

WEBROOT[®]
Secure*Anywhere*[™]

**Endpoint Protection
Administrator Guide**

Copyright

Endpoint Protection Administrator Guide

June, 2013

© 2012 - 2013 Webroot, Inc. All rights reserved. Webroot is a registered trademark and SecureAnywhere is a trademark of Webroot, Inc. All other product and company names mentioned may be trademarks or registered trademarks of their respective owners.

Table of Contents

Chapter 1: Getting Started	5
Preparing for setup	7
Overview of configuration steps	7
System requirements	8
Creating a Webroot account	9
Logging in and using the Setup Wizard	12
Logging in for the first time	12
Selecting a default policy during configuration	13
Selecting a deployment method and performing a test install	15
Using the Management Portal	19
Using the main tabs	21
Opening the Endpoint Protection Menu	22
Opening and collapsing panels	23
Exporting data to a spreadsheet	24
Opening video tutorials	24
Opening the Help files	24
Accessing product information	25
Sorting data in tables and reports	26
Chapter 2: Managing User Accounts	29
Editing your own account settings	30
Managing portal users	33
Creating new portal users	33
Editing user information	36
Setting permissions for portal users	38
Adding keycodes to your account	42
Adding consoles to your account	44
Adding a console	44
Renaming a console	46
Switching consoles	46
Renewing or upgrading your account	47
Chapter 3: Managing Endpoints	49
Deploying SecureAnywhere to endpoints	50

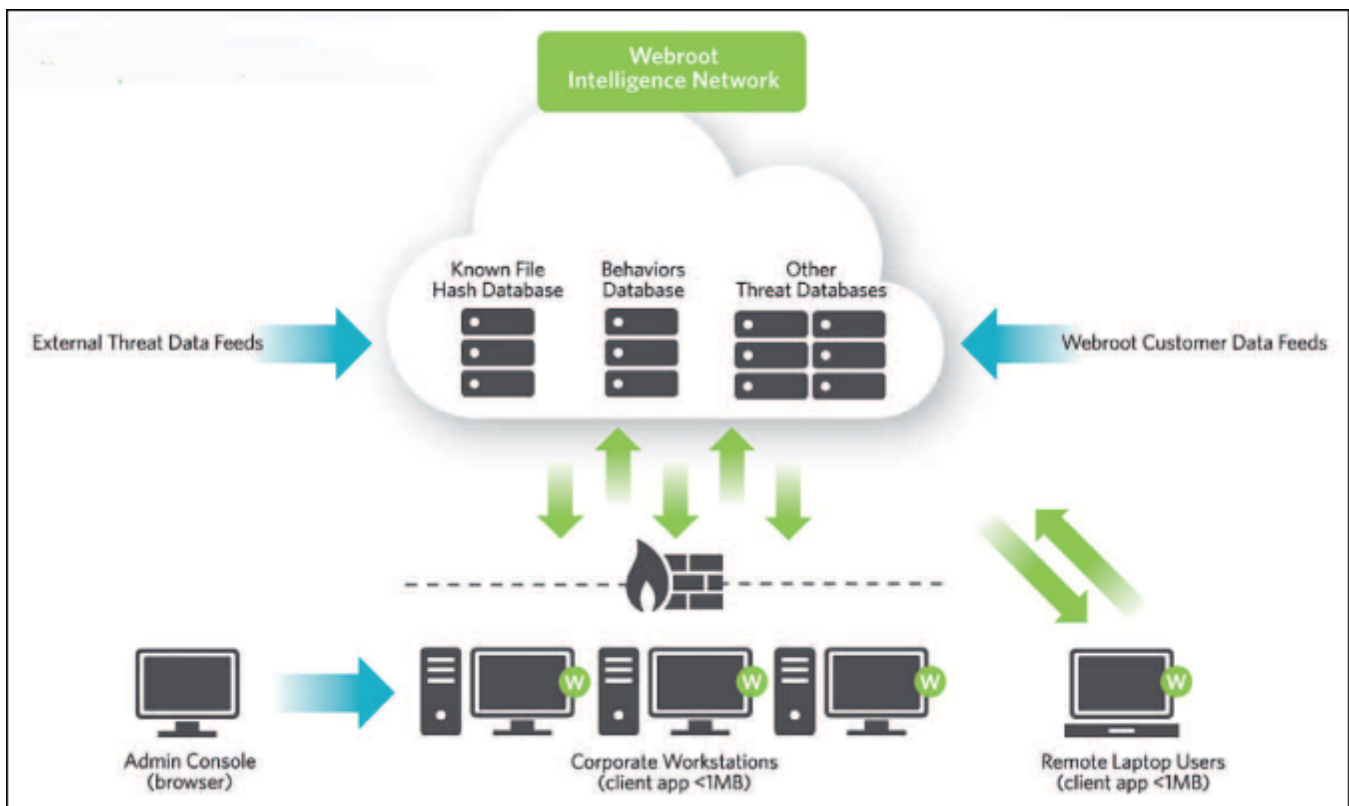
Using the SecureAnywhere installer	52
Using MSI for deployment	57
Using GPO for deployment	58
Changing an endpoint keycode	59
Renaming endpoints	61
Searching for endpoints	62
Issuing commands to endpoints	63
Checking scan results and managing threats	69
Viewing the scan history	69
Restoring a file from quarantine	70
Setting an override for the file	71
Deactivating endpoints	73
Deactivating an endpoint	73
Reinstalling SecureAnywhere on the endpoint	74
Managing endpoint upgrades and other changes	75
Migrating to a new operating system	75
Changing hardware on an endpoint	75
Moving endpoints to a new subnet	75
Forcing immediate updates (forced polling)	76
Using SecureAnywhere on the endpoint	77
Uninstalling SecureAnywhere	79
Chapter 4: Checking Status	81
Viewing endpoint status	82
Viewing recent threat status	84
Viewing an agent version overview	85
Chapter 5: Managing Policies	87
Implementing policies	88
Selecting a new default policy	89
Creating policies	90
Creating a new policy	90
Copying a policy	91
Changing policy settings	92
Basic Configuration	95
Scan Schedule	97

Scan Settings	98
Self Protection	99
Heuristics	100
Realtime Shield	103
Behavior Shield	104
Core System Shield	105
Web Threat Shield	106
Identity Shield	107
Firewall	108
User Interface	109
System Cleaner	109
Renaming a policy	114
Exporting policy settings to a spreadsheet	115
Deleting policies	116
Viewing endpoints assigned to a policy	117
Moving endpoints to another policy	118
Chapter 6: Managing Groups	119
Organizing endpoints into groups	120
Adding a new group	122
Applying a policy to endpoint groups	124
Applying a policy to a group	124
Applying a policy to a single endpoint	125
Moving endpoints to another group	127
Deleting groups	128
Renaming groups	129
Chapter 7: Viewing Reports	131
Generating Endpoint Protection reports	132
Generating the Agent Version Spread report	134
Generating the Agents Installed report	137
Generating the All Threats Seen report	139
Generating the All Undetermined Software Seen report	141
Generating the Endpoints with Threats on Last Scan report	143
Generating the Endpoints with Undetermined Software on Last Scan report	146
Generating the Threat History (Collated) report	148

Generating the Threat History (Daily) report	152
Chapter 8: Managing Alerts	155
Implementing alerts	156
Creating a distribution list	157
Creating customized alerts	158
Viewing your defined alert messages	162
Suspending or deleting alerts	164
Chapter 9: Using Overrides	165
Implementing overrides	166
Applying overrides from the Overrides tab	167
Applying overrides to files from groups	170
Applying overrides to files from reports	172
Viewing overrides	174
Deleting overrides	176
Exporting overrides to a spreadsheet	177
Chapter 10: Viewing Logs	179
Viewing the Change Log	180
Viewing the Command Log	182
Glossary	183
Index	187

Chapter 1: Getting Started

Webroot® SecureAnywhere™ Endpoint Protection secures your enterprise from malware and other threats by combining Webroot's behavior recognition technology with cloud computing. Endpoint Protection includes a Management Portal (also called an *Admin Console*), which is a centralized website used to view and manage your endpoints. (An *endpoint* can be any Windows corporate workstation, such as a PC, laptop, server, or virtual server.) You can deploy SecureAnywhere software to these endpoints within seconds, protecting users immediately. Once SecureAnywhere runs a scan on the endpoints, it reports their status into the Management Portal.



This user guide describes how administrators can deploy SecureAnywhere and use the Management Portal to view threat alerts, data charts, and other information about endpoint activity. The tasks you can perform depend on your access permissions and what mode of management you select during Endpoint Configuration. This guide is intended for *administrators* who are using Endpoint Protection with full access permissions.

Note: For an online version of this guide, go to:
http://www.webroot.com/En_US/SecureAnywhere/SME/EndpointProtection.htm.

To begin using Endpoint Protection, see the following topics:

Preparing for setup	7
Overview of configuration steps	7
System requirements	8
Creating a Webroot account	9
Logging in and using the Setup Wizard	12
Logging in for the first time	12
Selecting a default policy during configuration	13
Selecting a deployment method and performing a test install	15
Using the Management Portal	19
Using the main tabs	21
Opening the Endpoint Protection Menu	22
Opening and collapsing panels	23
Exporting data to a spreadsheet	24
Opening video tutorials	24
Opening the Help files	24
Accessing product information	25
Sorting data in tables and reports	26

Preparing for setup

Before you begin, review the configuration steps in this section and make sure your environment meets the system requirements.

Note: These configuration steps are intended for the Endpoint Protection administrator who has full access permissions.

Overview of configuration steps

1. Create an account using your keycode. You should have received the keycode in an email from Webroot. See "Creating a Webroot account" on page 9.
2. Log in to the Management Portal and open the Setup Wizard. In the wizard, you must select a default policy for SecureAnywhere installations on endpoints. (An *endpoint* can be any Windows corporate workstation, such as a PC, laptop, server, or virtual server. A *policy* defines the SecureAnywhere settings, including how the program scans for threats and manages detected items.) After you select a policy, a Welcome panel opens and provides information about how to deploy SecureAnywhere to endpoints. See "Logging in and using the Setup Wizard" on page 12.
3. *Optional.* Edit your account settings for the Management Portal, including your contact number and a time zone where you are located. See "Editing your own account settings" on page 30. You can also create logins for other administrators to access the Management Portal. See "Managing portal users" on page 33.
4. Deploy the SecureAnywhere software to the endpoints. See "Deploying SecureAnywhere to endpoints" on page 50.
5. Determine if the default policy is sufficient for your business needs. If desired, add new policies with different settings as described in "Implementing policies" on page 88. (You cannot change the Webroot default policies.) You may also need to create overrides for certain files that you consider legitimate applications. See "Applying overrides from the Overrides tab" on page 167.
6. Determine if you need to create separate groups of endpoints for different management purposes. When you deploy SecureAnywhere to your endpoints, Endpoint Protection places them all in one Default group. If desired, you can create new groups and assign them to new policies. See "Organizing endpoints into groups" on page 120.
7. *Optional.* Customize alert messages that will be sent to a distribution list whenever endpoints report an infection or whenever SecureAnywhere is installed on new endpoints. See "Implementing alerts" on page 156.

System requirements

You can use Endpoint Protection with the following browsers and server platforms.

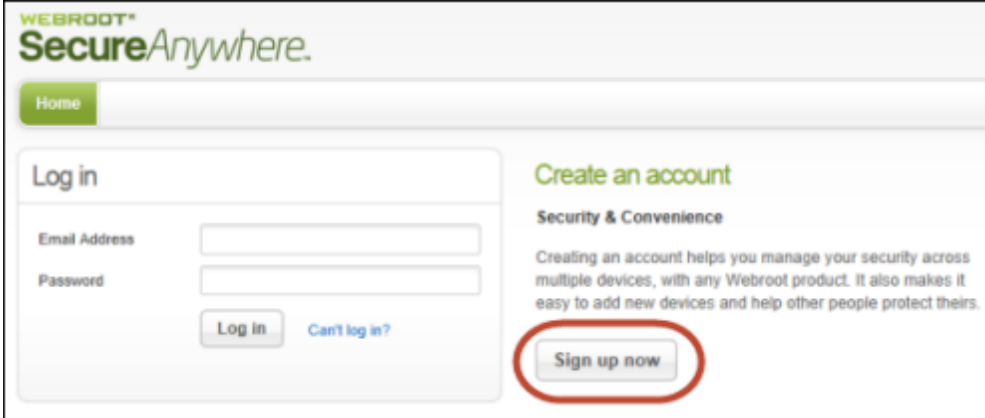
Browsers and platforms	
Browsers	Internet Explorer: versions 8, 9, and 10 Firefox: the latest 5 versions Chrome: the latest 5 versions Safari: versions 5.0 and above
Server platforms	Windows Server 2003 Standard, Enterprise, 32- and 64-bit Windows Server 2008 R2 Foundation, Standard, Enterprise Windows Small Business Server 2008 and 2011
Virtual server platform	VM Workstation 6.5, 7.0 Citrix XenDesktop 5 and XenServer 5.0, 5.5, 5.6
Endpoint requirements for PCs and laptops	Operating systems: Windows XP 32- and 64-bit SP2, SP3 Windows Vista 32-bit (all editions), Windows Vista SP1, SP2 32- and 64-bit (all editions) Windows 7 32- and 64-bit (all editions) Windows 7 SP1 32- and 64-bit (all editions) Processor: Intel Pentium/Celeron family AMD K6/Athlon/Duron family Other compatible processor with those listed above Memory: 128 MB RAM (minimum) Browsers: Internet Explorer: versions 8, 9, and 10 Firefox: the latest 5 versions Chrome: the latest 5 versions Safari: versions 5.0 and above Opera: the latest 5 versions

Creating a Webroot account

Before you can log in to Endpoint Protection, you must create an account using your license keycode. You should have received the keycode in an email sent from Webroot.

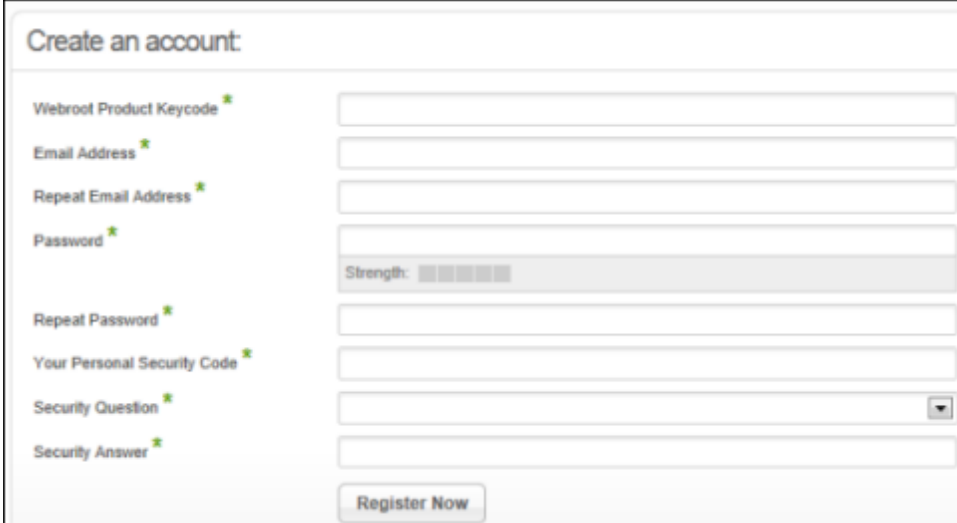
To create an account:

1. Go to the SecureAnywhere website: <https://my.webrootanywhere.com>.
2. In the **Log in** panel, click **Sign up now**.



The screenshot shows the Webroot SecureAnywhere login page. On the left, there is a 'Log in' section with input fields for 'Email Address' and 'Password', and buttons for 'Log in' and 'Can't log in?'. On the right, there is a 'Create an account' section with the heading 'Security & Convenience' and a paragraph of text. A red circle highlights the 'Sign up now' button.

The registration page opens.



The screenshot shows the 'Create an account' registration page. It features several input fields: 'Webroot Product Keycode', 'Email Address', 'Repeat Email Address', 'Password', 'Repeat Password', 'Your Personal Security Code', 'Security Question' (with a dropdown arrow), and 'Security Answer'. A 'Register Now' button is located at the bottom right. A password strength indicator is visible below the password field.

3. Complete the following information:

Account registration	
Webroot Product Keycode	Enter the license keycode you received when you purchased Endpoint Protection.
Email Address	Enter the email address for the administrator who will manage Endpoint Protection. The account activation confirmation is sent to this email address, which is also the username for logging in to the Management Portal.
Password	Enter a minimum of 9 characters. Your password must contain at least 6 alphabetic characters and 3 numeric characters. Your password can be longer than the required 9 characters. It can include special characters, except for the angle brackets: <>. Your password is case sensitive. As you type, the Strength meter shows how secure your password is. For optimum security, it's a good idea to make your password as strong as possible.
Your Personal Security Code	Enter a word or number, which will be used for an extra security step after you enter the password during login. Choose a code that is easy to remember, using a minimum of 6 characters. Every time you log in, the Management Portal prompts you to enter two random characters of this code. For example, if your code is 123456 and it prompts you for the fourth and sixth character, you would enter 4 and 6 . Your Personal Security Code is case sensitive.
Security Question	Choose a question from the drop-down list. If you forget details of your login later, you will need to provide the answer to this question to retrieve the information.
Security Answer	Type an answer to your security question. The Security Answer is case-sensitive.

4. Click **Register Now**.

Endpoint Protection verifies the keycode you entered, and then displays a License Agreement at the bottom of the panel as shown in the following example.

WEBROOT®
SecureAnywhere.

Home

Create an account:

Webroot Product Keycode *

Email Address *

Repeat Email Address *

Password *
Strength: Strong

Repeat Password *

Your Personal Security Code *

Security Question *

Security Answer *

I have read through and agree to the terms of the [Webroot SecureAnywhere Business Solution Agreement](#)

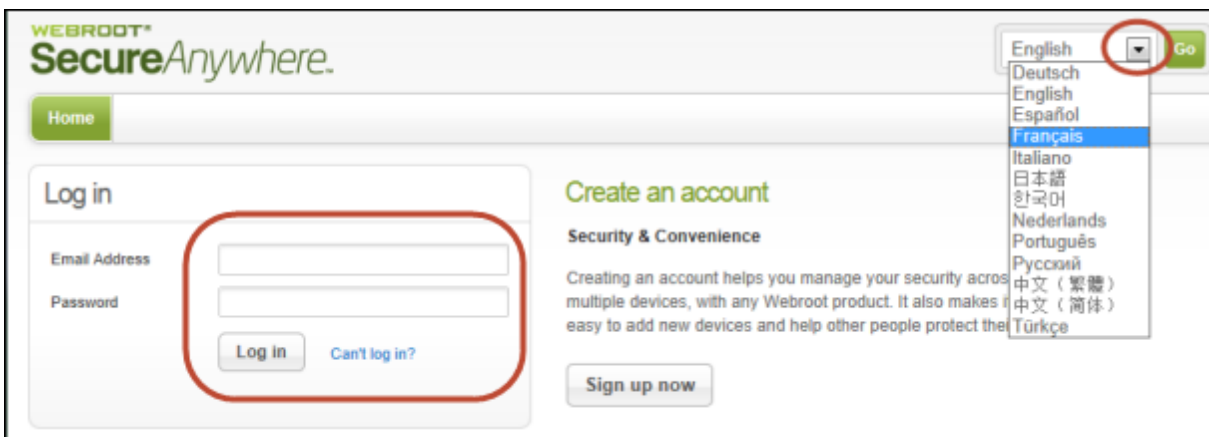
5. Click the link to read the agreement. When you're done, click the checkbox to accept the agreement and click **Register Now** again.
Webroot sends a confirmation message to the email address you specified.
6. Open your email application and click the link in the confirmation email message.
7. When the **Confirm Registration** page opens, enter the two randomly selected characters of the security code you specified when you created the account. Click **Confirm Registration Now**.
You can now log in to the Management Portal to begin configuring Endpoint Protection. See "Logging in and using the Setup Wizard" on page 12.

Logging in and using the Setup Wizard

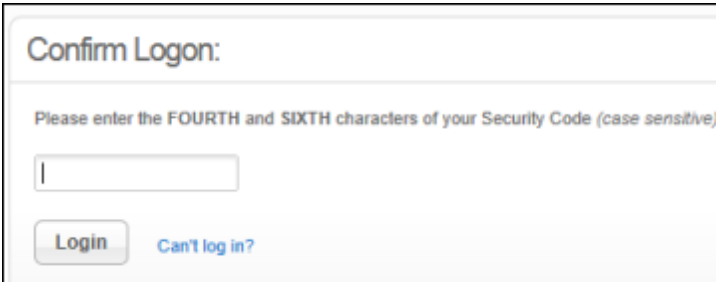
After you create an account (see "Creating a Webroot account" on page 9), you can log in to the Management Portal. On your first login, a Setup Wizard opens to help you begin configuration.

Logging in for the first time

1. Open a browser and go to the SecureAnywhere website: <https://my.webrootanywhere.com>.
Tip: To display a language other than English, click the drop-down arrow in the upper right corner of the page, select a language, then click **Go**. Be aware that to enable languages that use double-byte character sets, you must have the appropriate language pack installed on your computer.
2. In the **Log in** panel, enter the email address and password you specified when you created an account. Click **Log in**.
Tip: If you forget your password or security code, click the **Can't log in?** link, then click **I forgot my password** or **I forgot my security code**. Endpoint Protection prompts you to enter your email address, and sends you an email message containing a link for resetting your password or security code.



3. In the **Confirm Logon** panel, enter the requested characters of your security code and click **Login**. This personal security code was defined when you created a Webroot account. Every time you log in, Endpoint Protection will require this extra security step. Be aware that it prompts for two random characters of your code. For example, if your code is **123456** and it prompts you for the **fourth** and **sixth** characters, you would enter **4** and **6**.



Confirm Logon:

Please enter the FOURTH and SIXTH characters of your Security Code (case sensitive)

Login [Can't log in?](#)

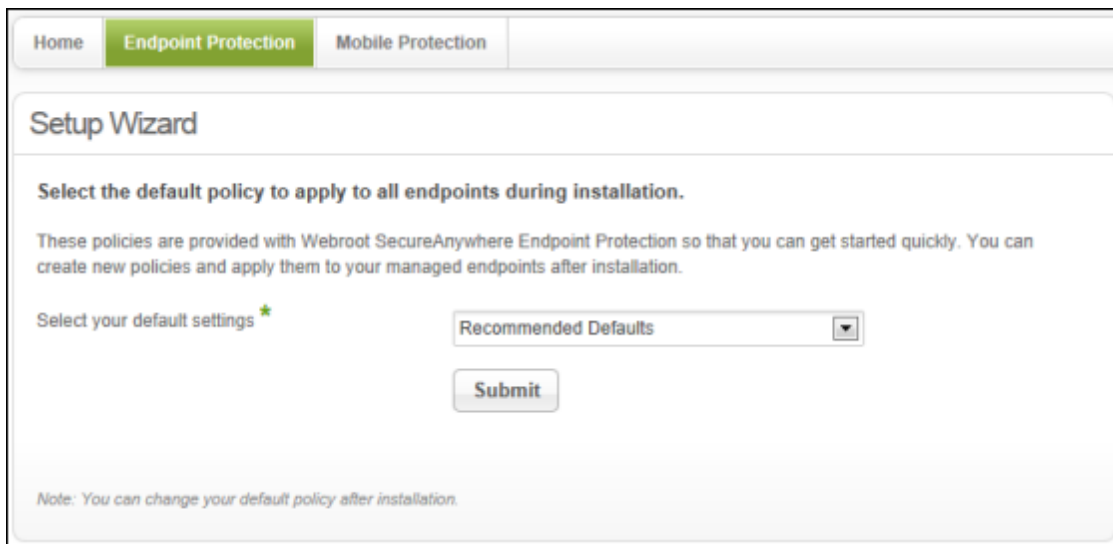
- When the SecureAnywhere website opens, click **Go to Endpoint Protection**.
Note: If you also purchased Mobile Protection, you will have access to the portal for Mobile Protection as well; otherwise, you will not see the Mobile Protection panel.



The first time you log in, the Setup Wizard opens. Continue with the next section to select a default policy.

Selecting a default policy during configuration

The Setup Wizard prompts you to select a default policy for new SecureAnywhere installations on endpoints. (A *policy* defines the SecureAnywhere settings, including how the program scans for threats and manages detected items.)



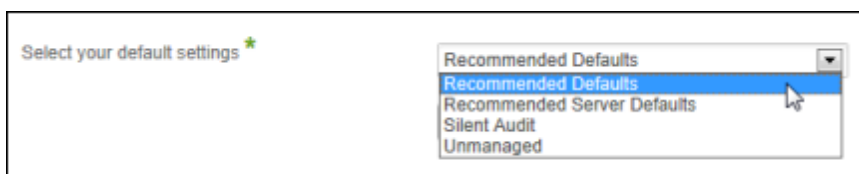
The Setup Wizard provides the following default policies:

- **Recommended Defaults.** Provides our recommended security, with threats automatically removed and quarantined.
- **Recommended Server Defaults.** Provides our recommended security for servers, with threats automatically removed and quarantined, while also allowing the servers to run with optimal performance.
- **Silent Audit.** Scans for threats without user interaction. Does not block or quarantine detected items. This policy allows you to review SecureAnywhere's threat detections first, so you can review detected items and add overrides for any legitimate application files. Use this policy if you are concerned about a false positive being detected or you are applying SecureAnywhere to a critical server. This policy is helpful if you want to preconfigure overrides before applying a stricter policy that will automatically remediate detected items. For more information about overrides, see "[Applying overrides from the Overrides tab](#)" on page 167.
- **Unmanaged.** Provides our recommended security, while also allowing users to change their own SecureAnywhere settings on their endpoints. Unmanaged endpoints still report into the Management Portal and show scan results. Administrators can also send them commands, but cannot change the policy settings.

Tip: If you are not sure which policy to select, the **Recommended Defaults** policy is a good starting point for protecting endpoints immediately. You can easily change the default policy later, as described in "Selecting a new default policy" on page 89, or create your own policies and assign them to groups of endpoints, as described in "Creating policies" on page 90.

To select a default policy:

1. Open the drop-down menu and select one of policies.



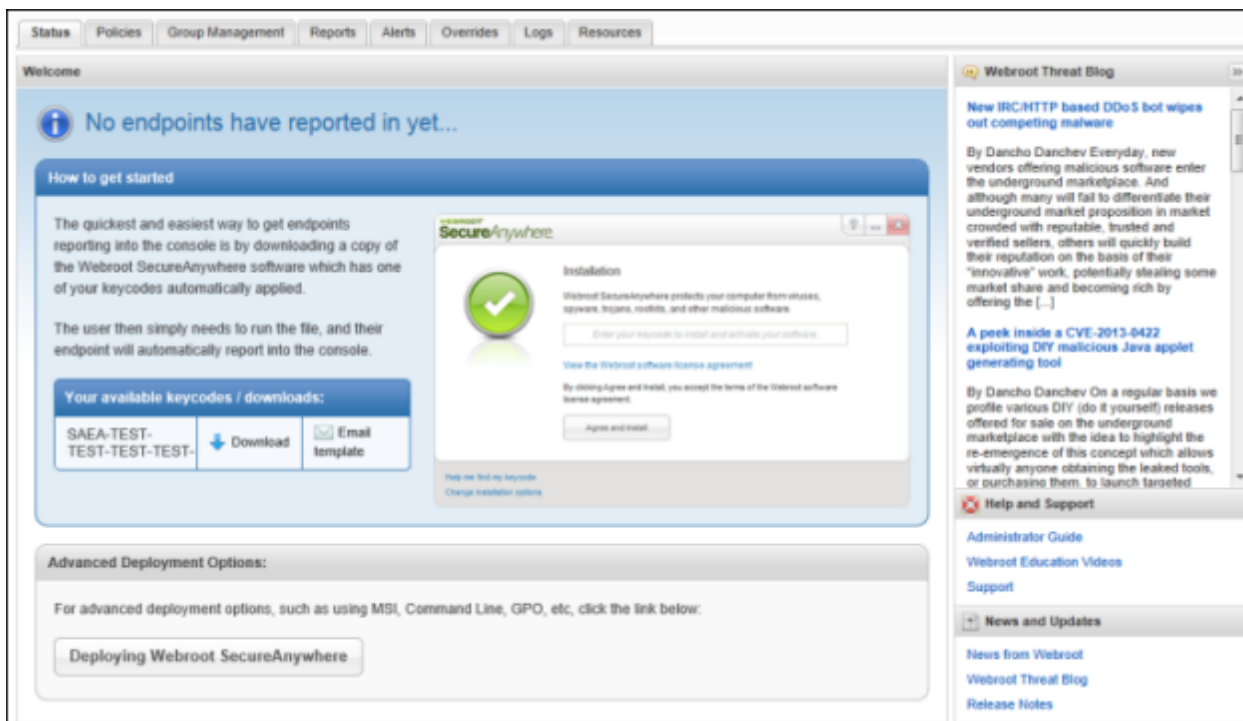
2. Click **Submit**.

The Endpoint Protection status page opens, showing a Welcome panel on the top, deployment options on the bottom, and Support resources on the right. Continue with the next section to select a deployment method.

Selecting a deployment method and performing a test install

The Welcome panel describes methods of deploying the SecureAnywhere program to endpoints.

- If you have a small network (less than 100 endpoints), you may want to use the quick method described in the **How to get started** panel. Follow the instructions provided.
- If you have a large network and use Active Directory, we recommend that you click **Deploying Webroot SecureAnywhere** at the bottom to learn more about advanced deployment options. See also "Deploying SecureAnywhere to endpoints" on page 50.



Note: If you close out of the Welcome panel, you can view the keycode and deployment information again by clicking the **Resources** tab.

To get started, we recommend that you deploy SecureAnywhere to at least one test endpoint so you can see its status in the Management Portal.

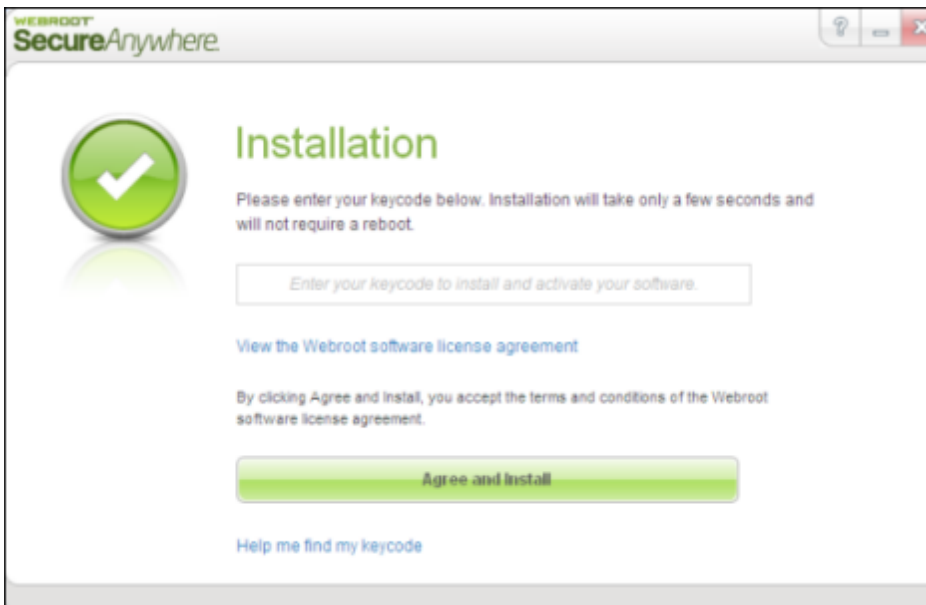
To deploy SecureAnywhere to a test endpoint:

1. Look for your keycode in the **How to get started** panel.
This keycode identifies your Endpoint Protection license.

2. Download the SecureAnywhere installer file by clicking the **Download** link.



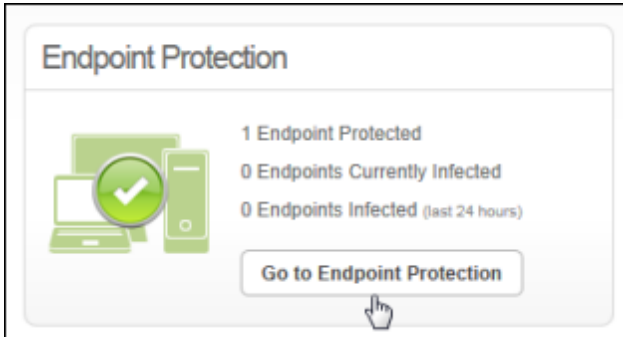
3. From the endpoint, run the installer file. When the following **Installation** panel appears, enter your Endpoint Protection keycode and click **Agree and Install**.



Alternatively, you can send a test email to an end user who will install SecureAnywhere. To do this, click the **Email template** link from the Welcome panel (or Resources tab), and then cut and paste the text into an email message. The link automatically adds the correct keycode for the user. Next, the user clicks the link to begin installation. The program installs silently in the background, with the correct keycode already entered. When it's done, a Webroot icon appears in the endpoint's system tray.

4. Wait for SecureAnywhere to finish its first scan. This should only take a few minutes. When it's done, SecureAnywhere reports into the Management Portal.

5. After the endpoint finishes a scan, log in to the SecureAnywhere website again and see its status. When you click **Go to Endpoint Protection**, the Management Portal opens (you won't see the Setup Wizard again). See "Using the Management Portal" on page 19.



Using the Management Portal

The Management Portal is a central website that administrators can use to view and manage network status. The administrator who first created the Webroot account has access to all functions in the portal (see "Creating a Webroot account" on page 9). If desired, the administrator can create additional users with full or limited access (see "Managing portal users" on page 33).

To log in to the Management Portal:

1. Go to the SecureAnywhere website: <https://my.webrootanywhere.com>.
2. In the **Log in** panel, enter the email address and password you specified when you created an account. Click **Log in**.

3. In the **Confirm Logon** panel, enter the requested characters of your security code and click **Login**.

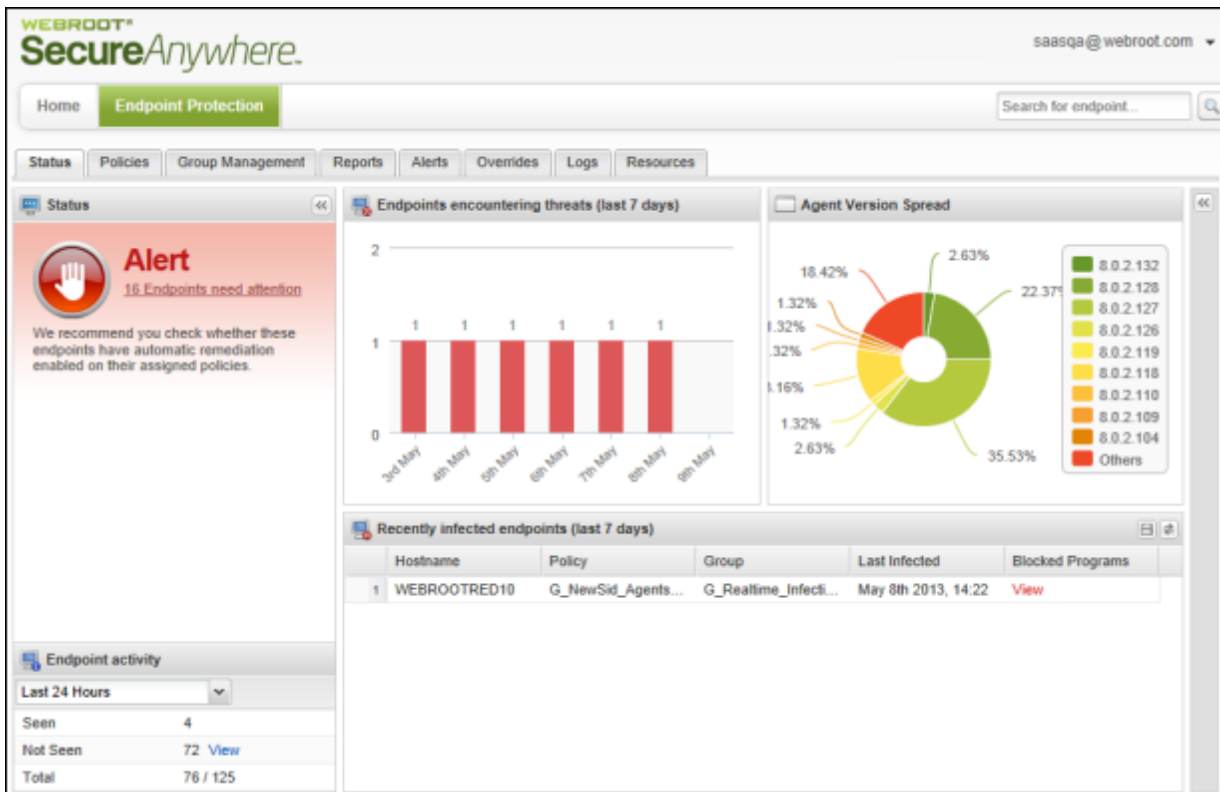
This personal security code was defined when you created a Webroot account. Every time you log in, Endpoint Protection will require this extra security step. Be aware that it prompts for two random characters of your code. For example, if your code is **123456** and it prompts you for the **fourth** and **sixth** characters, you would enter **4** and **6**.

The SecureAnywhere website opens and shows the total number of endpoints protected in your network, any endpoints that have threats, and any endpoints with threats detected in the last 24 hours.

4. From the Endpoint Protection panel (see the following example), you can click **Go to Endpoint Protection** to open the Management Portal or click an "Endpoint Infected" link (if any) to open the Management Portal and go directly to the threat information panel.



The Management Portal looks similar to the following example. The Status panel includes threat alerts, endpoint activity, and data charts. You can click tabs along the top that allow you to access configuration and other tasks.



The following sections describe the areas of the Management Portal, including its tabs, menus, panels, tables, search functions, and export functions.

Using the main tabs

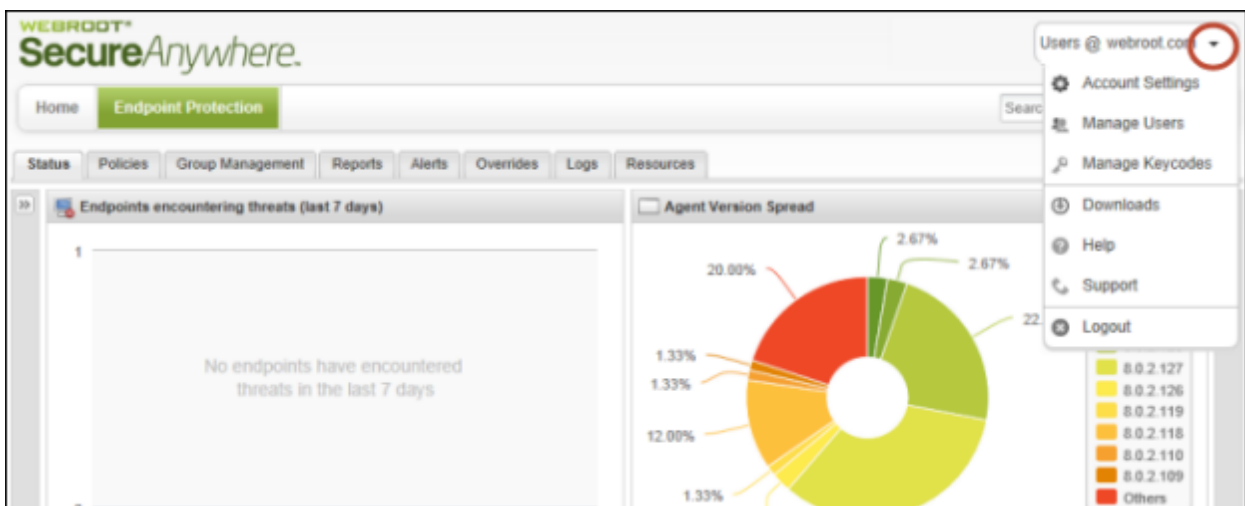
The following table describes the Endpoint Protection tabs.

Management Portal tabs	
Status	<p>A dashboard that shows:</p> <ul style="list-style-type: none"> • An alert notification panel, if endpoints need attention. Click the notification to see a list of endpoints that encountered threats. • A bar chart showing the number of endpoints that encountered threats in the last 7 days. • A pie chart showing the SecureAnywhere versions installed on your endpoints. • An endpoint activity panel showing the number of endpoints reporting into the Management Portal (based on a timeframe you select). If any endpoints have not reported their status recently, you can click the View link next to Not Seen to determine which endpoints are not reporting status. • A panel showing the endpoints with the most recent threats. You can click on a row to view more information and add an override, if desired. • A panel with links to Webroot's threat blog, guides, videos, release notes, and other news. (Not shown in the example above; see "Accessing product information" on page 25.)
Policies	Policies define the behavior of SecureAnywhere on the endpoints, such as when it runs a scan and how it blocks potential threats.
Group Management	Groups help you organize endpoints for easy management. You can view your groups and each endpoint in the group. You can also select individual endpoints to see their scan histories.
Reports	Reports show threats and unidentified software present on your endpoints, as well as the versions of SecureAnywhere they are running.
Alerts	Alerts allow you to customize warnings and status messages for a distribution list of administrators.

Management Portal tabs	
Overrides	Overrides provide administrative control over the files running in your environment. You can override files so they are not blocked or always quarantined.
Logs	Logs provide a view of changes and a history of command usage.
Resources	Resources provides information on deployment options for endpoints.

Opening the Endpoint Protection Menu

The arrow next to your login ID opens the menu for Endpoint Protection. The options available on the menu vary, depending on your access permissions.



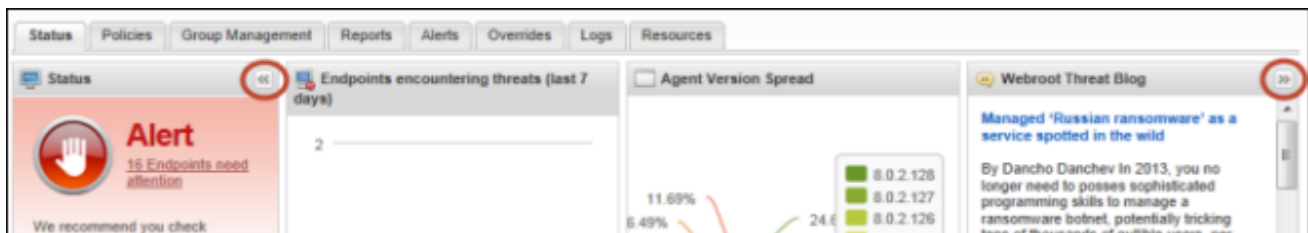
See the following table for more information about the Endpoint Protection Menu.

Endpoint Protection Menu	
Account Settings	Edit your account settings, including your password and other information. See "Editing your own account settings" on page 30.
Manage Users	Provide other users with access to the Management Portal. See "Managing portal users" on page 33.

Endpoint Protection Menu	
Manage Keycodes	View your current Endpoint Protection license keycodes and add more to the portal, if you purchased additional keycodes. See "Adding keycodes to your account" on page 42.
Downloads	Download the SecureAnywhere installer file and read more about deployment options.
Help	Open the online instructions for the Management Portal.
Support	Open the interactive knowledgebase to find product information.
Logout	Exit out of the Management Portal.

Opening and collapsing panels

For a larger view of the data charts, you can collapse the panels on the far left and the far right. Click the **Collapse** buttons (shown in the following example). The bar charts in the middle panel are static; you cannot collapse them or change the type of charts that display.

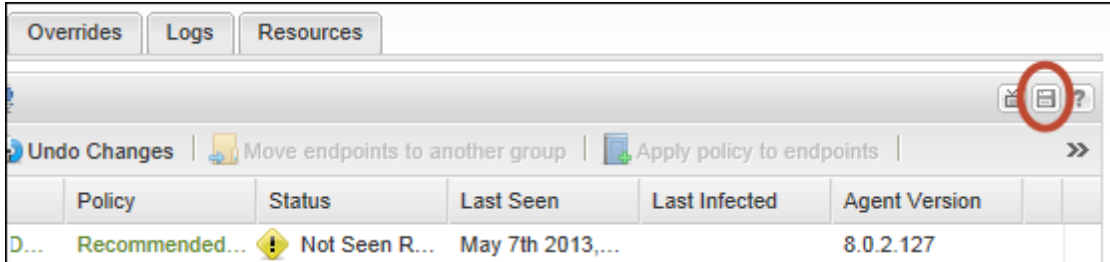


To re-open the panel, click the **Collapse** button again, as shown in the following example.



Exporting data to a spreadsheet

When you see a spreadsheet icon, you can click that icon to export the displayed data into a spreadsheet.



Opening video tutorials

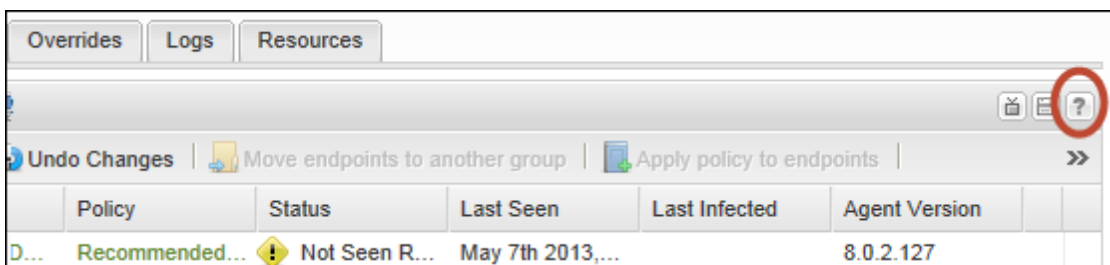
When you see a television icon (shown in the following example), you can click that icon to view a video that describes a procedure related to the panel.



Opening the Help files

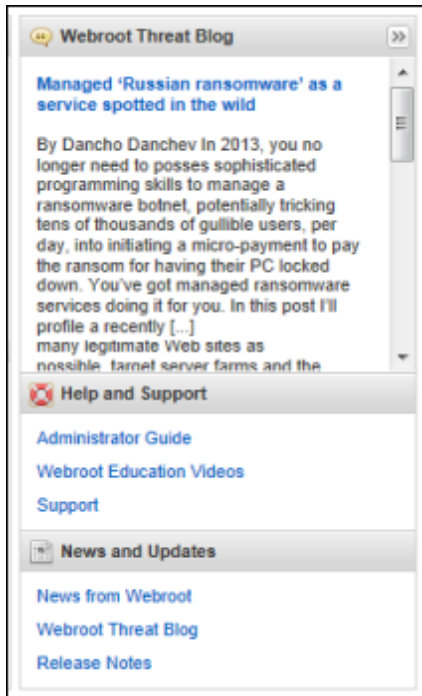
When you see a Question mark icon, you can click that icon to open Help for the current panel. You can also go to:

http://www.webroot.com/En_US/SecureAnywhere/SME/EndpointProtection.htm.

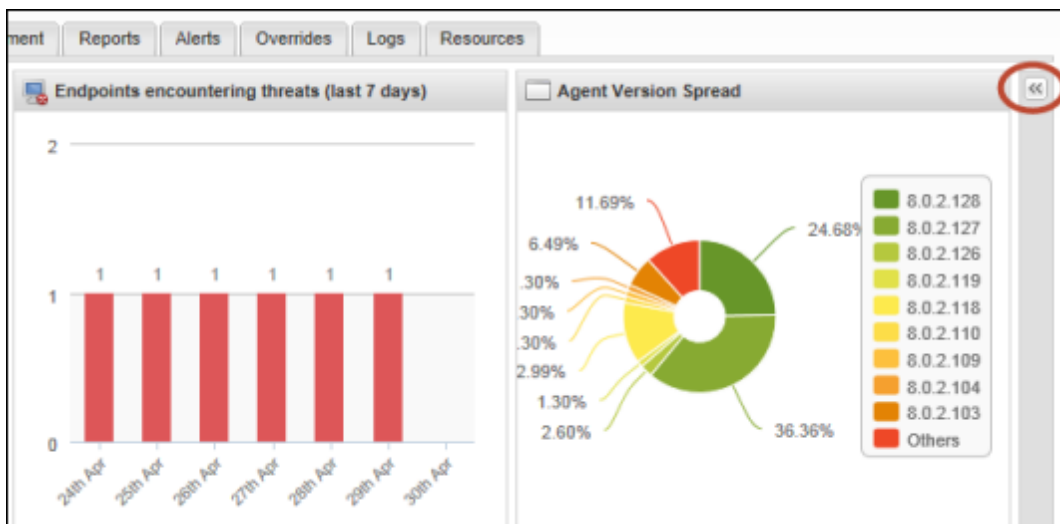


Accessing product information

Webroot's threat blog, guides, videos, release notes, and other news are available from the right panel. Click a link to access the resources under **Help and Support** or **News and Updates**.



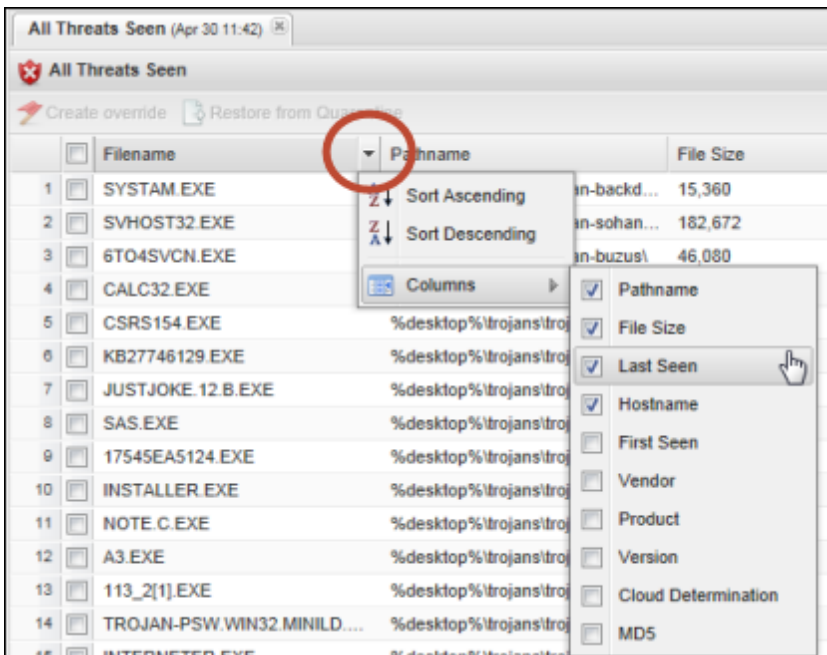
If this panel is not open, click on the **Collapse** button on the far right:



Sorting data in tables and reports

You can sort, hide, and show data in tables and reports, as follows:

- **Quick sort on a column:** Click the desired column head to sort by that subject. For example, if you want to sort data by policy name, you would click the Policy column header.
- **Change the ascending or descending order:** Click at the end of a column header to display the drop-down arrow, then click the arrow to open the menu. Select either **Sort Ascending** or **Sort Descending** to change the order of data points in a column.
- **Show or hide columns:** Click at the end of a column header to display the drop-down arrow, then click the arrow to open the menu. Select a box (check) to show a column. Deselect a box (uncheck) to hide a column.



The following table describes subject data that may appear in Endpoint Protection tables and reports. The data that appears depends on the type of table or report displayed.

Data points in tables and reports	
Agent Language	The language selected when SecureAnywhere was installed: en = English ja = Japanese es = Spanish fr = French de = German it = Italian nl = Dutch ko = Korean zh-cn = Simplified Chinese pt = Brazilian Portuguese ru = Russian tr = Turkish zh-tw = Traditional Chinese
Agent Version	The version of the SecureAnywhere software installed on the endpoint.
All Endpoints	More information about the endpoints where a file was detected and blocked.
All Versions	More information about the SecureAnywhere versions where a file was detected and blocked.
Approx Scan Time	The duration of a scan in minutes and seconds.
Area	A flag for the country where the endpoint is located.
Cloud Determination	The Webroot classification of the file, which can be Good , Bad , or Undetermined .
Days Infected	The number of days the endpoint remained infected.
Device MID	A Machine ID value that identifies the hardware for an endpoint. Webroot uses an algorithm to determine this value.
Endpoints Affected	The number of endpoints with a detected file.
File Size	The size of the file in bytes.
Filename	The filename of the detected threat.
First Infected	The date and time a threat was detected.
First Seen	The date and time this endpoint first checked into the Management Portal.
Group	The group assigned to the endpoint.
Hostname	The machine name of the endpoint.

Data points in tables and reports	
Instance MID	A value that identifies the Windows operating system SID (Security Identifier). Webroot uses an algorithm to determine this value.
IP Address	The IP address of the endpoint.
Keycode	The license used to install SecureAnywhere on the endpoint.
Last Infected	The date and time the endpoint reported an infection.
Last Scan Time	The time of the last scan on this endpoint.
Last Seen	The date and time this endpoint last checked into the Management Portal.
Malware Group	The classification of the malware; for example: Trojan or System Monitor .
MD5	The <i>Message-Digest algorithm 5</i> value, which acts like a fingerprint to uniquely identify a file.
OS	The operating system of the endpoint.
Pathname	The directory (folder) where the file was detected.
Policy	The policy assigned to the endpoint.
Product	The name of the product associated with the file, if SecureAnywhere can determine that information.
Scan Type	The type of scan: Deep Scan , Post Cleanup Scan , or Custom/Right-Click Scan .
Status	The current status of the endpoint: Protected (no infections), Infected (malware detected), Not Seen Recently (has not reported into the portal), Expired (SecureAnywhere license has lapsed), or Infected & Expired .
System Pack	The number of the service pack for the operating system.
System Type	Either 32-bit or 64-bit .
Vendor	The name of the vendor associated with the file, if SecureAnywhere can determine that information.
Version	The version of the product associated with the file, if SecureAnywhere can determine that information.
VM	Yes , if the endpoint is installed on a virtual machine.
Windows Full OS	The name of the Windows operating system.

Chapter 2: Managing User Accounts

To manage your Webroot account, see the following topics:

Editing your own account settings	30
Managing portal users	33
Creating new portal users	33
Editing user information	36
Setting permissions for portal users	38
Adding keycodes to your account	42
Adding consoles to your account	44
Adding a console	44
Renaming a console	46
Switching consoles	46
Renewing or upgrading your account	47

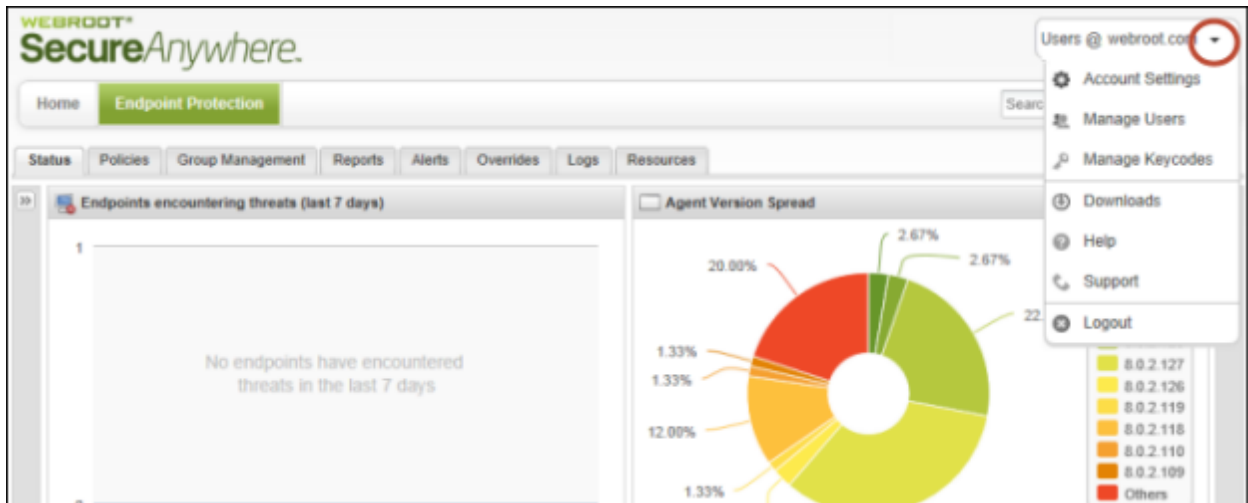
Editing your own account settings

An *account* defines your user details (login name, password, etc.) and access permissions. For your own account, you can change any setting except the email address specified for your login name.

Note: If you want to edit settings for other portal users, see "Managing portal users" on page 33.

To edit your account settings:

1. Open the Endpoint Protection menu by clicking the arrow next to your login ID, then click **Account Settings**.



2. In the **Account Settings** panel, click one of the **Change** links to open another panel where you can edit the information.

Account Settings

User Details		
Name		Change
Display Name		Change
Email	giri@webroot.com	
Password	*****	Change
Security Code	*****	Change
Security Question	*****	Change
Office Phone		Change
Mobile Phone		Change
Time Zone	United States, California, Los Angeles, San Francisco, San Diego, Sacramento (PDT)	Change
Alerts		Change

Access & Permissions

3. In the **User Details** panel, make the desired changes to your name and phone numbers.

Note: The *Display Name* is the name that appears in the Management Portal.

If you need to change the time zone, click the pencil icon at the right, then type the country, region, or city to open a drop-down menu of choices.

Account Settings

User Details | **Access & Permissions**


First Name: William

Last Name: User

Display Name: Bill

Office Phone: 555-555-5555

Mobile Phone:

Time Zone: United States, California, Los Angeles, San Francisco, San Diego, Sacramento 

Save Details

4. To check your access permissions, click the **Access & Permissions** tab. If you are the main Endpoint Protection administrator, we recommend that you keep the default settings as shown in the following example. For more information about the settings, see "Setting permissions for portal users" on page 38.

5. Click **Save Access & Permissions** when you're done.

The screenshot shows the 'Access & Permissions' configuration page. At the top, there are two tabs: 'User Details' and 'Access & Permissions', with the latter being selected and circled in red. Below the tabs, there is a question: 'Do you wish to give this user Console access?' with a checked checkbox and the word 'Yes' next to it. Underneath, there are two dropdown menus: 'SecureAnywhere Console' set to 'Admin' and 'Endpoint Protection Console' also set to 'Admin'. The main content area is divided into several sections, each with a header and a list of permissions:

- Groups:** 'Create & Edit' (checked), 'Deactivate/Reactivate Endpoints' (checked), 'Assign Endpoints to Groups' (checked).
- Policies:** 'Create & Edit' (checked), 'Assign Policies to Endpoints' (checked).
- Overrides:** 'MDS' (checked), 'Determination Capability' (dropdown menu set to 'Good & Bad').
- Commands:** Radio buttons for 'None', 'Simple', 'Advanced', and 'Expert'. 'Expert' is selected.
- Alerts:** 'Create & Edit' (checked).

At the bottom of the form, there is a button labeled 'Save Access & Permissions'.

Managing portal users

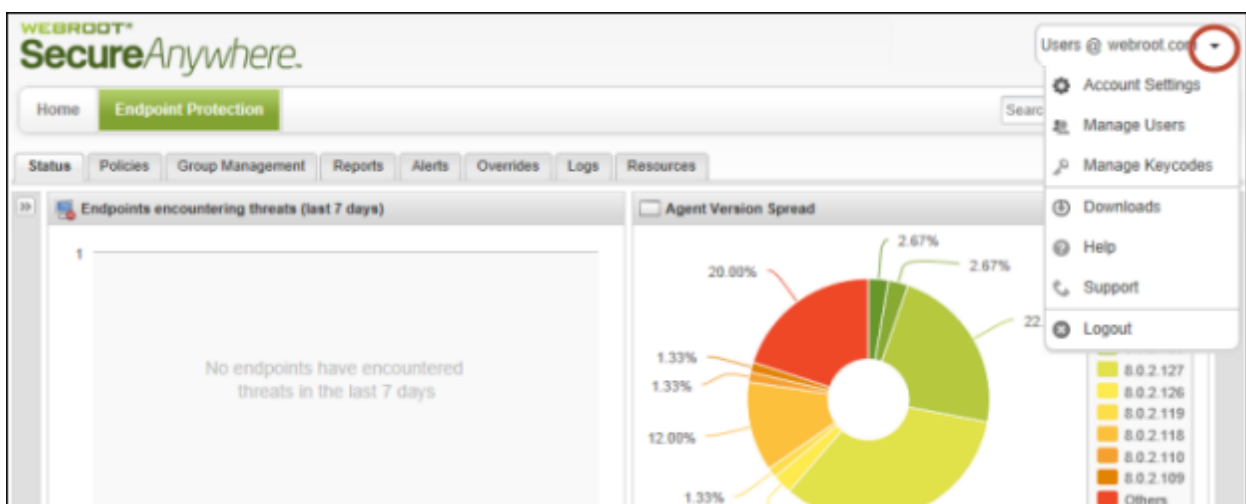
If you have *Admin* permission for Endpoint Protection (see "Setting permissions for portal users" on page 38), you can create new Management Portal users, set access permissions for them, and edit their information. When you create new users, Endpoint Protection sends them an email with further details for creating a password and logging in.

Creating new portal users

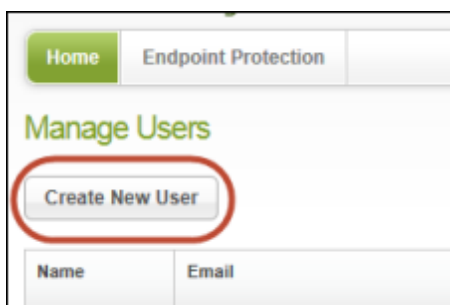
You might want to add other administrators so they can access Endpoint Protection reports. You can also add users with limited permissions so they can view data, but not make changes.

To create a new portal user:

1. Open the Endpoint Protection menu by clicking the arrow next to your login ID, then click **Manage Users**.



2. In the **Manage Users** panel, click **Create New User**.



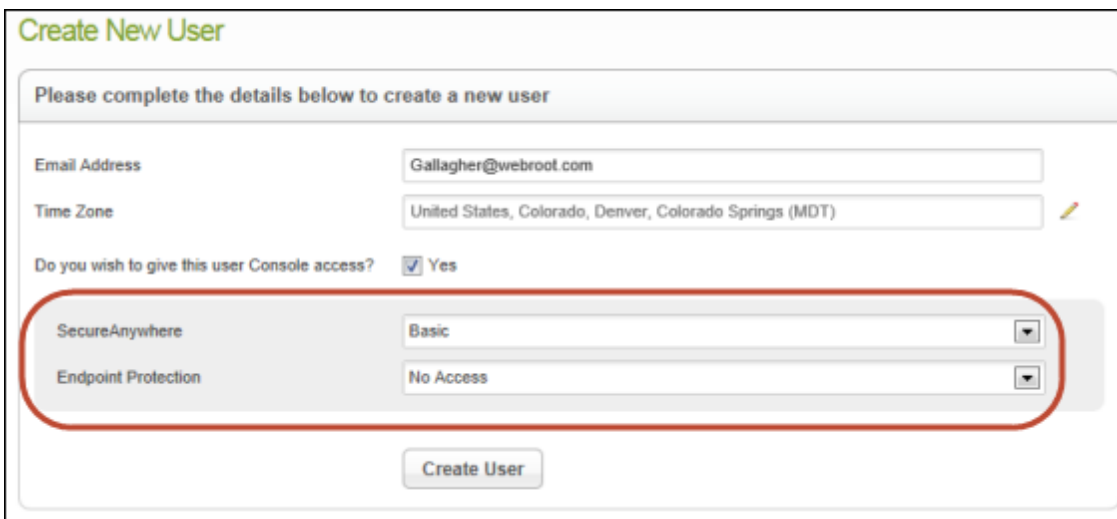
3. In the **Create New User** panel, enter the user's email address (the address where the user receives the confirmation message). The email address will also serve as the user's login name.
If you entered the wrong email address and the user does not receive the message, you will be able to change the email address and re-send it later. See "Editing user information" on page 36.
4. Select the time zone where this user is located. Click the pencil icon at the right, then type the country, region, or city to open a drop-down menu of choices.



The screenshot shows the 'Create New User' form with the following fields:

- Email Address:** Gallagher@webroot.com
- Time Zone:** United States, Colorado, Denver, Colorado Springs (MDT) (with a pencil icon on the right)
- Do you wish to give this user Console access?:** Yes

5. Next to **Do you wish to give this user Console access?**, click in the **Yes** checkbox. Additional fields appear at the bottom, as shown in the following example.



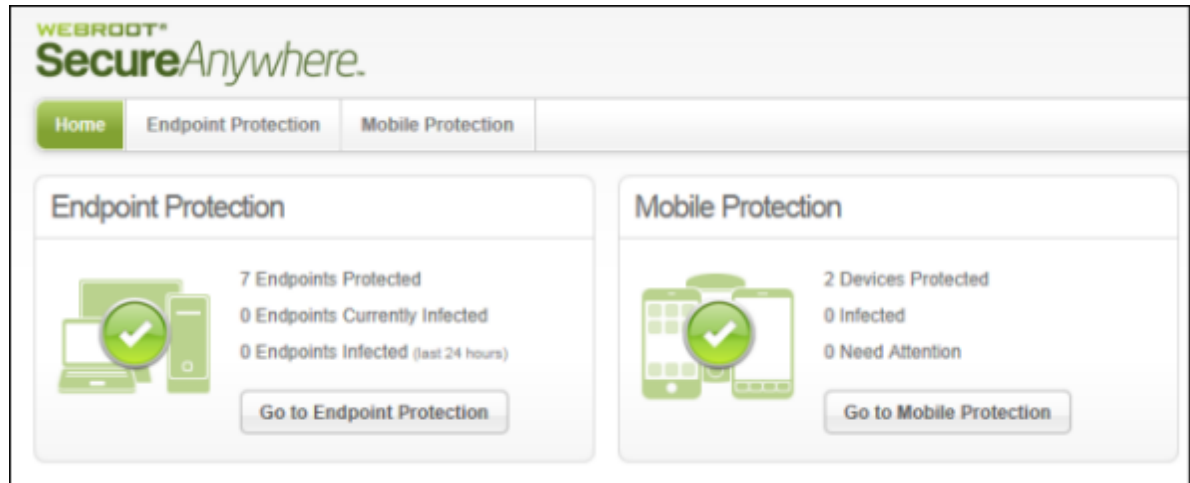
The screenshot shows the 'Create New User' form with the following fields:

- Email Address:** Gallagher@webroot.com
- Time Zone:** United States, Colorado, Denver, Colorado Springs (MDT) (with a pencil icon on the right)
- Do you wish to give this user Console access?:** Yes
- SecureAnywhere:** Basic (dropdown menu)
- Endpoint Protection:** No Access (dropdown menu)
- Create User** button

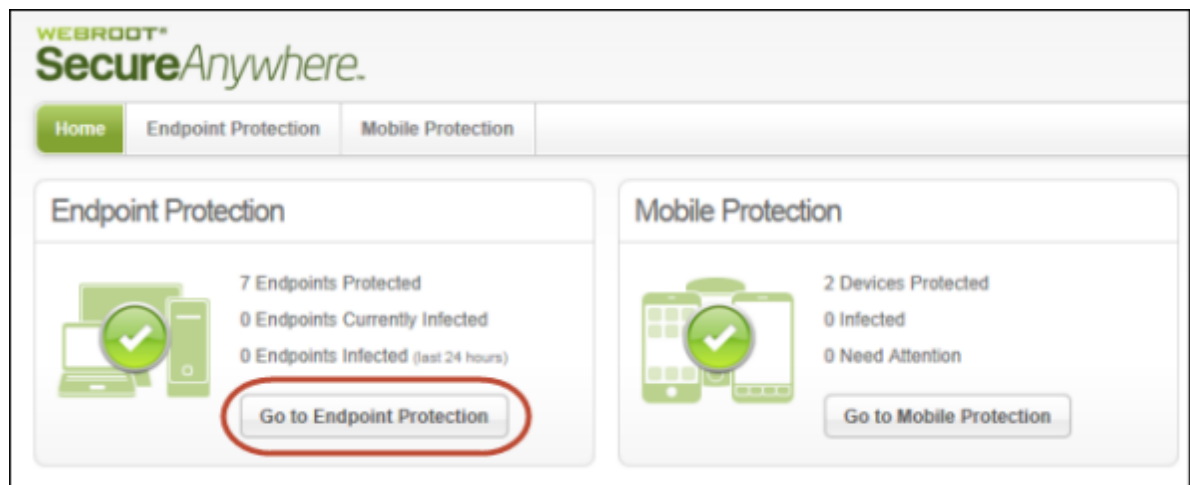
In these two fields, you must specify the level of access to give the user for **SecureAnywhere** or **Endpoint Protection**. The two types of consoles are described as follows:

- **SecureAnywhere:** The **Home** page of **my.webrootanywhere.com** (see the following example). From here, the user can access other Webroot portals, such as the Mobile

Protection portal (if your company purchased Mobile Protection).



- **Endpoint Protection:** The Management Portal (or *Admin Console*) for Endpoint Protection. When users have access to this portal, they will see the **Go to Endpoint Protection** button and can click it to enter the Management Portal (see the following example).



6. In the **SecureAnywhere** field, click the drop-down arrow to select either **Basic** (limited access to consoles and account settings) or **Admin** (full access to all keycodes, users, and account settings in Webroot portals).
7. In the **Endpoint Protection** field, click the drop-down arrow to change **No Access** to either **Basic** (read-only access to endpoint scans) or **Admin** (full access to all settings). You can further modify this user's permissions later, as described in "Setting permissions for portal users" on page 38.

- 8. When you're done, click **Create User** to send a confirmation email to the new user. The user's email message includes a temporary password for the first login. When the user clicks the confirmation link in the email, the Confirm Registration panel opens for the user to enter login information (see the following example).

Confirm Registration

A temporary password had been emailed to you.

Temporary Password *

Create New Password *

Strength: [Progress Bar]

Repeat New Password *

Your Personal Security Code *

Security Question *

Security Answer *

Confirm


Editing user information

After the user confirms registration, you can return to the Manage Users panel and edit information for that user. (You cannot view or edit other users' passwords, security codes, or security questions; only they have access to that information.)

If the user has not confirmed registration, you will see the user's status as *Awaiting Confirmation*. The status changes to *Activated* when the user receives the email and confirms the registration. If desired, you can resend the confirmation email by clicking the envelope icon next to the *Awaiting Confirmation* status.

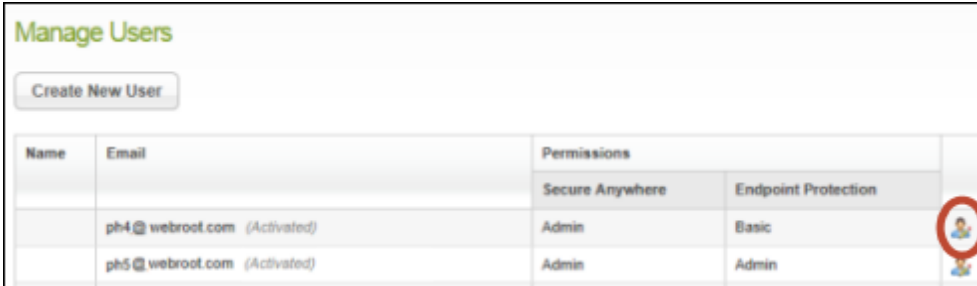
Manage Users

Create New User



Name	Email
	bj@webroot.com (Activated)
	jan@webroot.com (Awaiting Confirmation) 
	giri@webroot.com (Activated)

To edit portal users:

1. Locate the row for the user you want to edit, then click that user's edit icon. The edit icon is at the far right, as shown in the following example.

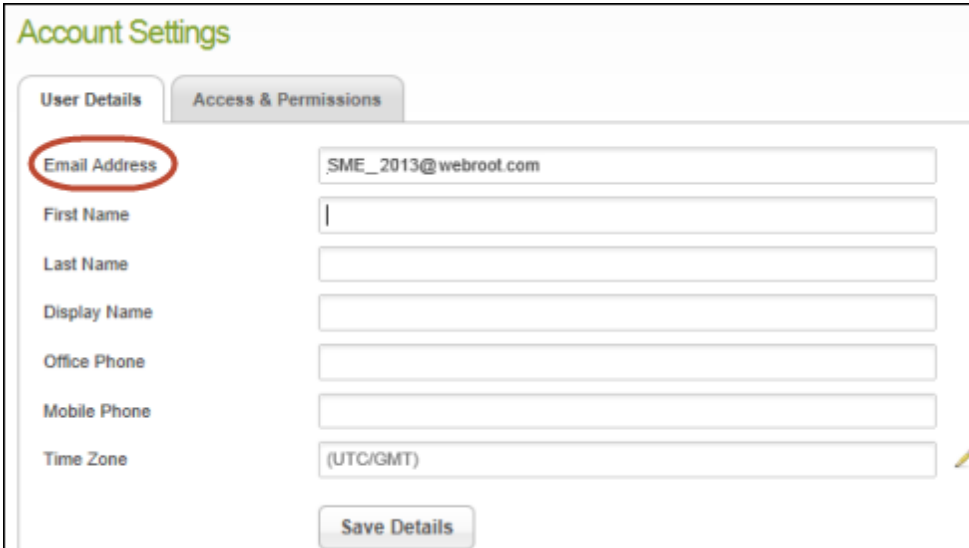


The screenshot shows the 'Manage Users' interface. At the top left is a 'Create New User' button. Below it is a table with columns for Name, Email, Permissions, and an edit icon. The table contains two rows of user data. The edit icon for the second row is circled in red.


Name	Email	Permissions		Edit Icon
		Secure Anywhere	Endpoint Protection	
	ph4@webroot.com (Activated)	Admin	Basic	
	ph5@webroot.com (Activated)	Admin	Admin	

Note: If your account has multiple consoles, you see only users who are associated with the keycodes for the currently active console. For more information about consoles, see "Adding consoles to your account" on page 44.

2. In the **User Details** panel, make the desired changes to the name and phone numbers. If the user has an *Awaiting Confirmation* status, this dialog shows an email field at the top. You might want to change the email address if you entered an incorrect address for the user and need to resend the registration.



The screenshot shows the 'Account Settings' dialog with the 'User Details' tab selected. The 'Email Address' field is circled in red. Below it are fields for First Name, Last Name, Display Name, Office Phone, Mobile Phone, and Time Zone. A 'Save Details' button is at the bottom.

Account Settings	
User Details Access & Permissions	
Email Address	SME_2013@webroot.com
First Name	
Last Name	
Display Name	
Office Phone	
Mobile Phone	
Time Zone	(UTC/GMT) 
Save Details	

3. If you want to change the settings under **Access & Permissions**, see "Setting permissions for portal users" on page 38 for further instructions.
4. Click **Save Details** when you're done.

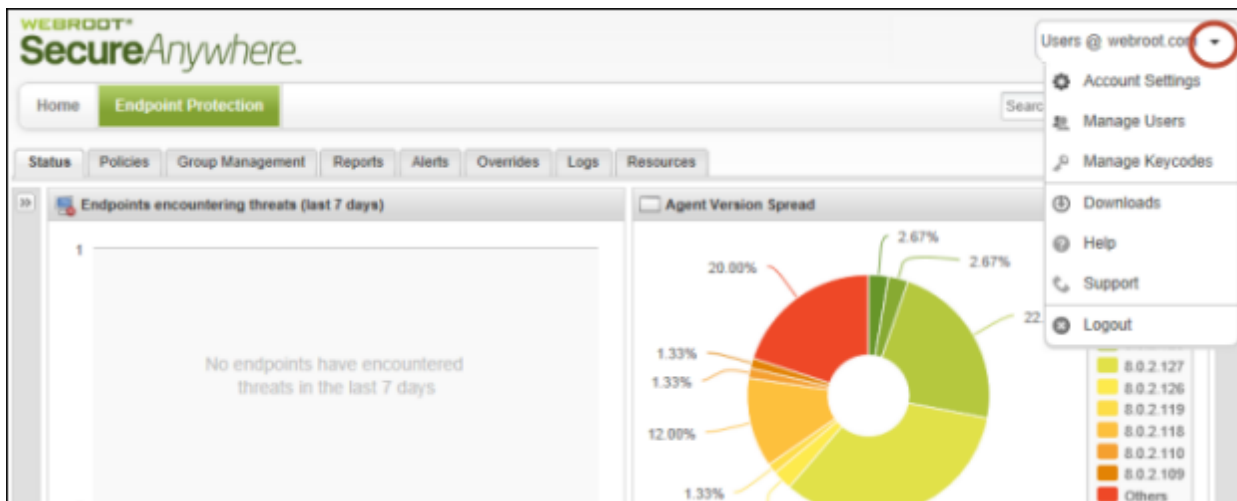
Setting permissions for portal users

If you have *Admin* permission for Endpoint Protection, you can edit the following permissions for other Management Portal users:

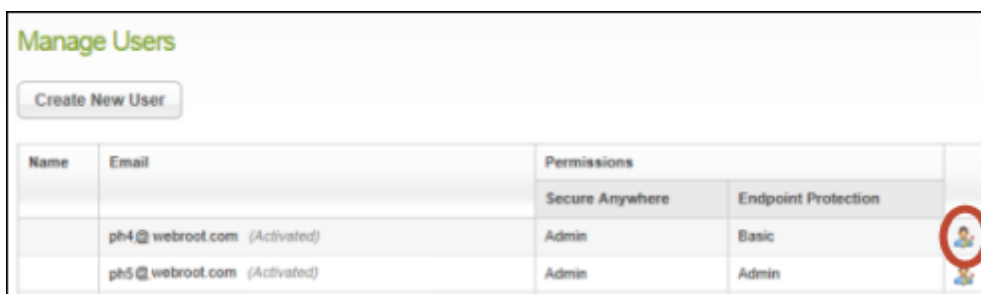
- **Site access.** Change the level of access between Basic and Admin levels for the SecureAnywhere website (Home panel of my.secureanywhere.com) and the Management Portal of Endpoint Protection.
- **Groups.** Specify whether the user can create and modify groups of endpoints, deactivate or reactivate endpoints, or assign endpoints to groups.
- **Policies.** Specify whether the user can create and modify policies or assign policies to endpoints.
- **Overrides.** Specify whether the user can make overrides to files, designating them as "good" or "bad."
- **Commands.** Specify what types of commands the user can issue to the endpoints.
- **Alerts.** Allow this user to create and edit warning messages.

To set user permissions:



1. Open the Endpoint Protection menu by clicking the arrow next to your login ID, then click **Manage Users**.



2. Locate the row for the user you want to edit, then click that user's edit icon. The edit icon is at the far right, as shown in the following example.



The screenshot shows a 'Manage Users' interface. At the top left, there is a 'Create New User' button. Below it is a table with columns for 'Name', 'Email', and 'Permissions'. The 'Permissions' column is further divided into 'Secure Anywhere' and 'Endpoint Protection'. Two users are listed: 'ph4@webroot.com (Activated)' with 'Admin' permissions for 'Secure Anywhere' and 'Basic' for 'Endpoint Protection', and 'ph5@webroot.com (Activated)' with 'Admin' permissions for both. A red circle highlights a user icon in the rightmost column of the table.

Name	Email	Permissions		
		Secure Anywhere	Endpoint Protection	
	ph4@webroot.com (Activated)	Admin	Basic	
	ph5@webroot.com (Activated)	Admin	Admin	

The User Details panel opens.

3. Click the **Access & Permissions** tab to see the list of Endpoint Protection functions and their associated access permissions.

The screenshot shows the 'Access & Permissions' configuration page for a user. At the top, there are two tabs: 'User Details' and 'Access & Permissions', with the latter being selected and circled in red. Below the tabs, there is a question: 'Do you wish to give this user Console access?' with a checked 'Yes' radio button. Underneath, there are two dropdown menus for 'SecureAnywhere Console' and 'Endpoint Protection Console', both set to 'Admin'. The main content area is divided into several sections: 'Groups' with three checked items (Create & Edit, Deactivate/Reactivate Endpoints, Assign Endpoints to Groups); 'Policies' with two checked items (Create & Edit, Assign Policies to Endpoints); 'Overrides' with 'MDS' checked and 'Determination Capability' set to 'Good & Bad'; 'Commands' with radio buttons for 'None', 'Simple', 'Advanced', and 'Expert' (where 'Expert' is selected); and 'Alerts' with 'Create & Edit' checked. At the bottom of the form is a 'Save Access & Permissions' button.

4. Assign access permissions for this user, as described in the following table. When you're done, click **Save Access & Permissions**.

Access & Permissions	
Groups	<p>Create & Edit. Define and modify groups of endpoints.</p> <p>Deactivate/Reactivate Endpoints. Deactivate and reactivate endpoints from the Management Portal. See "Deactivating endpoints" on page 73.</p> <p>Assign Endpoints to Groups. Allows the portal user to move one or more endpoints from one group to another. See "Organizing endpoints into groups" on page 120.</p>
Policies	<p>Create & Edit. Define, delete, rename, copy, and export policies.</p> <p>Assign Policies to Endpoints. Associate a policy with an endpoint or group of endpoints. See "Implementing policies" on page 88.</p>
Overrides	<p>MD5. Override how a file is detected by entering the MD5 value of a file. MD5 (Message-Digest algorithm 5) is a cryptographic hash function that acts like a fingerprint to uniquely identify a file.</p> <p>Determination Capability. Specify overrides based on these settings:</p> <ul style="list-style-type: none"> • Good — Allow files containing the specified MD5 value. • Bad — Block files containing the specified MD5 value. When a scan encounters this file, it flags it and requests action from the SecureAnywhere user. • Good & Bad — Allow either Good or Bad. <p>See "Implementing overrides" on page 166.</p>
Commands	<p>None. Do not allow this user to send commands to endpoints.</p> <p>Simple. Access to the Agent and Clear Data commands, and view commands for selected endpoints.</p> <p>Advanced. Access to Agent, Clear Data, Keycode, Power & User Access, Antimalware Tools, Files & Processes commands, and view commands for selected endpoints.</p> <p>Expert. Access all commands, including Expert Advanced options. See "Issuing commands to endpoints" on page 63.</p>
Alerts	<p>Create & Edit. Configure instant or scheduled alerts for endpoint activity. See "Implementing alerts" on page 156.</p>

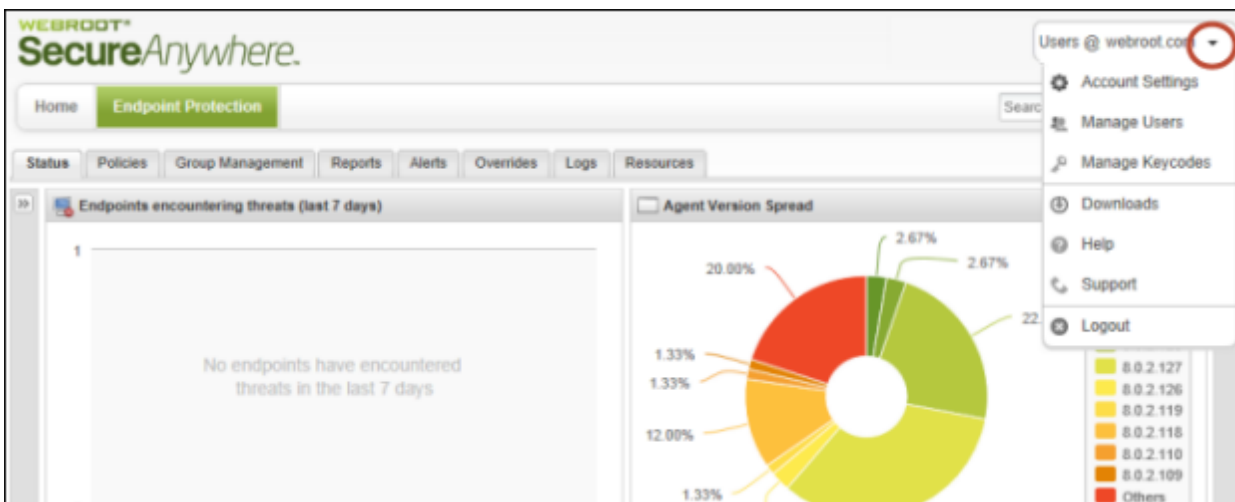
Adding keycodes to your account

You can have one or more keycodes in your Webroot account. A *keycode* is a 20-character license used to install SecureAnywhere on endpoints, which identifies how many seats you have available for installations. If you purchase more keycodes, you must add them manually as described in this section.

Note: To view existing keycodes and add new ones, you must have *Admin* permission for Endpoint Protection (see "Setting permissions for portal users" on page 38).

To purchase and add keycodes:

1. Open the Endpoint Protection menu by clicking the arrow next to your login ID, then click **Manage Keycodes**.



The Manage Keycodes panel opens.

Note: If your account has multiple consoles, you see only the keycodes that are associated with the currently active console.

The screenshot shows the 'Manage Keycodes' panel. It has two buttons: 'Add Product Keycode' and 'Buy a Keycode now'. Below is a table with columns: Keycode, Edition, Devices, Days Remaining, Renew, and Upgrade. Two rows of keycodes are visible, with the first two columns redacted by black bars.

Keycode	Edition	Devices	Days Remaining	Renew	Upgrade
[REDACTED]	Endpoint Protection	25	318 (Feb 23 2014)	Renew	Upgrade
[REDACTED]	Endpoint Protection	100	296 (Jan 31 2014)	Renew	Upgrade

The Keycode list shows the attributes associated with each Endpoint Protection license.

Manage Keycodes panel	
Keycode	The 20-character license you received when you purchased Endpoint Protection.
Edition	Endpoint Protection, or another Webroot product you purchased.
Devices	Number of endpoints that can use this keycode.
Days Remaining	Number of days remaining for this keycode to be active, and the expiration date.
Renew	A link for renewing your subscription. See "Renewing or upgrading your account" on page 47.
Upgrade	A link for purchasing more endpoint seats for this license. See "Renewing or upgrading your account" on page 47.

- If you need to purchase another keycode, click **Buy a Keycode** now at the top of the list. The Webroot Business website opens. From here, you can buy another keycode.
- After you purchase the keycode, you can add it to Endpoint Protection by clicking **Add Product Keycode**.

Manage Keycodes					
Add Product Keycode		Buy a Keycode now			
Keycode	Edition	Devices	Days Remaining	Renew	Upgrade
████████████████████	Endpoint Protection	25	318 (Feb 23 2014)	Renew	Upgrade
████████████████████	Endpoint Protection	100	296 (Jan 31 2014)	Renew	Upgrade

- In the **Add a Keycode** dialog, enter the keycode you just purchased and click **Add**. Your new keycode will appear in the Manage Keycodes panel and in the **Resources** tab.

Adding consoles to your account

When you first created an account, Endpoint Protection organized your managed devices into a single console. A *console* is a collection of one or more endpoints running SecureAnywhere or other Webroot products. If you have a large network with hundreds of endpoints, you might want to create multiple consoles for simplified views of device groups. For example, you can create separate consoles for endpoints in remote offices or endpoints in separate departments.

Note: Adding a console requires that you obtain a new keycode from Webroot. Keep in mind that our Endpoint Protection billing system is based on the number of seats you have, not on the number of keycodes. You do not need to purchase a new keycode, unless you have exceeded your maximum allowance of endpoint seats. Contact your Webroot sales representative for more information.

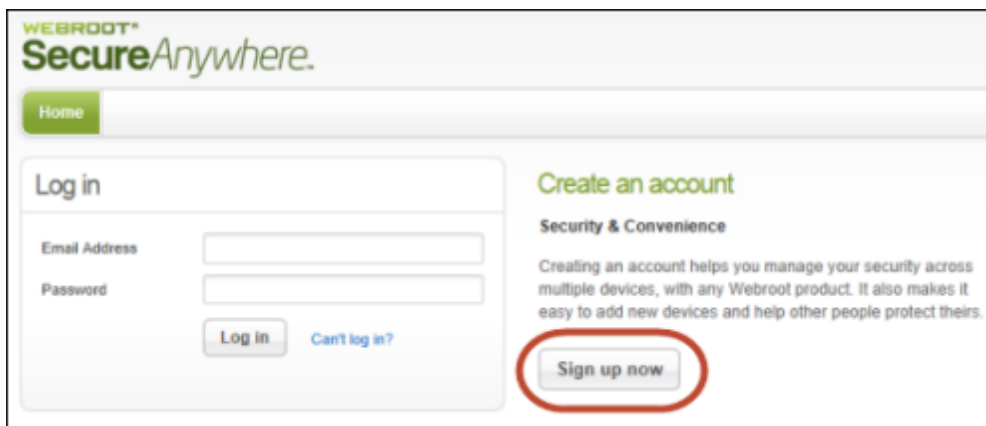
This section describes how to add a console, rename a console, and switch between consoles.

Adding a console

Before you create a console, ***you must first obtain a new keycode*** and deploy SecureAnywhere to the endpoints with that keycode. When you create the console, it will automatically discover the endpoints that use the new keycode. (If you need to migrate existing endpoints from one console to another, you must contact [Webroot Business Support](#) for assistance.)

To add a console to your account:

1. Go to the SecureAnywhere website: <https://my.webrootanywhere.com>.
2. Instead of logging in to your account, click **Sign up now**.



3. In the first field, enter the new keycode.

Create an account:

Webroot Product Keycode * (Enter new keycode here)

Email Address *

Repeat Email Address *

Password *
Strength: [Progress Bar]

Repeat Password *

Your Personal Security Code *

Security Question * [Dropdown]

Security Answer *

Register Now

4. In the remaining fields, specify your *existing* account information for the email address, password, security code, and security question and answer.
5. Click **Register Now**.
As shown in the following example, Webroot recognizes your account information and prompts you to either create a new console for the keycode or add the keycode to an existing console.

Have we seen you before?

We have recognised some of your details, and have found an existing Webroot SecureAnywhere console already owned by you.

Please Select from the following two options:

I would like a new console for this key code

What happens if I select this option?

- You will continue to login using your **original** login details.
- You can access any of your consoles under this single login.

Select

Add this key code to an existing console

How to do this:

- Log into your existing account
- Click "Manage Key Codes"
- Click the "Add Product Key Code" button
- Enter your key code into the box and press "Add"
- Your key code has now been successfully added to your existing console!

6. Click **Select** in the left panel to add a new console.
The SecureAnywhere website creates the console and prompts you to log in.
7. Log in with your account information, then choose the new "Unnamed Console." (You can rename it as described in the following section.)
Your new console shows any endpoints that use the keycode you entered.

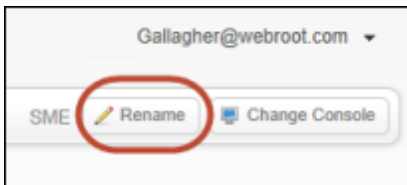
Select the Console you wish to view:

Console name	Date created	Keycodes	Devices allowed	Expired keycodes
Unnamed Console	Feb 8 2012 20:41	1	50	0
SME	Jan 12 2012 17:04	1	10	0

Renaming a console

To rename the console:

1. Click **Rename** (located below your login name in the upper right).

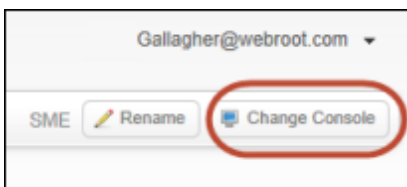


2. Enter the new name (using numbers and spaces, but not special characters), then click **Save**.

Switching consoles

To switch between consoles:

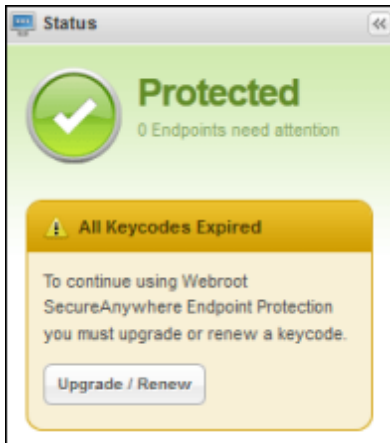
1. Click **Change Console** (located below your login name in the upper right).



2. Select the console name from the table.

Renewing or upgrading your account

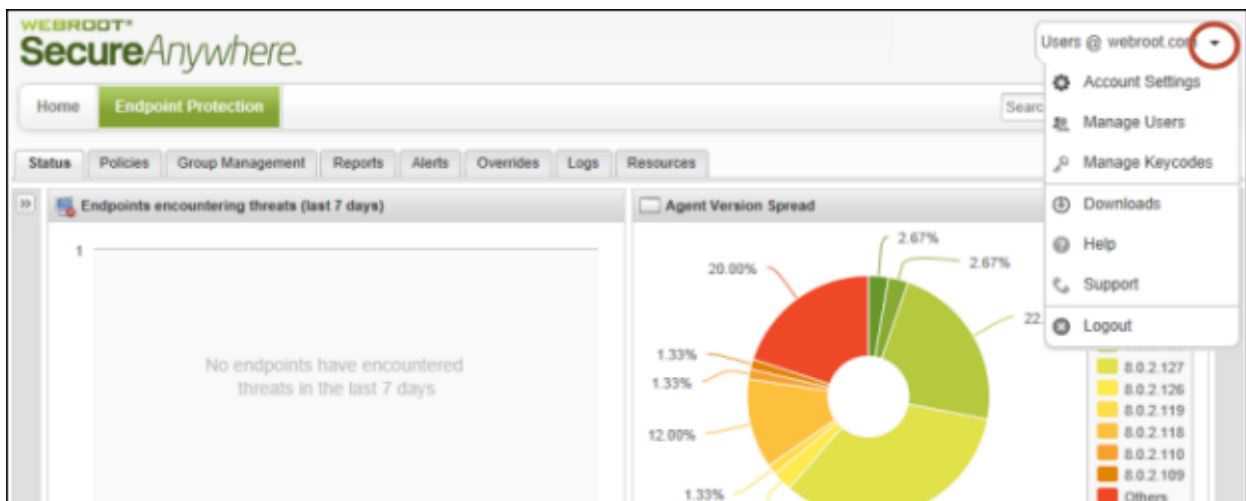
From the Management Portal, you can easily renew your Endpoint Protection license or add more seats to your license. When your license is about to expire or has already expired, you will see a warning message on the Status panel, similar to the example below:



You can click **Upgrade/Renew** from this message or you can go to the Manage Keycodes panel as described below.

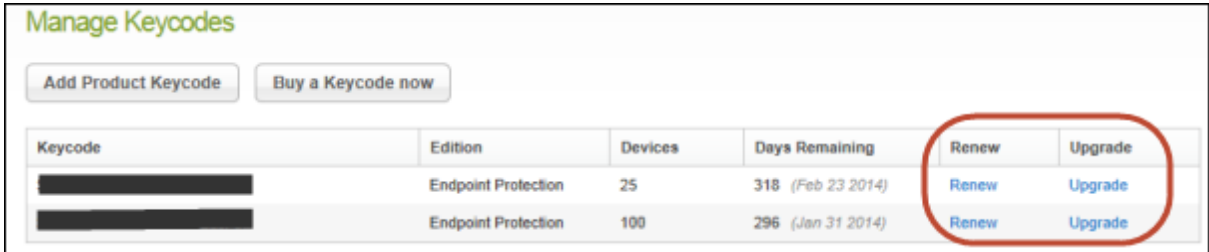
To renew or upgrade your account:

1. Open the Endpoint Protection menu by clicking the arrow next to your login ID, then click **Manage Keycodes**.



- 2. In the Manage Keycodes panel, click either **Renew** to extend your license or **Upgrade** to add more seats to your license.

Note: Your license is tied to a keycode, so select the appropriate row for the keycode you need to renew or upgrade.



Keycode	Edition	Devices	Days Remaining	Renew	Upgrade
[REDACTED]	Endpoint Protection	25	318 (Feb 23 2014)	Renew	Upgrade
[REDACTED]	Endpoint Protection	100	296 (Jan 31 2014)	Renew	Upgrade

The Webroot website opens with further instructions.

Chapter 3: Managing Endpoints

To deploy SecureAnywhere to endpoints and to manage endpoints in the portal, see the following topics:

Deploying SecureAnywhere to endpoints	50
Using the SecureAnywhere installer	52
Using MSI for deployment	57
Using GPO for deployment	58
Changing an endpoint keycode	59
Renaming endpoints	61
Searching for endpoints	62
Issuing commands to endpoints	63
Checking scan results and managing threats	69
Viewing the scan history	69
Restoring a file from quarantine	70
Setting an override for the file	71
Deactivating endpoints	73
Deactivating an endpoint	73
Reinstalling SecureAnywhere on the endpoint	74
Managing endpoint upgrades and other changes	75
Migrating to a new operating system	75
Changing hardware on an endpoint	75
Moving endpoints to a new subnet	75
Forcing immediate updates (forced polling)	76
Using SecureAnywhere on the endpoint	77
Uninstalling SecureAnywhere	79

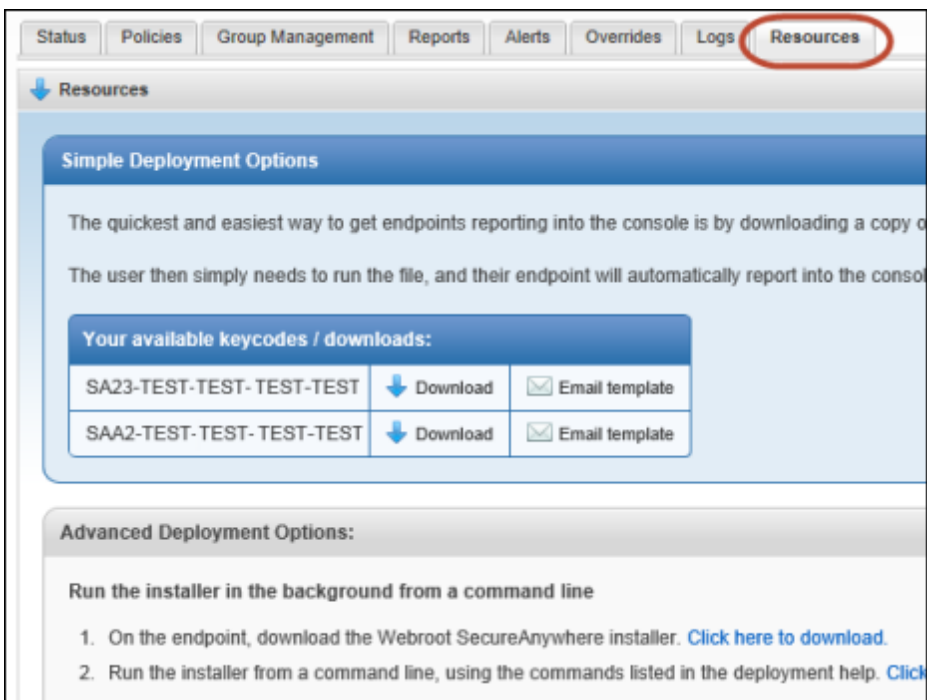
Deploying SecureAnywhere to endpoints

You can deploy SecureAnywhere to endpoints using a variety of methods, depending on your business requirements and network size. An *endpoint* can be a Windows PC, laptop, server, or virtual server installed in your network. (A list of endpoint system requirements is provided in "Preparing for setup" on page 7.)

Tip: You can configure alerts so that administrators receive notification whenever new endpoints are installed. See "Implementing alerts" on page 156.

To deploy SecureAnywhere to endpoints, follow these steps:

1. Find your keycode. If you don't know your keycode, look in the **Resources** tab of the Management Portal.



Note: Devices must use the Endpoint Protection keycode before they can report into the Management Portal. If there are endpoints in your network that already have SecureAnywhere installed with a different keycode, see "Changing an endpoint keycode" on page 59.

2. Select a method of deployment that best suits your environment. The following table describes methods of deployment.

Deployment options	
Deploy the SecureAnywhere executable file	<p>Deploy the SecureAnywhere installer file using one of these methods:</p> <ul style="list-style-type: none"> • Manually install the executable file on each endpoint. • Send emails to end users, so they can install the software by clicking on the link provided in the email template. • Rename the executable file using your keycode. (The email template also provides a renamed executable file with the keycode.) • Use additional commands with the executable file to deploy it in the background. • Use command-line options with the installer to deploy to endpoints that are behind a proxy server.
Use MSI deployment options	Deploy the SecureAnywhere installer file using the Microsoft Installer (MSI).
Use Windows Group Policy Object (GPO)	Deploy the SecureAnywhere installer file using GPO (Group Policy Object). You should have experience with Microsoft's Active Directory and the Group Policy Object editor.

Tip: If you have a small network with less than 100 endpoints, we recommend that you use the simple deployment options described in the Resources tab. If you have a large network and use Active Directory, you should use the advanced deployment options. For large networks, you may also want to organize endpoints into separate consoles for simplified views into smaller groups (see "Adding consoles to your account" on page 44).

3. Deploy SecureAnywhere to the endpoints, as described in one of these sections:
 - "Using the SecureAnywhere installer" on page 52.
 - "Using MSI for deployment" on page 57.
 - "Using GPO for deployment" on page 58.
4. Check the Management Portal to make sure the endpoints have reported their status. See "Viewing endpoint status" on page 82.
 All endpoints are first assigned to your default policy and a default group. You can change those assignments later, if desired. See "Implementing policies" on page 88 and "Applying a policy to endpoint groups" on page 124.

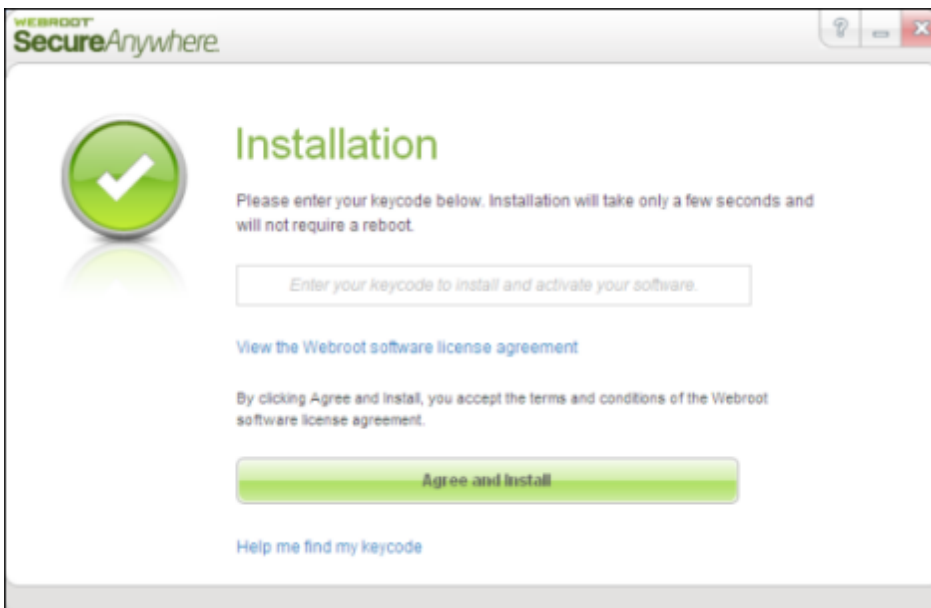
Using the SecureAnywhere installer

You can deploy the SecureAnywhere installer file using one of these methods:

- Install SecureAnywhere on each endpoint.
- Send emails to end users, so they can install the software by clicking on the link provided in the email template.
- Rename the executable file using your keycode. This method is useful if you plan to use your own deployment tool and if you prefer not to use MSI commands to run the installation in the background.
- Use additional commands with the executable file to deploy it in the background.
- Use command-line options with the installer to deploy to endpoints that are behind a proxy server.

To use the SecureAnywhere installer:

1. On the endpoint, download the SecureAnywhere installer file.
The installer file is available from the **Resources** tab or by clicking this link:
<http://anywhere.webrootcloudav.com/zerol/wsasme.exe>
2. In the installation panel (shown below), enter the keycode.
Your keycode is shown in the **Resources** tab.



3. Optionally, you can click **Change installation options** at the bottom of the installation panel and set these options:
 - **Create a shortcut to SecureAnywhere on the desktop.** This option places a shortcut icon on the Windows Desktop for SecureAnywhere.
 - **Randomize the installed filename to bypass certain infections.** This option changes the Webroot installation filename to a random name (for example, “QrXC251G.exe”), which prevents malware from detecting and blocking Webroot’s installation file.
 - **Protect the SecureAnywhere files, processes, and memory from modification.** This option enables self protection and the CAPTCHA prompts. (CAPTCHA requires you to read distorted text on the screen and enter the text in a field before performing any critical actions.)
 - **Change Language.** To change the language displayed in SecureAnywhere, click the Change Language button and select from the supported languages. (You can only change the displayed language during installation, not after.)
4. Click **Agree and Install**.
During installation, SecureAnywhere runs an immediate scan on the endpoint.

To send an email to end users so they can install SecureAnywhere themselves:

1. Click the **Resources** tab.
2. Click the **Email template** link.
The email template opens in the panel below.



3. Cut and paste the text into an email message. The link automatically adds the correct keycode for the user. Send the email to the users.
The user clicks the link to begin installation. The program installs silently in the background, with the correct keycode already entered. When it's done, a Webroot icon appears in the endpoint's system tray.

To run a background installation by renaming the executable file:

You can deploy SecureAnywhere by renaming the executable file with the keycode. This method is useful if you plan to use your own deployment tool and if you prefer not to use MSI commands to run the installation in the background. You can also use the email template (described above), which is preconfigured to include a renamed installer file with your keycode.

Note: In User Account Control environments, the account used to run the installer must have local admin rights. You must run the installer from a process that has elevated privileges in UAC environments, to prevent the end user from seeing a UAC prompt.

1. On the endpoint, download the SecureAnywhere installer file:
<http://anywhere.webrootcloudav.com/zerol/wsasme.exe>
2. Rename the installer file by replacing *wsasme* with your keycode.
The resulting file name will have this format: *XXXX-XXXX-XXXX-XXXX-XXXX.exe*
3. Install the SecureAnywhere software on your endpoints, using your own deployment tool.

To run a background installation from a command line:

1. On the endpoint, download the SecureAnywhere installer file:
<http://anywhere.webrootcloudav.com/zerol/wsasme.exe>
2. Run the installer from a command line, using any of the command options listed in the following table. (More options are available; contact [Webroot Business Support](#) for more information.)

Command line options	
<code>/key=keycode</code>	Installs with the provided keycode, with or without hyphens. For example: <code>wsasme.exe/key=xxxx-xxxx-xxxx-xxxx-xxxx</code>
<code>/silent</code>	Installs in the background.
<code>/nostart</code>	Installs without starting SecureAnywhere.

Command line options	
<code>/lockautouninstall= password</code>	<p>Allows automatic uninstallation of SecureAnywhere using the password you specify. This option is useful if you need to silently uninstall SecureAnywhere later. To uninstall, use the <code>/autouninstall</code> command.</p> <p>When you use <code>/lockautouninstall</code>, SecureAnywhere is not included in the Add/Remove Programs list in the Control Panel. Use the <code>/exeshowaddremove</code> command to include SecureAnywhere in Add/Remove Programs.</p>
<code>/autouninstall= password</code>	<p>Corresponds to <code>/lockautouninstall</code>. Example: <code>wsasme.exe/autouninstall=password</code></p> <p>By default, SecureAnywhere does not appear in the Add/Remove Programs list in the Control Panel, which prevents the user from removing the software in unmanaged mode.</p>
<code>/exeshowaddremove</code>	<p>Includes SecureAnywhere in the Control Panel Add/Remove Programs list.</p> <p>Example: <code>wsasme.exe /key=xxxx-xxxx-xxxx-xxxx /lockautouninstall=password /exeshowaddremove</code></p> <p>Note: Adding SecureAnywhere to Add/Remove Programs enables the endpoint user to remove the software in unmanaged mode.</p>
<code>/group=groupname</code>	<p>Deploys endpoints directly into a specified group. For example: <code>wsasme.exe /key=xxxxxxxx /silent /group=Sales</code></p> <p>Note: Does not support spaces or localized characters in the group name. Certain characters like “-”, “_”, or “@” are supported.</p> <p>Other requirements:</p> <ul style="list-style-type: none"> • The group must already exist in the console. • You can only use this option for new installs on systems that the console has not previously seen. • For MSI installs you must use command line and not an MSI editor.

Command line options	
<p>-proxyhost=X - proxyport=X - proxyuser=X - proxypass=X - proxyauth=#</p>	<p>Specifies proxy settings.</p> <p>Note about proxy settings: If the endpoint connects through a proxy server, SecureAnywhere will automatically detect the proxy settings. SecureAnywhere checks for changes to the proxy settings every 15 minutes and when the endpoint restarts. We recommend using auto-detection for proxy settings; however, you can use command-line options if you prefer.</p> <p>To enable proxy support, use these command-line options: wsasme.exe -proxyhost=nn.nn.nn.nn -proxyauth=<i>n</i> (where <i>n</i> can be 0=Any, 1=Basic, 2=Digest, 3=Negotiate, 4=NTLM) -proxyuser=<i>proxyuser</i> -proxypass=<i>password</i> -proxyport=<i>port_number</i></p> <p>We recommend that you use a specific value for <code>-proxyauth</code>, instead of 0 (any). The <code>any</code> option requires the endpoint to search through all authentication types, which might result in unnecessary errors on proxy servers as well as delayed communications.</p> <p>If you use this command-line option, use all parameters and blank out any value you don't need with double quotes (i.e. <code>proxypass=""</code>).</p>
<p><code>/lang=LanguageCode</code></p>	<p>Specifies the language to use for the product, rather than allow default language detection.</p> <p>Codes include:</p> <ul style="list-style-type: none"> en = English ja = Japanese es = Spanish fr = French de = German it = Italian nl = Dutch ko = Korean zh-cn = Simplified Chinese pt = Brazilian Portuguese ru = Russian tr = Turkish zh-tw = Traditional Chinese <p>Example: <code>wsasme.exe /key=xxxxxxxxxxxxx /silent /lang=ru</code></p>

Using MSI for deployment

The Microsoft Installer (MSI) requires commands during installation, which apply the keycode and options that activate Endpoint Protection installation mode. The MSI installer is interactive by default, and requires the `msiexec.exe` option `/qn` to run an automated installation in the background. This is an example of an MSI command: `msiexec /i wsasme.msi GUILIC=licensekey CMDLINE=SME,quiet /qn /l*v install.log`.

Note: In User Account Control environments, the account used to run the installer must have local admin rights. You must run the installer from a process that has elevated privileges in UAC environments, to prevent the endpoint user from seeing a UAC prompt.

To remove SecureAnywhere later (if desired):

If you need to remove the SecureAnywhere software from the endpoint later, use the standard MSI command:

```
msiexec /x wsasme.msi /qn /L*v uninstall.log
```

To use an MSI editor:

If you use your own methods to deploy the SecureAnywhere software on endpoints, see the following table for commands you can pass to **msiexec.exe** during installation.

CMDLINE	SME,quiet
GUILIC	The license key, with or without hyphens. Note: If you don't provide a keycode, the installation will continue; however, the endpoint will not have a keycode associated with it and will not be protected. If you install without a keycode, you must uninstall the software and re-install to add it.

You can also modify these commands directly, using an MSI editor such as ORCA:

- Set the CMDLINE property in the Property table to the appropriate value.
- Set the GUILIC property in the Property table to your keycode.

Using GPO for deployment

To install SecureAnywhere using GPO (Group Policy Object), you should have experience with Microsoft's Active Directory and the Group Policy Object editor.

You can also watch a video for using GPO at:

[How to Deploy Using Group Policy - Webroot SecureAnywhere Business](#)

To install SecureAnywhere using GPO:

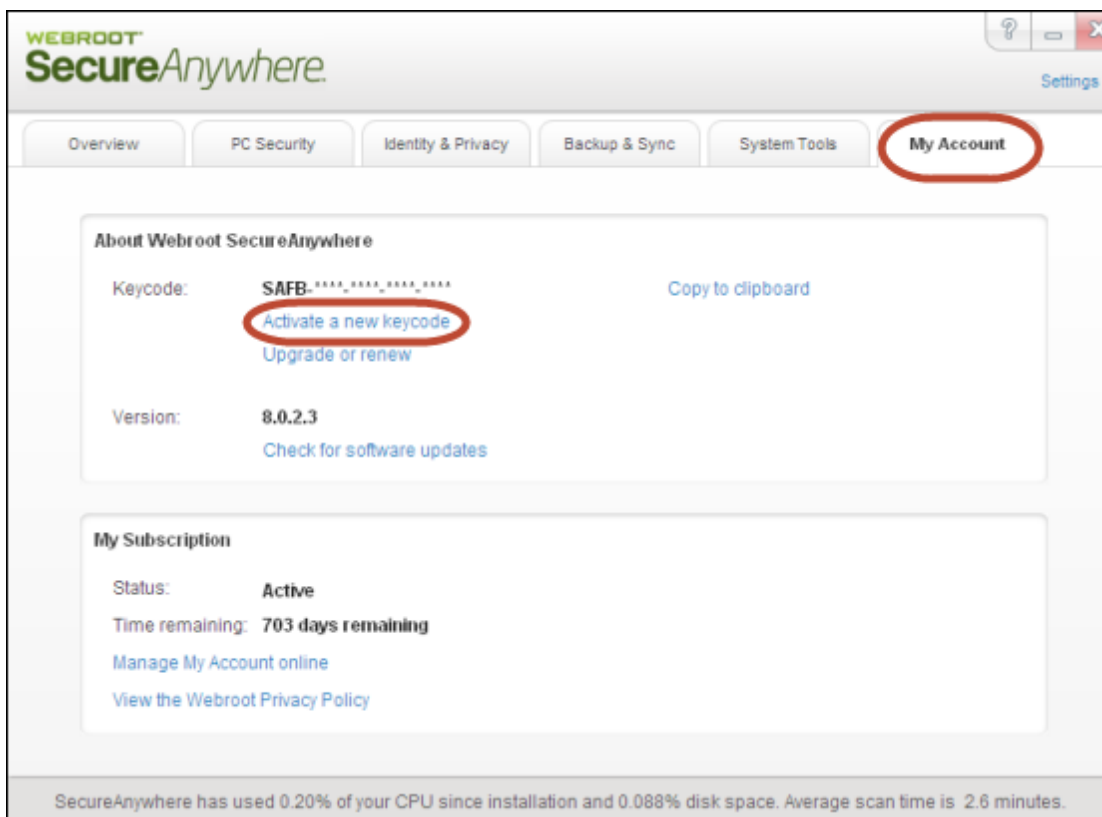
1. Download the SecureAnywhere MSI installer to a network share:
<http://anywhere.webrootcloudav.com/zerol/wsasme.msi>
Downloading the file makes it accessible to all endpoints on which you will deploy SecureAnywhere.
2. Go to the server that is the domain controller for the deployment group.
3. Open the GPO editor on the domain controller and create a policy for the deployment group.
4. Assign SecureAnywhere to all endpoints that belong to the Organizational Unit where the Group Policy is created.
SecureAnywhere installs on the endpoints in the group when they restart.

Changing an endpoint keycode

Endpoints must use the Endpoint Protection keycode before they can report into the Management Portal. If there are endpoints in your network that already have SecureAnywhere installed with a different type of keycode (for example, a Consumer version of SecureAnywhere), change the keycode either by issuing a Change Keycode command (see "Issuing commands to endpoints" on page 63) or by activating a new keycode directly from the endpoint, as described below.

To change a keycode on an endpoint:

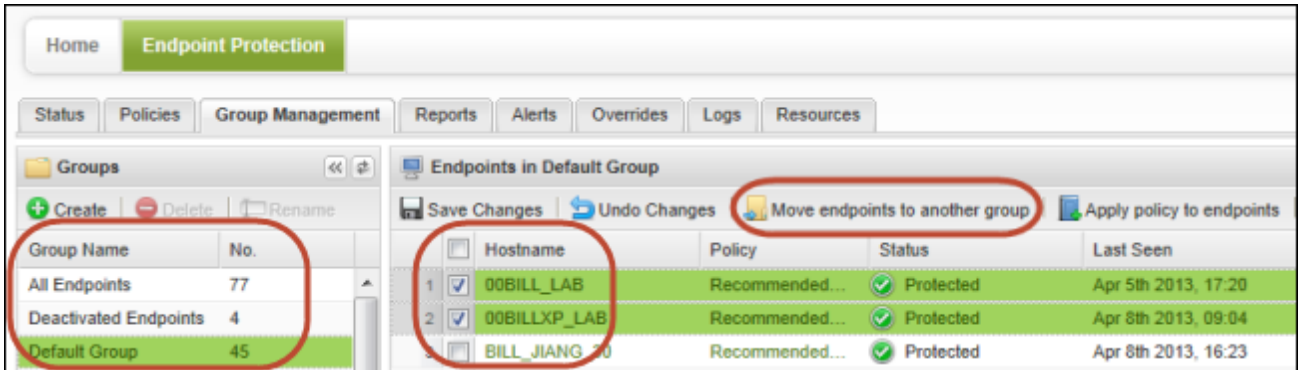
1. From the endpoint, open SecureAnywhere by double-clicking the Webroot icon in the system tray.
2. Click the **My Account** tab.
3. Click **Activate a new keycode**, as shown in the following example.



4. In the dialog, enter your Endpoint Protection keycode and click the **Activate** button. When you enter a new keycode, SecureAnywhere launches a scan. (If it does not launch a scan

automatically, go to the **PC Security** tab, then click **Scan My Computer**.) When the scan completes, SecureAnywhere reports into the Management Portal.

5. Return to the Management Portal and look for the new endpoint in the Default group. If desired, you can reassign the endpoint to another group. See "Moving endpoints to another group" on page 127.



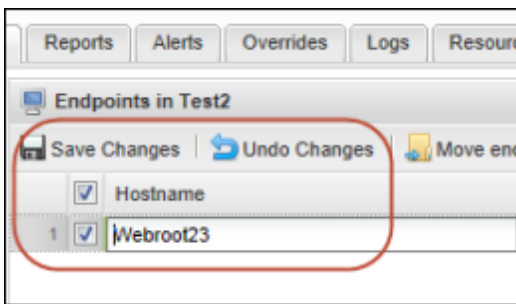
Renaming endpoints

When you add an endpoint, SecureAnywhere identifies it in the Management Portal by its machine name. You might want to change the machine name to something more meaningful, such as "Gallagher-Laptop" or "LabTest-1."

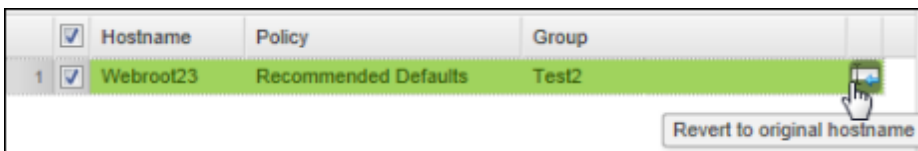
Note: Do not change the name of an endpoint on a *virtual* machine. If you do, it will appear as a new endpoint in the Management Portal and will use an extra seat in your license.

To rename an endpoint:

1. Click the **Group Management** tab.
2. From the **Groups** panel on the left, select the group that contains the desired endpoint.
3. From the **Endpoints** panel on the right, double-click on the endpoint name (in the **Hostname** column).

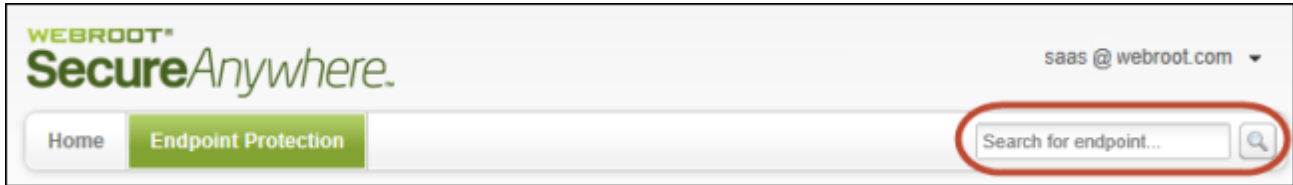


4. Enter the new name and press the **Enter** key.
A red flag appears in the upper left of the field to indicate that the change is not yet saved.
5. Click **Save Changes** from the command row.
The new name appears in the Hostname column.
6. If you decide later to revert to the original name, you can click the **Revert** button on the far right of the row.



Searching for endpoints

You can search for a specific endpoint from the field in the upper right of the Management Portal. This field is accessible from any area of the portal. Enter a full or partial endpoint name (case-insensitive) and click the magnifying glass search icon.



The Management Portal displays all endpoints matching the search criteria in the bottom panel.

Issuing commands to endpoints

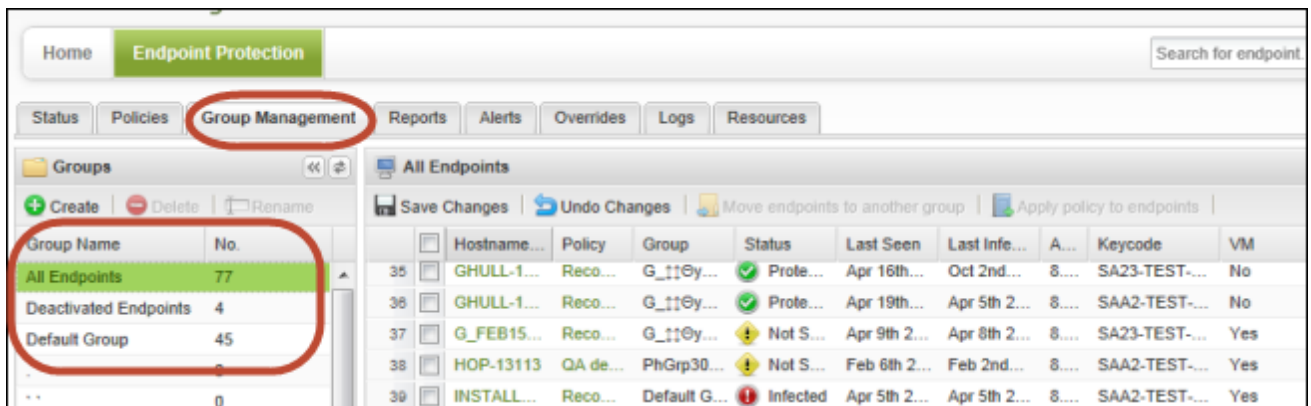
From the Management Portal, you can issue commands to individual endpoints or to a group of endpoints. For example, you might want to scan an endpoint at a remote location. With these commands, you can easily run all the same commands that are available on the endpoint's SecureAnywhere software.

Be aware that the endpoint may not receive the command until the next polling interval. If necessary, you can change the polling interval in its associated policy (see "Changing policy settings" on page 92) or you can force an immediate polling, as described in "Forcing immediate updates (forced polling)" on page 76.

Note: Depending on your access permissions for Commands (**Simple**, **Advanced**, or **Expert**), you may not see all the commands listed in this section. Administrators can change access permissions, as described in "Setting permissions for portal users" on page 38.

To issue commands to endpoints:

1. Click the **Group Management** tab.
2. From the **Groups** panel on the left, select the group that contains the desired endpoints.

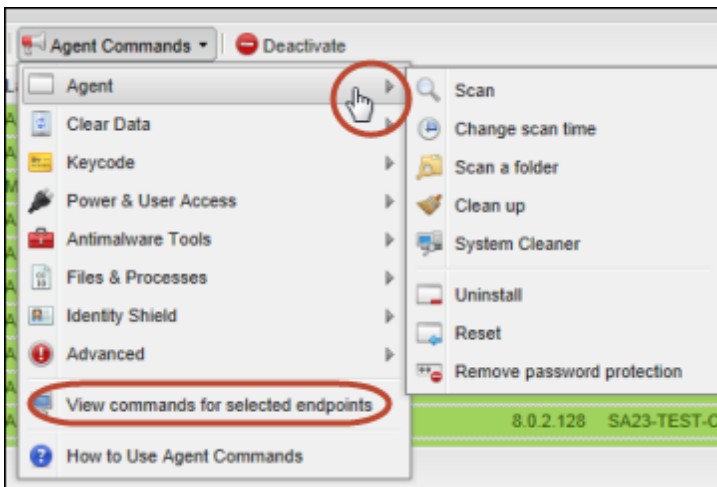


3. From the **Endpoints** panel on the right, select one or more endpoints.
Tip: You can select all endpoints within the group by clicking the **Hostname** checkbox at the top of the list (first column).

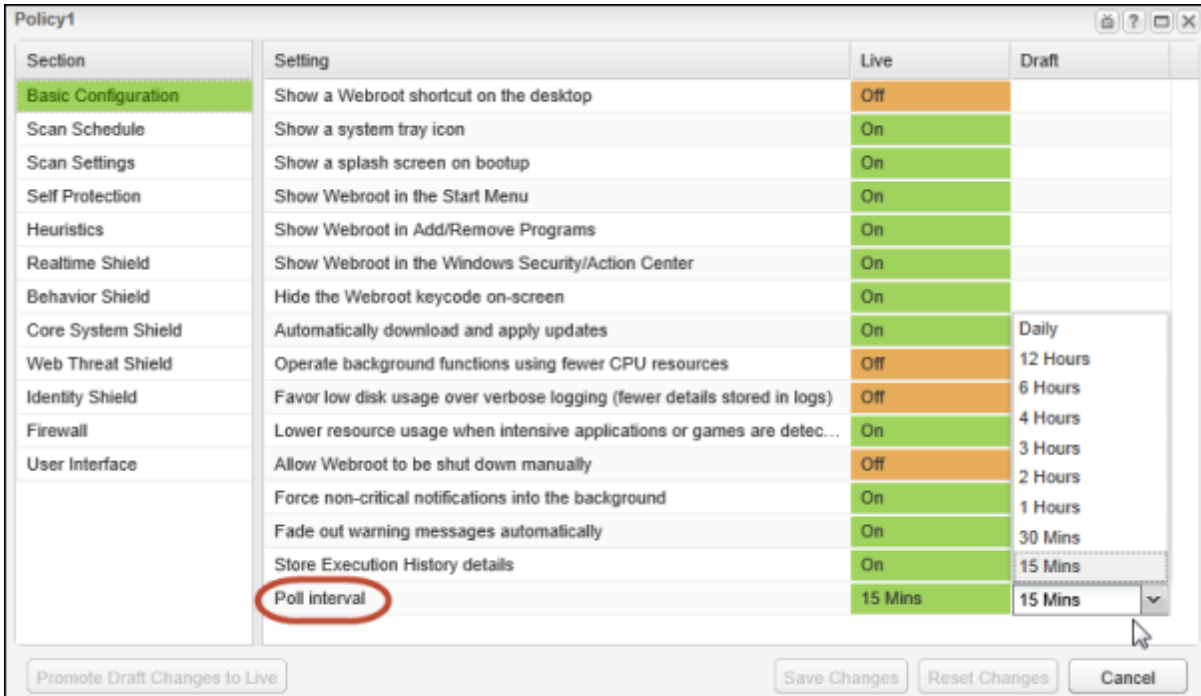
- 4. Click **Agent Commands** from the command bar.



- 5. From the dialog that opens, select a category of agent commands and then a command to run. For a description of each command, see the tables following these steps.
- 6. To see the status of commands you sent, you can click **View commands for selected endpoints** near the bottom of the menu. You can also review the Command Log on the **Logs** tab.



Endpoint Protection will issue the commands on the next polling interval. If necessary, you can either change the polling interval in **Basic Configuration** of the group's policy (see the following example) or you can force the changes immediately as described in "Forcing immediate updates (forced polling)" on page 76.



The following tables describe each of the endpoint commands:

Agent commands	
Scan	Run a Deep scan in the background as soon as the endpoint receives the command. When the scan completes, the Scan History panel shows the results for a Deep scan. Be aware that any detected threats are not automatically quarantined. You must take action yourself in the portal by running a Clean-up or by creating an override.
Change scan time	Select a new time of day to scan the endpoint. By default, SecureAnywhere runs a scan every day at about the same time it was installed. For example, if you installed SecureAnywhere on the endpoint at noon, a scan will always run around 12 p.m. With this command, you can change it to a different hour.
Scan a folder	Runs a full, file-by-file scan on a specific folder. Be sure to enter the full path name. For example: C:\Documents and Settings\Administrator\My Documents\ When the scan completes, the Scan History panel shows results for the Custom/Right Click Scan .

Agent commands	
Clean up	Start a scan and automatically quarantine malicious files. When the scan completes, the Scan History panel shows results for the Post Cleanup Scan .
System Cleaner	Run the System Cleaner on the endpoint, which removes all traces of web browsing history, files that reveal the user's activity, and files that consume valuable disk space (files in the Recycle Bin and Windows temp files). You can change the System Cleaner options in the Policy settings.
Uninstall	Uninstall SecureAnywhere from the endpoint. With this command, the endpoint is still shown in the Management Portal. If you want to uninstall SecureAnywhere and free up a seat in your license, deactivate the endpoint instead. See "Deactivating endpoints" on page 73 .
Reset	Return SecureAnywhere settings on the endpoint to their default values.
Remove password protection	Disable password protection from the endpoint user's control, which allows administrators to gain access to the endpoint if they are locked out.

Clear Data commands	
Clear files	Erase current log files, which frees space on the endpoint.
Disable proxy settings	Disable any proxy settings the endpoint user set on the endpoint. Note: Do not use this command if the endpoint's only Internet access is through the proxy server. The endpoint will no longer be able to communicate with the cloud.

Keycode commands	
Change keycode	Enter a different keycode. Note: The drop-down list shows only keycodes that are assigned to this console.
Change keycode temporarily	Switch the keycode used for this endpoint temporarily, which might be necessary for testing purposes. In the dialog box, choose a keycode from the drop-down list, then specify the dates for SecureAnywhere to use it. When the specified time for the change elapses, the keycode reverts to the original.

Power & User Access commands	
Lock endpoint	Lock this endpoint by activating the Windows Login screen. The user must enter a user name and password to log back in.
Log off	Log the user out of the account.
Restart	Restart this endpoint when it reports in.
Reboot in Safe Mode with Networking	Restart this endpoint in Safe Mode with Networking.
Shutdown	Shut down this endpoint when it reports in.

Antimalware Tools commands	
Reset desktop wallpaper	Reset the desktop wallpaper to the default settings, which might be necessary if the endpoint was recently infected with malware that changed it. After sending this command, the user must restart the endpoint.
Reset screen saver	Reset the screen saver to the default settings, which might be necessary if the endpoint was recently infected with malware that changed it.
Reset system policies	Reset the Windows system policies, which might be necessary if the endpoint was recently infected with malware that changed such policies as the Task Manager settings. Note: This command resets Windows policies, not Endpoint Protection policies.
Restore file	Restores a quarantined file to its original location, using its MD5 value. For more information about how to locate a file's MD5 value, see " Applying overrides from the Overrides tab " on page 167.

File & Processes commands	
Reverify all files and processes	Re-verify this file's classification when the next scan runs. This command is useful if you have established some overrides and need them to take effect on an endpoint.
Consider all items as good	Consider all detected files on this endpoint as safe to run. This command is useful if you find numerous false positives on an endpoint and need to quickly tag them as "Good."
Allow processes blocked by firewall	Allow communication for all processes that are blocked by the Firewall setting.
Stop untrusted processes	Terminate any untrusted processes, which might be necessary if a regular scan did not remove all traces of a malware program. The processes stop immediately, but are not prevented from running again later.

Identity Shield commands	
Allow application	Allow an application to run on the endpoint. To identify the application, you must enter its MD5 value. (To determine an MD5 value, see "Applying overrides from the Overrides tab" on page 167.)
Deny application	Block an application from running on the endpoint. To identify the application, you must enter its MD5 value. (To determine an MD5 value, see "Applying overrides from the Overrides tab" on page 167.)
Allow all denied applications	Re-set all applications previously blocked, so they can run on the endpoint.
Protect an application	Add extra security to an application running on the endpoint. To identify the application, you must enter its MD5 value. (To determine an MD5 value, see "Applying overrides from the Overrides tab" on page 167.)
Unprotect an application	Re-set the application to standard protection, if you previously used the Protect an application command to add extra security. To identify the application, you must enter its MD5 value. (To determine an MD5 value, see "Applying overrides from the Overrides tab" on page 167.)

Advanced commands	
Run Customer Support script	Run a clean-up script on the endpoint to remove malware infections. You must specify a network path to the file.
Customer Support Diagnostics	Run the WSABLogs utility to gather information about an infected endpoint. The Customer Support Diagnostics dialog shows the location of the utility's executable file, and the email address associated with the endpoint account. Clicking Submit runs the utility and sends the results to Webroot Business support. You can specify optional advanced settings to send an additional file, to save the log locally instead of sending it, and gather a memory dump.
Download and run a file	Specify a file's direct URL to download it to the agent, and then run it remotely at the system level. You can also enter command-line options; for example, you could specify the /s parameter so that the file you download runs silently in the background. Command-line options must be supported by the file you are downloading and executing.
Run a DOS command	Specify the DOS command to run remotely at the system level, which is useful for simple changes or for running a script. Keep in mind that the Management Portal will not display results.
Run a registry command	Specify the registry command to run remotely at the system level. This command uses the same syntax as reg.exe, but does not call reg.exe. You can only refer directly to local registry hive paths (for example, HKLM\Software\). You cannot include the name of the computer in the path.

Checking scan results and managing threats

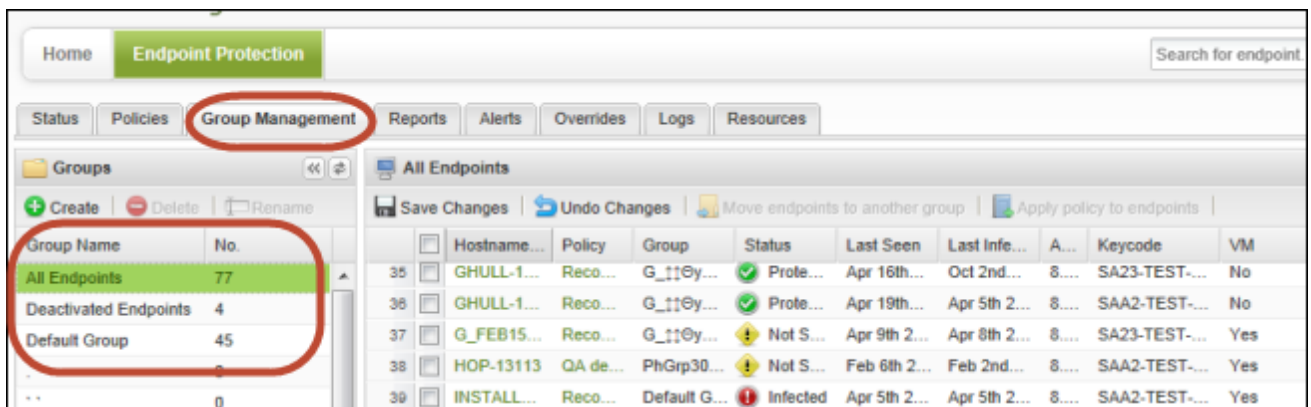
From Group Management, you can view the scan history of endpoints and manage any detected threats. You can restore a file from quarantine if you know it is legitimate (see "Restoring a file from quarantine" on page 70). You can also reclassify a file as "Good" (allowed to run) or "Bad" (auto-quarantined), as described in "Setting an override for the file" on page 71.

Viewing the scan history

You can view a scan history for endpoints from the Group Management panel, which helps you determine where threats were found.

To view the scan history:

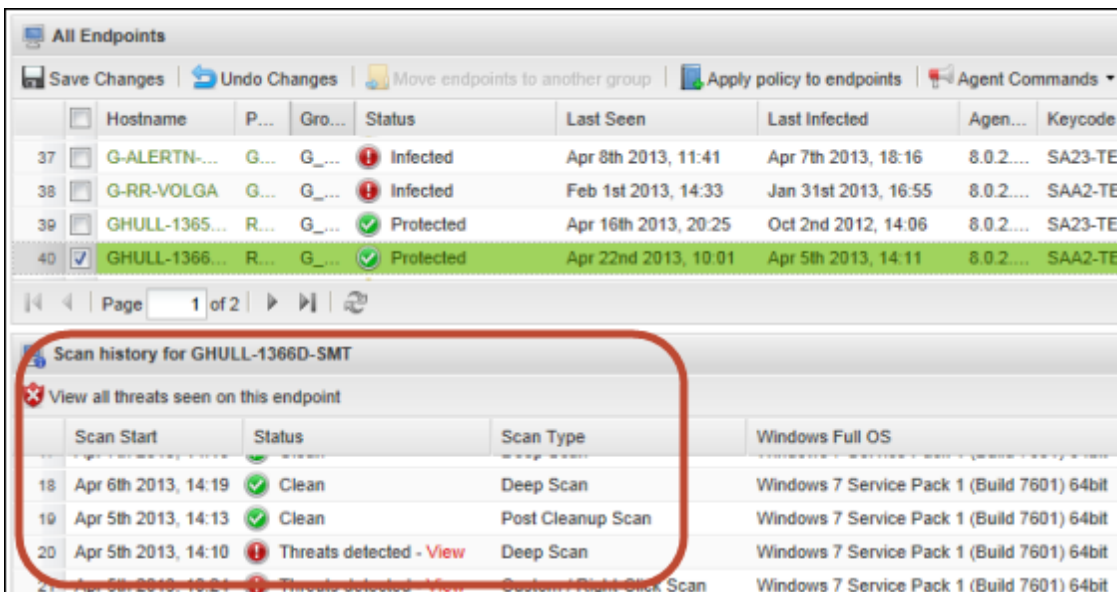
1. Click the **Group Management** tab.
2. From the **Groups** panel on the left, select a group with the desired endpoints.



3. From the **Endpoints** panel on the right, select one of the endpoints as shown in the following example. The Scan History panel opens, showing scan activity and any threats detected on the endpoint.

Note: If the pathname where a threat was identified includes a drive letter, the letter is masked with a question mark. For example, you might see a pathname that looks similar to the following:

?:\users\user1\desktop.



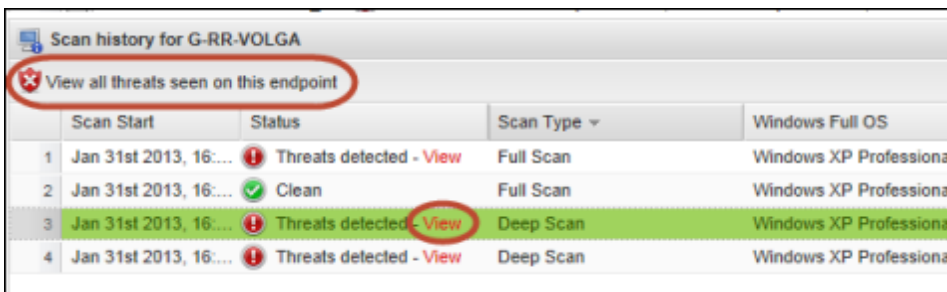
4. If desired, you can show or hide additional data about the endpoint and the scan history. Click a column header to open the drop-down menu, then click in the checkboxes to select the columns to add or remove. For descriptions of the data in the columns, see "Sorting data in tables and reports" on page 26.

Restoring a file from quarantine

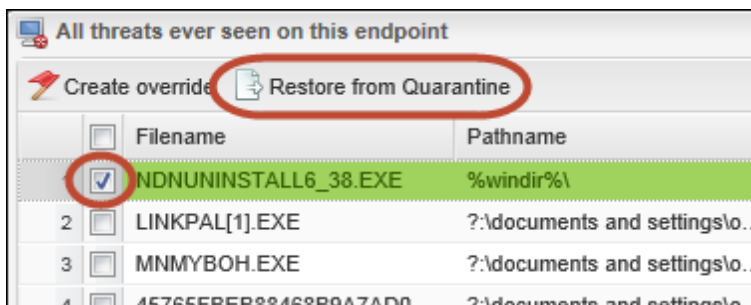
You can restore a file from quarantine from the Scan History panel (as described below) or from the All Threats Seen report (see "Generating the All Threats Seen report" on page 139). The file is automatically returned to its original location on the endpoint.

To restore a file:

1. View the scan history for a particular endpoint, as described previously in this section.
2. In the Scan History panel, locate the file by either clicking **View** in the Status column for the date when the threat was detected or by clicking **View all threats seen on this endpoint**.



3. In the dialog that opens, select a file by clicking on its checkbox.
4. Click **Restore from Quarantine**.



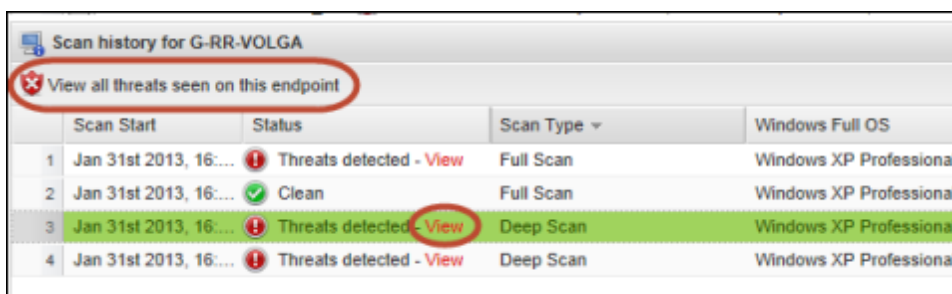
The file returns to its original location on the endpoint.

Setting an override for the file

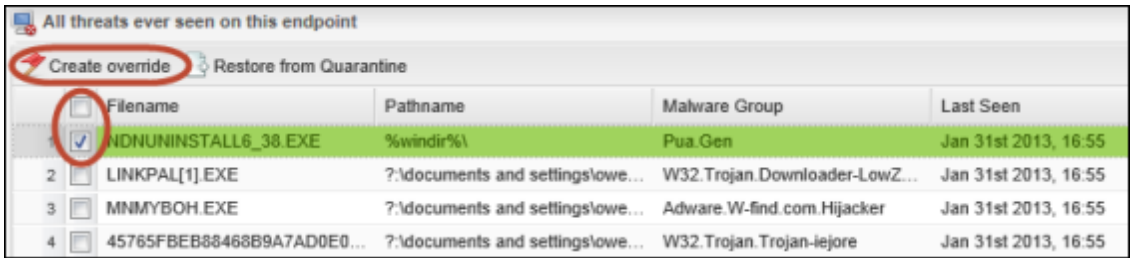
You can set an override for a file from the Scan History panel (as described below) or from the Overrides tab (see "Applying overrides from the Overrides tab" on page 167).

To set an override:

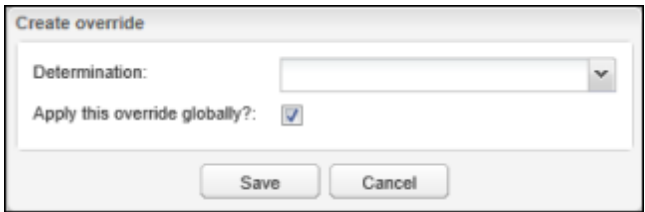
1. View the scan history for a particular endpoint, as described previously in this section.
2. In the **Scan History** panel, locate the file by either clicking **View** in the Status column for the date when the threat was detected or by clicking **View all threats seen on this endpoint**.



3. In the dialog that opens, select a file in the list.
4. Click **Create override**.



The following dialog opens:



5. Open the **Determination** drop-down menu by clicking the arrow to the right of the field. Select one of the following:
 - **Good**: Always allow the file to run.
 - **Bad**: Always send the file to quarantine.
6. You can apply this override globally or to an individual policy, as follows:
 - To apply the override to all policies, keep the **Apply the override globally** checkbox selected.
 - To select an individual policy for the override, deselect the checkbox. When the **Policy** field appears, click the drop-down arrow to the right of the field and select a policy.

Deactivating endpoints

You can deactivate an endpoint so that it no longer reports in to Endpoint Protection. (You can reactivate an endpoint later, if necessary.) By deactivating an endpoint, you can free the license seat so you can install another endpoint in its place.

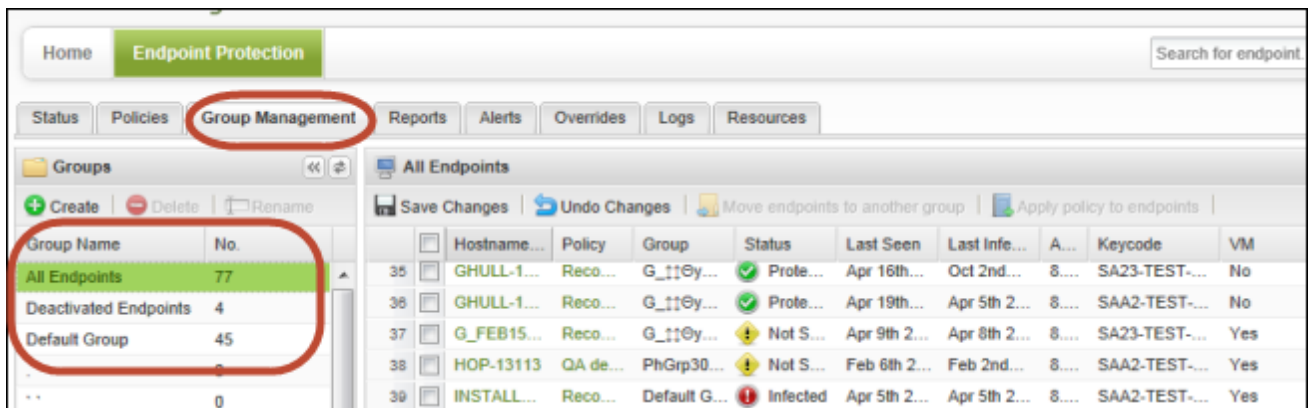
Note: If you don't want to deactivate the endpoint from the Management Portal, you can send an **Uninstall** command to the endpoint instead. This action retains the endpoint entry in the Management Portal (although it displays as "not seen" after 7 days). See "Issuing commands to endpoints" on page 63.

Deactivating an endpoint

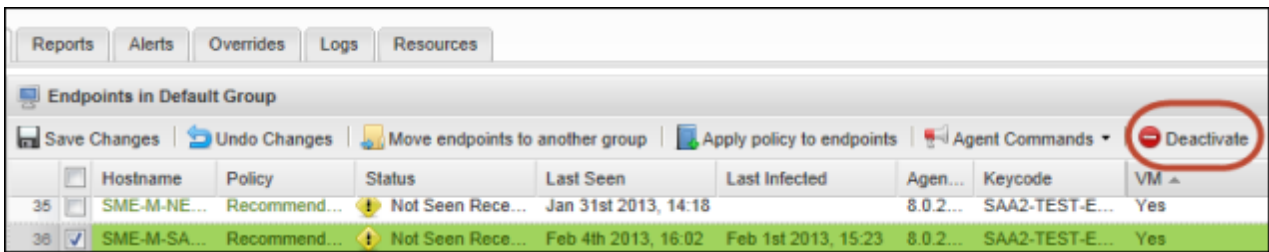
Deactivation sends an Uninstall command to the endpoint and removes the endpoint entry from the Management Portal.

To deactivate an endpoint:

1. Click the **Group Management** tab.
2. From the **Groups** panel on the left, select a group that includes the desired endpoints.



3. Select one or more endpoints and click **Deactivate** from the command bar.



A dialog warns you that a deactivated endpoint will no longer be able to report to Endpoint Protection.

4. Click **Yes** to send an Uninstall command to the endpoint, so that it removes SecureAnywhere. Once SecureAnywhere is removed, the endpoint is shown in the Deactivated Endpoints group. After 7 days, the status changes to "Not Seen Recently."

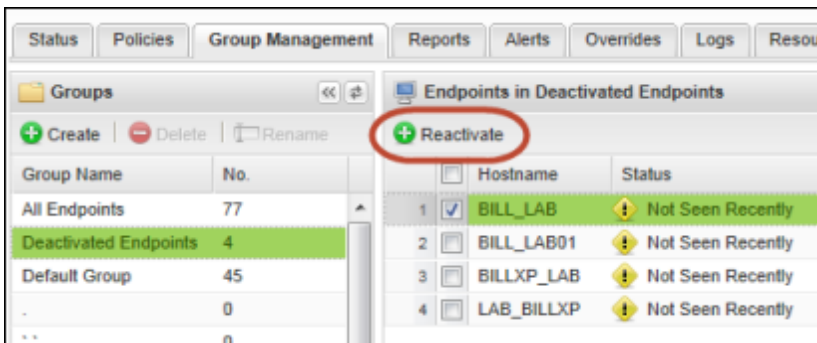
Note: You cannot permanently remove endpoints from the Deactivated Endpoints group yourself. Contact [Webroot Technical Support](#) if you need to clean up this list and remove old items.

Reinstalling SecureAnywhere on the endpoint

If you deactivate an endpoint from the Group Management tab, you can reactivate it later if necessary.

To reactivate the endpoint:

1. Reinstall SecureAnywhere on the endpoint.
2. Open the Management Portal and click the **Group Management** tab.
3. Select the endpoint from the **Deactivated Endpoints** group.
4. Click **Reactivate** from the command bar.



The endpoint is then moved back into its former group.

Managing endpoint upgrades and other changes

This section describes some special circumstances you may encounter when you change hardware and operating systems on endpoints.

Migrating to a new operating system

If you install a new operating system on an endpoint, the change will create duplicate endpoint entries in the Management Portal. Before you install a new operating system, you should deactivate the endpoint. See "Deactivating endpoints" on page 73.

If you have already performed the OS installation, you can simply deactivate the oldest entry in the Management Portal. The extra license is then removed and the duplicate endpoint is placed in the Deactivated Endpoints group.

Note: In most cases, a simple upgrade to an operating system will not create duplicate entries.

Changing hardware on an endpoint

If you install a new hard drive in an endpoint and reinstall SecureAnywhere on it, it will appear as a new entry in the Management Portal. Before you switch out a hard drive, you should first deactivate the endpoint from the Management Portal so you do not use an extra license. See "Deactivating endpoints" on page 73.

If you change other types of hardware on an endpoint (for example, you install a new motherboard, processor, or network adaptor), that upgraded computer will *not* appear as a new entry in the Management Portal. You do not need to deactivate the endpoint first.

Moving endpoints to a new subnet

If you move endpoints to a new subnet, make sure the same communication lines are open as on the previous subnet. These domains should be allowed through the firewall:

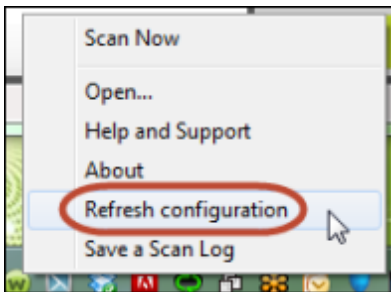
- *.webrootcloudav.com
- *.*.webrootcloudav.com
- *.p4.webrootcloudav.com
- *.compute.amazonaws.com
- *.webroot.com
- *.webrootanywhere.com
- *.prevx.com

Forcing immediate updates (forced polling)

The polling interval determines how often the endpoint sends its status and receives commands (for example, every 15 minutes or every hour). If necessary, you can change the polling interval in **Basic Configuration** of the group's policy (see "Changing policy settings" on page 92) or you can force an immediate update as described below.

To force an update:

1. Go to the endpoint and look for the Webroot icon in the system tray.
2. Right-click on the Webroot icon.
3. Click **Refresh configuration**.



Using SecureAnywhere on the endpoint

On occasion, you may need to access an endpoint to change settings in the SecureAnywhere interface. This might be necessary if you assign an endpoint to the Unmanaged policy, which is not controlled through the Management Portal.

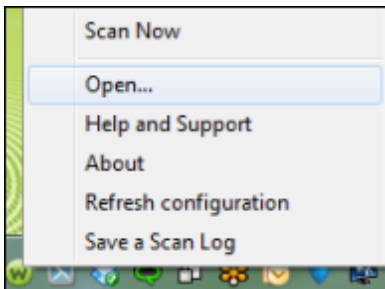
Note: For complete instructions on using the SecureAnywhere interface on the endpoint, see [SecureAnywhere User Guide for PCs](#) or the [Webroot SecureAnywhere for PCs Online Help](#).

To open the SecureAnywhere main interface, go to the endpoint and do one of the following:

- Double-click the Webroot shortcut icon on the desktop:



- Right-click on the Webroot icon  from the system tray menu, then click **Open**.



- If the system tray icon is hidden, open the Windows **Start** menu, click **All Programs** (or **Programs**), **Webroot SecureAnywhere**, then **Webroot SecureAnywhere** again.

The Overview panel opens, similar to the following example.



Along the top of the panel, the main interface includes navigation tabs.

Main Interface tabs	
Overview	View the system status and manually scan the computer.
PC Security	Run custom scans, change shield settings, and manage the quarantine.
Identity & Privacy	Protect sensitive data that may be exposed during online transactions.
System Tools	Use tools to manage processes and files, view reports, and submit a file to Webroot Support. Also use the System Cleaner to remove Internet browser activity and to remove temp files.
My Account	View SecureAnywhere account information and check for updates.

Uninstalling SecureAnywhere

You can remove the SecureAnywhere program from an endpoint by using one of the following methods:

- Deactivate an endpoint so that it no longer reports in to Endpoint Protection. (You can reactivate an endpoint later, if necessary.) By deactivating an endpoint, you can free the license seat so you can install another endpoint in its place. See "Deactivating endpoints" on page 73.
- Send an **Uninstall** command to the endpoint from the Management Portal. See "Issuing commands to endpoints" on page 63. Be aware that by using this method, the endpoint is still shown in the Management Portal. If you want to uninstall SecureAnywhere and free up a seat in your license, deactivate the endpoint instead.

Chapter 4: Checking Status

To learn more about the Status panel, see the following topics:

Viewing endpoint status	82
Viewing recent threat status	84
Viewing an agent version overview	85

Viewing endpoint status

You can see the status of all endpoints in the Management Portal. Endpoints report their status when SecureAnywhere runs a scan on them or when a polling interval has completed.

Note: To see more detailed information about an endpoint's scan history, see "Checking scan results and managing threats" on page 69.

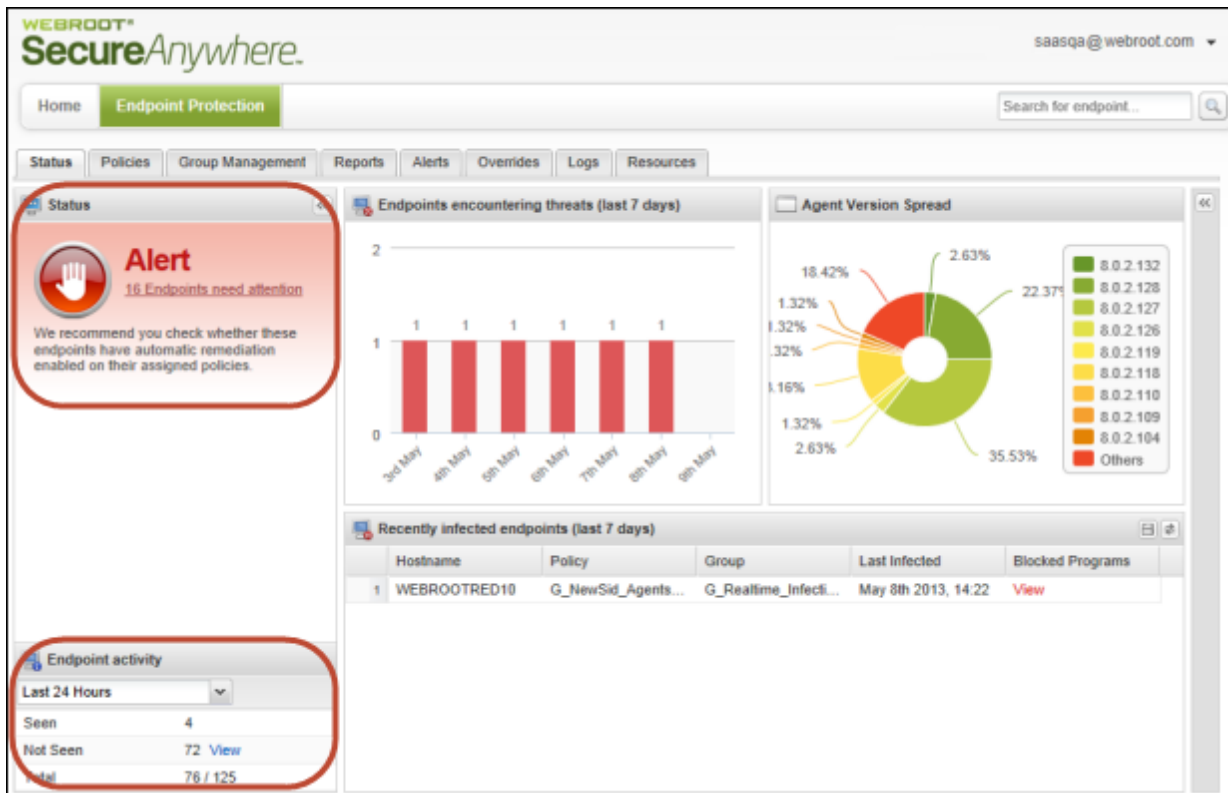
To view endpoint status:

1. Log in to the SecureAnywhere website: <https://my.webrootanywhere.com>.
2. Click **Go to Endpoint Protection**.

If any endpoints are infected, you can click a link for those endpoints to go directly to a details panel.



When the Management Portal opens, you can see the endpoint status in the left panels for **Status** (top) and **Endpoint activity** (bottom).



You can drill down for more detail in both of these panels:

- If you see an alert message in the top panel, click the link to see more information about the endpoints.
- If any endpoints have not reported into the portal (Not Seen), click the **View** link in the **Endpoint activity** panel.

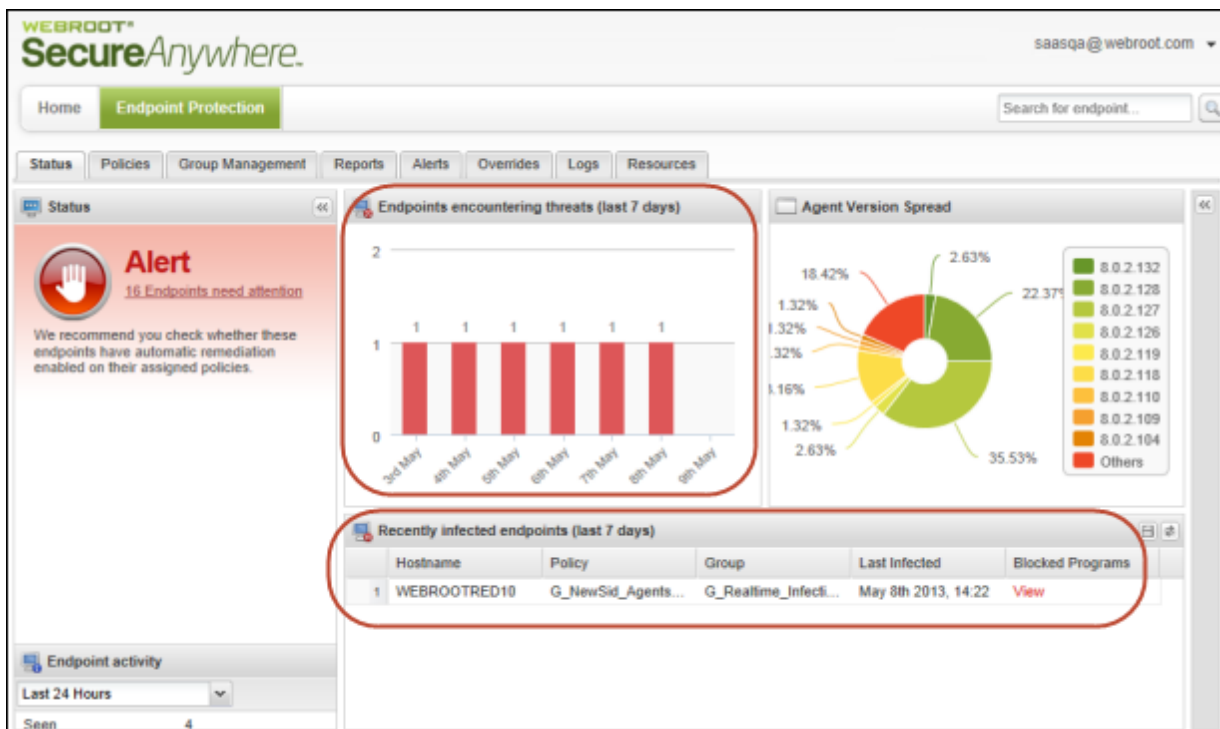
You can see endpoints in the Status tab (home panel) and the Group Management tab. The Group Management tab provides more detailed information (see "Organizing endpoints into groups" on page 120).

Viewing recent threat status

From the Status tab, you can quickly view endpoints that reported a threat in the past week.

To view endpoints encountering threats in the past week:

1. Make sure the **Status** tab is selected.
The bar chart at the top shows a daily summary of threats found on endpoints. The table at the bottom of the panel shows more details about the endpoints.



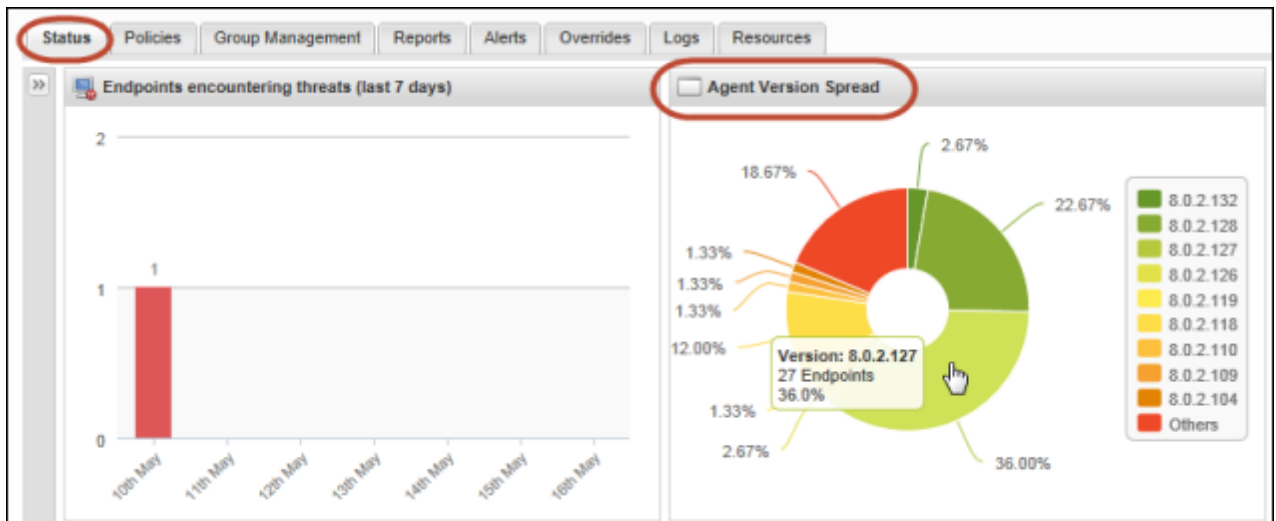
2. To learn more about a threat, locate the threat in the row and click the **View** link in the **Blocked Programs** column.
3. If desired, you can show or hide additional data about the recently infected endpoints in the bottom panel. Click a column header to open the drop-down menu, then click in the checkboxes to select the columns to add or remove. For descriptions of the data in the columns, see "Sorting data in tables and reports" on page 26.
4. For more details about threats and further options, you can generate the **Endpoints with Threats on Last Scan** report. From this report, you can change the endpoint's policy, run a scan, create an override for a file, or restore a file from quarantine. See "Generating the Endpoints with Threats on Last Scan report" on page 143.

Viewing an agent version overview

The Agent Version Spread pie chart on the Status tab shows a high-level overview of the SecureAnywhere versions installed on endpoints. (An *agent* is the SecureAnywhere software running on the endpoint.)

To view the Agent Version Spread pie chart:

1. Make sure the **Status** tab is selected.
The Agent Version Spread chart is located on the right.
2. To see more details, move your cursor over sections of the pie chart.



3. For more details, see "Generating the Agent Version Spread report" on page 134.

Chapter 5: Managing Policies

To manage policies, see the following topics:

Implementing policies	88
Selecting a new default policy	89
Creating policies	90
Creating a new policy	90
Copying a policy	91
Changing policy settings	92
Basic Configuration	95
Scan Schedule	97
Scan Settings	98
Self Protection	99
Heuristics	100
Realtime Shield	103
Behavior Shield	104
Core System Shield	105
Web Threat Shield	106
Identity Shield	107
Firewall	108
User Interface	109
System Cleaner	109
Renaming a policy	114
Exporting policy settings to a spreadsheet	115
Deleting policies	116
Viewing endpoints assigned to a policy	117
Moving endpoints to another policy	118

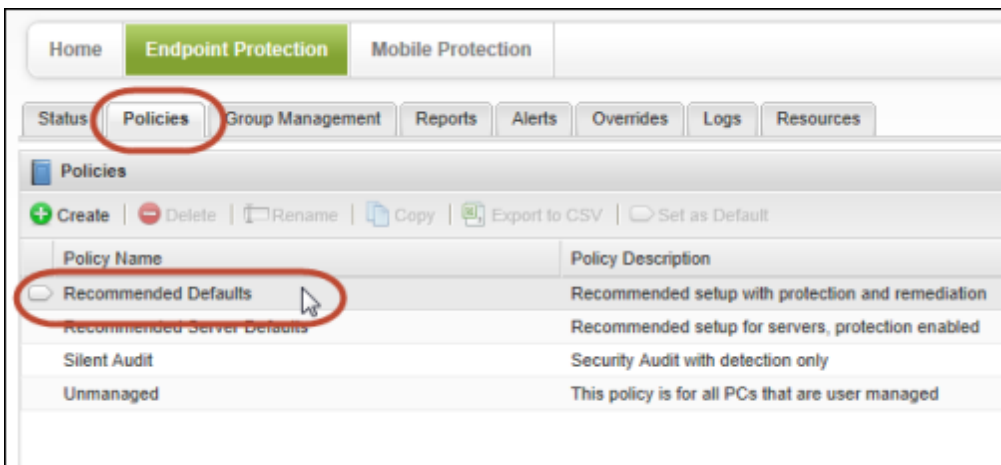
Implementing policies

When you first configured Endpoint Protection, you selected one of its default policies. (A *policy* defines the SecureAnywhere settings on endpoints, such as the scan schedule and shielding behavior.) You can continue to use your selected default policy or you can define more policies and assign them to endpoints. For example, you might want to give system administrators more control than you would other employees. In that case, you could create a new policy for administrators and keep everyone else on the default policy.

Note: To fully implement policies, you must have access permissions for **Policies: Create & Edit** and **Policies: Assign Policies to Endpoints**. To change access permissions, see "Setting permissions for portal users" on page 38.

To begin implementing policies, follow these steps:

1. Decide if you want to keep using your default policy. All policies appear in the **Policy** tab. Your default policy is indicated by a gray arrow on the far left (see the highlighted row in the following example). Double-click on your default policy name to open the settings. (You cannot see any settings for the Unmanaged policy, because that policy specifies that endpoint users have control, not the administrator.) You can then review the SecureAnywhere settings and determine if the default policy meets your business requirements. If not, you need to create a new policy (you cannot modify the Webroot defaults).



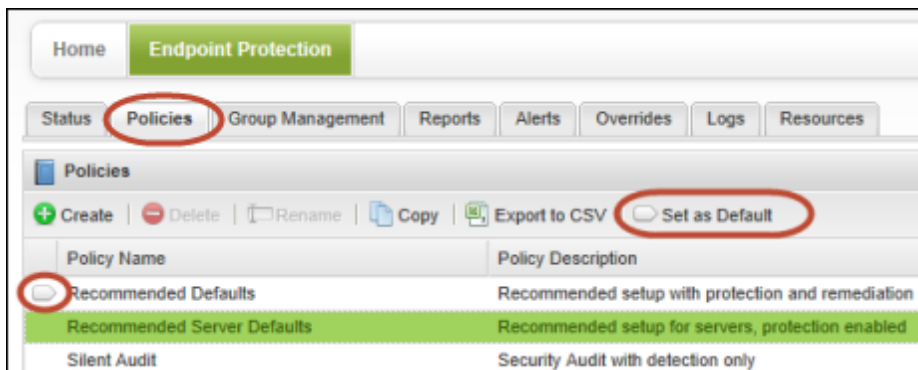
2. To add a new policy, see "Creating policies" on page 90.
Tip: We suggest you determine policy names and settings first to make the process easier.
3. Once you create new policies, you can assign them to endpoints in the **Group Management** tab. See "Applying a policy to endpoint groups" on page 124.

Selecting a new default policy

Whenever you install SecureAnywhere on new endpoints, Endpoint Protection assigns them to your default policy. If desired, you can set a different default policy for any endpoints that you install in the future.

To select a new default policy:

1. Click the **Policies** tab.
A list of policies appears in the bottom panel. A gray arrow indicates the current default policy (on the far left), as shown in the following example.
2. In the **Policy Name** column, click on the policy you want to use as the new default.
Once highlighted, **Set as Default** activates in the command bar.



3. Click **Set as Default** from the command bar.
4. When prompted, click **Yes**.
The gray arrow moves to that new policy. From now on, this policy is applied to any new SecureAnywhere installations.

Creating policies

You can add policies in one of two ways, either by creating a new policy or by copying an existing policy as a starting point. Each method is described below. Once you have defined a policy name and given it a description, you can then determine the policy settings as described in "Changing policy settings" on page 92.

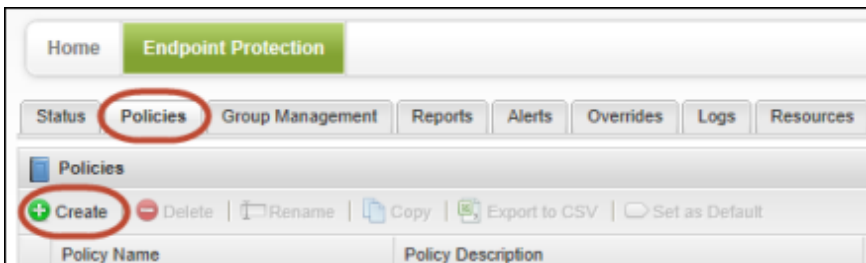
Tip: Policy names must be unique, so plan your policies in advance to avoid conflicts later. Once you give a policy a name, you cannot re-use that same name even after a policy has been deleted.

Creating a new policy

You create a new policy by giving it a name and description. Your new policy will pick up the Recommended Default settings as a starting point, but you can change those settings later.

To create a new policy:

1. Click the **Policies** tab.
2. Click **Create** from the command bar.



3. In the **Create Policy** dialog, enter a policy name and description of up to 50 alphanumeric characters, then click **Create Policy**.



4. Locate your new policy in the **Policy** tab. Double-click the policy you just created and modify the settings. See "Changing policy settings" on page 92.

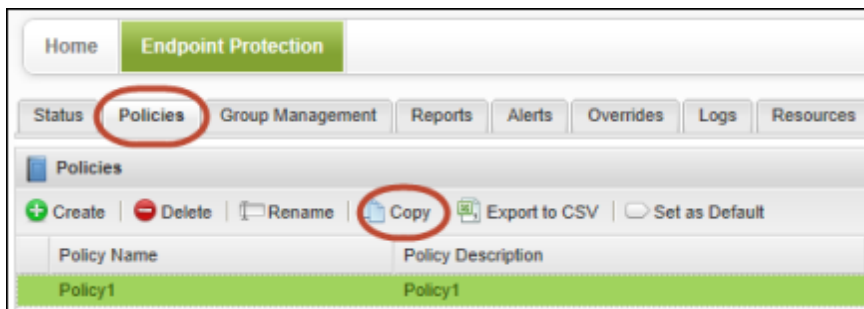
You can apply a policy to an individual endpoint or to a group of endpoints. See "Applying a policy to endpoint groups" on page 124.

Copying a policy

If you have a similar policy already defined, you can copy it and rename it. Your new policy will use the settings from the policy you copied, but you can change the settings later.

To copy a policy:

1. Click the **Policies** tab.
2. In the **Policy Name** column, click the policy you want to use as a starting point and then click **Copy** from the command bar.



In the Copy Policy dialog, the policy you selected is displayed in the first field. You can select a different one, if desired.

3. In the next two fields, enter a unique name and a description of up to 50 alphanumeric characters, then click **Create Policy**.



4. Locate your new policy in the **Policy** tab. Double-click the policy you just created and modify the settings as desired. See "Changing policy settings" on page 92.

You can apply a policy to an individual endpoint or to a group of endpoints. See "Applying a policy to endpoint groups" on page 124.

Changing policy settings

Once you create a policy (see "Creating policies" on page 90), you can change its settings to suit your business purposes. If desired, you can make temporary changes (create drafts) and then implement them later (promote to live).

Note: You cannot change the settings for Webroot default policies.

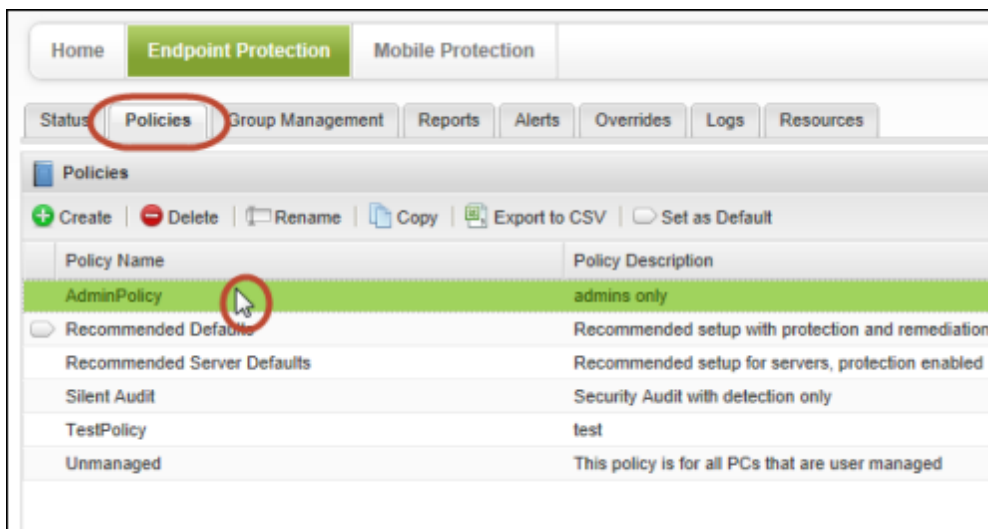
Policies control the following SecureAnywhere settings on managed endpoints:

SecureAnywhere settings controlled by policies	
Basic settings	General preferences that change the behavior of the SecureAnywhere program, such as whether the program icon appears in the endpoint's system tray and whether the user can shut down the program.
Scan schedule settings	Settings that allow you to run scans at different times, change the scanning behavior, or turn off automatic scanning. If you do not modify the scan schedule, SecureAnywhere launches scans automatically every day, at about the same time you installed the software.
Scan settings	Settings that provide more control over scans, such as performing a more thorough scan.
Self protection settings	Additional protection that prevents malicious software from modifying the SecureAnywhere program settings and processes on the endpoint. If SecureAnywhere detects another product attempting to interfere with its functions, it launches a protective scan to look for threats.
Heuristics	Threat analysis that SecureAnywhere performs when scanning endpoints. Heuristics can be adjusted for separate areas of the endpoints, including the local drive, USB drives, the Internet, the network, CD/DVDs, and when the endpoint is offline.
Realtime shield settings	Settings that block known threats listed in Webroot's threat definitions and in Webroot's community database.
Behavior shield settings	Settings that analyze the applications and processes running on the endpoints.
Core shield settings	Settings that monitor the computer system structures to ensure that malware has not tampered with them.

SecureAnywhere settings controlled by policies	
Web shield settings	Settings that protect endpoints as users surf the Internet and click links in search results.
Identity shield settings	Protection from identity theft and financial loss. It ensures that sensitive data is protected, while safe-guarding users from keyloggers, screen-grabbers, and other information-stealing techniques.
Firewall settings	Firewall protection that monitors data traffic traveling out of computer ports. It looks for untrusted processes that try to connect to the Internet and steal personal information. The Webroot firewall works in conjunction with the Windows firewall, which monitors data traffic coming into the endpoints.
User interface settings	User access to the SecureAnywhere program on the endpoint.
System Cleaner	Settings that control the System Cleaner behavior, such as an automatic cleanup schedule and what types of files and traces to remove from the endpoint.

To change policy settings:

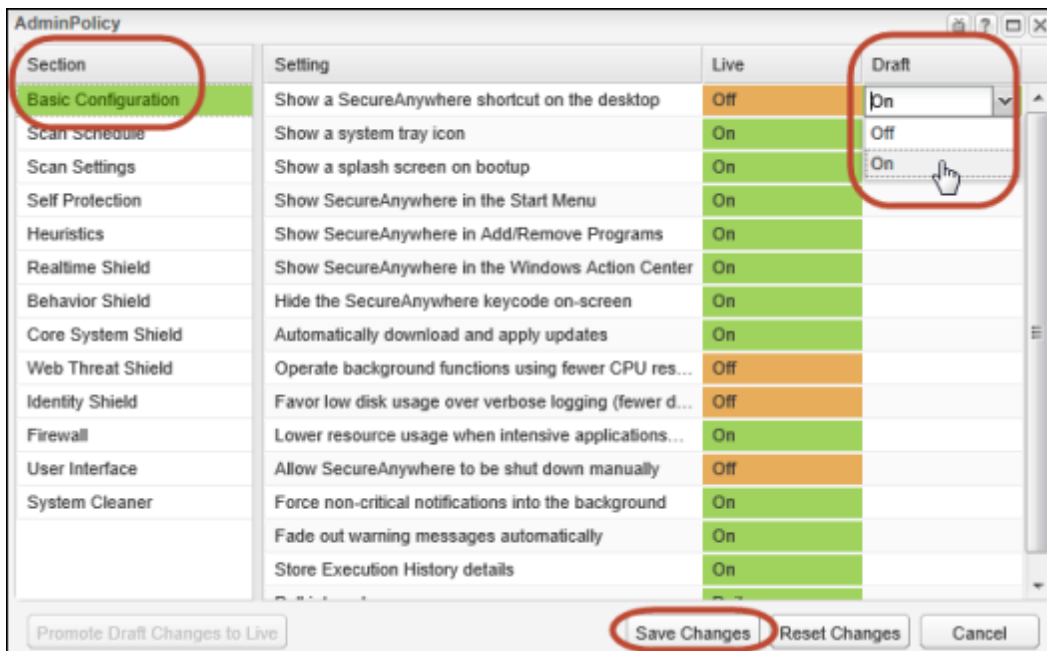
1. Click the **Policies** tab.
A list of policies opens in the bottom panel.
2. In the **Policy Name** column, find the policy in the list and double-click anywhere in the row.



The Policy dialog opens, with the Basic Configuration category selected (see the following example).

The **Live** column shows how the setting is currently implemented on the endpoints. The **Draft** column is where you can make changes.

3. Under the **Section** column (left side), choose the category to edit.
4. Under the **Draft** column (far right side), click in the cell to view the options, then select the desired setting.
A complete description of each setting follows these steps.
5. When you're done with a section, click **Save Changes** at the bottom. (For example, when you have finished editing Basic Configuration, save your changes before moving to Scan Schedule.)



6. Continue editing the policy, making sure to click **Save Changes** before you move to another section.
7. If you're *not* ready to implement the changes (promote to live), you can return to the **Policy** tab. Any policy with changes not yet implemented displays **Yes** in the **Draft Changes** column.

Policies		
Policy Name	Policy Description	Draft Changes
Policy1	Policy1	No
Policy2	Policy2	Yes
Policy3	Policy3	No
Recommended Defaults		
Recommended setup with protection and remediation		
Recommended Server Defaults		Recommended setup for servers, protection enabled
Silent Audit		Security Audit with detection only
Unmanaged		This policy is for all PCs that are user managed

8. To implement the changes, return to the Policy dialog and click **Promote Draft Changes to Live** (bottom left). *Your changes do not take effect until you promote them.*

Section	Setting	Live	Draft
Basic Configuration	Show a Webroot shortcut on the desktop	Off	On
Scan Schedule	Show a system tray icon	On	
Scan Settings	Show a splash screen on bootup	On	
Self Protection	Show Webroot in the Start Menu	On	
Heuristics	Show Webroot in Add/Remove Programs	On	
Realtime Shield	Show Webroot in the Windows Security/Action Center	On	
Behavior Shield	Hide the Webroot keycode on-screen	On	
Core System Shield	Automatically download and apply updates	On	
Web Threat Shield	Operate background functions using fewer CPU resources	Off	
Identity Shield	Favor low disk usage over verbose logging (fewer details st...	Off	
Firewall	Lower resource usage when intensive applications or game...	On	
User Interface	Allow Webroot to be shut down manually	Off	
	Force non-critical notifications into the background	On	
	Fade out warning messages automatically	On	
	Store Execution History details	On	
	Poll interval	Daily	

Promote Draft Changes to Live

Save Changes Reset Changes Cancel

Basic Configuration

The Basic Configuration settings control the behavior of the SecureAnywhere software on managed endpoints.

Basic Configuration settings	
Show a Webroot shortcut on the desktop	Provides quick access to the main interface by placing the shortcut icon on the endpoint desktop.
Show a system tray icon	Provides quick access to SecureAnywhere functions by placing the Webroot icon in the endpoint system tray.
Show a splash screen on bootup	Opens the Webroot splash screen when the endpoint starts.
Show Webroot in the Start Menu	Lists SecureAnywhere in the Windows Startup menu items.
Show Webroot in Add/Remove Programs	Lists SecureAnywhere in the Windows Add/Remove Programs panel.
Show Webroot in Windows Security/Action Center	Lists SecureAnywhere in the Windows Security/Action Center, under Virus Protection information.
Hide the Webroot keycode on-screen	Hides the keycode on the endpoint's My Account panel. Asterisks replace the code, except for the first four digits.
Automatically download and apply updates	Downloads product updates automatically without alerting the endpoint user.
Operate background functions using fewer CPU resources	Saves CPU resources by running non-scan related functions in the background.
Favor low disk usage over verbose logging (fewer details stored in logs)	Saves disk resources by saving only the last four log items.
Lower resource usage when intensive applications or games are detected	Suppresses SecureAnywhere functions while the user is gaming, watching videos, or using other intensive applications.
Allow Webroot to be shut down manually	Shows a Shutdown command in the endpoint's system tray menu. Deselecting this option removes the Shutdown command from the menu.
Force non-critical notifications into the background	Suppresses information-only messages from appearing in the system tray.
Fade out warning messages automatically	Closes warning dialogs in the system tray after a few seconds. If you disable this option, the user must manually click on a message to close it.

Basic Configuration settings	
Store Execution History details	Stores data for the Execution History logs, available under Reports.
Poll interval	Specifies how often the endpoint checks for updates. For example: 15 minutes, 30 minutes, 1 hour, or 2 hours.

Scan Schedule

SecureAnywhere runs scans automatically every day, at about the same time you installed the software. You can use the Scan Schedule settings to change the schedules and run scans at different times.

Scan Schedule settings	
Enable Scheduled Scans	Allows scheduled scans to run on the endpoint.
Scan Frequency	Determines how often to run the scan. You can set a day of the week or select "on bootup" (when the computer starts).
Time	Specifies the time to run the scan: <ul style="list-style-type: none"> • Scan time options for when computer is idle are before 8:00 a.m., before noon, before 5:00 p.m., or before midnight. • Scan time options for when resources are available are hourly, from 12:00 a.m. to 11:00 p.m.
Scan on bootup if the computer is off at the scheduled time	Launches a scheduled scan within an hour after the user turns on the computer, if the scan did not run at the normally scheduled time. If this option is disabled, SecureAnywhere ignores missed scans.
Hide the scan progress window during scheduled scans	Runs scans silently in the background. If this option is disabled, a window opens and shows the scan progress.
Only notify me if an infection is found during a scheduled scan	Opens an alert only if it finds a threat. If this option is disabled, a small status window opens when the scan completes, whether a threat was found or not.
Do not perform scheduled scans when on battery power	Helps conserve battery power. If you want SecureAnywhere to launch scheduled scans when the endpoint is on battery power, deselect this option.

Scan Schedule settings	
Do not perform scheduled scans when a full screen application or game is open	Ignores scheduled scans when the user is viewing a full-screen application, such as a movie or a game. Deselect this option if you want scheduled scans to run anyway.
Randomize the time of scheduled scans up to one hour for distributed scanning	Determines the best time for scanning (based on available system resources) and runs the scan within an hour of the scheduled time. If you want to force the scan to run at the scheduled time, deselect this option.
Perform a scheduled Quick Scan instead of a Deep Scan	Runs a quick scan of memory. We recommend that you keep this option deselected, so that deep scans run for all types of malware in all locations.

Scan Settings

Scan settings give advanced control over scanning performance.

Scan Settings	
Enable Realtime Master Boot Record (MBR) Scanning	Protects the endpoint against master boot record (MBR) infections. An MBR infection can modify core areas of the system so that they load before the operating system and can infect the computer. We recommend that you keep this option selected. It adds only a small amount of time to the scan.
Enable Enhanced Rootkit Detection	Checks for rootkits and other malicious software hidden on disk or in protected areas. Spyware developers often use rootkits to avoid detection and removal. We recommend that you keep this option selected. It adds only a small amount of time to the scan.
Enable "right-click" scanning in Windows Explorer	Enables an option for scanning the currently selected file or folder in the Windows Explorer right-click menu. This option is helpful if the user downloads a file and wants to scan it quickly.
Update the currently scanned folder immediately as scanned	Displays a full list of files as SecureAnywhere scans each one. If you want to increase scan performance slightly, deselect this option so that file names only update once per second on the panel. SecureAnywhere will still scan all files, just not take the time to show each one on the screen.

Scan Settings	
Favor low memory usage over fast scanning	Reduces RAM usage in the background by using less memory during scans, but scans will also run a bit slower. Deselect this option to run faster scans and use more memory.
Favor low CPU usage over fast scanning	Reduces CPU usage during scans, but scans will also run a bit slower. Deselect this option to run faster scans.
Save non-executable file details to scan logs	Saves all file data to the scan log, resulting in a much larger log file. Leave this option deselected to save only executable file details to the log.
Show the "Authenticating Files" popup when a new file is scanned on-execution	Opens a small dialog whenever the user runs a program for the first time. Leave this option deselected if you do not want users to see this dialog.
Scan archived files	Scans compressed files in zip, rar, cab, and 7-zip archives.
Automatically reboot during cleanup without prompting	Restarts the computer after running a clean-up, which is the process of removing all traces of a malware file.
Never reboot during malware cleanup	Prevents the endpoint from restarting during cleanup, which is the process of removing all traces of a malware file.
Automatically remove threats found during background scans	Removes threats during scans that run in the endpoint's background and sends them to quarantine.
Automatically remove threats found on the learning scan	Removes threats during the first scan on the endpoint and sends them to quarantine.
Enable Enhanced Support	Allows logs to be sent to Webroot customer support.
Show Infected Scan Results	Shows scan results. If not enabled, the endpoint does not show scan results even if malware is detected.

Self Protection

Self Protection prevents malicious software from modifying the SecureAnywhere program settings and processes. If SecureAnywhere detects that another product is attempting to interfere with its functions, it launches a protective scan to look for threats. It will also update the internal self protection status to prevent incompatibilities with other software.

Note: We recommend that you leave Self Protection at the **Maximum** settings, unless you use other security software in addition to SecureAnywhere. If you use additional security software, adjust Self Protection to **Medium** or **Minimum**. The **Maximum** setting might interfere with other security software.

Self Protection settings	
Enable self-protection response cloaking	Turns self-protection on and off.
Self-protection level	Sets the detection level to: <ul style="list-style-type: none"> • Minimum. Protects the integrity of the SecureAnywhere settings and databases. Recommended if the endpoint has several other security products installed. • Medium. Prevents other programs from disabling protection. Provides maximum possible compatibility with other security software. • Maximum. Provides the highest protection of the SecureAnywhere processes. Recommended.

Heuristics

With heuristics, you can set the level of threat analysis that SecureAnywhere performs when scanning managed endpoints. SecureAnywhere includes three types of heuristics: advanced, age, and popularity.

- **Advanced Heuristics.** Analyzes new programs for suspicious actions that are typical of malware.
- **Age Heuristics.** Analyzes new programs based on the amount of time the program has been in the community. Legitimate programs are generally used in a community for a long time, but malware often has a short life span.
- **Popularity Heuristics.** Analyzes new programs based on statistics for how often the program is used in the community and how often it changes. Legitimate programs do not change quickly, but malware often mutates at a rapid pace. Malware may install as a unique copy on every computer, making it statistically unpopular.

You can adjust these types of heuristics for several areas: the local drive, USB drives, the Internet, the network, CD/DVDs, and when your computer is offline. For each of these areas, you can set the following options:

- **Disable Heuristics.** Turns off heuristic analysis for the local drive, USB drives, the Internet, the network, CD/DVDs, or when your computer is offline. Not recommended.
- **Apply advanced heuristics before Age/Popularity heuristics.** Warns against new programs as well as old programs that exhibit suspicious behavior on the local drive, USB drives, the Internet, the network, CD/DVDs, or when your computer is offline.
- **Apply advanced heuristics after Age/Popularity heuristics.** Warns against suspicious programs detected with Advanced Heuristics, based on Age/Popularity settings on the local drive, USB drives, the Internet, the network, CD/DVDs, or when your computer is offline.
- **Warn when new programs execute that are not known good.** Warns when malicious, suspicious, or unknown programs try to execute on the local drive, USB drives, the Internet, the network, CD/DVDs, or when your computer is offline. (This setting may result in false detections.)

Heuristics levels	
Advanced Heuristics	<p>Disabled turns off Advanced Heuristics, leaving it vulnerable to new threats. (However, it will still be protected against known threats.)</p> <p>Low detects programs with a high level of malicious activity. This setting ignores some suspicious behavior and allows most programs to run.</p> <p>Medium balances detection versus false alarms by using our tuned heuristics in the centralized community database.</p> <p>High protects against a wide range of new threats. Use this setting if you think your system is infected or at very high risk. (This setting may result in false detections.)</p> <p>Maximum provides the highest level of protection against new threats. Use this setting if you think that your system is infected or at very high risk. (This setting may result in false detections.)</p>
Age Heuristics	<p>Disabled turns off Age Heuristics, leaving it vulnerable to new threats. (However, it will still be protected against known threats.)</p> <p>Low detects programs that have been created or modified very recently.</p> <p>Medium detects programs that are fairly new and not trusted, preventing zero-day or zero-hour attacks. We recommend using this setting if you do not allow unpopular programs to be installed on your managed endpoints and you want extra security to prevent mutating threats.</p> <p>High detects programs that have been created or modified in a relatively short time and are not trusted. This setting is recommended only if new programs are rarely installed on your managed endpoints, and if you feel that your systems are relatively constant. This setting might generate a higher level of false detections on more obscure or unpopular programs.</p> <p>Maximum detects all untrusted programs that have been created or modified fairly recently. Use this setting only if your managed endpoints are in a high-risk situation, or if you think that they are currently infected.</p>

Heuristics levels	
Popularity Heuristics	<p>Low detects programs that are seen for the first time. This setting is recommended if new or beta programs are frequently installed on your managed endpoints, or if endpoint users are software developers who frequently create new programs.</p> <p>Medium detects unpopular and mutating programs, preventing zero-day and zero-hour attacks. We recommend using this setting if you do not allow new programs to be installed frequently on your managed endpoints and you want extra security over standard settings.</p> <p>High detects programs that a significant percentage of the community has seen. This setting is recommended if you do not allow new programs on your managed endpoints and you suspect that they are currently infected.</p> <p>Maximum detects programs that a large percentage of the community has seen. We recommend this setting if you think your managed endpoints are at very high risk, and you accept that you might receive false detections because of the strict heuristic rules.</p>

Realtime Shield

The Realtime shield blocks known threats that are listed in Webroot's threat definitions and community database. If the shield detects a suspicious file, it opens an alert and prompts you to block or allow the item. If it detects a known threat, it immediately blocks and quarantines the item before it causes damage to the endpoint or steals its information.

Realtime shield settings	
Realtime Shield Enabled	Turns the Realtime shield on and off.
Enable Predictive Offline Protection from the central Webroot database	Downloads a small threat definition file to your managed endpoints, protecting them even when they are offline. We recommend that you leave this setting on.
Remember actions on blocked files	Remembers how the user responded to an alert (allowed a file or blocked it) and will not prompt again when it encounters the same file. If this setting is deselected, SecureAnywhere opens an alert every time it encounters the file in the future.

Realtime shield settings	
Automatically quarantine previously blocked files	Opens an alert when it encounters a threat and allows the user to block it and send it to quarantine. If this setting is off, the user must run a scan manually to remove a threat.
Automatically block files when detected on execution	Blocks threats and sends them to quarantine. If this setting is off, the user must respond to alerts about detected threats.
Scan files when written or modified	Scans any new or modified files that are saved to disk. If this setting is off, it ignores new file installations (however, it still alerts the user if a threat tries to launch).
Block threats automatically if no user is logged in	Stops threats from executing even when managed endpoints are logged off. Threats are sent to quarantine without notification.
Show realtime event warnings	Opens an alert when suspicious activity occurs.
Show realtime block modal alerts	Shows alerts when Heuristics detects malware, and prompts the user to allow or block the action. Note: This setting must be set to "on" if Heuristics is set to "Warn when new programs execute that are not known good." Otherwise, users will not see the alert.
Show realtime block notifications	Shows a tray notification if the Realtime shield detects malware. If this setting is off, there is no tray notification, but malware is blocked and the home page shows that threats were detected.

Behavior Shield

The Behavior shield analyzes the applications and processes running on your managed endpoints. If it detects a suspicious file, it opens an alert and prompts you to block or allow the item. If it detects a known threat, it immediately blocks and quarantines the item before it causes damage to managed endpoints or steals information.

Behavior shield settings	
Behavior Shield Enabled	Turns the Behavior shield on and off.
Assess the intent of new programs before allowing them to execute	Watches the program's activity before allowing it to run. If it appears okay, SecureAnywhere allows it to launch and continues to monitor its activity.

Behavior shield settings	
Enable advanced behavior interpretation to identify complex threats	Analyzes a program to examine its intent. For example, a malware program might perform suspicious activities like modifying a registry entry, then sending an email.
Track the behavior of untrusted programs for advanced threat removal	Watches programs that have not yet been classified as legitimate or as malware.
Automatically perform the recommended action instead of showing warning messages	Does not prompt the user to allow or block a potential threat. SecureAnywhere determines how to manage the item.
Warn if untrusted programs attempt low-level system modifications when offline	Opens an alert if an unclassified program tries to make changes to your managed endpoints when they are offline. (SecureAnywhere cannot check its online threat database if endpoints are disconnected from the Internet.)

Core System Shield

The Core System shield monitors system structures of your managed endpoints and makes sure malware has not tampered with them. If the shield detects a suspicious file trying to make changes, it opens an alert and prompts the user to block or allow the item. If it detects a known threat, it immediately blocks and quarantines the item before it causes damage or steals information.

Core System shield settings	
Core System Shield Enabled	Turns the Core System shield on and off.
Assess system modifications before they are allowed to take place	Intercepts any activity that attempts to make system changes on your managed endpoints, such as a new service installation.
Detect and repair broken system components	Locates corrupted components, such as a broken Layered Service Provider (LSP) chain or a virus-infected file, then restores the component or file to its original state.
Prevent untrusted programs from modifying kernel memory	Stops unclassified programs from changing the kernel memory.

Core System shield settings	
Prevent untrusted programs from modifying system processes	Stops unclassified programs from changing system processes.
Verify the integrity of the LSP chain and other system structures	Monitors the Layered Service Provider (LSP) chain and other system structures to make sure malware does not corrupt them.
Prevent any program from modifying the HOSTS file	Stops spyware from attempting to add or change the IP address for a website in the Hosts file, and opens an alert for the user to block or allow the changes.

Web Threat Shield

The Web Threat shield protects your endpoints as users surf the Internet. If it detects a website that might be a threat, it opens an alert for users to block the site or continue despite the warning. When they use a search engine, this shield analyzes all the links on the search results page, then displays an image next to each link that signifies whether it's a trusted site (green checkmark) or a potential risk (red X).

Web Threat shield settings	
Web Threat Shield Enabled	Turns the Web Threat shield on and off.
Analyze search engine results and identify malicious websites before visitation	Analyzes search engine results, SecureAnywhere analyzes all links displayed on the search results page by running the URLs through its malware-identification engine. It then displays an image next to each link that signifies if the site is safe (green checkmark) or a potential risk (red X).
Enable deep content analysis	Analyzes all data traffic on your managed endpoints as users visit websites. If threats try to install, it blocks the threat's activity.
Look for malware on websites before visitation	Analyzes URLs in a browser's address bar and links to sites. If the site is associated with malware, it blocks it from loading in your browser.
Look for exploits in website content before visitation	Looks for cross-site scripting attacks that might try to redirect users to a different website.
Suppress the user's ability to make local Web Threat Shield overrides	Prevents the endpoint user from overriding the Web Threat Shield settings. If disabled, endpoint users can create overrides when they are blocked from accessing a website.

Identity Shield

The Identity shield protects sensitive data that might be exposed during online transactions. You can change the behavior of the Identity shield and control what it blocks.

Identity shield settings	
Identity Shield Enabled	Turns the Identity shield on and off.
Look for identity threats online	Analyzes websites as users browse the Internet or open links. If the shield detects malicious content, it blocks the site and opens an alert.
Analyze websites for phishing threats	Analyzes websites for phishing threats as users browse the Internet or open links. If the shield detects a phishing threat, it blocks the site and opens an alert.
Verify websites when visited to determine legitimacy	Analyzes the IP address of each website to determine if it has been redirected or is on our blacklist. If the shield detects an illegitimate website, it blocks the site and opens an alert.
Verify the DNS/IP resolution of websites to detect Man-in-the-Middle attacks	Looks for servers that could be redirecting users to a malicious website (man-in-the-middle attack). If the shield detects a man-in-the-middle attack, it blocks the threat and opens an alert.
Block websites from creating high risk tracking information	Blocks third-party cookies from installing on your managed endpoints if the cookies originate from malicious tracking websites.
Prevent programs from accessing protected credentials	Blocks programs from accessing login credentials (for example, when you type your name and password or when you request a website to remember them).
Warn before blocking untrusted programs from accessing protected data	Opens an alert any time malware attempts to access data, instead of blocking known malware automatically.
Allow trusted screen capture programs access to protected screen contents	Allows screen capture programs, no matter what content is displayed on the screen.

Identity shield settings	
Enable Identity Shield compatibility mode	Allows certain applications to run that the Identity shield might block during normal operations. You can enable this option if you notice problems with an application's functions after SecureAnywhere was installed on the endpoint. With this compatibility mode enabled, the endpoint is still protected by the Identity shield's core functionality.
Enable keylogging protection in non-Latin systems	Allows endpoints with non-Latin systems (such as Japanese and Chinese) to be protected from keyloggers.

Firewall

The Webroot firewall monitors data traffic traveling out of endpoint ports. It looks for untrusted processes that try to connect to the Internet and steal personal information. It works with the Windows firewall, which monitors data traffic coming into your managed endpoints. With both the Webroot and Windows firewall turned on, network data has complete inbound and outbound protection.

The Webroot firewall is preconfigured to filter traffic on your managed endpoints. It works in the background without disrupting normal activities. If the firewall detects unrecognized traffic, it opens an alert. You can either block the traffic or allow it to proceed.

Firewall settings	
Enabled	Turns the Firewall on and off.
Firewall level	<p>Default Allow: Allows all processes to connect to the Internet, unless explicitly blocked.</p> <p>Warn unknown and infected: Warns if any new, untrusted processes connect to the Internet, if the endpoint is infected.</p> <p>Warn unknown: Warns if a new, untrusted process connects to the Internet.</p> <p>Default Block: Warns if any process connects to the Internet, unless explicitly blocked.</p>

Firewall settings	
Show firewall management warnings	<p>Controls the alert shown by SecureAnywhere when the Windows firewall is off:</p> <ul style="list-style-type: none"> • On. The user sees an alert when SecureAnywhere detects that the Windows firewall is off. • Off. No alert appears when the Windows firewall is off.
Show firewall process warnings	<p>Controls the firewall alerts. If this is setting is Off, no firewall alerts appear. This option works in conjunction with the Firewall Level settings. For example, if Show firewall process warnings and Default Block options are both set to On, the endpoint user sees an alert if a new process tries to connect. If Show Firewall process warnings is set to Off, no alert appears to the endpoint user and the process is allowed.</p>

User Interface

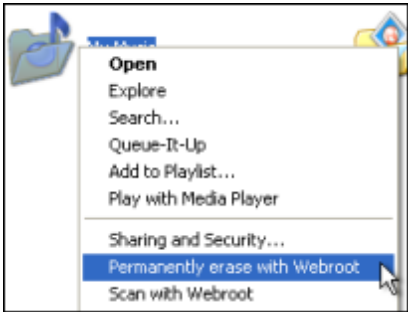
Gives administrative control over the SecureAnywhere interface on the endpoints using this policy.

User Interface setting	
GUI	<p>Blocks or allows endpoint user access to the main SecureAnywhere interface. If users try to open SecureAnywhere when this option is set to Hide, a message tells them to contact the administrator to access the interface.</p> <p>Note: This option does not also hide the Webroot system tray icon.</p>

System Cleaner

The System Cleaner removes traces of the end user's web browsing history, files that show computer use, and unnecessary files that consume valuable disk space, such as files in the Recycle Bin or Windows temporary files. The System Cleaner does not run automatically; you need to schedule cleanups and select the items you want removed.

Note: Cleanups remove unnecessary files and traces, not malware threats. Malware (spyware and viruses) are removed during scans. You can think of the System Cleaner as the housekeeper of a computer, while the Scanner serves as the security guard.

System Cleaner settings	
Manage System Cleaner centrally	<p>Enables the administrator to change System Cleaner settings, as follows:</p> <ul style="list-style-type: none"> • On. The System Cleaner settings are shown in the panel and are available to change. • Off. No settings appear in this panel.
Scheduled Cleanup (Monday through Sunday)	Sets the days of the week (one or more) to automatically run the System Cleaner.
Cleanup at specific time of day - hour	Sets the hour of the day the System Cleaner runs on the endpoints.
Cleanup at specific time of day - minute	Sets the time (in 15-minute increments) the System Cleaner runs on the endpoints.
Run on bootup if the system was off at the scheduled time	Launches a missed scheduled cleanup when the endpoint powers on (applicable only if the endpoint was off during a scheduled cleanup). Otherwise, skips the missed cleanup.
Enable Windows Explorer right click secure file erasing	<p>Includes an option for permanently erasing a file or folder in Windows Explorer on the endpoint. A menu item appears when the user right-clicks on a file or folder:</p> 
Windows Desktop:	
Recycle Bin	Removes all files from the Recycle Bin in Windows Explorer.

System Cleaner settings	
Recent document history	Clears the history of recently opened files, which is accessible from the Windows Start menu. (The cleanup does not delete the actual files.)
Start Menu click history	Clears the history of shortcuts to programs that end users recently opened using the Start menu.
Run history	Clears the history of commands recently entered into the Run dialog, which is accessible from the Start menu. Note: After the cleanup, the end user may need to restart the computer to completely remove items from the Run dialog.
Search history	Clears the history of files or other information that the end user searched for on the computer. This history displays when the end user starts entering a new search that starts with the same characters. (The cleanup does not delete the actual files.)
Start Menu order history	Reverts the list of programs and documents in the Start menu back to alphabetical order, which is the default setting. After the cleanup runs, the list reverts back to alphabetical order after a system re-boot.
Windows System:	
Clipboard contents	Clears the contents from the Clipboard, where Windows stores data used in either the Copy or Cut function from any Windows program.
Windows Temporary folder	Deletes all files and folders in the Windows temporary folder, but not files that are in use by an open program. This folder is usually: C:\Windows\Temp.
System Temporary folder	Deletes all files and folders in the system temporary folder, but not files that are in use by an open program. This folder is usually in: C:\Documents and Settings\[username]\Local Settings\Temp.
Windows Update Temporary folder	Deletes all files and subfolders in this folder, but not files that are in use by an open program. Windows uses these files when a Windows Update runs. These files are normally in C:\Windows\Software\Distribution\Download.
Windows Registry Streams	Clears the history of recent changes made to the Windows registry. (This option does not delete the registry changes themselves.)

System Cleaner settings	
Default logon user history	Deletes the Windows registry entry that stores the last name used to log on to your computer. When the registry entry is deleted, end users must enter their user names each time they turn on or restart the computer. This cleanup option does not affect computers that use the default Welcome screen.
Memory dump files	Deletes the memory dump file (memory.dmp) that Windows creates with certain Windows errors. The file contains information about what happened when the error occurred.
CD burning storage folder	Deletes the Windows project files, created when the Windows built-in function is used to copy files to a CD. These project files are typically stored in one of the following directories: C:\Documents and Settings\[username]\Local Settings\Application Data\Microsoft\CDBurning or C:\Users\[username]\AppData\Local\Microsoft\Windows\Burn\Burn
Flash cookies	Deletes bits of data created by Adobe Flash, which can be a privacy concern because they track user preferences. (Flash cookies are not actually “cookies,” and are not controlled through the cookie privacy controls in a browser.)
Internet Explorer:	
Address bar history	Removes the list of recently visited websites, which is stored as part of Internet Explorer’s AutoComplete feature. You see this list when you click the arrow on the right side of the Address drop-down list at the top of the Internet Explorer browser.
Cookies	Deletes all cookies from the endpoint. Be aware that if you remove all cookie files, the end user must re-enter passwords, shopping cart items, and other entries that these cookies stored.
Temporary Internet Files	Deletes copies of stored web pages that the end user visited recently. This cache improves performance by helping web pages open faster, but can consume a lot of space on the hard drive.
URL history	Deletes the History list of recently visited websites of the Internet Explorer toolbar.
Setup Log	Deletes log files created during Internet Explorer updates.

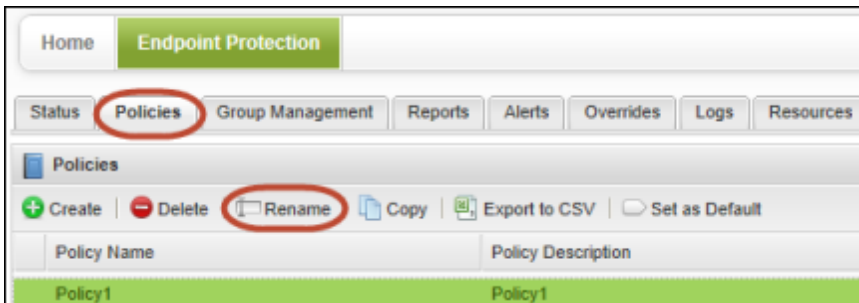
System Cleaner settings	
Microsoft Download Folder	Deletes the contents in the folder that stores files last downloaded using Internet Explorer.
MediaPlayer Bar History	Removes the list of audio and video files recently opened with the media player in Internet Explorer. (The cleanup does not delete the files themselves.)
Autocomplete form information	Deletes data that Internet Explorer stores when the end user entered information into fields on websites. This is part of Internet Explorer's AutoComplete feature.
Clean index.dat (cleaned on reboot)	Marks files in the index.dat file for deletion, then clears those files after the system reboots. The index.dat file is a growing Windows repository of web addresses, search queries, and recently opened files. This option works when you also select one or more of the following options: Cookies, Temporary Internet Files, or URL History. Note: Index.dat functions like an active database. It is only cleaned after you reboot Windows.
Secure File Removal:	
Control the level of security to apply when removing files	Removes files permanently in a "shredding" process, which overwrites them with random characters. This shredding feature is a convenient way to make sure no one can ever access the endpoint's files with a recovery tool. By default, file removal is set to Normal, which means items are deleted permanently (bypassing the Recycle Bin). However, with the Normal setting, data recovery utilities could restore the files. If you want to make sure files can never be recovered, select Maximum. Medium overwrites files with three passes, whereas Maximum overwrites files with seven passes and cleans the space around the files. Also be aware that cleanup operations take longer when you select Medium or Maximum.

Renaming a policy

You can rename a policy from the Policies tab. Keep in mind that policy names must be unique.

To rename a policy:

1. Click the **Policies** tab.
2. From the **Policy Name** column, select the policy to rename.
3. Click **Rename** from the command bar.



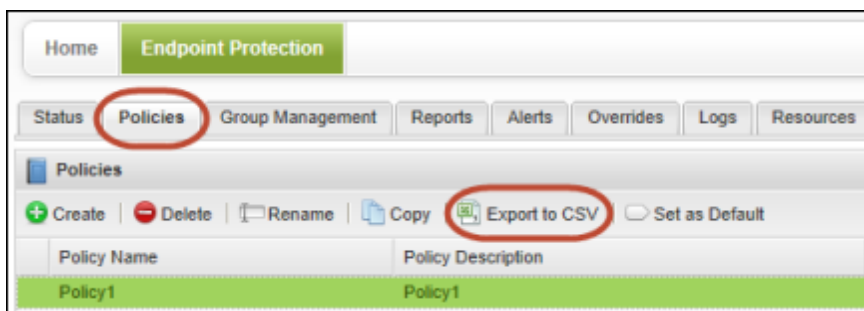
4. In the **Rename Policy** dialog, enter a new name and a description for the policy.
5. Click **Rename Policy**.

Exporting policy settings to a spreadsheet

You can export all policy information to a spreadsheet, which is convenient if you want to review policy settings with IT colleagues.

To export a policy:

1. Click the **Policies** tab.
2. From the **Policy Name** column, select the desired policy.
3. Click **Export to CSV** from the command bar.



4. From the prompt, save the policy to a CSV file.
Endpoint Protection saves it to a file with the policy name and a CSV extension. For example, if the policy is named "Policy 1," the file is saved to **Policy1.csv**.

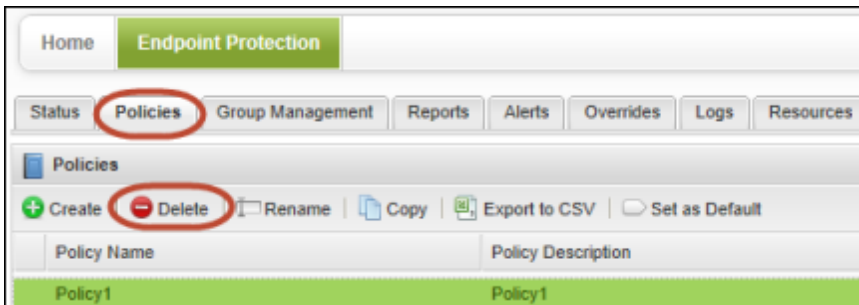
Deleting policies

You can delete all policies except for the original default policies. When you delete a policy, Endpoint Protection removes it from the list of active policies and moves it to a Deleted Policies list, so it is still accessible to the report logs.

Note: Be aware that if you delete a policy, you cannot re-use the same policy name again. Also, you cannot restore a deleted policy, but you can copy and rename it.

To delete a policy:

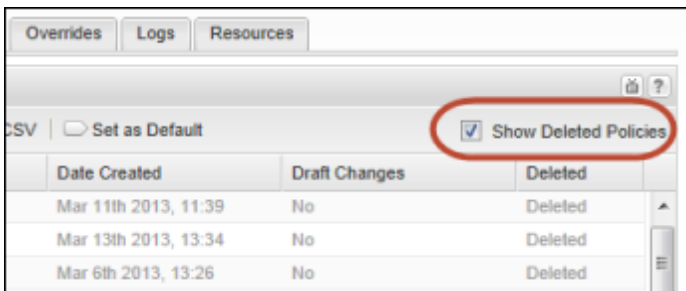
1. Click the **Policies** tab.
2. From the **Policy Name** column, select the desired policy and click **Delete** from the command bar.



After you confirm the deletion, you are prompted to move any endpoints from the deleted policy to another.

3. Open the drop-down list in the **Move any endpoints** dialog and select a new policy for the endpoints.
4. Click **Save** to remove the policy from the list.

Note: Deleted policies are moved to a Deleted Policies list. To view them, select the **Show Deleted Policies** checkbox on the **Policies** tab to display them in the list. The Deleted policies are shown in gray:



Viewing endpoints assigned to a policy

From the Policies tab, you can quickly view which endpoints are assigned to a policy.

To view endpoints assigned to a policy:

1. Click the **Policies** tab.
2. From the **Policy Name** column, select the desired policy.
The bottom panel shows which groups use this policy.
3. To view endpoints, you can do either of the following:
 - Click **View all endpoints using this policy** from the command bar.
 - Select the **View** link in the row for the group.

The screenshot shows the 'Policies' tab in a management console. At the top, there are navigation tabs: Status, Policies, Group Management, Reports, Alerts, Overrides, Logs, and Resources. Below the tabs, there's a 'Policies' section with a command bar containing: Create, Delete, Rename, Copy, Export to CSV, and Set as Default. A table lists policies:

Policy Name	Policy Description	Date Created
Policy1	Policy1	Jan 31st 2013, 13:15
Policy2	Policy2	Feb 1st 2013, 14:04
Policy3	Policy3	Feb 4th 2013, 13:06
<input checked="" type="checkbox"/> Recommended Defaults	Recommended setup with protection and remediation	
Recommended Server Defaults	Recommended setup for servers, protection enabled	
Silent Audit	Security Audit with detection only	
Unmanaged	This policy is for all PCs that are user managed	

Below the table, there's a section titled 'Groups and endpoints using Recommended Defaults'. It has a command bar with: Save Changes, Undo Changes, Move all endpoints on this policy to another policy, and View all endpoints using this policy (circled in red). Below this is a table:

Group Name	Number of endpoints
Default Group	6 View

A dialog opens and shows the endpoint names and status.

4. If desired, you can show or hide additional data about the endpoints. Click a column header to open the drop-down menu, then click in the checkboxes to select the columns to add or remove. For descriptions of the data in the columns, see "Sorting data in tables and reports" on page 26.

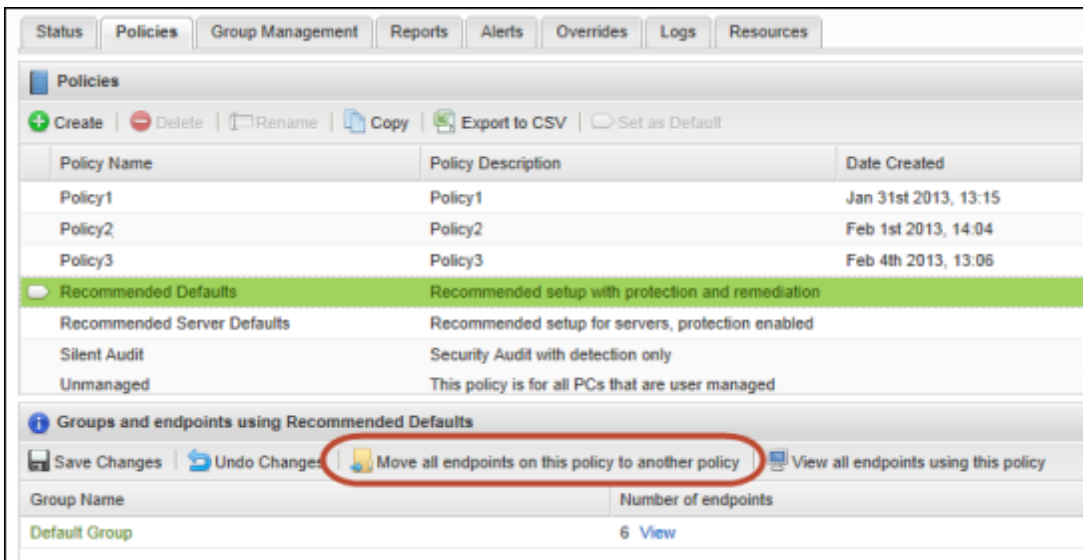
Moving endpoints to another policy

From the Policy tab, you can move all endpoints assigned to one policy to another policy.

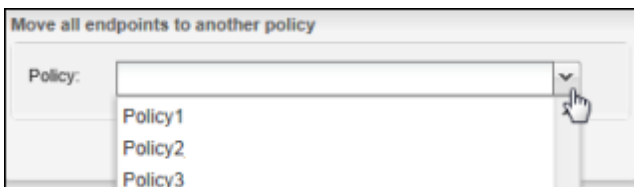
Note: If you want to move individual endpoints to a policy, see "Applying a policy to endpoint groups" on page 124.

To move endpoints to another policy:

1. Click the **Policies** tab.
2. From the **Policy Name** column, select the desired policy. The bottom panel shows which groups use this policy.
3. Click **Move all endpoints on this policy to another policy** from the command bar.



4. In the dialog, click the drop-down arrow to open a list of policies. Select the policy and click **Save**.



5. Check the Policies list to make sure the new endpoints are shown under the new assignment.

Chapter 6: Managing Groups

To manage groups and the endpoints within each group, see the following topics:

Organizing endpoints into groups	120
Adding a new group	122
Applying a policy to endpoint groups	124
Applying a policy to a group	124
Applying a policy to a single endpoint	125
Moving endpoints to another group	127
Deleting groups	128
Renaming groups	129

Organizing endpoints into groups

When you install SecureAnywhere on endpoints, those endpoints are automatically assigned to your default policy and to the Default group. (A *group* is a collection of endpoints, which helps you organize your devices for easy management.) Once endpoints report into the Management Portal (after performing the first scan), you can move them to a different group. For example, you might organize endpoints by time zone so that you can schedule the same scan time for all of them.

Note: To fully manage groups, you must have access permissions for **Groups: Create & Edit**, **Groups: Deactivate/Reactivate Endpoints**, and **Groups: Assign Endpoints to Groups**. To change access permissions, see "Setting permissions for portal users" on page 38.

You can view all groups in the Group Management tab, which looks similar to the example below. Select a group from the Groups panel on the left to see the endpoints and policies associated with that group on the right. Endpoints are shown on the top; policies are shown on the bottom.

The screenshot displays the 'Group Management' tab in the Management Portal. On the left, the 'Groups' panel shows a table with columns 'Group Name' and 'No.'. The 'Default Group' is selected and highlighted in green, showing 46 endpoints. The main area is divided into two sections: 'Endpoints in Default Group' and 'Policies used in Default Group'. The 'Endpoints in Default Group' section contains a table with columns: Hostname, Policy, Status, Last Seen, and Last Infected. The 'Policies used in Default Group' section contains a table with columns: Policy Name, Endpoints using this policy, and Policy Description.

Group Name	No.
All Endpoints	77
Deactivated Endpoints	4
Default Group	46

Hostname	Policy	Status	Last Seen	Last Infected
1 ADMIN405	Rec...	Protected	Apr 30th 2013, 12:33	8
2 ADMIN405	Rec...	Protected	Apr 30th 2013, 12:20	8
3 G-0409-FIRENZE	Rec...	Not Seen Recently	Apr 8th 2013, 17:48	8
4 G-0409-SUMATRA	Rec...	Infected	Apr 8th 2013, 17:45	8
5 G-0409-VOLGA	Rec...	Not Seen Recently	Apr 8th 2013, 17:42	8

Policy Name	Endpoints using this policy	Policy Description
Recommended Defaults	39	Recommended setup with protection and remediation
Unmanaged	6	This policy is for all PCs that are user managed
QA default policy	1	QA default policy

Note: All endpoints are assigned to the Default group, unless you used the `/groupname` switch in the command line during a silent installation. See "Deploying SecureAnywhere to endpoints" on page 50.

To create more groups and move endpoints, follow these steps:

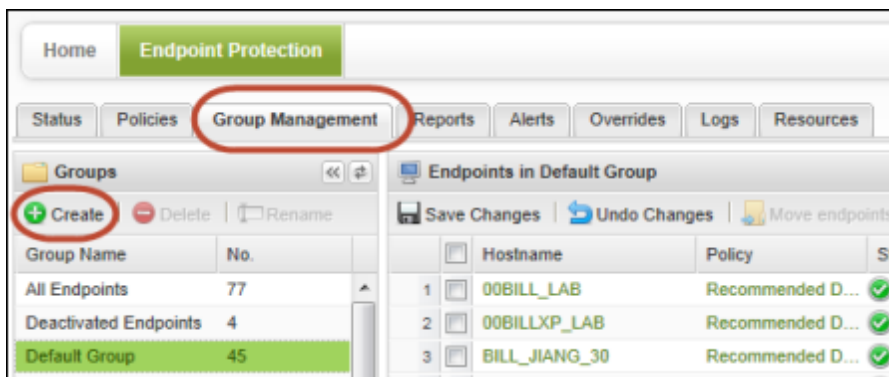
1. Add one or more new groups, as described in "Adding a new group" on page 122.
2. Move endpoints to the newly created groups, as described in "Moving endpoints to another group" on page 127.
3. Assign a policy to the new group of endpoints, as described in "Applying a policy to endpoint groups" on page 124.

Adding a new group

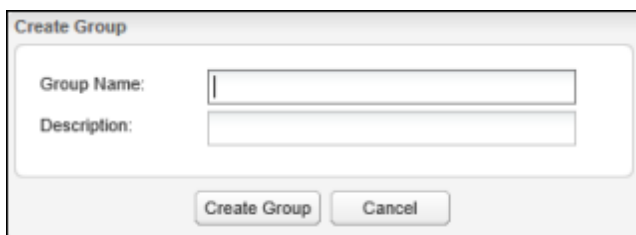
When you first deploy SecureAnywhere to endpoints, Endpoint Protection assigns them all to the Default group. If desired, you can add more groups for different management purposes and re-assign endpoints to those new groups.

To create a group:

1. Click the **Group Management** tab.
2. Click **Create** from the command bar.



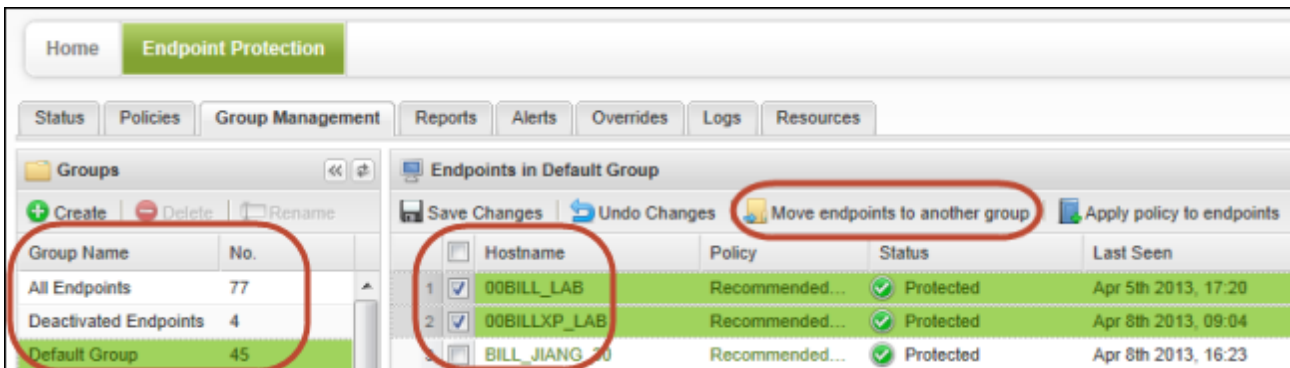
3. In the **Create Group** dialog, enter a group name and description, then click **Create Group**.



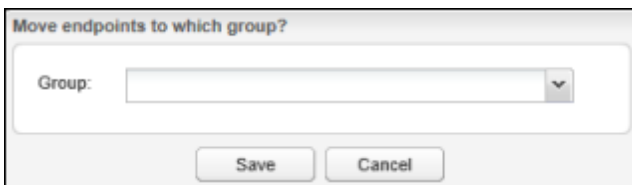
The new group appears in the **Groups** panel on the left.

4. To move endpoints into this group, click the group where the endpoints currently reside.
5. Select one or more endpoints from the **Endpoints** panel on the right.
Tip: You can select all endpoints within the selected group by clicking the **Hostname** checkbox at the top of the list (first column).

- Click **Move endpoints to another group** from the command bar.



- When the **Move** dialog opens, click the drop-down arrow to display the list of groups. Select your new group from the drop-down field and click **Save**.



- You can then apply policies to the entire group or to individual endpoints, as described in "Applying a policy to endpoint groups" on page 124.

Applying a policy to endpoint groups

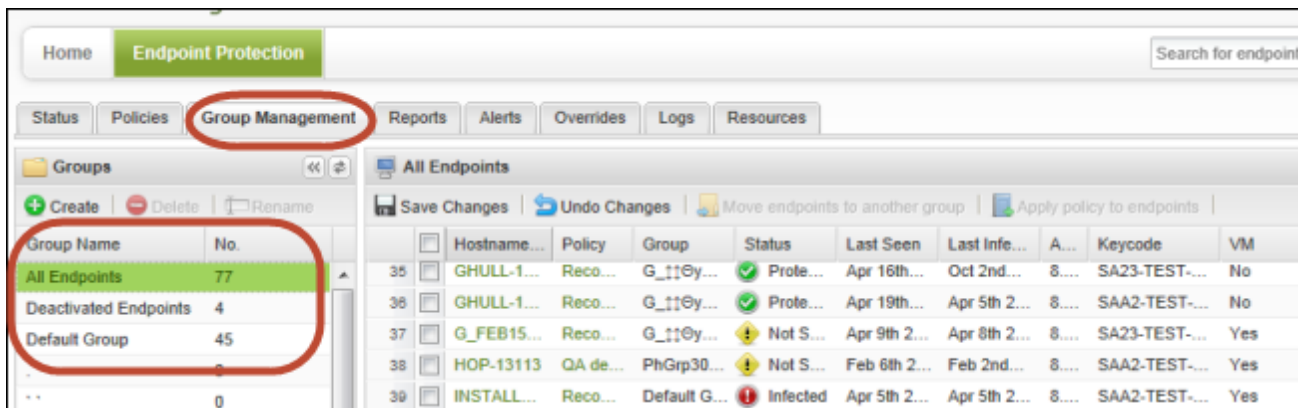
All endpoints are first assigned to your default policy. If you want to change the policy assignment, you must first define a new policy (see "Implementing policies" on page 88), then follow the instructions below to apply that policy to a group.

Applying a policy to a group

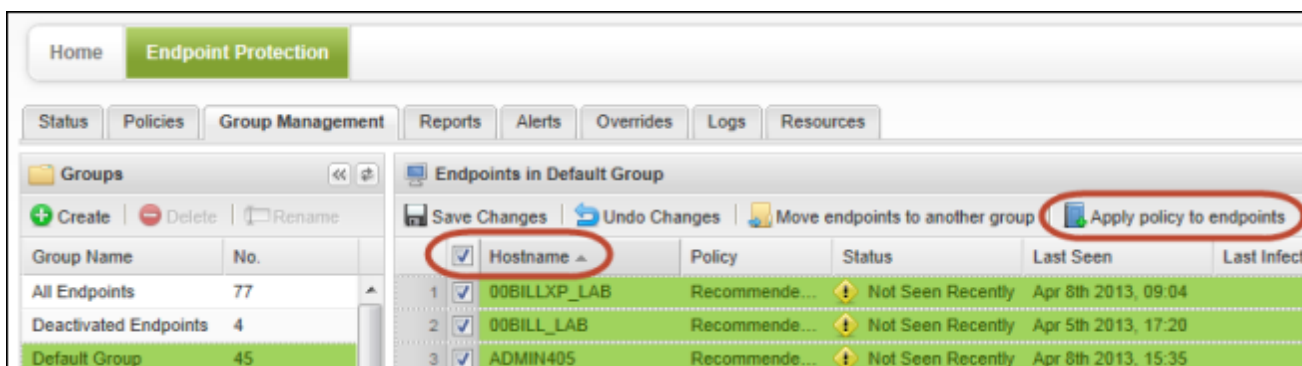
From the Group Management tab, you can apply a policy to multiple endpoints.

To apply a policy to a group of endpoints:

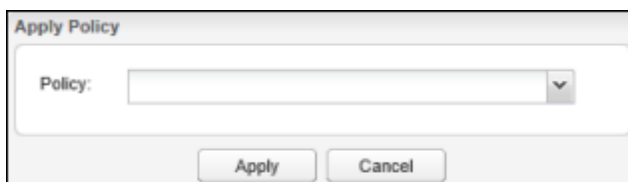
1. Click the **Group Management** tab.
2. From the **Groups** panel on the left, select a group that includes the desired endpoints.



3. From the **Endpoints** panel on the right, select one or more endpoints.
Tip: You can select all endpoints within the selected group by clicking the **Hostname** checkbox at the top of the list (first column).
4. Click **Apply policy to endpoints** from the command bar.
Note: If the group has more than one page of endpoints, the dialog prompts you to apply the policy either to the endpoints on the current page or to all pages of endpoints.



5. Select the new policy for the group, and click **Apply**.



6. Check the **Policy** column to make sure the new policy is applied to the selected endpoints.

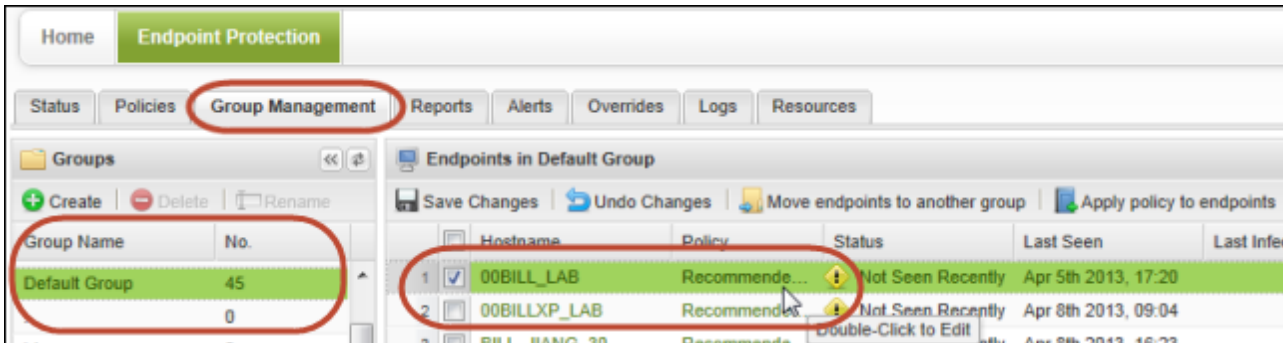
Applying a policy to a single endpoint

If you want to apply a policy to only one endpoint, the quickest method is to double-click in the Policy column and change it there.

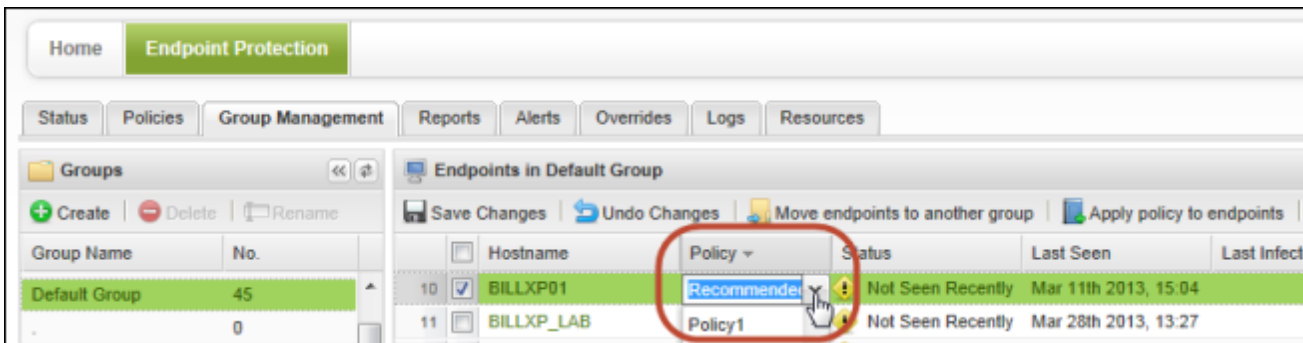
To apply a policy to an individual endpoint:

1. Click the **Group Management** tab.
2. From the **Groups** panel on the left, select a group that includes the desired endpoint.

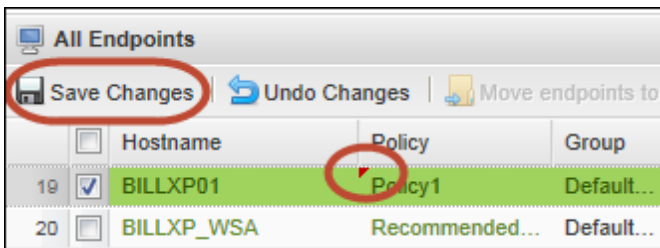
- From the **Endpoints** panel on the right, select the endpoint.



- In the **Policy** column of the selected endpoint, double-click the policy name to open a drop-down of available policies.



- Select the policy and press **Enter**.
You will see the new policy name in the column with a red flag at the upper left corner. This indicates that your changes are in a draft stage and you can still select **Undo Changes** to revert back to the previous settings. If desired, you can continue making other changes in this panel until you are ready to save the changes.
- To apply the change, click **Save Changes**.



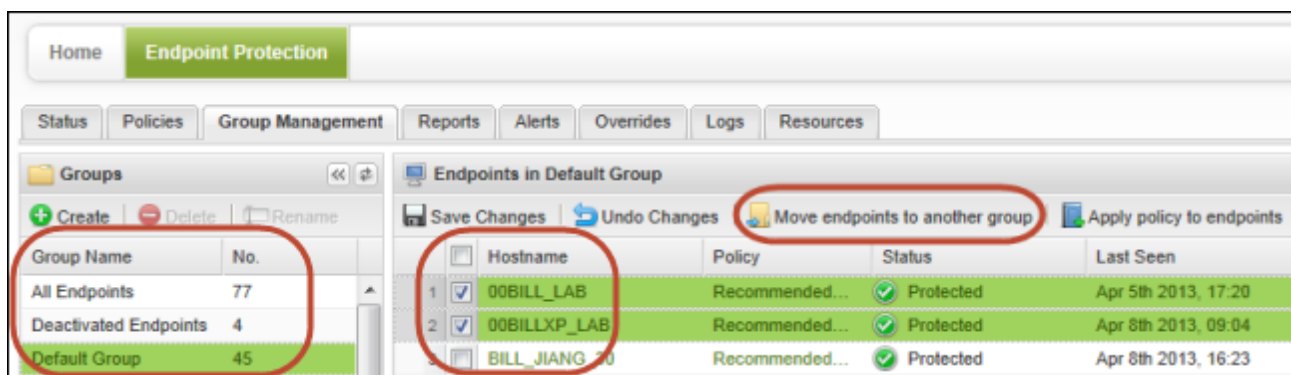
The red flag is then removed from the row.

Moving endpoints to another group

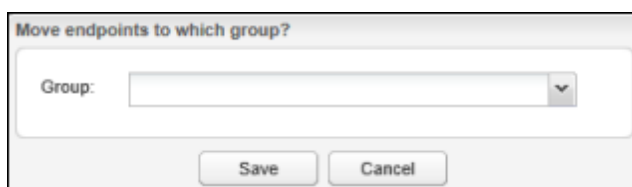
You can move endpoints into a different group, as described in this section. You can move individual endpoints or an entire group of endpoints.

To move endpoints to another group:

1. Click the **Group Management** tab.
2. From the **Groups** panel on the left, select the group that contains the endpoints you want to move.
Note: For this procedure you must select a specific group, not **All Endpoints**.
3. From the **Endpoints** panel on the right, select one or more endpoints.
Tip: You can select all endpoints within the selected group by clicking the **Hostname** checkbox at the top of the list (first column).
4. Click **Move endpoints to another group** from the command bar.
Note: If the group has more than one page of endpoints, the dialog prompts you to apply the policy either to the endpoints on the current page or to all pages of endpoints.



5. When the Move dialog opens, click the drop-down arrow to display the list of groups. Select the group from the drop-down field and click **Save**.



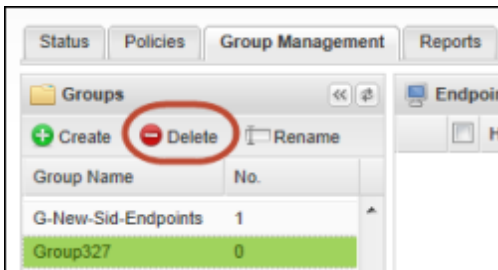
6. Click the group you selected from the left panel. Make sure all the endpoints are shown in the Endpoints panel on the right.

Deleting groups

In the Group Management tab, you can easily delete a group from the list and move its endpoints to another group. (You cannot retrieve a deleted group; however, you can re-use a deleted group name.)

To delete a group:

1. Click the **Group Management** tab.
2. Select the group from the left panel.
3. Click **Delete** from the command bar.



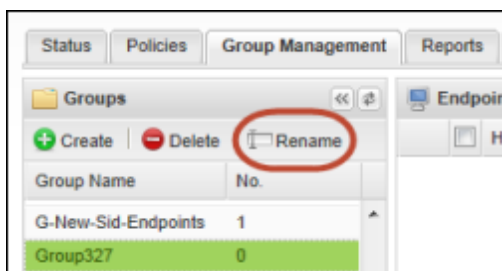
4. Click **Yes** at the prompt.
If endpoints are assigned to this group, another dialog asks you to select a group where you want the endpoints moved.
5. Select the target group, then click **Save**.

Renaming groups

In the Group Management tab, you can easily rename a group in the list. The endpoints remain in that renamed group; you do not need to move them.

To rename a group:

1. Click the **Group Management** tab.
2. Select the group from the left panel.
3. Click **Rename** from the command bar.



The Rename Group dialog opens

4. Enter a new name and description, then click **Rename Group**.

Chapter 7: Viewing Reports

To generate reports, see the following topics:

Generating Endpoint Protection reports	132
Generating the Agent Version Spread report	134
Generating the Agents Installed report	137
Generating the All Threats Seen report	139
Generating the All Undetermined Software Seen report	141
Generating the Endpoints with Threats on Last Scan report	143
Generating the Endpoints with Undetermined Software on Last Scan report	146
Generating the Threat History (Collated) report	148
Generating the Threat History (Daily) report	152

Generating Endpoint Protection reports

With Endpoint Protection, you can view detailed reports about SecureAnywhere versions and threat activity on the endpoints. The following table provides suggestions for the types of reports you might want to generate, depending on your business needs.

Reports	
To locate endpoints with different SecureAnywhere versions installed:	<p>Generate the Agent Version Spread report. (An <i>agent</i> is the SecureAnywhere software running on the endpoint.) You can use this report to locate endpoints that should be upgraded.</p> <p>Note: You can also view the Agent Version Spread pie chart shown on the Status panel, although this chart is less detailed than the Agent Version Spread report.</p> <p>See "Generating the Agent Version Spread report" on page 134.</p>
To locate endpoints with newly installed SecureAnywhere software:	<p>Generate the Agent Installed report. From here, you can see the dates when SecureAnywhere was installed on an endpoint, as well as the number of endpoints receiving the installations. See "Generating the Agents Installed report" on page 137.</p>
To locate and manage detected threats:	<p>Generate either the All Threats Seen report or the Endpoints with Threats on Last Scan report.</p> <ul style="list-style-type: none"> • The All Threats Seen report lists threats by filename, along with where SecureAnywhere detected them. From here, you can create an override for a file or restore it from quarantine. See "Generating the All Threats Seen report" on page 139. • The Endpoints with Threats on Last Scan report shows threats by endpoint location. From here, you can change the endpoint's policy, run a scan, create an override for a file, or restore a file from quarantine. See "Generating the Endpoints with Threats on Last Scan report" on page 143.

Reports	
To locate files classified as Undetermined:	<p>Generate either the All Undetermined Software Seen or the Endpoints with Undetermined Software on Last Scan report.</p> <ul style="list-style-type: none"> • The All Undetermined Software Seen report shows a list of files that are classified as "Undetermined" (they appear legitimate, but also exhibit questionable behavior). This report lists items by filename, along with where SecureAnywhere detected them. You can use this report to create overrides and tag files as either Good or Bad, so SecureAnywhere knows how you want to classify them in the future. See "Generating the All Undetermined Software Seen report" on page 141. • The Endpoints with Undetermined Software on Last Scan report shows a list of endpoints reporting Undetermined files during the last scan. You can use this report to create overrides and tag files as either Good or Bad, so SecureAnywhere knows how you want to classify them in the future. See "Generating the Endpoints with Undetermined Software on Last Scan report" on page 146.
To view a summary of detected threats:	<p>Generate the Threat History (Collated) report. This report shows a bar chart for endpoints with detected threats and blocked programs. From here, you can create overrides for blocked programs and restore files from quarantine. See "Generating the Threat History (Collated) report" on page 148.</p>
To view a summary of threats detected on a daily basis:	<p>Generate the Threat History (Daily) report. This report shows each day where SecureAnywhere found threats on endpoints. See "Generating the Threat History (Daily) report" on page 152.</p>

Generating the Agent Version Spread report

To locate endpoints with different SecureAnywhere versions installed, you can generate the Agent Version Spread report. (An *agent* is the SecureAnywhere software running on the endpoint.) You can use this report to locate endpoints that should be upgraded. The report displays a bar chart showing the version numbers in your network and the endpoints using each version.

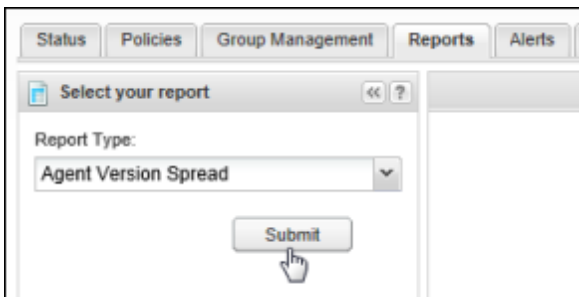
You can modify the report data as follows:

- View all versions within a selected group, which is helpful if you need to narrow search results to a specific set of endpoints.
- Drill down to see the endpoints using a specific version, which is helpful if you want to determine which endpoints should be upgraded.

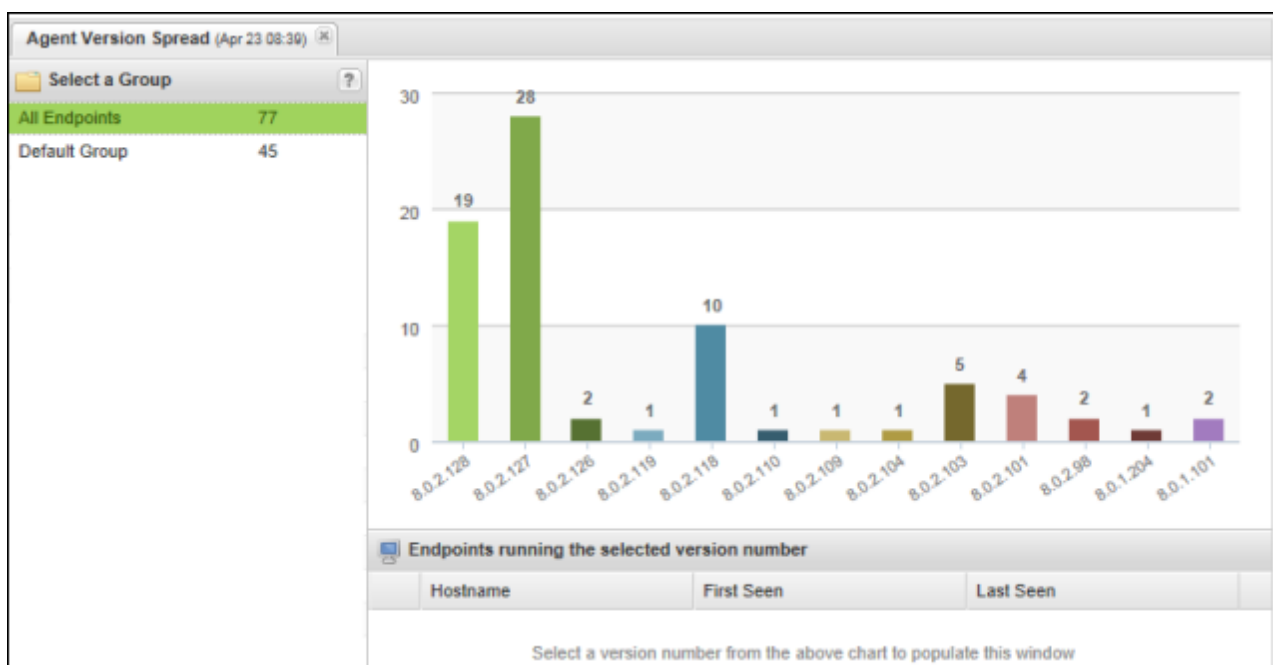
Note: You can quickly glance at the Status tab to see a pie chart of the agent version spread. For more information, see "Viewing an agent version overview" on page 85.

To generate the Agent Version Spread report:

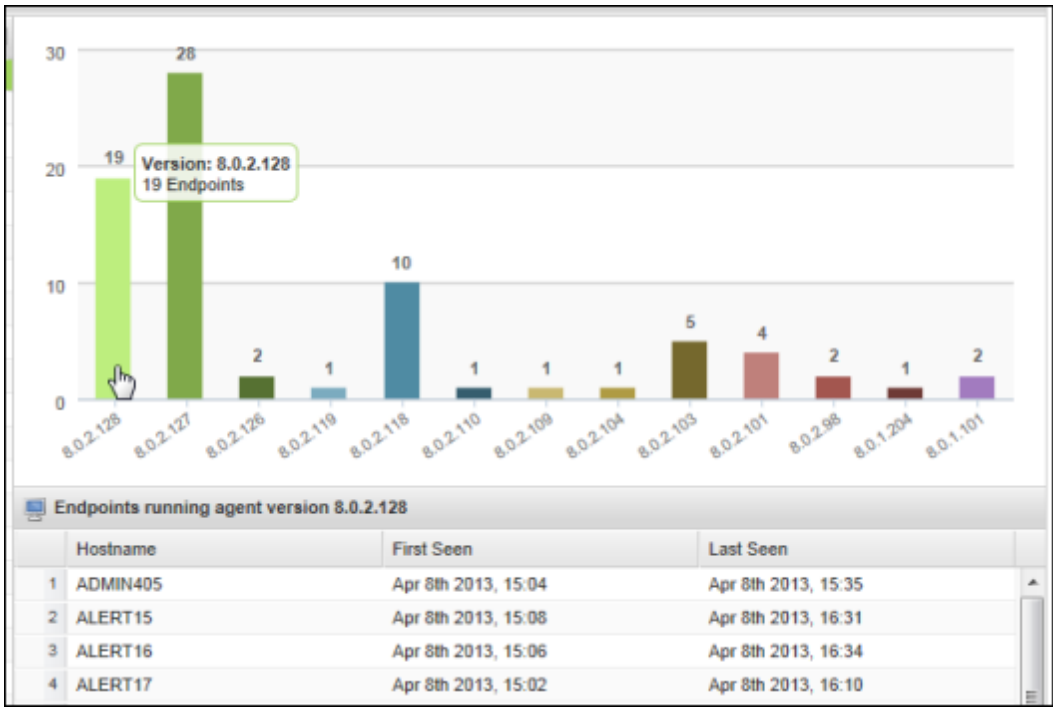
1. Click the **Reports** tab.
2. In the **Report Type** field, click the drop-down arrow to display a list of reports.
3. Select **Agent Version Spread** and click **Submit**.



A list of groups opens along with the Agent Version Spread report, as shown in the following example.



4. To view data for a specific group, click the group name on the left. The bar chart redisplay the data with only the selected group.
5. To view the endpoints using the version, click a bar to see details. The bottom panel displays data about each endpoint.



- If desired, you can show or hide additional data for the report. Click a column header to open the drop-down menu, then click in the checkboxes to select the columns to add or remove. For descriptions of the data in the columns, see "Sorting data in tables and reports" on page 26.

Generating the Agents Installed report

To see a chart of SecureAnywhere installations, generate the Agents Installed report. (An *agent* is the SecureAnywhere software running on the endpoint.) This report displays a bar chart showing the dates when SecureAnywhere was installed on endpoints, as well as the number of endpoints receiving the installations. You can modify the report data as follows:

- View all SecureAnywhere installations within a selected policy or group, which is helpful if you need to narrow search results to a specific set of endpoints.
- Drill down to see the endpoints with SecureAnywhere installed on the same date, which is helpful if you need to narrow the results to a time period and need to assign policies to a set of endpoints installed on a specific date.

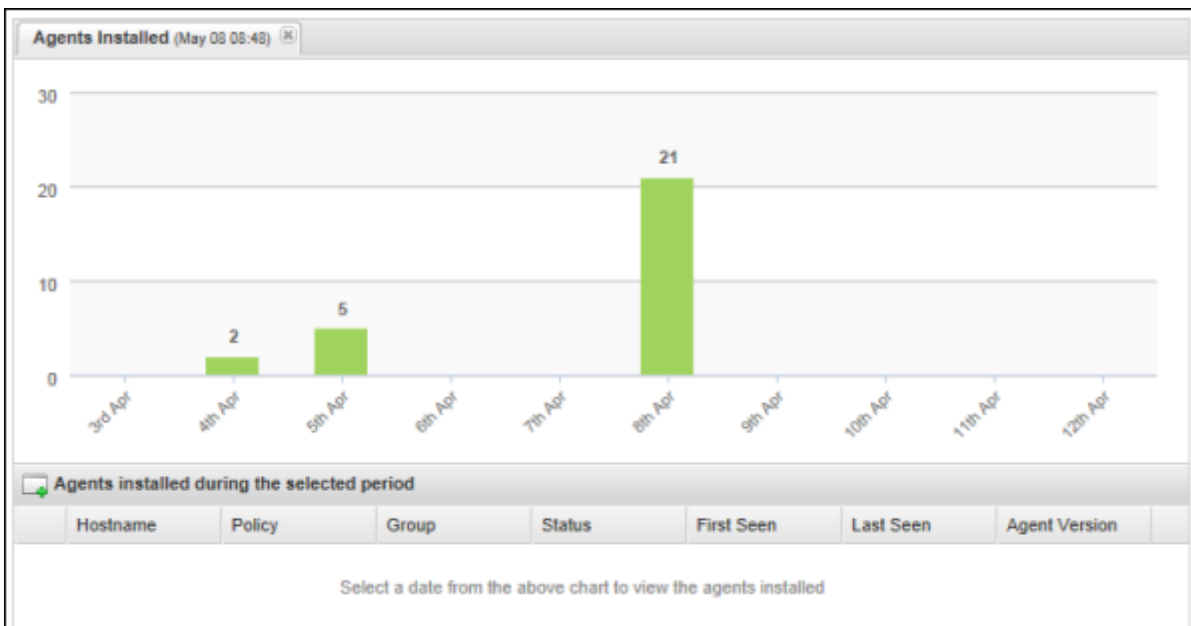
To generate the Agents Installed report:

1. Click the **Reports** tab.
2. In the **Report Type** field, click the drop-down arrow to display a list of reports.
3. Select **Agents Installed**.
4. If desired, select a specific policy or group.
Otherwise, the report data shows all policies and groups, and may take a long time to generate (depending on your environment).
5. In the bottom two fields, enter a start and end date for the report data.
6. Click **Submit**.

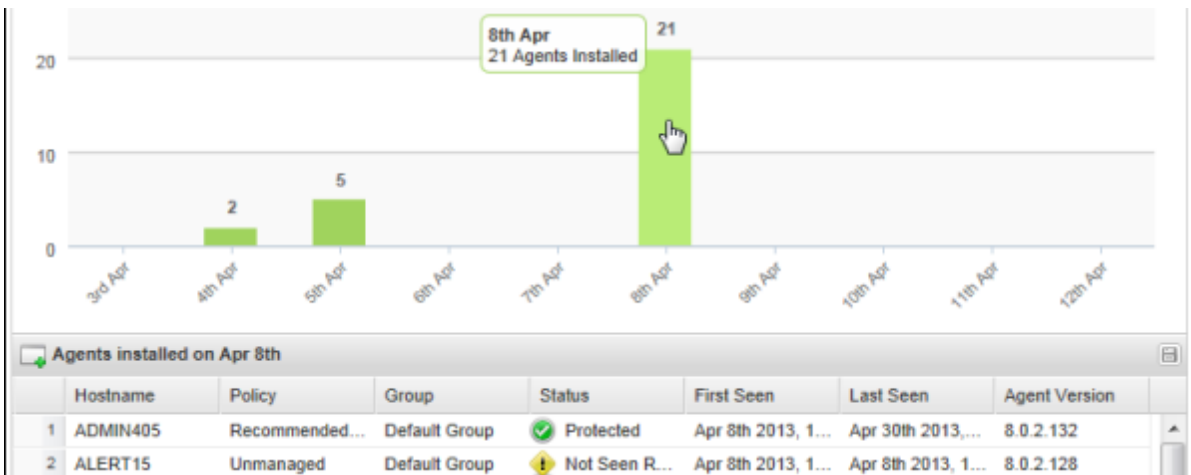
The screenshot shows a web interface with a 'Reports' tab selected. A dialog box titled 'Select your report' is open. It contains the following fields:

- Report Type:** A dropdown menu with 'Agents Installed' selected.
- Policy:** A dropdown menu with 'All' selected.
- Group:** A dropdown menu with 'All' selected.
- Between:** An empty text input field with a calendar icon to its right.
- And:** An empty text input field with a calendar icon to its right.
- Submit:** A button at the bottom of the dialog.

The report opens in the right panel, as shown in the following example.



- To view the endpoints where SecureAnywhere was installed on a specific date, click a bar to see details.
The bottom panel displays data about each endpoint.



- If desired, you can show or hide additional data for the report. Click a column header to open the drop-down menu, then click in the checkboxes to select the columns to add or remove. For descriptions of the data in the columns, see "Sorting data in tables and reports" on page 26.

Generating the All Threats Seen report

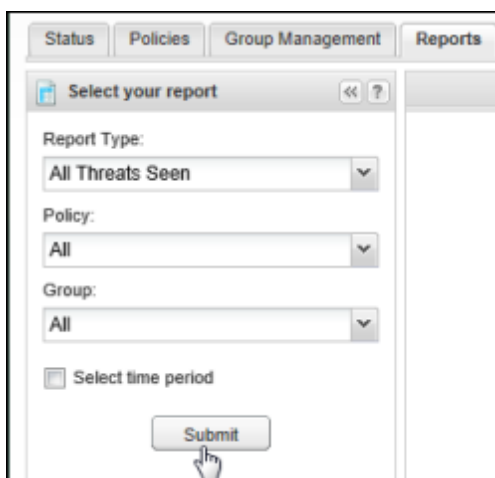
To locate and manage detected threats, you can generate the All Threats Seen report. This report lists threats by filename, along with when and where SecureAnywhere detected them. This report might show duplicate entries if the threats were detected multiple times or in multiple places. From here, you can create an override for a file or restore it from quarantine.

You can modify the report data as follows:

- View all detected threats within a selected policy or group, which is helpful if you need to narrow search results to a specific set of endpoints.
- Drill down to see the threats detected within a date range, which is helpful if you want to narrow the search results to a specific time period.

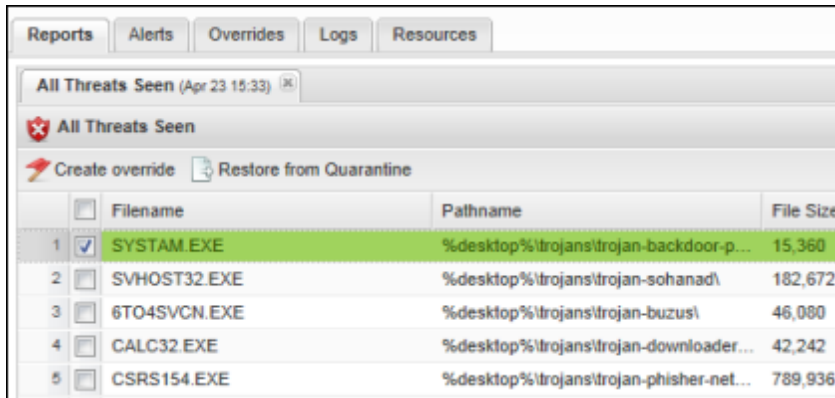
To generate the All Threats Seen report:

1. Click the **Reports** tab.
2. In the **Report Type** field, click the drop-down arrow to display a list of reports.
3. Select **All Threats Seen**.
4. If desired, select a specific policy and group.
Otherwise, the report data shows all policies and groups, and may take a long time to generate (depending on your environment).
5. Optionally, you can click the **Select time period** checkbox to enter a date range for the data.
6. Click **Submit**.



The report opens in the right panel. Each threat is listed by its filename, along with where and when

SecureAnywhere detected and removed it.



7. From this panel, you have the following options:

- **Create override:** If you want to bypass Endpoint Protection and designate the file as Good (allow the file to run) or Bad (detect and quarantine the file), click **Create override** from the command bar. For further instructions, see "Applying overrides to files from reports" on page 172.
- **Restore from Quarantine:** If the file is safe and you want to restore it to the original location on the endpoint, click **Restore from Quarantine** from the command bar.

8. If desired, you can show or hide additional data for the report. Click a column header to open the drop-down menu, then click in the checkboxes to select the columns to add or remove. For descriptions of the data in the columns, see "Sorting data in tables and reports" on page 26.

Generating the All Undetermined Software Seen report

SecureAnywhere may sometimes detect a file that appears legitimate, but also exhibits questionable behavior. In these cases, it classifies the file as "Undetermined." To locate files that SecureAnywhere classified as "Undetermined," you can generate the All Undetermined Software Seen report. The All Undetermined Software Seen report shows all undetermined software (typically executable files) that SecureAnywhere cannot classify as either safe or as malware.

This report lists items by filename, along with when and where SecureAnywhere detected them. This report might show duplicate entries if the undetermined software was detected multiple times or in multiple places. You can also use this report to create overrides and tag files as either Good or Bad, so SecureAnywhere knows how you want to classify them in the future.

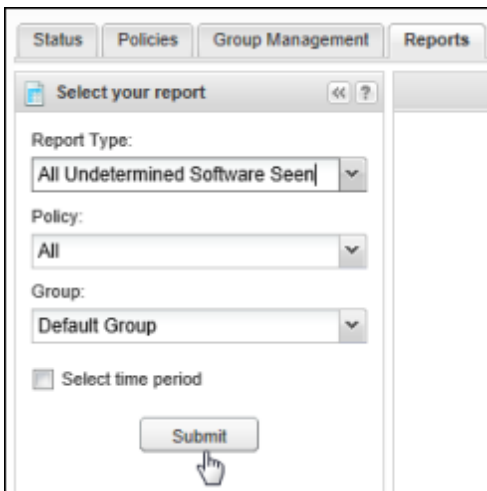
Note: To view the most recent endpoints with undetermined software, see "Generating the Endpoints with Threats on Last Scan report" on page 143.

From the report, you can modify the report data as follows:

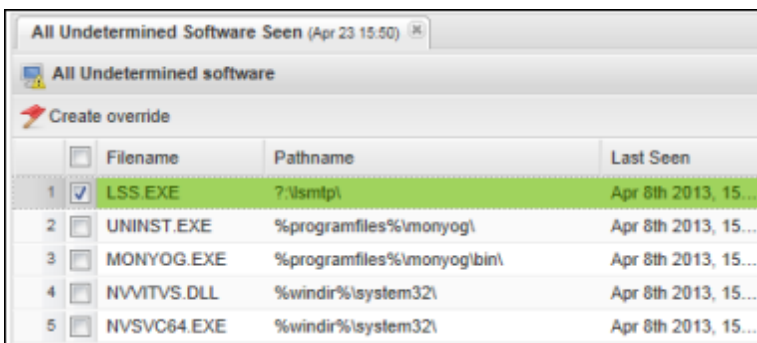
- View all undetermined software within a selected policy or group, which is helpful if you need to narrow search results to a specific set of endpoints.
- Drill down to see the files detected within a date range, which is helpful if you want to narrow the search results to a specific time period.

To generate the All Undetermined Software Seen report:

1. Click the **Reports** tab.
2. In the **Report Type** field, click the drop-down arrow to display a list of reports.
3. Select **All Undetermined Software Seen**.
4. If desired, select a specific policy and group.
Otherwise, the report data shows all policies and groups, and may take a long time to generate (depending on your environment).
5. Optionally, you can click the **Select time period** checkbox to enter a date range for the data.
6. Click **Submit**.



The report opens in the right panel:



7. From this panel, you can select a file and click **Create override** to reclassify it as follows:

- **Good:** Always allow the file to run on the endpoint. Do not detect the file during scans or send it to quarantine. After you select Good, the file is listed in the Overrides tab with Good as the Manual Determination, but the Cloud Determination remains Undetermined.
- **Bad:** Always send the file to quarantine when detected during scans. After you select Bad, the file is listed in the Overrides tab with Bad as the Manual Determination, but the Cloud Determination remains Undetermined.

You can also select whether you want to apply this override to all policies or selected policies, so you don't need to create this override again on other endpoints.

8. If desired, you can show or hide additional data for the report. Click a column header to open the drop-down menu, then click in the checkboxes to select the columns to add or remove. For descriptions of the data in the columns, see "Sorting data in tables and reports" on page 26.

Generating the Endpoints with Threats on Last Scan report

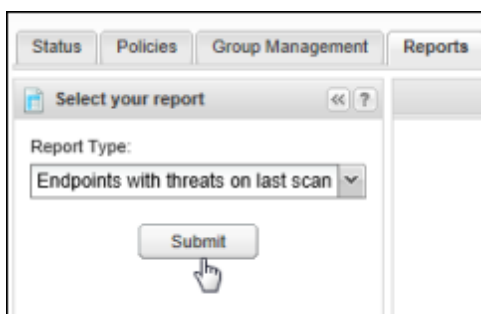
To locate and manage detected threats from the last scan, you can generate the Endpoints with Threats on Last Scan report. This report shows threats by endpoint location. From the report, you can change the endpoint's policy, run a scan, create an override for a file, or restore a file from quarantine.

You can modify the report data as follows:

- View all detected threats within a selected policy or group, which is helpful if you need to narrow search results to a specific set of endpoints.
- Drill down to see the threats detected within a date range, which is helpful if you want to narrow the search results to a specific time period.

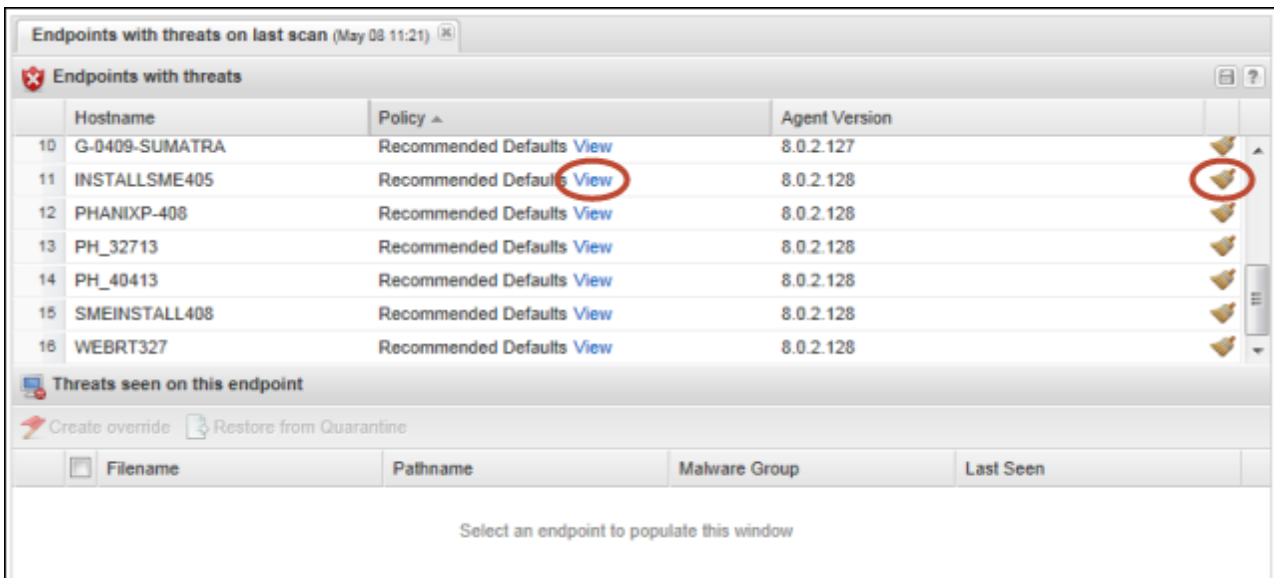
To generate the Endpoints with Threats on Last Scan report:

1. Click the **Reports** tab.
2. In the **Report Type** field, click the drop-down arrow to display a list of reports.
3. Select **Endpoints with Threats on Last Scan**, then click **Submit**.

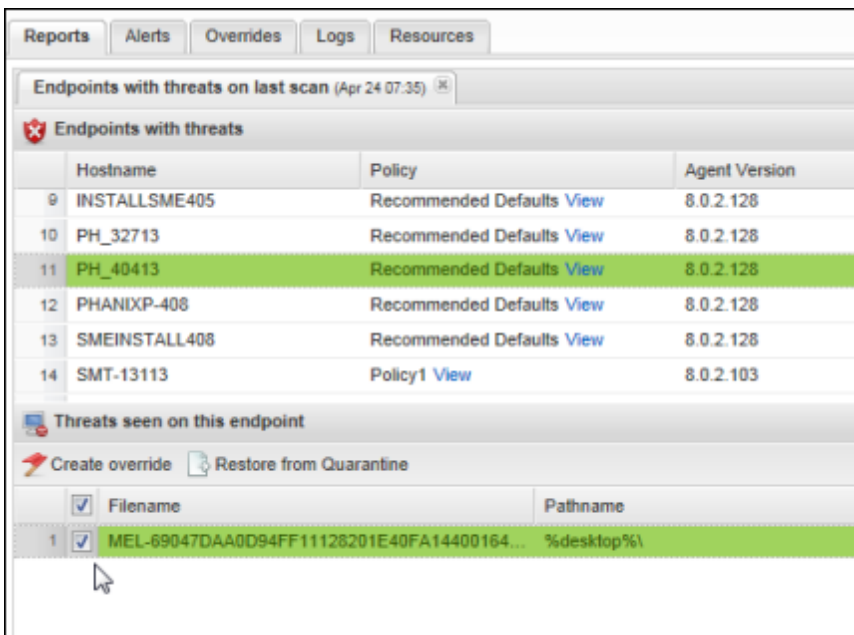


The report opens in the right panel, where you have the following options:

- **View and change the policy:** To open the policy settings for that endpoint and change the settings, you can click the **View** link. (Endpoints assigned to the Unmanaged policy have no **View** link because they are controlled at the endpoint level.)
- **Launch scan.** Click the broom icon on the far right to initiate a scan and auto-quarantine threats.



- To view more details about threats found on an endpoint, click a hostname from the upper panel to see details in the bottom panel.



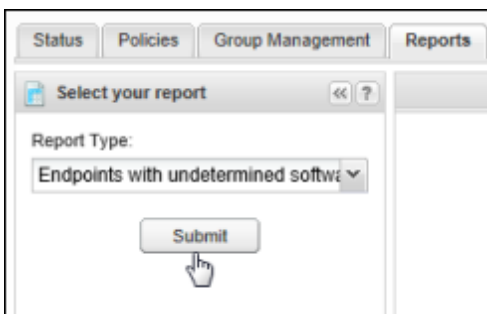
5. From the bottom panel, you can perform one of the following actions on a selected threat:
 - **Create override:** If you want to bypass Endpoint Protection and designate the file as Good (allow the file to run) or Bad (detect and quarantine the file), click **Create override** from the command bar. For further instructions, see "[Applying overrides to files from reports](#)" on page 172.
 - **Restore from Quarantine:** If the file is safe and you want to restore it to the original location on the endpoint, click **Restore from Quarantine** from the command bar.
6. If desired, you can show or hide additional data for the report. Click a column header to open the drop-down menu, then click in the checkboxes to select the columns to add or remove. For descriptions of the data in the columns, see "[Sorting data in tables and reports](#)" on page 26.

Generating the Endpoints with Undetermined Software on Last Scan report

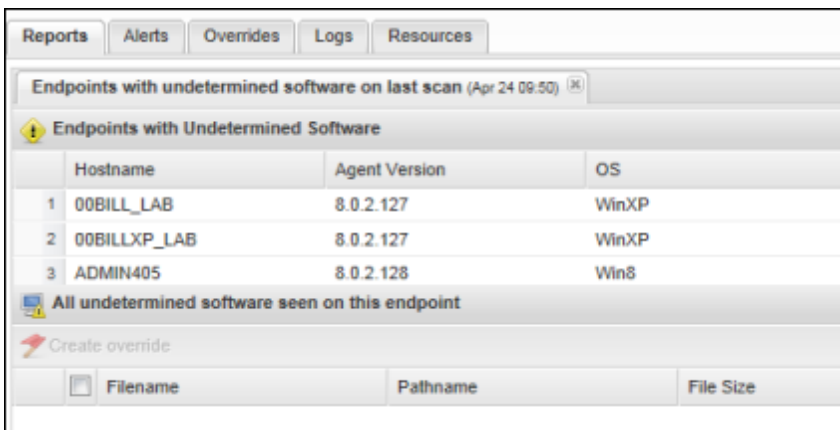
SecureAnywhere may sometimes detect a file that appears legitimate, but also exhibits questionable behavior. In these cases, it classifies the file as "Undetermined." To locate files that SecureAnywhere classified as "Undetermined" on the last scan, you can generate the Endpoints with Undetermined Software on Last Scan report. You can select an endpoint to drill down for more details about the files.

To generate the Endpoints with Undetermined Software on Last Scan report:

1. Click the **Reports** tab.
2. In the **Report Type** field, click the drop-down arrow to display a list of reports.
3. Select **Endpoint with undetermined software on last scan**, then click **Submit**.



The report opens in the right panel, showing all the endpoints.



4. To view more details about the undetermined software found, click an endpoint's row to see details in the bottom, as shown in the following example.

The screenshot shows a web-based interface for managing endpoints. The top section is titled "Endpoints with undetermined software on last scan (Apr 24 09:50)". Below this is a table of endpoints with undetermined software. The third row is highlighted in green. Below the table is a section titled "All undetermined software seen on this endpoint" with a "Create override" button. This section contains a table of files to be overridden, with the first row highlighted in green.

Endpoints with undetermined software on last scan (Apr 24 09:50)			
Endpoints with Undetermined Software			
	Hostname ▲	Agent Version	OS
1	00BILLXP_LAB	8.0.2.127	WinXP
2	00BILL_LAB	8.0.2.127	WinXP
3	ADMIN405	8.0.2.128	Win8
4	BILLXP_LAB	8.0.2.118	WinXP
5	BILLXP_WSA	8.0.2.118	WinXP
6	BILL_JIANG_30	8.0.2.127	WinXP
All undetermined software seen on this endpoint			
Create override			
	Filename	Pathname	File Size
1	<input checked="" type="checkbox"/> UNITY.DLL	%programfiles%\vmware\vmwar...	2,185,880
2	<input type="checkbox"/> DESKTOPEVENTS.DLL	%programfiles%\vmware\vmwar...	34,968
3	<input type="checkbox"/> HGFSSERVER.DLL	%programfiles%\vmware\vmwar...	18,584

5. From this panel, you can select a file and click **Create override** to reclassify the file as follows:

- **Good:** Always allow the file to run on the endpoint. Do not detect the file during scans or send it to quarantine. After you select Good, the file is listed in the Overrides tab with Good as the Manual Determination, but the Cloud Determination remains Undetermined.
- **Bad:** Always send the file to quarantine when detected during scans. After you select Bad, the file is listed in the Overrides tab with Bad as the Manual Determination, but the Cloud Determination remains Undetermined.

You can also select whether you want to apply this override to all policies or selected policies, so you don't need to create this override again on other endpoints.

6. If desired, you can show or hide additional data for the report. Click a column header to open the drop-down menu, then click in the checkboxes to select the columns to add or remove. For descriptions of the data in the columns, see "Sorting data in tables and reports" on page 26.

Generating the Threat History (Collated) report

To view a summary of detected threats, you can generate the Threat History (Collated) report. This report shows a bar chart for endpoints with detected threats and blocked programs. From here, you can create overrides for blocked programs and restore files from quarantine.

Note: To view a summary of threats, see "Generating the Threat History (Daily) report" on page 152. The Threat History (Daily) report is just a summary; you cannot manage threats from that report.

You can modify the report data as follows:

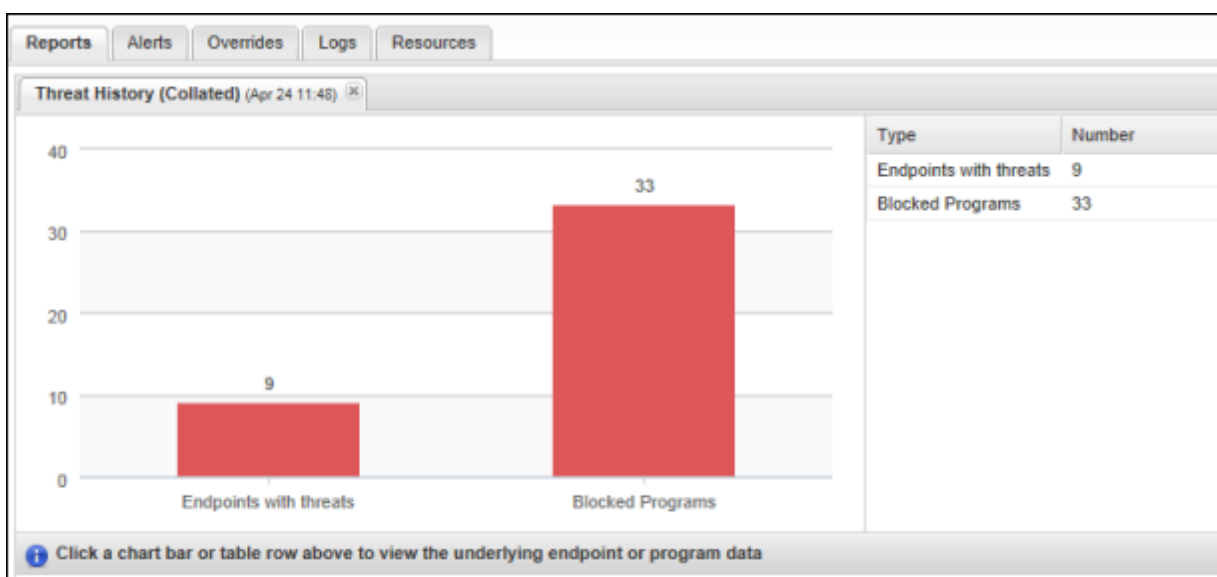
- View all threats within a selected policy or group, which is helpful if you need to narrow search results to a specific set of endpoints.
- Drill down to see the threats detected within a date range, which is helpful if you want to narrow the search results to a specific time period.

To generate the Threat History (Collated) report:

1. Click the **Reports** tab.
2. In the **Report Type** field, click the drop-down arrow to display a list of reports.
3. Select **Threat History (Collated)**.
4. If desired, select a specific policy or group.
Otherwise, the report data shows all policies and groups, and may take a long time to generate (depending on your environment).
5. In the bottom two fields, enter a start and end date for the report data.
6. Click **Submit**.

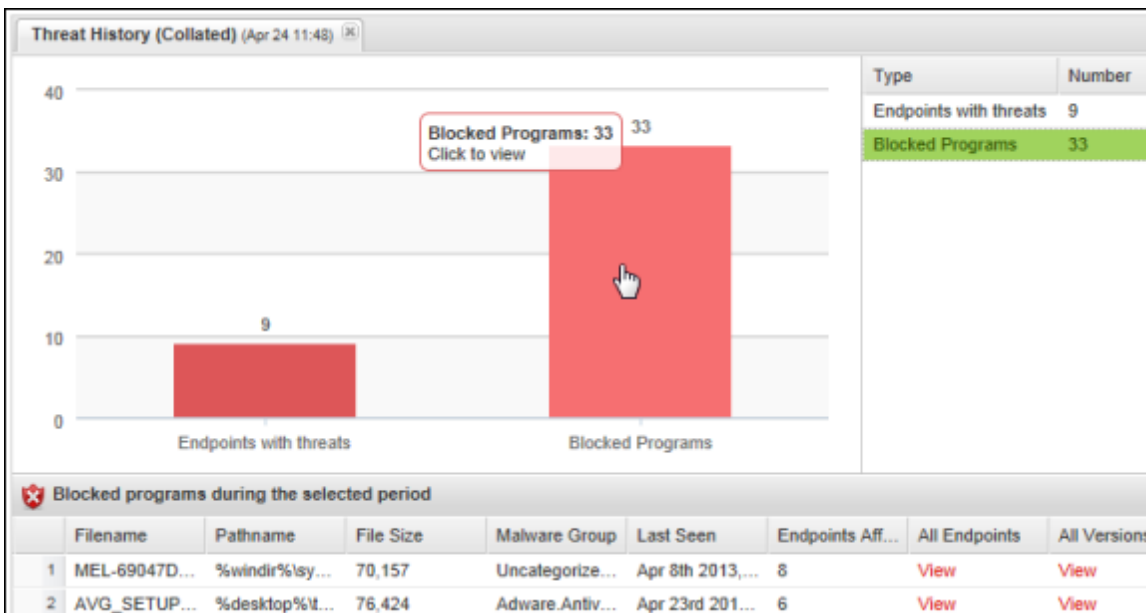
Status Policies Group Management Reports
 Select your report << ?
 Report Type:
 Threat History (Collated) v
 Policy:
 Recommended Defaults v
 Group:
 Default Group v
 Between:
 04/01/13 g
 And:
 04/24/13 g
 Submit

The report opens in the right panel.



- From this panel, you can click one of the bars to view more details about **Endpoints with threats** or **Blocked Programs**.

If you click the **Blocked Programs** bar chart, the bottom panel shows details about the programs.



- From the bottom panel you can click the **View** links in the **All Endpoints** and **All Versions** column to view more information.

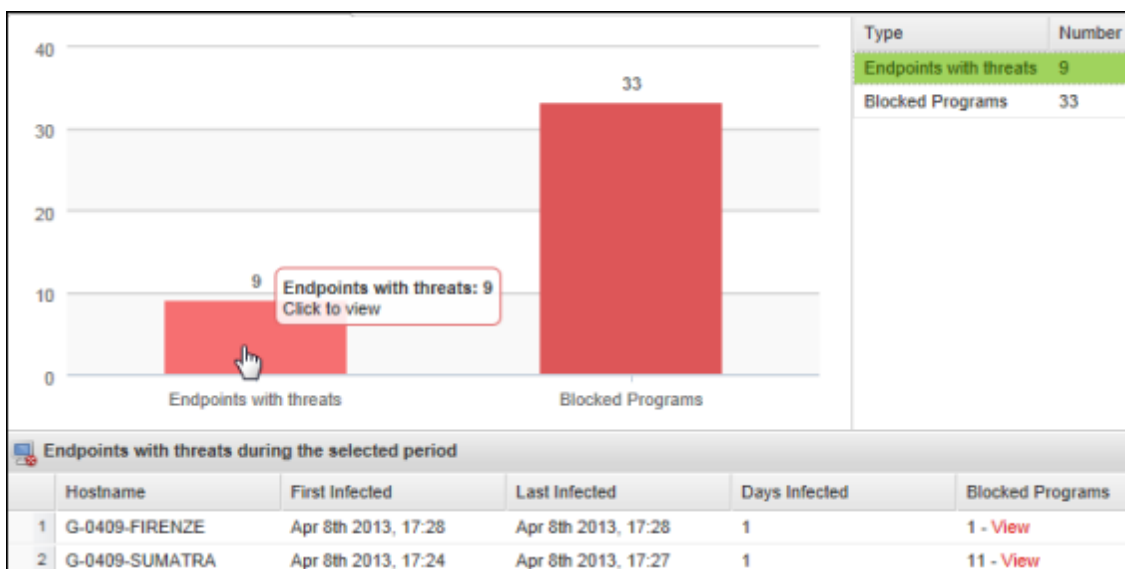
The **View** link under All Endpoints displays this panel:

	Hostname	First Infected	Days Infected
1	G_FEB15_WIN8	Apr 6th 2013, 14:24	1
2	G-0306-SUMATRA	Mar 26th 2013, 06:59	13
3	G-0408-SUMATRA	Apr 8th 2013, 15:03	1

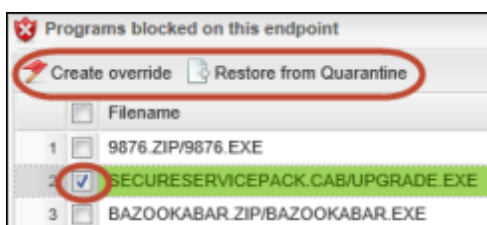
The **View** link under All Versions displays this panel:

	Filename	Pathname	Last Seen	Hostname	Cloud Determination
1	ALL EXE	%desktop%\trojan h...	Apr 8th 2013, 17:26	G-0409-SUMATRA	Bad
2	ALL EXE	%desktop%\trojan h...	Apr 8th 2013, 15:04	G-0408-SUMATRA	Bad
3	ALL EXE	?:\trojan horses\troja...	Apr 7th 2013, 18:16	G-ALERTN-VOLGA	Bad

- If you want to set an override for the file or restore it from quarantine, select the **Endpoints with threats** bar to display more information in the bottom panel.



10. Locate the row for the endpoint that has the blocked program and select the **View** link in the **Blocked Programs** column to open the following dialog:



11. From this dialog, you have the following options:

- **Create override:** If you want to bypass Endpoint Protection and designate the file as Good (allow the file to run) or Bad (detect and quarantine the file), click **Create override** from the command bar. For further instructions, see "Applying overrides to files from reports" on page 172.
- **Restore from Quarantine:** If the file is safe and you want to restore it to the original location on the endpoint, click **Restore from Quarantine** from the command bar.

You can also select whether you want to apply this override to all policies or selected policies, so you don't need to create this override again on other endpoints.

12. If desired, you can show or hide additional data for the report. Click a column header to open the drop-down menu, then click in the checkboxes to select the columns to add or remove. For descriptions of the data in the columns, see "Sorting data in tables and reports" on page 26.

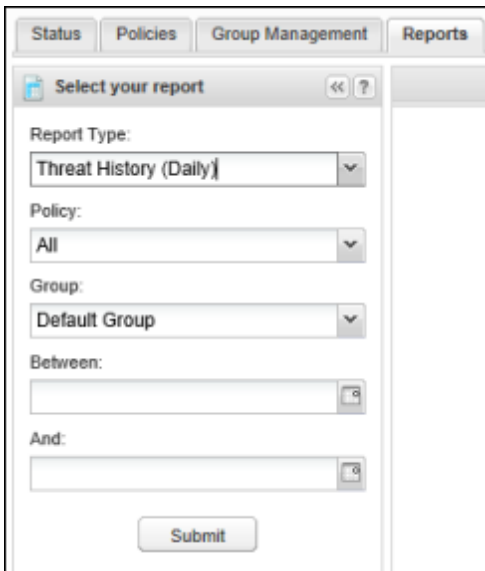
Generating the Threat History (Daily) report

To view a summary of threats detected on a daily basis, you can generate the Threat History (Daily) report. This report shows each day where SecureAnywhere found threats on endpoints. You can modify the report data as follows:

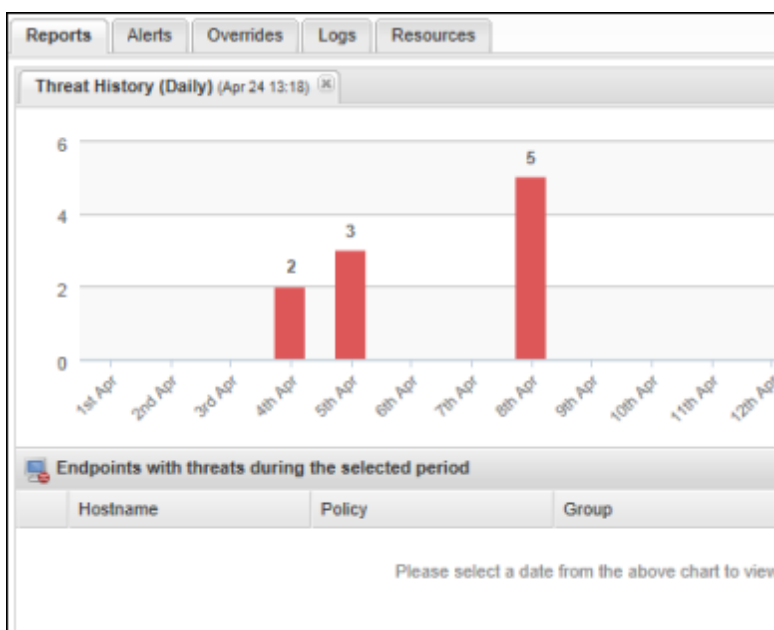
- View daily threats within a selected policy or group, which is helpful if you need to narrow search results to a specific set of endpoints.
- Drill down to see the threats detected within a date range, which is helpful if you want to narrow the search results to a specific time period.

To generate the Threat History (Daily) report:

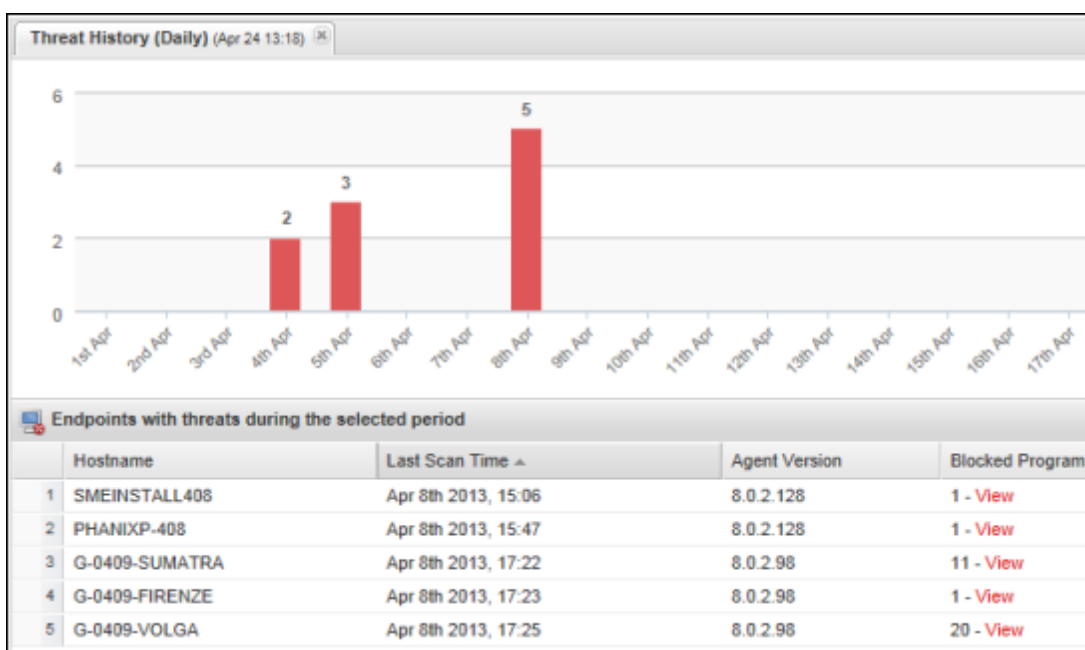
1. Click the **Reports** tab.
2. In the **Report Type** field, click the drop-down arrow to display a list of reports.
3. Select **Threat History (Daily)**.
4. If desired, select a specific policy or group. Otherwise, the report data shows all policies and groups, and may take a long time to generate (depending on your environment).
5. In the bottom two fields, enter a start and end date for the report data.
6. Click **Submit**.



The report opens in the right panel.



- To view more details about threats, click on a bar to see details for a specific day. The bottom panel shows details about the endpoints with the detected threats.



- To view more information about a block program, click a **View** link in the Blocked Programs column.

9. If desired, you can show or hide additional data for the report. Click a column header to open the drop-down menu, then click in the checkboxes to select the columns to add or remove. For descriptions of the data in the columns, see "[Sorting data in tables and reports](#)" on page 26.

Chapter 8: Managing Alerts

To learn more about alerts, see the following topics:

Implementing alerts	156
Creating a distribution list	157
Creating customized alerts	158
Viewing your defined alert messages	162
Suspending or deleting alerts	164

Implementing alerts

You can customize alert messages and send them to a distribution list whenever the following types of events occur:

- Endpoints reporting an infection
- New SecureAnywhere installations on endpoints

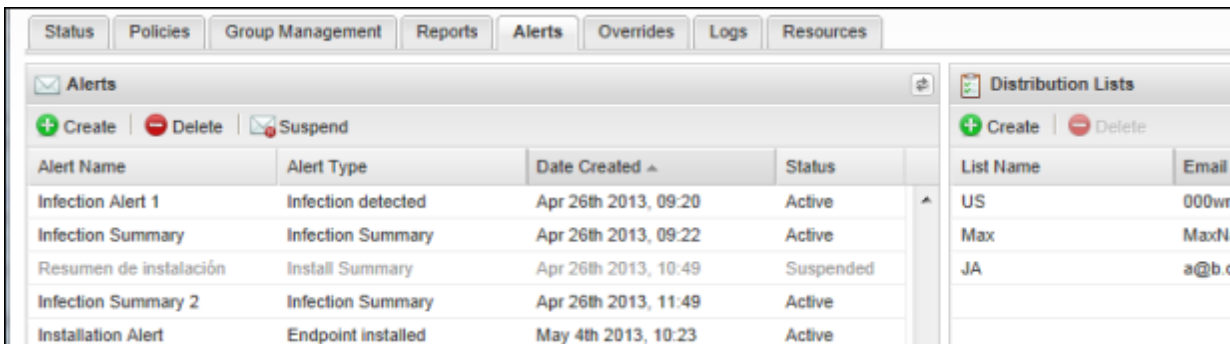
For both of these event types, you can customize the alerting method so administrators receive a message as soon as the event occurs or on a schedule (daily, weekly, or monthly). Using a setup wizard in the Alerts tab, you can customize the subject heading and body of the messages. You can also use variables to add information for the endpoints triggering the alerts, affected groups, and other specifics about the event.

Note: To customize alerts, you must have access permissions for **Alerts: Create & Edit**. To change access permissions, see "Setting permissions for portal users" on page 38.

To create customized alerts:

1. Create a distribution list based on email addresses (list members do not need to be defined in the Manage Users panel of the Management Portal). See "Creating a distribution list" on page 157.
2. Create alert messages that are sent to the distribution list whenever endpoints report an infection or SecureAnywhere is installed on an endpoint. See "Creating customized alerts" on page 158.

All your customized alerts will appear in the Alerts tab.



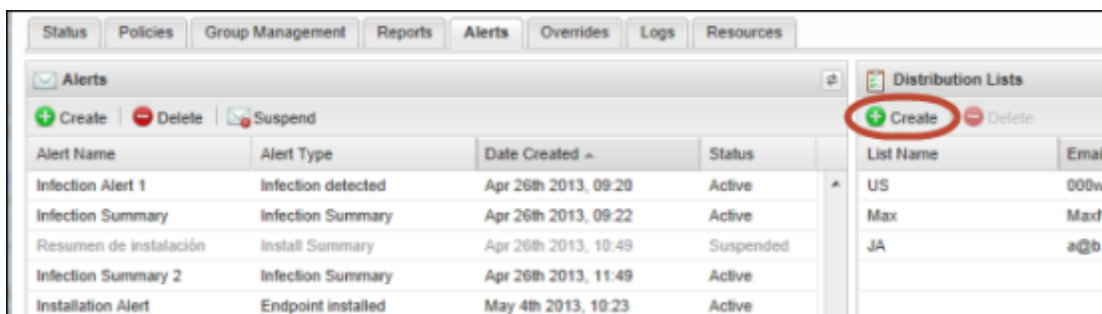
Creating a distribution list

From the Alerts tab, you can easily create a distribution list of users who will receive alert messages. For example, you might want to create a list of administrators who need to respond to threat detections at a remote office.

Note: You can also create a distribution list in the Create Alert wizard, as described in "Creating customized alerts" on page 158.

To create a distribution list:

1. Click the **Alerts** tab.
2. In the **Distribution Lists** panel on the right, click **Create** from the command bar.



3. In the dialog, enter a name for the list and the email addresses of the recipients.

The 'Create Distribution List' dialog box is shown. It has two input fields: 'List Name' and 'Email Addresses (comma separated, maximum of 10)'. The 'List Name' field contains the text 'Distribution List'. The 'Email Addresses' field contains the text 'user@company.com'. At the bottom of the dialog are 'Save' and 'Cancel' buttons.

4. Click **Save**.
The new list is added to the **Distribution Lists** panel.

If you need to delete the list later, click the name and click **Delete** from the command bar.

Creating customized alerts

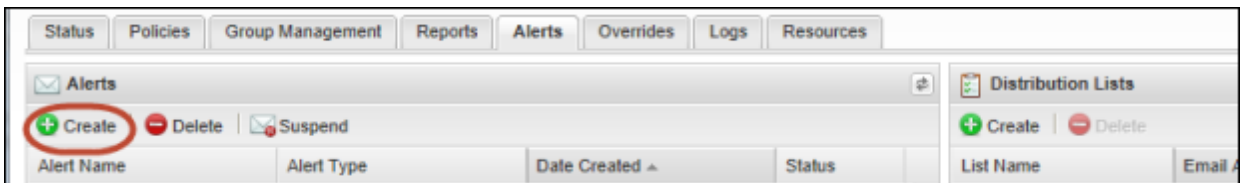
You can customize the alert messages sent to a distribution list for the following types of events:

- **Infection Detected.** An immediate message sent when an endpoint reports an infection.
- **Endpoint Installed.** An immediate message sent as soon as SecureAnywhere is installed on an endpoint and it reports into the Management Portal.
- **Infection Summary.** A summary message that provides an overview of threats detected on endpoints. The summary can be scheduled for a daily, weekly, or monthly distribution.
- **Install Summary.** A summary message that provides an overview of SecureAnywhere installations. The summary can be scheduled for a daily, weekly, or monthly distribution.

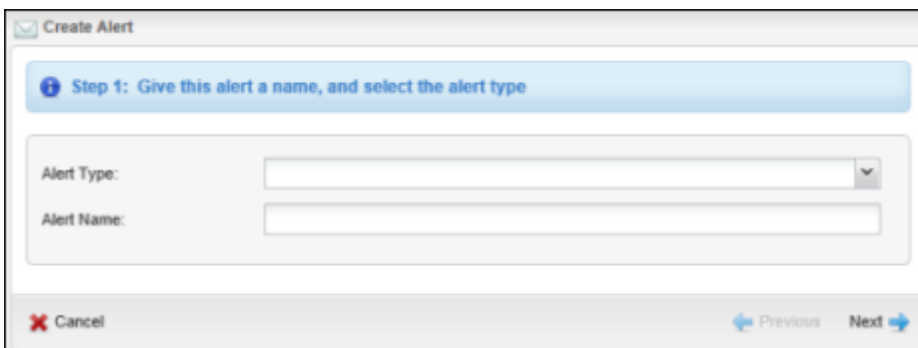
You can use the Create Alert wizard to define the messages and a distribution list, as described below. (You can also define a distribution list separately, as described in "Creating a distribution list" on page 157.)

To create a custom alert:

1. Click the **Alerts** tab.
2. In the **Alerts** panel on the left, click **Create** from the command bar.



The following dialog opens.

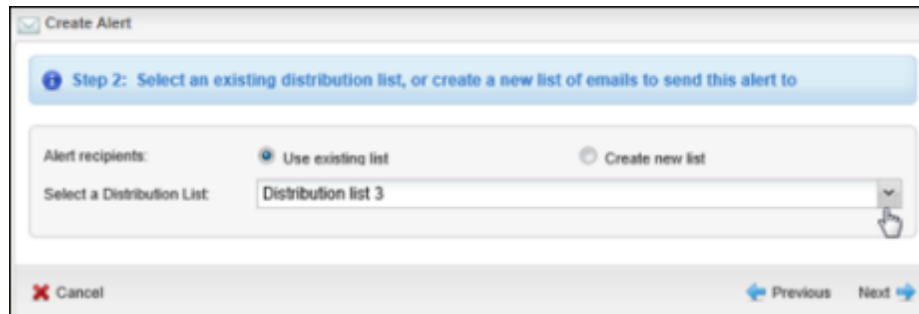


3. In the **Alert Type** field, click the drop-down arrow to select an alert type. In the **Alert Name** field, enter a description for this alert. Click **Next** at the bottom right.

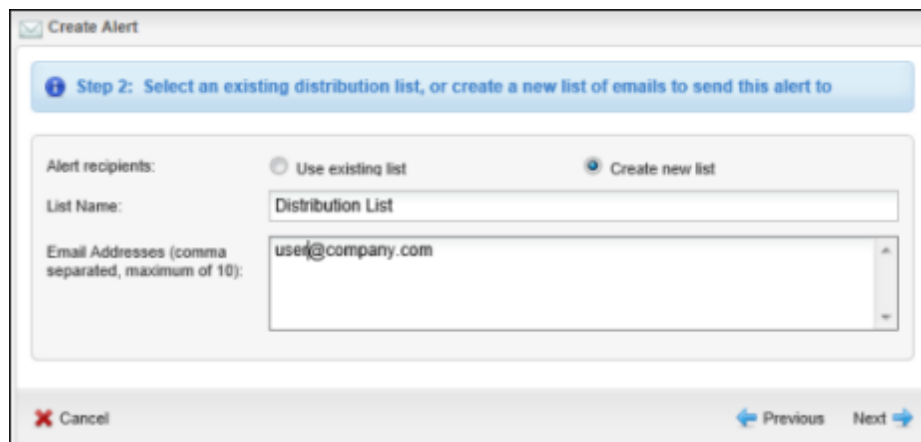
If you select one of the summary alerts, another field appears where you must select the frequency for sending the alerts: either daily, weekly, or monthly.

4. In the next panel, you can select from an existing distribution list or you can create a new one.

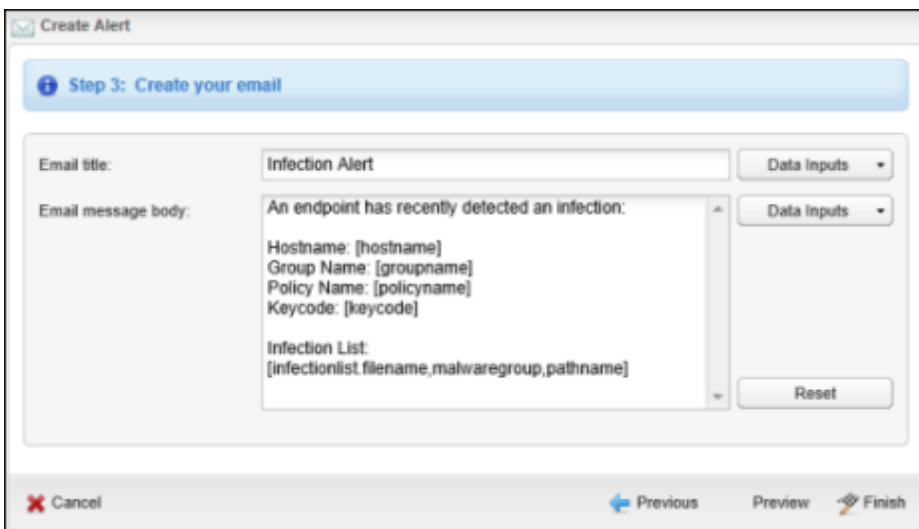
If you already created a distribution list, click **Use existing list** and then click **Next**.



If you have not yet created a distribution list, click **Create new list**, enter a list name, then enter the email addresses. When you're done, click **Next**.

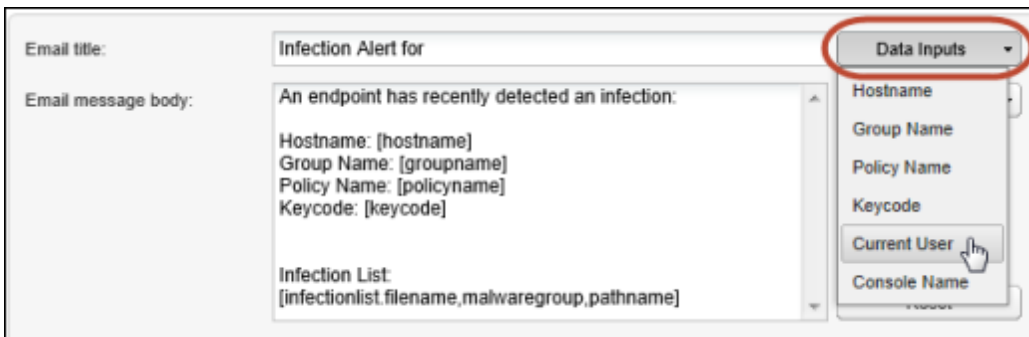


5. In the next panel, you can enter the subject and message for the email message. In the **Email title** field, enter the subject head for the message. In the **Email message body** field, enter the text for the message.



The wizard also provides "data inputs" within the text, which are variables you can use for automatically inserting such information as the hostname of the endpoint. Some data inputs are already displayed for you in the sample text. Data inputs are shown in brackets.

- 6. To add your own data inputs, click inside the text where you want a variable to appear, then click the drop-down arrow for one of the **Data Inputs** buttons. There is one button for the subject head and one for the body.



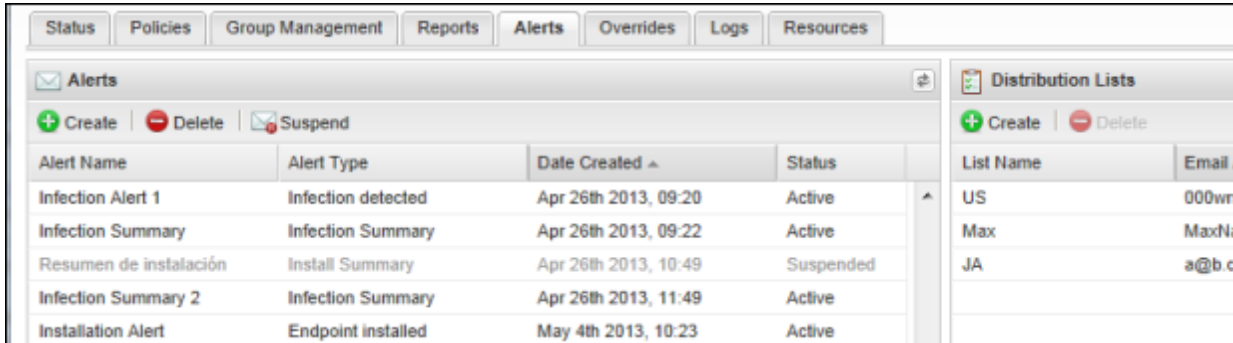
- 7. Select from the data inputs, which are all described below.
Note: Depending on the type of alert message you are defining, only the applicable data inputs appear in the drop-down menu.

Data inputs for alert messages	
Hostname	The name of the endpoint triggering the alert.
Group Name	The group assigned to the endpoint triggering the alert.
Policy name	The policy assigned to the endpoint triggering the alert.
Keycode	The keycode used for the endpoint triggering the alert.
Current User	The user of the endpoint triggering the alert.
Console Name	The name of the Console where the endpoint is included.
First Seen	The date and time when this event was first detected.
Last Seen	The date and time when this event was last detected.
Last Infected	The date and time the endpoint triggering the alert was last infected.
Operating System	The operating system version on the endpoint triggering the alert.
Agent Version	The version number of the SecureAnywhere software installed on the endpoint triggering the alert.
MAC Address	The Media Access Control address (MAC address) on the network where the endpoint triggering the alert is installed.
Workgroup	The network workgroup where the endpoint is located (if any).
Active Directory	The name of the Active Directory.
Infection List	A list of infections.
Infection Summary	A summary of the infections.
Install Summary	A summary of the SecureAnywhere installations.

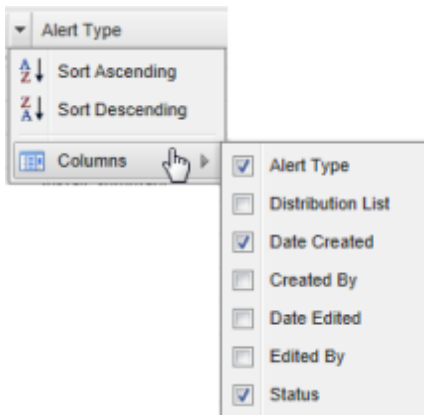
8. To view the email message, click **Preview** at the bottom of the wizard.
9. If you are satisfied with the message, click **Finish**.

Viewing your defined alert messages

All your customized alerts will appear in the Alerts tab with a status of *Active*. From here, you can edit the alert by double-clicking in its row. On the right side of the panel are the distribution lists you defined.



If desired, you can show or hide additional data about the alert messages. Click a column header to open the drop-down menu, then click in the checkboxes to select the columns to add or remove.



The columns provide the data described in the following table.

Columns in the Alerts panel	
Alert Name	The name defined in the Create Alert wizard. This column is static and cannot be hidden.
Alert Type	One of the alert types: Infection Detected, Endpoint Installed, Infection Summary, Install Summary.

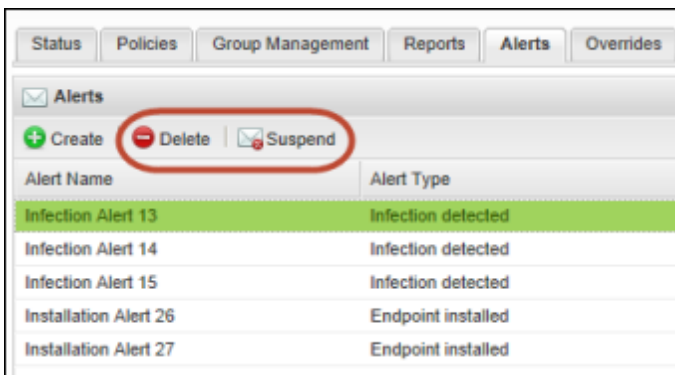
Columns in the Alerts panel	
Distribution List	The email recipients for this alert.
Date Created	The date the alert message was defined.
Created By	The administrator who created the alert message.
Date Edited	The date (if any) that the alert message was modified.
Edited By	The administrator who modified the alert message (if applicable).
Status	The alert status, which is either Active or Suspended .

Suspending or deleting alerts

After customizing alert messages for a distribution list, you may decide later that an alert is no longer necessary. You can permanently delete an alert; or if you think it might be useful again sometime in the future, you can temporarily suspend it instead.

To suspend or delete an alert:

1. Click the **Alerts** tab.
2. Select an alert from the left panel.
3. Click **Delete** or **Suspend** from the command row.



If you selected **Suspend**, the alert is grayed out in the panel with "Suspended" in the Status column. Later, you can select the alert again and click **Resume**.

If you selected **Delete**, click **Yes** in the prompt. The alert is permanently removed from Endpoint Protection.

Chapter 9: Using Overrides

To use overrides, see the following topics:

Implementing overrides	166
Applying overrides from the Overrides tab	167
Applying overrides to files from groups	170
Applying overrides to files from reports	172
Viewing overrides	174
Deleting overrides	176
Exporting overrides to a spreadsheet	177

Implementing overrides

Overrides provide administrative control of the files and applications in your environment, allowing you to designate files as Good (always run) or Bad (always quarantine). For example:

- You may decide to quarantine legitimate files for certain business purposes. For example, if you don't allow users to make Skype voice calls during business hours, you can set an override that always sends the Skype executable file to quarantine when detected during scans.
- Conversely, if Endpoint Protection is quarantining a file that you want to allow, you can set an override that ignores the file during scans.

Note: To fully manage overrides, you must have access permissions for **Overrides: MD5** and **Overrides: Determination Capability**. To change permissions, see "Setting permissions for portal users" on page 38.

To change how a file is detected and managed, you can apply one of the following overrides:

- **Good:** Always allow the file to run on the endpoint. Do not detect the file during scans or send it to quarantine.
- **Bad:** Always send the file to quarantine when detected during scans.

You can add overrides from several locations:

- From the **Overrides** tab, you can create either a "Good" or "Bad" override for any type of file. To do this, you must first scan the endpoint, save its scan log, and locate the MD5 value of the file. *MD5* (Message-Digest algorithm 5) is a cryptographic hash function that produces a 128-bit value, which acts like a fingerprint to uniquely identify a file. For more information, see "Applying overrides from the Overrides tab" on page 167.
- From the **Group Management** tab, you can search for endpoints where threats were detected and quickly apply overrides. The MD5 value is already identified for the file. For more information, see "Applying overrides to files from groups" on page 170.
- From the **Reports** tab, you can search for endpoints where threats were detected in certain reports and quickly apply overrides. The MD5 value is already identified for the file. For more information, see "Applying overrides to files from reports" on page 172.

An override can have different settings at the global level and at the policy level. Be aware that Policy settings take precedence over Group settings.

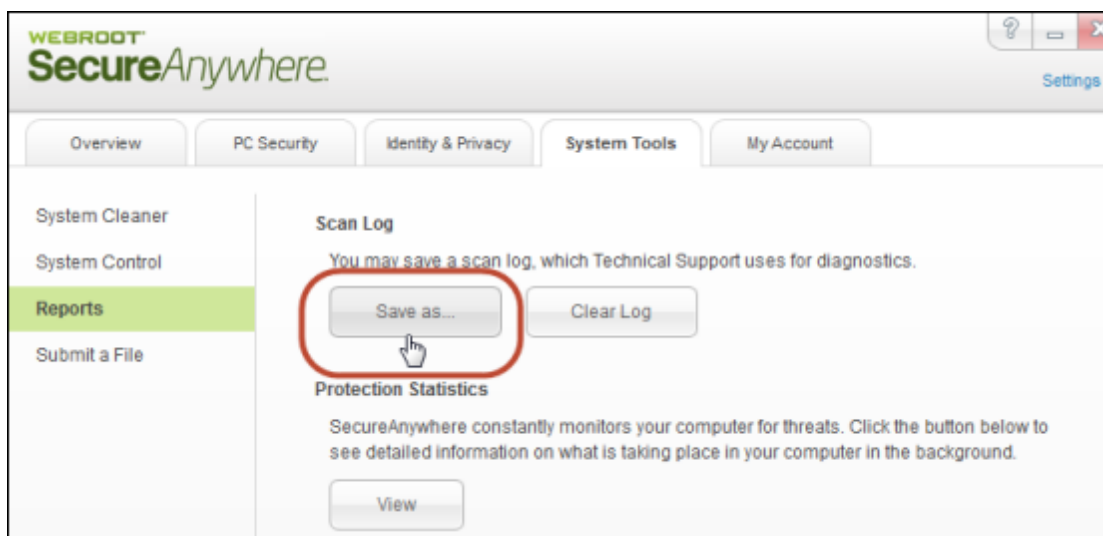
Applying overrides from the Overrides tab

When you add overrides from the Overrides tab, you must first locate the MD5 values of files by running a scan on the endpoint. When SecureAnywhere scans the device, it creates a scan log where it stores the path name, file name, and MD5 value for executables and other types of files that run a process. You need that MD5 value to create the override.

Tip: If you want to override a file designated as "Bad," you should go to the **Groups** or **Reports** tabs. These tabs show detected threats and their associated MD5 values, which saves you time in creating "Bad" overrides.

To locate and save MD5 values:

1. Run a scan on the endpoint to capture MD5 values.
You can run the Scan command either from the endpoint itself or by using the Scan command from the Groups tab (see "Issuing commands to endpoints" on page 63).
2. On the *endpoint* (the PC or other device), open SecureAnywhere. Click the **System Tools** tab, then **Reports**. In the **Scan Log** section of the page, click **Save as** and specify a name and location for the log.



3. Open the scan log and locate the MD5 value to the right of the filename.
The following example shows the MD5 value for a file named **csrss.exe**.

```
SecureAnywhere Scan Log (version v8.0.2.132)
Log saved at Thu 2013-04-25 13:43:08

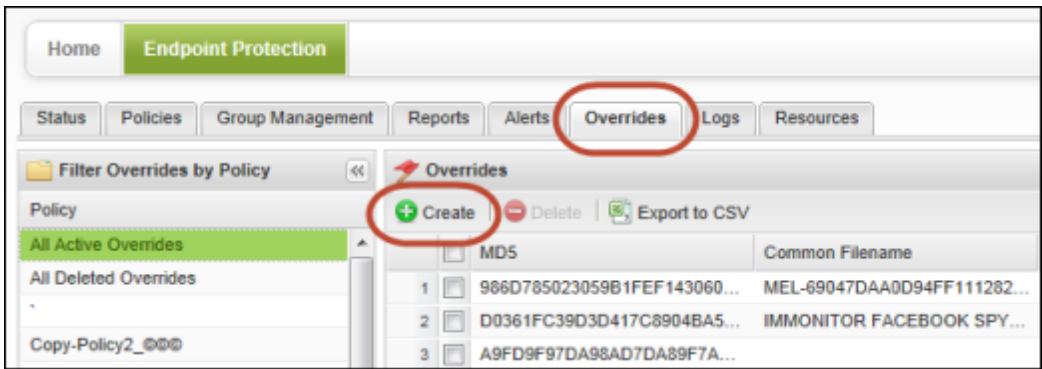
v8.0.2.132
Windows 7 Service Pack 1 (Build 7601) 64bit (Hostname: JGALL-1884L-BRM - Local IP: )
Scan Started: Thu 2013-04-25 10:00:16
Files Scanned: 2715
Malicious Files: 0
Duration: 22s

Some legitimate files are not included in this log
[G] c:\windows\system32\csrss.exe [MD5: 60C2862B4BF0FD9F582EF344C2B1EC72] [Flags: 40110000.195]
[G] c:\windows\system32\wininit.exe [MD5: 9433C28C1970033A3183FE32EB7CEBA] [Flags: 40110000.718]
[G] c:\windows\system32\services.exe [MD5: 24ACB7E58E595468E3B9AA488B9B4FCB] [Flags: 40110000.1257]
[G] c:\windows\system32\winlogon.exe [MD5: 1151818AA6F350B1DB6598E0FEA7C457] [Flags: 40110000.1493]
[G] c:\windows\system32\lsass.exe [MD5: C118A82CD78818C29AB228366EBF81C3] [Flags: 50110000.781]
[G] c:\windows\system32\lsmon.exe [MD5: 9662EE182644511439F1C53745DC1C88] [Flags: 40110000.1337]
[G] c:\windows\system32\svchost.exe [MD5: C78655BC80301D76ED4FEF1C1EA40A7D] [Flags: 50110000.424]
[G] c:\windows\system32\ntdll.dll [MD5: E73B0F1819602CB6EF176FB78D76A47B] [Flags: 40001000.1777]
[G] c:\windows\system32\kernel32.dll [MD5: AC086F41882FC6ED186962D770EBF1D2] [Flags: 00080000.17592]
[G] c:\windows\system32\kernelbase.dll [MD5: E954A79D6A754A5475582CACE1565E6] [Flags: 00000000.17567]
[G] c:\windows\system32\advapi32.dll [MD5: 95E2376B3323F062EB562B8586D0F14A] [Flags: 40000000.1438]
```

- 4. Copy the value, so you can paste it into the Management Portal.

To add an MD5 override from the Overrides tab:

- 1. Return to Endpoint Protection and click the **Overrides** tab.
- 2. Click **Create** from the command bar.



- 3. In the **Create Override** dialog, paste the copied MD5 value into the **MD5** field.

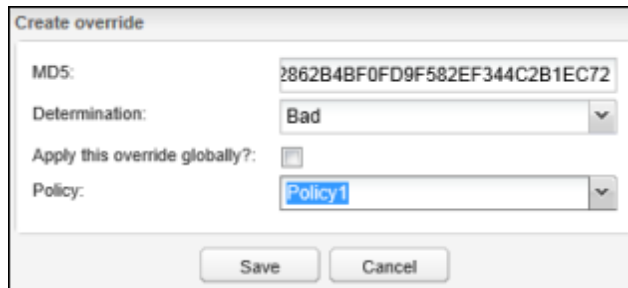
MD5: 2862B4BF0FD9F582EF344C2B1EC72

Determination: [dropdown]

Apply this override globally?:

Save Cancel

4. Open the **Determination** drop-down menu by clicking the arrow to the right of the field. Select one of the following:
 - **Good**: Always allow the file to run.
 - **Bad**: Always send the file to quarantine.
5. You can apply this override globally or to an individual policy, as follows:
 - To apply the override to all policies, keep the **Apply the override globally** checkbox selected.
 - To select an individual policy for the override, deselect the checkbox. When the **Policy** field appears, click the drop-down arrow to the right of the field and select a policy.



The screenshot shows a dialog box titled "Create override". It contains the following fields and controls:

- MDS:** A text field containing the hash value "2862B4BF0FD9F582EF344C2B1EC72".
- Determination:** A dropdown menu currently showing "Bad".
- Apply this override globally?:** A checkbox that is currently unchecked.
- Policy:** A dropdown menu currently showing "Policy1".
- At the bottom, there are two buttons: "Save" and "Cancel".

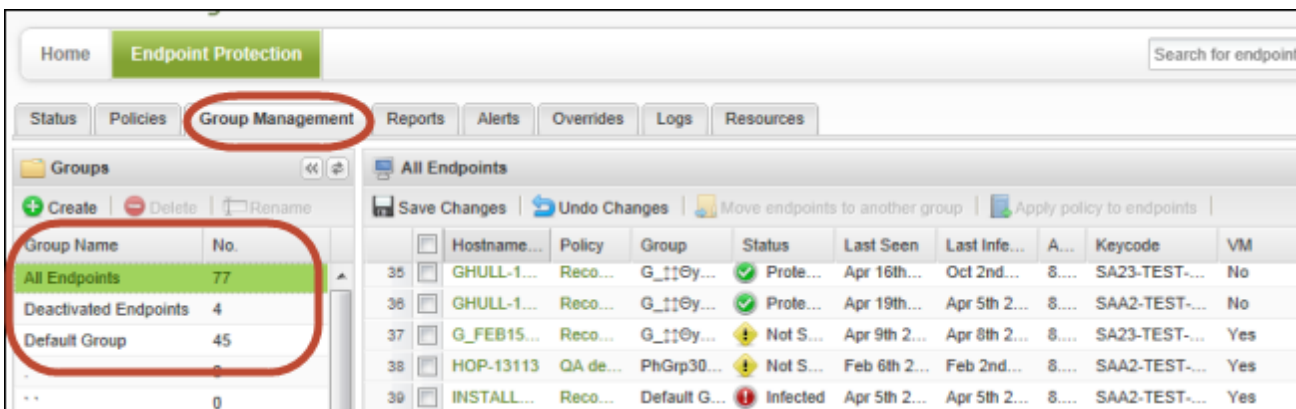
6. When you're done, click **Save**.
7. If you want to test how SecureAnywhere will detect the file, you can send the endpoint a **Reverify all files and processes** command (see "Issuing commands to endpoints" on page 63).

Applying overrides to files from groups

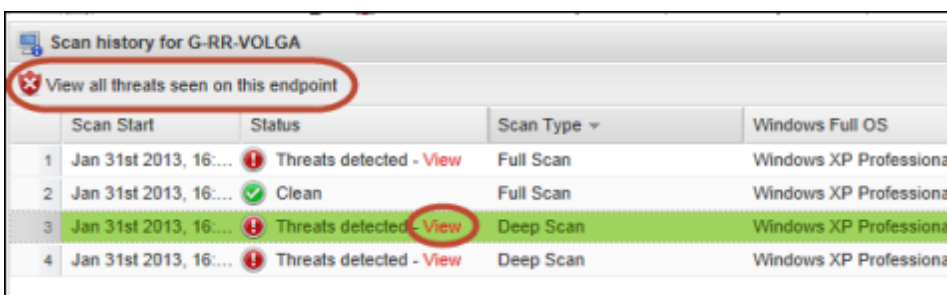
From a group level, you can apply an override to a file designated as a threat so it won't be detected and quarantined again in the future.

To apply an override from groups:

1. Click the **Group Management** tab.
2. From the left panel, select the group for the endpoint where the file was detected.



3. In the right panel, select the endpoint where the file was detected.
4. In the Scan History list at the bottom, you can click **View** in the Status column for the date when the threat was detected or you can click **View all threats seen on this endpoint**.



5. In the dialog, select the desired filename by clicking in its checkbox.
6. Click **Create override**.

Filename	Pathname	Malware Group	Last Seen
<input checked="" type="checkbox"/> NDNUNINSTALL6_38.EXE	%windir%\	Pua.Gen	Jan 31st 2013, 16:55
<input type="checkbox"/> LINKPAL[1].EXE	?:\documents and settings\lowe...	W32.Trojan.Downloader-LowZ...	Jan 31st 2013, 16:55
<input type="checkbox"/> MNMYBOH.EXE	?:\documents and settings\lowe...	Adware.W-find.com.Hijacker	Jan 31st 2013, 16:55
<input type="checkbox"/> 45765FBEB88468B9A7AD0E0...	?:\documents and settings\lowe...	W32.Trojan.Trojan-iejore	Jan 31st 2013, 16:55

The following dialog opens:

Create override

Determination: ▼

Apply this override globally?:

Save Cancel

7. Open the **Determination** drop-down menu by clicking the arrow to the right of the field. Select one of the following:
 - **Good**: Always allow the file to run.
 - **Bad**: Always send the file to quarantine.
8. You can apply this override globally or to an individual policy, as follows:
 - To apply the override to all policies, keep the **Apply the override globally** checkbox selected.
 - To select an individual policy for the override, deselect the checkbox. When the **Policy** field appears, click the drop-down arrow to the right of the field and select a policy.

Create override

Determination: ▼

Apply this override globally?:

Policy: ▼

Save Cancel

9. When you're done, click **Save**.
10. If you want to test the file's detection, you can send the endpoint a **Reverify all files and processes** command (see "Issuing commands to endpoints" on page 63).

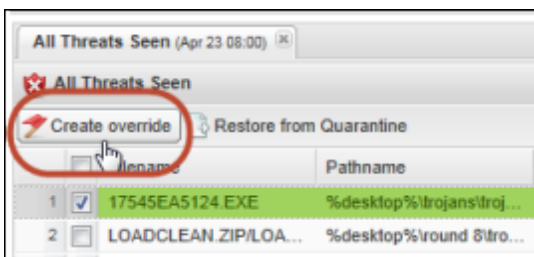
Applying overrides to files from reports

From the Reports tab, you can apply an override to a file designated as a threat so it won't be detected and quarantined again in the future. You can add overrides from these reports:

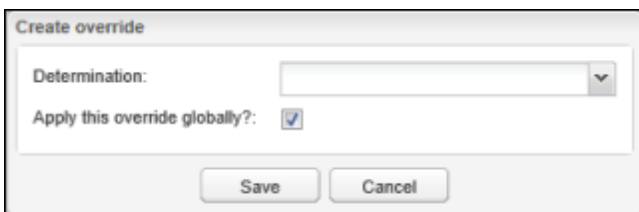
- All Threats Seen.
- All Undetermined Software Seen.
- Endpoints with Threats on Last Scan, in the panel for Threats Seen on this Endpoint panel (individual endpoints only).
- Endpoints with Undetermined Software on Last Scan, in the panel for All Undetermined Software Seen on this Endpoint (individual endpoints only).

To create an override from reports:

1. Click the **Reports** tab and generate one of the reports listed above.
2. Select the desired filename and click **Create override** from the command bar.



The following dialog opens:



3. Open the **Determination** drop-down menu by clicking the arrow to the right of the field. Select one of the following:
 - **Good**: Always allow the file to run.
 - **Bad**: Always send the file to quarantine.

4. You can apply this override globally or to an individual policy, as follows:
 - To apply the override to all policies, keep the **Apply the override globally** checkbox selected.
 - To select an individual policy for the override, deselect the checkbox. When the **Policy** field appears, click the drop-down arrow to the right of the field and select a policy.

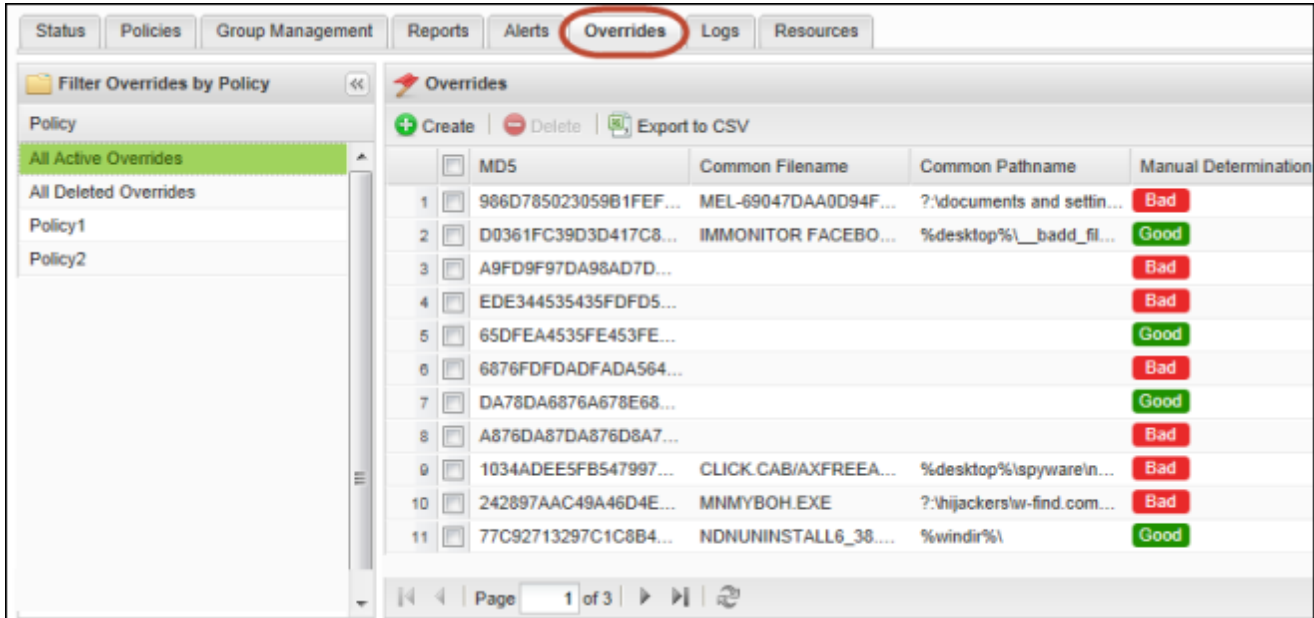


The image shows a dialog box titled "Create override". It has three main sections: "Determination:" followed by a dropdown menu, "Apply this override globally?:" followed by a checkbox, and "Policy:" followed by another dropdown menu. At the bottom of the dialog are two buttons: "Save" and "Cancel".

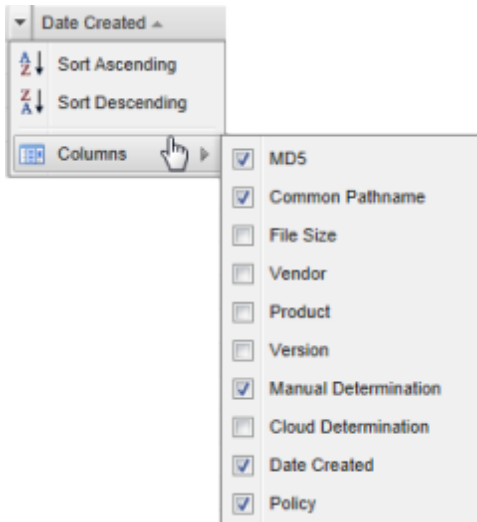
5. When you're done, click **Save**.
6. If you want to test the file's detection, you can send the endpoint a **Reverify all files and processes** command (see "Issuing commands to endpoints" on page 63).

Viewing overrides

After you add overrides to Endpoint Protection, you can view them in the Overrides tab. Select a policy from the left panel to narrow the results shown on the right. Your selected overrides appear under the Manual Determination column.



If desired, you can show or hide additional data about the overrides. Click a column header to open the drop-down menu, then click in the checkboxes to select the columns to add or remove.



The columns provide the following data:

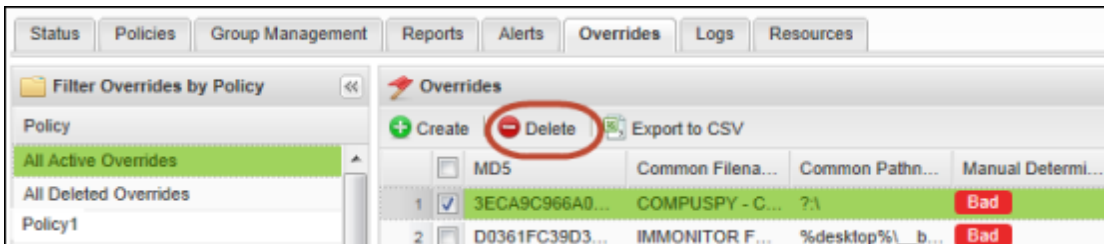
Columns in the Overrides tab	
MD5	The <i>Message-Digest algorithm 5</i> value, which acts like a fingerprint to uniquely identify a file.
Command Filename	The name of the Windows file as it would display in a file folder. This column is static; you cannot hide it.
Common Pathname	The name of the Windows folder structure.
File Size	The file size in bytes.
Vendor	The name of the vendor associated with the file, if SecureAnywhere can determine that information.
Product	The name of the product associated with the file, if SecureAnywhere can determine that information.
Version	The version of the product associated with the file, if SecureAnywhere can determine that information.
Manual Determination	Your designation for the file, which is either Good or Bad .
Cloud Determination	Webroot's classification for the file, which is Good , Bad , or Undetermined .
Data Created	The date and time this override was defined.
Policy	The policy where this override is applied.

Deleting overrides

If you want to remove an override that you previously defined, you can delete it from the Overrides tab.

To delete an override:

1. Click the **Overrides** tab.
2. If you want to narrow the results in the right panel, select a specific policy from the left.
3. Click **Delete** from the command bar.



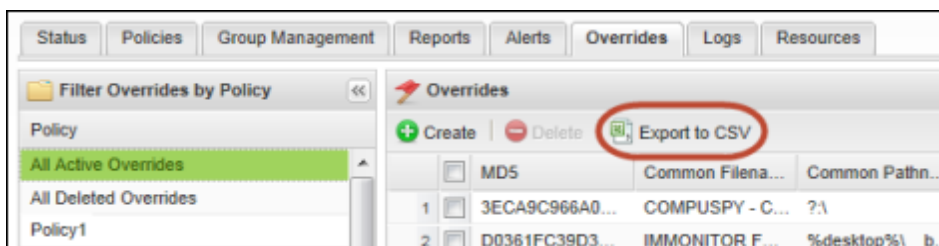
After you confirm the deletion, the override is moved to the "deleted" list. You can view all deleted overrides by selecting **All Deleted Overrides** from the left panel. Be aware that you cannot restore deleted overrides.

Exporting overrides to a spreadsheet

You can export all override information to a spreadsheet, which is convenient if you want to review settings with your colleagues.

To export override settings:

1. Click the **Overrides** tab.
2. If you want to narrow the results in the right panel, select a specific policy from the left.
3. Click **Export to CSV** from the command bar.



4. From the prompt, save the overrides to a CSV file. Endpoint Protection saves it to a file named **Overrides.csv**. If you save additional files, it appends a number to the base name, such as **Overrides (2).csv**.

Chapter 10: Viewing Logs

To use logs, see the following topics:

Viewing the Change Log	180
Viewing the Command Log	182

Viewing the Change Log

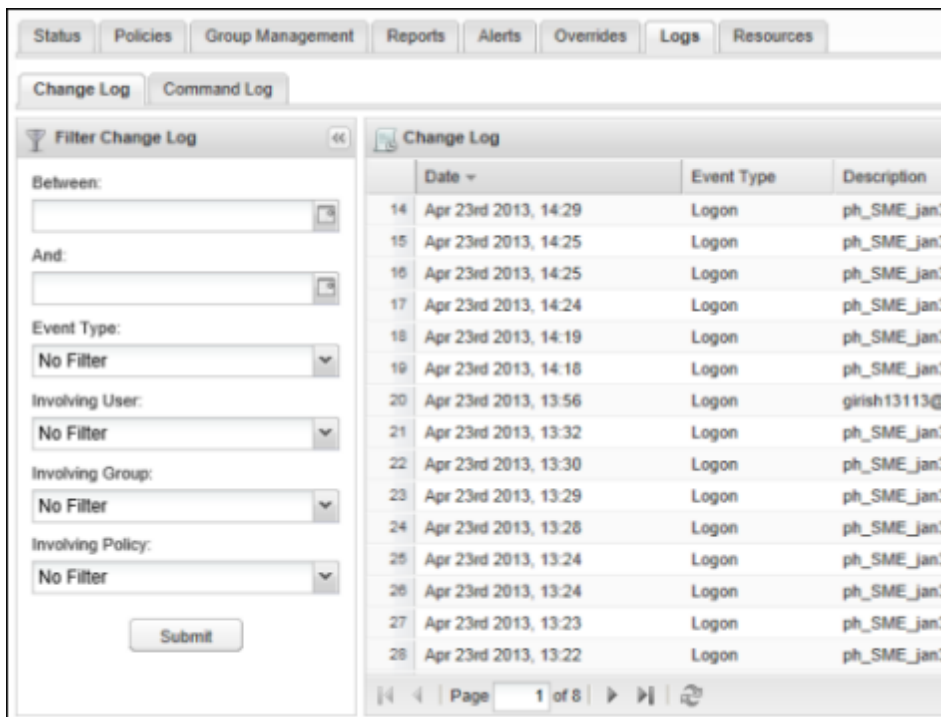
In the Change Log, you can see when the following types of events have occurred:

- **Logon:** When the administrator logged into the Management Portal.
- **Policy:** Any policies created, changed, or deleted.
- **Agent Commands:** When a command was initiated.
- **Override:** Any overrides created, changed, or deleted.
- **Group:** Any groups created, changed, or deleted.
- **Endpoint:** Any endpoints renamed or moved to another group.
- **Reports:** Any reports generated.

You can filter the Change Log by date range, event type, user, group, and policy.

To view the Change Log:

1. Click the **Logs** tab.
The Change Log opens by default. It lists change events, and provides filters for narrowing the list.



2. You can use the **Filter Change Log** options in the left panel to narrow the data. When you have selected the filtering criteria, click **Submit**.

You can choose to filter the data, as follows:

- **Between and And:** Enter the time frame in these two fields in MM/DD/YYYY format or by clicking the calendar icons to choose dates.
 - **Event Type:** Select an event from the drop-down list. Events include changes in groups, endpoints, or policies, as well as overrides and user logons.
 - **Involving User:** Select a user from the drop-down list.
 - **Involving Group:** Select a group from the drop-down list.
 - **Involving Policy:** Select a policy from the drop-down list.
3. If the data exceeds 50 items, you can use the navigation buttons at the bottom to move between additional pages.



You can also use the **Refresh** button to update the data:



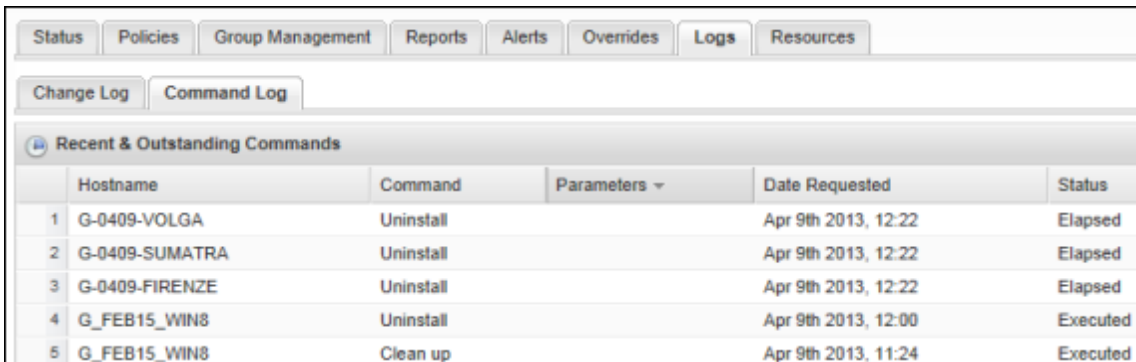
Viewing the Command Log

In the Command Log, you can review information about recent and outstanding commands. The log includes data for:

- **Hostname.** The name of the endpoint that received the command.
- **Command.** The command issued to the endpoint.
- **Parameters.** Additional parameters for executing the command, such as the full path name.
- **Date Requested.** The date the command was sent from the Management Portal.
- **Status.** Either Elapsed or Executed. The Elapsed time is 24 hours.

To view the Command Log:

1. Click the **Logs** tab.
2. Click the **Command Log** tab.
The Command Log opens.



The screenshot shows a web interface with a navigation bar at the top containing tabs: Status, Policies, Group Management, Reports, Alerts, Overrides, Logs, and Resources. Below this is a sub-navigation bar with 'Change Log' and 'Command Log' tabs. The main content area is titled 'Recent & Outstanding Commands' and contains a table with the following data:

	Hostname	Command	Parameters ▾	Date Requested	Status
1	G-0409-VOLGA	Uninstall		Apr 9th 2013, 12:22	Elapsed
2	G-0409-SUMATRA	Uninstall		Apr 9th 2013, 12:22	Elapsed
3	G-0409-FIRENZE	Uninstall		Apr 9th 2013, 12:22	Elapsed
4	G_FEB15_WIN8	Uninstall		Apr 9th 2013, 12:00	Executed
5	G_FEB15_WIN8	Clean up		Apr 9th 2013, 11:24	Executed

3. If the data exceeds 50 items, you can use the navigation buttons at the bottom to move between additional pages:



You can also use the **Refresh** button to update the data:



Glossary

A

adware

Software designed to display advertisements on your system or hijack web searches (rerouting searches through its own web page). It may also change your default home page to a specific website. Adware generally propagates itself using dialog boxes and social engineering methods.

agent

The SecureAnywhere software installed on a PC or other type of endpoint.

C

console

A console is a collection of one or more devices running a Webroot product and displays as separate sites in the Management Portal. When you first registered an account, SecureAnywhere organized your managed devices into a single console. You can add more consoles for management purposes, if desired.

cookies

Small strings of text designed to help websites remember your browser and preferences. Cookies cannot steal information off your machine, but some do store personal information that you may not want outside parties to gather. You can manage cookie settings in your browser's security or privacy preferences. You can also remove cookies using SecureAnywhere's System Cleaner.

CSV file

Comma-Separated Values file. A file format that stores tabular data.

G

GPO

Group Policy Object.

H

Hostname

The name of the endpoint, which is displayed in the Management Portal.

K

keycode

Your keycode is the 20-character license that identifies your Webroot account.

keylogger

A system monitor that records keyboard activity. Keyloggers can be used for legitimate purposes, but can also record sensitive information for malicious purposes.

L

LDAP

Lightweight Directory Access Protocol. A software protocol for enabling anyone to locate resources such as files and devices in a network, whether on the public Internet or on a corporate intranet.

LSP

Layered Service Provider.

M

malware

Malicious software that is designed to destroy or harm your computer system. Malware includes viruses, spyware, adware, and all types of threats.

Management Portal

The centralized website used for Endpoint Protection, where administrators can view and manage endpoints and network status. The portal can be divided into sub-portals called "consoles."

MD5

Message-Digest algorithm 5 is a cryptographic hash function that acts like a fingerprint to uniquely identify a file.

MID

A machine ID that Webroot uses to identify the hardware and OS of an endpoint.

MSI

Microsoft Installer.

P

phishing

A fraudulent method criminals use to steal personal information. These criminals design websites or email messages that appear to originate from trustworthy sources, such as eBay, PayPal, or even your own bank. Typical scams can trick you into entering your user names, passwords, and credit card information.

policy

A policy defines the SecureAnywhere settings on endpoints, including how the program scans for threats and manages detected items.

portal

A centralized website used to view and manage endpoints and network status. See "Management Portal."

R

registry

A database of hardware and software settings about your computer's configuration, such as the types of programs that are installed. Spyware can create entries in the Windows registry, which can ultimately slow down your computer and cause problems in your system.

rootkit

A collection of tools that enables administrator-level access to a computer or network. By using file-obfuscation techniques, rootkits can hide logins, processes, files and logs, and may include software to capture information from desktops or a network. Spyware developers often use rootkits to avoid detection and removal.

S

seat

A SecureAnywhere installation on an endpoint.

spyware

A program that may either monitor your online activities or install programs without your knowledge. Spyware may get bundled with freeware, shareware, or email attachments. You can also accidentally install spyware by clicking on dialog boxes in websites. Once installed, spyware can send information about your online activities to a third party for malicious purposes.

T

Trojan Horse

A program that takes control of your computer files, allowing a hacker to install, execute, open, or close programs. A Trojan is usually disguised as a harmless software program. It may also be distributed as an email attachment. When you open the program or attachment, the Trojan can launch an auto-installation process that downloads third-party programs onto your computer.

U

Undetermined software

A file that may appear legitimate, but also exhibits questionable behavior. In these cases, SecureAnywhere classifies the file as "Undetermined."

V

virus

A self-replicating program that can infect computer code, documents, or applications. While some viruses are purposefully malignant, others are more of a nuisance, replicating uncontrollably and inhibiting system performance.

VM

Virtual machine.

Z

zero-hour virus

New viruses that do not yet have recorded definitions.

Index

A

Access & Permissions 39
account
 changing email address with users awaiting status 37
 creating 9
 editing administrative settings 30
 registering more users 33
 renewing or upgrading 47
Account Settings 30
admins, adding portal users 33
Advanced commands 68
Advanced Heuristics 100
Age Heuristics 100
agent
 commands for 65
 deploying to endpoints 50
 generating Agent Version Spread report 134
 generating installation report 137
 opening on main interface 77
Agent Commands 63
Agent Version Spread chart (Status tab) 85
Agent Version Spread report (Reports tab) 134
Agents Installed report 137
alerts
 assigning permissions for creating 41
 creating a distribution list 157
 creating customized messages 158
 deleting a distribution list 157
 overview of configuration 156
 resuming 164
 suspending 164

 viewing in Status tab 82
All Threats Seen report 139
All Undetermined Software Seen report 141
Allow all denied applications command 68
Allow application command 68
Allow processes blocked by firewall command 67
Antimalware Tools commands 67

B

Basic Configuration policy settings 96
Behavior Shield policy settings 104
browsers supported 8

C

Change Console 46
Change keycode command 66
Change keycode temporarily command 66
change log, generating 180
Change scan time command 65
Clean up command 66
cleaner settings 110
cleanup script 68
Clear Data commands 66
Clear files command 66
Cloud Determination 27
Collapse button in portal 23
columns, sorting in tables 26
command log 182
commands
 assigning permissions for using 41
 issuing to endpoints 63
Confirm Logon 12
Consider all items as good command 67
consoles
 creating separate consoles in the portal 44
 providing access to 34
 renaming 46

- switching between consoles 46
- cookies, removing 112
- Core System Shield policy settings 105
- Create New User 33
- Create Override 71, 145
- Custom/Right-Click Scan 65
- Customer Support Diagnostics command 68

D

- Data Inputs, entering for alerts 160
- Deep Scan command 65
- Deep Scan, changing to 98
- default policies
 - overview of 14
 - selecting a new default 89
- Deny application command 68
- deploying SecureAnywhere 50
- Device MID 27
- diagnostics for Customer Support 68
- Disable proxy settings command 66
- distribution lists
 - creating for alerts 157
 - deleting 157
- DOS commands, sending to endpoint 68
- Download and run a file command 68
- Draft column in policy settings 93

E

- email address
 - changing when user does not confirm registration 37
 - limitation on changing 30
- email template for deployment 15, 53
- Endpoint Installed alerts 158
- Endpoint Protection access permissions 35
- Endpoint Protection menu 22
- Endpoint with undetermined software on last scan report 146

- endpoints
 - adding seats to your license 42
 - assigning to a policy 124
 - changing a keycode 59
 - changing hardware for 75
 - creating a shortcut for SecureAnywhere 53
 - deactivating and uninstalling 73
 - deploying SecureAnywhere to 50
 - duplicates created with new OS 75
 - Endpoint Infected links 82
 - issuing commands to 63
 - locking from portal 67
 - logging off user from portal 67
 - migrating from one policy to another 118
 - migrating to new OS 75
 - moving to a new group 127
 - moving to new subnet 75
 - opening SecureAnywhere interface 77
 - operating systems allowed 8
 - reinstalling 75
 - renaming 61
 - requirements for 8
 - restarting from portal 67
 - sending Uninstall command to 66
 - using search to locate 62
 - viewing assignments in Policies tab 117
- Endpoints with Threats on Last Scan report 143
- Explorer, enabling right-click scan 98
- exporting data to a spreadsheet 24

F

- File & Processes commands 67
- firewall
 - allowing blocked processes 67
 - stopping untrusted processes 67
- Firewall policy settings 108

G

- GPO, using for deployment 58

groups

- adding new groups 122
- applying a policy to 124
- assigning permissions for creating 41
- deleting 128
- directly deploying endpoints to 55
- moving endpoints to another group 127
- overview of implementation 120
- renaming 129

H

Heuristics policy settings 100

I

- icons in browser search results 106
- Identity Shield commands 68
- Identity Shield policy settings 107
- Infection Detected alerts 158
- Infection Summary alerts 158
- Install Summary alerts 158
- installation and configuration
 - deploying SecureAnywhere 50
 - deploying SecureAnywhere (quick method)
15
 - installing agent in background (silent) 50
 - overview of 7
 - selecting a policy 14
 - system requirements for 8
 - using GPO for installation 58
 - using MSI for deployment 57
 - using proxy commands during
installation 56
 - using setup wizard 12
- Instance MID 28

K**keycode**

- adding to your account 42
- changing from endpoint 59
- changing temporarily 66
- entering during deployment 50
- hiding from endpoint user 96
- using agent command to change 66

Keycode commands 66

L

- language codes for installation 56
- language codes in portal 27
- language, changing for portal 19
- license, renewing 47
- Live column in policy settings 93
- Lock endpoint 67
- Log off command 67
- login
 - after configuration 19
 - first-time login after account creation 12
- logs
 - Change Log 180
 - Command Log 182
 - erasing on endpoint 66

M

- Malware Group 28
- malware reports 132
- Manage Keycodes 42
- Manage Users 33
- Management Portal
 - adding users for 33
 - alerts in 82
 - charts in 21
 - collapsing panels in 23
 - logging in 19

- removing endpoints from 73
- setting access permissions 38
- MD5 value
 - locating and saving 167
 - shown in tables 28
- MSI, using for installation 57
- O**
- operating systems
 - migrating to new 75
 - supported versions for endpoints 8
- overrides
 - applying the "Good" designation 167
 - assigning permissions for creating 41
 - creating from Group Management 170
 - creating from Reports 172
 - creating from Scan History panel 71
 - deleting 176
 - exporting to spreadsheet 177
 - implementation overview 166
 - locating and entering MD5 values 167
 - testing 67
 - viewing all overrides 174
- P**
- password for account
 - changing 30, 33
 - defined during registration 10
 - forgotten password 12
- permissions for portal use 38
- policies
 - assigning endpoints to another policy 118
 - assigning permissions for creating 41
 - changing settings 92
 - copying policies 91
 - creating new policies 90
 - deleting 116
 - exporting to spreadsheet 115

- live settings and draft changes 93
- overview of implementation 88
- promoting changes to live 95
- renaming 114
- selecting a default during configuration 14
- selecting a new default policy 89
- viewing endpoints assigned to 117
- poll interval, changing for endpoint 97
- polling, forcing an immediate poll 76
- Popularity Heuristics 100
- portal
 - adding users for 33
 - alerts in 82
 - charts in 21
 - collapsing panels in 23
 - logging in 19
 - removing endpoints from 73
 - setting access permissions 38
- Post Cleanup Scan 66
- Power & User Access commands 67
- Protect an application command 68
- proxy commands, using during installation 56

Q

- quarantine
 - restoring a file using agent commands 67
 - restoring a file using Scan History panel 70
- Question mark icon 24
- Quick Scan, changing to 98

R

- Realtime Shield policy settings 103
- Reboot in Safe Mode command 67
- Refresh configuration on endpoints 76
- registering an account 9
- registry command, sending to endpoint 68
- release notes 25
- Remove password protection 66

renewing your license 47
reports
 overview of 132
 sorting data in 26
Reset desktop wallpaper command 67
Reset screen saver command 67
Reset system policies command 67
resetting SecureAnywhere settings 66
resources, conserving for endpoint 95
Restart command 67
Restore file command 67
Restore from Quarantine 70, 145
Reverify all files and processes command 67
Right-click scan in Explorer, enabling 98
Run a DOS command 68
Run a registry command 68
Run Customer Support script command 68

S

Safe Mode reboot 67
Scan a folder command 65
Scan command 65
Scan History panel 69
Scan policy settings 98
Scan Schedule policy settings 97
Scan Type shown in tables 28
scanning
 changing command time for 65
 changing frequency 97
 changing scan settings 98
 checking results from Group Management 69
 generating a threat report 132
 issuing command to endpoints 65
 scanning a single folder 65
 scanning with cleanup 66
screen saver, resetting 67
scripts for cleanup 68
Search for endpoint 62

secure file removal 113
SecureAnywhere
 changing settings by using policies 92
 deploying to endpoints 50
 generating a version report 134
 generating installation report 137
 hiding from endpoint user 109
 opening main interface 77
 using installer file 52
SecureAnywhere website access 34
security code
 changing 30
 defining during registration 10
 entering during login 12
security question and answer 10
Self Protection policy settings 100
servers supported 8
setup wizard 12
shortcut, creating for SecureAnywhere on
 endpoint 53, 96

Shutdown command 67
spreadsheet, exporting data to 24
Status shown in tables 28
Stop untrusted processes command 67
subnet, moving endpoints to new subnet 75
subscription, renewing 47
System Cleaner
 command for 66
 settings for 109
system requirements 8
system tray icon, hiding or showing on
 endpoint 96

T

tables, sorting columns 26
task manager settings, changing on endpoint 67
Technical Support 25
television icon 24

threat blog 25
Threat History (Collated) report 148
Threat History (Daily) report 152
threat reports 132

U

Undetermined software, locating on
 endpoints 133
Uninstall command 66
Unnamed Console 45
Unprotect an application command 68
updates, forcing immediate on endpoint 76
upgrading your account 47
user guides 25
User Interface policy settings 109
user permissions 38
users for portal, adding 33

V

videos
 icon available in panels 24
 link from the Product Information panel 25
View commands for selected endpoints 64
virtual servers supported 8

W

wallpaper, resetting 67
Web Threat Shield policy settings 106
Webroot account 9
Webroot Support 25
Windows Explorer, enabling right-click scan 98
Windows systems supported 8
wsasme.exe 52