



PureConnect®

2021 R4

Generated:

04-November-2021

Content last updated:

13-May-2020

See [Change Log](#) for summary of changes.



# Configuration of CIC Phone Features for Polycom Phones

## Technical Reference

### Abstract

This document applies to non-managed phones. It describes the manual configuration of Polycom IP phones where an administrator changes the Polycom phone configuration files. It details the configuration of Shared Line Appearances (SLAs), Zone Paging, Call Park, and Group Call Pickup. These features require configuration settings in Interaction Administrator and Polycom configuration files.

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

For copyright and trademark information, see [https://help.genesys.com/pureconnect/desktop/copyright\\_and\\_trademark\\_information.htm](https://help.genesys.com/pureconnect/desktop/copyright_and_trademark_information.htm).

# Table of Contents

Table of Contents	2
Introduction to CIC Phone Features Configuration for Polycom Phones	3
CIC client	3
SIP auto-provisioning	3
Managed phones vs. non-managed phones	3
Requirements	3
Polycom Configuration Files	4
Manual configuration	4
Interaction Administrator Configuration Settings	5
SNTP Server	6
CIC installed on a domain controller Windows Server 2008	6
CIC installed on a non-domain controller Windows Server 2008	6
CIC installed on a non-domain controller Windows Server 2008 system in a domain without a reliable NTP source	6
DHCP Server	7
About TFTP Server	8
TFTP server subdirectories	8
TFTP server interface	8
Installation and basic configuration	8
View the TFTP Server Configuration	8
Monitor TFTP Server Activities	9
Activity view options	11
Configure the TFTP Server	12
Modify the phone configuration files	14
Change the TFTP Server Credentials	15
Reset user name and password	15
Shared Line Appearances	16
Terminology	16
Operation	16
Shared line appearances configuration	17
Interaction Administrator Station Configuration	17
Interaction Administrator primary station configuration	17
Interaction Administrator secondary station configuration	18
Polycom Configuration Settings for SLAs	18
Polycom SLA settings examples	19
Polycom display examples	20
Set the Number of Call Appearances	20
Call Park	22
Polycom configuration settings for Call Park	22
Interaction Administrator configuration settings for Call Park	22
Group Call Pickup	23
Polycom configuration settings for Group Call Pickup	23
Interaction Administrator configuration settings for Group Call Pickup	23
Zone Page	24
Limitations	24
Polycom configuration settings for Zone Page	24
Interaction Administrator configuration settings for Zone Page	24
*90x Dialing Options	26
Change Log	27

# Introduction to CIC Phone Features Configuration for Polycom Phones

The *Configuration of CIC Phone Features for Polycom Phones Technical Reference* addresses the manual configuration of Customer Interaction Center (CIC) phone features for Polycom phones. It includes configuration and setup instructions for the following features:

- [Shared Line Appearances](#)
- [Call Park](#)
- [Group Call Pickup](#)
- [Zone Page](#)

## CIC client

CIC supports two interaction management client applications. *CIC client* refers to either Interaction Connect or Interaction Desktop.

## SIP auto-provisioning

CIC includes the SIP auto-provisioning feature, which allows you to configure supported Polycom IP phones or SIP Soft Phones automatically. For more information, see "Use Auto Provisioning" in the [SIP Soft Phone Help](#).

Interaction Administrator includes the Managed IP Phones container and other enhancements that support auto-provisioning. For more information, see the [CIC Managed IP Phones Administrator's Guide](#).

## Managed phones vs. non-managed phones

The managed phone approach is the preferred method for configuring, setting up, and managing Polycom IP phones or SIP Soft Phones. You can use auto-provisioning and still have the flexibility to create custom configuration files as needed. For more information, see the [CIC Managed IP Phones Administrator's Guide](#).

Manual configuration of Polycom IP phones occurs when an administrator modifies the Polycom phone configuration files directly. Support of CIC phone features requires configuration changes in the Polycom configuration files and in Interaction Administrator.

Adopt one approach or the other for the configuration and setup of your IP phones. For the Shared Line Appearances feature, you cannot mix managed and non-managed phone types.

The Call Park and Zone Page features are available for managed phones and require no additional changes to the individual phone configuration files. However, it is also necessary to configure the appropriate station groups in Interaction Administrator to support the Call Park and Zone Page features. For more information about station group configuration, see the [Interaction Administrator Help](#). For more information about zones, see [Zone Page](#).

## Requirements

Polycom firmware requirements for each model are listed on the **SIP IP Phones** information page available at the [Genesys Testlab site](#). For more information about determining the firmware version number for a particular phone, see your Polycom documentation.

# Polycom Configuration Files

IC phone features require changes to the Polycom configuration files. The SIP configuration file (`sip.cfg`) contains SIP protocol and core configuration settings that typically affect an entire installation. This file is supplied in the Polycom firmware.

File Name	Description
<code>xIC.cfg</code>	This site-wide settings file provides overrides to attributes in the <code>sip.cfg</code> . <b>Note:</b> If you are not in the United States, or any other country that uses the same DST scheme, also adjust some site-specific settings in <code>xIC.cfg</code> , such as GMT offset and daylight savings time attributes.
<code>&lt;group name&gt;.cfg</code>	This optional file provides overrides to attributes in the individual phone configuration files, <code>phone name- &lt; Ethernet address &gt;.cfg</code> .
<code>&lt;Ethernet address&gt;.cfg</code>	This file is unique for each phone. This bootstrap file tells the phone which configuration files to load. <b>Note:</b> The <code>Ethernet address</code> part of the file name is the <b>MAC address</b> of the phone. <code>&lt; Ethernet address &gt;.cfg</code> is the term used in the Polycom documentation.
<code>phone name- &lt;Ethernet address&gt;.cfg</code>	This file is unique for each phone. It contains phone configuration settings for one phone. The <code>phone name</code> part of this file name is the individual phone name you specify in this tool. If you import data to Interaction Administrator, it is also the station name for the phone.
<code>&lt;any name&gt;.csv</code>	Use this phone configuration data export file to import station data to Interaction Administrator.
<code>&lt;any name&gt;.ipc</code>	Use this data file to save and retrieve phone and phone group data. Also use it to organize phone configuration data by site, company, vendor, or other identifier.

## Manual configuration

Polycom configuration files are in XML format. After you create these files, it is easier to modify them using an XML editor.

**Note:** Genesys recommends that you do not modify the `sip.cfg` file.

# Interaction Administrator Configuration Settings

Along with changes to Polycom configuration files, some of the CIC phone features require configuration settings in Interaction Administrator. The *Configuration of CIC Phone Features for Polycom Phones Technical Reference* contains examples of the appropriate settings in Interaction Administrator. For more information about the configuration settings, see the [Interaction Administrator Help](#).

# SNTP Server

The CIC installation process sets the SNTP (Simple Network Time Protocol) service to run on the CIC server. Depending on where CIC is installed, it may require more SNTP configuration.

**Note:** You can also configure SNTP settings through DHCP. For more information, see "Configure the Time Server (Polycom and IIS)" in the [CIC Managed IP Phones Administrator's Guide](#). These settings are valid for both managed and non-managed phones.

## CIC installed on a domain controller Windows Server 2008

No additional SNTP service configuration necessary.

## CIC installed on a non-domain controller Windows Server 2008

It's possible that the NTPServer is not enabled. The system is an NTP/SNTP client, but not a server.

Do the following for the SNTP service:

1. Change a registry entry on the CIC server:
  - a. Locate `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\TimeProviders\NtpServer` and set the value of **Enabled** to **1**.
  - b. Open a command window, and type:

```
net stop w32time && net start w32time
```

**Note:**

The NTP/SNTP server-side functionality is not active on non-domain controllers by default.

2. Supply the address of the SNTP server in the `xIC.cfg` file.

## CIC installed on a non-domain controller Windows Server 2008 system in a domain without a reliable NTP source

Polycom phones do not use this NTP server. A reliable NTP source can be external or direct.

Do the following for the SNTP service:

1. On the CIC server locate `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config` and set the value of **AnnounceFlags** to **5**.
2. Locate `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\TimeProviders\NtpServer` and set the value of **Enabled** to **1**.
3. Open a command window, and type:
  - a. `net stop w32time && net start w32time`

**Note:**

These registry changes makes the time services a trusted authority using the local clock. A system that uses an external NTP server is preferred, but the default configuration is to try to use an external NTP server. If that is not working, these parameters treat the computer clock as a trusted source for computers connecting to this SNTP server.

4. Supply the address of the SNTP server in the `xIC.cfg` file.

# DHCP Server

Polycom phones also support dynamic host configuration protocol (DHCP). When set up, DHCP permits Plug and Play TCP/IP network setup.

Basic network settings can be derived from DHCP or typed manually using the LCD-based user interface on the phone. Polycom recommends using DHCP where possible to eliminate repetitive manual data entry. You can change phone network configuration settings by means of a main menu and two submenus: **DHCP Menu** and **Server Menu**.

Parameters obtained from a DHCP server can override manually typed networking parameters. These parameters include the TFTP server (boot server) address and the SNTP server address. For more information, see your *Polycom® Administrator Guide*.

# About TFTP Server

CIC provides a built-in TFTP server. When a Polycom phone is switched on, it downloads its configuration files from the TFTP root directory. By default, Polycom phones also write log files to this TFTP directory (if the TFTP server is configured to accept write operations).

**Note:** The TFTP server does not directly facilitate the creation or modification of Polycom phone configuration files. The TFTP root directory is available only by means of the network (if you set it up as a shared folder) or by direct access to the CIC server. The TFTP server is not used for managed phones.

## TFTP server subdirectories

By default, the IP phone files are stored in the main TFTP server directory. Or you can use separate subdirectories on the TFTP server for phone logs, contact directories, and override files. Specify these subdirectory names in the Polycom master configuration file (`<Ethernet address>.cfg`) to make the phones write the files to the appropriate subdirectories.

These types of files can be stored in subdirectories on the TFTP server .

File Type	Description
Phone Logs	Both startup and application event log files are maintained for each phone. These event log files are stored in the flash file system on the phone and are periodically uploaded to the TFTP server. The event log files are <code>&lt;Ethernet address&gt;-boot.log</code> and <code>&lt;Ethernet address&gt;-app.log</code> .
Contact Directories	Each phone maintains a local contact directory. The person using the phone can change the directory contents at will. Changes are stored in the flash file system on the phone and are backed up to the boot server copy of <code>&lt;Ethernet address&gt;-directory.xml</code> (if configured). Only updated contact directories are stored in this subdirectory. When the phone starts up, the boot server copy of the directory, if present, replaces the local copy.
Overrides	The <code>&lt;Ethernet address&gt;-phone.cfg</code> files are also referred to as boot server override files. Configuration overrides made at the phone are written to this subdirectory. Storing the updated phone configuration files in a specific subdirectory helps to separate them from the files you often modify which are stored in the root directory.

## TFTP server interface

You can use a web-based interface for the CIC TFTP server to:

- Monitor the TFTP client file transfer activity.
- Specify upload file types.
- Configure the upload subdirectories.

## Installation and basic configuration

The CIC server install automatically installs the necessary TFTP server component files. You can use Setup Assistant to change the TFTP server **Service Startup Type** from **Manual** to **Automatic**. For more information, see the [PureConnect Installation and Configuration Guide](#).

**Note:** If you change the TFTP server **Service Startup Type**, restart the service.

**Phone Feature Configuration of Polycom Phones Technical Reference**

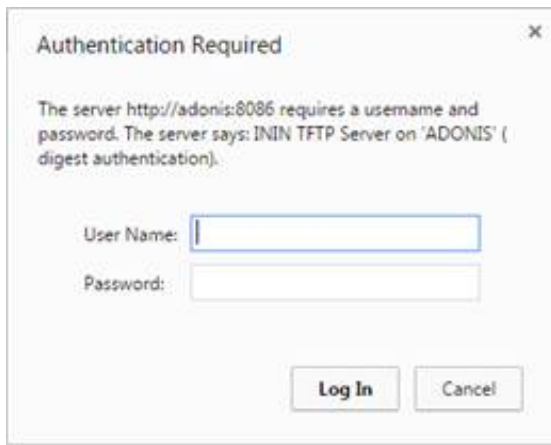
## View the TFTP Server Configuration

You can view the TFTP server configuration in its web-based configuration interface.

**To view the TFTP server configuration**

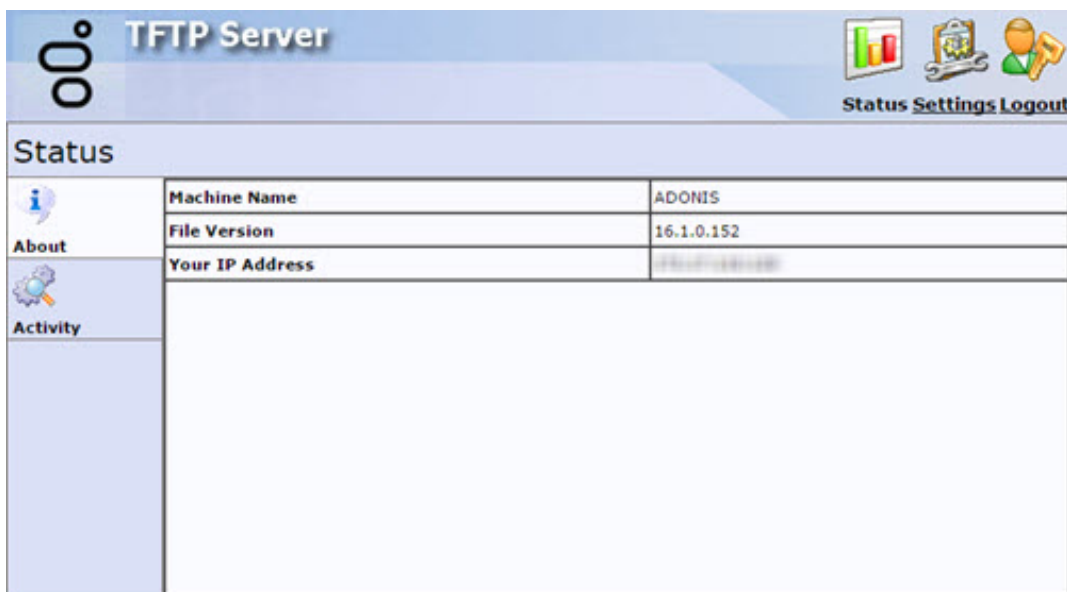
1. Point your browser to the TFTP server and its port number (for example, <http://spyhunter:8086>). The **Authentication Required** dialog box appears.





**Note:** The default TFTP server port number is 8086, but you can change this setting in the registry. See `HKEY_LOCAL_MACHINE\SOFTWARE\Interactive Intelligence\TFTPServer\Config Port`.

2. In the **User Name** and **Password** boxes, type the TFTP server credentials and then click **Log In**. The **TFTP Server About** configuration page appears.



**Machine Name:** TFTP server computer name.

**File Version:** TFTP server files version number. PureConnect Customer Care representatives sometimes ask for this number.

**Your IP Address:** IP address of the computer where you are running the browser.

**Note:** The TFTP server credentials are defined in the initial installation. Unless otherwise specified, the default user name is `admin` (all lowercase) and the default password is `1234`. For more information about changing these credentials, see [Change the TFTP Server Login Credentials](#).

**Tip:** You can also display this page by selecting **Status** from the menu bar and then clicking **About** in the left navigation of the **Status** page.

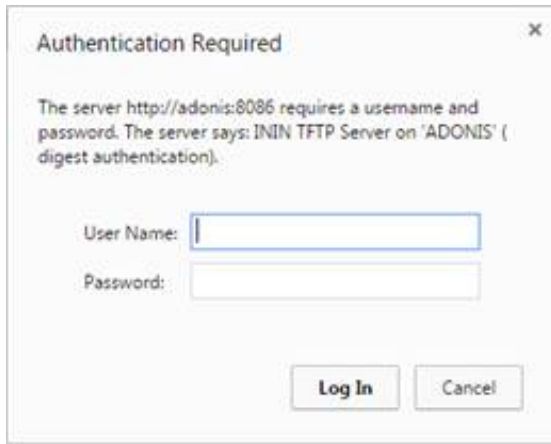
*Copyright and trademark*

## Monitor TFTP Server Activities

You can monitor and review the client file transfer activities on the TFTP server.

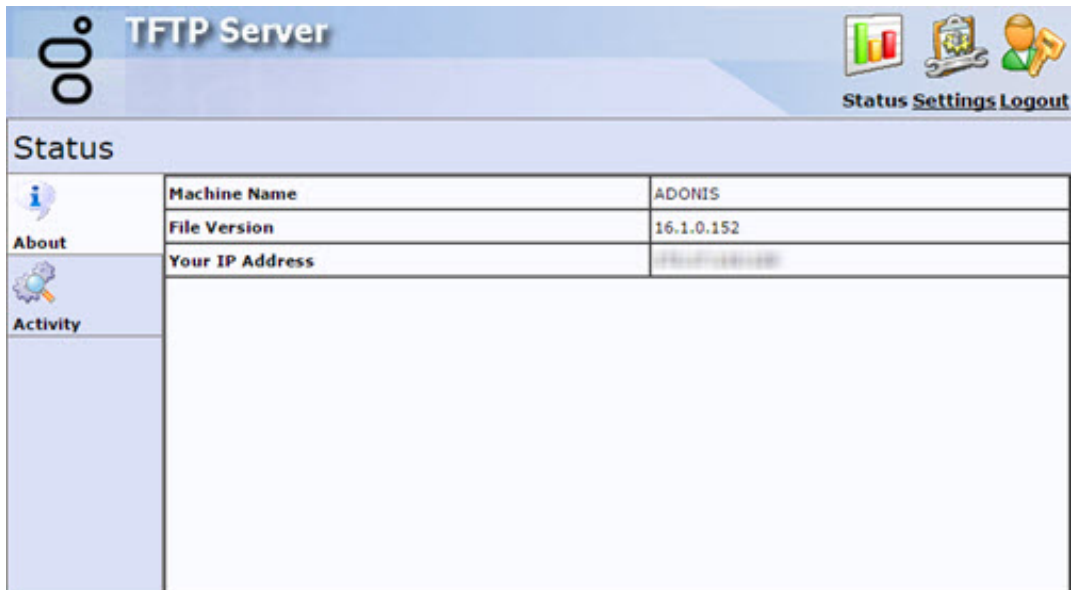
To monitor TFTP server activities

1. Point your browser to the TFTP server and its port number (for example, <http://spyhunter:8086>). The **Authentication Required** dialog box appears.




The screenshot shows a standard Windows-style dialog box titled "Authentication Required". The text inside reads: "The server http://adonis:8086 requires a username and password. The server says: ININ TFTP Server on 'ADONIS' ( digest authentication)." Below the text are two input fields: "User Name:" and "Password:". At the bottom of the dialog are two buttons: "Log In" and "Cancel".

2. In the **User Name** and **Password** boxes, type the TFTP server credentials and then click **Log In**. The **TFTP Server About** configuration page appears.



The screenshot displays the "TFTP Server" web interface. The top header includes the "TFTP Server" logo and navigation links for "Status", "Settings", and "Logout". The main content area is titled "Status" and contains a table with the following information:

	<b>Machine Name</b>	ADONIS
<b>About</b>	<b>File Version</b>	16.1.0.152
	<b>Your IP Address</b>	172.17.0.152

Below the table is a large empty box labeled "Activity".

3. In the left navigation of the **Status** page, click **Activity**. The **TFTP Server Activity** page appears.

**TFTP Server** Status Settings Logout

---

**Status**

Activity Results 1 - 10 of 10

Navigation: [Home] [Previous] [Next] [End]

Type	Date	Time	Client	File	Details
↑	2015/07/14	14:19:10	172.18.108.64	0004f262bbcc-app.log	17315 (16 KB)
✘	2015/07/14	14:19:09	172.18.108.64	logs/0004f262bbcc-app.log	Directory specifications aren't allowed against this server. Only Root path GETs and PUTs are allowed.
↑	2015/07/14	14:19:09	172.18.108.64	0004f262bbcc-boot.log	73216 (71 KB)
✘	2015/07/14	14:19:06	172.18.108.64	logs/0004f262bbcc-boot.log	Directory specifications aren't allowed against this server. Only Root path GETs and PUTs are allowed.
✘	2015/07/14	14:19:06	172.18.108.64	000000000000.cfg	Provision mode file not retrieved
✘	2015/07/14	14:19:05	172.18.108.64	contacts/000000000000-directory.xml	Provision mode file not retrieved
✘	2015/07/14	14:19:04	172.18.108.64	0004f262bbcc.cfg	Provision mode file not retrieved
✘	2015/07/14	14:19:02	172.18.108.64	contacts/0004f262bbcc-directory.xml	Provision mode file not retrieved
↑	2015/07/14	14:18:14	172.18.108.64	0004f262bbcc-app.log	29003 (28 KB)
✘	2015/07/14	14:18:12	172.18.108.64	logs/0004f262bbcc-app.log	Directory specifications aren't allowed against this server. Only Root path GETs and PUTs are allowed.

Clear Refresh  Auto-refresh every 10s

**Type:** Indicates the direction of the file transfer, a file transfer failure, or a message.

↓	File successfully downloaded from phone to TFTP server.
↑	File successfully uploaded from TFTP server to phone.
✘	File transfer failure.
🚫	IP Address is not in the allowed range.
⚠	Phone has returned an error during the file transfer. The message from the phone appears in the <b>Details</b> column.

**Date and Time:** Date and time of the file transfer activity. Activities are presented in reverse chronological order, with the most recent activity first on the list.





**Client:** IP address for the telephone.

**File:** Name of the file that transferred.

**Details:** Details about the activity, such as transfer size for uploads and downloads. If a File Transfer Error occurs, the message displays here.

**Note:** Transfer size is not always the same as file size. If a phone knows that it does not need the entire file, it is common for it to quit downloading a large file. For example, the phone can determine the file version from the header (first set of bytes) of `sip.id` and if it has the current version, it stops the download process.

## Activity view options

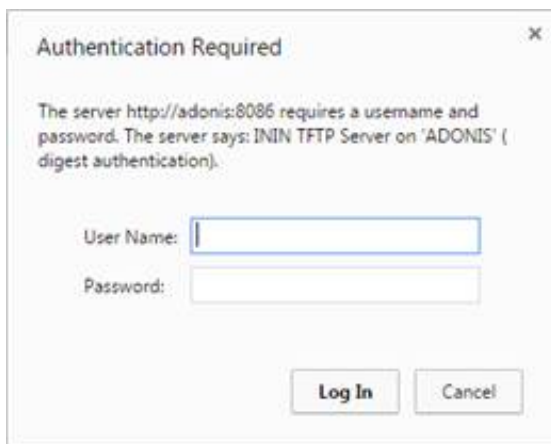
	Display first page of <b>Activity</b> view.
	Display previous page of <b>Activity</b> view.
1 <u>2</u>	Click a page hyperlink to explore the <b>Activity</b> view page by page.
	Display next page of <b>Activity</b> view.
	Display last page of <b>Activity</b> view.
<b>Clear</b>	Clear all activity history from the <b>Activity</b> view.
<b>Refresh</b>	Refresh the <b>Activity</b> view with the latest file transfer information.
<b>Auto-refresh every 10s</b>	<p>Select this check box to refresh the <b>Activity</b> view automatically every 10 seconds.</p> <p><b>Note:</b> This option is available only on the first page. It updates the display so you always see the 15 most recent file transfer activities.</p> <p><b>Tip:</b> You can control the number of items displayed in each page by adding <code>size=X</code> to the URL string, for example <code>http://spyhunter:8086/status/activity?size=30</code>. You can use <b>Auto-refresh</b> to see <i>X</i> number of the most recent file transfer activities.</p>

## Configure the TFTP Server

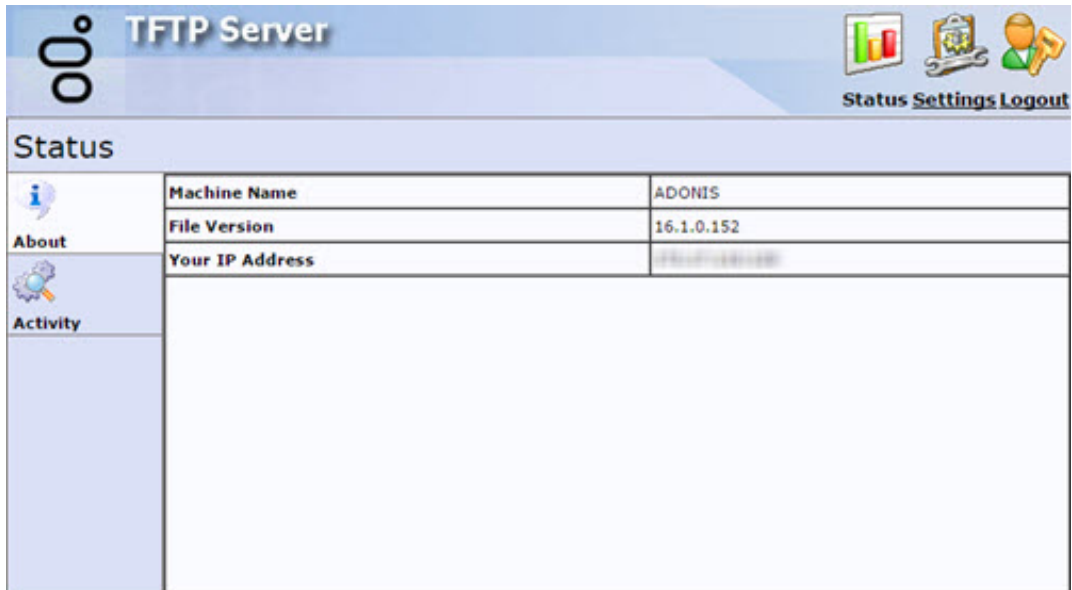
You can configure the TFTP server from its web interface.

### To configure the TFTP server

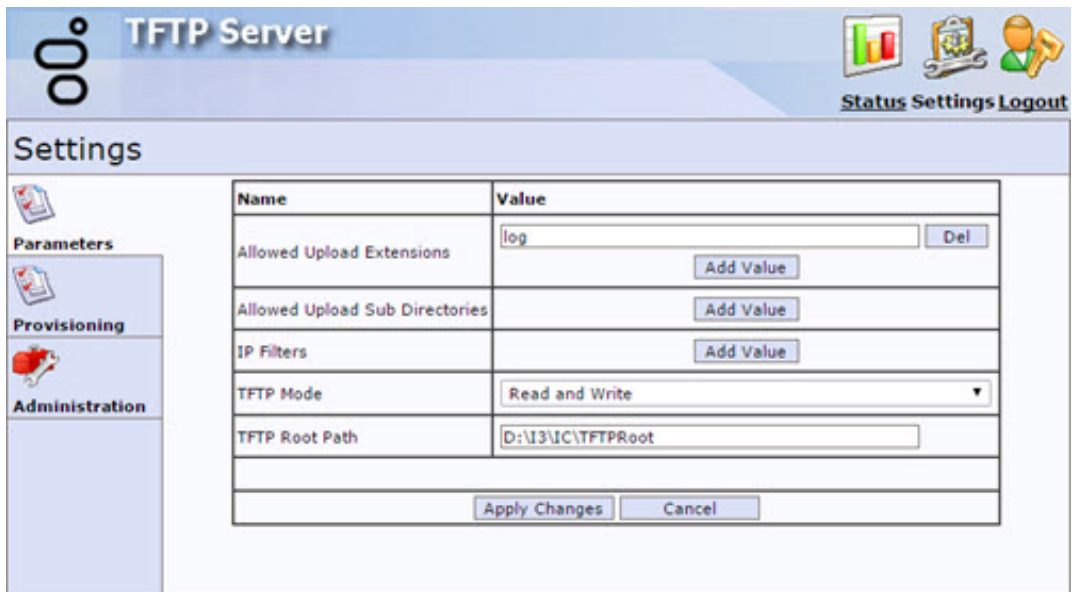
1. Point your browser to the TFTP server and its port number (for example, <http://spyhunter:8086>). The **Authentication Required** dialog box appears.



2. In the **User Name** and **Password** boxes, type the TFTP server credentials and then click **Log In**. The **TFTP Server About** configuration page appears.



- From the menu bar, click **Settings** and then, in the left navigation of the **Settings** page, click **Parameters**. The TFTP Server Parameters page appears.



- In **Allowed Upload Extensions**, do one of the following:

- To add an allowed extension for files that can upload to the TFTP server, click **Add Value**.
- To delete an allowed extension, click **Del** on the appropriate line.

The default value is log.

**Note:** Specify an allowed extension without any prefix or period. For example, specify \*.log as log to allow only \*.log files to be uploaded. If **Allowed Upload Extensions** values are not set or are blank, the TFTP server accepts any file name when the server is configured for write or read/write mode.

- In **Allowed Upload Sub Directories**, do one of the following:

- To specify the name of a subdirectory in the TFTP server root directory that can accept files uploaded from the phones, click **Add Value**.
- To delete the name of an allowed subdirectory, click **Del** on the appropriate line.

The default value is blank.

**Note:** Directory names can contain only upper or lowercase letters, numbers, and underscores. Spaces and punctuation are not allowed.

**Warning!**

Physically create the appropriate subdirectories on the TFTP server and identify them here. Phone logs, configuration files, or contact directories cannot be saved until the subdirectories exist. Allowed subdirectory names must match the ones used in the `<Ethernet address>.cfg` files for each phones. For more information, see [Modify the phone configuration files](#).

6. In **IP Filters**, do one of the following:

- To specify a range of IP addresses that have access to the TFTP server, click **Add Value**. The address range format is: `X.X.X.X-X.X.X.X`.
- To delete an allowed IP address range, click **Del** on the appropriate line.

The default value is blank.

**Note:** Addresses outside the ranges provided are not allowed access. You can specify multiple address ranges.

**Warning!**

If no values are specified, access is not limited.

7. In **TFTP Mode**, select the mode the TFTP server runs in. The possible settings are:

<b>Read</b>	TFTP server sends files, but does not accept TFTP uploads. This setting is the most secure mode.
<b>Read and Write</b>	TFTP server allows upload and download of files.
<b>Write</b>	TFTP server accepts TFTP uploads, but does not allow phones to download files. This mode would almost never be used for supporting IP phones.

8. In **TFTP Root Path**, specify the directory the TFTP server uses as its home or root directory.

**Default value:** `C:\I3\IC\TFTPRoot`

The CIC install creates this registry value and sets it to `[i3 install disk][i3 install directory]\TFTPRoot` (example: `D:\i3\ic\TFTPRoot`) and creates the directory automatically.

9. Do one of the following:

- To save changes to the TFTP server configuration, click **Apply Changes**. The changes are effective immediately.
- To discard your changes to the TFTP server configuration, click **Cancel**.

## Modify the phone configuration files

To direct the phone logs, contact directories, and overrides files to the appropriate TFTP server subdirectories, also modify each `<Ethernet address>.cfg` file.

Using an XML editor, supply the appropriate directory names in these attributes:

- LOG\_FILE\_DIRECTORY
- OVERRIDES\_DIRECTORY
- CONTACTS\_DIRECTORY

# Change the TFTP Server Credentials

You can change the TFTP server user name and password at any time.

## To change the TFTP server credentials

1. Open a browser on the TFTP server computer.

**Note:** You can log on to the TFTP server from another computer, but we recommend that you open the browser on the server computer when changing the logon credentials. For more information about displaying the TFTP server configuration pages, see [Configure the TFTP Server](#).

2. From the menu bar, click **Settings** and then, from the left navigation of the **Settings** page, click **Administration**. The **Change Login Credentials** page appears.

The screenshot shows the TFTP Server web interface. At the top, there is a header with the TFTP Server logo and navigation links for Status, Settings, and Logout. Below the header is a 'Settings' section with a left-hand navigation menu containing 'Parameters', 'Provisioning', and 'Administration'. The 'Administration' menu item is selected. The main content area is titled 'Change Login Credentials:' and contains six input fields: 'Old User Name', 'Old Password', 'New User Name', 'New Password', and 'Confirm New Password'. Below the input fields is an 'Important:' warning message: 'This is not a secure (https) session. The credentials are thus sent to the server in plain text. We recommend you run the browser on the server machine to change the credentials.' At the bottom of the form are two buttons: 'Apply' and 'Revert'.

3. In the **Old User Name** and **Old Password** boxes, type the user name and password for the user logged on to the TFTP Web Configuration pages currently.

**Note:** The CIC server install sets the default user name to `admin` (all lowercase) and the default password to `1234`.

4. In the **New User Name** and **New Password** boxes, type a new user name and password.
5. In the **Confirm New Password** box, retype the new password.
6. Do one of the following:
  - To save your changes, click **Apply**.
  - To discard your changes, click **Revert**.

---

## Reset user name and password

If you forget the TFTP server configuration logon user name and password, you can reset them to the default values of `admin` and `1234` by deleting the following registry entries. Then, you can use the default values to log on and reset the logon credentials.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Interactive Intelligence\TFTPServer\Config Username  
HKEY_LOCAL_MACHINE\SOFTWARE\Interactive Intelligence\TFTPServer\Config Password
```

# Shared Line Appearances

Users can employ Shared Line Appearances (SLAs) to use their phones to manage calls for other users. They can answer and make calls as if they were using an CIC station belonging to another user or using a group extension. An SLA is associated with a line key on the Polycom phone. Users can have both shared and private lines associated with different line keys on the same phone.

**Note:** Ensure all the phones that use the Shared Line Appearances feature are either managed or non-managed. You cannot mix the two types.

## Terminology

The following table lists some terms for configuration and setup of SLAs.

Term	Description
Call Appearance	Active call on a line appearance or shared line appearance.
Line Appearance	Appearance for a telephone line, a single-user circuit on a telephone system. A phone can have more than one line appearance for the same line or shared line.
Multiple Call Appearances	More than one call on one line appearance or on a shared line appearance. Only one of the calls can be active at one time; the other calls on the same line appearance are on hold.
Primary Station	Station to which the line appearance is assigned.
Primary User	User whose station is the <b>Primary Station</b> .
Secondary Station	Station on which an SLA appears. Secondary stations must have their own private (non-shared) line in addition to the SLA.
Secondary User	User whose station is the <b>Secondary Station</b> .
Shared Line Appearance	Line appearance that appears on multiple phones.

## Operation

An SLA occurs when a single CIC station (or *line*) appears on multiple phones. There is a single logical entity for the shared *line*, even though it can appear on several distinct physical devices (phones). A device using the shared line appearance does not have a unique identity or addressability.

SLAs are similar to extension phones in your home. When a call comes in, all of the extensions ring and you can answer the call from any extension. When you call from an extension, nobody else can call on the same line until you are finished. However, there is one important difference. The line belongs to a specific station in IC. This station is the *primary* and all the other stations on which this line appears are *secondary*. This distinction becomes important when CIC user status for the user associated with the primary station is set to **Available**, **Forward**, or one of the *not available* statuses.

Following are some features of the user experience with shared line appearances:

- Shared line appearances make the same line available on more than one phone.
- Shared line appearances can be associated with more than one line key on a phone.
- A specific icon on the phone display indicates a Shared Line Appearance. This icon is typically a telephone that is half black and half gray.
- In most cases, incoming calls to a shared line appearance cause all of the phones with the shared line appearance to ring.

**Note:** If the status for the CIC user of the primary station is one of the *not available* statuses, incoming calls do not ring on the primary station. Incoming calls ring on secondary stations when the primary user is not available. These calls ring regardless of the secondary user's CIC status unless the secondary user presses the **Do Not Disturb** button on the phone.

- If the CIC status for the primary station user for the SLA is set to **Available**, **Forward**, none of the phones with the SLA ring for alerting calls. The call is sent to the forwarded number for the primary station user. If the forwarded number does not answer the call, it goes to voice mail for the primary station user.
- Any user who is party to an SLA can answer an alerting call or a held call on an SLA. Only one user is connected to the call if multiple users attempt to pick up the call simultaneously.
- Any call made on an SLA is reported as if the primary station user called.
- If an SLA is in use on one phone, it cannot be used on another phone at the same time. If two users attempt to use an SLA simultaneously, the system permits one to succeed and indicates to the other that the line is in use.



- The phone display indicates when an SLA is alerting, off-hook, on hold, or connected.
- Calls on SLAs can be transferred, put on hold, or added to a conference.
- If no one answers an alerting call on an SLA, the call goes to voice mail for the primary station user.

## Shared line appearances configuration

You configure SLAs in both the Polycom phone configuration files and in Interaction Administrator.

The following example is for a situation where an assistant is able to answer and place calls on the line belonging to the manager through the use of shared line appearances. The assistant also has three private line appearances which are not shared with the phone for the manager.

	Manager	Assistant
<sup>1</sup> IA stands for Interaction Administrator. <sup>2</sup> Nb. is an abbreviation for number. <sup>3</sup> This example uses 70011 as the IA Identification Address on the first secondary station. You could number any other secondary stations in sequence. For example, you could use 70012 for the next secondary station.		
Station type	Primary	Secondary
Private line appearances	0	3
Shared line appearances	3	3
IA <sup>1</sup> Station Name	hal1	hal3
IA Station Extension	7001	7003
IA Nb. <sup>2</sup> Calls	3	3
IA Identification Addr.	70011 <sup>3</sup>	

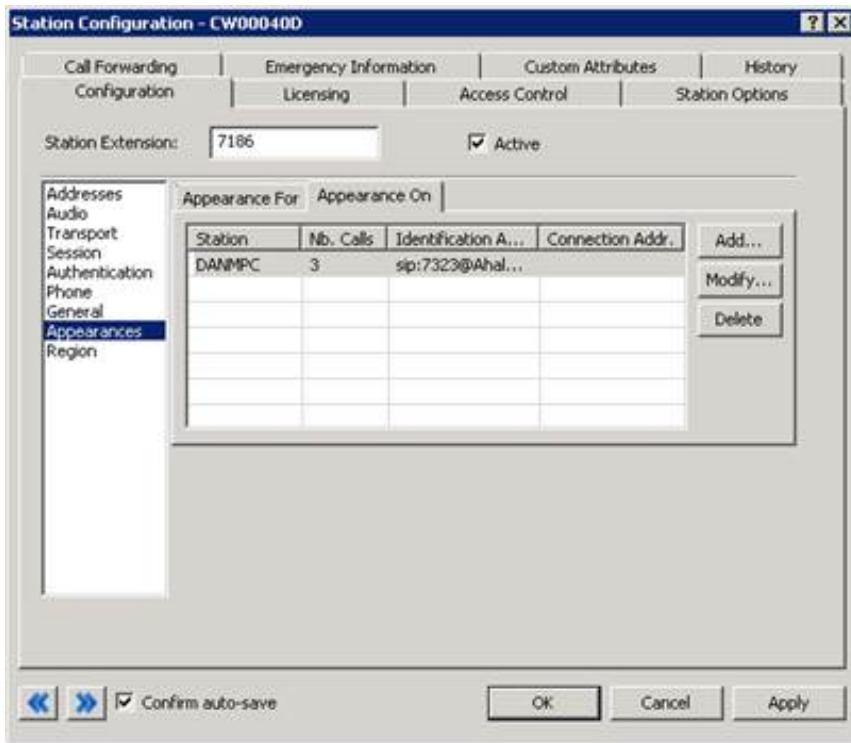
## Interaction Administrator Station Configuration

Configure the primary and secondary stations in Interaction Administrator. For more information about configuring line appearances, see "SIP Station Appearances" in the [Interaction Administrator Help](#).

### Interaction Administrator primary station configuration

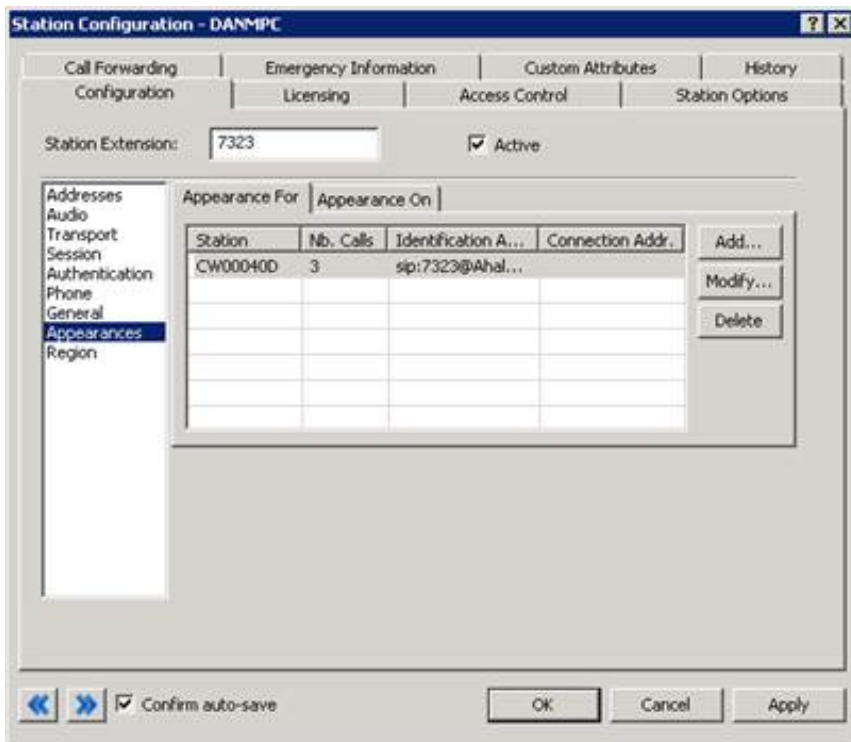
When you configure the primary station, you *specify the secondary stations on which the primary station appears*. In this example, you list the station for the assistant in the **Appearance On** tab of the station configuration for the manager. This setting indicates that the station for the manager appears *on* the phone belong to the assistant as a shared line appearance.

**Identification Addr.:** This address is the SIP ID number for the primary phone and a sequential number. In this example, it is 70011 (the SIP ID number for the primary station and 1). For example, if multiple secondary stations monitor the same primary station, use 70011 for the first monitoring station and 70012 for the second monitoring station. Then number additional monitoring stations in sequence. This address must match the `reg.x.address` used for the shared line appearance in the Polycom phone configuration file for the secondary station. For more information, see [Polycom Configuration Settings for SLAs](#).



## Interaction Administrator secondary station configuration

When you configure the secondary station, you specify the stations which appear as secondary line appearances on the secondary station. In this example, you list the station for the manager in the **Appearance For** tab of the station configuration for the assistant. These secondary line appearances appear for other stations.



## Polycom Configuration Settings for SLAs

All the SLA settings are in the Polycom phone configuration files. Set the following attributes in the Registration (<reg/>) section of the <Ethernet address>-phone.cfg files for the stations involved in shared line appearances.

Attribute	Notes
reg.x.address	<p>This address corresponds to this registration (<i>userPart</i> or <i>userPart@polycom.com</i>).</p> <p>On the primary station, this number matches the user portion of the <b>Identification Address of the SIP station</b> in Interaction Administrator.</p> <p>For a shared line appearance on a secondary station, this number matches the user portion of the <b>Identification Address of the Shared Line Appearance</b> configured in Interaction Administrator.</p> <p>In both cases, this number must be unique across all SIP stations and shared line appearances.</p>
reg.x.label	<p>This text label appears on the phone display next to the associated line key. It can be the same as <i>reg.x.address</i>.</p> <p>On secondary stations, set this label to the <i>reg.x.address</i> of the primary station. This setting makes the label on the secondary line appearance the same as the one on the primary station.</p>
reg.x.type	<p>Set this attribute to <i>private</i> for line appearances that appear only on this phone.</p> <p>Set this attribute to <i>shared</i> for shared line appearances.</p>
reg.x.thirdpartyname	<p>Set this attribute to a string in the same format as <i>reg.x.address</i>.</p> <p>On the primary station, this attribute matches the <i>reg.x.address</i> for the primary station.</p> <p>On the secondary station, this attribute also matches the <i>reg.x.address</i> for the primary station.</p>
reg.x.lineKeys	<p>This attribute defines the number of line appearances on this phone which are associated with this address (the number of line keys on the phone associated with this registration.)</p> <p>Set this attribute from 1 to the maximum number of line keys on the phone.</p>
reg.x.callsPerLineKey	<p>This attribute defines the number of concurrent calls or conferences that can be active or on hold for each line key on the phone.</p> <p>Set this attribute to blank on the individual phones. Use the <b>Call Appearances</b> setting in Interaction Administrator to specify this value. For more information, see <a href="#">Call Appearances</a>.</p>


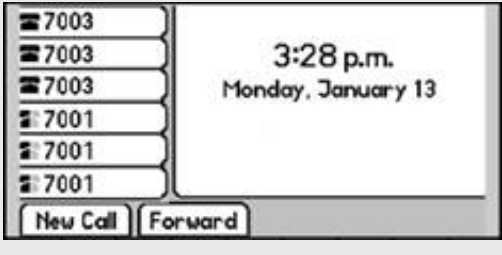
## Polycom SLA settings examples

In the following examples, the primary station configuration has one shared line that appears on three line keys (three shared line appearances). Configuration of the secondary station describes three line appearances of the private line for the assistant in the *reg.1* attributes and three shared line appearances in the *reg.2* attributes.

Primary Station	Secondary Station
<pre>reg.1.displayName="7001" reg.1.address="7001" reg.1.label="7001" reg.1.type="shared" reg.1.thirdPartyName="7001" reg.1.auth.userId="" reg.1.auth.password="" reg.1.server.1.address="172.18.24.58" reg.1.server.1.port="5060" reg.1.server.1.transport="UDPonly" reg.1.server.1.expires="" reg.1.server.1.register="" reg.1.server.1.retryTimeOut="" reg.1.server.1.retryMaxCount="" reg.1.server.1.expires.lineSeize="" reg.1.acd-login-logout="0" reg.1.acd-agent- available="0" reg.1.ringType="6" reg.1.lineKeys="3" reg.1.callsPerLineKey=""</pre>	<pre>reg.1.displayName="7003" reg.1.address="7003" reg.1.label="7003" reg.1.type="private" reg.1.thirdPartyName="" reg.1.auth.userId="" reg.1.auth.password="" reg.1.server.1.address="172.18.24.58" reg.1.server.1.port="5060" reg.1.server.1.transport="UDPonly" reg.1.server.1.expires="" reg.1.server.1.register="" reg.1.server.1.retryTimeOut="" reg.1.server.1.retryMaxCount="" reg.1.server.1.expires.lineSeize="" reg.1.acd-login- logout="0" reg.1.acd-agent-available="0" reg.1.ringType="2" reg.1.lineKeys="3" reg.1.callsPerLineKey="1" reg.2.displayName="70011" reg.2.address="70011" reg.2.label="7001" reg.2.type="shared" reg.2.thirdPartyName="7001" reg.2.auth.userId="" reg.2.auth.password="" reg.2.server.1.address="172.18.24.58" reg.2.server.1.port="5060" reg.2.server.1.transport="UDPonly" reg.2.server.1.expires="" reg.2.server.1.register="" reg.2.server.1.retryTimeOut="" reg.2.server.1.retryMaxCount="" reg.2.server.1.expires.lineSeize="" reg.2.acd-login- logout="0" reg.2.acd-agent-available="0" reg.2.ringType="2" reg.2.lineKeys="3" reg.2.callsPerLineKey=""</pre>

## Polycom display examples

Following are examples of the Polycom phone displays that are the result of the preceding settings examples. The appearances vary depending on the phone model.

Primary station	Secondary station
	
<p>This example shows the three shared lines as they would appear on a Polycom SoundPoint IP 500 SIP display.</p>	<p>This example shows the three private lines and three shared lines as they would appear on a Polycom SoundPoint IP 600 SIP display.</p>

## Set the Number of Call Appearances

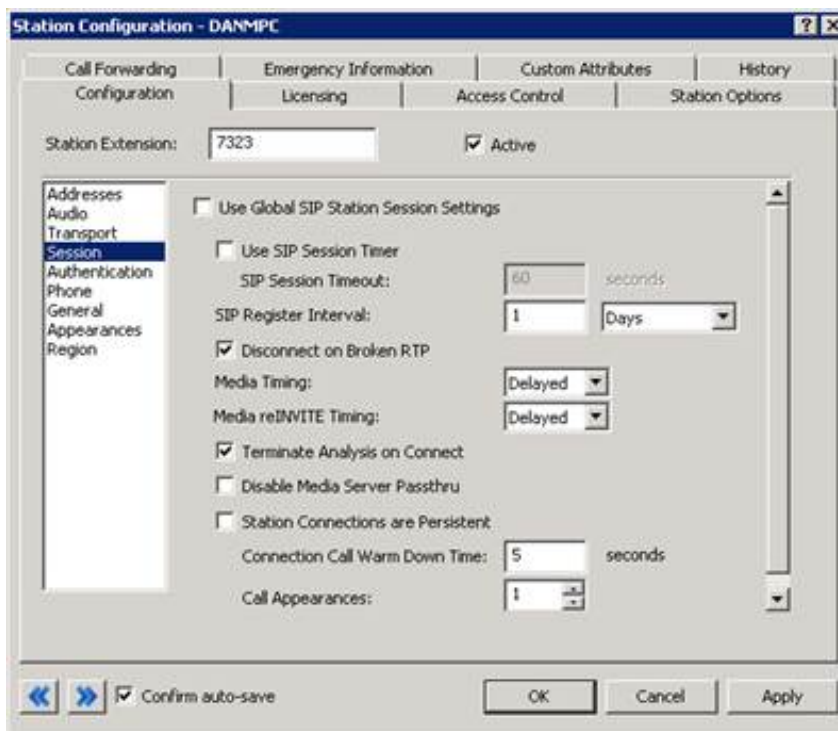
Polycom SoundPoint® IP phones support multiple calls for each line key. You can define the number of concurrent calls or conferences that can be active or on hold for each line key on the phone.

**Note:** Users can employ the Hold feature to pause activity on one call and switch to another call on the same line. The maximum number of calls for each line key varies by phone model. For more information, see the most recent version of your *Polycom Administrator Guide SoundPoint®/SoundStation® IP SIP*.

The following steps describe how to set the number of call appearances for each line key for a particular phone.

### To set the number of call appearances

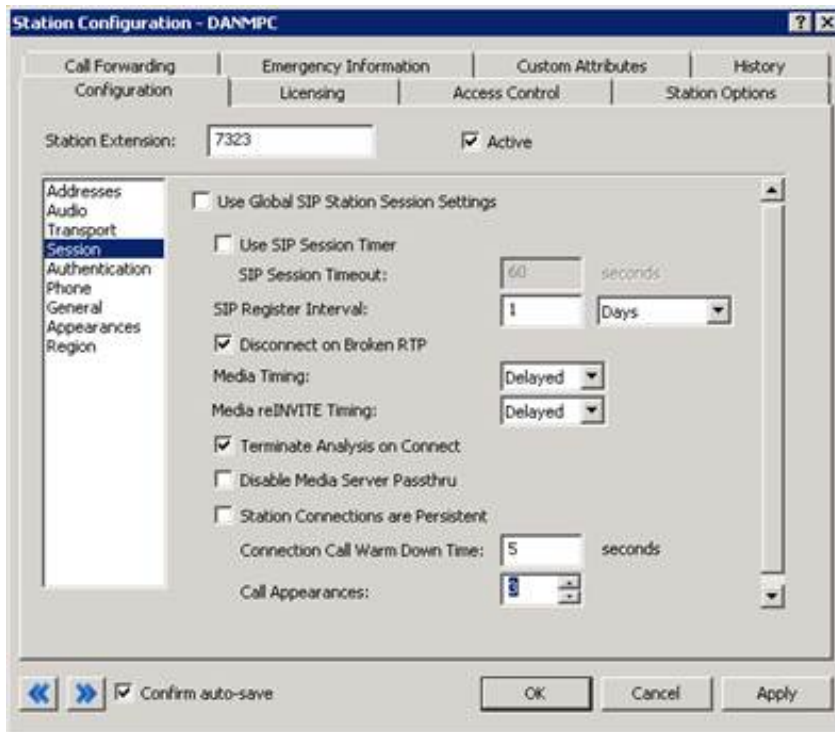
1. In Interaction Administrator, in the **Stations** container, select the station that corresponds to the phone you are configuring.
2. Right-click on the station name and select **Properties**. The **Station Configuration** dialog box appears.
3. Select the **Configuration** tab and then select **Session**.
4. Clear the **Use Global SIP Station Session Settings** check box.



**Note:** This selection prevents the phone from inheriting the SIP Session settings defined at the Station Space level. And then you can set unique values for this station.

5. In **Call Appearances**, set the number of appearances for each line key.

**Note:** The maximum number of calls for each line key varies by phone model. For more information, see the most recent version of your *Polycom Administrator Guide SoundPoint@/SoundStation@ IP SIP*.



6. Click **Apply** to save the settings.
7. Click **OK** to close the **Station Configuration** dialog box.

# Call Park

Users can employ Call Park to place the current call on hold in a specific orbit. An orbit can hold one call. The user who puts a call in orbit assigns the orbit a number. And then any user can pick up that call from another station.

While on a connected call, a user can press the call park soft key and type an orbit number. If that orbit is vacant, the system holds the call and removes it from the queue for the user. To pick up the call, a user presses the call park soft key and presses the orbit number.

Using other IVR digit sequences, users can also play a list of all the calls in orbit or hear details about a selected call in a specific orbit.

**Note:** The Call Park feature is available for managed phones.

## Polycom configuration settings for Call Park

Make *Call Park* and *Call Retrieval* available by setting the `enabled` attribute for the `call-park` feature to 1 in the **Feature** (`<feature/>`) section of the `xIC.cfg` file.

```
<feature
...
feature.11.name="call-park" feature.11.enabled="1"
```

**Note:** In preceding example, Call Park is feature "11". Feature numbers vary by release. For more information, see your *Polycom Administrator Guide SoundPoint@/SoundStation@ IP SIP*.

## Interaction Administrator configuration settings for Call Park

No Interaction Administrator configuration settings are required for Call Park.

# Group Call Pickup

Group Call Pickup allows a user to answer an alerting call on any phone in their station group. The user does not need to know the extension number of the ringing phone, but can press the Pickup and Group soft keys.

**Note:** A phone can belong to more than one station group. If calls are ringing on multiple station groups, a user picks up the *oldest* station group call from a station belonging to multiple groups.

## Polycom configuration settings for Group Call Pickup

Make Group Call Pickup available by setting the `enabled` attribute for the `group-call-pickup` feature to `1` in the **Feature** (`<feature/>`) section of the `xIC.cfg` file.

```
<feature
...
  feature.12.name="group-call-pickup"

feature.12.enabled="1"
```

## Interaction Administrator configuration settings for Group Call Pickup

Group call pickup applies to phones (stations) in the same station group. You can use existing station groups or create new ones for group call pickup. For more information about station group configuration, see the [Interaction Administrator Help](#).

# Zone Page

Make Zone page allows a user to make a live, one-way broadcast to a small, selected group of phones.

A user dials a short sequence of numbers (\*901 + zone number) to start a zone page. After hearing a beep, the user speaks into the handset to begin the page. The zone page recipients hear it through the speakers on their phones and do not have to pick up a handset.

**Note:** The Zone Page feature is automatically available for managed phones. However, to use these extensions as zone numbers, you need to configure CIC station group extensions, workgroup extensions, user extensions, or station extensions in Interaction Administrator.

Other zone page features include:

- Zone numbers are CIC station group extensions, workgroup extensions, user extensions, or station extensions.
- A zone page cannot interrupt another zone page. If a phone is playing a page and someone attempts to page a group that includes that phone, the phone does not interrupt the first page for the second page.
- If an intended recipient is already using the phone at the start of a zone page, the zone page does not play on the speaker for that phone.

## Limitations

Zone page is supported only on Polycom phones.

At sites with poor network performance, a significant delay can occur before some stations receive the page. In an environment where the listener can hear more than one phone at a time, a noticeable echo between the broadcasting phones can occur.

Zone paging causes the phones to go "off hook" before accepting the page. The more phones there are in a zone, the greater the delay before the page is broadcast. Zone paging is not intended for live paging to an entire organization. It is intended for paging to a small geographical zone in the office or to a small group.

## Polycom configuration settings for Zone Page

To receive a zone page, the phones must go *off hook* automatically. Configure this setting in the **Alert Information** (<alertInfo/>) section of the `xIC.cfg` file. The `alertInfo` value is a string that is compared against the `Alert-Info` value in the SIP message header. If there is a match, the behavior described in the ring class occurs. Ring class 3 auto-answers the incoming call.

In the `xIC.cfg` file, set the `alertInfo` value to `http://localhost/AutoAnswer` and its class to 3.

```
<voIPProt
<SIP
<alertInfo VoIpProt.SIP.alertInfo.1.value="<http://localhost/AutoAnswer>"
```

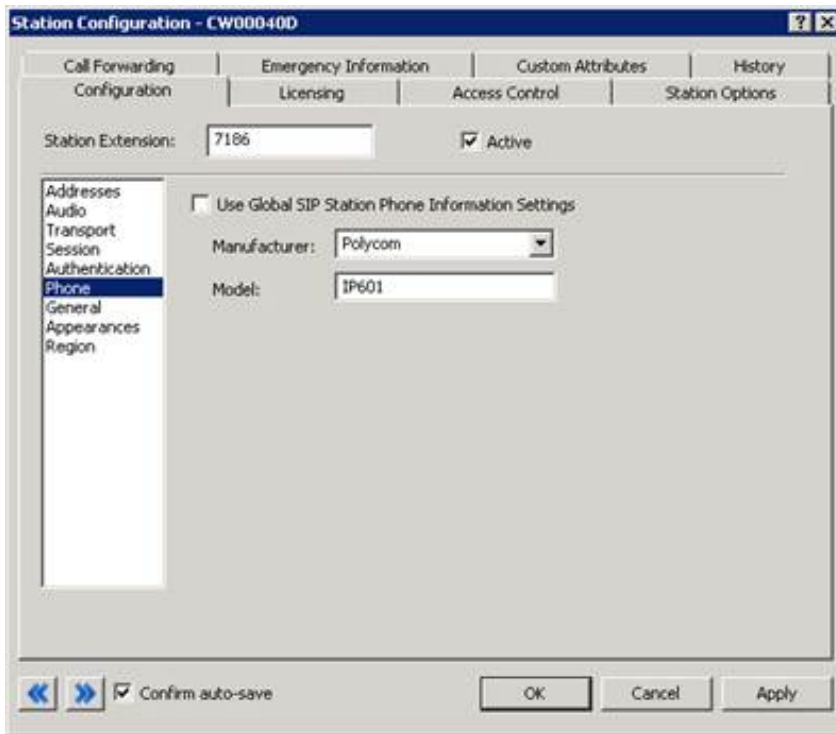
```
voIpProt.SIP.alertInfo.1.class="3" />
```

## Interaction Administrator configuration settings for Zone Page

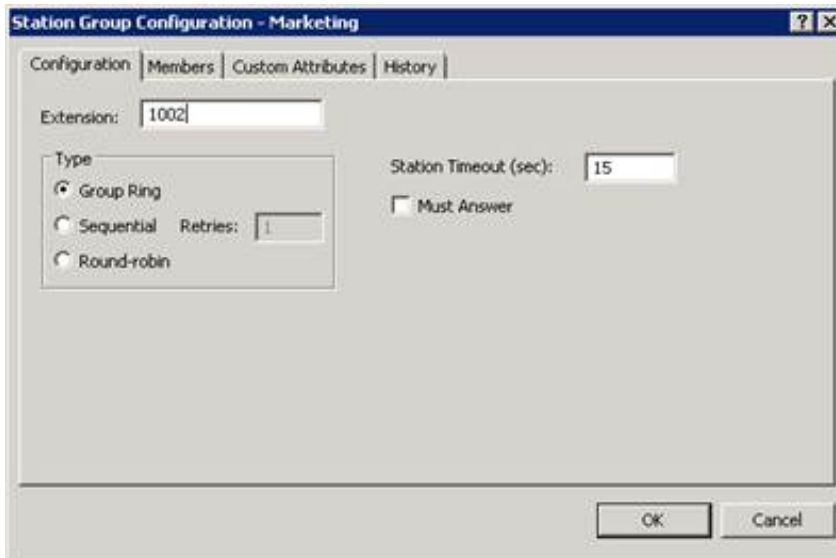
On the **Phone** page in the **Configuration** tab of **Station Configuration**, set **Manufacturer** to **Polycom** and **Model** to the appropriate Polycom model number. This configuration makes auto answer work with zone page and dialing through the CIC client.

Setting **Manufacturer** to **Polycom** instructs CIC to include an `Alert-Info` field in the SIP header. The value of `Alert-Info` is set to `http://localhost/AutoAnswer`.





Because zone numbers are CIC station group extensions, workgroup extensions, user extensions, or station extensions, you do not need to create special zone numbers in order to use zone paging. For example, you can create station groups that correspond to physical locations (zones) in your office and add or delete members. For more information about maintaining the appropriate extensions, see the [Interaction Administrator Help](#). Ensure that you specify an extension for any group that you intend to page.



## \*90x Dialing Options

CIC provides SIP business features that are used by pressing \*90 and a feature number on the telephone dialing pad. These features include:

*901	Page	Page a zone, station extension, station group extension, user extension, or workgroup extension. Press the complete sequence to bypass the prompt; for example, *901 1234 where 1234 is the zone number. The phone beeps to prompt you to start talking.
*902	Park a call	Park the active call in a specific orbit which places it on hold and removes it from your station. Press the complete sequence to bypass the prompt; for example, use *902 11 where 11 is the orbit number.
*903	Pick up a parked call	Pick up a parked call from any station. Press the complete sequence to bypass the prompt, for example, use *903 11 where 11 is the orbit number.
*904	List parked calls	Play a list of parked calls. Or you can press *904 <orbit number> to hear the orbit number, who the call is from, and how long the call has been on hold.
*905	Pick up a group call	Answer a call ringing on any extension in your group.

However, if you press the NewCall softkey on a Polycom phone and then start dialing, the phone immediately connects the call. This connection occurs after you press \* and before you can press the 9 and the rest of the string.

The phone administrator can modify the Digit Map in the Dial Plan map so that Polycom phones pause after NewCall is pressed and attempt to match any \*90x string. This pause is configured in the xIC.cfg file.

### To configure Polycom phones to allow users to type \*90x options

Add the following string to the dialplan.digitmap attribute in the xIC.cfg file:

```
|*T|*905|*90[1-4]x.T
```

*T	The phone accepts * after the digitmap timeout.
*905	The phone accepts *905 immediately.
*90[1-4]x.T	The phone accepts *901 - *904 and an optional set of digits.

For example, based on the default sip.cfg, the modified <dialplan> element would look like:

```
<dialplan
dialplan.impossibleMatchHandling="0"
dialplan.removeEndOfDial="1">
<digitmap dialplan.digitmap="[2-9]11|0T|011xxx.T|[0-1][2-9]xxxxxxxx|[2-9]xxxxxxxx|[2-9]xxxT|*T|*905[1-4]x.T"
dialplan.digitmap.timeOut="3"/>
```

For more information, see section "4.6.1.2.1 Digit Map <digitmap/>" in your *Polycom Administrator Guide*.

# Change Log

The following table lists the changes to the *Configuration of CIC Phone Features for Polycom Phones Technical Reference* since its initial release.

Date	Changes
31-July-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 Interactive Intelligence Product Information site URLs, and copyright and trademark information.
31-March-2015	Updated document to reflect the changes required for the transition from Interaction Client .NET Edition to Interaction Desktop. This includes a new CIC client section. Updated the Copyright and Trademarks page.
25-June-2015	Rebranding changes, new logo and font colors. Updated Copyright and Trademark Information page.
28-July-2015	<ul style="list-style-type: none"> <li>• IC-131357 Make rebranding changes in technical references</li> <li>• In the CIC client section:               <ul style="list-style-type: none"> <li>◦ Removed all references to Interaction Client .NET Edition. (This is no longer distributed.)</li> <li>◦ Removed from boilerplate: Starting with CIC 2015 R3, Interaction Desktop replaces Interaction Client .NET Edition as the primary CIC client.</li> </ul> </li> <li>• In IP Phone Configurator section, changed IP Phone Configuration documentation URL,               <ul style="list-style-type: none"> <li>◦ FROM: It is available under Polycom Related Files on the SIP-Related Download Files page on the Interactive Intelligence Support website: <a href="https://my.inin.com/products/sip-platforms/Pages/SIP-Related-Download-Files.aspx#polycomrelatedfiles">https://my.inin.com/products/sip-platforms/Pages/SIP-Related-Download-Files.aspx#polycomrelatedfiles</a>.</li> <li>◦ TO: See Download the IP Phone Configurator utility under Polycom Related Files on the SIP-Related Download Files page on the Interactive Intelligence Product &amp; Support Information website: <a href="https://my.inin.com/products/sip-platforms/Pages/SIP-Related-Download-Files.aspx">https://my.inin.com/products/sip-platforms/Pages/SIP-Related-Download-Files.aspx</a>.</li> </ul> </li> <li>• In the Configuring the TFTP Server section,               <ul style="list-style-type: none"> <li>◦ In step 2, changed OK to Log In.</li> <li>◦ Updated screen capture of login dialog box.</li> <li>◦ Updated screen capture of and of result.</li> </ul> </li> <li>• In the Monitoring TFTP Server Activities section,               <ul style="list-style-type: none"> <li>◦ Updated screen capture of Server Activity Page.</li> </ul> </li> <li>• In the Configuring the TFTP Server section               <ul style="list-style-type: none"> <li>◦ Updated screen capture of Server Parameters page.</li> </ul> </li> <li>• In the Changing the TFTP Server Login Credentials section               <ul style="list-style-type: none"> <li>◦ Updated screen capture of Change Login Credentials page.</li> </ul> </li> <li>• Verified IA screen captures are accurate in:               <ul style="list-style-type: none"> <li>◦ Interaction Administrator primary station configuration</li> <li>◦ Interaction Administrator secondary station configuration</li> <li>◦ Call Appearances</li> <li>◦ Interaction Administrator configuration settings for Zone Page</li> </ul> </li> </ul>
07-April-2017	Removed reference to Interaction Client Web Edition. Updated copyright page.
21-September-2017	Rebranded to Genesys.
19-March-2018	Updated document to new format.
08-May-2019	Reorganized the content only, which included combining some topics and deleting others that just had an introductory sentence such as, "In this section..."
10-September-2019	Added link to instructions on how to auto-provision supported Polycom IP phones or SIP Soft Phones automatically in <a href="#">Introduction to CIC Phone Features Configuration for Polycom Phones</a> .
13-May-2020	Update or remove links to "my.inin.com" as appropriate.