Symantec Endpoint Protection Small Business Edition (cloud-managed) Administrator's Guide

Symantec Endpoint Protection Small Business Edition (cloud-managed) Administrator's Guide

Documentation version: August 2017

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Contents

Chapter 1

Installing the cloud agent

This chapter includes the following topics:

System requirements

You manage your Symantec Endpoint Protection Small Business Edition (SEP SBE) cloud account through your web browser. For the computers that you use to manage your account, you can use most Windows, Linux or Macintosh computers. Computers running the Endpoint Protection agent require a Windows operating system.

Management console browser access requirements

- Cookies enabled
- JavaScript enabled
- SSL enabled

- Firewall ports 80 and 443 permitted
- Email address for user accounts, alerts, and reports

Table 1-1 Browser requirements

Browser	Version(s)
Microsoft Internet Explorer	11, Edge, and later. Microsoft no longer provides security updates or technical support for older versions of Internet Explorer. The management console may still work on older versions but it is encouraged to use later versions.
Mozilla Firefox	Only the latest version is supported
Google Chrome	Only the latest version is supported. Use Google Chrome for best viewing experience.
Other browsers	May work but not supported

Note: Older browsers are less stable and more vulnerable to virus, spyware, malware, and other security issues.

Upgrading to the latest version makes your experience using SEP SBE noticeably greater and more secure.

Cloud Service Agent and Symantec Endpoint Protection Small Business Edition endpoint (client) requirements

- AMD or Intel-based hardware
- Disk space
  - Desktops and laptops: 800 MB
  - Servers: 1000 MB

Table 1-2 Operating system (OS) requirements

Operating system	Edition	Service pack (SP)	Architecture	Endpoint Protection	Local Update Host
Microsoft Windows 7	Enterprise	SP1	x64 and x86	Yes	Yes
Microsoft Windows 7	Professional	SP1	x64 and x86	Yes	Yes
Microsoft Windows 7	Ultimate	SP1	x64 and x86	Yes	Yes
Microsoft Windows 8			x64 and x86	Yes	Yes

Table 1-2 Operating system (OS) requirements *(continued)*

Operating system	Edition	Service pack (SP)	Architecture	Endpoint Protection	Local Update Host
Microsoft Windows 8	Enterprise		x64 and x86	Yes	Yes
Microsoft Windows 8	Pro		x64 and x86	Yes	Yes
Microsoft Windows 8.1			x64 and x86	Yes	Yes
Microsoft Windows 8.1	Enterprise		x64 and x86	Yes	Yes
Microsoft Windows 8.1	Pro		x64 and x86	Yes	Yes
Microsoft Windows 10	Pro		x64 and x86	Yes	Yes
Microsoft Windows 10	Enterprise		x64 and x86	Yes	Yes
Microsoft Windows 10	Home		Enterprise	Yes	Yes
Microsoft Windows Server 2008 R2	Datacenter	SP1	x64	Yes	Yes
Microsoft Windows Server 2008 R2	Enterprise	SP1	x64	Yes	Yes
Microsoft Windows Server 2008 R2	Standard	SP1	x64	Yes	Yes
Microsoft Windows Server 2012	Datacenter		x64	Yes	Yes
Microsoft Windows Server 2012	Standard		x64	Yes	Yes
Microsoft Windows Server 2012 R2	Standard		x64	Yes	Yes
Microsoft Windows Server 2016			x64		
Microsoft Windows Small Business Server 2008	Standard	SP2	x64	Yes	Yes
Mac 10.13, 10.12, 10.11, and 10.10				Yes	No

See “Internet access requirements” on page 9.

Internet access requirements

For networks using proxies such as the Microsoft ISA or Linux Squid, it may be necessary to add Endpoint Protection URLs to the proxy whitelist. If an application firewall is in use, the whitelist should extend to the IPS section as well and settings like "Deep Packet Inspection" need to be disabled. Adding these URLs to your proxy whitelist allows all necessary agent communications:

- www.symantec.com
- www.norton.com
- liveupdate.symanteclive update.com
- ratings-wrs.symantec.com
- stats.qalabs.symantec.com
- avs-avpg.crsi.symantec.com
- bash-avpg.crsi.symantec.com
- csasmain.symantec.com
- csasalt.symantec.com
- central.b6.crsi.symantec.com
- central.nrsi.symantec.com
- central.avsi.symantec.com
- cloudconnect.norton.com
- cloudconnect2.norton.com
- definitions.symantec.com
- ent-shasta-rrs.symantec.com
- faults.qalabs.symantec.com
- faults.norton.com
- hb.lifecycle.norton.com
- lcsitemain.symantec.com
- lc1alt.symantec.com
- oem.lifecycle.norton.com
- o2.norton.com
- pif2.symantec.com

- sasmain.symantec.com
- sas1alt.symantec.com
- sigs.symantec.com
- sitedirector.symantec.com
- spoc.symantec.com
- stnd-ipsg.crsi.symantec.com
- shasta-ars.symantec.com
- shasta-clt.symantec.com
- shasta-mr-healthy.symantec.com
- shasta-mr-clean.symantec.com
- shasta-nco-stats.symantec.com
- shasta-rrs.symantec.com
- siaw.symantec.com
- ssaw.symantec.com
- stats.qalabs.symantec.com
- stats.norton.com
- ss.symcb.com
- spoc-pool-gtm.norton.com
- heartbeat.s2.spn.com
- message.s2.spn.com
- hostedendpoint.spn.com
- ins.spn.com
- https://manage.symanteccloud.com
- https://activate.symanteccloud.com
- http://help.elasticbeanstalk.com

Testing

For instructions regarding how to test and confirm the connectivity to installation and activation URLs please consult the following article:

http://www.symantec.com/docs/TECH216421

LiveUpdate Host Troubleshooting

http://www.symantec.com/docs/TECH217557

See “System requirements” on page 6.

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:

Table 1-3 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
12.1.3001.165	SEP SBE 12.1 RU3	SEP 12.1 RU3

Table 1-4 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 1-5 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

To assist you in removing antivirus and firewall products from your computers, Symantec Support suggests that you review this listing of vendor-specific removal tools.

See "Uninstalling antivirus and firewall products" on page 14.

Uninstalling antivirus and firewall products

The website that you are about to access has an extensive list of product removal tools. Some links on the page directly download executable files. Removal tools always carry the risk of damage to your computers, please ensure that you have a recent backup before using any of these tools.

Note: Symantec is not responsible for the linked content and has not verified the safety of the sites listed.

Antivirus and firewall product removal tool list

See "Removing existing antivirus and firewall products" on page 11.

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.

For Windows computers continue reading this topic. For Mac computers, see

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.

See "System requirements" on page 6.

See "Internet access requirements" on page 9.

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.

See "Removing existing antivirus and firewall products" on page 11.

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 fulfill 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
Redistributable installer package	Enables a network administrator to push out agents to the computers requiring protection. It provides a silent install of the agent and the services that are selected for use in the package. **Note:** The redistributable package can also be configured for deployment using Microsoft Active Directory. An Administrator can revoke the invitation, if necessary.
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 groups drop-down.
4. Under **Download Windows 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 use the redistributable installer package for silent installation

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 Windows Installer** > **Download a Redistributable Package** section, click **Download**.

   Depending on your browser, the file is automatically downloaded or you may be asked to run or save the file.
5. When the SymantecPackageCreator.exe file download is complete, run the file.
6. When the **Package Creator** dialog box opens, click **edit** to identify where to save the redistributable package.
7. In the **Advanced** section, click **edit** next to **Operating Systems** to choose the Windows versions that you want your package to support.
8. In the **Advanced** section, click **edit** next to **Proxy Settings** to enter your organization's proxy settings for use by the Package Creator. This step is optional and only necessary when these settings are required for Internet access. Click **Save**.
9. If you intend to deploy using Active Directory, check **Create Active Directory Group Policy deployment** in the **Advanced** section.

   See “Installing the cloud agent using Active Directory” on page 22.

10 Click **Begin**.

11 When the download is complete, click **Finish**.

12 The selected files are downloaded and then the package is created. Browse to the location where SymRedistributable.exe and package files are saved. You may want to copy the redistributable installer package to a directory of your choice.

This command-line application can be used to perform a silent install at user logon or in other network push processes. The following parameters can be passed to the application:

Usage: `SymRedistributable.exe [options]`

Command	Description
-silent	Orders silent operation.
-force	Replaces existing SEP SBE 12.1.x product. Requires -silent to be present.
-refresh	Reinstalls only if the installed files are outdated compared to the files in the redistributable. The computer automatically restarts during the process. Requires –silent to be present.
-refreshall	Reinstalls regardless of the installed version. The computer automatically restarts during the process. Requires –silent to be present.
-rebootinstall	Restarts the computer automatically following a successful installation if one is required. Requires –silent to be present.
-rebootwarn	Displays a message to the logged-on user that after a successful installation the computer restarts in 5 mins. Requires –silent to be present. Requires –silent to be present.
-installpath <path>	Specifies install path as: "c:\path\to\install\to". Requires -silent to be present. The -installpath parameter defaults to %programfiles%
-proxyhost <host>	Specifies the HTTP proxy IP address or the host name. Requires -silent and -proxyport to be present.
-proxyport <port>	Specifies the HTTP proxy network port number. Requires -silent and -proxyhost to be present.
-proxytype [HTTP|SOCKS]	Specifies the HTTP proxy or SOCKS proxy type; the default proxy type is HTTP. Requires -silent and -proxyhost to be present.
-proxyauthuser <user>	Specifies the proxy authentication user. Requires -silent and -proxyhost to be present.
-proxyauthpassword <password>	Specifies the proxy authentication password. Requires -silent and -proxyhost to be present.

Command	Description
-help, -h, -?	Prints help menu to screen.

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 Windows 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.

   See "Sending users a procedure explaining their download invitations" on page 27.

Installing the cloud agent using the redistributable installer package

The redistributable package enables you to deploy Symantec Small Endpoint Protection Small Business Edition (SEP SBE) cloud throughout your organization with a silent install. The package is an executable that runs silently, without any user interface, and installs the cloud agent to any computer running a supported operating system. Larger organizations may distribute the package with a specialized tool; smaller organizations can distribute it using a network share available in Explorer. Administrative rights are required to install the cloud agent onto a computer.

Note: Accounts that are provisioned through Symantec eStore must verify that there are adequate licenses before you deploy agents using the redistributable package.

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

See "Removing existing antivirus and firewall products" on page 11.

This command-line application can be used to perform a silent install at user logon or in other network push processes. The following parameters can be passed to the application:

Usage: `SymRedistributable.exe [options]`

Table 1-6 Command-line flags for redistributable package

Command	Description
-silent	Orders silent operation.
-force	Replaces existing SEP SBE 12.1.x product. Requires -silent to be present.
-refresh	Reinstalls only if the installed files are outdated compared to the files in the redistributable. The computer automatically restarts during the process. Requires –silent to be present.
-refreshall	Reinstalls regardless of the installed version. The computer automatically restarts during the process. Requires –silent to be present.
-rebootinstall	Restarts the computer automatically following a successful installation if one is required. Requires –silent to be present.
-rebootwarn	Displays a message to the logged-on user that after a successful installation the computer restarts in 5 mins. Requires –silent to be present. Requires –silent to be present.
-installpath <path>	Specifies install path as: "c:\path\to\install\to". Requires -silent to be present. The -installpath parameter defaults to %programfiles%
-proxyhost <host>	Specifies the HTTP proxy IP address or the host name. Requires -silent and -proxyport to be present.
-proxyport <port>	Specifies the HTTP proxy network port number. Requires -silent and -proxyhost to be present.
-proxytype [HTTP|SOCKS]	Specifies the HTTP proxy or SOCKS proxy type; the default proxy type is HTTP. Requires -silent and -proxyhost to be present.
-proxyauthuser <user>	Specifies the proxy authentication user. Requires -silent and -proxyhost to be present.
-proxyauthpassword <password>	Specifies the proxy authentication password. Requires -silent and -proxyhost to be present.
-help, -h, -?	Prints help menu to screen.

To download a redistributable install package

1. In the SEP SBE Management Console, click **Computers**.
2. In the **Computers** page, click **Add Computer**.
3. In the **Protect Computer** page, use the groups drop-down to select a computer group to populate with this install package.
4. In the **Download Windows Installer** > **Download a Redistributable Package** section, click **Download**.

   Depending on your browser, the file is automatically downloaded or you may be asked to run or save the file.
5. When the SymantecPackageCreator.exe file download is complete, run the file.
6. When the **Package Creator** dialog box opens, click **edit** to identify where to save the redistributable package.
7. In the **Advanced** section, click **edit** next to **Operating Systems** to choose the Windows versions that you want your package to support. Click **Save**.
8. In the **Advanced** section, click **edit** next to **Proxy Settings** to enter your organization's proxy settings for use by the Package Creator. This step is optional and only necessary when these settings are required for Internet access. Click **Save**.

   Note: You may create a number of distribution packages to fit the needs of your organization's different network locations.

   ---
9. If you intend to deploy using Active Directory, check **Create Active Directory Group Policy deployment** in the **Advanced** section.

   See "Installing the cloud agent using Active Directory" on page 22.
10. Click **Begin**.

    The selected files are downloaded and then the package is created. The redistributable package files are associated with a specific organization and should not be used outside of that organization.

    When the download is complete, click **Finish**.

Installing the cloud agent using Active Directory

Deploying Symantec Endpoint Protection Small Business Edition (SEP SBE) cloud with Microsoft Active Directory involves the following steps:

- Downloading the package

- Setting up a domain controller for deployment

Note: All antivirus products and firewall products must be removed from your computers before you install SEP SBE cloud.

See "Removing existing antivirus and firewall products" on page 11.

Note: Administrators of the SEP SBE cloud accounts that are provisioned through eStore, must ensure that they have adequate licenses for the number of computers targeted in the Active Directory deployment. If you run out of licenses during your Active Directory deployment, the installations fail for computers without licenses. Active Directory reports a successful install, but that is a false-positive.

Downloading the package

During the download of the Active Directory-ready redistributable installer package, three files are compiled for use by the organization's IT department. These files must always reside in the same folder to function properly and should not be mixed with different downloads of the redistributable package:

- SYMRedistributable.exe
- SYMGroupPolicyDeployment.msi
- GPO-YYYYMMDDHHMM.mst
  SYMGroupPolicyDeployment.mst is now saved as GPO-YYYYMMDDHHMM.mst.

For more information about using MST files, see the Microsoft documentation for:

- Windows 2008, Windows Server 2008 R2, or Windows Server 2012
- Windows 2003

Another Microsoft article that may be useful in preparing for an Active Directory deployment is: How to assign software to a specific group by using Group Policy

To download a redistributable installer package for Active Directory deployment

1. In the SEP SBE Management Console, click **Computers**.
2. In the **Computers** page, click **Add Computer**.
3. In the **Protect Computer** page, use the groups drop-down to select a computer group to populate with this install package.
4. In the **Download Windows Installer** > **Download a Redistributable Package** section, click **Download**.

   Depending on your browser, the file is automatically downloaded or you may be asked to run or save the file.

5 When the SymantecPackageCreator.exe file download is complete, run the file.

6 When the **Package Creator** dialog box opens, click **edit** to identify where to save the redistributable package.

7 In the **Advanced** section, click **edit** next to **Operating Systems** to choose the Windows versions that you want your package to support. Click **Save**.

Note: The latest version of SEP SBE is compatible on Windows Server 2016, but it is not certified. A certified version will be available in the near future.

---

8 In the **Advanced** section, click **edit** next to **Proxy Settings** to enter your organization's proxy settings for use by the Package Creator. This step is optional and only necessary when these settings are required for Internet access. Click **Save**.

Note: You may create a number of distribution packages to fit the needs of your organization's different network locations.

---

9 In the **Advanced** section, check **Create Active Directory Group Policy deployment**.

The following options are available when **Create Active Directory Group Policy deployment** is selected.

- **Restart computers automatically** - The computer automatically restarts to complete installation if required. User interaction is not required. If you are logged on to the computer during the installation process and if a restart is required, a message is displayed notifying you of the restart.
- **Upgrade outdated computers** - Reinstalls only if the installed files are outdated compared to the files in the redistributable. The computer automatically restarts during the process if required. This option works regardless of if SEP SBE was first installed manually or by Group Policy.
  If you have deployed software package using Group Policy before this installation, you can add this upgrade version to the Active Directory Server. You can add either alongside older packages or mark as an upgrade of the older packages to avoid installing the old version to computers that have been newly added to the group.
  Because servers require two restarts, we recommend that you also select **Restart computers automatically** to complete server installations without user interaction.

Selecting both the options ensures that the new installations automatically restart and the existing installations are upgraded if required.

10 Click **Begin**.

11 The selected files are downloaded and then the package is created. The redistributable package files are associated with a specific organization and should not be used outside of that organization.

12 When the download is complete, click **Finish**.

13 The files: SYMRedistributable.exe, SYMGroupPolicyDeployment.msi, and GPO-YYYYMMDDHHMM.mst are in the destination directory. These files must be kept together as a single package; mixing different versions of these files breaks the redistributable package.

Setting up a domain controller for deployment

When the download is complete, the domain controller must be set up for the SEP SBE cloud deployment. The procedures for accomplishing this task are well documented in the following Microsoft knowledge base article:

How to use group policy to remotely install software in Windows Server 2003 and in Windows Server 2008

- When you add a new SEP SBE package to GPO you must select **Advanced** rather than **Published** or **Assigned**. You then select the **Modifications** tab of the GPO deployment properties and add the MST file from the SEP SBE package. The Microsoft's article does not mention this scenario.
- GPO deployment and other installation logs can be found on client's end at C:\ProgramData\Symantec.cloud\syminstall\
- The default SEP SBE GPO deployment does not uninstall or upgrade other versions except in limited cases, and the MST file must first be modified to add the -force or -refresh/refreshall command line options.
  See "Installing the cloud agent using the redistributable installer package" on page 20.
- To go to Software Settings in Group Policy Management
  1. Under **Administrative Tools**, open **Group Policy Management**.
  2. Right click **Default Domain Policy** or the name of the policy the GPO is to be added to.
  3. Select **Edit**.
  4. If the software is to be installed per computer, select **Computer Configuration**->**Policies**->**Software Settings**.

  Or

  If the software is to be installed per user, select **User Configuration**->**Policies**->**Software Settings**.

  Symantec recommends installing per computer as this option allows all windows systems on the network to get the install package.

To install Orca

1. The Orca installer editor can be installed from "MSI Tools" of Windows SDK.
2. Using Orca, open the MSI file from the SymADFiles_Cloud files.
3. Select **Apply Transform** from the **Transform** menu, and then choose the MST from the same files.
4. Go to **Property** table, and modify SHS_PARAM_REDIST_COMMAND_ARGS property to include desired command-line option(s)
5. Go to **Transform** menu and select **Generate Transform** and save the new transform to the same location, but with a different file name (e.g. GPO-201611201532-force.mst).
6. Add your package to GPO as before, but use modified MST file.

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 you 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.

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.

   See "Removing existing antivirus and firewall products" on page 11.

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.

Upgrading the cloud agent

Symantec Endpoint Protection Small Business Edition (SEP SBE) cloud uses LiveUpdate to upgrade the cloud and the endpoint protection agents on workstations and servers. There also multiple methods for manually updating agents if required.

- Server LiveUpdate
  Server upgrades are handled independently of workstations and often require manual intervention.
- Workstation LiveUpdate

Workstation upgrades are independent of server upgrades and tend to happen more frequently.

Workstations get the latest antivirus, policy, and agent upgrades automatically. However, you can use LiveUpdate to force the workstations to update using the **Check for Updates** menu option in the notification area of the agent. This option is useful when an agent has been offline for a considerable period of time.

The upgrade does not require any user interaction, but it may prompt for a computer restart.

- Manual upgrade

  Use any of the manual methods available to upgrade if you don't have the latest agent.

- Mac upgrade

  Use any of the manual methods available to upgrade your unmanaged (but licensed) Mac computer to the latest macOS.

- Are my agents upgraded?

  You can check if an agent requires an update from the **Computers** page of the console.

- How to check agent version?

  You can check an agent's version from the **Computer Profile** page of the console.

  You can also view the version from **Help->About** on the agent's user interface.

- Unused agents

  To ensure full protection across your entire organization, delete the agents that are no longer used and are offline.

- Troubleshoot

  If you experience issues during the upgrade or install process, see the following:

  - Cannot install or activate clients due to blocked domains
  - Error: "Pending License Activation" or "Service Expired" on the client
  - Error: "LiveUpdate operations are unable to finish" when the server upgrades using LiveUpdate

Chapter 2

Customizing Endpoint Protection

This chapter includes the following topics:

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, under Services, click **Endpoint Protection**.
3. You can either create a new policy from scratch or save a copy of the default policy.

   To save a copy of default policy, click on the **Endpoint Protection Default Policy** link. A warning is displayed saying that default policies cannot be edited. Click **Save a Copy**.

   To create a policy from scratch, click **Add Policy**.
4. 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.

   - Table 2-1
   - Table 2-2
   - Table 2-3
   - Table 2-4

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

These categories of protection offer a defense in-depth security solution. **Computer Protection** features focus on the high risk communications reaching a computer.

Table 2-1 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. See "Creating custom exclusions" on page 44. **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

Table 2-1 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 2-1 Computer Protection *(continued)*

Protection Setting	Description	Desktops & Laptops	Servers
Full-screen Detection	Full-screen detection stops antivirus scans and prioritizes performance of the computer over antivirus scanning. Endpoint Protection still runs in the background providing continuous protection.	X	

USB Device Control enables administrators to prevent malicious code injection and intellectual property theft by controlling employee use of USB removable storage devices. USB mice and keyboards are unaffected by **USB Device Control** because they do not provide data storage.

Table 2-2 USB Device Control

Protection Setting	Description	Desktops & Laptops	Servers
USB device access	The drop-down enables a policy configuration to either allow or to block access to a USB device. Blocking events are logged for review and reporting.	X	X
Read only access	The check box allows USB device access to be restricted to read-only access. **Note:** This function is not available for servers.	X	
Enable user notifications	Enables the toast messages on the endpoint alerting the user to USB device blocking.	X	X

Web Protection defends Internet Explorer and Firefox from attack; presents website safety ratings; and evaluates downloads from the web.

Table 2-3 Web Protection

Protection Setting	Description	Desktops & Laptops	Servers
Browser Protection	With the increase in Internet use, your web browser is prone to attack by malicious websites. These websites detect and exploit the vulnerability of your web browser to download malware programs to your system without your consent or knowledge. These malware programs are also called drive-by downloads. Norton Internet Security protects your web browser against drive-by downloads from malicious websites. Norton Internet Security proactively blocks new or unknown malware programs before they attack your computer. By protecting your web browser, Norton Internet Security secures your sensitive information and prevents the attackers from controlling your system remotely. The **Browser Protection** feature checks for browser vulnerabilities in the following browsers: ■ Internet Explorer ■ Firefox ■ Chrome You must turn on the **Browser Protection** option to enable this feature. **Note:** This feature applies only to desktops and laptops.	X	

Table 2-3 Web Protection *(continued)*

Protection Setting	Description	Desktops & Laptops	Servers
Download Intelligence		X	

Table 2-3 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		

Table 2-3 Web Protection *(continued)*

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.

Table 2-4 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	

Table 2-4 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. See "Configuring Firewall Rules" on page 49.	X	

Table 2-4 Network Protection *(continued)*

Protection Setting	Description	Desktops & Laptops	Servers
Email Protection	Provides the protection to the inbound and the outbound emails by guarding against the most common email viruses, worms, and Trojans.	X	

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**.

See "Creating custom exclusions" on page 44.

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.

Configuring USB Device Control

In Symantec Endpoint Protection Small Business Edition (SEP SBE) cloud, **USB Device Control** enables administrators to prevent malicious code injection and intellectual property theft by controlling employee use of USB removable storage devices. USB mice and keyboards are unaffected by **USB Device Control** because they do not provide data storage. **USB Device Control** configuration is part of either a new policy or an existing Endpoint Protection policy. Endpoint Protection policies enable you to enforce the following levels of security over USB storage devices based on groups.

- Allow
  The default Endpoint Protection policy setting for device control allows full access to USB storage devices.
- Block
  By default, small pop-up notifications on the endpoint are disabled.

Note: Device control restrictions do not apply to servers.

When your policy allows USB devices, all computers in the groups to which the policy applies have complete access to USB storage devices. Allow is the default setting. You may specify read-only access for USB storage devices.

When your policy blocks USB devices, you may enable notifications on the endpoint. The notifications appear as small pop-up messages in the bottom, right-side corner of the endpoint computer. Notifications are off by default.

All blocking events are logged for review and reporting. The blocking events are recorded in a number of locations:

- As a line item in the **Endpoint Protection** widget on the **Home** page.
- As line items on the **Computer Profile > Services** tab
- As individual events that are recorded on **Computer Profile > History** tab
- In the **USB Device Control** portion of the **Endpoint Protection Security Overview** report

To configure USB device control in an existing Endpoint Protection policy

1. In SEP SBE Management Console, click **Policies**.
2. On the **Policies** page, locate the Endpoint Protection policy to modify and double-click it.
3. In the **USB Device Control** section, use the drop-down to **Allow** or to **Block** access to USB devices.
4. Use the checkboxes to:
   - Disable or enable read-write access to the USB storage device.

     Note: Only active for the **Allow** option.

   - Enable or disable user notification of USB blocking.

     Note: Only active for the **Block** option.

5. When you are done, click **Save and Apply**.

Overriding USB Device Control on an endpoint

USB Device Control can temporarily prevent the insertion of a USB thumb drive into a computer by setting a password. This capability reduces the risk of malicious code injection or theft of an organization's intellectual property. This security service can thwart the legitimate efforts of network administrators. Many administrators carry USB storage devices containing management software with them to service the computers on their network.

Note: Best practices suggest that the use of USB devices for software installation is a security risk.

To configure an override password for agent administrators

1. In SEP SBE Management Console, click **Settings** and then **Computer Settings**.
2. Under **Agent Administrator Password**, select **Use this password for features displaying the lock icon**.

3 Enter the new password and confirm the password.

4 The agent administrator password can now override USB device controls or uninstall password protection on an endpoint.

This feature enables a trusted administrator to insert and use a USB device in endpoint computers.

To override USB Device Controls on an endpoint

1 From the notification area on the endpoint computer, open Symantec.cloud Agent.

2 From the main interface page, click **Endpoint Protection**.

3 When the main Endpoint Protection page opens, click the **Override USB Device Control** option in the right side menu.

4 Enter the administrator password into the USB Device Control password box when it opens and click **OK**.

The agent Administrator password provides full access to the inserted USB storage device until you restart the computer.

Note: The administrator's password must be entered and confirmed before the USB device is inserted into the computer. If the USB device is inserted before the password is entered, remove the USB device, reenter the administrator password, then reinsert the USB device.

Creating custom exclusions

In Symantec Endpoint Protection Small Business Edition (SEP SBE) cloud, custom exclusions make it possible to exclude specific files, folders and-or file types.

Endpoint Protection policies exclude any network drives mapped for desktops and laptops by default but permit scanning of removable drives on those computers. Checkboxes enable easy configuration of those two options.

As a convenience in configuring file and folder locations, the interface enables you to pick a predefined path variable for common Windows locations. Use the ... drop down portion of the path entry box to make your selection. You may append path statements to the variable.

Table 2-5 Predefined path variables - Windows Vista, Windows Server 2008 and later

Predefined path variables	Variable path in default Windows install
[COMMON_APPDATA]	C:\ProgramData
[PROGRAM_FILES]	C:\Program Files

Table 2-5 Predefined path variables - Windows Vista, Windows Server 2008 and later *(continued)*

Predefined path variables	Variable path in default Windows install
[PROGRAM_FILES_COMMON]	C:\Program Files\Common Files
[COMMON_PROGRAMS]	C:\ProgramData\Microsoft\Windows\Start Menu\Programs
[COMMON_STARTUP]	C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup
[COMMON_DESKTOPDIRECTORY]	C:\Users\Public\Desktop
[COMMON_DOCUMENTS]	C:\Users\Public\Documents
[SYSTEM]	C:\Windows\System32
[WINDOWS]	C:\Windows

Table 2-6 Predefined path variables - Windows XP and Windows 2003

Predefined path variables	Variable path in default Windows install
[COMMON_APPDATA]	C:\Documents and Settings\All Users\Application Data
[PROGRAM_FILES]	C:\Program Files
[PROGRAM_FILES_COMMON]	C:\Program Files\Common
[COMMON_PROGRAMS]	C:\Documents and Settings\All Users\Start Menu\Programs
[COMMON_STARTUP]	C:\Documents and Settings\All Users\Start Menu\Programs\Startup
[COMMON_DESKTOPDIRECTORY]	C:\Documents and Settings\All Users\Desktop
[COMMON_DOCUMENTS]	C:\Documents and Settings\All Users\Documents
[SYSTEM]	C:\Windows\System32
[WINDOWS]	C:\Windows

The accepted formats for a **File** exclusion path include:

- [drive letter]:\path\filename
- [path_macro]\path\filename
- Wildcards and trailing "\" are not accepted

The accepted formats for a **Folder** exclusion path include:

- [drive letter]:\path to directory\
- [path_macro]\path to directory\
- Wildcards are not accepted
- The trailing "\" is recommended, but not required
- Activate the **Subfolders** check box to add all files and child directories to the exclusion rule

In manually configuring an **Extension** exclusion the accepted format requires:

- Use only the characters in the extension, such as mdb
- Each extension must be used in a unique rule
- Wildcards and dot-characters are ignored

To exclude a file in a policy

1. In the SEP SBE Management Console > **Policies** page, click **Add Policy**.
2. In the **Computer Protection** section of the policy configuration page, click **Custom Exclusions**.
3. Select **File** from the drop-down menu.
4. Enter the file you want to exclude using the format: *[drive_letter]:\path_to_file\filename*
5. Click **Add** and the exclusion appears in the **Current Exclusions** list.
6. To finish, click **Save & Apply** at the bottom of the policy configuration page.

To exclude a file in a common location

1. In the SEP SBE Management Console > **Policies** page, click **Add Policy**.
2. In the **Computer Protection** section of the policy configuration page, click **Custom Exclusions**.
3. Select **File** from the drop-down menu.
4. Using the ... drop down, select **[PROGRAM_FILES]**.
5. Add the directory you want to exclude to the predefined path variable. It should appear as: *[PROGRAM_FILES]\Directory_Path_to_file_to_be_excluded\name_of_file_to_exclude*. In actual use it might appear as [PROGRAM_FILES]\W2_v3\Word2WAV_v3.exe
6. Click **Add** and the exclusion appears in the **Current Exclusions** list.
7. To finish, click **Save & Apply** at the bottom of the policy configuration page.

To exclude a folder

1. In the SEP SBE Management Console > **Policies** page, click **Add Policy**.
2. In the **Computer Protection** section of the policy configuration page, click **Custom Exclusions**.
3. Select **Folder** from the drop-down menu.
4. Enter the directory you want to exclude using the format: *[drive_letter]:\path_to_folder*
5. If you want to exclude all subdirectories within the excluded folder, click the **Subfolders** check box.
6. Click **Add** and the exclusion appears in the **Current Exclusions** list.
7. To finish, click **Save & Apply** at the bottom of the policy configuration page.

To exclude a folder in a common location

1. In the SEP SBE Management Console > **Policies** page, click **Add Policy**.
2. In the **Computer Protection** section of the policy configuration page, click **Custom Exclusions**.
3. Select **Folder** from the drop-down menu.
4. Using the ... drop down, select **[PROGRAM_FILES]**.
5. Add the directory you want to exclude to the predefined path variable. It should appear as: *[PROGRAM_FILES]\Directory_Path_to_folder_to_be_excluded*. In actual use it might appear as [PROGRAM_FILES]\W2_v3\
6. If you want to exclude all subdirectories within the excluded folder, click the **Subfolders** check box.
7. Click **Add** and the exclusion appears in the **Current Exclusions** list.
8. To finish, click **Save & Apply** at the bottom of the policy configuration page.

To exclude a file type

1. In the SEP SBE Management Console > **Policies** page, click **Add Policy**.
2. In the **Computer Protection** section of the policy configuration page, click **Custom Exclusions**.
3. Select **Extension** from the drop-down menu.

4 Using the ... drop down, you can pick from commonly used file types, or you can enter the file extension directly without the leading period. File type exclusions are system-wide; specifying a drive letter is unnecessary.

Note: File type exclusions must be entered singly; delimited lists of extensions are not accepted.

5 To finish, click **Save & Apply** at the bottom of the policy configuration page.

See "Configuring Endpoint Protection policies" on page 30.

Configuring Smart Firewall

Smart Firewall rules enable an administrator to tailor firewall security to the needs of their organization through custom policies. The smart firewall is not a boundary firewall device at the edge of an organization's network. Smart firewall resides on and defends endpoint computers individually based on policies for groups of computers.

Smart Firewall is part of the **Network Protection** settings for desktops & laptops in any policy you create for your organization. It monitors the communications between your computer and other computers on the Internet. It also protects endpoint computers from common security problems such as:

Improper connection attempts	Warns you of connection attempts from other computers and of attempts by programs on your computer to connect to other computers
Port scans	Cloaks the inactive ports on your computer thereby providing protection against attacks through hacking techniques such as port scanning
Intrusions	Monitors the network traffic to or from your computer for suspicious behavior and stops any attack before they threaten your system

Smart Firewall has four configuration controls:

- **User can disable Firewall** to allow users to disable the firewall a specified time period
  - 15 minutes
  - one hour
  - 5 hours
  - Until the system restarts
- **Report Blocked Events** to deliver firewall activity to your reporting database

- **Firewall Rules** to enable administrators to create rules suitable for their organization
- **Program Control** to simplify rule making for Agent-discovered programs.

The **User can disable Firewall** and **Report Blocked Events** check boxes turn a control on or off. **Firewall Rules** and **Program Control** provide additional configuration options.

Configuring Firewall Rules

In Symantec Endpoint Protection Small Business Edition cloud, a Smart Firewall is a barrier protecting an endpoint computer from dangerous or unwanted communications. Communications occur between source and destination IP addresses using a transport protocol and port number to access a service. Commands are sent to the service port number of the offered service. Responses are returned to the port that is specified by the computer initiating the communication. Firewall administrators can block or allow traffic between two computers using:

- IP addresses only
- Port number of the needed service
- Both IP address and service port number

While this capability is available within Endpoint Protection, manual configuration of firewall rules is risky for administrators without training and-or experience. We recommend thorough testing of any rules that you create.

The **Smart Firewall** configures a rule based on three characteristics:

- **Connections**
- **Computers**
- **Communications**

These rules are then applied to a group or groups of computers which represent internal IP addresses for the firewall rule.

Connections

The first step in defining a firewall rule is to declare what should be done with a connection meeting the criteria defined by the rule. Two actions are possible:

Allow	Allows the communication of this type to take place
Block	Prevents the communication of this type to take place

The direction of the connection is the next element identified for the connection:

Inbound	Inbound connections include communications from another computer to your computer.
Outbound	Outbound connections include communications from your computer to another computer.
Inbound and Outbound	Inbound and outbound connections include the incoming and the outgoing communications to and from your computer.

Computers

Specify the computers to which the rule should apply:

Any computer	The rule applies to all computers
Any computer in the local subnet	The rule applies only to computers in the local subnet
Choose computers	The rule applies only to the computers, sites, or domains that are listed. The options include: ■ Individually - by entering a computer name or URL ■ Using Range - by entering a range of IP addresses ■ Using Network Address - by entering an IP address and its subnet mask The computer identification options can be mixed within the defined addresses.

Communications

The final step in creating a new firewall rule is to define the communications protocols that are used for the connection. You can specify these protocols:

TCP, UDP, TCP and UDP, ICMP, ICMPv6, or All

When a protocol other than **ALL** is selected, communications of all types of the selected protocol are allowed. Whenever you need to be more restrictive build a **Custom List**.

A **Custom List** lets you build the list by:

Known Ports from List	The rule applies to the ports that are selected using **Click to view list**. Known Ports offer well-known services. Less common or proprietary applications require that you identify the ports that are used by the application.
Individual specified ports	The rule applies to the ports that you enter. Delimit multiple ports with spaces.
Port Range	The rule applies to all of the ports between the lowest to highest port number. Enter the Port Range from lowest to highest port number.

Finally, you must identify the ports in the list as **Local** or **Remote**.

Local	Local ports refer to a port on an Endpoint Protection protected computer. These are usually used for inbound connections.
Remote	Remote ports are on the computer with which your computer communicates. They are usually used for outbound connections.

Warning: Badly conceived or misconfigured firewall rules can expose an organization's network to penetration and-or loss of mission critical services. Safely test all new firewall rules before deploying to your organization.

To create a custom endpoint protection policy

- See "Configuring Endpoint Protection policies" on page 30.

To configure a computer group for testing policies and firewall rules

1. Create a computer group for testing firewall rules.
2. Move several test computers into the test group.
3. Create a test policy and apply it to the test group.
4. Create a new firewall rule and save & apply the policy with the new rule.
5. Test the rule using the computers in the test group.
6. Repeat the process and test the policy for each new rule added.
7. Verify that your rules are entered in the correct order.
8. Deploy the rule to your organization only after thorough testing.

To allow access to a well-known program (Post Office Protocol v3)

1. From the **Network Protection** portion of a policy configuration page, click **Firewall Rules**.
2. Click **Add Rule** to open the rule configuration page.
3. Enter a **Rule Name**: Allow POP3 email.
4. In the **Connections** section, set the **Connection** drop-down to **Allow** and the **Connection Type** to **Outbound**.
5. In the **Computers** section, set the drop-down to **Choose Computer, Individually** and www.POP3_mailserver.com (URL or IP address).
6. Click **>>** to add the computer to the list.
7. In the **Communications** section, set the drop-down to **TCP, Custom List** and **Known Ports from List**. Skip down to the **Local/Remote** drop-down and set it to **Remote**.

8 Click **Click to View List** to see the list of well-known TCP ports, check **110** for the POP 3 protocol, and then click **Apply**.

Note: Most modern POP mail servers use SSL/TLS security for communications so additional rules may be necessary to make a service accessible.

---

9 Click **OK** to complete the rule.

10 When you are finished creating or modifying the policy, click **Save & Apply** at the bottom of the policy configuration page. This action pushes out the policy and any new or any modified firewall rules to groups using the policy.

To allow access to a specific port at a specific address

1 From the **Network Protection** portion of a policy configuration page, click **Firewall Rules**.

2 Click **Add Rule** to open the rule configuration page.

3 Enter a **Rule Name**: Allow service on port 54321 from OurVendor.com.

4 In the **Connections** section, set the **Connection** drop-down to **Allow** and the **Connection Type** to **Outbound**.

5 In the **Computers** section, set the drop-down to **Choose Computer, Individually** and enter www.OurVendor.com (URL or IP address).

6 Click **>>** to add the computer to the list.

7 In the **Communications** section, set the drop-down to **TCP, Custom List** and **Individual Specified Ports**.

8 Change the **Local/Remote** drop-down to **Remote**.

9 Enter the Port number: 54321, and then click **>>** to add the port to the communications list.

10 Click **OK** to complete the rule.

11 When you are finished creating or modifying the policy, click **Save & Apply** at the bottom of the policy configuration page. This action pushes out the policy and any new or any modified firewall rules to groups using the policy.

To allow a trusted, external network access to a service on an internal computer

1 From the **Network Protection** portion of a policy configuration page, click **Firewall Rules**.

2 Click **Add Rule** to open the rule configuration pop-up.

3 Enter a **Rule Name**: Allow access to internal service from trusted, external network.

4 In the **Connections** section, set the **Connection** drop-down to **Allow** and the **Connection Type** to **Inbound**.

5 Under **Computers**, select **Choose Computers, Using Network Address**, and enter the trusted Network Address/Subnet Mask. Click **>>** to add the computer to the computers list.

6 Under **Communications**, select **TCP, Custom List, Port Range, Local**, and enter the port 6000 to 6005. Click **>>** to add the port to the communications list.

7 Click **OK** to complete the rule.

8 When you are finished creating or modifying the policy, click **Save & Apply** at the bottom of the policy configuration page. This action pushes out the policy and any new or any modified firewall rules to groups using the policy.

Enabling file and printer sharing

The default policy disables file and printer sharing and the default firewall rules cannot be modified, deleted, or re-ordered. However, administrators can add rules to the smart firewall that serve the needs of their organization.

To view the default firewall rules

1 From the **Policies** page, click **Add Policy**.

2 In the **Network Protection** portion of the policy configuration page, click **Firewall Rules** and then click **Show Default Rules**. The default rules cannot be modified, deleted, or re-ordered.

To use the default policy with file and printer sharing enabled

1 From the **Policies** page, click **Endpoint Protection > Endpoint Protection Default Policy**.

2 At the top of the Endpoint Protection policy configuration page, click **Save a Copy**.

3 Change the **Name** and **Description** to identify the policy as the default policy with file and printer sharing enabled.

4 In the **Network Protection** portion of the policy configuration page, click **Firewall Rules**.

5 Click the **Enable File and printer sharing** policy option so that it is green, or active.

6 In the **Groups** portion of the policy configuration page, select the groups that should use the modified, default policy. Click **Save & Apply**.

Blocking a program from connecting to the Internet

In Symantec Endpoint Protection Small Business Edition, the cloud agent detects the well-known programs running on each endpoint and adds the programs to an organization's database. The Smart Firewall allows these programs to run safely. However, an administrator can prevent

the discovered programs from connecting to the Internet if an organization's security policy prohibits it.

To create a custom endpoint protection policy

- See "Configuring Endpoint Protection policies" on page 30.

To block a program discovered using Program Control

1. From the **Network Protection** portion of a policy configuration page, click **Program Control**, and then click **Add Discovered Program**. To display the Agent-discovered programs.
2. Select the prohibited programs and click **OK**.
3. The selected programs appear in a **Discovered Program** list. Use the drop-down box that is associated with the program to **Block** it.
4. When you are finished click **Save & Apply**.

Scanning computers remotely

Endpoint computers can be scanned from a computer's profile page, an entire group of computers can be scanned from the computer group page.

Note: Agents that are installed on Windows 2008 do not support the management console fix, restore, and delete files feature.

Note: Agents that are installed on Windows Server 2012 do not support the management console restore of quarantined files.

To remotely scan a computer

1. Log into your account.
2. On the **Computers** page, click the name of the computer you want to scan.
3. On the **Computer Profile** page **> Services** tab, under the **Tasks** menu, click **Scan Now**.
4. Confirm your intention to scan a computer remotely by clicking **Scan Now** again.

   The scan runs silently on the remote computer.

To remotely scan computers or a group of computers

1. Log into your account.
2. Go to the **Computers** page.
3. On the left pane, select the group or you can select various filter options.

4 Based on the filters selected, the applicable computers are displayed in the right pane.

5 Select the check box in the header to select all computers that are listed or select specific computers individually.

6 Click the **Quick Scan** or **Full Scan** icon, and then click **OK** to confirm scan.

The scan runs silently on the remote computers.

Installing the on-premises Endpoint Protection Small Business Edition

Your license for Symantec Endpoint Protection entitles you to either the cloud or the on-premises version of Endpoint Protection.

To download the on-premises version of Endpoint Protection

1 From any page, click **Subscriptions**.

2 If you do not have your serial number written down, click **Subscription Details** under **Endpoint Protection Small Business Edition**, to retrieve it.

You must have your serial number information to both access and download your on-premises software.

3 Under **Endpoint Protection Small Business Edition**, locate and click **Download On-Premise Manager**.

4 A separate window opens enabling you to both access and download your software.

5 Install the downloaded software using your serial number to activate it.

Chapter 3

Implementing the Local Update Service

This chapter includes the following topics:

About the Local Update Service

The Local Update Service enables you to designate computers to serve as local update hosts. The local update hosts efficiently share software updates and definition files with other computers on the same network. This feature reduces Internet traffic to SEP SBE cloud by directing agents to download needed updates from the designated local update host. The conservation of Internet bandwidth by using Local Update Services may be substantial.

Deciding if the Local Update Service can work for you

The Local Update Service provides a tremendous benefit to networks with limited bandwidth for Internet access. The service enables you to configure local update hosts for each network segment. The local update hosts check for definition and software updates every 4 hours and downloads when updates are available. The rough download math for a local update host is:

```
(35MB*30 days)+170MB/month for additional files=1220MB/month
```

Without local update hosts, each of your endpoint protection computers does the same thing, consuming your Internet bandwidth. The heavy network load can be complicated when workers turn on their computers in the morning and agents look to the Cloud for updates. Even when you deploy local update hosts, Endpoint Protection computers still consume local network bandwidth to download updates and definition files. However, the downloads consume only

local network bandwidth rather than Internet bandwidth. Your strategy for local update host placement can mitigate heavy network loads by spreading out local update hosts by network segment.

To successfully deploy local update hosts to your network, planning and forethought are essential. However, there is no configuration required once you determine the best candidates to be your local update hosts.

Choosing local update hosts

Among the matters to consider are:

- How many agents exist on your network?
- What is the capacity of your Internet connection?
- Is your organization's network routed or bridged between locations?
- What is the capacity of the connection between locations?
- Does your organization support multiple networks at each location?
- What is the network utilization on each network segment?

As a general rule, small to medium-sized businesses using a switched gigabit ethernet network are unlikely to have local network utilization problems. The key topology concern is likely to be a remote office that is bridged to the main network and accesses the Internet over the connection. In such cases, software and definition updates for your agents may clog the network connection between the remote network and the main network. Whether agents seek updates from a local update host on the main network or go to the Internet for updates, the remote office connection suffers. In this case, deploying a local update host to a computer in the remote office relieves the strain on the remote network connection.

When remote offices are routed to the main organization's network and support a local connection to the Internet, the concerns are different. In this case you must consider:

- The capacity of the Internet connection
- The number of computers supported

If the remote office is small, the potential benefit is small. However, as the number of agents increases so do the benefits. A single local update host can support about 100 agents, 50 agents concurrently.

After considering your network topology and network utilization, you must delegate computers to be local update hosts. Some key requirements are:

- Microsoft server operating system preferred
- Extended uptime; 24-7 is preferred
- Computer name must be unique

- VMware hosts are not recommended

Symantec recommends using a dedicated server for the best performance. A local update host reserves 1 GB for cache. This memory consumption makes a few specific computer hardware requirements important:

- At least 4GB RAM to enable a local update host on a 32-bit computer.
- A fast hard drive; at least 7200 rpm.

See "Configuring a local update host" on page 58.

See "Understanding local update host vulnerabilities" on page 59.

Configuring a local update host

In Symantec Endpoint Protection Small Business Edition (SEP SBE) cloud, you designate the computers best suited for the role of local update hosts within the **Computers** page of the SEP SBE Management Console. In the absence of a System Policy assigning local update hosts to groups, endpoint protection computers discover their host during the regular Agent home call. The Agent home call is every 12 hours. From then on, local update host clients receive software updates and definition files from their local update host, reducing the load on the Internet connection.

When a local update host goes offline for any sort of problem, the local update host clients automatically failover to SEP SBE cloud. When a worker's laptop goes on the road, the agent fails over to SEP SBE cloud when it cannot find its local update host.

Note: Local update hosts use port 3128 so it must be accessible.

To designate a computer to be a local update host

1. In SEP SBE Management Console, click **Computers**.
2. On the **Computers** page, click on the computer name of the computer that you want to designate as a local update host.
3. On the **Computer Profile** page, in the list of actions on the right side, click **Enable as Local Update Host**.
4. Confirm the local update host promotion.
5. As agents update **Global System** policy or learn of a local update host on their network, the agent begins downloading updates from the local update host

   ---

   Note: It may take up to 12 hours for agents to connect to new local update hosts.

To view the computers assigned to a local update host

1. In SEP SBE Management Console, click **Computers**.
2. On the **Computers** page, click on the computer name of the local update host.
3. On the **Computer Profile** page, in the **Local Update Host** section, click the number link next to **Assigned Computers** to view a listing of the assignments.

To disable a local update host

1. In SEP SBE Management Console, click **Computers**.
2. On the **Computers** page, click on the computer name of the local update host that you want to decommission.
3. On the **Computer Profile** page, in the list of actions on the right side, click **Disable as Local Update Host**
4. Confirm that you want to decommission the local update host.
5. As other computers on the network communicate with SEP SBE cloud, the computers either resume getting updates from the cloud or are assigned to a new local update host on their network.

See "Understanding local update host vulnerabilities" on page 59.

See "About the Local Update Service" on page 56.

Understanding local update host vulnerabilities

A vulnerability scan on a local update host may present a number of new vulnerabilities for the computer serving as the local update host. Among the vulnerabilities you might find are:

High risk vulnerabilities:

- PHP Built-in web server 'Content-Length' denial of service Vulnerability
- HTTP TRACE XSS attack
- Apache chunked encoding
- Cisco VoIP phones denial of service
- NT IIS 5.0 Malformed HTTP Printer Request Header buffer overflow Vulnerability
- Squid information-disclosure vulnerability

Medium risk vulnerabilities:

- Squid HTCP Packets Processing denial of service Vulnerability
- Squid External Auth Header Parser DOS Vulnerabilities
- Squid Header-Only Packets Remote denial of service Vulnerability

Low risk vulnerabilities:

- Clock accuracy checker (by HTTP)
- Relative IP Identification number change

Note: The vulnerability names come from a customer-provided Security Space Security Audit. Different vendors use different names to describe similar vulnerabilities.

These vulnerabilities cannot be ignored. We mitigate the issues presented by the vulnerabilities in several ways:

- Anonymous access to the Squid proxy is not permitted.
- All communications with the proxy are limited to customer agents.
- Symantec recommends that a local update host be placed in inside of network perimeters on a stationary computer.
- Symantec also recommends blocking access from untrusted networks to local update host service port 3128. However, the firewall must permit communications between the local update host and Symantec services.

These mitigation factors protect the local update host from external attack. Administrators must, however, be alert for possible internal threats.

See “Configuring a local update host” on page 58.

See “About the Local Update Service” on page 56.

Chapter 4

Managing your computers

This chapter includes the following topics:

Performing actions on multiple computers

An administrator can move computers, run scans, update virus definitions, or delete computers simultaneously on multiple computers, computers belonging to a group, or on all of an organization's groups.

Note: Update virus definitions require adequate disk space to run successfully. Please ensure that your computers have 1 GB of available disk space to avoid update failures. Also, computers must be online to run a Quick Scan, a Full Scan, or to Update Virus Definitions.

To perform actions on multiple computers

1. Log into your account.
2. On the **Computers** page, in the left pane, select the applicable filters. For example: you can select a group and all computers that needs attention.

   The computers matching the filter options are displayed in the list pane.
3. You can select all computers or only the computers you want to perform an action on.

4 Select **Move Computers**, **Quick Scan**, **Full Scan**, or **Update Virus Definitions**, or **Delete Computers**.

5 SEP SBE cloud then dispatches the action to all of the computers that are connected when the action is performed.

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.
  See "Configuring the local agent's proxy settings" on page 64.
- In the absence of globally-assigned local update hosts, agents still discover a local update host.
  See "Configuring a local update host" on page 58.

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

To assign local update hosts

To configure a LiveUpdate schedule

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**.

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.

To configure a LiveUpdate schedule

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.

Configuring the local agent's proxy settings

In Symantec Endpoint Protection Small Business Edition (SEP SBE) cloud, the local agent proxy settings override the proxy settings in a global System Policy. The global policies are configured in the Management Console **Policies** page.

The policy-controlled proxy settings that are configured within the Management Console are applied to selected groups in your organization. Before you implement proxy settings from the

Management Console, Symantec recommends testing the intended configuration on a number of test computers first. Incorrectly configuring Proxy Settings in the management console risks locking out all of your cloud agents. Fortunately, the **Endpoint Protection** agent interface can override an errant configuration, but the correction requires manual intervention.

To configure proxy settings for a computer using the Endpoint Protection agent user interface

1. Double-click the **Symantec.cloud** icon in the notification area.
2. When the user interface opens, click **Settings** in the banner bar.
3. Click **Proxy Settings** from the **Settings** menu.
4. Activate the **Override Proxy Settings** check-box.
5. Activate the **Enable Proxy** check-box in the proxy configuration portion of the window.
6. Enter the **Host** and **Port** addresses for the proxy.
7. Activate the **Authenticated** check-box if authentication to the proxy is required and enter a **User name** and **Password**.
8. When you are finished, click **Apply** and **Close** to save your configuration.

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 for the alert and make the changes.

Chapter 5

Finding help

This chapter includes the following topics:

Getting help with Symantec Endpoint Protection Small Business Edition cloud

Symantec Endpoint Protection Small Business Edition cloud provides a number of resources for customers to get help with:

- Using the services
- Technical assistance
- Customer care
- Symantec sales

Table 5-1 User assistance resources

Resource type	Resource location
Online user assistance	■ Online Help ■ FAQ ■ Getting Started Guide ■ Administrator's Guide ■ See "Symantec Endpoint Protection Small Business Edition videos" on page 68.
Technical support	For helpful troubleshooting articles, contact options, videos, and other support resources, click here.

Table 5-1 User assistance resources *(continued)*

Resource type	Resource location
Customer care Customer care team can help with credit card-free trials, billing, invoices, renewals, licensing, and other concerns.	(800) 339-1136
Symantec sales	(800) 745-6054 opt 3

Note: Customers of Symantec partners should contact their partner directly for prompt assistance.

Symantec Endpoint Protection Small Business Edition videos

Here are the links to the Symantec Endpoint Protection Small Business Edition cloud videos:

- Using the Symantec Endpoint Protection Small Business Edition Wizard
- Removing existing antivirus & firewall products before installing Endpoint Protection
- Downloading the Agent for Symantec Endpoint Protection Small Business Edition cloud
- Conserving your Internet bandwidth with Symantec cloud services
- Creating policies to manage endpoint computers
- Creating and using groups in your Symantec cloud account
- Configuring an Endpoint Protection Firewall rule
- Configuring and using Program Control with Endpoint Protection
- Deploying Symantec Endpoint Protection Small Business Edition with Active Directory Windows Server 2003
- Deploying Symantec Endpoint Protection Small Business Edition with Active Directory Windows Server 2008