Symantec™ Endpoint Detection and Response 4.6 Release Notes

Table of Contents

Copyright statement

Symantec EDR documentation support

Symantec EDR support site

Open a troubleshooting ticket, obtain a license, access training, and get product downloads:

https://support.broadcom.com/security

Symantec EDR documentation set

Access online Symantec EDR documentation at the following site:

http://techdocs.broadcom.com/content/broadcom/techdocs/us/en/symantec-security-software/endpoint-security-and-management/endpoint-detection-and-response/4-6.html

The Symantec EDR documentation set consists of the following:

Document	Description
Symantec EDR online help	All of the topics that you need to: • Size your Symantec EDR deployment • Install and upgrade Symantec EDR and perform the initial configurations • Configure the Symantec EDR appliance • Set up users and roles to access the EDR appliance console • Integrate Symantec EDR with third-party applications (e.g., Splunk and ServiceNow) • Use Symantec EDR to detect indicators of compromise and remediate threats in your environment
Symantec Endpoint Detection and Response Release Notes	Information you need to know about this release of Symantec EDR, including what's new in this release, upgrade considerations, and known and resolved issues. To learn about any issues that arose after the publication of the Release Notes, see Late Breaking News at: Symantec EDR Late Breaking News
Symantec Endpoint Detection and Response Installation Guide for Dell 8840 and 8880 appliances	Complete explanations of the planning, installation, and setup tasks for the Dell 8840 and 8880 physical appliance.
Symantec Endpoint Detection and Response Installation Guide for the Symantec S550 appliance	Complete explanations of the planning, installation, and setup tasks for the S550 appliance.
Symantec Endpoint Detection and Response Installation Guide for virtual appliances	Complete explanations of the planning, installation, and setup tasks for a virtual appliance.
Symantec Endpoint Detection and Response Threat Discovery Guide	Information, including queries and descriptions, to help you discover threats to your network environment using Symantec EDR.
Symantec Endpoint Detection and Response Sizing and Scalability Guide	Sizing considerations and vertical scaling, and other topics designed to help you with recommendations on how to grow your deployment.

Access Symantec EDR .pdfs in the Related Documents topic.

https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-detection-and-response/4-6/Related-Documents.html

Symantec EDR assets

You can view assets, such as the License Agreement, Product Use Rights Supplement, Third-party Notice, on the following site:

https://www.broadcom.com/support/download-search

To view assets related to Symantec EDR, select the following fields:

- **Product Group**: Symantec Cyber Security
- **Product Family**: Endpoint Security
- **Product Name**: Endpoint Detection and Response
- **Asset Type**: Click the drop-down menu to select that asset that you want to view (e.g., License Agreement).

What's new in Symantec Endpoint Detection and Response 4.6

Feature	Description
Export/import Symantec EDR configuration settings.	Export/import Symantec EDR configuration settings to: • Restore an appliance after an unexpected failure • Migrate installations (such as data center relocations, setting up test labs, etc.) • Restore settings on the appliance after a fresh installation • Replicate settings to other appliances, thereby eliminating the need to manually configure each appliance
Targeted Attack Analytics (TAA) is automatically enabled when a valid Symantec EDR is registered.	In prior releases of Symantec EDR, you had to upload a Symantec Endpoint Protection (SEP) license in the EDR appliance console to enable TAA detections. Now TAA is automatically enabled when you initially install or renew a valid, Symantec EDR license.
Mac SEP agent support	Symantec EDR supports enrolling Mac endpoints that meet the following requirements: • The Mac endpoint must be running the SEP 14.3 RU2 or later client. This version of the SEP client is only supported on Mac 10.5 and 11. • You must be running SEPM 14.3 RU2 or later. Important information about upgrading The ability to specify which events are forwarded from Mac clients to Symantec EDR is currently unsupported. However, Mac endpoints forward the following event types to Symantec EDR: • 8001: Process Event • 8003: File Event • 8016: Startup Application Configuration Change
New incident detections.	Symantec EDR includes the following detection types: • Multiple failed logon attempts detected on {device_name} • Multiple account enumeration attempts have been detected on {device_name}
New event type.	Symantec EDR now detects Startup Application Configuration Changes (type_id 8016). This event type is supported on Windows and Mac endpoints. You can also configure Symantec EDR to forward this event type to third-party SIEMs (such as Splunk or ICDx).
New Splunk requirements.	The Symantec EDR app supports Splunk Enterprise version 8.1 or later using Python interpreter version 3. For more information about the *Symantec™ Endpoint Detection and Response App for Splunk® Administration Guide*.

Important information about upgrading

Upgrading Symantec EDR 4.6 before you upgrade to SEPM 14.3 RU2

A connect token is generated immediately after you install or upgrade to Symantec EDR 4.6, and that token is pushed to SEPM 14.3 RU1 as part of the private cloud policy. But SEPM 14.3 RU1 doesn't support the connect token. So the token is dropped. After you upgrade to SEPM 14.3 RU2, the Mac agent won't have the connect token needed to enroll with Symantec EDR.

If you install or upgrade to Symantec EDR 4.6 before you upgrade to SEPM 14.3 RU2 or make changes to SEPM Controller group inclusions, you must run the following command-line command to ensure that connection token is pushed to the SEPM private cloud settings and Mac endpoints can enroll with Symantec EDR.

```
generate_new_connect_token
```

Synapse Log Collector utility and Symantec EDR embedded database changes

Symantec Endpoint Protection Manager (SEPM) 14.3 RU1 updates its embedded database to Microsoft SQL Express. SEPM no longer supports the Sybase embedded database or the Synapse Log Collector. If SEPM detects the Sybase embedded database and Synapse Log Collector when you upgrade to SEPM 14.3 RU1, it uninstalls them.

Symantec recommends that you upgrade to Symantec EDR 4.5 or later first, then upgrade to SEPM 14.3 RU1. When performed in this order, Symantec EDR automatically re-establishes the database connection to SEPM's Microsoft SQL Express embedded database. You might see a connection error while the re-configuration to the MS SQL Express embedded database occurs. If the issue persists, you can manually configure the MS SQL Express embedded database connection.

If you upgrade to SEPM 14.3 RU1 first before you upgrade to Symantec EDR 4.5 or later, SEPM uninstalls the Sybase embedded database and the Synapse Log Collector. Symantec EDR no longer receives logs from SEPM until you do either of the following tasks:

- Upgrade to Symantec EDR 4.5 or later (upon upgrade, Symantec EDR automatically configures the connection to the MS SQL Express embedded database). For the connection to be automatically re-established, you must also have SEPM Controller connection for same SEPM server.
- Edit the existing SEPM database connection and change the type to MS SQL. Or you can delete the existing connection to the SEPM embedded database and then configure a new connection to the MS SQL Express embedded database.

If you were not using the SEPM embedded database and instead had configured an external MS SQL Server database before you perform either upgrade, no changes are required.

If a self-signed certificate was used in the SEPM Sybase embedded database setup, the connection appears in the EDR appliance console as "Unencrypted".

Reconfigurations to the SEPM database are logged in the Symantec EDR Audit log.

If you are upgrading from Symantec EDR 4.3 or earlier and are using the Synapse Log Collector, and you are using SEPM 14.3 MP1 or earlier, you must reinstall the log collector with a new SEPMLogCollector.msi for Symantec EDR. Configure the log collector on the **Settings > Global** page. The new log collector enables Symantec EDR to perform enhanced correlation between Advanced Attack Technique-based incidents and SEP detections.

When you install the new log collector .msi file for Symantec EDR 4.5 or later, you receive this enhanced functionality. If you continue to use a log collector installed from a prior version of Symantec EDR, the prior functionality still exists.

Migration of endpoint activity recorder exclusions to recorder rules

The endpoint activity recorder exclusions that you created when you configured the SEPM Controller in Symantec EDR 4.4 and earlier are migrated to the **Recorder** policy tab. The migrated rules are designated as **Disable Monitoring Rules**, and there is no limit as to how many rules can be migrated. However, you cannot create any additional **Disable Monitoring Rules** until the count of **Disable Monitoring Rules** is 200 rules or less.

The **Endpoint Activity Recorder Exclusions** page in Symantec EDR 4.4 and earlier is renamed to the **Endpoint Activity Recorder Rules** in Symantec EDR 4.5.

Changes to the single sign-on (SSO) feature

If you upgrade from Symantec EDR 4.3 and earlier, changes to the SSO feature require that you perform actions after migration to continue to use this feature.

- If you use Norton Secure Login (NSL):
  NSL is no longer supported. Upon migration, the SSO link on the EDR appliance console logon page and related settings on the **Settings > Data Sharing** page no longer appear. To continue using SSO, configure a new identity provider (IdP) (for example, Okta).
- If you use any IdP other than NSL:
  a. In the EDR appliance console on the left navigation pane, click **Settings > Data Sharing**.
  b. In the **Single Sign-On** section, click the three vertical dots to reveal edit icons for each of the SSO configuration panels.

  c. Click **URLs for Identity Provider**.
  d. Copy and paste the Symantec EDR URLs to the appropriate fields in your IdP administration console.
  e. Download the Symantec EDR `sso.cert` and upload it to your IdP.
  f. Verify that the fields in the other panels are still the proper parameters for your IdP.

Understanding the upgrade path

If you run the Symantec Advanced Threat Protection (ATP) 3.1, 3.2 or Symantec EDR 4.0 or later, you can upgrade to Symantec EDR 4.6.

Troubleshooting

Release notes, new fixes, and system requirements for Endpoint Security and all versions of Endpoint Protection

About software updates

Symantec Endpoint Detection and Response software updates are periodically available to provide improved performance, functionality, enhancements, and security. Symantec EDR checks daily for updates. You are notified of an available update as follows:

- The EDR appliance console System Health appears in yellow with the status **System Needs Attention**. Mousing over the message displays a pop-up message that an update is available.
- An update notifications appears in the EDR appliance console on the **Settings** > **Appliances** page.

  NOTE
  The **Update Software** option may not appear until 24-48 hours after the update is available.
- You'll receive an email if you configured Symantec EDR to send email notifications.

It's important that you do the following when updating the software:

- Perform a backup.
  To mitigate risks, complete a full backup before you perform a software update. Do not perform or restore a backup during the upgrade process.
  Refer to the following knowledge base article for backup/restore procedures related to Symantec EDR builds prior to version 4.3:
  Preparation checklist for reinstalling ATP 3.x
- Each appliance must be updated separately.
- Upgrade the management platform before you upgrade remote scanners.
- Do not turn off your appliance or restart Symantec EDR during the upgrade process.
- Do not change any of your configuration settings during the upgrade process.
  If you change your settings during the upgrade process, you may corrupt your database.

Performing an upgrade from the command line

Performing an upgrade from the command line

Before you begin, make sure you review the important information about software updates.

About software updates

1. From your Symantec EDR Management Platform server, open a console window.
2. At the command prompt, type `update download`.

   The latest version of Symantec EDR downloads to your local cache.
3. Type `update install`.

   Symantec EDR installs, and then the server automatically reboots.
4. Repeat steps 1-3 on each of your remote scanner servers.

   NOTE

   Check the status of the update by typing the following command:

   `update status`

Troubleshooting

See the following article if you upgrade Symantec EDR after you have recently updated your license and the following error appears:

```
[Error 14] HTTPS Error 471 - The requested URL returned error: 471 inactivated key
```

.

Unable to update Symantec Advanced Threat Protection or Symantec Endpoint Detection and Response via CLI

Symantec EDR version support for appliances

The Symantec S550 appliance supports Symantec EDR 4.1 and later.

The following appliance models support Advanced Threat Protection 3.0 and later and Symantec EDR 4.0 and later:

- Dell 8880
- Dell 8840

Symantec EDR 8880 and 8840 appliances include an Integrated Dell Remote Access Controller (iDRAC). The iDRAC console requires the latest version of the Java Runtime Environment (JRE) installed on your administrative client.

Warranty information for Dell appliances

Browser requirements for the EDR appliance console

Browser requirements for the EDR appliance console lists the web browsers that are compatible with the EDR appliance console. JavaScript must be enabled in the browser and cookies must be allowed. The minimum resolution for viewing the EDR appliance console is 1280x1024.

Table 1: Browser requirements for the EDR appliance console

Browser	Version
Mozilla Firefox	86.0 or later (64-bit)
Google Chrome	Version 88.0.4324.190 or later (64-bit)
Microsoft Edge	Version 88.0.705.81 or later (64-bit)

NOTE
Browsers not listed above are unsupported.

System requirements for the virtual appliance

IMPORTANT
It's imperative that your virtual computer has the proper resources allocated **before** you power on the VM. Otherwise, you will experience disk space or high-memory usage errors. Also, a lack of CPU cores could also result in failure to raise services during the boot sequence and/or an inability to open the EDR appliance console. See the *Symantec Endpoint Detection and Response Installation Guide for virtual appliances* for more information.

System requirements for a virtual appliance installation lists the system requirements for the virtual appliance. These requirements differ if you use Symantec EDR's endpoint activity recorder feature. The endpoint activity recorder collects data from your endpoints, which is then stored in Symantec EDR's database. As such, Symantec EDR requires more system resources and storage space when the endpoint activity recorder is enabled.

Table 2: System requirements for a virtual appliance installation

Requirement	Minimum per VM for production environment without endpoint activity recorder feature	Minimum per VM for production environment with endpoint activity recorder feature
Disk space	500 GB	1.5 TB (1 TB hard disk in addition to the VM's existing 500 GB hard disk)
CPU	12 Cores	12 Cores
Memory	48 GB	48 GB
VMware	VMware ESXi version 6.5 U1 or later OVA template ESX 6.5 or later Refer to your VMware documentation for VMware system requirements and configuration of virtual machines.	

Additional requirements are as follows:

- Use the proper block size, depending upon the VMFS version of your system. If your ESXi server is using VMFS-2, then set block size to 4MB or greater.
- If you are using a file system later than VMFS-2, then set block size to 8MB or greater.

System requirements for SEP integration

Symantec Endpoint Protection version requirements

Symantec Endpoint Detection and Response can integrate with Symantec™ Endpoint Protection for enhancing event information and providing Endpoint Communications Channel (ECC) functionality. Symantec EDR has certain version requirements based on various components of SEP.

The minimum SEPM version is 12.1 RU6 or later. Symantec EDR can connect to multiple SEP sites with one connection per SEP site, up to a total of ten connections to SEPM hosts.

Symantec EDR can manage the client endpoints that run SEP version 12.1 RU 6 MP3 or later with full ECC functionality. However, clients must be running SEP 14 or later to take advantage of ECC 2.0 functionality.

Client endpoints that run versions earlier than SEP 12.1 RU5 are not supported. Some functionality is limited for the clients that run on versions between SEP 12.1 RU5 and 12.1 RU6 MP3. The Symantec EDR documentation describes any functionality limits based on the version of the SEP client.

Synapse log collector database requirements

SEPM 14.3 RU1 or later uses Microsoft SQL Express as its database for log collection. Symantec EDR can access the database without any special host system requirements.

SEPM 14.3 MP1 or earlier supports either the MS SQL Server database or an embedded database. When SEPM uses an embedded database, Symantec EDR uses a log collector on the SEPM host. This log collector requires the SEPM host to be running one of the following operating systems:

- Windows 7 (64-bit only)
- Windows 8 (64-bit only)
- Windows Server 2008
- Windows Server 2012
- Windows Server 2012 R2 or later (recommended)

See the Symantec Endpoint Protection documentation for SEPM system requirements.

Required firewall ports

Depending on your network layout, you may need to open some ports on your firewall and edit your firewall rules. These changes let you access the important web addresses that are essential for Symantec Endpoint Detection and Response operations.

Symantec EDR web and IP addresses lists the web and IP addresses to which Symantec EDR requires access.

Table 3: Symantec EDR web and IP addresses

Web addresses/IP Address	Protocol	Port	Description
• remotetunnel1.edrc.symantec.com • remotetunnel2.edrc.symantec.com • remotetunnel3.edrc.symantec.com • remotetunnel4.edrc.symantec.com • remotetunnel5.edrc.symantec.com	HTTPS	443	Permits Symantec Support remote access to the Symantec EDR appliance.
https://api-gateway.symantec.com	TCP	443	Accesses Symantec's Targeted Attack Analytics service.
licensing.dmas.symantec.com	TCP	443	Used to get the Cynic license.
api.us.dmas.symantec.com api.eu.dmas.symantec.com	TCP	443	Used to perform queries to the Cynic US and UK servers (required).
liveupdate.symantec.com	TCP	80	Used to check for and download definitions for Symantec's detection technologies.
ratings-wrs.symantec.com	TCP	443	Used to query Norton Safe Web server to identify malicious websites.
stnd-avpg.crsi.symantec.com stnd-ipsg.crsi.symantec.com https://central.b6.crsi.symantec.com https://bash-avpg.crsi.symantec.com	TCP	443	Used to send detection telemetry to Symantec.
register.brightmail.com	TCP	443	Used to register the appliance.
swupdate.brightmail.com	TCP	443	Used to check for and download new releases of Symantec EDR.
shasta-rrs.symantec.com shasta-mrs.symantec.com	TCP	443	Used to perform reputation lookups for Windows executable and APK installable files.
datafeedapi.symanteccloud.com	TCP	443	Used to download Email Security.cloud and EDR: Roaming events.
telemetry.broadcom.com	TCP	443	When telemetry is configured, used to send statistics telemetry to Symantec.
EDR appliance console	TCP	443 (inbound) or in the range of 1024 to 9997	Access to Symantec EDR public API.
https://sso1.edrc.symantec.com	TCP	443	Used for SSO.

Symantec EDR ports and settings describes the ports that Symantec EDR uses for communications, content updates, and interactions with Symantec.cloud detection services.

Table 4: Symantec EDR ports and settings

Service	Protocol	Port	From	To	Description
Back up	FTP; SSH	20 TCP, UDP 21 TCP 22 TCP, UDP	Management platform or all-in-one appliances	Configured backup storage server (Internal traffic)	FTP server: FTP ports 20, 21 SSH server: SSH port 22
Email notifications	SMTP	25 TCP 587 TCP	Management platform or all-in-one appliance	SMTP server (Internal traffic)	Communication with the SMTP server.
Content updates	HTTP	80 TCP	All appliances	Symantec (External traffic)	Virus and Vantage definitions, and other content that LiveUpdate delivers . This port is required for proper functioning of the product.
Statistics delivery	HTTP	80 TCP	All appliances	Symantec (External traffic)	Sends the data to Symantec for statistical and diagnostic purposes. Private data is not sent over this port.
(ECC) 2.0	HTTPS HTTP	443 80	Managed SEP endpoints	Symantec EDR	Communicates commands to the endpoints.
ECC 1.0	HTTPS	8446	Symantec EDR	SEPM	Commands to SEPM.
RRS/endpoint submissions ECC 2.0	HTTPS HTTP	443 8080	SEP	Symantec EDR	The SEPM private cloud that lets endpoints communicate with Symantec EDR.
RRS/endpoint submissions ECC 1.0	HTTPS HTTP HTTP	443 80 8443[1]	SEP	Symantec EDR	The SEPM private cloud that lets endpoints communicate with Symantec EDR.
Symantec cloud detection, analysis, and correlation services and telemetry services	If endpoint activity recorder enabled If endpoint activity recorder disabled	443 TCP	All appliances	Symantec (External traffic)	Cloud service queries and telemetry data exchanges . If the endpoint activity recorder is enabled SEP sends conviction events directly to Symantec EDR.
Antivirus and intrusion prevention conviction information	HTTPS	HTTP 8080 TCP or HTTPS 443 TCP HTTP 80 TCP or HTTPS 8443 TCP	SEP clients	Symantec EDR management platform	Information about the files and the network traffic that SEP detects.
Antivirus and intrusion prevention conviction information	HTTPS HTTP	443 TCP 80	Symantec EDR management platform	Symantec (External traffic)	Information about files and the network traffic that SEP detects.
Product updates	HTTPS	443 TCP	All appliances	Symantec (External traffic)	Finds and delivers new versions of Symantec EDR.
EDR appliance console	HTTPS	443 TCP 443 (inbound) or in the range of 1024 to 9997	Client connecting to manage an appliance	Management platform or all-in-one appliance (Internal traffic)	EDR appliance console access for an all-in-one appliance or management platform.

Service	Protocol	Port	From	To	Description
EDR appliance console, network scanners, and all-in-one	SSH	22	Client connecting to manage an appliance	Management platform, scanner, or all-in-one appliance (Internal traffic)	Command-line access for an all-in-one appliance or management platform.
Synapse SEPM connection with Microsoft SQL Server (optional)	JDBC	1433 TCP (default)	Management platform or all-in-one appliance	SEPM Microsoft SQL Server (Internal traffic)	Required if using the Microsoft SQL Server for SEPM and Synapse. SEPM administrators can configure a different port for this communication.
Communication channel (management platform and network scanner installations only)	AMQP	5671 TCP 5672 TCP	Network scanner appliance	Management platform (Internal traffic)	Communications between the management platform and network scanners. Not required for an all-in-one installation. After the initial exchange on this port, the communication is secured.
Blocking page (Inline Block mode only)	HTTP	8080 TCP	Network scanner	Protected endpoints (Internal traffic)	Sends the blocking page when content is blocked at an endpoint. Not required for Inline Monitor or Tap/Span modes.
Synapse SEPM connection with Embedded DB (optional) Supported for SEPM 14.3 MP1 and earlier.	HTTPS	8081 TCP (default)	Management platform or all-in-one appliance	SEPM server (Internal traffic)	Required if using the embedded database for Synapse connection to SEPM.
Connection to SEPM database	HTTPS	2638 TCP (default)	Management platform or all-in-one appliance	MS SQL Express	
Synapse SEPM connection with the SEPM web services Remote Management and Monitoring (RMM) service (optional)	HTTPS	8446 TCP (default)	Management platform or all-in-one appliance	SEPM Server	Required if connecting to the SEPM server for executing management operations. For example, adding or removing items from the blacklist or placing an endpoint under quarantine.
Syslog	Syslog	TCP (preferred) or UDP port should be the same as configured in the EDR appliance console for syslog	All appliances	Configured Syslog server (Internal or external traffic based on your environment)	If syslog is configured, this connection delivers log messages to remote syslog.
EDR: Email EDR: Roaming	HTTPS	443 TCP	Management platform or all-in-one appliance	Symantec	This connection lets Symantec EDR collect conviction events from EDR: Roaming and EDR: Email when Synapse Correlation is enabled for either one of these services.

Service	Protocol	Port	From	To	Description
Active Directory	LDAPS	636	Management platform or all-in-one appliance	Active Directory server	This connection allows Symantec EDR to integrate with Active Directory for user authentication.
Security Analytics link	HTTPS TCP/UDP	443	Management platform or all-in-one appliance	Symantec Security Analytics appliance or virtual appliance	This connection lets Symantec EDR integrate with Symantec Security Analytics to provide a link on individual log events to navigate users to additional information on related network motion.

[1] Port 8443 is only available if you were using this port on previous versions of Symantec EDR and have since updated. If you are installing Symantec EDR for the first time, this port is not available.

Troubleshooting

SEDR logs show connections towards URL "central.crsi.symantec.com"

Known issues in Symantec EDR 4.6

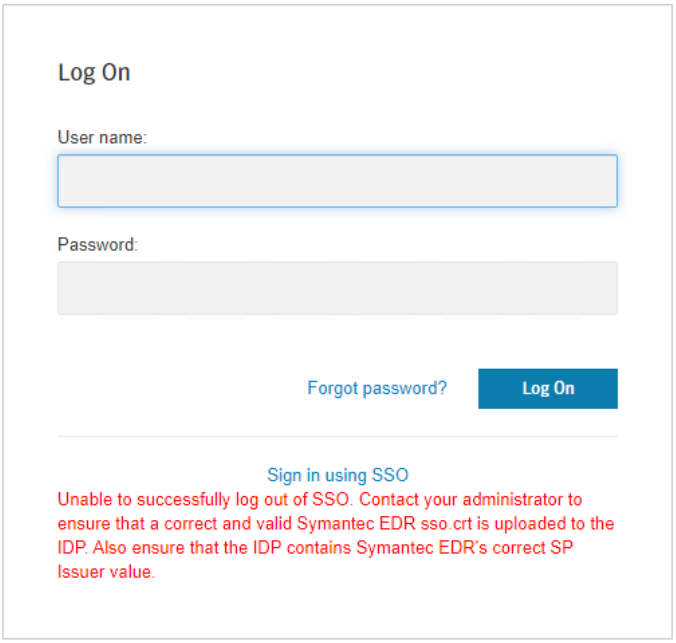
Known issue	Description
Exception policy rules are not removed from SEPM server after SEPM Controller is removed from Symantec EDR.	After you export the EDR configuration settings, you are able to successfully import the configuration settings file. But when you open the **SEPM Controller Connection** dialog box and add the SEPM password, you see the following error message: `SEPM communication has encountered an unexpected error` https://knowledge.broadcom.com/external/article?articleId=208385
After switching a Symantec EDR Scanner mode between Inline and TAP, no detections are seen.	When switching a Symantec EDR appliance in Scanner or All-in-One mode from Inline to TAP, or TAP to Inline, there are no further detections. https://knowledge.broadcom.com/external/article?articleId=210128
Unable to upgrade.	See the following KB article about how to upgrade using the command line. https://knowledge.broadcom.com/external/article?legacyId=TECH232126
Events reporting fDenyTSConnections reg key changes are not accurate in the description or are missing.	When launching the following command to disable RDP on a Windows endpoint with a Symantec Endpoint Protection (SEP) client installed, Symantec EDR either shows no event or has an event that in-accurately reports "RDP enabled." Reg add “HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server” /v fDenyTSConnections /t REG_DWORD /d **1** /f This behavior is the result of an error in the global Intellifilter rules within the SEP client. https://knowledge.broadcom.com/external/article/200340
Alerts about certificate expiration for SEPM Controller that was removed from Symantec EDR.	You may see a system health alert for an expired SEPM certificate, even if the host or IP address that the certificate is for is no longer configured on the Symantec EDR appliance. This can occur if an older SEPM was previously configured and the database entry for it was not properly purged. Contact Broadcom technical support for manual remediation. https://knowledge.broadcom.com/external/article?articleId=194797
VM endpoints taking longer than standard endpoints to enroll.	Enrollment for non-persistent VDIs into Symantec EDR is significantly slower and can take anywhere from 30 minutes to several hours. https://knowledge.broadcom.com/external/article?articleId=209338
Network slowness when adding subnets in "Internal Network Configuration".	Network Latency was observed for traffic that is sent through Inline EDR scanners with large number of Policy entries. https://knowledge.broadcom.com/external/article/205995

Known issue	Description
Inherited sub-groups count does not update the first time the SEPM Controller launches.	If the **Settings > Global** page is opened when you add sub-groups to the SEPM, the inherited sub-groups count in the EDR appliance console does not update. Do one of the following tasks for a workaround: • Navigate to another page in the EDR appliance console, then go back to the **Settings > Global > SEPM Group Inclusions** page. • Close the browser tab, log into the EDR appliance console again, then go to the **Settings > Global > SEPM Group Inclusions** page. https://knowledge.broadcom.com/external/article?articleId=192406
Multi-select option is slow when there are a lot SEPM groups.	Symantec engineering is investigating this issue. https://knowledge.broadcom.com/external/article?articleId=192409
EDR appliance console times-out before a console operation finishes.	You should be able to edit the settings again, and the list of groups are cached. https://knowledge.broadcom.com/external/article?articleId=192410
When configuring the endpoint activity **Recorder Group Exceptions** settings, the settings are lost if they are saved with a SEPM group name that has since been renamed.	Before making changes to the endpoint activity recorder settings, consider editing the **SEPM Group Inclusions** list first and refreshing the list of SEPM groups. The list can become out-of-date if your SEPM admins have made recent changes that have not replicated or changes were made to in Active Directory to AD-connected SEPM groups. https://knowledge.broadcom.com/external/article?articleId=192407
Multi-column search for Database Entity does not work on OS and some other columns.	Symantec engineering is investigating this issue. https://knowledge.broadcom.com/external/article?articleId=192209
Endpoint activity recorder searches fail with "CLIENT_ERROR_UPLOAD_RESULTS"	Symantec EDR aborts commands if the client is in the process of shutting down. https://knowledge.broadcom.com/external/article?articleId=192212
Symantec EDR API and EDR appliance console event query is not working as expected.	Symantec engineering is investigating this issue. https://knowledge.broadcom.com/external/article?articleId=192098
File name with Right To Left Order character causes Symantec EDR to display string backwards.	Symantec engineering is investigating this issue. https://knowledge.broadcom.com/external/article?articleId=192191
Synapse Error- Symantec EDR license expired. Functionality disabled despite a new, valid license being uploaded.	Symantec EDR recovers if it passes from an unlicensed to licensed state either by the passage of time or installing license files. The system behaves as expected if passing from licensed to unlicensed by passage of time. There is no scenario to un-license a system by installing files. However, the EDR appliance console appears to not automatically update itself in a timely fashion. https://knowledge.broadcom.com/external/article?articleId=192173
Inconsistent enrollment.	The Enrollment Summary can display a wrong count of enrolled and online clients. It can also vary over time when clients are powered off or disconnected (e.g. over the weekend). https://knowledge.broadcom.com/external/article?articleId=210247
Endpoint search results same the same file having multiple SHA256 hashes.	This issue occurs because SEP forwards the alternate data streams for the file to Symantec EDR. All reported SHA256 hashes for the file are valid. https://knowledge.broadcom.com/external/article?articleId=210123
Fail to send SEP event to Symantec EDR.	The .json files that are provided to Symantec EDR by SEPM are not formatted properly or blank . https://knowledge.broadcom.com/external/article?articleId=210261

Known issue	Description
Context-sensitive help in EDR appliance console doesn't work if browser language is not a English.	When clicking one of the blue ? icons in the EDR appliance console to access context-sensitive help, if the browser language is anything other than one of the supported localized languages (EN, ES, FR, JA), no help topic does not appear. https://knowledge.broadcom.com/external/article?articleId=210361
IPv6 support on Symantec EDR appliance.	The Symantec EDR software supports IPv6 for endpoint event data and supports IPv6 network traffic for Inline scanning interfaces. There is no way to assign an IPv6 address for the Management interface. https://knowledge.broadcom.com/external/article?articleId=174564
When importing Active Directory settings in to Symantec EDR from exported settings, the import fails.	Edit the DNS settings to match those on Active Directory, then re-import the Active directory settings. https://knowledge.broadcom.com/external/article/210374
Endpoint scan and remediation commands are stuck in the 'Started' state.	This action can occur if the endpoint's operating system was restarted after the search or remediation command was issued in Symantec EDR. https://knowledge.broadcom.com/external/article?articleId=210038

Resolved issues in Symantec EDR 4.6

Issue	KB link
Events reporting fDenyTSConnections reg key changes are not accurate or missing in the **Description** field.	When launching a command to disable RDP on a Windows endpoint with Symantec Endpoint Protection (SEP) client installed, Symantec EDR either shows no event or has an event that inaccurately reports "RDP enabled". https://knowledge.broadcom.com/external/article?articleId=200340
Upgrade to Symantec 4.5 will replace existing default self-signed certificate.	If you are using the default self-signed Symantec EDR certificate, it is replaced with a new self-signed certificate when you upgrade to Symantec EDR 4.5.0. In this case, if you have not replaced the default self-signed certificate, you may see a browser warning when you open the EDR appliance console. A workaround to the browser warning is to ensure that your browser trusts Symantec EDR's self-signed certificate. Some examples are to use a trusted CA signed certificate, or import Symantec EDR's self-signed certificate into a Windows certificate store where the browser is being used. Upon upgrade, the new, default self-signed certificate is automatically pushed to your managed SEP endpoint agents for continued secure communication with Symantec EDR. https://knowledge.broadcom.com/external/article?articleId=203226
The **edr_data_protocols** field is not present in event type_id 8007 from SEP 14.2 RU2 client.	The Symantec EDR engineering team is working to resolve this issue. https://knowledge.broadcom.com/external/article?articleId=200341
Targeted Attack Analytics (TAA) status that is stuck at PENDING after license upload.	The Symantec EDR engineering team is working to resolve this issue. There is no related KB for this issue.
Extraneous error when entering domain information after choosing **Submit to Sandbox** for a non-PE file.	This issue is resolved in Symantec EDR 4.5 by requiring the FQDN for the domain, including the TLD. Example: adfs.contoso.net https://knowledge.broadcom.com/external/article?articleId=192189
Most TAA incidents not displaying in EDR appliance console.	This can occur under the following circumstances: 1. The license file(s) uploaded to the appliance are used on a SEPM other than the one configured in the appliance. SEP clients upload telemetry submissions and are correlated by their license file. 2. The SEPM is configured correctly, but the SEPM group(s) to which the unknown endpoint(s) belong to have not been selected for group inclusion. 3. The SEP client was previously known to Symantec EDR, but the record may have been purged from the appliance database. https://knowledge.broadcom.com/external/article?articleId=173639
Symantec EDR shows "DUMMY" MD5 hash for events.	EDR shows bd2103035a8021942390a78a431ba0c4 in some events/incidents. https://knowledge.broadcom.com/external/article?articleId=192099

Issue	KB link
In 'Summary' of Executive Report, the **Total # of infected endpoints with SEP** is high.	The Symantec EDR engineering team is working to resolve this issue. https://knowledge.broadcom.com/external/article?articleId=200242
Closed incident gets re-created (same event appears as a "CLOSED" incident and "NEW" incident).	When reviewing incidents on the Symantec EDR appliance, a new incident is created that contains events from the same date and time as those in a previously closed incident. The incident continues to get generated even though the incident is repeatedly closed. https://knowledge.broadcom.com/external/article?articleId=200435
Client information related to 64-32 bit is incorrect in the EDR appliance console.	On the Details page for a Win10 client-64 in the Symantec Endpoint Protection Manager (SEPM) console, SEPM reflects that 64-bit is "yes". In the EDR appliance console, on the search results or entity page for a 64-bit Windows endpoint, Symantec EDR displays a 64-bit state of "no" for the same endpoint. https://knowledge.broadcom.com/external/article?articleId=190477
Dashboard graph display issue.	The EDR appliance console Network graph does not display on Dashboard. https://knowledge.broadcom.com/external/article?articleId=200344
SSO logout error message can't be removed from EDR appliance console, even after page refresh or successful local user login/ logout.	When users logout of the EDR appliance console, if the IdP session has already been closed and the IdP failed the logout request, the EDR appliance console logon page contains the following error message:  Contact your administrator to ensure that a correct and valid Symantec EDR sso.crt is uploaded to the IdP. Also ensure that the IdP contains Symantec EDR's correct SP Issuer value. https://knowledge.broadcom.com/external/article?articleId=200520
Symantec EDR sends alerts about certificate expiration for a SEPM Controller that was removed from the EDR appliance console.	This can occur if an older SEPM was previously configured and the database entry for it was not properly purged. https://knowledge.broadcom.com/external/article?articleId=194797

Issue	KB link
The field "reg_value_result.data" is not forwarded to Splunk.	When reviewing data sent from Splunk to Symantec SEDR, the field "reg_value_result.data" is missing. https://knowledge.broadcom.com/external/article?articleId=192033
JVM heap is high.	Engineering is investigating this issue. https://knowledge.broadcom.com/external/article?articleId=202448
S550 cannot sustain workload after the Elasticsearch size is over ~30% of volume size.	Engineering is investigating this issue. https://knowledge.broadcom.com/external/article?articleId=202450
Scanner (730) in Tap mode on distributed environment: Not seeing events in EDR appliance console and also errors in PIE logs.	Engineering is investigating this issue. https://knowledge.broadcom.com/external/article?articleId=202758
The `status_check` admin CLI tool URLs may need updating.	Symantec EDR 4.5 status_check CLI command contains invalid tests. https://knowledge.broadcom.com/external/article?articleId=210237
Deleting the SEPM controller with a custom SEPM database certificate causes an exception if the replication checkbox is selected on the EDR appliance console.	Upgrade to Symantec EDR 4.6.0, where this error is corrected. https://knowledge.broadcom.com/external/article?articleId=210235
Incident list blank after sorting by "Detection Type".	When sorting the list of incidents in Symantec EDR Incident Manager by "Detection Type" the list of incidents is no longer displayed. Navigating away from, and then back to, Incident Manager causes the list of incidents to be displayed again, however the list is still not sorted by "Detection Type". https://knowledge.broadcom.com/external/article?articleId=208934
Post upgrade to Symantec EDR 4.5, the EDR appliance console was available on both the default port (443) as well as the custom configured port.	Before upgrading, the Settings -> Global -> Management Port was changed from 443 to a custom port number. After upgrading to Symantec EDR 4.5, the EDR appliance console becomes available on both the default port (443) as well as the custom configured port. https://knowledge.broadcom.com/external/article/203724
Sometimes message not getting displayed after marking any query as "Shared".	When clicking "Mark Shared" for a saved search query in Symantec EDR, no success message appears. Reviewing the shared searches shows that the search was shared successfully. This is a cosmetic issue; the search is still marked as shared. https://knowledge.broadcom.com/external/article/209529
In a freshly installed Symantec EDR 4.4, R3 keeps increasing after a few hours of workload.	After deploying Symantec EDR 4.4 or 4.5 on the S550 appliance, there are many times when the appliance cannot start all services during boot and requires several reboots. https://knowledge.broadcom.com/external/article?articleId=210142
Endpoint searches hang.	Endpoint searches appear to be stopped or hung in the EDR appliance console. https://knowledge.broadcom.com/external/article/209808
Incident Grid - Sort by Detection_Type or Suspected_Breach column results in an empty page.	After the update to Symantec EDR 4.5, the Dashboard no longer shows data on the Global Adversary map. There may be further issues, such as no Incidents being generated. See the following KB for patch instructions. https://knowledge.broadcom.com/external/article?articleId=208228

Issue	KB link
CA signed certificate shows an error when uploading it in the EDR appliance console.	When uploading the certificate in the EDR appliance console, there is an error. This error occurred because the certificate was created with a DOS end of line (EOL) instead of a Unix style EOL. This causes an error in the system because it is unable to read the DOS EOL correctly. https://knowledge.broadcom.com/external/article?articleId=209629
Device is encountering a lot of events reported for 22k clients on the 8880 appliance.	Within the EDR appliance console, the system health state is "Needs Attention". When the mouse hovers over the system health state, the console displays the Alert: `Device is encountering a large number of events. Some events are not logged in the database.` https://knowledge.broadcom.com/external/article?articleId=171942
ICDx event transform issues for 4117 and 4098 events.	Please upgrade to change the behavior. https://knowledge.broadcom.com/external/article?articleId=210233
Global Adversaries by Location does not display attack circles on World Map of Incidents Of Compromise (IoCs).	On Symantec EDR 4.5, the map may not show any circle indicators or markers on map indicating IoCs. This occurred because of data format incompatibilities between the releases of Symantec EDR and Symantec's Dynamic Adversary Intelligence (DAI) feed. https://knowledge.broadcom.com/external/article?articleId=209827
Exclude timeout state endpoint activity recorder full dump command from in-progress count for concurrency calculation.	When attempting to perform a full dump of a client using the Symantec EDR appliance, the full dump status is always "Queued - Concurrent limit reached" and there are 2 or more previously running full dumps, which have been canceled but can not be deleted. https://knowledge.broadcom.com/external/article/206416
Full dumps queued with maximum concurrent limit reached.	When attempting to perform a full dump of a client using the Symantec Endpoint Detection and Response (SEDR) appliance, the full dump status is always "Queued - Concurrent limit reached" and there are 2 or more previously running full dumps which have been canceled but can not be deleted. https://knowledge.broadcom.com/external/article/206416
After Symantec EDR 4.5 replaces self-signed cert, SEP clients unenroll in bulk.	Workaround: re-insert the self-signed certificate you used before. https://knowledge.broadcom.com/external/article?articleId=210232
Some events from Symantec EDR are not being sent through API communication channel (EDR app/add-on for Splunk).	See the Splunk pre-installation checklist. https://knowledge.broadcom.com/external/article/176198
Some logs are not being deleted.	When performing a diagnostics on the Symantec Endpoint Detection and Response, it is noted that there are a large number of older log files that may be several years old. The current log rotation configuration does not include removing some older files. https://knowledge.broadcom.com/external/article/206655
Unable to login to the SEDR GUI after reboot	After rebooting the Symantec Endpoint Detection and Response (SEDR) attempts to access the GUI result in the following message: `Symantec EDR Manager is currently unavailable.` There may be a delayed, or failed, response from one or more of the configured DNS servers. https://knowledge.broadcom.com/external/article/202976

Issue	KB link

No data on Global Adversaries map on the EDR appliance console Dashboard page.	Run the `patch` command on the SEDR CLI with the following parameters:
	`patch list`
	`patch install atp-patch-4.5.0-1`
	https://knowledge.broadcom.com/external/article/208228

One client's invalid version string fails all endpoints enrollment in same group.	The SEPM console displays a partial SEP version of 14.3.3384 when it should display the full 14.3.3384.1000. This ultimately stops all of the clients in the group from properly enroll in the SEPM. https://knowledge.broadcom.com/external/article?articleId=209424
The management port on my appliance is no longer accessible after rebooting my appliance.	The EDR appliance is using dual inline mode and after rebooting the 8880 network interface's alias mapping is incorrect. https://knowledge.broadcom.com/external/article?articleId=209730
AMSI/ETW event should be treated as endpoint activity recorder event.	In Symantec SEDR 4.5.0, AMSI and ETW events are not treated as FDR events. https://knowledge.broadcom.com/external/article?articleId=209531
"Invalid Synapse Config" error message when trying to change a setting on Symantec EDR 4.3.	Previous versions of the ATP software allowed punctuation in the SEPM DB name field. Symantec EDR 4.0 and later versions do not allow any characters besides alphanumeric, space and _ (underscore). https://knowledge.broadcom.com/external/article?articleId=186205
Symantec EDR public API command status for endpoint search is not returning status for unenrolled SEP and SEP 12.x.	Attempts to check the command status of endpoint searches using the Symantec EDR API for unenrolled SEP clients or SEP 12.x client does not return a status. https://knowledge.broadcom.com/external/article/209945
Private cloud settings are not written to SEPM after adding certificate to Symantec EDR certificate store until service is restarted.	After configuring a Synapse entry, Symantec EDR retrieves a certificate used for communication with the SQL server from the SEPM. As part of this process, an error occurs when the force encryption functionality is enabled on the SQL server, and the "replication is enabled between all SEPM's" option on Symantec EDR is also enabled. The issue occurs due to the handling of applying policies to the SEPM under these specific circumstances until a reboot is done https://knowledge.broadcom.com/external/article?articleId=210260
'Device encountered a service error' showing on the System Health status of the EDR appliance console.	After a deployment of Symantec EDR 4.4 or earlier, the appliance may show an error status regarding a service failure. This is caused by a service restart when new engine content is downloaded. https://knowledge.broadcom.com/external/article?articleId=210677


Symantec
A Division of Broadcom