Media Server, MRCP server). The following parameters specify how the HTTP clients connect to this HTTP Prompt Server.

Address to use: This drop-down menu shows the available friendly names of network adaptors associated with the HTTP or HTTP port. If a network adapter is renamed and no longer exists, there is a warning icon displayed next to that adaptor. CIC supports IPv4 and IPv6 addressing schemes.

HTTP Port: This specifies a local port on the CIC server that Prompt Server uses to service HTTP requests. The default value is 8098 and must not be set to conflict with any other port number on the CIC server.

If set to 0, Prompt Server does not have an HTTP listener and therefore is disabled. If the media server is in a different location and there is a firewall between the media server and the CIC server, then you must configure the firewall to open the port used by Prompt Server.

> **Note**: If you change the HTTP Port setting, you must immediately restart the Prompt Server subsystem, using IC System Manager, to activate the new HTTP port. Until you restart Prompt Server, HTTP client connections will fail.

Use HTTPS: This optional check box specifies whether resources (e.g. audio files) are served only through a secure TLS connection. It is off by default. If selected, HTTP requests will be redirected to the specified HTTPS Port. Using this option requires that the Interaction Media Server certificate is trusted by the CIC server.

HTTPS Port: This specifies a local port on the CIC server that Prompt Server uses for servicing (secure) HTTPS requests. The default value is 8099 and must not be set to conflict with any other port number on the CIC server. If set to 0, Prompt Server will not have an HTTP listener and therefore be disabled. If the media server is in a different location and there is a firewall between the media server and the CIC server, you must configure the firewall to open the port used by Prompt Server.

> **Note**: If you change the HTTPS Port setting, you must immediately restart the Prompt Server subsystem, using IC System Manager, to activate the new HTTPS port. Until you restart Prompt Server, HTTPS client connections will fail.

Mutual Authentication Required: This specifies whether mutual authentication of certificates is required between the CIC server and the Interaction Media Server. The check box is clear (off) by default. If selected, remote subsystem certificates will automatically be exchanged between the Interaction Media Server and CIC server.

> **Note**: If any changes are made to the **HTTP Port**, **HTTPS Port** or **Use HTTPS** settings, the prompt server must be restarted immediately.

Cache Options

In order to efficiently process prompt requests, Prompt Server manages a local cache of audio file properties on the CIC server. Most of these cache options are good default values and don't need to be changed in the normal case of Interaction Media Server processing audio plays. Some options are only for special cases when another application may access a prompt not tagged with release information by Prompt Server.

Note that the Interaction Media Server keeps its own local cache of prompts as well, but that cache is not affected by these options.

Maximum age of files without a version (sec)

This specifies the maximum age, in seconds, of cached files that have not been tagged with a release identifier. The default value is 600 seconds (10 minutes).

In the typical case of Prompt Server serving files to and receiving requests from Interaction Media Server, all audio files are tagged with release information, which is used to determine if a file has changed. In some cases, an MRCP server may use SSML documents that reference audio files not tagged by Prompt Server. In this case, Prompt Server sets the max-age HTTP header directive to the specified value when these files are requested.

Cached prompt idle time (sec)

This specifies the number of seconds to wait before removing a cached prompt that has not been used or requested. Once a prompt is played, the idle time counter is reset for that prompt. As long as the prompt is being used within the idle time limit, it will remain in the cache. If a prompt has not been used or requested in that idle time period, it will be removed from the cache on the next cache cleanup event. The default value is 600 seconds (10 minutes).

Cache cleanup interval (sec)

This specifies the number of seconds between cache cleanup events. Files that have been identified as having exceeded the cached prompt idle time will be cleaned out of the cache at this interval. The default setting is 300 seconds (5 minutes).

Cached prompt refresh interval (sec)

This specifies the interval Prompt Server uses to determine whether or not to scan the cache for updated file attributes when a file is requested. It is used to help prevent excessive refreshing of cached file attributes. The default value is 10 seconds. That means, for example, once Prompt Server reads a file's attributes and that data is cached, if there is another request for that file within the interval (10 sec), Prompt Server does not read the file attributes again – it assumes the file is current. If a request for that file occurs after the interval, Prompt Server reads the file attributes again to determine if it has changed.

Click Configure File Extensions... to enter or edit prompt server file extensions.

Click Configure Virtual Directories... to enter or edit prompt server virtual directories.

For more information, see *Interaction Media Server Technical Reference*, which is in the **Technical Reference Documents** section in the PureConnect Documentation Library.

Related Topics

Media Servers

Prompt Server File Extensions

Prompt Server - Add File Extension

Prompt Server - Virtual Directories

Prompt Server - Add Virtual Directory

Prompt Server File Extensions

Interaction Media Server plays .wav .snd and .au prompt files. These file extensions are configured by default in the Prompt Server File Extensions dialog box. In the typical case, you do not need to add or change the default file extensions. The ininmodel file extension (with application/xml Content Type) is required for call analysis to work on the Interaction Media Server.

In the more rare case where a CIC server sends audio to an MRCP server that supports additional audio formats, you may need to add that file extension and content type here.

Click Add to add a prompt server file extension, or highlight an existing file extension and click **Delete** to remove it.

Related Topics

Media Servers

Prompt Server

Prompt Server - Add File Extension

Prompt Server - Virtual Directories

Prompt Server - Add Virtual Directory

Prompt Server - Add File Extension

Use this page to enter the prompt server file extension information.

File Extension

Enter a unique prompt server file extension, such as "wav". Extensions are case-insensitive.

Content Type

Enter the prompt server file content type in the format of "xxxx/xxx", such as "audio/x-wav". An error is displayed if not entered in the proper format. This information is contained in the HTTP or HTTPS header for the associated file extension.

Related Topics

Media Servers

Prompt Server

Prompt Server File Extensions

Prompt Server - Virtual Directories

Prompt Server - Add Virtual Directory

Prompt Server - Virtual Directories

Prompt Server provides access to audio files residing in the file system on the CIC server. In order to limit access to the CIC server file system and provide a degree of security, Prompt Server creates virtual directories for Interaction Media Server to access the files. A media server or other third party server can only access audio files residing in (or in a subdirectory under) one of the virtual directories defined on the Prompt Server configuration page.

By default, Prompt Server creates virtual directories for the common audio resource folders on an CIC server, including

- Recording Directory (x:\server\IC\Recordings)
- Resource Directory (x:\server\IC\Resources)
- Work Directory (x:\server\IC\Work)

By default , handlers use prompts under one of these directories, but you can choose to omit any of these or create additional virtual directories that map to a specific location on the CIC server.

The **Use resource directory** option is required for call analysis to work on the Interaction Media Server.

Click Add to add a virtual directory, or highlight an existing directory and click **Delete** to remove it.

> **Note**: For security reasons, only prompt files that are located in one of the virtual directories (or the subdirectories) are mapped to URIs.

Related Topics

Media Servers

Prompt Server

Prompt Server File Extensions

Prompt Server - Add File Extension

Prompt Server - Add Virtual Directory

Prompt Server - Add Virtual Directory

Use this page to add a registered virtual directory and the corresponding root paths.

Virtual Directory Name

Enter a unique virtual directory name for the prompt server. The name is case-sensitive.

Root Server Path

Enter the file path prefix which this virtual directory references on the local system. Click **...** to browse the server directory. If Interaction Administrator is not running on the server, then the browse button is not available.

The root server path is matched against files to be mapped to URIs. CIC uses the virtual directory with the longest matching local root path to compose the URI.

Related Topics

Media Servers

Prompt Server

Prompt Server File Extensions

Prompt Server - Add File Extension

Prompt Server - Virtual Directories

Text to Speech

Default Text to Speech (TTS) voice configuration is performed in the Windows Control Panel Speech Applet.

Use the **Text to Speech** tab of the **System Configuration** dialog box to perform the following advanced TTS configuration:

- Set the maximum number of sessions to be allowed at one time
- Add multiple languages and voices

For more information, see *Text-to-Speech Engines Technical Reference* in the PureConnect Documentation Library.

Default TTS Provider

When CIC receives a TTS request, it must select which TTS technology to use to complete the request. The **Default TTS Provider** field indicates which TTS technology to use when a TTS request does not indicate a specific TTS technology. The options are:

- SAPI: This is a Windows-only API.
- MRCP: This is a standardized TTS protocol. Many third-party TTS vendors support only MRCP.
- Media Server: This is CIC's proprietary Text-to-Speech engine. This option is available only if you have installed a license for it.

Concurrent Session Limit

Enter the maximum number of concurrent sessions to attempt. This limit is either a license-enforced limit or a load-enforced limit. TTS will not attempt to create more sessions than what is defined here. Additional requests will fail and an event log entry will be logged.

Concurrent Session Warning Level

Enter the maximum concurrent sessions. When this threshhold is exceeded an event log entry will be created. Use this warning level to see when you are getting close to exceeding your license limit so you can plan ahead.

Number of Sessions Currently in Use

This is the number of TTS sessions currently in use in the CIC system.

Volume Control (0 - 100)

Use the up and down arrow keys to set the volume level for the voice resource. The default value for this field is 100 decibels.

Voices

You can choose to write custom applications for multiple languages and voices by creating a voice name parameter for each voice and then making the necessary handler modifications using these voice name parameters.

Click **Add** to add voice resources. Enter the voice name and the registry path. Select the Language from the pull-down list.

For example, you may define "Mary" as the name, "HKEY_LOCAL_MACHINE\Software\Microsoft\Speech\Voices\Tokens\MSMary" as the path, and "English (United States) as the language. Once defined, you can then just pass "Mary" to the TTS defined tool.

There is no limit to the number of voices to add. By default , the system refreshes every 5 seconds.

Click **Edit** to change existing voice resources or **Delete** to remove them.

> **Notes:** Only configured voices on the CIC server are listed.
> Each language can only be associated with one voice.
> Voice configuration settings in this dialog will override the voice configuration settings in the Windows Control Panel Speech applet.

Display Name Format

Use this page to configure the way names are displayed in the system. Select one of three options:

- **FirstName MiddleNameOrInitial Last Name**
  For example, Sonya M Mullins
- **LastName, FirstName, MiddleNameOrInitial**
  For example, Mullins, Sonya, M
- **LastNameFirstName**
  For example, MullinsSonya

Set Asian Names to "LastNameFirstName"

Use this option to set LastNameFirstName as the default format if an Oriental name is detected.

Example

This section displays an example based on the format chosen above.

Languages

For sites that support multiple languages (such as English, French, Spanish, etc.), the handlers that play prompts can select which language (*and time zones will be available in a future release) to* use when playing these prompts. Use this page to define the languages available at a site and to specify the default language. Use the prompt editor to record prompts in different languages.

Include User's Time Zone in Announcements (*available in a future release)*

Select this check box to include the user's time zone information in announcements. For example, you may want to include "..10:00 AM **savings daylight time**...". . By default, this option is not enabled.

Languages

Click the **Add** button to define a new language for this site.

To remove a language from this site, select a language name and click the **Delete** button.

> **Note:** Languages available depend on the language installed by the add-on language pack install. For non-supported language prompts, you can create a language prompt set as prompt handlers, and add the language to CIC using the option in this dialog box.

Default Language

The languages defined in the Languages box appear in this list box. Select the default language used in all system prompts. In addition, the GetLanguage handler uses this Default Language value if the "'Language"' attribute is not set on a call.

> **Notes**: If you install a non-English language pack and require call analysis for that language, you must set the Call Analysis Language server parameter on the Interaction Center server. For more information, see “Specify Interaction Media Server call analysis language model” in *Interaction Media Server Technical Reference* in the PureConnect Documentation Library.
>
> For more information about the GetLanguage handler and the Play Prompt tool, see **Reference (Tools and more) > Tools > Telephony** in the Interaction Designer Help.

Mailboxes

Select the default email account (or distribution list) for each of the following roles in CIC message distribution. Handlers can send email to these designated accounts by specifying the Directory Services (DS) attributes for each recipient. See the Mailboxes Configuration online Help for details on how to select a mailbox if you don't know its name.

> **Note:** The actual IC Administrator mailbox should not be used in these fields, as it could result in the administrator's mailbox receiving excessive mail. On your email server, you might create an account and mailbox (that the IC Administrator can log on to and check periodically) to be used in these fields.

Voice Mail Recipient

Select the mailbox account to receive voicemail when the intended recipient is not known or cannot be reached. This prevents voicemail from getting lost because an incorrect or ambiguous email address was used. The DS attribute for this account is: **Default Voice Mail Recipient**, found in the $CONFIGPATH\Configuration registry key.

Fax Recipient

Select the Mailbox account (or distribution list) to use to receive faxes when they arrive. This account must be a group or individual who is entrusted with the responsibility of reading the cover page on each fax and then forwarding it to the intended recipients. The DS attribute for this account is: **Default Fax Recipient**, which is found in the $CONFIGPATH\Configuration registry key.

IC Administrator

Select the mailbox account to receive email if a handler needs to report an event. You can customize handlers to send an email notification for any event to the mailbox you select. For example, you could create an email account and mailbox named ICMail, and the CIC administrator could check it periodically for email.

The DS attribute for this account is: **IC Administrator Recipient**, found in the $CONFIGPATH\Configuration registry key.

Voice Mail TUI XML File

This setting supports the migration of Voicemail TUI definitions from handlers to XML.

Default

By default this option is selected and the standard Voicemail TUI XML file is used that is shipped with CIC. The XML file (and other related files) is stored in a standard directory location (defined by the Resources Path server parameter) which is populated during installation.

Custom

Select this option to create a custom Voicemail TUI XML file. Click the Browse button to browse to the custom XML file location.

Host Server

The optionally licensed host tools and host server executable provide an interface between CIC and data stored on mainframe or AS400 computers. CIC's host server subsystem supports a specific number of concurrent connections to the host computer, based on the number of licenses purchased.

> **Note:** Contact your authorized reseller or Genesys to purchase a CIC license key for host access tools.

Maximum number of concurrent sessions:

Enter a number that corresponds to the maximum number of threads you want CIC's host server (HostServerU.exe) to support at one time. The largest number you can enter is equal to the number of concurrent session licenses you purchased from Genesys. For example, if you purchased 24 concurrent session licenses for host computer connections, you could set this field to 24, or any number less than 24 if you wanted to restrict the maximum number of concurrent sessions allowed. Licenses are sold in bundles of 10, 24, and 50.

Host Tools Path:

By default the Host Tools Path is {SERVER PATH}\HostTools. Use this field If you need to change the default path to a local path. The path you enter here overrides the default path.

See Also

CIC Host Integration Solutions document in the **Technical Reference Documents** section of the PureConnect Documentation Library on the CIC server.

Trace Logs

Use this tab to configure the behavior of trace logs.

Log File Compression

Select this option for the CIC system to compress the prior day's log files at the specified time. This option is turned on by default.

Log File Compression Time

Enter the time for the log file compression to start. This option is grayed out unless **Log File Compression is checked** (and enabled). The default time is 12:40 a.m.

CPU Usage

Select the type of compression to use. The faster the compression the higher the CPU usage. The options are:

- High (Fastest Compression)
- Medium(Fast Compression)
- Low (slow compression)
- Very Low (very slow compression)

Disable Logging when there is less than...

Enter the amount of free space remaining in MB that when reached, will disable logging. The default value is 100 MB.

Re-enable Logging when there is more than...

Enter the amount of free space remaining in MB, that when reached, will re-enable logging. This option is only used if logging has been disabled. The default value is 200 MB.

> **Note**: By default, CIC retains logs for 8 days.

Site Information

Enter site information that Interaction Tracker and other CIC components require.

Interaction Tracker uses the information to create user Organization and Location records during the CIC user import. Tracker uses the records to link interactions to CIC users.

Organization Name

Enter the name of your company, for example,"Acme Corporation" or "Acme". The default is OrganizationName.

In a Multi-Site environment, the name should be the same for each site.

Location Name

(Optional) Enter an identifier for physical location, for example, "Indianapolis" or "HQ" or "2nd Floor". The location should generally reflect a mailing address.

If you configured for Multi-Site during installation the Site ID is set. You can change this if it does not suit the location scheme for your customer site. (Note that Site ID is not related to physical location.)

> **Note:** There are no requirements for how to name a location. Choose the scheme that works best for your customer site.

ACD Options

Use this page to configure ACD options at the CIC system configuration level.

Reset Available Time on ACD Available state change

Enable this check box to reset agents' time when they change their status from a non-ACD Available state to an ACD Available state. By default this option is disabled.

Reset Available Time on Logon

Enable this check box to reset agents' time when they log in to a CIC client. By default this option is disabled.

Maintain ACD Skills on transfer

Enable this check box to maintain ACD skills and categories when a call is transferred to a different workgroup or user. By default this option is disabled.

Interaction Client

Use this tab to configure which user records a user sees in the CIC clients.

Company Directory and Transfer Dialog Users' Visibility

To ensure that the user sees only members of the workgroups that the user can view or modify, select **Restrict User's Visibility**. If this option is not selected, the user can see all user records.

> **Note**: Whether a user can view or modify a workgroup depends on access rights.

Update Service

To streamline the configuration of Interactive Update local provider information on CIC client machines, complete the fields on this page. If you do not complete the fields on this page, then you will need to manually configure the local provider on each of your client machines, either during the installation process, through the configuration file, or through Interactive Update.

For complete information on Interactive Update, see the *Interactive Update Technical Reference* in the PureConnect Documentation Library.

> **Important**: In order for this feature to work, IC Server, Interactive Update, and the client applications on client machines must all be on 2016 R2 or later versions.

Update Service Available

Select this check box to enable Interactive Update to receive the information you specify on this page. Then complete the additional fields in the **Update Service URI** group.

If you deleselect this check box, you must manually configure each of your CIC clients.

Auto-configured

Interactive Administrator automatically detects the preferred local provider URI for you. If the displayed URI is correct, you do not need to specify a different URI in the **Override** box.

> **Notes:**
>
> Depending on your network topology, the auto-configured URI may work from server machines but not from client machines. To provide a different override URI that can be reached from all machines, specify the accessible URI in the **Override** box.
>
> Do not specify a remote provider in this box.
>
> If you multiple local providers, specify only one of them here. All local providers share the same database and the data is managed appropriately.

Override

If you want to manually configure the local provider URI that your client machines will use, type its URI here.

> **Note:** Be sure to specify a URI that your CIC client machines can reach.

Administrative Alerts

If CIC detects that a message delivery failed, CIC contacts the administrator via an email message and a phone message. The message contains the error generated by the system.

Use this page to activate or deactivate the administrative alerts and to configure the email address and phone number that CIC uses to notify the administrator.

Enable Administrative Alerts

Use this check box to activate or deactivate administrative alerts.

Phone Number

Type the phone number for the system to send the phone alert message.

Email Address

Type the email address for the system to send an email alert message.

Interaction Processor

Review the IP configuration of your CIC server

To review the IP configuration of your CIC server

1. In the ***<IC Server>*** container, in the list view window, double-click **Configuration**.
   The **Server Configuration** dialog box appears. The boxes on the **IP Configuration** tab are automatically completed for you. For more information, see *IP configuration options*.

> **WARNING:** Do **not** modify the boxes on this tab unless you know what changes need to be made, or you have been instructed to modify the settings by a PureConnect Customer Care representative.
>
> If you get an event log message stating that some handlers did not run immediately because the thread pool limit was reached, contact PureConnect Customer Care or your support representative. A representative will advise you if it is necessary to increase the number of available threads.

Related topics

IP configuration options

Overview of CIC server configuration

Configure your CIC server

Handlers

Handlers

Handlers are the programs that define the interaction processing functionality of the CIC system. A handler is a group of actions (steps) that start when an event occurs on the CIC system. For example, the IVR system that callers interact with is a handler. Handlers can record and send voice mail, for example. Almost every call processing action that occurs on the CIC server is the results of a handler.

For more information about handlers, see the Interaction Designer Help.

Handler Configuration

Handlers published to the CIC server from Interaction Designer appear in the comprehensive list of available handlers under Handler Names. To move a handler from being available (present) on the server to being activated to run on the server, see the Handlers and Monitor Handlers property pages in the **Server Configuration** dialog box.

File Name

Handlers published to the default location are stored in Java class files. In general, you should never need to change the handler's Java class file name unless instructed by qualified technical support personnel. Each time a handler is published, Interaction Designer appends a new date code at the end of each handler's Java class file name (for example, DialPlan0_857349795.class). Do not change these names.

Configuring Handlers

It is possible you will never have to change the following default settings for Handlers. If you get any of the messages stated below, we suggest you contact your PureConnect Customer Care representative before changing any of the values.

Maximum Number of Concurrent Handlers

This number determines the maximum number of handlers that can run concurrently. The default, **0**, means there is no limit to the number of concurrent Handlers.

> If there is a value in this box, and a message appears in the event log stating the Handler has reached its concurrent limit and additional requests to run this handler will be queued up, you can increase the limit. Again, we suggest you contact PureConnect Customer Care before changing this value.
>
> **Note:** This limit applies only to first-level handler calls. Handlers called from within another handler via the "Subroutine" initiator are not subject to concurrent handler limits. This is a safety mechanism to ensure that ongoing handler operations do not stall when calling a subroutine due to handler concurrency limits.

Maximum Number of Handlers Queued

When the maximum number of concurrent Handlers is reached, this field indicates how many handler requests can be queued until a slot becomes available.

If the **Maximum Number of Concurrent Handlers** is set to the default, the **Maximum Number of Handlers Queued** field is gray, and not available. When it is not available, a large allowable maximum value has been pre-set.

This box becomes available when you put a value in the **Maximum Number of Concurrent Handlers** box. If you get a message in the event log stating the Handler has exceeded its maximum queue limit and request to run this handler will be discarded, you can increase the limit in this box. Type a number in the box, or if you select **No Limit**, a **-1** appears in the box. Again, we suggest you contact Customer Support before changing this value.

Handler Priority

You can select **Low**, **Normal**, or **High**. The default setting is **Normal**.

Step Limit

You might need to increase the step limit if you get a message in the error log stating the Handler has exceeded its step limit. If the Handler should not have exceeded this step limit, there may be an infinite loop in the Handler. The default, **0**, has a value of 10,000. If you click **No Limit**, a **-1** appears in the box. Again, we suggest you contact Customer Support before changing this value.

Initialization Functions

Initialization Function

Initialization functions are functions that perform some system initialization when the CIC system starts. These functions are contained in DLLs that must be registered on the CIC server in Interaction Administrator. Multiple initialization functions can be called during system initialization.

Initialization Function Name

Type the name of an initialization function. Use a meaningful and unique name.

Initialization Function Configuration

Type the initialization function's name and the name of the DLL containing the function. Select the **Active** check box to make it available to the Interaction Processor.

> **Warning:** Do not modify or remove the default CIC initialization functions or the system might not work.

Introduction to Table Editor

Interaction Administrator and Interaction Designer (through the Table Lookup tool) both provide access to a table editor that allows you to create simple, indexed, in-memory databases for fast lookups during CIC interaction processing. The tables are stored on the CIC server and reside in Virtual Memory (VM) while CIC is running. These tables are read-only in the current release.

The Table Editor portrays the table as a set of rows and columns much like a spreadsheet or relational database. You can easily add columns and rows using the toolbar buttons or menu commands. To edit a cell, double-click on it or use one of the keyboard shortcuts. All cell editing is done in place (within each cell). The editor supports multi-level undo and redo operations. When you click on the Save button, CIC re-reads the table into memory and the table values are immediately available for access.

Each column has a label and an index. The label is used to identify each column, and indexed column labels appear in the list of "Columns for Lookup" in the Table Lookup tool in Interaction Designer. Indexes define columns you search quickly for specific values. If a column does not have an index, you cannot use that column as a search key.

Each table is a stand-alone entity. Tables do not obey typical relational operations such as joins and views. Tables are stored on and referenced from the CIC server. Each table and column in that table has a globally unique identifier, a GUID, which uniquely defines each table and each column.

In order to perform a lookup on a table, at least one column in the table must have an index. Table Editor supports two kinds of indexes:

Unique - each entry in the column is unique (for example, account number) and it cannot contain duplicate values. Table Editor warns you if it finds duplicates. Lookups on unique index columns are faster than on columns with duplicate values.

Multiple - each entry in the column may have one or more occurrences of that value in the column (for example, account type, date, and so on). Lookups on multiple value indexes are slower than on columns with unique indexes.

What is the difference between an .i3Table and a .i3TableEX file?

Normally, table data is stored in 2 locations: (1) The column information is stored in the registry; and (2) the data is stored in the .i3Table file. You shouldn't care about these storage structures, they are internal and could change at any time. CIC keeps data in the registry to make lookups/browsing of the different table types quicker.

When you export a table to the .i3TableEx file, it contains the columns found in the registry (1) plus the table data (2). A complete stand-alone 'table'.

CIC stores the data in .i3Table internal format because it may be too big to fit in the registry. We envision large tables may be stored.

> **Note**: For the best performance, tables should contain no more than 2,000 records. Also note that table lookups are case sensitive.

Phone Numbers

Overview of the Phone Numbers container

For information on the **Phone Numbers** container, click the links under *Related topics*.

Related topics

Old dial plans

Regional dial plans

DID/DNIS

Private lines

Old Dial Plans

Overview of old dial plans

An old dial plan was created with an older version of Interaction Administrator (pre-2.4). Old dial plans have a two-table format and a .i3pnum extension.

In the **Phone Numbers** container, you can import old dial plans and use them with the current release of Interaction Administrator. However, you will not gain the benefits of the newer regional dial plans.

> **Note**: Only one dial plan format (old dial plan or regional dial plan) can be active. CIC uses the active dial plan to perform dial plan lookups and make calls.
> If necessary, you can modify an inactive dial plan and test it by simulating calls.

For more information about old dial plans, click the links under *Related topics*.

Related topics

Import a dial plan

Configure an old dial plan

Manage phone number classifications

Simulate a call

Advanced dial plan options

Import a dial plan

You can import an entire CIC phone number plan that was saved (with the **Export** button) by any CIC server. Exported CIC phone number files have a `.i3dplan` extension and include all of the input conversion objects, dial plan objects, and classification names.

To import a dial plan

1. In the **System Configuration** container, click the **Phone Numbers** subcontainer.
2. In the list view, double-click **Configuration**.
3. In the **Phone Number Configuration** dialog box, on the **Regional Dial Plan** tab, click **Dial Plan**.
4. Click **Import**.
5. Click **Browse** button to select a `.i3dplan` file, and then click **Next.**
6. Click **Next** to navigate through the dialog boxes that display the contents of the dial plan file.
7. When you are presented with import options (replace or skip the merge), select the appropriate check boxes and then click **Next**.
8. Review the changes and then click **Finish**.
9. When the message appears that indicates that you have not yet saved your changes, click **OK**. You save your changes when you click **OK** on the **Regional Dial Plan** dialog box.

Related topics

Configure a regional dial plan in Interaction Administrator

Export a dial plan

Configure an old dial plan

To configure an old dial plan

1. In the **System Configuration** container, click the **Phone Numbers** subcontainer.
2. In the list view, double-click **Configuration**.
3. In the **Phone Number Configuration** dialog box, on the **Old Dial Plan** tab, click **Dial Plan**.
4. Complete the tabs in the dialog box. For more information, click the links under *Related topics*.

Related topics

Overview of input conversion

Configure input conversion

Configure dial plan objects

Simulate a call

Overview of input conversion objects

When you configure an old dial plan, you can create and modify the objects in the input conversion table. CIC uses the objects in this table to find a match between the raw dialed input (however it was initiated) and the input pattern. If it finds a match, the input is converted into a standardized output pattern. This output pattern number is then used as input in the dial plan table. If you are unfamiliar with the syntax for specifying input patterns and the output pattern format, see *CIC Regionalization and Dial Plan Technical References*, in the PureConnect Documentation Library.

Related topics

Configure input conversion objects

Configure input conversion objects

To configure input conversion objects

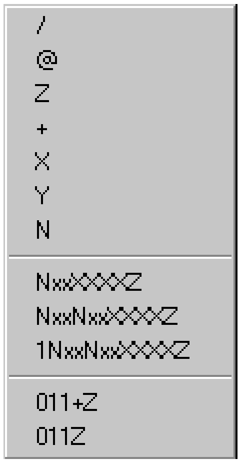
1. In the **System Configuration** container, click the **Phone Numbers** subcontainer.
2. In the list view, double-click **Configuration**.
3. In the **Phone Number Configuration** dialog box, on the **Old Dial Plan** tab, click **Dial Plan**.
4. On the **Input Conversion** tab, configure input conversion object names. Each input conversion object name represents an input pattern and an output pattern pair. The order in which the input conversion object names appear determines the order in which CIC searches for a match between the dialed input and one of the input patterns. Complete the following steps as necessary.
   - To add a new input conversion object, click **Add**. Type a name in the **Entry Name** dialog box and then click **OK**. Then select the object and click **Up** or **Down** until the object is in the appropriate position in the list.
   - To create a new object that is similar to an existing object, click an object in the list and then click **Copy**. Type a name in the **Entry Name** dialog box and then click **OK**. Modify the **Input Pattern** and **Output Pattern** fields as necessary.
   - To rename an object, select the object and click **Rename**. Type the new name in the **Entry Name** dialog box and then click **OK**.
   - To delete an object, select it and then click **Remove**.
   - To create a group of similar input conversion objects that map to a group of similar dial plan objects, click **Add Many**. For example, you can specify a list of exchanges included in local, toll-free dialing. You can enter (or import) the list of exchanges once and create a rule that substitutes these exchanges into the input conversion object and the dial plan object. For more information, see *Add Many Input Object Configuration*.

- To export all phone number objects (input conversion, dial plan, classification names, and many input pattern objects) to a file, click **Export**. The file has the extension .i3pnum (for example, *PhoneNumbers.i3pnum).* This is a good way to preserve your entire dial plan data, or to transfer this data to another CIC server where you can import it into the local phone number configuration.
- To import an .i3pnum file into CIC, click **Import**. This import operation detects new objects (for example, new dial plan objects, new classifications, etc.) and adds them to the existing phone numbers. It also merges identically named objects by replacing them. If any of the imported objects depend on line groups that are not defined in the current system, CIC warns you about this. You must create the expected line groups or modify the dial plan entries to be able to use these imported numbers.

5. In the **Input Pattern** field, enter a string of literal numbers, variables, or both. CIC tries to match the dialed input with this pattern. If it does not find a match with any of the defined input patterns, it passes the number through to the Dial Plan table unchanged.

   To create an input pattern, you must be familiar with wildcard pattern syntax. If the following tables and the input assistance prompts (**->**) do not provide enough detail to help you understand how to use the pattern syntax, see C*IC Dial Plan*, in the Technical Reference Documents section of the PureConnect Documentation Library on the CIC server.

   The input assistance prompt displays a drop-down menu containing the special input characters allowed in the **Input Pattern** field, as well as some commonly used input patterns, which you can select and modify if necessary.



The commonly used patterns in the list represent the following types of phone numbers (in the NANP):

Input Patterns	Description
NxxXXXXZ	Local toll free calls
NxxNxxXXXXZ	Long distance toll calls

1NxxNxxXXXXZ	Direct-dial long distance toll calls
011+Z	Any international number dialed from input containing '+'
011Z	Any international number without a '+' sign

The most commonly used wildcard characters are:

Characters	Variables (wildcards)
0 - 9	'X' (or 'x') represents a single digit character in that range
1 - 9	'Y' (or 'y') represents a single digit character in that range
2 - 9	'N' (or 'n') represents a single digit character in that range
'0' - '9', '#', '*', ','	'?' represents zero or more of these characters. (Note that '/', '@', and '+' are not included).
Any characters after the required digits	'Z' (or 'z') represents zero or more trailing characters of any value. Using Z allows the dialer to enter extra characters after the required digits without interfering with the dial string. This wildcard character must be the last character of the pattern; it is an error for it to appear anywhere else (which means there can be only one occurrence of this character in each number).

Phone number templates can consist of all digits, all wildcard characters, some non-dialing characters such as '+', '@', and '/', or any combination of these characters. The '/' character is generally used as a prefix to introduce an extension for direct extension dialing. The '@' character is used as a prefix before an extension, but that extension is not automatically dialed (that is, it is stored as informational data with the number). The '+' is used as a prefix to introduce a country code. These three characters are not actually dialed, but they are preserved as part of the stored phone number. The spaces these characters hold within the number are counted when determining ordinal positions in the formatted number (that is, which number is in the first position, second position, and so on).

6. In the **Output Pattern** field, enter numbers that represent the unknown dialed digits. To do this, click the button on the right side of **Output Pattern** field. Select characters from the list of ordinal numbers that appears in the list.

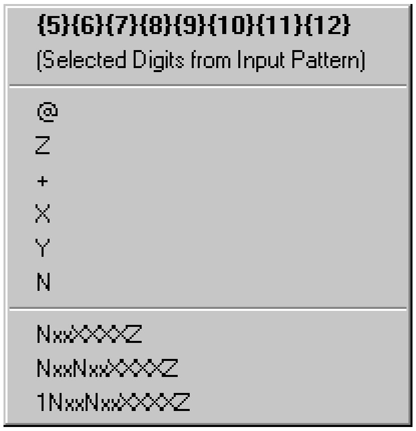
You can enter numbers in two different ways: 1) using the input pattern (that is, wildcard) characters, or 2) using the ordinal positions of wildcard characters (or any characters) in the number. The ordinal positions of characters in the standardized phone number patterns are represented by: {1}, {2}, {3}, and so on. (Ordinal numbers identify the position or order in a sequence, such as 1st, 2nd, 3rd, and so on.)

To illustrate this, consider a pair of input pattern and output pattern templates for local phone numbers.

Local Number Input Pattern	Output Pattern--Wildcard List	Output Pattern--Ordinal List
NxxxxxxZ	+1317NxxxxxxZ	+1317{1}{2}{3}{4}{5}{6}{7}{8}
317NxxxxxxZ	+1317NxxxxxxZ	+1317{4}{5}{6}{7}{8}{9}{10}{11}
1317NxxxxxxZ	+1317NxxxxxxZ	+1317{5}{6}{7}{8}{9}{10}{11}{12}

Both the wildcard list style (middle column) and the ordinal list style (right column) of the output pattern represent the dialed local number in the same way. To CIC, the numbers are interchangeable.

The list to the right of the **Output Pattern** field provides an easy way to specify the ordinal numbers for the input pattern above.



7. In the **Conversion Description** field, explain the purpose of the object. This helps to distinguish the object from similar objects in the table.
8. Click **OK**.

Related topics

Configure an old dial plan

Overview of input conversion objects

Add Many Input Object Configuration

☎Configure dial plan objects

To configure dial plan objects

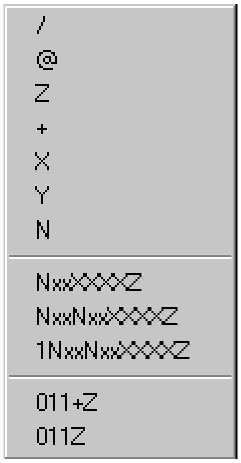
1. In the **System Configuration** container, click the **Phone Numbers** subcontainer.
2. In the list view, double-click **Configuration**.
3. In the **Phone Number Configuration** dialog box, on the **Old Dial Plan** tab, click **Dial Plan**.
4. On the **Dial Plan** tab, configure dial plan objects.
    - To add a new dial plan object, click **Add**. Type a name in the **Entry Name** dialog box and then click **OK**. Then select the object and click **Up** or **Down** until the object is in the appropriate position in the list. This list controls the order in which CIC searches the input pattern list (from top to bottom), based on the order of the names.

    > **Notes:** This order is critical to the dial plan processing stage of dialing.
    >
    > The packaged dial plan objects that come with CIC serve as a good example of the kinds of names and the kind of order you may want to use in your own dial plan.

    - To create a new object that is similar to an existing object, click an object in the list and then click **Copy**. Type a name in the **Entry Name** dialog box and then click **OK**. Modify the **Dial Plan Object** fields as necessary.
    - To rename an object, select the object and click **Rename**. Type the new name in the **Entry Name** dialog box and then click **OK**.
    - To delete an object, select it and then click **Remove**.
5. Complete the **Input Pattern** field. Phone numbers in the **Input Pattern** box on the **Dial Plan** tab are formatted exactly like the numbers in the **Output Pattern** field on the **Input Conversion** tab. This is because the phone number input for dial plan processing is already in a standardized format (in the **Output Pattern** field) based on the results of the input conversion step. However, the input patterns used on the **Dial Plan** tab are not limited to, nor are they necessarily the same as the output pattern used on the **Input Conversion** tab, but they can be identical if necessary. This input pattern table is the key to successfully managing your dial plans.

    For example, within the 317 area code, there are long distance exchanges and local exchanges. Depending on your location within the area, there may be just a few local exchanges and many long distance exchanges. In that case, it would be more efficient for you to create an Input Pattern list that includes a pattern for each local exchange and a single general pattern to match all long distance calls within the area. In other locations, the opposite approach may be more efficient.

The **Input Pattern** field displays a list of the special input characters that are allowed in the **Input Pattern** field. It also displays some commonly used input patterns, which you can select and modify if necessary.



The commonly used patterns in the list represent the following types of phone numbers (in the NANP):

Input Patterns	Description
NxxXXXXZ	Local toll free calls
NxxNxxXXXXZ	Long distance toll calls
1NxxNxxXXXXZ	Direct-dial long distance toll calls
011+Z	Any international number dialed from input containing '+'
011Z	Any international number without a '+' sign

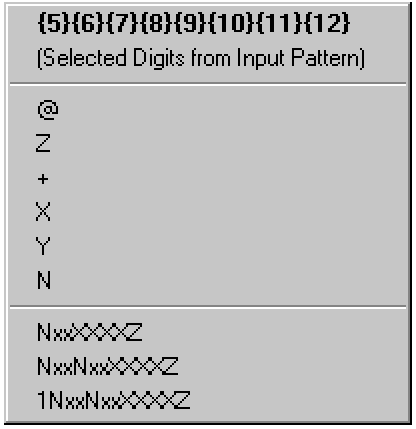
The following **Characters** are represented by these **Variables**:

Characters	Variables (wildcards)
0 - 9	'X' (or 'x') represents a single digit character in that range
1 - 9	'Y' (or 'y') represents a single digit character in that range

2 - 9	'N' (or 'n') represents a single digit character in that range
'0' - '9', '#', '*', ','	'?' represents zero or more of these characters. (Note that '/', '@', and '+' are not included).
Any characters after the required digits	'Z' (or 'z') represents zero or more trailing characters of any value. Using Z allows the dialer to enter extra characters after the required digits without interfering with the dial string. This wildcard character must be the last character of the pattern; it is an error for it to appear anywhere else (which means there can be only one occurrence of this character in each number).

To specify the ordinal numbers for the input pattern above:

- Select the characters in the **Input Pattern** field you want to convert to ordinal numbers.
- Click the {} button on the right side of the **Default Dial String** or **Display String** field. The following list appears.



- Select from the list of ordinal numbers.

6. In the **Standardized Number** field, enter the standard format for all phone numbers. This information is used by applications that perform reverse white pages lookups.
7. In the **Default Dial String** field, enter the actual string of characters sent to the CO to place a call. You can specify the dial string based on the dialing requirements the CO may have on your lines. For example, some areas may require you to dial the local area code, even for non-toll local calls. In the **Default Dial String** field, you can add the local area code as a prefix to all local calls, so that CIC users do not need to dial the local area code. As another example, some trunks may require you to dial a '1' or a '9' prefix before certain numbers, or perhaps you need to add a long distance prefix to specify a long distance carrier (for example, 1010550). You can add any prefix (or suffix) to any type of phone number using the **Default Dial String** field. Users do not need to dial the numbers you include as a prefix in the **Default Dial String** field.

The dial string variable uses the same standardized format syntax described in the *Input Pattern* section on the **Input Conversion** tab. You can use either the wildcard character syntax or the ordinal number. However, if you use the wildcard characters, pay attention to the two conditions where you might have to use the ordinal number syntax in this field, and the potential efficiency of ordinal numbers over wildcard characters. For more information about syntax, search for *Ordinal or Wildcard Syntax* or *Dial Plan Phone Numbers* in the PureConnect Documentation Library on the CIC server.

> **Note:** Even though the '+', '/', and '^' symbols are not dialable characters, you can include them in a dial string entry if you want to. CIC ignores the '+' character when dialing. The '/' precedes digits to dial (for example, an extension) after the main number connects. The '^' indicates numbers stored with the main number (for example, an extension), but are not dialed.
>
> If you use '/' and '^' together (in either order), CIC knows to dial the extension. If you use '^' by itself as a prefix for an extension, CIC does not dial the extension.

8. In the **Display String** field, enter the formatted phone number that appears to users when the user is not allowed to edit the phone number before the call is placed. You can control the numbers displayed to end users by the template you use in the **Display String** field. For example, if the standardized form of the number includes a special long distance carrier prefix (for example, 1010550), you can drop that part from the phone number you display to CIC client users.

   The display string variable uses the standardized format syntax. You can use either the wildcard character syntax or the ordinal number. However, if you use the wildcard characters, pay attention to the two conditions where you might have to use the ordinal number syntax in this field, and the potential efficiency of ordinal numbers over wildcard characters. For more information about syntax, search for *Ordinal or Wildcard Syntax* or *Dial Plan Phone Numbers* in the PureConnect Documentation Library on the CIC server.

9. In the **Default Classification** list, select the descriptive name for the group of phone numbers. Phone number classifications allow you to control the kinds of phone numbers each user, workgroup, or station can dial. You assign dialing privileges by selecting access control rights for workgroups, roles, or stations.

   You must select a classification name for each dial plan object. For more information on how to add new classifications, see *Manage dial plan classifications*.

10. In the **Components** box, specify the different parts of a phone number in each dial plan entry that need to be tracked in the report logs (such as area code, long distance prefix, country code, and so on). These components are used for tracking different parts of the phone number in the reporting databases.

> **Note:** If you create new dial plan objects for the Local and Long Distance categories, you must copy the content of the default Components field (such as the ReportingCode1 and ReportingCode2 components) and paste them in to your components field. Failure to do this may result in incomplete call data in your reports.

The default dial plan objects in the Local and Long Distance classifications created during installation contain two components: ReportingCode1 and ReportingCode2. These components represent the digits in the ordinal positions indicated by the ordinal number syntax in the field. For example, the syntax for the first entry is:

ReportingCode1:{3}{4}{5};

The part before the colon is the name or label for this component ("ReportingCode1"). The ordinal numbers after the component refer to the 3rd, 4th, and 5th digits in the current dial plan object. In the case of a Local or Long Distance classified number in the NANP, these digits always refer to the area code. The semicolon at the end is simply a separator between components.

In another example, the syntax for the second component in the Components field is:

ReportingCode2:{6}{7}{8}

Again, the part before the colon is the component name ("ReportingCode2"). The ordinal numbers after the component refer to the 6th, 7th, and 8th digits in the current dial plan object. In the case of a Local or Long Distance classified number in the NANP, these digits always refer to the local exchange.

If these same digits refer to a different part of the phone number in another location (such as city code, prefecture code, etc.), you can keep these components as they are and they will work for your location. If you need to track other parts of the phone number, you must:

- Create new components in the **Components** box.
- Customize the CallDisconnectMonitor handler to add the new components to one of the extra columns in the Call Detail report log.
- Modify or add a new column in a Crystal Report template that is based on the Call Detail report log.

11. In the **Description** box, document the purpose, along with any details, of each dial plan entry. This information will be valuable to other CIC administrators, especially if you have more than one administrator managing CIC or more than one person editing the dial plan configuration.
12. To use account codes, select the **Account Code Verification** option. After you select this option, you can track that call type with a verified account code that the user provides for the outbound call. You can use this feature to track call types for billing purposes.

Note: You should **not** apply Account Code Verification to the **911** and **Intercom** Dial Plan Objects.

13. Configure dial groups for the object. Dial groups enable you to specify which outbound lines or channels to use for each type (classification) of phone number. For example, international calls may be directed to one dial group that uses lines with the best rate for international calls. Local calls may be directed to another dial group called "Local" over low-cost analog lines from the local CO. If you do not specify a dial group for a dial plan entry, calls placed via that dial plan object use the first available line with a direction of Outbound or Both.

Note: All of the lines or channels in a dial group must have identical dialing requirements. For example, in a dial group, you cannot have some lines that require a 9 prefix and other lines that do not.

Do the following, as necessary:

- To add a dial group, click **Add Group**. Select the dial group and then click **OK**. If there are no dial groups, create them in the **Line Groups** container.
- To edit a dial group, select it and then click **Edit**.
- To remove a dial group, select it and then click **Remove.**
- To add a secondary dial group to an existing dial group entry, select the dial group and then click **Add Group.**

Related topics

Configure an old dial plan

Manage phone plan classifications

Overview of phone number classifications

Phone numbers that can be identified by a pattern in the numbers, or an explicit group of phone numbers with a common purpose are called phone number classifications. For example, internal calls could be identified by the "Internal" classification, toll free (for example, 800 numbers) could be identified by the "Toll Free" classification, and calls to emergency services (such as 911, fire department, police, and hospital) could be identified by the "Emergency" classification.

These named groups of phone numbers are used to control individual users, workgroups, and station dialing privileges in CIC. For example, stand-alone phones may have only Emergency and Internal dialing privileges, while members of the Sales workgroup may have full dialing privileges provided in all classifications.

When CIC users dial a phone number, CIC matches the number dialed with the appropriate classification pattern. It then checks the user's dialing privileges to determine if the user or station is authorized to place the call. In this way, CIC uses phone number classifications to control individual users, workgroups, roles, and station dialing privileges.

You also use classifications to configure forced authorization codes. Administrators set forced authorization codes to require users to enter an extension and a password to make a call.

You create a list of classifications on the **Classifications** dialog box in the **Phone Number Configuration** dialog box. To create the number pattern for the classification, use the **Dial Plan** dialog box.

> For more information about phone numbers see the *CIC Regionalization and Dial Plan Technical Reference* in the PureConnect Documentation Library.

Related topics

Configure an old dial plan

Manage phone number classifications

Manage phone number classifications

To manage phone number classifications

1. In the **System Configuration** container, click the **Phone Numbers** subcontainer.
2. In the list view, double-click **Configuration**.
3. In the **Phone Number Configuration** dialog box, on the **Old Dial Plan** tab or on the **Regional Dial Plan** tab, click **Manage Classifications**.
4. In the **Dial Plan Classifications** dialog box, do one of the following:
   - To add a classification, click **Add**. Type the name of the classification (for example, "900 Service" or "International"), and then click **OK**. Then continue with the next step.
   - To edit a classification, select it and then click **Edit**. Then continue with the next step.
   - To delete a classification, select it and then click **Remove**.
5. In the **Classification** dialog box, the name of the classification appears in the **Display Text** field. You can change this if necessary.
6. In the **Category** list, select the appropriate category.
7. In the **Alerting** section, select the **Send email and client alerts for calls of this classification** check box, and enter the users to receive the alerts in the **To...** field. You can also click the **To...** button and select the available users from the list that is displayed. Alerting sends an email notification and displays a popup notification in the CIC clients, to the specified users and/or workgroups when a call is made with this classification.
8. As necessary, complete the **Multi-Language Support** tab. For more information, see *Multi-Language Support*.
9. Click **OK**.

Related topics

Configure an old dial plan

Overview of phone number classifications

Set up an emergency classification

Simulate a call

This property page enables you to test your dial plan configuration by entering real phone numbers in any format you can imagine. Since users may enter phone numbers in a variety of ways (with or without a leading 1, with or without a local area code, etc.), you can test different kinds of input without actually placing a live call to different numbers. This page just simulates calls as if they were dialed from a CIC station; it does not actually place calls to the dialed numbers.

To simulate a call

1. In the **System Configuration** container, click the **Phone Numbers** subcontainer.
2. In the list view, double-click **Configuration**.
3. In the **Phone Number Configuration** dialog box, click **Simulate Call**. This button appears in the following places:
    - On the **Old Dial Plan** tab
    - On the **Simulate Call tab** in the **Old Dial Plan** dialog box
4. Under **Call Input**, in the **Number** field, enter a phone number. You can type letters or digits.
5. Click **Simulate Call**.
   CIC passes your number input through the input conversion objects and dial plan objects you created. The **Call Results** fields display the results.

   If you applied the account code verification feature properly to a dial plan object, the box is checked here for information purposes only. You can track that call type by using a verified account code that the user provides for the outbound call. Use this feature to track call types for billing purposes. You should **not** apply account code verification to the **911** and **Intercom** dial plan objects.

   The most important results you might look at first are in the three-column list box at the bottom of the **Call Results** group. This box shows which dial group (if any) the call would go out on, the phone number classification for which users would need access rights to dial, and the actual dial string - the number CIC sends to the CO when dialing. The other call results fields indicate which entries in the **Input Conversion** dialog box and the **Dial Plan** dialog box the input matched.

   If you manage to enter a number that does not match any of the standard input conversion objects or dial plan objects, the unknown classification will appear in the three-column list box, and the other call results fields will display the raw number you entered. This indicates that you do not have an Input Conversion object to match this input and the program could not convert the number into an output pattern to process in the dial plan.

> **Tip:** To see where each classification is used, go to the **Classifications** dialog box and select **Usage**.

Related topics

Configure an old dial plan

Activate a dial plan

> **Note:** Only one dial plan format (Old Dial Plan or Regional Dial Plan) can be active. CIC uses the active dial plan to perform dial plan lookups and make calls.
> If necessary, you can modify an inactive dial plan and test it by simulating calls.

To activate a dial plan

1. In the **System Configuration** container, click the **Phone Numbers** subcontainer.
2. In the list view, double-click **Configuration**.
3. In the **Phone Number Configuration** dialog box, on the **Old Dial Plan** tab or the **Regional Dial Plan** tab, click **Advanced**.
4. Under **Active Dial Plan**, select the dial plan that you want to activate.
5. Click **OK**.

Related topics

Overview of old dial plans

Configure a regional dial plan in Interaction Administrator

Select which dial plan to view

If you have both an old dial plan and a regional dial plan, you can select which one to view in the **Phone Numbers** container.

> **Note:** If you choose to view both dial plans, the **Phone Number Configuration** dialog box displays a separate tab for each one.
>
> Only one of the plans can be active at a time.

To select which dial plan to view

1. In the **System Configuration** container, click the **Phone Numbers** subcontainer.
2. In the list view, double-click **Configuration**.
3. In the **Phone Number Configuration** dialog box, on the **Old Dial Plan** tab or the **Regional Dial Plan** tab, click **Advanced**.
4. Under **Dial Plan View**, select the dial plan that you want to view.
5. Click **OK**.
6. Close the **Phone Number Configuration** dialog box.
7. Reopen the **Phone Number Configuration** dialog box.

Related topics

Activate a dial plan

Overview of old dial plans

Configure a regional dial plan in Interaction Administrator

Regional Dial Plans

Overview of regional dial plans

A regional dial plan is a set of rules that determines how a dialed phone number is handled. Ideally, every phone number that a user dials through CIC should match an entry in the dial plan. However, if a dialed number does not match a pattern in the dial plan, CIC dials the number as it was entered.

For more information on how to represent phone numbers in CIC, see *CIC Regionalization and Dial Plan* in the PureConnect Documentation Library.

Related topics

Overview of how to add a dial plan

Configure a regional dial plan in Interaction Administrator

Managed named lists of phone numbers

Manage phone number classifications

Simulate a call

Advanced dial plan options

Add a dial plan in Setup Assistant

You can use Setup Assistant to create a North American dial plan or to import and localize a dial plan file.

To add a dial plan in Setup Assistant

1. Start **Setup Assistant** and select **Dial Plan**.
2. Do one of the following:

- Select **Import a Dial Plan File**.
  Select this option to import an existing dial plan file. For example, a reseller may have created specific complete dial plans for customers in different regions of the country, county, or city. Setup Assistant uses macro substitutions to enable localizers to set up a dial plan for their locale from the imported dial plan file.

  This option is recommended for countries using numbering plans *other than* the North American Numbering Plan.

  Specify the path to the dial plan file. By default, Setup Assistant looks in the \server\IC\Manifest directory. If the dial plan file is not located in this directory, browse to the appropriate directory.

> **Note**: CIC uses a regional dial plan, enhanced for SIP, with an .i3dplan extension. For more information about dial plans, see *CIC Regionalization and Dial Plan* in the PureConnect Documentation Library.

- Select **I don't have a dial plan; help me create one**.
  Select this option if you want Setup Assistant create a dial plan for you. This option is recommended for countries using the North American Numbering Plan. You only need to define a few elements —local area codes and exchanges — and Setup Assistant will do the rest to create a North American dial plan.

3. After the new installation is completed, you can modify your dial plan in the **Phone Numbers container** in Interaction Administrator to:

- Change the default dialing privileges (classifications) set by Setup Assistant.
- Add extensions, area codes, or change the number of digits dialed.

Related topics

Configure a regional dial plan in Interaction Administrator

Configure a regional dial plan in Interaction Administrator

To configure a regional dial plan in Interaction Administrator

1. In the **System Configuration** container, click the **Phone Numbers** subcontainer.
2. In the list view, double-click **Configuration**.
3. In the **Phone Number Configuration** dialog box, on the **Regional Dial Plan** tab, click **Dial Plan**.
4. On the **Regional Dial Plan** dialog box, do one of the following:
    - To add a dial plan pattern, click **Add**. When you add a dial plan pattern, you can also configure dial groups. For more information, see *Configure a dial group entry*.
    - To edit a dial plan pattern, select it and then click **Edit**. When you edit a dial plan pattern, you can also configure dial groups. For more information, see *Configure a dial group entry*
    - To copy a dial plan pattern, select it and then click **Copy**. When you copy a dial plan pattern, you can also configure dial groups. For more information, see *Configure a dial group entry*
    - To delete a dial plan pattern, select it and then click **Remove**.
5. Configure the lists of phone numbers for the dial plan. For more information, see *Configure named lists of phone numbers*.
6. Configure the classifications for the dial plan. For more information, see *Manage phone number classifications*.
7. Test the dial plan. For more information, see *Simulate a call*.

8. Click **OK**.

Related topics

Configure the pattern of a regional dial plan

Configure a dial group entry

Import a dial plan

Export a dial plan

Manage named lists of phone numbers

Manage phone number classifications

Simulate a call

Configure the pattern of a regional dial plan

When you configure a regional dial plan, you must configure its pattern.

To configure the pattern of a regional dial plan

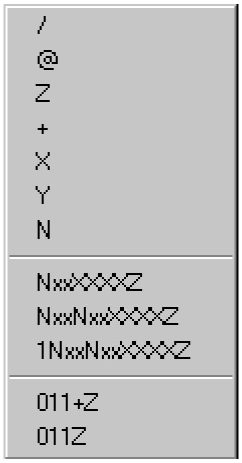
1. In the **System Configuration** container, click the **Phone Numbers** subcontainer.
2. In the list view, double-click **Configuration**.
3. In the **Phone Number Configuration** dialog box, on the **Regional Dial Plan** tab, click **Dial Plan**.
4. On the **Regional Dial Plan** dialog box, do one of the following:
    - To add a dial plan pattern, click **Add**.
    - To edit a dial plan pattern, select it and then click **Edit**.
    - To copy a dial plan pattern, select it and then click **Copy**.
5. In the **Regional Dial Plan - Edit Pattern** dialog box, in the **Input Pattern** field, enter a series of literal numbers, variables, or both. CIC tries to match the dialed input with this pattern.

    The combination of the input pattern, list name, and location filter define a unique dial plan entry.

    The input assistance prompt displays a list of the special input characters that are allowed in the **Input Pattern** field. It also contains commonly used input patterns, which you can select and modify if necessary. You should also be familiar with wildcard pattern syntax.

> **Note**: Quoted and escaped string literals
>
> The Regional Dial Plan enables CIC administrators to embed literal characters or strings in a dial plan input pattern, even if it contains wildcard characters. These literal characters in an input pattern can be used by handler customizations to do special processing, or provide visible indicators to CIC administrators. For example, “Oldphone:”+1NxxNxxxxxxZ , or

sip:"?"@"inin.com". Previously, this would not be possible because certain characters (such as "?" and "n") were only treated as wildcard characters.



Phone number templates can consist of all digits, all wildcard characters, some non-dialing characters such as '+', '^', and '/', or any combination of these characters. The '/' character is generally used as a prefix to introduce an extension for direct extension dialing. The '^' character is used as a prefix before an extension, but that extension is not automatically dialed (that is, it is stored as informational data with the number). The '+' is used as a prefix to introduce a country code. These three characters are not actually dialed, but they are preserved as part of the stored phone number. The spaces these characters hold within the number are counted when determining ordinal positions in the formatted number (that is, which number is in the first position, second position, and so on).

6. In the **Location Filter** list, optionally select a filter to apply for a specific location. This is a feature of regionalization. Locations are used to restrict or filter access to dial plan entries. You can use a **location filter** for the dial group entries. The combination of the location filter, list name, and input pattern define a unique dial plan entry.

   The **Location Filter** options are:

   - **<All>** - Select this option to make this dial plan entry specific to all stations, regardless of location.
   - **<Skip>** - Select this option to ignore the location filter completely.
   - **<Many Locations...>** - Select this option to choose multiple locations for this dial plan entry. This option is available only if you have defined one or more locations.
   - <Default Location> - Select this option to choose the <Default Location> for this dial plan entry.
   - Specific locations - Select a specific location from the list for this dial plan entry. This option is available only if you have defined one or more locations.

Notes: For stations that do not belong to a location, (those that have an empty location string), the **All** option is the only option that will match these stations.

> If a dial plan entry does not have <All> access, then those specific options (patterns or dial groups) are removed from the dial plan and are not presented as dialing choices on dialing lookup in the describe number tool.
>
> Any input pattern that has the <All> filter may require special care when defining the dial groups for the dial plan entry. For example a 911 pattern, the default line groups specified should be local to the location region as possible.

7. In the **List Name** list, select the list name. For information on how to add or edit the list names, see *Managed named lists of phone numbers*. The combination of the list name, pattern, and location filter define a unique dial plan entry.
8. In the **Classification** list, select the classification of phone numbers. For information n how to add or edit the classifications, see *Manage phone number classifications*.

   Phone numbers that can be identified by a pattern in the numbers, or an explicit group of phone numbers with a common purpose are called phone number "classifications." For example, internal calls could be identified by the "Internal" classification, toll free (for example, 800 numbers) could be identified by the "Toll Free" classification, and calls to emergency services (such as 911, fire department, police, and hospital) could be identified by the "Emergency" classification.

   These named groups of phone numbers are used to control individual users, workgroups, and station dialing privileges in CIC. For example, stand-alone phones may have only Emergency and Internal dialing privileges, while members of the Sales workgroup may have full dialing privileges provided in all classifications.
9. In the **Standardized Number** field, select the standardized number entry and modify it if necessary. The standardized number is a standard format for all phone numbers. Its primary use is to store called numbers in a +1 calling format.

> **Note**: This standardized number is used to make a call, so input patterns should be defined to match the standardized numbers. For example, the 7-digit pattern 715xxxx maps to +1317715xxxx, so there should be a +1317715xxxx, or an equivalent input pattern, in the table to match the standardized number.

10. In the **Default Dial String** field, enter the default dial string. You can select the dial string entries from the list and modify the numbers and characters, if necessary. The dial string is the actual string of characters sent to the CO to place a call. You can specify the dial string based on the dialing requirements the CO may have on your lines. For example, some areas may require you to dial the local area code, even for non-toll local calls. Using the **Dial String** field, you can add the local area code as a prefix to all local calls so CIC users do not need to dial the local area code. As another example, some trunks may require you to dial a '1' or a '9' prefix before certain numbers, or perhaps you need to add a long distance prefix to specify a long distance carrier (for example, 1010550). You can add any prefix (or suffix) to any type of phone number using the Dial String field. CIC client users do not need to dial the numbers you include as a prefix in the Dial String field.

11. In the **Display String** field, enter the formatted phone number that is displayed in the CIC clients when the user is not allowed to edit the phone number before the call is placed. You can control the numbers displayed to end users by the template you use in the **Display String** field. For example, if the standardized form of the number includes a special long distance carrier prefix (for example, 1010550), you can drop that part from the phone number you display to CIC client users.

    The display string variable uses the standardized format syntax. You can use either the wildcard character syntax or the ordinal number. However, if you use the wildcard characters, pay attention to the two conditions where you might have to use the ordinal number syntax in this field, and the potential efficiency of ordinal numbers over wildcard characters. For more information about syntax, search for *Ordinal or Wildcard Syntax* or *Dial Plan Phone Numbers* in the PureConnect Documentation Library on the CIC server.

12. In the **Edit Base** field, select an entry from the list and then modify the numbers and characters as necessary. The edit base is an existing phone number from the system that the user can modify before the call is placed. For example, in the CIC clients, the edit base number could be any of the following:

    - A Directory or Speed Dial Contact phone number that the user has permission to modify
    - A Follow-Me configuration number
    - A forward status forward number
    - A remote number station

13. To use account codes, select the **Account Code Verification** option. After you apply account code verification to a dial plan object, you can track that call type with a verified account code that the user provides for the outbound call. You can use this feature to track call types for billing purposes.

> **Note:** Do **not** apply Account Code Verification to the **911** and **Intercom** Dial Plan Objects.

14. In the **Components** box, specify the different parts of a phone number in each dial plan entry that need to be tracked in the report logs (such as area code, long distance prefix, country code, and so on). These components are used for tracking different parts of the phone number in the reporting databases.

> **Note:** If you create new dial plan objects for the Local and Long Distance categories, you must copy the content of the default Components field (such as the ReportingCode1 and ReportingCode2 components) and paste them in to your components field. Failure to do this may result in incomplete call data in your reports.

The default dial plan objects in the Local and Long Distance classifications created during installation contain two components: ReportingCode1 and ReportingCode2. These components represent the digits in the ordinal positions indicated by the ordinal number syntax in the field. For example, the syntax for the first entry is:

ReportingCode1:{3}{4}{5};

The part before the colon is the name or label for this component ("ReportingCode1"). The ordinal numbers after the component refer to the 3rd, 4th, and 5th digits in the current dial plan object. In the case of a Local or Long Distance classified number in the NANP, these digits always refer to the area code. The semicolon at the end is simply a separator between components.

In another example, the syntax for the second component in the Components field is:

ReportingCode2:{6}{7}{8}

Again, the part before the colon is the component name ("ReportingCode2"). The ordinal numbers after the component refer to the 6th, 7th, and 8th digits in the current dial plan object. In the case of a Local or Long Distance classified number in the NANP, these digits always refer to the local exchange.

If these same digits refer to a different part of the phone number in another location (such as city code, prefecture code, etc.), you can keep these components as they are and they will work for your location. If you need to track other parts of the phone number, you must:

- Create new components in the **Components** box.
- Customize the CallDisconnectMonitor handler to add the new components to one of the extra columns in the Call Detail report log.
- Modify or add a new column in a Crystal Report template that is based on the Call Detail report log.

15. In the **Description** box, document the purpose, along with any details, of each dial plan entry. This information will be valuable to other CIC administrators, especially if you have more than one administrator managing CIC or more than one person editing the dial plan configuration.
16. To use account codes, select the **Account Code Verification** option. When you select this option, you can track that call type by using a verified account code that the user provides for the outbound call. For example, you would use this feature to track call types for billing purposes.

> **Note:** You should **not** apply Account Code Verification to the **911** and **Intercom** Dial Plan Objects.

17. Configure dial groups for the object. Dial groups enable you to specify which outbound lines or channels to use for each type (classification) of phone number. For example, international calls may be directed to one dial group that uses lines with the best rate for international calls. Local calls may be directed to another dial group called "Local" over low-cost analog lines from the local CO. If you do not specify a dial group for a dial plan entry, calls placed via that dial plan object use the first available line with a direction of Outbound or Both.

> **Note:** All of the lines or channels in a dial group must have identical dialing requirements. For example, in a dial group, you cannot have some lines that require a 9 prefix and other lines that do not.

Do the following, as necessary:

- To add a dial group, click **Add Group**. Select the dial group and then click **OK**. If there are no dial groups, create them in the **Line Groups** container.
- To edit a dial group, select it and then click **Edit**.

- To remove a dial group, select it and then click **Remove.**
- To add a secondary dial group to an existing dial group entry, select the dial group and then click **Add Group.**

Related topics

Configure a regional dial plan in Interaction Administrator

Manage named lists of phone numbers

Manage phone number classifications

Import a dial plan

You can import an entire CIC phone number plan that was saved (with the **Export** button) by any CIC server. Exported CIC phone number files have a `.i3dplan` extension and include all of the input conversion objects, dial plan objects, and classification names.

To import a dial plan

1. In the **System Configuration** container, click the **Phone Numbers** subcontainer.
2. In the list view, double-click **Configuration**.
3. In the **Phone Number Configuration** dialog box, on the **Regional Dial Plan** tab, click **Dial Plan**.
4. Click **Import**.
5. Click **Browse** button to select a `.i3dplan` file, and then click **Next.**
6. Click **Next** to navigate through the dialog boxes that display the contents of the dial plan file.
7. When you are presented with import options (replace or skip the merge), select the appropriate check boxes and then click **Next**.
8. Review the changes and then click **Finish**.
9. When the message appears that indicates that you have not yet saved your changes, click **OK**. You save your changes when you click **OK** on the **Regional Dial Plan** dialog box.

Related topics

Configure a regional dial plan in Interaction Administrator

Export a dial plan

Export a dial plan

To export a dial plan

1. In the **System Configuration** container, click the **Phone Numbers** subcontainer.
2. In the list view, double-click **Configuration**.
3. In the **Phone Number Configuration** dialog box, on the **Regional Dial Plan** tab, click **Dial Plan**.
4. Click **Export**.
5. Navigate to your preferred file location and specify a name. Then click **Save**.

Related topics

Configure a regional dial plan in Interaction Administrator

Configure a dial group entry

When you configure a regional dial plan in Interaction Administrator, you can configure a dial group entry.

To configure a dial group entry

1. In the **Regional Dial Plan - Edit Pattern** dialog box, do one of the following:

    - To add a dial group, click **Add Group**. Continue with step 2.
    - To edit a dial group, select it and then click **Edit**. Continue with step 2.
    - To remove a dial group, select it and then click **Remove**.
    - To change the order of dial groups, click the **Up** and **Down** buttons.

2. In the **Location Filter** list, select the location filter for this dial group. The location filter determines which dial group entries are applicable based on the location for a station. This filter is used in conjunction with pattern selection based on the classification.

> **Notes**: If a dial plan entry does not have <All> access then those specific options (patterns or dial groups) are removed from the dial plan and are not presented as dialing choices on dialing lookup in the describe number tool.
>
> Any input pattern that has the <All> filter may require special care when defining the dial groups for the dial plan entry. For example a 911 pattern, the default line groups specified should be local to the location region as possible.

3. In the **Classification** list, select a value to differentiate between different identically dialed numbers based on the dial group and classifications that are used.
4. In the **Dial String** field, if necessary, change the dial string if the dialing requirements for one dial group are different from the another dial group. For example, if the number dialed failed to go out on the first dial group, it may be dialed on the second dial group, which might require a prefix or other dialing requirement.

> **Note:** All of the lines or channels in a dial group must have identical dialing requirements. In other words, you cannot have some lines that require a 9 prefix and other lines that don't within the same dial group.

5. Click **OK**.

Related topics

Overview of dial group entries

Configure a regional dial plan in Interaction Administrator

Line selection order

Locations

Manage named lists of phone numbers

You can manage multiple lists of phone numbers for a dial plan. For example, you can create lists of local exchanges for an area code or toll free numbers.

To manage named lists of numbers

1. In the **System Configuration** container, click the **Phone Numbers** subcontainer.
2. In the list view, double-click **Configuration**.
3. In the **Phone Number Configuration** dialog box, on the **Regional Dial Plan** tab, click **Manage Lists**.
4. To view details of a number list, click it in the **Number Lists** list.
5. To add a new phone number list, under the **Number Lists** list click **Add**.
6. To remove a phone number list, first select it. Under the **Number Lists** list, click **Remove**.
7. To rename a phone number list, first select it. Under the **Number Lists** list, click **Rename**.
8. To add phone numbers to a list, first select the list. Then click **Add i**n the right side of the dialog box. Separate numbers with spaces or commas.
9. To import a text file or CSV file of phone numbers for a list, first select the list. Then click **Import** in the right side of the dialog box.
10. To remove a phone number from a list, first select the list. Then select the number in the right side of the dialog box and click **Remove**.

Related topics

Manage phone number classifications

Simulate a call

Perform advanced operations

Overview of phone number classifications

Phone numbers that can be identified by a pattern in the numbers, or an explicit group of phone numbers with a common purpose are called phone number classifications. For example, internal calls could be identified by the "Internal" classification, toll free (for example, 800 numbers) could be identified by the "Toll Free" classification, and calls to emergency services (such as 911, fire department, police, and hospital) could be identified by the "Emergency" classification.

These named groups of phone numbers are used to control individual users, workgroups, and station dialing privileges in CIC. For example, stand-alone phones may have only Emergency and Internal dialing privileges, while members of the Sales workgroup may have full dialing privileges provided in all classifications.

When CIC users dial a phone number, CIC matches the number dialed with the appropriate classification pattern. It then checks the user's dialing privileges to determine if the user or station is authorized to place the call. In this way, CIC uses phone number classifications to control individual users, workgroups, roles, and station dialing privileges.

You also use classifications to configure forced authorization codes. Administrators set forced authorization codes to require users to enter an extension and a password to make a call.

You create a list of classifications on the **Classifications** dialog box in the **Phone Number Configuration** dialog box. To create the number pattern for the classification, use the **Dial Plan** dialog box.

> For more information about phone numbers see the *CIC Regionalization and Dial Plan Technical Reference* in the PureConnect Documentation Library.

Related topics

Configure an old dial plan

Manage phone number classifications

Manage phone number classifications

To manage phone number classifications

1. In the **System Configuration** container, click the **Phone Numbers** subcontainer.
2. In the list view, double-click **Configuration**.
3. In the **Phone Number Configuration** dialog box, on the **Old Dial Plan** tab or on the **Regional Dial Plan** tab, click **Manage Classifications**.
4. In the **Dial Plan Classifications** dialog box, do one of the following:

   - To add a classification, click **Add**. Type the name of the classification (for example, "900 Service" or "International"), and then click **OK**. Then continue with the next step.
   - To edit a classification, select it and then click **Edit**. Then continue with the next step.
   - To delete a classification, select it and then click **Remove**.

5. In the **Classification** dialog box, the name of the classification appears in the **Display Text** field. You can change this if necessary.
6. In the **Category** list, select the appropriate category.
7. In the **Alerting** section, select the **Send email and client alerts for calls of this classification** check box, and enter the users to receive the alerts in the **To...** field. You can also click the **To...** button and select the available users from the list that is displayed. Alerting sends an email notification and displays a popup notification in the CIC clients, to the specified users and/or workgroups when a call is made with this classification.
8. As necessary, complete the **Multi-Language Support** tab. For more information, see *Multi-Language Support*.
9. Click **OK**.

Related topics

Configure an old dial plan

Overview of phone number classifications

Set up an emergency classification

Set up an emergency classification

Calls to emergency services (such as 911, fire department, police, and hospital) should be identified by the "Emergency" classification.

To set up an Emergency classification

1. In the **System Configuration** container, click the **Phone Numbers** subcontainer.
2. In the list view, double-click **Configuration**.
3. In the **Phone Number Configuration** dialog box, on the **Old Dial Plan** tab or on the **Regional Dial Plan** tab, click **Manage Classifications**.
4. In the **Dial Plan** Classifications dialog box, click **Add**.
5. In the Entry Name dialog box, type the name of the classification (for example, "911 Emergency Service").
6. Click **OK**.
7. In the Classification dialog box, the name of the classification appears in the **Display Text** field. You can change this if necessary.
8. In the **Category** list, select **Emergency**.

9. In the **Alerting** section, select the users or workgroups to alert when a call is made with this classification. For more information, see *Overview of classification alerts*.
10. Complete the **Multi-Language Support** tab. For more information, see *Multi-Language Support*.
11. Click **OK**.

Related topics

Station emergency information settings

Multi-Language Support

Simulate a call

You can test your dial plan configuration by entering real phone numbers in any format you can imagine. Since users may enter phone numbers in a variety of ways (with or without a leading 1, with or without a local area code, etc.), you can test different kinds of input without actually placing a live call to different numbers. This page just simulates calls as if they were dialed from a CIC station; it does not actually place calls to the dialed numbers.

To simulate a call

1. In the **System Configuration** container, click the **Phone Numbers** subcontainer.
2. In the list view, double-click **Configuration**.
3. In the **Phone Number Configuration** dialog box, click **Simulate Call**. This button appears in the following places:
    - On the **Regional Dial Plan** tab
    - On the **Regional Dial Plan** dialog box
4. In the **Number** field, enter a phone number. You can type letters or digits, and you can use the keypad.
5. In the **Location Filter** list, select a filter to apply to the simulated call.
6. Click **Simulate Call**.
   CIC passes your number input through the input conversion objects and dial plan objects you created on their respective property pages. The program displays the resulting output in the **Call Results** fields on the right side of this page.

   The most important results you might look at first are in the three-column list box at the bottom of the **Call Results** section. This list box shows which dial group (if any) the call would go out on, the phone number classification for which users would need access rights to dial, and the actual dial string, which is the number CIC sends to the CO when dialing.

   If you applied the account code verification feature to a dial plan entry, **Account Code Verification** is listed as **Yes**. You can track that call type by using a verified account code that the user provides for the outbound call. Use this feature to track call types for billing purposes. You should **not** apply account code verification to the **911** and **Intercom** Dial Plan Objects.

If you enter a number that does not match any of the standard input conversion objects or dial plan objects, **Unknown** will appear as the classification in the list box, the description in the call results section will indicate **No pattern match**, and other call results fields display the raw number you entered. This indicates that CIC cannot match the input with an input pattern in the dial plan.

Related topics

Configure a dial plan in Interaction Administrator

Manage named lists of phone numbers

Manage classifications of phone numbers

Select which dial plan to view

If you have both an old dial plan and a regional dial plan, you can select which one to view in the **Phone Numbers** container.

> **Note:** If you choose to view both dial plans, the **Phone Number Configuration** dialog box displays a separate tab for each one.
>
> Only one of the plans can be active at a time.

To select which dial plan to view

1. In the **System Configuration** container, click the **Phone Numbers** subcontainer.
2. In the list view, double-click **Configuration**.
3. In the **Phone Number Configuration** dialog box, on the **Old Dial Plan** tab or the **Regional Dial Plan** tab, click **Advanced**.
4. Under **Dial Plan View**, select the dial plan that you want to view.
5. Click **OK**.
6. Close the **Phone Number Configuration** dialog box.
7. Reopen the **Phone Number Configuration** dialog box.

Related topics

Activate a dial plan

Overview of old dial plans

Configure a regional dial plan in Interaction Administrator

Activate a dial plan

> **Note:** Only one dial plan format (Old Dial Plan or Regional Dial Plan) can be active. CIC uses the active dial plan to perform dial plan lookups and make calls.
> If necessary, you can modify an inactive dial plan and test it by simulating calls.

To activate a dial plan

1. In the **System Configuration** container, click the **Phone Numbers** subcontainer.
2. In the list view, double-click **Configuration**.
3. In the **Phone Number Configuration** dialog box, on the **Old Dial Plan** tab or the **Regional Dial Plan** tab, click **Advanced**.
4. Under **Active Dial Plan**, select the dial plan that you want to activate.
5. Click **OK**.

Related topics

Overview of old dial plans

Configure a regional dial plan in Interaction Administrator

DID/DNIS

Overview of DID/DNIS

If your phone lines provide the called number as part of the incoming call packet (for example, DID (Direct Inward Dialing) or DNIS (Dialed Number Identification Service)), you can map the called number directly to a CIC user, workgroup, or station queue. When a new call to one of the mapped numbers arrives, CIC immediately routes that call to the mapped destination.

To do this, you simply create the appropriate call routing map using the DID/DNIS Configuration page and the DID/DNIS Route page (which appears when you click Add on the DID/DNIS page). For more information on how to use this feature to route calls, see *Automatic Call Routing Overview*.

Related topics

Overview of automatic call routing

Configure DID/DNIS

Configure DID/DNIS

To configure DID/DNIS

1. In the **System Configuration** container, click the **Phone Numbers** subcontainer.

2. In the list view, double-click **Configuration**.
3. In the **Phone Number Configuration** dialog box, click the **DID/DNIS** tab.
   For information on the information you see in the table, see *Columns in the DID/DNIS table*.
4. To add a DNIS call route to the table, click **Add**. In the **DID/DNIS Identifier** box, enter the DID/DNIS extension. You can use either simple mapping, substitute a prefix, or replace digits. Select a user name, workgroup name, or station name destination to route calls that dialed the number. Click **OK**. For more information, see *Add a new DID/DNIS routing entry*.
5. To edit a DID/DNIS call route entry, select the entry to edit and then click **Edit**. Make the necessary changes and then click **OK**.
6. To edit the digits in a DID/DNIS number, select the entry and then click **Edit Digits**. Make the necessary changes and then press the Enter key.
7. To remove a DID/DNIS call route entry, select the entry and then click **Remove**.

Related topics

Overview of automatic call routing

Columns in the DID/DNIS table

Add a new DID/DNIS routing entry

Routing entry configuration

Each dialed number can be routed to a CIC user, station, station group (including fax group), or workgroup extension. Depending on the quantity and format of DNIS numbers you receive, you can use one of these three methods to set up a map table for routing calls: Simple Mapping, Substitute Prefix, and Replace N Digits. For more information about these methods, see *Overview of automatic call routing*.

Simple Mapping

Select this method if you have only a few call routes to create, or the DNIS numbers have different prefixes. This method allows you to add one call route to the map table at a time. To do this:

1. Select the **Simple Mapping** option.
2. Type the complete DNIS number and then single-click on a Destination field in the list at the right, or

   Type the prefix of the DNIS number in the adjacent field, select a Destination queue in the list at the right, and click **Grab Extension** to add the destination extension to the field.
3. Type a brief description of the purpose of this call route. This serves as useful documentation for the CIC administrators looking at the DID/DNIS configuration.
4. Verify the route in the explanation field at the bottom and click **OK** if the map is correct.

> **Notes:** The next two methods allow you to select multiple entries from the **Destination** list:

> To select a contiguous range of entries from the list, click on the first entry in the list, scroll down (or up) to view the last entry in the list, hold the Shift key down and then click on the last entry in the list.
>
> To select entries from the list randomly, click on an entry, hold the Ctrl key down, and then click on one or more other entries in the list. To sort the list before selecting entries, click on one of the column names to sort the list by that name.

Substitute Prefix

Select this method if you have a range of DNIS numbers, all with the same prefix and a group of extensions with the same number of digits. This method allows you to build a map table for a large range of extensions with the same DNIS prefix at one time. The DNIS prefix can be three or four digits, depending on the DNIS numbers you have reserved, and whether the extensions are all three-digit numbers or all four-digit numbers.

1. Select the **Substitute Prefix** option.
2. Type the three or four digit DNIS prefix in the adjacent field.
3. Select a range of destination queues in the **Destinations** list to the right. If it would help to select the names in a particular order, click on one of the column headings in the list to sort the list by that column. For example, in the **Destination** list, click the **Extension** column heading to sort the list by extensions.
4. Type a brief description of the purpose of this call route. This serves as useful documentation for the CIC administrators looking at the DID/DNIS configuration.
5. Verify the routes in the explanation field at the bottom and click **OK** if the map is correct.

Replace N Digits

Select this method if you have a range of DNIS numbers with the same prefix, but the DNIS numbers map to extensions with one, two, three, or four digits. You provide a phone number template and this method builds a map table by substituting the number of digits in each extension (N) for that same number of digits at the end of the template phone number. The template DNIS number is usually a seven-digit phone number using the first three digits of the prefix in the DNIS numbers.

1. Select the **Replace N Digits** option.
2. Type a DNIS phone number template in the adjacent field. This is a 7-digit number in the North American Numbering Plan, but it could be more or less than seven digits in other locations.
3. Select a range of destination queues in the **Destinations** list to the right. If it would help to select the names in a particular order, click on one of the column headings in the list to sort the list by that column. For example, in the **Destination** list, click the **Extension** column heading to sort the list by extensions.
4. Type a brief description of the purpose of this call route. This serves as useful documentation for the CIC administrators looking at the DID/DNIS configuration.
5. Verify the routes in the explanation field at the bottom and click **OK** if the map is correct.

Description

This field contains a brief description of the purpose of the DID/DNIS entry. The text entered in this box appears on the DID/DNIS configuration page under the **Description** column. It can provide useful documentation for the CIC administrator who has to manage the call routing later.

> **Note:** There is a tool to process the DID/DNIS routing table from Interaction Administrator. The tool takes the DNIS string of a telephone call and returns a scoped queue name based on the DID/DNIS configuration in Interaction Administrator. For more information, see the Interaction Designer help.

Related topics

Configure DID/DNIS

Overview of automatic call routing

Private Lines

Overview of private lines

Private lines allows you to assign trunk lines or trunk line groups to a specific user's extension or a phone number classification. This ensures that a trunk line will always be available to place a call. You can use this feature to handle 911 emergency calls, or ensure that a specific user always has an available line.

Related topics

Configure private lines

Create a private line assignment

Overview of line groups

Configure private lines

This procedure describes how to configure private lines in the **Private Line Assignment Table**. After you complete this procedure, you can assign the private lines to users.

To configure private lines

1. In the **System Configuration** container, click the **Phone Numbers** subcontainer.
2. In the list view, double-click **Configuration**.
3. In the **Phone Number Configuration** dialog box, click the **Private Lines** tab.
4. To add a private line, click **Add**. For more information on how to complete the fields, see *Add a private line*.
5. To Edit a private line, click **Edit**.

> **Note:** You cannot edit the **Assigned To** field. If you need to assign a private line to another user or classification, first delete the existing entry from the **Private Line Assignment Table**. Then add another entry with the new assigned user or classification.

6. To delete a private line, select the entry and then click **Delete**.
7. Click **OK**.

Related topics

Add a private line

Overview of private lines

Create a private line assignment

Add a private line

To add a private line to the Private Line Assignment Table

1. In the **Private Line Dial Group** list, select a dial group from the list.

> **Note:** For a line group to be available for a private line assignment, the **Use as Dial Group** and **Use for Private Line Assignment** boxes must be selected on the **Line Group Configuration** page.

2. Under **Assigned to**, do one of the following:
    - To assign the private line group to a user, select the **User** option. Then select user from the list.
    - To assign the private line group to phone classification, select the **Classification** option. Then select the classification from the list.
3. Click **OK**.

Related topics

Configure private lines

Create a private line assignment

To create a private line assignment

1. In the **Line Groups** container, add a line group to be used for a private line. On the **Configuration** tab, select the **Use as Dial Group** and **Use for Private Line Assignment** options.
2. In the **Phone Number Configuration** dialog box, on the **Private Lines** tab, use the **Private Line Assignment** field to associate a private line with a user or classification.
3. In the **Phone Number Configuration** dialog box, on the **Regional Dial Plan** tab, associate a dial plan object name with a dial group.

Related topics

Overview of private line assignment

Overview of line groups

Configure private lines

Remove a private line assignment

To remove a private line assignment

> **Note**: If a Private Line Assignment line group is in the **Private Line Association** field, you cannot delete it. Also, if a dial group or a Private Line Assignment line group is used in a dial plan, you cannot delete the line group.

1. In the **Phone Number Configuration** dialog box, on the **Regional Dial Plan** tab, delete the dial group that is associated with the dial plan.
2. In the **Phone Number Configuration** dialog box, on the **Private Lines** tab, delete the private line dial group from the **Private Line Assignment** field.
3. In the **Line Groups** container, delete the line group.

> **Note:** If a line belongs to a PLA line group, you cannot be delete it from the **Lines** container. If a PLA line group is in the Private Line Association field, you cannot delete it. If a dial group or PLA line group is used in a dial plan, you cannot delete the line group.

Related topics

Overview of private line assignment

Overview of line groups

Report Logs

Overview of report logs

For each event that passes through the CIC system (for example, each call, line event, or status change) the IC StatServer subsystem captures data for that event and passes it to the Interaction Processor subsystem or it triggers an initiator and passes the data to a handler. In both cases, Interaction Processor or the handler formats the statistics to match the appropriate report log table and the uses SQL transactions to commit the report log data to an SQL Server database.

Interaction Processor formats and outputs report log data that cannot be customized or that have no custom attributes (for example, Line Configuration Mirror, Line Group Configuration, etc.) Handlers format and output the report log data that contains call information, which could include user-defined call attributes. You can include these custom call attributes in the report logs by modifying the Custom fields in the appropriate tool step (for example Statistics Group Interval) in the appropriate handler.

Handler-generated report logs are built in Interaction Designer using a report log tool specifically created for each report log. For example, the CallDisconnectMonitor handler is responsible for writing data to the CDR Log and it uses a tool called Call Detail Record to gather the data for that log.

> **Note:** To understand the entire report log data gathering process and how that data turns into reports, see the *CIC Reporting Technical Reference* in the PureConnect Documentation Library.
>
> Beginning in 2016 R1, CIC provides the Interaction Administrator Change Notification Log. This log provides robust logging for changes made in the Users, Workgroups, and Licenses Allocation containers. The Interaction Administrator Change Notification Log also tracks changes to user and station licenses. For more information about the enhanced logging capabilities, see About the *Enhanced Interaction Administrator Change Notification Log*.

Related topics

Report log descriptions

Configure basic report log information

Configure report log retention

Configure report mappings

Configure custom attributes

View and update history

About the Enhanced Interaction Administrator Change Notification Log

Report log descriptions

CIC provides basic report logs that store all line, call, and user-related CIC interaction data. In Interaction Administrator, all report logs are identified with numbers (for example, 1, 2, 3, … 50, 51, and so on).

> For more information about the basic report logs, see the *PureConnect Data Dictionary Technical Reference* in the PureConnect Documentation Library. For more information on how to run and export reports, and how to use the reporting tools, see the *PureConnect Reporting Technical Reference* in the *PureConnect* Documentation Library.

Descriptions

> **Note:** A more detailed description of each report log appears on the Basic page of the Report Log Configuration dialog box. To see it, double-click the name of the report log in the Report Logs subcontainer.

Log number	Description
7	Interaction Administrator Change Notification Log
8	IC Change Notification Log

9	IC Application Login Logout Change Log
20	Interaction Custom Attributes Log
30	Interaction Summary and Detail Log
40	Interaction Wrap-up Log
50	ETL Data Log
70	User To Workgroup Relationships
71	Line Configuration Mirror
72	Line Group Configuration
73	Line Group to Lines Relationship Mirror
74	Account Code Mirror
80	Agent Activity Log
81	Interval Line Group Statistics
82	Interval Line Statistics
83	Fax Envelope History
84	IVR History
85	IVR Interval
86	Agent Queue Activation History
93	Pre 4.0 Wrap-up Statistics
110	Agent Queue Statistics Interval
111	Statistics Group Interval
112	Workgroup Queue Statistics Interval

9999	Custom Passthrough

Related topics

Overview of report logs

Configure basic information

Configure retention time

Configure report mappings

Configure custom attributes

View and update history

Configure basic report log information

To configure basic report log information

1. In the **Report Logs** subcontainer, double-click the report log you want to configure. Use the **Basic** page to view and update the following fields.
2. The **Log Name** box displays the name of this report log.
3. The **Display Name** box displays the name of the report log appears here as it appears in the Reports tool in Interaction Designer.
4. The **Description** box displays a brief description of the purpose of this report log appears here.
5. The **Data Destination** box contains the server parameter **ServerReportLogDataDestination** by default. This parameter contains the default label for the queue used to deliver data to CIC report logs in the report log database. You can specify a different queue label by typing it in this field. If you do, you must first create this queue and then specify the new queue in the EicLoggingService command line argument on the report log database server.
6. The **Client DB Source** field contains the system parameter ClientReportLogEICDataSourceName. This parameter contains the CIC data source name (DSN) that represents the ODBC data source called IC Report Logs. Reports use IC Report Logs to access the report logs. You may specify a different DSN by typing it in this field. If you do, you must define the new DSN in the ODBC configuration and use Crystal Reports to modify the default DSN expected in CIC reports.
7. The **Active** check box controls whether the data is written to the reporting database. By default, it is selected, which means that CIC sends data to the report log automatically (**auto logging**). Regardless of whether this check box is selected or not, the StatServer generates the raw statistics. If you clear the check box the statistics are still generated, but they are not logged to the database. CIC recognizes changes to this check box immediately.

> **Note:** By default, the IC Application Login Change Log is inactive. You must set this report log to active in order for it to work.

8. **Auto logging** refers to the ability of StatServer to receive its own statistics sent out in a notification and then log the statistics to the database. Turn off auto logging if you want handlers to catch this information and log it to the database. **This parameter is for advanced administrator use only.**

Related topics

Overview of report logs

Report log descriptions

Configure retention time

Configure report mappings

Configure custom attributes

View and update history

Configure report log retention time

The retention time determines how long the data in the report log is saved. Records older than the expiration age can be purged automatically or manually.

To configure report log retention time

1. In the **Report Logs** subcontainer, double-click the report you want to configure.
2. Click the **Retention** page.
3. In the **Purge records older than [x] days** box, type the expiration age for records for this report log.
4. To configure automatic purging, select the **Enable automatic purging for this report log** check box. You must also configure the purging schedule on the **Report Log Purging** page of the **Server Configuration** dialog box, which is located in the Server Configuration container. For more information on how to configure the purge schedule, see *Configure report log purging for your CIC server*.
5. To immediately purge the expired records from this report log, click **Purge Now**. In the message box, click **Yes**.

> **Note:** You cannot undo a purge.

6. Click **OK**.

Related topics

Overview of report logs

Report log descriptions

Configure basic information

Configure report mappings

Configure custom attributes

View and update history

Configure report log purging for your CIC server

Configure report log mappings

Report log mappings specify what data is logged in which column in the database.

> **Notes:** If you are using this advanced feature, please see the *PureConnect Reporting Technical Reference* in the PureConnect Documentation Library located on the CIC server.
>
> You may also search the knowledge base for articles regarding custom report mappings.

To configure report log mappings

1. In the **Report Logs** subcontainer, double-click the report you want to configure.
2. Click the **Mappings** page. Do one of the following:

- To use the default mappings and ignore any custom output mappings that you have defined, select the **Use default mappings** check box. By default, this check box is selected.
- To have CIC dynamically process a custom mapping, deselect the **Use default mappings** check box. Then, in the **Map string** box, type the value that CIC should use to bind the columns.

3. Click **OK**.

Related topics

Overview of report logs

Report log descriptions

Configure basic information

Configure retention time

Configure custom attributes

View and update history

Custom attributes

The Custom Attributes page allows you to add customized attributes so that you can reference your own variables and settings through the IceLib interface.

> **Note:** If you enabled the Enhanced Interaction Administrator Change log, then all of your changes to the Custom attributes page in the User Configuration dialog box and the Workgroup Configuration dialog box dialog box are tracked in that log. For more information, see *About the Enhanced Interaction Administrator Change Log*.

The page contains a list for the attributes and displays a **Name** and a **Value** column, and has the following buttons:

Add

Click **Add** and select an existing custom attribute from the pull-down list, enter a new custom attribute. If creating a new attribute, use a unique name, otherwise the existing attribute will be overwritten.

Edit

Click **Edit** to change the value of an existing custom attribute.

Delete

Click **Delete** to delete an existing custom attribute.

Manage Attributes

Click **Manage Attributes** to open a dialog box that displays a list of custom attributes. Click **Add** or **Delete** to manage the appearance of the custom attributes in the pull-down list.

The custom attributes are saved in the path of the root container. This **Path** is displayed at the bottom of the dialog box.

> **Note**: For more information on the Interaction Center Extension Library (IceLib), see The **System APIs section** in the PureConnect Documentation Library on the CIC server.

History

This page provides a way to manually document configuration changes and when they occurred. Changes made in Interaction Administrator are also automatically logged in the Interaction Administrator Change Notification Log (Log ID 7). Later, authorized users can run reports against this log to summarize all configuration changes.

> **Note:** If you enabled the Enhanced Interaction Administrator Change log, then all of your changes to the History page in the User Configuration dialog box and the Workgroup Configuration dialog box dialog box are tracked in that log. For more information, see *About the Enhanced Interaction Administrator Change Log*.

Last Modified

This date is automatically updated each time you click the **OK** button, presumably after you make changes to the configuration. To avoid updating this date, exit the page by clicking the **Cancel** button.

> **Note:** If you click **Cancel**, none of the changes made to this page will be preserved.

In addition, the history is updated when changes are made to the record elsewhere in Interaction Administrator. For example, when a user change his or her password, the **Last Modified** date is updated.

> **Note:** Changes to the licenses for a user or a station do not update the Last Modified date.

Date Created

This date is automatically set when the user creates the initial configuration for this page. If the page was initially created during setup, the date could be blank.

Notes

Type notes about configuration settings and changes. If you change the configuration page and click **OK**, the **Last Modified** date is updated.

You must manually enter the date beside each entry in the **Notes** field to identify the date of each note.

To create a new line in the **Notes** field, press Enter.

Enhanced Interaction Administrator Change Log

About the Enhanced Interaction Administrator Change Log

The **Enhanced Interaction Administrator Change Notification Log (6)** provides robust logging for changes to users, workgroups, skills, licenses, stations, roles and default user.

> **Warning: Enable the Enhanced Interaction Administrator Change Log only during non-peak production hours and only if all CIC clients are upgraded to CIC 2016 R1 or later.**
>
> Enabling this log is an intensive operation that requires significant computing resources. You must do it during non-peak production hours.
>
> If you enable this feature before you upgrade all CIC clients to CIC 2016 R1 or later, the CIC clients that run earlier versions of CIC will log incomplete audit data.

> **Note:** The enhanced logging feature is available beginning with CIC 2016 R1. It is available for Microsoft SQL Server and Oracle.

This help topic contains the following sections:

How to start enhanced logging

About the Snapshot Tool

Summary of logged data

Summary of data that is not logged

How to access the change log data

How to purge change log data

How to start enhanced logging

By default, the Enhanced Interaction Administrator log is not actively logging changes. If you want to use this log, you must enable it. For information, see *Enable the Enhanced Interaction Administrator Change Log*.

> **Note:** If you choose to not enable the Enhanced Interaction Administrator Change Log, Interaction Administrator will continue to provide its regular logging capabilities via the Interaction Administrator Change Notification Log report log, it is enabled.

About the Snapshot Tool

When you enable the Enhanced Change Notification Log, the Snapshot tool automatically runs. The Snapshot tool takes a snapshot of the current Directory Service data and updates the Enhanced Change Log database tables. This data acts as a baseline for future views of the log and it ensures that the views remain accurate.

> **Notes:** Enable the Enhanced Interaction Administrator Change Log during off-peak hours. During the snapshot process, you may experience a large amount of processing on your CIC server and database server. While this process lasts only a short time, it is best if you enable the log this during off-peak hours.
>
> The provided database views display only data from the time when the last snapshot was taken. The audit trail data remains in the database tables.
>
> For troubleshooting purposes, you may want to re-run the Snapshot tool. For more information, see *Logging administrative changes from other applications*.

Summary of logged data

Interaction Administrator data

The Enhanced Interaction Change Notification Log tracks changes to the following information in Interaction Administrator:

- **Users** container: All changes made to all pages
- **Default User** container: All changes made to all pages
- **Roles** container: All changes made to all pages
- **Workgroups** container: All changes made to all pages

> **Note:** Supervisors can change workgroup membership from IC Business Manager. Those changes are also tracked in the Enhanced Interaction Administrator Change Log.

- **Skills:** All changes made to all pages
- **Licenses Allocation** container: All changes made to station licenses and user licenses
- **Stations** container: All changes to station licenses

IceLib and ICWS data

If you enable the enhanced logging feature, all administrator configuration changes from ICWS and IceLib are logged. However, the enhanced logging feature consistently formats only the administrative changes that are logged from Interaction Administrator.

> **Note:** If you have custom applications that use the IceLib or ICWS API's that configure the CIC server, then you might see the additional logging data in those applications.

For more information about the data that is and is not affected by the Enhanced Interaction Administrator Change Notification Log, see *Troubleshooting the Enhanced Interaction Administrator Change Notification Log*.

Summary of data that is not logged

The following data is not logged by the enhanced logging feature:

- License activations from external files
- Changes to any Interaction Administrator containers other than Users, Skills, Workgroups, Licenses, Roles and Default User.

How to access the change log data

CIC provides several views that you can use to access the change log data. You access these views directly via a database query. For more information on these views, see *Database views for the log*.

How to purge the change log data

You can configure automated data purging for the Enhanced Interaction Administrator Change Notification Log in the same way as all other logs. You can also do an immediate data purge, if necessary. For more information, see *Configure report log retention time*.

Related topics

Enable the Enhanced Interaction Administrator Change Log

Database tables for the Enhanced Interaction Administrator Change Log

Examples of changes to database tables

Database views for the Enhanced Interaction Administrator Change Log

Troubleshoot the Enhanced Interaction Administrator Change Log

Enable the Enhanced Interaction Administrator Change Log

In order to take advantage of the Enhanced Interaction Administrator Change Log, you must enable it.

> **Notes:**
>
> By default, the Enhanced Interaction Administrator Change Log is **not** enabled. If you enable this feature and then upgrade CIC, the feature will remain enabled.
>
> When you enable the Enhanced Interaction Administrator Change Log, the Snapshot Tool creates a baseline of your data. This process takes time and can affect system performance. Therefore, it is best to enable the Enhanced Interaction Administrator Change Log during off-peak hours. For more information, see *About_the_Snapshot_Tool*.

To enable the Enhanced Interaction Administrator Change Log

1. In the **Report Logs** subcontainer, double-click the Enhanced Interaction Administrator Change Notification Log (6).
2. On the **Basic** page, select the **Active** check box.
3. Click **OK**.

Related topics

About the Enhanced Interaction Administrator Change Log

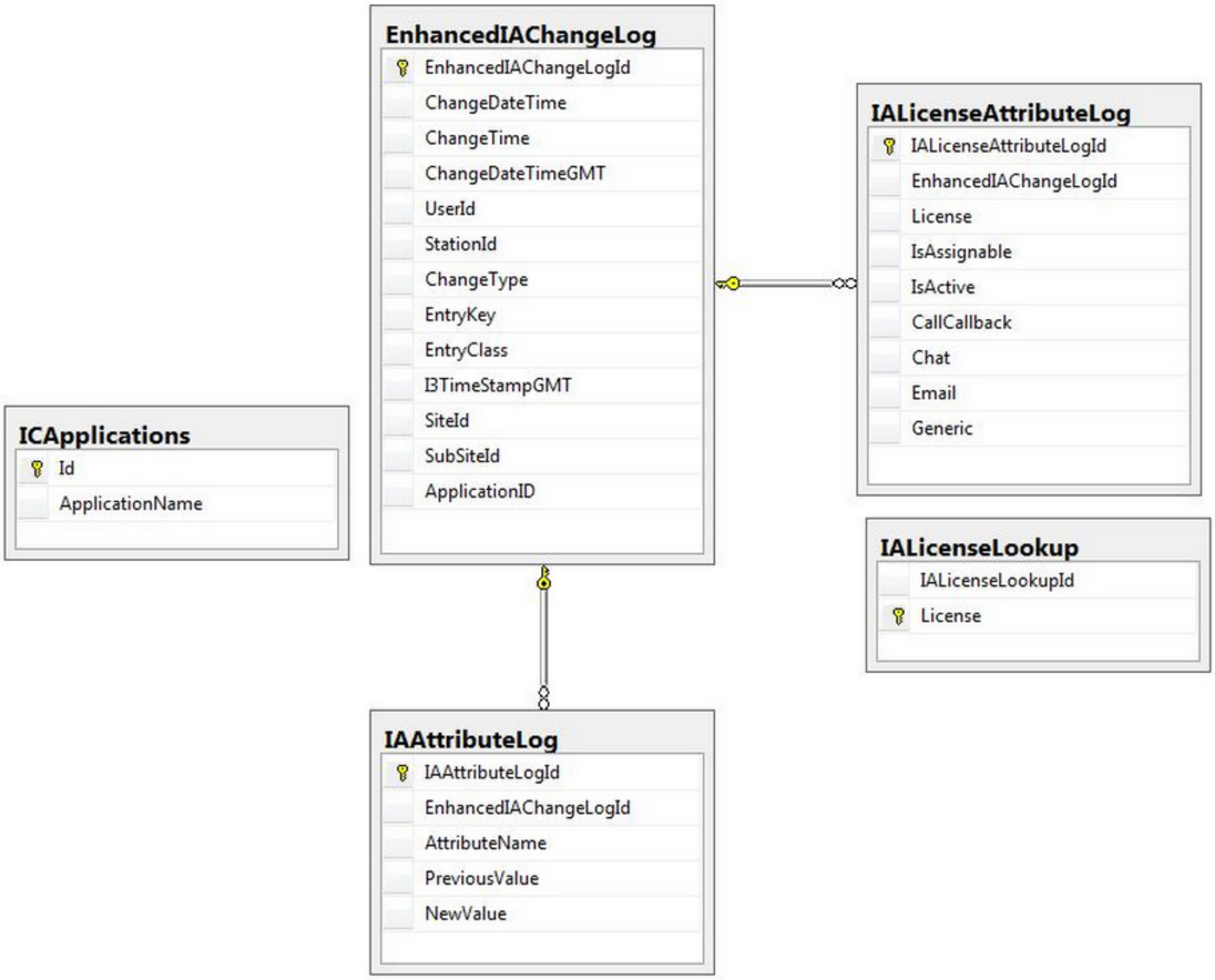
Database tables for the Enhanced Interaction Administrator Change Log

Troubleshooting the Enhanced Interaction Administrator Change Log

Database tables for the Enhanced Interaction Administrator Change Log

For complete information about the database tables that are used with the Enhanced Interaction Administrator Change Log, see the *PureConnect Data Dictionary* in the PureConnect Documentation Library.

Click a database table for more details about its purpose and its columns.



EnhancedIAChangeLog Table

The **EnhancedIAChangeLog** table is the primary table that is used for the Enhanced Interaction Administrator Change Log. If you enable the log, changes in supported Interaction Administrator containers are logged in this table.

Column Name	Description
EnhancedIAChangeLogId	Unique ID for the change
ChangeDateTime	Local server date and time when the change was made
ChangeTime	Local time of the change

ChangeDateTimeGMT	Greenwich Mean Time for when the change was made
UserId	User ID that made the change
StationId	ID of the computer from which the change was made
ChangeType	Type of change that was made. The values are Addition, Modification, Deletion, and Initial. Initial is the data taken when the system takes a snapshot point of the DS data
EntryKey	Item affected by the change
EntryClass	The Interaction Administrator container for which the change was made. **Note:** Log records for licenses and skills are handled in this manner: • “License” denotes a license change made in the **License Allocation** container. • “UserLicense” denotes a license change made in the **Users** container. • “StationLicense” denotes a license change was made from the **Stations** container. **Note:** Log records for skills are handled in this manner: • "Skills" denotes a change from **Skills** container. • "SkillsUser" denotes a change to the user from the **Skills** container. • "SkillsWorkgroup" denotes a change to the workgroup from the **Skills** container. **Note**: Log records for roles are handled in this manner: • "Roles" denotes a change from **Roles** container. • "RolesUser" denotes a change to the user from the **Roles** container. • "RolesWorkgroup" denotes a change to the workgroup from the **Roles** container.
I3TimeStampGMT	GMT Timestamp
SiteId	Site ID
SubsiteId	Subsite Id

ApplicationId -	ID of the application from where the change was made. The ID number corresponds to the ID found in the **ICApplications** table.

IAAttributeLog Table

The **IAAttributeLog** table is a child table of the **IAChangeLog** table. This table contains the specific attribute that was changed, the previous value, and the new value. There may be multiple records in the **IAAttributeLog** table that are for a single record in the **IAChangeLog** table.

> **Note:** Changes involving licenses are not recorded in this table.

Column Name	Description
IAAttributeLogId	Unique ID for the attribute that was changed
EnhancedIAChangeLogId	The foreign key to the IAChangeLog table
AttributeName	The name of the attribute that was changed
PrevousValue	The value before the change was made. This field can contain an empty string if the value was never been set before change logging was enabled, or if the field was cleared of its value.
NewValue	The new value for the attribute. This field can contain an empty string if the field was cleared of its value.

IALicenseAttributeLog Table

The **IALicenseAttributeLog** table is a child table of **EnhancedIAChangeLog**. This table captures the changes made for a user or a workstation license attribute.

> **Note:** There are several attributes for each user or workstation license. When a change is made to a user or a workstation license attribute, this table does not record which attribute was changed. Instead, all of the licenses for the user or station are written to the table.
>
> To determine which specific attribute was changed, do a diff to compare the current set of license attributes with the previous set of license attributes. A set of records for a single change will have the same EnhancedIAChangeLogID.

Column Name	Description
IALicenseAttributeLogId	Unique ID for the license change

EnhancedIAChangeLogId	Foreign key to the IAChangeLog table
License	License ID. This ID corresponds to the ID found in the **IALicenseLookup** table.
IsAssignable	Indicates whether the license allocation method for the given **IAChangeLog** entry key is assignable or concurrent: • A value of 1 means assignable • A value of 0 means concurrent.
IsActive	Indicates whether licenses are enabled for the given IAChangeLog entry key: • 1 means enabled. • 0 means disabled.
CallCallback	Denotes whether call/callback is selected as the ACD media type. This field is valid only for ACD Media 2 and ACD Media 3 licenses.
Chat	Denotes whether chat is selected as the ACD media type. This field is valid only for ACD Media 2 and ACD Media 3 licenses.
Email	Denotes whether email is selected as the ACD media type. This field is valid only for ACD Media 2 and ACD Media 3 licenses.
Generic	Denotes whether generic is selected as the ACD media type. This field is valid only for ACD Media 2 and ACD Media 3 licenses.

Related topics

About the Enhanced Interaction Administrator Change Log

Examples of changes to database tables

Database views for the Enhanced Interaction Administrator Change Log

Examples of changes to database tables

This help topic shows how the following types of database changes are tracked when the Enhanced Interaction Administration Change Log is enabled:

Snapshot of initial data

Change to a user attribute

Addition of a user

Setting or changing a user license

Deletion of a user

Assignment of a skill to a workgroup or user

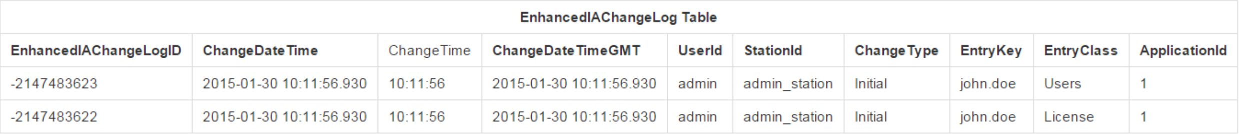
Removal of a skill from a workgroup or user

Modification to a Role

Change to a Default User attribute

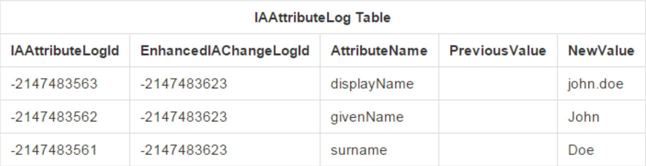
Snapshot of initial data

This example shows a snapshot of data that was taken when the Enhanced Interaction Administrator Change Log was enabled. Notice that value in the ChangeType column is “Initial.” You can also see that both the **IAAttributeLog** table and the **IALicenseAttributeLog** table have multiple records tied to a single record in the **EnhancedIAChangeLog** table.



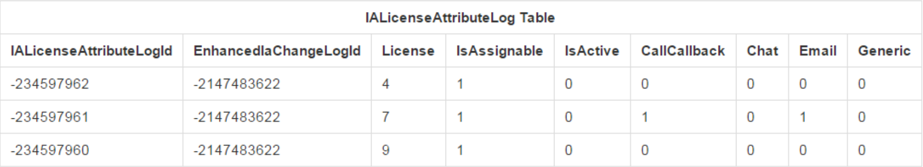
EnhancedIAChangeLog Table

EnhancedIAChangeLogID	ChangeDateTime	ChangeTime	ChangeDateTimeGMT	UserId	StationId	ChangeType	EntryKey	EntryClass	ApplicationId
-2147483623	2015-01-30 10:11:56.930	10:11:56	2015-01-30 10:11:56.930	admin	admin_station	Initial	john.doe	Users	1
-2147483622	2015-01-30 10:11:56.930	10:11:56	2015-01-30 10:11:56.930	admin	admin_station	Initial	john.doe	License	1



IAAttributeLog Table

IAAttributeLogId	EnhancedIAChangeLogId	AttributeName	PreviousValue	NewValue
-2147483563	-2147483623	displayName		john.doe
-2147483562	-2147483623	givenName		John
-2147483561	-2147483623	surname		Doe



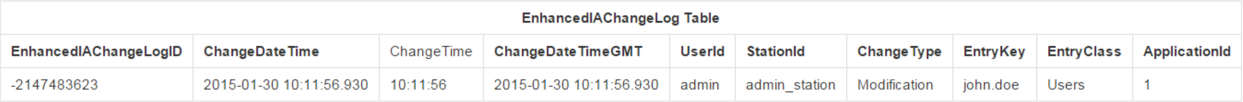
IALicenseAttributeLog Table

IALicenseAttributeLogId	EnhancedIaChangeLogId	License	IsAssignable	IsActive	CallCallback	Chat	Email	Generic
-234597962	-2147483622	4	1	0	0	0	0	0
-234597961	-2147483622	7	1	0	1	0	1	0
-234597960	-2147483622	9	1	0	0	0	0	0

Back to top

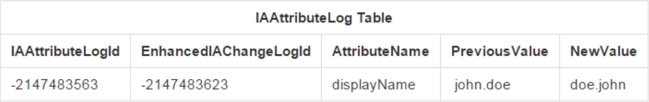
Change to a user attribute

This example shows the change log records that are created when you change an attribute on any property page in the **Users** container.



EnhancedIAChangeLog Table

EnhancedIAChangeLogID	ChangeDateTime	ChangeTime	ChangeDateTimeGMT	UserId	StationId	ChangeType	EntryKey	EntryClass	ApplicationId
-2147483623	2015-01-30 10:11:56.930	10:11:56	2015-01-30 10:11:56.930	admin	admin_station	Modification	john.doe	Users	1



IAAttributeLog Table

IAAttributeLogId	EnhancedIAChangeLogId	AttributeName	PreviousValue	NewValue
-2147483563	-2147483623	displayName	john.doe	doe.john

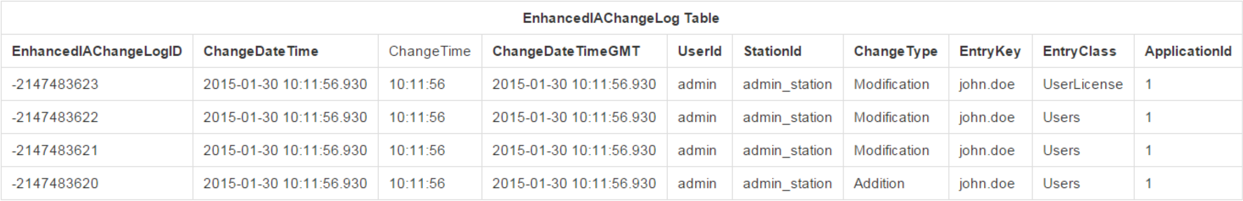
Back to top

Addition of a user

This example shows the change log records that are updated when you add a user:

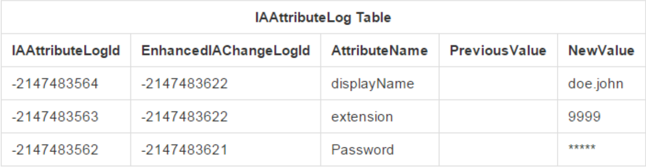
- The UserLicense modification is tied to a record in the **IALicenseAttributeLog** table.
- The Password attribute generates its own change log record.
- The other properties are tied to the other **EnhancedIAChangeLog** modification record.

- A record in the **EnhancedIAChangeLog** with a ChangeType of Addition denotes that a user was added to the system; there are no attribute records tied to that entry.



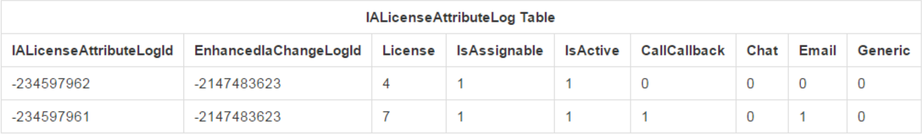
EnhancedIAChangeLog Table

EnhancedIAChangeLogID	ChangeDateTime	ChangeTime	ChangeDateTimeGMT	UserId	StationId	ChangeType	EntryKey	EntryClass	ApplicationId
-2147483623	2015-01-30 10:11:56.930	10:11:56	2015-01-30 10:11:56.930	admin	admin_station	Modification	john.doe	UserLicense	1
-2147483622	2015-01-30 10:11:56.930	10:11:56	2015-01-30 10:11:56.930	admin	admin_station	Modification	john.doe	Users	1
-2147483621	2015-01-30 10:11:56.930	10:11:56	2015-01-30 10:11:56.930	admin	admin_station	Modification	john.doe	Users	1
-2147483620	2015-01-30 10:11:56.930	10:11:56	2015-01-30 10:11:56.930	admin	admin_station	Addition	john.doe	Users	1



IAAttributeLog Table

IAAttributeLogId	EnhancedIAChangeLogId	AttributeName	PreviousValue	NewValue
-2147483564	-2147483622	displayName		doe.john
-2147483563	-2147483622	extension		9999
-2147483562	-2147483621	Password		*****



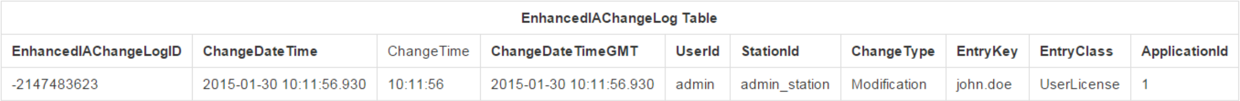
IALicenseAttributeLog Table

IALicenseAttributeLogId	EnhancedIaChangeLogId	License	IsAssignable	IsActive	CallCallback	Chat	Email	Generic
-234597962	-2147483623	4	1	1	0	0	0	0
-234597961	-2147483623	7	1	1	1	0	1	0

Back to top

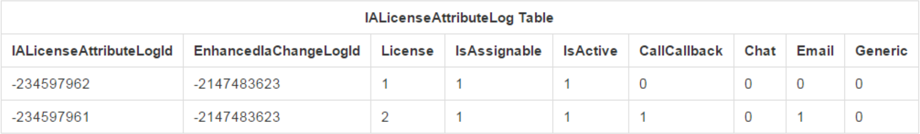
Setting or changing a user license

This example shows the change log records that are inserted when the client access license and the ACD Media 2 licenses (with call and email qualifiers) are assigned for a user.



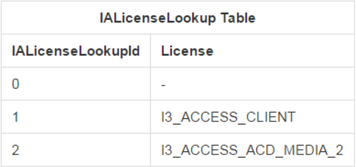
EnhancedIAChangeLog Table

EnhancedIAChangeLogID	ChangeDateTime	ChangeTime	ChangeDateTimeGMT	UserId	StationId	ChangeType	EntryKey	EntryClass	ApplicationId
-2147483623	2015-01-30 10:11:56.930	10:11:56	2015-01-30 10:11:56.930	admin	admin_station	Modification	john.doe	UserLicense	1



IALicenseAttributeLog Table

IALicenseAttributeLogId	EnhancedIaChangeLogId	License	IsAssignable	IsActive	CallCallback	Chat	Email	Generic
-234597962	-2147483623	1	1	1	0	0	0	0
-234597961	-2147483623	2	1	1	1	0	1	0



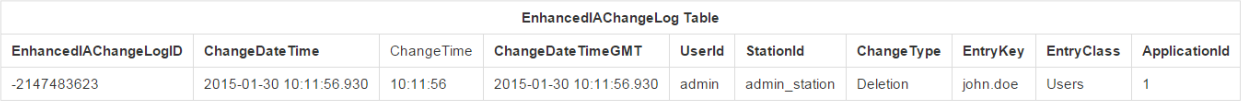
IALicenseLookup Table

IALicenseLookupId	License
0	-
1	I3_ACCESS_CLIENT
2	I3_ACCESS_ACD_MEDIA_2

Back to top

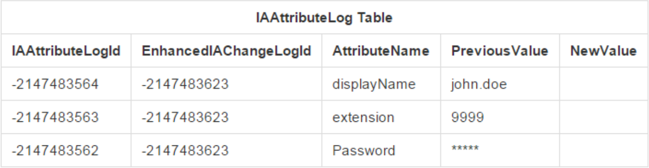
Deletion of a user

This example shows the change log record with the Change Type of Deletion. This indicates that the user record was deleted. The **IAAttributeLog** table is also updated to show what attributes were set on that user when the user was removed.



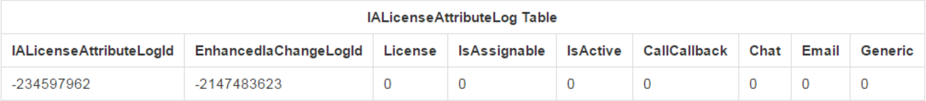
EnhancedIAChangeLog Table

EnhancedIAChangeLogID	ChangeDateTime	ChangeTime	ChangeDateTimeGMT	UserId	StationId	ChangeType	EntryKey	EntryClass	ApplicationId
-2147483623	2015-01-30 10:11:56.930	10:11:56	2015-01-30 10:11:56.930	admin	admin_station	Deletion	john.doe	Users	1



IAAttributeLog Table

IAAttributeLogId	EnhancedIAChangeLogId	AttributeName	PreviousValue	NewValue
-2147483564	-2147483623	displayName	john.doe	
-2147483563	-2147483623	extension	9999	
-2147483562	-2147483623	Password	*****	



IALicenseAttributeLog Table

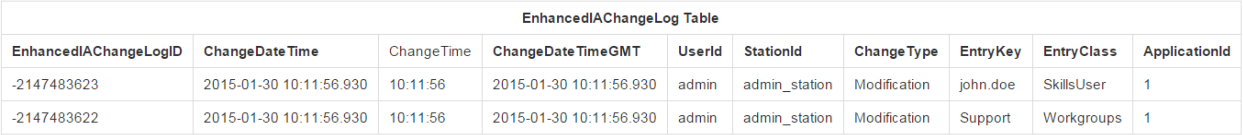
IALicenseAttributeLogId	EnhancedIaChangeLogId	License	IsAssignable	IsActive	CallCallback	Chat	Email	Generic
-234597962	-2147483623	0	0	0	0	0	0	0

Back to top

Assignment of a skill to a workgroup or user

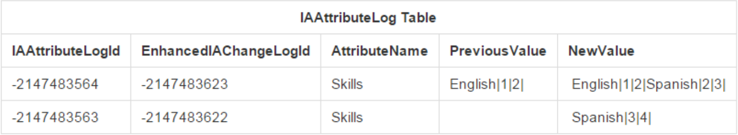
This example illustrates how the database tables are updated when a skill is added to a workgroup and a user.

> **Note**: If the EntryClass shows "SkillsUser" or "SkillsWorkgroup," then the skill was added from the **Skills** container.



EnhancedIAChangeLog Table

EnhancedIAChangeLogID	ChangeDateTime	ChangeTime	ChangeDateTimeGMT	UserId	StationId	ChangeType	EntryKey	EntryClass	ApplicationId
-2147483623	2015-01-30 10:11:56.930	10:11:56	2015-01-30 10:11:56.930	admin	admin_station	Modification	john.doe	SkillsUser	1
-2147483622	2015-01-30 10:11:56.930	10:11:56	2015-01-30 10:11:56.930	admin	admin_station	Modification	Support	Workgroups	1



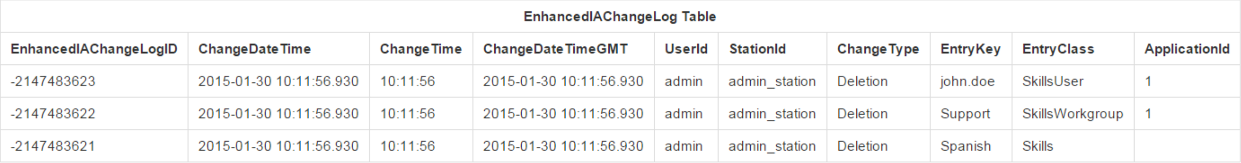
IAAttributeLog Table

IAAttributeLogId	EnhancedIAChangeLogId	AttributeName	PreviousValue	NewValue
-2147483564	-2147483623	Skills	English|1|2|	English|1|2|Spanish|2|3|
-2147483563	-2147483622	Skills		Spanish|3|4|

Back to top

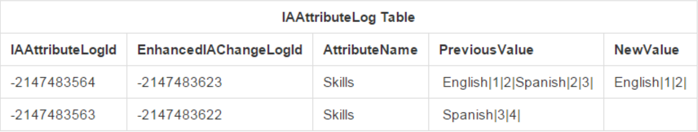
Removal of a skill from a workgroup or user

This example shows the change log records that are updated when a skill is unassigned from a workgroup or a user. Change log records are logged for the users and workgroups that were assigned that skill, along with the deletion record.



EnhancedIAChangeLog Table

EnhancedIAChangeLogID	ChangeDateTime	ChangeTime	ChangeDateTimeGMT	UserId	StationId	ChangeType	EntryKey	EntryClass	ApplicationId
-2147483623	2015-01-30 10:11:56.930	10:11:56	2015-01-30 10:11:56.930	admin	admin_station	Deletion	john.doe	SkillsUser	1
-2147483622	2015-01-30 10:11:56.930	10:11:56	2015-01-30 10:11:56.930	admin	admin_station	Deletion	Support	SkillsWorkgroup	1
-2147483621	2015-01-30 10:11:56.930	10:11:56	2015-01-30 10:11:56.930	admin	admin_station	Deletion	Spanish	Skills	



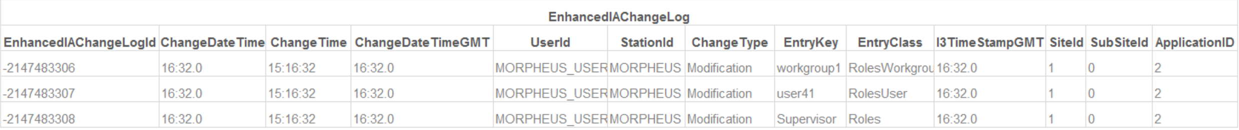
IAAttributeLog Table

IAAttributeLogId	EnhancedIAChangeLogId	AttributeName	PreviousValue	NewValue
-2147483564	-2147483623	Skills	English|1|2|Spanish|2|3|	English|1|2|
-2147483563	-2147483622	Skills	Spanish|3|4|	

Modification to a Role

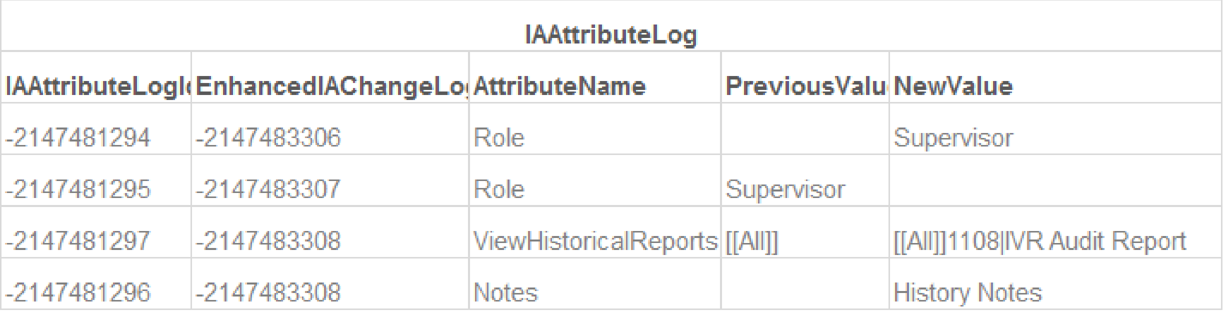
This example shows the change log records that are created when you change an attribute on any property page in the **Roles** container.

> **Note**: If the EntryClass shows "RolesUser" or "RolesWorkgroup," then the role was added/deleted from the **Roles** container.



EnhancedIAChangeLog

EnhancedIAChangeLogId	ChangeDateTime	ChangeTime	ChangeDateTimeGMT	UserId	StationId	ChangeType	EntryKey	EntryClass	I3TimeStampGMT	SiteId	SubSiteId	ApplicationID
-2147483306	16:32.0	15:16:32	16:32.0	MORPHEUS_USER	MORPHEUS	Modification	workgroup1	RolesWorkgrou	16:32.0	1	0	2
-2147483307	16:32.0	15:16:32	16:32.0	MORPHEUS_USER	MORPHEUS	Modification	user41	RolesUser	16:32.0	1	0	2
-2147483308	16:32.0	15:16:32	16:32.0	MORPHEUS_USER	MORPHEUS	Modification	Supervisor	Roles	16:32.0	1	0	2

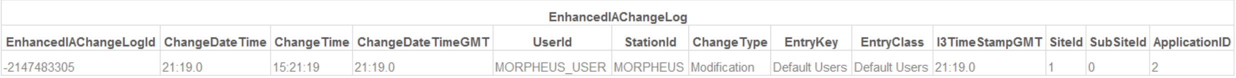


IAAttributeLog

IAAttributeLogI	EnhancedIAChangeLo	AttributeName	PreviousValu	NewValue
-2147481294	-2147483306	Role		Supervisor
-2147481295	-2147483307	Role	Supervisor	
-2147481297	-2147483308	ViewHistoricalReports	[[All]]	[[All]]1108|IVR Audit Report
-2147481296	-2147483308	Notes		History Notes

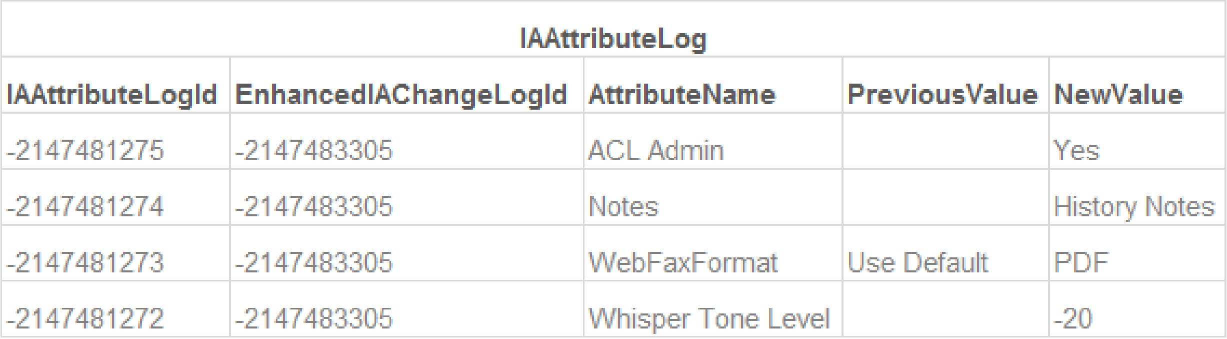
Change to a Default User attribute

This example shows the change log records that are created when you change an attribute on any property page in the **Default User** container.



EnhancedIAChangeLog

EnhancedIAChangeLogId	ChangeDateTime	ChangeTime	ChangeDateTimeGMT	UserId	StationId	ChangeType	EntryKey	EntryClass	I3TimeStampGMT	SiteId	SubSiteId	ApplicationID
-2147483305	21:19.0	15:21:19	21:19.0	MORPHEUS_USER	MORPHEUS	Modification	Default Users	Default Users	21:19.0	1	0	2



IAAttributeLog

IAAttributeLogId	EnhancedIAChangeLogId	AttributeName	PreviousValue	NewValue
-2147481275	-2147483305	ACL Admin		Yes
-2147481274	-2147483305	Notes		History Notes
-2147481273	-2147483305	WebFaxFormat	Use Default	PDF
-2147481272	-2147483305	Whisper Tone Level		-20

Back to top

Related topics

About the Enhanced Interaction Administrator Change Log

Database tables for the Enhanced Interaction Administrator Change Log

Database views for the Enhanced Interaction Administrator Change Log

Database views for the Enhanced Interaction Administrator Change Log

The following views are available for use with the Enhanced Interaction Administrator Change Log:

- EIACL_CurrentLicenses
- EIACL_HistoricalLicenses
- EIACL_HistoricalLicensesDP
- EIACL_CurrentSkills
- EIACL_HistoricalSkills
- EIACL_HistoricalSkillsDP

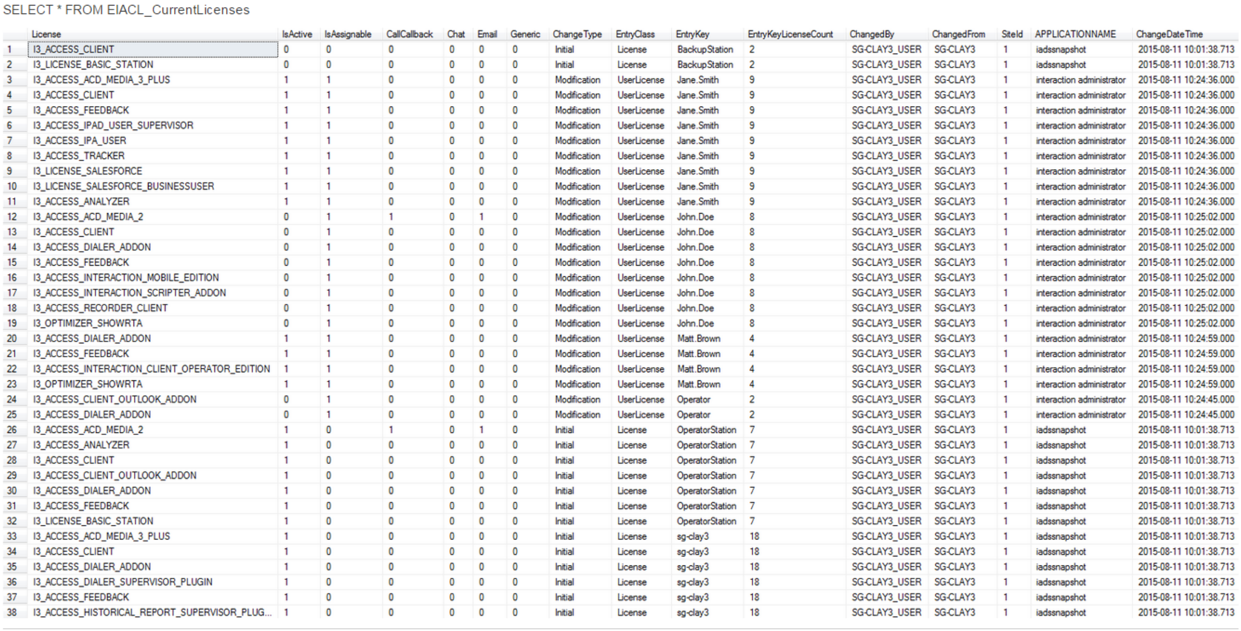
For more information on how to use these views, see the *PureConnect Data Dictionary Technical Reference* in the PureConnect Documentation Library.

> **Note:** Some of the values recorded for attributes may have multiple entries. The delimiter is the unit separator character (0x1F).

EIACL_CurrentLicenses

This view shows the current license allocation.

- This view will always be ordered by EntryKey. It displays only the most recent entry for each entry key. The entry key is always going to be a user or a station.
- The EntryKeyLicenseCount column provides a quick way to see how many licenses are currently allocated to a specific entry key.
- The License column displays license names the same way that they are displayed in the License Management dialog box.



SELECT * FROM EIACL_CurrentLicenses

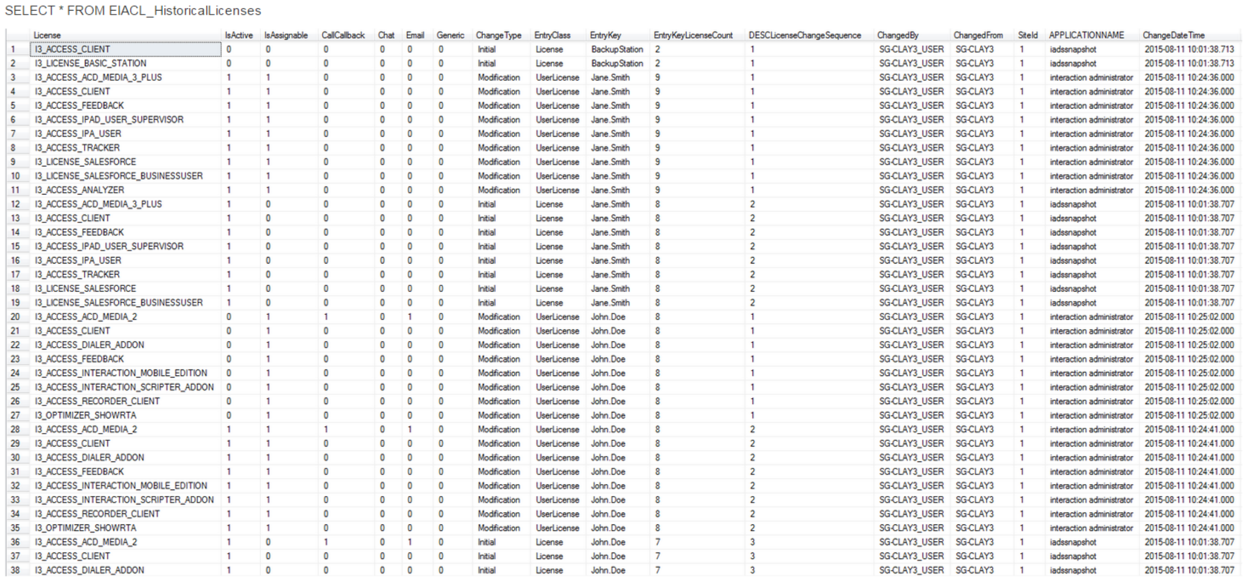
	License	IsActive	IsAssignable	CallCallback	Chat	Email	Generic	ChangeType	EntryClass	EntryKey	EntryKeyLicenseCount	ChangedBy	ChangedFrom	SiteId	APPLICATIONNAME	ChangeDateTime
1	I3_ACCESS_CLIENT	0	0	0	0	0	0	Initial	License	BackupStation	2	SG-CLAY3_USER	SG-CLAY3	1	iadssnapshot	2015-08-11 10:01:38.713
2	I3_LICENSE_BASIC_STATION	0	0	0	0	0	0	Initial	License	BackupStation	2	SG-CLAY3_USER	SG-CLAY3	1	iadssnapshot	2015-08-11 10:01:38.713
3	I3_ACCESS_ACD_MEDIA_3_PLUS	1	1	0	0	0	0	Modification	UserLicense	Jane.Smith	9	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator	2015-08-11 10:24:36.000
4	I3_ACCESS_CLIENT	1	1	0	0	0	0	Modification	UserLicense	Jane.Smith	9	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator	2015-08-11 10:24:36.000
5	I3_ACCESS_FEEDBACK	1	1	0	0	0	0	Modification	UserLicense	Jane.Smith	9	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator	2015-08-11 10:24:36.000
6	I3_ACCESS_IPAD_USER_SUPERVISOR	1	1	0	0	0	0	Modification	UserLicense	Jane.Smith	9	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator	2015-08-11 10:24:36.000
7	I3_ACCESS_IPA_USER	1	1	0	0	0	0	Modification	UserLicense	Jane.Smith	9	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator	2015-08-11 10:24:36.000
8	I3_ACCESS_TRACKER	1	1	0	0	0	0	Modification	UserLicense	Jane.Smith	9	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator	2015-08-11 10:24:36.000
9	I3_LICENSE_SALESFORCE	1	1	0	0	0	0	Modification	UserLicense	Jane.Smith	9	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator	2015-08-11 10:24:36.000
10	I3_LICENSE_SALESFORCE_BUSINESSUSER	1	1	0	0	0	0	Modification	UserLicense	Jane.Smith	9	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator	2015-08-11 10:24:36.000
11	I3_ACCESS_ANALYZER	1	1	0	0	0	0	Modification	UserLicense	Jane.Smith	9	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator	2015-08-11 10:24:36.000
12	I3_ACCESS_ACD_MEDIA_2	0	1	1	0	1	0	Modification	UserLicense	John.Doe	8	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator	2015-08-11 10:25:02.000
13	I3_ACCESS_CLIENT	0	1	0	0	0	0	Modification	UserLicense	John.Doe	8	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator	2015-08-11 10:25:02.000
14	I3_ACCESS_DIALER_ADDON	0	1	0	0	0	0	Modification	UserLicense	John.Doe	8	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator	2015-08-11 10:25:02.000
15	I3_ACCESS_FEEDBACK	0	1	0	0	0	0	Modification	UserLicense	John.Doe	8	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator	2015-08-11 10:25:02.000
16	I3_ACCESS_INTERACTION_MOBILE_EDITION	0	1	0	0	0	0	Modification	UserLicense	John.Doe	8	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator	2015-08-11 10:25:02.000
17	I3_ACCESS_INTERACTION_SCRIPTER_ADDON	0	1	0	0	0	0	Modification	UserLicense	John.Doe	8	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator	2015-08-11 10:25:02.000
18	I3_ACCESS_RECORDER_CLIENT	0	1	0	0	0	0	Modification	UserLicense	John.Doe	8	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator	2015-08-11 10:25:02.000
19	I3_OPTIMIZER_SHOWRTA	0	1	0	0	0	0	Modification	UserLicense	John.Doe	8	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator	2015-08-11 10:25:02.000
20	I3_ACCESS_DIALER_ADDON	1	1	0	0	0	0	Modification	UserLicense	Matt.Brown	4	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator	2015-08-11 10:24:59.000
21	I3_ACCESS_FEEDBACK	1	1	0	0	0	0	Modification	UserLicense	Matt.Brown	4	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator	2015-08-11 10:24:59.000
22	I3_ACCESS_INTERACTION_CLIENT_OPERATOR_EDITION	1	1	0	0	0	0	Modification	UserLicense	Matt.Brown	4	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator	2015-08-11 10:24:59.000
23	I3_OPTIMIZER_SHOWRTA	1	1	0	0	0	0	Modification	UserLicense	Matt.Brown	4	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator	2015-08-11 10:24:59.000
24	I3_ACCESS_CLIENT_OUTLOOK_ADDON	0	1	0	0	0	0	Modification	UserLicense	Operator	2	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator	2015-08-11 10:24:45.000
25	I3_ACCESS_DIALER_ADDON	0	1	0	0	0	0	Modification	UserLicense	Operator	2	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator	2015-08-11 10:24:45.000
26	I3_ACCESS_ACD_MEDIA_2	1	0	1	0	1	0	Initial	License	OperatorStation	7	SG-CLAY3_USER	SG-CLAY3	1	iadssnapshot	2015-08-11 10:01:38.713
27	I3_ACCESS_ANALYZER	1	0	0	0	0	0	Initial	License	OperatorStation	7	SG-CLAY3_USER	SG-CLAY3	1	iadssnapshot	2015-08-11 10:01:38.713
28	I3_ACCESS_CLIENT	1	0	0	0	0	0	Initial	License	OperatorStation	7	SG-CLAY3_USER	SG-CLAY3	1	iadssnapshot	2015-08-11 10:01:38.713
29	I3_ACCESS_CLIENT_OUTLOOK_ADDON	1	0	0	0	0	0	Initial	License	OperatorStation	7	SG-CLAY3_USER	SG-CLAY3	1	iadssnapshot	2015-08-11 10:01:38.713
30	I3_ACCESS_DIALER_ADDON	1	0	0	0	0	0	Initial	License	OperatorStation	7	SG-CLAY3_USER	SG-CLAY3	1	iadssnapshot	2015-08-11 10:01:38.713
31	I3_ACCESS_FEEDBACK	1	0	0	0	0	0	Initial	License	OperatorStation	7	SG-CLAY3_USER	SG-CLAY3	1	iadssnapshot	2015-08-11 10:01:38.713
32	I3_LICENSE_BASIC_STATION	1	0	0	0	0	0	Initial	License	OperatorStation	7	SG-CLAY3_USER	SG-CLAY3	1	iadssnapshot	2015-08-11 10:01:38.713
33	I3_ACCESS_ACD_MEDIA_3_PLUS	1	0	0	0	0	0	Initial	License	sg-clay3	18	SG-CLAY3_USER	SG-CLAY3	1	iadssnapshot	2015-08-11 10:01:38.713
34	I3_ACCESS_CLIENT	1	0	0	0	0	0	Initial	License	sg-clay3	18	SG-CLAY3_USER	SG-CLAY3	1	iadssnapshot	2015-08-11 10:01:38.713
35	I3_ACCESS_DIALER_ADDON	1	0	0	0	0	0	Initial	License	sg-clay3	18	SG-CLAY3_USER	SG-CLAY3	1	iadssnapshot	2015-08-11 10:01:38.713
36	I3_ACCESS_DIALER_SUPERVISOR_PLUGIN	1	0	0	0	0	0	Initial	License	sg-clay3	18	SG-CLAY3_USER	SG-CLAY3	1	iadssnapshot	2015-08-11 10:01:38.713
37	I3_ACCESS_FEEDBACK	1	0	0	0	0	0	Initial	License	sg-clay3	18	SG-CLAY3_USER	SG-CLAY3	1	iadssnapshot	2015-08-11 10:01:38.713
38	I3_ACCESS_HISTORICAL_REPORT_SUPERVISOR_PLUG...	1	0	0	0	0	0	Initial	License	sg-clay3	18	SG-CLAY3_USER	SG-CLAY3	1	iadssnapshot	2015-08-11 10:01:38.713

Back to top

EIACL_HistoricalLicenses

This view shows all the changes for licenses.

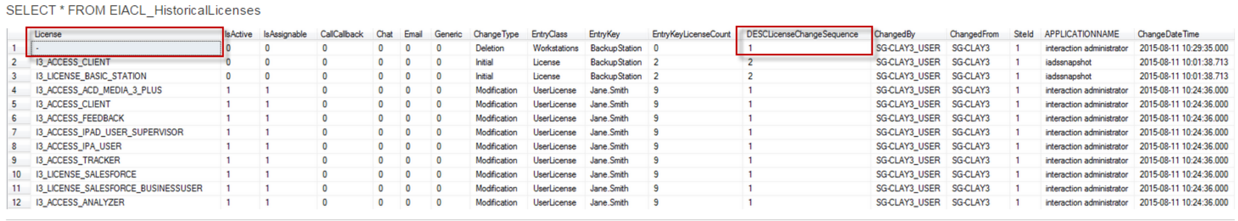
- This view will always be in descending order by EntryKey and ChangeDateTime. It displays all of the changes for each entry key. The entry key will always be a user or a station.
- The DESCLicenseChangeSequence column displays the ranking of changes for a specific entry key in descending order. A value of 1 always indicates the most recent license change for a specific entry key.
- The EntryKeyLicenseCount column provides a quick way to see how many licenses are currently allocated to a specific entry key and change sequence.
- The License column will display license names in the same way that they appear in the License Management dialog box.



SELECT * FROM EIACL_HistoricalLicenses

	License	IsActive	IsAssignable	CallCallback	Chat	Email	Generic	ChangeType	EntryClass	EntryKey	EntryKeyLicenseCount	DESCLicenseChangeSequence	ChangedBy	ChangedFrom	SiteId	APPLICATIONNAME	ChangeDateTime
1	I3_ACCESS_CLIENT	0	0	0	0	0	0	Initial	License	BackupStation	2	1	SG-CLAY3_USER	SG-CLAY3	1	iadssnapshot	2015-08-11 10:01:38.713
2	I3_LICENSE_BASIC_STATION	0	0	0	0	0	0	Initial	License	BackupStation	2	1	SG-CLAY3_USER	SG-CLAY3	1	iadssnapshot	2015-08-11 10:01:38.713
3	I3_ACCESS_ACD_MEDIA_3_PLUS	1	1	0	0	0	0	Modification	UserLicense	Jane.Smith	9	1	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator	2015-08-11 10:24:36.000
4	I3_ACCESS_CLIENT	1	1	0	0	0	0	Modification	UserLicense	Jane.Smith	9	1	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator	2015-08-11 10:24:36.000
5	I3_ACCESS_FEEDBACK	1	1	0	0	0	0	Modification	UserLicense	Jane.Smith	9	1	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator	2015-08-11 10:24:36.000
6	I3_ACCESS_IPAD_USER_SUPERVISOR	1	1	0	0	0	0	Modification	UserLicense	Jane.Smith	9	1	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator	2015-08-11 10:24:36.000
7	I3_ACCESS_IPA_USER	1	1	0	0	0	0	Modification	UserLicense	Jane.Smith	9	1	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator	2015-08-11 10:24:36.000
8	I3_ACCESS_TRACKER	1	1	0	0	0	0	Modification	UserLicense	Jane.Smith	9	1	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator	2015-08-11 10:24:36.000
9	I3_LICENSE_SALESFORCE	1	1	0	0	0	0	Modification	UserLicense	Jane.Smith	9	1	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator	2015-08-11 10:24:36.000
10	I3_LICENSE_SALESFORCE_BUSINESSUSER	1	1	0	0	0	0	Modification	UserLicense	Jane.Smith	9	1	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator	2015-08-11 10:24:36.000
11	I3_ACCESS_ANALYZER	1	1	0	0	0	0	Modification	UserLicense	Jane.Smith	9	1	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator	2015-08-11 10:24:36.000
12	I3_ACCESS_ACD_MEDIA_3_PLUS	1	0	0	0	0	0	Initial	License	Jane.Smith	8	2	SG-CLAY3_USER	SG-CLAY3	1	iadssnapshot	2015-08-11 10:01:38.707
13	I3_ACCESS_CLIENT	1	0	0	0	0	0	Initial	License	Jane.Smith	8	2	SG-CLAY3_USER	SG-CLAY3	1	iadssnapshot	2015-08-11 10:01:38.707
14	I3_ACCESS_FEEDBACK	1	0	0	0	0	0	Initial	License	Jane.Smith	8	2	SG-CLAY3_USER	SG-CLAY3	1	iadssnapshot	2015-08-11 10:01:38.707
15	I3_ACCESS_IPAD_USER_SUPERVISOR	1	0	0	0	0	0	Initial	License	Jane.Smith	8	2	SG-CLAY3_USER	SG-CLAY3	1	iadssnapshot	2015-08-11 10:01:38.707
16	I3_ACCESS_IPA_USER	1	0	0	0	0	0	Initial	License	Jane.Smith	8	2	SG-CLAY3_USER	SG-CLAY3	1	iadssnapshot	2015-08-11 10:01:38.707
17	I3_ACCESS_TRACKER	1	0	0	0	0	0	Initial	License	Jane.Smith	8	2	SG-CLAY3_USER	SG-CLAY3	1	iadssnapshot	2015-08-11 10:01:38.707
18	I3_LICENSE_SALESFORCE	1	0	0	0	0	0	Initial	License	Jane.Smith	8	2	SG-CLAY3_USER	SG-CLAY3	1	iadssnapshot	2015-08-11 10:01:38.707
19	I3_LICENSE_SALESFORCE_BUSINESSUSER	1	0	0	0	0	0	Initial	License	Jane.Smith	8	2	SG-CLAY3_USER	SG-CLAY3	1	iadssnapshot	2015-08-11 10:01:38.707
20	I3_ACCESS_ACD_MEDIA_2	0	1	1	0	1	0	Modification	UserLicense	John.Doe	8	1	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator	2015-08-11 10:25:02.000
21	I3_ACCESS_CLIENT	0	1	0	0	0	0	Modification	UserLicense	John.Doe	8	1	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator	2015-08-11 10:25:02.000
22	I3_ACCESS_DIALER_ADDON	0	1	0	0	0	0	Modification	UserLicense	John.Doe	8	1	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator	2015-08-11 10:25:02.000
23	I3_ACCESS_FEEDBACK	0	1	0	0	0	0	Modification	UserLicense	John.Doe	8	1	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator	2015-08-11 10:25:02.000
24	I3_ACCESS_INTERACTION_MOBILE_EDITION	0	1	0	0	0	0	Modification	UserLicense	John.Doe	8	1	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator	2015-08-11 10:25:02.000
25	I3_ACCESS_INTERACTION_SCRIPTER_ADDON	0	1	0	0	0	0	Modification	UserLicense	John.Doe	8	1	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator	2015-08-11 10:25:02.000
26	I3_ACCESS_RECORDER_CLIENT	0	1	0	0	0	0	Modification	UserLicense	John.Doe	8	1	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator	2015-08-11 10:25:02.000
27	I3_OPTIMIZER_SHOWRTA	0	1	0	0	0	0	Modification	UserLicense	John.Doe	8	1	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator	2015-08-11 10:25:02.000
28	I3_ACCESS_ACD_MEDIA_2	1	1	1	0	1	0	Modification	UserLicense	John.Doe	8	2	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator	2015-08-11 10:24:41.000
29	I3_ACCESS_CLIENT	1	1	0	0	0	0	Modification	UserLicense	John.Doe	8	2	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator	2015-08-11 10:24:41.000
30	I3_ACCESS_DIALER_ADDON	1	1	0	0	0	0	Modification	UserLicense	John.Doe	8	2	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator	2015-08-11 10:24:41.000
31	I3_ACCESS_FEEDBACK	1	1	0	0	0	0	Modification	UserLicense	John.Doe	8	2	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator	2015-08-11 10:24:41.000
32	I3_ACCESS_INTERACTION_MOBILE_EDITION	1	1	0	0	0	0	Modification	UserLicense	John.Doe	8	2	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator	2015-08-11 10:24:41.000
33	I3_ACCESS_INTERACTION_SCRIPTER_ADDON	1	1	0	0	0	0	Modification	UserLicense	John.Doe	8	2	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator	2015-08-11 10:24:41.000
34	I3_ACCESS_RECORDER_CLIENT	1	1	0	0	0	0	Modification	UserLicense	John.Doe	8	2	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator	2015-08-11 10:24:41.000
35	I3_OPTIMIZER_SHOWRTA	1	1	0	0	0	0	Modification	UserLicense	John.Doe	8	2	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator	2015-08-11 10:24:41.000
36	I3_ACCESS_ACD_MEDIA_2	1	0	1	0	1	0	Initial	License	John.Doe	7	3	SG-CLAY3_USER	SG-CLAY3	1	iadssnapshot	2015-08-11 10:01:38.707
37	I3_ACCESS_CLIENT	1	0	0	0	0	0	Initial	License	John.Doe	7	3	SG-CLAY3_USER	SG-CLAY3	1	iadssnapshot	2015-08-11 10:01:38.707
38	I3_ACCESS_DIALER_ADDON	1	0	0	0	0	0	Initial	License	John.Doe	7	3	SG-CLAY3_USER	SG-CLAY3	1	iadssnapshot	2015-08-11 10:01:38.707

When a user or station is deleted, the most recent entry for that entry key shows a **-** in the license column and a **1** in the DescLicenseChangeSequence column. This provides an easy way to tell which licenses were allocated to the user or station when the user or station was deleted, in case you need to recreate the user or station later with the same licenses.



SELECT * FROM EIACL_HistoricalLicenses

	License	IsActive	IsAssignable	CallCallback	Chat	Email	Generic	ChangeType	EntryClass	EntryKey	EntryKeyLicenseCount	DESCLicenseChangeSequence	ChangedBy	ChangedFrom	SiteId	APPLICATIONNAME	ChangeDateTime
1	-	0	0	0	0	0	0	Deletion	Workstations	BackupStation	0	1	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator	2015-08-11 10:29:35.000
2	I3_ACCESS_CLIENT	0	0	0	0	0	0	Initial	License	BackupStation	2	2	SG-CLAY3_USER	SG-CLAY3	1	iadssnapshot	2015-08-11 10:01:38.713
3	I3_LICENSE_BASIC_STATION	0	0	0	0	0	0	Initial	License	BackupStation	2	2	SG-CLAY3_USER	SG-CLAY3	1	iadssnapshot	2015-08-11 10:01:38.713
4	I3_ACCESS_ACD_MEDIA_3_PLUS	1	1	0	0	0	0	Modification	UserLicense	Jane.Smith	9	1	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator	2015-08-11 10:24:36.000
5	I3_ACCESS_CLIENT	1	1	0	0	0	0	Modification	UserLicense	Jane.Smith	9	1	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator	2015-08-11 10:24:36.000
6	I3_ACCESS_FEEDBACK	1	1	0	0	0	0	Modification	UserLicense	Jane.Smith	9	1	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator	2015-08-11 10:24:36.000
7	I3_ACCESS_IPAD_USER_SUPERVISOR	1	1	0	0	0	0	Modification	UserLicense	Jane.Smith	9	1	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator	2015-08-11 10:24:36.000
8	I3_ACCESS_IPA_USER	1	1	0	0	0	0	Modification	UserLicense	Jane.Smith	9	1	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator	2015-08-11 10:24:36.000
9	I3_ACCESS_TRACKER	1	1	0	0	0	0	Modification	UserLicense	Jane.Smith	9	1	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator	2015-08-11 10:24:36.000
10	I3_LICENSE_SALESFORCE	1	1	0	0	0	0	Modification	UserLicense	Jane.Smith	9	1	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator	2015-08-11 10:24:36.000
11	I3_LICENSE_SALESFORCE_BUSINESSUSER	1	1	0	0	0	0	Modification	UserLicense	Jane.Smith	9	1	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator	2015-08-11 10:24:36.000
12	I3_ACCESS_ANALYZER	1	1	0	0	0	0	Modification	UserLicense	Jane.Smith	9	1	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator	2015-08-11 10:24:36.000

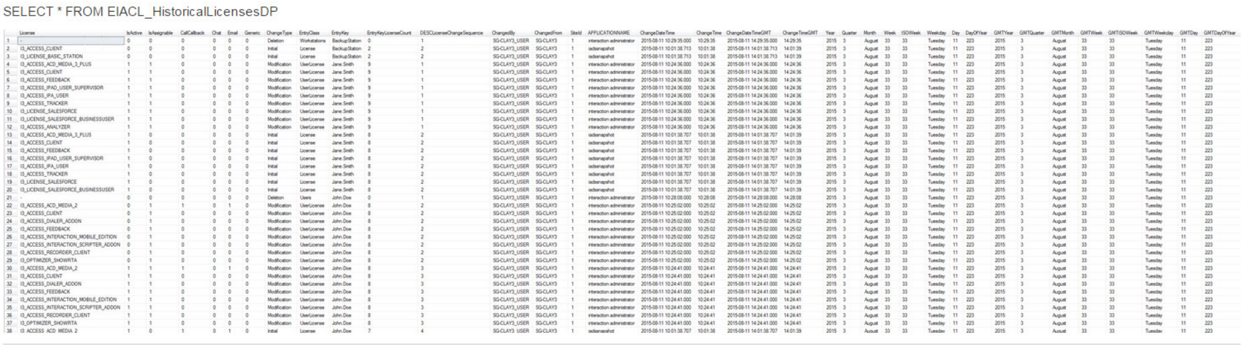
Back to top

EIACL_HistoricalLicensesDP

This view shows all the changes for licenses. It also includes some date part columns for use in sorting and grouping the data.

- This view will always be in descending order by EntryKey and ChangeDateTime. It displays all of the changes for each entry key. The entry key will always be a user or a station.
- The DESCLicenseChangeSequence column displays the ranking of changes for a specific entry key in descending order. A value of 1 always indicates the most recent license change for a specific entry key.
- The EntryKeyLicenseCount column provides a quick way to see how many licenses are currently allocated to a specific entry key and change sequence.
- The License column will display license names in the same way that they appear in the License Management dialog box.

- Additional columns have been added to show date parts of the local and gmt date time columns.



SELECT * FROM EIACL_HistoricalLicensesDP

	License	IsActive	IsAssignable	CallCallback	Chat	Email	Generic	ChangeType	EntryClass	EntryKey	EntryKeyLicenseCount	DESCLicenseChangeSequence	ChangedBy	ChangedFrom	SiteId	APPLICATIONNAME
1	-	0	0	0	0	0	0	Deletion	Workstations	BackupStation	0	1	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator
2	I3_ACCESS_CLIENT	0	0	0	0	0	0	Initial	License	BackupStation	2	2	SG-CLAY3_USER	SG-CLAY3	1	iadsnapshot
3	I3_LICENSE_BASIC_STATION	0	0	0	0	0	0	Initial	License	BackupStation	2	2	SG-CLAY3_USER	SG-CLAY3	1	iadsnapshot
4	I3_ACCESS_ACD_MEDIA_3_PLUS	1	1	0	0	0	0	Modification	UserLicense	Jane.Smith	9	1	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator
5	I3_ACCESS_CLIENT	1	1	0	0	0	0	Modification	UserLicense	Jane.Smith	9	1	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator
6	I3_ACCESS_FEEDBACK	1	1	0	0	0	0	Modification	UserLicense	Jane.Smith	9	1	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator
7	I3_ACCESS_IPAD_USER_SUPERVISOR	1	1	0	0	0	0	Modification	UserLicense	Jane.Smith	9	1	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator
8	I3_ACCESS_IPA_USER	1	1	0	0	0	0	Modification	UserLicense	Jane.Smith	9	1	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator
9	I3_ACCESS_TRACKER	1	1	0	0	0	0	Modification	UserLicense	Jane.Smith	9	1	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator
10	I3_LICENSE_SALESFORCE	1	1	0	0	0	0	Modification	UserLicense	Jane.Smith	9	1	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator
11	I3_LICENSE_SALESFORCE_BUSINESSUSER	1	1	0	0	0	0	Modification	UserLicense	Jane.Smith	9	1	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator
12	I3_ACCESS_ANALYZER	1	1	0	0	0	0	Modification	UserLicense	Jane.Smith	9	1	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator
13	I3_ACCESS_ACD_MEDIA_3_PLUS	1	0	0	0	0	0	Initial	License	Jane.Smith	8	2	SG-CLAY3_USER	SG-CLAY3	1	iadsnapshot
14	I3_ACCESS_CLIENT	1	0	0	0	0	0	Initial	License	Jane.Smith	8	2	SG-CLAY3_USER	SG-CLAY3	1	iadsnapshot
15	I3_ACCESS_FEEDBACK	1	0	0	0	0	0	Initial	License	Jane.Smith	8	2	SG-CLAY3_USER	SG-CLAY3	1	iadsnapshot
16	I3_ACCESS_IPAD_USER_SUPERVISOR	1	0	0	0	0	0	Initial	License	Jane.Smith	8	2	SG-CLAY3_USER	SG-CLAY3	1	iadsnapshot
17	I3_ACCESS_IPA_USER	1	0	0	0	0	0	Initial	License	Jane.Smith	8	2	SG-CLAY3_USER	SG-CLAY3	1	iadsnapshot
18	I3_ACCESS_TRACKER	1	0	0	0	0	0	Initial	License	Jane.Smith	8	2	SG-CLAY3_USER	SG-CLAY3	1	iadsnapshot
19	I3_LICENSE_SALESFORCE	1	0	0	0	0	0	Initial	License	Jane.Smith	8	2	SG-CLAY3_USER	SG-CLAY3	1	iadsnapshot
20	I3_LICENSE_SALESFORCE_BUSINESSUSER	1	0	0	0	0	0	Initial	License	Jane.Smith	8	2	SG-CLAY3_USER	SG-CLAY3	1	iadsnapshot
21	-	0	0	0	0	0	0	Deletion	Users	John.Doe	0	1	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator
22	I3_ACCESS_ACD_MEDIA_2	0	1	1	0	1	0	Modification	UserLicense	John.Doe	8	2	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator
23	I3_ACCESS_CLIENT	0	1	0	0	0	0	Modification	UserLicense	John.Doe	8	2	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator
24	I3_ACCESS_DIALER_ADDON	0	1	0	0	0	0	Modification	UserLicense	John.Doe	8	2	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator
25	I3_ACCESS_FEEDBACK	0	1	0	0	0	0	Modification	UserLicense	John.Doe	8	2	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator
26	I3_ACCESS_INTERACTION_MOBILE_EDITION	0	1	0	0	0	0	Modification	UserLicense	John.Doe	8	2	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator
27	I3_ACCESS_INTERACTION_SCRIPTER_ADDON	0	1	0	0	0	0	Modification	UserLicense	John.Doe	8	2	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator
28	I3_ACCESS_RECORDER_CLIENT	0	1	0	0	0	0	Modification	UserLicense	John.Doe	8	2	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator
29	I3_OPTIMIZER_SHOWRTA	0	1	0	0	0	0	Modification	UserLicense	John.Doe	8	2	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator
30	I3_ACCESS_ACD_MEDIA_2	1	1	1	0	1	0	Modification	UserLicense	John.Doe	8	3	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator
31	I3_ACCESS_CLIENT	1	1	0	0	0	0	Modification	UserLicense	John.Doe	8	3	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator
32	I3_ACCESS_DIALER_ADDON	1	1	0	0	0	0	Modification	UserLicense	John.Doe	8	3	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator
33	I3_ACCESS_FEEDBACK	1	1	0	0	0	0	Modification	UserLicense	John.Doe	8	3	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator
34	I3_ACCESS_INTERACTION_MOBILE_EDITION	1	1	0	0	0	0	Modification	UserLicense	John.Doe	8	3	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator
35	I3_ACCESS_INTERACTION_SCRIPTER_ADDON	1	1	0	0	0	0	Modification	UserLicense	John.Doe	8	3	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator
36	I3_ACCESS_RECORDER_CLIENT	1	1	0	0	0	0	Modification	UserLicense	John.Doe	8	3	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator
37	I3_OPTIMIZER_SHOWRTA	1	1	0	0	0	0	Modification	UserLicense	John.Doe	8	3	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator
38	I3_ACCESS_ACD_MEDIA_2	1	0	1	0	1	0	Initial	License	John.Doe	7	4	SG-CLAY3_USER	SG-CLAY3	1	iadsnapshot

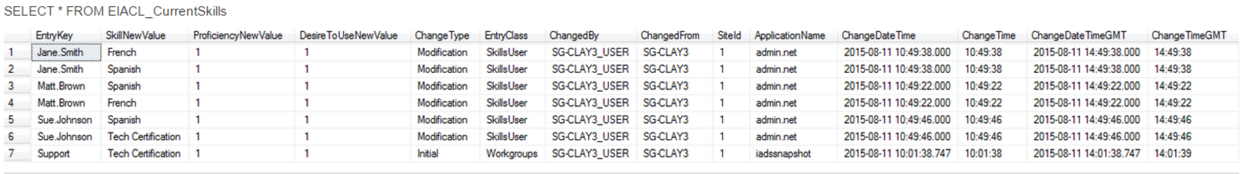
	ChangeDateTime	ChangeTime	ChangeDateTimeGMT	ChangeTimeGMT	Year	Quarter	Month	Week	ISOWeek	Weekday	Day	DayOfYear	GMTYear	GMTQuarter	GMTMonth	GMTWeek	GMTISOWeek	GMTWeekday	GMTDay	GMTDayOfYear
1	2015-08-11 10:29:35.000	10:29:35	2015-08-11 14:29:35.000	14:29:35	2015	3	August	33	33	Tuesday	11	223	2015	3	August	33	33	Tuesday	11	223
2	2015-08-11 10:01:38.713	10:01:38	2015-08-11 14:01:38.713	14:01:39	2015	3	August	33	33	Tuesday	11	223	2015	3	August	33	33	Tuesday	11	223
3	2015-08-11 10:01:38.713	10:01:38	2015-08-11 14:01:38.713	14:01:39	2015	3	August	33	33	Tuesday	11	223	2015	3	August	33	33	Tuesday	11	223
4	2015-08-11 10:24:36.000	10:24:36	2015-08-11 14:24:36.000	14:24:36	2015	3	August	33	33	Tuesday	11	223	2015	3	August	33	33	Tuesday	11	223
5	2015-08-11 10:24:36.000	10:24:36	2015-08-11 14:24:36.000	14:24:36	2015	3	August	33	33	Tuesday	11	223	2015	3	August	33	33	Tuesday	11	223
6	2015-08-11 10:24:36.000	10:24:36	2015-08-11 14:24:36.000	14:24:36	2015	3	August	33	33	Tuesday	11	223	2015	3	August	33	33	Tuesday	11	223
7	2015-08-11 10:24:36.000	10:24:36	2015-08-11 14:24:36.000	14:24:36	2015	3	August	33	33	Tuesday	11	223	2015	3	August	33	33	Tuesday	11	223
8	2015-08-11 10:24:36.000	10:24:36	2015-08-11 14:24:36.000	14:24:36	2015	3	August	33	33	Tuesday	11	223	2015	3	August	33	33	Tuesday	11	223
9	2015-08-11 10:24:36.000	10:24:36	2015-08-11 14:24:36.000	14:24:36	2015	3	August	33	33	Tuesday	11	223	2015	3	August	33	33	Tuesday	11	223
10	2015-08-11 10:24:36.000	10:24:36	2015-08-11 14:24:36.000	14:24:36	2015	3	August	33	33	Tuesday	11	223	2015	3	August	33	33	Tuesday	11	223
11	2015-08-11 10:24:36.000	10:24:36	2015-08-11 14:24:36.000	14:24:36	2015	3	August	33	33	Tuesday	11	223	2015	3	August	33	33	Tuesday	11	223
12	2015-08-11 10:24:36.000	10:24:36	2015-08-11 14:24:36.000	14:24:36	2015	3	August	33	33	Tuesday	11	223	2015	3	August	33	33	Tuesday	11	223
13	2015-08-11 10:01:38.707	10:01:38	2015-08-11 14:01:38.707	14:01:39	2015	3	August	33	33	Tuesday	11	223	2015	3	August	33	33	Tuesday	11	223
14	2015-08-11 10:01:38.707	10:01:38	2015-08-11 14:01:38.707	14:01:39	2015	3	August	33	33	Tuesday	11	223	2015	3	August	33	33	Tuesday	11	223
15	2015-08-11 10:01:38.707	10:01:38	2015-08-11 14:01:38.707	14:01:39	2015	3	August	33	33	Tuesday	11	223	2015	3	August	33	33	Tuesday	11	223
16	2015-08-11 10:01:38.707	10:01:38	2015-08-11 14:01:38.707	14:01:39	2015	3	August	33	33	Tuesday	11	223	2015	3	August	33	33	Tuesday	11	223
17	2015-08-11 10:01:38.707	10:01:38	2015-08-11 14:01:38.707	14:01:39	2015	3	August	33	33	Tuesday	11	223	2015	3	August	33	33	Tuesday	11	223
18	2015-08-11 10:01:38.707	10:01:38	2015-08-11 14:01:38.707	14:01:39	2015	3	August	33	33	Tuesday	11	223	2015	3	August	33	33	Tuesday	11	223
19	2015-08-11 10:01:38.707	10:01:38	2015-08-11 14:01:38.707	14:01:39	2015	3	August	33	33	Tuesday	11	223	2015	3	August	33	33	Tuesday	11	223
20	2015-08-11 10:01:38.707	10:01:38	2015-08-11 14:01:38.707	14:01:39	2015	3	August	33	33	Tuesday	11	223	2015	3	August	33	33	Tuesday	11	223
21	2015-08-11 10:28:08.000	10:28:08	2015-08-11 14:28:08.000	14:28:08	2015	3	August	33	33	Tuesday	11	223	2015	3	August	33	33	Tuesday	11	223
22	2015-08-11 10:25:02.000	10:25:02	2015-08-11 14:25:02.000	14:25:02	2015	3	August	33	33	Tuesday	11	223	2015	3	August	33	33	Tuesday	11	223
23	2015-08-11 10:25:02.000	10:25:02	2015-08-11 14:25:02.000	14:25:02	2015	3	August	33	33	Tuesday	11	223	2015	3	August	33	33	Tuesday	11	223
24	2015-08-11 10:25:02.000	10:25:02	2015-08-11 14:25:02.000	14:25:02	2015	3	August	33	33	Tuesday	11	223	2015	3	August	33	33	Tuesday	11	223
25	2015-08-11 10:25:02.000	10:25:02	2015-08-11 14:25:02.000	14:25:02	2015	3	August	33	33	Tuesday	11	223	2015	3	August	33	33	Tuesday	11	223
26	2015-08-11 10:25:02.000	10:25:02	2015-08-11 14:25:02.000	14:25:02	2015	3	August	33	33	Tuesday	11	223	2015	3	August	33	33	Tuesday	11	223
27	2015-08-11 10:25:02.000	10:25:02	2015-08-11 14:25:02.000	14:25:02	2015	3	August	33	33	Tuesday	11	223	2015	3	August	33	33	Tuesday	11	223
28	2015-08-11 10:25:02.000	10:25:02	2015-08-11 14:25:02.000	14:25:02	2015	3	August	33	33	Tuesday	11	223	2015	3	August	33	33	Tuesday	11	223
29	2015-08-11 10:25:02.000	10:25:02	2015-08-11 14:25:02.000	14:25:02	2015	3	August	33	33	Tuesday	11	223	2015	3	August	33	33	Tuesday	11	223
30	2015-08-11 10:24:41.000	10:24:41	2015-08-11 14:24:41.000	14:24:41	2015	3	August	33	33	Tuesday	11	223	2015	3	August	33	33	Tuesday	11	223
31	2015-08-11 10:24:41.000	10:24:41	2015-08-11 14:24:41.000	14:24:41	2015	3	August	33	33	Tuesday	11	223	2015	3	August	33	33	Tuesday	11	223
32	2015-08-11 10:24:41.000	10:24:41	2015-08-11 14:24:41.000	14:24:41	2015	3	August	33	33	Tuesday	11	223	2015	3	August	33	33	Tuesday	11	223
33	2015-08-11 10:24:41.000	10:24:41	2015-08-11 14:24:41.000	14:24:41	2015	3	August	33	33	Tuesday	11	223	2015	3	August	33	33	Tuesday	11	223
34	2015-08-11 10:24:41.000	10:24:41	2015-08-11 14:24:41.000	14:24:41	2015	3	August	33	33	Tuesday	11	223	2015	3	August	33	33	Tuesday	11	223
35	2015-08-11 10:24:41.000	10:24:41	2015-08-11 14:24:41.000	14:24:41	2015	3	August	33	33	Tuesday	11	223	2015	3	August	33	33	Tuesday	11	223
36	2015-08-11 10:24:41.000	10:24:41	2015-08-11 14:24:41.000	14:24:41	2015	3	August	33	33	Tuesday	11	223	2015	3	August	33	33	Tuesday	11	223
37	2015-08-11 10:24:41.000	10:24:41	2015-08-11 14:24:41.000	14:24:41	2015	3	August	33	33	Tuesday	11	223	2015	3	August	33	33	Tuesday	11	223
38	2015-08-11 10:01:38.707	10:01:38	2015-08-11 14:01:38.707	14:01:39	2015	3	August	33	33	Tuesday	11	223	2015	3	August	33	33	Tuesday	11	223

Back to top

EIACL_CurrentSkills

This view shows the current skills allocation for skills that have users or workgroups allocated to them.

- This view will always be ordered by EntryKey and ChangeDateTime descending and display all of the changes for each entry key. The entry key is always going to be a user or a workgroup.
- The SkillNewValue column displays the skill name.



SELECT * FROM EIACL_CurrentSkills

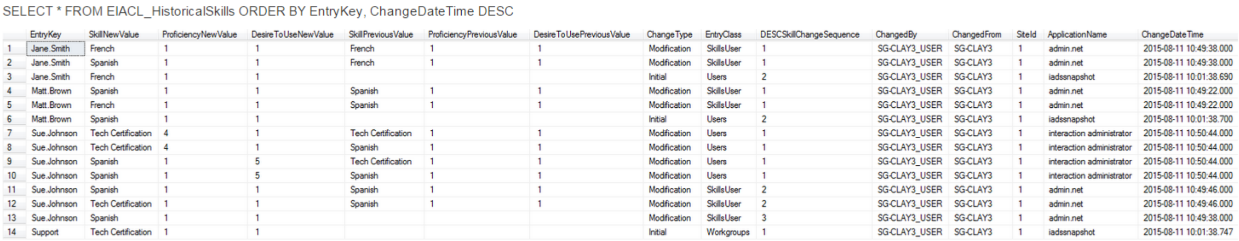
	EntryKey	SkillNewValue	ProficiencyNewValue	DesireToUseNewValue	ChangeType	EntryClass	ChangedBy	ChangedFrom	SiteId	ApplicationName	ChangeDateTime	ChangeTime	ChangeDateTimeGMT	ChangeTimeGMT
1	Jane.Smith	French	1	1	Modification	SkillsUser	SG-CLAY3_USER	SG-CLAY3	1	admin.net	2015-08-11 10:49:38.000	10:49:38	2015-08-11 14:49:38.000	14:49:38
2	Jane.Smith	Spanish	1	1	Modification	SkillsUser	SG-CLAY3_USER	SG-CLAY3	1	admin.net	2015-08-11 10:49:38.000	10:49:38	2015-08-11 14:49:38.000	14:49:38
3	Matt.Brown	Spanish	1	1	Modification	SkillsUser	SG-CLAY3_USER	SG-CLAY3	1	admin.net	2015-08-11 10:49:22.000	10:49:22	2015-08-11 14:49:22.000	14:49:22
4	Matt.Brown	French	1	1	Modification	SkillsUser	SG-CLAY3_USER	SG-CLAY3	1	admin.net	2015-08-11 10:49:22.000	10:49:22	2015-08-11 14:49:22.000	14:49:22
5	Sue.Johnson	Spanish	1	1	Modification	SkillsUser	SG-CLAY3_USER	SG-CLAY3	1	admin.net	2015-08-11 10:49:46.000	10:49:46	2015-08-11 14:49:46.000	14:49:46
6	Sue.Johnson	Tech Certification	1	1	Modification	SkillsUser	SG-CLAY3_USER	SG-CLAY3	1	admin.net	2015-08-11 10:49:46.000	10:49:46	2015-08-11 14:49:46.000	14:49:46
7	Support	Tech Certification	1	1	Initial	Workgroups	SG-CLAY3_USER	SG-CLAY3	1	iadssnapshot	2015-08-11 10:01:38.747	10:01:38	2015-08-11 14:01:38.747	14:01:39

Back to top

EIACL_HistoricalSkills

This view shows all the changes for skills that have users or workgroups allocated to them.

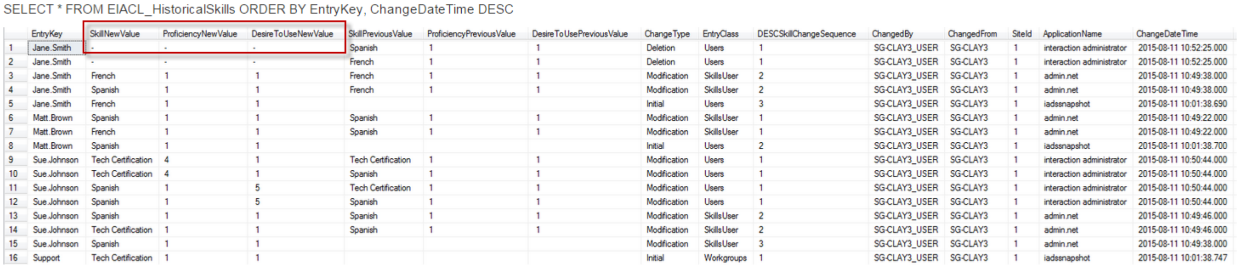
- The entry key is always going to be a user or a workgroup.
- The SkillNewValue column displays the skill name.
- The SkillPreviousValue column displays the skill name for the previous value.
- This view is different from EIACL_CurrentSkills in that it also displays the previous values for the skill on the same row as the new value.
- In order to make this data easier to consume, it is recommended that you order the view by EntryKey and ChangeDateTime DESC.
- The DESCSkillChangeSequence column will show the ranking of the EntryKeys ordered by ChangeDateTimeGMT DESC



SELECT * FROM EIACL_HistoricalSkills ORDER BY EntryKey, ChangeDateTime DESC

	EntryKey	SkillNewValue	ProficiencyNewValue	DesireToUseNewValue	SkillPreviousValue	ProficiencyPreviousValue	DesireToUsePreviousValue	ChangeType	EntryClass	DESCSkillChangeSequence	ChangedBy	ChangedFrom	SiteId	ApplicationName	ChangeDateTime
1	Jane.Smith	French	1	1	French	1	1	Modification	SkillsUser	1	SG-CLAY3_USER	SG-CLAY3	1	admin.net	2015-08-11 10:49:38.000
2	Jane.Smith	Spanish	1	1	French	1	1	Modification	SkillsUser	1	SG-CLAY3_USER	SG-CLAY3	1	admin.net	2015-08-11 10:49:38.000
3	Jane.Smith	French	1	1				Initial	Users	2	SG-CLAY3_USER	SG-CLAY3	1	iadssnapshot	2015-08-11 10:01:38.690
4	Matt.Brown	Spanish	1	1	Spanish	1	1	Modification	SkillsUser	1	SG-CLAY3_USER	SG-CLAY3	1	admin.net	2015-08-11 10:49:22.000
5	Matt.Brown	French	1	1	Spanish	1	1	Modification	SkillsUser	1	SG-CLAY3_USER	SG-CLAY3	1	admin.net	2015-08-11 10:49:22.000
6	Matt.Brown	Spanish	1	1				Initial	Users	2	SG-CLAY3_USER	SG-CLAY3	1	iadssnapshot	2015-08-11 10:01:38.700
7	Sue.Johnson	Tech Certification	4	1	Tech Certification	1	1	Modification	Users	1	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator	2015-08-11 10:50:44.000
8	Sue.Johnson	Tech Certification	4	1	Spanish	1	1	Modification	Users	1	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator	2015-08-11 10:50:44.000
9	Sue.Johnson	Spanish	1	5	Tech Certification	1	1	Modification	Users	1	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator	2015-08-11 10:50:44.000
10	Sue.Johnson	Spanish	1	5	Spanish	1	1	Modification	Users	1	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator	2015-08-11 10:50:44.000
11	Sue.Johnson	Spanish	1	1	Spanish	1	1	Modification	SkillsUser	2	SG-CLAY3_USER	SG-CLAY3	1	admin.net	2015-08-11 10:49:46.000
12	Sue.Johnson	Tech Certification	1	1	Spanish	1	1	Modification	SkillsUser	2	SG-CLAY3_USER	SG-CLAY3	1	admin.net	2015-08-11 10:49:46.000
13	Sue.Johnson	Spanish	1	1				Modification	SkillsUser	3	SG-CLAY3_USER	SG-CLAY3	1	admin.net	2015-08-11 10:49:38.000
14	Support	Tech Certification	1	1				Initial	Workgroups	1	SG-CLAY3_USER	SG-CLAY3	1	iadssnapshot	2015-08-11 10:01:38.747

When a user or workgroup is deleted, the SkillNewValue, ProficiencyNewValue and DesireToUseNewValue columns display a **-**. This provides an easy way to tell what skills were allocated to a user or workgroup when it was deleted in case you need to recreate the user or workgroup later with the same skill allocations.



SELECT * FROM EIACL_HistoricalSkills ORDER BY EntryKey, ChangeDateTime DESC

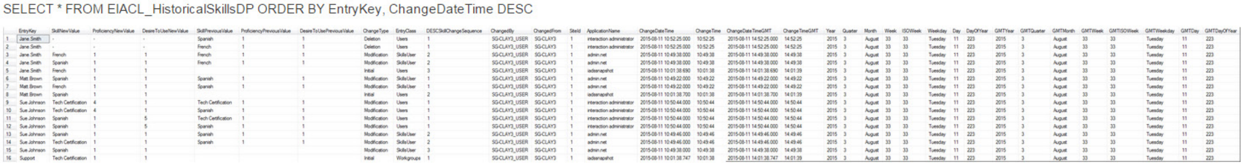
	EntryKey	SkillNewValue	ProficiencyNewValue	DesireToUseNewValue	SkillPreviousValue	ProficiencyPreviousValue	DesireToUsePreviousValue	ChangeType	EntryClass	DESCSkillChangeSequence	ChangedBy	ChangedFrom	SiteId	ApplicationName	ChangeDateTime
1	Jane.Smith	-	-	-	Spanish	1	1	Deletion	Users	1	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator	2015-08-11 10:52:25.000
2	Jane.Smith	-	-	-	French	1	1	Deletion	Users	1	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator	2015-08-11 10:52:25.000
3	Jane.Smith	French	1	1	French	1	1	Modification	SkillsUser	2	SG-CLAY3_USER	SG-CLAY3	1	admin.net	2015-08-11 10:49:38.000
4	Jane.Smith	Spanish	1	1	French	1	1	Modification	SkillsUser	2	SG-CLAY3_USER	SG-CLAY3	1	admin.net	2015-08-11 10:49:38.000
5	Jane.Smith	French	1	1				Initial	Users	3	SG-CLAY3_USER	SG-CLAY3	1	iadssnapshot	2015-08-11 10:01:38.690
6	Matt.Brown	Spanish	1	1	Spanish	1	1	Modification	SkillsUser	1	SG-CLAY3_USER	SG-CLAY3	1	admin.net	2015-08-11 10:49:22.000
7	Matt.Brown	French	1	1	Spanish	1	1	Modification	SkillsUser	1	SG-CLAY3_USER	SG-CLAY3	1	admin.net	2015-08-11 10:49:22.000
8	Matt.Brown	Spanish	1	1				Initial	Users	2	SG-CLAY3_USER	SG-CLAY3	1	iadssnapshot	2015-08-11 10:01:38.700
9	Sue.Johnson	Tech Certification	4	1	Tech Certification	1	1	Modification	Users	1	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator	2015-08-11 10:50:44.000
10	Sue.Johnson	Tech Certification	4	1	Spanish	1	1	Modification	Users	1	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator	2015-08-11 10:50:44.000
11	Sue.Johnson	Spanish	1	5	Tech Certification	1	1	Modification	Users	1	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator	2015-08-11 10:50:44.000
12	Sue.Johnson	Spanish	1	5	Spanish	1	1	Modification	Users	1	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator	2015-08-11 10:50:44.000
13	Sue.Johnson	Spanish	1	1	Spanish	1	1	Modification	SkillsUser	2	SG-CLAY3_USER	SG-CLAY3	1	admin.net	2015-08-11 10:49:46.000
14	Sue.Johnson	Tech Certification	1	1	Spanish	1	1	Modification	SkillsUser	2	SG-CLAY3_USER	SG-CLAY3	1	admin.net	2015-08-11 10:49:46.000
15	Sue.Johnson	Spanish	1	1				Modification	SkillsUser	3	SG-CLAY3_USER	SG-CLAY3	1	admin.net	2015-08-11 10:49:38.000
16	Support	Tech Certification	1	1				Initial	Workgroups	1	SG-CLAY3_USER	SG-CLAY3	1	iadssnapshot	2015-08-11 10:01:38.747

Back to top

EIACL_HistoricalSkillsDP

This view shows all the changes for skills.

- The entry key is always going to be a user or a workgroup.
- The SkillNewValue column displays the skill name.
- The SkillPreviousValue column displays the skill name for the previous value.
- This view is different from EIACL_CurrentSkills in that it also displays the previous values for the skill on the same row as the new value.
- In order to make this data easier to consume, it is recommended that you order the view by EntryKey and ChangeDateTime DESC.
- The DESCSkillChangeSequence column will show the ranking of the EntryKeys ordered by ChangeDateTimeGMT DESC
- This view includes some date part columns for use in sorting and grouping the data.



SELECT * FROM EIACL_HistoricalSkillsDP ORDER BY EntryKey, ChangeDateTime DESC

	EntryKey	SkillNewValue	ProficiencyNewValue	DesireToUseNewValue	SkillPreviousValue	ProficiencyPreviousValue	DesireToUsePreviousValue	ChangeType	EntryClass	DESCSkillChangeSequence	ChangedBy	ChangedFrom	SiteId	ApplicationName	ChangeDateTime
1	Jane.Smith	-	-	-	Spanish	1	1	Deletion	Users	1	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator	2015-08-11 10:52:25.000
2	Jane.Smith	-	-	-	French	1	1	Deletion	Users	1	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator	2015-08-11 10:52:25.000
3	Jane.Smith	French	1	1	French	1	1	Modification	SkillsUser	2	SG-CLAY3_USER	SG-CLAY3	1	admin.net	2015-08-11 10:49:38.000
4	Jane.Smith	Spanish	1	1	French	1	1	Modification	SkillsUser	2	SG-CLAY3_USER	SG-CLAY3	1	admin.net	2015-08-11 10:49:38.000
5	Jane.Smith	French	1	1				Initial	Users	3	SG-CLAY3_USER	SG-CLAY3	1	iadssnapshot	2015-08-11 10:01:38.690
6	Matt.Brown	Spanish	1	1	Spanish	1	1	Modification	SkillsUser	1	SG-CLAY3_USER	SG-CLAY3	1	admin.net	2015-08-11 10:49:22.000
7	Matt.Brown	French	1	1	Spanish	1	1	Modification	SkillsUser	1	SG-CLAY3_USER	SG-CLAY3	1	admin.net	2015-08-11 10:49:22.000
8	Matt.Brown	Spanish	1	1				Initial	Users	2	SG-CLAY3_USER	SG-CLAY3	1	iadssnapshot	2015-08-11 10:01:38.700
9	Sue.Johnson	Tech Certification	4	1	Tech Certification	1	1	Modification	Users	1	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator	2015-08-11 10:50:44.000
10	Sue.Johnson	Tech Certification	4	1	Spanish	1	1	Modification	Users	1	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator	2015-08-11 10:50:44.000
11	Sue.Johnson	Spanish	1	5	Tech Certification	1	1	Modification	Users	1	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator	2015-08-11 10:50:44.000
12	Sue.Johnson	Spanish	1	5	Spanish	1	1	Modification	Users	1	SG-CLAY3_USER	SG-CLAY3	1	interaction administrator	2015-08-11 10:50:44.000
13	Sue.Johnson	Spanish	1	1	Spanish	1	1	Modification	SkillsUser	2	SG-CLAY3_USER	SG-CLAY3	1	admin.net	2015-08-11 10:49:46.000
14	Sue.Johnson	Tech Certification	1	1	Spanish	1	1	Modification	SkillsUser	2	SG-CLAY3_USER	SG-CLAY3	1	admin.net	2015-08-11 10:49:46.000
15	Sue.Johnson	Spanish	1	1				Modification	SkillsUser	3	SG-CLAY3_USER	SG-CLAY3	1	admin.net	2015-08-11 10:49:38.000
16	Support	Tech Certification	1	1				Initial	Workgroups	1	SG-CLAY3_USER	SG-CLAY3	1	iadssnapshot	2015-08-11 10:01:38.747

	EntryKey	ChangeTime	ChangeDateTimeGMT	ChangeTimeGMT	Year	Quarter	Month	Week	ISOWeek	Weekday	Day	DayOfYear	GMTYear	GMTQuarter	GMTMonth	GMTWeek	GMTISOWeek	GMTWeekday	GMTDay	GMTDayOfYear
1	Jane.Smith	10:52:25	2015-08-11 14:52:25.000	14:52:25	2015	3	August	33	33	Tuesday	11	223	2015	3	August	33	33	Tuesday	11	223
2	Jane.Smith	10:52:25	2015-08-11 14:52:25.000	14:52:25	2015	3	August	33	33	Tuesday	11	223	2015	3	August	33	33	Tuesday	11	223
3	Jane.Smith	10:49:38	2015-08-11 14:49:38.000	14:49:38	2015	3	August	33	33	Tuesday	11	223	2015	3	August	33	33	Tuesday	11	223
4	Jane.Smith	10:49:38	2015-08-11 14:49:38.000	14:49:38	2015	3	August	33	33	Tuesday	11	223	2015	3	August	33	33	Tuesday	11	223
5	Jane.Smith	10:01:38	2015-08-11 14:01:38.690	14:01:39	2015	3	August	33	33	Tuesday	11	223	2015	3	August	33	33	Tuesday	11	223
6	Matt.Brown	10:49:22	2015-08-11 14:49:22.000	14:49:22	2015	3	August	33	33	Tuesday	11	223	2015	3	August	33	33	Tuesday	11	223
7	Matt.Brown	10:49:22	2015-08-11 14:49:22.000	14:49:22	2015	3	August	33	33	Tuesday	11	223	2015	3	August	33	33	Tuesday	11	223
8	Matt.Brown	10:01:38	2015-08-11 14:01:38.700	14:01:39	2015	3	August	33	33	Tuesday	11	223	2015	3	August	33	33	Tuesday	11	223
9	Sue.Johnson	10:50:44	2015-08-11 14:50:44.000	14:50:44	2015	3	August	33	33	Tuesday	11	223	2015	3	August	33	33	Tuesday	11	223
10	Sue.Johnson	10:50:44	2015-08-11 14:50:44.000	14:50:44	2015	3	August	33	33	Tuesday	11	223	2015	3	August	33	33	Tuesday	11	223
11	Sue.Johnson	10:50:44	2015-08-11 14:50:44.000	14:50:44	2015	3	August	33	33	Tuesday	11	223	2015	3	August	33	33	Tuesday	11	223
12	Sue.Johnson	10:50:44	2015-08-11 14:50:44.000	14:50:44	2015	3	August	33	33	Tuesday	11	223	2015	3	August	33	33	Tuesday	11	223
13	Sue.Johnson	10:49:46	2015-08-11 14:49:46.000	14:49:46	2015	3	August	33	33	Tuesday	11	223	2015	3	August	33	33	Tuesday	11	223
14	Sue.Johnson	10:49:46	2015-08-11 14:49:46.000	14:49:46	2015	3	August	33	33	Tuesday	11	223	2015	3	August	33	33	Tuesday	11	223
15	Sue.Johnson	10:49:38	2015-08-11 14:49:38.000	14:49:38	2015	3	August	33	33	Tuesday	11	223	2015	3	August	33	33	Tuesday	11	223
16	Support	10:01:38	2015-08-11 14:01:38.747	14:01:39	2015	3	August	33	33	Tuesday	11	223	2015	3	August	33	33	Tuesday	11	223

Back to top

Related topics

About the Enhanced Interaction Administrator Change Log

Database tables for the Enhanced Interaction Administrator Change Log

Examples of changes to database tables

Troubleshoot the Enhanced Interaction Administrator Change Log

This help topic contains the following sections:

Logging administrative changes from other applications

If you upgrade and then downgrade

Duplicate records for workgroup media types

Side effect changes in Directory Services

Logging administrative changes from other applications

If you are using an version of Interaction Administrator that is earlier than CIC 2016 R1, with a server that supported enhanced logging, the changes will not be logged and may introduce inconsistencies with the data. The detailed changes in the Users, Workgroups, Skills, License Allocation, Stations, Roles and Default User containers will not be logged.

If you notice data inconsistencies, disable and re-enable logging. This takes a new snapshot and creates a new baseline for your data.

> **Note:** If you take a new snapshot, the views display data back to the last snapshot. However, your complete change log information remains in the database.

Duplicate records for workgroup media types

You may see duplicate records for workgroup media types. This is because the earlier Interaction Administrator logging feature still exists and it logs data for these items. This feature was preserved for backward compatibility purposes.

If you upgrade and then downgrade

If you upgrade to 2016 R1 and then downgrade to an earlier version, you will see the Enhanced Interaction Administrator Change Log in Interaction Administration. However, the log will not function. When you re-upgrade to 2016 R1, and if the enhanced logging was previously enabled, a new snapshot will be taken during the upgrade process and enhanced logging will begin. If you had not enabled the enhanced logging before downgrading, the logging will not begin until you enable it.

Side effect changes in Directory Services

During the implementation of the Enhanced Interaction Administrator Change Log, certain Interaction Administrator behaviors were affected. This section describes those side effect changes.

The following are the categories of side effect changes that have been noticed in Directory Services:

Side effects with delayed manifestation in Directory Services

Side effects with immediate manifestation in Directory Services

Side effects with delayed manifestation in Directory Services

Field	DS Key	Notes
Default Language	Users\[USER]\Preferred Language	If the preferred language for a user or workgroup's is deleted, the default language is automatically assigned to the user or workgroup. However, the Enhanced Interaction Administrator Change Log does not log this change until another action or event updates or saves the user's or workgroup's configuration.
Recording/Beep Tone	Workgroups\[WORKGROUP]\SelectedTone	If the recording beep tone for a workgroup is deleted, the default recording beep tone is automatically assigned to the workgroup. However, the Enhanced Interaction Administrator Change Log does not log this change until another action or event updates or saves the workgroup's configuration.
Default Workstation	Users\[USER]\Default Workstation	If a user's default workstation is deleted, the Enhanced Interaction Administrator Change Log does not log this

		change until another action or event updates or saves the user's configuration.
CSV User Import	Users\	When a user record is imported by a .CSV file, an administrator can view the user's properties in Interaction Administrator. When the administrator clicks OK to close the user's Configuration dialog box, additional configuration settings are automatically set by Interaction Administrator. The Enhanced Interaction Administrator Change Log logs those additional settings changes.
Time Zone	Users\[USER]\TimeZone	See Location.

Back to the top of the section

Side effects with immediate manifestation in Directory Services

Field	DS Key	Notes
Unified Messaging	Users\[USER]\UM Destination	If a Unified Messaging station is deleted and a user was configured to use that station, the Enhanced Interaction Administrator Change Log logs that the station was deleted. It does not, however, log that the user record was also changed.

		If a location is deleted, the Enhanced Interaction Administrator Change Log logs that the location was deleted. It does not, however, log that the user records that used that location were also changed.
Location	Users\[USER]\Location	When a location is deleted, the user records that were configured to use that location are changed to use the time zone of the default location. However, the Enhanced Interaction Administrator Change Log does not log this change to the user records.
		If the time zone for the default location is changed, the Enhanced Interaction Administrator Change Log does not log this change to the users that use the default location.
Password Policy	Users\[USER]\Password Policies	If a user is configured to use a password policy, and that password policy is deleted, the Enhanced Interaction Administrator Change Log does not log that

		the password policy has been removed from the user. If a role is configured to use a password policy, and that password policy is deleted, the Enhanced Interaction Administrator Change Log does not log that the password policy has been removed from the role.
Roles	Users\[USER]\Role	If a user is configured to use a role, and that role is deleted, the Enhanced Interaction Change Log logs that the role was deleted. It does not, however, log the change to the user's configuration. If a workgroup is configured to use a role, and that role is deleted, the Enhanced Interaction Change Log logs that the role was deleted. It does not, however, log the change to the workgroup's configuration.
Secure Input Forms	Workgroups\[WORKGROUP]\SecureInputForms	If a workgroup is configured to use a secure input form, and that form is deleted, the Enhanced Interaction Change Log does not log that the form was deleted. It also does not log

		the change to the workgroup's configuration.
Actions	Users\[USER]\Call Disconnected Users\[USER]\Call Offering	If an action is deleted, the Enhanced Interaction Change Log does not log the deletion of that action. In addition, if that action is configured as either an alerting or disconnected action for a user, the Enhanced Interaction Change Log does not log the change to the user's configuration.
Wrap-up Codes	Workgroups\[WORKGROUP]\Wrap-up Codes	If a workgroup is configured to use a wrap-up code, and that wrap-up code is deleted, the Enhanced Interaction Change Log does not log the deletion of the wrap-up code or the change to the workgroup's configuration.
Client Configuration	Users\[USER]\Client Configuration Template	If a client configuration template is deleted, the Enhanced Interaction Change Log logs the deletion. However, if a user is configured to use that template, the Enhanced Interaction Log does not log the change to the user's configuration.

On Hold Music	Workgroups\[WORKGROUP]\Workgroup On Hold Music	If an audio source is deleted, the Enhanced Interaction Change Log logs the deletion. However, if the audio source is configured as the on hold music for a workgroup, the Enhanced Interaction Change Log does not log the change to the workgroup's configuration.

Back to the top of the section

Related topics

About the Enhanced Interaction Administrator Change Log

Accumulators

Accumulator

Accumulators are generic, on-the-fly, global variables. The accumulator tools in Interaction Designer create and modify the way accumulators behave and the types of information they accumulate. Accumulators provide a place to store a value. For example, they provide a way for someone to gather (accumulate) a total number of calls. While values in handler variables are lost when the handler stops running, accumulator values are stored in the system and retain values across handlers.

Related topics

Accumulator configuration

Accumulator configuration

Accumulators are similar to system registers. They count events as they occur in Interaction Processor. Instances of these events are stored in variables and are accessible in report logs or other handlers using the Accumulator tools in Interaction Designer.

Use this configuration page to define characteristics for each accumulator on the CIC server. When you create a new accumulator, be sure to assign it to the server on the Server Configuration - Accumulators dialog box. Handlers built with the Accumulator tools in Interaction Designer must use the accumulator names defined on this page.

Data Type

The data type specifies the type of data that held in this accumulator. Select one of the available types based on the kind of data to accumulate. Data types include:

Data Type	Description
Boolean	True or false
DateTime	The year, month, day, hour, minute, and second.
Integer	Any positive or negative non-decimal number including zero. Includes all whole numbers.
Numeric	Any positive whole or decimal number including zero. Includes all real numbers.
String	Any sequence of alpha-numeric characters.

Instance Type

Accumulator handlers create and modify instances of the data stored in the accumulator (see the Set Acc. tools in Interaction Designer). The accumulator specifies what kind of instances it can store. Select one of the following instance types.

Instance Type	Description
Any Instance	Allows the Accumulator handler to insert any instance (of the correct data type) into the accumulator. No Instance List is necessary. This is the least restrictive option; use it when accumulating values for an indeterminate list (for example, all CIC users referenced by UserID as a Value in the Set Acc. accumulator tool). This is similar to a predefined dynamic array.
Fixed List	The only instances captured by the accumulator are specified in the Instance List (for example, NewIncomingCall, NewOutgoingCall). Use this to capture a fixed set of values of a specific data type.
Single Instance	The accumulator captures only one specific instance of a value, which is specified in the Instance List (for example, CallOnHold).

Instance List

Use the **Instance List** to define one or more instance names if the instance type is either fixed list or single instance. The developer who creates accumulator steps in a handler uses these instance names in the Interaction Designer. For example, to accumulate a call attribute for a specific list of three CIC user accounts, specify the three user names in the instance list, one entry for each name.

> To create an instance name, click **Add** and type a name in the **Entry Name** dialog box.
>
> To delete an instance name, select the name and click **Delete**.
>
> **Note**: When a new accumulator instance is created, it must be deactivated and reactivated in Interaction Administrator --> Server Configuration --> Accumulators in order to use it. It this is not done, a warning message is displayed.

Active

Select the **Active** check box to activate this accumulator in CIC, assuming you added it to the list of Currently Selected Accumulators in the Server Configuration - Accumulators dialog box. Once you select the check box and click **OK**, the accumulator is immediately available to collect data. Clear the check box and the accumulator stops accepting data.

> **Note:** A newly-defined accumulator immediately appears in the list of **Available Accumulators** in Server Configuration. **You must move this newly defined accumulator to the list of Currently Selected Accumulators before you can activate it with the Active check box.**

Related topics

Accumulators

System Parameters

System Parameter Configuration

Type a value for the system parameter.

Parameters are like macro names that can be included as a variable in a handler step, a path to a report, and so on. When the handler runs or the report is generated, the parameter is expanded and its value is used in the process.

> **Note**: Parameters can have either a server-level scope which is known as a server parameter, or parameters can have a system-wide (for example, enterprise) scope which is known as a system parameter. Their names and configuration are otherwise identical. Server parameters are available only on a particular IC server and system parameters are available on all IC servers on a network. For example, server parameter values could include a valid directory path, a DLL file name, a database name, and so on. A system parameter might contain a corporate phone number or some other enterprise-wide value referenced by handlers on multiple servers.

Using Parameters

If you use multiple references to the content of a particular directory whose location may change, or if you use multiple references to some other value that may change, you should probably define a server or system parameter. Using a parameter in such cases allows you to change the value in one location (where the parameter is defined) instead of looking for and changing all locations of the value.

> For example, suppose a few handlers and a configuration attribute need to reference the directory containing report files. Create a server parameter named ReportsPath whose value is, for example, D:\EIC\Reports\. Then, wherever you need to refer to the contents of that directory, specify the

> name ${ReportsPath} instead of the physical directory name. Such references work in Interaction Administrator fields.
>
> **Note:** Parameters containing directory paths (for example, ServerReportLogOutputPath) are not updated, nor are they recognized immediately, when you change a path. To update these values, you must restart CIC.

Packaged System Parameters

CIC includes a few pre-configured system parameters that are used in the default handlers and by a few modules on the CIC server.

The pre-configured system parameters include:

System Parameter	Purpose
ClientReportLogEICDataSourceName	Specifies the CIC data source name Interaction Reporting uses when running reports on CIC report logs. The CIC data source references an ODBC Data Source Name (DSN) that points to the SQL Server database containing the report log data. This scheme allows you to change the report log database type In the future without having to change the Interaction Reporting interface. Report logs are stored in SQL Server tables on the CIC server or on a separate server on the network.
Use Old TUI	Users that are assigned the Interaction Mobile Office role are speech-enabled TUI users, and users that are not assigned the Interaction Mobile Office role are DTMF-only TUI users. If you want DTMF-only users to use the old (original) DTMF TUI instead of the new DTMF TUI, you can change the value of the new **Use Old TUI** system parameter. The first time any DTMF-only user (a user not assigned the Interaction Mobile Office role) logs into the TUI, CIC creates the **Use Old TUI** parameter, and sets the value to **False**, meaning all DTMF-only users will use the new DTMF TUI. If you set the system parameter value to **True**, all DTMF-only users will use the old DTMF TUI with customizations available only with handler modifications. **Note**: The Use Old TUI system parameter applies only to users that have not been assigned Interaction Mobile Office role. Any users who are assigned the Interaction Mobile Office role will have the new speech-enabled TUI, regardless of the value of the system parameter. For more information on this parameter, see the *System Administration Guide*.

Status Messages

Add a status message

To add a status message to the My Status list in Interaction Client

1. In the **System Configuration** container, double-click the **Status Messages** subcontainer.
2. Click **New**.
3. Type the name of the new status message entry, and then click **OK**.
   The **Status Message Configuration** dialog box appears.
4. In the **Status Message** box, type the message text you want to appear in the CIC clients on the **My Status** list.
5. In the **Status Icon** box, type the full path and file name with an .ICO extension. This is the icon that will appear next to the status message.
6. In the **Status Group** list, select a name that most closely describes or categorizes the status message.
7. Depending on your configuration, additional fields may appear that allow you to map the CIC status messages to the status messages in other systems. Select the appropriate options from these fields.
8. Select all of the status attribute boxes that apply to the new status message. The status attribute boxes define the behavior of CIC clients when the status is activated. For more information about the status attributes, see *Configuration*.

> **Note:** While you can select any combination of attributes, choose them carefully. Some combinations do not make sense.

9. Click **OK**.
   The new status message immediately appears in the **Status Messages** container in Interaction Administrator and in **My Status** in the CIC clients.

To have CIC play the status message as a DND (not available) prompt when a CIC client has that status set, record a prompt with this message and then modify the CustomIVRSetUserStatus handler in Interaction Designer by adding the new prompt. See *Queue Announcements* for more information.

Related topics

Overview of status messages

Multi-Language Support

Queue Announcements

Add a status message

To add a status message to the My Status list in Interaction Client

1. In the **System Configuration** container, double-click the **Status Messages** subcontainer.
2. Click **New**.
3. Type the name of the new status message entry, and then click **OK**.
   The **Status Message Configuration** dialog box appears.
4. In the **Status Message** box, type the message text you want to appear in the CIC clients on the **My Status** list.
5. In the **Status Icon** box, type the full path and file name with an .ICO extension. This is the icon that will appear next to the status message.
6. In the **Status Group** list, select a name that most closely describes or categorizes the status message.
7. Depending on your configuration, additional fields may appear that allow you to map the CIC status messages to the status messages in other systems. Select the appropriate options from these fields.
8. Select all of the status attribute boxes that apply to the new status message. The status attribute boxes define the behavior of CIC clients when the status is activated. For more information about the status attributes, see *Configuration*.

> **Note:** While you can select any combination of attributes, choose them carefully. Some combinations do not make sense.

9. Click **OK**.
   The new status message immediately appears in the **Status Messages** container in Interaction Administrator and in **My Status** in the CIC clients.

To have CIC play the status message as a DND (not available) prompt when a CIC client has that status set, record a prompt with this message and then modify the CustomIVRSetUserStatus handler in Interaction Designer by adding the new prompt. See *Queue Announcements* for more information.

Related topics

Overview of status messages

Multi-Language Support

Queue Announcements

Status message name

Type the name of a status message to appear in the My Status list in the CIC clients.

Status Message Configuration

Status Message

Type the message text to appear on the CIC clients' My Status list. For example, "On Vacation".

Localized Message

If the appropriately localized language is supported, the value of the localized status message is displayed.

Status Icon

Select a path, parameter, or type a full path and file name with an .ICO extension that contains an icon representing the status message. The directory that contains the default CIC status icon files is **\\[IC server]\Resources** where Server is the name of your CIC server computer. Status message icons should be 32 x 32 and 16 colors.

Status Group

Select a status group that most closely describes or categorizes the status message. The status data is grouped, by default, in one of the five initial status groups. If necessary, you can create a new status group by typing a name in the list box field. The Agent Activity Log (report log ID 80) logs all user status changes and provides data for user and supervisor reports based on these status changes.

To use a newly created status group in a report, you must:

- Type a new Status Group name in the list box field for a status message. CIC starts logging data for this status with the new group name as soon as the change is saved.
- Add references to the custom column in Agent Activity Log to any appropriate reports.

Status is Do Not Disturb

Select this check box if the status should indicate the user is unavailable or should not be interrupted. When a CIC client user selects a status with the Do Not Disturb attribute set, no calls are sent to that user's station until the status changes to a non-DND status. When CIC detects a DND (Do Not Disturb) status, callers are typically directed to the user's voicemail or given other options, according to the SystemIVR handler.

Clear the **Status is Do Not Disturb** check box if the status indicates the user is available to receive calls.

> **Note:** If the user has selected a status in a CIC client with a Do Not Disturb attribute and has selected the Activate Out of Office Message check box, the caller will hear the user's Out of Office message. See Queue Announcements for more information.

Status has Date

Select this check box if the status message should indicate an ending date, typically used when the Status is Do Not Disturb attribute is set. When a CIC client user selects a status with a date attribute set (for example, Out of town), an "Ending date for current status" field appears beside the status message. If the user types an ending date, callers are told the person is unavailable until the specified date.

Clear the **Status has Date** check box if the status indicates the user is available to take calls.

Status has Time

Select this check box if the status message should indicate an ending time and the Status is Do Not Disturb attribute is selected. When an Interaction Client user selects a status with a time attribute set (for example, Out to lunch), an "Ending time for current status" field appears beside the status message. If the user types an ending time, callers are told the person is unavailable until the specified time.

Clear the **Status has Time** check box if the status indicates the user is available to take calls.

Status is Forward

Select this check box if the status message indicates the user is available at a different phone number. If a CIC client user sets a status with this attribute selected, CIC checks for a forwarding number and dials it to complete the incoming call. Users must provide a forwarding phone number for CIC to forward calls based on this status. Users can set forwarding numbers on the Incoming Calls tab of the Configuration page in Interaction Client, or remotely using Interaction Mail.

Status is Allow Follow Up

Select this check box if the status message indicates that an agent's status can change to "Follow Up" after an ACD call terminates. For example, in an ACD environment, the "Available" status message may have the Status allows ACD Calls attribute set. If the Status is Allow Follow Up attribute is also set, then the agent's status will automatically change to a "Follow Up" status after every ACD call terminates.

> **Note:** If this check box is clear, terminating ACD calls does not automatically change the agent's status to Follow Up.

Status is User Selectable

Select this check box if the user can select the status message from the CIC client interface or the system tray icon.

If this check box is clear, the status is grayed out or not available for selection by users. It implies the status is set only by CIC using handlers.

Status allows ACD Calls

Select this check box if the status message indicates an agent is available to receive calls from both ACD queues and non-ACD queues. For information on how calls are placed to ACD queues, see *Workgroup Configuration*.

Status is Persistent

Select this check box if the status message can persist when the agent logs out of CIC (for example, exits a CIC client). For example, status messages like "On Vacation" should have this attribute.

Clear this check box if the status should not persist after a user logs out of CIC while the status is selected. If a user logs out of CIC with such a status, the user's status is automatically set to the last persistent status message used.

> **Note**: In Interaction Administrator, you can change an agent's current status to another status only if the current status is persistent.

Status is ACW (After Call Work)

Select this check box if the status message indicates an agent is in a "Follow Up" mode after an ACD call. An agent's time is counted as logged in for ACD calls while the status with this attribute is selected. An ACW status is generally also a DND status, but that can be configured on this page.

Clear this check box if the status is not a follow-up status for ACD calls. You cannot configure a message as both ACW and Persistent. They are mutually exclusive. A warning dialog appears if you try.

Status and Personal prompts

The following table shows you when a caller would hear the user's personal prompts.

Personal Prompt	Is played when:
Name	A caller dials a user's extension, or dials by name, the caller hears the user's **Name** prompt.
No Answer	The caller hears the user's **No Answer** prompt when the user is Available but doesn't answer the phone.
Out of the Office	When the user has selected a status with a **Do Not Disturb** attribute and checked the **Activate Out of Office Message** box, the caller hears the **Out of the Office** message. **Note** If the Activate Out of the Office Message box is not selected, the CIC client directs the call to the user's voicemail or to other options.
Agent Greeting	A caller in an ACD queue assigned to the user hears the user's **Agent Greeting** prompt for up to 10 seconds before the user answers the call.

Related topics

Overview of status messages

Add a status message

Workgroup Configuration

Multi-Language Support

Multi-Language Support

Multi-language support refers to the translation of data that are displayed in the CIC clients, and in reports, in a language appropriate to the login locale you specified created during setup.

If the appropriately localized language is not supported, the values are displayed in the default language.

> **Note**: Languages available depend on the language installed by the add-on language install. An error message is displayed if the selected language is not installed.

Parameters

The **Multi-Language Support** tab contains three parameters: **Attribute**, **Language**, and **Value**.

Parameter	Definition
Attribute	The name of the value to be translated. Translation is elected for only a few values that are displayed in reports or status messages
Language	The language used for the translation. The default language is that currently set by the administrator. A list of 100 + additional languages appears in the **Languages** dialog when you click **Add Language**. This value is **Default** if no language is specified for your login country in the **Languages** list.
Value	The value to display; the translated value.

Buttons

The Multi-Language Support tab also contains the buttons: **Edit Value**, **Add Language**, and **Remove Language**. This is the function they perform:

- Edit Value
- Add Language
- Remove Language

For more information on the function of the scroll buttons and the **Confirm auto-save** check box, see Interaction Administrator Interface.

Related topics

Overview of status messages

Add a status message

Configuration

Actions

Actions

Configuring actions is a way for two Windows programs to share data or send commands to each other. Actions can be thought of as a direct communications link between two application programs. In CIC, the CIC clients can function with other applications as a client and a server application.

Action Names

Use this page to enter the action name and select the type of action.

Name:

Enter a descriptive name for an action (for example, Start Call DB, Stop Call DB, and so on). If you use a Force and a non-Force version of the commands, it may be helpful to name the commands accordingly. This name appears as an Alerting Action, Disconnected Action, or a Transfer Action.

Type:

Select the type of action from the drop-down list. The options are 'DDE', 'Custom Screen Pop', and 'Web Browser Screen Pop'.

Action Configuration

Each action must specify the required action protocol components in the following fields. Click here for an example procedure.

Executable

Type the name of the server application's executable file (for example, C:\Windows\MSOffice\Word.exe).

Application

Type the name of the server application, which is generally the name of the executable without the .EXE extension (for example, Word)

Topic

Type the name of the server application topic (also called the action item name) that specifies the exact group or category of data to use (for example, a bookmark, TOC, System, and so on).

Command List

Add one or more action commands that direct the server application to the desired point for the user or ACD agent. This action will not work unless you enter at least one command for this action. The order in which the commands appear in this list is significant. Commands are executed in order from the top to the bottom of the list.

To add a command, click the **Add** button and type the name of the command in the list. After you enter all of the commands for this action, use the **Up** and **Down** buttons to arrange the order of execution, starting at the top of the list.

Add

Click **Add** to enter each new command in the Command List box. Each command must be on its own line. Click **OK** to complete the entry.

Edit

Select a command in the list and click **Edit** to change the command. Click **OK** to save the edits.

Delete

Select one or more commands in the list and click **Delete** to remove one or more commands from the list.

Up

Select a command in the list and click **Up** to move the command higher in the order of execution.

Down

Select a command in the list and click **Down** to move the command lower in the order of execution.

> **Note:** You must restart the CIC client for any changes to Actions to take effect.

Custom Screen Pop Configuration

Screen Pop configuration allows you to pop open a third party application screen to perform an action. This screen design provides information about the screen to the .NET plug-in.

Screen Pop Type

Enter a unique name for the screen pop type.

Input Values

This section displays the name and associated default value of the inputs. Click Add... to add a new input value for this screen pop action. Click **Edit...** to change an existing input, or click **Remove** to delete an input.

Web Browser Screen Pop

Web Browser Screen Pop configuration allows you to open your browser to a specific location or URL on a specific event. For example, on an incoming call, your browser can open to web page.

URL

Enter a URL to open in the browser. Use the http:// format. For example, use http://my.yahoo.com/. To pass a specific parameter to the URL, click Insert a URL parameter into the URL string.

Popup Type

Select **Pop to a new browser (only supported in Internet Explorer and Firefox)** to open the URL in a new browser instance. Select **Pop to a new tab on an existing browser session** to open the URL in a new page or tab in a currently opened browser.

URL Parameters

This is a list of parameters that are being passed to the URL. Click **Edit...** to change an existing parameter.

> **Note:** CIC encodes the URL parameters. Therefore, put special characters, such as "=," in the URL field and not in the values of the URL parameters.

Command Entries

Type an actual command associated with this action. An action can consist of one or more commands. Each command must be on its own line in the Command Entry field. Use the Add button to add each command on its own line. Since the top to bottom order of the commands in this list determines the order in which the commands are executed, use the Up and Down buttons to arrange the order in the list.

Request commands (that is, commands initiated from a client application to the CIC server) can be:

- Called by a specific function in the client application
- Called by a generic execute function in the client application

If a specific function is used in a command, type the function name followed by the requested CIC attributes. For example:

```
MyFunction($(CallID),$(LineName),$(StationName))
```

If a client application requests CIC attributes (that is, not using a unique function), you can type just the CIC attributes to return. For example:

```
$(CallID),$(LineName),$(StationName)
```

Log Retrieval Assistant (LRA)

Log Retrieval Assistant

Log Retrieval Assistant (LRA) is a feature that allows support organizations and certified partners to configure logging and retrieve logs from CIC servers at specific times.

Use the **Log Retrieval Assistant Configuration** dialog box to configure the following items:

- Company
- Email
- Firewall
- FTP

LRA Company Configuration

Use this page to configure your organization information.

Organization

This is the name of your company you entered in the Company Name field. This name identifies your organization in the master database and in email messages sent by LRA at your site.

LRA Monitored Mailbox

This field shows the display name of the email account on the customer site that LRA monitors to pick up requests. Log requests are mailed to this account for processing by LRA.

SMTP Address for LRA's Monitored Mailbox

This is the SMTP address for the monitored mailbox. For example, you would enter "i3recorder@dev2000.com".

Work Directory

This required field stores the fully qualified path to a working directory where log files are compressed (zipped) prior to FTP transfer. If for some reason the FTP process fails, log files will persist in this location until a subsequent FTP attempt is successful, or until files are manually deleted. The logs directory [drive]:\[server name]\IC\Logs (or \\IC\Logs) is used by default.

Off-Peak Begin and Off-Peak End

These fields indicate a block of time when the CIC server is not at peak utilization. Deferred log retrieval requests are executed during this period to minimize impact on the server.

Standard Slowdown and Off-Peak Slowdown

You can set "slowdown factors" that limit the amount of CPU and network bandwidth that LRA can consume. Throttling forces CPU-intensive processes such as snipping, zipping, FTP, etc. to sleep intermittently so that LRA does not degrade the overall performance of the CIC system.

LRA runs at normal speed when the slowdown factor is 1. It runs at half speed (and consumes half the resources) when the slowdown factor is 2. A factor of 4 means LRA is operating at one-quarter speed with a corresponding decrease in system resources used. This factor applies to requests processed during normal hours and must be between 1 and 100.

Different slowdown factors can be set for peak-time and non-peak times. For example, you might set the slowdown factor to 2 during business hours, and allow LRA to run at normal speed during non-peak hours.

Defer By Default

Check this option to defer all LRA requests until off-peak hours. In an emergency, support personnel can override this setting on a per-request basis, meaning that they can flag a request to be processed immediately.

LRA Email Configuration

Use this page to configure email settings for LRA.

Send Status Email To

Status messages are sent to recipients listed in this field. LRA sends status emails when jobs start and finish. Leave this field blank if you do not want to receive status emails.

Send Error Email To

In the event that an error occurs, LRA will send an error notification message to the recipients listed in this field. Leave this field blank if you do not want to receive error notification emails.

LRA Firewall Configuration

Use this page to configure firewall settings for LRA.

IP Address

If your CIC server is behind a firewall, you must specify additional information that allows outbound payloads and data to pass through the firewall. Contact your local network administrator to find out if your CIC server is behind a firewall. This person can help you complete Firewall type, FTP Passive Mode, Firewall address, FTP Port, Id, and Password fields. Firewall Address is the host name (or IP address) of the firewall.

Port

This number identifies the port used by FTP to pass data through firewalls. Contact your local network administrator to find out which port on the firewall is opened to FTP traffic.

Username

This field stores the User Id needed to pass data through the firewall. It is likely that you will need to contact your local network administrator to obtain this information.

Password

This field stores the password for the Username specified above.

Type

This field identifies the type of firewall used. The choices are None, Socks4 or Socks5. Socks4 is a protocol that relays TCP sessions at a firewall host to allow application users transparent access across the firewall.

Socks5 does the same thing, except that it also resolves issues that Socks4 does not fully address or omitted. Socks5 provides strong authentication, authentication method negotiation, address resolution proxy, and other features.

Sensitive information about your firewall, such as ID and password information, is never transmitted to a remote server or passed to a remote database. LRA uses firewall configuration information to transmit outbound data through the firewall. The firewall Id and password is stored locally in a configuration (.cfg) file in the server\LRA directory so that LRA can retrieve it. If this poses an unacceptable security risk, you should deny user access to the \server\LRA folder.

LRA FTP Configuration

Use this page to enable or disable FTP configuration settings for LRA.

Use Passive Mode

This check box determines whether FTP operations will be performed in passive or active FTP mode. Passive mode allows FTP operations to pass data through certain types of firewalls that would not otherwise allow the flow of data. Check with your local network administrator to find out if your firewall requires passive FTP. Passive FTP mode is the default.

Auto Send

This check box determines whether requested data is automatically FTP'd from the customer site to the requester's FTP site. When checked, the I3LRAU server process FTP's zip files as soon as it finishes staging them in the working directory. When this option is unchecked, zip files remain in the working directory until they are manually FTP'd to the requester by the customer. As a rule of thumb, you should leave this option checked unless you wish to inhibit all LRA-related file transfers for some reason.

When Autosend is unchecked, LRA extracts logs and zips them, but does not do anything else. Customers must use an Internet FTP utility (e.g. WSFTP or equivalent) to manually transfer zip files to the Product Information site.

Mail

Overview of Mail

You use the **Mail** container to define mail storage sources, such as voice mail stored on the server (file-based mail), Microsoft Exchange, IBM Notes, Groupwise, LDAP, and IMAP4/SMTP-compliant mail servers, such as SunOne (formerly iPlanet).

Some of the mail features that you can configure are prefixes, message thresholds and compression, directories, transports, and providers.

> **Note:** If you configured your email providers when you ran IC Setup Assistant, then you can use the **Mail** container to change those settings. You cannot re-run IC Setup Assistant to make mail configuration changes.

Related topics

Configure mail storage sources

Configure a mail storage source

To configure a mail storage source

1. In the **System Configuration** container, click the **Mail** subcontainer.
2. In the view pane, double-click **Configuration**.
3. In the **Mail Configuration** dialog box, complete the tabs. See the links under *Related topics* for complete information.
4. Click **OK**.

Related topics

Providers

Directories

Transports

Prefixes and Voicemail

Options

Monitored Mailboxes

Attendant Mailboxes

Providers

Providers

Use this page to set the properties, enable, or disable available email providers.

Properties

Highlight the mail provider and click **Properties**. Depending on which provider you have selected, different settings are display. Click on the Providers listed below for more information:

- Exchange
- Notes
- Interaction Message Store
- Novell GroupWise
- LDAP
- SMTP
- IMAP
- Gmail

Enable Provider or Disable Provider

Highlight the mail provider then click **Enable Provider** or **Disable Provider** to turn on or off the provider. Again, depending on which provider you wish to enable, the system performs different functions.

If you are using Gmail, select SMTP or IMAP. For more information on using Gmail, see the *Gmail Integration Technical Reference* in the PureConnect Documentation Library.

Exchange

Overview of Exchange

Exchange enables users to retrieve appointments from their Microsoft Outlook calendars via the telephone user interface (TUI).

> **Note**: Exchange calendar access is a Interaction Mobile Office feature (available with the Interaction Mobile Office license), and is available for use only with Microsoft Exchange/Outlook.

Supported Exchange servers

Microsoft Exchange Web Services (EWS)-based integration is an officially supported CIC mail system. Microsoft Exchange Web Services is recommended as an alternative to the Microsoft Exchange MAPI-based integration. See System Software Requirements in the PureConnect Documentation Library for the latest requirements.

Requirements

- The Exchange server must be connected to the network.
- The CIC administrator permissions must be established.

Configure users to use the mailbox provider

After you configure the provider in the **Mail** container, you must also configure the CIC users to use the mailbox. For more information, see the help for *Configure a User* and the help for *Configuration* page in the **User Configuration** dialog box.

Related topics

Configure an Exchange provider

Configure domain properties for an Exchange provider

Configure a user

Configuration page in the User Configuration dialog box

Configure an Exchange provider

To configure an Exchange provider

1. In the **Mail Configuration** dialog box, click the **Providers** tab. For information on how to access the **Mail Configuration** dialog box, see *Configure a Mail storage source*.
2. In the list of providers, select Exchange.
3. Click **Enable Provider**.
4. In the **Exchange Configuration** dialog box, in the **Host** box, type the URL of the Exchange server that runs the calendar service, in the “http://ServerName” format. If you plan to use SSL/TLS, use “https://ServerName” format.

> **Note**: Point to the Exchange 2010 server acting in the Client Access role.

5. In the **User** box, type an administrative user account name (CIC administrator account) that has "Receive As" rights on the Exchange server. The field should contain the domain and username (domain\username).
6. In the **Password** box, type the password for the user ID.
7. In the **Confirm** box, re-type the password for the user ID.
8. Select **Enable Exchange Web Services**. Clear **Enable MAPI**. Exchange MAPI is no longer supported.

9. To specify an Exchange server in addition to the default Exchange server, click **Add** and continue with *Configure domain properties*.

> **Note**: If you do not specify the domain to use to access mailboxes, CIC connects to the default Exchange server. That is, Exchange Web Services will try to use the CIC service account's mailbox for autodiscovery and impersonation over other mailboxes for message retrieval and queuing. If you want to use another Exchange server in addition to the default Exchange server to access mailboxes, you must specify the domain to use for the default Exchange server and the domain to use for the additional Exchange server.

10. Click **OK**.

Related topics

Configure a Mail storage source

Configure domain properties for an Exchange provider

Configure domain properties for an Exchange provider

To configure domain properties for an Exchange provider

1. In the **Service account email address** box, type the email address that is used to access mailboxes.
2. To use the CIC Administrator account credentials to access mailboxes, select the **Use IC Administrator account credentials** option. Otherwise, skip to step 7.
3. To use another account's credentials to access mailboxes, select the **Use the following credentials** option. Then complete steps 4, 5, and 6.
4. In the **User name** box, type an administrative user account name (CIC administrator account) that has impersonation rights on the Exchange server. For network credentials, type the domain and user name (domain\username). For Web credentials, type the account name @ domain (username@domain).
5. In the **Password** box, type the password for the account.
6. In the **Confirm password** box, re-type the password for the account.
7. To use OAuth to authenticate with Exchange, under **Use OAuth**, enter the certificate, certificate password, and the application ID that were generated during the application registration in the Microsoft Azure portal to request an access token that is passed during requests to Exchange.
8. To use the Exchange Autodiscover feature to identify the Exchange Web Services URL, select the **Autodiscover to get the Exchange Web Services URL** option.

> **Note**: The Autodiscover process can be time-consuming. As an alternative, manually specify the Exchange Web Services URL, as described in step 8.

9. To manually specify the Exchange Web Services URL, select the **Use this Service URL** option. Then type the Service URL in the corresponding box.

10. If Exchange information is not stored in Active Directory, using SCP lookup during the autodiscover process to find service endpoints will result in unnecessary delays. To disable this the SCP lookup, deselect the **Enable SCP Lookup** check box.

11. In the **Seconds before timeout** box, type the number of seconds that CIC should attempt to contact the Exchange server.

12. Click **OK**.

Related topics

Configure an Exchange provider

Notes

Overview of Notes

Requirements

- IBM Domino server must be connected to the network.
- You must establish the CIC administrator mail profiles.
- IBM Notes client must be installed on the CIC server.

Configure users to use the mailbox provider

After you configure the provider in the **Mail** container, you must also configure the CIC users to use the mailbox. For more information, see the help for *Configure a User* and the help for *Configuration* page in the **User Configuration** dialog box.

Related topics

Configure a Notes provider

Configure a user

Configuration page in the User Configuration dialog box

Configure a Notes provider

To configure a Notes provider

1. In the **Mail Configuration** dialog box, click the **Providers** tab. For information on how to access the **Mail Configuration** dialog box, see *Configure a Mail storage source*.
2. In the list of providers, select Notes.
3. Click **Enable Provider**.

4. In the **Notes Configuration** dialog box, in the **Password** box, type the CIC administrator's IBM Domino password. It should be the same password used to log into the Domino server when IBM Notes is started. (It is not the Windows domain or CIC password.)
5. In the **Confirm** box, re-type the password.

> **Note**: If you used IC Setup Assistant to configure your Notes provider, the IC Setup Assistant verified that you typed the same password in both fields. However, it did not authenticate the password with the IBM Domino server. For more information, see the *Installation and Configuration Guide* in the PureConnect Documentation Library on the CIC server.

6. To filter voice mails and faxes with a database filter, select the **Use Database Search** option. This option provides a significant performance improvement when a user accesses a mailbox via the TUI. However, it is recommended that you also select the **Use Folder References** option. Together, these options limit the voice mails and faxes to the user's inbox (or other selected folder). If you select only the Use Database Search option, then all of voice mails and faxes for the entire mail database appear.
7. To apply a filter that includes a reference to the currently selected folder to the mail database, select the **Use Folder References** option.

> **Note:** In order this feature to work, the IBM Domino administrator must enable folder references on the IBM Domino server(s) for the mail database of each CIC user.
>
> If you select both the **Use Database Search** option and the **Use Folder References** option, but do not enable folder references, then no voice mails or faxes may be returned. After you select the **Use Folder References** option, the only voice mails and faxes returned are those remaining after folder references have been enabled. For more information, see the *PureConnect Installation and Configuration Guide* in the PureConnect Documentation Library on the CIC server.

Related topics

Configure a Mail storage source

Notes requirements

Interaction Message Store

Overview of Interaction Message Store

Interaction Message Store is a messaging option that provides storing and tracking capabilities for voice mail and fax messages without connection to an email system.

Interaction Message Store stores voice mail and faxes as files on the CIC server (small implementations) or a network file server (large implementations). Users are associated with mailboxes in a file directory structure, and voice mails and faxes are routed to these mailboxes. CIC users can access voice mail messages from the CIC clients or the telephone user interface (TUI). From the CIC clients, a user can view a fax message and forward it to another fax number.

Configure users to use the mailbox provider

After you configure the provider in the **Mail** container, you must also configure the CIC users to use the mailbox. For more information, see the help for *Configure a User* and the help for *Configuration* page in the **User Configuration** dialog box.

Related topics

Configure Interaction Message Store

Configure Interaction Message Store mailboxes

Configure a user

Configuration page in the User Configuration dialog box

Configure Interaction Message Store

To configure Interaction Message Store

1. In the **Mail Configuration** dialog box, click the **Providers** tab. For information on how to access the **Mail Configuration** dialog box, see *Configure a Mail storage source*.
2. In the list of providers, select Interaction Message Store.
3. Click **Enable Provider**.
   The **Interaction Message Store** dialog box appears. CIC confirms the **Root Directory** location for message storage. The default root directory is \\[server name]\IC\FBMC.
   When the Interaction Message Store is not located on the CIC server, use one of the following to specify the Message Store Path:

- UNC Path Using a DNS resolved host

  Example: \\fileserver\FBMC

- UNC Path Using an IP address for the host - **Note:** This method is preferred as it removes a potential point of failure (DNS resolution)**.**

  Example: \\192.168.2.27\FBMC

> **Note:** Do not set the root directory to the root of the drive (for example C:\IMS). For more information, see the *Interaction Message Store Technical Reference* in the Technical Reference Documents section of the CIC Documentation Library on the CIC server.

4. To configure individual mailboxes, click **Mailboxes configuration**. For more information, see Configure Interaction Message Store mailboxes.
5. In the **Maximum Storage Space (bytes)** field, select the maximum amount of storage space, in bytes, to allocate to voice mail messages. Select No Limit if you do not want to limit the storage space for voice mail messages.

6. In the **Maximum Message Count** field, select the maximum number of messages to allocate for voice mail messages. Select **No Limit** if you do not want to limit the storage space or message count for voice mail messages.
7. Click **OK**.

Related topics

Configure a Mail storage source

Configure Interaction Message Store mailboxes

Configure Interaction Message Store mailboxes

To configure Interaction Message Store mailboxes

1. To view only unused IMS mailboxes, select the **Show Only Unused Mailboxes** checkbox.
2. To refresh the list of IMS mailboxes, click **Refresh List**.
3. To select all mailboxes, click **Select All**.
4. To delete selected mailboxes, click **Delete Mailbox**.

> **Note:** If a mailbox is still being used by another user, the mailbox will not be deleted.
>
> Valid mailbox names and address use only alpha-numerical characters. Other characters are not recognized by CIC.

Related topics

Configure Interaction Message Store

Overview to Interaction Message Store

Groupwise

Overview of GroupWise

Prerequisites

- GroupWise must be connected to the network.
- Create the necessary user accounts in GroupWise.
- Configure the GroupWise POA(s) for SOAP. For each GroupWise Post Office Agent (POA) that will be accessed by CIC, enable SOAP, select the SOAP port, and (optionally) enable SSL for SOAP. If you want to use SSL for SOAP, you must obtain a certificate for this POA and assign it to the POA in GroupWise. The certificate for the POA must be trusted by the CIC server.
- In the GroupWise snap-in in ConsoleOne, generate the Trusted Application Key file. Copy the Trusted Application key file to the CIC server.

Supported versions

For IC 4.0 SU 4 and later, use GroupWise 8.0 or GroupWise 2012.

Configure users to use the mailbox provider

After you configure the provider in the **Mail** container, you must also configure the CIC users to use the mailbox. For more information, see the help for *Configure a User* and the help for *Configuration* page in the **User Configuration** dialog box.

Related topics

Configure a GroupWise provider

Configure a user

Configuration page in the User Configuration dialog box

Configure a GroupWise provider

To configure a GroupWise provider

1. In the **Mail Configuration** dialog box, click the **Providers** tab. For information on how to access the **Mail Configuration** dialog box, see *Configure a Mail storage source*.
2. In the list of providers, select GroupWise.
3. Click **Enable Provider**.
4. In the **GroupWise Configuration** dialog box, in the Server box, type the name or IP address of the GroupWise server hosting the POA containing the most CIC users. While the new GroupWise Connector can connect to any POA with SOAP enabled, it is most efficient to connect to the POA that will be used the most. If the GroupWise Connector attempts to access a mailbox on a different post office than the one handled by the POA selected here, it will be redirected to the correct POA.
5. In the **Port** field, select the port value. The port value should be the same as the SOAP port for this POA, which by default is 7191. If the POA uses a different port value, select it here.
6. In the **Username** box, type the account that will be used to access the system address book and to send voice mails left by external callers. Typically, it is an account created just for use by CIC.
7. Click **Browse** to select the **GWTApp.xml** file from the appropriate CIC server directory.

   The Groupwise Connector requires that you install CIC as a Trusted Application in GroupWise. This enables CIC to automatically provide GroupWise users access to their mailboxes through email or TUI.

   If you have not yet generated the Trusted Application Key file in ConsoleOne and copied the resulting GWTApp.xml file to a directory on the CIC Server, do so now. For instructions, see the *Novell GroupWise Support for CIC Technical Reference* in the PureConnect Documentation Library.

8. To authenticate the server and encrypt subsequent communications, select **Use Secure Connections (SSL/TLS)**.

   If you are using TLS/TLS for SOAP and have obtained the certificate, assigned it to the POA, and enabled SSL for SOAP in the POA, select this option to enable SSL for SOAP in CIC. **Prerequisites**: The server certificate must be available and trusted, before **Use Secure Connections (TLS)** takes effect. For more information see *CIC Security Features* in the PureConnect Documentation Library.

> **Note**: GroupWise uses certificates stored in the Windows certificate store. The GroupWise server has to be using a certificate that has been issued by a CA (Certification Authority, like Verisign) and trusted in the Windows certificate store. If the certificate is self-signed (not issued by a CA), manually add the server's certificate to your Windows certificate store. To view certificates, run the certificate manager (certmgr.msc) from the Start menu.
>
> Examples:
>
> • The GroupWise administrator has a certificate issued from Verisign. Since Verisign shows up in certmgr.msc under Trusted Root Certification Authorities, just select **Use Secure Connections (TLS)**, and TLS is enabled.
>
> • The GroupWise administrator has a certificate issued from a certificate shop that does not have a Windows certificate store listing. Manually add the certificate to your Trusted Root Certification Authorities, then select **Use Secure Connections (TLS)**.
>
> • The GroupWise administrator created a self-signed certificate (not issued by a CA). Manually add the certificate to your Trusted Root Certification Authorities, then select **Use Secure Connections (TLS)**.

9. To enable GroupWise server tracing for troubleshooting purposes, select the **Enable GroupWise Server-side Tracing** checkbox.

> **Note:** For more information, see *Novell GroupWise Support for CIC* in the **Technical Reference Documents** section of the PureConnect Documentation Library.

10. Click **OK**.

Related topics

Configure a Mail storage source

GroupWise requirements

LDAP

Overview of LDAP, SMTP, and IMAP

LDAP is a protocol for retrieving personal information (given name, surname, address, company, and so on), SMTP is a protocol for delivering email messages, and IMAP is a protocol for retrieving email messages. LDAP, SMTP, and IMAP can all be enabled and configured independently. You can configure what is needed either when you run Setup Assistant as part of a new installation, or later in Interaction Administrator.

Examples:

- If you want delivery of voice mail messages, faxes, and CIC notification email messages (for example, “caller left a voice mail less than 2 seconds” or “you haven’t recorded your name prompt”) to email addresses (even external SMTP email addresses, such as a Hotmail account), and you want to associate users with address book entries, **then you only need to configure SMTP and LDAP**.
- If you want delivery of voice mail messages, faxes, and CIC notification email messages, but you do not want retrieval of messages (through the TUI), **then you only need to configure SMTP, not IMAP.**
- If you want retrieval of email messages through the TUI (again, even from an external IMAP account), but you do not want delivery of voice mails, faxes, and CIC notification-email messages to email addresses, **then you only need to configure IMAP, not SMTP.**

If you want users to access messages on CIC client workstations via email software in addition to or instead of the telephone, you must fulfill the following requirements:

- Establish a mail account on the IMAP server for each CIC user.
- Install IMAP-capable email software (such as Outlook Express, Windows Mail, Thunderbird, etc.) on CIC client workstations. (It is not necessary to install the email software on the CIC server.)

Configure users to use the mailbox provider

After you configure the provider in the **Mail** container, you must also configure the CIC users to use the mailbox. For more information, see the help for *Configure a User* and the help for *Configuration* page in the **User Configuration** dialog box.

Related topics

Configure an LDAP provider

Configure an LDAP directory

Configure an SMTP provider

Configure an SMTP transport

Configure an IMAP provider

Configure an IMAP server

Configure a user

Configuration page in the User Configuration dialog box

Configure an LDAP directory

To configure an LDAP directory

1. In the **Directory Name** box, type the LDAP directory name. The name entered here is arbitrary and used solely within CIC to identify this configured directory.
2. In the **Server** box, type the FQDN or IP address of the LDAP server.
3. In the **Port** box, modify the default port number if necessary. The default port number used on most LDAP servers is 389 (non-SSL) or 636 (SSL). The port number on your LDAP server may vary.
4. In the **Search Base** box, type the distinguished name of the base entry (starting point) for searches in the directory, if required. This entry can be for a country, an organization, or other type of grouping. Whether a search base is required depends on the directory server in use.
5. If the LDAP server requires authentication so that the CIC server can connect to it, select the **Requires Authentication** check box. Then enter the user name and password information.
6. Click O**K**.

Related topics

Configure an LDAP provider

Configure an LDAP provider

To configure an LDAP provider

1. In the **Mail Configuration** dialog box, click the **Providers** tab. For information on how to access the **Mail Configuration** dialog box, see *Configure a Mail storage source*.
2. In the list of providers, select LDAP.
3. Click **Enable Provider**.
4. In the **LDAP Configuration** dialog box, click **Add** to add LDAP directories. You can select an existing directory in the worksheet to edit or delete it. For more information, see *Configure an LDAP directory*.
5. In the **Timeout (seconds)** field, enter how long the CIC server should allow a search to proceed through the directory before it times out. The default timeout is 10 seconds.
6. In the **Search Limit** field, select the maximum number of matching entries the LDAP server should return when the directory is searched. The default is 1000 entries.
7. To authenticate the server and encrypt subsequent communications, select the **Use secure connections (SSL/TLS)** option.
   If you are using SSL/TLS for LDAP, select this option to enable SSL/TLS for CIC.

   Prerequisites: The server certificate must be available and trusted, before **Use Secure Connections (TLS)** takes effect. For more information see *PureConnect Security Features* in the

Technical Reference Documents section in the PureConnect Documentation Library on the CIC server.

> **Note**: LDAP uses certificates stored in the Windows certificate store. The LDAP server has to be using a certificate that has been issued by a CA (Certification Authority, like Verisign) and trusted in the Windows certificate store. If the certificate is self-signed (not issued by a CA), manually add the server's certificate to your Windows certificate store. To view certificates or manually import certificates in the Windows certificate store, run the certificate manager (certmgr.msc) from the Start menu.
>
> Examples:
>
> • The LDAP administrator has a certificate issued from Verisign. Since Verisign shows up in certmgr.msc under Trusted Root Certification Authorities, just select **Use Secure Connections (TLS)**, and TLS is enabled.
>
> • The LDAP administrator has a certificate issued from a certificate shop that does not have a Windows certificate store listing. Manually add the certificate to your Trusted Root Certification Authorities, then select **Use Secure Connections (TLS)**.
>
> • The LDAP administrator created a self-signed certificate (not issued by a CA). Manually add the certificate to your Trusted Root Certification Authorities, then select **Use Secure Connections (TLS)**.

8. Click **OK**.

Related topics

Configure a Mail storage source

Overview to LDAP SMTP and IMAP

Configure an LDAP directory

SMTP

Overview of LDAP, SMTP, and IMAP

LDAP is a protocol for retrieving personal information (given name, surname, address, company, and so on), SMTP is a protocol for delivering email messages, and IMAP is a protocol for retrieving email messages. LDAP, SMTP, and IMAP can all be enabled and configured independently. You can configure what is needed either when you run Setup Assistant as part of a new installation, or later in Interaction Administrator.

Examples:

- If you want delivery of voice mail messages, faxes, and CIC notification email messages (for example, "caller left a voice mail less than 2 seconds" or "you haven't recorded your name prompt") to email addresses (even external SMTP email addresses, such as a Hotmail account), and you want to associate users with address book entries, **then you only need to configure SMTP and LDAP**.

- If you want delivery of voice mail messages, faxes, and CIC notification email messages, but you do not want retrieval of messages (through the TUI), **then you only need to configure SMTP, not IMAP.**
- If you want retrieval of email messages through the TUI (again, even from an external IMAP account), but you do not want delivery of voice mails, faxes, and CIC notification-email messages to email addresses, **then you only need to configure IMAP, not SMTP.**

If you want users to access messages on CIC client workstations via email software in addition to or instead of the telephone, you must fulfill the following requirements:

- Establish a mail account on the IMAP server for each CIC user.
- Install IMAP-capable email software (such as Outlook Express, Windows Mail, Thunderbird, etc.) on CIC client workstations. (It is not necessary to install the email software on the CIC server.)

Configure users to use the mailbox provider

After you configure the provider in the **Mail** container, you must also configure the CIC users to use the mailbox. For more information, see the help for *Configure a User* and the help for *Configuration* page in the **User Configuration** dialog box.

Related topics

Configure an LDAP provider

Configure an LDAP directory

Configure an SMTP provider

Configure an SMTP transport

Configure an IMAP provider

Configure an IMAP server

Configure a user

Configuration page in the User Configuration dialog box

Configure an SMTP provider

To configure an SMTP provider

1. In the **Mail Configuration** dialog box, click the **Providers** tab. For information on how to access the **Mail Configuration** dialog box, see *Configure a Mail storage source*.
2. In the list of providers, select SMTP.
3. Click **Enable Provider**.
4. In the **SMTP Configuration** dialog box, click **Add** to add SMTP transports. You can select an existing transport in the worksheet to edit or delete it. For more information, see *Configure an SMTP transport*.

5. In the **Default Sender** box, type the email address of the default sender. The default sender is used for messages in which a sender has not been explicitly specified.

6. In the **Timeout** (seconds) list, specify how long the CIC server should wait for a response from the SMTP server before abandoning an attempt to send an email message. The default timeout is 10 seconds.

7. To authenticate the server and encrypt subsequent communications, select the **Use secure connections (SSL/TLS)** option. If you are using SSL/TLS for SMTP, check this setting to enable SSL/TLS.

   Prerequisites: For TLS to be fully enabled, additional configuration is required. For more information see *PureConnect Security Features* in the **Technical Reference Documents** section in the PureConnect Documentation Library on the CIC server.

8. Click **OK**.

Related topics

Configure a Mail storage source

Add an SMTP transport

Configure an SMTP transport

To add an SMTP transport

1. In the **Transport Name** box, type the SMTP transport name. The name you type is used solely within CIC to identify this configured transport.

2. In the **Server** box, type the FQDN or IP address of the SMTP server.

3. In the **Port** box, modify the default port number if necessary. The default TCP/IP port number used on most SMTP servers is 25 (non-SSL) or 465 (SSL). The port number on your SMTP server may vary.

4. In the **Domain Serviced** box, if you want to limit the domain serviced by this transport, type the recipients' domain name. For example, if you type **example.com**, then this transport will attempt to deliver emails intended for john@example.com, but not for john@inin.com. In most cases, you leave this field blank.

> **Note**: This field is not related to the **Server** field. It simply acts as a filter for the recipient (To:) addresses that this SMTP transport serves.

5. If the SMTP server requires authentication so that the CIC server can connect to it, select the **Requires Authentication** check box. Then specify the user name and password information.

6. Click **OK**.

Related topics

Configure an SMTP provider

IMAP

Overview of LDAP, SMTP, and IMAP

LDAP is a protocol for retrieving personal information (given name, surname, address, company, and so on), SMTP is a protocol for delivering email messages, and IMAP is a protocol for retrieving email messages. LDAP, SMTP, and IMAP can all be enabled and configured independently. You can configure what is needed either when you run Setup Assistant as part of a new installation, or later in Interaction Administrator.

Examples:

- If you want delivery of voice mail messages, faxes, and CIC notification email messages (for example, “caller left a voice mail less than 2 seconds” or “you haven’t recorded your name prompt”) to email addresses (even external SMTP email addresses, such as a Hotmail account), and you want to associate users with address book entries, **then you only need to configure SMTP and LDAP**.
- If you want delivery of voice mail messages, faxes, and CIC notification email messages, but you do not want retrieval of messages (through the TUI), **then you only need to configure SMTP, not IMAP.**
- If you want retrieval of email messages through the TUI (again, even from an external IMAP account), but you do not want delivery of voice mails, faxes, and CIC notification-email messages to email addresses, **then you only need to configure IMAP, not SMTP.**

If you want users to access messages on CIC client workstations via email software in addition to or instead of the telephone, you must fulfill the following requirements:

- Establish a mail account on the IMAP server for each CIC user.
- Install IMAP-capable email software (such as Outlook Express, Windows Mail, Thunderbird, etc.) on CIC client workstations. (It is not necessary to install the email software on the CIC server.)

Configure users to use the mailbox provider

After you configure the provider in the **Mail** container, you must also configure the CIC users to use the mailbox. For more information, see the help for *Configure a User* and the help for *Configuration* page in the **User Configuration** dialog box.

Related topics

Configure an LDAP provider

Configure an LDAP directory

Configure an SMTP provider

Configure an SMTP transport

Configure an IMAP provider

Configure an IMAP server

Configure a user

Configuration page in the User Configuration dialog box

Configure an IMAP provider

Note: An IC mail account on the IMAP server is not required to configure an IMAP provider.

To configure an IMAP provider

1. In the **Mail Configuration** dialog box, click the **Providers** tab. For information on how to access the **Mail Configuration** dialog box, see *Configure a Mail storage source*.
2. In the list of providers, select IMAP.
3. Click **Enable Provider**.
4. In the **IMAP Configuration** dialog box, click **Add** to add IMAP servers. You can select an existing server in the worksheet to edit or delete it. For more information, see *Configure an IMAP server*.
5. In the **Timeout (seconds)** field, enter how long the IC server should wait for a response from the IMAP server before abandoning the attempt to receive an email message. The default timeout is 10 seconds.
6. To authenticate the server and encrypt subsequent communications, select the **Use secure connections (SSL/TLS)** option.
   If you are using SSL/TLS for IMAP, select this option to enable SSL/TLS for CIC.

   Prerequisites: For TLS to be fully enabled, additional configuration is required. For more information see *CIC Security Features* in the **Technical Reference Documents** section in the PureConnect Documentation Library on the CIC server.

Related topics

Configure a Mail storage source

Configure an IMAP server

Configure an IMAP server

To configure an IMAP server

1. In the **Name** box, type the IMAP server name. The name entered here is arbitrary and used solely within CIC to identify this configured server.
2. In the **Server** box, type the FQDN or IP address of the IMAP server.
3. In the **Port** box, modify the default port number if necessary. The default TCP/IP port number used on most IMAP servers is 143 (non-SSL) or 993 (SSL) The port number on your IMAP server may vary.
4. Select the **Supports PROXYAUTH** check box if the IMAP server supports a non-standard extension to the IMAP4rev1 protocol called PROXYAUTH. The PROXYAUTH extension enables CIC to access users’ mailboxes without having to know their IMAP passwords. To use this extension, CIC must still be able to determine the users’ IMAP logon names (either via an IMAP user account file or via the LDAP server), and CIC must also be granted the necessary privileges

on the IMAP server. Then enter the user name and password. The values will depend on the configuration of the IMAP server.

5. Click **OK**.

Related topics

Configure an IMAP provider

Gmail

Overview of Gmail

CIC provides an integration with Gmail through Google Apps for Work. To configure the Gmail integration, complete the following steps.

Configure your Gmail account

Configure your Gmail account with Google. In the Google Developer Console, create a client ID and obtain the following:

- Certificate file
- Password
- JSON file

For more information about how to configure your Gmail account with Google, see *Gmail Integration Technical Reference* in the PureConnect Documentation Library on the CIC server.

Install the Gmail integration

To install the Gmail integration, re-run the IC Setup Assistant. On the first page of the IC Setup Assistant, select the **Identity** option and then click **Proceed.**

Configure the Gmail provider and domain

In Interaction Administrator, in the **Mail** container, configure the Gmail provider and the Gmail domain(s).

Configure users to use the mailbox provider

After you configure the provider in the **Mail** container, you must also configure the CIC users to use the mailbox. For more information, see the help for *Configure a User* and the help for *Configuration* page in the **User Configuration** dialog box.

Related topics

Configure a Gmail provider

Configure a Gmail domain

Configure a user

Configuration page in the User Configuration dialog box

Configure a Gmail provider

To configure a Gmail provider

1. In the **Mail Configuration** dialog box, click the **Providers** tab. For information on how to access the **Mail Configuration** dialog box, see *Configure a Mail storage source*.
2. In the list of providers, select Gmail.
3. Click **Enable Provider**.
4. To view, add, edit, or delete domains for the provider, click **Properties**. For more information, see *Configure a Gmail domain*.

Related topics

Configure a Mail storage source

Overview of Gmail

Configure a Gmail domain

Configure a Gmail domain

In the **Gmail Configuration** dialog box, you can add, edit, and delete a domain. You can also designate a default domain to deliver messages when neither the domain of the sender nor the domain of any of the recipients is one of the configured domains. For example, if a user requests that an email alert be delivered to a personal email address for a voice mail or fax.

To configure a Gmail domain, you need to obtain several items from the Google Developer Console in your Gmail account. For a list of these items, see *Overview of the Gmail integration configuration.* For more information about how to obtain these items, see *Gmail Integration Technical Reference* in the PureConnect Documentation Library.

To configure a Gmail domain

1. To add a domain, click **Add**. Then complete the procedure, *Configure the properties of a Gmail domain*.
2. To edit a domain, select it in the list and then click **Edit**. Then complete the procedure, *Configure the properties of a Gmail domain*.
3. To delete a domain, select it in the list and then click **Delete**.
4. To select a default domain, select it in the list and then click **Set default**.
5. To specify the timeout for IMAP and SMTP requests, in the **Timeout** box, specify the duration in seconds after which the system will stop trying to send a message to the domain.

> **Note:** the timeout value is the same for all domains.

Related topics

Configure the properties of a Gmail domain

Directories

Use this page to select the default directory which is used for email name searches, and set the order of priority for searches. Use the **Up** and **Down** buttons to change the order of the directories.

Directory Search Order

The directory contains the lookup information for contacts (first name, last name, and so on).

This list shows the default order of email provider directories that CIC will use to search for a user's mailbox.

- Interaction Message Store will not be listed because it does not maintain any contact information.
- If you defined more than one LDAP directory, each will be listed.

Related topics

Configure a Mail storage source

Transports

Use this page to select the transport which is used for delivering email, and set the order of priority for delivery. Use the **Up** and **Down** buttons to change the order of the transports.

The SMTP transport handles the delivery of mail.

This list shows the default order of email provider transport vehicles that CIC will use to search for a user's mailbox. (If you defined more than one SMTP transport, each will be listed.)

> **Note**: If you have multiple transports and one of them is of the type SMTP for an SMTP mail provider (e.g., Sun ONE), you must move the SMTP provider to the top of the Transports list. Configure each transport to handle messages only in its domain, so messages to each domain are passed to the appropriate transport.

Related topics

Configure a Mail storage source

Prefixes and Voice Mail

Use this page to configure email subject prefixes and voice mail options.

Email Subject Prefixes

Use this section to set the email subject prefixes for faxes and voice mails.

Fax

Enter the prefix that you want to appear for faxes in the subject line. By default, the system uses **IC Fax:**.

Voice

Enter the prefix that you want to appear for voice mails in the subject line. By default, the system uses **IC Voicemail:**.

Reply

Enter the prefix that you want to appear for replies to interactions in the subject line. By default, the system uses **RE:**.

> **Note:** This option is used only with emails that are created by handler email tools. Emails that users create in the CIC clients do not use this option. For more information on using handlers, see the Interaction Designer Help in the PureConnect Documentation Library.

Forward

Enter the prefix that you want to appear for forwarded interactions in the subject line. By default, the system uses **FW:**.

> **Note:** This option is used only with emails that are created by handler email tools. Emails that users create in the CIC clients do not use this option. For more information on using handlers, see the Interaction Designer Help in the PureConnect Documentation Library.

Voicemail Options

Use this section to set voice mail message options.

Normalize Voice Mails

This setting determines whether or not the audio is normalized. **Normal Voice Mails** attempts to correct any problems in which the person leaving the voicemail could not be heard). Select the check box to turn on this option.

Long Message Compression

This setting is the compression format which is used to compress the audio for "long" messages. Select the format from the pull-down list. The available settings are:

- DSP Group TrueSpeech
- GSM 6.10
- G711 Mu-Law PCM

Related topics

Configure a Mail storage source

ACD Options

Use this page to configure message delivery behavior.

Message Count Limit

Use the up and down arrow keys to set the count that is used as the maximum number of messages that will be loaded when a user accesses a folder in the telephone user interface (TUI). The default value for this setting is 100.

Polling Intervals

Directory Synchronization (Minutes)

Use this field to set the interval for importing user information from the directory service (what is displayed in the Mailbox Info page in Interaction Administrator and in the Company Directory view in the CIC clients. The default value is 15 minutes.

New Messages (Seconds)

This setting specifies the time in seconds that each message store provider polls for new messages. The default is 120 seconds.

Failed Message Delivery

Use this section to configure failed message delivery behavior.

Delivery Retry Limit

This setting specifies how many times the system will retry the delivery of a message. By default the CIC email server will attempt to transmit a message a maximum of ten times before deciding that there is something wrong with the message itself and moving it to the MAIL\NORETRY directory. The email server will never attempt the second transmission on a message whose first transmission failed until after some other message has been successfully transmitted. Therefore, it is somewhat unlikely, but not impossible, that a transient condition such as network problems would cause an otherwise perfectly valid message transmission to fail twice.

Use the up and down arrow keys to change the limit.

Retry Interval (minutes)

This setting specifies (in minutes) the time to wait between message delivery retries. Use the up and down arrow keys to change the number of minutes. The default value for this setting is 5 minutes.

Failed Message Expiration (days)

This setting specifies the time (in days) to save a message that could not be delivered. If this time expires, the undeliverable message is deleted. Use the up and down arrow keys to change the number of days. The default value for this setting is 7 days.

Threaded Email

CIC can track email messages based on text contained in the messages. This text is the conversation identifier, which CIC uses to associate these email conversations or "Threaded Email". Select the **Add conversation Identifier on Emails** check box to enable the text identifier for this feature.

Related topics

Configure a Mail storage source

Monitored Mailboxes

A monitored mailbox is a mailbox that is configured so that the Incoming Mail initiator is started whenever a new message arrives in the "Inbox" folder for that mailbox.

Mailbox Number

This is the number that corresponds to the Object ID that will be passed to the Incoming Mail initiator (the Notification Event will always be New Mail). Valid mailbox numbers are 1 through 32767.

Mailbox Address

Click **Select** to set the **Mailbox Address**. The Mailbox Selection dialog box is used to associate a User, Workgroup, Email Queue, Monitored Mailbox, etcetera, with a mailbox. The four options available are:

- **No mailbox** - (this doesn't apply to an Email Queue or a Monitored Mailbox). Assign a **Display Name**. No mailbox will be associated with this entry.
- **Interaction Message Store** - (formerly Voicemail Only or FBMC). Assign a **Display Name** and click **Assign Address.** The generated address will be i.e., "FBMC: JohnDoe".
- **IMAP -** No directory entry is associated with the object, but a mailbox exists on an IMAP server, so you must provide the IMAP server, port, username, and password to access the mailbox.
- **Search for a mailbox in the following directories** - Because the directory entry has associated attributes, the directories can be searched to find the associated entry. Once found, the attributes are populated using the corresponding attributes from that entry.

> **Notes:** If attributes are stored in an LDAP directory, but a mailbox exists on an IMAP server, and the attributes (server, port, username, and password) for the mailbox are not stored as attributes of the LDAP directory, then you will need to provide the attributes separately.
>
> Mailbox names and addresses must contain only valid (alpha-numerical) characters.

Related topics

Configure a Mail storage source

Attendant Mailboxes

Use this page to configure the mailboxes that Interaction Attendant can use.

Mailbox Address

Click **Select** to set the **Mailbox Address**. The Mailbox Selection dialog box is used to associate a User, Workgroup, Email Queue, Monitored Mailbox, etcetera, with a mailbox. The four options available are:

- **No mailbox** - (this doesn't apply to an Email Queue or a Monitored Mailbox). Assign a **Display Name**. No mailbox will be associated with this entry.
- **Interaction Message Store** - (formerly Voicemail Only or FBMC). Assign a **Display Name** and click **Assign Address.** The generated address will be i.e., "FBMC: JohnDoe".

- **IMAP -** No directory entry is associated with the object, but a mailbox exists on an IMAP server, so you must provide the IMAP server, port, username, and password to access the mailbox.
- **Search for a mailbox in the following directories** - Because the directory entry has associated attributes, the directories can be searched to find the associated entry. Once found, the attributes are populated using the corresponding attributes from that entry.

> **Notes:** If attributes are stored in an LDAP directory, but a mailbox exists on an IMAP server, and the attributes (server, port, username, and password) for the mailbox are not stored as attributes of the LDAP directory, then you will need to provide the attributes separately.
>
> Mailbox names and addresses must contain only valid (alpha-numerical) characters.
>
> The "email" right must be assigned in the Access Control tab of User Configuration.

Allow to Receive Encrypted Email

Select this option to support the use of the S/MIME type in email. Selecting this check box enables support of email encryption, but other configuration, such as installing certificates, is necessary. For more information see *PureConnect Security Features Technical Reference* in the **Technical Reference Documents** section in the PureConnect Documentation Library on the CIC server.

Related topics

Configure a Mail storage source

Adding an ACD Email Routing Mailbox

Email Certificates Configuration

Single Sign-On

Overview of single sign-on

Use the **Single Sign-On** container to enable streamlined access to CIC applications. When single sign-on is enabled, a user can log in once and then access multiple CIC applications without being prompted to log in again.

> **Note:** To simplify the configuration of a SAML-based single sign-on Assertion for your Interaction Center Server, you can use the Single Sign-on Configuration Utility plug-in. To activate this plug-in, you must enable the **EnableSSOConfiguration** server parameter. For more information, see **EnableSSOConfiguration** in Optional General Server Parameters.

For more information about single-sign on and the Single Sign-on Configuration Utility plug-in, see the *Identity Providers Technical Reference* in the PureConnect Documentation Library.

Enable single sign-on

By default, single sign-on is enabled for CIC. However, in order for the feature to work, you must configure at least one identity provider or service provider, and you must configure the secure token server.

> **Note:** To disable single sign-on, change the setting of the **Allow Single Sign-On authentication** check box in the **Login Authentication Configuration** dialog box, which is found in the **System Configuration** container.

About identity providers and service providers

An identity provider authenticates a login request from a user and provides the user with an authentication response. The user then presents this authentication response to a service provider, who validates that the authentication response came from a trusted identity provider.

You configure the identity providers in the **Identity Providers** subcontainer.

About the secure token server

The secure token server can be used as either the identity provider or the service provider, or both. If a user's login is authenticated, the secure token server issues a token, which Interaction Center uses to grant that user access to specific CIC applications.

The token includes standard attributes that are used by the CIC applications to determine which application-specific privileges that user has. For example, the token includes attributes which indicate the role(s) that the user has in CIC. You can specify additional attributes to include in the token.

There is one secure token server on each CIC server. Be sure to verify the configuration of the secure token server on each CIC server at your company.

> **Note:** You must configure the secure token server before you configure the identity providers.

Related topics

Login Authentication Configuration **dialog box**

Configure a secure token server

Configure a connection for a secure token server

Configure an identify provider

Secure Token Server

Configure the secure token server

The **Configuration** page of the **Secure Token Server Configuration** dialog box displays the default configuration values for the secure token server. In most cases, you do not need to change the default values that appear here. However, if the secure token server is known by a different hostname on a remote machine that needs to access it, configure that hostname in the **Machine Name** box.

> **Note:** You must configure the secure token server before you configure the identity providers.

To configure the secure token server

1. In the **Single Sign-on** container, click **Configuration**.
   The **Secure Token Server Configuration** dialog box appears. The **Configuration** tab is automatically displayed.
2. In the **Private Key Path** box, type the file path to the location of the private key.
3. In the **Certification Path** box, type file path to the location of the certificate.

4. In the **Port** box, select the port. The default port is 8043.

> **Note:** If you specify a different port, select one that is allowed by your firewall and that does not conflict with any other applications. For information on other ports used by PureConnect products, see the *CIC Port Maps and Data Flow Diagrams Technical Reference*, which is available in the PureConnect Documentation Library.

5. In the **Machine Name** box, type a logical name for this server. The machine name allows other machines to locate this specific server by its IP address or FQDN.

> **Note:** Only one alternative name is allowed per server. The alternate name for the server may be either its IP address or its FQDN, but not both.

6. By default, all tokens issued by this secure token server expire in 14 days. To change this, in the **Token Expiration** group, do one of the following:

- If the token never expires, select the **Never** option button.
- If the token expires, select the **After** option button and then specify the expiration time in the corresponding boxes.

1. Click **OK**.

Related topics

Configure a connection for a secure token server

Configure an identity provider

Configure the secure token server

The **Configuration** page of the **Secure Token Server Configuration** dialog box displays the default configuration values for the secure token server. In most cases, you do not need to change the default values that appear here. However, if the secure token server is known by a different hostname on a remote machine that needs to access it, configure that hostname in the **Machine Name** box.

> **Note:** You must configure the secure token server before you configure the identity providers.

To configure the secure token server

1. In the **Single Sign-on** container, click **Configuration**.
   The **Secure Token Server Configuration** dialog box appears. The **Configuration** tab is automatically displayed.
2. In the **Private Key Path** box, type the file path to the location of the private key.
3. In the **Certification Path** box, type file path to the location of the certificate.
4. In the **Port** box, select the port. The default port is 8043.

> **Note:** If you specify a different port, select one that is allowed by your firewall and that does not conflict with any other applications. For information on other ports used by PureConnect products, see the *CIC Port Maps and Data Flow Diagrams Technical Reference*, which is available in the PureConnect Documentation Library.

5. In the **Machine Name** box, type a logical name for this server. The machine name allows other machines to locate this specific server by its IP address or FQDN.

> **Note:** Only one alternative name is allowed per server. The alternate name for the server may be either its IP address or its FQDN, but not both.

6. By default, all tokens issued by this secure token server expire in 14 days. To change this, in the **Token Expiration** group, do one of the following:

- If the token never expires, select the **Never** option button.
- If the token expires, select the **After** option button and then specify the expiration time in the corresponding boxes.

1. Click **OK**.

Related topics

Configure a connection for a secure token server

Configure an identity provider

Configure a connection for a secure token server

Use the **Connections** page of the **Secure Token Server Configuration** to configure connections to the secure token server.

To prevent a "denial-of-service" attack on the CIC server, CIC allows a server to make up to 5 simultaneous connections to the secure token server. If you know of a server that needs more than this number of simultaneous connections, then create a connection for it.

To configure a connection

1. On the **Connections** page, do any of the following:
   - To add a connection, click **Add**.
     The **New Connection** dialog box appears.
   - To edit a connection, select it in the list and then click **Edit**.
     The **Edit Connection** dialog box appears.
   - To delete a connection, select it in the list and then click **Delete**.
     A confirmation message appears. Click **OK**.
2. Do one of the following:
   - Click **OK** to close the dialog box.
   - Click **Apply** to save your changes and continue with the configuration process.

Related topics

New Connection dialog box

E**dit Connection dialog box**

Configure a secure token server

Identity Providers

Configure an identity provider

Use the **Configuration** tab of the **Identity Provider Configuration dialog** box to configure identity providers. For more information about identity providers, see the *Identity Providers Technical Reference* in the PureConnect Documentation Library.

To configure an identity provider

1. In the **Single Sign-on** container, click the **Identity Providers** sub-container.
2. In the container, right-click to display the pop-up menu and then click **New**.
   The **Identity Provider Configuration** dialog box appears. The **Configuration** tab automatically appears.
3. In the **Name** box, type a meaningful name for the identity provider.
4. In the **Connection** group, do one of the following:
   - If you configured the identity provider to use single sign-on for a release prior to CIC 2016 R1, select the **Connect to Secure Token Server** option.
   - If you are configuring a new identity provider, select the **Connect to Session Manager** option. This option allows IceLib clients to connect to the local session manager (CIC or OSSM, if it exists). This is the preferred option for new identity providers.
5. In the **UI display** group, do one of the following:
   - To prompt the user for his or her user name and password, select **Allow user to specify username and password**.
   - To prompt the user for his or her Windows credentials, select **Logged in Windows username must be used**.
   - To have CIC automatically use a browser-based authentication site to validate user credentials, select **Use webbrowser for authentication**.
6. In the **Authentication Types** list, select the appropriate authentication type for your identity provider:
   - Select **SAML 2 Enhanced Client or Proxy** for any application that can complete the authentication request, but that is not a web-based application. For example, the CIC clients.
   - Select **SAML 2 Web Browser Post** for the web page of an application that can complete the authentication request.
   - Select **SAML 2 Web Browser Redirect** for a web page that redirects the authentication request to a web page where the authentication can be completed.
7. To import an XML file containing your authentication details, click **Import** and then click **Browse** to select the file. After you import the file, continue with the next step.

> **Note:** The file must contain valid SAML 2 Metdata.

8. Do one of the following:

    - If this is a new configuration, click **Enable**.
    - If this is an existing configuration that you are updating, click **Configure**.

9. Continue with *Configure an endpoint*.

Related topics

Configure a secure token server

Configure an endpoint

Configure SAML attributes

Configure validation certificates

Configure claims

Configure an identity provider

Use the **Configuration** tab of the **Identity Provider Configuration dialog** box to configure identity providers. For more information about identity providers, see the *Identity Providers Technical Reference* in the PureConnect Documentation Library.

To configure an identity provider

1. In the **Single Sign-on** container, click the **Identity Providers** sub-container.
2. In the container, right-click to display the pop-up menu and then click **New**.
   The **Identity Provider Configuration** dialog box appears. The **Configuration** tab automatically appears.
3. In the **Name** box, type a meaningful name for the identity provider.
4. In the **Connection** group, do one of the following:

    - If you configured the identity provider to use single sign-on for a release prior to CIC 2016 R1, select the **Connect to Secure Token Server** option.
    - If you are configuring a new identity provider, select the **Connect to Session Manager** option. This option allows IceLib clients to connect to the local session manager (CIC or OSSM, if it exists). This is the preferred option for new identity providers.

5. In the **UI display** group, do one of the following:

    - To prompt the user for his or her user name and password, select **Allow user to specify username and password**.
    - To prompt the user for his or her Windows credentials, select **Logged in Windows username must be used**.
    - To have CIC automatically use a browser-based authentication site to validate user credentials, select **Use webbrowser for authentication**.

6. In the **Authentication Types** list, select the appropriate authentication type for your identity provider:
    - Select **SAML 2 Enhanced Client or Proxy** for any application that can complete the authentication request, but that is not a web-based application. For example, the CIC clients.
    - Select **SAML 2 Web Browser Post** for the web page of an application that can complete the authentication request.
    - Select **SAML 2 Web Browser Redirect** for a web page that redirects the authentication request to a web page where the authentication can be completed.
7. To import an XML file containing your authentication details, click **Import** and then click **Browse** to select the file. After you import the file, continue with the next step.

> **Note:** The file must contain valid SAML 2 Metdata.

8. Do one of the following:
    - If this is a new configuration, click **Enable**.
    - If this is an existing configuration that you are updating, click **Configure**.
9. Continue with *Configure an endpoint*.

Related topics

Configure a secure token server

Configure an endpoint

Configure SAML attributes

Configure validation certificates

Configure claims

Configure an endpoint

Use the **Endpoint** box to specify the URI of your identity provider. The endpoint is the place where the process of obtaining your credentials begins.

> **Notes:**
>
> The **Endpoint** box appears only after you configure and enable one of the available authentication types on the **Configuration** tab. For information on how to do this, see *Configure an identity provider*.
>
> The endpoint must support SAML 2.0.

To configure an endpoint

1. In the **Endpoint** box, type the URL of the identity provider that is used to authenticate the user's credentials.

2. Do one of the following:

- To save the configuration and close the dialog box, click **OK**.

  Note: You cannot close the dialog box unless you fully configure the identity provider details. These include at least one claim and one validation certificate (unless identity provider does not sign its responses). CIC displays messages if you need to complete your identity provider configuration before closing the dialog box.

- To save the configuration and continue with the configuration process, click **Apply**.

3. Continue with *Configure SAML attributes*.

Related topics

Configure an identity provider

Configure SAML attributes

Configure validation certificates

Configure claims

Configure SAML attributes

Use the **SAML Attributes** page to configure optional data values to return in the secure token certificate.

> **Note:** The predefined secure token certificate contains all of the data values that are necessary to ensure security. Configuring additional SAML attributes is optional.

For complete information on configuring SAML attributes, contact PureConnect Customer Care.

To configure a SAML attribute

1. On the **SAML Attributes** page, do any of the following:

- To add a SAML attribute, click **Add**.
  The **New Attribute** dialog box appears.

- To edit a SAML attribute, select it in the list and then click **Edit**.
  The **Edit Attribute** dialog box appears.

- To delete a SAML attribute, select it in the list and then click **Delete**.
  A confirmation message appears. Click **OK**.

2. Do one of the following:

- Click **OK** to close the dialog box.

- Click **Apply** to save your changes and continue with the configuration process.

3. Continue with *Configure validation certificates*.

Related topics

New Attribute dialog box

Edit Attribute dialog box

Configure an identify provider

Configure an endpoint

Configure validation certificates

Configure claims

Configure validation certificates

Use the **Validation Certificates** page to configure the files that your secure token server uses to verify the SAML responses from the identity provider.

To configure a validation certificate

1. On the **Validation Certificates** page, do any of the following:

- To add a validation certificate, click **Add**.
  The **New Validation Certificate** dialog box appears.
- To edit a validation certificate, select it in the list and then click **Edit**.
  The **Edit Validation Certificate** dialog box appears.
- To delete a validation certificate, select it in the list and then click **Delete**.
  A confirmation message appears. Click **OK**.

2. Do one of the following:

- Click **OK** to close the dialog box.
- Click **Apply** to save your changes and continue with the configuration process.

3. Continue with *Configure claims*.

Related topics

New Validation Certificate dialog box

Edit Validation Certificate dialog box

Configure an endpoint

Configure SAML attributes

Configure claims

Configure claims

Use the **Claims** page to configure the assertions that are included in the SAML responses. A claim maps each SAML assertion to a user's CIC attribute. If the value of the SAML assertion matches the value of a particular user's CIC attribute, then the authentication is considered to be made for that CIC user. For example, if the SAML assertion "NT Account" has a value of "John.Doe," and it is mapped in a claim to the CIC attribute "Windows Domain Account," then the authentication is applied for the CIC user, "John.Doe."

Tip: Look in the **Users** container for the attributes that are defined for CIC users.

Every identity provider must provide at least one claim (a SAML assertion) that is mapped to a CIC attribute.

To configure a claim

1. On the **Claims** page, do any of the following:

- To add a claim, click **Add**.
  The **New Claim** dialog box appears.
- To edit a claim, select it in the list and then click **Edit**.
  The **Edit Claim** dialog box appears.
- To delete a claim, select it in the list and then click **Delete**.
  A confirmation message appears. Click **OK**.

2. Do one of the following:

- Click **OK** to close the dialog box.
- Click **Apply** to save your changes and continue with the configuration process.

Related topics

New Claim dialog box

Edit Claim dialog box

Configure an identify provider

Configure an endpoint

Configure SAML attributes

Configure validation certificates

Logon Authentication Configuration

Use this page to configure authentication methods for CIC client applications. This feature allows for additional security mandated by some highly sensitive environments and applications.

Note: You cannot delete the <Default> user agreement.

To Configure the Logon Authentication

1. Select the check box for each authentication method that you want to enable. You must select at least one of the following methods:

    - **Allow IC authentication:** Select this option to use specific CIC user names and passwords when a user logs in to CIC client applications.

  - **Allow defaulting to the current Windows user credentials:** Select this option to use Windows credentials when logging in to CIC client applications. To use this type of authentication, a CIC Administrator must link Windows user names and CIC Client user names.
  - **Allow manual entry of Windows authentication credentials:** Select this option to require a user to manually enter his or her domains, user names, and passwords to authenticate every time they log in to a client application. This option does not allow credentials to be passed in from CIC or Windows. The credentials of the currently logged in user cannot be used.
  - **Allow Single Sign-On authentication:** Select this option to enable streamlined access to CIC client applications. For more information, see Single Sign-On.

2. Do you want a user's credentials to automatically be populated in the **Logon** dialog box after the user logs on the first time?
   - If yes, select the **Allow cached credentials** check box.
   - If no, skip to the next step.
3. When a user logs on to a client application, do you want to display a splash screen with a user agreement? If yes, select the **Display language-specific user agreement after logon** check box. In the **Languages** box, select **<Default>** to select the CIC system language or click **Add** to select other languages. In the **Agreement** box, type the text of the agreement.
4. Click **OK**.

Related Topics

Connection Security

Certificate Management

PureCloud

About PureCloud for CIC

The PureCloud for CIC Integration allows you to enrich your users' experience by leveraging the power and data of CIC and the collaborative features of PureCloud. PureCloud for CIC brings users together into a single environment that allows for seamless communication between CIC and PureCloud-only users. Information such as CIC users and statuses are automatically and continuously synced into a paired PureCloud organization. For more information about the integration, see the *PureCloud for CIC Administrator's Guide* in the PureConnect Documentation Library.

Prerequisites

CIC users

In order to sync properly, PureCloud for CIC requires that CIC user accounts have the following information configured in the Users container:

- Personal Info tab>General tab>**Display Name**

- Personal Info tab>Internet tab>**Business Email**

After the integration is configured, you can change the values of these attributes in the PureCloud Admin web interface.

> **Notes:**
>
> *Ideally you should configure all of your users in CIC before you configure the integration. However, if you configure additional users after you configure the integration, CIC automatically syncs them for you.
>
> *If the required Display Name and Email address information is not configured for CIC users, the users will not be synced in the PureCloud organization when you configure PureCloud for CIC.

PureCloud Organization

Your CIC server can integrate with only one PureCloud organization.

If you do not already have an existing PureCloud organization, PureCloud for CIC automatically creates one for you during the PureCloud for CIC configuration.

If you already have a PureCloud organization, make a note of these items:

- Administrator email address
- Administrator password
- Organization long name - name you entered when you created the PureCloud organization
- Organization short name - generated from the organization long name, in compliance with DNS restrictions (a-z, 0-9, A-Z)
- Region

> **Note:** If you are unsure of the organization short name, log in to PureCloud and navigate to **Admin>Account Settings>Organization Settings**. Both the organization long name and short name are listed here.

User passwords and permissions in CIC, Interaction Connect, and PureCloud

> **Note:** If a user uses PureCloud for CIC from Interaction Connect, no passwords are involved. However, if the user chooses to log in to PureCloud without using the integration, the user must create a password for PureCloud.

User passwords for CIC are separate than user passwords for PureCloud. They may be different passwords. If a user chooses a different password in PureCloud, it will not affect their ability to log in to CIC.

CIC does not recognize PureCloud roles and permissions. PureCloud does not recognize CIC user security settings.

About the PureCloud Admin user

When you configure the PureCloud for CIC Integration, a new PureCloudAdmin user is automatically created in the CIC Users container.

> **Notes:**
>
> Do not delete the PureCloudAdmin user.

PureCloud Bridge considerations

As part of the PureCloud for CIC configuration, PureCloud Bridge is installed to manage the data transfer between CIC and PureCloud.

Local bridge

For small and medium implementations, select Local Bridge as part of the PureCloud for CIC configuration in Interaction Administrator. PureCloud Bridge will be installed automatically on the CIC server.

Off-server bridge

We recommend that large implementations start with a local bridge. After the CIC server has been running for a while with a local bridge, you may determine the need for an off-server bridge.

An off-server PureCloud Bridge install is located on a CIC server share. If you choose to have an off-server bridge, you will need to install it after performing the PureCloud for CIC configuration in Interaction Administrator.

Switchover

When you select Bridge Location>Automatic Local Install as part of PureCloud for CIC configuration on the active server in a Switchover pair, PureCloud Bridge is automatically installed on both the active and backup servers.

The bridge operates independently from the active and backup CIC servers.

If the backup server is down at the time that you configure PureCloud for CIC, a bridge will be installed on the backup server the next time that IC is started.

If the primary CIC server stops, but the computer itself is healthy and running, then the bridge on that computer will automatically talk to the new Primary CIC server after the switchover completes.

Related topics

PureCloud Configuration

PureCloud Web Page

Bridge Status

PureCloud Dial Groups

PureCloud Configuration

System Configuration > PureCloud > Configuration

For complete instructions on how to configure the PureCloud for CIC Integration, see the *PureCloud for CIC Administrator's Guide* in the PureConnect Documentation Library.

Enable PureCloud Integration

Select this check box to configure the PureCloud for CIC Integration. In the confirmation message, click **Yes** to continue with the configuration.

> **Note:**
>
> Click **No** in the confirmation message if you wish to configure additional CIC user information in Interaction Administrator before configuring PureCloud for CIC, or if you do not wish to configure PureCloud for CIC at this time.

Administrator Email

Type the email address you wish to use for the PureCloud administrator. If you have an existing PureCloud organization, this is the existing administrator email address for the organization.

If you do not have an existing PureCloud organization, we recommend using a general administrator or IT-related distribution email address, for example, "ITServices," instead of a person's email address.

Password

Type the PureCloud administrator password. If you have an existing PureCloud organization, type the existing administrator password for the organization.

> **Notes:**
>
> • The password must follow standard PureCloud password requirements.
>
> • PureCloud does not use CIC password policies.

Confirm Password

Re-type the PureCloud administrator password.

Organization Name

Do one of the following:

- If you have an existing PureCloud organization, type its name. If you are unsure of the organization short name, log in to PureCloud and navigate to **Admin>Account Settings>Organization Settings**.
- If you do not have an existing PureCloud organization name, type the name you would like.

> **Note:**
>
> The name must follow PureCloud naming conventions.

Region

Select your closest region. The default is North America. User access to PureCloud will be routed to the location of the Amazon data center for the region you select, whether users are in the office, at home, or traveling.

Bridge Location

Click **Edit** and then select one of the following:

- To install the bridge on the CIC server, select the **Automatic Local Install** check box. This is the recommended selection. The PureCloud Bridge will automatically be installed on the CIC server.

> **Note:**
>
> When you select **Automatic Local Install**, any backup CIC servers automatically install the bridge and connectors when running in backup mode.

- If you have decided you need an off-server bridge, select the **Manual Off-Host Install** check box. After you configure the fields in this tab, be sure to install the off-server bridge. **The integration is not complete** until you install the bridge server. For more information about how to install a bridge on a different server, see the *PureCloud for CIC Administrator's Guide* in the PureConnect Documentation Library.

> **Notes:**
>
> • If you select the **Manual Off-Host Install** check box, the integration creates a paired organization in PureCloud, but no data is synced. As soon as you complete the installation of the off-server bridge, the data will sync.
>
> • To install the Off-Host bridge server, you must use the ICBridgeSetupUtility in the IC/Install/PureCloudIntegration folder .

After you make your selection, click **Apply** in the **PureCloud Configuration** tab. A message box appears; you must confirm that you want to provision the organization.

- If you are creating a new PureCloud organization, click **Yes** to confirm that the new organization will be created.
- If you entered the credentials for an already existing PureCloud organization, click **Yes** to confirm that this organization already exists and will be populated with your CIC users.

A message box confirms that the PureCloud organization was successfully created. Click **OK**.

Test PureCloud Connection

After you provision to PureCloud, click the **Test PureCloud Connection** button to verify that single sign-on works and that the internet connection to your PureCloud organization is healthy.

If this test fails, try to log in to your PureCloud organization manually using https://login.mypurecloud.com. (The URL will be different if you used the Ireland or Australia/New Zealand regions.) If you can log in successfully, then the root cause of the problem may lie with CIC. If that is the case, you can reprovision the integration by disabling and then re-enabling the integration. For more information, see the *PureCloud for CIC Administrator's Guide* in the CIC Documentation Library.

Enable CIC web-based phone

The **Enable CIC web-based phone** check box is automatically enabled when you complete the CIC web-based phone configuration wizard. If, after that point, you want to disable CIC web-based phone for all users, disable the **Enable CIC web-based phone** check box.

Configure CIC web-based phone

Select the **Configure CIC web-based phone** button to start a wizard application that configure the necessary options and associations between PureCloud and CIC. If the **Enable CIC web-based phone** check box is disabled, successfully completing the wizard enables the check box. If you had previously configured CIC web-based phone, a subsequent running of the wizard reconfigures the feature with the options you select.

> **Important!**
>
> The CIC web-based phone configuration wizard is for use with PureCloud organizations that are associated with only one CIC server.

Remove Configuration

This button deletes any bridges on the primary CIC server. Before you can complete this action, you must first use the ICBridgeSetupUtility to uninstall all bridges that are not on the primary CIC server.

To remove a configuration, first deselect the **Enable PureCloud Integration** checkbox. Then click **Remove Configuration**.

> **Notes:**
>
> You must deselect the **Enable PureCloud Integration** check box in order to use the Remove Configuration button.
>
> After you click this button, its name changes to **Check Remove Status**. Click the button to see whether the remove process is ongoing or completed.
>
> While a configuration is being removed, you can change no values and perform no other functions on the PureCloud Configuration page.

Related topics

About PureCloud for CIC

PureCloud Web Page

Bridge Status

PureCloud Dial Groups

PureCloud Web Page

Click Launch Web Page to go directly to your PureCloud organization.

- You are automatically logged as the PureCloud Admin user that was created for you in CIC.
- If your CIC user accounts were configured with Display Name and Business Email before you configured PureCloud for CIC, CIC user account data was sync'd and those users appear in PureCloud Directory.

Additional configuration in PureCloud Admin

You may wish to:

- Further configure your organization by adding to the PureCloud Admin profile, setting up groups, etc. See Admin>Overview.

- Modify organization settings in Admin>Account Settings.
- Review PureCloud Bridge settings and check for updates in Admin>Integrations. For more information see the *PureCloud for CIC Administrator's Guide*.

For information about PureCloud administration, see the PureCloud Resource Center at help.mypurecloud.com.

Related topics

About PureCloud for CIC

PureCloud Configuration

Bridge Status

PureCloud Dial Groups

Bridge Status

This page lets you quickly see whether the bridge and connectors for the PureCloud integration are online and syncing properly.

> **Note:** In PureCloud, you can see these same connector details in **Admin > Integrations > Bridge > Connectors**.

To see the details of a connector, click its node. The following table describes the icons that you may see when you expand the connector details.

Icon	Description
✓	**Status**: This connector is online and data is syncing properly.
✗	**Status**: This connector is not online and not syncing. You may see this icon if the connector has been deleted in PureCloud. Click **Refresh** to see updated information from PureCloud.
🌐	**Location:** The bridge is installed here.
ℹ	**Information:** This icon indicates some information; it does not indicate the status of the bridge. **Note:** One type of information is Leader. The leader is set when there are 2 or more connector instances. **Leader: True** indicates that this server is the active server in the switchover pair. **Leader: False** indicates that this server is not the active server in the switchover pair.
⚠	**Caution:** An event has occurred which requires your attention.
🕒	**Timestamp:** An event at this time.
🖧	**FQDN:** This is the fully qualified domain name of the bridge.

Refresh

Click **Refresh** to verify that you are viewing the most up-to-date information. The information shown may change as connectors are added or deleted from the integration.

Related topics

PureCloud Configuration

PureCloud Web Page

PureCloud Dial Groups

PureCloud Browser Client Applications

System Configuration > PureCloud > PureCloud Configuration > PureCloud Browser Client Applications

You must configure the URIs of Interaction Connect or other browser-based client applications that use PureCloud integrations. This enables these applications to use the PureCloud API from a web browser.

Required: This is required for the WebRTC and Co-browse integrations in Interaction Connect. This is not needed for CIC for Saleforce's WebRTC integration since CIC for Salesforce itself is hosted from PureCloud origins; those origins are automatically allowed when the organization is provisioned by CIC.

To add a URI, type it in the text box and click **Add**. The list box contains the URI's you have configured.

For information about PureCloud administration, see the PureCloud Resource Center at help.mypurecloud.com.

Related topics

About PureCloud for CIC

PureCloud Configuration

PureCloud Web Page

Bridge Status

PureCloud Dial Groups

System Configuration > PureCloud > PureCloud Configuration > PureCloud Dial Groups

The **PureCloud Dial Groups** tab enables you configure which dial groups are used for the Web-based phone integration. Connection calls are placed to the PureCloud Edges using these dial groups.

Available Dial Groups

This list box displays the existing dial groups of this CIC server. You can select a dial group in this box.

Add button

With an item in the **Available Dial Groups** box selected, select this button to move that CIC dial group to the **Currently Selected Dial Groups** box.

Currently Selected Dial Groups

This list box displays the existing dial groups that CIC is currently configured to use to communicate with PureCloud Edges for the Web-based phone integration.

For information about PureCloud administration, see the PureCloud Resource Center at help.mypurecloud.com.

Related topics

About PureCloud for CIC

PureCloud Configuration

PureCloud Web Page

Bridge Status

CIC web-based phone configuration wizard

CIC web-based phone configuration wizard prerequisites

To use CIC web-based phone configuration wizard, ensure that the following prerequisites are met:

- Your organization purchased a PureCloud Communicate license.
- You did the procedures for integrating CIC with PureCloud as documented in *PureCloud for CIC Administrator's Guide*.
- You installed and configured one or more PureCloud Edge devices.

Failure to do these prerequisites will result in an error message when you click the **Configure CIC web-based phone** button.

CIC Location to PureCloud Site Associations (1 of 6)

This panel of the CIC web-based phone wizard associates CIC *Locations* with PureCloud *Sites*. This mapping enables the users assigned to the CIC Location to use CIC web-based phone.

> **Note:**
> The PureCloud Site must include a PureCloud Edge device to facilitate WebRTC communications.

CIC Location

Select an existing CIC Location for which you want to use CIC web-based phone.

> **Important!**
> Users in CIC Locations that are not mapped to PureCloud Sites cannot use CIC web-based phone.

PureCloud Site

Select an existing PureCloud Site to associate with the selected CIC Location.

Create Mapping

Select this button to associate the selected CIC Location with the selected PureCloud Site.

> **Important!**
> The CIC web-based phone feature requires that you map at least one CIC Location to a PureCloud

> Site. If you do not map at least one CIC Location to one PureCloud Site, you cannot use CIC web-based phone.

Map list

This list box displays existing mappings between CIC Locations and PureCloud Sites.

Remove Mapping

Select this button to remove the currently-selected, existing mapping in the Map list.

When you have finished mapping CIC Locations to PureCloud Sites, select the **Next** button to continue to the next panel of the CIC web-based phone wizard.

> **Tip:**
>
> To remove all existing mappings between CIC Locations and PureCloud Sites, ensure that no entries are specified in the **CIC Location** and **PureCloud Site** list boxes. Then, select the **Next** button.
>
> The wizard, then, displays the **PureCloud Edge Tie Lines** dialog box, bypassing the **Select PureCloud Edge Devices** and **Select Local NIC** dialog boxes. The **PureCloud Edge Tie Lines** dialog box displays the lines that the wizard will remove from the configuration. Select the **Next** button to continue with the removal of those items.

Related topics

Select PureCloud Edge Devices

Select Local NIC

PureCloud Edge Tie Lines

PureCloud Edge Line Groups

Commit Changes

Select PureCloud Edge Devices (2 of 6)

This panel of the CIC web-based phone wizard enables you to select which PureCloud Edge devices in the mapped PureCloud Sites will facilitate CIC web-based phone communications. You must select at least one PureCloud Edge devices in a PureCloud Site that is mapped to a CIC Location to be able to use CIC web-based phone.

> **Important!**
> When this dialog box is displayed for the first time, Windows displays a security message box stating that the wizard is requesting access to the network. Select the appropriate network location displayed in the message box and grant the wizard access to the network so that it can make the appropriate PureCloud configuration.
>
> **Note:**
> To successfully complete this step of the CIC web-based phone wizard, PureCloud Edge devices must be configured and assigned to your PureCloud Sites. The PureCloud Edge devices do not have to be operational or online at the time when this wizard is run.

Available Detected Edges

This list box displays the detected PureCloud Edge devices in all PureCloud Sites that are associated with CIC Locations. PureCloud Edge devices in this list box cannot service CIC web-based phone communications.

Add button

Select this button to move the selected PureCloud Edge device in the **Available Detected Edges** list box to the **Currently Selected Edges** list box.

Remove button

Select this button to remove the selected PureCloud Edge device in the **Currently Selected Edges** list box.

Currently Selected Edges

This list box displays the PureCloud Edge devices in PureCloud Sites that can service CIC web-based phone communications.

The **Connectivity** column provides a visual indicator if the associated PureCloud Edge device is currently active and responsive.

Manual Edge/Proxy

This group of controls enables you to define a PureCloud Edge device that is not displayed in one of the list boxes. In some environments, a PureCloud Edge device may be located behind a *SIP proxy* or *SBC*. This wizard cannot detect SIP proxy or SBC devices through which you want to connect to a PureCloud Edge device.

Additionally, you could use this set of controls to enter a PureCloud Edge device that has not yet been installed and configured.

Address

Enter the IP address of SIP proxy, SBC, or unavailable PureCloud Edge device.

> **Note:**
> The IP address must be consistent. Do not attempt to manually enter an address if the device receives its IP address through *DHCP* and a range of IP addresses is available for assignment.

Name

Enter a name to use for the tie line of the IP address that you entered.

Site

Enter the PureCloud Site that includes this PureCloud Edge device.

Add button

Select this button to add the manually-defined PureCloud Edge device to the **Currently Selected Edges** list box.

When you have finished selecting which PureCloud Edge devices will service CIC web-based phone communications, select the **Next** button.

> **Note:**
> If you do not select a PureCloud Edge device in this dialog box, the wizard will bypass the Select Local NIC dialog box and display the PureCloud Edge Tie Lines dialog box.

Related topics

CIC Location to PureCloud Site Associations

Select Local NIC

PureCloud Edge Tie Lines

PureCloud Edge Line Groups

Commit Changes

Select Local NIC (3 of 6)

This panel of the CIC web-based phone wizard enables you to select the NIC on the CIC server that will communicate with any PureCloud Edge device that is configured to service CIC web-based phone communications.

In the **Local NIC for New Edges** list box, select a listed network interface of the CIC server through which it will send SIP messages to PureCloud Edge devices.

After selecting the appropriate NIC of the CIC server, select **Next**.

Related topics

CIC Location to PureCloud Site Associations

Select PureCloud Edge Devices

PureCloud Edge Tie Lines

PureCloud Edge Line Groups

Commit Changes

PureCloud Edge Tie Lines (4 of 6)

This panel of the CIC web-based phone wizard provides a summary of the *tie lines* that will be created by the CIC web-based phone configuration wizard.

Tie lines are logical circuits that link PureCloud Edge devices to CIC servers without requiring the dialing of a telephone number in E.164 format.

Tie Lines To Be Generated

This box lists the tie lines that the wizard will create on the specified PureCloud Edge devices.

Existing Tie Lines

This box lists any existing tie lines that will not be updated or removed by the wizard.

Tie Lines To Be Removed

This box lists the existing tie lines that the wizard will remove.

If, after reviewing the tie lines changes, you are satisfied with the tie line configuration, select the **Next** button.

Related topics

CIC Location to PureCloud Site Associations

Select PureCloud Edge Devices

Select Local NIC

PureCloud Edge Line Groups

Commit Changes

PureCloud Edge Line Groups (5 of 6)

This panel of the CIC web-based phone configuration wizard displays the changes that the wizard will make for PureCloud *line groups*.

There will be only one line group for each PureCloud site.

Tie Line Groups To Be Generated

This box lists the PureCloud line groups and the dial plan entry pattern for telephone extensions that this configuration wizard will create in PureCloud.

Existing Tie Line Groups

This box lists the existing PureCloud line groups that will not be modified by this wizard.

Tie Line Groups To Be Removed

This box lists the existing PureCloud line groups that the wizard will remove.

> **Note:**
> Removing a PureCloud line group also removes any corresponding extension pools.

After you review and approve the line group changes that this wizard will make, select the **Next** button.

Related topics

CIC Location to PureCloud Site Associations

Select PureCloud Edge Devices

Select Local NIC

PureCloud Edge Tie Lines

Commit Changes

Commit Changes (6 of 6)

The final panel of the CIC web-based phone wizard enables you to confirm the configuration changes and cause the wizard to implement them. You can use the **Back** button to return to the previous panels and make changes.

If you are satisfied with the configuration for the CIC web-based phone feature, select the **Commit Changes** button to initiate the changes. Upon successful completion, the wizard changes the **Status** message to **Changes Complete!**.

Select the **Finish button** to close the CIC web-based phone configuration wizard.

Related topics

CIC Location to PureCloud Site Associations

Select PureCloud Edge Devices

Select Local NIC

PureCloud Edge Tie Lines

PureCloud Edge Line Groups

Interaction Process Automation

Interaction Process Automation

The **Interaction Process Automation** container displays a list of the current processes. For each process, it displays the published version number, owner, and current status.

Use this page to configure Interaction Process Automation settings.

Active

A process automatically becomes active once a user publishes it in **Interaction Process Automation Designer**. However, as an administrator, you can also deactivate or activate a process when necessary from Interaction Administrator. When a process is deactivated, it cannot be launched.

To activate a process:

1. In the Interaction Process Administrator container, double-click the process to activate. The **Interaction Process Automation Configuration** dialog box appears.
2. Select the **Active** check box.
3. Click **OK**.

To deactivate a process:

1. In the Interaction Process Administrator container, double-click the process to activate. The **Interaction Process Automation Configuration** dialog box appears.
2. Clear the **Active** check box.
3. Click **OK**.

> **Note**: Deactivating a process does not revert any actions the process has already performed.

Security Specifications

Interaction Process Automation provides data-level security that allows each customer the flexibility to specify which users, workgroups, and/or roles can access each data variable.

If your company needs to track sensitive information as part of a process, you can use a security specification to grant access to only those users or workgroups who need to view that data.

You assign users or workgroups to a security specification to give them access to any data that is bound to that specification. If no security specification is assigned to a data variable, everyone has access to that data.

You can add and modify security specifications in Interaction Administrator, and then bind them to data variables in the **Property** tab in **Interaction Process Automation Designer**. You can also delete security specifications. This topic includes instructions for:

- Adding a Security Specification
- Modifying a Security Specification
- Deleting a Security Specification

Adding a Security Specification

To add a security specification:

1. Expand the **Interaction Process Automation** container in Interaction Administrator.
2. Within the **Interaction Process Automation** container, click the **Security Specifications** sub-container.
3. Right-click in the area on the right side of the Interaction Administrator window, and then click **New** from the shortcut menu that appears.
4. In the **Entry Name** dialog, type a name for the new security specification, and then click **OK**. The **Security Specifications Configuration** dialog appears.
5. On the **Configuration** tab, click **Members**.
6. In the **Select Users** dialog, select each user, workgroup, or role for which you want to grant access, and then click **Add**.
7. Once you have selected all the users, click **OK**.
8. *This option is reserved for a future release.* Under **For members that don't have full-access**, choose either of the following or leave both options unselected:

Choose this option…	**If…**
Do not show data	You don't want the data to appear at all for users, workgroups, and roles not in the Members list.
Show only right 4 characters	You only want to display the right four

	characters for users, workgroups, and roles not in the Members list. (useful for data such as credit card numbers).

9. Click **OK**.

The security specifications you added should now be available to apply to data variables in Interaction Process Automation Designer.

Modifying a Security Specification

You can modify a security specification to add or remove members.

To modify a security specification:

1. In the **Security Specifications** sub-container, double-click the security specification to modify. The **Security Specifications Configuration** dialog appears.
2. On the **Configuration** tab, click **Members** .
3. Do one of the following:

- To add a member, select the member from the list and then click **Add**.
- To remove a member, select the name in the list at the bottom of the dialog and then press **Delete**.

4. Once you have added or removed the appropriate members, click **OK**.
5. Click **OK** to close the **Security Specifications Configuration** dialog.

Deleting a Security Specification

> **Caution**: If you delete a security specification that has been assigned to a data variable in **Interaction Process Automation Designer**, you could cause the data to be unreadable.

To delete a security specification:

1. In the **Security Specifications** container, right-click the security specification to delete. Interaction Administrator displays a message to warn you that deleting a security specification that has been assigned to a data variable will make that data unreadable.
2. Click **Yes** to confirm the deletion or click **No** to cancel the deletion.

Interaction Feedback Settings

Use this page to configure Interaction Feedback settings.

Prompts Path

Type the path from which the survey prompts are loaded. The default value for the prompts is \\[server name]\IC\Resources\\SurveyPrompts.

Recordings Path

Type the path where the recorded surveys are stored. This is where free-form survey answers are stored. The default value for the recordings is \\[server name]\ICompressed Recordings\.

Audio Compression

Select the Audio Compression protocol to use when compressing survey recordings. The values are: audio/PCMU, audio/PCMA, audio/GSM, audio/x-truespeech, and audio/G726-32. The default value is audio/x-truespeech.

Enable Audio Encryption

Select this check box to enable audio encryption. *This feature will be available in a future release*.

Fax Configuration

Fax Configuration

The configuration options in this container provide the ability configure fax appearance, send and receive options, servers and fax groups. All faxing is done through media server.

How Media Server Faxing Works

When receiving a fax, the call comes into the system, telephony services looks for fax tones using the media server for the audio processing. If the call is determined to be a fax call it is, then the call is forwarded to handlers that decide how to process it. Typically, a handler asks the fax server to receive the fax. The fax server asks telephony services to connect the call to the media server and it sets up a fax termination there. The media server does all of the processing to emulate a fax machine. It stores the fax locally in a TIFF file format, and sends notifications to the fax server when pages complete, errors occur, etc. Once the fax is complete the fax server gets the TIFF file from the media server via HTTP and converts it to *.i3f format (the CIC fax file format). The handlers determine how to process the received fax.

Sending a fax is similar; the same process happens in reverse. If the source pages need conversion (e.g., conversion of a PDF) before sending a fax, a render server can be used instead of the fax server to off-load PDF conversions to relieve processing burden of the CIC server.

This container has the following fax configuration pages:

- Appearance
- Send/Receive Options
- Fax Server
- Advanced

Related topics

Fax Group Configuration

SIP Line Configuration

Appearance

Use this page to configure the appearance options for server faxes. This information is sent as part of the outgoing fax notification.

Header Text

Type the text to appear in the top margin on each page, the area called the page header. The length of the text is limited to 256 characters. If this field is left blank, no text will appear at the top of each page.

Cover Page

Select the cover page (.I3C file) to use as the default cover page sent as the first page of each fax. If values are not specified by the sender in Interaction Fax Viewer, the values specified in the fields below (that is, Name, Company Name, Fax Number, Display Number, and Voice Number) are used in the corresponding fields on the cover page.

Cover pages are stored in the same directory as the Interaction Fax Cover Page Editor (that is, the \bin directory under your IC root directory). Use the Interaction Fax Cover Page Editor (IFaxCovrA.exe) to create or modify cover pages.

Name

Type the default name of the person sending the fax.

Company Name

Type the default name of the company sending the fax.

Fax Number

Type the default phone number for the sending fax device.

Display Number

Type the sending fax phone number. This number is displayed on the receiving fax station's display window and in the fax log. Typically, it is the same number as the **Fax Number** field.

Voice Number

Type the default voice phone number where the fax recipient should call to reach the person sending the fax.

Related topics

Send and Receive Options

Fax Server

Advanced

SIP Line Configuration

Send/Receive Options

Use this page to configure send and receive options for faxes.

Fax Group

Select a fax group from the pull-down menu. A fax group is a group of fax resources on the media server dedicated for that particular purpose.

Fax Speed

Select the fax transmission speed from the pull-down menu according to the fax modem capacity of the recipients. This speed is the maximum receive baud rate in bps. The default value is 4800 bps. Use "Best" for the maximum support speed by device.

Number of Retries

Use the up and down arrow keys to select the number of times the system will retry to send a fax if it fails to send it on the first attempt (for example, the line is busy or down). The default number of retries allowed for a fax send is 3.

Retry Delay (sec)

Use the up and down arrow keys to select the delay in seconds that the system should wait between the end of a fax failure and the next time it tries to send. The default value is 30 seconds.

No Answer Timeout (sec)

Use the up and down arrow keys to select the time in seconds the system should wait before determining there is no answer when a called fax number rings but does not connect. If the number does not answer within this amount of time, the system terminates the attempted call. The default value is 30 seconds, which represents approximately five rings (in North America).

Do Not Send Faxes During Peak Hours

Select this check box to not send faxes during peak hours as defined in the **Begin** and **End** times in **Peak Hours** below. If selected, the system will not send a fax during the time range entered. For example, if this option is enabled, **Begin** is set to "08:00", and End is set to "20:00", then no faxes will be sent from 8:00am through 8:00pm.

The default peak hours are 07:00 for beginning time, and 22:00 for ending time.

> **Note**: The time is based on the time zone of the fax server.

Max Fax Call Rate (cps)

Use the up and down arrow keys to select the maximum calls per second or rate that the media server process faxes. The default value is 5 calls per second. The valid range is 1 to 10 million calls per second.

Related topics

Media Server Fax Configuration - Appearance

Media Server Fax Configuration - Fax Server

Media Server Fax Configuration - Advanced

SIP Line Configuration

Fax Server

Use this page to configure fax server options.

Servers

You can optionally use a render server and external fax converter for media server faxing.

Use IC Render Server

Select this option to use the IC render server as the fax server. When selected, enter the name of the server in the **Server** field. By default this setting is not enabled. When it is enabled, the default value is the local host.

The render server is used instead of the fax server to off-load PDF conversions to a remote server. This relieves some of the processing burden of the IC server. For information see *CIC Render Server Technical Reference* in the **Technical Reference Documents** section in the PureConnect Documentation Library on the CIC server.

Use External Fax Converter

Select this option to use an external fax converter such as Adobe for converting faxes instead of pdf2image. By default this setting is not enabled. when enabled, CIC uses third-party software installed on the IC render server to convert fax files, so using this setting is not recommended. For information see *IC Render Server Technical Reference* in the **Technical Reference Documents** section in the PureConnect Documentation Library on the CIC server.

Options

Use this section to set fax server options.

Discard Partial Pages on Failure

Select this option to discard partial fax pages on a fax error. By default, this setting is not enabled. Default unchecked. If enabled, the user receives an email message listing only the pages that succeeded when inbound faxes fail during transmission. If a page is partially received, that page is not sent in an email message to the user.

Notify Event Viewer on Failure

Select this option to send fax failures to the event viewer.

Use Error Correction Mode

Select this option to use Error Correction Mode (ECM) when sending a fax. By default this setting is not enabled. ECM breaks image data into HDLC (High-level Data Link Control) frames and multiple fields, which each hold 256 or 64 octets of image data. There is 16 bit Frame Checking Sequence (FCS) used to check for transmission errors.

Use Call Analysis

Select this option to detect answering machines, SIT tones, or live response to calls when sending a fax. By default this setting is checked (enabled), which means faxes are terminated immediately for cases such as live responses, and a description of the termination is provided.

Override Default Paths

You can optionally override default paths.

Cover Pages

This is the fax cover page directory used by the fax server. The default path for cover pages is \\[server name]\IC\Resources\CoverPages. If Interaction Administrator is installed on the CIC server, then you may click **Browse...** to change the location.

Fax Files

This is the work directory used by the fax server. The default path for fax files is \\[server name]\IC\Work\FaxWork. If Interaction Administrator is installed on the CIC server, then you may click **Browse...** to change the location.

Related topics

Appearance

Send and Receive Options

Advanced

SIP Line Configuration

Advanced

Use this page to configure advanced options for faxing.

Web Server Options

Address to Use

Select the interface name from the drop-down list. This is used to determine the local server IP address. The default value is <All>, and "Local Area Connection" is an option. CIC supports IPv4 and IPv6 addressing schemes.

HTTP Port

Select the local port from the drop-down list to use for servicing HTTP requests. The default port is "8112". Acceptable values are between "2000" and "65535".

Use HTTPS

Select this check box to specify whether resources are only served through a TLS connection. HTTP requests will be re-directed to the HTTPS port. Enter the **HTTPS Port** when selecting this check box.

HTTPS Port

Select the secure local port from the drop-down list to use for servicing HTTPS requests. The default port is "8113". Acceptable values are between "2000" and "65535".

Host Format

Select which format from the drop-down list to use for resolved URI authorities. The default value is “FQDN” (Fully Qualified Domain Name), and the other options are “IP” (Internet Protocol), “Host Name”, or “Custom”. If you choose "Custom", then a text box appears that you may enter any desired text.

Cache Options

Remove Unversioned Files After (sec)

Use the up and down arrows to set the time in seconds before unversioned files are removed from the cache. The default value is "600".

Remove Unused Files After (sec)

Use the up and down arrows to set the time in seconds before unversioned files are removed from the cache. The default value is "600".

Only Cleanup Idle Files Every (sec)

Use the up and down arrows to set the time in seconds between cache cleanups. The default value is "300".

Only Update File Attributes Every (sec)

Use the up and down arrows to set the amount of time in seconds that has to elapse before a cached prompt will be queried for freshness. This is an optimization to prevent unnecessary file refreshes. The default is "10".

Related topics

Appearance

Send and Receive Options

Fax Server

SIP Line Configuration

Fax Groups

Fax Groups

This section contains the following information:

Fax Group Names

Fax Group Configuration

Fax Group Names

Type a descriptive name for a fax group, which is a group of fax resources dedicated for a particular purpose.

Fax Group Configuration

A media server fax group is a named group of media server fax resources. The system automatically creates a fax group named <DefaultFaxGroup>.

Description

Type a sentence that describes the purpose of this group of media server fax resources.

Maximum Number of Faxes

In the **Inbound** field enter the maximum number of inbound faxes allowable, or select **No Limit** to be limited by only the number of fax licenses available.

In the **Outbound** field, enter the maximum number of outgoing faxes allowable, or select **No Limit** to be limited by only the number of fax licenses available.

Related topics

Media Server Fax Configuration

IC Data Sources

Overview of CIC Data Sources and Contact Lists

Some components of CIC depend on data stored in a variety of repositories, such as SQL Server databases, Access databases, different Exchange or IBM Domino data sources, and so on.

Rather than tie CIC components directly to an external data source, these components reference a local CIC data source name, which points to a particular type of data repository. This allows CIC developers and administrators to change a data repository without having to change references to that repository.

For example, CIC report logs are currently stored in SQL Server databases and accessed via a CIC data source (called IC Report Logs in this case). This CIC data source points to a SQL Server database and the ODBC DSN to set up connections to the report logs. However, future versions of CIC may store report log data in databases other than SQL Server. Since the report logs and reports point to a CIC data source, they will not have to be reconfigured to support a new data source. Only the CIC data source must be reconfigured.

Contact List Sources in Interaction Administrator use CIC data sources and a particular CIC-specific driver to define contact lists that can appear as directory tabs in the CIC clients.

The default drivers provide access to and a formatted view of the contact data in the specified data source repository. You can create views for contact lists in other kinds of data sources not directly supported in CIC by creating a view into that repository that matches the format of the supported CIC data source repositories.

For example, you can set up a SQL table view as contacts list for a tab instead of a 'real' table, by setting TABLE=<tableOrViewName>; entry in the Additional Information field of the Data Manager Contact List Source (not the CIC data source).

The Contact Data Manager Configuration page controls how the CIC client users access the speed dial data source for a site. This page specifies how many simultaneous write operations can be performed, the name of the speed dial data source, and a control to refresh connections to the data source repository.

IC Data Source Name

Type the name of an IC data source that generally describes the kind of data another part of CIC might need to access. CIC data sources generically define a gateway to a particular kind of data repository, including:

- An ODBC database
- A JDBC interface to an ODBC database
- The old JDBC-ODBC database interface
- Lightweight directory access protocol (LDAP)
- White Pages directory data

CIC data source names appear in the **Type** field in the **Contact List Sources Configuration** page. The Contact List Sources actually define the directory pages that can appear as a directory view in the CIC clients (such as Company Directory).

IC Data Source Configuration

IC Data Source Configuration

Some components of CIC depend on data stored in a variety of repositories (such as SQL Server databases, Access databases, different Exchange or IBM Domino data sources). Rather than tie CIC components directly to an external data source, these components reference a local CIC data source name, which points to a particular type of data repository. This allows CIC developers and administrators to change a data repository without having to change references to that repository.

For example, CIC report logs are currently stored in SQL Server databases and accessed via a CIC data source (called IC Report Logs in this case). This data source points to a SQL Server database and the ODBC DSN to set up connections to the report logs. Since the report logs and reports point to a CIC data source, they will not have to be reconfigured to support a new data source. Only the CIC data source must be reconfigured.

CIC supports basic data sources, including:

- ODBC - for most relational databases that include an ODBC driver (for example, SQL Server and Oracle)
- JDBC - for Java applications that use JDBC drivers to access ODBC compliant databases (not used in CIC by default)

- JDBC-ODBC - for the JDBC-ODBC bridge to let Java applications access ODBC compliant databases via ODBC drivers.
- MAPI - CIC no longer supports Microsoft Exchange MAPI-based integrations.
- LDAP - for contact directories that use an LDAP-enabled directory server.
- White Pages - for white pages directory data on the IC server.

Click on the above data source types to see help on how to configure that data source.

ODBC Data Source Configuration

IC Data Sources > *<Data source>* > IC Data Source Configuration > ODBC Data Source Configuration

Select the appropriate values or enter the appropriate configuration data to create a CIC data source for an ODBC-compliant data repository.

If you use an ODBC data source for speed dial entries, it must have identical data layout as the SQL Server SpeedDial table (found in I3EIC.mdb on the SQL Server computer), and it must provide read/write access. Alternatively, if the layout is not identical, you must create a view to match the data layout.

Subtype

This is an ODBC data type. Therefore, Subtype is one of the listed ODBC compliant relational databases, or another database that includes an ODBC driver. The default setting is "DB2 Family", and other options are "Informix", "Ingres", "Oracle", "MS Access", "MS SQL Server", "Sybase", and "Other".

Read Only

Select this check box if CIC client users cannot update this data source. Clear the check box if CIC client users will be able to add, modify, or delete entries in this data source.

File DSN

Select this check box if the ODBC driver requires a file Data Source Name.

ODBC DSN

Type the name of the System Data Source Name field in the ODBC Administrator used to create the data source. The DSN must be a System DSN, not a User DSN.

Qualifier

If one is required, type the table qualifier used to access the tables in this data source. The qualifier may be the owner or creator of the table, or it may be the path to the table, depending on the database.

User ID

Type a user ID if one is required to connect to the data source.

The user ID is determined by the administrator and the database tool used to create the data source.

Password

Type a password if one is required to connect to the data source.

The password is determined by the administrator and the database tool used to create the data.

Manually enter connection string

Select this check box if you wish to manually enter an ODBC connection string in the **Connection String** field below.

Connection String

This field remains blank unless you first select the **Manually enter connection string** check box above. Type the customized ODBC connection string to connect to the target database. This uses the Qualifier entered above, if any.

Additional Information

Some CIC data sources may need to specify additional information or need a way to temporarily override the default behavior. Values in this field could include the Catalog= and Schema= statements, as illustrated in the IC Report Logs CIC data source.

For example:

DATABASE=i3_eic;SERVER=(local)

Related topics

Overview of CIC Data Sources and Contact Lists

Report connection configuration

Configure reports for your CIC server

JDBC Data Source Configuration

Select the appropriate values or enter the appropriate configuration data to create a CIC data source for a JDBC compliant data repository.

Subtype

This is a JDBC data source. Subtype is one of the listed ODBC compliant relational databases, or another database that can be accessed by a JDBC driver. The default setting is "DB2 Family", and other options are "Informix", "Ingres", "Oracle", "MS Access", "MS SQL Server", "Sybase", and "Other".

Read Only

Select this check box if CIC client users cannot update this data source. Clear the check box if CIC client users will be able to add, modify, or delete entries in this data source.

User ID

Type a user ID if one is required to connect to the data source.

> The user ID is determined by the administrator and the database tool used to create the data source.

Password

Type a password if one is required to connect to the data source.

> The password is determined by the administrator and the database tool used to create the data.

Qualifier

If one is required, type the table qualifier used to access the tables in this data source. The qualifier may be the owner or creator of the table, or it may be the path to the table, depending on the database.

Driver

Type the name of the JDBC driver (you may have to ask the vendor for your driver name).

URL

Type the URL used to connect to this JDBC data source. This uses the Qualifier entered above, if any.

Additional Information

Some CIC data sources may need to specify additional information or need a way to temporarily override the default behavior. Values in this field could include the Catalog= and Schema= statements, as illustrated in the IC Report Logs CIC data source.

For example:

DATABASE=i3_eic;SERVER=(local)

JDBC-ODBC Data Source Configuration

Select the appropriate values or enter the appropriate configuration data to create a CIC data source for an ODBC compliant data repository.

> **Note:** If you use an ODBC data source for speed dial entries, it must have identical data layout as the SQL Server SpeedDial table (found in I3EIC.mdb on the SQL Server computer), and it must provide read/write access. Alternatively, if the layout is not identical, you must create a view to match the data layout.

Subtype

This is a JDBC-ODBC data source. Subtype is one of the listed ODBC compliant relational databases, or another database that includes a Type 1 ODBC driver. The default setting is "DB2 Family", and other options are "Informix", "Ingres", "Oracle", "MS Access", "MS SQL Server", "Sybase", and "Other".

Read Only

Select this check box if CIC client users cannot update this data source. Clear the check box if CIC client users will be able to add, modify, or delete entries in this data source (that is, it is Read/Write accessible).

ODBC DSN

Type the name of the System Data Source Name field in the ODBC Administrator used to create the data source. The DSN must be a System DSN, not a User DSN.

Qualifier

If one is required, type the table qualifier used to access the tables in this data source. The qualifier may be the owner or creator of the table, or it may be the path to the table, depending on the database.

User ID

Type a user ID if one is required to connect to the data source.

> The user ID is determined by the administrator and the database tool used to create the data source.

Password

Type a password if one is required to connect to the data source.

> The password is determined by the administrator and the database tool used to create the data.

Manually enter connection string

Select this box to manually enter an ODBC connection string in the **Connection String** field below.

Connection String

This field appears dimmed and is unavailable, unless you first select the **Manually enter connection string** box above. Type the customized ODBC connection string to connect to the target database. This uses the Qualifier entered above, if any.

Additional Information

Some CIC data sources may need to specify additional information or need a way to temporarily override the default behavior. Attributes in the **Additional Information** field could include the Catalog= and Schema= statements, as illustrated in the IC Report Logs CIC data source. For example:

DATABASE=i3_eic;SERVER=(local)

> Multiple attributes are separated by semicolons (;).

LDAP Data Source Configuration

IC Data Sources > *<Data source>* > IC Data Source Configuration > LDAP Data Source Configuration

Use the following to configure an LDAP-compatible data source.

> **Tip**: For more information, see *Using LDAP for IC Contact Lists*, in the PureConnect Documentation Library.

Subtype

This is an LDAP data type. The options are Other, iPlanet, OpenLDAP, and Active Directory.

Read Only

Select this check box if CIC client users cannot update this data source. Clear the check box if CIC client users will be able to add, modify, or delete entries in this data source (that is, it is Read/Write accessible).

Host Name

Type the name of the Netscape Directory Server. For example: BocaSitePC

Port

Type the port number used by the Netscape Directory Server. If blank, then the default **389** is used.

Bind DN

The **distinguished name** (DN) used to authenticate the password. This should be in the format: domain\user name.

For example:

Uid:AiriusDomain\ic_admin, ou=People, o=Airius.com

Password

The password used to bind with.

Search DN

The **distinguished name** (DN) of the node where searching begins.

> **Note:** Because a search DN is usually specified in the contact list source, any information added here is overridden. Typically, this field is left empty.

Additional Information

This field can indicate the connection to specific authentication types. Use the following format: auth=xxx

Examples:
auth=ssl+simple
auth=ssl
auth=tls+simple
auth=tls

If you do not use this field to indicate an authentication type, the system uses the authentication type selected during the installation of Interaction Web Portal.

This field can indicate the timeout values for Interaction Web Portal. Use the following format: search=xxx;load=xxx;bind=xxx

Example: search=1030;load=4002;bind=12345

search indicates the time in milliseconds that Interaction Web Portal attempts to search (for example, search for a user, workgroup, or interaction) before timing out and returning an error. If you do not use this parameter, Interaction Web Portal uses 8000 milliseconds.

load indicates the time in milliseconds that Interaction Web Portal attempts to load a page or view before timing out and returning an error. If you do not use this parameter, Interaction Web Portal uses 4000 milliseconds.

bind indicates the time in milliseconds that Interaction Web Portal attempts to bind to the LDAP connection before timing out and returning an error. If you do not use this parameter, Interaction Web Portal uses 4000 milliseconds.

If you do not use this field to indicate the timeout values, Interaction Web Portal uses the default of 8000 milliseconds for searching, 4000 milliseconds for loading and binding.

> **Tip**: For additional information about how CIC supports LDAP-enabled Netscape directory servers, see *Using LDAP for IC Contact Lists* in the PureConnect Documentation Library.

MAPI Data Source Configuration

> CIC no longer supports Microsoft Exchange MAPI-based integrations. Use a Microsoft Exchange EWS-based integration as the alternative. The options for configuring Microsoft Exchange MAPI-based integrations remain visible in Interaction Administrator but setting the options no longer enables Microsoft Exchange MAPI-based integrations.

White Pages Data Source Configuration

Use this dialog box to configure your White Pages data sources. CIC includes two White Pages data sources, I3 Text File and Redi-Connect. You may add other data sources to the list if you wish.

Subtype

In the Subtype list, select the data source to configure. Among the choices of compliant databases could be:

Data Source	Description
I3 Text File	Select this to add the WhitePages.txt database. CIC knows which driver to add.
Think Direct Marketing	**Note:** Think Direct Marketing has been replaced by Redi-Connect. Do not select this option.
Redi-Connect	Select this to add the Redi-connect database. CIC knows which driver to add. **Note**: Redi-connect is a realtime lead verification service that you must be registered to use.
Other	Select this to add a third-party driver for another White Pages data source.

Read Only

Select this check box if CIC client users cannot update this data source. Clear the check box if CIC client users will be able to add, modify, or delete entries in this data source (that is, it is Read/Write accessible).

Connection Information

If the driver requires a User ID, Password, or Program ID, type it in one of the following fields:

Field	Description

User ID	Type your Redi-Connect ClientID, which Redi-Data provided to you. Leave the other fields blank; you do not need to specify any additional information to configure this driver.
Password	Type a password to access the data source. I3Text File and TDM do not require a password.
Program ID	If the driver Subtype is **Other**, you must type a Program ID (PROGID). An example PROGID could be I3PDBwp.Rwp.1

> Type any additional information your driver may require, (in ATTRIBUTE=VALUE; syntax). This is optional information, not required for I3Text and Redi-Connect drivers.

Reverse White Pages Lookup Sequence

You can configure any public Data Manager contact list source to participate in the reverse white page (RWP) lookup sequence. By default, Data Manager searches CIC *businessphone*, *businessphone2*, and *homephone* attributes. However, you can configure each contact list source to have its own list of phone attributes to search on. This is specified with the RWP_LOOKUP_PHONE_TYPES attribute.

Follow these steps.

1. From Interaction Administrator, select **Contact List Sources**, and then press the **Insert** key.
2. Type the name of a new white pages contact list source, and then click **OK**.
   The Contact List Source Configuration window appears.
3. From the **IC Data Source** list, select the name of the white pages data source that you previously created.
4. Select the **Public** option for public contact sources, if applicable.
5. From the **Driver** list, select **White Pages**.
6. Type the appropriate attributes in the **Additional Information** box, for example:

   RWP_LOOKUP_PHONE_TYPES=HomePage,BusinessPhone,BusinessPhone2,Mobile;

   You can use any combination upper- or lower-case letters for the RWP_LOOKUP_PHONE_TYPE attribute and phone number type values. Valid phone number types are:

- BusinessPhone
- BusinessPhone2
- HomePhone
- HomePhone2
- AssistantPhone

- Mobile
- Fax
- Pager

If an LDAP source is included in the RWP lookup sequence, then you must index each phone number that you want Data Manager to search for. For information about adding indexes, see *Using LDAP for IC Contact Lists* in the PureConnect Documentation Library.

Report Connection Configuration

IC Data Sources > *<Data source>* > IC Data Source Configuration > Report Connection Configuration

This page lets you configure the connection to an Oracle or SQL Server data source for the purposes of running reports. For more information about reports, see the *CIC Reporting Technical Reference* in the PureConnect Documentation Library.

About Internet enabled reports

Beginning in CIC 2016 R3, you can configure a data source to run Crystal Reports in IC Business Manager with a direct connection to the database server via the Internet. If you do this, you must also configure reports for your CIC server.

If you are adding an Oracle data source for Internet enabled reporting, after you save the fields on this page, you must re-open this page to specify the Oracle service name and to view the client TNS entry.

Select method to connect to data source

- To connect through the CIC server, select **Direct client connection to the data source.** This is the default configuration.
- To enable a direct connection to the database server via the Internet, select **Proxy through HttpPluginHost**.

Port number to proxy report connection on client workstations

Oracle data sources only (required)

Type the port number for your proxy report connection. The valid range of port connections is 1024-64000.

Oracle service name

> **Note:** This field appears only when you edit an existing Oracle data source.

Type the Oracle service name to which the reports will connect.

View client TNS entry button

> **Note:** This button appears only when you edit an existing Oracle data source.

Click this button to view the TNS entry in Notepad. Copy the TNS and paste it to each of the client workstations. This points the TNS entry to the reporting proxy instead of the database.

Related topics

ODBC Data Source Configuration

Configure reports for your CIC server

Contact Data Manager

Contact Data Manager

This section contains the following information:

Contact Data Manager Configuration

Contact Data Manager Icons

Contact List Sources Configuration

Contact Data Manager Configuration

Data Manager configuration covers all data sources used to display contact information on the Directory and Speed Dial views in the CIC clients. Specific data source configuration is discussed in the IC Data Source Configuration page found under the Data Manager container.

Thread Pool Size

Type a number to specify how many threads are available for data operations between CIC client speed dial pages and the CIC server. A higher number of threads requires more server system resources. A lower number increases the possibility of contention for the threads needed to access the speed dial data sources.

Each data operation request (for example, database read, database update, and so on) is performed in a separate thread on the server. When the operation is complete, the used thread is returned to a pool of available threads. The Thread Pool Size value determines the maximum number of simultaneous data operations (16 by default). If more than sixteen (16) data operations occur at the same time, the seventeenth (17)--and subsequent--operation will have to wait until an operation completes and a thread becomes available.

To see if users require more than the default 16 threads, check the Windows Server’s Event Viewer program found in the Administrative Tools folder. Look at the Event Details of the Data Manager application events to see if the number of requests exceeds the number of available threads.

Speed Dial Source

Select the data source containing the speed dial data for this site. The names in this list are based on the data sources defined in the Contact List Sources container. The default CIC Contacts database is contained in a SQL Server database. This database contains the Contacts and the SpeedDial tables.

> If you use an ODBC data source for speed dial entries, it must have identical data layout as the SQL Server SpeedDial table, and it must provide read/write access.

Refresh Connections

Click this button to cause CIC to quickly drop and reestablish connections to the contact list data sources. This may be necessary if one or more of the contact list data sources hangs or crashes.

Reverse White Pages Lookup Sequence

The program allows you to arrange your contact lists in the order they should be searched.

Use the **Reverse White Pages Lookup Sequence** box to arrange the lists to:

- Add a contact list, click **Add**. In the Entry Name dialog box, select a list in the drop-down box and click **OK**
- Change the lookup sequence, select a list and use the **Up** and **Down** buttons
- Remove a list, select it and click **Remove**

> **Note:** You cannot add private contact list sources if Interaction Tracker is not licensed.

Contact Data Manager Icons

Each speed dial button on the CIC client interface can have an icon to identify the kind of phone number displayed for each contact. For example, if the contact named Jeff Swinson has phone numbers for home, business, fax, and pager, Jeff's name appears only once in the list, but you can select one of the numbers to display by default. Each kind of phone number can have a different icon to help CIC client users quickly identify which number is displayed.

Select a path, parameter, or a full path and file name with an .ICO extension that contains an icon representing each phone number type. The directory that contains the default CIC icon files is \\Server\IC_Client\IC_Client\Resources where Server is the name of your CIC server computer.

Business Phone

Click **Browse** and select the name of an icon file to appear beside Business Phone numbers. For example:
\\Server\Resources\BusPhone.ico

Business Phone2

Click **Browse** and select the name of an icon file to appear beside secondary Business Phone numbers. For example:
\\Server\Resources\BusPhone2.ico

Assistant Phone

Click **Browse** and select the name of an icon file to appear beside your contact's Assistant Phone numbers. For example:
\\Server\Resources\AsstPhone.ico

Home Phone

Click **Browse** and select the name of an icon file to appear beside Home Phone numbers. For example:
\\Server\Resources\HmPhone1.ico

Home Phone2

Click **Browse** and select the name of an icon file to appear beside secondary Home Phone numbers. For example:
\\Server\IC_Client\IC_Client\Rresources\HmPhone2.ico

Mobile Phone

Click **Browse** and select the name of an icon file to appear beside Mobile Phone numbers. For example:
\\Server\Resources\MobPhone.ico

Fax Phone

Click **Browse** and select the name of an icon file to appear beside Fax Phone numbers. For example:
\\Server\Resources\FaxPhone.ico

Pager Phone

Click **Browse** and select the name of an icon file to appear beside Page Phone numbers. For example:
\\Server\Resources\Pager1.ico

Contact List Sources

Contact List Sources Configuration

Select the appropriate values to define a contact list source that can appear as a directory view in the CIC clients.

IC Data Source

Select one of the existing CIC data sources that represent the kind of repository holding the contact list data. If no names appear in this list, go to the IC Data Sources container and create a CIC data source first.

Label

This is the name displayed in the CIC clients for this contact list. The default value is the actual name used in the contact list.

Public

Use this check box to specify if this contact list is public or private. A public data source contains contacts accessible by all users and a private data source is accessible only to the user who enters or owns the contacts.

Has Status

Use this check box specify whether this data source supports status information.

Driver

Select one of the predefined CIC drivers that provide access and formatting to the data in the target data source.

IC Driver	Provides access to:
IC Exchange Contacts	A public address list on the Exchange server
IC Outlook Contacts	An individual address list on the Exchange server
IC Contacts	Contact data in an ODBC compliant database
IC LDAP Contacts	Data in an LDAP-enabled directory server
IC White Pages	The white pages directory data on the CIC server
IC Tracker Contacts	Interaction Tracker contact data on the CIC server

> **Note:** There currently is no support for selecting specific organizations or sub-organizations, only the global address list in Exchange.

Contact List Sources - Options

Add values for the following contact list source options.

Timeout (sec)

Type the number of seconds CIC should wait for a response from the data source before returning an error. If you leave this field blank, CIC uses the default timeout value of 60 seconds.

Query Row Limit

Enter the maximum number of rows the CIC data source can return in one query of the data source. The default value is 1000 rows.

Note: If you are configuring Interaction Tracker contact list sources, consider your operating conditions when setting the values for Timeout and Query Row Limit:

Timeout (sec)

• Under normal operating conditions, set the value to 300.

• Under heavy load or high tracing conditions—for example when diagnosing a problem—set the value to 900.

Query Row Limit

Set the value for this box to no less than 500,000. You can increase this value if needed by the client site. It should be higher than the combined counts of Individuals, Addresses, Attributes and Connections.

Contact List Source Name

Type a descriptive name of the contact list you wish to make available as a directory tab in the CIC clients.

Note: The name you type appears as a selection in the CIC clients.

CIC LDAP Contacts

You can add configuration information to extend the settings of an LDAP contact. In the **Additional Information** box, use the following syntax:

```
<Attribute>=<Value>[;<Attribute>=Value…]
```

Where:

Syntax	Description
Attribute	Uppercase or lowercase letters are allowed. Case is not preserved.
Value	Uppercase or lowercase letters are allowed. Case is preserved.
=	Blank spaces around equal sign (=) are allowed. When Value contains one or more equal signs (=), then Value must be enclosed by double quotation marks.
;	Blank spaces around semi-colon (;) are allowed. When Value contains one or more semi-colons (;), then Value must be enclosed by double quotation marks.

Additional Information attributes:

Search_DN=

Use to override the search DN specified in the Interaction Administrator CIC Data Source configuration. In LDAP, a search involves three parameters:

Parameter	Description
SEARCH_DN=	A place (node) in the directory tree to start searching from.
SEARCH_FILTER=	A filter/query to be applied to the contact entries.
SEARCH_SCOPE=	A specification for how/if the search is to proceed down the tree.

> **Tip**: When specifying the search DN, enclose the string in double quotation marks (" "), since the standard DN format contains equal signs (=).

You can use one or more user substitution variables inside the DN; this is particularly useful when setting up private contacts (see USERNAME_MAPPING_FILE= below).

In addition, you can use one or more built-in substitution variables. They are:

Variables	Description
$ICUID	The CIC user ID. Generally only useful for private contact sources.
$CONTACTSOURCE	The name of the contact list source used by the Data Manager. For example: Our Public Contacts.
$BINDDN	The DN used to bind with, as specified in the Interaction Administrator CIC Data Source configuration.

> **Note:** The above variables must be all uppercase letters.

SEARCH_FILTER=

Contains, in LDAP search syntax, the search filter/query to be used.

For example: (&(objectclass=i3person)(i3owner=$ICUID))

You can use one or more user substitution variables inside the DN; this is useful when setting up private contacts (see the section on USERNAME_MAPPING_FILE= below).

In addition, you can use one or more built-in substitution variables. They are:

Variables	Description
$ICUID	The CIC user ID. Generally only useful for private contact sources.
$CONTACTSOURCE	The name of the contact list source used by Data Manager. For example:

	Our Public Contacts.
$BINDDN	The DN used to bind with, as specified in the Interaction Administrator CIC Data Source configuration.
$SEARCDN	The search DN as specified in the Interaction Administrator CIC Data Source configuration (SEARCH DN field), or as overridden in the contact list source.
$SEARCHDNPARENT	The parent DN of the configured search DN.

Note: These variables must be all uppercase letters.

SEARCH_SCOPE=

Specifies how/if the search proceeds down the sub-tree rooted by the search DN. This attribute can have one of three values:

Values	Description
ONE	Searches only entries directly below the search DN. This is the default.
SUB	Starts the search at the base DN and then searches everything below, including the base DN.
BASE	Searches only the base DN entry.

ATTRIBUTE_MAPPING_FILE=

By default, CIC uses an object class called **i3person** (which inherits from **inetorgperson**) for storing contact information. However, you are free to choose whatever object class you like, including a custom object class. To do this, you must create a file that contains the mappings between the CIC attributes and the attributes of your object class. CIC provides two sample mapping files, I3PERSON_MAP.TXT and INETORPERSON_MAP.TXT, that contain syntax and usage documentation in the files themselves.

Note: I3PERSON_MAP.TXT is provided for informational purposes, and – unless you want to modify any of the defaults – you do not need to have an ATTRUBUTE_MAPPING_FILE= entry, since CIC knows about the mapping for the i3person object class.

USES_FOLDERS=

The default is True. Set to False if the contact entries are not rooted by a folder/container entry that you want CIC to create. CIC has a default folder object class called i3genfolder that you can use.

FOLDER_ATTRIBUTE_FILE=

You can use your own folder type (such as a folder other than i3genfolder) and still have CIC automatically create the folders to contain your contacts. To do this you must create a file that contains information about the attributes of the folder object class you wish to use. An example file

I3GENFOLDER_MAP.TXT is provided whose syntax and usage is the same as the attribute mapping file and is documented in comments inside the file itself.

> **Note:** CIC knows about the mappings for i3genfolder, so unless you need to modify the defaults, you don't need to have a FOLDER_ATTRIBUTE_FILE= entry if you plan on using the default i3genfolder object class.

RDN_ATTRIBUTE=

Each newly created contact must have a globally unique distinguished name (DN). The left-most component of a distinguished name is called a *relative* distinguished name (RDN), and contains the attribute-value pair that uniquely defines the contact entry within the current directory. By default, Data Manager will use the *userid* attribute as the attribute for the RDN. However, you can choose whatever attribute you want by setting this attribute.

> **Note:** Even though you can specify any attribute as an RDN attribute, Data Manager will always set it to a unique timestamp value (for example "2000092314564500010000"). Therefore, when choosing an RDN attribute, make sure the semantics of the attribute are such that a unique timestamp value like this will not cause any problems.

USERNAME_MAPPING_FILE=

When accessing private contacts, the only information CIC has when distinguishing one user's contact data from another user's contact data is the CIC user ID value. These values might or might not be the same as the LDAP user ID attribute's values.

If they are not the same, you can set up a file to specify the mapping from the CIC user ID to the LDAP user ID. In fact, you can do this even if they are the same in order to specify other substitution values for a user.

The ICUSER_MAP.TXT example mapping file provides syntax and usage documentation.

> **Tip**: For additional information about how CIC supports LDAP-enabled Netscape directory servers, see *Using LDAP for CIC Contact Lists* located in the PureConnect Documentation Library.

LDAP contact list attributes

Syntax for public contact source that uses the default folders:

SEARCH_DN="cn=$CONTACTSOURCE, ou=People, o=Airius.com";

Syntax for private contact source that uses the default folders:

SEARCH_DN="cn=$CONTACTSOURCE, uid=$ICUID, ou=People, o=Airius.com";

Syntax for private contact source that does not use the default folders:

USES_FOLDERS=FALSE; SEARCH_DN="uid=$ICUID, ou=People, o=Airius.com";SEARCH_FILTER="(objectclass=i3person)";

Web Services

Preparing to Use Web Interactions

If your site uses CIC's Web Services to process web interactions, you can create any number of boilerplate text messages, standard URLs and text files for agents to easily send to web visitors. In addition, you can optionally have each agent's picture appear on the dialogs that visitors see.

How it Works

> You must have CIC's web services installed and configured on your web server (see *Interaction Web Tools Technical Reference* in the PureConnect Documentation Library on the CIC server).

- When a visitor requests an interactive **Chat** session or an **Instant Question**, an agent is alerted by the CIC client and can "pick up" the interaction request.
- For a chat, a dialog pops up on the agent's workstation enabling the agent to begin an interactive typing session with the customer. The **Responses** tab of the agent's Chat dialog can contain the names of preset standard text messages, URLs to which the agent can push the visitor's browser, and text file names. The agent can drag any combination of these responses into the **Response** field.
- For an **Instant Question**, the agent's Responses tab can contain the same mix of items. However, if the agent drags a URL into the Response field the program sends only the URL address as text and does not push the visitor's browser.

For more information on how to use the Chat dialog interface, see the help for the CIC client.

Creating Text Messages and URLs

- Use the Interaction messages sub-container in Interaction Administrator to create preset text that an agent can send to a visitor during an interactive session.
- Use the Interaction URLs sub-container in Interaction Administrator to create a list of standard URLs from which agents can select during an interactive session. The URLs can point to HTML documents on your website or other websites.

- In a **Chat** session, drag a URL to the Send field and click Send to push the visitor's browser to that URL. Alternatively, the agent can drag the URL directly into the Conversation pane and immediately push the Web visitor's browser to that address.
- In an **Instant Question**, drag the URL to the **Response** pane and click **Send to** send the URL in the message as text.
- Use the Interaction files sub-container in the Interaction Administrator to create a list of text file names from which agents can select during an interactive session.

> You control which Chat text messages and URLs appear on the Chat dialog for each agent by using the Access Control page on the Default User, Users, Roles, and Workgroups configuration pages.
>
> For example, you can create a group of text messages that address specific technical support issues and another group of text messages that answer typical marketing information requests. You can then make the technical support documents available to all agents in the Tech Support workgroup and all the marketing documents available only to agents in the Marketing workgroup.

Adding the Agent's Picture to the Chat Dialog

You can optionally display each agent's picture to the customer on the Chat dialog. See the "Agent Photo" section in *Interaction Web Tools Technical Reference* in the PureConnect Documentation Library

Also, for more information, see the CIC client help.

Related Topics

Interaction Message Name

Interaction URL Configuration

User Configuration

Web Services Configuration

Use this page to define the settings for the HTTP and HTTPS behavior for Web Services.

> **Notes**: You must have CIC's web services installed and configured on your web server (see *Interaction Web Tools Technical Reference* in the PureConnect Documentation Library on the PureConnect server).
>
> In order for these settings to take effect, restart WebProcessor and WebProcessorBridge.

See also Web Services Parameters.

Web Services Parameters

After installing IC Web Services, the Web Services container appears in Interaction Administrator. In that container you can configure the following chat parameters:

Required Parameters

Parameter	Description
CollaborationLaunchURL	The URL on which the Web Collaboration will start when the agent pushes out the web page to the visitor.
HoldMsg	Message displayed when interaction is placed on hold. Preset to: “%1 has put the conversation on hold.” %1 delimiter is replaced by agent name.
InteractionsAllowedUnitTime	See the description in MaxInteractionsAllowedPerUnitTime the default is 1
MaxActiveInteractionsAllowed	This determines the maximum number of active interactions (web chats/callback) allowed through WebProcessorBridge at any point of time. For example, if its value is 5000. WPB can create 5000 active web chats/callbacks. If 10 chats/callbacks are disconnected, WPB can create another 10 web chats/callbacks. This limitation doesn't apply on intercom chats/callbacks. The default is 5000.
MaxAnonymousInteractionsAllowed	This limits the total number of active web chats/callbacks, anonymous users can create at any point of time. the default is 5000.
MaxAnyInteractionsAllowedPerQueue	This limits the total number of active chats and callback requests that are allowed on an ACD queue at any point in time. The default is 5000. Note: The Web Processor adheres to this setting. This setting does not affect the number of active calls, e-mails, and faxes allowed on an ACD queue at any point in time.
MaxInteractionsAllowedPerIP	This limits the total number of active web chats/callbacks that can be created from one IP address at any point of time. The default is 15.
MaxInteractionsAllowedPerUnitTime	MaxInteractionsAllowedPerUnitTime and InteractionsAllowedUnitTime together define the web chat/callback burst time. For example, if

	MaxInteractionsAllowedPerUnitTime = 5 and InteractionAllowedUnitTime = 1, then no more than a burst of 5 chats per 1 second would be allowed. The default is 5.
MaxInteractionsAllowedPerUser	This limits the total number of active web interactions (chats or callbacks), an Interaction Tracker registered user can create at any point of time. The default is 5.
SystemName	Identifies the server name to display as a prefix for server messages. Preset to: IC. For example, if you changed IC to WebAdmin you would see "WebAdmin: DebbiH has joined the conversation." To change the preset value, right-click the parameter name and select Properties. You see the Parameter Configuration dialog where you can enter a new parameter value.
WebCGIRequestTimeout	This is used with the CGI request/response parameter. This time out (in seconds) determines the maximum time a handler can take to reply to the CGI request. The default is 300.

Optional Parameters

The following Web Services parameters are optional and must be set manually in Interaction Administrator.

Parameter	Description
AgentConnectedMsg	Sets the message that appears in the Chat dialog when an Agent joins a chat. Preset to: "<Name> has joined the conversation." A visitor to the Website who has not registered, would appear as WebUser. A visitor who has registered is identified by name. For example, if the agent's ID was TomS, you would see "TomS has joined the conversation." If the visitor was unregistered, you would see "WebUser has joined the conversation." To change the preset value, right-click the parameter name and select Properties. You see the Parameter Configuration dialog where you can enter a new parameter value.
AgentDisconnectedMsg	Sets the message that appears in the Chat dialog when an Agent leaves a chat. Preset to: "<Name> has left the conversation." A visitor to the Website who has not registered, would appear as WebUser. A visitor who has registered is identified by name. For example, if a registered visitor's ID was DebbiH@framis.com, you would see DebbiH@framis.com has left the conversation. To change the preset value, right-click the

	parameter name and select Properties. You see the Parameter Configuration dialog where you can enter a new parameter value.
CallbackAccessControl	In IC 4.0 SU3 or later, this controls whether WPB allows visitors to create callback requests. In IC 4.0 SU4 or later, this also determines whether the radio buttons for both anonymous and authenticated access appear in the webpage where a visitor requests a callback. • 0=block all • 1=allow all • 2=authenticated only • 3=anonymous only Example: If CallbackAccessControl=2 and your custom web interface ignores the presence or absence of supportAuthenticationAnonymous, WPB prevents website visitors from creating anonymous callback requests. Example 2: If CallbackAccessControl=1 (allow all) and MaxAnonymousInteractions=0 (anonymous users cannot start a chat or create a callback request), supportAuthenticationAnonymous is sent from WebProcessor Bridge to the visitor’s browser.
ChatAccessControl	In IC 4.0 SU 3 or later, this controls whether WPB allows visitors to create chat requests. In IC 4.0 SU 4 or later, this also determines whether the radio buttons for both anonymous and authenticated access appear in the webpage where a visitor starts a chat interaction. • 0=block all • 1=allow all • 2=authenticated only • 3=anonymous only Example: If ChatAccessControl=2 and your custom web interface ignores the presence or absence of supportAuthenticationAnonymous, WPB prevents website visitors from creating anonymous callback requests. Example 2: When ChatAccessControl=1 (allow all) and MaxAnonymousInteractions=0 (anonymous users cannot start a chat or create a callback request),

	supportAuthenticationAnonymous is sent from WebProcessor Bridge to the visitor’s browser.
EnableIdleTimeout	0 = Disable timeout. (Default value) 1 = Enable timeout.
IdleDisconnectMessage	Specifies the message sent to all parties after the chat is disconnected. You can customize this default message: "%1 has been disconnected from chat since being idle for %4." %1 = Visitor name %2 = Idle Time %3 = Grace time %4 = Idle Time + Grace Time Curly brackets, {}, are not used. All time display are localized so they appear in the manner in which the visitor is used to seeing them.
IdleWarningMessage	Specifies the warning message sent to all parties after the time defined in PartyIdleTime. You can customize this default message: "%1 has been idle for %2. The party has to type something within next %3 to remain active in chat". %1 = Visitor name %2 = Idle Time %3 = Grace time %4 = Idle Time + Grace Time Curly brackets, {}, are not used. All time displays are localized so they appear in the manner in which the Visitor is used to seeing them.
MaxPollFrequency	Sets the interval after which the Javascript client polls during a chat. the default is 2000ms (2 seconds). Note: Setting this value lower can seem to speed up the pace of a chat conversation, but it increases the CIC server’s workload. Setting it to a higher value eases the CIC server’s workload but can make chats seem sluggish. Recommended values are between 1000 ms and 5000 ms.
PartyIdleGraceTime	Set the maximum number of seconds the web user can remain idle after the warning message is sent. The default is 120

	seconds. See also SMS Configuration. **Note:** If you want to use this parameter, you must also add the **EnableIdleTimeout** parameter and set that parameter to 1.
PartyIdleTime	Set the time (in seconds) the visitor can be idle before the warning is displayed. The default is 300 seconds. See also SMS Configuration. **Note:** If you want to use this parameter, you must also add the **EnableIdleTimeout** parameter and set that parameter to 1.
QueryQueueAccessControl	Controls whether the radio buttons for both anonymous and authenticated access to the Chat and Callback links appear to website visitors when the appropriate queue is not busy. • 0=block all • 1=allow all • 2=authenticated only • 3=anonymous only The query queue tool enables you to find out programmatically how many agents are available and what the wait time is. You can write your own code to do something with that information. Your code could implement certain rules that control the display of the Chat and Callback links. For example: • Display the Chat link if wait time is less than 3 minutes. • Display the Chat link if agents are free or the wait time is less than 1 minute. Otherwise, show the • Callback link. • Display the link to everyone if agents are free. If not, and the wait time is less than 8 minutes, display the link to every third visitor. Otherwise don't display the link.
VisitorConnectedMsg	Sets the message that appears in the Chat dialog when a visitor joins a chat. Preset to: "<Name> has joined the conversation." A visitor to the Website who has not registered, would appear as WebUser. A visitor who has registered is identified by name. For example, if the agent's ID was TomS, you would see "TomS has joined the conversation." If the visitor was unregistered, you would see "WebUser has joined the conversation." To change the preset value, right-click the parameter name and select Properties. You see the Parameter Configuration dialog

	where you can enter a new parameter value.
VisitorDisconnectedMsg	Sets the message that appears in the Chat dialog when a visitor leaves a chat. Preset to: "<Name> has left the conversation." A visitor to the Website who has not registered, would appear as WebUser. A visitor who has registered is identified by name. For example, if a registered visitor's ID was pattyj@nville.com, you would see pattyj@nville.com has left the conversation. To change the preset value, right-click the parameter name and select Properties. You see the Parameter Configuration dialog where you can enter a new parameter value.

Note: Changes to the parameters will not take effect until you restart web services.

Recognition

Overview of automatic speech recognition

Automatic speech recognition (ASR) in CIC unifies speech and DTMF input and provides the ability to extend handler based IVRs with speaker independent speech recognition in a constrained grammar setting.

To configure automatic speech recognition, you must first complete the tabs in the **Recognition Configuration** dialog box. Then, you must configure the specific ASR engine that you want to use.

For more information, use the links under *Related topics*.

Related topics

- General
- Grammar Cache
- Properties
- Preloaded Grammars
- ASR Engines
- Overview of ASR engine configuration

Recognition Configuration - General

Use this page to configure the general behavior of speech recognition.

Input Modes Mask

These are the input modes that are supported by the system. For example, if this mask is “dtmf”, only DTMF input will be considered.

Default Input Modes

This is the default input mode used for all interactions where the input mode is not explicitly overridden in Reco Initialize tool.

See the Handler help in the PureConnect Documentation Library on the CIC server for more information on this tool.

Default Grammar Base URI

This is the URI (or file path) that is used to resolve relative grammar URIs. It is commonly a file path to the grammars, for example d:/I3/IC/Resources. If this parameter is not specified, the “Resource Path” server parameter is used.

For example, assuming a base URI of “d:/I3/IC/Resources”, specifying a relative grammar URI of “main_menu.gram” will be resolved to “d:/I3/IC/Resources/main_menu.gram” by the RecoSubsystem.

Recognition Configuration - Grammar Cache

Use this page to configure the settings for the grammar cache.

> **Note:** These settings should only be modified under the direction of PureConnect Customer Care. Any modifications to these values can have a significant impact on the behavior of the system.

Grammar Cache Directory

This is the directory where the RecoSubsystem maintains the grammar cache. If no directory is specified, the system uses the “Work Path” server parameter.

Grammar Source Data Size Limit (bytes)

This is the maximum number of bytes the source of a single parsed grammar may be comprise of. This setting is used to prevent denial of service attacks by specifying excessively large grammar source files. This limit does not apply to grammars that are not parsed (to allow large binary, engine specific grammars).

Max Per Grammar Data Memory Size (bytes)

This is the maximum size (in characters) the source of a grammar may have before it is cached in a file. Data of grammars that is smaller than this value are cached in memory.

Max Total Grammar Data Memory Cache (bytes)

This is the maximum number of bytes the in-memory cache of the grammar source may contain. If the size of all grammar data cached in memory exceeds this value, the data of subsequently cached grammars is cached in a file (regardless of size).

> **Note:** This does not include the memory occupied by the parse-trees of parsed grammars.

Grammar Cache Cleanup Interval (sec)

This is the interval between garbage collections in the grammar cache (time in seconds).

Min Grammar Idle Time (sec)

This is the minimum amount of time that has to elapse since the last reference to a grammar before that grammar is eligible for garbage collection (in seconds).

Grammar Cache Idle Baseline

This setting specifies the minimum number of idle grammars always left in the cache. Even after idle grammars are eligible for removal because the amount of time passed since last use, the number of grammars specified by this setting is kept in the cache. If there are more idle grammars, the oldest ones are removed. This setting prevents excessive grammars if a system has very low traffic and uses only a few grammars. Without the baseline idle grammars, the grammars would be unloaded between a call and then re-loaded in the next call (for example if the system is not used for a long time during the night).

> **Note:** Setting this value too high may lead to excessive virtual memory usage.

Parsed Grammar Cache Size (bytes)

This is the maximum combined size of all parsed grammars held in memory. If all the grammars in the parsed grammar cache occupy more than this, the oldest grammars are serialized to disk and then released. The next time the grammar is accessed, it's reloaded from disk. Grammars that have been accessed in the last “Min Parsed Grammar Idle Time” seconds or are smaller than “Parsed Grammar Compact Threshold” are not considered.

> **Note:** The calculation of the size of the parsed grammars is only approximate. Setting this value very low can lead to churn when large grammars are registered frequently. The default of 16MB should be appropriate in most cases.

Parsed Grammar Compact Threshold (bytes)

Parsed grammars of size less than this setting will never be compacted (saved to disk and parsed object released). This reduces the likelihood that DTMF grammars are being compacted, as they tend to be rather small.

Min Parsed Grammar Idle Time (sec)

This is the minimum amount of time that must pass since the last access before a parsed grammar is considered for compacting (serializing to disk and then releasing the parsed grammar object).

Properties

Use this page to Add, Edit or Delete speech recognition properties. These properties constitute name and value pairs that are maintained by the recognition subsystem. They are retrieved and modified through the ‘Reco Get Property’ and ‘Reco Set Property’ tools.

The “namespace prefix” classifies properties. This is important to distinguish between VoiceXML, I3, and engine specific properties. Properties that have no namespace prefix correspond to their VoiceXML counterparts of the same name. See the table below for a list of property names and values.

> **Note:** For more information on the tools, see the Handler help in the PureConnect Documentation Library.

To add a property click **Add** and enter the **Property Name**. Click **Add Value** and enter the property value. Click **Remove Value** to delete a property.

To edit a property select the property and click **Edit.** Make changes then click **OK** to save your changes.

To delete a property select the property and click **Delete**.

Property Name	Description and Value
reco:ASREngine	This is the name of the ASR (Automatic Speech Recognition) engine used by the current session.
reco:ASRServer	Machine name of the ASR server on which the port of the session is located. Empty string if lazy port allocation and port has not yet been allocated.
reco:ASRSupportedFeatures	**This Property is reserved for future release.** Space separated list of features supported by the ASR engine of a session. Handlers can enforce support for features in the 'Reco Initialize' and check for individual support through the 'Reco Has Feature' tool. The following features are currently defined: asr_multiple_grammars - The ASR engine supports multiple simultaneously active grammars (multiple ASR grammars may be referenced by the 'Reco Input' tool at once). asr_grammar_weights - The ASR engine supports weights for individual grammars. If not supported, 1.0 is assumed. asr_grammar_fragments - The ASR engine supports fragments in the grammar URIs. asr_sisr_conditionals - The engine supports conditional expressions in semantic interpretation tags. asr_sisr_func_reject -The engine supports the 'Reject' function in semantic interpretation tags. asr_inline_grammars - The ASR engine supports adding grammars defined as source at runtime, thus the tools 'Reco Register Grammar String' and 'Reco Register Inline Grammar' are supported. asr_agile - Engine does not tie the session.
reco:ASRMinResultConf	Minimum confidence an ASR recognition hypothesis must have in order to be included in the recognition

	result. Default: "0.1"
reco:GrammarBaseURI	Base URI used to resolve relative grammar URIs.
reco:ASRDebugWaveLogging	Boolean property to enable logging of wave data for debugging purposes. The default is "false." **Note:** When the reco:RestrictResultTracing property is set to True, the reco:ASRDebugWaveLogging property will automatically be set to False.
reco:RestrictResultTracing	The purpose of this property is to prevent sensitive data from being logged in the IP logs. Set this property to True for an input operation. This sets a flag in the recognition result that suppresses tracing of the utterance and slot values in the trace logs. **Note:** When this property is set to True, it will also disable the ASR Debug Wav recordings.
reco:ASRBargeinDisabled	Boolean property to disable barge-in. If this property is set to "true", the plays are not cancelled when speech is detected. The plays will be cancelled when the recognition is complete (successful or failed). Default: "false"
reco:ASRANII	Defines the ANII value of the current call. Used for logging.
reco:ASRApplicationName	Defines the Application Name to be logged for the current call.
reco:ASRConfidenceMapping	Defines a list of confidence mapping pairs which are used to map the native engine confidences into the confidence values returned in the recognition result. This property is thus used to normalize differing confidence values returned by the ASR engines. Each mapping pair consists of two floating point values between 0.0 and 1.0, separated by an equal sign. The first value designates the native value (returned by the engine) and the second value the resulting mapped

	confidence for that particular engine value. The property may contain an arbitrary number of mapping points. Linear interpolation is used to map confidence values that lie between two point. When mapping confidence calues, two implicit mapping points "0.0=0.0" and "1.0=1.0" are always assumed. This results in an identity mapping if no propery is defined and to ensure correct handling at the boundaries.
reco:EnableSpeakerVerification	Specifies whether speaker identification/verification features should be enabled for an engine.
reco:GrammarCompileTimeout	Specifies the timeout (in seconds) to use when waiting on grammars to be compiled. Depending on the engine, this may not be able to be set through IA and may only have an affect if set in the server's xml config file. Default: 300.0 (5 minutes)
reco:EndOfSpeechNotifyDelay	Specifies the delay after the end of speech has been detected before the server sends an end-of-speech notification. Default: 0.1 (100 ms)
recocfg:ASRMaxProxySessionCount	Maximum number of sessions a server proxy may host. Creating more sessions than the maximum number will be refused. Sessions will not be killed if the maximum session count is changed to a lower value than the number of currently active sessions.
recocfg:ASRServerProxyEnabled	Configuration property specifying whether a server proxy is enabled. A disabled proxy will not allow new sessions (similar proxies whose recocfg:MaxProxySessionCount property are set to 0.
recocfg:AudioAdvertisedAddress	IP address or DNS name under which the CIC server sees the RTP endpoint of the ASR server. The address specified through this property must refer to the same physical device as recocfg:AudioListenInterfaceAddress. IMPORTANT: This property must be used with care and only if the implications are well understood. Misconfiguration may lead to hard to diagnose problems or failures in the audio delivery to the ASR servers.
recocfg:AudioConnectionProbeInterval	Interval between audio connection probes in seconds. It specifies the minimum interval between successful

	connection probe attempts.
recocfg:AudioConnectionProbeMaxFail	Maximum number of failed audio connection probe attempts before a connection configuration problem is assumed and reported.
recocfg:AudioListenInterfaceAddress	Local IP address of the NIC which the server should use to receive audio. This address must refer to the same physical device as the recocfg:AudioAdvertisedAddress property. The local NIC address must be specified as "dot" address (no DNS name). IMPORTANT: This property must be used with care and only if the implications are well understood. Misconfiguration may lead to hard to diagnose problems or failures in the audio delivery to the ASR servers.
recocfg:EnableAudioConnectionProbe	Enables the audio connection probes to check the connection between the CIC servers and ASR servers at regular intervals.
recocfg:ServerProxyPriority	Priority of a server proxy compared to other server proxies for the same engine. When choosing a server for a session, the proxies with low priorities are picked first until their session limit is reached.
recocfg:SupportedLanguages	List of languages supported by an EIM or ASR server. **Note:** A value of "en" indicates that all versions of English are supported. A value of "en-US" indicates that only the U.S. English version is supported.
sensitivity	VoiceXML related property: Relative sensitivity to speech input. 1.0 means highly sensitive to quiet input and 0.0 very insensitive to noise. Not all engines will support this. Default: 0.5
speedvsaccuracy	VoiceXML related property: Relative tradeoff between recognition accuracy and CPU utilization (faster recognition). 0.0 means fastest recognition, 1.0 means highest recognition accuracy. Not all engines support this. Default: 0.5
bargeintype	Type of barge-in performed by the voice input. This property corresponds to the ‘bargeintype’ VoiceXML

	property. Possible values defined by VoiceXML: speech - The barge-in occurs when speech or DTMF is detected. hotword - The barge-in occurs after a grammar has accepted voice or DTMF input. Input that does not match a grammar is ignored. Thus, the tool will never take the “No Match” exit. The default is “speech”.

Preloaded Grammars

Use this page to configure preloaded grammars.

Name

This is the name of the preloaded grammar. This name is used to identify the preloaded grammar in the “Reco Register Preloaded Grammar” tool.

URI

This is the URI or filename of the grammar to be preloaded.

MIME Type

This is the MIME type of the grammar referenced by the URI.

Mode

This is the mode of the grammar. Currently, only “voice” grammars can be preloaded.

To add a preloaded grammar click **Add** and enter the **Preloaded Grammar Name**, **URI**, **MIME Type**, and the **Mode**, then click **OK**.

To edit a preloaded grammar select the grammar and click **Edit.** Make changes then click **OK** to save your changes.

To delete a preloaded grammar select the grammar and click **Delete**.

Recognition Configuration - ASR Engines

Use this page to arrange in order the list of available ASR engines. Select the engine then use the **Move Up** or **Move Down** buttons to change the order.

Engines appear in this list when they’re enabled (which is done by the install based on the manifest). The order of engines determines in which order the RecoSubsystem picks engines when multiple engines match the parameters (such as the language of the call).

ASR server configuration

Location

Select the location from the list where this ASR server resides. By default, when an ASR server logs in to the CIC server, it is automatically assigned to the default location. You must reassign it if it belongs in a different location. You can also set the location in the **Regionalization Locations** container.

Launch Web Configuration...

Click this button to update the configuration of the ASR server. For more information on configuring ASR servers, see the *ASR Technical Reference* in the PureConnect Documentation Library on the CIC server.

Related topics

Selection Rules

Regionalization Location

ASR engine configuration

Overview of ASR engine configuration

To configure any of the supported ASR engines, open the ASR engine-specific subcontainer in the **Recognition** container. Then complete the tabs. See the links under *Related topics* for more information.

For more information on configuring ASR servers, see the *ASR Technical Reference* in the PureConnect Documentation Library.

Related topics

General

Properties

Preloaded Grammars

General

Use this page to set general configuration options.

Enabled

This check box enables the use of this ASR engine. For performance reasons, only ASR engines for which there are ASR servers available should be enabled.

EIM Module DLL

This is the DLL that implements the engine integration component for this ASR engine. This field is populated by the install and should not be modified unless directed by support services.

Properties

Use this page to Add, Edit or Delete speech recognition properties. These properties constitute name and value pairs that are maintained by the recognition subsystem. They are retrieved and modified through the ‘Reco Get Property’ and ‘Reco Set Property’ tools.

The “namespace prefix” classifies properties. This is important to distinguish between VoiceXML, I3, and engine specific properties. Properties that have no namespace prefix correspond to their VoiceXML counterparts of the same name. See the table below for a list of property names and values.

> **Note:** For more information on the tools, see the Handler help in the PureConnect Documentation Library.

To add a property click **Add** and enter the **Property Name**. Click **Add Value** and enter the property value. Click **Remove Value** to delete a property.

To edit a property select the property and click **Edit.** Make changes then click **OK** to save your changes.

To delete a property select the property and click **Delete**.

Property Name	Description and Value
reco:ASREngine	This is the name of the ASR (Automatic Speech Recognition) engine used by the current session.
reco:ASRServer	Machine name of the ASR server on which the port of the session is located. Empty string if lazy port allocation and port has not yet been allocated.
reco:ASRSupportedFeatures	**This Property is reserved for future release.** Space separated list of features supported by the ASR engine of a session. Handlers can enforce support for features in the ‘Reco Initialize’ and check for individual support through the ‘Reco Has Feature’ tool. The following features are currently defined: asr_multiple_grammars - The ASR engine supports multiple simultaneously active grammars (multiple ASR grammars may be referenced by the ‘Reco Input’ tool at once). asr_grammar_weights - The ASR engine supports weights for individual grammars. If not supported, 1.0 is assumed. asr_grammar_fragments - The ASR engine supports fragments in the grammar URIs. asr_sisr_conditionals - The engine supports conditional expressions in semantic interpretation tags. asr_sisr_func_reject -The engine supports the ‘Reject’

	function in semantic interpretation tags. asr_inline_grammars - The ASR engine supports adding grammars defined as source at runtime, thus the tools ‘Reco Register Grammar String’ and ‘Reco Register Inline Grammar’ are supported. asr_agile - Engine does not tie the session.
reco:ASRMinResultConf	Minimum confidence an ASR recognition hypothesis must have in order to be included in the recognition result. Default: "0.1"
reco:GrammarBaseURI	Base URI used to resolve relative grammar URIs.
reco:ASRDebugWaveLogging	Boolean property to enable logging of wave data for debugging purposes. The default is "false." **Note:** When the reco:RestrictResultTracing property is set to True, the reco:ASRDebugWaveLogging property will automatically be set to False.
reco:RestrictResultTracing	The purpose of this property is to prevent sensitive data from being logged in the IP logs. Set this property to True for an input operation. This sets a flag in the recognition result that suppresses tracing of the utterance and slot values in the trace logs. **Note:** When this property is set to True, it will also disable the ASR Debug Wav recordings.
reco:ASRBargeinDisabled	Boolean property to disable barge-in. If this property is set to "true", the plays are not cancelled when speech is detected. The plays will be cancelled when the recognition is complete (successful or failed). Default: "false"
reco:ASRANII	Defines the ANII value of the current call. Used for logging.
reco:ASRApplicationName	Defines the Application Name to be logged for the

	current call.
reco:ASRConfidenceMapping	Defines a list of confidence mapping pairs which are used to map the native engine confidences into the confidence values returned in the recognition result. This property is thus used to normalize differing confidence values returned by the ASR engines. Each mapping pair consists of two floating point values between 0.0 and 1.0, separated by an equal sign. The first value designates the native value (returned by the engine) and the second value the resulting mapped confidence for that particular engine value. The property may contain an arbitrary number of mapping points. Linear interpolation is used to map confidence values that lie between two point. When mapping confidence calues, two implicit mapping points "0.0=0.0" and "1.0=1.0" are always assumed. This results in an identity mapping if no propery is defined and to ensure correct handling at the boundaries.
reco:EnableSpeakerVerification	Specifies whether speaker identification/verification features should be enabled for an engine.
reco:GrammarCompileTimeout	Specifies the timeout (in seconds) to use when waiting on grammars to be compiled. Depending on the engine, this may not be able to be set through IA and may only have an affect if set in the server's xml config file. Default: 300.0 (5 minutes)
reco:EndOfSpeechNotifyDelay	Specifies the delay after the end of speech has been detected before the server sends an end-of-speech notification. Default: 0.1 (100 ms)
recocfg:ASRMaxProxySessionCount	Maximum number of sessions a server proxy may host. Creating more sessions than the maximum number will be refused. Sessions will not be killed if the maximum session count is changed to a lower value than the number of currently active sessions.
recocfg:ASRServerProxyEnabled	Configuration property specifying whether a server proxy is enabled. A disabled proxy will not allow new sessions (similar proxies whose recocfg:MaxProxySessionCount property are set to 0.
recocfg:AudioAdvertisedAddress	IP address or DNS name under which the CIC server sees the RTP endpoint of the ASR server. The address

	specified through this property must refer to the same physical device as recocfg:AudioListenInterfaceAddress. IMPORTANT: This property must be used with care and only if the implications are well understood. Misconfiguration may lead to hard to diagnose problems or failures in the audio delivery to the ASR servers.
recocfg:AudioConnectionProbeInterval	Interval between audio connection probes in seconds. It specifies the minimum interval between successful connection probe attempts.
recocfg:AudioConnectionProbeMaxFail	Maximum number of failed audio connection probe attempts before a connection configuration problem is assumed and reported.
recocfg:AudioListenInterfaceAddress	Local IP address of the NIC which the server should use to receive audio. This address must refer to the same physical device as the recocfg:AudioAdvertisedAddress property. The local NIC address must be specified as "dot" address (no DNS name). IMPORTANT: This property must be used with care and only if the implications are well understood. Misconfiguration may lead to hard to diagnose problems or failures in the audio delivery to the ASR servers.
recocfg:EnableAudioConnectionProbe	Enables the audio connection probes to check the connection between the CIC servers and ASR servers at regular intervals.
recocfg:ServerProxyPriority	Priority of a server proxy compared to other server proxies for the same engine. When choosing a server for a session, the proxies with low priorities are picked first until their session limit is reached.
recocfg:SupportedLanguages	List of languages supported by an EIM or ASR server. **Note:** A value of "en" indicates that all versions of English are supported. A value of "en-US" indicates that only the U.S. English version is supported.
sensitivity	VoiceXML related property: Relative sensitivity to speech input. 1.0 means highly sensitive to quiet input

	and 0.0 very insensitive to noise. Not all engines will support this. Default: 0.5
speedvsaccuracy	VoiceXML related property: Relative tradeoff between recognition accuracy and CPU utilization (faster recognition). 0.0 means fastest recognition, 1.0 means highest recognition accuracy. Not all engines support this. Default: 0.5
bargeintype	Type of barge-in performed by the voice input. This property corresponds to the ‘bargeintype’ VoiceXML property. Possible values defined by VoiceXML: speech - The barge-in occurs when speech or DTMF is detected. hotword - The barge-in occurs after a grammar has accepted voice or DTMF input. Input that does not match a grammar is ignored. Thus, the tool will never take the “No Match” exit. The default is “speech”.

Preloaded Grammars

Use this page to configure preloaded grammars.

Name

This is the name of the preloaded grammar. This name is used to identify the preloaded grammar in the “Reco Register Preloaded Grammar” tool.

URI

This is the URI or filename of the grammar to be preloaded.

MIME Type

This is the MIME type of the grammar referenced by the URI.

Mode

This is the mode of the grammar. Currently, only “voice” grammars can be preloaded.

To add a preloaded grammar click **Add** and enter the **Preloaded Grammar Name**, **URI**, **MIME Type**, and the **Mode**, then click **OK**.

To edit a preloaded grammar select the grammar and click **Edit.** Make changes then click **OK** to save your changes.

To delete a preloaded grammar select the grammar and click **Delete**.

Media Servers

Media Servers

The primary purpose of the Interaction Media Server is to handle the RTP/SRTP audio streams for one or more CIC servers.   Interaction Media Server supports supervisory monitoring of calls, and it handles recording (and optionally encrypting) calls that CIC users choose to record,or that the Interaction Recorder system flags for recording. Interaction Media Server enables multiple devices using different coders/decoders (codecs) to communicate by transcoding between RTP streams (e.g., G.711,G.729, etc.) that come into an Interaction Media Server.   It also handles Secure RTP (SRTP) audio,when properly configured, and the Interaction Media Server can pass through SRTP or transcrypt between SRTP and RTP audio streams,if one device sends SRTP and another receiving device can handle only RTP audio. Interaction Media Server plays all IVR prompts and on-hold music hosted on the CIC server. It can also perform call analysis on outbound calls. Interaction Media Server is also the engine for Interaction Speech Recognition and does keyword spotting in conversations for Interaction Analyzer.

> **Notes**: You do not define Interaction Media Servers through Interaction Administrator. Once an Interaction Media Server is licensed, you use the Interaction Media Server web interface to connect to a specific CIC server. Interaction Administrator shows all active, licensed, and connected Interaction Media Servers within the Media Servers object in the left pane of the Interaction Administrator window.

Related topics

Media Server Configuration

Media Server General Configuration

Media Server Properties

Media Server Web Configuration

Regionalization

Location Assistant

Select Media Server

Call Analysis Language

Media Server Configuration Properties

Use this page to set global properties for all Interaction Media Servers, or properties for a specific Interaction Media Server. The list displays the **Name** and **Value** of the properties. Click **Add** to add a new property, click **Edit** to edit a property, or click **Delete** to remove a property.

For a list of valid properties see the **Properties Configuration Page** section of the *Interaction Media Server Technical Reference* document in the **Technical Reference Documents** section in the PureConnect Documentation Library.

> **Notes**: For more information on properties, see *the Interaction Media Server* document available on the Product Information site.

> Setting global properties in IA overrides the properties set in the Interaction Media Server web interface and applies to all connected Interaction Media Servers.

Related topics

Media Server Introduction

Media Server General Configuration

Media Server Properties

Media Server Web Configuration

Regionalization

Location Assistant

Select Media Server

Packaged Server Parameters

Telephony Parameters - General

Optional Server Parameters

Media Server General Configuration

Use this page to set a specific location of an Interaction Media Server.

Select the **Location** from the list where this Interaction Media Server resides. By default, when a media server logs in to the CIC server, it is automatically assigned to the **<Default Location>**. To change the virtual location of an Interaction Media Server, use the Regionalization Locations container.

Related topics

Media Server Configuration Properties

Servers

Servers

Use this section to change the configuration of any Interaction Media Server that is connected to the CIC server.

Servers Configuration Properties

Servers Configuration Web Configuration

Media Server Properties

Interaction Media Server properties are name-value pairs that control the operations of the media server.

These properties can be set in four different places – two in the Media Server configuration pages and two in Interaction Administrator. The properties are used in a hierarchical relationship order, which enables an administrator to have specific control over the scope of these properties, as needed. The default properties are established on each media server, but each property can be overridden by defining it and assigning a different value in Interaction Administrator. Any property can be set from any location, depending on the scope of the property (i.e., which media servers and CIC servers it applies to). If you don't set any media server properties in Interaction Administrator, the default properties apply, or whatever you set locally on each media server.

> Note: When you define media server properties with a different value in Interaction Administrator, those properties are not visibly displayed in the Interaction Media Server's interface, as they are when you define them locally on the media server. To see the complete set of all properties in effect on a media server, look in Interaction Administrator and the Interaction Media Server interface.

The four property configuration locations and the scope and purpose of each are summarized in the following table:

Evaluation Order	Property Configuration	Purpose and Scope
1	**Global** media server properties – defined on the media server from the **Config -> Properties** configuration page	These properties apply to all CIC servers connected to this media server. This is the lowest level of priority in the hierarchy as all other property settings can override these. Even properties that are not displayed here have a default value and they may be overridden if set elsewhere. Click here for a location example.
2	**Server properties** – defined on the media server from the Properties page linked from the **Config** -> **Servers** configuration page	These properties apply only to the connection between the selected CIC server and that media server. If there is overlap, properties defined here override the same property defined in the Global **Properties** page. Click here for a location example.
3	**IC server Global Properties** – defined in Interaction Administrator Media Servers/ Configuration on the Properties tab	These properties apply to all media servers logged in to this CIC server. If there is overlap, these properties override all of the properties set on the web configuration pages of all connected media servers. Click here for a location example.
4	**IC server properties** – defined in Interaction Administrator, in Media Servers/Server/ <*servername*> Properties tab	These properties apply only to the selected media server logged in to this CIC server. If there is overlap, these properties override the CIC server Global Properties, as well as all

		properties defined on the web configuration pages of the specified media server.. Click here for a location example.

When the CIC server performs a media server operation (e.g., start a recording), the Interaction Media Server uses the aggregate set of properties to determine the current configuration. It evaluates the properties in this order:

1. Start with all of the properties defined in its global **Properties** page (1st in the table)
2. Add all of the properties defined in the Server **Properties** page (2nd in the table). If any of the server properties are also set in the global properties, use the server properties.
3. Add all of the properties defined in the global Media Server Properties in Interaction Administrator (3rd in the table). If any of these properties are also defined on the media server, use the global properties from Interaction Administrator.
4. Add all of the properties defined in the specific Media Server <*servername*> **Properties** page in Interaction Administrator (4th in the table). Use these properties to override any other property defined with the same name.
5. Add all of the properties together for a specific operation.

Using this hierarchy, you can have a default configuration but choose to override any part of it for a specific operation or server combination. If the properties you need to set are identical on all media servers, you can set them all once in Interaction Administrator and you won't have to set them at all in the Interaction Media Server interface.

Property Configuration Example:

Consider the RecordingMimeTypeDefault property, which controls the audio recording format when Interaction Recorder is configured to use “µ-Law (Mono)” as its compression format, or when a custom handler initiates a recording and does not specify a “Mime Type” parameter.

Suppose you specified audio/PCMA as the recording format in the **Config --> Properties** page of the Media server. That means when a recording is created, it is in that format unless specifically overridden. If you later realize the need to record all calls on a particular CIC server in the audio/GSM format, you can add the RecordingMimeTypeDefault property with the audio/GSM value to the **Config --> Server --> Properties** page. However, if a CIC server uses several media servers, you would have to go to each media server and add that property to the **Properties** page of that CIC server’s configuration on the media server. Instead, you can use Interaction Administrator and add that property/value to the **Properties** tab on the **Media Servers --> Configuration --> Properties** dialog. Now all recordings created by that CIC server will be recorded in audio/GSM. If you discover that you really need all but one of the media servers to use audio\GSM, you can open the configuration container for that particular media server in Interaction Administrator and specify a different format for that server on the **Properties** tab.

Related topics

Media Server Introduction

Media Server Configuration

Media Server General Configuration

Media Server Web Configuration

Regionalization

Location Assistant

Select Media Server

SIP Line Configuration - Session

SIP Station Configuration - Session

Media Server Web Configuration

Use this page to launch the web configuration interface for the currently selected Interaction Media Server.

When you click the **Launch Web Interface** button, your default browser will attempt to open the configuration interface on the selected media server. However, if this is the first time that this browser has connected to the media server, you will likely see a certificate warning message because the media server's certificates are self-signed, and it is not yet a trusted site.

Select the **Accept this certificate permanently** radio button to accept the media server's certificate

If you have multiple media servers connected to a CIC server and you want to deactivate an individual media server but keep other media servers active, you can deactivate it in the web interface for that specific media server.

1. Click the **Launch Web Interface** button to open the media server's interface, and log on to the media server.
2. Click the **Config** button in the top right corner of the media server's web interface.
3. On the **Servers** page, click the **Server** button for the media server you want to deactivate.
4. In the **Accept sessions** drop down list, select **No** and click **Apply Changes**. This prevents the media server from accepting any more requests from the CIC server.

Related topics

Media Server Introduction

Media Server Configuration

Media Server General Configuration

Media Server Properties

Regionalization

Location Assistant

Select Media Server

SIP Line Configuration - Session

SIP Station Configuration - Session

SIP Proxies

SIP Proxies

The Interaction SIP Proxy Server must be configured to log on to the CIC server using valid CIC account credentials. Once the SIP Proxy is logged on to CIC, Interaction Administrator detects the connection and the Interaction SIP Proxy server name appears in the SIP Proxies container. You can not add a SIP Proxy server from Interaction Administrator – the connection must be initiated from the SIP Proxy server side

Once the Interaction SIP Proxy server appears, open it and click on the General tab.

> **Note**: A SIP proxy server can be added by configuring the proxy server to point to the CIC server, and initiating the connection. You can not add a SIP Proxy server from Interaction Administrator.

Related topics

SIP Proxy Configuration - General

SIP Proxy Configuration - Web Configuration

Add SIP Proxy

Endpoints

Add Registration

SIP Proxy Configuration - General

Use this page to configure general settings for the SIP Proxy server.

If you want SIP devices to register to both CIC and Interaction SIP Proxy, you must define a SIP proxy in Interaction Administrator and set a registration group to use both a SIP line and the SIP proxy.

Trust this Proxy

Select this button to enable the CIC server to communicate with the Interaction SIP Proxy server. This button is not displayed if the Interaction SIP Proxy server is currently trusted. If you want to reset or stop using a proxy, you must delete it.

Location

Select the location associated with the SIP Proxy server. Each SIP Proxy server can include device configuration data from only one location at a time. Location(s) are available in the list assuming one or more locations are defined in the Regionalization Locations container.

Once you select the location, click **OK** and the CIC server will exchange certificates and share its Location configuration data with the SIP Proxy server. The Version, Registration Address and Ports are displayed below the location.

CIC sends updates in the location configuration data to the Interaction SIP Proxy server as needed.

Related Topics:

SIP Proxy Configuration - Web Configuration

Add SIP Proxy

Endpoints

Add Registration

SIP Proxy Configuration - Web Configuration

If you know the user name and password (see the CIC Administrator) to the Interaction SIP Proxy server, you can access the web configuration interface. Click on the **Launch Web Configuration...** button to open the web configuration interface for the Interaction SIP Proxy server. You must have a valid user name and password to log in to the SIP Proxy server.

Related Topics:

SIP Proxy Configuration - General

Add SIP Proxy

Endpoints

Add Registration

MRCP Servers

MRCP Servers Configuration

The Media Resource Control Protocol (MRCP) allows a client device to control media processing resources on the network. Some media processing resources include speech recognition engines, speech synthesis engines, speaker verification engines, and speaker identification engines. MRCP relies on a session management protocol, such as the Session Initiation Protocol (SIP), to establish the session between the client and the server, and then the media processing control is passed to the client.

Use this page to set the global MRCP server options.

> **Note:** To set MRCP as the default TTS provider, use the **Text to Speech** tab of the **System Configuration** dialog box. For more information, see *Text to Speech*.

Protocol

Select TCP or UDP, depending on protocols supported by your IP-enabled devices (e.g., gateway, phones, etc.) The default protocol is TCP to initiate the session. After the session is established, MRCP uses TCP and cannot be changed. *If you make changes to the protocol setting or to the network interface* *card, you must restart the MRCP server.* If you change the protocol, you must restart the MRCP subsystem in order for the change to take effect.

Address to Use

Select the network interface for the MRCP server to use. Local Area Connection is the default setting. If you change the address, you must restart the MRCP subsystem in order for the change to take effect.

Connection Timeout

Enter the value in seconds to disconnect the connection if it does not enter a connected state before the expiration of the timeout. The default value is 5 seconds. The acceptable values are 1 through 60.

Use Media Streaming Server to Play Voicemails

Select this check box to enable any Interaction Media Streaming Server to play voice mail messages that are stored as attachments in e-mail messages. You must use the Interaction Media Streaming Server web interface to configure the settings for the e-mail server. If this check box is not enabled, voice mail messages are inserted into the call by Interaction Media Server.

Related Topics

Configuration

Supported Resources

Server Properties

Text to Speech

MRCP Servers Configuration

Use this page to set the MRCP server configuration options.

> **Notes:** In order to configure an MRCP server, you must have either the Master Administrator right or the admin access right to edit the MRCP server. For more information, see Assign the master administrator right, Assign administrator access rights, and Administrator access control groups:System category.
>
> If you make changes to the protocol setting, or to the network interface card, you must restart the MRCP server.

Active

This check box indicates if this MRCP server is active. By default, this check box is selected (enabled).

SIP Address

Enter the SIP address of this MRCP server. The address is in the SIP URI format, i.e., sip:x@y:port, where x=username and y=host (domain or IP). Some examples include:

- sip:buzz.mullins@123.123.1.123
- sip:customercare@inin.com

- sip:12345@inin.com

Port 6060 is recommended for MRCP servers with CIC installations to avoid potential conflicts with default ports for SIP endpoints.

Location

Select the region to associate this MRCP Server with.

> **Notes**: When creating an MRCP session, the Location setting of the MRCP Server is taken into consideration. The MRCP Server selection process based on region, where MRCP Servers in a preferred region are considered before MRCP Servers in other regions, is performed before load balancing, where the MRCP Server is selected with the least amount of sessions.
>
> When a new MRCP resource is required, Telephony Services selects the Media Server to use for the audio resource. Telephony Services passes the region/location of the Media Server to the MRCP subsystem. The MRCP subsystem evaluates all the MRCP Servers in the region, and then selects the MRCP Server with the least amount of sessions to create the resource on. If no MRCP Servers are available in the selected Location for the region, the MRCP subsystem defaults to other available MRCP Servers. The MRCP Server with the least amount of sessions is selected to create the resource on.

Priority

Select the priority level for this MRCP server. The MRCP subsystem uses this setting in the load balancing algorithm. When multiple servers can satisfy a request, sessions are created on servers with a lower priority number. By default, the priority is 1.

Vendor

Use this field to optionally describe the MRCP server’s vendor.

Capabilities

This section differs depending on the server's vendor; the **Retrieve from server** option is not available in a third party server configuration.

Retrieve from server: Select this option to have the MRCP server provide its available capabilities to the Interaction Center server. Select the associated button to immediately request the capabilities of the MRCP specified in the **SIP Address** box.

- **Use refresh interval (sec)** – Enable this check box if you want the Interaction Center server to continuously request the capabilities of the MRCP server. Use the associated spin box to set the number of seconds that should elapse between requests.

Use custom: Select this option if you want to manually specify the capabilities of the MRCP server, even if those features are not yet enabled or configured on the MRCP server.

- **Text to speech** – Enable this check box to allow the MRCP server to convert text to synthesized speech in calls.
- **External audio sources** – Enable this check box to allow the MRCP server to provide streaming audio that is injected into calls, such as Music on Hold.

- **Voicemail** – Enable this check box to allow the MRCP server to insert voice mail messages into calls.

SIP Create Session Supported

Select this check box to indicate that the TTS server supports INVITES to create an empty session with no specific resources defined. By default, this check box is not selected (enabled).

Enable Session TTL

This setting enables TTL sessions, when selected. When enabled, either the **Indefinite - Session Stays Live until BYE** option or the **Defined TTL Session Time** option is selected. These options are the time in seconds that an MRCP session is kept alive by the server after the last request. This is used to allow the client to cache the session if needed. If **Defined TTL Session Time** is selected, the default time is 15 seconds. Possible values are from 1 to 3600.

If this check box is not selected, TTL sessions are not enabled, and the options below are grayed-out or unavailable.

MRCP Version

This field displays the version of the MRCP server.

External Audio Sources

This tab displays the external audio sources that you have defined in the Interaction Media Streaming Server web interface.

> **Note:** Interaction Center can use only those external audio sources for which you have provided a name in the Interaction Media Streaming Server web interface.

Supported Resources

Use this page to select the resources that are supported for this MRCP server. The options are:

- **Speech Recognition**: This is a full speech recognition resource that is capable of receiving a media stream containing audio, and interpreting it to recognition results. It also has a natural language semantic interpreter to post-process the recognized data according to the semantic data in the grammar, and to provide semantic results along with the recognized input. The recognition resource may also support enrolled grammars, where the client can enroll and create new personal grammars for use in future recognition operations.
- **DTMF Recognition**: This is a recognition resource capable of extracting and interpreting DTMF digits in a media stream, and matching them against a supplied digit grammar. It could also do a semantic interpretation based on semantic tags in the grammar.
- **Speech Synthesizer**: This is a full-capability speech synthesis resource capable of rendering speech from text. Such a synthesizer *should* have full SSML [25] support.

- **Basic Synthesizer**: This is a speech synthesizer resource with very limited capabilities that can generate its media stream exclusively from concatenated audio clips. The speech data is described using a limited subset of SSML [25] elements. A basic synthesizer *must* support the SSML tags <speak>, <audio>, <say-as> and <mark>.
- **Speak Verify**: This is a resource capable of verifying the authenticity of a claimed identity by matching a media stream containing spoken input to a pre-existing voice-print. This may also involve matching the caller's voice against more than one voice-print, also called multi-verification or speaker identification.
- **Recorder**: This is a resource capable of recording audio and saving it to a URI. A recorder *should* provide some end-pointing capabilities for suppressing silence at the beginning and end of a recording, and *may* also suppress silence in the middle of a recording. If such suppression is done, the recorder *must* maintain timing metadata to indicate the actual time stamps of the recorded media.

By default, **Speech Synthesizer** is selected as a supported resource.

Server Properties

Use this page to Add, Edit, or **Remove** custom server properties for this MRCP server.

Voices

Use this page to configure the voices (or audio) for the MRCP server. The voices specified on this page are the MRCP voices used to synthesize the text to speech.

Select a voice from the pull-down menu. Click **Add** to enter a synthesizer voice name, or click **Remove** to disable a selected voice.

Gender

Select the gender of the voice. The default value is **Neutral**. The other possible values are **Female** and **Male**.

Supported Languages

A voice can support specific languages. By default, the selected voice supports all languages, and the languages are displayed in the **Currently Selected** list. **Add** moves selected languages from the **Available** list to the **Selected** list. **Remove** moves selected languages from the **Selected** list to the **Available** list. **Add All** moves all languages to the **Selected** list, and **Remove All** removes them all from the **Selected** list.

Custom attributes

The Custom Attributes page allows you to add customized attributes so that you can reference your own variables and settings through the IceLib interface.

> **Note:** If you enabled the Enhanced Interaction Administrator Change log, then all of your changes to the Custom attributes page in the User Configuration dialog box and the Workgroup Configuration dialog box dialog box are tracked in that log. For more information, see *About the Enhanced Interaction Administrator Change Log*.

The page contains a list for the attributes and displays a **Name** and a **Value** column, and has the following buttons:

Add

Click **Add** and select an existing custom attribute from the pull-down list, enter a new custom attribute. If creating a new attribute, use a unique name, otherwise the existing attribute will be overwritten.

Edit

Click **Edit** to change the value of an existing custom attribute.

Delete

Click **Delete** to delete an existing custom attribute.

Manage Attributes

Click **Manage Attributes** to open a dialog box that displays a list of custom attributes. Click **Add** or **Delete** to manage the appearance of the custom attributes in the pull-down list.

The custom attributes are saved in the path of the root container. This **Path** is displayed at the bottom of the dialog box.

> **Note**: For more information on the Interaction Center Extension Library (IceLib), see The **System APIs section** in the PureConnect Documentation Library on the CIC server.

History

This page provides a way to manually document configuration changes and when they occurred. Changes made in Interaction Administrator are also automatically logged in the Interaction Administrator Change Notification Log (Log ID 7). Later, authorized users can run reports against this log to summarize all configuration changes.

> **Note:** If you enabled the Enhanced Interaction Administrator Change log, then all of your changes to the History page in the User Configuration dialog box and the Workgroup Configuration dialog box dialog box are tracked in that log. For more information, see *About the Enhanced Interaction Administrator Change Log*.

Last Modified

This date is automatically updated each time you click the **OK** button, presumably after you make changes to the configuration. To avoid updating this date, exit the page by clicking the **Cancel** button.

> **Note:** If you click **Cancel**, none of the changes made to this page will be preserved.

In addition, the history is updated when changes are made to the record elsewhere in Interaction Administrator. For example, when a user change his or her password, the **Last Modified** date is updated.

> **Note:** Changes to the licenses for a user or a station do not update the Last Modified date.

Date Created

This date is automatically set when the user creates the initial configuration for this page. If the page was initially created during setup, the date could be blank.

Notes

Type notes about configuration settings and changes. If you change the configuration page and click **OK**, the **Last Modified** date is updated.

You must manually enter the date beside each entry in the **Notes** field to identify the date of each note.

To create a new line in the **Notes** field, press Enter.

Session Manager Configuration

CIC can use an off-server session manager to handle some of the CPU and memory demands on the CIC server, thereby improving performance. Use this page to view or manage the off-server domain names and locations of session manager servers.

Session manager servers provide this information to IceLib (Interaction Center Extension Library). Regionalization can use a session manager server as an endpoint to define a location where users and stations are located.

> **Note**: See the *Session Manager Development Application Note* for information on the Off-server Session Manager Install. For session manager server hardware requirements, see **Interaction Application Servers** on testlab.genesys.com.

Fully Qualified Domain Name:

This is the FQDN of this session manager server. This field is read-only.

Override

Select this check box and enter a different FQDN in the text box to let a connecting client know that the FQDN of the this session manager server is not the FQDN stored in Interaction Administrator.

Location:

By default, the off-server session manager server uses the location of the CIC server as indicated in **Use the location of:**. If the client should connect to another location, select **Use this location** and choose the location (as defined in Location configuration) from the drop-down menu.

The full name of the location displayed here is the same name as it appears in the location's endpoint container.

> **Note:** If you set the location of the session manager to the location of a CIC server, then the session manager cannot be removed from that location in the location's endpoint container.

Switchover Behavior:

In a switchover environment, off-server session manager servers can connect to the primary CIC server, or to the particular CIC server they were installed against. It is recommended to use the **Always reconnect to the primary IC server on switchover** option or 'no switch' mode. The other option, **Always connect to: [IC server]**, is not common and intended mainly for backwards compatibility for WAN switchover sites.

Related Topics

Regionalization

Regionalization Location

Endpoints

Subsystem Certificates

Certificate Management

CPU Load Detection

Interaction Client

Optional General Server Parameters

SMS

SMS

CIC provides an integrated SMS (Short Message Service) server subsystem that connects with external SMS brokers to exchange messages. The SMS server arbitrates between external SMS brokers and internal CIC subsystems, such as the ACD server, reporting, and Interaction Recorder.

CIC can send outbound SMS messages using handlers by connecting to the SMS gateway or an HTTP broker. CIC can also route inbound SMS messages to users or workgroups by putting the original text into an email message.

> **Note**: For more information on SMS see *Short Message Service Technical Reference* in the Technical Reference Documents section of the PureConnect Documentation Library on the CIC server.

The topics included in this section are:

- SMS Inbound Routing

- SMS Inbound Route Configuration
- SMS Outbound Routing
- SMS Outbound Route Configuration
- SMS Broker: Configuration
- SMS Broker: Accounts
- SMS Broker: Proxy
- SMS Broker: Message Originated
- SMS Broker: Message Terminated

SMS Inbound Routing

Use this page to configure an ordered set of rules for routing SMS messages through CIC. Based on regular expression matching of the ANI, DNIS, or body, a message can be routed to either a user or workgroup queue, chat or a handler.

The routes are defined by type, regular expression, and destination.

Click **Add** to add a new inbound route.

Related Topics:

SMS Inbound Route Configuration

SMS Outbound Routing

SMS Outbound Route Configuration

SMS Inbound Route Configuration

Use this page to configure inbound SMS routes. Use the **Move Up** and **Move Down** buttons to order the routes in priority. If no inbound routes are configured, messages travel through the email message routing system. If one or more inbound routes are configured, a default inbound route must also be configured.

> **Note**: Only one default inbound route can exist, and it must always be the last route in order.

Type

Select the type of route from the drop-down menu. the options are ANI, Body (body of the message), and DNIS.

Expression

Enter the expression associated with the type of route. The expressions available are:

Expression	Meaning
*	Zero or more

+	One or more
\d	Any digit (0-9)
.	Any character
[]	Character in set
[^]	Character not in set
?	Preceding group is optional
|	Or
^	Beginning of line
$	End of line

Destination

Select from the drop-down list where to route the message. Setting his option indicates to CIC the type of routing this is required when an inbound SMS matches the expression. The options are Chat (default), Handler and Queue. If a handler is the destination, the handler name must be specified in the **Name** field. If a queue is the destination, select a workgroup or user from the list that appears.

Name

Enter the name of the handler if the **Destination** is "Handler", otherwise the user or workgroup is displayed here that is associated with the queue. Name doesn't apply to a Chat type destination.

Related topics

SMS Inbound Routing

SMS Outbound Routing

SMS Outbound Route Configuration

SMS Outbound Routing

Use this page to configure an ordered set of rules for routing outbound SMS messages through CIC. Based on regular expression matching of DNIS, CIC sends outbound directed SMS messages to a broker using the proper destination number formatting.

The routes are defined by type, regular expression, formatted number, broker and account ID.

To configure outbound routes

1. To add a new outbound route, click Add.
2. To change the configuration of an existing outbound route, select it in the list and then click Edit.
3. To delete an outbound route, select it and then click Delete.
4. To change the sequence of the outbound routes, click a route in the list and then use the Move Up and Move Down buttons.
5. To consolidate outbound messages, select the Consolidate Messages check box.
   CIC maintains a queue of outbound messages for an interaction. If an outbound message is added to a queue while another outbound message is waiting to be sent, the second outbound message can be added to the first outbound message provided that this check box is selected and the combined length of the messages is less than the SMS maximum length (160 characters).
6. Click OK.

Related Topics:

SMS Inbound Routing

SMS Inbound Route Configuration

SMS Outbound Route Configuration

SMS Outbound Route Configuration

Use this page to configure outbound SMS routes. Use the **Move Up** and **Move Down** buttons to order the routes in priority. If no routes are configured, messages travel through the email message routing system. If one or more outbound routes are configured, a default outbound route must also be configured.

Note: Only one default outbound route can exist, and it must always be the last route in order.

Type

Select the type of route from the drop-down menu. Currently, DNIS is the supported type.

Regular Expression

Enter the expression that CIC uses match the route against the associated type, This also provides the pattern matches that are used for the formatted number The expressions available are:

Expression	Meaning
*	Zero or more
+	One or more
\d	Any digit (0-9)

.	Any character
[]	Character in set
[^]	Character not in set
?	Preceding group is optional
|	Or
^	Beginning of line
$	End of line

Formatted Number

Type the formatted number that CIC should use as the outbound dial number for the SMS message. All characters are valid and regular expression pattern replacements are denoted using the $ symbol. $0 represents the input expression as a whole; $1 is the first grouped match, and so on.

Broker

Select from the pull-down list the value of the available brokers that CIC should use to deliver this SMS message. By default, CIC uses the default broker (indicated with <Default>). We recommend using the default broker if no other brokers are configured in CIC. Other options are Gateway and HTTP.

Account ID

Select from the drop-down list the value of the available accounts for the selected broker that CIC should use to deliver this SMS message. By default, CIC uses the <Default> account, or no account if one is not configured. The default account appears first in the list even when multiple accounts have been configured.

Access Control

Click the **Access Control** button to select the phone number classifications for the selected outbound SMS route.

> **Notes:**
>
> You must select at least one phone number classification for the outbound SMS route. If you do not select a phone number classification, or do not select a call classification that provides the correct access permissions, then agents and workgroups using this SMS route see an error message when they try to send SMS messages.
>
> You manage the available call classifications as part of your regional dial plans. For more information about call classifications, see Overview of phone number classifications.

Related Topics:

SMS Inbound Routing

SMS Inbound Route Configuration

SMS Outbound Routing

SMS Purge Data

Use this page to configure when old SMS data is purged from the database.

To configure when SMS data is purged

1. In the **Purge data older than box**, type a number greater than 1.
2. Click **OK**.

SMS Broker

SMS Broker

An SMS broker is a company that takes care of routing SMS messages to and from cell phones. To accomplish this, SMS brokers maintain hardware at the premises of cell phone providers, called Short Message Service Centers (SMS-C's).

Use the following pages to configure the SMS gateway broker or HTTP broker behavior:

- SMS Broker: Configuration (Gateway and HTTP)
- SMS Broker: Accounts (HTTP)
- SMS Broker: Message Originated (HTTP)
- SMS Broker: Message Terminated (HTTP)
- SMS Broker: Proxy (HTTP)

SMS Broker: Configuration

CIC also includes a default HTTP broker, however you can configure any number of additional HTTP brokers. This help topic explains the following SMS HTTP broker configuration options

Enable

This check box enables or disables the broker configuration for MO and MT processing.

Broker

Select from the drop-down list the specific broker communication interface that should be used to send and receive SMS messages.

Profile

Select from the drop-down list the configuration profile of the broker that should be used as the communication protocol. Many brokers only have one option. This selection must match the communication protocol that was defined when ordering the broker account from the provider.

Encryption

Choose type of HTTP communication security to use for the HTTP broker. By default, CIC does not use encryption. When you set the encryption as HTTPS (Basic), CIC uses HTTPS with basic encryption.

> **Note**: Select HTTPS (Basic) if you are using SSL. If you select this, you must use HTTPS for both inbound and outbound messages. For more information about using SSL, see the *PureCloud for CIC Administration Guide* in the PureConnect Documentation Library.

Related Topics

SMS Broker: Accounts

SMS Broker: Proxy

SMS Broker: Message Originated

SMS Broker: Message Terminated

SMS Broker: Accounts

This page displays a list of accounts you have configured for this broker. Click Edit... to make changes to existing accounts, or click **Delete** the currently selected account.

Click Add... to configure a new broker account.

Click Associate to associate a broker account with a workgroup or user.

Related Topics

SMS Broker: Configuration

SMS Broker: Serial Ports and Cell Phones

SMS Broker: Proxy

SMS Broker: Message Originated

SMS Broker: Message Terminated

SMS Broker: Message Originated

A Mobile Origination (MO) message is an inbound SMS message that comes from a cellphone. Use this page to configure settings when polling for new messages and receiving new messages.

Enable

Select this check box to enable or disable the MO functionality of this broker configuration. However, the broker configuration Enable setting has precedence over this setting.

Incoming HTTP Port

Type the IP port that should be used to receive inbound HTTP requests (messages) from the broker provider. Do not share this port with any other application on the CIC server, and make sure it is accessible by the public network.

Incoming Path

Type the path that an incoming request’s URL should be validated against which determines that the request should be processed by this broker configuration.

> **Notes:**
>
> If this broker shares an incoming HTTP port with other brokers on this CIC server, make sure that the **Incoming Path** and **Delivery Receipt URL** values are unique among all brokers that share this port.
>
> When ordering a service from an SMS provider, you must provide the information on this page. Typically, the information should be in the form of a URL that the provider can send messages to. This URL is composed of http://<CIC Server IP>:< HTTP Port><Path>, so for example,
> http://172.10.10.10:8080/MyBroker/IncomingSMS.

Delivery Receipt URL

Type the path where the broker pushes incoming delivery receipt notifications for outbound messages.

Most brokers support delivery receipts in one of the following ways:

- The delivery receipt URL is set in the broker account configuration, for example through the broker's web portal.
- The delivery receipt URL is passed by CIC with each outbound message. In this case, you must go to the Message Terminated tab and specify a value for the **ExternalDeliveryStatusURI** option.

> **Note:** If this broker shares an incoming HTTP port with other brokers on this CIC server, make sure that the **Incoming Path** and **Delivery Receipt URL** values are unique among all brokers that share this port.

If the broker provides delivery receipts, CIC writes the success or failure counts to the SMSDeliveryReceipts database table.

Related Topics

SMS Broker: Accounts

SMS Broker: Serial Ports and Cell Phones

SMS Broker: Proxy

SMS Broker: Message Terminated

SMS Broker: Configuration

SMS Broker: Message Terminated

A mobile terminated message (MT) is an outbound SMS message that goes to a cell phone. This is the only type of message that can be used by handlers.

Use this page to configure settings used when CIC sends SMS messages.

Enable

Select this check box to enable or disable the MT functionality of this broker configuration. However, the broker configuration Enable setting has precedence over this setting.

Gateway

Type the destination of the HTTP request to reach the provider. CIC combines this destination with a service path by the application, before sending the request to create the complete URL. For some brokers the default gateway may be sufficient, however some brokers require a URL with a unique identifier. The default gateway is http://www.24x.com.

Outgoing Path

Type the path against which an outgoing URL should be validated. By default, the field contains the outgoing path from the broker file, however, you can override this value.

> **Note**: Both inbound and outbound messages must use either HTTPS or HTTP. For more information about using SSL, see the *PureCloud for CIC Administration Guide* in the PureConnect Documentation Library.

Timeout

Type a timeout value in seconds for CIC to use for outbound HTTP requests. If no response is received prior to this timeout, then CIC considers the SMS message as failed. The default is 60 seconds.

Internationalize Phone Numbers

Select this option to send internationalized phone numbers to SMS brokers. Internationalized phone numbers are formatted as FQTN (+CCdddddddd).

Message Parsing

An SMS message has a limit of either 70 characters or 160 characters, depending on the character encoding. The Message Parsing setting lets you configure how messages should be handled if they exceed the size limit:

- None: Do not alter any MT message that exceeds the SMS limit.
- Split messages: Split an MT message that exceeds the SMS limit into multiple messages.
- Truncate Messages: Truncate a message that exceeds the SMS limit. Send only the characters that fit within the limit.

Options

Options are values that are required by some brokers and are too specialized for CIC to consider as a general configuration option. The broker configuration predefines the Names as empty values. You can specify a value for a name by double-clicking on the name, and add or modify the value. Some brokers may fail SMS messages if you do not populate the information with correct values.

> **Note:** If the **ExternalDeliveryStatusURI** option appears, then you must specify a value for it in order to receive delivery receipts for SMS messages. This option contains the external URL that receives delivery receipts for SMS messages:
>
> *If the CIC server is directly connected to the Internet, the external URL is typically http://<CIC Server IP>:<HTTP Port><Delivery Receipt URL>.
> *If the CIC server is behind a reverse proxy or other device, the external URL may be different.
>
> For more information, see the description of the **Delivery Receipt URL** box in the SMS Broker: Message Originated topic.

Related Topics

SMS Broker: Accounts

SMS Broker: Proxy

SMS Broker: Message Originated

SMS Broker: Configuration

SMS Broker Proxy

Use this page to configure the HTTP broker proxy settings if you use a proxy between the CIC server and the HTTP broker endpoint, for example, a corporate HTTP proxy. You set the login and password credentials on the HTTP broker as the ‘Proxy-Authorization’ tag using basic scheme authentication.

Address

Type the address of the proxy server.

Login

Type the user name to use when logging in to the proxy server.

Password

Type the password (associated with the log in user name) to use when logging in to the proxy server.

Confirm Password

Type the password again to avoid typos.

Encryption

Select the type of encryption. The options are None or SSL.

Related Topics

SMS Broker: Accounts

SMS Broker: Message Originated

SMS Broker: Message Terminated

SMS Broker: Configuration

Problem Reporter

Problem Reporter enables an authorized user to report a problem with the CIC clients to the user's support representative. When a user selects the **Report a Problem** option from the Help menu in the CIC client, Problem Reporter automatically creates an email message and addresses it to the user's designated representative. The Problem Reporter also uploads a copy of the user's CIC client logs and, optionally a screen capture of the user's desktop, to the CIC server. Specify the upload location with the ProblemReporterPath server parameter.

To specify a problem reporter email message recipient, type a valid email address. Separate multiple address with a comma.

Note: Problem Reporter is enabled for users that have the Problem Reporter security right.

Layouts

View Layouts

You can add layouts to identify station locations on floor plan images. This can be helpful in call centers, and is used in applications such as Interaction Supervisor iPad Edition.

To view layouts:

1. Click the **View Layouts** action under the **System Configuration** category.

   ...or Click **View Layouts** in the breadcrumbs if available.

2. The **View Layouts** page is displayed.
3. The details of the selected layout are displayed in the details view.

Related Topics:

Add Layout

Add a New Layout

To add a new layout

1. Right-click in the master view area and select **New,** or click the **New** button in the master view toolbar:

   The **New Item** appears in the details view.

2. Complete the following configuration in the first section:

- Type a unique **Name** for the layout.
- Optionally select a **Location** from the drop-down list. If you do not set the location, the default location as configured in Regionalization is used.
- Optionally type a word or phrase that describes this layout.
- Use the up and down arrows to set the pixel width of the layout image. The default is 10 pixels, and the acceptable range is 10 to 2048.

- Use the up and down arrows to set the pixel height of the layout image. The default is 10 pixels, and the acceptable range is 10 to 2048.

3. Complete the layout configuration in the Positions and Advanced details tabs. The links below open the topics containing procedures for completing each details tabs configuration:

- Positions
- Advanced

Related topics

Layouts: positions

Layouts: advanced

Layouts: positions field descriptions

Layouts: advanced field descriptions

Layouts: Positions

The **Positions** details tab allows you to upload an image to use for the layout display. You can then add positions to represent stations on the layout. Click the name of the details tab for field descriptions.

> **Note:** The image for a layout is automatically removed when it is no longer referenced.

To add an image for the layout:

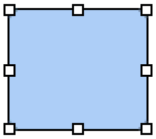
1. Click the **Positions** detail tab to display the details view.
2. Click the **Browse** button to choose an image to upload.
3. Type a unique **Name** for layout image.
4. Save the new image or modified image.

   If necessary, the new image or changes made to an existing image can be reverted.

To add a position on an image:

> **Note:** You can add a maximum of 200 positions per layout.

1. Right-click the image to display the menu.
2. Add a position to the layout. A resizable and moveable box appears.



3. Type a unique name for the position.
4. Set the position's location on the image and its size.

   > **Note:** Positions must not overlap. Any overlapping areas are highlighted in red.

5. Select a CIC station from the drop-down list to associate to the position.

6. You can also do any of the following:
    1. Delete an existing position.
    2. Select a position and **Align**. You can select multiple positions using Ctrl-click, and **Align** in more positions on the image.
    3. Select multiple positions using Ctrl-click, and **Size**.
7. Save the new position(s) or the modified position.

    If necessary, the new code or changes made to an existing position can be reverted.

    Related Topics:

    Add a New Layout

    Layouts: Advanced

    Layouts: Positions Field Descriptions

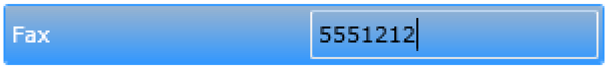
    Layouts: Advanced Field Descriptions

Layouts: Advanced

The Advanced details tab contains the custom attributes and history of the layout. Click the name of the details tab for field descriptions.

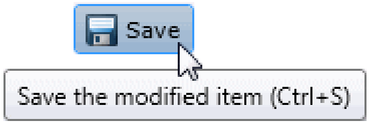
To complete the layout's advanced information:

1. Click the **Advanced** details tab to display the details view.
2. Click Custom Attributes section expander to display the custom attributes section's contents, and complete the following information:
    - To create a custom attribute, click ➕ and type an attribute name. You must also enter a value for the new attribute.



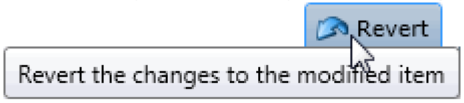
Fax 5551212

3. Click History section expander to display (or hide) the history section's contents, and complete the following information:
    - View the **Created** and **Modified** dates for this layout.
    - Type or view information in the **Notes** field for the layout.
4. Save the new layout or modified layout.



Save the modified item (Ctrl+S)

If necessary, the new layout or changes made to an existing layout can be reverted.



Related topics

Add a New Layout

Layouts: Positions

Layouts: Positions Field Descriptions

Layouts: Advanced Field Descriptions

Layouts: Positions Field Descriptions

This topic contains the descriptions for each field in the **Positions** details view under the **View Layouts** page.

Layout Image section

The following fields are related to the image you are associating with the layout.

Browse

This button opens the **Open** dialog box where you select an image. Supported image types include .jpg, .jpeg, and .png.

Image Display Name

By default, the file name of the image you select for the layout is displayed here. If necessary, rename the image. All image names must be unique across all layouts.

Image to Upload

This is the actual file name that you have uploaded. It is view-only.

Image Dimensions

This is the size in pixels of the image you uploaded.

New Image...

Click this button to upload a new image for the layout.

Clear Image...

Click this button to remove the image from the layout.

Selected Position section

The following fields are related to the positions you associate with stations and place on the layout image. You must have the administrative access right to a position in order to view it and select it.

Name

Type a name for this position on the layout. The name must be unique across all positions in this layout. You might use a person's name associated with the station, like PattyJ for a station named PattyJ_SIP_Station.

Left

Use the up and down arrows to set the left alignment of the selected position.

Width

Use the up and down arrows to set the width of the selected position.

Top

Use the up and down arrows to set the top alignment of the selected position.

Height

Use the up and down arrows to set the height of the selected position.

Station

Select the station from the pull-down list that you want to associate with this position. You can not add a new station here. The station must be an existing station that is already configured, and it must not be assigned to another position. You can select a station only if you have the administrative access right for it.

Related topics

Add a New Layout

Layouts: Positions

Layouts: Advanced

Layouts: Advanced Field Descriptions

Layouts: Advanced Field Descriptions

This topic contains the descriptions for each field in the **Advanced** details view under the **View Layouts** page.

Custom Attributes

Use customized attributes to reference other variables and settings through the IceLib interface. When adding a new attribute, use a unique name, otherwise an existing attribute with the same name will be overwritten. Click **Edit** to change the value of an existing custom attribute, or **Delete** to delete an existing custom attribute.

History

History provides a way to manually document configuration changes and when they occurred. Changes made in Interaction Administrator are also automatically logged in the Interaction Administrator Change Notification Log (Log ID 7). Later, authorized users can run reports against this log to summarize all configuration changes.

Created

This date is automatically set when the user creates the initial configuration for this layout. If the layout was initially created during setup, the date could be blank.

Modified

This date is automatically updated each time the user clicks the **OK** button, presumably after making changes to the layout configuration. To avoid updating this date, exit the page by clicking Revert.

> **Note:** If you click Revert, none of the changes made to this layout since the changes were last saved are preserved.

Notes

Type notes about configuration settings and changes. If you change the configuration and click Save, the **Last Modified** date is updated.

You must manually enter the date beside each entry in the **Notes** field to identify the date of each note.

Related Topics:

Add a New Layout

Layouts: Positions

Layouts: Advanced

Layouts: Positions Field Descriptions

Analytics

Analytics Configuration

Use this page to configure the parameters for Analytics.

Config URI

Enter the endpoint IC will use to communicate configuration changes to the connector.

Data URI

Enter the endpoint IC will use to send statistics to the connector.

Web Proxy URI

Enter the endpoint the web app will use to communicate with the MicroStrategy web server.

Secret

Enter the code that will be used for secure connections between IC and the Config, Data, and Web Proxy endpoints.

Interaction Tracker

About Interaction Tracker

Interaction Tracker allows CIC users to view interaction histories between other CIC users or between a CIC user and an outside contact. When you choose to track an individual, the system stores information specific to a person. When users view a detailed record for an individual, they will be able to see a history of their interactions with this individual. Users can narrow down the interaction history by specifying a date range.

Related topics

Configuring Interaction Tracker

Defining Interaction Tracker types

Interaction Tracker security

Configuring Interaction Tracker

Configuring Interaction Tracker

To use Interaction Tracker you must have the appropriate Interaction Tracker license. For more information, see *the Interaction Tracker Technical Reference* in the PureConnect Documentation Library..

The Interaction Tracker Configuration section includes:

Naming

Server

Database

Multi-language Support

Data Purging

Import and Reassignment

Image and URL

Items Tracked

External Utilities

Timesheet Reporting

Naming

There are four main logical contact entity labels used by Interaction Tracker. These labels are what appears in the Tracker Client. The singular and plural default values can be changed to any label. For example, you may want to see Person\People, Division\Divisions, Company\Companies or ConnValue for iAddress, instead of the label defaults. Each label is limited in length to 15 characters:

Individual

This entity is where the information specific to a person is stored. Individuals can belong to either a location or an Organization; however, they are not required to belong to either. By default, an individual inherits some of the parent location or organization information, like business address and phone number.

Location

The Location entity typically corresponds to physical location. By default, a location inherits some of the parent organization information, like address and phone number. Locations must belong to an Organization.

Organization

The Organization entity typically correspond to companies. Organizations can have individuals directly associated with them, although it is more likely that individuals will be associated with Locations.

iAddress

The iAddresses entity is where the physical addresses for organizations, locations, and individuals are stored. Addresses have types, such as Home, Business, Business2, Shipping, etc. You can extend the address types. An address entry can also be flagged as the default.

Related topics

Server

Multi-language Support

Server

Interaction Tracker encompasses two new server-side subsystems: Tracker Server and Tracker Tran Server. Tracker Server listens for specific events from QueueManager and inserts and updates interaction records. Tracker Tran Server processes insert and update requests from Tracker Server and insert, update, and query requests from Interaction Tracker Clients.

Use this Server page to configure Interaction Tracker behavior.

> **Note:** Change these values only at the request of a certified PureConnect Customer Care representative.

Max Thread Count

Enter the maximum thread count for Tracker Server. The default value is 64. The valid range of values is 16 through 128.

Num seconds before thread considered being hung

Enter the number of seconds to allow a thread to process for Tracker Server. The default value is 60.

Restore Defaults

Click this button to restore settings on the Server tab to default values.

Database

Interaction Tracker stores all information about interactions and participants in tables in the Interaction Tracker Database. These tables are queried for information. Use this Database tab to configure the database behavior.

> **Note:** Interaction Tracker data is stored in the same database as Reporting and IC Public and Private Contacts data, although in different tables.

IC Data Source Name

Enter the IC Data Source Name for the Interaction Tracker database. The default value is IC Tracker.

Query Row Limit

Enter the maximum number of rows to query. The default value is 500.

Query Timeout (sec)

Enter the number of seconds to allow for a database query before timing out. The default value is 45.

Transaction Timeout (sec)

Enter the number of seconds to allow a database transaction before timing out. The default value is 10.

Enable Query Optimizations with Hints (SQL Server)

This query optimization only for SQL Server. By selecting this check box, SQL Server Query processor will use join strategy specified by the Tracker application instead of using the default one.

This setting does not apply to Oracle databases.

Restore Defaults

Click this button to restore settings on the Database tab to default values.

> **Note:** For more information regarding the Interaction Tracker database schema and database planning, see the Interaction Tracker Technical Reference.

Multi-language Support

Multi-language support refers to the translation of data that is displayed in the Interaction Tracker, and in reports, in a language appropriate to the login locale you specified created during setup.

If the appropriately localized language is not supported, the values are displayed in the default language.

Parameters

The Multi-Language Support tab contains three parameters: **Attribute**, **Language**, and **Value**.

Parameter	Definition
Attribute	The name of the value to be translated. Translation is elected for only a few values that are displayed in reports or status messages
Language	The language used for the translation. The default language is that currently set by the administrator. A list of 100 + additional languages appears in the **Languages** dialog when you click **Add Language**. This value is **Default** if no language is specified for your login country in the **Languages** list.
Value	The value to display; the translated value.

Buttons

The Multi-Language Support tab also contains the buttons: **Edit Value**, **Add Language**, and **Remove Language**. This is the function they perform:

- Edit Value
- Add Language
- Remove Language

For more information on the function of the scroll buttons and the **Confirm auto-save** check box, see Interaction Administrator Interface.

Data Purging

Use this page to schedule when the system deletes expired records in the Interaction Tracker database. Expired records are those that have exceeded their retention time.

Enable Purging

Select this check box to enable data purging. By default this checkbox is enabled.

Purge data at this time of day

Type the time of day to begin the data purge. The default value is 2:30:00 AM.

Purge data older than

Type the number of days that defines expired data. The default value is 34.

Related Topics

Cache clean up

Database

Configure Interaction Tracker server cache clean up

The Interaction Tracker server maintains data about active interactions in its in-memory caches. Some custom call scenarios may result in improper cache cleanup, which can lead to incorrect data for impacted interactions. to ensure proper cache clean up, you may want to enable and customize the automated cache clean up mechanism. See the How to enable automated cache clean up in Tracker Server knowledge base article for more information.

Import and Reassignment

This page contains import and reassignment utilities.

The import utility is provided as an easy way of importing or re-importing individuals from current CIC users at a given a Site ID, multiple Side IDs, or all Site IDs.

The reassignment utility is provided as an easy way of reassigning individuals to other locations at a given a Site ID, multiple Side IDs, or all Site IDs.

IC User Location Reassignment

In this reassignment area of the page, enter the home site IDs to reassign to the selected location.

Location

Select the location to reassign the Home Site(s) to.

Home Site IDs

Enter the **Home Site IDs** separated by commas and click **Reassign Now.** Leave this field empty to specify all sites.

IC User Import

In the import area pf the page, enter the home site IDs from which to import users.

Update existing entries

Select this check box to overwrite already existing entries.

Home Site IDs

Enter the **Home Site IDs** separated by commas and click **Import Users Now.** Leave this field empty to specify all sites.

Image and URL

Use this page to set images and URLs for CIC users. The Image and URL set the image path and URL of the CIC user's picture in the CIC clients.

Set Images for CIC Users

Enter the filename and path for the image to be associated with the CIC user. Click **Set Images Now** to save your settings.

Set URL for CIC Users

Enter the location of the URL for the CIC user. Click **Set URLs Now** to save your settings.

Items Tracked

Use this page to configure the items for Interaction Tracker to track. Remember, an interaction is a communication between two or more individuals, where one of the individuals is a CIC client user.

Interaction Types Tracked

Select the types of interactions to track. The options include:

- Calls
- Chats
- Direct Messages
- Emails
- Faxes
- Generic Objects
- SMS
- Social Media

> **Note:** As of CIC 2016 R4, inbound SMS messages are tracked separately from chats.
>
> If the Recorder license is enabled on the system, then call, chat, email, and SMS interactions are logged in the database and tracked, regardless of the selections under Interaction Types Tracked.

Track Intercom Interactions

Select this check box for Tracker Server to track intercom interactions. An intercom interaction is a call or chat from one person to another internally or "interoffice". By default, this check box is checked.

Track Routing Exceptions

Select this check box for Tracker Server to track routing exceptions, including events like abandons, flowouts, and transferred interactions. By default, this check box is not checked.

Track Interactions Without a User Connect Event

Select this check box for the Tracker Server to continue tracking an interaction without a connect event. A user connect event is when a party connects to an interaction, e.g. the user picks up a call in the CIC client or with the headset. By default, this check box is not checked.

Track Voicemails

Select this check box for Tracker Server to track voicemail messages.

Track Additional Segments (i.e., System, Workgroup, Queue, Alert, Messaging, and Hold)

You can also track additional segments by clicking the check box for the desired option:

- Workgroup queue based interactions
- Non-workgroup queue based interactions
- Intercom interactions
- Interactions without a user connect event

System Segment Optimizations

You can configure Interaction Tracker to discard tracked segments that are less than a specific number of seconds.

Related Topics

Track_Abandoned_Dialer_Interactions_in_InteractionSummary

External Utilities

Reserved for future use.

Launch External Utilities

If external utilities for Interaction Tracker are available in the future, you will be able to launch them here.

Timesheet Reporting

Use this page to configure the distribution of timesheets for individual users who have been assigned the Billable-Time User Role in Interaction Administrator under the People container.

Enable Timesheet Reporting

If you have a Timesheet reporting license, select this check box for Timesheets to be emailed to members of your Billable-Time User role.

Run the Report

Select when you want your Timesheets delivered, either Weekly or Daily.

Time

Select or type the time to run the data for your timesheet.

Day

From the drop-down list, select the day to run the data for your timesheet.

Role of Users to Receive Timesheet

From the drop-down list, select the Role of the users you want to receive this report. The default role is Billable-Time User.

Smallest Billable Time Unit

Type or select the smallest billable time in minutes. This field is enabled only if "Billing Units" is selected in the **Billable Time Format** field.

Billable Time Format

Select or type the time format for your timesheet.

> **Note**: Timesheets are delivered in XML format, and can be viewed in an Excel spreadsheet. The XML file is attached to the e-mail that is sent to the members of your Billable-Time User role.

Related topics

Roles

Defining Interaction Tracker Entity Types

Defining Interaction Tracker Types

To begin using Interaction Tracker, you must first define types. Define types for Interactions, Individuals, Organizations, and iAddresses. You can further define iAddress Sub-types to extend this type. You may also define Tracker Attributes and Titles.

The Defining Interaction Tracker Types section includes:

Individual Types

Organization Types

iAddress Types

iAddress Sub-types

Tracker Attribute Types

Tracker Address Types

Titles

Individual Types

You must define your individual types. Enter types such as Public Relations Manager, Marketing Director, Finance Executive, etc.

Database ID

This is the database ID of the new attribute. This ID is automatically generated for the new attribute and cannot be changed.

> **Note:** Individuals can belong to either a Location or an Organization; however, they are not required to belong to either. By default, an individual will inherit some of its parent location or the organization information, like business address and phone number.

Organization Types

You must define your organization types. Enter types such as Public Relations, Marketing, Finance, etc.

Database ID

This is the database ID of the new attribute. This ID is automatically generated for the new attribute and cannot be changed.

iAddress Types

You must define iAddress types. Enter types such as Home, Mobile, Shipping, etc. An iAddress type can be flagged as default.

Database ID

This is the database ID of the new attribute. This ID is automatically generated for the new attribute and cannot be changed.

iAddress Sub-types

You may define iAddress Sub-types. Use iAddress Sub-types to extend iAddress types. Enter Sub-types such as Home 1, Business 2, etc.

Database ID

This is the database ID of the new attribute. This ID is automatically generated for the new attribute and cannot be changed.

Tracker Attribute Types

You may define attribute types for some of the Interactions, Interaction Participants, Individuals, Locations and Organizations to extend the types.

Tracker Attribute Name

Enter the name of the attribute.

Show if Empty

Select this check box to if you want the attribute name to be displayed in Interaction Tracker Client even if it is empty.

Database ID

This is the database ID of the new attribute. This ID is automatically generated for the new attribute and cannot be changed.

Applies to (Select all that apply)

Select any of these entities you want for the attribute to apply:

- Individuals
- Locations

- Organizations
- Interaction Segments - default - (selecting this option will enable the Segment Attribute Mapping below)

Custom Attribute to Interaction Segment Attribute Mapping (server-specific)

You can specify an interaction attribute name and Tracker Server will retrieve the value at interaction deallocation time and store it with the interaction segment. This custom mapping option is only available if you have selected **Interaction Segments** above.

Get Value From custom Interaction Attribute check box

Check this if you want the value of the attribute to come from an interaction attribute.

Custom Interaction Attribute to Use

Specify the name of the interaction attribute that will be retrieved at interaction deallocation time. For example, you might create a custom attribute named "Gender".

> **Note**: Restart the client for the change to take effect.

Legal Values Presented in Tracker Client

Add or Remove values to assign to the attribute. Use the Up and Down buttons to arrange order of selection. For example, for Gender you can specify legal values that will appear as selectable items in a drop down list for the Gender attribute. The order in the list is the order the values appear in the Tracker Client dialog boxes.

Tracker Address Types

You may define Address types. Enter types such as Home, Billing, Shipping, etc.

Database ID

This is the database ID of the new attribute. This ID is automatically generated for the new attribute and cannot be changed.

Titles

You may define titles. Enter titles such as Mr., Mrs., Miss, Ms., etc.

Database ID

This is the database ID of the new attribute. This ID is automatically generated for the new attribute and cannot be changed.

Security

Interaction Administrator controls Interaction Tracker's security. You control access and rights in Interaction Tracker features by setting Tracker Policies in the Security tab in the User configuration. The rights available to apply to a user are:

- Add Individuals
- Modify Individuals
- Delete Individuals
- Add Organizations
- Modify Organizations
- Delete Organizations
- Modify Interactions
- View Other People's Private Interactions
- Have Private Contacts
- Tracker Administration

Notes:

Organizations include Locations.

Interactions include Interaction Participants.

The ability to see other people's non-private interactions is administered via the 'View User Interaction History' category on the Access Control tab of the User Configuration.

Add, Modify, and Delete rights apply to manual operations using the Tracker Client – automatic insertion and modification of interactions by the system is not affected by these rights.

Interaction Recorder's access control is used to determine whether or not users can playback any recorded media for the interaction. The exception to this is when the user is a participant in the interaction; in this case he/she will always be able to playback any recordings for his/her segment of the interaction.

The user who creates a record becomes the current owner. Owners of a record always have full rights (the system prevents you from deleting a record that is being used).

Interaction Recorder

Interaction Recorder

Use the Interaction Recorder (IR) Configuration dialog box to determine what interactions are recorded and to configure how interactions are recorded, how the recordings are compressed, where they're stored, how they're retrieved, etc. Interaction Recorder data is stored in the same database as Reporting and CIC Public and Private Contacts data, although in different tables.

> **Note:** For more information see *Installing and Configuring Interaction Recorder* in the PureConnect Documentation Library.

This section includes:

Configuration

Policy Editor

Screen Recording

Remote Content Server

Who can see and listen to recordings

Configuration

Interaction Recorder Configuration

Click on the following options for specific configuration information.

- Recording Processing
- Email
- Recording Generation
- Key Generation
- Cloud Services Configuration
- Screen Recording
- Remote Content Server

Recording Processing

Use this page to configure Interaction Recorder's (IR) Recording Processing.

Compression Format

Select the compression format for recordings from the drop-down list:

- **µ-Law (Mono)** - This format does not compress recordings.
- **True Speech (Mono)**
- **GSM 6.1 (Mono)**
- **Opus (Mono)**
- **Opus (Dual-channel)**

> **Note:**
> The Opus recording and compression format options are available for Interaction Media Server version 2017 R1 or later. If previous versions of Interaction Media Server are connected to this CIC server, it creates the recordings on those servers with the GSM 6.1 format and creates entries in the error log for an unsupported Interaction Media Server version.

> The Opus recording and compression formats generate larger recordings due to the increased fidelity of the audio and, in the case of Dual-channel, two channels of audio. Ensure that Interaction Media Servers, Interaction Recorder Remote Content Servers, and Interaction Recorder have enough free storage space to accommodate the larger recordings.
>
> For more information about Opus, see *Interaction Recorder and Quality Manager Technical Reference* and *Interaction Media Server Technical Reference*.

For other recording options that you can set on a SIP line, see SIP Line Recorder.

Database Processing

Use this utility to initiate the recovery of failed database transactions. Clicking the Recover Errors button makes Interaction Recorder process the PMQ error files. This function can be used when your database has been unavailable and you want to get the data that has been logged into the PMQ error files into the database.

Secure Recording Pause Duration (seconds)

Enter the number of seconds an audio recording is paused when an agent presses the Secure Pause button on the queue toolbar in the CIC clients. The default setting is 20 seconds.

Related Topic

Media Servers

Email

The e-mail option contains the configuration information necessary for the Interaction Recorder Server to communicate with the e-mail system in order to send recordings.

System E-mail Address

Enter the e-mail address to be used as the Reply To (from) e-mail address when a recording is e-mailed from Interaction Recorder Client.

Reply To Address For Recordings E-mailed From Recorder Client

Select **Use System E-mail Address** to use the e-mail addressed specified in the **System E-mail Address** box. Select **Use E-mail Address of User Logged in to Recorder Client** to use the Recorder Client's user's e-mail address.

Recording Generation

Use this page to configure Interaction Recorder's recording generation options.

Recording

Select the options in the Recording box to configure how Interaction Recorder server initiates recordings.

Enable Recording

Select this check box to record all interactions that qualify for recording based on Interaction Recorder Initiation Policies. If this box is *not* selected, recordings will not be generated.

Stop Interaction Recorder Initiated Recordings at Transfers

Select this check box to stop recording a call when it is transferred. If this check box is selected, each transferred segment of a call will be its own recording and database entry.

If this check box is clear (not selected), recording continues after the transfer. This applies only to calls that were defined to be recorded by the Initiation Policy. Also, if this box is not selected, it is not possible to play only a segment of the call or skip to a specific segment.

Default Audio playback device of recordings to the handset

Select this check box to set the handset as the default audio playback device for a recording. When listening to a recording, the audio playback device can be changed on the Audio menu in the Interaction Recorder Audio Playback window, in IC Business Manager.

Enable Snippet Recordings

To enable the snippet recording feature on this CIC server, select this check box. This feature allows users to create ad hoc recordings of their interactions.

Encrypt Snippet Recordings

To enable the encryption of snippet recordings, select the **Encrypt Snippet Recordings** check box. This option is available only if you enable snippet recordings.

> **Note:**
>
> For more information about configuring encryption for recordings, see Key Generation.
>
> In order for users to make snippet recordings, you must also assign the appropriate security rights and permissions to them. Depending on the person, some combination of the following items is necessary:
>
> * Security Rights > Interaction Command Rights > **Snip**
> * Security Rights > My Interaction Rights > **Snip Interactions**
> * Access Control > Queues category > User Queues > Advanced Access Details > Monitor > **Snip**
>
> For more information about the security rights and permissions that you set in Interaction Administrator, see Assign security rights and Assign access control rights.
>
> For more information about Snippet Recordings, including information about the necessary licenses, see the *Interaction Recorder and Interaction Quality Manager Technical Reference* in the PureConnect Documentation Library.

Enable HTTPS Exchanges for Playback, Archiving, and Exporting Recordings

Select this check box to use HTTPs for: communication and traffic for playback, archiving; and exporting of calls, chat, and email recordings.

Unlicensed Recordings

Recordings are encumbered if the user or station was not properly licensed for Interaction Recorder when the recording was made. Encumbered recordings are listed in a search result in the Interaction Recorder client search results view when the **Recording is Encumbered** search attribute is used. Encumbered recordings cannot be played back.

To unencumber a recording, first fix the licensing for the user that has encumbered recordings. Next, contact PureConnect Customer Care to get an unencumber key to unlock the encumbered recording that needs to be played back. Then in the Unlicensed Recordings field, enter a valid unlock code to unencumber the encumbered recordings on the server.

Key Generation

Use this page to generate a Master Key for Recording Encryption. A master key securely protects Recording Keys (media keys), which are generated every time a media file is recorded.

Master Key File

The first step in generating a master key is to specify the location of the master key file. Master keys are stored in the master key file in plain text. For security purposes, make sure the location of the master key file has restricted access.

Generate New Key

Click **Generate New Key** to manually generate a new Master Key. When you click OK or Apply for the first time, an initial Master Key is created and appended to the Master Key file. You can also use this button to manually create a new key and append it to the Master Key file.

Import Key File

Click **Import key file** to import a key file and merge it with the existing Master Key File. An Open dialog is displayed to specify the location of the file to be imported. When the key file is successfully imported, a confirmation message is displayed. If the key file import fails, an error message is displayed.

Import key file can be used to import a 3.0 Recorder key file to the current release. You can also use it to import a key file in order to replace a bad key file. For example, if a switchover pair did not share a key file location.

Master Key Password

Use the Master Key Password box to password protect the Master Key File and securely encrypt master key data. To create, change, or deactivate a Master Key Password, the user must be assigned the Security Right **Master Key Password Administrator**.

> **Important**: PureConnect Customer Care cannot recover encrypted recordings if a Master Key Password is lost.
>
> **Important**: The master key password is not replicated to the backup PureConnect server in a switchover environment. It needs to be activated after every switchover or system start-up.

Change Password

Click **Change password** to create a new Master key password or to change the current password.

Deactivate/Activate Password

When you create a new Master key password or change the password, the password is Activated, and the Deactivate password button is displayed. To deactivate the password, click **Deactive password**. To activate the password, click **Activate Password**, and on the Activate Password dialog, type the password and click **Activate**.

Recurring Key Generation

Use the **Recurring Key Generation** box to configure parameters to automatically generate a new Master Key on a recurring basis.

Generate New Key Recurrently

To automatically generate a new Master Key, select the **Generate New Key Recurrently** check box.

To schedule an automatic key generation: in the Recur every box, type the number for the weekly recurrence; in the drop down-list, select the day of the week to generate the key; and in the time field, select the time of day to run the key generation.

> **Note:** For more information on recording encryption and key generation, see *Interaction Recorder and Interaction Quality Manager Technical Reference* in the PureConnect Documentation Library.

Cloud Services Configuration

Use this page to configuration Interaction Recorder's Cloud Services.

You can use Amazon Simple Storage Service (Amazon S3; also referred to as AWS S3) to store your recordings and to archive your retention polices in Policy Editor. For more information on Amazon S3, see http://aws.amazon.com/s3.

> **Prerequisite:** Before you begin, configure your Amazon S3 account. Make note of your bucket name and your secret key. For more information, see "Using Amazon Simple Storage Service" in the *Interaction Recorder and Interaction Quality Manager Technical Reference*.

Amazon S3 Bucket Keys Configuration

New Bucket

Follow these steps to configure a new bucket.

1. Click **New Bucket**.

   The **S3 Keys Editing** dialog appears.

2. In the **Bucket name** box, type the name of the Amazon S3 bucket.

   > **Note:** Use the exact name that you assigned to the bucket in your Amazon S3 account.
   > If you are using HTTPS, the S3 Bucket name cannot contain periods as Amazon's SSL wildcard certificate only matches buckets that do not contain periods.

3. In the **Account ID** and **Secret Key** boxes, type the corresponding information from your Amazon S3 account. The Account ID is the AWSAccessKeyID, and the Secret Key is the AWSSecretKey.

4. In the **Region Endpoint** list, select the region where recordings are stored or accessed. This information helps reduce data latency when you access or store recordings with the Amazon S3 service.

> If the region endpoint is not in the list, you can select **Specify Custom S3 Endpoint**, and then click **Configure**. In the **Specify Custom Endpoint** dialog, enter the endpoint information. When adding a custom region and endpoint, the display name must match the region name defined for the given endpoint. Endpoints are defined in Amazon S3.

5. Click **Test**. This validates that the specified bucket and region configuration is valid and that a test communication with the Amazon S3 service can be successfully completed for read, write, and delete access. The field is not available unless you have specified a bucket name.

> **Note**: You can also create a new bucket when you create a retention policy in Policy Editor.

Modify Bucket

To modify an existing bucket, select the bucket and click **Modify Bucket**. The S3 Keys Editing dialog appears. You can modify the **Account ID** and the **Secret Key**.

> **Note:** You cannot modify the region endpoints.

Delete Bucket

To delete an existing bucket, select the bucket and click **Delete Bucket**.

Enable HTTPS exchanges

This check box determines whether the exchanges between Amazon S3 cloud services and Interaction Recorder Server are HTTP or HTTPS. By default, HTTPS is selected.
Note The S3 Bucket name cannot contain periods as Amazon's SSL wildcard certificate only matches buckets that do not contain periods.

Policy Editor

Double-click on **Configuration** to open the Interaction Recorder Policy Editor. Interaction Recorder Policy Editor is a single, simple user interface used for creating Polices.

Access the help from the Policy Editor interface for more information.

Who can see and listen to recordings

The following table summaries the conditions under which users can see recordings.

Under these conditions...			You can see...			

You have the Monitor Columns security right	The EnableSupervisoryRecordAndMonitor server parameter is enabled	You are a supervisor	Your own recording	A supervisor's recording	A non-supervisor's recording	A syst record by Intera Recor
No	(Any)	(Any)	Yes	No	No	No
Yes	No	(Any)	Yes	Yes	Yes	Yes
Yes	Yes	No	Yes	No	No	No
Yes	Yes	Yes	Yes	Yes	Yes	No

> **Note:** Users can always see their own recordings. If the **EnableSupervisoryRecordandMonitor** server parameter is turned on, then only supervisors can see recordings for other users.

For more information about the **EnableSupervisoryRecordAndMonitor** parameter, see Packaged Server Parameters.

For more information about the **Monitor Columns** security right, see Assign security rights

Related topics

Interaction Recorder

Screen Recording

Interaction Screen Recorder

Interaction Screen Recorder adds screen recording capability to Interaction Recorder. In addition to Interaction Recorder features including multi-media recording for phone calls, emails, faxes, and Web chats, Screen Recorder provides another contact center solution.

Synchronizing the audio recording of an agent with the workstation activity, screen recording provides a complete management tool. Screen Recorder assists contact center managers and supervisors in improving their contact center's productivity and assessing agents' skills.

Configuring Screen Recorder

Capture settings and location for Screen Recorder is configured on the Screen Recording Configuration Settings page. Screen Recorder is applied to Recording Rules in Interaction Recorder Selector.

Related topics

Screen Recording Configuration

Screen Recording

Use this page to configure Interaction Screen Recorder.

General

From the **Default Regional Location** drop-down list, select the location for which region screen recordings will use if Interaction Recorder cannot determine the region based on the interaction or station.

Capture Settings

Use the following fields to configure these settings.

Capture Rate (fps)

Use this box to type or select the capture rate in frames per second (fps). The default is 1 fps. The available values are: 0.25, 0.5, 1, 2, 4, or 8 fps. Here is a chart of the capture rate settings to consider for storage capacity (The higher the setting the more storage used):

Capture Rate Settings	
Setting	Equals
0.25	1 frame every 4 seconds
0.5	1 frame every 2 seconds
1	1 frame per second
2	2 frames per second
4	4 frames per second
8	8 frames per second

Mouse Capture Rate

Use this box to type or select the mouse capture rate in times per frame. The default is 4. The available values are: 1, 2, 4, 8, or 16.

Compression

Use this box to set the compression rate. The default is set to 9. The available options are any integer from 0—no compression, to 9—maximum compression.

Stop Recording When Agent Becomes Available

Configure this setting to control the recording of an agent’s screen. Set the value to **Yes** to stop the recording when the agent becomes available. When the value is set to **Yes**, the recording stops even if the agent is in lag time.

If the value is set to **No**, the recording continues when the agent becomes available; the number of seconds the recording continues is set by Lag Time.

Lag Time (sec)

Use this box to add configurable lag time at the end of an interaction for screen capture. The Interaction Recorder Server terminates a screen recording when the lag time expires. The default is **120** seconds (2 minutes). The available options are any integer from 0 to 3600 (60 minutes).

> **Note:** As a result of internal batch processing, your agents might experience up to an additional 10 seconds of lag time during screen recordings. For example, if you set the lag time to be 15 seconds your agents might experience a lag time from between 15 seconds to 25 seconds during screen recordings.

Color Depth (bpp)

Use this box to set the color depth in bits per pixel (bpp). The default is set to Native. The available options are: Auto, 8-bit, 16-bit, and 24-bit. The values will be stored as 0, 8, 16, and 24.

Max simultaneous screen recordings per agent

Use the drop-down list to set the value for the maximum number of simultaneous screen recordings per Interaction Screen Recorder Capture Client. When the maximum limit is reached, every new screen recording stops the oldest one in progress.

Remote Content Server

You configure Interaction Recorder Remote Content Service through Interaction Administrator. The **Remote Content Server Configuration** dialog box contains the following fields:

Alternate Fully Qualified

If you are using PureConnect Cloud, enter a replacement fully-qualified domain name (FQDN) for this Interaction Recorder Remote Content Service server in your domain.

In a PureConnect Cloud environment, this feature enables Interaction Recorder to retrieve and play the recording from this Interaction Recorder Remote Content Service server.

Active Locations

Select the check box for the region where you want Interaction Recorder Remote Content Service to reside. You create regions through the **Regionalization** sub-container under the container for your CIC server.

> **Note**: For Interaction Recorder Remote Content Service to function properly, it must reside in the same region as the media server from which it processes recordings.

Entries are automatically added when a Remote Content Service starts. After the service appears, you can use this page to specify directories. For more information, see *Interaction Recorder Remote Content Service Installation and Configuration Guide* in the **Technical Reference Documents** section of the PureConnect Documentation Library on the CIC server.

Disable Screen Capture Transfers from this RCS

Select this check box if you want to prevent Interaction Recorder Remote Content Service from transferring screen recordings from the computers on which they are recorded.

Disable Other Recording Transfer from this RCS

Enable this check box if you want to prevent this Interaction Recorder Remote Content Service instance from transferring any recordings—other than screen recordings—from the servers on which they are recorded.

Related topics

Configuring Remote Content Services

Regionalization

Interaction Optimizer

Interaction Optimizer

Customer Interaction Center and Interaction Optimizer provide a complete workforce management solution. Interaction Optimizer uses forecasting, scheduling, and real-time schedule adherence allowing a contact center to plan for and ensure optimal staffing and service levels at any given time.

Workforce management process overview

At a high level, the workforce management (or workforce optimization) process involves the following step:

- **Select Your Service Level Objective**: Determine the appropriate service level based on the specific services provided, and on the analysis of forecasting data and real-time adherence. Service level is expressed as “X percent of interactions answered in Y seconds”.
- **Collect Data**: CIC's Stat Server collects ACD data that shows the number of ACD interactions received, the interaction duration, and the interaction patterns.
- **Forecast Interaction Load**: Use volume forecasting based on the collected ACD data to determine accurate predictions for future interaction load.
- **Forecast Headcounts**: Use ACD simulation or Erlang_C based on volume forecast to determine accurate staffing level predictions.
- **Publish and Manage Schedules**: Generate schedules based on forecasting, make adjustments if necessary, and publish the schedules.
- **Analyze Performance**: Use data obtained from the agents’ adherence to the schedule, and determine the schedule’s accuracy regarding the actual interactions received. Based on this information, make adjustments to the volume and heacount forecasts for generating the next week's schedule.

Configure your options and monitor results

> **Note:** Beginning in CIC 4.0 SU6, most Interaction Optimizer functionality, including configuration settings, is available only through IC Business Manager.

To fulfill the workforce management functions, use the following applications:

- Interaction Administrator: Use Interaction Administrator to configure:
    - Optimizer Database
    - Agents
- **Interaction Optimizer:** Use the **Interaction Optimizer** module in the **Interaction Center Business Manager** application to do the following:
    - Configure client options
    - Configure server options
    - Map status messages to activity types
    - Manage special days (day classifications)
    - Configure scheduling units
    - Configure forecast and schedule entries
    - Complete the steps to create forecasts and schedules
    - Manage time-off requests
    - Make normal scheduling edits
    - Apply time off requests
    - Publish the schedule
    - View real-time adherence (RTA) events on current or previous schedules
    - Use intraday monitoring to compare activity
- **Interaction Supervisor:** Use Interaction Supervisor to view or monitor:
    - User and Schedule Statistics
    - Real Time Adherence Events
    - Time Off Requests
    - Reports
- **CIC Clients:** Use Interaction Desktop to:
    - View Published Schedules
    - Submit Time Off Requests

> **Note:** Interaction Optimizer availability and behavior depends on how it is licensed, and how access control is configured. For more information, see the *Interaction Optimizer Technical Reference* in the

> **Technical Reference Documents** section in the PureConnect Documentation Library on the CIC server.

For more information

For information on configuring and running Interaction Optimizer, see the Interaction Optimizer help.

For more information on Interaction Supervisor, see the Interaction Supervisor help.

For more information on the CIC clients, see the Interaction Desktop help and the Interaction Connect help.

Interaction Optimizer Configuration

Advanced Configuration

Interaction Optimizer Configuration

Use the following page in the **Advanced Configuration** dialog box in the Interaction Optimizer Configuration container to configure database options for Interaction Optimizer. These configuration parameters affect the performance of the Interaction Optimizer forecasting and scheduling engine.

- Database

Interaction Optimizer Database Configuration

This page displays the settings that control the behavior of Interaction Optimizer database transactions.

> **Note:** Change these values only at the request of a certified PureConnect Customer Care representative.

IC Data Source

This is the data source that Interaction Optimizer uses to locate the tables of data necessary to generate volume and headcount forecasts, and to generate schedules. The data source is set during installation.

Transaction Timeout (seconds)

This setting is the number of seconds before a database transaction will timeout. Database performance could be involved in a transaction timeout, but there could also be overall databases problem, network load issues, etc.

The default value for this setting is 10 seconds. Acceptable values are 10 through 3600 seconds.

Web Server URI

This is the URL for Interaction Optimizer - Web Edition. When you type the URL here, agents see the Interaction Optimizer web applications in Interaction Desktop My Schedule view.

> **Note:** If you specify a web address for any other website, an error message appears.
>
> When you specify the URL for Interaction Optimizer - Web Edition, then Interaction Desktop no longer displays the .NET version of the My Schedule view. If you clear this field, Interaction Desktop displays the original My Schedule view again.

Defaults

Click this button to return these settings to the default values.

Agents

Agents

Use this page to add agent schedule exceptions (constraints) to weekly shift definitions. The scheduling engine uses these settings when it generates schedules for agents.

Examples

Daily agent constraint example

John Smith is one of many agents who are assigned to a weekly shift definition. However on Tuesdays, John must leave an hour early (4:00 P.M.) to attend physical therapy sessions. You can add this exception as a **Daily Agent Constraint** by setting the **Latest Shift Stop Time** value to 4:00 P.M.

Weekly agent constraint example

Sally Jones is normally paid for 40 hours a week. She is one of many agents assigned to a weekly shift definition. However every day of the week for several weeks, Sally will be attending a "Lunch and Learn" session during her lunch break. These sessions are considered paid time. You can add this exception as a **Weekly Agent Constraint** by setting the **Minimum Paid Time** value to 45 hours.

Agent Configurations

The **User Name** box contains the names of the agents for whom agent schedule exceptions have been configured. Click **Add** to select agents and then configure the schedule exceptions. Click **Remove** to remove an agent and the schedule exceptions.

Agent Configuration Settings

Select Daily Agent Constraints or Weekly Agent Constraints. Then complete the corresponding details.

Daily Agent Constraints

Do one of the following things:

- To add a constraint, click **Add**. Complete the **Daily Agent Availability Constraints** dialog box.
- To edit a constraint, select the constraint and then click **Edit**.
- To remove a constraint, select the constraint and then click **Remove**.

Weekly Agent Constraints

Specify the requirements for paid time, shift time, and shift days for the selected weekly shift definition.

> **Note**: There are default values for each of the configurable items, however the defaults are **not** enabled unless you select the corresponding check boxes. By default the scheduling engine uses the maximums of the maximums and minimums of the minimums to generate schedules for agents.

Minimum Paid Time

Select this check box to set the agent's desired minimum number of paid hours per week. In the box, type any value between 0 and 168. The default value is 20 hours.

Desired Maximum Paid Time

Select this check box to set the agent's desired maximum number of paid hours per week. In the box, type any value between 0 and 168. The default value is 40 hours. For example, an agent might want to work 50 paid hours a week to earn extra income.

> **Note**: If the desired service level cannot be met, the scheduling process schedules agents above their maximum number of desired paid time hours. See **Absolute Maximum Paid Time**.

Absolute Maximum Paid Time

Select this check box to specify the agent's absolute maximum paid time in hours per week. In the box, type any value between 0 and 168. The default value is 50 hours. For example, a company may not allow any agent to work more than 40 paid hours a week.

> **Note**: The scheduling process observes the absolute maximum paid time hours regardless if the agents can meet the desired service level. See the **Desired Maximum Paid Time**.

Minimum Time Between Shifts

Select this check box to set the minimum number of hours between shifts for the agent. In the box, type any value between 0 and 168. The default value is 12 hours. For example, a company might allow agents to work a 3:00 P.M. to 11:00 P.M. shift on Monday, and then another shift at 7:00 A.M. to 3:00 P.M. on Tuesday. In this case, set the minimum time between shifts to 8 hours.

Maximum days

Select this check box to set the maximum number of days that the agent can work. In the box, type any value between 1 and 7. The default value is 7 days.

Related topics

Service level

Agent constraints versus shift constraints

Daily Agent Availability Constraints dialog box

Agent Activity Configuration dialog box

Daily Agent Availability Constraints

Use this page to configure the availability constraints for the selected agent. Occasionally, agents have work schedule conflicts that need to be accounted for in the shift schedule. These conflicts are less common to schedule around than the more general shift constraints that apply to everyone. Click here for more information on the differences in agent constraints vs. shift constraints.

Interaction Optimizer uses the most constrained value of the daily agent availability constraints and the daily shift constraints, using the maximum of the minimums and the minimums of the maximums.

For example, if an agent's minimum paid time in the daily agent availability constraint has a value of 0, but the agent's minimum paid time in the daily shift constraint has a value of 2, the daily shift constraint value of 2 is used because it's more constrained.

See Agents for a daily agent constraint example.

Shift Configuration

Use this section to set start, stop and paid time for this agent. Hours and minutes can be specified in each field. Click on the hours position or the minutes position, then click the up or down arrow keys. Each active day that is assigned a constraint, is listed as an **Active Day** in the **Agent Configuration** dialog box.

Earliest Shift Start Time

Select this check box to set the earliest time in the AM or PM hour this agent will be allowed to start the shift. 8:00 AM is the default value for this setting.

Latest Shift Stop Time

Select this check box to set the latest time in the AM or PM hour this agent can end the shift. 5:00 PM is the default value for this setting.

Minimum Paid Time

Select this check box to set the minimum time in hours this agent can be paid for this shift. 4 hours is the default value for this setting. For example, a value of 0 means that the agent is not required to have any paid time for that day.

Maximum Paid Time

Select this check box to set the maximum time in hours this agent can be paid for this shift. 10 hours is the default value for this setting.

Active Days

Select the days that this agent is available for a shift.

Activities

This section lists the scheduled activities during a shift for the selected agent. The Activity Type, Earliest Start, Latest Start, and Activity Length are displayed. Click Add to add a new activity, click **Edit** to change the existing activity, or click **Remove** to remove an activity for the selected agent.

Agent Activity Configuration

Use this page to configure an agent activity. An agent activity is an activity that a specific agent completes during the agent's shift.

An agent activity is different than a shift activity. A shift activity is a reoccurring activity for all agents in the shift.

The settings for agent activities either compliment or override the settings for shift activities.

Activity Type

Select an activity type from the list. Activity types are mapped to agent status in Activity Types.

Length

Set the duration of the activity. Use the format HH:MM. The default length is 1 hour. The minimum length is 5 minutes.

Start Time Configuration

Use the section to specify the start time settings for this activity for this agent. Select the hour or minute position to change the time.

Use Relative Times

Select this check box to use times relative to start times. If selected, *Earliest Start Time From Shift Start* and *Latest Start Time From Shift Start* appear below. If this check box is not selected, absolute times are used. Absolute times are represented by A.M. and P.M. By default, this check box is not selected.

If the agent is assigned different shifts, then use relative time so that the settings are valid for all of the agent's shifts. For example, select **2:00 hours from shift start** rather than **10:00 A.M**.

Earliest Start Time (From Shift Start)

Select the hour or minute position, and then use the up and down arrows to set the earliest time this activity can start. The default value for this field is 8:00 A.M.

Latest Start Time (From Shift Start)

Select the hour or minute position, and then use the up and down arrows to set the latest time this activity can start. The default value for this field is 9:00 A.M.

Start Time Increment

Select the hour or minute position, and then use the up and down arrows to set the increment in minutes that this activity can start. The default value for this field is 15 minutes. The system uses this increment during schedule generation. To avoid excessive work or time for schedule generation, the number of possible start times can not exceed 50.

For example, if the earliest activity start time is 9:00 A.M., the latest start time is 10:15 A.M., the start time increment is 15 minutes, and the length is 15 minutes, then the scheduling process would first try scheduling this activity at 9:00, then at 9:15, then at 9:30 and so on every 15 minutes until 10:15.

Counts Toward Paid Time

Select this check box if this activity counts toward paid time. For example, lunch is normally not considered paid time. By default, this check box is not selected (enabled).

Counts Toward Contiguous Work Time

Select this check box if this activity counts toward contiguous work time. For example, if an agent needs to attend a meeting from 7:00 A.M. to 8:00 A.M., then start a shift at 8:00 A.M., then this meeting is considered contiguous work time. By default, this check box is not selected.

Schedule generation uses this setting when it assigns activities to an agent. It factors in the minimum and maximum contiguous work time constraints settings in Daily Shift Constraints.

Replaces Shift Activity of the Same Type

Select this check box if this activity should replace another activity of the same type. For example, if this is a lunch activity type, and an agent needs to take lunch exactly at 12:00 P.M., but the weekly shift definition specifies lunch anytime between 11:30 and 1:30, then the schedule generation will force the lunch activity in the 12:00 to 1:00 time slot.

If this check box is not selected and this activity type exists in the **Activities** section of the Daily Shift Constraints, then the agent will have this activity scheduled in addition to existing activities. By default, this check box is not selected.

Attendance Requirement Type

Select any of the following values:

- **Unspecified**: This is the default selection. This option does the following things:
    - It *discards* schedules that have agent activities that have been skipped (all remaining activities to be scheduled do not have a start time greater than or equal to the current time).
    - It *suppresses* schedules that end in agent activities that are both non-paid and non-contiguous.
    - It *suppresses* schedules that have unscheduled agent activities that are both paid and contiguous.
- **Do Not Schedule**: This option causes the scheduling engine to ignore this agent activity.
- **Optional**: This option causes the scheduling engine to keep schedules that meet minimum constraints and that have optional, unscheduled agent activities.
- **Include**: This option causes the scheduling engine to discard potential schedules that do not contain the scheduled agent activity.

> **Note**: If required **Include** activities occur during a paid time-off request, then the required activities are ignored. Instead, a schedule containing the time-off request is created.

Description

Enter a description of the activity. You can enter up to 2000 characters.

The description appears in a tooltip when a user moves their cursor over an activity in a schedule in Interaction Desktop. It also appears if you double-click an activity to edit it.

Related topics

Shift activities versus agent activities

Interaction Optimizer

Interaction Optimizer has add-on module in IC Business Manager that supports a wide range of workforce management functionality. Within the module, you can make configuration changes, work with schedules, and evaluate intraday differences between forecast and actual values. Use the intuitive user interface to make all the normal scheduling edits, apply time off requests, and then publish the schedule.

The new interface also allows you to see real-time adherence (RTA) events on current or previous schedules, and to use intraday monitoring to compare actual activity of the day to forecast activity of the day.

> **Note:** Beginning in CIC 4.0 SU6, most Interaction Optimizer functionality, including configuration settings, is available only through IC Business Manager.

For more information on configuring and using Interaction Optimizer, see the *Interaction Optimizer* help.

Related topics

Database Configuration

Daily Agent Availability Constraints

Agent Activity Configuration

Interaction Conference

Interaction Conference Configuration

Interaction Conference is a an application plug-in, that allows you to host scheduled conference calls for internal and external use. The Interaction Conference container appears in new and update installations if you have installed Interaction Conference and CIC detects your Interaction Conference feature license.

Use this container to configure global conference settings that apply to all conferences.

> **Note**: To configure these conference settings, the Interaction Conference administrative access right must be granted. This administrative access right is available at the default user, user, roles, and workgroup configuration levels. See Admin Access Categories in the **Admin Access** page for more information.

Enable call control for all conferences

Select this check box to add call control options (mute, disconnect, etc.) next to names of conference attendees in the Interaction Conference web application. By default, this option is not enabled.

Require account codes for all conferences

Select this check box to associate specific account codes (as defined in Account Codes Configuration) to conferences. By default, this option is not enabled.

Configure Access Type

Select the access type in the drop-down list. The type selected here determines whether conference attendees are required to supply a personal identification number (PIN) to enter the conference, and is the default access type for all conferences. PIN numbers may be required, not required, or optionally required by individual conferences. When PINs are used, conference attendees are granted a system-generated PIN number in a notification email message. The options are:

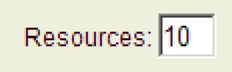
- **Require PIN**: (Default) This option sets PIN usage as a requirement, meaning that all conferences will require a PIN by default.
- **Disallow PIN**: This option sets the default for all conferences not to allow PIN usage.
- **PIN Optional**: This option sets PIN usage as optional, meaning that conferences may or may not require them. Select this option if you want the option to use PINs on a case-by-case basis. If you select this option, use the **Require a PIN for these conferences** setting in **Conference Rooms Configuration** dialog box to determine whether a conference requires a PIN.

Conference Resource Limit

This setting determines the maximum number of conference resources that Interaction Conference can use on the CIC server. This must be less than or equal to the total number of conference resources on the CIC server. To find the number of conference resources available, click on the Telephony Resources container in Interaction Administrator. In HMP environments, the number of conference resources is determined by license. You cannot leave this field blank - you must enter a positive integer. Typically, one conference resource is required for each conference invitee.

Enforce Resource Limit When Joining a Conference

When an Interaction Conference user creates a new conference, that person can optionally specify the number of conference resources to use for that conference. The default value is 10, but it can be set to any number (up to the Conference Resource Limit). Select this check box to enforce the limit set in the Resources field on the New Conference configuration page.



Resources: 10

Default notification sender address

If a conference host does not have a valid email address, Interaction Conference uses the **Default notification sender address** specified in this field to send notifications when a conference is created, updated, or deleted. This might be a CIC Administrator or a department manager's email address to use as a fallback for notifications.

Related Topics:

Conference Room Configuration

Interaction Conference

Conference Room Configuration

You must define at least one conference room before scheduling an Interaction Conference. Additional conference rooms can be defined at any time.

Use this container to configure conference rooms and associated settings.

> **Note**: To configure these conference room settings, the Interaction Conference Room administrative access right must be granted. This administrative access right is available at the default user, user, roles, and workgroup configuration levels. See Admin Access Categories in the **Admin Access** page for more information.

To create a conference room:

1. Double-click the *Configuration* entry in the Interaction Conference container. The **Conference Room Configuration** name dialog box appears.
2. Enter a descriptive name in the **Display Name** field. This is the name that appears in notification email messages sent to conference attendees, when a conference is scheduled to use this room.
3. If the General Configuration Settings allow PIN numbers to be defined, you may optionally check **Require a PIN for these conferences**. When checked, attendees must specify a personal identification number when joining a conference held in this room. Selecting this check box also allows more than one conference to occur at the same time in the room because the PINs route each caller to the correct conference.
4. Conference rooms can be physical (a room with a station phone on your premises) or virtual, meaning that the conference is associated with a telephone number. When you select **Physical**, the **Station** drop list is enabled. When you select **Virtual**, you can specify a telephone number. The telephone number associated with a conference room must be configured in your telephony hardware (in a gateway, for example) to route calls to the CIC server running Interaction Conference. Do not use a telephone number in more that one conference room.

> **Note:** To add one or more phone numbers to the Phone Numbers text box, type the number in the second text box under Phone Numbers, then click **Add**. You can remove a number by highlighting it in the list and clicking **Remove**. You can determine the order which phone numbers are used by moving a phone number up or down in the list by highlighting it in the list and clicking **Move Up** or **Move Down**.

Special Considerations for Toll-Free Numbers

Special considerations apply to the use of toll-free numbers in Interaction Conference.

- Due to the limitation of call routing in CIC, callers cannot directly reach a physical room using a toll free number. However, a physical station can call into a virtual room that is configured to be reached by a toll free number.

- Use toll free numbers with virtual rooms so guests can call directly to that conference room.

5. To limit the resources available for the room (by default, resources are unlimited up to the limit set in general configuration settings):

a. Select the **Specify Resource Limit** radio button.

b. In the corresponding text box, type the maximum number of resources to allow.

If necessary, you can select the **Disable this room** option to prevent the conference room from appearing in the list of available rooms, but without deleting the configuration.

6. Click **OK** to save changes.

Related topics

Interaction Conference Configuration

Setting Default Conference Options

Station Configuration

Interaction Conference

Interaction Conference Email Templates

Interaction Conference Email Templates

Interaction Conference allows the administrator to define email templates for meeting invitations and cancellations. Features include:

- The ability to create separate templates for invitations, updates, and cancellations.
- The ability to create separate templates (of all three types) for use by hosts and guests.

To create an email template:

1. Double-click the *Configuration* entry in the Interaction Conference container. The **Interaction Conference Configuration** dialog box appears.
2. Click the **Email Templates** tab.
3. Click **Add**. The New Template dialog box is displayed.
4. Design the template:
    a. In the **Name** text box, type a name for the template.
    b. In the **Subject** text box, type a default subject for the e-mail message (e.g., "Meeting invitation").
    c. In the **Body** text box, type the default text of the e-mail message, inserting macros (4) as needed:
    - **Additional numbers:** Phone numbers, other than the main conference number, on which attendees can call into the conference.

- **Date:** The date of the conference.
- **Host:** The host of the conference.
- **Invitee:** The name of the invitee (the recipient of the email message).
- **Invitees:** The names of the invitees (the recipients of the email message).
- **Notes:** Any explanatory notes about the conference.
- **Phone:** The main (or only) phone number that attendees should use to call into the conference.
- **PIN:** The PIN number attendees should use to gain access to the conference.
- **Room:** The room identifier for the conference.
- **Time:** The time at which the conference will be held.
- **Title:** The title of the conference.

d. Click **OK**. Interaction Administrator creates the new template and lists it on the **Email Templates** tab of the Interaction Conference Configuration dialog box.

5. In the Selected Templates area, use the list boxes to assign the template to a message type.

Related Topics

Conference Room Configuration

Setting Default Conference Options

Setting Default Conference Options

Use Interaction Conference configuration to set default options for conferences. You can also either allow conference organizers to change the options or prevent them from doing so by using the **Lock** check box.

To set default conference options:

1. Double-click the *Configuration* entry in the Interaction Conference container. The **Interaction Conference Configuration** dialog box appears.
2. Click the **Default Conference Options** tab.
3. Select the desired options:

   Lock - Select the Lock check box to prevent conference organizers from changing the setting beside the Lock check box. These options will appear in the selected state by grayed out so the conference organizer cannot change them in the Interaction Conference Web Administrator interface.

Host Required to Start - Select this check box to delay starting a conference until a host attendee has joined.

Enforce End - Select this check box to automatically terminate a conference call at the specified ending time. . If the ending is enforced, Interaction Conference automatically plays a warning message two minutes before the end of the conference.

Allow Mute - Select one of the options to determine the default audio behavior for guests joining the conference and the level of control hosts have on muting.

> **Start Muted** – Select this option to mute all guests by default. Conference guests enter the conference muted, but the conference host may unmute individual participants. Use this option if you plan to have more than 20 unmuted participants in the conference. The host can selectively unmute up to 20 participants to speak.
>
> **Manual** – Select this option to give the host manual control over muting individual guests in the conference. In this case, guests join the conference unmuted. If there are more than 20 participants, only the first 20 to join the conference are audible. The 21st participant who is a guest (and other guests after) will hear a prompt that they are joining the conference muted. If the conference host un-mutes a host or guest, and there are 20 audible participants, Interaction Conference automatically mutes an audible guest who has been unmuted the longest to stay within the 20-audible-caller limit.
>
> **Note**: This limit on 20 unmuted callers is temporary and is expected to be removed in a subsequent update.
>
> **No** – Select this option to prevent hosts from muting any guests in the conference.

Record - Select one of the options to determine the default call recording behavior for conferences.

> **Yes, send to all –** Select this option to have CIC record the conferences and send the recording to all of the hosts and guests listed on the conference.
>
> **Yes, send to hosts** – Select this option to have CIC record the conference and send the recording to all of the hosts listed on the conference.
>
> **No –** Select this option to not record conferences by default.

Announce Entry - Select one of the options to determine the default announcement behavior when a guest or host joins a conference. By default, CIC plays a tone as each person joins a conference.

> N**one** – Select this option if you do not want any audio alert or notification when someone joins a conference.
>
> **Tone** – (Default) Select this option if you want CIC to play a tone when someone joins a conference.
>
> **Name** – Select this option if you want guests and hosts to be prompted to say their name before joining the conference. Interaction Conference will then play that name for the rest of the conference participants to hear as they join.

Announce Exit - Select one of the options to determine the default behavior when a guest or host exits a conference. By default, CIC plays a tone as each person exits a conference.

N**one –** Select this option if you do not want any audio alert or notification when someone exits a conference.

Tone – (Default) Select this option if you want CIC to play a tone when someone exits a conference.

Name – Select this option if you want to hear the name of the guests and hosts as they exit the conference.

Announce Number of Attendees - Select one of the options to determine the default behavior if Interaction Conference announces (by playing a prompt) the number of attendees in the conference.

None – (Default) Select this option if you do not want CIC to play an announcement of the number of attendees on a call.

To Hosts – Select this option if you want CIC to announce the number of attendees only to the hosts on the call.

To All – Select this option if you want CIC to announce the number of attendees to all guests and hosts on the call

4. Click **OK** to save the changes.

Related topics

Interaction Conference Configuration

Interaction Conference

Interaction Analyzer

Overview of Interaction Analyzer

Interaction Administrator allows you to define the keywords that Interaction Analyzer uses to monitor conversations between agents and customers. You can assign scores to keywords to indicate their importance, and define thresholds for each keyword to indicate how certain Interaction Analyzer must be in its identification of a keyword. When a keyword is spoken in a phone conversation associated with a workgroup queue, Interaction Analyzer detects the word or phrase and identifies and marks the location in the recording where the word or phrase was spoken. CIC subsystems use this information to evaluate customer interactions.

> **Note**: For more information regarding Interaction Analyzer, see the *Interaction Analyzer Technical Reference* in the PureConnect Documentation Library.

Related topics

Keyword concepts

Manage keyword sets

Manage keywords

Keyword concepts

Keyword concepts

This section contains the following help topics:

Keyword considerations

Keyword definitions

Keyword examples

Keyword organization

Keyword considerations

This topic describes factors to consider to ensure you are monitoring the most important keywords and phrases for your contact center.

Factors to consider include:

- Purpose of your contact center
- Problems and effectiveness
- Meaningfulness of keywords
- Keywords from other areas of your business
- Agent training
- Customer Feedback
- Basic keywords

Purpose of your contact center

One factor to consider is the purpose of your contact center. What is it supposed to achieve? Your contact center may be designed for:

- Technical support/Customer support
- Sales/Lead generation
- Information services

- Complaints
- Collections
- Notifications/Dispatching
- Order taking/Event registrations
- Appointment scheduling
- Surveys/Market research
- Donations/Charities
- Screenings

With all of the possibilities, you must determine the areas on which you want to focus. Do you want to monitor agent interactions to see who is performing well and who is not? Do you want to monitor customer interactions to see what their concerns are or if they are upset? Perhaps, you want to monitor both sides of the interaction to measure many different aspects of your contact center.

Regardless of these considerations, the most important thing you can do is determine those factors upon which you define the success or failure of your contact center.

Problems and effectiveness

In your contact center, there are many factors for you to consider to determine the effectiveness of your contact center and how your business is meeting customer needs. The following list provides insight into what keyword categories you could monitor:

- **Customer satisfaction** – Are your customers happy at the end of a call? Are they going to be repeat customers? What do they think about your company, product, or service?
- **Customer problems** – What negative words are customers using in interactions? What products or services do customers mention? Do customers threaten legal action? What common problems are customers experiencing? What questions do customers most often ask?
- **Customer loss** – Do your customers mention competitors or their products? Are customers canceling accounts or stopping service? Do customers demand refunds? Do customers keep calling back?
- **Agent effectiveness** – Are your agents using positive words? Are the agents using the provided script? Do customers praise the agents who helped them? Do agents use words and phrases that indicate apathy to customer problems? Do customers ask to speak to managers or supervisors?
- **Agent satisfaction** – Are some agents getting too many difficult calls? Are agents using positive words that indicate their satisfaction? Are agents using negative words when becoming frustrated? Do customers thank agents for their help?
- **Agent training** – Are agents using personalized language when addressing customers? Do agents use the same words as their customers? Do agents know what to say to customers? Do agents know the solutions to problems? Are agents retaining customers or losing them?

What keywords are involved in the answers to these factors? What would a customer likely say in these situations? What would an agent say? Do you want to track every indication of someone using words that indicate emotion? The answers vary according to the purpose of your contact center, and in what you deem important.

Meaningfulness of keywords

When thinking of possible keywords and phrases, determine which are often-used keywords and what information the keyword provides to you.

For example, for a technical support contact center, you could track the word "problem". However, doesn't everyone who calls into that contact center have a problem? What other information does it provide? Instead, try to identify keywords that define the nature of the problem. Is there a specific problem that most customers are having? Does this problem affect customer retention or repeat business?

Careful analysis of recorded interactions and listening to live conversations helps you identify what keywords are most often said, which have the most impact to your business, and which of these differentiate normal interactions from interactions with more importance.

Keywords from other areas of your business

To leverage the most out of Interaction Analyzer for your business, consider what words or phrases are important to other departments. For example, are customers asking questions about a certain product? If so, these calls could be valuable sales leads or indicate the success of a marketing campaign.

Other business units can benefit greatly from the keywords you define. Consider asking for input from these other units and ensure valuable customer information is passed on to them. Customer satisfaction and successful sales are great. Business intelligence and customer metrics are even better.

Agent training

How well do you train your agents? Do they read from a script? Are they trained to use certain words and phrases in their interactions? Are the agents able to resolve customer problems or answer their questions? If you answer "yes" to any of these questions, you already have a set of keywords you can monitor. Monitoring the use of these keywords and phrases can indicate the success of your training methods. It also can help determine which agents need refresher training.

Customer Feedback

Determine which keywords and phrases are important to the direction of your business. Are customers asking for the same new features? Do customers complain about the same things? Are agents constantly defending the position of the company or a business practice?

Ensure you define both positive and negative keywords. Monitoring positive customer keywords enables you to track the general happiness of your customers with your contact center. Conversely, monitoring negative customer keywords helps you identify common problems and agent ineffectiveness.

Collecting this information is valuable to your business. It indicates if your business is achieving or failing to meet customer needs. This data can inform you as to where your business must go and what services, products, or solutions it offers.

Basic keywords

When you determine keyword phrases you want to monitor, think about how that phrase can be said in different ways. One of the most important aspects in creating keyword phrases is to define only those words that are always said. The following examples show how some keyword phrases can be dissected to contain only important words. The optional portions of these phrases are displayed within parentheses.

- (*They/The company/My boss*) didn't train me (*for/to/on*)
- I completely understand (*the situation/your concerns/the problem/the trouble*)
- (*Since/Because*) you are a valued (*customer/client/partner*)
- Your satisfaction is (*important/very important/our main concern/my goal*)
- Is there anything else (*I can do/I can help you with/causing you problems*)
- You're not listening (*to me/ to a word I say/at all*)

Related topics

Keyword organization

Keyword definitions

Example keywords

Interaction Analyzer keyword definitions

This topic provides descriptions of the various methods you can use to create keywords for use in Interaction Analyzer.

- Interaction Analyzer keyword entry
- Interaction Analyzer keyword spelling entries
- Keyword synonyms
- Keyword acronyms
- Keyword punctuation
- Keyword numbers
- Keyword contractions
- Keyword abbreviations
- Interaction Analyzer anti-spellings
- User-defined pronunciations

Interaction Analyzer keyword entry

You enter keywords, up to 120 characters, through the Interaction Analyzer interface of Interaction Administrator or Interaction Center Server Manager. Spell keywords as you would enter them in any document intended for communication. The speech recognition engine uses that spelling entry to match it to its usual phonetic pronunciation.

Interaction Analyzer keyword spelling entries

You can also add multiple spelling entries of a keyword, depending on the different ways in which a person pronounces a word, such as *data*. For this word, some people pronounce it as *dayta* while others pronounce it as *dahta*. The dictionary through which Interaction Analyzer compares pronunciations already handles many words with multiple pronunciations. However, if you enter terms that are specific to a specialized field, such as medicine or science, you may need to provide alternate spelling entries or user-defined pronunciations to ensure recognition by Interaction Analyzer.

Keyword synonyms

One method you must avoid regarding spelling entries is that of synonyms. For example, if you wanted a keyword of *home*, do not enter the following synonyms as alternate spelling entries:

1. House
2. Abode
3. Domicile
4. Casa
5. Hacienda
6. Chateau
7. Castle
8. Shack
9. Hut
10. Home
11. Condominium
12. Apartment
13. Dwelling

Do not enter synonyms as alternate spelling entries because Interaction Analyzer determines the spotability factor by the lowest, least discernible entry. In the previous example, the lowest, least discernible spelling entry would be "Hut." Instead, create a keyword set with the name of **home** and enter each synonym as a keyword. This method insures that each synonym keyword has a separate spotability factor and confidence threshold, and can be further discerned through more spelling entries and user-defined pronunciations.

Keyword acronyms

If you want to create a keyword that contains an acronym that is pronounced as separate letters, enter the acronym with either periods or spaces between letters.

Examples:

1. U S A
2. F.B.I.
3. I D
4. E.T.A.
5. E U
6. C.O.D.

7. H T T P

8. F.T.P.

For acronyms that are pronounceable as a word, enter the acronym as you would any other keyword without spaces or periods between letters. Letter case is not important.

Examples:

9. SCSI (scuzzy)

10. RAM

11. PIN

12. NASA

13. SCUBA

In the case of mixed pronunciation acronyms, such as DVD-ROM, you must enter the acronym so that the portion pronounced as letters contain spaces or periods between letters while the portion pronounced as a single word does not, as in the following example:

D.V.D.-ROM

Keyword punctuation

Interaction Analyzer ignores any punctuation characters in keywords. These characters include commas, periods, exclamation points, hyphens, dashes, question marks, colons, semicolons, special characters ($, %, &, (,), @), and quotation marks.

Keyword numbers

Each digit that you enter in a keyword is recognized as a word. For example, if you enter **H20**, Interaction Analyzer recognizes this keyword as "H two O." However, if you enter multiple digits, Interaction Analyzer recognizes each number separately. For example, if you enter **100**, Interaction Analyzer recognizes this keyword as "one, zero, zero", not "one-hundred." Likewise, "21" is identified as "two, one", not "twenty-one."

Keyword contractions

Interaction Analyzer recognizes contractions when you enter them as keywords. Words such as "don't," "can't," "won't," "couldn't," "it's," and "I'll" are acceptable.

Keyword abbreviations

Interaction Analyzer does not recognize abbreviations, such as Dr., Mrs., Mr., Jr., Sr., and others.

Interaction Analyzer anti-spellings

After you define keywords, you have the option of entering anti-spellings that specify similar-sounding words that you do not want mistaken for that keyword. These words could confuse Interaction Analyzer, which could mark them incorrectly as instances of that keyword; these mistakes are *false positives*.

For example, the following table presents some keywords and possible anti-spellings that you can add to the definitions:

Keyword	Anti-keywords
Lawyer	Lower Loiter Foyer Employer
Surely	Charlie Surly Purely Journey
Guarantee	Warranty Guillotine Green tea
Unfair	Conveyor Unveil Affair A fare On there

Additionally, you can also specify anti-spellings where the keyword is part of a larger word. For example, consider the word *form*. You probably would not want Interaction Analyzer to spot this word when it is a part of larger words, such as *uniform*, *formatted*, and *formation*. In this case, if Interaction Analyzer does spot the keyword within the larger words, you can enter the larger words as anti-spellings.

Do not try to determine anti-spellings when you define a keyword. Instead, when your keywords are used in real interactions in a test environment or in the contact center, you can analyze recordings, identify words mistaken as keywords, and then add them as anti-spellings to the keyword definitions.

If you eventually enter anti-spellings in a keyword definition, you can also consult numerous websites that list other rhyming words for that specific keyword.

Interaction Analyzer keyword user-defined pronunciations

When you define keywords, Interaction Analyzer also enables you to enter phonetic, user-defined spellings, which are referred to as *pronunciations*. The set of phonemes that Interaction Analyzer uses is a customized version of ARPAbet. ARPAbet was a project that used ASCII characters to define the phonemes that make up all possible sounds in the English (US) language. The Interaction Analyzer phonemes differ from ARPAbet to provide more robust keyword spotting and to support languages other than English (US).

Some languages have sequences of letters that are pronounced differently when they appear in different words. For example, in English (US), *tough*, *cough*, *dough*, *through*, and *bough* are all similar in their spellings ("ough"), but have different pronunciations. Using user-defined pronunciations enables Interaction Analyzer to identify these words correctly. For example, the following table displays how these words are specified using phonemes:

Word	Pronunciation
tough	t ah f
cough	c ao f
dough	d ow
through	th r uw
bough	b aw

> **Note:** The example words in the pervious table are common and already phonetically-defined in the Interaction Analyzer dictionary. The example words are for conceptual purposes only.

User-defined pronunciations are also useful for the different dialects that you can encounter in a language. For example, consider the English (US) word "lawyer" (l ao y er). Someone from the New England region of the United States could pronounce the word as "lahyah" (l aa y ah) while someone from the Deep South of the United States could pronounce it "lawryer" (l ao r y uh r). User-defined spellings enable you to define the keyword further so that Interaction Analyzer can correctly produce a match.

> **Important!**
>
> There are words in the medical and scientific fields that are based on Latin and Greek, but the associated pronunciations transformed over centuries of usage, such as *peritonitis*. If Interaction Analyzer has difficulty identifying the keyword based on the correct spelling, enter user-defined pronunciations to ensure proper identification of those unique keywords.

Defining multiple words in pronunciations

If you want to create a pronunciation or anti-pronunciation, which use phonemes, and it consists of multiple words, you must enter a **wd** character string between each word. This character string enables Interaction Analyzer to focus on the phonemes for each word, which provides a more accurate comparison, instead of the entire phrase.

For example, "Hi my name is" would be entered as "hh ay **wd** m ay **wd** n ey m **wd** ih s." Enter a user-defined pronunciation only for keywords that Interaction Analyzer does not recognize.

Related topics

Keyword considerations

Keyword organization

Keyword examples

Keyword examples

This topic provides example keywords and phrases you might set up for use in Interaction Analyzer to spot usage when spoken by agents, customers, or both. Use these examples to help you think about what keywords and phrases are important to your contact center or business and then build upon it.

> **Note:** These keywords are only examples and do not represent a comprehensive collection of keywords that can achieve the goals for your contact center.

Examples are provided for the following keyword categories:

- Agent greetings
- Agent training issues
- Call conclusion
- Call escalation
- Competitors
- Cursing
- First Call Resolution (FCR)
- Marketing
- Negative statements
- Positive statements
- Problem identification
- Problem resolution
- Sales
- Service improvement
- Threats
- Upset customer

The following tables contain example keywords, sorted by category and keyword set name.

Example Keyword Set Category: Agent greetings

Keyword Set Name	Keywords

(Agent) Collections Statements	• This is your final • You are obligated to • Garnish • We will send this account to collections • We are demanding full payment on this account • Forfeiture of discount • Final deadline • Offer expires • Last chance • No choice but to • Shut off • Suspended
(Agent) Opening Statements	• Hi my name is • Hello my name is • How are you today • My goal is to
(Agent) Sales Pitch	• You will be able to enjoy • You will only be charged • We have a variety of • It's a wonderful service • Won't take much of your time • For special customers like you • What can I do to get you to • All I need is your • Could I have your credit card number • What would convince you • You can't go wrong

(Agent) Survey Pitch	• What is the reason for your call today • How do you like • How would you rate • What is the most important

Example Keyword Set Category: Agent training issues

Keyword Set Name	Keywords
(Customer) Broken Trust	• You said • You told me • Wait a minute • Wait a second • Ask me that before • Asked me that before • You even listening • You listening • You're not listening • Don't know what you're doing • I don't care • Don't give me • You don't understand • Report you • I didn't get my • I did not receive
(Agent) Excuses	• I just work here • It's not my job • I'm just doing my job • I'm new here • I just started here • They didn't train me

(Agent) Improper Statements	• Calm down • Hold on • Can't do that • Lost your record • Lost your file • File is lost • Shut up
(Agent) Lack of Knowledge	• I don't know • Beats me • Let me get back to you later • Let me call you back later • I guess so

Example Keyword Set Category: Call conclusion

Keyword Set Name	Keywords
(Agent) Ending Statements	• Have a great day • Again, my name is

Example Keyword Set Category: Call escalation

Keyword Set Name	Keywords
(Customer) Redirection Requests	• Your supervisor • A supervisor • Your manager • A manager • Let me speak to • Let me talk to • I want to talk • I want to speak • Transfer me to someone who • I demand

Example Keyword Set Category: Competitors

Keyword Set Name	Keywords
Competitor Names	• *XYZ Company* • *111 Corporation* • *ABC Incorporated*
Competitor Products	• *Product Name 1* • *Product Name 2* • *Product Name 3*

Example Keyword Set Category: Cursing

Keyword Set Name	Keywords
Cursing	• Darn • Heck • Freak • Crap • Sucks • Shove it

Example Keyword Set Category: First Call Resolution (FCR)

Keyword Set Name	Keywords
(Customer) Subsequent Call	• Last time • Called before • Calling again • Calling back • Called back • Keep calling • Time I've called

Example Keyword Set Category: Marketing

Keyword Set Name	Keywords

(Agent) Ad Placement	• How did you hear about • What referred you to our • How you heard about • Did you see our
(Customer) Ad Placement	• I saw your • I heard your • I read your • On your Web site

Example Keyword Set Category: Negative statements

Keyword Set Name	Keywords
(Agent) Astonishment	• You're kidding me • Got to be kidding • That's unbelievable • You're putting me on • No way
(Agent) Condescension	• You're not the only one • How I feel • That's too bad • Aren't you just • Why are you so
(Agent) Poor Attitude	• I don't care • I don't believe you • Sucks to be you • I'd hate to be you • Tell someone who cares • I can't handle this • Out of luck • You should call back

	- That isn't my responsibility - Will tell you the same thing
(Customer) Collection Excuses	- Unemployed - Bankruptcy - I don't have a job - Lost my job - Was fired - Laid off

Example Keyword Set Category: Positive statements

Keyword Set Name	Keywords
(Agent) Action	- Right away - I will make sure - I am going to - What we can do - I will address this - The best thing I can do - What I will do for you
(Agent) Adverbs	- Definitely - Absolutely - Surely - Certainly - Quickly - Positively
(Agent) Advice	- I would suggest - I recommend - Your best option is - As soon as you receive - To avoid this problem

	• All you need to do is • The best thing you can do
(Agent) Cooperation	• Let's work on this together • We can resolve this • Let's figure out what • Let's look at this together • Let's go ahead and • Let's take care • We can fix this
(Agent) Empathy	• I see • I understand • Understand the inconvenience • I completely understand • How can I help you • I'm sorry to hear that • Sorry for the inconvenience • You are a valued
(Agent) General	• Please • Thank you • I appreciate your patience
(Agent) Reassurance	• Rest assured • I will try my best • More than glad • More than happy • Based on our experience • I will ensure that • I assure you that • Your satisfaction is • We value

	• Of course • Guarantee
(Customer) Trust	• Trust you • I can believe that • Straightforward • Honest with me • Honest with you

Example Keyword Set Category: Problem identification

Keyword Set Name	Keywords
(Customer) Account Identification	• My account number is • My number is • My user name is • My customer ID is • My account is
Product Identification	• *Product name 1* • *Product name 2* • *Product name 3*

Example Keyword Set Category: Problem resolution

Keyword Set Name	Keywords
(Agent) Resolution Indicators	• Is there anything else I can help you with • I'm glad I could help
(Customer) Resolution Indicators	• I'm happy • I'm pleased • Great • Amazing • Amazed • Excellent

	• Fantastic • Perfect • Working now • It works • Wonderful • Relieved • Terrific • Fabulous • Satisfied • Outstanding • That was easy • Very helpful • I appreciate • Thank you • Thanks • Thankful • That's better • That's much better • You deserve a • You really know • Great job • Good work • Job well done

Example Keyword Set Category: Sales

Keyword Set Name	Keywords
(Customer) Loss of Business	• Cancel my account • Canceling my account • Close my account • Cancel my service • Stop service

	• Money back • Refund • I'll never purchase • I'll never buy • Never get another • Hears about this • Better Business Bureau
(Customer) Referral	• I'll tell everyone • I'll tell my • Will love this • For my friends
(Customer) Repeat Business	• Where can I get • When can I get • When does • I'm going to order • I'll order • Get another • Next version • Next release • Next update
(Customer) Sale Success	• When will I receive • What can I expect • My credit card number is • I'll go with • Purchase • I'll buy

Example Keyword Set Category: Service improvement

Keyword Set Name	Keywords

(Customer) Suggestions	• It would be great if • What you should do is • Would be better if • Would be so much better if • Want to see • Want to hear about • Like to see • You should consider • You should make

Example Keyword Set Category: Threats

Keyword Set Name	Keywords
Legal Action	• Attorney • Lawyer • Legal action • I'll sue you • I'll sue your • Take you to court • Lawsuit
Threats	• Come down there • I'll find you • Kill you • Don't make me • I'll get you • Get even • Blow up • Revenge • Pay back • Hurt you • Where it hurts

	• Blow you away • Gun down • Shoot you • Stab you

Example Keyword Set Category: Upset customer

Keyword Set Name	Keywords
(Customer) Emotional Words	• Unacceptable • Frustrated • Unfair • Isn't fair • You people • Angry • Makes me mad • Makes me so mad • Outraged • I don't understand • Ridiculous • Upset • Ticked off • Is that the best • Unhappy
(Customer) Time Issues	• I can't wait • I don't have time • Take all day • Hours and hours • Put me on hold • Can you hurry • Waste my time • Wasting my time

	- Taking so long - Do you know what time it is

Related topics

Keyword considerations

Keyword definitions

Keyword organization

Keyword organization

This topic contains the purpose of categories, keyword set names, and keywords. The following table displays a brief example of how you can use categories and keyword set names to organize your keyword definitions:

Category	Keyword set name	Keywords
Marketing	(Agent) Ad placement	- Where did you see our ad - Where you saw our ad - How did you hear about us
	(Customer) Ad placement	- I saw your ad - I saw your commercial - I read your ad - I heard your commercial
Sales	(Agent) Sale success	

Manage keyword sets

Manage keyword sets

This section contains the following help topics:

View keyword sets

Add a keyword set

Copy a keyword set

Delete a keyword set

Search for a keyword set

Modify a keyword set

Add keyword set notes

Managing custom attributes

View keyword sets

The **View Keyword Sets** page displays keyword sets in a list in the master view, and displays details of the currently selected keyword set in the details view. You can take actions on the keyword sets in the list view, such as add, delete, and copy and paste, and you can add a new keyword set. You can change the way the list is displayed, such as change visible columns, sort by column, and filter.

To view keyword sets

1. Under Interaction Analyzer, click **Keyword Sets** or click **Interaction Analyzer** in the breadcrumbs if available.
2. The **View Keyword Sets** page appears.

Related topics

Add a keyword set

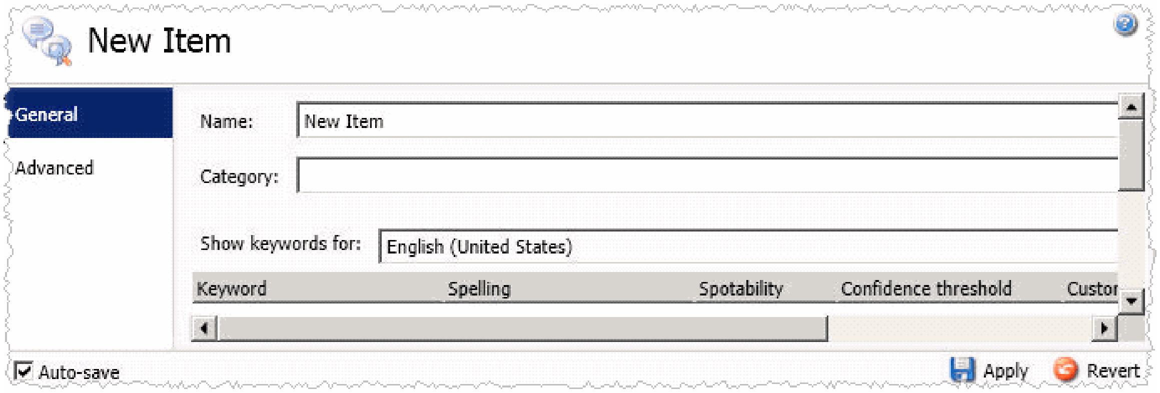
Search for a keyword set

Add a keyword set

> **Important:** It is strongly recommended to define keywords, keyword set names, and categories before attempting to enter keywords. This can save a great deal of time, as opposed to entering keywords without having a defined structure.

To add a keyword set

1. In the upper-right pane of Keyword Sets, click ✚. A **New Item** is created in the lower pane. This new item is a keyword set, which enables you to enter multiple keywords and phrases.



Name: New Item

Category:

Show keywords for: English (United States)

Keyword	Spelling	Spotability	Confidence threshold	Custor

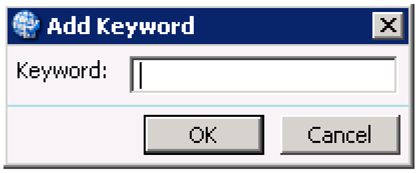
☑ Auto-save

2. In the **Name** box, type the name to assign to this keyword set.

The keyword set name must be unique from other keyword set names and be descriptive enough to enable you to identify the types of keywords it contains. This name is only for your use in locating keywords through this administrative interface. Other CIC products associated to Interaction Analyzer do not use the keyword set name.

3. In the **Category** box, type the name of the category to assign to this keyword set. See Keyword categories for more information about categories, their purpose, and how they are used.

4. On the right side of the lower pane, click ✚. The **Add Keyword** dialog box appears.



5. In the **Keyword** box, type a keyword or phrase you want Interaction Analyzer to monitor and then click **OK**. The keyword is added to the current keyword set.

6. In the lower-right corner of the lower pane, click 💾 to apply your changes.

Copy a keyword set

To copy a keyword set

1. Under Interaction Analyzer, click **Keyword Sets** or click **Interaction Analyzer** in the breadcrumbs if available.
2. In the upper pane, click the **Keyword Set** you want to copy and then click ⧉. The selected keyword set is copied to the Clipboard.

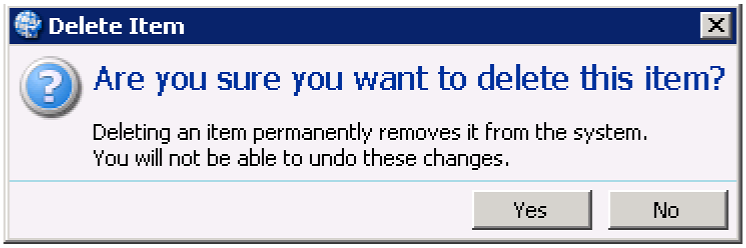
3. In the upper pane, click 📋. A **New item** is created in the lower pane that contains the information from the copied keyword set.
4. Type a new name for the keyword set in the **Name** box, make any other desired changes, and click 💾 to apply your changes.

Tip: You can undo your changes by clicking ↺ in the lower right corner of the lower pane.

Delete a keyword set

To delete a keyword set

1. Under Interaction Analyzer, click **Keyword Sets** or click **Interaction Analyzer** in the breadcrumbs if available.
2. In the upper pane, click the **Keyword Set** you want to delete and then click ✖. The Delete Item dialog box appears.


Delete Item

Are you sure you want to delete this item?

Deleting an item permanently removes it from the system.
You will not be able to undo these changes.

3. Click **Yes**. The selected keyword set is deleted.

Tip: You can undo your changes by clicking in the lower right corner of the lower pane.

Search for a keyword set

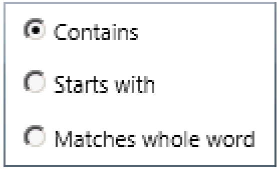
This topic contains the steps for searching for a keyword set by name or category.

The filter options for searching for a keyword set are:

- **Contains** – Searches for keyword set names that contain the characters you specify in the **Name** box.
- **Starts with** – Searches for keyword set names that start with the characters you specify in the **Name** box.
- **Matches whole word** – Searches for keyword set names that match the entire word you specify in the **Name** box.

To search for a keyword set by name

1. In the upper-right pane of Keyword Sets, click to the right of the **Name** box and select one of the filter options.

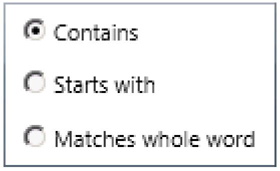

● Contains
○ Starts with
○ Matches whole word

2. Type the keyword set name to search for in the **Name** box. As you are typing characters, keyword set names that match what you are typing appear below the **Name** box.

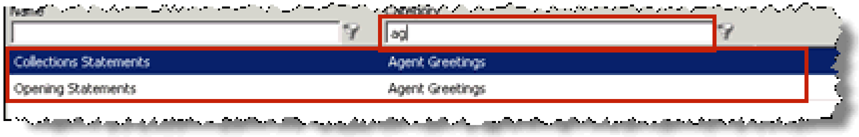
3. Click the desired **Keyword Set** to display its information in the lower pane.

To search for a keyword set by category

1. In the upper-right pane of Keyword Sets, click to the right of the **Category** box and select one of the options.


● Contains
○ Starts with
○ Matches whole word

2. Type the category to search for in the **Category** box. As you are typing characters, categories that match what you are typing appear below the **Category** box.



Category: ag

Name	Category
Collections Statements	Agent Greetings
Opening Statements	Agent Greetings

3. Click the desired **Keyword Set** to display its information in the lower pane.

Related topics

Keyword definitions

Keyword organization

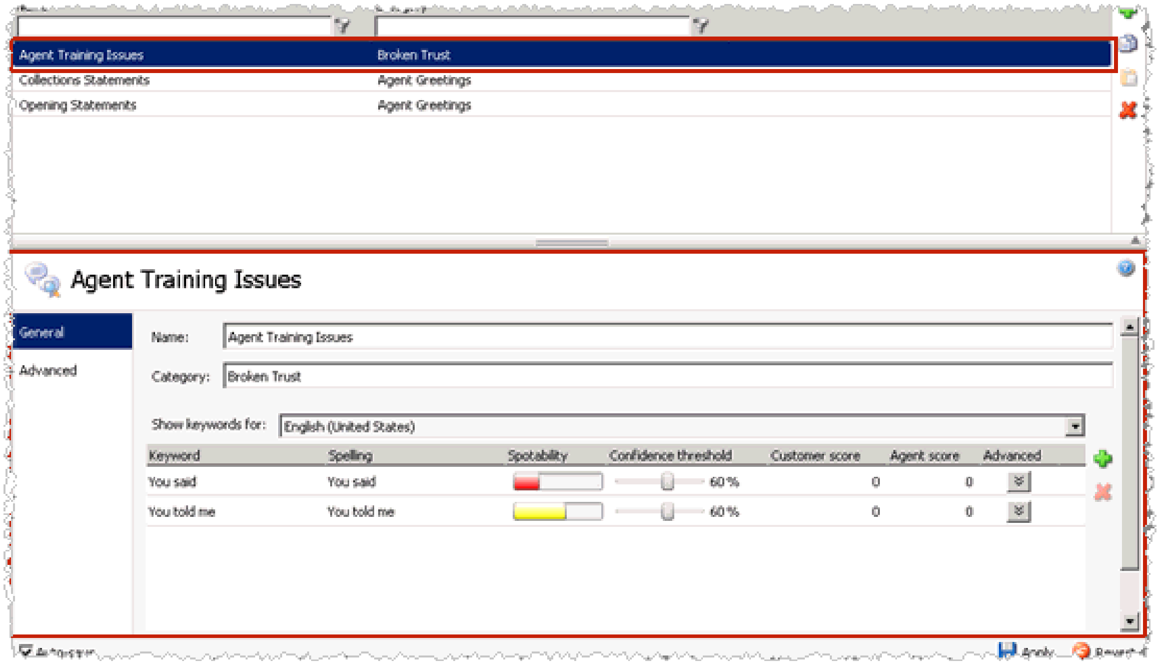
Modify a keyword set

This topic contains the steps for modifying keyword sets, keyword categories, and keywords. It also contains steps for deleting a keyword from a keyword set.

> **Important:** It is strongly recommended to define keywords, keyword set names, and categories before attempting to enter keywords. This can save a great deal of time, as opposed to entering keywords without having a defined structure.

To modify a keyword set

1. Under Interaction Analyzer, click **Keyword Sets** or click **Interaction Analyzer** in the breadcrumbs if available.
2. Click the **Keyword Set** to modify. The keyword set appears in the lower pane.



Name	Category
Agent Training Issues	Broken Trust
Collections Statements	Agent Greetings
Opening Statements	Agent Greetings

Agent Training Issues

Name: Agent Training Issues

Category: Broken Trust

Show keywords for: English (United States)

Keyword	Spelling	Spotability	Confidence threshold	Customer score	Agent score	Advanced
You said	You said	🟥	60 %	0	0	≚
You told me	You told me	🟨	60 %	0	0	≚

- To modify the keyword set name, in the **Name** box, type the name to assign to this keyword set.

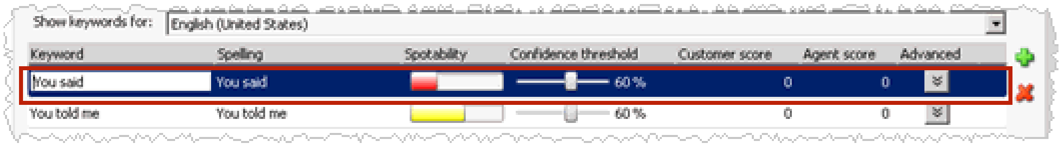
- The keyword set name must be unique from other keyword set names and be descriptive enough to enable you to identify the types of keywords it contains. This name is only for your use in locating keywords through this administrative interface. Other CIC products associated with Interaction Analyzer do not use the keyword set name.
- To modify the category, in the **Category** box, type the category name to assign to this keyword set. See *Keyword organization* for more information about categories, their purpose, and how they are used.
- To modify a keyword in this keyword set, click the **Keyword** to modify and make your changes. For more information, see Setting the Confidence Threshold for a Keyword and Set the Score for a Keyword.

3. In the lower-right corner of the lower pane, click 💾 to apply your changes.

> **Tip**: You can undo your changes by clicking ↶ in the lower right corner of the lower pane.

To delete a keyword from a keyword set

1. In the upper pane, click the **Keyword Set** that contains the keyword to delete. The selected keyword set appears in the lower pane.
2. In the lower pane, click the **Keyword** to delete and then click ✖. The selected keyword is removed from the keyword set.



Show keywords for: English (United States)

Keyword	Spelling	Spotability	Confidence threshold	Customer score	Agent score	Advanced
You said	You said		60 %	0	0	
You told me	You told me		60 %	0	0	

> **Tip**: You can undo your changes by clicking ↶ in the lower right corner of the lower pane.

Related topics

Add a keyword set

Keyword considerations

Keyword definitions

Keyword organization

Set the score for a keyword

Add keyword set notes

This topic contains the steps for adding notes about changes you make to the keyword set.

To add keyword set notes

1. In the upper-right pane of Keyword Sets, click the **Keyword Set** for which to add a note. The keyword set appears in the lower pane.

2. In the lower pane, click **Advanced** in the left navigation box. The Custom Attributes and History bars appear.

3. Click **History**. The **Notes** box appears.

4. Click in the **Notes** box and type information regarding changes you made to the keyword set.

5. In the lower-right corner of the lower pane, click 💾 to apply your changes. The last modified and created dates are automatically updated.

Tip: You can undo your changes by clicking ↺ in the lower right corner of the lower pane.

Related topics

Manage custom attributes

Modify a keyword set

Manage custom attributes

This topic contains the steps for adding, modifying, and deleting a custom attribute for a keyword set.

To access custom attributes

1. In the upper-right pane of Keyword Sets, click the **Keyword Set** for which to add, modify, or delete a custom attribute. The keyword set appears in the lower pane.

2. In the lower pane, click **Advanced** in the left navigation box. The **Custom Attributes** and **History** bars appear.

3. Click **Custom Attributes**. The Custom Attributes appear.

To add a custom attribute

1. Click ➕ to the right of the Custom Attributes box. The **Name** and **Value** boxes are available for entry.

2. Click in the **Name** box and type a unique name for the custom attribute.

3. Click in the **Value** box and type a value for the custom attribute.
4. In the lower-right corner of the lower pane, click 💾 to apply your changes.

Tip: You can undo your changes by clicking ↺ in the lower right corner of the lower pane..

To modify a custom attribute

1. Click in the **Name** box of the custom attribute to modify and type a unique name for the custom attribute.

2. Click in the **Value** box of the custom attribute to modify and type a value for the custom attribute.
3. In the lower-right corner of the lower pane, click 💾 to apply your changes.

> **Tip**: You can undo your changes by clicking ↺ in the lower right corner of the lower pane..

To delete a custom attribute

- Click the **Custom Attribute** you want to delete and then click ✖. The selected custom attribute is deleted.

> **Tip**: You can undo your changes by clicking ↺ in the lower right corner of the lower pane.

Related topics

Add keyword set notes

Modify a keyword set

Manage keywords

Manage keywords

This section contains the following help topics:

- Set the score for a keyword
- Set the confidence threshold for a keyword
- Modify advanced keyword definition settings

Set the score for a keyword

This topic contains the steps for setting the score of a keyword or phrase. It is through scoring that Interaction Supervisor displays score statistics, including the largest positive and negative scores and the cumulative score in the real-time workgroup queue view.

Scoring allows you to assign a degree of importance to the keywords and phrases you defined. For example, you want to assign a low score to keywords and phrases that indicate a customer is becoming upset. Conversely, you want to assign a high score to words and phrases that indicate a customer is responding in a positive manner. You can assign point values to keywords and phrases for both agents and customers.

You can assign to a keyword or phrase any point value from +/-1 to +/-100. Scoring is used to determine which calls need the most attention from the contact center supervisor, who monitors the workgroup queue using a few simple metrics.

> **Note**: The maximum cumulative score an Interaction can have is -99999 to 99999. Assigned point values should be within a reasonable range so the cumulative score for the entire Interaction does not exceed the maximum value.

To set scores for a keyword

1. In the upper-right pane of Keyword Sets, click the **Keyword Set** that contains the keyword for which to set a score. The keyword set appears in the lower pane.

2. In the lower pane, click the **Customer score** or **Agent score** for the keyword for which to set a score. The keyword entry is highlighted and the scoring field is available to edit.

> **Tip**: If you assign the keyword set to one channel, it is not necessary for you to set a score for both channels.

3. Assign the score by typing a number in the box or using the up and down arrows to increase or decrease the value.

4. In the lower-right corner of the lower pane, click 💾 to apply your changes.

> **Tip**: You can undo your changes by clicking ↶ in the lower right corner of the lower pane.

Related topics

Keyword considerations

Keyword definitions

Keyword organization

Set the confidence threshold for a keyword

This topic contains the steps for setting the confidence threshold for a keyword. The confidence threshold feature allows you to specify how much certainty Interaction Analyzer uses in reporting an instance of the defined keyword. See Interaction Analyzer confidence threshold for more information about this feature.

> **Important:** The confidence threshold does not affect the spotability factor of a keyword. The feature only informs Interaction Analyzer how certain it must be to report an identification during real-time analysis of the interaction.

Confidence thresholds use a percentage value to determine the amount of scrutiny that Interaction Analyzer uses. A high percentage value indicates that Interaction Analyzer reports the associated keyword if it matches perfectly. A low percentage value indicates that Interaction Analyzer reports the associated keyword if it loosely matches that keyword. The default percentage value for any newly defined keyword is 50%.

To alter the confidence threshold for a defined keyword:

1. In the upper-right pane of Keyword Sets, click the **Keyword Set** that contains the keyword for which to set the confidence threshold. The keyword set appears in the lower pane.

2. In the lower pane, click and hold the left mouse button on the slider control for the keyword for which to set the confidence threshold.

3. Move the slider control to the right to increase the confidence threshold or to the left to decrease the confidence threshold.

4. In the lower-right corner of the lower pane, click to apply your changes.

> **Tip**: You can undo your changes by clicking in the lower right corner of the lower pane.

Related topics

Keyword considerations

Keyword definitions

Keyword organization

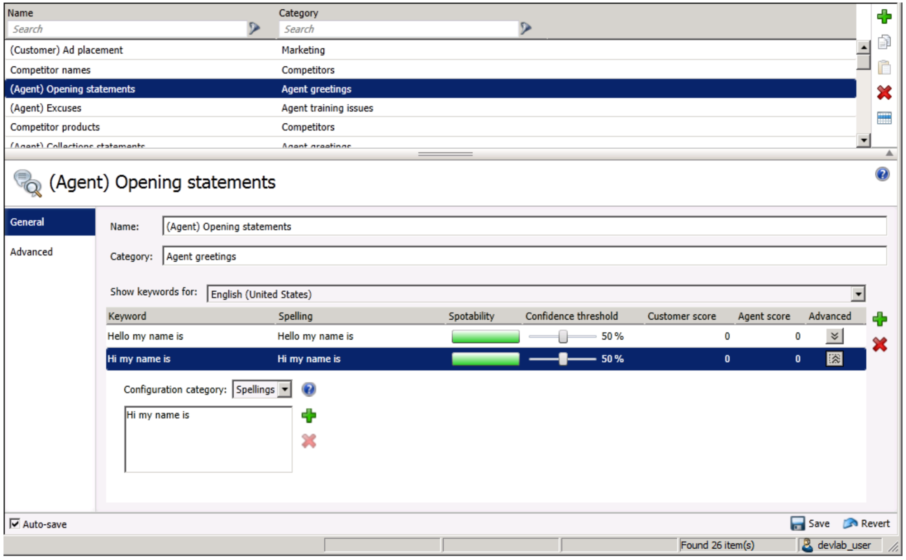
Modify advanced keyword definition settings

Once you define a keyword, you can add additional settings for that keyword, such as more accurate spellings and anti-spellings of the keyword. This topic contains the steps for setting these advanced features.

> **Important:** Do not attempt to use these advanced features unless Interaction Analyzer is having difficulty in identifying the keyword or is mistaking other words for the keyword. Only through careful analysis can you determine the additions that you must make for the keyword definition.

To modify the advanced settings for a keyword definition

1. In the upper pane of Keyword Sets, click the keyword set that contains the keyword that you want to modify.



Name	Category
Search	Search
(Customer) Ad placement	Marketing
Competitor names	Competitors
(Agent) Opening statements	Agent greetings
(Agent) Excuses	Agent training issues
Competitor products	Competitors
(Agent) Collections statements	Agent greetings

(Agent) Opening statements

General

Advanced

Name: (Agent) Opening statements

Category: Agent greetings

Show keywords for: English (United States)

Keyword	Spelling	Spotability	Confidence threshold	Customer score	Agent score	Advanced
Hello my name is	Hello my name is	🟩	50 %	0	0	≚
Hi my name is	Hi my name is	🟩	50 %	0	0	≙

Configuration category: Spellings

Hi my name is

☑ Auto-save

2. In the lower pane, select the advanced button for the keyword definition that you want to modify.
   A new set of controls is displayed below the selected keyword definition.

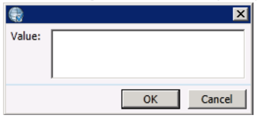
3. In the **Configuration category** list box, select the advanced feature that you want to modify:

   1.

   - **Spellings** – This feature allows you to enter an alternative spelling for the defined keyword. For example, if the keyword is "read the fine print", you could enter a new spelling of "reed the fine print" to ensure Interaction Analyzer does not identify the alternative pronunciation of "red the fine print".
   - **User-Defined Pronunciations** – This feature enables you to enter the phonetic spelling of the keyword as defined through phonemes. For more information on the ARPAbet phonemes, see the *Interaction Analyzer Technical Reference* in the PureConnect Documentation Library. When you enter a pronunciation that consists of more than one word, you must enter a **`wd`** character string between each word. For more information about defining multiple words in a pronunciation, see *the Interaction Analyzer Technical Reference* in the PureConnect Documentation Library.
   - **Anti-Spellings** – This feature enables you to enter spellings that Interaction Analyzer must not mistake for the keyword. For example, if the keyword is "lawyer," you can enter "employer" as an anti-spelling if Interaction Analyzer is mistaking that word for the keyword.
   - **User-Defined Anti-Pronunciations** – This feature enables you to enter phonemes as a series of sounds that Interaction Analyzer must not mistake for the keyword.
     For example, if the keyword is "lawyer" and an anti-spelling of "employer" has not corrected the misinterpretation of the keyword, you would enter "eh m p l oy er" in this field. For more information about phonemes, the *Interaction Analyzer Technical Reference* in the PureConnect Documentation Library.

> **Note**: For each advanced configuration item you add, the keyword count for this definition increases. For example, if you defined a keyword without any advanced configuration, Interaction Analyzer counts it as one keyword. For each spelling, user-defined pronunciation, anti-spelling, or user-defined anti-pronunciation item that you add, Interaction Analyzer increments the cost by 1.

4. To add an entry for the selected advanced feature, click the green **Add** icon to the right of these controls.
   A dialog box is displayed that enables you to enter the text for the selected advanced feature.



5. In the **Value** box, type the text that you want to add as an entry and click **OK**. The entry is added to the selected advanced feature.
6. Click **Save**.
   The advanced configuration for the selected keyword is saved.

Related topics

Keyword definitions

Keyword organization

Report Management

Report Management

Report Management allows you to create custom parameters and related report metadata. The report management help includes these help topics:

- Report Configuration
- Report Configuration Export
- Report Configuration Import
- Report System Settings

For more information about configuring reports, see the *PureConnect Reporting Technical Reference* in the PureConnect Documentation Library.

Report Configuration

Use Report Management to create custom parameters and related report metadata. The reports configured in Report Management are run in Interaction Reporter in IC Business Manager. The Report Configuration page allows you to edit and manage metadata related to a report.

Report Configuration page

The Report Configuration page has two views, the master view and the details view.

Master View

The master view displays a list of report **Categories** and the **Reports** associated with them.

You can take actions on the master view. The actions include: Adding, Editing, Copying, Deleting, and Ordering Categories and Reports in the lists.

> **Note:** In order to edit a report, you must click the lock icon to unlock the report. You can unlock reports if you have the **Interaction Report Administrator** security right. For more information, see Assign security rights.
>
> If Genesys updates the definition of a standard report, the new version will overwrite any customizations that have been made to it. Therefore, if you want to create a custom report, first copy a standard report. On the **General** details tab, change the value in the **File Name** field. Then make your customizations and save the report. Your copied report will not be overwritten by future PureConnect releases.

Details View

The details view displays specific information about the item selected in the master view, grouped by tabs.

Report Management groups the metadata information in the details view in the following tabs:

- General
- Parameters
- Flexible Columns
- Sections
- Tables
- Custom Data
- Advanced

General Tab

The General details tab contains basic information for the selected report. The detailed information for the fields on this tab is described in the following table.

General Tab	
Field	**Description**
Name	Name of the report
SubTitle	Subtitle of the report
Description	Description of the report
Friendly Key	A unique value that easily identifies the instance in the database
Assembly Name	The assembly within which the report exists
Class Name	The class name that identifies the report with the assembly
Orientation	Identifies if the report is printed in landscape or portrait
IC Data Source	The CIC data source of the report
File Name	This is the file name of a Crystal Reports report. All Crystal Reports reports must have a file name with an .RPT extension. This field is not used for Active reports.

Parameters Tab

The Parameters details tab contains metadata information for report parameters. The parameter list displays parameters for the selected report in the master view. The parameter information is defined in sub-tabs by: General, Data, Custom Data, Miscellaneous, SQL Table Columns, and the sub-tab fields are defined in the following table. You can take actions on the Parameters tab. The actions include: Adding, Editing, Deleting, and Ordering Parameters in the list.

Parameters Tab		
Sub-tab	**Field**	**Description**
General	Name	Name of the parameter
	Description	Description of the parameter
	Friendly Key	A unique value that easily identifies the instance in the database
	Assembly Name	The assembly that houses the parameter
	Class Name	The class name of the parameter within the defined assembly
	Required	Check box to select if the parameter is required to run the report
Data	Source	The source of the parameter, user supplied or fixed
	Data Type	The type of data the parameter is expecting, for example, number, date, or string
	Default Value	Default value for the parameter
	Convert Date to GMT	Check box to select if the datetime value of the parameter should be converted to GMT (does not work for reports that use stored procedures, such as Crystal Reports and Active reports)
Custom Data	Custom Data 1	A bucket field that can be used for any purpose when building your own parameters
	Custom Data 2	A bucket field that can be used for any purpose

		when building your own parameters
	Custom Data 3	A bucket field that can be used for any purpose when building your own parameters
Miscellaneous	Allow Sample	A check box to indicate if the parameter allows for a search of distinct values from the reports stored procedure that uses the stored procedure sample
	Allow Or	A check box to indicate if the parameter supports OR logic
	Allow And	A check box to indicate if the parameter supports AND logic
	Parameter Type	Drop-down box to select parameter type, Filter, Informational, or Threshold
	Visible	A check box to select if the parameter is visible within IC Business Manager
	User Control Assembly Name	The assembly that houses the parameter
	User Control Class Name	The class name of the parameter within the defined assembly
SQL Table Columns	Column Name	The name of the parameter in the Crystal template that maps to the data in the database column.
	Column Name2	An additional column name to use if the parameter references two columns in the stored procedure

> **Note:** You can configure secure report parameters to limit which data users can report on. For more information, see Configure secure report parameters.

Flexible Columns Tab

The Flexible Columns details tab contains metadata information for the selected report. The detailed information for the fields on this tab is described in the following table. You can take actions on the Flexible Columns tab. The actions include: Adding, Editing, and Deleting Flexible Columns in the list.

Flexible Columns Tab

Field	Description
Name	Name of the flexible column as used by metadata
Description	Description of the flexible column
Flexible Column Name	Name of the flexible column as shown on the report

Sections Tab

The Sections details tab contains metadata information for the selected report. The detailed information for the fields on this tab is described in the following table. You can take actions on the Sections tab. The actions include: Adding, Editing, and Deleting Sections in the list.

Sections Tab	
Field	**Description**
Name	Name of the report section
Section Visible	Check box that indicates if the report section is visible in the final report

Tables

The Tables details tab displays the where the data used to build Crystal Reports comes from. For active reports, the fields in the Tables detail tab are unavailable.

Custom Data Tab	
Field	**Description**
Table Name	Name of the database table
IC Data Source	Name of the CIC data source.

Custom Data Tab

The Custom Data details tab contains metadata information for the selected report. The detailed information for the fields on this tab is described in the following table. You can take actions on the Custom Data tab. The actions include: Adding, Editing, and Deleting Custom Data elements in the list.

Custom Data Tab	
Field	**Description**
Name	Name of the custom data
Description	Description of the custom data
Custom Data	A bucket field that can be used for any purpose when building your own report
Encrypted	A check box that indicates if the data put in the custom data field should be encrypted when saving to the database

Advanced Tab

The Advanced details tab contains metadata information for the selected report. The detailed information for the fields on this tab is described in the following table.

> **Note:** Most of the fields on this details tab are for Active reports only. They do not apply to Crystal Reports.

Advanced Tab	
Field	**Description**
Report Visible	Check box that indicates if the report is visible in IC Business Manager
Report Type	A list that displays the report type: Active Report or Crystal Report.
Stored Procedure	Stored procedure the report runs to retrieve its data
Stored Procedure Count	Stored procedure run to indicate the size of the total return of the reports stored procedure
Stored Procedure Samp	Stored procedure that returns a subset of the report's stored procedure, usually a collection of single distinct values

Linked Report Friendly Key	This value represents a Friendly Key of another report. The Linked Report Friendly Key is used to link reports, such as when a summary report might have detail links that a user can click to see all the information for a particular detail.
Allow Edit Params	A check box that indicates if the user can edit the report's parameters within IC Business Manager
Allow Count Button	A check box that indicates if the report allows for the stored_procedure_count sproc to be run in IC Business Manager
Require ACL	A check box, selected for true, indicates that the Access Control List is checked to verify that the user has permission to view the report from the report list in Interaction Reporter.
Report Timeout Period	The period of time, in seconds, before the report times out--default is 1800
Notes	User notes field

Related Topics

Report Configuration Export

Report Configuration Import

Report System Settings

Report Management

Restrict report results with secure parameters

Report Configuration Export

Use Report Configuration Export to export the report configuration metadata to an XML format file.

Select the reports to export

To export the metadata for one or more reports, expand the report category and select the reports to be exported to XML format. For example:

You can use **Select All** to select all reports to be exported. And you can use the **De-Select All** to clear your selections and select again.

Specify the destination folder

Next, specify the destination folder and file name, and export the file.

1. In the **Export File Destination** field, click **Browse**.
2. In the **Save As** dialog, navigate to the destination folder.

3. In the **File Name** field, name your export file. The default file name is `ReportConfiguration.xml`
4. Click **Save**. The full path name is displayed in the Export File Destination field.
5. Click **Export**. The **Export Completed** confirmation message is displayed.

Related Topics

Report Configuration

Report Configuration Import

Report System Settings

Report Management

Report Configuration Import

Use Report Configuration Import to import the report configuration metadata from a previously exported XML format file.

> **Note:** Only supported data types, as listed in the following section, are accepted by the report configuration import feature. If an unknown data type occurs in imported data, an error message appears and the details of the error are logged to the Interaction Administrator log.

Supported data types

The following table lists each supported data type and its corresponding numeric value as it is stored in the data_type column of the RPT_Parameters table.

Data type	Numeric value
None	0
Boolean	1
Date	2
ICWorkflowName	3
Number	4

String	5
Time	6
User	7
DistributionQueue	8
Role	9
Guid	10
Duration	11
CrystalString	12

Import an exported file

To import the metadata from an exported file, follow these steps.

1. In the **Select File** field click **Browse**.
2. In the **Open** dialog, navigate to the saved exported XML file.
3. Select the file to be imported, and click **Open**. The report **Categories/Reports** are displayed in the list.
4. Click **Accept Import**. The **Import Complete** confirmation message is displayed.

Related Topics

Report Configuration

Report Configuration Export

Report System Settings

Report Management

Report System Settings

Use Report System Settings to update reporting system settings, to configure the value for the first day of your work week and set the value for report timeout.

Update Report System Settings

To set the values for report system settings, follow these steps.

1. To set the first day of the week, in the **First Day of Week** drop-down list, select the day to begin your week.
2. To set the report timeout period, use the up and down arrows and select the timeout period in seconds.
3. Click **Save** to save your selections, or click **Revert** to cancel your changes.

Related Topics

Report Configuration

Report Configuration Export

Report Configuration Import

Report Management

Configure secure report parameters

You can configure report parameters that limit which data users see based on the ACLs to which they have access. Secure report parameters are available for all Crystal Reports that use queue parameters.

Example

Suppose your call center managers want to monitor how workgroups are handling their queues. The Queue Detail Report shows this information, but because it indicates employee performance, you want to limit access to it. To ensure that only the users who should see the report can see the sensitive information, you can configure the report to use secure report parameters. You then assign the user queue ACL to only those users who should see the report results. When a user attempts to run the report in IC Business Manager, the user can select only the workgroups that they have access to.

Secure and unsecure parameter classes

To configure a Crystal Reports report that uses queue parameters, you must indicate a parameter class name.

For each secure parameter class name, there is a corresponding unsecure parameter name.

- If you choose a secure parameter class name, then the user is presented with a list of valid parameter choices based on their access level.
- If you choose an unsecure parameter class name, then a user type any value for the parameter when the user runs the report. This potentially allows the user to report on sensitive information, or to run reports using invalid (non-existent) parameter values.

The following table displays the secure parameter classes and their corresponding unsecure parameter classes

Secure Parameter Class Name	Unsecure Parameter Class Name
SecuredAutoCompleteUsersComboBox	AutoCompleteUsersComboBox

SecuredDistributionQueueComboBox	DistribututionQueueComboBox
SecuredUserList	UsersList

For more information on the SecuredUserList parameter, see Configure the visibility of user data in reports

Parameter class and control class

For each secure parameter, you must specify both the parameter class name and the control class.

- The parameter class name indicates that the parameter is secure.
- The control class name indicates which type of field the user sees in IC Business Manager.

The following are the secure parameter class names:

- ININ.Reporting.Historical.Engine.Module.Parameters.ViewModels.SecuredAutoCompleteUsersComboBox
- ININ.Reporting.Historical.Engine.Module.Parameters.ViewModels.SecuredDistributionQueueComboBox
- ININ.Reporting.Historical.Engine.Module.Parameters.ViewModels.SecuredUserList

The following are the control class names that work with secure parameters

- AutoCompleteComboBox

A note about migrating from an earlier version

> **Note:** Secure report parameters are available in CIC 2016 R3 and later releases. If you configured Crystal Reports that use queue parameters for an earlier version of CIC, you must edit those reports to use either the secure or unsecure parameters.

Configure the Queue Detail Report to limit which workgroups a user can report on

This section shows the configuration steps in order to limit which workgroups a user can report on. You can substitute other secure report parameters, reports, and ACLs as necessary.

Configure the report

1. **Report Management > Report Configuration > Categories > Queue Reports**
2. Select the **Queue Detail Report.** This report takes a workgroup as a parameter.
3. On the Parameters tab, click **Workgroup**.
4. On the General tab, in the **Class Name** box, type ININ.Reporting.Historical.Engine.Module.Parameters.ViewModels.SecuredDistributionQueueComboBox.

5. On the Miscellaneous tab, in the **User Control Class Name** box, type ININ.Reporting.Historical.Engine.Module.Parameters.Views.AutoCompleteComboBox.
6. Click **Save**.

Configure the user

1. **Users > User Configuration > Security > Access Control**
2. In the **Search** box, type workgroup queue.
3. Under the **Search** column, select the workgroups on which the user can report.
4. Click **Close**.

Configure the User Call Detail Report to limit which users and workgroups a user can report on

Configure the report

1. **Report Management > Report Configuration > Categories > User Reports**
2. Select the **User Call Detail Report.** This report takes a workgroup as a parameter.
3. On the Parameters tab, click **User**.
4. On the General tab, in the **Class Name** box, type ININ.Reporting.Historical.Engine.Module.Parameters.ViewModels.SecuredAutoCompleteUsersComboBox.
5. On the Miscellaneous tab, in the **User Control Class Name** box, type ININ.Reporting.Historical.Engine.Module.Parameters.Views.AutoCompleteComboBox.
6. Click **Save**.

Configure the user

1. **Users > User Configuration > Security > Access Control**
2. In the **Search** box, type user queue.
3. Under the **Search** column, select the users and workgroups on which the user can report.
4. Click **Close**.

Related topics

Report Configuration

Configure the visibility of user data in reports

Glossary

ACD term

Automatic Communication Distribution is a system that routes interactions based on agent availability, caller input, agent skill levels, volume of interactions, time of day, agent groups, trunk line, or other variables. Several subroutines provided with the CIC clients offer ACD functionality.

> For more information on ACD processing, see *the white paper ACD Processing: CIC's Automatic Communication Distribution* and the *ACD Processing Technical Reference* in the PureConnect Documentation Library on the CIC server.

DND

Abbreviation for Do Not Disturb. In status messages, the DND attribute tells the Interaction Processor to play one of the "unavailable" audio messages and not send calls to this station. A "non-DND" status indicates the user is available to take calls or is, at least, in the office.

CIC Port Number

CIC's registered port number for TCP/IP communications is **2633** with the string **interintelli**. System administrators may need to know this number to allow external users access to the CIC if a firewall exists between the remote user and the CIC server.

CIC Registry Entries

Interaction Designer provides a tool palette called System tools. These tools, such as GetDSAttr, Lookup, etc., enable advanced users to access CIC configuration information stored in registry entries on the server.

> **Caution**
>
> As an advanced technical support administrator or VAR, you may need to verify CIC's registry entries on the CIC server or workstations running a CIC client. This should be done with extreme care and only under direction from an authorized PureConnect Customer Care technical support representative since any modifications to these entries can render the system inoperable.

CIC Server Registry Entries

Start the registry editor on a CIC server. The CIC registry entries, created primarily by the Interaction Administrator and the CIC installation program, are stored in the following tree structure:

HKEY_LOCAL_MACHINE --> SOFTWARE --> Interactive Intelligence

CIC Client Registry Entries

Start the registry editor on a workstation running a CIC client. Interaction Client registry entries are stored in the following tree structure:

HKEY_USERS--> Default --> Interactive Intelligence

Immediate Mode

A T 1 channel using immediate response requires the called party to be ready to receive call identification data immediately when an incoming call arrives from the central phone office (CO). For outgoing calls, the caller sends the phone number expecting the CO to immediately receive the call without waiting for an acknowledgment signal (wink) from the CO.

Initialization Function

Initialization functions are functions that perform some system initialization when the CIC system starts. These functions are contained in DLLs that must be registered on the CIC server in Interaction Administrator. Multiple initialization functions can be called during system initialization.

Wink Mode

A wink is a very brief signal sent by CIC to the phone company after it detects an incoming call. This signal is part of an optional digital handshake protocol. After CIC initiates an outgoing call, the phone company sends a wink signal back to CIC to verify the connection. Use of the wink signal depends on the T1 service and implementation provided by the phone company.

Diagnosing Problems

Solving problems

If you experience problems on the IC server, use the Windows Event Viewer to look for an explanation of these problems. For example, if an error occurs on a T-1 trunk or line, the CIC Telephony Services module writes a message to the Windows 2008 event log as a Telephony Services event.

All software and hardware systems register errors in the Windows 2008 Event Log. If CIC modules are running on different Windows 2008 servers, the server running the IC AdminServerU.exe is the primary repository of CIC events. If AdminServerU.exe is not available, distributed CIC modules will log events to the local Windows 2008 event log.

To view the Windows 2008 event log:

1. From the Start menu, select Programs, Administrative Tools (Common), and Event Viewer.
2. In the navigation pane, expand Windows Logs, and select Application to display CIC event sources.
3. Once the Events are displayed, double-click on an event entry in the log to display the Event Detail dialog box. This dialog box contains detailed information about the event.

> **Note:** Detailed event information might be requested by a PureConnect Customer Care representative. For more information on Event Viewer, see the Event Viewer help.

Restarting the Server

If your CIC server experiences a problem that requires restarting the server, we recommend a complete power cycle of the server.

If PureConnect Customer Care staff ask you to turn on tracing for a particular subsystem, see Using LogSnipper for more details.

IC subsystem Logs and the LogSnipper application

Each IC subsystem keeps a log of its actions in the \\IC\Logs\[date] directory where date represents the log date. For example, the TsServerU subsystem's activities on December 10, 2018 are logged in \\IC\Logs\2018-12-10\TsServer.ininlog. Each subsystem logs a basic level of detail that can be increased with the Trace Configuration utility. If tracing is set to a verbose mode or if many actions are logged, the log files can grow to be very large and difficult to open with standard text file editors (such as Notepad).

LogSnipper is an application that extracts a portion of an IC subsystem trace log and saves it to a file. It is useful when you troubleshoot a specific time period within a large trace log.

If PureConnect Customer Care asks you to extract a portion of a trace log, you will need to use LogSnipper. For complete up-to-date information, see the white paper Using LogSnipper located on your PureConnect Documentation Library on the CIC server.

Troubleshooting ICELib-based Containers

Some configuration containers in Interaction Administrator are ICELib-based and therefore connect to Session Manager instead of Notifier. For these containers, it's best to use the Session Manager log to find a resolution:

People Containers

- AccountCodesConfiguration
- AccountCodes
- ClientTemplates
- ResponseManagement
- Skills
- ACGs
- Wrapup Categories
- Wrapup Codes

Analyzer Containers

- KeywordSets

System Configuration Containers

- ProblemReporter
- Layouts

Integrations Containers

- Salesforce Configuration

Errors with other containers may indicate that Interaction Administrator is having trouble parsing information.

Revisions

CIC 2018 R4

Widgets

Widgets are streamlined and lightweight elements you can add to your company’s website to support activities like chatting with an agent. Two new rights control access to widget configuration in

Interaction Connect. the **Widgets Configuration** Administrator Access right enables a user to display the Widgets view in Interaction Connect. The **Widget Configuration Master** Security right enables a user to create widgets and configure every widget property. For more information, see Widgets in the Interaction Connect help.

Social Media

PureConnect now supports incoming Facebook and Twitter messages and direct message as interactions. The following social media options are new in Interaction Administrator:

- ACD Social Media license. Users with this option enabled are eligible to receive routed social media interactions. For more information, see
- Workgroup Queue Service Level configuration for social conversations and direct messages.
- Interaction Tracker items tracked now include social conversations and direct messages.

For more information, see the PureConnect Social Media Technical Reference.

CIC 2018 R2

PureConnect data privacy feature

Customers can prevent potentially sensitive data from appearing in trace logs. The PureConnect data privacy feature can suppress the trace logging of data that might be sensitive. This feature is enabled by setting server parameters. See Server parameters to suppress logging of sensitive data in this document. For background information, see PureConnect data privacy feature, in Chapter 6 of the Security Precautions Technical Reference. To access the technical reference, you must login to the Genesys Product Information website.

Optional server parameter to switch ITTS models

Starting with CIC 2018 R2, Interaction Text to Speech (ITTS) supports enhanced models, providing more natural sounding voices for a better caller experience. These models, trained with Deep Neural Networks, are used by default. To opt out and use GMM models instead, add the EnableEnhancedTTS server parameter and set its value False. No action is required to use the new DNN models. For details, see EnableEnhancedTTS in the Optional General Server Parameters topic.

Option to automatically sort the Workgroup Overview in IC Business Manager

To enhance performance, IC Business Manager no longer sorts the Workgroup Overview. To automatically sort that view, add the AutoSortWorkgroupOverview server parameter, and set its value true. See AutoSortWorkgroupOverview in the Optional General Server Parameters topic.