PRIVACY GUIDE | May 2021 | 3725-49732-002B

Poly VVX Business Media and IP Phones

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....3

Related Poly and Partner Resources....3

Privacy-Related Options....4

How to Control Your Personal Data....4

Device Analytics Settings....5

Call Data Record (CDR)....7

Provisioning Settings....8

Administrator and User Passwords....8

Change the Phone Default Administrator Password in Skype for Business....9

Change the Default Passwords in the System Web Interface....9

Administrator and User Password Parameters....9

Encryption....10

Encrypting Configuration Files....10

Configuration File Encryption Parameters....12

Local Contact Directory....12

Local Contact Directory Parameters....13

Creating Per-Phone Directory Files....14

Search for a Local Directory Contact....15

Add a Contact to the Local Directory....15

Corporate Directory Parameters....15

Call Lists....16

Call List Parameters....16

Call List Elements and Attributes....18

Resetting Contacts and Recent Calls Lists on Your Phone....19

Clear Uploaded Calls/Directory....20

User Profiles....20

User Profile Parameters....20

Remotely Logging Out Users....22

User Profile Authentication....22

Download Logs....25

Uploading Logs to a USB Flash Drive....26

USB Logging Parameter....26

How Data Subject Rights Are Supported....27

Right to Access....27

Right to Be Informed....27

Right to Data Portability..... 28
Right to Erasure..... 28
Right to Rectification..... 28

Purposes of Processing Personal Data..... 29

How Administrators are Informed of Any Security Anomalies (Including Data Breaches)..... 30

How Personal Data is Deleted..... 31

Resetting a Phone to Factory Defaults..... 32
Reset the Phone to Factory Defaults in Skype for Business..... 32
Reset to Default Settings..... 33
Reset to Factory Configuration Parameters..... 33

Before You Begin

Topics:

- Related Poly and Partner Resources

This Polycom VVX Business Media and IP Phone Privacy Guide provides information regarding the implementation of Privacy by Design for this product.

The terms “the phone” and “your phone” refer to any of the VVX business media and IP phones. Unless specifically noted in this guide all phone models operate in similar ways.

This guide contains details about configurable privacy options and how personal data is processed.

Related Poly and Partner Resources

See the following sites for information related to this product.

- The Poly Online Support Center is the entry point to online product, service, and solution support information including Video Tutorials, Documents & Software, Knowledge Base, Community Discussions, Poly University, and additional services.
- The Poly 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 Poly 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 Poly Partner Network is a program where resellers, distributors, solutions providers, and unified communications providers deliver high-value business solutions that meet critical customer needs, making it easy for you to communicate face-to-face using the applications and devices you use every day.
- The Poly Services help your business succeed and get the most out of your investment through the benefits of collaboration.

Privacy-Related Options

Topics:

- How to Control Your Personal Data
- Administrator and User Passwords
- Encryption
- Local Contact Directory
- Corporate Directory Parameters
- Call Lists
- Resetting Contacts and Recent Calls Lists on Your Phone
- Clear Uploaded Calls/Directory
- User Profiles
- Download Logs
- Uploading Logs to a USB Flash Drive

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 on the customer's premises and managed by the customer.

Related Links

Right to Rectification on page 28
Right to Access on page 27

How to Control Your Personal Data

By default, no device analytics data or identifiable personal data is sent to Poly. However, if you enable certain settings on your phone, it automatically sends device analytics data to a Poly device analytics service.

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

If configured the phone sends the following types of information to a Poly analytics service:

- 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

It’s important to understand your options for controlling what personal data is sent and when. The following sections provide configuration parameters that assist with this task.

Device Analytics Settings

The phone may be configured to send device analytics data to Poly if a customer has registered for a Poly device analytics service.

Note: These settings don't affect data used for provisioning purposes.

The following example shows a phone correctly configured to send all available device analytics data to Poly Lens analytics service:

- `feature.lens.enabled` = "1"
- `device.da.enabled.set` = "1"
- `device.da.enabled` = "1"
- `da.supported.services` = "all"

The following example shows a phone correctly configured to NOT send device analytics data to Poly Lens analytics service:

- `feature.lens.enabled` = "1"
- `device.da.enabled.set` = "1"
- `device.da.enabled` = "0"
- `da.supported.services` = "all"

Note: If you configure the `da.supported.services` parameter to send Call Detail Report (CDR) data to a Poly analytics service, only CDR is sent, not call lists.

Device Asset Details

Device asset details include details for a primary device, secondary device, and SIP service. A primary device consists of Poly phones, and a secondary device consists of Bluetooth or USB headsets, expansion modules (if supported), connected cameras, and a PC port.

When you enable device analytics, the phone sends the following primary device details to the cloud:

- Manufacturer
- Product Family
- Power Source
- MAC Address
- PCS Number
- PCS Account Code
- Region Code
- Version Information
- Hardware Model
- Hardware Revision
- Hardware Part number
- Serial Number
- OBi Number

- Offset GMT
- Reboot Type
- Mac Address
- Software Release
- Upload Time
- Updater Version

Device Analytics Parameters

Use the following parameters to configure device analytics. You can configure the device analytics feature to only enable services of your choice.

`feature.da.enabled`

0 (default) - Disable device analytics.

1 - Enable device analytics.

Change causes system to restart or reboot.

`device.da.enabled.set`

0 (default) - Don’t use the `device.da.enabled` value.

1 - Use the `device.da.enabled` value.

`device.da.enabled`

0 (default) – Disable the device analytics feature.

1 – Enable the device analytics feature.

Change causes system to restart or reboot.

`feature.obitalk.enabled`

0 (default) - Disable the connection to the OBiTALK cloud.

1 - Enable the connection to the OBiTALK cloud.

Change causes system to restart or reboot.

`obitalk.accountCode`

Null (default)

String (maximum of 256 characters).

Change causes system to restart or reboot.

`da.supported.services`

Specify the device analytics service to enable.

all (default)

Configure the following strings (maximum of 2048 characters) using a comma-separated list.

sdi

ni

service

tsid

pcap

log

config

core

vqmon

cdr

uptimeanalytics

hardwareanalytics

uianalytics

blf

sca

restart

reboot

resettofactory

restapi

Change causes system to restart or reboot.

`deviceAnalytics.note`

Sets the self-note value on the phone and sends to cloud with primary device information message.

Null (default)

String (maximum of 512 characters).

Call Data Record (CDR)

When the phone ends an active call and you set the `da.supported.services` parameter value to `all` or `cdr`, the phone sends following call summary details to the cloud:

- User
- Remote Party
- Call Direction
- Disconnect Information
- Start Time
- Call Duration
- Protocol Type
- Call Rate

- Call ID
- Remote Tag
- Local Tag
- OBi number

Related Links
Call Lists on page 16

Provisioning Settings

The phone may be configured to use a provisioning server. If a provisioning server is configured on the phone, call lists, directory, and device logs are sent to the server for secure backup by default.

Note: These parameters don't affect data used for device analytics purposes.

Restrict Upload of Call Lists and Directory

To prevent the upload of the call lists and directory to the provisioning server, set the following parameter:

- `feature.uploaddir.enabled` = "0"

To prevent the upload of device logs to the provisioning server, set the following parameter:

- `log.render.file` = "0"

To turn off all call lists so they're no longer written on the phone, set the following parameter:

- `feature.callList.enabled` = "0"

Administrator and User Passwords

You can change the default administrator and user passwords.

When you set the Base Profile to Skype for Business, the phone displays a message prompting you to change the default administrator password.

Poly strongly recommends that you change the phone's default administrator and user passwords. This phone's administrator and user passwords are separate from the Skype for Business user password. The default administrator password enables administrators to access advanced settings menu on the phone menu and to log in to a phone's system web interface as an administrator.

Poly UC Software version 6.3.0 and higher meet California SB-327 password mandates that require administrators to generate a new password before granting access to the system and the system web interface.

You can't use the default password as the newly generated password. If your phone uses the default administrator password, the system requires you to change it to a unique password following an update to UC Software 6.3.0 or higher.

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 (Web Configuration Utility)

- From the configuration files by `device.auth.localAdminPassword` = "<administrator password>" and `device.auth.localAdminPassword.set` = "1" parameters.

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

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

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.

Change the Phone Default Administrator Password in Skype for Business

Poly strongly recommends that you change the phone's default administrator password on the phone.

When registering Poly phones with Microsoft Skype for Business Server, a message displays on the phone screen prompting you to change the default password.

Procedure

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

Change the Default Passwords in the System Web Interface

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

Procedure

1. In your web browser, enter the phone's IP address into the URL field to access the system web interface.
2. Go to **Settings** > **Change Password**.
3. Update the passwords for the **Admin** and **User**.

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 Poly Software Development Kit (SDK) to facilitate key generation.

Note: The primary configuration file can’t be encrypted. You can encrypt the contact directory files and configuration override files. The local contact directory files and configuration override files can be encrypted using the `sec.encryption.upload.dir` and `sec.encryption.upload.overrides` parameters.

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 Poly SDK.

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

The Contact Directory is the central database for several phone features including speed dial, distinctive incoming call treatment, presence, and instant messaging.

You can configure the phones to hide the Contact Directory and Favorites options from all screens in the user interface on all phones. You can also set the local directory as read-only and restrict users from modifying the speed dials only.

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'.

VVX 101, 150, 201: Default 99 contacts, Maximum 99 contacts

VVX 3xx, 4xx, 5xx, 6xx, and business media phones and business IP phones: Default 500 contacts, Maximum 500 contacts

Change causes system to restart or reboot.

`dir.local.passwordProtected`

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

1 - Enables password protection of the local Contact Directory.

`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.

0 - The local contact directory is disabled.

1 (default) - The local contact directory is enabled.

`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.UIenabled

1 (default) - The Directory menus provide access to Favorites/Speed Dial and Contact Directory entries and display the Favorites quick access menu on the Home screen of the VVX 500/501 and 600/601 business media phones.

0 - The local Contact Directory and Favorites/Speed Dial menu entries aren't available. The Favorites quick access menu on the Home screen isn't available on the VVX 500/501 and 600/601 business media phones.

Set to 0 when `dir.local.readOnly` is set to 1 to add speed dials and macros on the phone and prevent user modification.

If your call control platform provides direct contact integration and you want to prevent any access to the local directory, set `feature.directory.enabled=0`.

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 restart. 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.

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**.

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 Poly 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.password`

Enter the password used to authenticate to the LDAP server.

Null (default)

UTF-8 encoding string

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.

Note: All details in this section of the guide refer to call lists, not CDR.

There are several similar terms related to call information stored on the phone, which have different meanings.

- Call detail record (CDR) refers to an archive of all previous calls and is only used for device analytics purposes. There's only one CDR per phone and it contains call information such as user, caller ID, and remote party name.
- Call lists contain different types of data than the CDR that are only used on the phone itself and with a provisioning server (if configured). The phone maintains all the calls in three separate user accessible call lists; Missed Calls, Received Calls, and Placed Calls. Call lists also contain additional information, such as the IP address, dial number, and/or SIP URI for local and remote calls.

Note: Other terms that should be interpreted as referring to call lists are call log and call history.

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 primary configuration file. All call lists are enabled by default.

Related Links

Call Data Record (CDR) on page 7

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 dialpad.

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 List Elements and Attributes

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

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

Call List 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
count The number of consecutive missed and abandoned calls from a call destination.	Positive Integer
destination	Address

Element	Permitted Values
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 that is different from any SIP URI assigned to any lines on the phone).	
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**.

Related Links

Right to Erasure on page 28

Clear Uploaded Calls/Directory

If the phone is configured to use a provisioning server, it uploads all call lists and directory for secure backup by default. You may clear call lists and directory entries from the phone itself. Additionally, to clear all call lists and directory entries from both the phone itself and from the provisioning server, use the following procedure:

Procedure

1. On the phone, go to **Settings** > **Basic** > **Clear Uploaded Calls/Directory**.
2. Select **Yes**.

Related Links

Right to Erasure on page 28

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 can't 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 doesn't 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 isn't logged out and the phone returns to the user profile after reboot.

If a user isn't logged out from a phone and other users aren't 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 primary 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**.

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 primary 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 phone 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. The log package doesn't include call lists, directory, or user profiles.

Related Links

Right to Data Portability on page 28
Right to Access on page 27
How Administrators are Informed of Any Security Anomalies (Including Data Breaches) on page 30

Uploading Logs to a USB Flash Drive

You can configure your phone to copy application and boot logs to a USB flash drive connected to the phone.

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.

Related Links

Right to Data Portability on page 28
Right to Access on page 27
How Administrators are Informed of Any Security Anomalies (Including Data Breaches) on page 30

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:

- Right to Access
- Right to Be Informed
- Right to Data Portability
- Right to Erasure
- Right to Rectification

Right to Access

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

Related Links

Uploading Logs to a USB Flash Drive on page 26
Download Logs on page 25
Privacy-Related Options on page 4

Right to Be Informed

What personal data is collected?

See the table, Purposes of Processing Personal Data on page 29.

How personal data is used?

See the table, Purposes of Processing Personal Data on page 29.

How long is personal data kept?

Any personal data made available when working with Poly support is only retained until each specific issue is resolved and then it's purged. Customer contact information is retained by Poly support until the support relationship ends or is requested to be removed by the customer.

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 / 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.

Right to Data Portability

Poly customers have a right to receive a copy of all personal data in a commonly used, machine-readable format.

Related Links

Uploading Logs to a USB Flash Drive on page 26
Download Logs on page 25

Right to Erasure

A data subject has the right to remove all personal data for a specific data subject.

Any personal data made available when working with Poly support is only retained until each specific issue is resolved and then it's purged. Customer contact information is retained by Poly support until the support relationship ends or is requested to be removed by the customer.

Related Links

How Personal Data is Deleted on page 31
Resetting a Phone to Factory Defaults on page 32
Resetting Contacts and Recent Calls Lists on Your Phone on page 19
Clear Uploaded Calls/Directory on page 20

Right to Rectification

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

Room data 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 sent to Poly support must be performed by customer directly.

Related Links

Privacy-Related Options on page 4

Purposes of Processing Personal Data

Refer to the Security and Privacy White Paper for Unified Communications Software for Polycom VVX Series at https://www.poly.com/us/en/legal/privacy/products.

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.

Related Links

Download Logs on page 25
Uploading Logs to a USB Flash Drive on page 26

How Personal Data is Deleted

Topics:

- Resetting a Phone to Factory Defaults

How Customer Personal Data is Deleted

Data Type	Steps to Delete	Deletion Method
Clear Uploaded Calls/Directory	▪ You can clear uploaded call lists and contacts from the provisioning server. ▪ On the phone, go to **Settings** > **Basic** > **Clear Uploaded Calls/ Directory**. Select **Yes**.	Simple delete on provisioning server.
Call lists and call detail record (CDR)	▪ By default, the CDR is overwritten by a new CDR periodically via rolling logs configurable by device administrator. ▪ Call lists and the CDR can be deleted by performing a standard or comprehensive restore operation. ▪ Call lists and the CDR may be reset by the Administrator from **Settings** > **Advanced** > **Administration Settings** > **Reset to Defaults** > **Reset User Data**. ▪ Note that in Skype for Business mode, as Poly doesn't control the call lists, Poly can't delete call lists in the same way as with OpenSIP. This is controlled by the Skype for Business server.	Simple delete on phone.
Directory/Contacts	▪ User data may be reset by the Administrator from **Settings** > **Advanced** > **Administration Settings** > **Reset to Defaults** > **Reset User Data**. ▪ The contacts can also be deleted by resetting the system.	Simple delete on phone.

Data Type	Steps to Delete	Deletion Method
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.	Delete from database and file delete.
All other personal data stored locally on the phone	Factory reset system.	Simple delete on phone.

Related Links

Right to Erasure on page 28

Resetting a Phone to Factory Defaults

You can reset the entire phone or some of the phone's configurations to factory defaults using the local interface.

The following list describes the different phone reset options and their effects.

- **Reset Local Configuration**: Clears the override file generated when you make changes using the phone's local interface.
- **Reset Web Configuration**: Clears the override file generated by changes made using the system web interface.
- **Reset Device Settings**: Resets the phone's flash file system settings that aren't stored in an override file. These settings are your network and provisioning server settings and include custom certificates and encryption keys. Local, web, and other configuration files remain intact.
- **Format File System**: Formats the phone's flash file system and deletes the software application, log, configuration, and override files. Note that if the override file is stored on the provisioning server, the phone redownloads the override file when you provision the phone again. Formatting the phone's file system doesn't delete those device settings affecting network and provisioning, and any certificates and encryption keys remain on the phone.
- **Reset to Factory**: Removes the web and local override files, any stored configuration files in the flash file system, as well as any custom certificates and encryption keys. All network and provisioning settings are reset but the UC Software application and updater remain intact.
- **Reset to Factory Partial**: Removes the web and local override files, any stored configuration files in the flash file system, as well as any custom certificates and encryption keys. All network and provisioning settings are reset but the UC Software application, updater, and administrator password remain intact.
- **Reset User Data**: Resets the call list and removes all contacts from the phone and server.
- **Out-of-Box Wizard**: Resets the selections made during the initial out-of-box setup wizard. You can then make the selections again, and the phone reboots.

Related Links

Right to Erasure on page 28

Reset the Phone to Factory Defaults in Skype for Business

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 Cloud Configuration**
   - **Reset Device Settings**
   - **Format File System**
   - **Reset to Factory**
   - **Reset to Factory Partial**
   - **Reset User Data**
   - **Out-of-box Wizard**

Reset to Default Settings

You can reset your phone settings to default using the Web Configuration Utility.

Procedure

1. Enter your phone's IP address into a web browser on your computer.
2. Select **Admin** as the login type, enter the admin password (the default is `456`), and click **Submit**.
3. Click **Simple Setup** and then click **Reset to Default**.

Reset to Factory Configuration Parameters

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.

`device.system.recoveryType`

Defines what settings the phone resets via MKC updater boot-up when a user tries a factory reset.

FullRecovery (default) - All settings are returned to factory default.

PreserveAdmin - All settings are returned to factory default except the administrator password.

CloudProv - All settings are returned to factory default except the administrator password and provisioning. Provisioning is changed to ZTP.