# Poly Edge E Series Phones

## Privacy Guide

Current as of PVOS 8.0.1 | October 2022 |
3725-47506-001A

# Before You Begin

This Poly Edge E Series phone provides information regarding the implementation of Privacy by Design for this product.

The terms “the phone” and “your phone” refer to any of the Poly Edge E Series 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.

- Poly Support is the entry point to online product, service, and solution support information. Find product-specific information such as Knowledge Base articles, Support Videos, Guide & Manuals, and Software Releases on the Products page, download software for desktop and mobile platforms from Downloads & Apps, and access additional services.
- The Poly Documentation 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.
- Poly Services help your business succeed and get the most out of your investment through the benefits of collaboration. Enhance collaboration for your employees by accessing Poly service solutions, including Support Services, Managed Services, Professional Services, and Training Services.
- With Poly+ you get exclusive premium features, insights and management tools necessary to keep employee devices up, running, and ready for action.
- Poly Lens enables better collaboration for every user in every workspace. It is designed to spotlight the health and efficiency of your spaces and devices by providing actionable insights and simplifying device management.

## Privacy Policy

Poly products and services process customer data in a manner consistent with the Poly Privacy Policy. Please direct comments or questions to privacy@poly.com.

# Privacy-Related Options

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.

**Note:** Poly Edge E Series devices 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 application with Poly Edge E Series.

## 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"
- feature.da.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"
- feature.da.enabled = "0"
- 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.da.enabled`**

1 (default) – Enable the Device Analytics feature.

0 – Disable the Device Analytics feature.

Change causes system to restart or reboot.

### feature.obitalk.enabled

0 (default) - Disable the connection to the OBiTALK (rebranded as Poly Device Management Service for Service Providers (PDMS-SP)) cloud.

1 - Enable the connection to the PDMS-SP 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

### 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"

## Phone Passwords

The default configuration includes administrative- and user-level access through the phone's local interface or the system web interface.

The administrator password grants full access to all configuration settings. The user password grants limited access to basic settings and preferences. The default passwords are:

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

### Configure Password Settings

Configure administrative and user password rules for your phone using a configuration file.

Make sure your configuration file includes `device.set="1"`.

**Important:** These settings override any locally set passwords.

**Note:** For each device parameter, be sure that your configuration file includes `device.x.set="1"` to allow the parameter to be written to the phone's flash.

**Task**

1. Open the configuration file.
2. Set the minimum allowed password character counts for administrative and user passwords.

```
sec.pwd.length.admin="<min password length>"
sec.pwd.length.user="<min password length>"
```

3. Set the administrator and user passwords.

   **Note:** You can't set the administrator password as the default password: `456`.

```
device.auth.localAdminPassword="<administrator password string>"
device.auth.localAdminPassword.set="1"
device.auth.localUserPassword="<user password string>"
device.auth.localUserPassword.set="1"
```

4. Save the configuration file.

### Set the Administrator Password on the Local Interface

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

**Task**

1. Open the configuration file.
2. Select **Settings > Advanced**.
3. Enter the default password and select **Enter**.
4. Select **Change Admin Password**.
5. 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 (`<, >`).
6. Save the configuration file.

### Set the User Password on the Local Interface

Set the user password at any time from the **Advanced** settings menu.

**Task**

1. Open the configuration file.
2. Select **Settings > Advanced**.
3. Enter the user password and select **Enter**.
4. Select **Change User Password**.
5. 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 (`<, >`).
6. Save the configuration file.

### 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.

**Task**

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.

### California SB-327 Password Requirement Compliance

Your phone meets the California SB-327 password mandate that requires administrators to generate a new password before granting access to the system and the system web interface.

When you first power on a phone or following a factory reset, the phone requires you to change the default administrator password. You must change the default administrator password to a unique password to access the local interface and system web interface.

If the phone is automatically redirected to the provisioning server using DHCP Options or ZTP, and the provisioning server changes the admin password in the configuration file, you don't need to manually change the admin password.

**Note:** You can’t use the default password as the newly generated password.

### Change the Phone Default Administrator Password in Microsoft Teams

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

**Task**

1. Go to **Settings > Device Settings**.
2. Select **Admin Only**.
3. Select **Admin Password**.
4. Enter the default password, enter a new password, and confirm the new password.

## Encryption

Encryption ensures that information remains secure. Configure your phone to encrypt configuration files before sending them to the provisioning server over your network.

### Encrypt Files for Upload

Configure the phone to encrypt files you upload to the provisioning server.

**Important:** Configuring the following parameter(s) causes the phone to reboot. Dependencies and overrides may affect other parameters.
For more information, see the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

**Task**

1. Open the configuration file.
2. Enable encryption for the following file types:
   - Configuration file:

     ```
     sec.encryption.upload.config="1"
     ```
   - Call lists:

     ```
     sec.encryption.upload.callLists="1"
     ```
   - Contact directory:

     ```
     sec.encryption.upload.dir="1"
     ```
   - MAC address configuration file:

     ```
     sec.encryption.upload.overrides="1"
     ```
3. Save the configuration file.

### Change the Encryption Key

Change the encryption key on the phones to maintain secure files.

Make sure your configuration file includes `device.set="1"`.

**Important:** Configuring the following parameter(s) causes the phone to reboot. Dependencies and overrides may affect other parameters.
For more information, see the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

**Note:** For each device parameter, be sure that your configuration file includes `device.x.set="1"` to allow the parameter to be written to the phone's flash.

**Task**

1. Place all encrypted configuration files that you want to update on the provisioning server.

The phone may reboot multiple times.

2. Enter the new key into the configuration file included in the list of files downloaded by the phone, specified in 000000000000.cfg or <*MACaddress*>.cfg.
3. Open the configuration file.
4. Specify a new encryption key:

```
device.sec.configEncryption.key.set="1"
device.sec.configEncryption.key="<encryption key>"
```

5. Save the configuration file.
6. Provision the phone.
7. After you update the encryption key, you must decrypt the files on the server with the old encryption key, then encrypt again it with the new key. Alternatively, you can make the files available in unencrypted format.
8. Delete any 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 encryption 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

Configure phones with a local contact directory and link contacts to speed dial buttons.

### 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.

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.

**`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 501 and 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 501 and 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.

### Disable the Local Contact Directory

If you don't want phone users to store contacts on a phone, disable the local contact directory.

**Important:** Configuring the following parameter(s) causes the phone to reboot. Dependencies and overrides may affect other parameters.
For more information, see the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

#### Task

1 Open the configuration file.
2 Disable the local contact directory.

```
feature.directory.enabled="0"
```

3 Save the configuration file.

### Disable Local Speed Dial Edits

Prevent users from editing the speed dial entries on their phones.

#### Task

1 Open the configuration file.
2 Disable local edits to speed dial entries.

```
dir.local.readonly="1"
```

3 Save the configuration file.

## Corporate Directory

Connect your phones to a corporate directory server that supports LDAP version 3. Setting up the corporate directory on the phone enables users to search for and place calls to these directory contacts.

Poly phones support corporate directories with server-side sorting. If the directory doesn't support server-side sorting, the phone performs sorting locally.

**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*.

### Connect to a Corporate Directory Using LDAP

Connect to and download corporate directory contacts to your phones.

**Important:** Configuring the following parameter(s) causes the phone to reboot. Dependencies and overrides may affect other parameters.
For more information, see the parameter reference topic(s) in the *Poly Edge E Series Phones Parameter Reference Guide*.

Access to a corporate directory on the phone is read only. Phone users can't add or remove contacts to the corporate directory.

#### Task

1 Open the configuration file.

2 Enter the IP address or host name of the LDAP server.

```
dir.corp.address="<LDAP IP address or host name>"
```

3 By default, the phone uses the TCP transport protocol to transfer the LDAP file from the server. If your network requires it, change the transport protocol to TLS.

```
dir.corp.transport="TLS"
```

4 Save the configuration file.

### Configure the LDAP Server Base Domain

Configure the base domain to use for the LDAP server.

**Task**

1 Open the configuration file.

2 Configure the base domain. The maximum string length is 255 characters.

```
dir.corp.baseDN="<Base Domain>"
```

3 Save the configuration file.

### Configure the LDAP Server Connection Port

Configure the port to connect to the LDAP server.

Set this parameter if the LDAP server is not using the standard ports (389 for TCP transport and 636 for TLS transport.

**Task**

1 Open the configuration file.

2 Configure the server connection port. The default is 0. Permitted values are 0 to 65535.

```
dir.corp.port="<Server Connection Port">
```

3 Save the configuration file.

### Configure the LDAP Search Query Filter Prefix String

Configure the predefined filter prefix string to use for all LDAP search queries.

**Task**

1 Open the configuration file.

2 Configure the predefined search query filter prefix string. The default is (objectclass=person). The maximum string length is 255 characters.

```
dir.corp.filterPrefix="<search_query_prefix>"
```

3 Save the configuration file.

### Configure LDAP Server Credentials

Configure the username and password to use to authenticate the LDAP server.

**Task**

1 Open the configuration file.

2 Configure the LDAP server username. The maximum string length is 255 characters.

```
dir.corp.user="<user name>"
```

3 Configure the LDAP server password. The maximum string length is 255 characters.

```
dir.corp.password="<password>"
```

4 Save the configuration file.

### Configure LDAP Search Attributes

Configure search attributes for LDAP.

For each parameter, *x* is a list of defined attributes to use for searching. You can define up to 8.

**Task**

1 Open the configuration file.

2 Configure a search attribute name to match an attribute in the directory entries on the LDAP server. The maximum string length is 255 characters.

Consult the LDAP server for supported attribute names.

```
dir.corp.attribute.x.name="<Attribute Name>"
```

3 Configure the label for the search attribute. The maximum string length is 255 characters.

```
dir.corp.attribute.x.label="<Attribute Label>"
```

4 Configure the attribute type that the phone uses to interpret the returned search results.

Possible values:

- first_name
- last_name (default)
- phone_number
- SIP_address
- H323_address
- URL
- other

```
dir.corp.attribute.x.type="<Attribute Type>"
```

5 Configure the filter string for the attribute. The maximum string length is 255 characters.

```
dir.corp.attribute.x.filter="<Filter String>"
```

6 Determine if the filter string criteria is reset or retained after a reboot. The default is 0 (reset after a reboot). To retain filter string criteria after a reboot, set the value to 1.

```
dir.corp.attribute.x.sticky="<Reset or Retain Criteria>"
```

7 Determine if the LDAP search query includes the attribute. The default is 0 (not searchable). To make the attribute searchable, set the value to 1.

```
dir.corp.attribute.x.searchable="<Searchable Attribute>"
```

8 Determine if the wildcard character is appended to the LDAP search query for the attribute. The default is 1 (append wildcard character). To disable appending a wildcard character, set the value to 0.

```
dir.corp.attribute.x.addstar="<Wildcard Character>"
```

9 Save the configuration file.

## Securely Store LDAP Credentials

Enable multiple users to enter their LDAP user credentials directly in the phone to access the corporate (LDAP) directory and store those credentials on the phone.

Any LDAP credentials that users enter on the phone are encrypted and stored only on the phone. The credentials also persist after the phone restarts or reboots.

### Task

1. Open the configuration file.
2. Enable the phone to securely store and encrypt LDAP directory user credentials.

```
dir.corp.persistentCredentials="1"
```

3. Enable the login prompt if the phone doesn't log in to the LDAP server as part of the phone's configuration.

```
dir.corp.allowCredentialsFromUI.enabled="1"
```

4. Save the configuration file.

## 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 Poly 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.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

other

Change causes system to restart or reboot.

### dir.corp.auth.useLoginCredentials

0 (default) - Disabled

1 - Enabled

### 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)

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 the phone to 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 - 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.

**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.

### Call List Parameters

Use the following parameters to configure call lists.

**`callLists.collapseDuplicates`**

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`**

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)

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<br>Call direction with respect to the user. | In, Out |
| disposition<br><br>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<br>The line (or registration) index. | Positive integer |
| protocol<br>The line protocol. | SIP |
| startTime<br><br>The start time of the call. For example: 2010-01-05T12:38:05 in local time. | String |
| duration<br><br>The duration of the call, beginning when it is connected and ending when the call is terminated. For example: `PT1H10M59S`. | String |
| count<br><br>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.<br>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.<br>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<br><br>The source of the call (caller ID from the call recipient's perspective). | Address |
| Connection<br><br>An array of connected parties in chronological order.<br>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<br><br>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.

**Task**

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**.

## 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:

**Task**

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

## User Profiles

Users can access their personal phone settings from any phone on the network with user profiles.

Remote and mobile workers who don't have a dedicated work space can benefit from this feature. Offices with a common conference phone where multiple users need to access their personal settings can also use user profiles.

**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.

Users can change their own password on any phone on the network. If a user changes any settings while logged into a phone, the settings save and display the next time that user logs in to another phone. When the user logs out, the corresponding user options clear from the device until someone enables the user profile-related configuration on the phone again.

## User Profile Authentication

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

Enable users to log in to any phone on the network with their user profile.

To enable server authentication, set up user accounts on the provisioning server so users can authenticate their phones 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.

### Enable the Phone to Use Server Authentication

Configure the phone to use its provisioning server for user authentication.

Enable the phone to use multiple user profiles.

**Task**

1. Open the configuration file.
2. Enable server authentication.

```
prov.login.useProvAuth="1"
```

3. Save the configuration file.

### Create a Generic User Profile for Server Authentication

Create a user profile to use with a provisioning server or locally on a shared phone.

If you enable server authentication of user profiles, the following parameters don't apply:

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

**Task**

1. Open the configuration file.
2. On the server, create an account and directory for the generic profile.
   `Generic_Profile`
3. In the directory, create a configuration file for the generic profile the phone uses by default.
   genericprofile.cfg
4. Open the generic profile configuration file.

5 Include registration and server details, and set the following phone feature parameters:

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

**Note:** If you enable prov.login.enabled and don't enable prov.login.useProvAuth, the phone authenticates users by matching with credentials you store in the <*user*>.cfg user configuration file.

6 Save the generic profile configuration file.

7 Create a primary configuration file 000000000000.cfg for all the phones or a <*MACAddress*>.cfg for each phone, and add the generic profile configuration file to the **CONFIG_FILES** field.

8 Set the provisioning server address and provisioning server username and password credentials for the generic user account on the phone at **Settings > Advanced > Provisioning Server**.

9 Save the configuration file.

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 User Profiles for Server Authentication

Create user profiles in the **Home** directory of each user with a specific configuration file that you store on the provisioning server. User profiles have unique names as well as 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.

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

### Task

1 On the server, create an account and a directory for each user.
`User1` and `User2`

2 In each user directory, create a configuration file for each user that contains the user's registration details and feature settings.
User1.cfg and User2.cfg

3 Open the user profile configuration file.

4 Enable the user profile.

```
prov.login.enabled="1"
```

5 Optional: Set the user's default password. The default is 123 until the user changes it.

```
prov.login.localPassword="<string>"
```

6 Save the user profile configuration file.

## User Profile Phone Authentication

Enable multiple users to log in to one phone.

Users can provide their credentials on the phone without using a server. This is helpful for shared phones in common areas without a connection to a provisioning server.

### 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 users update their password or other user-specific settings on the phone, the updates save to <*user*.-phone.cfg, not <*MACaddress*.-phone.cfg.
- If users update their contact directory while logged in to a phone, the updates save to <*user*.-directory.xml.
- Directory updates display each time users log in to a phone. For certain phones, the <*user*.-calls.xml contains an up-to-date call list history. This list updates each time users log in to their phone.

The following list provides 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

**Task**

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.
   If the user's login ID is *user100*, name the user configuration file user100.cfg.
2. Open the user configuration file.
3. In each <*user*>.cfg file, you must add and set values for the user's login password.
4. 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 force the phone to restart or reboot to complete the update.
5. Save the user configuration file.

### Convert a Phone to User-Based Deployment

Configure a phone in a deployment that depends on user login instead of a traditional phone deployment.

**Task**

1. Open the user configuration file.
2. Copy the <*MACaddress*>-phone.cfg file to <*user*>-phone.cfg.
3. Copy the phoneConfig<*MACaddress*>.cfg file to <*user*>.cfg.
4. Save the user configuration file.

### Create Default Credentials and a Profile for a Phone

Create a default user profile for the phone to automatically log in to each time a user logs out or the phone restarts.

The default user profile is like any other user profile, except it's designated as the phone's own profile. When the phone logs in using the default login credentials, a default phone profile displays. Users retain the option to log in and view their personal settings.

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

**Task**

1. Open the configuration file.
2. Enter the default user login credentials.

```
prov.login.defaultUser="<Default User Profile Username>"
prov.login.defaultPassword="<Account User Profile Password>"
```

3. Save the configuration file.

### Require a User Login

Configure the phone to require a user to log in to the phone to use it.

**Task**

1. Open the configuration file.
2. Require a user to log in to use the phone.

```
prov.login.required="1"
```

3. Save the configuration file.

### Mask the User Password Entry

Use pound signs (#) to mask the user's password on the phone's screen as they enter it.

Password entries on the phone's screen to prevent prying eyes from seeing user's password. For example, `password` displays as `########`.

**Task**

1. Open the configuration file.
2. Mask the user's password entry with pound signs.

```
prov.login.localPassword.hashed="1"
```

3. Save the configuration file.

### Enable User Login Persistence

Enable the phone to maintain the last user logged in following a phone reboot.

**Task**

1. Open the configuration file.
2. Enable the phone to retain the last user login when it reboots.

```
prov.login.persistent="1"
```

3. Save the configuration file.

## System Logs

System log files contain information about system activities and the system configuration profile.

After you set up system logging, you can retrieve system log files.

The detailed technical data in the system log files can help Poly Global Services resolve problems and provide technical support for your system. Your support representative may ask you to download log archives and send them to Poly Global Services.

You must contact Poly Customer Support to obtain the template file (techsupport.cfg) that contains the parameters that configure log levels.

For information on configuring system log parameters, refer to the *Poly Edge E Series Phones Parameter Reference Guide*.

## Configuring Log Files

Configure how the phone creates log files.

Log file names use the following format: `[MAC address]-[Type of log].log`. For example, if the MAC address of your phone is `0004f2203b0`, the log file name is `0004f2203b0-app.log`.

The phone writes information into several different log files. The types of information in each type of log file are:

- **Application Log** – The application log file contains complete phone functionality data including SIP signaling, call controls and features, digital signal processor (DSP), and network components.
- **System Log** - The system log file contains the android logs.

## Retrieve Logs Using the System Web Interface

You can view and export log files using a phone's system web interface.

**Task**

1. Log in to the system web interface as an administrator
2. Go to **Diagnostics > View & Download Logs > Audit**.

## Retrieve Logs from the Support Information Package

Export the **Support Information Package** (.tar file) using the system web interface.

The support information package includes the following log files:

- PBU file
- App log file
- Boot log file
- Audit log file

**Task**

1. Log in to the system web interface as an administrator.
2. Go to **Diagnostics > Download Support Information Package** and download the support information package.
3. On your computer, unzip the .tar file to view the log files.

## Enable Log Uploads to a USB Flash Drive

Configure your phones to copy application and boot logs to a USB flash drive connected to the phone.

You can configure the phone to copy the application logs and boot 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 and boot logs to the USB flash drive periodically using `log.render.file.upload.period` parameter.

**Task**

1. Open the configuration file.
2. Enable the phone to upload logs to a connect USB flash drive.

```
feature.usbLogging.enabled="1"
```

3. Save the configuration file.

# How Data Subject Rights Are Supported

## 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.

For any data processed by third parties such as service providers, contact those parties directly.

## Right to Be Informed

**What personal data is collected?**

See Purposes of Processing Personal Data on page 30.

**How personal data is used?**

See Purposes of Processing Personal Data on page 30.

**How long is personal data kept?**

Data residing on the device itself is retained according to customer's device administrator. Data residing in any Poly cloud or analytics service may be retained for as long as needed to provide the customer with any Poly cloud services for which they have subscribed and for product improvement purposes.

**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.

For any data processed by third parties such as service providers, contact those parties directly.

**Related Links**

System Logs on page 27

## 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 is purged. Customer contact information is retained by Poly support until the support relationship ends or is requested to be removed by the customer.

For data that is sent to any Poly cloud or analytics service, when a customer makes a request for deletion to privacy@poly.com, Poly will delete the requested data within 30 days, unless the data is required to be retained to provide the service to customer. Poly may “anonymize” personal data in lieu of deletion. In cases where anonymization occurs, the process is irreversible and includes, but is not limited to, searching and sanitizing all customer-specific data (including name, site information, and IP address) with randomly generated alphanumeric characters.

**Related Links**

How Personal Data is Deleted on page 32

## 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.

Correction requests for data residing on the device itself should be directed to the device administrator. Requests related to data sent to Poly cloud or analytics services should be sent to dataprotection@poly.com.

# Purposes of Processing Personal Data

Refer to the *Security and Privacy White Paper* for Poly Edge E Series phones 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. |

# How Personal Data is Deleted

**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.<br>• 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.<br>• Call lists and the CDR can be deleted by performing a standard or comprehensive restore operation.<br>• Call lists and the CDR may be reset by the Administrator from **Settings > Advanced > Administration Settings > Reset to Defaults > Reset User Data**.<br>• 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**.<br>• The contacts can also be deleted by resetting the system. | Simple delete on phone. |
| 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. |

## Resetting a Phone to Factory Defaults

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

### Reset the Phone and Configuration

When you reset your phone, you can choose a complete configuration reset or choose partial reset options.

**Task**

1 Go to **Settings > Advanced > Administration Settings**.

2 Select **Reset to Defaults** and choose a reset option:

- **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 Cloud Configuration**: Clears any configuration received from the configuration source identified by `cfgParamSourceCloud`.
- **Reset Device Settings**: Resets the phone's flash file system settings not 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 PVOS 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 PVOS 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.

## Enable Users to Reset the Phone to Factory

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

Make sure your configuration file includes `device.set="1"`.

**Note:** For each device parameter, be sure that your configuration file includes `device.x.set="1"` to allow the parameter to be written to the phone's flash.

### Task

1 Open the configuration file.

2 Display the **Reset to Factory** option under the **Basic** settings.

```
up.basicSettings.factoryResetEnabled="1"
```

3 Optional: Adjust which settings the phone resets when a user performs a factory reset. You can preserve just the administrator password or the administrator password and the provisioning settings.

Enable device.set for device.system.recoveryType:

```
device.system.recoveryType.set="1"
```

To preserve just the administrator password, set the following parameter:

```
device.system.recoveryType="PreserveAdmin"
```

To preserve the administrator password and the provisioning settings, set the following parameters:

```
device.system.recoveryType="CloudProv"
```

4 Save the configuration file.