

Cisco Secure Client Customer Experience Feedback Module

Note BY DEFAULT YOUR PRIVATE AND CORPORATE DATA IS COLLECTED.

The customer experience feedback (CEF) module provides us with information about which features and modules customers use and have enabled. This information gives us insight into the user experience so that Cisco can continue to improve the quality, reliability, performance, and user experience of Cisco Secure Client.

For details about the collection and use of information, refer to the Cisco Online Privacy Statement Highlights page where you can access the Cisco Secure Client Supplement. All data is collected anonymously and does not contain personally identifiable data. The data is also securely sent.

Cisco collects the following types of data:

- Usability data—See the privacy policy for details. This data is collected and sent once every month.
- Web threat data—Sent whenever a threat is reported.
- Crash reports—Crash dump files generated by Cisco Secure Client are checked every 24 hours, collected, and sent to the customer experience feedback server.

The major components in the customer experience feedback modules are as follows:

- Feedback Module—Cisco Secure Client software component that collects the information and periodically sends it to the server.
- Cisco Feedback Server—Cisco-owned cloud infrastructure that collects the customer experience feedback data and stores it in temporary storage as raw format.

- Configure Customer Experience Feedback, on page 1

Configure Customer Experience Feedback

The Cisco Secure Client Customer Experience Feedback module is deployed with Cisco Secure Client, and enabled by default. You can modify what feedback is sent by creating a Customer Experience Feedback

profile, including opting out of experience feedback entirely. This method is the preferred method to disable the feedback module, but you can also remove it altogether during Cisco Secure Client deployment.

Before you begin

The customer experience feedback module is enabled automatically.

Procedure

Step 1 Open the standalone Customer Experience Feedback Profile Editor or in ASDM, navigate to **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **AnyConnect Client Profile**.

Step 2 Create your Cisco Secure Client profile with Profile Usage of **Feedback Service Profile**.

Step 3 If you do not want to provide feedback, uncheck **Enable customer Experience Feedback Service**.

You can disable feedback any time after installation.

Step 4 If you do not want to send crash reports generated by Cisco Secure Client, uncheck **Include Crash Report**.

The default is to include a crash report.

Step 5 Enter a customer key or ID of your choice.

This ID allows Cisco to identify information from your organization.