# Security and Monitoring



# Logout Inactivity Timer

| Clients | | | |
|---|---|---|---|
| **Windows** | **Mac** | **iPhone and iPad** | **Android** |
| Yes | Yes | Yes | Yes |

| Deployments | | | |
|---|---|---|---|
| **On-Premises** | **Webex Messenger** | **Team Messaging Mode** | **Softphone for VDI** |
| Yes | Yes | Yes | Yes |

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

| Clients | | | |
|---|---|---|---|
| **Windows** | **Mac** | **iPhone and iPad** | **Android** |
| Yes | — | — | — |

| Deployments | | | |
|---|---|---|---|
| **On-Premises** | **Webex Messenger** | **Team Messaging Mode** | **Softphone for VDI** |
| Yes | Yes | Yes | Yes |

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 PrtLogServerUrl 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`.

### 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\CUCILync\` 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`

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.

# Collect PRT Logs Remotely

Instead of waiting for a user to upload the PRT logs, you can generate the logs remotely in **Unified CM Administration**.

### Before you begin

To use this feature, your deployment requires Unified CM Release 12.5.1 SU 1 or later. The RemotePRTServer parameter specifies the script to upload the PRT logs to your server.

### Procedure

**Step 1** Select **Device** > **Phone**.

**Step 2** Choose the devices for which you need logs.

**Step 3** Click **Generate PRT for selected**.

The script uploads the PRT logs to your server.

**Note** To collect logs from Cisco Sunkist headsets, you require firmware version 1.3 or later.

## Set Up for Remote PRT Log Collection

Before you can remotely collect PRT logs, you must specify a script to upload the logs in **Unified CM Administration**.

### Procedure

**Step 1** Select **User Management** > **User Setting** > **UC Service**.

**Step 2** Add a new UC service with a **UC Service Type** of **Jabber Client Configuration (jabber-config.xml)**.

**Step 3** Add a **Jabber Configuration Parameter** with these values:

- **Section**—`Policies`
- **Parameter**—`RemotePRTServer`
- **Value**—The URL for your upload script.

# Set Device PIN

| Clients | | | |
|---|---|---|---|
| **Windows** | **Mac** | **iPhone and iPad** | **Android** |
| — | — | Yes | Yes |

| Deployments | | | |
|---|---|---|---|
| **On-Premises** | **Webex Messenger** | **Team Messaging Mode** | **Softphone for VDI** |
| Yes | Yes | Yes | — |

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

| Clients | | | |
|---|---|---|---|
| **Windows** | **Mac** | **iPhone and iPad** | **Android** |
| — | — | Yes | Yes |

| Deployments | | | |
|---|---|---|---|
| **On-Premises** | **Webex Messenger** | **Team Messaging Mode** | **Softphone for VDI** |
| Yes | Yes | Yes | — |

Cisco Jabber supports authentication by fingerprint or facial recognition for users to securely sign in. 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 authentication by fingerprint or facial recognition is used in the following scenarios:

- When a Cisco Jabber for Android user signs in to Jabber after signing out manually or an automatic sign out, they can use authentication by fingerprint or facial recognition.
- 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 or facial recognition. 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 or facial recognition. The users can decide if they want to use biometric authentication to sign into Cisco Jabber.
- AdminDisabled—Cisco Jabber doesn't use authentication by fingerprint or facial recognition. 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 Biometric Authentication

This feature is available only on devices whose operating systems support biometric authentication.

# Silent Monitoring and Call Recording

| Clients | | | |
|---|---|---|---|
| **Windows** | **Mac** | **iPhone and iPad** | **Android** |
| Yes | Yes | Yes | Yes |

| Deployments | | | |
|---|---|---|---|
| **On-Premises** | **Webex Messenger** | **Team Messaging Mode** | **Softphone for VDI** |
| Yes | Yes | Yes | Yes |

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*.

# On-Demand Recording

| Clients | | | |
|---|---|---|---|
| **Windows** | **Mac** | **iPhone and iPad** | **Android** |
| Yes | Yes | — | — |

| Deployments | | | |
|---|---|---|---|
| **On-Premises** | **Webex Messenger** | **Team Messaging Mode** | **Softphone for VDI** |
| Yes | Yes | Yes | Yes |

Rather than record every call, you can offer your users the flexibility to choose when they want to record.

In deployments with Unified Communications Manager Release 12.5(1) and later, Jabber can support Unified CM's on-demand recording using Jabber's Built-In Bridge (BiB). In Cisco Unified CM Administration, set **Device** > **Phone** > **Recording Option** to **Selective Call Recording Enabled** to enable the feature. Also enable the BiB, either cluster-wide or for individual phones.

When you enable this feature, the call control menu includes a **Record** option for the user to start and stop recording at any time.

### Preference Between Available Recorders

By default, if the user joins a conference call that has an external bridge set up to record calls, Jabber uses that external bridge for recording. However, some organizations might prefer all recording to use the Jabber BiB for compliance reasons. In those cases, use the Prefer_BIB_recorder parameter to enforce recording on the Jabber BiB.

# Telemetry with Cisco Jabber Analytics

| Clients | | | |
|---|---|---|---|
| **Windows** | **Mac** | **iPhone and iPad** | **Android** |
| Yes | Yes | Yes | Yes |

| Deployments | | | |
|---|---|---|---|
| **On-Premises** | **Webex Messenger** | **Team Messaging Mode** | **Softphone for VDI** |
| Yes | Yes | Yes | Yes |

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.

# Jabber Analytics in Webex Control Hub

| Clients | | | |
|---|---|---|---|
| **Windows** | **Mac** | **iPhone and iPad** | **Android** |
| Yes | Yes | Yes | Yes |

| Deployments | | | |
|---|---|---|---|
| **On-Premises** | **Webex Messenger** | **Team Messaging Mode** | **Softphone for VDI** |
| Yes | Yes | — | — |

You can now access Jabber analytics through Webex Control Hub. Your data is available on the **Jabber** tab of the **Analytics** page. Jabber analytics provides key performance indicators with trending, such as:

- Active users
- Messages sent
- Calls made or received from Jabber
- Screen share from Jabber

To access Jabber analytics, you must have Webex Control Hub set up. Set these parameters in `jabber-config.xml`:

- TelemetryEnabled to true
- TelemetryEnabledOverCellularData to true
- TelemetryCustomerID to your OrgID from Control Hub

This feature is available for these deployment modes:

- On-premises with full UC
- On-premises IM-Only
- On-premises Phone-Only
- Jabber with Webex Messenger

**Note** This is a new feature in Webex Control Hub that impacts Jabber deployments. You can access this feature for any release of Jabber.

# Wireless Location Monitoring Service

**Applies to:** All clients

| Clients | | | |
|---|---|---|---|
| **Windows** | **Mac** | **iPhone and iPad** | **Android** |
| Yes | Yes | Yes | Yes |

| Deployments | | | |
|---|---|---|---|
| **On-Premises** | **Webex Messenger** | **Team Messaging Mode** | **Softphone for VDI** |
| Yes | Yes | Yes | Yes |

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*.

# Security Labels for Instant Messages

| Clients | | | |
|---|---|---|---|
| **Windows** | **Mac** | **iPhone and iPad** | **Android** |
| Yes | — | — | — |

| Deployments | | | |
|---|---|---|---|
| **On-Premises** | **Webex Messenger** | **Team Messaging Mode** | **Softphone for VDI** |
| Yes | — | — | Yes |

Customers often have data handling rules that restrict who can see which data. Your deployment can use a compliance server to filter instant messages. From Release 12.7, Jabber includes support for the *XEP-0258: Security Labels in XMPP* standard to enable such filtering.

You can define a catalog of security labels with the InstantMessageLabels parameter. The catalog populates a selection list above the chat input field.

When you implement security labels, the general work flow for sending IMs is as follows:

1. The user must choose a security label before they can send their IM.
2. Jabber appends the XMPP security label to the IM.
3. The IM goes to a compliance server.
4. The compliance server checks if its routing rules allow the recipient to see IMs with that classification:
   - If yes, the compliance server allows the IM.
   - If no, the compliance server rejects the IM.
5. When Jabber displays the IM in the chat window, the security label appears above the text.

For more information about using the InstantMessageLabels parameter, see the *Parameter Reference Guide for Cisco Jabber*. You can configure this setting in the Unified CM Administration or in the `jabber-config.xml` configuration file.

The following example shows how you could use the <label> element in the security labels tag:

```
<InstantMessageLabels>
  <item selector="Classified|SECRET">
    <securitylabel xmlns='urn:xmpp: sec-label:0'>
     <displaymarking fgcolor='black' bgcolor='red'>SECRET </displaymarking>
      <label>
       <edhAttrs xmlns="https://www.surevine.com/protocol/xmpp/edh">
       <specification>2.0.2</specification>
       <version>XXXX:1.0.0</version>
       <policyRef></policyRef>
       <originator>Acme</originator>
       <custodian>Acme</custodian>
       <classification>A</classification>
       <nationalities>Acme</nationalities>
       <organisations>Acme</organisations>
       </edhAttrs>
     </label>
    </securitylabel>
  </item>
<item…> … </item>
</InstantMessageLabels>
```

After you set this parameter, Jabber detects the configuration change and asks users to sign back into Jabber. For devices running on Jabber versions that don't support security labels, the IMs display the content of the message without the security label.