Transitioning to Symantec Endpoint Security

A Step by Step Guide

6/19/20

This document is designed for SEP Cloud (SEPC) and SEP Small Business Edition (SEP SBE) customers who are transitioning to Symantec Endpoint Security (SES).

> **Note to SEPC customers**: Your SES subscription includes mobile device support, but mobile devices are currently managed separately from other device types. The information in this document about product setup is designed to help you transition servers, desktops, and laptops to SES. Before you transition your mobile devices, open the Symantec Endpoint Protection Mobile documentation and review the Getting Started topics.

Verifying your SES account

Once the SESE order is submitted and provisioned through the Marketplace, it will automatically create a new SESE entitlement for you. Your SES account will be provisioned automatically and then you will receive a welcome email from the CyberDefense team. Follow the link provided in the email to verify your account and create your password. You don't need to obtain an SES license number. The email contains all the information you need to provision your SES entitlement. In that email, you will also see your Enterprise Site ID and your contract number. Make a note of these two identifiers as you may need them as you transition. You will also find the same information on the Support portal, from where you can raise a case, should you need any assistance with your transition. You can find instructions on how to enroll your devices into that entitlement here.

For more information about whether you qualify for an upgrade to SES or what to do if you qualify but have not received your email, contact your partner or reseller.

Preparing SES for the transition

You should review the default device group and policy configurations in SES and make any needed changes before transitioning devices from SEPC or SEP SBE.

Step 1: Create additional administrator accounts if needed

Ensure that all of your SEPC or SEP SBE administrators can work in SES by adding SES administrator accounts for them.

For more information, open the Symantec Endpoint Security documentation and search for “creating an administrator account”.

 Version 1.0 May 2020

Note for SEPC customers: You don't need to create accounts for every endpoint user. You only create accounts for other administrators who will manage SES.

Step 2: Create new device groups if needed

SES comes with a Default device group that has a set of policies already assigned to it. You can create new groups under the Default device group if you need to apply different policy configurations to some devices.

For more information, open the Symantec Endpoint Security documentation and search for "creating device groups".

Note for SEPC customers: In SES, you add all devices directly to device groups to manage them.

Step 3: Review the policies applied to the Default device group

The Default device group already has a set of policies assigned to it. These policies are configured to provide optimal protection, but you may need to modify some settings for your environment – for example, if you use a proxy server or want to exclude certain files from security scans.

For more information, in the Symantec Endpoint Security documentation, search for "about policies".

To view the policies that are assigned to the Default device group:
In SES, on the Devices page, on the Device Groups tab, in the Group Hierarchy pane, select Default. Then, in the pane on the right, select Policies. You can click any policy in the list to review its settings.

The following table lists some commonly customized security settings, the SES policy that governs them, and the search term to use to get more information in the Symantec Endpoint Security documentation:

Configuration Type	SES Policy Type	SES TechDocs Search Term
Proxy server	System	proxy server configuration
Scan exclusions	Whitelist	policy scan exceptions

Firewall rules	Firewall	firewall management
File and printer sharing	Device Control	device control policy settings
Connected storage	Device Control	blocking or allowing an external device

Step 4: Reconfigure policy settings and create new policies if needed

You can modify any policy, including default policies. You don't need to create new policies unless you created child device groups to which you need to apply different policy settings.

To update the policies applied to the default device group:
In SES, go to the Policies page, click the policy you want to modify, and update the settings as needed. (Most settings include help buttons with links to detailed information about the setting.) When you save your changes, a new version of the policy is saved automatically, and you are prompted to apply the new version to the device group. Press Apply Policy to confirm.

To create new policies to apply to child device groups:
You can create a new policy from a template, or you can duplicate an existing policy.

For more information, in the Symantec Endpoint Security documentation, search for "creating a policy" or "duplicating a policy".

To apply policies to child device groups:
Any child device groups that you added will automatically inherit policy settings from the parent (Default) device group. However, you can apply specific policies with different settings directly to child device groups and the child group will use the directly applied policy instead of the equivalent policy that is applied to the parent group.

For more information, in the Symantec Endpoint Security documentation, search for "applying a policy to a device group".

Enrolling your devices in SES

SES provides multiple methods that you can use to enroll devices. Depending on the type of device, you can use push-enrollment or create and distribute installation packages.

Step 1: Identify the devices that you want to enroll

You can use the SES device discovery feature to find all devices in your network that aren't currently managed by SES. To perform device discovery, you first have to enroll a Windows device and make it a discovery agent.

For more information, in the Symantec Endpoint Security documentation, search for "adding a discovery agent to find unmanaged devices" and "finding devices for enrollment".

You can easily review all devices that are discovered and sort them by operating system or other relevant criteria to help you plan enrollment.

To view discovered devices:
In SES, on the Devices page, select the Unmanaged Devices tab, which lists all discovered devices that aren't yet managed by SES.

> **Note:** Discovery is a way to keep track of your overall device transition process, because the Unmanaged Devices tab lists only those devices that haven't yet been enrolled in SES. You can rerun discovery as often as you need to until all devices have been enrolled, after which they appear in the Managed Devices tab.

Step 2: Enroll your devices in SES

SES provides several methods to enroll devices. You can push enroll most Windows devices and you can create and distribute installation packages for Windows, Mac, and Linux.

For an overview of all enrollment options, in the Symantec Endpoint Security documentation, search for "installation methods for the Symantec Agent".

For details about push enrollment, in the Symantec Endpoint Security documentation, search for "enrolling unmanaged devices" and "viewing push enrollment status".

About un-enrolling devices from SEPC or SEP SBE
You can un-enroll all devices from SEPC or SEP SBE before you enroll them in SES, but in many cases this isn't necessary. If you want to "over-enroll" devices - that is, enroll devices in SES that are currently enrolled in SEPC or SEP SBE - we recommend that you test the process with each device type in your environment first.

> **Note**: The exact actions performed during un-enrollment vary based on the device type: the process may revert the client on the device to unmanaged status or uninstall the client from the device. For more information, see the SEPC or SEP SBE help topics on un-enrolling devices.

Enrolling your mobile devices in SEP Mobile

Several methods are available to enroll devices in SEP Mobile, depending on your needs and environment. For an overview, search the SEP Mobile documentation for “adding users and devices“. The option applicable to most SEPC customers is to add users to SEP Mobile, who are then automatically invited to enroll their own devices.

Before you do so, however, decide whether you want users to “over-enroll” iOS and Android devices that are already enrolled in SEPC. You should test the process with representative device types before you continue. If necessary, you can un-enroll mobile devices first, as described in the SEPC help. And if you have any issues, see the following section of this document for troubleshooting tips.

Troubleshooting any enrollment issues that occur

You can troubleshoot issues with any devices that don’t enroll seamlessly. For example, some devices may require different credentials to complete push enrollment, or you may need to un-enroll some devices from SEPC or SEP SBE before you enroll them in SES.

> **Note**: If you use the SES push enrollment option to enroll Windows devices, the push enrollment status page will provide information about any issues. You may be able to fix a problem and try the push enrollment again.

If another option isn’t applicable, un-enroll the device completely from SEPC or SEP SBE and then perform a fresh enrollment into SES. You can perform the following tasks, in the order listed, until the problem is resolved:

- Un-enroll a device from the SEPC or SEP SBE console
- Uninstall the client manually on a device
- Run a removal tool on a device

For specific options and methods not covered in the SEPC or SEP SBE help, see the following KB article: https://knowledge.broadcom.com/external/article?legacyId=tech251239