



Release Notes for Cisco Secure Email Reporting Plug-in 1.1.0

Published: June 29, 2020


Last Updated: January 25, 2021

Contents

- [Cisco Email Reporting Plug-in 1.1.0 Update, page 2](#)
- [Supported Configurations, page 2](#)
- [Upgrading to Cisco Secure Email Reporting Plug-in 1.1.0, page 2](#)
- [Installing Cisco Secure Email Reporting Plug-in 1.1.0, page 4](#)
- [Related Documentation, page 4](#)
- [Service and Support, page 5](#)
- [Obtaining Documentation and Submitting a Service Request, page 5](#)



What's New in This Release

Feature/Enhancement	Description
Re-branded Product and Related Documentation	We have re-branded the product, and related documentation from “Cisco Email Reporting Plug-In” to “Cisco Secure Email Reporting Plug-In.”
	 Note The installer name and file paths still use the existing naming convention (Cisco Email Reporting).

The Cisco Secure Email Reporting Plug-in 1.1.0-136 release consists of various bug fixes. For more information, see [List of Fixed Issues, page 5](#).

Supported Configurations

The following configurations are supported for the Cisco Secure Email Reporting Plug-in 1.1.0:

Cisco Secure Email Reporting Plug-in 1.1.0	Outlook 2016 (32 bit)	Outlook 2016 (64 bit)	Outlook 2019 (64 bit)	Office 365
Win 10 32 bit	compatible	—	compatible	—
Win 10 64 bit	compatible	certified	certified	certified



Note

When you upgrade to Office 365, Cisco Secure Email Reporting Plug-in may be disabled in your Outlook. In that case, you must enable it manually.



Note

Support for Microsoft Windows 7 and 8.1 versions was available till the Cisco Secure Email Reporting Plug-in version 1.1.0-129. From this release onwards, there is only support for Microsoft Windows 10 and Office 365.

Upgrading to Cisco Secure Email Reporting Plug-in 1.1.0

- [Upgrade Paths, page 2](#)
- [Upgrading the Cisco Secure Email Reporting Plug-in, page 3](#)
- [Upgrading from the Cisco Secure Email Security Plug-in to the Cisco Secure Email Reporting Plug-in, page 3](#)

Upgrade Paths

You can upgrade to Cisco Secure Email Reporting Plug-in 1.1.0-136 release from any one of the following component versions.

- Cisco Secure Email Security Plug-in 7.6.2.037
- Cisco Secure Email Reporting Plug-in 1.1.0-133



Note If you plan to upgrade to Cisco Secure Email Reporting Plug-in 1.1.0-136 release from Cisco Secure Email Reporting Plug-in 1.1.0-133 version, it is a silent installation process.



Note After you update the Cisco Secure Email Security Plug-in 7.6.2.037, the Cisco Secure Email Security Plug-in is removed and the Cisco Secure Email Reporting Plug-in is available instead.

Upgrading the Cisco Secure Email Reporting Plug-in

To upgrade the Cisco Secure Email Reporting Plug-in:

- Step 1** Download the Email Reporting Plug-in installer from the Cisco Software Download Center.
- Step 2** Double-click the *Cisco Email Reporting Plug-in.exe* file.
- Step 3** In the **Cisco Email Reporting Plug-in Setup** window, select a language, and then click **OK**.
- Step 4** In the message that appears, click **OK** to start an upgrade. The previous version of the Cisco Secure Email Reporting Plug-in will be removed.
- Step 5** Click **Next** to continue upgrading the Cisco Secure Email Reporting Plug-in.
- Step 6** Click **Install** to start installing the latest version.
- Step 7** Wait until the Setup Wizard installs the Cisco Secure Email Reporting Plug-in, and click **Finish**.



Note If you cannot upgrade the Cisco Secure Email Reporting Plug-in, uninstall all previous versions of the plug-in and then perform a fresh install.

Upgrading from the Cisco Secure Email Security Plug-in to the Cisco Secure Email Reporting Plug-in

To upgrade from the Cisco Secure Email Security Plug-in to the Cisco Secure Email Reporting Plug-in:

- Step 1** Download the Email Reporting Plug-in installer from the Cisco Software Download Center.
- Step 2** Double-click the *Cisco Email Reporting Plug-in.exe* file.
- Step 3** In the **Cisco Email Reporting Plug-in Setup** window, select a language, and then click **OK**.
- Step 4** In the message that appears, click **OK** to start an upgrade. The Cisco Secure Email Security Plug-in is removed and the Cisco Secure Email Reporting Plug-in is installed.
- Step 5** Click **Next** to continue upgrading the Cisco Secure Email Reporting Plug-in.
- Step 6** Click **Install** to start installing the latest version.
- Step 7** Wait until the Setup Wizard installs the Cisco Secure Email Reporting Plug-in, and click **Finish**.

Note The Cisco Secure Email Security Plug-in is removed from the Outlook tool bar, and the Cisco Secure Email Reporting Plug-in is available instead.

Installing Cisco Secure Email Reporting Plug-in 1.1.0

- [Installing the Cisco Secure Email Reporting Plug-in, page 4](#)
- [Performing Mass Installation of Cisco Secure Email Reporting Plug-in, page 4](#)

Installing the Cisco Secure Email Reporting Plug-in

To install the Cisco Secure Email Reporting Plug-in:

-
- Step 1** Download the Email Reporting Plug-in installer from the Cisco Software Download Center.
 - Step 2** Double-click the *Cisco Email Reporting Plug-in.exe* file.
 - Step 3** In the **Cisco Email Reporting Plug-in Setup** window, select a language, and then click **OK**.
 - Step 4** Click **Next** to start the installation program.
 - Step 5** Click **Install**.
 - Step 6** Wait until the Setup Wizard installs the Cisco Secure Email Reporting Plug-in, and click **Finish**.
-

Performing Mass Installation of Cisco Secure Email Reporting Plug-in

See [Cisco Secure Email Reporting Plug-in 1.1 Administrator Guide](#) for instructions on how to perform mass installation of Cisco Secure Email Reporting Plug-in.



Note

If you have questions or problems, click the **Help** or **Feedback** links at the top right side of the tool. There is also an interactive tour; to view it, click the link in the orange bar above the search fields

Related Documentation

For more information about the Cisco Secure Email Reporting Plug-in, see:

- [Cisco Secure Email Reporting Plug-in 1.1 Administrator Guide](#). This guide provides instructions for installing and configuring the Cisco Secure Email Reporting Plug-in, and it may help you to understand how to configure your reporting settings to work with the plug-in settings you configure.
- [Cisco Secure Email Reporting Plug-in 1.0 Open Source Documentation](#). This document contains licenses and notices for open source software used in this product.

Service and Support

You can request support by phone, email, or online 24 hours a day, 7 days a week. Cisco Customer Support service level agreement details are available on the Support Portal. You can contact Cisco Customer Support using one of the following methods:

- Cisco Support Portal: <https://www.cisco.com/support>
- Phone support: Contact Cisco Technical Assistance Center (TAC) within U.S. /Canada at 800-553-2447 and at Worldwide Phone Numbers.
- Email: tac@cisco.com

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: <http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>.

To have a list of all new and revised Cisco technical documentation delivered directly to your desktop using a reader application, subscribe to *What's New in Cisco Product Documentation* as an RSS feed by clicking the RSS icon on the What's New page. The RSS feeds are a free service.

This document is to be used in conjunction with the documents listed in the “[Related Documentation](#)” section.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved

