Symantec™ Endpoint Protection 14.2.2.1 Release Notes

Symantec
A Division of Broadcom

Symantec Endpoint Protection Release Notes

Documentation version: 1

Product version: 14.2.2.1 (14.2 RU2 MP1)

This document was last updated on: January 23, 2020 at 16:53

Legal Notice

Broadcom
1320 Ridder Park Drive
San Jose, California
95131

https://www.broadcom.com

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

Symantec Support

All support services will be delivered in accordance with your support agreement and the then-current Enterprise Technical Support policy.

Knowledge Base Articles and Symantec Connect

Before you contact Technical Support, you can find free content in our online Knowledge Base, which includes troubleshooting articles, how-to articles, alerts, and product manuals. In the search box of the following URL, type the name of your product:

https://support.symantec.com

Access our blogs and online forums to engage with other customers, partners, and Symantec employees on a wide range of topics at the following URL:

https://www.symantec.com/connect

Technical Support and Enterprise Customer Support

Symantec Support maintains support centers globally 24 hours a day, 7 days a week. Technical Support's primary role is to respond to specific queries about product features and functionality. Enterprise Customer Support assists with non-technical questions, such as license activation, software version upgrades, product access, and renewals.

For Symantec Support terms, conditions, policies, and other support information, see:

https://entced.symantec.com/default/ent/supportref

To contact Symantec Support, see:

https://support.symantec.com/en_US/contact-support.html

Release notes

This document includes the following topics:

What's new for 14.2 RU2 MP1 (14.2.2.1)

- The Integrations policy includes a new option, **Allow direct traffic when WSS protection is not available**. You use this option to give users access to the web if user authentication with the WSS cloud proxy (ProxySG) fails. This situation occurs if the administrator sets up WSS Traffic Redirection, but not the WSS roaming users.
  Configuring WSS Traffic Redirection
- The Syslog logs for Splunk differentiate whether a scan is a full system scan, quick scan, a manual scan, or a scheduled scan. The logs also show the location information.
- Updated the REST API to include location IDs and location names.
- Support was added for email addresses and distribution lists with special characters.
- Upgraded multiple third-party components to newer versions.

What's new in all releases of Symantec Endpoint Protection

See “Known issues and workarounds” on page 6.

Known issues and workarounds

The items in this section apply to this release of Symantec Endpoint Protection.

- See "Upgrade information" on page 6.
- See "Client information" on page 6.
- See "Symantec Endpoint Protection Manager information" on page 7.

You can view a list of resolved issues for this release at the following location:

New fixes and component versions in Symantec Endpoint Protection 14.2 RU2

Upgrade information

This section contains information about upgrading to the current release of the product.

Custom names may prevent the firewall policy from updating during an upgrade to 14.2 or later

For an upgrade to Symantec Endpoint Protection 14.2 or later, firewall policies cannot incorporate the changes for IPv6 if you changed some default names. The default names include the names of default policies and default rule names. If the rules cannot be updated during the upgrade, the IPv6 options do not appear. Any new policies or rules that you create after the upgrade are not affected.

If possible, revert any changed names back to the default. Otherwise, ensure that any custom rules that you added to a default policy do not block IPv6 communication in any way. Ensure the same for any new policies or rules that you add.

Client information

This section contains information about the Symantec Endpoint Protection client for Windows, Mac, or Linux.

Mac clients that enable WSS Traffic Redirection do not honor custom proxy settings for LiveUpdate

You have configured your managed Mac clients for Symantec Endpoint Protection 14.2 RU1 MP1 or later to use custom proxy settings for LiveUpdate through External Communications Settings. After you enable WSS Traffic Redirection (WTR) for your Mac clients through the Symantec Endpoint Protection Manager policy, however, you find that LiveUpdate traffic no longer honors your custom proxy settings. Instead, LiveUpdate attempts a direct connection.

To work around this issue, only use custom proxy settings for LiveUpdate when WSS Traffic Redirection is disabled.

Microsoft Edge unexpectedly allows PDF downloads with Hardening enabled

With Application Hardening enabled in the Symantec Endpoint Protection client, you are unexpectedly able to download PDF files if you use the Microsoft Edge browser. The prevention of the download of PDF files works as expected with other browsers.

A fix for this issue is planned for a future release.

Symantec Endpoint Protection Manager information

This section contains information about Symantec Endpoint Protection Manager.

"Deployment in progress" still appears in Symantec Endpoint Protection Manager after the client receives an updated policy for Endpoint Threat Defense for AD

You apply a policy for Symantec Endpoint Threat Defense for Active Directory 3.3 to a group. This group contains some clients that run Symantec Endpoint Protection 14.2 RU1 or earlier. These clients receive and apply the policy as expected, but the status in Symantec Endpoint Protection Manager continues to show the message **Deployment in progress**.

This behavior is expected. Endpoint Threat Defense for AD 3.3 policies are only supported on the client as of version 14.2 RU1 MP1.

Remote Java Console access to Symantec Endpoint Protection Manager fails with FIPS enabled

In a FIPS-compliant environment, access to Symantec Endpoint Protection Manager 14.2 RU1 MP1 or later using the Java remote console fails with the error: "Failed to validate certificate. The application will not be executed." This error results from an incompatibility between Crypto-J and JRE 8. To work around this issue, access Symantec Endpoint Protection Manager using the web console.

Remote Java Console access to Endpoint Protection Manager fails with FIPS enabled

System requirements for Symantec Endpoint Protection

In general, the system requirements for the following are the same as those of the operating systems on which they are supported:

- Symantec Endpoint Protection Manager
- The Symantec Endpoint Protection clients

The system requirements for this release appear on the following pages:

- System requirements for Symantec Endpoint Protection 14.2 RU1 MP1 through 14.2 RU2 MP1

Supported upgrade paths to the latest version of Symantec Endpoint Protection 14.x

Symantec Endpoint Protection Manager and Windows client

The following versions of Symantec Endpoint Protection Manager and Symantec Endpoint Protection Windows client can upgrade directly to the current version:

- 11.x and Small Business Edition 12.0 (Symantec Endpoint Protection clients only, for supported operating systems)
- 12.1.x, up to 12.1.6 MP10
- 14
- 14 MP1
- 14 MP2
- 14 RU1
- 14 RU1 MP1
- 14 RU1 MP2
- 14.2
- 14.2 MP1
- 14.2 RU1
- 14.2 RU1 MP1
- 14.2 RU2

Mac client

The following versions of Symantec Endpoint Protection client for Mac can upgrade directly to the current version:

- 12.1.4 - 12.1.6 MP9
  The Mac client did not update for version 12.1.6 MP10.
- 14
- 14 MP1
- 14 MP2

- 14 RU1
- 14 RU1 MP1
- 14.2
- 14.2 MP1
- 14.2 RU1
- 14.2 RU1 MP1
- 14.2 RU2

Note: The Symantec Endpoint Protection client for Mac was not updated for 14.0.1 MP2.

Linux client

The following versions of Symantec Endpoint Protection client for Linux can upgrade directly to current version:

- 12.1.x, up to 12.1.6 MP9
  The Linux client did not update for version 12.1.6 MP10.
- 14
- 14 MP1
- 14 MP2
- 14 RU1
- 14 RU1 MP1
- 14 RU1 MP2
- 14.2
- 14.2 MP1
- 14.2 RU1
- 14.2 RU1 MP1
- 14.2 RU2

Symantec AntiVirus for Linux 1.0.14 is the only version that you can migrate directly to Symantec Endpoint Protection. You must first uninstall all other versions of Symantec AntiVirus for Linux. You cannot migrate a managed client to an unmanaged client.

Unsupported upgrade paths

You cannot migrate to Symantec Endpoint Protection from all Symantec products. You must uninstall the following products before you install the Symantec Endpoint Protection client:

- The unsupported Symantec products Symantec AntiVirus and Symantec Client Security
- All Symantec Norton™ products
- Symantec Endpoint Protection for Windows XP Embedded 5.1
- Versions of Symantec Endpoint Protection for Mac earlier than 12.1.4

You cannot upgrade Symantec Endpoint Protection Manager 11.0.x or Symantec Endpoint Protection Manager Small Business Edition 12.0.x directly any version of Symantec Endpoint Protection Manager 14. You must first uninstall these versions or perform an upgrade to 12.1.x before an upgrade to 14.x.

Downgrade paths are not supported. For example, if you want to migrate from Symantec Endpoint Protection 14.2.1.1 to 12.1.6 MP10, you must first uninstall Symantec Endpoint Protection 14.2.1.1.

If you have a build number but you are not sure how it translates to release version, see:

- Released versions of Symantec Endpoint Protection
- About Endpoint Protection release types and versions

Where to get more information

Table 1-1 displays the websites where you can get best practices, troubleshooting information, and other resources to help you use the product.

Table 1-1 Symantec website information

Types of information	Website link
Trial versions	Trialware

Table 1-1 Symantec website information *(continued)*

Types of information	Website link
Manuals and documentation updates	**English:** ■ Symantec Product Documentation ■ Product guides for all versions of Symantec Endpoint Protection 14.x **Other languages:** ■ Brazilian Portuguese ■ Chinese (simplified) ■ Chinese (traditional) ■ French ■ German ■ Italian ■ Japanese ■ Korean ■ Spanish * Czech, Polish, and Russian files are on the English page.
Technical Support	Endpoint Protection Technical Support Includes knowledge base articles, product release details, updates and patches, and contact options for support.
Threat information and updates	Symantec Security Center
Training	Symantec Education Services Access the training courses, the eLibrary, and more.
Symantec Connect forums	Endpoint Protection