Symantec.cloud Administrator's Guide

Symantec.cloud Administrator's Guide

Last document update: 2014-02-19.

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Contents

Chapter 1

Deploying Agents to your computers

This chapter includes the following topics:

System requirements

You manage your Symantec.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 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	8 or later (For best results use IE 10+)
Mozilla Firefox	Only the latest version is supported
Google Chrome	Only the latest version is supported
Other browsers	May work but not supported

Platform Agent, Symantec Endpoint Protection Small Business Edition 2013, and BackupExec.cloud client requirements

- AMD ot 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	Storage Server
Microsoft Windows 7	Enterprise	SP1	x64 and x86	Yes
Microsoft Windows 7	Professional	SP1	x64 and x86	Yes
Microsoft Windows 7	Ultimate	SP1	x64 and x86	Yes (x86 only)
Microsoft Windows 8			x64 and x86	No
Microsoft Windows 8	Enterprise		x64 and x86	No
Microsoft Windows 8	Pro		x64 and x86	No
Microsoft Windows 8.1			x64 and x86	No
Microsoft Windows 8.1	Enterprise		x64 and x86	No
Microsoft Windows 8.1	Pro		x64 and x86	No

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

Operating system	Edition	Service pack (SP)	Architecture	Storage Server
Microsoft Windows Server 2003	Enterprise	SP2	x64 and x86	No
Microsoft Windows Server 2003	Standard	SP2	x64 and x86	No
Microsoft Windows Server 2003 R2	Standard	SP2	x64 and x86	No
Microsoft Windows Server 2008	Enterprise	SP2	x64 and x86	No
Microsoft Windows Server 2008	Standard	SP2	x64 and x86	No
Microsoft Windows Server 2008 R2	Datacenter	SP1	x64	Yes
Microsoft Windows Server 2008 R2	Enterprise	SP1	x64	Yes
Microsoft Windows Server 2008 R2	Standard	SP1	x64	Yes
Microsoft Windows Server 2012	Datacenter		x64	Yes
Microsoft Windows Server 2012	Standard		x64	Yes
Microsoft Windows Server 2012 R2	Standard		x64	No
Microsoft Windows Small Business Server 2008	Standard		x64	
Microsoft Windows Vista	Business	SP2	x64 and x86	No
Microsoft Windows Vista	Enterprise	SP2	x64 and x86	No
Microsoft Windows Vista	Ultimate	SP2	x86	No
Microsoft Windows XP	Professional	SP2	x64	No
Microsoft Windows XP	Professional	SP3	x86	No

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. These are the servers contacted by Cloud Endpoint Protection Agents for different tasks:

- hb.lifecycle.norton.com
- www.norton.com
- liveupdate.symantecliveupdate.com

- ratings-wrs.symantec.com
- stats.qalabs.symantec.com
- shasta-rrs.symantec.com
- sasmain.symantec.com
- sas1alt.symantec.com
- www.symantec.com
- ssaw.symantec.com
- siaw.symantec.com
- heartbeat.s2.spn.com
- message.s2.spn.com
- hostedendpoint.spn.com
- ins.spn.com
- https://manage.symanteccloud.com
- https://activate.symanteccloud.com
- backup.sp1.symanteccloud.com through backup.sp15.symanteccloud.com

Adding these URLs to your proxy whitelist allows all necessary Agent communications.

Removing existing antivirus and firewall products

To get the best performance from Symantec Endpoint Protection, 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 Endpoint Protection 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 Cloud Endpoint Protection 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.cloud clicking the **Support** link 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

Table 1-3 Auto-removable Symantec Endpoint Protection, Endpoint Protection Small Business Edition versions *(continued)*

Version	Endpoint Protection Small Business Edition	Symantec Endpoint Protection
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 Anti-Virus for Windows Workstations 6.0 Endpoint Security 10 for Windows (for workstations)
Windows InTune	Endpoint Protection

If the Endpoint Protection install program does not detect the product installed on your computer, please submit the details of the undetected product to us. Use the Request Form found by clicking the **Support** link in the Management Console banner. Please enter the:

- Name of the manufacturer
- Name of the product
- Version of the installed product

Your contribution is appreciated.

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 12.

See "Downloading the Package" on page 20.

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 9.

Downloading and installing the Symantec.cloud Agent

Before you can protect your computers with Symantec.cloud, you must download the agent and install it onto the computers you want to protect. 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.

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

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

These different methods can be use 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 login for your Symantec.cloud account
- Your physical presence at the computer or a remote connection to it

Email invitation	Enables you to send email invitations to download the Agent to computer users in your organization: ■ Up to 50 email addresses, 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 An Administrator can revoke the invitation, if necessary.
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 selected for use in the package. **Note:** The Redistributable Package can also be configured for deployment using Microsoft Active Directory.

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 9.

Note: Small Business Server 2011 may require a restart when the Platform and Backup Exec.cloud agents are installed.

To install the agent onto an individual computer

1. Log into your Management Console account.
2. Click **Add computer** in your **Home** page **Quick Tasks** widget or **Add Computers** on the **Computers** page.
3. On the **Add a New Computer or Service** page, select the service or services you want to install on the computer.
4. 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.
5. Under **Download Your Installer**, click **Install Now** and run the SymantecExtractor.exe.

   It's also possible to save the file if required.
6. The **File Download** dialog box gives you the option to **Run** or **Save** the file. Click **Run**.

7 When the SymantecExtractor.exe file download is complete, you are asked for permission to Run the software. Click **Run**.

8 The **Symantec.cloud Setup Wizard** opens. From the welcome screen, click **Next**.

9 The component configuration screen appears showing the status the components comprising your installation. You may also configure your Proxy Settings or change the destination folder if required. Click **Install**.

10 When the success screen appears, click **Finish**.

To use the Redistributable installer package for silent installation

1 Log into your Management Console account.

2 Click **Add computer** in your **Home** page **Quick Tasks** widget or **Add Computers** on the **Computers** page.

3 On the **Add a New Computer or Service** page, select the service or services you want to install on the computer.

4 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.

5 In the **Download your installer** portion of page, click **Download** in the **Download a Redistributable Package** area.

See "Deploying with the Redistributable Installer" on page 17.

6 The **File Download** dialog box gives you the option to **Run** or **Save** the SymantecPackageCreator file. Click **Run**.

7 When the file download is complete, you are asked for permission to run the software. Click **Run**.

8 When the **Symantec Package Creator** dialog box opens, click **Browse** to identify where to save the redistributable package.

9 In **Advanced Options**, click **Operating Systems** to choose the versions Windows that you want your package to support.

10 In **Advanced Options**, click **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.

11 If you intend to deploy using Active Directory, activate the **Require Active Directory Group Policy deployment** check box in **Advanced Options**.

For more information on deploying Symantec.cloud on Active Directory, see the following topic:

See "Deploying Symantec.cloud using Active Directory" on page 19.

12 To disable warnings during deployments, check **Suppress installer warnings during deployment**.

13 Click **Begin**.

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

15 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 login or in other network push processes. The following parameters can be passed to the application:

Usage: `SymRedistributable.exe [options]`

Options	Description
-silent	Orders silent operation
-suppresswarnings	Supresses installer warnings, requires -silent to be present
-installpath <path>	Specifies install path as: "c:\path\to\install\to", requires -silent The -installpath parameter defaults to %programfiles%
-proxyhost <host>	Specifies HTTP proxy IP address or hostname, requires -silent and -proxyport to be present
-proxyport <port>	Specifies HTTP proxy network port number, requires -silent and -proxyhost to be present
-proxytype [HTTP|SOCKS]	Specifies HTTP proxy or SOCKS proxy type, the default proxy type is HTTP, requires -silent and -proxyhost to be present
-proxyauthpassword <password>	Specifies proxy authentication password, requires -silent and -proxyhost to be present
-help, -h, -?	Prints help menu to screen

See "Deploying with the Redistributable Installer" on page 17.

To send email invitations to download the Agent

1 Log into your Management Console account.

2 Click **Add computer** in your **Home** page **Quick Tasks** widget or **Add Computers** on the **Computers** page.

3 On the **Add a New Computer or Service** page, select the service or services you want to install on the computer.

4 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.

5 In the **Download your installer** section, enter up to 50 user email addresses in the **Send Download Invites** text box. The specified users receive invitations with a download link to the Agent.

Multiple email addresses must be delimited with a semicolon.

Click **Send Email Invites**.

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

See "Sending users a procedure explaining their download invitations" on page 23.

Deploying with the Redistributable Installer

The Redistributable Install Package enables you to deploy Symantec.cloud throughout your organization with a silent install. The package is an executable that runs silently, without any user interface, and installs the Protection 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 Protection Agent onto a computer.

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 9.

Note: Accounts that are provisioned through Symantec eStore must verify that there are adequate licenses before you deploy Agents using the Redistributable Install Package.

Table 1-6 Command-line flags for Redistributable Package

Command	Description
-silent	Orders silent operation
-suppresswarnings	Supresses installer warnings, requires -silent to be present
-installpath <path>	Specifies install path as: "c:\path\to\install\to", requires -silent The -installpath parameter defaults to %programfiles%
-proxyhost <host>	Specifies HTTP proxy IP address or hostname, requires -silent and -proxyport to be present
-proxyport <port>	Specifies HTTP proxy network port number, requires -silent and -proxyhost to be present
-proxytype [HTTP|SOCKS]	Specifies HTTP proxy or SOCKS proxy type, the default proxy type is HTTP, requires -silent and -proxyhost to be present
-proxyauthpassword <password>	Specifies proxy authentication password, requires -silent and -proxyhost to be present
-help, -h, -?	Prints help menu to screen

To download a redistributable package

1. Log on to your Symantec.cloud account and click **Add Computer** in the **Quick Tasks** widget.
2. From the **Add a New Computer or Service** page, select the services that you want to be included in the package.
3. In step 2, **Choose Your Group**, use the drop-down to select a computer group to populate with this install package.
4. From the **Download Your Installer** section under **Download a Redistributable Package**, click **Download**.
5. When the **Opening SymantecPackageCreator.exe** dialog box opens, click **Save File**.
6. Double-click **SymantecPackageCreator.exe**, and then click **Run**.
7. When the **Symantec.cloud Package Creator** opens, in the **Advanced Options** section, click **Operating Systems**.
8. In the **Customize Targeted Operating Systems** dialog box, select the Windows versions that you want in the Symantec.cloud distribution package using the check boxes.

   When you are ready, click **Save**.

9 In the **Advanced Options** section, click **Proxy Settings** to enter the proxy settings for the Package Creator to use.

Specify the proxy type, host, and port number.

If the proxy requires authentication provide a user name and password.

When you finish, click **Save**.

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

---

10 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**.

Deploying Symantec.cloud using Active Directory

Deploying with Microsoft Active Directory involves a number of steps:

- Downloading the package
  See "Downloading the Package" on page 20.
- Setting up a domain controller for deployment
  - Create a Distribution Point
  - Create a group policy Object
  - Assign a Package

  See "Setting up a domain controller for deployment" on page 22.

The Microsoft documentation for deploying with Active Directory is available 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

---

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 9.

Note: Administrators of Symantec.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 Package, three files are compiled for use by the organization's IT department:

- SYMRedistributable.exe
- SYMGroupPolicyDeployment.msi
- SYMGroupPolicyDeployment.mst

These files must always reside in the same folder to function properly and should not be mixed with different downloads of the Redistributable Package.

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

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

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 9.

Note: Administrators of Symantec.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.

To download a Redistributable Package for Active Directory deployment

1. Log on to your Symantec.cloud account and click **Add Computer** in the **Quick Tasks** widget.
2. From the **Add a New Computer or Service** page, select the services that you want to be included in the package.
3. In step 2, **Choose Your Group**, use the drop-down to select a computer group to populate with this install package.

4 From the **Download Your Installer** section under **Download a Redistributable Package**, click **Download**.

5 When the **Opening SymantecPackageCreator.exe** dialog box opens, click **Save File**.

6 Double-click **SymantecPackageCreator.exe**, and then click **Run**.

7 When the **Symantec.cloud Package Creator** opens, in the **Advanced Options** section, click **Operating Systems**.

8 In the **Customize Targeted Operating Systems** dialog box, select the Windows versions that you want in Symantec.cloud distribution package using the check boxes.

When you are ready, click **Save**.

9 In the **Advanced Options** section, click **Proxy Settings** to provide proxy settings for the Symantec.cloud Package Creator. distribution package that you create.

Specify the proxy type, host, and port number.

If the proxy requires authentication enter the user name and password.

When you finish, click **Save**.

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

---

10 In the **Advanced Options** section, check **Require Active Directory group policy deployment**.

11 To disable warnings during deployments, check **Suppress installer warnings during deployment**.

12 Click **Begin**.

13 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.

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

15 The files: SYMRedistributable.exe, SYMGroupPolicyDeployment.msi, and SYMGroupPolicyDeployment.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.

See "Deploying Symantec.cloud using Active Directory" on page 19.

Setting up a domain controller for deployment

When the download is complete, the domain controller must be set up for the Symantec.cloud deployment. Three steps are involved in this process:

- Creating a Distribution Point
- Creating a group policy Object
- Assigning a Package

The procedures for accomplishing these tasks are well documented in Microsoft the support knowledge base. The knowledge base article :

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

The article covers how to:

- Create a Distribution Point.
- Create a group policy Object.
- Assign a Package.
- Publish a Package.

Note: The Redistributable Package does not support publishing a package.

- Redeploy a Package.
- Remove a Package.

Note: The administrator must complete the removal of an installation within the Symantec.cloud management console.

- Troubleshoot.

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

See “Deploying Symantec.cloud using Active Directory” on page 19.

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 Protection Agent.
- View your download invitation history.
- Deactivate download invitations.

The Send Invites portion 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 shut down. Download invitations expire 30 days after issuance.

To send download invitations and view your invitation history

1. Log into your Symantec.cloud account.
2. In the **Quick Task** box on your Home page, click **View Invitation History**.
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 Protection Agent

1. Log into your Symantec.cloud account.
2. In the **Quick Task** box on your Home page, click **View Invitation History**.
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

Symantec.cloud provides a method for you to allow your users to download and install the Cloud Endpoint Protection 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 Symantec.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 Symantec.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 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 9.

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.cloud Installation** box 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 Cloud Endpoint Protection Agent components are installed. Click **Next**.
9. When the success screen appears, uncheck the **Launch Website** checkbox and click **Finish**.
10. In most cases, your Symantec.cloud installation is automatically added to your organization's list of protected computers.

Chapter 2

Customizing Endpoint Protection

This chapter includes the following topics:

Understanding Endpoint Protection Policies

When any computer is added as an Endpoint Protection computer, it is immediately added to the default group and the default policy for immediate protection. The default group is only modified when computers are added or deleted; the default policy cannot be modified. The default configuration may serve your organization well, however, you can configure Groups and Policies that are tailored to your needs.

Symantec Endpoint Protection enables you to create and impose policies to protect your computers based on the security requirements of the computers. Four categories of protection that can be used in a policy:

- Computer Protection
- USB Device Control
- Web Protection
- Network Protection

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

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.

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. **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

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 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 increasing 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 7.0 or later ■ Firefox 10.0 or later ■ Chrome 17.0 or later 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
Safe Surfing	When Symantec Endpoint Protection installs on your computer, it adds the Norton Toolbar to Internet Explorer, Chrome, and Firefox. Norton Internet Security protects your supported browsers by enabling the Safe Surfing option by default. When Safe Surfing is turned on, Norton Internet Security enables the Antiphishing feature and the Norton Safe Web feature. Antiphishing analyzes the security levels of the websites you visit and displays the results in the Norton Site Safety pop-up. The Norton Safe Web feature displays site-rating icons next to web search results. **Warning:** When you turn off Safe Surfing, the Antiphishing feature and Norton Safe Web feature are disabled. In this case, Identity Safe can autofill fraudulent websites with your confidential information. Symantec recommends that you do not browse the web when Safe Surfing is turned off. **Note:** The Antiphishing and Norton Safe Web features are supported in the Internet Explorer, Firefox, or Chrome web browsers. **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 Insight 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 Insight 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 Insight 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 Insight. Download Insight 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 Insight 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 Insight 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.	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 Agent Group and are assigned the Endpoint Security default policy for each agent's installed service or services. No further configuration required.

To create computer groups

1. Log into your account and click the **Computers** page.
2. On the left pane, click the **Add Group** link in the **Groups** section.
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, in the header with group information, click the **Move Computers** link 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 Agent Group (or other assigned group) into your new computer group.

To create security policies

1. Log into your account and click the **Policies** page.
2. On the left pane, under **Services**, select the service for which you want to create a policy and click **Add Policy**.
3. On the **Policies** page, do the following:

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

   Assign the appropriate **Protection Settings** using the checkboxes.

   Consider and set Exclusions for your scans using the checkboxes. To exclude specific files, folders, or file types, click **Custom Exclusions**.

   Set a **Scan Schedule** by designating the scan frequency, time to start, and the computers to scan.

   Assign the policy to the appropriate groups in the **Groups** section of the page.
4. Click **Save & Apply**. The policy is applied to the computers in the selected group or groups.

About USB Device Control

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. The control provides the following levels of security enforced through policy at the endpoint:

- Allow.
- Block.

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 Home page widget
- As line items on the Computer Profile Services tab
- As individual events recorded on Computer Profile History tab
- In the USB Device Control portion of the Endpoint Protection Security Overview report

Configuring Device Control

Endpoint Protection policies enable you to create suitable controls over USB storage devices based on groups. Device Control affects USB thumb drives and hard drives, but not USB mice and keyboards because they do not provide data storage. USB Device Control configuration is part of either a new policy or an existing Endpoint Protection policy.

- 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.

To configure USB device control in an existing Endpoint Protection policy

1. From any page, 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 prevent the insertion of a USB thumb drive into a computer. 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. The **Computer Settings** portion of the **Settings** tab enables administrators a way to override the Block action set by an Endpoint Protection policy.

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. From any page, click **Settings** and then **Computer Settings**.
2. Under **Agent Administrator Password**, activate the **Specify the password for protected features** checkbox.

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 system tray on the endpoint computer, open the Cloud Endpoint Protection 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.

Using Exclusions

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. Custom Exclusions make it possible to exclude specific files, folders and-or file types.

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

Predefined path variables	Variable path in default Windows install
[COMMON_APPDATA]	C:\Documents and Settings\All Users\Application Data

Table 2-5 Predefined path variables *(continued)*

Predefined path variables	Variable path in default Windows install
[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. From the **Exclusions** section of a policy configuration page, click **Custom Exclusions**.
2. Select **File** from the drop-down menu.
3. Enter the file you want to exclude using the format: *[drive_letter]:\path_to_file\filename*
4. Click **Add** and the exclusion appears in the **Current Exclusions** list.
5. To finish, click **Save & Apply** at the bottom of the policy configuration page.

To exclude a file in a common location

1. From the **Exclusions** section of a policy configuration page, click **Custom Exclusions**.
2. Select **File** from the drop-down menu.
3. Using the ... drop down, select **[PROGRAM_FILES]**.
4. 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
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 folder

1. From the **Exclusions** section of a policy configuration page, click **Custom Exclusions**.
2. Select **Folder** from the drop-down menu.
3. Enter the directory you want to exclude using the format: *[drive_letter]:\path_to_folder*
4. If you want to exclude all subdirectories within the excluded folder, click the **Subfolders** checkbox.
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 folder in a common location

1. From the **Exclusions** section of a policy configuration page, click **Custom Exclusions**.
2. Select **Folder** from the drop-down menu.

3 Using the ... drop down, select **[PROGRAM_FILES]**.

4 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\

5 If you want to exclude all subdirectories within the excluded folder, click the **Subfolders** checkbox.

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 file type

1 From the **Exclusions** section of a policy configuration page, click **Custom Exclusions**.

2 Select **Extension** from the drop-down menu.

3 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.

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

Configuring Smart Firewall

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
  - five 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.

Using Firewall Rules

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.

Endpoint Protection uses default rules to ensure the proper operation of the service. The default rules also provide essential network functionality and protection from known Internet risks. Examples of default firewall rules include the following:

Default Allow Specific Inbound ICMP	Permit all types of outbound and safe types of inbound ICMP (Internet Control Message Protocol) messaging.
Default Allow Specific Outbound ICMP	ICMP messages provide status and control information.
Default Block EPMAP	The Endpoint Mapper protocol enables one computer to change the configuration of services that are running at another computer.
Default Allow Inbound Bootp	Permit the use of the Bootp service.
Default Allow Outbound Bootp	Bootp is short for Bootstrap Protocol, which enables a computer to discover its own IP address.

The firewall rules that are used in the default Endpoint Protection policy meets the needs of most organizations. 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 Security** to open the default policy.
2. At the top of the Endpoint Security policy configuration page, click **Save a Copy**.
3. Change the **Policy 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**.

Configuring Firewall Rules

A firewall is a barrier protecting a network or, in the case of Smart Firewall, 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 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 of Endpoint Protection 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.

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.

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.

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

- TCP
- UDP
- TCP and UDP
- ICMP
- ICMPv6
- 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 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 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 FW 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 the **>>** button 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 the **>>** button 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 the **>>** button 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 the **>>** button 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 the **>>** button 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.

Using Program Control

The Cloud Endpoint Protection 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, an organization's security policy prohibits it.

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 or 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 Symantec Endpoint Protection account.
2. From the **Computers** page, click the name of the computer you want to scan.
3. From the **Computer Profile** page **Services** tab, locate the **Task** menu and 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.
5. When the first scan is completed, the **Tasks** menu provides options to **View Quarantine** and **View Unresolved Risks**.

To remotely scan a group of computers

1. Log into your Symantec Endpoint Protection account.
2. From the **Computers** page, click a group name in the **Groups** section on the left pane.
3. From the **Computer Group** page, click **Group Scan**.
4. The **Group Scan** dialog box opens. Select **Quick Scan** or **Full System Scan**, and then click **Scan Now**.
5. Confirm your intention to scan a computer remotely by clicking **Scan Now** again.

   The scan runs silently on the remote computers.
6. When the first scan is completed, the **Tasks** menu provides options to **View Quarantine** and **View Unresolved Risks**.

Installing the On-Premises Endpoint Protection

Your license for Symantec Endpoint Protection entitles you to either the Cloud or the on-premises version of Endpoint Protection. The on-premises version of Endpoint Protection offers support for Mac OS X.

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 the **Endpoint Protection**, to retrieve it.

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

3 Under the **Endpoint Protection**, locate and click **Download On-Premise Manager**.

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

Click **Finish**.

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

Chapter 3

Configuring Backup Exec.cloud

This chapter includes the following topics:

Configuring the default group backup policy

Backup Exec.cloud uses policies to backup your servers and users' computers. You must create the policies that you want to apply to your computers. As new computers are added to your Backup Exec.cloud account, the computers are automatically added to the Default Group which uses the default group policy.

Warning: An Administrator must configure the default group policy before it becomes active.

You configure the default group policy on the **Policies** page.

Your organization's backup policy requires careful consideration before implementation. You must evaluate the needs of your organization.

- Do you need to protect the entire computer or do you only need to protect the user's files?
- Do you need to protect the complete server configuration or only the application configuration and the application data?
- Do you need to have different backup strategies for different users in your organization based on their roles?

For your initial deployment of Backup Exec.cloud, we advise that you use the default policy to provide immediate protection for every newly installed server and computer. As time permits, you can allocate computers to appropriate groups with backup policies designed for the requirements of the group.

To configure the default backup policy

1. In the Management Console, click **Policies->Backup Exec.cloud**.
2. In the right pane, click the **Backup Exec.cloud Default Policy**. It is the only policy listed in a new account.
3. In the **Backup Selections & Options** area there are four configuration tags.
   - **Local Volumes**
   - **Applications**
   - **System Components**
   - **Custom Paths**

   You use these tabs to configure your default backup. As you make each new selection, it appears in the **Storage Settings** section if a storage server is configured.

   See "Configuring backups to a storage server" on page 82.
4. The **Local Volumes** tab enables you to back up components common to Windows operating systems.

All Desktop (recommended)	This selection backs up all of the files and folders on the desktop of each Agent computer. It includes these paths: ■ C:\Windows\ServiceProfiles\LocalService\Desktop ■ C:\Windows\ServiceProfiles\NetworkService\Desktop ■ C:\Users\user_name\Desktop

All Documents (recommended)	This selection backs up the My Documents folders on each Agent computer. It includes these paths: ■ C:\Windows\ServiceProfiles\LocalService\Documents ■ C:\Windows\ServiceProfiles\NetworkService\Documents ■ C:\Users\user_name\Documents
All Favorites (recommended)	This selection backs up the Internet Explorer favorites on each Agent computer. It includes these paths: ■ C:\Windows\system32\config\systemprofile\Favorites ■ C:\Windows\ServiceProfiles\LocalService\Favorites ■ C:\Windows\ServiceProfiles\NetworkService\Favorites ■ C:\Users\user_name\Favorites
All Local Fixed Disks	This selection backs up all of the fixed disks that are attached to the Agent computer.
All Mailbox	This selection backs up the Outlook PST and other the data there when the PST is found in its default location. This is the typical path: ■ C:\Users\user_name\AppData\Local\Microsoft\Outlook
System Drive	This selection backs up the disk containing the operating system.

Note: These paths may vary based on the Windows version or the use of customized paths.

5 On the **Applications** tab, you configure the backup of a Microsoft Exchange Server or SQL Server using the checkboxes. In most cases the default settings for the **SQL Backup Options** and **Exchange Backup Options** work well.

6 On the **System Components** tab, individual components of **Service State** maybe selected for backup. The **System State** components are not individually selectable.

7 On the **Custom Paths** tab, you can configure a backup for specific files or for folders that may be stored in common paths across the organization. If you have a standard path for user data on your organization's computers, enter it into the **Custom Paths**.

Backing up **DRIVE_LETTER:\Documents and Settings** for Windows XP endpoints or **DRIVE_LETTER:\Users** for Windows 7 endpoints usually captures the user data on those operating systems.

The Custom Paths path entry box includes macros pointing to well known locations on Windows operating systems.

All Users	This macro points to the Users directory. It includes these paths: ■ C:\Windows\system32\config\systemprofile ■ C:\Windows\ServiceProfiles\LocalService ■ C:\Windows\ServiceProfiles\NetworkService ■ C:\Users\user_name
All Users Application Data	This macro points to the AppData directory each computer user. It includes these paths: ■ C:\Windows\system32\config\systemprofile\AppData ■ C:\Windows\ServiceProfiles\LocalService\AppData ■ C:\Windows\ServiceProfiles\NetworkService\AppData ■ C:\Users\user_name\AppData
All Users Profiles	This macro points to the location where the user profile configuration files are commonly kept. ■ C:\ProgramData
Program Files	This macro points to the Program Files directory on the root of system drive.

Note: These paths may vary based on the Windows version or the use of customized paths.

After selecting a macro for use in a custom path, you may append additional directories or a file name. When you are completed entering the path, click **Add Path** and your path is added to the **Custom Paths** list.

Note: If the specified files or folders do not exist on any endpoint, the custom path is ignored and the backup proceeds.

8 Each backup selection that you make is added to the selection list for backup to a storage server. You may change the default from **onsite & cloud** to **onsite** for data that you want stored locally.

You can activate the check box to enable computers using the policy to backup to the cloud when there is no connection to the storage server. Any data that is backed up to the cloud during an outage, synchronizes with the storage server when it becomes available again.

Note: All data is first backed up to the storage server and then to the cloud if configured. Only when a computer has no storage server assignment is the data automatically backed up only to the cloud.

---

9 Accept the default **Override Settings**. The default settings allow computer-specific modifications to the selections, settings, and throttling parameters that are applied to individual computers within a group. The overrides do not change the group policy itself.

Note: For users to modify the backup policy that is applied to their computer, they must have a login account to the Symantec.cloud Management Console and have Management Console permissions to the Backup Exec.cloud Agent that is running the backup policy that they want to modify.

---

10 In the **Backup Schedule** section, decide if the Backup Exec.cloud Agent should run continuously or to run continuously only on specific days and at specific times. The computers must be on and connected to the Internet to backup files and folders.

Note: Always Running is recommended.

Note: The **Allow the backup agent to complete recovery points even though the scheduled backup time expired** check box allows a backup to resume if interrupted by the schedule. The check box is enabled by default.

---

11 Backup Exec.cloud Agents use network bandwidth as necessary by default. However, **Throttling Parameters** enable you to increase or decrease the bandwidth Backup Exec.cloud Agents may consume under the policy. Consumption may be adjusted from between 32 kilobytes per second and 1000 kilobytes per second (KB/sec). Whenever you control bandwidth consumption, the amount of time required to backup the data on a computer increases. This increase in the time required to back up may be a critical concern when both bandwidth throttling and a custom schedule are used.

Note: Throttling Parameters can be overwritten by users if the Override Settings permit it.

12 Under **Groups**, the **Default Group** is the only group listed and selected by default unless you have created other groups. Click **Save & Apply** to complete the configuration of your default policy.

Note: The default policy is automatically applied to every newly installed Agent running Backup Exec.cloud.

Establishing policies by groups

Backup Exec.cloud can backup your laptops, desktops, and servers based on the needs of your organization. You may need different backup strategies for computers that are used by executives, finance, human resources, and support staff. There may also be different backup schemes for different types of servers. To accomplish this task, you must:

- Make logical groups for your computers.
- Develop backup policies suitable for each group.
  See "Developing backup policies suitable for different groups" on page 59.

To create logical groups for different backup policies

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

2 Click the **Add Group** link beside the **Groups** title on the left pane .

3 Enter a **Name** and **Description** for the group in the screen. Click **Save**.

4 In the header on the right side, click the **Move Computers** link to add computers to the group.

5 In the **Move Computers** screen, filter and then select the computers you want to add to the group. Click **Save**.

This action moves the selected computers out of the **Default Agent Group** (or other assigned group) into your new computer group.

Developing backup policies suitable for different groups

When you complete your needs assessment of the different user groups and server types, you can proceed to configure suitable backup policies. Most small organizations can be adequately served with policies for:

- The computers used for non-critical tasks where recovery of the most recent work files is sufficient.

  Note: Care must be exercised when configuring a backup policy governing all of an organization's deployed computers. Backing up the favorite music, pictures, or other non-essential items of employees may push your account into an overage condition.

- The computers used for mission critical work or sensitive information where a complete system recovery may be required.
- SQL and mail servers where the ability to recover databases is essential.

You may find it necessary to more critically parse the needs of your organization. Establishing groups provides you more flexibility when designing a backup policy for your organization.

To create a backup policy for non-critical desktops and laptops

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

2 Click **Add Policy**.

3 In the **Name** and **Description** portion of the **Policies** page enter a name and description for the policy. For example, **Non-critical desktops and laptops**.

4 In the **Backup Selections & Options** area, use the **Local Volumes** tab to designate the most useful items to back up for your organization's requirements.

All Desktop (recommended)	This selection backs up all of the files and folders on the desktop of each Agent computer. It includes these paths: ■ C:\Windows\ServiceProfiles\LocalService\Desktop ■ C:\Windows\ServiceProfiles\NetworkService\Desktop ■ C:\Users\user_name\Desktop
All Documents (recommended)	This selection backs up the My Documents folders on each Agent computer. It includes these paths: ■ C:\Windows\ServiceProfiles\LocalService\Documents ■ C:\Windows\ServiceProfiles\NetworkService\Documents ■ C:\Users\user_name\Documents
All Favorites (recommended)	This selection backs up the Internet Explorer favorites on each Agent computer. It includes these paths: ■ C:\Windows\system32\config\systemprofile\Favorites ■ C:\Windows\ServiceProfiles\LocalService\Favorites ■ C:\Windows\ServiceProfiles\NetworkService\Favorites ■ C:\Users\user_name\Favorites
All Local Fixed Disks	This selection backs up all of the fixed disks that are attached to the Agent computer.
All Mailbox	This selection backs up the Outlook PST and other the data there when the PST is found in its default location. This is the typical path: ■ C:\Users\user_name\AppData\Local\Microsoft\Outlook
System Drive	This selection backs up the disk containing the operating system.

Note: These paths may vary based on the Windows version or the use of customized paths.

The tabs for **Applications** and **System Components** usually serve no purpose for a non-critical computer. However, in addition to the **Local Volumes** selections, the **Custom Path** tab may be to specify your organization's locations for user files.

5 Each backup selection that you make is added to the selection list for backup to a storage server. You may change the default from **onsite & cloud** to **onsite** for data that you want store locally.

You can activate the check box to enable computers using the policy to backup to the cloud when there is no connection to the storage server. Any data that is backed up to the cloud during an outage, synchronizes with the storage server when it becomes available again.

Note: All data is first backed up to the storage server and then to the cloud if configured. Only when a computer has no storage server assignment is the data automatically backed up only to the cloud.

---

6 In the **Override Settings** section, the default settings permit endpoint users to override portions of your backup policy. However, unless you create Symantec.cloud Management Console user accounts for them and give permissions to the computer that they use, the setting has no effect.

Note: If you choose to set up the user accounts and computer rights for them, your users can create an endpoint-specific backup policy for their computer.

---

7 In the **Backup Schedule** section, you decide if user data should be backed up as it changes or only during certain time periods. The default setting is **Always running**. However, you can specify a custom schedule during which the Backup Exec.cloud Agent is permitted to transmit backups.

Note: A file that changes five times during the day is backed up only once when using a custom schedule. As a result, the four other changes made during the day are not available for restore.

Warning: Computers using a Custom Schedule to back up must be on and connected to the Internet when the Custom Schedule or the backup policy runs. The Custom Schedule must also allow enough run time for an Agent to complete the backup.

Note: The **Allow the backup agent to complete recovery points even though the scheduled backup time expired** check box allows a backup to resume if interrupted by the schedule. The check box is enabled by default.

---

8 Backup Exec.cloud Agents use network bandwidth as necessary by default. **Throttling Parameters** enable you to increase or decrease the bandwidth Backup Exec.cloud Agents may consume under the policy. Consumption may be adjusted from between 32 kilobytes per second and 1000 kilobytes per second (KB/sec). Whenever you control bandwidth consumption, the amount of time required to backup the data on a computer increases. This increase in the time required to back up may be a critical concern when both bandwidth throttling and a custom schedule are used.

Note: Throttling Parameters can be overwritten by users if the Override Settings permit it.

9 In the **Groups** section of the page, assign the policy to govern the appropriate groups.

Click **Save and Apply**.

To create a backup policy for a complete computer restore

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

2 Click **Add Policy**.

3 In the **Name** and **Description** portion of the **Policies** page enter a name and description for the policy.

4 In the **Backup Selections & Options** section, click and select the **Local Volumes**, **Applications**, and **System Components** required for the backup. If the computers governed by this policy do not run SQL server or Microsoft Exchange, you may turn off the **SQL Backup Options** or **Exchange Backup Options**. You may also accept the defaults.

5 Each backup selection that you make is added to the selection list for backup to a storage server. You may change the default from **onsite** to **onsite & cloud** for data that you want protected locally and to the cloud.

You can activate the check box to enable computers using the policy to backup to the cloud when there is no connection to the storage server. Any data that is backed up to the cloud during an outage, synchronizes with the storage server when it becomes available again.

Note: All data is first backed up to the storage server and then to the cloud if configured. Only when a computer has no storage server assignment is the data automatically backed up only to the cloud.

6 In the **Override Settings** section, the default settings enable endpoint users to override the policies of this backup policy. It requires that you create a user account to the Symantec.cloud Management Console for them and then give them rights to the computer that they use.

Note: If you choose to set up the user accounts and computer rights for them, your users can create an endpoint-specific backup policy for their computer.

7 Set a **Backup Schedule** for the computer. Backup is always running, but you can create windows of time during which the agent is permitted to transmit backups. Always running is the preferred configuration.

Warning: Computers using a Custom Schedule to back up must be on and connected to the Internet when the Custom Schedule or the backup policy runs. The Custom Schedule must also allow enough run time for an Agent to complete the backup.

Note: The **Allow the backup agent to complete recovery points even though the scheduled backup time expired** check box allows a backup to resume if interrupted by the schedule. The check box is enabled by default.

8 Backup Exec.cloud Agents can use all of the network bandwidth available by default. However, **Throttling Parameters** enable you to increase or decrease the bandwidth Backup Exec.cloud Agents may consume under the policy. Consumption may be adjusted from between 32 kilobytes per second and 1000 kilobytes per second (KB/sec).

Note: Throttling Parameters can be overwritten by users if the Override Settings permit it.

9 Assign the policy to the appropriate groups in the **Groups** section of the page.

Click **Save and Apply**.

To create a backup policy for an SQL or Exchange server

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

2 Click **Add Policy**.

3 In the **Name** and **Description** portion of the **Policies** page enter a name and description for the policy.

4 In the **Backup Selections & Options** section, click and select the **Local Volumes**, **Applications**, and **System Components** required for your backup.

Local Volumes includes:

- **All Local Fixed Disks**
- **All Profiles Desktop**
- **All Profiles Documents**
- **All Profiles Favorites**
- **All Profiles Mailbox**
- **System Drive**

Application selections include:

- **Exchange Server**
- **SQL Server**

System Components selections include:

- **Service State**
  Dynamic Host Configuration Protocol
  Event Logs
  Network Policy Service
  Remote Storage
  Removable Storage Manager
  Terminal Server Gateway
  Terminal Services Licensing
  Windows Internet Name Service
  Windows Management Instrumentation
- **System State**
  - **Active Directory**
  - **Automated System Recovery**
  - **Certificate Services**
  - **COM+ Reg DB**
  - **Internet Information Services**
  - **Registry**
  - **System Files**
  - **SYSVOL**
  - **Volume Metadata**

Note: Individual components of System State cannot be selected. System State is an all-or-nothing selection.

5 In the **SQL Backup Options** and **Exchange Backup Options**, check the options appropriate for your policy.

See "Understanding Backup Selections & Options" on page 65.

6 Each backup selection that you make is added to the selection list for backup to a storage server. You may change the default from **onsite** to **onsite & cloud** for data that you want protected locally and to the cloud.

You can activate the check box to enable computers using the policy to backup to the cloud when there is no connection to the storage server. Any data that is backed up to the cloud during an outage, synchronizes with the storage server when it becomes available again.

Note: All data is first backed up to the storage server and then to the cloud if configured. Only when a computer has no storage server assignment is the data automatically backed up only to the cloud.

7 In the **Override Settings** section, decide if you want to permit server administrators to be able to override these policy settings. Permitting policy overrides requires that you create a user account to the Symantec.cloud Management Console for them and then give them rights to the servers that they manage. If they use the privilege, it creates an endpoint-specific backup policy for that server.

8 Set a **Backup Schedule** for the server. Accepting the **Always Running** default is recommended.

Assign the policy to the appropriate groups in the **Groups** section of the page.

9 Click **Save and Apply**.

Understanding Backup Selections & Options

The **Backup Selection & Options** section of the policies configuration page enables the creation of policies serving many levels of backup requirements. Using these options, policies can be defined to back up:

- Non-critical user data
- Critical user data
- Servers and databases

Each of these asset-types can be backed up with a policy that conforms to an organization's security policies.

Backup Exec.cloud can fully protect the system and applications on a computer. A full restore from Backup Exec.cloud requires that the following components are selected in the policy:

- **Local Volumes** for profile components and local volume data; specific hard drives can be backed up with the Custom Paths option
- **Applications** that are installed and in use on a server
- **System Components** for all of the services available on the computer
- **Custom Paths** for organizationally-unique paths or local drive backups

Restoring application and system components back to a previous state is only possible on the original computer. Service and System State restore is not currently supported in the case where an entire system is lost or operating system reinstalled. In a system loss scenario, applications can be recovered by a redirected recovery to a flat file and subsequent import from the application. This sort of recovery method also may be used for user data or volume data in general.

Protecting the entire system consumes significant storage space and may not be appropriate for all situations. The full protection policy is most appropriate for mission critical application servers or mission critical user systems. A policy that targets specific data locations is likely more appropriate for typical file servers and user systems.

Each of Backup Selections & Options is described in these tables.

Table 3-1 Local volumes

Component	Description
All Local Fixed Disks	This selection backs up all of the fixed disks that are attached to the Agent computer. **Note:** Using this selection can dramatically increase your storage consumption. This option is important for a backup policy that is used to restore a failed system.
All Profiles Desktop	This selection backs up all of the files and folders on the desktop of each Agent computer. It includes these paths: ■ C:\Windows\ServiceProfiles\LocalService\Desktop ■ C:\Windows\ServiceProfiles\NetworkService\Desktop ■ C:\Users\user_name\Desktop

Table 3-1 Local volumes *(continued)*

Component	Description
All Profiles Documents	This selection backs up the My Documents folders on each Agent computer. It includes these paths: ■ C:\Windows\ServiceProfiles\LocalService\Documents ■ C:\Windows\ServiceProfiles\NetworkService\Documents ■ C:\Users\user_name\Documents
All Profiles Favorites	This selection backs up the Internet Explorer favorites on each Agent computer. It includes these paths: ■ C:\Windows\system32\config\systemprofile\Favorites ■ C:\Windows\ServiceProfiles\LocalService\Favorites ■ C:\Windows\ServiceProfiles\NetworkService\Favorites ■ C:\Users\user_name\Favorites
All Profiles Mailbox	This selection backs up the Outlook PST and other the data there when the PST is found in its default location. This is the typical path: ■ C:\Users\user_name\AppData\Local\Microsoft\Outlook
System Drive	This selection backs up the disk containing the operating system.

Table 3-2 Applications

Component	Description
Exchange Server	Enables backup of Microsoft Exchange Server.
SQL Server	Enables backup of SQL server.

Note: When all application components are selected, the backup agent skips any components that are not installed during the backup.

Table 3-3 System Components

Component	Description
Other Data	Used for data components not easily categorized.

Table 3-3 System Components *(continued)*

Component	Description
Service State	When selected it activates all of the sub-components, however, these components can be backed up individual. Each of these services is independent of the state of other components. **Note:** Selected components are only backed up if they exist on the computer being backed up.
Service State - **Dynamic Host Configuration Protocol**	Enables backup of the DHCP service.
Service State - **Event Logs**	Enables backup of computer event logs. **Note:** Backing up event logs consumes storage. If you do not use the logs for forensics, it may be unnecessary to back them up.
Service State - **Network Policy Service**	Enables backup of the Remote Authentication Dial-In User Service (RADIUS) server and proxy.
Service State - **Remote Storage**	Enables backup of the Remote Storage service configuration.
Service State - **Removable Storage Manager** (RSM)	Enables backup of the RSM service configuration.
Service State - **Terminal Server Gateway** (TS Gateway)	Enables backup of the TS Gateway service.
Service State - **Terminal Services Licensing** (TS Licensing)	Enables backup of the TS Licensing service.
Service State - **Windows Internet Name Service** (WINS)	Enables backup of the WINS service.
Service State - **Windows Management Instrumentation** (WMI)	Enables backup of the WMI service.
System State	When selected it activates all of the sub-components. The sub-components are not individually selectable.

Table 3-3 System Components *(continued)*

Component	Description
System State - **Active Directory**	Active Directory is the directory service used by Windows domain controllers. **Note:** This component is not individually selectable.
System State - **Automated System Recovery**	Automated system recovery facilitates the recovery the Windows operating state in the event of a catastrophic failure. **Note:** This component is not individually selectable.
System State - **Certificate Services**	Windows Certificate Services facilitate an organization's ability to manage its public key infrastructure. **Note:** This component is not individually selectable.
System State - **COM+ Reg DB**	The COM+ Reg DB service provides a registry independent database for storing component registration information. **Note:** This component is not individually selectable.
System State - **Internet Information Services**	IIS is the Microsoft web server application with a number of feature extension modules. It is not turned on, by default, on Windows Servers. **Note:** This component is not individually selectable.
System State - **Registry**	The Registry is the Windows hierarchical database that stores essential configuration information and options on a Windows computer. **Note:** This component is not individually selectable.
System State - **System Files**	This component is not individually selectable. **Note:** This component is not individually selectable.

Table 3-3 System Components *(continued)*

Component	Description
System State - **SYSVOL**	The SYSVOL folder on a Windows server enables replication of file-based data among domain controllers. **Note:** This component is not individually selectable.
System State - **Volume Metadata**	Volume Metadata is comprised of the master file table and the metadata files stored in it. **Note:** This component is not individually selectable.

Note: When all system components are selected, the backup agent skips any components that are not installed during the backup.

Table 3-4 SQL Backup Options

Option	Description
Perform consistency check before backup	Selecting this option performs both a logical and a physical integrity check of all objects in the database before the backup begins. Performing the consistency check is time and resource intensive.
Continue with backup if consistency check fails	Selecting this option begins the backup even if the consistency check fails.
Truncate database transaction logs	Selecting this option truncates the transaction log at each snapshot attempt. This option substantially reduces storage consumption and the time that is required to perform the backup. It also reclaims disk space when the database is restored.

Table 3-5 Exchange Backup Options

Option	Description
Perform consistency check before backup	Selecting this option performs both a logical and a physical integrity check of all objects in the database before the backup begins. Performing the consistency check is time and resource intensive.
Continue with backup if consistency check fails	Selecting this option begins the backup even if the consistency check fails.

Custom Paths enable an administrator to include specific paths in a backup policy. For user computers, backing up **DRIVE_LETTER:\Documents and Settings** for Windows XP or **DRIVE_LETTER:\Users** for Windows 7 endpoints usually captures the user's data. If your organization uses a common path to user files and folders, enter it in **Custom Paths** to back up that data.

Macros may also be used in the configuration of a custom path. The macros are:

Table 3-6 Custom Path Macros

Macro name	Description
All Users	This macro points to the Users directory. It includes these paths: ■ C:\Windows\system32\config\systemprofile ■ C:\Windows\ServiceProfiles\LocalService ■ C:\Windows\ServiceProfiles\NetworkService ■ C:\Users\user_name
All Users Application Data	This macro points to the AppData directory each computer user. It includes these paths: ■ C:\Windows\system32\config\systemprofile\AppData ■ C:\Windows\ServiceProfiles\LocalService\AppData ■ C:\Windows\ServiceProfiles\NetworkService\AppData ■ C:\Users\user_name\AppData
All Users Profiles	This macro points to the location where the user profile configuration files are commonly kept. ■ C:\ProgramData

Table 3-6 Custom Path Macros *(continued)*

Macro name	Description
Program Files	This macro points to the Program Files directory on the root of system drive. **Note:** This macro option expand to include both **Program Files (x86)** and **Program Files** when used on a x64-based system.

Each selection made in your backup configuration is added to the list of backup selections. The selection is set up to backup only to a local storage server. You may change the default from **onsite & cloud** to **onsite** for data that you want to store locally. All data is first backed up to the storage server and then to the cloud if configured. Only when a computer has no storage server assignment is the data automatically backed up only to the cloud. You can activate the check box to enable computers using the policy to backup to the cloud when there is no connection to the storage server.

Using a custom backup schedule

An ill-conceived custom backup schedule can create concerning computer health status conditions and much worse. The typical problem is that a custom backup schedule fails to provide enough time for configured backups to run successfully. This issue is further complicated when computer users turn off their computers at the end of their day.

If your operating conditions demand that you implement a custom backup schedule, keep in mind these points:

- Bandwidth throttling of an Always Running backup schedule may be a better alternative than a custom backup schedule.
- If users turn off their computer at the end of their day, a custom backup schedule may never run.
- Not all computers require every file and every directory to be backed up. Some workplace computers can be safely backed up by selecting only the important files and directories.

A large backup that does not have adequate time to run eventually fails. Please plan your backups accordingly.

Restoring your data

Backup Exec.cloud enables you to restore data from:

- Assigned storage servers
- The Cloud when the assigned storage server is unavailable or the computer is not on the network

When the restore is to a computer on the local network, the restore always downloads from the assigned storage server. When a storage server is unavailable or the computer is not on the local network, the restore data downloads from the cloud.

Note: If the backup configuration was only to the storage server, the data is not available from the cloud.

You have control over what backed-up files you want to restore, and can choose the most recent or the historical versions. Before you restore files, make sure that the files are closed. If files are open, the agent waits until the files are no longer in use before proceeding with the restore.

You can find the data that you need by:

- Searching for files
- Browsing through files and folders

Note: The Resilient File System that is used on Windows 8 and Windows Server 2012 may lose integrity support information on files and folders in a restore. This loss of configuration information requires you to reconfigure the integrity support for those files and folders. However, any file or folder getting its integrity support configuration through inheritance recovers its integrity support information.

Warning: When you restore the System State node you should also restore the Service State components and the volume where Windows is installed. These should all be restored from the same recovery point. If this data is not restored at the same time, the system may become unstable. Service and system state restore is not currently supported in the case where the entire system is lost or the operating system reinstalled.

To restore your data

1. On the **Computers** page, click the name of the computer you want to restore.
2. On the **Computer Proflile** page, in the **Backup Exec.cloud** section, under **Tasks** click **Restore Data**.
3. On the **Configure Restore** page, on the left pane, use the **System to restore** drop-down to pick the correct computer.

   Whenever the data is on a storage server, the name of the storage server appears under the **Assigned Storage Server** display.
4. When you know what you need to restore by name, enter the name into the **Search** box and click the magnifying glass to start the search. Then you add the results to your **Restore Cart**.

   When you do not know the exact file or folder name that you need to restore, use the restore interface to locate the data.
5. Choose a recovery point using the Oldest to Latest recovery point slider.

   Once the slider is engaged, you can use the drop-down selector to pick a specific recovery point. The drop-down displays multiple recovery points on the same date as choices.
6. Locate the data that you need to restore. Click **Files and Folders** and then click **Add Items** on the **Which Files or Folders would you like to restore?** page. Use restore point browse tool to find the data that you need.

   Activate the checkbox(s) next to the data you want to restore. Click **Done**.
7. The **Which Files or Folders would you like to restore?** page opens again. You can either locate and select more data to restore by clicking **Add Items** or continue by clicking **Proceed**.
8. The **Select the data you want to restore** page opens again. The **change selection(s)** link under **Files & Folders** enables you to further modified your restore selections.
9. The **Files & Folders Options** section enables you to **Configure Files & Folders restore options** by clicking the **change** link.

10 On the **Set restore options** page you can configure **File Conflict Rules** and set a **Restore Location**. File Conflict Rules are set to overwrite by default.

Note: The **Restore to a different computer** option can be used to rebuild a computer after a hard drive failure. You must first reinstall the operating system, software, and the Backup Exec.cloud agent. The restore can then be directed to the newly installed agent. However, service and system state restore is not currently supported in the case where the entire system is lost or operating system reinstalled. In a system loss scenario, applications can be recovered by redirected recovery to a flat file and subsequent import from the application.

After you set your restore options, click **Proceed** to continue.

11 The **Transfer Drive Option** now appears on the **Select the data you want to restore** page if you are a Management Console administrator.

When you restore large amounts of data, the restore requires a significant amount of time over the Internet. Transfer drives containing your restore data are delivered to your location in less time than a large restore over the Internet.

Click **order**.

Read the **Confirm Transfer Drive** and click **OK** to confirm your order.

12 Enter the shipping address for your location.

If you have previously ordered a Transfer Drive, the **Select Address** drop-down menu lists your previously used addresses. If this is your first order, you must enter a **Street Address**.

When you complete the form, click **Proceed**.

Warning: Do not remove the Backup Exec.cloud agent from the computer you want to restore. The transfer drive only restores to the Backup Exec.cloud agent that is identified as the **Restore Location** on the **Set restore options** page. If the system to restore is the same as the restore location, the computer name does not need to be specified.

---

13 You can review your restore job by clicking the **view** link in the **Restore Cart** section.

When you are finished, click **Submit Transfer Drive Order**.

14 Click **OK** in the **Submit Job** dialog box to confirm your restore job submission.

Once submitted, you return the **Computer Profile** page which displays the **Transfer drive restore request** order status.

The status is updated as the request is processed.

Enabling a computer user to perform restores

Your computer users cannot restore files to their computers without your intervention. If you want to allow your executives and power-users to perform their own restores, you must:

- Create a user account for them to the Management Console.
- Give them access to their computers.

Making these assignments for key users may save you a considerable amount of time.

Using a transfer drive

Restoring from the Cloud is the preferred way to restore your Backup Exec.cloud data to a computer. You can quickly restore presentations, documents, photos and other small files and folders. However, when you need to restore an Exchange or SQL database or the boss' entire computer, restoring from the Cloud is too slow.

A transfer drive containing a restore of up to two terabytes can be shipped to any of your organization's locations. The external drive plugs into the computer that is specified as the Restore Location during the restore job configuration. The restore begins automatically when plugged into the correct computer. The data on the transfer drive is secured with AES encryption keyed to the Backup Exec.cloud agent running on that specific computer. The encrypted restore data is unreadable by other Symantec.cloud agents.

This strong data security comes at a price:

- You must carefully specify the Restore Location when configuring a transfer drive restore job
- You cannot remove either the Backup Exec.cloud product agent or the Symantec.cloud platform agent from the selected Restore Location computer before performing the restore

As a global security company, Symantec complies with a wide assortment of trade regulations. As a result, your transfer drive order may be delayed for a usually brief trade compliance check. Whenever a longer delay is anticipated, a customer service representative contacts you.

To order a transfer drive

- See "To restore your data" on page 74.

To recover from a hardware failure or lost computer

1. Rebuild the computer by reinstalling the operating system and the appropriate software.

   Note: Restoring application and system components back to a previous state is only possible with the original computer and agent. Service and system state restore is not currently supported in the case where the entire system is lost or operating system reinstalled. In a system loss scenario, recover applications by redirecting the recovery to a flat file and then import from the application.

2. Install the Symantec Backup Exec.cloud agent onto the computer.

   Note: If the computer also had Endpoint Protection running at the time of the loss or failure, it may also be installed.

3. Carefully configure a restore job with the new Backup Exec.cloud agent as the designated Restore Location.
4. When the USB transfer drive arrives, plug it into the computer, the device drivers are loaded by Windows, and the data is automatically restored.

   Note: When using Symantec Endpoint Protection device control, use the Agent Administrator password to disable device control before plugging in the transfer drive.

   See "Overriding USB Device Control on an endpoint" on page 39.

Chapter 4

Onsite Backup

This chapter includes the following topics:

About storage servers

Backup Exec.cloud Onsite Backup enables you to back up data to local network storage servers as well as to the cloud. Three configurations are possible:

- Onsite-only
- Onsite and cloud
- Cloud-only

Note: Agents cannot be assigned to a storage server in this configuration.

Local backups, or on-site backups, are stored on a properly equipped computer called an onsite storage server or simply, storage server.

Two key benefits of using storage servers are:

- Backing up large amounts of data at local network speeds
- Restoring large amounts of data at local network speeds

Symantec.cloud administrators can configure Agents to back up to and restore from:

- An onsite storage server
- Both an onsite storage server and then to the cloud in the synchronization process

Your storage server and the cloud stay in sync when enabled by policy. This synchronization process allows traveling users to back up and retrieve data as necessary using the cloud. And the two-way synchronization ensures that the traveling user's data is available on the storage server when they return to the office.

Note: Data that is backed up as **onsite** rather than **onsite & cloud** is backed up only to the designated storage server. The data is never backed up to the cloud even though references to that local backup data are available within the Management Console. The references are used for reporting and other management functions.

A storage server must meet the following requirements to properly serve all of the Agents assigned to it:

- Windows 7 (32 bit or 64 bit)
- Windows Server 2008 R2 (64 bit only)

The computer or server must have a NTFS-formatted, local fixed drive.

Before installing the storage server agent onto a computer or server, consider:

- Availability of the computer
- Current computer usage or load
- Storage space available on storage server hard drive or the USB attached hard drive

  ---

  Note: The rule of thumb for storage capacity is 2 GB of storage for every 1GB of data protected. The additional storage enables us to keep multiple revisions and storage history for the protected computer. Some backup scenarios may require more storage than suggested by the rule of thumb.

The policies governing storage server use may be set up as:

- Onsite-only
- Onsite and cloud

Note: Your data always goes to the onsite storage server first. The data goes to the cloud during the synchronization process. The cloud data is always a subset of the data on the storage server.

Implementing storage servers makes it possible to restore large data files more rapidly. When backups are both local and cloud, you gain the security of having backups in geographically diverse locations.

Note: Storage servers use the same retention rules as our cloud storage.

Getting started with storage servers

Storage servers are useful for most organizations. With storage servers deployed, you can back up data to a computer on the local network with selected data synchronized to the cloud.

Picking the correct computer for a storage server is an important consideration. The designated storage server needs to have enough disk space to hold the backup data for the protected computers on the local network. The rule of thumb is 2 GB of storage for every 1 GB of backup data. The 2:1 storage ratio includes storage history and multiple revisions. Some backup scenarios may require more storage than suggested by the rule of thumb.

Note: Storage servers use the same retention rules as our cloud storage.

A single, default storage server serves most smaller organizations well, however, you may set up as many storage servers as required. The clear exception to using a single storage server is when your organization has multiple offices that connect over a network of leased lines. In this case, using a storage server at each local office is practical.

When you identify the computers or servers to use as storage servers, log in to your Management Console account:

- Create a new group or groups to serve the varied needs of your organization.

- Download the storage server agent onto your designated storage server or storage servers.
- Configure your storage server.
  See "Configuring and managing storage servers" on page 85.

Note: When a storage server is the storage default of an organization, all new endpoint Agents are automatically assigned to the storage server without manual intervention. When your organization has multiple, geographically-diverse locations, a single, default storage server may not be an appropriate configuration. The default parameter is found and may be disabled or enabled within the **Server Settings** portion of the **Configure Storage** page for the storage server.

- Create a backup policy or backup policies that are well-suited to the needs of your various groups.
- Install the Backup Exec.cloud Agent onto your computers using the **Choose Your Group** option.
- Manually point any existing Backup Exec.cloud Agents to the storage server using the **Configure Backup**->**Storage Settings** option.

Following this order minimizes the amount of manual work that is required to begin using Onsite Backup.

To create an onsite storage server:

1. From the **Actions** section of the **Computers** page, click **Add New Computer(s)**.
2. On the **Add New Computer or Service** page, in **Select Your Services** section, click **Select** for the Backup Exec.cloud Agent.
3. Within the Backup Exec.cloud Agent box, click **Storage Options** and activate the option that you want:
   - **Backup Agent**
   - **Storage Agent**
   - **Both Agents**

Note: A storage server may also back up itself, so you may select both of the Agents for installation for the download.

---

4 In **Choose Your Group**, use the drop-down to select a group and the new Agent(s) are installed into the selected group.

Note: A group may be used to collectively assign computers to a storage server using the **Update Assigned Computers** operation of **Configure Storage** page.

5 In **Download Your Installer**, decide if you want to install the Agent onto:

An individual computer, **Install Now**

Do a large-scale deployment using a redistributable package, **Download**

Specify computers by invitation, **Send Email Invites**

6 Click the appropriate button to begin.

Configuring backups to a storage server

Storage server assignments are managed from the **Configure Storage** page of a storage server. Smaller organizations may choose a basic storage server setup that assigns all protected computers to the designated, default storage server. However, there may be multiple storage servers with assigned computers or computers with no storage server assignment. The different approaches to storage server deployment present three cases:

- Computers that are assigned to a single, default storage server
- Computers that are assigned to storage servers based on an organization's needs
- Computers with no storage server assignment

The storage server assignment determines where backup data is physically stored on a local network. Backup policies designate the data that goes to the storage server, the cloud, or both except for computers without a storage server assignment. Computers without a storage server assignment always backup to the cloud.

When you configure a new backup policy, you select the data to backup and then specify each selection as either **onsite** or **onsite & cloud**. You may also enable computers using the policy to backup to the cloud when there is no connection to the storage server. Any data that is backed up to the cloud during an outage, synchronizes with the storage server when it becomes available again.

Note: All data is first backed up to the storage server and then to the cloud if configured. Only when a computer has no storage server assignment is the data automatically backed up only to the cloud.

Assigning backup agents to a storage server

Using a default storage server is the recommended solution for most smaller organizations. Backup Agents are automatically assigned to the default storage server when one exists. This approach directs backups to a computer on a local network which synchronizes selected data with the cloud.

When organizations need to segregate backup data, the computers must be assigned to storage servers. This segregation of data is accomplished using groups. The group is then assigned to the correct storage server within the **Server Settings** on the **Configure Storage** page. Individual computers may be assigned within the **Server Settings** or by using the **Storage Settings** in the **Configure Backup** wizard.

To manually assign a computer to a storage server from the Configure Storage page

1. Click the **Computers** tab. Locate the storage server to use for the assignment. Click the **Storage** link of the storage server. The **Configure Storage** page appears.
2. On the **Configure Storage** page, open the **Assigned Computers** option and click **Update Assigned Computers**.
3. Use the **Select Computers** interface to locate groups or individual computers to assign to the storage server.
4. Activate the check box to assign the computer to the storage server and click **Done**.
5. Click **Submit Storage Settings** to update the storage server configuration.

Configuring computers without a storage server

Your organization may use one backup policy per department, however, some computers using the policy may need to backup only to the cloud. This objective is accomplished by disassociating those computers from the storage server manually.

To manually disassociate a computer from a storage server

1. Click the **Computers** tab. Locate the storage server currently associated with the computer. Click the **Storage** link of the storage server. The **Configure Storage** page appears.
2. On the **Configure Storage** page, click **Assigned Computers** then **Update Assigned Computers**.

   Locate the computer and uncheck the check box to remove the computer from the list.

   Note: If the computer is listed as part of a group, you must delete it from the group.

3. Click **Done** and then **Update Storage Settings** to update the storage server configuration.

Using Onsite Backup with mobile users

The way that you manage users who take their laptops home every night may be different from managing your truly mobile users. You can design backup policies to:

- Backup data only to the assigned onsite storage server
- Backup data to the assigned onsite storage server and to the cloud
- Back up only to the cloud

  Note: This configuration is only for computers with no storage server assignment.

Each backup selection may be configured as **onsite** or as **onsite & cloud**:

- The **onsite** only configuration always backs up only to the storage server
- The **onsite & cloud** configuration backs up data to both the storage server and to the cloud

The **Enable backup directly to the cloud when disconnected from an Onsite Storage Server** check box enables roaming for the **onsite & cloud** configuration of mobile users. The check box is enabled by default. Symantec recommends keeping the default. The feature is intended for use in advanced configurations.

Note: Disabling the check box disables roaming for mobile users who are assigned to a storage server. The setting does not affect cloud-only users.

With an **onsite & cloud** configuration, the data goes first to the storage server and is then synchronized to the cloud. When mobile, a laptop with that configuration, backups to the cloud which synchronizes with its storage server. On returning to the office network, any onsite-only data that was not backed up while mobile, is backed up to the assigned storage server.

This configuration works well for occasional mobile users. Due care in identifying **onsite** and **onsite & cloud** data in the backup policy design, provides occasional mobile users access to their important data while mobile. Occasional mobile users retrieve data from the cloud, unless they connect to the company network. Restore speeds over a VPN connection are slower than a restore over an office network.

For users who frequently travel, a storage server assignment may not be necessary. The more frequently the user travels, the less necessary a storage server assignment is for them. Without a storage server assignment, their data is always backed up to the cloud; and is always available to them from the cloud, anywhere.

Configuring and managing storage servers

You may have as many Onsite Backup storage servers as you need. However, you are encouraged to develop a sensible plan for storage server deployment. The plan might center around geographic locations, organizational groups, or other criteria, but you should have a plan.

You need to monitor storage consumption on your storage servers. The Management Console provides a number of monitoring mechanisms:

- **Home** page widgets to display computer health
- News Alerts on your **Home** page
- Service-specific computer health indicators

See “Changing the storage location of your storage server ” on page 89.

To configure an onsite storage server:

1. From any page click **Computers** and then click the **Storage** link under the computer name of the storage server. The **Configure Storage** page opens.
2. Click **Storage Location**, enter the directory path to the storage repository on the storage server.

   Note: There must be adequate storage available in the storage location. The rule of thumb is 2 GB of storage for every 1 GB of data. This rule of thumb is subject to wild variations based on the environment. The additional backup capacity is used for multiple revisions and history of your backups.

   Clicking the arrow icon next to the identified disk enables you to browse to a specific location.

   Clicking the **folder+** icon enables you to create a new directory.

3 **Server Settings** provide these configuration options:

Default Storage Server	The **Off-On** button designates a storage server as the default storage server. There can be only one default storage server in an organization. All new computers backup to the default storage server unless manually assigned to other storage servers.
Network Port	This number indicates the port number computers use to communicate with the storage server. The default port number is 22501. **Note:** Symantec recommends that you use the default port number unless there is a conflict with other services offered on your network.
Throttling	Provides control over the bandwidth consumption of the storage server. The throttling value controls transmission of data from the storage server to your organization's account. Symantec recommends that you accept the default setting of **Use all available bandwidth**. If you decide that you must use throttling, activate the **Specify a maximum bandwidth** option. Then use the slider to designate the maximum amount of data the storage server can transmit per second. The slider ranges from 32 KB/sec to 2000 KB/sec.

4 The **Alerts** option enables you to set thresholds for alerts concerning the amount of free space available on the storage server.

Storage Free Space Warning	The **Storage Free Space Warning** value sets the number of free gigabytes required to avoid a warning condition. The default value is 10 GB, the minimum setting is 5GB. When there is less space the computer health indicator becomes yellow. **Note:** The **Storage Free Space Warning** value must always be larger than the **Storage Free Space Error** value.
Storage Free Space Error	The **Storage Free Space Error** value sets the number of free gigabytes required to avoid an error condition. The default value is 5 GB, the minimum setting is 1 GB. When there is less space the computer health indicator becomes red and the storage server begins to reject new backups. When backup rejection occurs, the new backup data goes directly to the cloud if enabled by policy. **Note:** The **Storage Free Space Error** value must always be less than the **Storage Free Space Warning** value.

5 Click **Assigned Computers** to add or remove computers from the storage server assignments.

Clicking the **Update Assigned Computers** button enables you to assign a group, groups, or computers within a group to a storage server for backup.

6 When you finish, click **Update Storage Settings** to complete the configuration.

To set up the computer health indicators for storage servers

1. From any page, click **Computers** to go to the **Computers** page.
2. Locate your storage server and click **Storage** to go to the **Configure Storage** page.
3. Click **Alerts**. Adjust the **Storage Free Space Warning** and the **Storage Free Space Error** values to meet your requirements.

   The **Storage Free Space Warning** turns the computer health indicator yellow when the hard drive has less space than specified in GB.

   The **Storage Free Space Error** turns the computer health indicator for the storage server red when the hard drive has less space than specified in GB.

Note: A computer's health color represents the value of the worst status reported by either the Backup Agent or the Storage Agent.

Changing the storage location of your storage server

In the event that you need to change the storage location of your storage server, you begin by assessing your storage needs. Then verify that your new storage location has adequate storage. A reasonable guideline for storage capacity is 2 GB for every 1 GB that you expect to backup. This guideline covers typical needs; your needs may require more capacity. When you are satisfied with your assessment, carefully follow the procedure.

See "Configuring and managing storage servers" on page 85.

To change the storage location of your storage server

1. Carefully review these instructions before changing the storage location for your storage server.

   When you are finished reviewing the procedure, return to your **Configure Storage** page browser window. If you are not already in your Management Console account, log into your account and open the storage server **Configure Storage** page. The page is accessed from the storage server **Computer Profile** page.
2. Change the current **Storage Location** path to the new storage location on the storage server and click **Submit Storage Settings**.
3. Wait for the Storage Agent to display the error: **The current storage server path is invalid or unreachable.**

4. From the storage server that you need to change, click **Start**->**All Programs**->**Accessories** then right-click **command prompt** and **Run as administrator** to open a command prompt window.
5. Stop the Storage Agent service by typing: **sc stop SymcStorageAgentSvc**
6. Confirm that the Storage Agent service did stop by typing: **sc query SymcStorageAgentSvc**
7. In Windows Explorer, locate the current storage path and the location of the new storage path. Use bautil.exe to copy the data in the current storage location into the new storage location.
   - Change your current working directory to: "DRIVE_LETTER:\Program Files\Symantec.cloud\StorageAgent"
   - Then use the command:

     ```
     bautil.exe -copy "SourceFolder" -d "DestinationFolder"
     ```

     Note: Before using the bautil.exe command, please verify that the service is stopped as described in step 5 and step 6.
8. Using Windows Explorer, locate and open the file **.sapodconfig.txt** on the storage server. This file is usually found here: **%PROGRAMFILE%\Symantec.cloud\StorageAgent\.state\servicepod**
9. Change the value of **StorageLocation** to the path of the new storage location by following this example:

   StorageLocation=OLD_DRIVE_LETTER:\old_storage_directory_name\.localstorageroot

   To the new location:

   StorageLocation=NEW_DRIVE_LETTER:\ new_storage_directory_name\.localstorageroot

   .localstorageroot must follow the trailing backslash without a space.

   Save and close the file.
10. Restart the Storage Agent service from the command prompt by typing: **sc start SymcStorageAgentSvc**
11. Confirm that the Storage Agent service did start by typing: **sc query SymcStorageAgentSvc**

Restoring your data from a storage server

When your network uses storage servers, all restores download from the assigned storage server. When a storage server is not available or when an endpoint user is not on the network, the restore comes from the cloud.

Note: If the backup configuration was only to the storage server, the data is not available from the cloud.

A restore from a storage server is the same as a restore from the cloud, except that a local network restore is much faster.

You can find the data that you need by:

- Searching for files
- Browsing through files and folders

See "Restoring your data" on page 73.

Your roaming users do not have rights to restore data to their computer. Providing them the needed access may simplify your user support.

See "Enabling a computer user to perform restores" on page 76.

Chapter 5

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 Symantec.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 four 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 do 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

Knowledge of your network topology and network utilization are important to developing a local update host deployment strategy. The question that you must answer is: Should local update hosts be deployed per local network or per network segment?

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.

Configuring a local update host

Within the **Computers** page of the Symantec.cloud Management Console, you designate the computers best suited for the role of local update hosts. You designate local update hosts on the Profile page of the selected computers. 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 Symantec.cloud. When a worker's laptop goes on the road, the agent fails over to Symantec.cloud when it cannot find its local update host.

The Local Update Service is designed to reduce network and Internet bandwidth consumption without the complexity usually associated with caching proxy configurations.

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

To designate a computer to be a local update host

1. From any page, click the **Computers** tab.
2. 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.

Managing a local update host

You manage local update hosts from the **Computer Profile** page of the local update host that requires attention. In the absence of a System Policy assigning local update hosts to groups, the Local Update Service is dynamically configured. From the **Computer Profile** page of a designated host, you can:

- View the computers that are assigned to a local update host.
- Disable a local update host.

Global System Policies can be administered from the Management Console **Policies** page.

See "Using Global policies" on page 99.

To view the computers assigned to a local update host

1. From any page, click the **Computers** page.
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. From any page, click the **Computers** page.
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 Symantec.cloud, the computers either resume getting updates from the cloud or are assigned to a new local update host on their network.

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.

Chapter 6

Managing your computers

This chapter includes the following topics:

Performing Group Actions

The **Perform Group Actions** option on the **Computers** page enables an administrator to run scans and trigger LiveUpdate simultaneously. The administrator can run a **Quick Scan** or a **Full Scan** as well as **Run LiveUpdate** on any or all of an organization's groups.

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.

To Perform Group Actions

1. Log into your Symantec.cloud account.
2. On the **Computers** page, on the left pane, under **Quick Tasks**, click **Perform Group Actions**.
3. In the **Group Action** pop-up, select the groups you want the actions to apply to.
4. In the **Group Scan** area, select **Quick Scan** or **Full Scan**.
5. If you want the endpoints to check for the latest virus definitions, check **Run LiveUpdate**.

6 Click **Perform Action**.

7 Symantec.cloud then dispatches the action to all of the endpoints that are connected when the action is performed. The **Group Action Dispatch Completed!** dialog summarizes the success of the dispatched action.

Using Global policies

Global policies are assigned to groups in addition to the already assigned service policies. The policies can be used to:

- Configure proxy settings.
- Assign local update hosts.
- Set a Live Update Schedule

A global policy can simplify proxy settings and local update host assignments for organizations with several offices.

- Proxy settings that are assigned through the local Agent, override global proxy settings.
  See "Using the local Agent's proxy settings" on page 102.
- In the absence of globally-assigned, local update hosts, Agents still discover a local update host.
  See "Configuring a local update host" on page 94.

The global policy for scheduling Live Updates 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 Live Update Schedule does not affect delivery of virus definitions.

To configure a global System Policy

1 From any page in the Management Console, click **Policies**. 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 **Policy Name** and **Description** to document the purpose of your System Policy.

4 You can now configure proxy settings and assign local update hosts.

See "Using the local Agent's proxy settings" on page 102.

See "Configuring a local update host" on page 94.

See "To configure a Live Update Schedule" on page 102.

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 **Proxy Username** and **Proxy 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. There are three options:

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 the **Add All** button.

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 Live Update Schedule

1 Carefully consider which scheduling option best serves your needs.

Anytime	This 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	Weeknds are defined as Saturday and Sunday.
Disable	This setting is automatically overridden after a software update is more than 30 days old.

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

2 Under **Live Update Schedule** choose the correct option for Live Update 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.

Using the local Agent's proxy settings

You can configure proxy settings on the local Agent. 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 Protection

Agents. Fortunately, the Protection Agent interface can override an errant configuration, but the correction requires manual intervention.

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

1. Double-click the **Symantec.cloud** icon in the system tray.
2. When the user interface opens, click **Settings** button 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 **Proxy Username** and **Proxy 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. To create an alert for yourself, hover over the email address associated with your account and click the **My Profile** link.

   To create an alert for another user, click the **Users** tab 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.

The **Add a new rule** dialog box appears.

4 In the **Rule Name** box, enter a useful name for the alert rule.

5 Select at least one of these settings:

Service	Select from your subscribed services
Category	Endpoint Protection: ■ **General** ■ **Detected Risks** Backup Exec.cloud: ■ **Backup** ■ **Restore** ■ **General** ■ **Storage**
Severity	■ **Informational+** Informational+ delivers informational, warning, and error messages. ■ **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 the **Save** button.

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

Chapter 7

Finding help

This chapter includes the following topics:

- Getting help with Symantec.cloud

Getting help with Symantec.cloud

Symantec.cloud provides a number of resources for customers to get help with:

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

Table 7-1 User assistance resources

Resource type	Resource location
Online user assistance	■ Online Help ■ FAQ ■ Getting Started Guide ■ Administrator's Guide ■ How-to videos
Management Console tools	
Technical support	■ US/Canada: +1 (866) 807 6047 ■ EMEA: +44 (0) 870 850 3014 ■ Australia: 1 (800) 088099 ■ Hong Kong: 1 (800) 901220 ■ Asia Pacific: +852 6902 1130 ■ Email: Support.Cloud@symantec.com

Table 7-1 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.