PRIVACY GUIDE | May 2020 | 3725-86489-001A

Poly Trio Conferencing Series

Getting Help
For more information about installing, configuring, and administering Poly/Polycom products or services, go to Polycom Support.

Plantronics, Inc. (Poly — formerly Plantronics and Polycom)
345 Encinal Street
Santa Cruz, California
95060

Contents

Before You Begin

Topics:

The Poly Trio system Privacy Guide provides information on how Poly products utilize customer data and how customers can configure Poly Trio systems to process personal data.

Related Poly and Partner Resources

See the following sites for information related to this product.

- The Polycom Support Site is the entry point to online product, service, and solution support information including **Licensing & Product Registration**, **Self-Service**, **Account Management**, **Product-Related Legal Notices**, and **Documents & Software** downloads.
- The Polycom Document Library provides support documentation for active products, services, and solutions. The documentation displays in responsive HTML5 format so that you can easily access and view installation, configuration, or administration content from any online device.
- The Polycom Community provides access to the latest developer and support information. Create an account to access Poly support personnel and participate in developer and support forums. You can find the latest information on hardware, software, and partner solutions topics, share ideas, and solve problems with your colleagues.
- The Polycom Partner Network are industry leaders who natively integrate the Poly standards-based RealPresence Platform with their customers' current UC infrastructures, making it easy for you to communicate face-to-face with the applications and devices you use every day.
- The Polycom Collaboration Services help your business succeed and get the most out of your investment through the benefits of collaboration.

Privacy-Related Options

Topics:

There are different deployment options for your phone, which may affect the privacy options and supporting requirements described in this guide. These details apply specifically to a phone deployed in a customer premises and managed by the customer.

Note: Poly Trio systems also support integration with certain third-party applications, which may result in one of these applications processing personal data. Please carefully review all security and privacy information provided by the applicable vendor prior to using their applications on Poly Trio systems.

System Usage Data Collected by Poly

Poly automatically collects and analyzes product usage data, device data, call detail records (CDRs), and quality of service (QoS) data from your system.

Data collected is used for the purposes of license verifications, product improvements, support operations, improving overall user experience, and future product innovations.

The system sends the following information to Poly:

- Device information, including the hardware and software versions of primary and secondary devices
- Device health data, including CPU and memory usage
- Call experience statistics
- Call detail record (CDR) and call health
- Device-level network analytics
- Data and statistics related to device or feature usage

Disable System Usage Data Collection

You can stop Poly Trio from sending system usage data to Poly.

Procedure

- **»** Set the following parameters to disable data collection:
  - `feature.pcc.enabled` **=** `0`
  - `feature.da.enabled` **=** `0`

Administrator and User Passwords

Administrator and user passwords control two levels of access to certain configuration menus in your Poly Trio system.

The administrator password grants full access to all configuration settings available on your system, and the user password grants limited access to configuration settings.

When you first power on a new Poly Trio system or following a factory reset, the system displays a message prompting you to change the default administrator password. You must change the default administrator password to a unique password to access the Poly Trio local interface and system web interface. You can’t use the default administrator password again.

You must have a user or administrator password before you can access certain menu options on the phone and in the system web interface. The default passwords are:

- Administrator password: `456`
- User password: `123`

You can change the default password using any of the following methods:

- The pop-up prompt when the phone first registers
- Phone menu
- System web interface (default user password only)
- Use the parameter `reg.1.auth.password`

You can use an administrator password where a user password is required to see all the user options. While you can use the user password where the administrator password is required, the phone displays a limited set of menu options. Note that the system web interface displays different features and options depending on which password you use.

Each time you connect a Poly Trio system with a Poly Trio Visual+ accessory, the Visual+ user password is reset to match the Poly Trio system user password. You can change the Poly Trio Visual+ password on the Poly Trio local interface or the system web interface.

When you set the **Base Profile** to `SkypeUSB`, you can set the keyboard entry mode for the password in the **Advanced** menu on the phone.

Change the Administrator Password on the Phone Menu

If the Poly Trio system uses the default administrator password, you can't use the local interface or the system web interface until you change it.

Procedure

1. On the phone, go to **Settings** > **Advanced** and enter the current administrator password.
2. Select **Change Admin Password**.
3. Enter the current password, enter a new password, and confirm the new password.

   Passwords can contain uppercase and lowercase letters, numerals, and special characters (`!, #, %, $,` etc.).

   Passwords cannot contain non-ASCII characters (`Ã, ç, ë,` etc.) or chevrons (`<, >`).

Change the User Password on the System

You can change the user password at any time from the **Advanced** settings menu.

Procedure

1. On the phone, go to **Settings** > **Advanced**.
2. Enter your user password and select **Enter**.
3. Select **Change User Password**.
4. On the **Change User Password** screen, enter your old and new user password and select **Enter**.

   Passwords can contain uppercase and lowercase letters, numerals, and special characters (`!, #, %, $,` etc.).

   Passwords cannot contain non-ASCII characters (`Ã, ç, ë,` etc.) or chevrons (`<, >`).

Change the Administrator Password in the System Web Interface

You can change the administrator password on a per-phone basis using the system web interface.

If the default administrator password is in use, you can't use the system web interface.

Procedure

1. Enter your phone's IP address into a web browser.
2. Select **Admin** as the login type, enter the administrator password, and click **Submit**.
3. Select **Settings** > **Change Password**.
4. Select **Admin**.
5. Enter the current password into the **Old Password** field.
6. Enter the **New Password** and confirm it.

   Passwords can contain uppercase and lowercase letters, numerals, and special characters (`!, #, %, $,` etc.).

   Passwords cannot contain non-ASCII characters (`Ã, ç, ë,` etc.) or chevrons (`<, >`).
7. Select **Save**.

Change the User Password in the System Web Interface

You can change the user password on a per-phone basis using the system web interface.

Procedure

1. Enter your phone's IP address into a web browser.
2. Select **Admin** as the login type, enter the administrator password, and click **Submit**.

3. Select **Settings** > **Change Password**.
4. Select **User**.
5. Enter the **New Password** and confirm it.

   Passwords can contain uppercase and lowercase letters, numerals, and special characters (`!, #, %, $,` etc.).

   Passwords cannot contain non-ASCII characters (`Ã, ç, ë,` etc.) or chevrons (`<, >`).
6. Select **Save**.

Administrator and User Password Parameters

Use the following parameters to set the administrator and user password and configure password settings.

`sec.pwd.length.admin`

The minimum character length for administrator passwords changed using the phone. Use 0 to allow null passwords.

1 (default)

0 -32

Change causes system to restart or reboot.

`sec.pwd.length.user`

The minimum character length for user passwords changed using the phone. Use 0 to allow null passwords.

2 (default)

0 -32

Change causes system to restart or reboot.

`up.echoPasswordDigits`

1 (default) The phone briefly displays password characters before masking them with an asterisk.

0 - The phone displays only asterisks for the password characters.

`device.auth.localAdminPassword`

Specify a local administrator password.

0 - 32 characters

You must use this parameter with: `device.auth.localAdminPassword.set="1"`

`device.auth.localAdminPassword.set`

0 (default) - Disables overwriting the local admin password when provisioning using a configuration file.

1 - Enables overwriting the local admin password when provisioning using a configuration file.

Encryption

Poly supports the use of encryption to protect configuration files and phone calls.

Encrypting Configuration Files

Download encrypted files from the provisioning server and encrypt files before uploading them to the provisioning server.

Encrypt configuration files from the system web interface and the local device interface. Determine whether encrypted files are the same as unencrypted files and use the Polycom Software Development Kit (SDK) to facilitate key generation.

Note: The master configuration file, contact directory files, and configuration override files can't be encrypted.

To encrypt and decrypt configuration files on a UNIX or Linux server, generate your own 32 hex-digit key, 128-bit key, or use the Polycom SDK.

Note: To request the SDK and quickly install the generated key, see *When Encrypting Polycom UC Software Configuration Files: Quick Tip 67442* at Polycom Engineering Advisories and Technical Notifications.

You can use the following parameters to set the key on the phone:

- `device.set`
- `device.sec.configEncryption.key`
- `device.sec.configEncryption.key.set`

If the phone doesn't have a key, download the key in plain text. To avoid security issues, use HTTPS to download the key file. Poly recommends that you name each key uniquely to help match the key with the encrypted files.

After encrypting a configuration file, it's useful to rename the file to avoid confusing it with the original version, for example, rename **site.cfg** to **site.enc**.

Note: If a phone can't decrypt a downloaded file, the phone logs the action, and an error message displays. The phone continues to do this until the provisioning server provides an encrypted file that can be read, an unencrypted file, or until the file is removed from the list in the master configuration file.

Change the Encryption Key on the Phone and Server

To maintain secure files, you can change the encryption key on the phones and the server.

You must update the files on the server to the new key or make the files available in unencrypted format. Updating to the new key requires that you decrypt the files with the old key, then re-encrypt it with the new key.

Procedure

1. Place all encrypted configuration files that you want to use with the new key on the provisioning server.

   The phone may reboot multiple times.
2. Put the new key into a configuration file that is in the list of files downloaded by the phone, specified in `000000000000.cfg` or `<MACaddress>.cfg`.
3. Use the `device.sec.configEncryption.key` parameter to specify the new key.
4. Provision the phone again so that it downloads the new key.

   Note: You may need to update configuration files, contact directory files, and configuration override files if they were already encrypted. You can delete configuration override files from the provisioning server so that the phone replaces them when it successfully boots.

   The phone automatically reboots another time to use the new key.

Configuration File Encryption Parameters

The following list provides the parameters you can use to encrypt your configuration files.

`device.sec.configEncryption.key`

Set the configuration encryption key used to encrypt configuration files.

string

Change causes system to restart or reboot.

`sec.encryption.upload.callLists`

0 (default) - The call list is uploaded without encryption.

1 - The call list is uploaded in encrypted form.

Change causes system to restart or reboot.

`sec.encryption.upload.config`

0 (default) - The file is uploaded without encryption and replaces the phone specific configuration file on the provisioning server.

1 - The file is uploaded in encrypted form and replaces the existing phone specific configuration file on the provisioning server.

`sec.encryption.upload.dir`

0 (default) - The contact directory is uploaded without encryption and replaces the phone specific contact directory on the provisioning server.

1 - The contact directory is uploaded in encrypted form and replaces the existing phone specific contact directory on the provisioning server.

Change causes system to restart or reboot.

sec.encryption.upload.overrides

0 (default) - The MAC address configuration file is uploaded without encryption and replaces the phone specific MAC address configuration file on the provisioning server.

1 - The MAC address configuration file is uploaded in encrypted form and replaces the existing phone specific MAC address configuration file on the provisioning server.

Local Contact Directory

Poly phones feature a contact directory file you can use to store frequently used contacts.

The UC Software package includes a template contact directory file named `000000000000-directory~.xml` that is loaded to the provisioning server the first time you boot up a phone with UC Software or when you reset the phone to factory default settings.

When you first boot the phone out of the box or when you reset the phone to factory default settings, the phone looks for contact directories in the following order:

- An internally stored local directory
- A personal `<MACaddress>-directory.xml` file
- A global `000000000000-directory.xml` file when the phone substitutes `<000000000000>` for its own MAC address.

In addition, make sure the `dir.local.readonly` parameter is enabled to restrict the users to modify speed dials.

Local Contact Directory Parameters

The following parameters configure the local contact directory.

dir.local.contacts.maxNum

Set the maximum number of contacts that can be stored in the Local Contact Directory. The maximum number varies by phone model, refer to section 'Maximum Capacity of the Local Contact Directory'.

- 2000 (default)
- Maximum 3000 contacts

Change causes system to restart or reboot.

dir.local.readonly

0 (default) - Disable read only protection of the local Contact Directory.

1 - Enable read-only protection of the local Contact Directory.

feature.directory.enabled

0 - The local contact directory is disabled when the Base Profile is set to Lync.

1 (default)- The local directory is enabled when the Base Profile is set to Lync.

dir.search.field

Specify whether to sort contact directory searches by first name or last name.

0 (default) - Last name.

1 - First name.

voIpProt.SIP.specialEvent.checkSync.downloadDirectory

0 (default) - The phone downloads updated directory files after receiving a checksync NOTIFY message.

1 - The phone downloads the updated directory files along with any software and configuration updates after receiving a checksync NOTIFY message. The files are downloaded when the phone restarts, reboots, or when the phone downloads any software or configuration updates.

Note: The parameter `hotelingMode.type` set to `2` or `3` overrides this parameter.

dir.local.passwordProtected

Specify whether you are prompted for an Admin/User password when adding, editing, or deleting contacts in the Contact Directory.

0 - Disabled (default)

1 - Enabled

feature.pauseAndWaitDigitEntryControl.enabled

1 (default) - Enable processing of control characters in the contact phone number field. When enabled, "," or "p" control characters cause a one second pause.

For example, "," or "p" control characters cause a one second pause. ";" or "w" control character cause a user prompt that allows a user-controlled wait. Subsequent digits entered to the contact field are dialed automatically.

0 - Disable processing of control characters.

up.regOnPhone

0 (default) – Contacts you assign to a line key display on the phone in the position assigned.

1 – Contacts you assign to a line key are pushed to the attached expansion module.

Change causes system to restart or reboot.

Creating Per-Phone Directory Files

To create a per-phone, personal directory file, replace <**000000000000**> in the global file name with the phone's MAC address: **<MACaddress** > **-directory.xml**.

Any changes users make to the contact directory from the phone are stored on the phone drive and uploaded to the provisioning server in the personal directory (**<MACaddress** > **-directory.xml**) file, which enables you to preserve a contact directory during reboots.

To create a global directory file that you can use to maintain the directory for all phones from the provisioning server, remove the tilde (~) from the template file name **000000000000-directory.xml**. When

you update the global directory file on the provisioning server, the updates are downloaded onto the phone and combined with the phone specific directory.

Maintaining Per-Phone Directory Files

Using the parameter `voIpProt.SIP.specialEvent.checkSync.downloadDirectory`, you can configure the phones to download updated directory files. The files are downloaded when the phone restarts, reboots, or when the phone downloads any software or configuration updates.

Any changes to either the global or personal directory files are reflected in the directory on the phone after a restarts. When merging the two files, the personal directory always takes precedence over the changes in the global directory. Thus, if a user modifies a contact from the global directory, the contact is saved in the personal directory file, and the contact from the global directory is ignored when the files are next uploaded.

The phone requests both the per-phone <MACaddress>-directory.xml and global contact directory 000000000000-directory.xml files and merges them for presentation to the user. If you created a per-phone <MACaddress>-directory.xml for a phone, and you want to use the 000000000000-directory.xml file, add the 000000000000-directory.xml file to the provisioning server and update the phone's configuration.

Note: You can duplicate contacts in the Contact Directory on phones registered with the Ribbon Communications server.

Note: To avoid users accidentally deleting the definitions in the contact directory, make the contact directory file read only.

Search for a Local Directory Contact

In the Local Directory, enter a search criteria to find your desired contact.

Procedure

1. Go to **Contacts** > **Local Directory**.
2. In the **Search** field, enter your contact's name.

Add a Contact to the Local Directory

When you add a contact to your local directory, you can choose how much information you want to enter for your contact. You're required to only enter a contact number for each new contact.

Note: You can add local directory favorites for your Poly Trio system. For details, refer to the *Poly Trio Solution User Guide* at Polycom Support.

Procedure

1. Go to **Local Directory** > **Add** ＋.
2. On the **Add Contact** screen, enter your contact's information in the available fields.
3. Select **Save**.
4. When Poly Trio is using , and you want to configure the contact format, do one of the following:
   - If the Poly Trio is using the Relay and is on line 2, the contact format should be `xxxx@sip.bjn.vc`. For more details, refer to the Configuration B topic in the *Polycom*

Interoperability Solution Guide at Polycom Support. Note that configuration files are also available on this web page.

- If the Poly Trio isn't using Exchange for Calendar and is on line 2, the contact format should be `xxxx@bjn.vc`. For more details, refer to the Configuration C topic in the *Polycom Interoperability Solution Guide* at Polycom Support. Note that configuration files are also available on this web page.

Local Directory Favorites

Favorites are the contacts in your local directory that you call most often.

Contacts that you add as favorites display on the **Home** screen. Only three favorites display onscreen at a time, however, you can swipe the screen from right to left to display additional favorites. Favorites also display at the top of the list of contacts in the **Local Directory**.

Add Favorites

Add any contact in the local directory as a favorite.

When you add a contact as a favorite, the contact displays on the **Home** screen.

Procedure

1. Go to **Contacts** > **Local Directory**.
2. Select a contact.
3. On the **Details** screen, select **Favorite** ★.

Remove a Favorite

Remove a favorite contact to make room for a new favorite.

Procedure

1. Go to **Contacts** > **Local Directory**.
2. Select a contact.
3. On the **Details** screen, select **Favorite** ★.

Speed Dials on Poly Trio Systems

You can link entries in the local contact directory to speed dial contacts to line keys on the Home screen to enable users to place calls quickly using dedicated speed dial buttons.

The number of supported speed dial entries varies by phone model

Speed Dial Index Ranges

Phone Model	Range
Poly Trio systems	1 - 20

Speed Dial Contacts Parameters

After setting up your per-phone directory file (**<MACaddress>-directory.xml**), enter a number in the speed dial `<sd>`field to display a contact directory entry as a speed dial contact on the phone. Speed dial entries automatically display on unused line keys on the phone and are assigned in numerical order.

On some call servers, enabling presence for an active speed dial contact displays that contact's status on the speed dial's line key label.

Use the parameter below, which identifies the directory XML file and the parameters you need to set up your speed dial contacts.

`dir.local.contacts.maxFavIx`

Configure the maximum number of speed dial contacts that can display on the Poly Trio Home screen.

Enter a speed dial index number in the <sd>x</sd> element in the <MAC address>-directory.xml file to display a contact directory entry as a speed dial key on the phone. Speed dial contacts are assigned to unused line keys and to entries in the phone's speed dial list in numerical order.

Corporate Directory

You can connect phones to a corporate directory server that supports the Lightweight Directory Access Protocol (LDAP), version 3.

After you set up the corporate directory on the phones, users can search for contacts in the directory, place calls to directory contacts, and save entries to the local contact directory on the phone.

Poly phones support corporate directories that support server-side sorting and those that do not. For servers that do not support server-side sorting, sorting is performed on the phone.

Note: Use corporate directories that have server-side sorting for better performance. Consult your LDAP administrator when making any configuration changes for the corporate directory. For more information on LDAP attributes, see RFC 4510 - Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map

---

Corporate Directory Parameters

Use the parameters in the following list to configure the corporate directory.

Note that the exact configuration of a corporate directory depends on the LDAP server you use.

Note: For detailed explanations and examples of all currently supported LDAP directories, see *Technical Bulletin 41137: Best Practices When Using Corporate Directory* on Polycom Phones at Polycom Engineering Advisories and Technical Notifications.

`dir.corp.address`

Set the IP address or hostname of the LDAP server interface to the corporate directory.

Null (default)

IP address

Hostname

FQDN

Change causes system to restart or reboot.

dir.corp.allowCredentialsFromUI.enabled

Enable or disable prompting users to enter LDAP credentials on the phone when accessing the Corporate Directory.

Note: Users are only prompted to enter their credentials when credentials are not added through configuration or after a login failure.

0 (default) – Disabled

1 – Enabled

dir.corp.alt.protocol

Set a directory protocol used to communicate to the corporate directory.

sopi (default)

UTF-8 encoding string

dir.corp.alt.transport

Choose a transport protocol used to communicate to the corporate directory.

TCP (default)

TLS

dir.corp.attribute.x.addstar

Determine if the wild-card character, asterisk(*), is appended to the LDAP query field.

0 - Wild-card character is not appended.

1 (default) - Wild-card character is appended.

Change causes system to restart or reboot.

dir.corp.attribute.x.filter

Set the filter string for this parameter, which is edited when searching.

Null (default)

UTF-8 encoding string

Change causes system to restart or reboot.

dir.corp.attribute.x.label

Enter the label that shows when data is displayed.

Null (default)

UTF-8 encoding string

Change causes system to restart or reboot.

dir.corp.attribute.x.name

Enter the name of the parameter to match on the server. Each name must be unique; however, a global address book entry can have multiple parameters with the same name. You can configure up to eight parameters (x = 1 to 8).

Null (default)

UTF-8 encoding string

Change causes system to restart or reboot.

dir.corp.attribute.x.searchable

Determine whether quick search on parameter x (if x is 2 or more) is enabled or disabled.

0 (default) - Disabled

1 - Enabled

Change causes system to restart or reboot.

dir.corp.attribute.x.sticky

Sets whether the filter string criteria for attribute x is reset or retained after a phone reboot. If you set an attribute to be sticky (set this parameter to 1), a '*' displays before the label of the attribute on the phone.

0 (default) – Reset after a phone reboot.

1 – Retain after a phone reboot.

Change causes system to restart or reboot.

dir.corp.attribute.x.type

Define how x is interpreted by the phone. Entries can have multiple parameters of the same type. If the user saves the entry to the local contact directory on the phone, first_name, last_name, and phone_number are copied. The user can place a call to the phone_number and SIP_address from the global address book directory.

first_name

last_name (default)

phone_number

SIP_address

H323_address URL

other

Change causes system to restart or reboot.

dir.corp.auth.useLoginCredentials

0 (default)

1

dir.corp.autoQuerySubmitTimeout

Set the timeout in seconds between when the user stops entering characters in the quick search and when the search query is automatically submitted.

0 (default)

0 - 60

Change causes system to restart or reboot.

dir.corp.backGroundSync

Determine if background downloading from the LDAP server is enabled or disabled.

0 (default) - Disabled

1 - Enabled

Change causes system to restart or reboot.

dir.corp.backGroundSync.period

Set the time in seconds the corporate directory cache is refreshed after the corporate directory feature has not been used for the specified period of time.

86400 (default)

3600 to 604800

Change causes system to restart or reboot.

dir.corp.baseDN

Enter the base domain name, which is the starting point for making queries on the LDAP server.

Null (default)

UTF-8 encoding string

Change causes system to restart or reboot.

dir.corp.bindOnInit

Enable or disabled use of bind authentication on initialization.

1 (default) - Enabled

0 - Disabled

Change causes system to restart or reboot.

dir.corp.cacheSize

Set the maximum number of entries that can be cached locally on the phone.

128 (default)

32 to 256

Change causes system to restart or reboot.

dir.corp.customError

Enter the error message to display on the phone when the LDAP server finds an error.

Null (default)

UTF-8 encoding string

dir.corp.domain

Enter the port that connects to the server if a full URL is not provided.

0 to 255

dir.corp.filterPrefix

Enter the predefined filter string for search queries.

(objectclass=person) (default)

UTF-8 encoding string

Change causes system to restart or reboot.

dir.corp.pageSize

Set the maximum number of entries requested from the corporate directory server with each query.

64 (default)

32 (default for Trio 8300)

8 to 64

Change causes system to restart or reboot.

dir.corp.password

Enter the password used to authenticate to the LDAP server.

Null (default)

UTF-8 encoding string

dir.corp.persistentCredentials

Enable to securely store and encrypt LDAP directory user credentials on the phone. Enable `dir.corp.allowCredentialsFromUI.enabled` to allow users to enter credentials on the phone.

Note: If you disable the feature after enabling it, then all the saved user credentials are deleted.

0 (default) - Disabled

1 - Enabled

dir.corp.port

Enter the port that connects to the server if a full URL is not provided.

389 (default for TCP)

636 (default for TLS)

0

Null

1 to 65535

Change causes system to restart or reboot.

dir.corp.querySupportedControlOnInit

Enable to make the phone make an initial query to check the status of the server when booting up.

0 - Disabled

1 (default) - Enabled

dir.corp.scope

sub (default) – a recursive search of all levels below the base domain name is performed.

one – a search of one level below the base domain name is performed.

base – a search at the base domain name level is performed.

Change causes system to restart or reboot.

dir.corp.serverSortNotSupported

0 (default) – The server supports server-side sorting.

1 – The server does not support server-side sorting, so the phone handles the sorting.

dir.corp.sortControl

Determine how a client can make queries and sort entries.

0 (default) – Leave sorting as negotiated between the client and server.

1 – Force sorting of queries, which causes excessive LDAP queries and should only be used to diagnose LDAP servers with sorting problems.

Change causes system to restart or reboot.

dir.corp.transport

Specify whether a TCP or TLS connection is made with the server if a full URL is not provided.

TCP (default)

TLS

Null

Change causes system to restart or reboot.

dir.corp.user

Enter the user name used to authenticate to the LDAP server.

Null (default)

UTF-8 encoding string

dir.corp.viewPersistence

0 (default) – The corporate directory search filters and browsing position are reset each time the user accesses the corporate directory.

1 – The search filters and browsing position from the previous session are displayed each time the user accesses the corporate directory.

Change causes system to restart or reboot.

dir.corp.vlv.allow

Determine whether virtual view list (VLV) queries are enabled and can be made if the LDAP server supports VLV.

0 (default)

1

Change causes system to restart or reboot.

dir.corp.vlv.sortOrder

Enter the list of parameters, in exact order, for the LDAP server to use when indexing. For example: `sn, givenName, telephoneNumber .`

Null (default)

list of parameters

Change causes system to restart or reboot.

feature.contacts.enabled

1 (default) - The Contacts icon displays on the Home screen, the global menu, and in the dialer.

0 - Disable display of the Contacts icon.

feature.corporateDirectory.enabled

0 (default) - The corporate directory feature is disabled and the icon is hidden.

1 (default) - The corporate directory is enabled and the icon shows.

Call Lists

The phone records and maintains user phone events to a call list, which contains call information such as remote party identification, time and date of the call, and call duration.

The list is stored on the provisioning server as an XML file named *<MACaddress>*`-calls.xml`. If you want to route the call list to another server, use the `CALL_LISTS_DIRECTORY` field in the master configuration file. All call lists are enabled by default.

The phone maintains all the calls in three separate user accessible call lists: Missed Calls, Received Calls, and Placed Calls. Users can clear lists manually on their phones, or delete individual records or all records in a group (for example, all missed calls).

Call List Parameters

Use the following parameters to configure call lists.

`callLists.collapseDuplicates`

Lync Base Profile - 0 (default)

Generic Base Profile - 1 (default)

1 - Consecutive incomplete calls to/from the same party and in the same direction are collapsed into one record in the calls list. The collapsed entry displays the number of consecutive calls.

0 - Each call is listed individually in the calls list.

`callLists.logConsultationCalls`

Lync Base Profile - 1 (default)

Generic Base Profile - 1 (default)

0 - Consultation calls not joined into a conference call aren't listed as separate calls in the calls list.

1 - Each consultation call is listed individually in the calls list.

`feature.callList.enabled`

1 (default) - Allows you to enable the missed, placed, and received call lists on all phone menus including the Home screen and dial pad.

0 - Disables all call lists.

`feature.callListMissed.enabled`

0 (Default) - The missed call list is disabled.

1 - The missed call list is enabled.

To enable the missed, placed, or received call lists, `feature.callList.enabled` must be enabled.

`feature.callListPlaced.enabled`

0 (Default) - The placed call list is disabled.

1 - The placed call list is enabled.

To enable the missed, placed, or received call lists, `feature.callList.enabled` must be enabled.

`feature.callListReceived.enabled`

0 (Default) - The received call list is disabled.

1 - The received call list is enabled.

To enable the missed, placed, or received call lists, `feature.callList.enabled` must be enabled.

`feature.exchangeCallLog.enabled`

If Base Profile is:

Generic - 0 (default)

Skype for Business - 1 (default)

1 - The Exchange call log feature is enabled, user call logs are synchronized with the server, and the user call history of Missed, Received, and outgoing calls can be retrieved on the phone.

You must also enable the parameter `feature.callList.enabled` to use the Exchange call log feature.

0 - The Exchange call log feature is disabled, the user call log history can't be retrieved from the Exchange server, and the phone generates call logs locally.

Call Log Elements and Attributes

The following table describes each element and attribute that displays in the call log.

You can place the elements and attributes in any order in your configuration file.

Call Log Elements and Attributes

Element	Permitted Values
direction Call direction with respect to the user.	In, Out
disposition Indicates what happened to the call. When a call entry is first created, the disposition is set to Partial.	Busy, Forwarded, Normal, Partial, Preempted, Rejected, RemotelyHandled, Transferred
line The line (or registration) index.	Positive integer
protocol The line protocol.	SIP or H323
startTime The start time of the call. For example: 2010-01-05T12:38:05 in local time.	String
duration The duration of the call, beginning when it is connected and ending when the call is terminated.For example: `PT1H10M59S` .	String

Element	Permitted Values
count The number of consecutive missed and abandoned calls from a call destination.	Positive Integer
destination The original destination of the call. For outgoing calls, this parameter designates the outgoing call destination; the name is initially supplied by the local phone (from the name field of a local contact entry) but may later be updated via call signaling. This field should be used for basic redial scenarios. For incoming calls, the called destination identifies the requested party, which may be different than any of the parties that are eventually connected (the destination may indicate a SIP URI which is different from any SIP URI assigned to any lines on the phone).	Address
source The source of the call (caller ID from the call recipient's perspective).	Address
Connection An array of connected parties in chronological order. As a call progresses, the connected party at the far end may change, for example, if the far end transfers the call to someone else. The connected element allows the progression of connected parties, when known, to be saved for later use. All calls that contain a connected state must have at least one connection element created.	Address
finalDestination The final connected party of a call that has been forwarded or transferred to a third party.	Address

Resetting Contacts and Recent Calls Lists on Your Phone

You can reset the Contacts list and Recent call lists stored locally on your phone to their default settings.

Procedure

1. On the phone, go to **Settings** > **Advanced**.
2. Enter the administrative password.
3. Select **Reset to defaults** > **Reset User Data**.
4. When prompted "Are you sure?", select **Yes**.

User Profiles

When you set up user profiles, you enable users to access their personal phone settings, including their contact directory, speed dials, and other phone settings from any phone on the network.

This feature is useful for remote and mobile workers who don’t have a dedicated work space and conduct their business in more than one location. This feature is also useful if an office has a common conference phone from which multiple users need to access their personal settings.

Note: You can configure all company phones so that anyone can call authorized and emergency numbers when not logged in to a phone. For more information, see `dialplan.routing.emergency.outboundIdentity`.

If you set up the user profile feature, users can do the following:

- Log in to a phone to access their personal phone settings using their user ID and password.
- Place a call to an authorized number from a phone that is logged out.
- Change their user password.
- Log out of a phone after they finish using it.

If a user changes any settings while logged in to a phone, the settings save and display the next time the user logs in to another phone. When a user logs out, the corresponding user options are cleared from the device until the user profile related configuration is enabled on the phone again.

User Profile Parameters

Before you configure user profiles, you must complete the following:

- Create a phone configuration file, or update an existing file, to enable the feature's settings.
- Create a user configuration file in the format <user>.cfg to specify the user's password, registration, and other user-specific settings that you want to define.

  Important: You can reset a user's password by removing the password parameter from the override file. This causes the phone to use the default password in the <user>.cfg file.

When you set up the user profile feature, you can set the following conditions:

- If users are required to always log in to use a phone and access their personal settings.
- If users are required to log in and have the option to use the phone as is without access to their personal settings.
- If users are automatically logged out of the phone when the phone restarts or reboots.
- If users remain logged in to the phone when the phone restarts or reboots.

Use the parameters in the following list to enable users to access their personal phone settings from any phone in the organization.

prov.login.automaticLogout

Specify the amount of time before a non-default user is logged out.

0 minutes (default)

0 to 46000 minutes

prov.login.defaultOnly

0 (default) - The phone cannot have users other than the default user.

1 - The phone can have users other than the default user.

prov.login.defaultPassword

Specify the default password for the default user.

NULL (default)

prov.login.defaultUser

Specify the name of the default user. If a value is present, the user is automatically logged in when the phone boots up and after another user logs out.

NULL (default)

prov.login.enabled

0 (default) - The user profile is disabled.

1 - The user profile feature is enabled.

prov.login.localPassword.hashed

0 (default) - The user's local password is formatted and validated as clear text.

1 - The user's local password is created and validated as a hashed value.

prov.login.localPassword

Specify the password used to validate the user login. The password is stored either as plain text or as an encrypted SHA1 hash.

123 (default)

prov.login.persistent

0 (default) - Users are logged out if the handset reboots.

1 - Users remain logged in when the phone reboots.

prov.login.required

Set whether the phone requires the user to log in to the phone to use it.

0 (default) - Login not required.

1 - Login is required.

prov.login.useProvAuth

0 (default) - The phone does not use server authentication.

1 - The phones use server authentication and user login credentials are used as provisioning server credentials.

voIpProt.SIP.specialEvent.checkSync.downloadCallList

0 (default) - The phone does not download the call list for the user after receiving a checksync event in the NOTIFY.

1 - The phone downloads the call list for the user after receiving a checksync event in the NOTIFY.

Remotely Logging Out Users

Note that if an unexpected reboot occurs while a user is logged in, the user is not logged out and the phone returns to the user profile after reboot.

If a user is not logged out from a phone and other users are not prevented from logging in, the user can ask the administrator to log out remotely. Administrators can log out a user remotely with a checksync event in the NOTIFY by setting the parameter `profileLogout=remote`.

User Profile Authentication

You can authenticate users with phone-based or server-based authentication methods.

Phone-based authentication authenticates credentials entered by the user against the credentials in the `<user>.cfg` file. Server-based authentication passes user credentials to the provisioning server for authentication.

User Profile Server Authentication

Instead of phone-based authentication of user profiles, you can authenticate user profiles using a server.

When you enable server authentication, you set up user accounts on the provisioning server and each user can authenticate their phone by entering correct server credentials.

The phone downloads log files (`app.log` and `boot.log`) from the generic profile on the provisioning server regardless of user logins.

Create a Generic Profile Using Server Authentication

Create a generic profile and generic credentials on the provisioning server when a user isn't logged into the phone.

If you enable server authentication of user profiles, the following parameters don't apply and you don't need to configure them:

- `prov.login.defaultUser`
- `prov.login.defaultPassword`
- `prov.login.defaultOnly`
- `prov.login.localPassword`
- `prov.login.localPassword.hashed`

Procedure

1. On the server, create an account and directory for the generic profile (for example, `Generic_Profile`).
2. In the **Generic_Profile** directory, create a configuration file for a generic profile the phone uses by default (for example, `genericprofile.cfg`).
3. In `genericprofile.cfg`, include registration and server details and set all phone feature parameters.

   You must set the following parameters to use server authentication:

   - `prov.login.enabled="1"`
   - `prov.login.useProvAuth="1"`
   - `prov.login.persistent="1"`

   Note: If you enable `prov.login.enabled=1` and don't enable `prov.login.useProvAuth=0`, users are authenticated by a match with credentials you store in the user configuration file *<user>*`.cfg`.

4. Create a master configuration file `000000000000.cfg` for all the phones, or a *<MACAddress>*`.cfg` for each phone, and add `genericprofile.cfg` to the **CONFIG_FILES** field.
5. Set the provisioning server address and provisioning server user name and password credentials for the generic user account on the phone at **Settings** > **Advanced** > **Provisioning Server** and inform users of their user profile credentials.

The following override files upload to the generic profile directory:

- Log files
- Local interface settings
- System web interface settings
- Call logs
- Contact directory file

Create a User Profile Using Server Authentication

Create a user profile in the `Home` directory of each user with a user-specific configuration file that you store on the provisioning server with a unique name as well as user-specific files such as settings, directory, and call lists.

When a user logs in with credentials, the phone downloads the user profile from the provisioning server. When the user logs out, the phone downloads the default user profile using the generic credentials.

Procedure

1. On the server, create an account and a directory for each user (for example, `User1`and `User2`).
2. In each user directory, create a configuration file for each user (for example, `User1.cfg` and `User2.cfg`), that contains the user's registration details and feature settings.

The following override files upload to the generic profile account on the server:

- Log files
- System web interface settings

The following override files upload to the user profile account on the server:

- Local interface settings
- Contact directory file

User Profile Phone Authentication

You can create default credentials and authenticate user profiles without using a server.

Create Default Credentials and a Profile for a Phone

You can choose to define default credentials for a phone, which the phone uses to automatically log itself in each time an actual user logs out or the phone restarts or reboots.

When the phone logs itself in using the default login credentials, a default phone profile displays, and users retain the option to log in and view their personal settings.

You can create a new phone configuration file for the default profile, then add and set the attributes for the feature. Or, you can update an existing phone configuration file to include the user login parameters you want to change.

Important: Poly recommends that you create a single default user password for all users.

Procedure

1. Add the `prov.login*` parameters you want to use to your configuration.
2. Set values for the user login parameters and save.

Create a User Configuration File

Create a configuration file for each user that you want to enable to log in to the phone.

Some things to note about user configuration files:

- If a user updates their password or other user-specific settings on the phone, the updates are stored in `<user>-phone.cfg`, not `<MACaddress>-phone.cfg`.
- If a user updates their contact directory while logged in to a phone, the updates are stored in `<user>-directory.xml`.
- Directory updates display each time the user logs in to a phone. For certain phones, an up-to-date call lists history is defined in `<user>-calls.xml`. This list is retained each time the user logs in to their phone.

The following list shows configuration parameter precedence (from first to last) for a phone with the user profile feature enabled:

1. `<user>-phone.cfg`
2. System web interface
3. Configuration files listed in the master configuration file (including `<user>.cfg`)
4. Default values

Note: To convert a phone-based deployment to a user-based deployment, copy the `<MACaddress>-phone.cfg` file to `<user>-phone.cfg` and copy `phoneConfig<MACaddress>.cfg` to `<user>.cfg`.

Procedure

1. On the provisioning server, create a user configuration file for each user. Specify the user's login ID in the name of the file.

   For example, if the user's login ID is *user100*, name the user configuration file `user100.cfg`
2. In each `<user>.cfg` file, you must add and set values for the user's login password.
3. Optional: Add and set values for any user-specific parameters you want to add:
   - Registration details, such as the number of lines the profile displays and line labels
   - Feature settings, such as microbrowser settings

Caution: If you add optional user-specific parameters to `<user>.cfg`, only add parameters that don't cause the phone to restart or reboot when the parameter is updated.

Download Logs

You can retrieve the logs associated with your Poly Trio system and some of its connected devices.

Procedure

1. In the system web interface, go to **Diagnostics** > **Logs**.
2. Select **Download Logs**.

   The log package, which includes call detail record (CDR) information, downloads as a `.tgz` file. The date and time of the log entries display in GMT.

Uploading Logs to a USB Flash Drive

You can configure your Poly Trio phone to copy application and boot logs to a USB flash drive connected to the phone. USB log collection is not supported on Poly Trio 8300.

Configure the phone to copy the application logs to the USB flash drive when the log file size reaches the limit defined in the `log.render.file.size` parameter. Similarly, you can configure the phone to copy application logs to the USB flash drive periodically using `log.render.file.upload.period` parameter.

USB Logging Parameter

The following parameters configure the USB logging feature.

`feature.usbLogging.enabled`

0 (default) - Disables collecting logs using a USB flash drive.

1 - Enables collecting logs using a USB flash drive.

How Data Subject Rights Are Supported

Topics:

The following information shows how data subject rights are supported.

Poly Trio systems also support integration with certain third-party applications which may result in one of these applications processing personal data. Please carefully review all security and privacy information that is provided by the applicable vendor prior to using their applications with Poly Trio systems.

Right to Access

A data subject has the right to view and/or obtain a copy of all of their own personal data.

Personal data about specific participants in conferences can be viewed or downloaded via the CDR.

For details about how to access personal data sent to Polycom RealPresence Resource Manager, see the User Data Collection section of the Polycom RealPresence Resource Manager Operations Guide.

To see details of the usage data sent to Poly, see the *Security and Privacy White Paper for Poly Trio Conferencing Series*.

See Download Logs on page 29.

See Uploading Logs to a USB Flash Drive on page 29.

Right to Be Informed

What personal data is collected?

See Purposes of Processing Personal Data on page 33.

How is personal data is used?

See Purposes of Processing Personal Data on page 33.

How long is personal data kept?

All data saved to the system is retained until manually deleted by the administrator. This includes saved content files, recent rooms information, and configuration settings. Log files are automatically deleted (oldest first) when the file limit is reached. By default, call detail records (CDRs) are overwritten by new CDR data via rolling logs configurable by the system administrator.

For details about how to access personal data sent to Polycom RealPresence Resource Manager, see the User Data Collection section of the *Polycom RealPresence Resource Manager Operations Guide*. To see details of the usage data sent to Poly, see the *Security and Privacy White Paper for Poly Trio Conferencing Series*.

See Purposes of Processing Personal Data on page 33 and How Personal Data is Deleted on page 35.

Is personal data shared with any third parties and if so, who?

If personal data is made available when working with Poly support, this data may be shared with Poly's engineering team (which may include third parties and contractors).

How can a data subject be notified of a data breach?

Data Subjects have a right to be notified when their data has been processed without authorization. Please contact your system administrator for the most appropriate method to receive this information.

See How Personal Data is Deleted on page 35 and How Administrators are Informed of Any Security Anomalies (Including Data Breaches) on page 34.

Right to Data Portability

A data subject has the right to receive a copy of all personal data in a commonly-used, machine-readable format.

- CDRs can be downloaded in CSV format.
- The Address Book can be exported in XML format.
- Audit and log files can be downloaded in plain text format.

For details about how to receive a copy of personal data sent to an optional provisioning server or device management service, please see the administrator's or privacy guide for the specific service being used.

See Download Logs on page 29.

See Uploading Logs to a USB Flash Drive on page 29.

Right to Erasure

A data subject has the right to remove all of his or her own personal data. A data subject may request deletion of their data, but based on the legal basis the controller employs, deletion may not be feasible in every case.

For details on how to erase customer personal data from the system, see How Personal Data is Deleted on page 35.

Any personal data made available when working with Poly support, specific to a support incident, is retained until the information is requested to be removed by the customer.

See Reset the Phone and Configuration on page 37.

Right to Rectification

A data subject has the right to make corrections to inaccurate or incomplete personal data.

Personal data specific to device configuration can be edited or updated by the device administrator.

Personal data about specific participants in conferences cannot be edited or updated because the information derives from the device of origin.

Poly does not manipulate data made available during the support process, so any rectification of inaccuracies of personal data must be performed by customer directly.

Right to Object to Processing

Not applicable.

Right to Restrict Processing

Not applicable.

Purposes of Processing Personal Data

For these details, see the *Security and Privacy White Paper for Poly Trio Conferencing Series*.

How Administrators are Informed of Any Security Anomalies (Including Data Breaches)

How Administrators are Informed of Any Security Anomalies

Security Anomaly Type	Where to Check	Recommended Frequency to Check
Critical events and login attempts	All critical system events and login attempts (both successful and unsuccessful) are written in the device log files, which can be reviewed by an administrator.	Once daily

How Personal Data is Deleted

How Customer Personal Data is Deleted

Data Type	Steps to Delete	Deletion Method
Call detail record (CDR)	▪ By default, CDRs are overwritten by new CDRs periodically via rolling logs configurable by device administrator. ▪ CDRs can also be deleted by performing a standard or comprehensive restore operation. ▪ User data may be reset by the Administrator from **Settings** > **Advanced** > **Reset to Defaults** > **Reset User Data**. ▪ See the "Resetting Contacts and Recent Call Lists" section in the *Poly Trio Solution Administrator Guide*. ▪ The contacts can also be deleted by resetting the system.	Simple delete on phone.
Directory/Contacts	▪ User data may be reset by the Administrator from **Settings** > **Advanced** > **Reset to Defaults** > **Reset User Data**. ▪ See the "Resetting Contacts and Recent Call Lists" section in the *Poly Trio Solution Administrator Guide*. ▪ The contacts can also be deleted by resetting the system.	Delete from database. File delete.
System log files	▪ Log files are automatically deleted by the system (oldest first) when the system reaches the file limit. These settings can be configured by the device administrator from **Diagnostics** > **Logs** > **Log Management**. ▪ Log files are also deleted by resetting the system.	Simple delete on phone.

Data Type	Steps to Delete	Deletion Method
All other personal data stored locally on the Poly Trio system	Factory reset system.	Simple delete on phone.

For details about how personal data is deleted on Polycom RealPresence Resource Manager, see the User Data Collection section of the Polycom RealPresence Resource Manager Operations Guide.

Reset the Phone and Configuration

Topics:

You can reset the phone and phone configuration partially or completely.

Procedure

1. On the phone's local interface, go to **Settings** > **Advanced** > **Administration Settings**.
2. Select **Reset to Defaults** and choose a reset option:
   - **Reset Local Configuration**
   - **Reset Web Configuration**
   - **Reset Device Settings**
   - **Format File System**
   - **Reset to Factory**

Reset to Factory Parameter

By default, only administrators can initiate a factory reset. However, you can make the **Reset to Factory** setting available to users.

`up.basicSettings.factoryResetEnabled`

0 (default) - Doesn't display the **Reset to Factory** option under **Basic** settings.

1 – Displays the **Reset to Factory** option under **Basic** settings.

`feature.restrictPerDataUploadMenu.enabled`

1 (default) Displays the **Restrict Personal Data Upload** menu under **Basic** settings.

0 - Doesn't display the **Reset to Factory** menu under **Basic** settings.

`feature.clearPerInfoMenu.enabled`

1 (default) - Displays the **Clear Personal Information** menu under **Basic** settings.

0 - Doesn't display the **Clear Personal Information** menu under **Basic** settings.