PureConnect®

2023 R3

Generated:

09-November-2023

Content last updated:

17-June-2019

See Change Log for summary of changes.

GENESYS™

Status Aggregator

Technical Reference

Abstract

This technical reference shows how to install and configure Status Aggregator.

For the latest version of this document, see the PureConnect Documentation Library at: http://help.genesys.com/pureconnect.

Table of Contents

Introduction to Status Aggregator

The *Status Aggregator Technical Reference* is for system administrators and others who want to:

- Understand the purpose, concepts, and architecture of the Status Aggregator.
- Install and configure Status Aggregator on the Status Aggregator server.
- Configure Interaction Administrator to work with Status Aggregator.
- Import Status Aggregator security certificates into each CIC server.
- Learn how to configure CIC clients to work with Status Aggregator.

CIC clients

Customer Interaction Center (CIC) supports two interaction management client applications. "CIC client" refers to either Interaction Connect or Interaction Desktop.

What is a status?

Status Aggregator consolidates status information about CIC users. That information has three components:

Status key

This key is a string value (Figure 1, a) that can be mapped to various attributes (b) specified in Interaction Administrator. It can correspond to a persistent status value (such as "Gone Home" or "On Vacation") or a non-persistent value (such as "Follow Up"). Persistent values are expected to survive across a server restart or user logout; non-persistent values are not. The status key may be accompanied by per-instance data, such as "Until" data indicating when the user expects to exit the status or a status detail string that can be displayed along with the user's status.

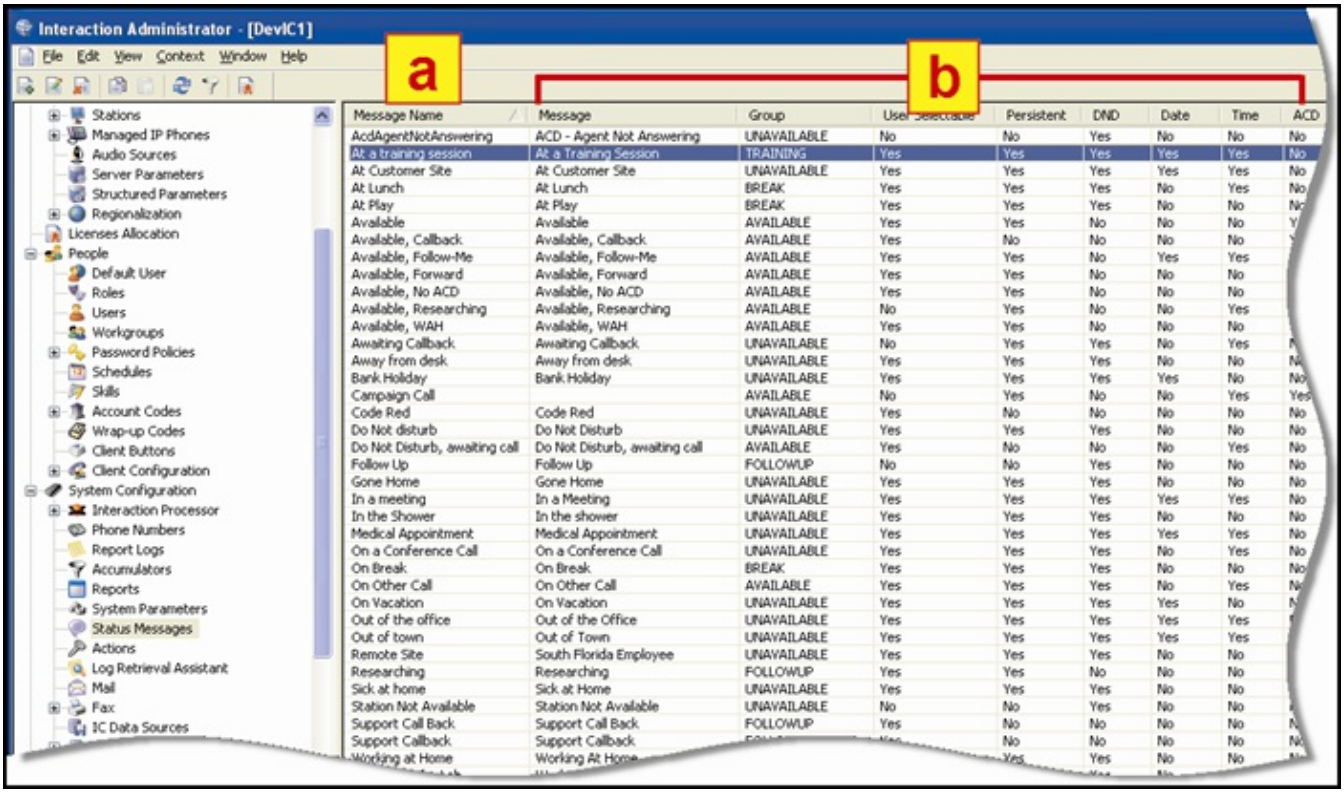
"On Phone" indication

The "On Phone" indication is a Boolean value, which indicates whether the user has any active interactions on his or her user queue. If the user is logged into a station, this also includes interactions on his or her station queue.

CIC logon indication

The CIC logon indicator is a string value. If empty, it indicates that the user is not currently logged in to a CIC server. If non-empty, it specifies the name of the CIC server where the user resides.

These status values are displayed in various user-side displays and are also used by various CIC subsystems (such as AcdServer). They are also used to implement the "Camp" feature that starts a call when a camped-on user changes his/her status.



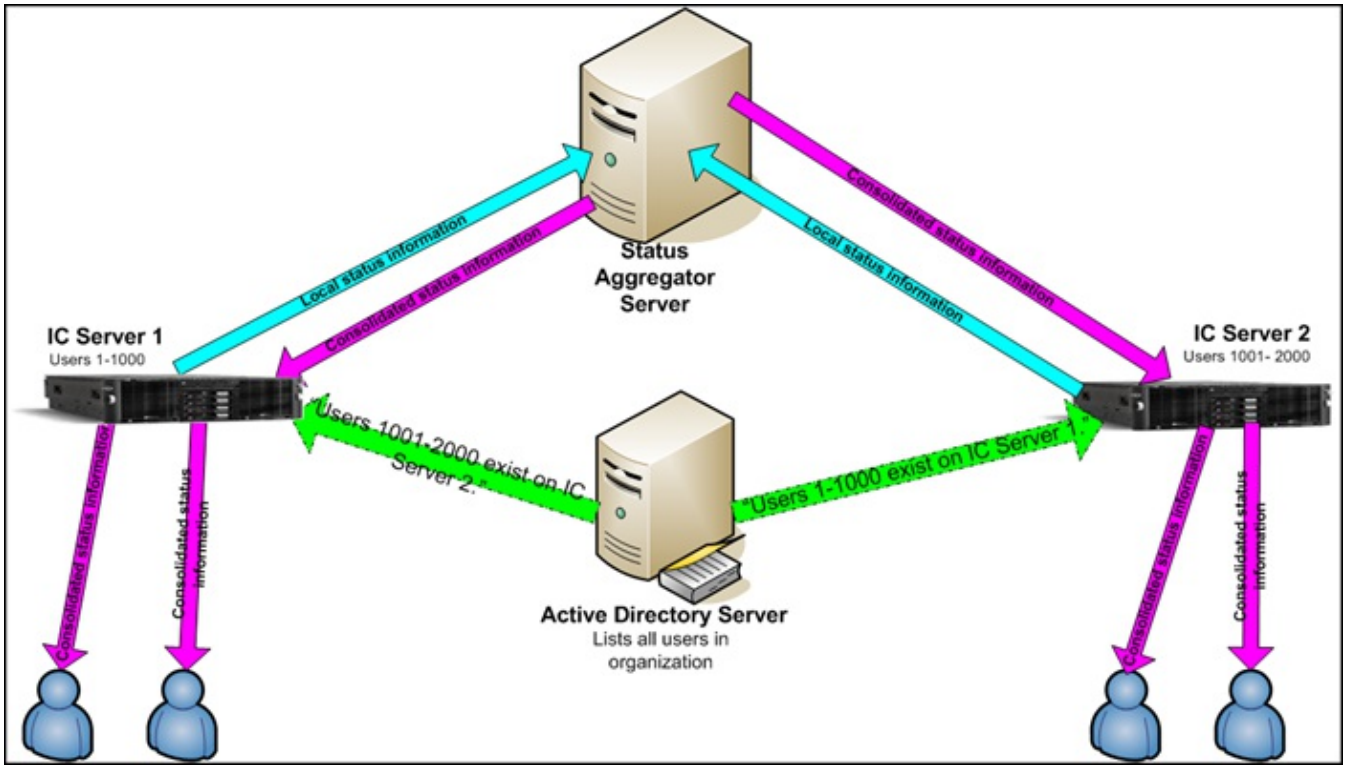
What is Status Aggregator?

Status Aggregator is a software subsystem that works with Customer Interaction Center. Status Aggregator allows users of the CIC clients to see the status not only of people in their own offices, but also in any remote office whose Customer Interaction Center server shares information with the Status Aggregator server.

Status Aggregator is intended for large organizations that have too many users to host on a single CIC server. Such organizations often have multiple sites and want to monitor employee or user status regardless of location. Status Aggregator makes users' status visible to all CIC servers that are connected to the Status Aggregator server.

What Status Aggregator does

Status Aggregator runs on a dedicated server. It consolidates status information about users residing on multiple CIC servers, whether in the same or in geographically separate offices. In turn, the Status Aggregator server makes this consolidated information available to all of the CIC servers.



Consolidated information flows from Status Aggregator to CIC servers to users.

The diagram shows a simplified example. In the diagram, each CIC server knows about its own users. CIC server 1, for example, knows about users 1–1,000. From the Active Directory server, CIC server 1 learns that users 1,001–2,000 are on some other CIC server, but does not have status information about those users. CIC server 1 can then go to the Status Aggregator server to obtain status information about those users if it is available. Users of CIC server 1 can then view status information about users who are logged in to CIC server 2.

Using a separate, dedicated Status Aggregator server solves the scalability problem that occurs when an organization has too many users to host on a single CIC server. When an organization wants to consolidate information about users from multiple CIC servers, the Status Aggregator server can scale up to the load and provide status information in real time.

Status Aggregator can work on a single Status Aggregator server or on multiple Status Aggregator servers to provide mirroring and fault tolerance. A single Status Aggregator server (or a single Status Aggregator server with a mirror server to provide nonstop operation if there is a problem) can:

- Efficiently handle up to five CIC servers.
- Efficiently handle up to 50,000 CIC users.

How Status Aggregator works

The Status Aggregator server:

- Receives notifications of user status changes and caches them.
- Receives queries for status values from client CIC servers.
- Receives and manages requests to monitor for changes in the status of specific users.

The server does not try to map from one status type to another and does not proactively request status values from other CIC servers. It is by design a passive subsystem.

CIC servers receive status information from the Status Aggregator server.

> **Note:** In order for Status Aggregator to include status information about a user, that user must have an associated email account matching his or her LDAP (or other data source) email account.

How Status Aggregator differs from Multi-site

The features of Status Aggregator overlap somewhat with CIC Multi-site, an optional software module that links together two or more CIC contact centers. However, the two products serve different purposes and are appropriate in different situations:

- Status Aggregator is designed to provide status information, while Multi-site is designed to provide user mobility.
- Status Aggregator consolidates status information from users on different CIC servers, while Multi-site links together CIC servers that all have the same set of users.

The following table compares the features of Status Aggregator to those of Multi-site.

Feature	Status Aggregator	Multi-site
Organization-wide directory	Yes	Yes
Universal user extensions (users keep their usual telephone extensions when in remote offices)	No	Yes
Real-time status	Yes	Yes
Scalable. Each Status Aggregator server efficiently handles status information for over 50,000 users and over five CIC servers.	Yes	No
Allows change of status	No	Yes
Server	Status Aggregator server. Must be on stand-alone server.	RTM server. For 200 or fewer users, can be on any CIC server. For more than 200 users, must be on stand-alone server.
Architecture	SA Server + SA clients. Each Status Aggregator server gets information from all connected IC Servers.	RTM server + CIC clients. Each RTM server gets information from the CIC servers that are in its collective. Each CIC server must include the EMSServer subsystem.
Fault tolerance	Two or more Status Aggregator servers can be "fail-over" backups for each other.	No fail-over backup between multiple RTM servers.

For more information about Multi-Site, see *CIC Multi-Site Technical Reference* at https://help.genesys.com/cic/mergedProjects/wh_tr/desktop/multi_site_technical_reference.htm.

How Status Aggregator works with different CIC editions

Status Aggregator must be at the same version level as your CIC server.

How Status Aggregator uses security certificates

Status Aggregator uses security certificates to verify the identities of the Status Aggregator and CIC servers with which it exchanges status data. Using security certificates prevents unauthorized systems or individuals from intercepting or modifying the exchanged status data.

For more information about how Status Aggregator uses certificates, see Generate SSL Security Certificates and 3: Import Certificates Into Each CIC Server in this document. For background information about security and certificates, see the *PureConnect Security Features Technical Reference* at https://help.genesys.com/cic/mergedProjects/wh_tr/desktop/security_features.htm.

Install and Configure Status Aggregator

For information about installing and configuring Status Aggregator, see the following:

Installation Pre-Requisites and System Requirements

Installing Status Aggregator requires the following:

- Customer Interaction Center 2015 R1 or later
- Microsoft Active Directory (any version compatible with Interaction Administrator)
- An account (such as local administrator) with permissions to install and run a service.
- A dedicated server for Status Aggregator. System requirements are the same as for a CIC server. For more information, see: https://my.inin.com/products/cic/Pages/Software-Requirements.aspx
- Security permissions to read Active Directory data. In particular, the CIC data source configured in Interaction Administrator must use an account that has read access to the Active Directory server.
- Two-way read access between the Status Aggregator and the CIC servers.
- Files for the AdminGenSSLCerts utility program. Contact Customer Care to obtain this utility. On each CIC server that connects to Status Aggregator, copy the AdminGenSSLCerts utility files to the `\I3\IC\Server` folder.

For installation instructions, see Install Status Aggregator.

Install Status Aggregator

Note: If you want to store log files in a folder other than the default (`\Windows\temp\inin_tracing`), create the folder before you begin installing Status Aggregator.

The Status Aggregator install is available to install from the CIC `.iso` file. For information about requirements, see Installation Pre-Requisites and System Requirements.

To install Status Aggregator:

1. If you have not done so already:
   a. Download the CIC 2015 R1 or later `.iso` file from the PureConnect Product Information site at https://my.inin.com/products/Pages/Downloads.aspx.
   b. Copy the `.iso` file to a file server (non-CIC server) with a high-bandwidth connection to the server(s) on which you will be running the CIC 2015 R1 or later installs.
   c. Mount the `.iso` file and share the contents to make them accessible to the server(s) on which you will be running the CIC 2015 R1 or later installs.
2. Navigate to the `\Installs\Off-ServerComponents` directory on the file server.
3. Copy the Status Aggregator `.msi` file, for example, `StatusAggregator_2015_R1.msi` to the server on which you plan to run this install and double-click to launch it.
4. In the **Welcome** window, click **Next**.
   The program displays the **Custom Setup** dialog box.
5. In the **Custom Setup** dialog box:
   - The Feature Selector icon lets you choose which features of a program to install. For Status Aggregator, ignore this icon because you need to install all the features of the program.
   - The **Reset** button lets you reset the dialog box's values to their default values.
   - The **Disk Usage** button lets you see how much disk space you have free on the drive where you will install Status Aggregator.
6. Click **Next**.
   The program displays the **Domain User Validation** dialog box.
   In this dialog box, the setup wizard typically fills in the **User** and **Domain** text boxes with your Windows login information. Usually, you only need to fill in your password.
7. In the **Domain User Validation** dialog box, type any required information in the text boxes, then click **Next**.
   The program displays the **Status Aggregator Servers** dialog box.
8. Click **Next**.
   The program displays the **Ready to Install Status Aggregator** dialog box.
9. Click **Install**.

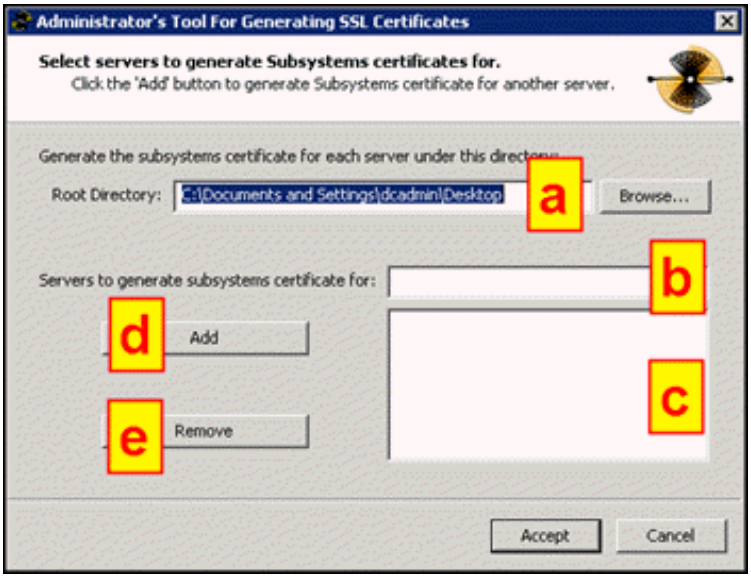
The program displays a progress bar while it installs Status Aggregator. When installation is complete, it displays the **Completed** message.

By default, the PureConnect QoS driver will be silently installed and the certificate will be added to the **Trusted Publishers** list. If your site has reasons to modify this default behavior, see KB article Q131006915300479 and follow the instructions provided to modify the QoS properties and run the install using Group Policy or other methods.

Generate SSL Security Certificates

After you click the **Finish** button in the final **Status Aggregator Setup Wizard** dialog box, the installation program displays the **Administrator's Tool for Generating SSL Certificates** dialog box. For installation instructions, see Install Status Aggregator.

Note: For the steps to generate certificates manually by using the GenSSLCertsU command-line utility, see "Generating Certificates Manually with GenSSLCertsU" in the *PureConnect Security Features Technical Reference* at https://help.genesys.com/cic/mergedProjects/wh_tr/desktop/security_features.htm.



In this dialog box, you specify the folder where you want to store your SSL security certificates. You then create a list of servers for which the program will generate SSL certificates. Use these controls:

(a) **Root Directory** box

Here, you enter the path of the folder where the program should store your SSL certificates for all the servers. Under this folder, the program creates a separate subfolder for each server in your list (c).

(b) **Servers To Generate Subsystems Certificate For** box

Here, you type the name of a server for which you want to generate SSL certificates.

(c) **Server list** box

Lists all the servers for which it will generate certificates.

(d) **Add** button

Clicking this button adds the server name in (b) to the list in (c).

(e) **Remove** button

If you have clicked a server name in box (c) to select it, clicking this button removes that server name from the server list.

To generate SSL security certificates

1. Click the **Browse** button (a) and browse to the folder where you want to store certificates.
2. In the **Servers** box (b), type the name of a server for which to generate certificates.
3. Click the **Add** button (d).
   The program adds the server name in (b) to the server list in (c).
4. Repeat steps 2 and 3 for each server that requires SSL certificates.
5. Click the **Accept** button.
   The program opens a command window and shows its progress as it creates a subfolder for the first server in the server list and puts certificates in the subfolder. Then, it displays a message telling you to move the subfolder to that server.
6. Click **OK** in the message.
   The program displays a command window and message for each server in the list.
7. Copy all the subfolders under the SSL certificates folder, which you entered in the **Root Directory** box, onto a USB key drive.

Later, you will import the certificates onto the CIC server in 3: Import Certificates Into Each CIC Server.

Overview of Configuring Status Aggregator

Configuring Status Aggregator has four major steps:

- 1: Configure Status Aggregator Data Sources
- 2: Configure Status Aggregator Contact List Sources
- 3: Import Certificates Into Each CIC Server
- 4: Set Parameters for the Status Aggregator Server

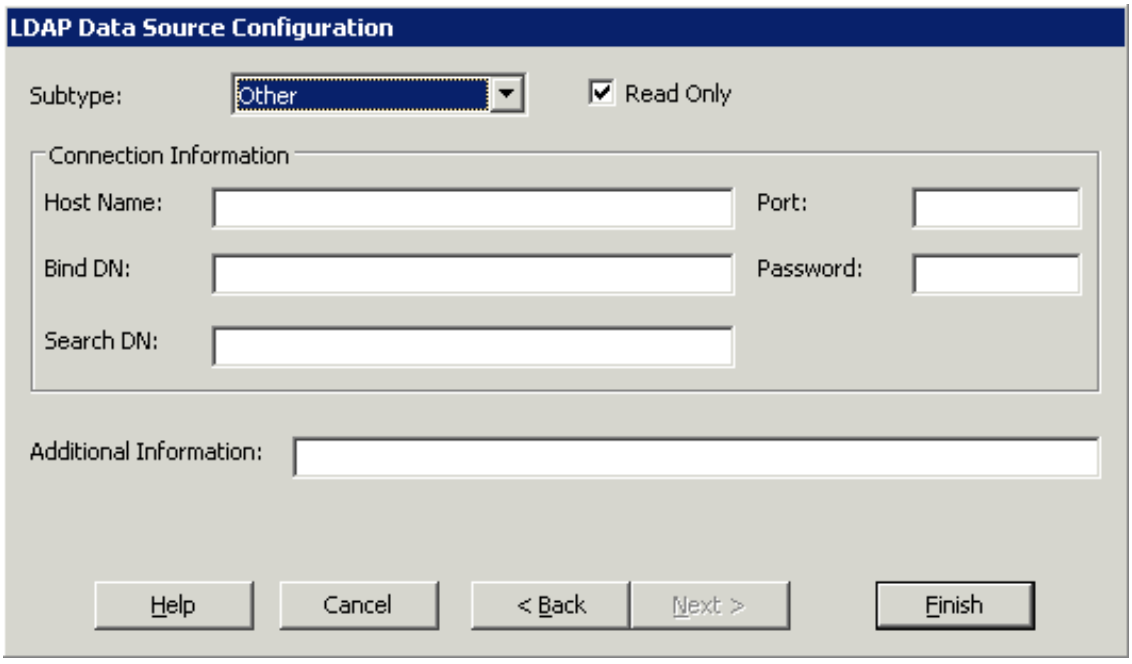
1: Configure Status Aggregator Data Sources

The first major step is to configure the Status Aggregator data source in Interaction Administrator on each CIC server. In a multi-CIC server environment, each CIC server should have a data source configuration pointing to the same source. The most common data source is a Lightweight Directory Access Protocol (LDAP) server, but it can be some other data source. This section shows how to configure Status Aggregator for an LDAP data source.

For information about other steps in the process, see Overview of Configuring Status Aggregator.

To configure Status Aggregator data sources in Interaction Administrator:

1. If needed, start Interaction Administrator.
2. Add a new data source:
   a. In the tree pane on the left, click the **IC Data Sources** container.
   b. In the IC data source pane on the right, right-click an empty area.
   c. In the shortcut menu, click **New**.
      Interaction Administrator displays the **Entry Name** dialog box.
   d. In the text box, type a name for your enterprise directory and click **OK**.
      Interaction Administrator displays the **IC Data Source type** dialog box.
   e. In the list box, click **LDAP** and then click the **Next** button.
      Interaction Administrator displays the configuration dialog.



3. Configure your new data source (Enterprise Directory):
   a. Expand the **Subtype** list box and click **Active Directory**.
   b. In the **Host Name** text box, type the domain name of your Active Directory host.
   c. If your Active Directory server listens on a specific port, type it in the **Port** text box.
      If you leave the **Port** text box blank, the CIC server will use the default port.
   d. In the **Bind DN** text box, type the distinguished name of the user account that the CIC server will use to connect to the Active Directory server. For example, you might type:
      `CN=Administrator, CN=Users, DC=domain, DC=com`

> **Note:** DN means *distinguished name*. The **Bind DN** text box contains credentials that let the CIC server log into the Active Directory server.

e. In the **Password** text box, type the appropriate password.
f. In the **Search DN** text box, type the distinguished name of the organizational unit to which you want to connect. For example, you might type:
```
OU=AllUsers, DC=domain, DC=com
```
g. Leave the **Additional Information** text box blank.
h. Click the **Finish** button.

Your new data source is configured.

2: Configure Status Aggregator Contact List Sources

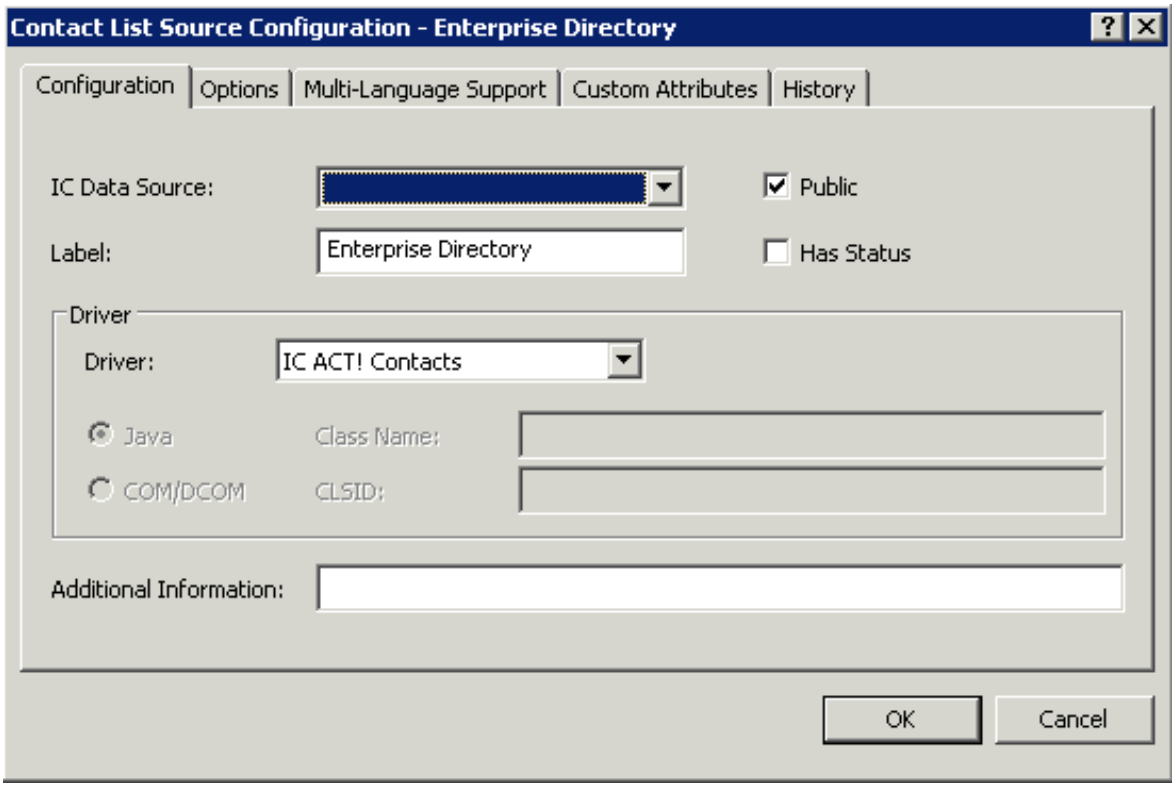
The second major step is to configure contact list sources in Interaction Administrator. Users can open the contact list in their clients. The list gets its information from the data source.

In other words, the name you give this contact list is the name that will appear in the **General Directories** list of pages in the CIC client. Users will select this name.

For information about other steps in the process, see Overview of Configuring Status Aggregator.

To configure Status Aggregator contact list sources in Interaction Administrator:

1. If needed, start Interaction Administrator.
2. Add a new contact list source:
   a. In the tree pane on the left, click the **Contact List Sources** container.
   b. In the contact list source names pane on the right, right-click an empty area.
   c. In the shortcut menu, click **New**.
   Interaction Administrator displays the **Entry Name** dialog box.
   d. In the text box, type the name of your enterprise directory and click **OK**.
   Interaction Administrator displays the **Contact List Source Configuration** dialog box.



3. Configure your new contact list data source:
   a. Expand the **IC Data Source** list box and click the IC data source that you configured for Status Aggregator.
   b. If needed, type the name of your contact list in the **Label** text box.
   c. Select the **Has Status** check box.

d. In the **Driver** area, expand the **Driver** list box and click **IC LDAP Contacts**.

e. If you use an object class other than the IC default object class of **i3person** to store contact information, then in the Additional Information text box, type:

```
ATTRIBUTE_MAPPING_FILE="<path to attribute file>\attributefile.txt";
NEXT_POLLING_TIME=2008-11-12 12:01:00; POLLING_INTERVAL=86400
```

> **Note:**
> These parameters are (1) The path to the attribute mapping file; (2) The next date and time when Status Aggregator should poll this source for information and (3) The time interval that Status Aggregator should wait after each poll before it polls this source again. The **NEXT_POLLING_TIME** parameter is in UTC time (Greenwich Mean Time), five hours later than U.S. Eastern Standard time. The **POLLING_INTERVAL** parameter is in seconds so, for example, 86400 stands for 24 hours.
> The attribute mapping file parameter is needed only if you use an object class other than the IC default object class of **i3person** to store contact information. If you create your own custom object class, you must create a text file that maps CIC attributes to the attributes of your object class. Use the file name and path as the attribute mapping file parameter. For more information, see "Using LDAP for Customer Interaction Center Contact Lists" on the PureConnect Customer Care site.
> The **NEXT_POLLING_TIME** parameter value should be set as UTC time in ISO 8601 format (`YYYY-MM-DD hh:mm:ss`). By default, the **NEXT_POLLING_TIME** value gets set to 12a.m. of the night of the install and the **POLLING_INTERVAL** value gets set to 86400.

4. Click **OK**.

Interaction Administrator adds and configures your new contact list data source.

3: Import Certificates Into Each CIC Server

The third major step is to import certificates into each CIC server. You should follow these steps on each CIC server and peer Status Aggregator server. Only administrator accounts can import certificates. In addition, the files `AdminGenSSLU.exe` and `AdminGenSSLU.dll` must be in the same directory on the CIC server.

For information about other steps in the process, see Overview of Configuring Status Aggregator.

To import certificates:

1. In Windows Explorer, open the `\Windows\temp` folder on the hard drive from which the computer starts.
2. Under the `\Windows\temp` folder, create a subfolder named `Certs`.
3. From the USB key drive, copy the certificates for this CIC server into the new `Certs` folder you just created.
4. In the `Certs` folder, double-click `ImportSubsystemsCertificate.bat`.

The batch file opens a command window and displays its progress as it imports the certificates. When complete, it displays the message "Successfully imported into the Subsystems certificate for …"

> **Warning!**
> If the batch file does not display the "success" message, then it did not import the certificates. Verify that you are using an administrator account. Press the spacebar to close the command window.

The Status Aggregator server and the CIC server are now in a *trusted* relationship and can communicate securely.

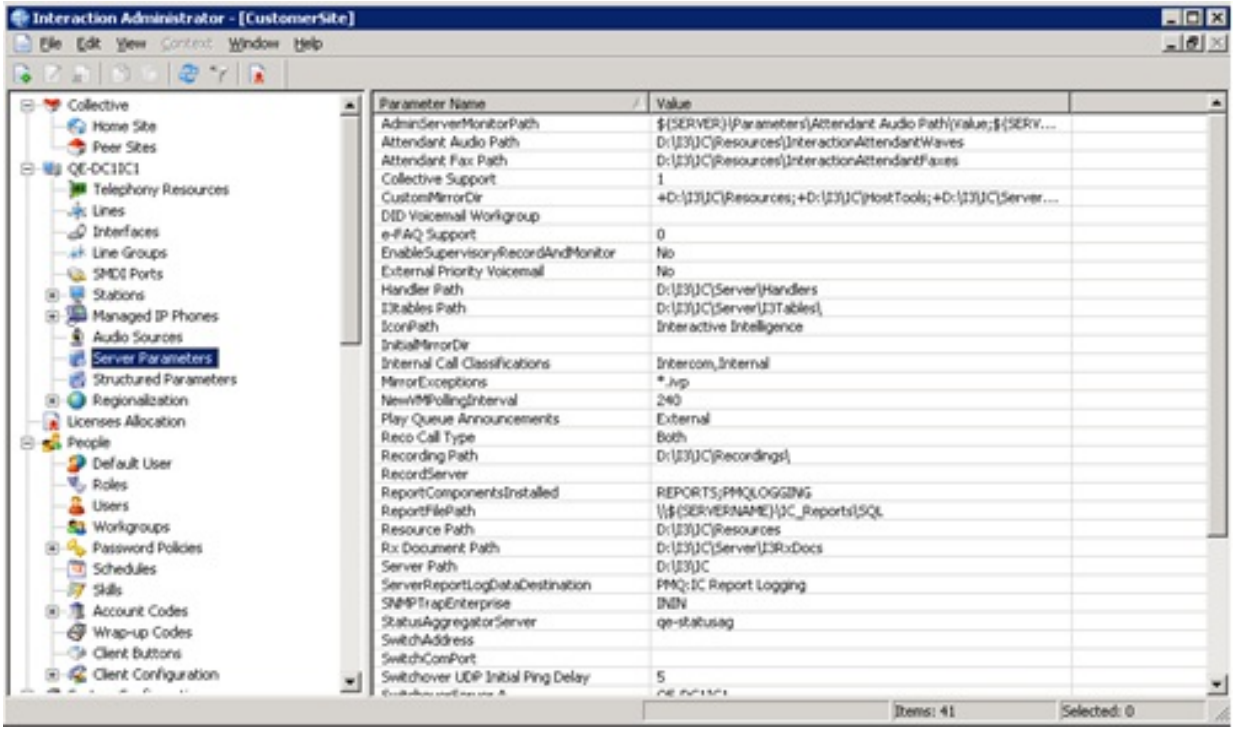
4: Set Parameters for the Status Aggregator Server

The fourth major step is to tell each CIC server the name of the Status Aggregator server that will provide aggregated status information from other CIC servers. Until you set this parameter, the CIC servers do not know where to look for aggregated status information.

For information about other steps in the process, see Overview of Configuring Status Aggregator.

To set parameters for the Status Aggregator server:

1. Start Interaction Administrator.
2. Display the **Server Parameters** container.



3. Add (or modify, if already present) a parameter named `StatusAggregatorServer`:

   Warning!
   The name of this parameter must be `StatusAggregatorServer`.

4. For the parameter value, enter the host name(s) of the Status Aggregator server(s). Use semicolons to separate names.

   Warning!
   Do not enter a fully-qualified domain name. Use only the host name.

Interaction Administrator adds the new parameter and gives it the value you entered.

Start and Run Status Aggregator

After you install and configure Status Aggregator, only two major steps remain:

- On the Status Aggregator server, the administrator starts Status Aggregator or verifies that it is already running.
- In each user's CIC client, each user views status information that Status Aggregator has collected from all its connected CIC servers.

Users access and view consolidated information from Status Aggregator by using the CIC client. In fact, because Status Aggregator runs behind the scenes, users might not even realize that they are viewing non-local status information.

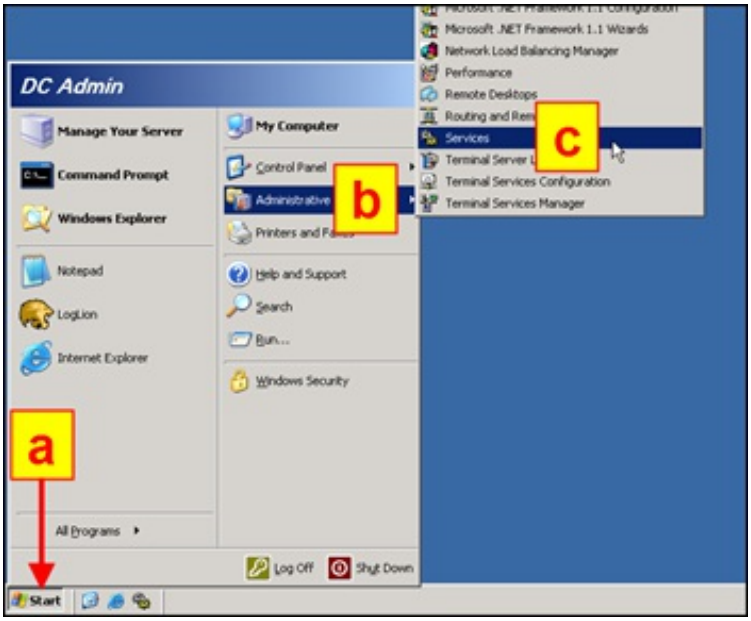
With Status Aggregator running, users access information in the CIC client in the same way as they always have. The only difference is that they now see status information from remote offices and from their local office.

Start Status Aggregator

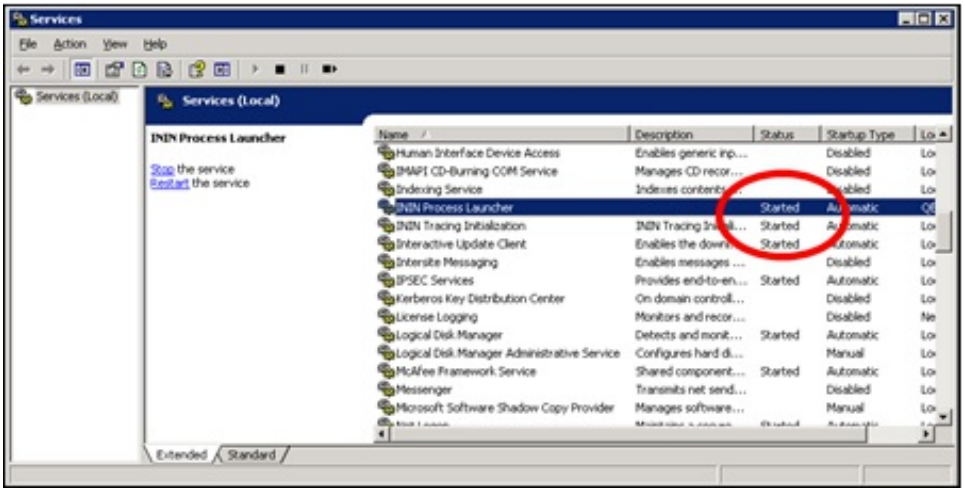
Status Aggregator starts automatically. Usually, you do not need to do anything to start the program. In case of a problem, however, you might want to verify that Status Aggregator has started and is running.

To start Status Aggregator or to verify that it is running:

1. On the Status Aggregator server, click the **Start** button (a), point to **Administrative Tools** (b), and click **Services** (c).



2. In the **Services** window, scroll down to for **ININ Process Launcher**.



3. In the **ININ Process Launcher** line, view the value in the **Status** column:
   a. If the **Status** column says **Running**, then Status Aggregator is already running and you do not need to do anything more.

b. If the **Status** column does not say **Running**, double-click the line to start Status Aggregator.

User operation of Status Aggregator

Strictly speaking, users don't run Status Aggregator at all. When they use the CIC client to look up status information, Status Aggregator runs in the background and supplies consolidated status information through the CIC client. The only difference that users will see is that they can now view status information not only for their local offices, but for any office or unit with a CIC server that feeds information to Status Aggregator.

Add Status Aggregator directory to the CIC clients

Once Status Aggregator has been installed and configured on the Status Aggregator server and its associated CIC servers, CIC client users can add directory pages to display all local and remote status data.

To add a new directory view to your version of the CIC client, see the following help topics in the PureConnect Documentation Library:

- Interaction Desktop: Add or Close Views and Working With Directories.

  Note:
  In the **New View** window, search for **General Directories**.
- Interaction Connect: Add or Close Views and Directories.

The new tab works the same way as the typical CIC client directory tab. Users can search for individual or group statuses by typing values in the text boxes at the top of the columns and can display an individual's status by right-clicking his/her line in the table.

Appendix A: Antivirus Requirements and Best Practices

Genesys has verified that McAfee VirusScan and Symantec AntiVirus software can be installed on the CIC server, other network servers (such as email servers), and workstations, as part of a system-wide antivirus strategy. The customer or partner has the option to install antivirus software. See the PureConnect Testlab site at http://testlab.genesys.com for the latest supported versions of McAfee VirusScan and Symantec AntiVirus.

Please note the following antivirus requirements and best practices:

Run a scan of all disks during off-peak hours once per day, or at least once per week. Synchronize this effort with other backup tasks that are typically run daily.

We highly recommend that active scanning be disabled while running Interaction Media Server installs and while updating the server. Active scanning locks files, causes excessive disk I/O, and high CPU utilization that can result in system slowdowns or failure.

However, if active scanning is a requirement, **it should not be turned on during business hours**, especially if the server is under a high CPU load.

Apply the following configuration changes to optimize the Interaction Media Server's CPU, disk, and memory usage:

1. Update the virus definition files daily.
2. Disable scanning files on reading from disk - configure the software to scan only when writing to disk.
3. Scan default files plus designated additional file types, not all files.
4. Exclude the following directories and their subdirectories from active scanning
   - `${Drive}\Program Files\Interactive Intelligence\Recordings` (or where specified during the installation)
   - The drive/directory specified during installation for PureConnect log files

   > **Note:**
   > Since the `Recordings` directory is shared on the network, you increase the risk of exposure to virus by excluding this directory from active scanning. However, if you chose to include it in the active scan and there is a high volume of recording activity, scanning may affect the performance of the system and the capacity of call recordings.
5. Exclude the following extensions from being scanned:
   - `.ivp`
   - `.dxs`
   - `.ininlog` (IC log file format)
   - `.ininlog.ininlog_idx` (IC log file format)

Change Log

The following table lists the changes to the *Status Aggregator Technical Reference* since its initial release.

Date	Changes
08-December-2008	Corrected GMT time.
27-October 27-2009	Corrected description of the StatusAggregatorServer parameter.
12-March-2010	Updated title page, copyright / trademark information, and platform statement.
15-July-2010	Updated installation instructions for SU10 New Patch Target.
23-August-2010	Corrected Figure 2-5 (setup complete).
30-November-2010	Updated information about how to obtain the AdminGenSSLCerts utility.
10-January-2011	Updated index.
25-May-2011	Clarified "Install Status Aggregator." Added explanation of attribute mapping file. Expanded "Configure Status Aggregator Contact List Sources." Updated references to OCS and Lync admin guides.
18-October-2011	Updated for IC 4.0.
11-November-2011	Updated system requirements section and support site link.
21-August-2012	Added back information about support for Lync-OCS.
07-March-2014	Made miscellaneous improvements in explanations of installation and configuration. Updated copyright page.
15-August-2014	Updated documentation to reflect changes required in the transition from version 4.0 SU# to CIC 2015 R1, such as updates to product version numbers, system requirements, installation procedures, references to Product Information site URLs, and copyright and trademark information.
12-January-2015	Made minor corrections in sections "Install Status Aggregator" and at the end of Chapter 2.
09-September-2015	• Updated documentation to reflect the addition of two CIC client applications, Interaction Desktop and Interaction Connect and the removal of Interaction Client .NET Edition. • Changed the name of "Verify Interaction Client Page Options" to "Add Status Aggregator Directory to the CIC Clients" and changed contents to reference help for the different client versions. • Updated document formatting and changed chapters to sections.
28-April-2017	Updated documentation to reflect the removal of Interaction Client Web Edition.
16-March-2018	Rebranded to Genesys.
17-June-2019	Reorganized the content only, which included combining some topics and deleting others that just had an introductory sentence such as, "In this section...".