Symantec Endpoint Protection: Administration Guide

Contents

Symantec Endpoint Protection: Administration Guide
Downloading and installing the cloud agent

Before you can protect your computers with Symantec Endpoint Protection Small Business Edition (SEP SBE) cloud, you must download the agent and install it onto the computers you want to protect.

The agent delivers services to your computers and communicates with the management console in your account. You must install the agent on every computer you want to protect. Make sure that your computers meet the system requirements and Internet access requirements.

Administrator rights are necessary to install the agent. This requirement poses no difficulty for organizations where users are administrators on their local computer.

When an organization's security policy prohibits local admin rights for computer users, systems management tools like Altiris can be used to push out the agents.

Note: By default, new agents are automatically confirmed into your account. If your Account Administrator disabled Auto-confirm new agents in your organization's settings, new agents must be confirmed before they become active.

Note: All antivirus products or firewall products must be removed from your computers before you install Symantec Endpoint Protection.

If you are running Windows Vista, User Account Control allows only your computer administrator to install a program that runs for every user account. Even if you have disabled User Account Control, administrative rights are required to install the Agent.

When you upgrade a protected computer from Windows XP to Windows Vista you must remove the Agent and restart the computer. When the computer restarts you can begin the upgrade to Windows Vista.

Three deployment options are available to install agents on to your computers:

- The standard download and install.
- Download and build a portable install package.
- Email invitations to install.

These different methods can be used to fulfil the needs of varying circumstances.

Standard Install	This installation method downloads a small installer that manages the full installation of the agent. It requires: • A user logon for your SEP SBE cloud • account Your physical presence at the computer or a remote connection to it
Email invitation	Enables you to send email invitations to download the agent to computer users in your organization:

	• Up to 50 email addresses that are separated by semicolons can be submitted • Invitation contains a URL valid for 30 days unless withdrawn by the administrator • Allows a computer user to perform the installation themselves without administrator intervention

To prepare to download the agent

1. In Internet Explorer, navigate to Tools > Internet Options > Advanced.
2. On the Advanced tab, scroll down to Security.
3. Verify Do not save encrypted pages to disk is unchecked and click OK.

To install the agent onto an individual computer

1. In SEP SBE Management Console, click Computers.
2. In the Computers page, click Add Computers.
3. If you want to add the new computer to a group other than the default group, select that group from the Choose Your Group drop-down.
4. Under Download Your Installer, click Install Now. (Depending on your browser, the file is automatically downloaded or you may be asked to run or save the file.)
5. When the SymantecExtractor.exe file download is complete, run the file.
6. The Installer opens. You may configure your Proxy Settings or change the destination folder if required. Configuring proxy is only necessary when these settings are required for Internet access.
7. Click Install.
8. When the success screen appears, click Finish.

To send email invitations to download the agent

1. In SEP SBE Management Console, click Computers.
2. In the Computers page, click Add Computers.
3. If you want to add the new computer to a group other than the default group, select that group from the Choose Your Group drop-down.
4. In the Download your installer section, enter up to 50 user email addresses in the Send Download Invites text box. The specified users receive invitations with a download link to the agent.

Multiple email addresses must be delimited with a semicolon.
Click Send Email Invites.

Your users receive an email saying that you have invited them to download and install the agent onto their computer. It provides a link enabling them to download the agent without a logon account to your organization's SEP SBE cloud account.

Symantec Endpoint Protection: Administration Guide

Managing agent download invitations

You manage your agent download invitations from the Agent Download Invitation page. You can:

- Invite members of your organization to download the cloud agent.
- View your download invitation history.
- Deactivate download invitations.

The Send Invites section of the page lets you send new download invitations by email. You can enter up to 50 semicolon delimited, email addresses.

The Deactivate Invites/History section displays when, to whom and how many download invitations you have sent. It also enables you to revoke an invitation with the Deactivate action. When you deactivate an invitation, the download link in the invitation, which is normally active for 30 days, is shutdown. Download invitations expire 30 days after issuance.

To send download invitations and view your invitation history

1. Log into your management console account.
2. In the Quick Task box on your Home page, click View Invitation History. (Note: You can also view your invitation history from the Computers page.)
3. Send invitations by adding semicolon delimited email addresses to the Send Invites box and clicking Send Email Invites.
4. View your invitation history at the bottom of the page.

To deactivate an email invitation to install the cloud agent

1. Log into your management console account.
2. In the Quick Task box on your Home page, click View Invitation History. Note: You can also deactivate an email invitation from the Computers page.
3. Identify the invitation you want to deactivate in Deactivate Invites/History and click Deactivate in the associated Actions column.

Note: Deactivating an invitation revokes the invitation for all of the email addresses listed in the invitation.

Symantec Endpoint Protection: Administration Guide

Sending users a procedure explaining their download invitations

SEP SBE cloud provides a method for you to allow your users to download and install the cloud agent themselves. Users are authorized for the download by the email address they enter during installation. The download invitation does not give them access to your SEP SBE cloud account.

The invitation that is delivered to users provides only a link to the download and no explicit instructions. We encourage you to:

- Inform the users receiving download invitations of the importance of your endpoint protection strategy.
- Provide invited users with the proxy information necessary for a successful installation (if necessary).
- Include this procedure to minimize the number of questions you receive about the installation.
- To install SEP SBE cloud on to your computer

1. Open your email application and look for an email from Symantec alerting service with the subject line: **Symantec.cloud agent download**. Download and open it.

   Note: If you cannot find the email, check your email application's Spam folder.

2. Click the link in the invitation email. The file download process begins.

   Note: The antivirus products and firewall products that are installed on your computer must be removed from your computer before you install Symantec Endpoint Protection.

3. The dialog box gives you the option to **Run** or **Save** the file. Click **Run**.
4. When the SymantecExtractor.exe file download is complete, you are asked for permission to **Run** the software. Click **Run**.
5. The Symantec Endpoint Protection Small Business Edition installer opens. It gives you the status of the installer and permits you to change the installation folder. Click **Next**.
6. Configure your proxy settings if required. Click **Next**.
7. When the installation progress screen appears, click **Install**.
8. When the overall progress is complete, the SEP SBE cloud components are installed. Click **Next**.
9. When the success screen appears, uncheck the **Launch Website** check box and click **Finish**.
10. In most cases, your SEP SBE cloud installation is automatically added to your organization's list of protected computers.

Symantec Endpoint Protection: Administration Guide

Removing existing antivirus and firewall products

To get the best performance from Symantec Endpoint Protection Small Business Edition cloud, you must remove any Symantec or other antivirus or firewall product before installing your agents. These programs intercept risky communications with your computers. The programming mechanisms intercepting these risky communications might interfere with the proper functioning of your cloud agents. To ensure that these products are removed from your endpoints, the installation program blocks the agent install until those applications are removed.

The installation program automatically removes other Symantec and Norton AntiVirus or firewall products as well as tested, antivirus, or firewall product removal tools. The identified applications appear on an Incompatible Applications page where you are prompted to remove them. With user authorization, the installation program launches that product's own Windows Add/Remove Programs tool.

Note: The automatic removal of an incompatible application manages that program's removal tool. If you encounter difficulty with the uninstall of that application, please contact customer support group for that product.

Whenever the installation program encounters an antivirus or a firewall application with an untested Windows Add/Remove Programs tool, the program is identified as incompatible. You must intervene to remove these applications. The installation program’s automatic removal tool and incompatible program identification feature is only available in attended or full UI mode.

Once the automatic uninstall operation is finished, the endpoint computer restarts and the agent installation continues. If you manually uninstalled the incompatible product, you must manually restart the agent install program.

Please uninstall any antivirus program or firewall program from your computer before installing Endpoint Protection. Uninstalling such programs is important even if the install program fails to detect the program or identifies it as incompatible. Running multiple antivirus or firewall programs simultaneously is inherently dangerous; the potential for interference between the applications is too risky to ignore. We encourage you to report these cases to Symantec Endpoint Protection Small Business Edition cloud by clicking the **Case Management** link in your email address drop-down in the management console banner.

In larger environments, you may prefer to use your customary techniques to uninstall software from your endpoints. If you perform these operations using Microsoft Active Directory, ensure that the application you remove is also removed from the policy governing these endpoints. This precaution prevents the reinstallation of an application based on your Active Directory policy.

When endpoints run less common antivirus or firewall products, or unrecognized versions of a product, install program may not detect the potentially conflicting product. Potentially incompatible products must always be removed for best results with Symantec Endpoint Protection.

We provide automatic removal of antivirus or firewall software for these products:

Symantec Endpoint Protection: Administration Guide

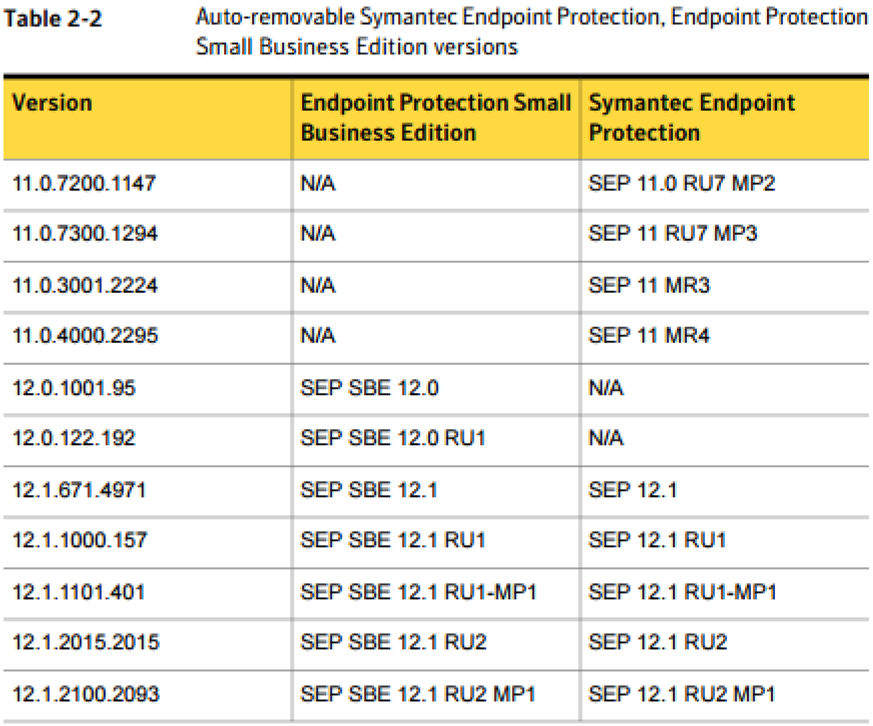


Table 2-2 Auto-removable Symantec Endpoint Protection, Endpoint Protection Small Business Edition versions

Version	Endpoint Protection Small Business Edition	Symantec Endpoint Protection
11.0.7200.1147	N/A	SEP 11.0 RU7 MP2
11.0.7300.1294	N/A	SEP 11 RU7 MP3
11.0.3001.2224	N/A	SEP 11 MR3
11.0.4000.2295	N/A	SEP 11 MR4
12.0.1001.95	SEP SBE 12.0	N/A
12.0.122.192	SEP SBE 12.0 RU1	N/A
12.1.671.4971	SEP SBE 12.1	SEP 12.1
12.1.1000.157	SEP SBE 12.1 RU1	SEP 12.1 RU1
12.1.1101.401	SEP SBE 12.1 RU1-MP1	SEP 12.1 RU1-MP1
12.1.2015.2015	SEP SBE 12.1 RU2	SEP 12.1 RU2
12.1.2100.2093	SEP SBE 12.1 RU2 MP1	SEP 12.1 RU2 MP1

Symantec Endpoint Protection: Administration Guide

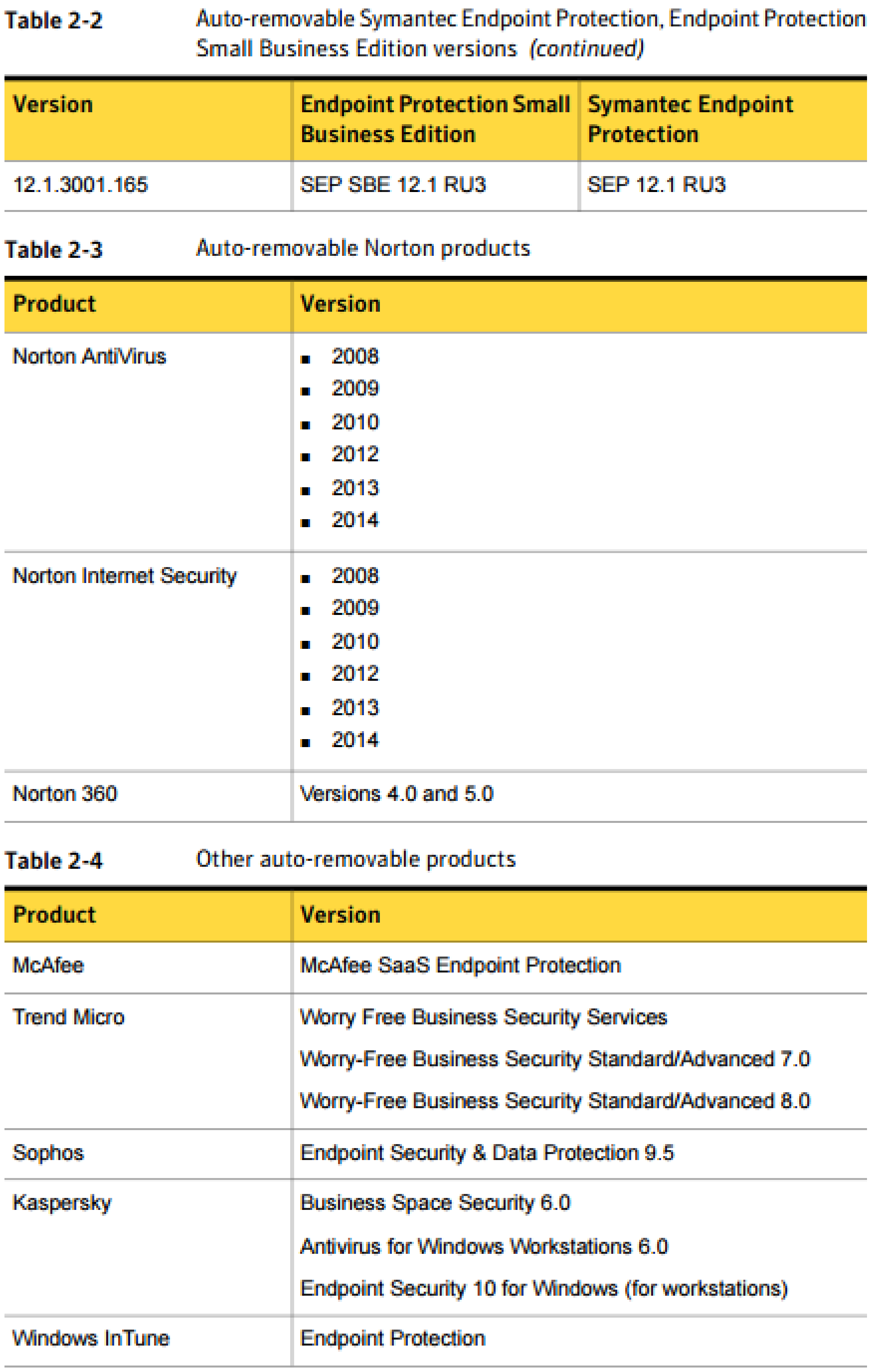


Table 2-2 Auto-removable Symantec Endpoint Protection, Endpoint Protection Small Business Edition versions *(continued)*

Version	Endpoint Protection Small Business Edition	Symantec Endpoint Protection
12.1.3001.165	SEP SBE 12.1 RU3	SEP 12.1 RU3

Table 2-3 Auto-removable Norton products

Product	Version
Norton AntiVirus	▪ 2008 ▪ 2009 ▪ 2010 ▪ 2012 ▪ 2013 ▪ 2014
Norton Internet Security	▪ 2008 ▪ 2009 ▪ 2010 ▪ 2012 ▪ 2013 ▪ 2014
Norton 360	Versions 4.0 and 5.0

Table 2-4 Other auto-removable products

Product	Version
McAfee	McAfee SaaS Endpoint Protection
Trend Micro	Worry Free Business Security Services Worry-Free Business Security Standard/Advanced 7.0 Worry-Free Business Security Standard/Advanced 8.0
Sophos	Endpoint Security & Data Protection 9.5
Kaspersky	Business Space Security 6.0 Antivirus for Windows Workstations 6.0 Endpoint Security 10 for Windows (for workstations)
Windows InTune	Endpoint Protection

Symantec Endpoint Protection: Administration Guide

Creating policies for Endpoint Protection

This chapter includes the following topics:

Configuring global policies

In Symantec Endpoint Protection Small Business Edition (SEP SBE) cloud, a global policy can simplify proxy settings and local update host assignments for organizations with several offices.

- The proxy settings that are assigned through the local agent, override global proxy settings.
- In the absence of globally-assigned local update hosts, agents still discover a local update host.

The global policy for scheduling LiveUpdate also enables the management of agent software updates. Whenever software updates are more than 30 days old, the updates are delivered without regard to the global policy schedule.

Note: The LiveUpdate schedule does not affect delivery of virus definitions.

To Configure a global System Policy

1. In SEP SBE Management Console, click **Policies**.

   In the **Policies** page, ensure that **System** is selected. The **System** selection is under **Global**.
2. To set up a new **System Policy**, click **Add Policy**.
3. Type a descriptive **Name** and **Description** to document the purpose of your System Policy.
4. You can now configure proxy settings and assign local update hosts.

To configure global system proxy settings

1. Under **Proxy Settings**, activate the **Enable Proxy** check-box to configure the proxy on your agents.

   Note: The proxy type is set to **HTTP** by default and cannot be changed.
2. Enter the **Host** and **Port** addresses for the proxy.
3. Activate the **Authenticated** check-box if authentication to the proxy is required and enter a **User name** and **Password**.
4. In the **Groups** section, assign the proxy settings to the groups that need them.

   Note: You can assign local update hosts in the **Local Update Service** section. The next procedure describes the process.

5. When you are finished, click **Save & Apply**.
6. Computers in the selected groups receive the new proxy settings when the policy change is dispatched.

To assign local update hosts

1. Under **Local Update Service** choose the correct approach for this System Policy.

Connect to any available local update host(s)	This option permits an agent to discover its local update host.
Do not connect to any available local update host(s)	This option disables the Local Update Service for this System Policy.
Specify the local update host(s) for this group	This option enables you to select suitable local update hosts for this System Policy.

If you select either of the first two options, skip to step 3.
If you selected the third option, continue to step 2.

2. When you select **Specify the local update host(s) for this group**, the host selection interface opens.
   Select the local update host(s) to assign for this System Policy and click **Add**. All of the local update hosts maybe selected at once with **Add All**.
3. In the **Groups** section, assign the **Local Update Service** configuration to the groups that need them.
4. When you are finished, click **Save & Apply**.
   Computers in the selected groups receive the new proxy settings when the policy change is dispatched.

1. Carefully consider the scheduling option that best serves your needs.

Anytime	This option is the default setting and is recommended.
During business hours	Business hours are Monday through Friday from 0800 to 1700 local time.
During non-business hours	Non-business hours are after 1700 local time and before 0800 local time.
Weekends only	Weekends are defined as Saturday and Sunday.
Disable	This setting is automatically overridden after a software update is more than 30 days old.

Note: LiveUpdate requires adequate disk space to run successfully. Please ensure that your computers have 1 GB of available disk space to avoid LiveUpdate failures.

2. Under **Live Update Schedule** choose the correct option for LiveUpdate agent software updates.

3. In the **Groups** section, assign the **Live Update Schedule** configuration to the groups that need them.
4. When you are finished, click **Save & Apply**.
   Computers in the selected groups receive the new proxy settings when the policy change is dispatched.

Symantec Endpoint Protection: Administration Guide

Configuring Endpoint Protection policies

Configuring Symantec Endpoint Protection Small Business Edition (SEP SBE) cloud to best suit the security needs of your organization requires only that you:

- Make logical groups for your computers.
- Decide which policies are best suited for each group

By default, all new computers are added to the **Default Group** and are assigned the Endpoint Security default policy. No further configuration required.

Note: Different agents are installed for desktops & laptops than for servers. The protection settings available for servers differ from the protection settings available for desktops & laptops.

To create policies

1. In the SEP SBE Management Console, click the **Policies** page.
2. On the left pane, select the **Endpoint Protection** service, and click **Add Policy**.
3. On the policy configuration page, do the following:

   Enter a **Name** and **Description** for the policy.
   Assign the appropriate protection settings using the check boxes.

   Set a **Scan Schedule** by designating the scan frequency, time to start, and the computers to scan.
   Assign the policy to the appropriate groups in the **Groups** section of the page.
   Click **Save & Apply**. The policy is applied to the computers in the selected group or groups.
4. These categories of protection offer a defense in-depth security solution. **Computer Protection** features focus on the high risk communications reaching a computer.

Symantec Endpoint Protection: Administration Guide

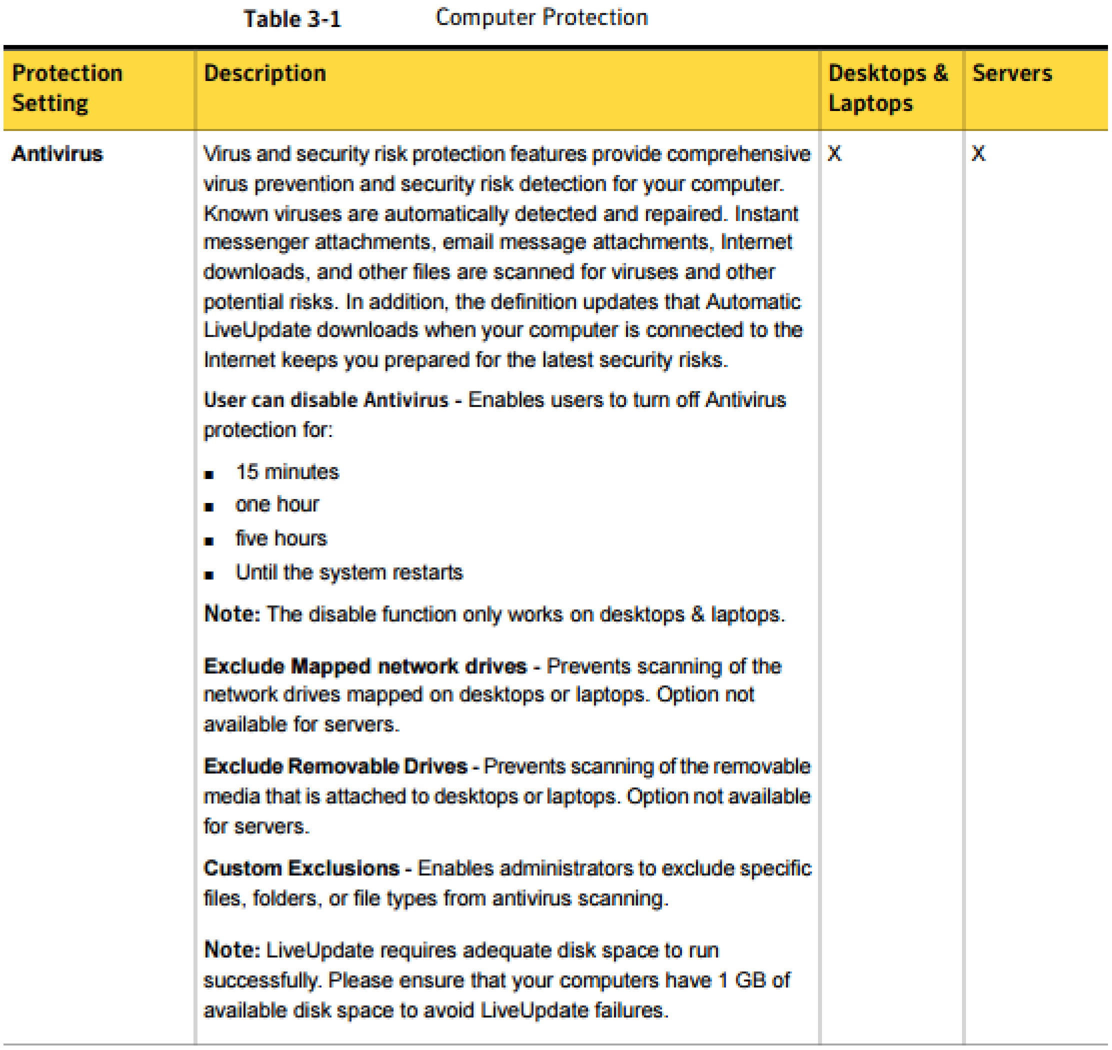
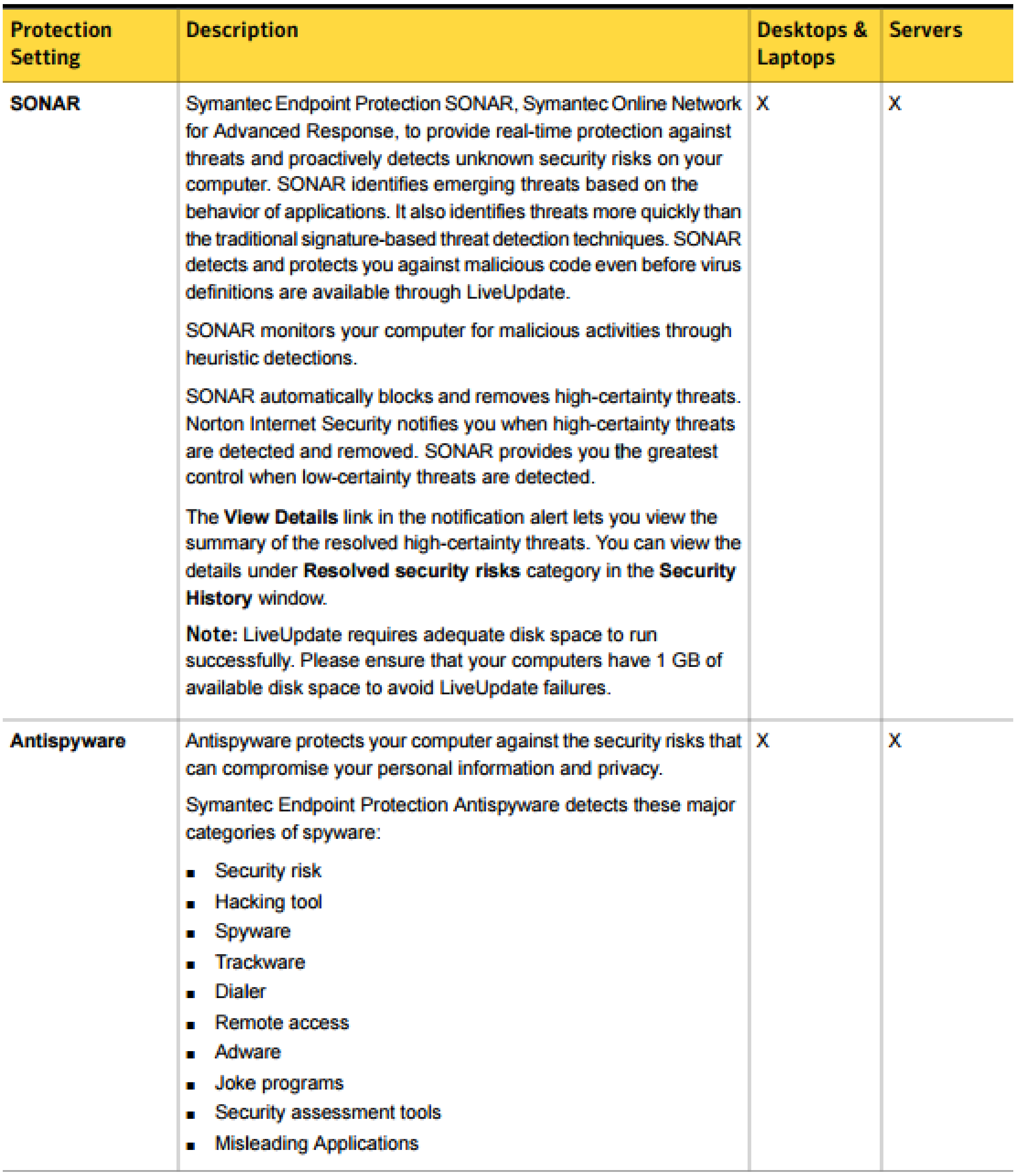


Table 3-1 Computer Protection

Protection Setting	Description	Desktops & Laptops	Servers
Antivirus	Virus and security risk protection features provide comprehensive virus prevention and security risk detection for your computer. Known viruses are automatically detected and repaired. Instant messenger attachments, email message attachments, Internet downloads, and other files are scanned for viruses and other potential risks. In addition, the definition updates that Automatic LiveUpdate downloads when your computer is connected to the Internet keeps you prepared for the latest security risks. **User can disable Antivirus** - Enables users to turn off Antivirus protection for: ▪ 15 minutes ▪ one hour ▪ five hours ▪ Until the system restarts **Note:** The disable function only works on desktops & laptops. **Exclude Mapped network drives** - Prevents scanning of the network drives mapped on desktops or laptops. Option not available for servers. **Exclude Removable Drives** - Prevents scanning of the removable media that is attached to desktops or laptops. Option not available for servers. **Custom Exclusions** - Enables administrators to exclude specific files, folders, or file types from antivirus scanning. **Note:** LiveUpdate requires adequate disk space to run successfully. Please ensure that your computers have 1 GB of available disk space to avoid LiveUpdate failures.	X	X

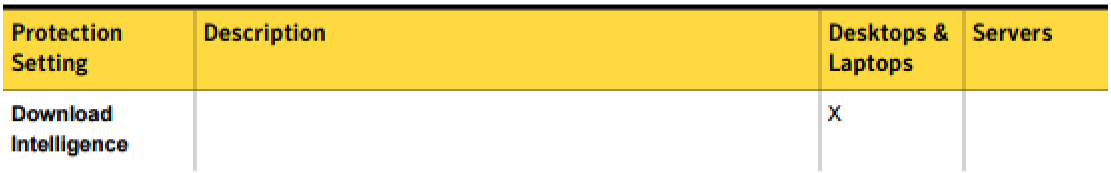
Symantec Endpoint Protection: Administration Guide

Table 3-1 Computer Protection *(continued)*



Protection Setting	Description	Desktops & Laptops	Servers
SONAR	Symantec Endpoint Protection SONAR, Symantec Online Network for Advanced Response, to provide real-time protection against threats and proactively detects unknown security risks on your computer. SONAR identifies emerging threats based on the behavior of applications. It also identifies threats more quickly than the traditional signature-based threat detection techniques. SONAR detects and protects you against malicious code even before virus definitions are available through LiveUpdate. SONAR monitors your computer for malicious activities through heuristic detections. SONAR automatically blocks and removes high-certainty threats. Norton Internet Security notifies you when high-certainty threats are detected and removed. SONAR provides you the greatest control when low-certainty threats are detected. The **View Details** link in the notification alert lets you view the summary of the resolved high-certainty threats. You can view the details under **Resolved security risks** category in the **Security History** window. **Note:** LiveUpdate requires adequate disk space to run successfully. Please ensure that your computers have 1 GB of available disk space to avoid LiveUpdate failures.	X	X
Antispyware	Antispyware protects your computer against the security risks that can compromise your personal information and privacy. Symantec Endpoint Protection Antispyware detects these major categories of spyware: ▪ Security risk ▪ Hacking tool ▪ Spyware ▪ Trackware ▪ Dialer ▪ Remote access ▪ Adware ▪ Joke programs ▪ Security assessment tools ▪ Misleading Applications	X	X

Table 3-3 Web Protection *(continued)*



Protection Setting	Description	Desktops & Laptops	Servers
Download Intelligence		X	

Symantec Endpoint Protection: Administration Guide

Table 3-3 Web Protection *(continued)*

Protection Setting	Description	Desktops & Laptops	Servers
	Download Intelligence provides information about the reputation of any executable file that you download from the supported portals. The reputation details indicate whether the downloaded file is safe to install. You can use these details to decide the action that you want to take on the file. Some of the supported portals are: ▪ Internet Explorer (Browser) ▪ Opera (Browser) ▪ Firefox (Browser) ▪ Chrome (Browser) ▪ AOL (Browser) ▪ Safari (Browser) ▪ Yahoo (Browser) ▪ MSN Explorer (Browser, email & Chat) ▪ QQ (Chat) ▪ ICQ (Chat) ▪ Skype (Chat) ▪ MSN Messenger (Chat) ▪ Yahoo Messenger (Chat) ▪ Limewire (P2P) ▪ BitTorrent (P2P) ▪ Thunder (P2P) ▪ Vuze (P2P) ▪ Bitcomet (P2P) ▪ uTorrent (P2P) ▪ Outlook (email) ▪ Thunderbird (email) ▪ Windows Mail (email) ▪ Outlook Express (email) ▪ FileZilla (File Manager) ▪ UseNext (Download Manager) ▪ FDM (Download Manager) ▪ Adobe Acrobat Reader (PDF viewer) The reputation levels of the file are safe, unsafe, and unknown. You can install safe files. Norton Internet Security removes the unsafe files. In the case of unknown files, **Download Intelligence** prompts you to take a suitable action on the file. You can run the		

Protection Setting	Description	Desktops & Laptops	Servers
	installation of the file, stop the installation, or remove a file from your computer. When you downloaded a file, **Download Intelligence** processes the file for analysis of its reputation level. Auto-Protect analyzes the reputation of the file. Auto-Protect uses the threat signatures that Norton Internet Security receives during definitions updates and other security engines to determine the safety of an executable file. If the file is unsafe, Auto-Protect removes it. Auto-Protect notifies the results of file analysis to **Download Intelligence**. **Download Intelligence** then triggers notifications to inform you whether the file is safe to install or needs attention. You must take a suitable action on the files that need attention. In case of an unsafe file, Download Insight informs you that Norton Internet Security has removed the file. Security History logs details of all events that **Download Intelligence** processes and notifies. It also contains information about the actions that you take based on the reputation data of the events. You can view these details in the **Download Intelligence** category in **Security History**.		

Network Protection defends your computer by detecting and preventing attacks through your network connection and evaluating the safety email attachments. 3-4 Network Protection

Protection Setting	Description	Desktops & Laptops	Servers
Intrusion Prevention	**Intrusion Prevention** scans all the network traffic that enters and exits your computer and compares this information against a set of attack signatures. Attack signatures contain the information that identifies an attacker's attempt to exploit a known operating system or program vulnerability. Intrusion prevention protects your computer against most common Internet attacks. For more information about the attacks that intrusion prevention blocks, visit: http://www.symantec.com/business/security_response/attacksignatures If the information matches an attack signature, intrusion prevention automatically discards the packet and breaks the connection with the computer that sent the data. This action protects your computer from being affected in any way. Intrusion prevention relies on an extensive list of attack signatures to detect and block suspicious network activity. You should run LiveUpdate regularly to ensure that your list of attack signatures is up to date. Note: LiveUpdate requires adequate disk space to run successfully. Please ensure that your computers have 1 GB of available disk space to avoid LiveUpdate failures.	X	

Email Protection	**Email Protection** protects your computer against the threats that you might receive through email attachments. It automatically configures your email program for protection against viruses and other security threats. Note: This feature applies only to desktops and laptops.	X	

3.4 Network Protection *(continued)*

Protection Setting	Description	Desktops & Laptops	Servers
Smart Firewall	The **Smart Firewall** monitors the communications between your computer and other computers on the Internet. It also protects your computer and alerts you to such common security problems as: ■ Improper connection attempts from other computers and of attempts by programs on your computer to connect to other computers ■ Port scans by unauthorized computers ■ Intrusions by detecting and blocking malicious traffic and other attempts by outside users to attack your computer A firewall blocks hackers and other unauthorized traffic, while it allows authorized traffic to pass. Turning off **Smart Firewall** reduces your system protection. Always ensure that the **Smart Firewall** is turned on. The **Smart Firewall** provides two configurable options: **User can disable Firewall** - Enables a local computer user to override the Smart Firewall for a certain period of time. This option permits an installation or other administrative function. The firewall can be disabled for: ■ 15 minutes ■ one hour ■ five hours ■ Until the system restarts **Report Blocked Events** - Uploads blocked firewall events from the computer to your Endpoint Protection account. The blocked events are added to the computer history page and the statistical data that is displayed on the **Home** page. Blocked events are also available within the **Security History** page of the local Norton Internet Security interface. No alerts are issued based on this data as they are low risk events. **Firewall Rules** - Enables administrators to customize firewall rules for their organization. **Program Control** - Enables administrators to allow or block Internet access for agent-discovered programs. Note: This feature applies only to desktops and laptops.	X	

Symantec Endpoint Protection: Administration Guide

Configuring Endpoint Protection to your needs

Configuring Endpoint Protection to best suit the security needs of your organization requires only that you:

- Make logical groups for your computers.
- Decide which policies are best suited for each group
-

By default, all new computers are added to the **Default Group** and are assigned the Endpoint Security default policy. No further configuration required.
To create computer groups

1. Log into your account and click the **Computers** page.
2. On the left pane, under **Groups**, click the **Add** link.
3. Enter a **Name** and **Description** for the group in the screen. Click **Save**.
4. On the left pane, under **Groups**, select the group you created.
5. On the right side of the page, click **Move Computers** to add computers to the group.
6. In the **Move Computers** screen, filter and select the computers you want to add to the group. Click **Save**. The selected computers are moved out of the **Default Group** (or other assigned group) into your new computer group.

To create policies

1 Log into your account and click the **Policies** page.

2 On the left pane, select the **Endpoint Protection** service, and click **Add Policy**.

3 On the policy configuration page, do the following:

Enter a **Name** and **Description** for the policy.

Assign the appropriate protection settings using the checkboxes.
Consider and set exclusions for your scans using the checkboxes. To exclude specific files, folders, or file types, click **Custom Exclusions**.
Set a **Scan Schedule** by designating the scan frequency, time to start, and the computers to scan.
Assign the policy to the appropriate groups in the **Groups** section of the page.

4 Click **Save & Apply**. The policy is applied to the computers in the selected group or groups.

Symantec Endpoint Protection: Administration Guide

Configuring Your Alerts

Creating Alerts

You create alerts by creating rules to determine when to alert.
You set up your alerts according to:

- Which events you want to receive alerts for
- Where you want to be notified of alerts

> Note: Your default email contact method is already set up using the email address that is associated with your account. You can receive alerts at another email address or an SMS device.

To create an alert

1. In the top-right of the management console banner, in your email address drop-down, click **My Profile**.

   To create an alert for another user, click the **Users** page and the user's name to create the alert.

2. Click **Alert Preferences**, and then expand the contact method you want to create an alert for by clicking "**+**".

   If you want to receive alerts at a contact method other than the ones shown, you must first add a new contact method.

3. Click the **Add Rule** link for the contact method you want to create an alert for.
4. In the **Rule Name** box, enter a useful name for the alert rule.
5. Select at least one of these settings:

Service	Select the subscribed service.
Category	Endpoint Protection: • **General** • **Detected Risks**
Severity	• **Informational+** Informational+ delivers informational, warning, and error messages. Note: **Informational+** is available only for the **General** category, • **Warning+** Warning+ delivers warning and error messages. • **Error** This selection delivers only error alerts.
Computers	By default, the rule applies to all computers. Select the **Apply rule to selected computers** to create an alerting rule for specific computers.

6. Click **Save.**

To edit an alert rule, click the name of the rule of the rule for the alert and make the changes.

Symantec Endpoint Protection: Administration Guide

Adding, changing, or deleting contact methods to receive alerts

You can add, change, or delete contact methods for your alerts.
You can also set up the types of alerts you receive.
See “Creating alerts” on page 46.

By default, you receive alerts at the email address that is associated with your account. If you want to receive alerts at a different email address, you must add a new contact method or modify the existing one.

To add a contact method

1. In the top-right of the management console banner, in your email address drop-down, click **My Profile**.
2. In your profile page, in the left pane, click **Alert Preferences**.
3. Click **Add Contact Method**.
4. In the **Name** box, type a description for the contact method, such as home phone.
5. In the **Type** box, use the drop-down menu to choose an **email** or **SMS** contact method.
6. In the **Address** box, enter the email or SMS address for delivery.
7. Make sure that the **Send alerts to my contact device** check box is selected. Otherwise only an alert notification is delivered and you must log on to the management console to view the alerts.
8. Click the **Save** option, and then close the **Add a new contact method** dialog box.
9. Beside the new contact method, click "**+**", and click **Add Rule** to set up the alerts you want to receive at this contact method.
10. In the **Rule Name** box, enter a useful name for the alert rule.

11. Select at least one of these settings:

Service	Endpoint Protection
Category	• **General** • **Detected Risks**
Severity	• Informational+ Informational+ delivers informational, warning, and error messages. Note: Informational+ is available only for the general category. • Warning+ Warning+ delivers warning and error messages. • Error This selection delivers only error alerts.
Computers	By default, the rule applies to all computers. However, you may choose from a number of options: • Apply rule to all computers. • Apply rule to selected computers. This choice presents a computer selection box that you use to select computers for notifications. • Apply rule to selected groups. This choice presents a groups selection box that you used to select groups for notifications.

12. Click **Save**.

To change a contact method

1 On the top of any page, hover over the email address that is associated with your account and click **My Profile**.

Your profile page appears.

2 Click **Alert Preferences**.

3 Click the name of the contact method you want to change, and make the appropriate changes.

4 Make sure that the **Send alerts to my contact device** check box is selected. Otherwise only an alert notification is delivered and you must log on to the management console to view the alerts.

5 Click **Save**.

To delete a contact method

1 On the top of any page, hover over the email address that is associated with your account and click **My Profile**.

Your profile page appears.

2 Click the **Alert Preferences** tab.

3 For the contact method you want to delete, click the **X** icon and confirm the deletion.

Note: You cannot delete your default email contact method

Symantec Endpoint Protection: Administration Guide

Reports

Running a report

Symantec Endpoint Protection Small Business Edition cloud reports can be run as-is or customized in the **Report Wizard** to better meet the needs of your organization.

- The reports feature offers a number of useful functions.
- Templates and schedules
- Customizing the look and feel of reports

Creating a report

When you run a report, it is available on the **Reports** page when generated and selected users receive a copy by email.
You can run these reports on your Symantec Endpoint Protection Small Business Edition cloud activity:

- General reports
  - Alert History: Shows the history of alerts for computers you select.
  - Security Audit: Shows the access activity for the account. The audit includes logons, jobs run, and modifications made.
  - Computer Status Summary: Shows a summary of the overall status for all computers.
  - Mac Computer Summary: Provides a summary of unmanaged Mac computers.

- Endpoint Protection reports
  - Firewall History: Provides a summary of firewall events for one or more computers.
  - Risk Detection: Details the numerous types of risks that are detected in one or more computers.
  - Security Overview: Provides a summary of the overall security of all computers.
  - Endpoint Summary: Provides a summary of the current health and security settings for one or more computers.

- To create a report

1. In the SEP SBE Management Console, click **Reports**.
2. On the left pane, click a report-type to open the **Report Wizard**.
3. Specify the report settings:

Report Selection	**Report Name**: A default name is provided for all reports, however, you may enter a report name better suited to your requirements. The name is useful for identification if you want to save the report as a template to run again. **Report Type**: You can change the report type from here.

Report Details	Specify the time frame that you want the report to cover: ■ ***Last __ Days*** (default value is 7 days) **Note:** When the last *X* days are specified, *X* days are calculated: *current_time - X days*. ■ **Current Month** ■ **Previous Month** ■ **Date Range (Start Date - End Date)** Depending on the report type, the following options are displayed: ■ **Show Details** provides a more exhaustive report. ■ **Active users only** excludes users who are suspended. ■ **Active computers only** excludes computers that are offline. ■ **Mac computers** includes unmanaged Mac computers. ■ **Report by Computers** list enables you to pick computers. ■ **Report by Groups** list enables you to pick groups.
Settings	**Select the format for the report:** ■ **PDF** generates the report as an Adobe postscript file ■ **HTML** generates the report as a hypertext markup language file Mozilla Firefox requires an extension to be installed to read and write MHT files. Many such extensions are freely available. ■ **XML** generates the report in an Extensible Markup Language file **Would you like to save these settings as a report template?**: ■ Select the check box to save the settings as a report template that you can run again or run on a schedule.
Report Delivery	■ **Email Recipients**: Specify the people you want to notify of the report upon completion. ■ **Email the report as an attached file**: Activate the check box to include a PDF, XML, or HTML copy of the report in the notification email.

4. Click **Build Report** to begin report generation.

   When the report is completed, report notifications are sent to the specified email recipients. Unless you attached a copy of the report, they must log in to their SEP SBE cloud account to see it.

Reports page

From the **Reports** page you can:

- See an overview of your recently generated reports
- Download a PDF, HTML, XML of completed reports.
- Mozilla Firefox requires an extension to be installed to read and write MHT files. Many such extensions are freely available.
- View the report by clicking the report name
- Remove the report from your report history. Check the box next to the report and click **Delete Report**.

To view a report

1. On the top of any page, click **Reports**.

   The **Reports** page appears with your report history displayed on the right side of the page.
2. Click the name of the report to save, open, and view it.

Rerunning, editing, or scheduling your reports

In Symantec Endpoint Protection Small Business Edition cloud, you can rerun, edit, or schedule the reports that you saved as a template. Saving a report as a template keeps all the settings you specified when you created the report. You can edit these settings whenever you like.

When you run a report, it is available on the **Reports** page when it is generated. Your selected users receive a copy by email.

To rerun a report

1. In the SEP SBE Management Console, click **Reports**.
2. In the left pane, click **Report Templates**.
3. Click **Generate Report** in the **Actions** column next to the template that you want to re-run.

To edit a Report Template

1. In the SEP SBE Management Console, click **Reports**.
2. In the left pane, click **Report Templates**.
3. Click the name of the report template that you want to modify to re-open the **Report Wizard**.
4. You can now modify the configuration of the report and save a new version of the report template.
5. For more information on modifying the report template, see:

To schedule a template to run reports automatically

1. In the SEP SBE Management Console, click **Reports**.
2. In the left pane, click **Scheduled Reports**.
3. Click **Add Scheduled Report** at the top of the scheduled reports listing to schedule a template to run automatically.
4. In the **Add Schedule** window:

   Use the **Report Template** drop-down menu to select a template to schedule.

   Use the **How Often** drop-down menu to set the report to run daily, weekly, monthly, or quarterly, and then select the options for the frequency.

   Use the **Starting At** drop-down menu to set the GMT hour that the report runs.

   Click **Submit** to create the new scheduled report.