Security and Monitoring

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.

This feature is configured 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.

This feature is configured on the desktop clients using the ForceLogoutTimerDesktop parameter.

If the parameter is not set, the client will 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 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`.
- `--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.

Silent Monitoring and Call Recording

Applies to: All clients

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

Call recording is a Cisco Unified Communications Manager feature that enables a recording server to archive agent conversations.

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

Server Requirements:

- Silent monitoring and call recording are supported for on-premises deployment 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.

Before you configure this feature on the server, there are releases of Cisco Unified Communications Manager that 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 is not 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, Release 11.0(1)*.

Telemetry

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.

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

Full details on what analytics data Cisco Jabber does and does not collect can be found in the Cisco Jabber Supplement to Cisco's On-Line Privacy Policy at https://www.cisco.com/web/siteassets/legal/privacy_02Jun10.html.