



Security and Monitoring

- [Logout Inactivity Timer, on page 1](#)
- [Problem Reporting, on page 1](#)
- [Set Device PIN , on page 3](#)
- [Biometric Authentication on Mobile Clients, on page 4](#)
- [Silent Monitoring and Call Recording, on page 5](#)
- [Telemetry with Cisco Jabber Analytics, on page 5](#)
- [Wireless Location Monitoring Service, on page 6](#)

Logout Inactivity Timer

Applies to: All clients

The sign-out inactivity timer allows you to automatically sign users out of the client after a specified amount of time of inactivity.

Inactivity on the mobile clients includes:

- The client goes into the background.
- No user interaction on voice calls.

You configure this feature on the mobile clients using the ForceLogoutTimerMobile parameter.

Inactivity on the desktop clients includes:

- No keyboard or mouse activity.
- No user interaction on connected accessories for making and answering calls.

You configure this feature on the desktop clients using the ForceLogoutTimerDesktop parameter.

If you do not set the parameter, the client does not automatically sign out.

Problem Reporting

Applies to: Cisco Jabber for Windows

Setting up problem reporting enables users to send a summary of issues that they encounter with the client. There are two methods for submitting problem reports as follows:

- Users submit the problem report directly through the client interface.
- Users save the problem report locally and then upload it at a later time.

The client uses an HTTP POST method to submit problem reports. Create a custom script to accept the POST request and specify the URL of the script on your HTTP server as a configuration parameter. Because users can save problem reports locally, you should also create an HTML page with a form to enable users to upload problem reports.

Before you begin

Complete the following steps to prepare your environment:

1. Install and configure an HTTP server.
2. Create a custom script to accept the HTTP POST request.
3. Create an HTML page that enables users to upload problem reports that are saved locally. Your HTML page should contain a form that accepts the problem report saved as a .ZIP archive and contains an action to post the problem report using your custom script.

The following is an example form that accepts problem reports:

```
<form name="uploadPrt" action="http://server_name.com/scripts/UploadPrt.php" method="post"
  enctype="multipart/form-data">
  <input type="file" name="zipFileName" id="zipFileName" /><br />
  <input type="submit" name="submitBtn" id="submitBtn" value="Upload File" />
</form>
```

Procedure

-
- | | |
|---------------|---|
| Step 1 | Host your custom script on your HTTP server. |
| Step 2 | Specify the URL of your script as the value of the <code>PrtLogServerUrl</code> parameter in your configuration file. |
-

Decrypt the Problem Report

The command line tool `CiscoJabberPrtDecrypter.exe` for decrypting the problem reports is only available on Windows machines and is included in the installer. The tool has the following arguments:

- `--help`—Show the help message.
- `--privatekey`—Specify the private key file, this is a privacy enhanced mail (.pem) or a personal information exchange PKCS#12 (.pfx) format.
- `--password`—Optional, if the input private key file is password protected.
- `--encryptionkey`—Specify the encryption secret key file, for example `file.zip.esk`.
- `--encryptedfile`—Specify the encrypted file, for example `file.zip.enc`.
- `--outputfile`—Specify the output file, for example `decryptedfile.zip`.

- `--mobile`—Specify for the problem reports from mobile clients.

Before you begin

To decrypt problem reports you need the following:

- Two files from the zip file created when you generated a problem report using encryption:
 - *file.zip.esk*—The encrypted symmetric key.
 - *file.zip.enc*—The original data encrypted using AES256.
- Private Key for the certificate used for encrypting the data.

Procedure

-
- Step 1** Open a command prompt in Windows.
 - Step 2** Navigate to the `C:\Program Files(x86)\Cisco Systems\Cisco Jabber\` directory.
 - Step 3** Enter the command and your parameters.

Example for desktop clients: `CiscoJabberPrtDecrypter.exe --privatekey C:\PRT\PrivateKey.pfx --password 12345 --encryptedfile C:\PRT\file.zip.enc --encryptionkey C:\PRT\file.zip.esk --outputfile C:\PRT\decryptedfile.zip`

Example for mobile clients: `CiscoJabberPrtDecrypter.exe --privatekey C:\PRT\PrivateKey.pfx --password 12345 --encryptedfile C:\PRT\file.zip.enc --encryptionkey C:\PRT\file.zip.esk --outputfile C:\PRT\decryptedfile.zip --mobile`

If the decryption is successful the output file is created. If there is an invalid parameter the decryption fails and an error is shown on the command line.

Set Device PIN

Applies to: Cisco Jabber for mobile clients.

We recommend that you use Jabber only on secured devices. To check if the device is secure, configure the `ForceDevicePin` parameter with the value `true`.

Example:

```
<ForceDevicePin>true</ForceDevicePin>
```

If the device is not secured:

- Then Jabber displays a notification to set PIN. This is a time bound notification, if the user doesn't tap on **SET PIN** within 13 seconds, then the user is signed out of Jabber.

After the user taps **SET PIN** option, the users must go the device settings and secure the device with a PIN or fingerprint authentication.

- If the user signs into Jabber, and then puts it in the background immediately, Jabber checks if the user has secured the device or not. If the device is not secured, then the user is signed out of Jabber.

Biometric Authentication on Mobile Clients

Applies to: Cisco Jabber for mobile clients.

Cisco Jabber supports fingerprint, Touch ID, or Face ID authentication for users to securely sign in. Cisco Jabber for Android supports fingerprint authentication and Cisco Jabber for iPhone and iPad supports Touch ID or Face ID authentication. You can use these authentication methods to ensure that your users can quickly and securely sign in to Cisco Jabber on their mobile devices.

The fingerprint, Touch ID, or Face ID authentication is used in the following scenarios:

- When Cisco Jabber for Android users sign in to Cisco Jabber after they sign out manually, or after an auto logout, they have to sign into Cisco Jabber only using fingerprint authentication.
- When Cisco Jabber for iPhone and iPad users sign in to Cisco Jabber after they sign out manually and after an auto logout they have to sign into Cisco Jabber only using Touch ID or Face ID authentication.

You can enable Cisco Jabber users to sign in using this authentication by configuring the parameter, `LocalAuthenticationWithBiometrics`.

You can configure this parameter using any of these values:

- `AdminEnabled`—Cisco Jabber prompts your users to authenticate using fingerprint, Touch ID, or Face ID. Users must use biometric authentication to sign into Cisco Jabber. However, if the user's device does not support biometric capability, then user have to sign in using their password.
- `UserDecision` (default)—Cisco Jabber prompts your users to authenticate using fingerprint, Touch ID, or Face ID. The users can decide if they want to use biometric authentication to sign into Cisco Jabber.
- `AdminDisabled`—Cisco Jabber doesn't use fingerprint, Touch ID, or Face ID authentication. There is no prompt displayed to the user.

If authentication fails, Cisco Jabber prompts your users to enter their credentials each time they sign in.

Example: `<LocalAuthenticationWithBiometrics>AdminDisabled</LocalAuthenticationWithBiometrics>`

Device Requirements for Touch ID and Face ID Authentication

Jabber iPhone and iPad support for Touch ID and Face ID authentication is dependent on the device operating system.

Device Requirements for Fingerprint Authentication

Any Android device that supports fingerprint authentication and has an Android OS 6.0 or later. However, the following devices have specific requirements:

- Xiaomi devices require Mi User Interface (MIUI) version 9.0 or later.
- Huawei devices require EMUI version 4.0 or later.
- Samsung devices with fingerprint authentication on devices earlier than Android 6.0, might not support fingerprint authentication after you upgrade the OS to 6.0.

Silent Monitoring and Call Recording

Applies to: All clients

Silent call monitoring is a Cisco Unified Communications Manager feature. It allows a supervisor to hear both call participants, but neither of the call participants can hear the supervisor.

Call recording is a Unified CM feature that enables a recording server to archive agent conversations.

- Jabber doesn't provide any interface to begin silent monitoring or call recording. Use the appropriate software to silently monitor or record calls.
- Jabber doesn't currently support monitoring notification tone or recording notification tone.
- You can use silent monitoring and call recording functionality only. Jabber doesn't support other functionality such as barging or whisper coaching.

Server Requirements:

- We support silent monitoring and call recording for on-premises deployments only.
- Cisco Jabber for Windows and Cisco Jabber for Mac require Cisco Unified Communications Manager 9.x or later.
- Cisco Jabber for iPhone and iPad and Cisco Jabber for Android require Cisco Unified Communications Manager 11.0 or later.

Some releases of Unified CM require a device package to enable monitoring and recording capabilities. Verify that the **Built In Bridge** field is available in the **Phone Configuration** window for the device. If the field isn't available, download and apply the most recent device packages.

For detailed information about how to configure silent monitoring or call recording, see the *Feature Configuration Guide for Cisco Unified Communications Manager*.

Telemetry with Cisco Jabber Analytics

Applies to: All clients

To improve your experience and product performance, Cisco Jabber may collect and send non-personally identifiable usage and performance data to Cisco. The aggregated data is used by Cisco to understand trends in how Jabber clients are being used and how they are performing.

You must install the following root certificate to use the telemetry feature: GoDaddy Class 2 Certification Authority Root Certificate. The telemetry server certificate name is "metrics-a.wbx2.com". To resolve any warnings about this certificate name, install the required GoDaddy certificate. For more information about certificates, see the Planning Guide.

By default, the telemetry data is on. You can configure the following telemetry parameters:

- `Telemetry_Enabled`—Specifies whether analytics data is gathered. The default value is true.
- `TelemetryEnabledOverCellularData`—Specifies whether analytics data is sent over cellular data and Wi-Fi (true), or Wi-Fi only (false). The default value is true.

- **TelemetryCustomerID**—This optional parameter specifies the source of analytic information. This ID can be a string that explicitly identifies an individual customer, or a string that identifies a common source without identifying the customer. We recommend using a tool that generates a *Global Unique Identifier* (GUID) to create a 36 character unique identifier, or to use a reverse domain name.



Note The option to disable telemetry is not available to Jabber team messaging mode users.

For more information about these parameters, see the *Parameters Reference Guide*.

You can find details on how Cisco handles analytics data at <https://www.cisco.com/c/en/us/about/legal/privacy-full.html>.

Wireless Location Monitoring Service

Applies to: All clients

Wireless location monitoring service allows you to determine the physical location from where your Cisco Jabber users connect to the corporate network. This information is stored in Cisco Unified Communications Manager.

You can configure wireless location monitoring service in Cisco Unified Communications Manager 11.5 or later, for more information see the [System Configuration Guide for Cisco Unified Communications Manager](#).

Cisco Jabber monitors your users' locations, gathers Service Set ID (SSID) and Basic Service Set ID (BSSID) information, and sends this information to Unified CM at least every 24 hours, or whenever:

- Their current access point changes.
- They sign in to Cisco Jabber.
- They switch between on-premises and Expressway for Mobile and Remote Access network.
- Cisco Jabber resumes from sleep or is made active.

For on-premises deployments, configure wireless location monitoring using `EnableE911OnPremLocationPolicy` parameter with the value `true`.

For Expressway for Mobile and Remote Access deployments, you can configure wireless location monitoring using the `EnableE911EdgeLocationPolicy` with the value `true` and `E911EdgeLocationWhiteList` with a list of up to 30 SSIDs, separated by a semicolon.

For more details on these parameters, see the latest *Parameter Reference Guide for Cisco Jabber*.