Copyright

Copyright 2019 Webroot. All rights reserved.

Webroot Endpoint Protection Admin Guide

Information in this document is subject to change without notice. The software described in this document is furnished under a license agreement or nondisclosure agreement. The software may be used or copied only in accordance with the terms of those agreements. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or any means electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Webroot.
# Table of Contents

**Chapter 1: WSA Business Endpoint Protection Admin Guide** ................................................. 1
  WSA Business - Endpoint Protection Admin Guide Overview .................................................. 2

**Chapter 2: Getting Started With Endpoint Protection** ....................................................... 3
  System Requirements ............................................................................................................. 4
  Preparing for Setup ............................................................................................................... 5
    Configuration Steps ........................................................................................................... 5
    Communicating Through Firewalls .................................................................................... 6
  Entering Proxy Bypasses ....................................................................................................... 8
  Entering Proxy Information Within the Installer ................................................................. 8
  Entering Proxy Information on Each Endpoint Post Deployment ........................................ 9
  Creating Accounts .............................................................................................................. 11
  Enabling 2-factor authentication (2FA) ............................................................................... 16
  Logging in and using the Setup Wizard .............................................................................. 24
    Selecting a Default Policy During Configuration ............................................................... 27
    Selecting a Deployment Method and Performing a Test Install ......................................... 29
  Using the Management Console ........................................................................................... 33
    Endpoint Protection Main Tabs ......................................................................................... 37
    Opening the Endpoint Protection Menu ............................................................................ 38
    Opening and Collapsing Panels ......................................................................................... 40
    Exporting Data to Spreadsheets ......................................................................................... 41
    Opening Video Tutorials ..................................................................................................... 41
    Opening the Help Files ....................................................................................................... 41
  Accessing Product Information ............................................................................................ 42
  Sorting Data in Tables and Reports ...................................................................................... 44
  Accessing the Management Console .................................................................................... 51

**Chapter 3: Managing User Accounts** ............................................................................... 53
  Editing Your Own Account Settings ..................................................................................... 54
  Managing Portal Users ......................................................................................................... 67
    Creating New Portal Users ............................................................................................... 67
    Editing User Information .................................................................................................... 71
  Setting Console User Permissions ....................................................................................... 74
  Adding Keycodes to Your Account ....................................................................................... 79
  Adding Consoles to Your Account ....................................................................................... 82
    Adding Consoles ................................................................................................................ 82
    Renaming Consoles ........................................................................................................... 88
Switching Between Consoles ................................................................. 88
Renewing or Upgrading Your Account .................................................... 89
Adding Site Admins ............................................................................... 91
Editing Site Admin Settings ................................................................. 96
Deleting Site Admins ........................................................................... 105

Chapter 4: Managing Endpoints ............................................................... 108
Deploying SecureAnywhere to Endpoints ............................................... 110
Using the SecureAnywhere Installer ..................................................... 113
Using MSI for Deployment .................................................................... 126
Using GPO for Deployment .................................................................. 127
Installer Options .................................................................................. 128
Installing on Terminal (RDS) Servers and Citrix XenApp ...................... 128
Installing on Duplicated Images or VMs ............................................... 128
Changing Endpoint Keycodes .............................................................. 131
Renaming Endpoints .......................................................................... 134
Searching for Endpoints ...................................................................... 135
Issuing Commands to Endpoints .......................................................... 140
Managing Endpoint Updates and Other Changes .................................. 157
Migrating to a New Operating System .................................................. 157
Changing Hardware on Endpoints ....................................................... 157
Moving Endpoints to New Subnets ....................................................... 157
Communicating Through Firewalls ...................................................... 158
Using SecureAnywhere on Endpoints .................................................. 160
Opening SecureAnywhere on Windows Computers ............................. 160
Opening SecureAnywhere on Mac Computers ..................................... 162
Mac Webroot SecureAnywhere Menu .................................................. 163
Mac System Tools Drop-Down Menu .................................................... 164
Checking Scan Results and Managing Threats ..................................... 166
Viewing Scan Histories ....................................................................... 166
Restoring Files From Quarantine ........................................................ 168
Setting Overrides for Files .................................................................. 169
Downloading and Forcing Updates ...................................................... 171
Forcing Immediate Updates ............................................................... 174
Installing Web Threat Shield Chrome Browser Extensions .................. 175
Using Active Directory Group Policies ............................................... 176
Using Google Suite to Force Install a Single Custom App .................... 182
Using Registry ..................................................................................... 186
Running Commands at Endpoints ....................................................... 188
Deactivating Endpoints ................................................................. 192
Deactivating Endpoints ................................................................. 192
Reactivating SecureAnywhere on Endpoints .................................. 193
Uninstalling SecureAnywhere ......................................................... 195

Chapter 5: Checking Statuses .......................................................... 196
Viewing Endpoint Statuses ............................................................ 197
Viewing Recent Threat Statuses ...................................................... 201
Viewing Agent Version Overviews ................................................. 205
About Dwell Time ........................................................................ 207
Exporting CSV Files From Endpoint Protection .............................. 209

Chapter 6: Managing Policies ......................................................... 214
Implementing Policies .................................................................. 215
Selecting New Default Policies ...................................................... 220
Creating Policies ......................................................................... 226
   Creating Policies .................................................................... 226
   Copying Policies .................................................................... 230
Renaming Policies ........................................................................ 235
Changing Policy Settings .............................................................. 240
   Basic Configuration ................................................................ 252
   Scan Schedule ...................................................................... 255
   Scan Settings ........................................................................ 257
   Self Protection Settings ......................................................... 262
Heuristics ................................................................................... 263
   Realtime Shield Settings ......................................................... 267
Behavior Shield Settings .............................................................. 270
Core System Shield ..................................................................... 272
Web Threat Shield ....................................................................... 274
Identity Shield ........................................................................... 277
Firewall ....................................................................................... 280
User Interface ............................................................................. 282
System Optimizer ....................................................................... 283
Viewing Endpoints Assigned to Policies ....................................... 293
Moving Endpoints Between Policies .............................................. 299
Deleting Policies .......................................................................... 304

Chapter 7: Managing Groups ......................................................... 310
Adding New Groups ..................................................................... 311
Renaming Groups ....................................................................... 313
Applying Policies to Endpoint Groups .......................................................... 316
Applying Policies to a Group of Endpoints .................................................. 316
Applying Policies to a Single Endpoint ....................................................... 317
Moving Endpoints Between Groups .............................................................. 320
Organizing Endpoints Into Groups .............................................................. 322
Using the Activity Directory Tab in Views ................................................... 324
Using the IP Range Tab in Views ................................................................. 326
Using the Workgroup Tab in Views .............................................................. 328
Deleting Groups ............................................................................................ 330

Chapter 8: Working With Reports ................................................................. 331
Generating Endpoint Protection Reports ...................................................... 332
Generating All Threats Seen Reports ............................................................ 334
Generating All Undetermined Software Seen Reports ................................... 341
Generating All URLs Blocked Reports ........................................................ 348
Generating Endpoints With Threats On Last Scan Reports .......................... 353
Generating Endpoints With Undetermined Software On Last Scan Reports ... 357
Generating Daily Threat History Reports ..................................................... 360
Generating Collated Threat History Reports ................................................. 368
Generating Daily Blocked URL History Reports .......................................... 377
Generating Agent Version Spread Reports ............................................... 381
Generating Agents Installed Reports ........................................................... 386
Downloading Report Spreadsheets ............................................................... 393

Chapter 9: Managing Alerts .......................................................................... 395
Implementing Alerts ..................................................................................... 396
Creating Distribution Lists .......................................................................... 397
Creating Customized Alerts ........................................................................ 399
Viewing Defined Alert Messages ............................................................... 410
Suspending or Deleting Alerts .................................................................... 412

Chapter 10: Using Overrides ......................................................................... 413
Implementing Overrides ................................................................................ 414
Creating Blacklist Overrides ......................................................................... 416
Creating Whitelist Overrides ........................................................................ 422
Applying Overrides From the Overrides Tab ............................................... 429
Applying Overrides to Files From Groups ................................................... 436
Applying Overrides To Files From Reports .................................................. 444
Applying Overrides From Dwell Time Popups .............................................. 449
Viewing Overrides ....................................................................................... 456
Chapter 1: WSA Business Endpoint Protection Admin Guide

To get started using Endpoint Protection, see the following topic:

WSA Business - Endpoint Protection Admin Guide Overview ................................................... 2
WSA Business - Endpoint Protection Admin Guide Overview

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 online help 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.
To get started with Endpoint Protection, see the following topics:

System Requirements ................................................................. 4
Preparing for Setup ................................................................. 5
   Configuration Steps .............................................................. 5
   Communicating Through Firewalls ........................................ 6
Entering Proxy Bypasses .......................................................... 8
Entering Proxy Information Within the Installer ......................... 8
Entering Proxy Information on Each Endpoint Post Deployment ...... 9
Creating Accounts ................................................................. 11
Enabling 2-factor authentication (2FA) ...................................... 16
Logging in and using the Setup Wizard ...................................... 24
   Selecting a Default Policy During Configuration ..................... 27
   Selecting a Deployment Method and Performing a Test Install .... 29
Using the Management Console ............................................... 33
   Endpoint Protection Main Tabs .............................................. 37
   Opening the Endpoint Protection Menu ................................ 38
   Opening and Collapsing Panels ............................................. 40
Exporting Data to Spreadsheets .............................................. 41
   Opening Video Tutorials ...................................................... 41
   Opening the Help Files ....................................................... 41
Accessing Product Information ................................................ 42
Sorting Data in Tables and Reports ........................................... 44
Accessing the Management Console ......................................... 51
System Requirements

The system requirements can be found here: System Requirements section of the Business Endpoint Protection webpage.
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.

**Configuration Steps**

1. Create an account using your keycode.
   
   You should have received the keycode in an email from Webroot. For more information, see [Creating Accounts on page 11](#).

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.
   
   - A policy defines the SecureAnywhere settings, including how the program scans for threats and manages detected items.
   - An endpoint can be any Windows corporate workstation, such as a PC, laptop, server, or virtual server.

   After you select a policy, a Welcome window displays and provides information about how to deploy SecureAnywhere to endpoints. For more information, see [Logging in and using the Setup Wizard on page 24](#).

3. Edit your account settings for the Management Portal, including your contact number and a time zone where you are located. For more information, see [Editing Your Own Account Settings on page 54](#).

   You can also create logins for other administrators to access the Management Portal. For more information, see [Managing Portal Users on page 67](#).

   **Note:** This step is optional.

4. Deploy the SecureAnywhere software to the endpoints. For more information, see [Deploying SecureAnywhere to Endpoints on page 110](#).
5. Determine if the default policy is sufficient for your business needs. You cannot change the Webroot default policies.

If needed, add new policies with different settings; for more information, see Implementing Policies on page 215. You may also need to create overrides for certain files that you consider legitimate applications. For more information, see Applying Overrides From the Overrides Tab on page 429.

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 needed, you can create new groups and assign them to new policies. For more information, see Organizing Endpoints Into Groups on page 322.

7. Customize alert messages that will be sent to a distribution list whenever endpoints report an infection or whenever SecureAnywhere is installed on new endpoints. For more information, see Implementing Alerts on page 396.

Note: This step is optional.

Communicating Through Firewalls

If a firewall is in place, please allow Webroot’s path masks through the firewall, as described in the following table.
<table>
<thead>
<tr>
<th>PATH</th>
<th>Port</th>
<th>INFORMATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>*.webrootcloudav.com</td>
<td>Port 443 (https)</td>
<td>Agent communication and updates.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> Some firewalls do not support double dotted subdomain names with a single wildcard mask, for example, g1.p4.webrootcloudav.com being represented by *.webrootcloudav.com, so some environments might require either *.p4.webrootcloudav.com or *.webrootcloudav.com.</td>
</tr>
<tr>
<td>*.webroot.com</td>
<td>Port 443 (https)</td>
<td>Agent messaging.</td>
</tr>
<tr>
<td>PATH</td>
<td>Port</td>
<td>INFORMATION</td>
</tr>
<tr>
<td>------</td>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>WSAWebFilteringPortal.elasticbeanstalk.com</td>
<td>Port 80 (http) &amp; 443 (https)</td>
<td>Required for agent Web Filtering, elasticbeanstalk is an amazon AWS domain.</td>
</tr>
<tr>
<td>*.webrootanywhere.com</td>
<td>Port 80 (http) &amp; 443 (https)</td>
<td>Management portal and support ticket logs upload.</td>
</tr>
</tbody>
</table>

When attempting to use proxy settings with Webroot SecureAnywhere Business – Endpoint Protection, there are additional methods to allow the Webroot product to communicate with our cloud servers. These are listed below.

**Entering Proxy Bypasses**

**Note:** This is the method that we recommend.

**To enter a proxy bypass:**

1. Enter a proxy bypass for g*.p4.webrootcloudav.com

**Note:** If you select this option, be sure that the wild card mask (*) is supported. If not, you must add 100 separate URLs, for example, g1, g2, g3, ..., g99, g100.

**Entering Proxy Information Within the Installer**

This is the alternate method that we recommend.
To enter proxy information within the installer:

1. Download the SecureAnywhere MSI installer to a network share:
   
   http://anywhere.webrootcloudav.com/zerol/wsasme.msi

2. Use an msi editor.

3. On the Property table, enter the subscription keycode in the GUILIC property and the proxy credentials on the CMDLINE property using the following commands:

   -proxyhost=X -proxyport=X -proxyuser=X -proxypass=X -proxyauth=#

4. Always use all parameters and blank out any value you don't need with double quotes, for example:

   proxypass=""

   proxyauth # being: 0 = Any authentication 1 = Basic 2 = Digest 3 = Negotiate 4 = NTLM

5. These arguments can also be applied with an executable install, for example:

   C:\wsasme.exe /key=xxxx-xxxx-xxxx-xxxx-xxxx /silent -proxyhost=nn.nn.nn.nn -proxyauth=n -proxyuser="proxyuser" -proxypass="password" -proxyport=port_number

**Entering Proxy Information on Each Endpoint Post Deployment**

We recommend that you use this method only if you are unable to enter a proxy bypass or enter proxy information within the installer.

1. Open the SecureAnywhere Endpoint Protection Group Management tab, open a group, and select an endpoint.

2. In the Policy column of the selected endpoint, double-click its policy name to open a list of available policies.

3. Select the unmanaged policy and apply. A red flag on the new policy name reminds you that you’ve made a change.

4. Click **Save Changes**.

5. Once applied, go to each individual endpoint workstation and follow the instructions below.

6. Open SecureAnywhere Endpoint Protection from the system tray icon.

7. Click **Settings**.

8. In the Settings window, click the **Proxy** tab.
9. Enter your proxy information.
10. Click **Save All** to save your changes.
11. After entering the proxy information, you can move the machine back to the original policy.

**Note:** The best way to test proxy settings is to ensure there is no Internet access via the default gateway. You can hardcode an IP address and subnet mask for the endpoint’s network card without adding a default gateway or DNS server. As long as the proxy server is on the same subnet, you can be sure that the only Internet access is via the proxy server.
Creating Accounts

Before you can log in to Endpoint Protection, you will need to create an account using your license keycode. Your keycode will be included in the activation and setup instruction email.

To create an account:

1. Go to the Management Console and click the Create Account button.

2. Enter your Product Keycode, the admin email address, and create a password and personal security code for your account using the information in the following table as reference.

<table>
<thead>
<tr>
<th>FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Webroot Product Keycode</td>
<td>Enter the license keycode you received when you purchased Endpoint Protection.</td>
</tr>
<tr>
<td>Email Address</td>
<td>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.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter a minimum of nine characters. Your password must contain at least six alphabetic characters and three numeric characters. Your password can be longer than the required nine characters. It can include special characters, except for the angle brackets: &lt;&gt;. Your password is case sensitive. As you type, the Strength meter displays how secure your password is. For optimum security, it’s a good idea to make your password as strong as possible.</td>
</tr>
<tr>
<td>FIELD</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Your Personal Security Code</td>
<td>Enter a word or number, which will be used for an extra security step after you enter the password during login. Pick a code that is easy to remember, using a minimum of six 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 the system prompts you for the fourth and sixth character, you would enter 4 and 6. Your Personal Security Code is case sensitive.</td>
</tr>
<tr>
<td>Security Question</td>
<td>Select 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.</td>
</tr>
<tr>
<td>Security Answer</td>
<td>Type an answer to your security question. The Security Answer is case-sensitive.</td>
</tr>
</tbody>
</table>
3. After you enter your account details, click the **Register Now** button.
Webroot Endpoint Protection Admin Guide

Create Account

Webroot Product Keycode

Email Address

Repeat Email Address

Password

Strength: 

Repeat Password

Your Personal Security Code

Security Question

Security Answer

Register Now
SecureAnywhere displays a confirmation message and sends an email to the administrator's email address you specified. This may take a few minutes.

4. Open your email application, and click the link in the confirmation email message.

When the SecureAnywhere Registration Confirmation page opens, enter the two randomly selected characters of the security code you specified when you created the account.

5. Click **Confirm Registration Now**.

After entering your security code, you will be presented with options about setting up 2-factor authentication (2FA), for more information on this topic see Enabling 2-factor authentication (2FA) on page 16.
Enabling 2-factor authentication (2FA)

Webroot SecureAnywhere allows users to enable two-factor authentication (2FA) to help prevent unauthorized users from gaining access to your account without permission.

To enable 2FA

1. First, visit the Webroot Management Console, and log in using your Business Admin account credentials.

2. The Setup 2FA screen will be presented. If this is the first time you have logged into the Management Console, you can either click Setup 2FA to start the process, or click Skip for now to continue to the Console.

If you have already logged into the Management Console and opted to skip the 2FA setup process previously, click here for instructions on enabling 2FA after initially skipping 2FA setup.

You can also start the 2FA setup process from the Account Settings in the top right-hand corner in the Endpoint Console which displays your details on the Account Settings page, and click Enable.
3. Next, the **Setup 2FA** screen displays and will prompt you to pick two security questions and provide your answers, and then click **Continue**.
Setup 2FA

Step 1
2FA requires you to choose two additional security questions. Please choose two questions below, type your answers and click 'Continue'.

It is important that you type the answers correctly because you will be asked again if your device gets lost or stolen.

Security Question
Choose a question from the list

Security Answer

Security Question
Choose a question from the list

Security Answer

Continue
4. You will need to download and install an authenticator app from the Google Play Store or the Apple App Store to a smartphone or tablet with a working camera.

Examples of mobile authentication apps include:

- Google Authenticator
- Microsoft Authenticator
- LastPass Authenticator
- Authy 2-Factor Authentication

5. Once you have downloaded an authenticator app, open the app, and follow the prompts to enable the app to access the camera on your smartphone, so you can scan the QR code shown that is presented in the Management Console. If you are unable to scan the QR code, try turning up the brightness on your display, or click **Can't scan the QR code?**, and enter the entire code shown into the authenticator app.
on your device. The code is case sensitive.
6. Enter the verification code from the authenticator app in the box under **Step 4**, and click **Verify Code**.
7. The code will be verified, and the screen will show a Verification Successful message. Click Complete Setup to finish setting up 2FA.

![Setup 2FA](image)

**Note:** If you receive a Verification Unsuccessful message when entering the code, you will need to enter a new code from the authenticator app as codes are only valid for 30 seconds, and click Verify Code.

8. 2FA is now enabled, and the Congratulations screen will display. Click Go to Console to log into the Endpoint Protection Console using 2FA.

The authenticator app will supply the authentication code you will be prompted to enter at login, which
replaces the Security Code.

![Webroot 2FA setup screen]

Note: The Security Code will be stored for your account and will be used if 2FA is disabled.

9. An email from no-reply@webrootanywhere.com will be sent to you informing you that 2FA has been enabled for your account.

---

You can now log in to the Endpoint Protection Console to begin configuring Endpoint Protection. For more information, see *Logging in and using the Setup Wizard on page 24*
Logging in and using the Setup Wizard

After you create an account, you can log in to the Management Portal. On your first login, a Setup Wizard opens to help you begin configuration.

This topic contains the following procedures:

- Logging In
- Selecting a Default Policy During Configuration
- Selecting a Deployment Method and Performing a Test Install

For more information, see Creating Accounts on page 11.

Logging in for the first time:

1. Go to the SecureAnywhere website.
2. To display a language other than English, click the drop-down arrow at the bottom of the page and select the desired language.

![Language selection dropdown](image)

**Note:** To enable languages that use double-byte character sets, you must have the appropriate language pack installed on your computer.
3. On the Log in screen, enter the email address and password you specified when you created an account.

**Note:** Hikari Tushin users can click the Phone tab to log in using their phone numbers and passwords. The Phone tab is visible to all users, but non-Hikari Tushin users should continue to login using their email and password.

4. Click the **Log in** button.

![Log in Screen](image.png)

After the third time you have attempted to log in and failed, the system sends you an email message, containing a link for resetting your password or security code.

In addition, the system displays the following message:

"Unfortunately you have exceeded the maximum number of attempts to access this console. You may try to access this console after 15 minutes. If you have forgotten your account details, please visit [https://my.webrootanywhere.com](https://my.webrootanywhere.com) and click the **Forgotten Password** link."

If you forget your password or security code, click the **Forgotten Password?** link, then click **I forgot my password** or **I forgot my security code**.

The system prompts you to enter your email address, and sends you an email message containing a link for resetting your password or security code.
5. If you have 2FA enabled, in the Confirm Logon window, enter the requested code from your Mobile Authenticator app, and click the Confirm button.

If you do not have 2FA enabled, on the Confirm Logon window, enter the security code you created when you registered for a Webroot account. Every time you log in, Endpoint Protection will require this extra security step. Be aware that it prompts you 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.
6. When the SecureAnywhere website opens, click the **Go to Endpoint Protection** button.

![SecureAnywhere website](image)

**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. For more information, see the [WSA Business - Mobile Protection Admin Guide](#).

The first time you log in, the Setup Wizard displays. Continue with [Selecting a Default Policy During Configuration](#).

### Selecting a Default Policy During Configuration

The Setup Wizard prompts you to select a default policy for new SecureAnywhere installations on Windows 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 re-mediate detected items. For more information about overrides, see *Applying Overrides From the Overrides Tab on page 429*.

- **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 display scan results. Administrators can also send them commands, but cannot change the policy settings.

**Note:** 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 New Default Policies on page 220*, or create your own policies and assign them to groups of endpoints, as described in *Creating Policies on page 226*.

To select a default policy:
1. From the Select your default settings drop-down menu, select the policy you want to apply.

![Select your default settings](image)

2. Click the **Submit** button.

The Endpoint Protection status page displays, with 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.

**Note:** These deployment methods are only available for Windows computers. If you need to install on Mac computers, see *Deploying SecureAnywhere to Endpoints on page 110* and follow the instructions for using the SecureAnywhere Mac installer.

- 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. For more information, see...
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. Click the **Download** link to download the SecureAnywhere installer file.

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

   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 displays in the endpoint's system tray.

5. 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.

6. 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.

For more information, see *Using the Management Console on page 33.*
Using the Management Console

The Management Console 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; for more information, see Creating Accounts on page 11.

If needed, the administrator can create additional users with full or limited access; for more information, see Managing Portal Users on page 67.

This topic contains the following procedures and information:

- Using the Management Console
- Endpoint Protection Main Tabs
- Opening the Endpoint Protection Main Menu
- Opening and Collapsing Panels
- Exporting Data to a Spreadsheet
- Opening Video Tutorials
- Opening Help Files

To use the Management Console:

1. Log in to the SecureAnywhere Management Console.
2. On the login page, enter the email address and password you specified when you created an account and click the Log in button.
Note: Hikari Tushin users can click the Phone tab to log in using their phone numbers and passwords. The Phone tab is visible to all users, but non-Hikari Tushin users should continue to login using their email and password.

3. On the Authentication Code page (for 2FA) or the Confirm Logon page, enter the requested characters of your security code or the code from your mobile authentication app, and click Log in.
Note: You defined your personal security code when you created a Webroot account. Each time you log in, Endpoint Protection will require this extra security step, and will prompt for two random characters of your code or the code from your mobile authentication app. 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 displays 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, click the Go to Endpoint Protection button 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 displays. The Status panel includes threat alerts, endpoint activity, and data charts.

5. Click the tabs along the top row to access configuration and other tasks.
# Endpoint Protection Main Tabs

This section describes the areas of the Management Portal, including its tabs, menus, panels, tables, search functions, and export functions.

The following table describes the Endpoint Protection tabs.

<table>
<thead>
<tr>
<th>TAB</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Back to Sites</td>
<td>Returns you to the management console. For more information see Accessing the Management Console on page 51.</td>
</tr>
<tr>
<td>Home</td>
<td>Returns you to the main console, where you can select other functionalites such as Security Awareness Training, Customer Support, and the Webroot Community.</td>
</tr>
<tr>
<td>Status</td>
<td>A dashboard that displays:</td>
</tr>
<tr>
<td></td>
<td>- An alert notification panel, if endpoints need attention. Click the notification to see a list of endpoints that encountered threats.</td>
</tr>
<tr>
<td></td>
<td>- A bar chart with the number of endpoints that encountered threats in the last 7 days.</td>
</tr>
<tr>
<td></td>
<td>- A pie chart with the SecureAnywhere versions installed on your endpoints.</td>
</tr>
<tr>
<td></td>
<td>- An endpoint activity panel with the number of endpoints reporting into the Management Portal based on a time frame you select. If any endpoints have not reported their status recently, click the View link next to Not Seen to determine which endpoints are not reporting status.</td>
</tr>
<tr>
<td></td>
<td>- A panel with the endpoints with the most recent threats. You can click on a row to view more information and add an override, if needed.</td>
</tr>
<tr>
<td></td>
<td>- A panel with links to Webroot's threat blog, guides, videos, release notes, and other news. Not included in the example above; for more information, see Accessing Product Information on page 42.</td>
</tr>
<tr>
<td>Policies</td>
<td>Policies define the behavior of SecureAnywhere on the endpoints, such as when it runs a scan and how it blocks potential threats.</td>
</tr>
<tr>
<td><strong>TAB</strong></td>
<td><strong>DESCRIPTION</strong></td>
</tr>
<tr>
<td>------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Group Management</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Reports</strong></td>
<td>Reports displays threats and unidentified software present on your endpoints, as well as the versions of SecureAnywhere they are running.</td>
</tr>
<tr>
<td><strong>Alerts</strong></td>
<td>Alerts allow you to customize warnings and status messages for a distribution list of administrators.</td>
</tr>
<tr>
<td><strong>Overrides</strong></td>
<td>Overrides provide administrative control over the files running in your environment. You can override files so they are not blocked or always quarantined.</td>
</tr>
<tr>
<td><strong>Logs</strong></td>
<td>Logs provide a view of changes and a history of command usage.</td>
</tr>
<tr>
<td><strong>Resources</strong></td>
<td>Provides downloads for the DWP client, configuration files to be used as templates, and links to documentation, such as the online help.</td>
</tr>
</tbody>
</table>

**Opening the Endpoint Protection Menu**

The Down arrow next to your login ID displays the Endpoint Protection menu. The options available on the menu vary, depending on your access permissions.
The following table describes the options on the Endpoint Protection Menu.

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Settings</td>
<td>Edit your account settings, including your password and other information.</td>
</tr>
<tr>
<td></td>
<td>For more information, see <em>Editing Your Own Account Settings on page 54</em>.</td>
</tr>
<tr>
<td>Manage Users</td>
<td>Provide other users with access to the Management Portal.</td>
</tr>
<tr>
<td></td>
<td>For more information, see <em>Managing Portal Users on page 67</em>.</td>
</tr>
<tr>
<td>Manage Keycodes</td>
<td>View your current Endpoint Protection license keycodes and add more to the</td>
</tr>
<tr>
<td></td>
<td>portal, if you purchased additional keycodes.</td>
</tr>
<tr>
<td></td>
<td>For more information, see <em>Adding Keycodes to Your Account on page 79</em>.</td>
</tr>
<tr>
<td>Downloads</td>
<td>Download the SecureAnywhere installer file and read more about deployment</td>
</tr>
<tr>
<td></td>
<td>options.</td>
</tr>
</tbody>
</table>
### Opening and Collapsing Panels

For a larger view of the data charts, click the **Collapse** buttons on the far left and the far right.

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.
Exporting Data to Spreadsheets

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

Opening Video Tutorials

When you see a Television icon, click it to view a video that describes a procedure related to the panel.

Opening the Help Files

When you see a Question Mark icon, click it to open Help for the current panel.
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 the Collapse button on the far right:
Sorting Data in Tables and Reports

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

- **Quick sort on a column** — Click the column head to sort by that subject. For example, to sort data by policy name, click the Policy column header.

- **Change the ascending or descending order** — Click the drop-down arrow at the end of a column header to display the drop-down 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 display the menu. Select a checkbox to display a column. Deselect a checkbox to hide a column.

The following table describes subject data that may display in Endpoint Protection tables and reports. The data that displays depends on the type of table or report displayed.
<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent Language</td>
<td>The language selected when SecureAnywhere was installed:</td>
</tr>
<tr>
<td></td>
<td>en — English</td>
</tr>
<tr>
<td></td>
<td>ja — Japanese</td>
</tr>
<tr>
<td></td>
<td>es — Spanish</td>
</tr>
<tr>
<td></td>
<td>fr — French</td>
</tr>
<tr>
<td></td>
<td>de — German</td>
</tr>
<tr>
<td></td>
<td>it — Italian</td>
</tr>
<tr>
<td></td>
<td>nl — Dutch</td>
</tr>
<tr>
<td></td>
<td>ko — Korean</td>
</tr>
<tr>
<td></td>
<td>zh-cn — Simplified Chinese</td>
</tr>
<tr>
<td></td>
<td>pt — Brazilian Portuguese</td>
</tr>
<tr>
<td></td>
<td>ru — Russian</td>
</tr>
<tr>
<td></td>
<td>tr — Turkish</td>
</tr>
<tr>
<td></td>
<td>zh-tw — Traditional Chinese</td>
</tr>
<tr>
<td>Agent Version</td>
<td>The version of the SecureAnywhere software installed on the endpoint.</td>
</tr>
<tr>
<td>OPTION</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>-------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>All Endpoints</td>
<td>More information about the endpoints where a file was detected and blocked.</td>
</tr>
<tr>
<td>All Versions</td>
<td>More information about the SecureAnywhere versions where a file was detected and blocked.</td>
</tr>
<tr>
<td>Approx Scan Time</td>
<td>The duration of a scan in minutes and seconds.</td>
</tr>
<tr>
<td>Area</td>
<td>A flag for the country where the endpoint is located.</td>
</tr>
<tr>
<td>Cloud Determination</td>
<td>The Webroot classification of the file, which can be Good, Bad, or Undetermined.</td>
</tr>
<tr>
<td></td>
<td>If you hover over the classification, the system displays information on how this classification was reached.</td>
</tr>
<tr>
<td>Days Infected</td>
<td>The number of days the endpoint remained infected.</td>
</tr>
<tr>
<td>Device MID</td>
<td>A Machine ID value that identifies the hardware for an endpoint. Webroot uses an algorithm to determine this value.</td>
</tr>
<tr>
<td>Dwell Time</td>
<td>The time the threat has been present on the device. It is calculated from the first time the file is active to when the file was last seen.</td>
</tr>
<tr>
<td></td>
<td>For more information, see <em>About Dwell Time on page 207</em>.</td>
</tr>
<tr>
<td>OPTION</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Endpoints Affected</td>
<td>The number of endpoints with a detected file.</td>
</tr>
<tr>
<td>File Size</td>
<td>The size of the file in bytes.</td>
</tr>
<tr>
<td>Filename</td>
<td>The file name of the detected threat.</td>
</tr>
<tr>
<td>First Threat</td>
<td>The date and time a threat was detected.</td>
</tr>
<tr>
<td>First Seen</td>
<td>The date and time this endpoint first checked into the Management Portal.</td>
</tr>
<tr>
<td>Group</td>
<td>The group assigned to the endpoint.</td>
</tr>
<tr>
<td>Hostname</td>
<td>The machine name of the endpoint.</td>
</tr>
<tr>
<td>Instance MID</td>
<td>A value that identifies the Windows operating system SID (Security Identifier). Webroot uses an algorithm to determine this value.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address of the endpoint.</td>
</tr>
<tr>
<td>Keycode</td>
<td>The license used to install SecureAnywhere on the endpoint.</td>
</tr>
<tr>
<td><strong>OPTION</strong></td>
<td><strong>DESCRIPTION</strong></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Last Infected</td>
<td>The date and time the endpoint reported an infection.</td>
</tr>
<tr>
<td>Last Scan Time</td>
<td>The time of the last scan on this endpoint.</td>
</tr>
<tr>
<td>Last Seen</td>
<td>The date and time this endpoint last checked into the Management Portal.</td>
</tr>
<tr>
<td>Malware Group</td>
<td>The classification of the malware; for example: Trojan or System Monitor.</td>
</tr>
<tr>
<td>MD5</td>
<td>The Message-Digest algorithm 5 value, which acts like a fingerprint to uniquely identify a file.</td>
</tr>
<tr>
<td>OS</td>
<td>The operating system of the endpoint.</td>
</tr>
<tr>
<td>Pathname</td>
<td>The directory or folder where the file was detected.</td>
</tr>
<tr>
<td>Policy</td>
<td>The policy assigned to the endpoint.</td>
</tr>
<tr>
<td>Product</td>
<td>The name of the product associated with the file, if SecureAnywhere can determine that information.</td>
</tr>
<tr>
<td>OPTION</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Scan Type</strong></td>
<td>The type of scan:</td>
</tr>
<tr>
<td></td>
<td>• Deep Scan</td>
</tr>
<tr>
<td></td>
<td>• Post Cleanup Scan</td>
</tr>
<tr>
<td></td>
<td>• Custom/Right-Click Scan</td>
</tr>
<tr>
<td><strong>Status</strong></td>
<td>The current status of the endpoint:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Protected</strong> — No infections.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Infected</strong> — Malware detected.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Not Seen Recently</strong> — Has not reported into the portal.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Expired</strong> — SecureAnywhere license has lapsed.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Infected &amp; Expired</strong></td>
</tr>
<tr>
<td><strong>System Pack</strong></td>
<td>The number of the service pack for the operating system.</td>
</tr>
<tr>
<td><strong>System Type</strong></td>
<td>Either 32-bit or 64-bit.</td>
</tr>
<tr>
<td><strong>Vendor</strong></td>
<td>The name of the vendor associated with the file, if SecureAnywhere can determine that information.</td>
</tr>
<tr>
<td><strong>Version</strong></td>
<td>The version of the product associated with the file, if SecureAnywhere can determine that information.</td>
</tr>
<tr>
<td>OPTION</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>-------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>VM</td>
<td>Yes, if the endpoint is installed on a virtual machine.</td>
</tr>
<tr>
<td>Windows Full OS</td>
<td>The name of the Windows operating system.</td>
</tr>
</tbody>
</table>
Accessing the Management Console

Follow this procedure to return to the Sites tab in the management console when you are in Endpoint Protection.

To access the management console:

1. When you are in the endpoint console, do either of the following:
   - Click the Back to Sites button.
   - From the console name drop-down menu, select Back to Sites.
2. The system returns you to the management console, with the Sites tab active.
Chapter 3: Managing User Accounts

To manage user accounts, see the following topics:

- Editing Your Own Account Settings ................................................................. 54
- Managing Portal Users .................................................................................... 67
  - Creating New Portal Users ........................................................................... 67
  - Editing User Information ............................................................................ 71
- Setting Console User Permissions ................................................................. 74
- Adding Keycodes to Your Account ................................................................. 79
- Adding Consoles to Your Account ................................................................. 82
  - Adding Consoles ......................................................................................... 82
  - Renaming Consoles .................................................................................... 88
  - Switching Between Consoles ..................................................................... 88
- Renewing or Upgrading Your Account ......................................................... 89
- Adding Site Admins ....................................................................................... 91
- Editing Site Admin Settings .......................................................................... 96
- Deleting Site Admins ................................................................................... 105
Editing Your Own Account Settings

An account defines your user details, such as 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: To edit settings for other portal users, see Managing Portal Users on page 67.

Refer to the following procedures to learn about editing your own account settings:

- **Editing Admin Details & Permissions: on page 54**
- **Disabling 2-factor authentication on page 58**
- **Changing your password on page 60**
- **Changing your security code on page 62**
- **Changing your security questions on page 64**

**Editing Admin Details & Permissions:**

1. Click the **Down** arrow next to your login ID, then click **Account Settings**.

2. On the Account Settings page, click **Edit Details** to display the Admin Details tab, where you can edit the information.
3. In the Admin Details panel, make changes to your name, phone numbers, and time zone, and then click **Save Details** to return back to the Account Settings page.

**Note:** The Display Name is the name that displays in the Management Console.
## Account Settings

<table>
<thead>
<tr>
<th>Admin Details</th>
<th>Access &amp; Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>First Name</td>
<td></td>
</tr>
<tr>
<td>Last Name</td>
<td></td>
</tr>
<tr>
<td>Display Name</td>
<td></td>
</tr>
<tr>
<td>Office Phone</td>
<td></td>
</tr>
<tr>
<td>Mobile Phone</td>
<td></td>
</tr>
<tr>
<td>Time Zone</td>
<td>(UTC/GMT)</td>
</tr>
</tbody>
</table>

[Image of SecureAnywhere interface with Account Settings and Admin Details]
4. Next, to check your access permissions, click the **Access & Permissions** tab.
Note: If you are the main Endpoint Protection administrator, we recommend that you keep the default settings.

For more information about the settings, see Setting Console User Permissions on page 74.

5. When you're finished, click the Save Access & Permissions button to return back to the Account Settings page.

Disabling 2-factor authentication

1. Log in to the Endpoint Console, and click on the Account Settings tab on the drop-down menu located in the top-right of the screen to view your Account Settings.

2. Click Disable next to 2FA to open the Disable 2FA workflow.
3. Enter your email/phone number associated with your account as well as your Password, and then click Continue.

![Image of the Disable 2FA screen with an example email and password entered, and a Continue button highlighted.]

4. Open your mobile authenticator app, and enter the code shown there into the Authentication Code box, and click Confirm.

![Image of the Authentication Code screen with a field for entering the code, and a Confirm button highlighted.]

5. Click Disable 2FA.

![Image of the Disable 2FA screen with a message about disabling 2FA and options to cancel or disable 2FA, and a Disable 2FA button highlighted.]

Chapter 3: Managing User Accounts
Note: If you disable 2FA, you will be required to enter the Security Code you created when you registered your account. You can re-enable 2FA at any time from the Admins tab of the Console. For more information, see Enabling 2-factor authentication (2FA) on page 16.

6. 2FA is now disabled. You will receive an email confirmation that 2FA has been disabled on your account.

![Example email](image)

**Changing your password**
1. On the Account Settings page, click **Change** next to Password to open the Change Password page.
2. Enter your current password, a new password, and then click **Change Password.**

![Change Password Form](image)

**Changing your security code**

1. From the Account Settings page, click **Change** next to Security Code to open the Change Security Code page.
2. Enter a new personal security code in the box, enter your password, then click Change Security Code.

![Change Security Code](image)

**Changing your security questions**

1. On the Account Settings page, click **Change** next to Security Question to open the Change Security Questions page.
2. Select your security questions by clicking on each of the drop-down arrows and picking a question from the list as well as entering your answers into the applicable boxes, and then click **Change Security**.
Questions to update your account security questions.
Managing Portal Users

If you have Admin permission for Endpoint Protection, 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.

For more information, see Setting Console User Permissions on page 74.

This topic contains the following procedures:

- Creating New Portal Users
- Editing User Information

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. Click the Down arrow next to your login ID, then select Manage Users.
2. In the Manage Users panel, click the **Create New User** button.

3. In the Create New User panel, enter the user's email address. This is the address where the user receives the confirmation message and also serves as the user's login name.

   If you entered the wrong email address and the user does not receive the message, you can change the email address and re-send it later. For more information, see [Editing User Information](#).

4. To the right of the Time Zone field, click the **Pencil** icon at the right, then type the country, region, or city to open a drop-down menu of time zones and select the one where your user is located.

5. Select the **Yes** checkbox.

   Additional fields display at the bottom of the pane.
- SecureAnywhere — The Home page of [my.webrootanywhere.com](http://my.webrootanywhere.com). From here, the user can access other Webroot portals, such as the Mobile Protection portal, if your company purchased Mobile Protection. For more information, see the WSA Business - Mobile Protection Admin Guide.

- Endpoint Protection — The Management Portal or Admin Console for Endpoint Protection. When users have access to this portal, they can click the **Go to Endpoint Protection** button to enter the
6. From the SecureAnywhere drop-down arrow, select one of the following:
   - **Basic** — Limited access to consoles and account settings.
   - **Admin** — Full access to all keycodes, users, and account settings in Webroot portals.

7. From the Endpoint Protection drop-down menu, select one of the following:
   - **No Access**
   - **Basic** — Read-only access to endpoint scans
   - **Admin** — Full access to all settings

For more information on how to modify this user's permissions later, see *Setting Console User Permissions on page 74*.

8. When you're done, click the **Create User** button.

   The system sends 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.
**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 needed, you can resend the confirmation email by clicking the envelope icon next to the Awaiting Confirmation status.

**To edit portal users:**
1. Locate the row for the user you want to edit, then click that user's Edit icon at the far right.

![Manage Users]

**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 82.*

2. In the User Details panel, make the any needed changes to the name and phone numbers.

   If the user has an Awaiting Confirmation status, this window displays 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.

![Account Settings]
Note: For information on how to change the settings under Access & Permissions, see Setting Console User Permissions on page 74.

3. When you're done, click the Save Details button.
Setting Console User Permissions

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, the Home panel of [my.secureanywhere.com](http://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 portal user permissions:

1. Click the **Down** arrow next to your login ID, then select **Manage Users**.

2. Locate the row for the user you want to edit, then click that user's **Edit** icon.

   The **Edit** icon displays at the far right.
The User Details panel displays.

3. Click the **Access & Permissions** tab to see the list of Endpoint Protection functions and their associated access permissions.
4. Assign access permissions for this user, as described in the following table.
### Groups

- **Create & Edit** — Define and modify groups of endpoints.
- **Deactivate/Reactivate Endpoints** — Deactivate and reactivate endpoints from the Management Portal. For more information, see *Deactivating Endpoints on page 192*.
- **Assign Endpoints to Groups** — Allows the portal user to move one or more endpoints from one group to another.

For more information, see *Organizing Endpoints Into Groups on page 322*.

### Policies

- **Create & Edit** — Define, delete, rename, copy, and export policies.
- **Assign Policies to Endpoints** — Associate a policy with an endpoint or group of endpoints.

For more information, see *Implementing Policies on page 215*.

### Overrides

- **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.
- **Determination Capability** — Specify overrides based on these settings:
  - **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.

For more information, see *Implementing Overrides on page 414*. 
<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Commands</td>
<td></td>
</tr>
<tr>
<td>None</td>
<td>Do not allow this user to send commands to endpoints.</td>
</tr>
<tr>
<td>Simple</td>
<td>Access to the Agent and Clear Data commands, and view commands for selected endpoints.</td>
</tr>
<tr>
<td>Expert</td>
<td>Access all commands, including Expert Advanced options.</td>
</tr>
<tr>
<td></td>
<td>For more information, see <em>Issuing Commands to Endpoints on page 140</em>.</td>
</tr>
<tr>
<td>Alerts</td>
<td></td>
</tr>
<tr>
<td>Create &amp; Edit</td>
<td>Configure instant or scheduled alerts for endpoint activity.</td>
</tr>
<tr>
<td></td>
<td>For more information, see <em>Implementing Alerts on page 396</em>.</td>
</tr>
</tbody>
</table>

5. When you're done, click the **Save Access & Permissions** button.
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. For more information, see Setting Console User Permissions on page 74.

To add a keycode to your account:

1. Click the Down arrow next to your login ID, then select Manage Keycodes.

The Manage Keycodes panel displays.

- The Keycode list displays the attributes associated with each Endpoint Protection license.
- If your account has multiple consoles, you see only the keycodes that are associated with the currently active console.
The Keycode list displays the attributes associated with each Endpoint Protection license.

<table>
<thead>
<tr>
<th>ATTRIBUTE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keycode</td>
<td>The 20-character license you received when you purchased Endpoint Protection.</td>
</tr>
<tr>
<td>Edition</td>
<td>Endpoint Protection, or another Webroot product you purchased.</td>
</tr>
<tr>
<td>Devices</td>
<td>Number of endpoints that can use this keycode.</td>
</tr>
<tr>
<td>Days Remaining</td>
<td>Number of days remaining for this keycode to be active, and the expiration date.</td>
</tr>
</tbody>
</table>
2. To purchase another keycode, click the **Buy a Keycode** button.

   The Webroot Business website opens. From here, you can buy another keycode.

3. After you purchase the keycode, add it to Endpoint Protection by clicking the **Add Product Keycode** button.

4. In the Add a Keycode dialog, enter the keycode you just purchased and click **Add**.

   Your new keycode displays 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 topic contains the following procedures:

- Adding Consoles
- Renaming Consoles
- Switching Between Consoles

Adding Consoles

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:**
2. Instead of logging into your account, click the Create Account button.
3. In the **Webroot Product Keycode** field, enter the new keycode.
Chapter 3: Managing User Accounts

Create Account

Webroot Product Keycode

Email Address

Repeat Email Address

Password

Strength: 

Repeat Password

Your Personal Security Code

Security Question

Security Answer

Register Now
4. In the remaining fields, specify your existing account information for the email address, password, security code, and security questions and answers.

<table>
<thead>
<tr>
<th>FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email Address</td>
<td>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 into the Management Console.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter a minimum of nine characters. Your password must contain at least six alphabetic characters and three numeric characters. Your password can be longer than the required nine characters. It can include special characters, except for the angle brackets: &lt; &gt;. Your password is case sensitive. As you type, the Strength meter displays how secure your password is. For optimum security, it’s a good idea to make your password as strong as possible.</td>
</tr>
<tr>
<td>Your Personal Security Code</td>
<td>Enter a word or number, which will be used for an extra security step after you enter the password during login. Pick a code that is easy to remember, using a minimum of six 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 the system prompts you for the fourth and sixth character, you would enter 4 and 6. Your Personal Security Code is case sensitive.</td>
</tr>
<tr>
<td>FIELD</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>----------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Security Question</td>
<td>Select 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.</td>
</tr>
<tr>
<td>Security Answer</td>
<td>Type an answer to your security question. The Security Answer is case-sensitive.</td>
</tr>
</tbody>
</table>

5. Click the **Register Now** button.

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.

6. In the left pane, click the **Select** button 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 select the newly created **Unnamed Console**. You can rename it as described in the Rename a Console section.

Your new console lists any endpoints that use the keycode you entered.
Renaming Consoles

To rename a console:

1. Below your login name in the upper right, click the Rename button.

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

Switching Between Consoles

To switch between consoles:

1. Below your login name in the upper right, click the Change Console button.

2. From the table that displays, select the console name.
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.

![Status Panel]

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

To renew or upgrade your account:

1. Clicking the Down arrow next to your login ID, then select Manage Keycodes.
2. In the Manage Keycodes pane, click one of the following:
   - **Renew** — To extend your license.
   - **Upgrade** — To add more seats to your license.

   ![Manage Keycodes](image)

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

   The Webroot website opens with further instructions.
Adding Site Admins

If you are an Admin for Endpoint Protection, you can create additional admins. You might want to add other admins so they can access Endpoint Protection reports and view data.

When you create new users, Endpoint Protection sends them an email with further details for creating a password and logging in.

To add a site admin:

1. Log in to my.webrootanywhere.com.
2. Click the Endpoint Protection tab.

   The Endpoint Protection console displays.

3. From the drop-down menu next to your login ID, select Manage Admins.
4. Click the **Create New Admins** button.

The Create New Admin panel displays.
5. In the Email Address field, enter the user's email address.

This is the address where the user will receive 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 can change the email address and re-send it. For more information, see Editing Site Admin Settings on page 96.

6. In the Time Zone field, click the Pencil icon at the right, then type the country, region, or city to display a drop-down menu of choices. From that drop-down menu, select the appropriate time zone for the new admin.

7. Select the Do you wish to give this user console access? checkbox.

The following fields display:

- SecureAnywhere
- Endpoint Protection
- Mobile Protection
8. From the SecureAnywhere drop-down menu, select one of the following:
   - **Basic** — Gives limited access to consoles and account settings.
   - **Admin** — Gives full access to all keycodes, users, and account settings in Webroot portals.

9. From the Endpoint Protection drop-down menu, select one of the following:
   - **No Access**
   - **Basic** — Gives read-only access to endpoint scans.
   - **Admin** — Gives full access to all settings.

10. From the Mobile Protection drop-down menu, select one of the following:
    - **Access**
    - **No Access**
11. When you're done, click the **Create Admin** button to send a confirmation email to the new user.

![Create New Admin form](image)

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 displays for the admin to enter login information.
Editing Site Admin Settings

After the admin confirms registration, you can return to the Manage Admins panel and edit information for that user.

The status changes to Activated when the user receives the email and confirms the registration.

If the user has not confirmed registration, you will see the user's status as Awaiting Confirmation. If needed, you can resend the confirmation email by clicking the Envelope icon next to the Awaiting Confirmation status.

To edit site admin settings:

1. Log in to my.webrootanywhere.com.
2. Click the Endpoint Protection tab.
   The Endpoint Protection console displays.
3. From the main, click the Admins tab.

A list of admins displays.
4. Locate the row for the user you want to edit, then click that user's **Edit** button.

The Account Settings window displays with the Admin Details tab active.
**Account Settings**

<table>
<thead>
<tr>
<th>Admin Details</th>
<th>Access &amp; Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>First Name</td>
<td></td>
</tr>
<tr>
<td>Last Name</td>
<td></td>
</tr>
<tr>
<td>Display Name</td>
<td></td>
</tr>
<tr>
<td>Office Phone</td>
<td></td>
</tr>
<tr>
<td>Mobile Phone</td>
<td></td>
</tr>
<tr>
<td>Time Zone</td>
<td>(UTC/GMT)</td>
</tr>
</tbody>
</table>

[Save Details]
5. When you're done, click the **Save Details** button.

6. Click the **Access & Permissions** tab.
## Account Settings

### Admin Details

- **Access & Permissions**

### SecureAnywhere Console

- Admin

### Endpoint Protection Console

- Admin

### Groups

- Create & Edit
- Deactivate/Reactivate Endpoints
- Assign Endpoints

### Policies

- Create & Edit
- Assign Policies to Endpoints

### Overrides

- File and Web Overrides
  - File Determination Capabilities | Good & Bad

### Commands

- None
- Simple
- Advanced
- Expert

### Alerts

- Create & Edit

---

**Save Access & Permissions**

© 2019 Webroot Inc. Privacy Statement
7. Change any of the settings as needed, using the information in the following table.

<table>
<thead>
<tr>
<th>SETTING</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| SecureAnywhere Console        | Select one of the following permission levels:  
                                - No Access  
                                - Basic  
                                - Admin |
| Endpoint Protection Console   | Select one of the following permission levels:  
                                - No Access  
                                - Basic  
                                - Admin |
| Groups                         |             |
| Create & Edit                 | Select the checkbox to allow the admin to define and modify groups of endpoints. |
| Deactivate/Reactivate Endpoints| Select the checkbox to allow the admin to deactivate and reactivate endpoints from the Management Portal.  
                                For more information, see Deactivating Endpoints on page 192.
<table>
<thead>
<tr>
<th>SETTING</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| **Assign Endpoints to Groups** | Select the checkbox to allow the admin to move one or more endpoints from one group to another.  
For more information, see [*Organizing Endpoints Into Groups on page 322.*](#) |
| **Policies**                 |                                                                             |
| **Create & Edit**            | Select the checkbox to allow the admin to define, delete, rename, copy, and export policies. |
| **Assign Policies to Endpoints** | Select the checkbox to allow the admin to associate a policy with an endpoint or group of endpoints.  
For more information, see [*Implementing Policies on page 215.*](#) |
| **Overrides**                |                                                                             |
| **MD5**                      | Select the checkbox to allow the admin to 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. |
# Setting

<table>
<thead>
<tr>
<th>SETTING</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Determination Capability</strong></td>
<td>From the drop-down menu, select one of the following to determine overrides:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Good</strong> — Allow files containing the specified MD5 value.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Bad</strong> — Block files containing the specified MD5 value. When a scan encounters this file, it flags it and requests action from the SecureAnywhere user.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Good &amp; Bad</strong> — Allow either Good or Bad.</td>
</tr>
<tr>
<td></td>
<td>For more information, see <em>Implementing Overrides on page 414.</em></td>
</tr>
<tr>
<td><strong>Commands</strong></td>
<td></td>
</tr>
<tr>
<td><strong>None</strong></td>
<td>To not allow the admin to send commands to endpoints, select this radio button.</td>
</tr>
<tr>
<td><strong>Simple</strong></td>
<td>To give the admin access to the Agent and Clear Data commands, and view commands for selected endpoints, select this radio button.</td>
</tr>
<tr>
<td><strong>Advanced</strong></td>
<td>To give the admin access to Agent, Clear Data, Keycode, Power &amp; User Access, Antimalware Tools, Files &amp; Processes commands, and view commands for selected endpoints, select this radio button.</td>
</tr>
<tr>
<td><strong>Expert</strong></td>
<td>To give the admin access all commands, including Expert Advanced options, select this radio button.</td>
</tr>
<tr>
<td>SETTING</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Alerts</td>
<td>To allow the admin to configure instant or scheduled alerts for endpoint</td>
</tr>
<tr>
<td></td>
<td>activity, select the checkbox.</td>
</tr>
<tr>
<td></td>
<td>For more information, see <em>Implementing Alerts on page 396</em>.</td>
</tr>
</tbody>
</table>

8. When you're done, click the **Save Access & Permissions** button.
Deleting Site Admins

To delete a site admin:

1. Log in to my.webrootanywhere.com.
2. Click the Endpoint Protection tab.
   
   The Endpoint Protection console displays.

3. From the drop-down menu next to your login ID, select Manage Admins.

   A list of admins displays.
4. Locate the row for the user you want to edit, then click that user's Delete icon.

A warning message displays.
5. Click the **Yes** button to confirm the deletion.

6. Refresh your browser to confirm that the site admin has been removed from the system.
# Chapter 4: Managing Endpoints

To manage endpoints, see the following topics:

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deploying SecureAnywhere to Endpoints</td>
<td>110</td>
</tr>
<tr>
<td>Using the SecureAnywhere Installer</td>
<td>113</td>
</tr>
<tr>
<td>Using MSI for Deployment</td>
<td>126</td>
</tr>
<tr>
<td>Using GPO for Deployment</td>
<td>127</td>
</tr>
<tr>
<td>Installer Options</td>
<td>128</td>
</tr>
<tr>
<td>Installing on Terminal (RDS) Servers and Citrix XenApp</td>
<td>128</td>
</tr>
<tr>
<td>Installing on Duplicated Images or VMs</td>
<td>128</td>
</tr>
<tr>
<td>Changing Endpoint Keycodes</td>
<td>131</td>
</tr>
<tr>
<td>Renaming Endpoints</td>
<td>134</td>
</tr>
<tr>
<td>Searching for Endpoints</td>
<td>135</td>
</tr>
<tr>
<td>Issuing Commands to Endpoints</td>
<td>140</td>
</tr>
<tr>
<td>Managing Endpoint Updates and Other Changes</td>
<td>157</td>
</tr>
<tr>
<td>Migrating to a New Operating System</td>
<td>157</td>
</tr>
<tr>
<td>Changing Hardware on Endpoints</td>
<td>157</td>
</tr>
<tr>
<td>Moving Endpoints to New Subnets</td>
<td>157</td>
</tr>
<tr>
<td>Communicating Through Firewalls</td>
<td>158</td>
</tr>
<tr>
<td>Using SecureAnywhere on Endpoints</td>
<td>160</td>
</tr>
<tr>
<td>Opening SecureAnywhere on Windows Computers</td>
<td>160</td>
</tr>
<tr>
<td>Opening SecureAnywhere on Mac Computers</td>
<td>162</td>
</tr>
<tr>
<td>Mac Webroot SecureAnywhere Menu</td>
<td>163</td>
</tr>
<tr>
<td>Mac System Tools Drop-Down Menu</td>
<td>164</td>
</tr>
<tr>
<td>Checking Scan Results and Managing Threats</td>
<td>166</td>
</tr>
<tr>
<td>Viewing Scan Histories</td>
<td>166</td>
</tr>
<tr>
<td>Restoring Files From Quarantine</td>
<td>168</td>
</tr>
<tr>
<td>Setting Overrides for Files</td>
<td>169</td>
</tr>
<tr>
<td>Downloading and Forcing Updates</td>
<td>171</td>
</tr>
<tr>
<td>Forcing Immediate Updates</td>
<td>174</td>
</tr>
<tr>
<td>Installing Web Threat Shield Chrome Browser Extensions</td>
<td>175</td>
</tr>
<tr>
<td>Using Active Directory Group Policies</td>
<td>176</td>
</tr>
<tr>
<td>Using Google Suite to Force Install a Single Custom App</td>
<td>182</td>
</tr>
<tr>
<td>Using Registry</td>
<td>186</td>
</tr>
<tr>
<td>Running Commands at Endpoints</td>
<td>188</td>
</tr>
<tr>
<td>Deactivating Endpoints</td>
<td>192</td>
</tr>
<tr>
<td>Deactivating Endpoints</td>
<td>192</td>
</tr>
<tr>
<td>Reactivating SecureAnywhere on Endpoints</td>
<td>193</td>
</tr>
</tbody>
</table>
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 5.

**Note:** You can configure alerts so that administrators receive notification whenever new endpoints are installed. For more information, see Implementing Alerts on page 396.

To deploy SecureAnywhere to endpoints:

1. Find your keycode. If you don't know your keycode, click 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 Endpoint Keycodes on page 131.
2. Select a method of deployment that best suits your environment.

The following table describes methods of deployment.

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Deploy the SecureAnywhere executable file</strong></td>
<td>Deploy the SecureAnywhere installer file using one of these methods:</td>
</tr>
<tr>
<td></td>
<td>• Manually install the executable file on each endpoint.</td>
</tr>
<tr>
<td></td>
<td>• Send emails to end users, so they can install the software by clicking on</td>
</tr>
<tr>
<td></td>
<td>the link provided in the email template.</td>
</tr>
<tr>
<td></td>
<td>• Rename the executable file using your keycode. The email template also</td>
</tr>
<tr>
<td></td>
<td>provides a renamed executable file with the keycode.</td>
</tr>
<tr>
<td></td>
<td>• Use additional commands with the executable file to deploy it in the</td>
</tr>
<tr>
<td></td>
<td>background.</td>
</tr>
<tr>
<td></td>
<td>• Use command-line options with the installer to deploy to endpoints</td>
</tr>
<tr>
<td></td>
<td>that are behind a proxy server.</td>
</tr>
<tr>
<td><strong>Use MSI deployment options</strong></td>
<td>Deploy the SecureAnywhere installer file using the Microsoft Installer</td>
</tr>
<tr>
<td></td>
<td>(MSI).</td>
</tr>
<tr>
<td></td>
<td>You should have experience with Microsoft’s Active Directory and the GPO</td>
</tr>
<tr>
<td></td>
<td>editor.</td>
</tr>
</tbody>
</table>

**Note:** 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. For more information, see *Adding Consoles to Your Account on page 82*.  


3. Deploy SecureAnywhere to the endpoints, as described in one of these sections:
   - Using the SecureAnywhere Installer
   - Using MSI for Deployment.
   - Using GPO for Deployment

   **Note:** Check the Management Portal to make sure the endpoints have reported their status. For more information, see *Viewing Endpoint Statuses on page 197.*

4. Do either of the following:
   - Allow the system to assign endpoints to your default policy and default group. All endpoints are first assigned to your default policy and a default group. You can change those assignments later, if needed. For more information see *Implementing Policies on page 215* and *Applying Policies to Endpoint Groups on page 316.*
   - Assign endpoints to a specify group by selecting the group you want to add endpoints to, then from the Actions drop-down menu, select *Deploy Endpoints to this Group.*

   ![Webroot Endpoint Protection Admin Guide](image)

   The system displays information required to install the software via the command link, and then adds the endpoint to the selected group.
5. When you're done, click the **OK** button.

**Using the SecureAnywhere Installer**

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

- Install SecureAnywhere on each endpoint. Use this option if installing on a Mac.
- 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 for Windows:**

1. On the endpoint, download the SecureAnywhere installer file.
   
   The installer file is available from the Resources tab or by clicking this link:


2. In the installation panel, enter the keycode.
   
   Your keycode displays in the Resources tab.
3. Optionally, you can click the **Installation options** button 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 determine the language displayed in SecureAnywhere, click the **Change Language** button and select from the supported languages. You can only determine the displayed language during installation, not after.

4. Click the **Agree and Install** button.

   During installation, SecureAnywhere runs an immediate scan on the endpoint.

**To use the SecureAnywhere installer for Mac:**
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/wsamac.dmg

2. Download the SecureAnywhere installer to your Mac.

3. Double-click `wsamac.dmg` to open the installer.

4. Double-click the `Applications` folder to open it.

5. In the Applications folder, double-click the **Webroot SecureAnywhere** icon to begin activation.

6. In the first activation window, from the Language Selection drop-down menu, select a language and click the **Next** button.

   **Note:** Make sure you select the appropriate language. Once SecureAnywhere installs, you cannot change it.
7. In the next panel, enter your keycode and click the Activate button.

8. Follow any remaining on-screen prompts to complete the installation.

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 displays in the How to get started window.

3. Cut and paste the text into an email message. The link adds the correct keycode for the user. Send the email to the users.
The user clicks the link to begin installation. The program installs in the background, with the correct keycode already entered. When the process completes, a Webroot icon displays 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, as 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; for more information, contact Webroot Business Support.

   Command Lines for Windows
<table>
<thead>
<tr>
<th>COMMAND LINE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>/key=keycode</td>
<td>Installs with the provided keycode, with or without hyphens. For example: \texttt{wsasme.exe /key=xxxx-xxxx-xxxx-xxxx-xxxx}</td>
</tr>
<tr>
<td>/silent</td>
<td>Installs in the background.</td>
</tr>
<tr>
<td>/nostart</td>
<td>Installs without starting SecureAnywhere.</td>
</tr>
<tr>
<td>/lockautouninstall=\texttt{password}</td>
<td>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 /autouninstall command. When you use /lockautouninstall, SecureAnywhere is not included in the Add/Remove Programs list in the Control Panel. Use the /exeshowaddremove command to include SecureAnywhere in Add/Remove Programs.</td>
</tr>
<tr>
<td>/autouninstall=\texttt{password}</td>
<td>Corresponds to /lockautouninstall. Example: \texttt{wsasme.exe/autouninstall=\texttt{password}} By default, SecureAnywhere does not display in the Add/Remove Programs list in the Control Panel, which prevents the user from removing the software in unmanaged mode.</td>
</tr>
<tr>
<td><strong>COMMAND LINE</strong></td>
<td><strong>DESCRIPTION</strong></td>
</tr>
<tr>
<td>------------------</td>
<td>------------------</td>
</tr>
</tbody>
</table>
| -clone           | For cloned machines/VMs use this to have the agent create a persistent, unique value on the PC which will change what is displayed in the portal for the machine IDs and the hostname of the PC.  

The product log will indicate this flag being present for the administrator to be aware of which PC they're looking at, for example "Applied unique machine ID: C8137921" where C8137921 matches the hostname, for example, PCHOSTNAME-C8137921, as well as the first 8 bytes of both the InstanceMID and DeviceMID to allow each of them to be identifiable and different than the original IDs.  

This value will persist if the agent is uninstalled/reinstalled so that existing agents won't move to other IDs. If the OS is reinstalled, the ID will change.  

Example:  

```
wsasme.exe /key=xxxx-xxxx-xxxx-xxxx-xxxx /silent -clone
```

**Note:** For use when InstanceMID's are matching causing duplicates in the console or endpoints replacing endpoints at each poll interval.
<table>
<thead>
<tr>
<th>COMMAND LINE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| /exeshowaddremove | Includes SecureAnywhere in the Control Panel Add/Remove Programs list.  
Example:  
wsasme.exe /key=xxxx-xxxx-xxxx-xxxx  
/lockautouninstall=password/exeshowaddremove |

**Note:** Adding SecureAnywhere to Add/Remove Programs enables the endpoint user to remove the software in unmanaged mode.
<table>
<thead>
<tr>
<th>COMMAND LINE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| /group=groupcode | Command line switch for deploying directly into groups.  
Example:  
wsasme.exe /key=xxxxxxxxx /group=-135260017840748808 /silent  
Assign endpoints to a specific group by selecting the group you want to add endpoints to, then from the Actions drop-down menu, select Deploy Endpoints to this Group. Note the GROUPCODE.  
Other requirements:  
- The group must already exist in the console.  
- This only works new for new installs on systems that have never been seen by the console previously.  
Example for command line:  
msiexec /i "C:\wsasme.msi" GUILIC="XXXX-XXXX-XXXX-XXXX" CMDLINE="SME,quiet,Group=-135260017840748808" /qn /l*v %windir%\wsa_install_log.txt  
For MSI installs you can use command line and an MSI editor.  
Example for MSI Editor in CMDLINE field: Group=-135260017840748808 |
<table>
<thead>
<tr>
<th>COMMAND LINE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| -proxyhost=X -proxyport=X -proxyuser=X -proxypass=X -proxyauth=# | Specifies proxy settings.  

**Note:** 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.  

To enable proxy support, use these command-line options:  
```
wsasme.exe -proxyhost=nn.nn.nn.nn -proxyauth=n (where n can be 0=Any, 1=Basic, 2=Digest, 3=Negotiate, 4=NTLM) 
-proxyuser=proxyuser -proxypass=password -proxyport=port_number
```

We recommend that you use a specific value for-proxyauth, instead of 0 (any). The any option requires the endpoint to search through all authentication types, which might result in unnecessary errors on proxy servers as well as delayed communications.

If you use this command-line option, use all parameters and blank out any value you don't need with double quotes, for example:  
```
proxypass=""
```
<table>
<thead>
<tr>
<th>COMMAND LINE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>/lang=LanguageCode</td>
<td>Specifies the language to use for the product, rather than allow default language detection. Codes include:</td>
</tr>
<tr>
<td></td>
<td>en — English</td>
</tr>
<tr>
<td></td>
<td>ja — Japanese</td>
</tr>
<tr>
<td></td>
<td>es — Spanish</td>
</tr>
<tr>
<td></td>
<td>fr — French</td>
</tr>
<tr>
<td></td>
<td>de — German</td>
</tr>
<tr>
<td></td>
<td>it — Italian</td>
</tr>
<tr>
<td></td>
<td>nl — Dutch</td>
</tr>
<tr>
<td></td>
<td>ko — Korean</td>
</tr>
<tr>
<td></td>
<td>zh-cn — Simplified Chinese</td>
</tr>
<tr>
<td></td>
<td>pt — Brazilian Portuguese</td>
</tr>
<tr>
<td></td>
<td>ru — Russian</td>
</tr>
<tr>
<td></td>
<td>tr — Turkish</td>
</tr>
<tr>
<td></td>
<td>zh-tw — Traditional Chinese</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>wsasme.exe /key=xxxxxxxxxxxxx /silent /lang=ru</td>
</tr>
<tr>
<td>COMMAND LINE</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| -silent      | Installation will be silent.  
|              | sudo "/Applications/Webroot SecureAnywhere.app/Contents/MacOS/Webroot SecureAnywhere" install -keycode=<keycode> -silent |
| -proxy_auth= | Designates proxy install arguments including authentication method, host, port, user and password.  
|              | auth_any_0  
|              | auth_basic_1  
|              | auth_digest_2  
|              | auth_negociate_3  
|              | auth_ntlm_4  
|              | open "/Applications/Webroot SecureAnywhere.app" --args install -keycode=<keycode> -proxy_auth=auth_any_0 -proxy_host=<host> -proxy_port=<port> -proxy_user=<user> -proxy_pass=<password> |
| -keycode=    | Installation will not prompt for keycode.  
<p>|              | open &quot;/Applications/Webroot SecureAnywhere.app&quot; --args install -keycode=&lt;keycode&gt; |</p>
<table>
<thead>
<tr>
<th>COMMAND LINE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>-language=</td>
<td>Installs with designated language.</td>
</tr>
<tr>
<td></td>
<td>open &quot;/Applications/Webroot SecureAnywhere.app&quot; --args install -language=en</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Complete list of languages TBD.</td>
</tr>
<tr>
<td>Full String</td>
<td>sudo &quot;/Applications/Webroot SecureAnywhere.app/Contents/MacOS/Webroot SecureAnywhere&quot; install -keycode=XXXX-XXXX-XXXX-XXXX -language=en -silent -proxy_auth=auth_basic_1 -proxy_host=proxy.proxy.com -proxy_port=8080 -proxy_user=proxyuser.com -proxy_pass=proxypass</td>
</tr>
</tbody>
</table>
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:

```plaintext
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:**

To remove the SecureAnywhere software from the endpoint later, use the standard MSI command:

```plaintext
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.
<table>
<thead>
<tr>
<th>COMMAND</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMDLINE</td>
<td>SME,quiet</td>
</tr>
<tr>
<td>GUILIC</td>
<td>The license key, with or without hyphens.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> 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.</td>
</tr>
<tr>
<td>ARPNOREMOVE</td>
<td>To prevent the uninstallation by end users</td>
</tr>
</tbody>
</table>

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.
- Set the ARPNOREMOVE property in the Property table to the appropriate value.

**Using GPO for Deployment**

To install SecureAnywhere using GPO, you should have experience with Microsoft’s Active Directory and the GPO editor.

You can also watch a video on how to use GPO at [How to Deploy Using Group Policy - SecureAnywhere Business](How+to+Deploy+Using+Group+Policy+-+SecureAnywhere+Business).

**To install SecureAnywhere using GPO:**

1. From the following location, download the SecureAnywhere MSI installer to a network share:

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.

**Installer Options**

The WSA agent comes in two installer formats, EXE and MSI, both of which are located under the Resources tab in your WSA console.

- **EXE** — The EXE file format can be downloaded and installed either using the generic EXE file, `wsasme.exe`, or by using the Windows Download link, which is the EXE file, renamed using your WSA keycode, which when run, imbeds the keycode into the installation process, and runs as a silent and unattended installation.

- **MSI** — The MSI format can be downloaded utilizing the `wsasme.msi` link under the Install using MSI section. The MSI can be edited to customize the installation including the keycode in the GUILIC property and Command-Line options in the CMDLINE property and be deployed using GPO.

**Installing on Terminal (RDS) Servers and Citrix XenApp**

When installed on a Terminal server (RDS server) or Citrix XenApp for desktop/session brokering or hosted shared desktops, the WSA agent protects the environment by sharing its kernel module across sessions and provides a user process for each. The Webroot Management console displays the hosting server and each session as a combined single entry or device for reporting and management. The WSA agent does not support being streamed via application visualization.

**Installing on Duplicated Images or VMs**

When Webroot SecureAnywhere Business Endpoint protection is installed a ‘machine ID’ is generated from various hardware and software data points including Hostname, SID and MAC address. If endpoint images are re-used without ‘sys prepping’ them, or in virtual environments where VMs are copied or provisioned from a master image and not sys prepped as part of their deployment or provisioning, the endpoints will report into the console using the same ‘machine ID’ and compete for the same position or potentially generate duplicates in the Webroot management console.
If this occurs in your Webroot management console, please uninstall Webroot SecureAnywhere Business Endpoint Protection from the affected endpoints. Be sure to remove or rename the folder “WRDATA” located in %PROGRAMDATA% to ensure no configuration files remain, then, reinstall it with the “uniquedevice” command line option.

For example:

**Executable Method**

```
"wsasme.exe /key=xxxx-xxxx-xxxx-xxxx /silent -uniquedevice"
```

**MSI Method**

<table>
<thead>
<tr>
<th>CMDLINE</th>
<th>-uniquedevice</th>
</tr>
</thead>
</table>

This will cause SecureAnywhere to create a unique identification for that system by taking a checksum of the hostname and modifying the ‘machine ID’ with it. This is useful if the machines OS or hardware are cloned but the hostnames are always different. In this case, the unique hostname will allow there to be unique instances of devices for reporting into the Webroot management console. The hostname remains untouched so it will be reported into the console exactly as it exists within the OS.

For this reason it is not recommended to install Webroot SecureAnywhere Business Endpoint protection within an image that will be copied or used for provisioning without first being sys prepped. In most virtual environments Webroot SecureAnywhere Business Endpoint protection should be installed after the VM has been deployed using Group policy or logon script, etc including non-persistent VM environments.

If hostnames are not unique within the deployment the “clone” install switch should be used. For example:

**Executable Method**

```
"wsasme.exe /key=xxxx-xxxx-xxxx-xxxx /silent -clone"
```

**MSI Method**

<table>
<thead>
<tr>
<th>CMDLINE</th>
<th>-clone</th>
</tr>
</thead>
</table>

This creates a registry key stored in: HKLM\System\CurrentControlSet\Control\CloneTimeStampFlags

Use this to have the agent create a persistent, unique value on the PC which will change what is displayed in the portal for the machine IDs and the hostname of the PC.
The scan log will indicate this flag being present for the administrator to be aware of which PC they're looking at, for example:

"Applied unique machine ID: C8137921"

where C8137921 matches the hostname reported in the Webroot management console, for example, PCHOSTNAME-C8137921. This value will persist if the agent is uninstalled/reinstalled so that existing agents won't move to other IDs. If the OS is reinstalled, the ID will change.

For more information on how to deploy within a Citrix environment specifically, please see this document:

http://download.webroot.com/Citrix/Citrix.pdf
Changing Endpoint Keycodes

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 by activating a new keycode directly from the endpoint, as described in this procedure.

For information on how to issue a change keycode command, see Issuing Commands to Endpoints on page 140.

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 My Account gear icon.
3. In the Activate a new keycode field, enter your keycode.
4. Click the Activate button.

When you enter a new keycode, SecureAnywhere launches a scan. If the system 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.
To change a keycode on a Mac endpoint:

1. From the endpoint, click the **Webroot** icon in the menu bar, then from the drop-down menu, select **Open Webroot SecureAnywhere**.
2. From the main window, select **My Account**.
3. In the My Account window, click the **Activate a New Keycode** button.

![My Account window with Activate a New Keycode button highlighted]

4. In the dialog, enter your Endpoint Protection keycode and click the **Activate** button.

   Once the new keycode has been activated, return to the Management Portal and look for the new endpoint in the Default group.

   If needed, reassign the endpoint to another group. For more information, see *Moving Endpoints Between Groups on page 320.*
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 *Winchester-Laptop* or *LabTest-1*.

**Note:** Do not change the name of an endpoint on a virtual machine. If you do, it will display 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 endpoint you want to rename.
3. From the Endpoints panel on the right, double-click on the endpoint name.
4. Enter the new name and press the **Enter** key.
   
   A red flag displays in the upper left of the field to indicate that the change is not yet saved.

5. In the Command bar, click the **Save Changes** button.
   
   The new name displays in the Hostname column.

6. To revert to the original name, click the **Revert** button on the far right of the row.
Searching for Endpoints

Use this procedure to search for a single endpoint or multiple endpoints through our dynamic and flexible search functionality. This procedure also includes advanced searching options.

Note that each field or drop-down menu allows you to filter on any combination of criteria. For example, if you want to search on the status type and the policy type, then you would populate those two fields only. For additional filtering capability, enter additional information.

To search for an endpoint:

1. From the Endpoint Protection panel, click the Group Management tab.
2. Click the Search tab.

   The Search panel displays.
3. In the Hostname field, enter the name of the host.

   This is a free-form field, and is not case sensitive.
4. From the Status drop-down menu, select any of the following:
   - Protected
   - Infected
   - Expired
   - Infected & Expired
   - Not Seen Recently

5. From the Group drop-down menu, select the group in which you want to search.

6. From the Policy drop-down menu, select the policy in which you want to search.

7. In the Active Directory field, do either of the following:
   - Enter the active directory name.
   - Browse to the location of the active directory.

8. From the Keycode drop-down menu, select the keycode you want to search on.

9. From the Platform drop-down menu, select the platform you want to search on.

10. From the Windows OS drop-down menu, select one of the following operating systems:
    - Windows XP
    - Windows Vista
    - Windows 7
    - Windows 8
    - Windows Server
    - MacOS
    - Other

11. Do either of the following:
    - To include deactivated endpoints, select the **Include Deactivated** checkbox.
    - To exclude deactivated endpoints, do not select the **Include Deactivated** checkbox.

12. When you're done, click the **Submit** button to filter the results.

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

**To perform an advanced search:**
1. From the Endpoint Protection panel, click the **Advanced Search** button in the upper right corner of the panel.

The Advanced Search panel displays.

2. In the Agent version field, enter the agent number.

This is a free-form field.
3. From the Agent Language drop-down menu, select from a pre-set list of supported languages.

4. From the VM drop-down menu, select either of the following:
   - **Yes** — This is the default.
   - **No**

5. In the Device MID field, enter the unique Webroot-based identifier for the device.
   This is a free-form field.

6. In the Instance MID field, enter the Webroot-based identifier for the instance.
   This is a free-form field.

7. In the Current User field, enter the name of the current user.
   This is a free-form field.

8. In the Public IP Address field, enter the public IP address.
   This is a free-form field.

9. In the Internal IP Address field, enter the internal IP address.
   This is a free-form field.

10. From the Workgroup drop-down menu, select from a pre-set list of available workgroups.

11. In the MAC Address field, enter address of the MAC.
    This is a free-form field.

12. When you're done, click the **Submit** button to filter the results.
    The Management Portal displays all endpoints matching the search criteria in the right 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 or you can force an immediate polling. For more information, see Changing Policy Settings on page 240 or Forcing Immediate Updates on page 174.

**Note:** Depending on your access permissions for Commands, such as Simple, Advanced, or Expert, you may not see all the commands listed in this section. Administrators can change access permissions; for more information, see Setting Console User Permissions on page 74.

To issue commands to endpoints:

1. From the Endpoint console, click the Group Management tab.

The Group Management tab displays.
2. In the **Groups** column, select the group that contains the endpoints you want to issue commands to.

3. In the **Endpoints** panel, do either of the following to display information about an endpoint:
   - Select the checkbox next to the one endpoint.
   - Select the checkbox at the top of the **Checkbox** column.

   When you select one or more checkboxes, additional commands in the command bar become active and ready for use.
4. In the command bar, click the **Agent Commands** down arrow.

Based on your selection, the Agent Commands menu displays.

- If you selected PC endpoints or PC and Mac endpoints, your Agent Commands menu displays as follows:

- If you selected only Mac endpoints, your Agent Commands menu displays as follows, and does not
include Identity Shield commands or the option to remove password protection:

5. Select a category of agent commands and then, from the menu that expands, select a command to run.

For a description of each command, see the tables following these steps.

<table>
<thead>
<tr>
<th>COMMAND</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>AGENT COMMANDS</td>
<td>Run a Deep scan in the background as soon as the endpoint receives the command.</td>
</tr>
<tr>
<td>Scan</td>
<td>When the scan completes, the Scan History panel shows the results for a Deep scan.</td>
</tr>
<tr>
<td></td>
<td>This command runs on both PC and Mac endpoints.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> 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.</td>
</tr>
<tr>
<td>COMMAND</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Change scan time</td>
<td>Select a new time of day to scan the endpoint.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>This command runs on both PC and Mac endpoints.</td>
</tr>
<tr>
<td>Scan a folder</td>
<td>Runs a full, file-by-file scan on a specific folder. Be sure to enter the full path name.</td>
</tr>
<tr>
<td></td>
<td>On a Windows system, for example, you would enter:</td>
</tr>
<tr>
<td></td>
<td><code>C:\Documents and Settings\Administrator\My Documents</code></td>
</tr>
<tr>
<td></td>
<td>On a Mac system, for example, you would enter:</td>
</tr>
<tr>
<td></td>
<td><code>/Applications</code></td>
</tr>
<tr>
<td></td>
<td>This command runs on both PC and Mac endpoints.</td>
</tr>
<tr>
<td>Clean up</td>
<td>Start a scan and automatically quarantine malicious files.</td>
</tr>
<tr>
<td></td>
<td>When the scan completes, the Scan History panel shows results for the Post Cleanup Scan.</td>
</tr>
<tr>
<td></td>
<td>This command runs on both PC and Mac endpoints.</td>
</tr>
</tbody>
</table>
### COMMAND | DESCRIPTION
---|---
**System Optimizer** | Run the System Optimizer 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, such as files in the Recycle Bin and Windows temp files.  
You can change the System Optimizer options in the Policy settings.  
This command runs on both PC and Mac endpoints.

**Uninstall** | Uninstall SecureAnywhere from the endpoint.  
With this command, the endpoint is still shown in the Management Portal.  
To uninstall SecureAnywhere and free up a seat in your license, deactivate the endpoint instead. For more information, see [Deactivating Endpoints on page 192](#).  
This command runs on both PC and Mac endpoints.

**Reset** | Return SecureAnywhere settings on the endpoint to their default values.  
This command runs on both PC and Mac endpoints.
<table>
<thead>
<tr>
<th>COMMAND</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remove password protection</td>
<td>Disable password protection from the endpoint user's control, which allows administrators to gain access to the endpoint if they are locked out. This command runs only on PC endpoints.</td>
</tr>
<tr>
<td>Showgui</td>
<td>Displays the UI if policy allows for it. Example: &quot;\program files\webroot\wrsa.exe&quot; --showgui</td>
</tr>
<tr>
<td></td>
<td>This command runs only on PC endpoints.</td>
</tr>
<tr>
<td>COMMAND</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>SilentScan</td>
<td>Initiates a silent scan where the scan UI will not be presented to the user but will be seen if hovering over tray icon.</td>
</tr>
<tr>
<td></td>
<td>Command example:</td>
</tr>
<tr>
<td>WRSA.exe -silentscan=&quot;c:\foldername&quot;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example of run command to scan a folder:</td>
</tr>
<tr>
<td>&quot;C:\Program Files\Webroot\WRSA.exe&quot; - silentscan=&quot;c:\Documents and Settings\Administrator\Desktop&quot;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example of run command to scan a file:</td>
</tr>
<tr>
<td>&quot;C:\Program Files\Webroot\WRSA.exe&quot; - silentscan=&quot;c:\Documents and Settings\Administrator\Desktop\eicar.com&quot;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>This command runs only on PC endpoints.</td>
</tr>
<tr>
<td>Clear Data Commands</td>
<td></td>
</tr>
<tr>
<td>Clear files</td>
<td>Erase current log files, which frees space on the endpoint.</td>
</tr>
<tr>
<td></td>
<td>This command runs on both PC and Mac endpoints.</td>
</tr>
<tr>
<td>COMMAND</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Disable proxy settings</td>
<td>Disable any proxy settings the endpoint user set on the endpoint.</td>
</tr>
<tr>
<td></td>
<td>This command runs on both PC and Mac endpoints.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Do not use this command if the endpoint's only</td>
</tr>
<tr>
<td></td>
<td>Internet access is through the proxy server. The endpoint</td>
</tr>
<tr>
<td></td>
<td>will no longer be able to communicate with the cloud.</td>
</tr>
</tbody>
</table>

### KEYCODE COMMANDS

<table>
<thead>
<tr>
<th>COMMAND</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change keycode</td>
<td>Enter a different keycode.</td>
</tr>
<tr>
<td></td>
<td>This command runs on both PC and Mac endpoints.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The drop-down list displays only keycodes that are assigned to this console.</td>
</tr>
<tr>
<td>Change keycode temporarily</td>
<td>Switch the keycode used for this endpoint temporarily, which might be necessary for testing purposes.</td>
</tr>
<tr>
<td></td>
<td>In the dialog box, choose a keycode from the drop-down list, then specify the dates for SecureAnywhere</td>
</tr>
<tr>
<td></td>
<td>to use it. When the specified time for the change elapses, the keycode reverts to the original.</td>
</tr>
<tr>
<td></td>
<td>This command runs only on PC endpoints.</td>
</tr>
<tr>
<td>COMMAND</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Power And User Access Commands</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Lock endpoint</strong></td>
<td>Lock this endpoint by activating the login screen. The user must enter a user name and password to log back in.</td>
</tr>
<tr>
<td></td>
<td>This command runs on both PC and Mac endpoints.</td>
</tr>
<tr>
<td><strong>Log off</strong></td>
<td>Log the user out of the account.</td>
</tr>
<tr>
<td></td>
<td>This command runs on both PC and Mac endpoints.</td>
</tr>
<tr>
<td><strong>Restart</strong></td>
<td>Restart this endpoint when it reports in.</td>
</tr>
<tr>
<td></td>
<td>This command runs on both PC and Mac endpoints.</td>
</tr>
<tr>
<td><strong>Reboot in Safe Mode with Networking</strong></td>
<td>Restart this endpoint in Safe Mode with Networking.</td>
</tr>
<tr>
<td></td>
<td>This command runs only on PC endpoints.</td>
</tr>
<tr>
<td><strong>Shutdown</strong></td>
<td>Shut down this endpoint when it reports in.</td>
</tr>
<tr>
<td></td>
<td>This command runs on both PC and Mac endpoints.</td>
</tr>
<tr>
<td><strong>Antimalware Tools Commands</strong></td>
<td></td>
</tr>
<tr>
<td>COMMAND</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| **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 PC endpoint.  
This command runs on both PC and Mac endpoints. |
| **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.  
This command runs on both PC and Mac endpoints. |
| **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.  
This command runs only on PC endpoints. |

**Note:** This command resets Windows policies, not Endpoint Protection policies.
<table>
<thead>
<tr>
<th>COMMAND</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restore file</td>
<td>Restores a quarantined file to its original location, using its MD5 value.</td>
</tr>
<tr>
<td></td>
<td>For more information about how to locate a file's MD5 value, see <em>Applying Overrides From the Overrides Tab on page 429</em>.</td>
</tr>
<tr>
<td></td>
<td>This command runs only on PC endpoints.</td>
</tr>
<tr>
<td>File and process commands</td>
<td></td>
</tr>
<tr>
<td>Reverify all files and processes</td>
<td>Re-verify this file's classification when the next scan runs.</td>
</tr>
<tr>
<td></td>
<td>This command is useful if you have established some overrides and need them to take effect on an endpoint.</td>
</tr>
<tr>
<td></td>
<td>This command runs only on PC endpoints.</td>
</tr>
<tr>
<td>Consider all items as good</td>
<td>Consider all detected files on this endpoint as safe to run.</td>
</tr>
<tr>
<td></td>
<td>This command is useful if you find numerous false positives on an endpoint and need to quickly tag them as &quot;Good.&quot;</td>
</tr>
<tr>
<td></td>
<td>This command runs only on PC endpoints.</td>
</tr>
<tr>
<td>Allow processes blocked by firewall</td>
<td>Allow communication for all processes that are blocked by the Firewall setting.</td>
</tr>
<tr>
<td></td>
<td>This command runs only on PC endpoints.</td>
</tr>
<tr>
<td>COMMAND</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Stop untrusted processes</td>
<td>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. This command runs only on PC endpoints.</td>
</tr>
</tbody>
</table>

**IDENTITY SHIELD COMMANDS**

<table>
<thead>
<tr>
<th>COMMAND</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| 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 429*.  
This command runs only on PC endpoints. |
| 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 429*.  
This command runs only on PC endpoints. |
<table>
<thead>
<tr>
<th>COMMAND</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow all denied applications</td>
<td>Re-set all applications previously blocked, so they can run on the endpoint. This command runs only on PC endpoints.</td>
</tr>
<tr>
<td>Protect an application</td>
<td>Add extra security to an application running on the endpoint.</td>
</tr>
<tr>
<td></td>
<td>• To identify the application, you must enter its MD5 value.</td>
</tr>
<tr>
<td></td>
<td>• To determine an MD5 value, see <em>Applying Overrides From the Overrides Tab on page 429</em>.</td>
</tr>
<tr>
<td></td>
<td>This command runs only on PC endpoints.</td>
</tr>
<tr>
<td>Unprotect an application</td>
<td>Re-set the application to standard protection, if you previously used the Protect an application command to add extra security.</td>
</tr>
<tr>
<td></td>
<td>• To identify the application, you must enter its MD5 value.</td>
</tr>
<tr>
<td></td>
<td>• To determine an MD5 value, see <em>Applying Overrides From the Overrides Tab on page 429</em>.</td>
</tr>
<tr>
<td></td>
<td>This command runs only on PC endpoints.</td>
</tr>
<tr>
<td>COMMAND</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Run Customer Support Script</td>
<td>Specify a URL to download an executable file to the agent and run it remotely. This command runs only on PC endpoints.</td>
</tr>
<tr>
<td>Customer Support Diagnostics</td>
<td>Run the WSABLogs utility to gather information about an infected endpoint. The Customer Support Diagnostics dialog displays the location of the utility's executable file, and the email address associated with the endpoint account.</td>
</tr>
<tr>
<td></td>
<td>Clicking Submit runs the utility and sends the results to Webroot Business support.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>This command runs on both PC and Mac endpoints.</td>
</tr>
</tbody>
</table>

**Note:** Optional settings do not apply to Mac, and are not necessary for that platform.

6. As needed, do either of the following:
   - To see the status of commands you sent, from the Agent Command menu, select **View commands for selected endpoints**.
• To review the Command Log, in the main Endpoint Protection console, click the Logs tab. For more information, see Viewing Command Logs on page 510.

Endpoint Protection will issue the commands on the next polling interval for Windows computers. If needed, you can either change the polling interval in Basic Configuration of the group's policy or you can force the changes immediately as described in Forcing Immediate Updates on page 174.
## Policy1

<table>
<thead>
<tr>
<th>Section</th>
<th>Setting</th>
<th>Live</th>
<th>Draft</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Configuration</td>
<td>Show a Webroot shortcut on the desktop</td>
<td>Off</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Show a system tray icon</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Show a splash screen on bootup</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Show Webroot in the Start Menu</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Hide the Webroot keycode on-screen</td>
<td>Off</td>
<td>Daily</td>
</tr>
<tr>
<td>Core System Shield</td>
<td>Automatically download and apply updates</td>
<td>On</td>
<td>Daily</td>
</tr>
<tr>
<td></td>
<td>Operate background functions using fewer CPU resources</td>
<td>Off</td>
<td>12 Hours</td>
</tr>
<tr>
<td></td>
<td>Favor low disk usage over verbose logging (fewer details stored in logs)</td>
<td>Off</td>
<td>6 Hours</td>
</tr>
<tr>
<td></td>
<td>Lower resource usage when intensive applications or games are detected</td>
<td>Off</td>
<td>12 Hours</td>
</tr>
<tr>
<td></td>
<td>Allow Webroot to be shut down manually</td>
<td>Off</td>
<td>2 Hours</td>
</tr>
<tr>
<td></td>
<td>Force non-critical notifications into the background</td>
<td>On</td>
<td>1 Hour</td>
</tr>
<tr>
<td></td>
<td>Fade out warning messages automatically</td>
<td>On</td>
<td>30 Mins</td>
</tr>
<tr>
<td></td>
<td>Store Execution History details</td>
<td>On</td>
<td>15 Mins</td>
</tr>
</tbody>
</table>

Poll interval: 15 Mins
Managing Endpoint Updates 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
- Changing Hardware on Endpoints
- Moving Endpoints to New Subnets
- Communicating Through Firewalls

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. For more information, see Deactivating Endpoints on page 192.

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 Endpoints

If you install a new hard drive in an endpoint and reinstall SecureAnywhere on it, it will display 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. For more information, see Deactivating Endpoints on page 192.

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

Moving Endpoints to New Subnets

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:
Communicating Through Firewalls

If a firewall is in place, please allow Webroot’s path masks through the firewall, as described in the following table.

For more information on firewalls, see Preparing for Setup on page 5.

<table>
<thead>
<tr>
<th>PATH</th>
<th>INFORMATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>*.webrootcloudav.com</td>
<td>Agent communication and updates.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Some firewalls do not support double</td>
</tr>
<tr>
<td></td>
<td>dotted subdomain names with a single wildcard</td>
</tr>
<tr>
<td></td>
<td>mask, for example, g1.p4.webrootcloudav.com</td>
</tr>
<tr>
<td></td>
<td>being represented by *.webrootcloudav.com, so</td>
</tr>
<tr>
<td></td>
<td>some environments might require either</td>
</tr>
<tr>
<td></td>
<td>*.p4.webrootcloudav.com or</td>
</tr>
<tr>
<td></td>
<td><em>.</em>.webrootcloudav.com.</td>
</tr>
<tr>
<td>*.webroot.com</td>
<td>Agent messaging.</td>
</tr>
<tr>
<td>*.s3.amazonaws.com</td>
<td>Agent file downloading and uploading.</td>
</tr>
<tr>
<td>PATH</td>
<td>INFORMATION</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>WSAWebFilteringPortal.elasticbeanstalk.com</td>
<td>Required for agent Web Filtering, elasticbeanstalk is an amazon AWS domain.</td>
</tr>
<tr>
<td>*.webrootanywhere.com</td>
<td>Management portal and support ticket logs upload.</td>
</tr>
</tbody>
</table>
Using SecureAnywhere on Endpoints

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.

This topic contains the following procedures and information:

- Opening SecureAnywhere on Windows Computers
- Opening SecureAnywhere on Mac Computers
- Mac Webroot SecureAnywhere Menu
- Mac System Tools Drop-Down Menu

**Note:** For complete instructions on using the SecureAnywhere interface on the endpoint, see the Webroot SecureAnywhere for PC User Guide. For Mac computers, see SecureAnywhere Mac User Guide.

Opening SecureAnywhere on Windows Computers

To open the SecureAnywhere main interface on a Windows Computer:

1. From the endpoint, do one of the following:
   - Double-click the Webroot shortcut icon on the desktop.
   - Right-click the Webroot icon from the system tray menu, then select Open.
Note: If the system tray icon is hidden, open the Windows Start menu and select All Programs > Webroot SecureAnywhere > Webroot SecureAnywhere.

The Overview window displays.

Along the right side of the panel, the main interface includes navigation tabs.
### Opening SecureAnywhere on Mac Computers

To open the SecureAnywhere main interface on a Mac Computer:

1. From the endpoint, do one of the following:
   - To display the main window, click the **Webroot** icon in the menu bar.
   - From the drop-down menu, select **Open Webroot SecureAnywhere**.

<table>
<thead>
<tr>
<th>GEAR ICON</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PC Security</strong></td>
<td>Run custom scans, change shield settings, and manage the quarantine.</td>
</tr>
<tr>
<td><strong>Identity &amp; Privacy</strong></td>
<td>Protect sensitive data that may be exposed during online transactions.</td>
</tr>
<tr>
<td><strong>Utilities</strong></td>
<td>Use tools to manage processes and files, view reports, and submit a file to Webroot Support. Also use the System Optimizer to remove Internet browser activity and to remove temp files.</td>
</tr>
<tr>
<td><strong>My Account</strong></td>
<td>View SecureAnywhere account information and check for updates.</td>
</tr>
<tr>
<td><strong>Support/Community</strong></td>
<td>Access customer support and the Webroot Community.</td>
</tr>
</tbody>
</table>
When your system is secure, the main window looks similar to the following example.

The Webroot interface changes colors to reflect your computer's protection status:

- **Green** — Your Mac is secure.
- **Yellow** — One or more potential risks require your attention.
- **Red** — One or more critical items require your intervention.

**Mac Webroot SecureAnywhere Menu**

When the SecureAnywhere interface is active, the menu bar displays the SecureAnywhere options:
The following table describes the Webroot SecureAnywhere drop-down menu items on a Mac.

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>About SecureAnywhere</td>
<td>Displays the SecureAnywhere version number.</td>
</tr>
<tr>
<td>Preferences</td>
<td>Allows you to change system preferences, scan schedules, and other settings.</td>
</tr>
<tr>
<td>My SecureAnywhere Account</td>
<td>Displays your keycode and other account details.</td>
</tr>
<tr>
<td>Check for Updates</td>
<td>Downloads and applies the latest program updates.</td>
</tr>
<tr>
<td>Hide Webroot SecureAnywhere</td>
<td>Hides the main window, but does not shut down SecureAnywhere protection. If you want to shut down protection, click the Webroot icon in the menu bar and select <strong>Shut Down SecureAnywhere</strong>.</td>
</tr>
</tbody>
</table>

**Mac System Tools Drop-Down Menu**

The following table describes the System Tools drop-down menu items on a Mac.
<table>
<thead>
<tr>
<th>ITEM</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Control</td>
<td>Allows you to adjust the threat-detection settings for all programs and processes running on your Mac.</td>
</tr>
<tr>
<td>Reports</td>
<td>Allows you to save a scan log, which might be helpful if you are working with Webroot Support to determine the cause of a problem.</td>
</tr>
<tr>
<td>Submit a File</td>
<td>Allows you to send the file to Webroot for analysis. You might want to submit a file if you think it's causing problems or if you know it's safe and want it reclassified.</td>
</tr>
<tr>
<td>System Analyzer</td>
<td>Provides a simple utility for locating threats, security vulnerabilities, and other computer problems. The completed report recommends how to increase system performance, privacy, and protection.</td>
</tr>
</tbody>
</table>
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. For more information, see Restoring Files From Quarantine.

You can also reclassify a file as Good (allowed to run) or Bad (auto-quarantined). For more information, see Setting Overrides for Files.

Viewing Scan Histories

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 endpoints you want.
3. From the Endpoints panel on the right, select one of the endpoints.

![Image of the Endpoints panel](image)

The Scan History panel displays, displaying 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 needed, you can display or hide additional data about the endpoint and the scan history. Click a column header to display the drop-down menu, then select checkboxes to add or remove columns. For descriptions of the data in the columns, see Sorting Data in Tables and Reports on page 44.

**Restoring Files From Quarantine**

You can restore a file from quarantine from the Scan History panel. The file is automatically returned to its original location on the endpoint.

Additionally you can restore a file from the All Threats Seen report; for more information, see Generating All Threats Seen Reports on page 334.

**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 doing either of the following:
   - Click View in the Status column for the date when the threat was detected
   - Click the View all threats seen on this endpoint button
3. In the dialog that displays, select a file by selecting its checkbox.

4. Click the **Restore from Quarantine** button.

The system returns the file to its original location on the endpoint.

**Setting Overrides for Files**

You can set an override for a file from the Scan History panel. Additionally, you can set an override from the Overrides tab; for more information, see *Applying Overrides From the Overrides Tab on page 429*.

**To set an override for 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 doing either of the following:
   - Click **View** in the Status column for the date when the threat was detected
   - Click the **View all threats seen on this endpoint** button
3. In the dialog that displays, select a file in the list.

4. Click the **Create override** button.

The Create override window displays.

5. From the Determination drop-down menu, 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, select the **Apply the override globally** checkbox.
   - To select an individual policy for the override, deselect the **Apply the override globally** checkbox. When the Policy field displays, from the drop-down menu, select a policy.
Downloading and Forcing Updates

Unlike previous versions of Webroot software, Webroot SecureAnywhere automatically downloads and installs all updates by default. When we release the version update, it is load balanced across our global user base and can take up to 72 hours to apply to all Endpoints.

Each time you run a scan, your Webroot communicates with our cloud and download and applies any new determinations or updates to your machine. As long as your computer is connected to the internet, your protection is always current, as SecureAnywhere handles updates as soon as they become available.

Note: For more information, see the Advanced Commands table in Issuing Commands to Endpoints on page 140.

To download and force an update:

1. Log in to Endpoint Protection.
2. Click the **Group Management** tab.

3. In the Groups Pane on the left, select **All Endpoints**, then in the right pane, select one or more endpoints.

The menu bar displays the Agent Commands button.
4. From the Agents Command drop-down menu, select **Advanced > Run Customer Support Script**.

5. In the URL field, enter the following URL:

   `http://anywhere.webrootcloudav.com/zerol/wsasme.exe`

   **Note:** You can also use the URL to download the installer locally on the endpoint, then run it manually.

6. Follow the download wizard to install the latest updates.
Forcing Immediate Updates

The polling interval determines how often the endpoint sends its status and receives commands, for example, every 15 minutes or every hour. If needed, you can change the polling interval in Basic Configuration of the group's policy or you can force an immediate update as described in this procedure.

For more information, see *Changing Policy Settings on page 240*.

To force an update:

1. From the endpoint, in the system tray, right-click the Webroot icon.
2. From the drop-down menu that displays, select **Refresh configuration**.

The system updates.
Installing Web Threat Shield Chrome Browser Extensions

Webroot follows Google and the Chromium Projects best practice concerning Browser Extension deployment. Webroot therefore cannot deploy Browser Extensions without notifying end users. Partners wishing to install Chrome browser extensions silently in managed environments may do so using the following methods for enforced installation.

Enforced installation of the Chrome extension for Enhanced Web Threat Shield (EWTS) for Webroot SecureAnywhere in managed environments can be achieved easily. Enforced installation will not prompt the user to activate or accept the extension, and also prevents the user from disabling it.

In a non-enforced environment, the user will be prompted to enable the extension for Chrome as depicted the following image.

A non-enforced extension can, by design, be enabled, disabled or removed by the user via chrome://extensions/ as shown in the following image.
Chrome extensions, which are deployed silently in managed environments, are marked as shown in the following image. The user in this scenario cannot disable or remove the extension himself, this is controlled by the administrator. Note that there will not be any user prompts for enabling the extension.

![Webroot Filtering Extension](image)

**Using Active Directory Group Policies**

Google provides administrative templates for Windows Server 2003 (ADM template) and Windows Server 2008+ (ADMX template) which, once imported, will provide Chrome specific policies for Group Policies.

Required administrative templates can be downloaded from Google via below link:

[Zip file of Google Chrome templates and documentation](#)

To create a forced installation of Chrome browser extensions via Active Directory Group Policies:

1. Open the Group Policy Management console. Right click your domain and select **Create and Link a GPO here**.
2. Name your new GPO; in this example it is called Chrome Enforced Policy.
3. Right click your new GPO and select **Edit**. You should get a new window as shown below.

![Edit GPO window](image)

4. Expand the Computer Configuration.

5. Right click **Administrative Templates**.
6. Click **Add/Remove Templates**.

7. Click **Add**.
8. Point to the ADM or ADMX file from the Google Chrome templates archive you downloaded.

9. Click **Open** and then click **Close**.

   You should now see Google as an additional folder inside the Administrative Templates.
10. Inside the Administrative Templates, expand **Google\Google Chrome\Extensions**.

11. Click **Configure the list of force-installed extensions**.

12. Click **Enable**.

13. Click **Show**.

14. Add the line of text below to the list of Extension/App IDs and update URLs to be silently installed.

   kjeghcllfecehndceplomkocfbkllff;https://clients2.google.com/service/update2/crx
15. Confirm all dialogs/buttons.

This will install the Webroot EWTS extension for Chrome on any domain computer that this policy applies to.

**Using Google Suite to Force Install a Single Custom App**

Enforced installation of the Chrome extension for EWTS is supported on Google Suite managed environments. General directions for installing extensions and applications can be found in Google Help.

To install the Chrome extension for the EWTS you will need to add a Custom App using the following steps.

**To install the Chrome extension:**
1. Sign in to the Google Admin console.
2. From the Admin console dashboard, click Device management.
3. On the left, click Chrome management.
4. Click App management.
5. On the right, click the three dots to bring up the overflow menu.

6. Select Add custom app.
7. In the custom app dialog, enter the ID:
   kjeghcllfecenhndceplokmcgfbklfffd

8. Enter the following
   URL: https://clients2.google.com/service/update2/crx

   for Webroot Filtering Extension.
9. Click **Add**.

![Add custom app](image)

You must supply both the extension id and the url where the extension is hosted.

**ID**: kjeghfclfeehndceplomkocgbklffd

**URL**: https://clients2.google.com/service/upd

**ADD**

10. From the App Management screen select the newly added extension identified by the ID.

![Device management > Chrome > App Management](image)
11. From the app options, select **User Settings**.

![User settings](image)

**User settings**
Configure this app for users that log in with an account in your domain.

**Public session settings**
Configure this app for users that log in to a public session on your devices.

**Kiosk settings**
Deploy this app as a Kiosk App.

12. Select the relevant Org you wish to install the Chrome extension for EWTS into and turn **Allow installation** and **Force installation** ON.
13. Click **Save**.

Users logging into Chrome using their credentials for the chosen Org will now receive the Webroot Filtering Extension in their Chrome browser. Please refer to the G Suite documentation from Google regarding Org structures and advanced options for managing applications.

**Note:** At this time we do not support Webroot SecureAnywhere on Chromebooks. In order to avoid a poor experience for users running on these devices you will need to utilize policy control within G Suite, please refer to the G Suite help documentation for more information.

**Using Registry**

If using Active Directory or Google Suite are not suitable, using the Windows Registry might be an alternative to silently install the Chrome extension for the EWTS. Note that this option requires the computers to be part of a Microsoft Windows Domain.

**Note:** Using this method might conflict with Active Directory Group Policies or G Suite managed environments.

Details about available policy settings for Chrome can be found at:
Use the Windows Registry Editor (regedit.exe) to:

1. Check whether the Registry key listed below exists.

   ```
   [HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\ExtensionInstallForcelist]
   ```

   Existence of this key may indicate that other management applications are enforcing Chrome policies, specifically forced installation of extensions, which can cause conflicts if below steps are continued.

2. Add the following Registry value:

   Windows Registry Editor Version 5.00

   ```
   [HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\ExtensionInstallForcelist]"1"
   ="kjeghcl1fsecnhndcplomkogfbkffd;https://clients2.google.com/service/update2/crx"
   ```

   If you want to register additional extensions, please ensure continuous numbering.
Running Commands at Endpoints

An endpoint can be a Windows PC, laptop, server, or virtual server installed in your network. Use this procedure to run commands locally at the endpoint.

To run a command at an endpoint:

1. Click the **Start** menu.

   ![Start Menu]

2. In the Search Programs and Files field, enter **CMD**.

   The Command window displays.
3. At the command line, enter any of the following commands:
<table>
<thead>
<tr>
<th>COMMAND</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>-poll</td>
<td>Poll via a commandline option. Example: &quot;c:\program files\webroot\wrsa.exe&quot; -poll This will trigger a poll on-demand, allowing an SME customer to force a poll to occur by whatever means they currently have for executing software, psexec, for example. This will perform a software update, a configuration update, an agent commands update, and a license check at the same time.</td>
</tr>
<tr>
<td>-showgui</td>
<td>UI is brought up and displayed if policy allows for it. Example: &quot;c:\program files\webroot\wrsa.exe&quot; -showgui</td>
</tr>
<tr>
<td>-silentscan</td>
<td>Initiate a silent scan where the scan UI will not be presented to the user but will be seen if hovering over tray icon. Command example: WRSA.exe -silentscan=&quot;c:\foldername&quot; Example of run command to scan a folder: &quot;C:\Program Files\Webroot\WRSA.exe&quot; -silentscan=&quot;c:\Documents and Settings\Administrator\Desktop&quot; Example of run command to scan a file: &quot;C:\Program Files\Webroot\WRSA.exe&quot; -silentscan=&quot;c:\Documents and Settings\Administrator\Desktop\eicar.com&quot;</td>
</tr>
</tbody>
</table>

**Note:** Command only available in build 8.0.1.196 and higher.
<table>
<thead>
<tr>
<th>COMMAND</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| -scan   | Initiate a scan of specific location and the scan progress UI will be presented to the user upon initiation. Format: WRSA.exe -scan="c:\foldername"  
Example of run command to scan a folder: "C:\Program Files\Webroot\WRSA.exe" -scan="c:\Documents and Settings\Administrator\Desktop"  
Example of run command to scan a file: "C:\Program Files\Webroot\WRSA.exe" -scan="c:\Documents and Settings\Administrator\Desktop\eicar.com"  
**Note:** Command only available in build 8.0.1.196 and higher. |
| -uninstall | Uninstall the product if installed; can be executed on WRSA.exe as well.  
The uninstallation will not be silent. Only works if the endpoint is unmanaged. If endpoint is managed this command will only work in Windows Safe Mode with Networking; no actual network connection is needed.  
Examples:  
wsasme.exe -uninstall  
"c:\program files\webroot\wrsa.exe" -uninstall |

4. When you're done, click the red X in the upper right corner of the Command window to close it.
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 seven days. For more information, see *Issuing Commands to Endpoints* on page 140.

This topic contains the following procedures:

- Deactivating Endpoints
- Reactivating SecureAnywhere on Endpoints

### Deactivating Endpoints

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 endpoints you want.
3. Select one or more endpoints and from the Command bar, click the **Deactivate** button.

   ![Deactivate Button](image)

   A warning message displays, indicating that 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 displayed in the Deactivated Endpoints group. After seven 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.

### Reactivating SecureAnywhere on Endpoints

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. From the Deactivated Endpoints group, select the endpoint.
4. From the Command bar, click the **Reactivate** button.

![Reactivate button highlighted](image)

The system moves the endpoint back into its former group.
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. For more information, see Deactivating Endpoints on page 192.

- Send an uninstall command to the endpoint from the Management Portal. If you use method, the endpoint is still displayed in the Management Portal.
  
  To uninstall SecureAnywhere and free up a seat in your license, deactivate the endpoint instead. For more information, see Issuing Commands to Endpoints on page 140.
Chapter 5: Checking Statuses

To check statuses, see the following topics:

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Viewing Endpoint Statuses</td>
<td>197</td>
</tr>
<tr>
<td>Viewing Recent Threat Statuses</td>
<td>201</td>
</tr>
<tr>
<td>Viewing Agent Version Overviews</td>
<td>205</td>
</tr>
<tr>
<td>About Dwell Time</td>
<td>207</td>
</tr>
<tr>
<td>Exporting CSV Files From Endpoint Protection</td>
<td>209</td>
</tr>
</tbody>
</table>
Viewing Endpoint Statuses

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 166.

To view an endpoint's status:

1. Log in to the SecureAnywhere website.
2. Click the Go to Endpoint Protection button.
3. If any endpoints are infected, you can click a link for those endpoints to go directly to a details panel.

4. When the Management Portal displays, view endpoint statuses in the left panels for Status and Endpoint activity.
5. Do either of the following to drill down for more detail in both of these panels:
   - If you see an alert message in the Status panel, click the link to display more information about the endpoints.
• If any endpoints have not reported into the portal, in the Endpoint activity panel, in the Not Seen row, click the View link.

6. You can see endpoints in the Status tab and the Group Management tab. For more information on the Group Management tab, see Organizing Endpoints Into Groups on page 322.
Viewing Recent Threat Statuses

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

To view recent threat statuses:

1. Click the Status tab.

   The bar chart at the top displays a daily summary of threats found on endpoints. The table at the bottom of the panel displays more details about the endpoints.

2. To learn more about a threat, locate the threat in the row, and in the Blocked Columns column, click the View link.

   The Blocked Programs view displays.

Note: For more information on Dwell Time, see About Dwell Time.
3. To display or hide additional data about the recently infected endpoints in the bottom panel, click a column header to open the drop-down menu, then select checkboxes to add columns or deselect checkboxes to remove columns.

4. For descriptions of the data in the columns, see *Sorting Data in Tables and Reports on page 44.*

5. For additional information on any risks posed by threats and undetermined file types, click on any file name.

The system displays the File Intelligence view.

The various aspects of this view are described in the following table.
### FIELD | DESCRIPTION
--- | ---
Determination | Hover the mouse over the determination to display agent, rule, and cloud information.
Global Popularity | Displays information on the first time (FS) the file has been seen by WIN and also its global popularity, that is, how much it has been seen by others.
Google Product/Vendor Links | Click the link to access additional information about the file. This can be useful when the admin is unsure about the classification.
Create Override | Click the button to override the file for white- or blacklisting purposes.
Console Popularity | Displays how many times the file has been seen within the console and when.
Console Dwell Time | Displays how many times the file has been seen within the console and for how long.
Endpoint Dwell Time | Displays how long the file has been seen on the device in question.

6. 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.

For more information, see *Generating Endpoints With Threats On Last Scan Reports on page 353.*
Viewing Agent Version Overviews

The Agent Version Spread pie chart on the Status tab displays 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. Click the Status tab.

   The Status panel displays with the Agent Version Spread chart on the right.

   ![Agent Version Spread Chart]

2. To see more details, move your cursor over sections of the pie chart.
3. For more information, see *Generating Agent Version Spread Reports on page 381.*
About Dwell Time

Webroot has the smallest, lightest least intrusive agent on the market with multiple protection mechanisms on the agent, which provide incredible protection against the latest threats.

On our Webroot Intelligence Network, we process millions of events a day to better improve the efficacy in the solution from a detection perspective. However, as we do not, nor can anyone in the industry, catch every piece of malware on the device at first sight, although Webroot does a very good job at this.

In 2014, Gartner Magic Quadrant named Webroot as the only vendor with the ability to see Dwell Time.

We continue to introduce more forensic-like capabilities to ensure our customers have as much context around malicious events as possible, without the noise associated with other event-based solutions.

So what happens with applications that have yet to be classified?

During the time which an application is yet to be classified, the agent journals the changes made on disk while ensuring persistent changes are not made. If the application has been classified as Bad, the agent will rollback those journal changes made by the application and remediate the PC. This acts as a safety net, along with components like the Identity Shield, against malware that has yet to be classified by Webroot.

What does Dwell Time mean?

- Dwell Time is defined as the time the threat has been present on the device. It is calculated from the first time the file is active to when the file was last seen.
- Dwell Times of zero (0) seconds mean that the file was blocked at first sight.

Dwell Times greater than zero (0) seconds mean that the file has been present for a period of time prior to Webroot removing the file from the system.

Reasons for a Dwell Time of greater than zero (0) seconds may be that the user has yet to complete the clean-up routine, the file has been re-introduced onto the system after being originally removed, or the file did not yield malicious behavior at first sight, therefore the file was not immediately classified as malicious.

Webroot SecureAnywhere constantly monitors the system and journals the changes made by any potentially malicious file. We then roll back the changes. Other protection mechanisms are in place, as well, to ensure that the system is protected against malicious attacks, no matter how long the dwell time is.
Why doesn't Webroot classify everything at first sight?

The model of blacklisting every file at first sight is unachievable and the only way to combat threats is by monitoring all the changes made on the device and ensuring these changes can be rolled back. This differentiates us further against the rest of our competition.

Where will Dwell Time be visible?

This first phase of implementation will display the Dwell Time in all reports and areas where an infection can be seen in the console. The next phases will include email alert integration and specific dwell time reports and summaries.
Exporting CSV Files From Endpoint Protection

Follow the steps in this topic to export a CSV file that contains information about endpoints that need attention. The CSV file can be retained for future access and shared as needed.

This functionality is available wherever the Export to CSV icon exists.

To export a CSV file from Endpoint Protection:
1. In Endpoint Protection, click the **Status** tab.

2. In the Status area, click the **Endpoint needs attention** link.

The Endpoints needing attention window displays.
3. Do either of the following:
   
   - To export information about Endpoints with threats, click the **Export to CSV** icon in the upper right corner.

   ![Endpoints with threats table]

   - To export information about threats seen on this endpoint, select an endpoint to populate the Threats seen on this endpoint area, then select the item you want, and click the **Export to CSV** icon.

   ![Threats seen on this endpoint table]
The system displays a message indicating that you have requested a CSV file.

4. To close the window, click the **OK** button.

The system sends a link to the email address that you used to log in to the system.
5. Click the link in the email to display the CSV file, which you can then save to your computer.
# Chapter 6: Managing Policies

To manage policies, see the following topics:

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Implementing Policies</td>
<td>215</td>
</tr>
<tr>
<td>Selecting New Default Policies</td>
<td>220</td>
</tr>
<tr>
<td>Creating Policies</td>
<td>226</td>
</tr>
<tr>
<td>Creating Policies</td>
<td>226</td>
</tr>
<tr>
<td>Copying Policies</td>
<td>230</td>
</tr>
<tr>
<td>Renaming Policies</td>
<td>235</td>
</tr>
<tr>
<td>Changing Policy Settings</td>
<td>240</td>
</tr>
<tr>
<td>Basic Configuration</td>
<td>252</td>
</tr>
<tr>
<td>Scan Schedule</td>
<td>255</td>
</tr>
<tr>
<td>Scan Settings</td>
<td>257</td>
</tr>
<tr>
<td>Self Protection Settings</td>
<td>262</td>
</tr>
<tr>
<td>Heuristics</td>
<td>263</td>
</tr>
<tr>
<td>Realtime Shield Settings</td>
<td>267</td>
</tr>
<tr>
<td>Behavior Shield Settings</td>
<td>270</td>
</tr>
<tr>
<td>Core System Shield</td>
<td>272</td>
</tr>
<tr>
<td>Web Threat Shield</td>
<td>274</td>
</tr>
<tr>
<td>Identity Shield</td>
<td>277</td>
</tr>
<tr>
<td>Firewall</td>
<td>280</td>
</tr>
<tr>
<td>User Interface</td>
<td>282</td>
</tr>
<tr>
<td>System Optimizer</td>
<td>283</td>
</tr>
<tr>
<td>Viewing Endpoints Assigned to Policies</td>
<td>293</td>
</tr>
<tr>
<td>Moving Endpoints Between Policies</td>
<td>299</td>
</tr>
<tr>
<td>Deleting Policies</td>
<td>304</td>
</tr>
</tbody>
</table>
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 Console User Permissions on page 74.

To implement a policy:

1. Log in to your Endpoint Protection console.

The Endpoint Protection console displays, with the Status tab active.
2. Click the **Policies** tab.

The Policies tab displays.
3. Decide if you want to keep using your default policy.

Your default policy is located on the left side of the pane, and is indicated by a white, horizontal arrow.
4. Double-click on your default policy to display the settings.

- Settings that apply to PC only are indicated by the Windows icon.
Settings that apply to PC and Mac are indicated by both the Windows icon and the Mac icon.

Note: You cannot see any settings for the Unmanaged policy, because that policy specifies that endpoint users have control, not the administrator.

5. Review the policy settings and determine if the default policy meets your business requirements. If not, as you cannot modify the Webroot defaults, you will need to create a new policy.

   For more information, see Creating Policies on page 226.

6. Once you create new policies, you can assign them to endpoints in the Group Management tab.

   For more information, see Applying Policies to Endpoint Groups on page 316.
Selecting New Default Policies

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

To select a new default policy:

1. Log in to your Endpoint Protection console.

The Endpoint Protection console displays, with the Status tab active.
2. Click the **Policies** tab.

The **Policies** tab displays.
Your default policy is located on the left side of the pane, and is indicated by a white, horizontal arrow.
3. In the Policy Name column, click the policy you want to use as the new default.

The Set as Default icon becomes active.
4. Click the **Set as Default** icon.

![Set as Default icon](image)

The Set Default Policy window displays.

![Set Default Policy window](image)

5. Click the **Yes** button.

![Yes button](image)
The white arrow moves to the new default policy, which 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 240*.

This topic contains the following procedures:

- Creating New Policies
- Copying Policies

**Note:** 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 Policies

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. Log in to your [Endpoint Protection console](#).

   The Endpoint Protection console displays, with the Status tab active.
2. Click the **Policies** tab.

The Policies tab displays.
3. In the Command bar, click the **Create** button.

The Create Policy window displays.
4. In the Policy Name field, enter a policy name.

5. In the Policy Description field, enter a description of up to 50 alphanumeric characters.
6. Click the **Create Policy** button.

   ![Create Policy dialog box](image)

7. In the Policy Name column, locate your new policy.

   You can do either of the following:

   - Double-click the policy and change the settings. For more information, see *Changing Policy Settings on page 240*.
   - Apply the policy to an individual endpoint or to a group of endpoints. For more information, see *Applying Policies to Endpoint Groups on page 316*.

### Copying Policies

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. Log in to your **Endpoint Protection console**.

   The Endpoint Protection console displays, with the Status tab active.
2. Click the **Policies** tab.

The Policies tab displays.
3. In the Policy Name column, select the policy you want to use as a starting point and then click the Copy icon.
The Copy Policy window displays, with the policy you selected in the Policy to Copy field.

4. As needed, from the **Policy to Copy** drop-down menu, select a different policy to copy.
5. In the Policy Name field, enter a unique name.

6. In the Policy Description field, enter a description of up to 50 alphanumeric characters.

7. In the Policy Name column, locate your new policy.

   You can do either of the following:

   - Double-click the policy and change the settings. For more information, see *Changing Policy Settings on page 240*.
   - Apply the policy to an individual endpoint or to a group of endpoints. For more information, see *Applying Policies to Endpoint Groups on page 316*. 
Renaming Policies

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

To rename a policy:

1. Log in to your Endpoint Protection console.

   The Endpoint Protection console displays, with the Status tab active.
2. Click the **Policies** tab.

The Policies tab displays.
3. In the Policy Name column, select the policy you want to rename.

The Rename icon becomes active.
4. Click the **Rename** icon.

The Rename Policy window displays.
5. In the Policy Name field, enter a new name and a description for the policy.

6. In the Policy Description field, update the description for the policy, as needed.

7. When you're done, click the Rename Policy button.

The Policy Name column reflects the new policy name.
Changing Policy Settings

Once you create a policy, you can change its settings to suit your business purposes. If needed, you can make temporary changes, called creating drafts, and then implement them later, called promoting to live. For more information, see Creating Policies on page 226.

Note: You cannot change Webroot default policy settings.

Policies control the following SecureAnywhere settings on managed endpoints.

<table>
<thead>
<tr>
<th>SECTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Configuration</td>
<td>General preferences that change the behavior of the SecureAnywhere program, such as whether the program icon displays in the endpoint's system tray and whether the user can shut down the program.</td>
</tr>
<tr>
<td>Scan Schedule</td>
<td>Allows 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.</td>
</tr>
<tr>
<td>Scan Settings</td>
<td>Provides more control over scans, such as performing a more thorough scan.</td>
</tr>
<tr>
<td>Self Protection</td>
<td>Provides 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.</td>
</tr>
<tr>
<td>SECTION</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>---------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Heuristics</td>
<td>Provides 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.</td>
</tr>
<tr>
<td>Realtime Shield</td>
<td>Blocks known threats listed in Webroot's threat definitions and in Webroot's community database.</td>
</tr>
<tr>
<td>Behavior Shield</td>
<td>Analyzes applications and processes running on the endpoints.</td>
</tr>
<tr>
<td>Core System Shield</td>
<td>Monitors the computer system structures to ensure that malware has not tampered with them.</td>
</tr>
<tr>
<td>Web Threat Shield</td>
<td>Protects endpoints as users surf the Internet and click links in search results.</td>
</tr>
<tr>
<td>Identity Shield</td>
<td>Protects 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.</td>
</tr>
<tr>
<td>Firewall</td>
<td>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.</td>
</tr>
</tbody>
</table>
### SECTION

<table>
<thead>
<tr>
<th>User Interface</th>
<th>Provides user access to the SecureAnywhere program on the endpoint.</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Optimizer</td>
<td>Controls System Optimizer behavior, such as an automatic cleanup schedule and what types of files and traces to remove from the endpoint.</td>
</tr>
</tbody>
</table>

**To change policy settings:**

1. Log in to your [Endpoint Protection console](webroot_endpoint_protection_admin_guide).

The Endpoint Protection console displays, with the Status tab active.
2. Click the **Policies** tab.

The Policies tab displays.
3. In the Policy Name column, find the policy you want to change and double-click it.

The settings window for that policy displays, with the Basic Configuration setting selected in the Section column.
The Setting column displays the name of the policy, in addition to which:

- Settings that apply to PC only are indicated by the Windows icon.
- Settings that apply to PC and Mac are indicated by both the Windows icon and the Mac icon.

- The Live column displays how the setting is currently implemented on the endpoints.

- The Draft column is where you make changes.
4. In the Section column, select the category you want to edit.
5. In the Draft column, for each Setting, double-click in the cell to view the options, then, from the drop-down menu, select the appropriate setting.

For a complete description of each setting, see the following tables in this procedure.

<table>
<thead>
<tr>
<th>Basic Configuration</th>
<th>Realtime Shield</th>
<th>Firewall</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan Schedules</td>
<td>Behavior Shield</td>
<td>User Interface</td>
</tr>
<tr>
<td>Scan Settings</td>
<td>Core System Shield</td>
<td>System Optimizer</td>
</tr>
<tr>
<td>Self Protection</td>
<td>Web Threat Shield</td>
<td></td>
</tr>
<tr>
<td>Heuristics</td>
<td>Identity Shield</td>
<td></td>
</tr>
</tbody>
</table>
6. When you're done making changes for a selection, click the **Save Changes** button.

![Example screenshot of a policy configuration page]

7. Continue editing each section for that policy, making sure to click **Save Changes** before you move to another section.

   Any policy with changes not yet implemented displays in the Draft Changes column.
8. Do either of the following:
   - If you’re not ready to implement the changes, click the **Save Changes** button and return to the Policy tab.
If you are ready to implement the changes, click the **Save Changes** button, then click the **Promote Draft Changes to Live** button.
Basic Configuration

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

<table>
<thead>
<tr>
<th>SETTING</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show a SecureAnywhere shortcut on the desktop</td>
<td>Provides quick access to the main interface by placing the shortcut icon on the endpoint desktop.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Show a system tray icon</td>
<td>Provides quick access to SecureAnywhere functions by placing the Webroot icon in the endpoint system tray.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Show a splash screen on bootup</td>
<td>Opens the Webroot splash screen when the endpoint starts.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Show SecureAnywhere in the Start Menu</td>
<td>Lists SecureAnywhere in the Windows Startup menu items.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>SETTING</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>----------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Show SecureAnywhere in Add/Remove Programs</td>
<td>Lists SecureAnywhere in the Windows Add/Remove Programs panel.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Show SecureAnywhere in Windows Action Center</td>
<td>Lists SecureAnywhere in the Windows Action Center, under Virus Protection information.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Hide the SecureAnywhere keycode and subscription information on-screen</td>
<td>Hides the keycode on the endpoint's My Account panel. Asterisks replace the code, except for the first four digits.</td>
</tr>
<tr>
<td></td>
<td>This setting applies to both PC and Mac endpoints.</td>
</tr>
<tr>
<td>Automatically download and apply updates</td>
<td>Downloads product updates automatically without alerting the endpoint user.</td>
</tr>
<tr>
<td></td>
<td>This setting applies to both PC and Mac endpoints.</td>
</tr>
<tr>
<td>Operate background functions using fewer CPU resources</td>
<td>Saves CPU resources by running non-scan related functions in the background.</td>
</tr>
<tr>
<td></td>
<td>This setting applies to both PC and Mac endpoints.</td>
</tr>
<tr>
<td>SETTING</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>--------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Favor low disk usage over verbose logging (fewer details stored in logs)</td>
<td>Saves disk resources by saving only the last four log items. This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Lower resource usage when intensive applications or games are detected</td>
<td>Suppresses SecureAnywhere functions while the user is gaming, watching videos, or using other intensive applications. This setting applies to both PC and Mac endpoints.</td>
</tr>
<tr>
<td>Allow SecureAnywhere to be shut down manually</td>
<td>Displays a Shutdown command in the endpoint's system tray menu. Deselecting this option removes the Shutdown command from the menu. This setting applies to both PC and Mac endpoints.</td>
</tr>
<tr>
<td>Force non-critical notifications into the background</td>
<td>Suppresses information-only messages from displaying in the system tray. This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Fade out warning messages automatically</td>
<td>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. This setting applies to both PC and Mac endpoints.</td>
</tr>
<tr>
<td>SETTING</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Store Execution History details</td>
<td>Stores data for the Execution History logs, available under Reports. This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Poll interval</td>
<td>Specifies how often the endpoint checks for updates. For example: 15 minutes, 30 minutes, 1 hour, or 2 hours. This setting applies to both PC and Mac endpoints.</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>SETTING</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Scheduled Scans</td>
<td>Allows scheduled scans to run on the endpoint. This setting applies to both PC and Mac endpoints.</td>
</tr>
<tr>
<td>Scan Frequency</td>
<td>Determines how often to run the scan. You can set a day of the week or select on bootup. This setting applies to both PC and Mac endpoints.</td>
</tr>
<tr>
<td>SETTING</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Time</td>
<td>Specifies the time to run the scan:</td>
</tr>
<tr>
<td></td>
<td>• Scan time options for when computer is idle are before 8:00 a.m., before noon, before 5:00 p.m., or before midnight.</td>
</tr>
<tr>
<td></td>
<td>• Scan time options for when resources are available are hourly, from 12:00 a.m. to 11:00 p.m.</td>
</tr>
<tr>
<td></td>
<td>This setting applies to both PC and Mac endpoints.</td>
</tr>
<tr>
<td>Scan on bootup if the computer is off at the scheduled time</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>This setting applies to both PC and Mac endpoints.</td>
</tr>
<tr>
<td>Hide the scan progress window during scheduled scans</td>
<td>Runs scans silently in the background. If this option is disabled, a window opens and displays the scan progress.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Only notify me if an infection is found during a scheduled scan</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>SETTING</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Do not perform scheduled scans when on battery power</td>
<td>Helps conserve battery power. If you want SecureAnywhere to launch scheduled scans when the endpoint is on battery power, deselect this option. This setting applies to both PC and Mac endpoints.</td>
</tr>
<tr>
<td>Do not perform scheduled scans when a full screen application or game is open</td>
<td>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. This setting applies to both PC and Mac endpoints.</td>
</tr>
<tr>
<td>Randomize the time of scheduled scans up to one hour for distributed scanning</td>
<td>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. This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Perform a scheduled Quick Scan instead of a Deep Scan</td>
<td>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. This setting applies only to PC endpoints.</td>
</tr>
</tbody>
</table>

**Scan Settings**

Scan settings give advanced control over scanning performance.
<table>
<thead>
<tr>
<th>SETTING</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Realtime Master Boot Record (MBR) Scanning</td>
<td>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. This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Enable Enhanced Rootkit Detection</td>
<td>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. This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Enable &quot;right-click&quot; scanning in Windows Explorer</td>
<td>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. This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>SETTING</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>---------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Update the currently scanned folder immediately as scanned | Displays a full list of files as SecureAnywhere scans each one.  
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 display each one on the screen.  
This setting applies only to PC endpoints.            |
| 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.  
This setting applies only to PC endpoints.            |
| 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.  
This setting applies only to PC endpoints.            |
| 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.  
This setting applies only to PC endpoints.            |
<table>
<thead>
<tr>
<th>SETTING</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| **Show the "Authenticating Files" popup when a new file is scanned on-execution** | Displays 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.  
This setting applies only to PC endpoints.                                                                 |
| **Scan archived files**                                                 | Scans compressed files in zip, rar, cab, and 7-zip archives.  
This setting applies to both PC and Mac endpoints.                                                                                                    |
| **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.  
This setting applies only to PC endpoints.                                                                                                         |
| **Never reboot during malware cleanup**                                | Prevents the endpoint from restarting during cleanup, which is the process of removing all traces of a malware file.  
This setting applies only to PC endpoints.                                                                                                         |
| **Automatically remove threats found during background scans**          | Removes threats during scans that run in the endpoint's background and sends them to quarantine.  
This setting applies only to PC endpoints.                                                                                                         |
<table>
<thead>
<tr>
<th>SETTING</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| Automatically remove threats found on the learning scan | Removes threats during the first scan on the endpoint and sends them to quarantine.  
This setting applies only to PC endpoints. |
| Enable Enhanced Support                    | Allows logs to be sent to Webroot customer support.  
This setting applies only to PC endpoints. |
| Show Infected Scan Results                 | Displays scan results. If not enabled, the endpoint does not display scan results even if malware is detected.  
This setting applies only to PC endpoints. |
### Setting Description

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Detect Possibly Unwanted Applications (PUAs) as malicious** | Detects PUAs and blocks them from installing.  
Potentially unwanted applications (PUAs) are programs that aren't necessarily malicious but contain adware, toolbars, or other unwanted additions to your system. Generally, PUAs are not malicious but may be unsuitable for use in a business environment, and may create security concerns.  
If a PUA is already on the system Webroot SecureAnywhere will detect the main program but may not be able to fully remove all aspects of it.  
This setting applies only to PC endpoints. |
| **Allow files to be submitted for threat research** | Allows potentially malicious files that our systems have not yet classified to be automatically uploaded to Webroot.  
This setting applies only to PC endpoints. |

### Self Protection Settings

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.
### Setting Description

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable self-protection response cloaking</td>
<td>Turns self-protection on and off. This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Self-protection level</td>
<td>Sets the detection level to:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Minimum</strong> — Protects the integrity of the SecureAnywhere settings and databases. Recommended if the endpoint has several other security products installed.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Medium</strong> — Prevents other programs from disabling protection. Provides maximum possible compatibility with other security software.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Maximum</strong> — Provides the highest protection of the SecureAnywhere processes. We recommend that you use this setting.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
</tbody>
</table>

### 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.

You can adjust these types of heuristics for several areas:

- **Local Heuristics** — Local drive
- **USB Heuristics** — USB drives
- **Internet Heuristics** — Internet
- **Network Heuristics** — Network
- **CD/DVD Heuristics** — CD/DVDs
- **Offline Heuristics** — 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. Keep in mind that this setting may result in false detections.
<table>
<thead>
<tr>
<th>SETTING</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Advanced Heuristics</strong></td>
<td>Analyzes new programs for suspicious actions that are typical of malware.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong> — Turns off Advanced Heuristics, leaving it vulnerable to new threats; however, it will still be protected against known threats.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Low</strong> — Detects programs with a high level of malicious activity. This setting ignores some suspicious behavior and allows most programs to run.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Medium</strong> — Balances detection versus false alarms by using our tuned heuristics in the centralized community database.</td>
</tr>
<tr>
<td></td>
<td>• <strong>High</strong> — 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.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Maximum</strong> — 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.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>SETTING</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| 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.  
|             |  
|             | - **Disabled** — Turns off Age Heuristics, leaving it vulnerable to new threats; however, it will still be protected against known threats.  
|             | - **Low** — Detects programs that have been created or modified very recently.  
|             | - **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.  
|             | - **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.  
|             | - **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.  
|             | This setting applies only to PC endpoints.                                                            |
## SETTING

<table>
<thead>
<tr>
<th>SETTING</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Popularity Heuristics</strong></td>
<td>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.</td>
</tr>
<tr>
<td>Low</td>
<td>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.</td>
</tr>
<tr>
<td>Medium</td>
<td>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.</td>
</tr>
<tr>
<td>High</td>
<td>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.</td>
</tr>
<tr>
<td>Maximum</td>
<td>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.</td>
</tr>
</tbody>
</table>

This setting applies only to PC endpoints.

---

## Realtime Shield Settings

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.
<table>
<thead>
<tr>
<th>SETTING</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| **Realtime Shield Enabled**                                   | Turns the Realtime shield on and off.  
This setting applies to both PC and Mac endpoints.                                                                                       |
| **Enable Predictive Offline Protection from the central SecureAnywhere 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.  
This setting applies only to PC endpoints.                                                                                          |
| **Remember actions on blocked files**                        | Remembers how the user responded to an alert, whether they allowed a file or blocked it, and will not prompt again when it encounters the same file.  
If this setting is deselected, SecureAnywhere displays an alert every time it encounters the file in the future.  
This setting applies only to PC endpoints.                                                                                          |
| **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.  
This setting applies to both PC and Mac endpoints.                                                                                   |
<table>
<thead>
<tr>
<th>SETTING</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatically block files when detected on execution</td>
<td>Blocks threats and sends them to quarantine.</td>
</tr>
<tr>
<td></td>
<td>If this setting is off, the user must respond to alerts about detected threats.</td>
</tr>
<tr>
<td></td>
<td>This setting applies to both PC and Mac endpoints.</td>
</tr>
<tr>
<td>Scan files when written or modified</td>
<td>Scans any new or modified files that are saved to disk.</td>
</tr>
<tr>
<td></td>
<td>If this setting is off, it ignores new file installations; however, it still alerts the user if a threat tries to launch.</td>
</tr>
<tr>
<td></td>
<td>This setting applies to both PC and Mac endpoints.</td>
</tr>
<tr>
<td>Block threats automatically if no user is logged in</td>
<td>Stops threats from executing even when managed endpoints are logged off. Threats are sent to quarantine without notification.</td>
</tr>
<tr>
<td></td>
<td>This setting applies to both PC and Mac endpoints.</td>
</tr>
<tr>
<td>Show realtime event warnings</td>
<td>Opens an alert when suspicious activity occurs.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>SETTING</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>--------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Show realtime block modal alerts</strong></td>
<td>Displays alerts when Heuristics detects malware, and prompts the user to allow or block the action.</td>
</tr>
<tr>
<td></td>
<td>If Heuristics is set to Warn when new programs execute that are not known good, then this setting must be set to On. Otherwise, users will not see the alert.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td><strong>Show realtime block notifications</strong></td>
<td>Displays 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 displays that threats were detected.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
</tbody>
</table>

**Behavior Shield Settings**

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.
<table>
<thead>
<tr>
<th>SETTING</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Behavior Shield Enabled</td>
<td>Turns the Behavior shield on and off.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Assess the intent of new programs before allowing them to execute</td>
<td>Watches the program's activity before allowing it to run. If it displays okay, SecureAnywhere allows it to launch and continues to monitor its activity.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Enable advanced behavior interpretation to identify complex threats</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Track the behavior of untrusted programs for advanced threat removal</td>
<td>Watches programs that have not yet been classified as legitimate or as malware.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>SETTING</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Automatically perform the recommended action instead of showing warning messages</td>
<td>Does not prompt the user to allow or block a potential threat. SecureAnywhere determines how to manage the item.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Warn if untrusted programs attempt low-level system modifications when offline</td>
<td>Displays 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.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
</tbody>
</table>

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.
<table>
<thead>
<tr>
<th>SETTING</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Core System Shield Enabled</td>
<td>Turns the Core System shield on and off.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Assess system modifications before they are</td>
<td>Intercepts any activity that attempts to make system changes on your managed endpoints, such as a new service installation.</td>
</tr>
<tr>
<td>allowed to take place</td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Detect and repair broken system components</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Prevent untrusted programs from modifying kernel</td>
<td>Stops unclassified programs from changing the kernel memory.</td>
</tr>
<tr>
<td>memory</td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Prevent untrusted programs from modifying system</td>
<td>Stops unclassified programs from changing system processes.</td>
</tr>
<tr>
<td>processes</td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>SETTING</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Verify the integrity of the LSP chain and other system structures</td>
<td>Monitors the Layered Service Provider (LSP) chain and other system structures to make sure malware does not corrupt them.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Prevent any program from modifying the HOSTS file</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>This setting applies to both PC and Mac endpoints.</td>
</tr>
</tbody>
</table>

**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, indicated by a green checkmark, or a potential risk, indicated by a red X.
<table>
<thead>
<tr>
<th>SETTING</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Web Shield</td>
<td>Turns the Web Threat shield on and off.</td>
</tr>
<tr>
<td></td>
<td>This setting is turned On by default, which is the setting we recommend.</td>
</tr>
<tr>
<td></td>
<td>This setting applies to both PC and Mac endpoints.</td>
</tr>
<tr>
<td>Activate browser extensions</td>
<td>Browser extensions provide blocking protection against malicious websites, realtime anti-phishing protection, and safety ratings when using search engines. Each function can be enabled or disabled separately using the individual controls for each function described in this table.</td>
</tr>
<tr>
<td></td>
<td>To completely disable and remove extensions from each supported browser, change the setting to Off.</td>
</tr>
<tr>
<td></td>
<td>This setting is turned On by default, which is the setting we recommend.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Block malicious websites</td>
<td>Any URLs and IPs you enter in a browser are checked and a block page displays for known malicious sites.</td>
</tr>
<tr>
<td></td>
<td>This setting is turned On by default, which is the setting we recommend.</td>
</tr>
<tr>
<td></td>
<td>This setting applies to both PC and Mac endpoints.</td>
</tr>
<tr>
<td>SETTING</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Enable real-time anti-phising   | Protects against zero-day phishing sites. Zero-day phishing sites are sites that have never been seen before, and their related viruses do not yet have a definition.  
This setting is turned On by default, which is the setting we recommend.  
This setting applies to both PC and Mac endpoints. |
| Show safety ratings when using search engines | Search result are annotated with an icon and tooltip, indicating the likelihood that a site is malicious.  
This setting is turned On by default, which is the setting we recommend.  
This setting applies to both PC and Mac endpoints. |
| Enable web filtering driver     | Provides additional protection against malicious connections, and in cases where the browser extensions are disabled.  
This setting is turned On by default, which is the setting we recommend.  
This setting applies only to PC endpoints. |
### 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.

<table>
<thead>
<tr>
<th>SETTING</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Suppress the user's ability to bypass blocked websites</td>
<td>Prevents users from bypassing the block page presented when a malicious website is detected. This setting is turned On by default, which is the setting we recommend.</td>
</tr>
<tr>
<td></td>
<td>This setting applies to both PC and Mac endpoints.</td>
</tr>
<tr>
<td>Suppress the user's ability to request website reviews</td>
<td>Prevents users from submitting website reviews from the block page when a malicious website is detected.</td>
</tr>
<tr>
<td></td>
<td>This setting is turned On by default, which is the setting we recommend.</td>
</tr>
<tr>
<td></td>
<td>This setting applies to both PC and Mac endpoints.</td>
</tr>
<tr>
<td>SETTING</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>----------------------------------------------------------</td>
</tr>
<tr>
<td>Identity Shield Enabled</td>
<td>Turns the Identity shield on and off.</td>
</tr>
<tr>
<td></td>
<td>This setting applies to both PC and Mac endpoints.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> On Mac, this controls the Secure Keyboard Entry Mode setting.</td>
</tr>
<tr>
<td>Look for identity threats online</td>
<td>Analyzes websites as users browse the Internet or open links. If the shield detects malicious content, it blocks the site and opens an alert.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Verify websites when visited to determine legitimacy</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Verify the DNS/IP resolution of websites to detect Man-in-the-Middle attacks</td>
<td>Looks for servers that could be redirecting users to a malicious website, such as a man-in-the-middle attack. If the shield detects a man-in-the-middle attack, it blocks the threat and opens an alert.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>SETTING</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>--------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Block websites from creating high risk tracking information</td>
<td>Blocks third-party cookies from installing on your managed endpoints if the cookies originate from malicious tracking websites.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Prevent programs from accessing protected credentials</td>
<td>Blocks programs from accessing login credentials, for example, when you type your name and password or when you request a website to remember them.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Warn before blocking untrusted programs from accessing protected data</td>
<td>Opens an alert any time malware attempts to access data, instead of blocking known malware automatically.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Allow trusted screen capture programs access to protected screen contents</td>
<td>Allows screen capture programs, no matter what content is displayed on the screen.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>SETTING</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>-------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Enable Identity Shield compatibility mode</td>
<td>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. This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Enable keylogging protection in non-Latin systems</td>
<td>Allows endpoints with non-Latin systems, such as Japanese and Chinese, to be protected from keyloggers.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
</tbody>
</table>

**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.
<table>
<thead>
<tr>
<th>SETTING</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| **Enabled** | Turns the Firewall on and off.  
This setting applies only to PC endpoints |
| **Firewall level** | - **Default Allow** — Allows all processes to connect to the Internet, unless explicitly blocked.  
- **Warn unknown and infected** — Warns if any new, untrusted processes connect to the Internet, if the endpoint is infected.  
- **Warn unknown** — Warns if a new, untrusted process connects to the Internet.  
- **Default Block** — Warns if any process connects to the Internet, unless explicitly blocked.  
This setting applies only to PC endpoints |
## SETTING | DESCRIPTION
--- | ---
**Show firewall management warnings** | Controls the alert displayed by SecureAnywhere when the Windows firewall is off:
- **On** — The user sees an alert when SecureAnywhere detects that the Windows firewall is off.
- **Off** — No alert displays when the Windows firewall is off.

This setting applies only to PC endpoints

**Show firewall process warnings** | Controls the firewall alerts. If this is setting is Off, no firewall alerts display. 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 displays to the endpoint user and the process is allowed.

This setting applies only to PC endpoints

### User Interface
Gives administrative control over the SecureAnywhere interface on the endpoints using this policy.
**Setting** | **Description**
---|---
GUI | 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. This setting applies to both PC and Mac endpoints.

**Note:** This option does not also hide the Webroot system tray icon on a PC. However, this option does hide the icon on a Mac.

**System Optimizer**

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

**Note:** Optimization removes unnecessary files and traces, not malware threats. Malware is removed during scans. You can think of System Optimizer as the housekeeper for a computer, while the Scanner serves as the security guard.
<table>
<thead>
<tr>
<th>SETTING</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage System Optimizer centrally</td>
<td>Enables the administrator to change System Optimizer settings, as follows:</td>
</tr>
<tr>
<td></td>
<td>• <strong>On</strong> — System Optimizer settings are displayed in the panel and are available to change.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Off</strong> — No settings displays in this panel.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Schedule</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Monday Through Sunday</td>
<td>Sets the days of the week, anything from one to seven, to automatically run System Optimizer.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Run at specific time of day - hour</td>
<td>Sets the hour of the day System Optimizer runs on the endpoints.</td>
</tr>
<tr>
<td>Run at specific time of day - minute</td>
<td>Sets the time in 15-minute increments that System Optimizer runs on the endpoints.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>SETTING</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Run on bootup if the system was off at the scheduled time</td>
<td>Launches a missed scheduled cleanup when the endpoint powers on. This is applicable only if the endpoint was off during a scheduled cleanup. Otherwise, skips the missed cleanup. This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Enable Windows Explorer right click secure file erasing</td>
<td>Includes an option for permanently erasing a file or folder in Windows Explorer on the endpoint. A menu item displays when the user right-clicks on a file or folder. This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Windows Desktop</td>
<td></td>
</tr>
<tr>
<td>Recycle Bin</td>
<td>Removes all files from the Recycle Bin in Windows Explorer. This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>SETTING</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>--------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Recent document history</td>
<td>Clears the history of recently opened files, which is accessible from the Windows Start menu. The cleanup does not delete the actual files. This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Start Menu click history</td>
<td>Clears the history of shortcuts to programs that end users recently opened using the Start menu. This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Run history</td>
<td>Clears the history of commands recently entered into the Run dialog, which is accessible from the Start menu. After the cleanup, the end user may need to restart the computer to completely remove items from the Run dialog. This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Search history</td>
<td>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. This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>SETTING</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Start Menu order history</strong></td>
<td>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. This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td><strong>Clipboard contents</strong></td>
<td>Clears the contents from the Clipboard, where Windows stores data used in either the Copy or Cut function from any Windows program. This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td><strong>Windows Temporary folder</strong></td>
<td>Deletes all files and folders in the Windows temporary folder, but not files that are in use by an open program. This folder is typically: C:\Windows\Temp. This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>SETTING</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| **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 typically in: C:\Documents and Settings\[username]\Local Settings\Temp.  
This setting applies only to PC endpoints. |
| **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 typically in C:\Windows\Software\Distribution\Download.  
This setting applies only to PC endpoints. |
| **Windows Registry Streams**  | Clears the history of recent changes made to the Windows registry.  
This option does not delete the registry changes themselves.  
This setting applies only to PC endpoints. |
| **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.  
This setting applies only to PC endpoints. |
<table>
<thead>
<tr>
<th>SETTING</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory dump files</td>
<td>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. This setting applies only to PC endpoints.</td>
</tr>
</tbody>
</table>
| 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  

This setting applies only to PC endpoints. |
| 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.  

This setting applies only to PC endpoints. |
<p>| Internet Explorer   | |</p>
<table>
<thead>
<tr>
<th>SETTING</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Address bar history</strong></td>
<td>Removes the list of recently visited websites, which is stored as part of</td>
</tr>
<tr>
<td></td>
<td>Internet Explorer’s AutoComplete feature.</td>
</tr>
<tr>
<td></td>
<td>This list can be seen from the Address drop-down menu at the top of the</td>
</tr>
<tr>
<td></td>
<td>Internet Explorer browser.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td><strong>Cookies</strong></td>
<td>Deletes all cookies from the endpoint. Be aware that if you remove all</td>
</tr>
<tr>
<td></td>
<td>cookie files, the end user must re-enter passwords, shopping cart items,</td>
</tr>
<tr>
<td></td>
<td>and other entries that these cookies stored.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td><strong>Temporary Internet</strong></td>
<td>Deletes copies of stored web pages that the end user visited recently.</td>
</tr>
<tr>
<td>Files</td>
<td>This cache improves performance by helping web pages open faster, but can</td>
</tr>
<tr>
<td></td>
<td>consume a lot of space on the hard drive.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td><strong>URL history</strong></td>
<td>Deletes the History list of recently visited websites of the Internet</td>
</tr>
<tr>
<td></td>
<td>Explorer toolbar.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>SETTING</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Setup Log</td>
<td>Deletes log files created during Internet Explorer updates.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Microsoft Download Folder</td>
<td>Deletes the contents in the folder that stores files last downloaded using</td>
</tr>
<tr>
<td></td>
<td>Internet Explorer.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>MediaPlayer Bar History</td>
<td>Removes the list of audio and video files recently opened with the media</td>
</tr>
<tr>
<td></td>
<td>player in Internet Explorer. The cleanup does not delete the files</td>
</tr>
<tr>
<td></td>
<td>themselves.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Autocomplete form information</td>
<td>Deletes data that Internet Explorer stores when the end user entered</td>
</tr>
<tr>
<td></td>
<td>information into fields on websites.</td>
</tr>
<tr>
<td></td>
<td>This is part of Internet Explorer’s AutoComplete feature.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>SETTING</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| **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. Index.dat functions like an active database. It is only cleaned after you reboot Windows.  
This setting applies only to PC endpoints. |
| **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.  
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.  
This setting applies only to PC endpoints. |

*Webroot Endpoint Protection Admin Guide*
Viewing Endpoints Assigned to Policies

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

To view endpoints assigned to a policy:

1. Log in to your Endpoint Protection console.

   The Endpoint Protection console displays, with the Status tab active.
2. Click the **Policies** tab.

The Policies tab displays.
3. From the Policy Name column, select the policy you want to view endpoint information for.

The Groups and endpoints area displays the groups that use the selected policy.
To view information about the endpoints, do either of the following:

- From the Command bar, click **View all endpoints using this policy**.

- Select the **View** link in the row for the group.

The All endpoints using Recommended Defaults window displays.
5. As needed, click any column header and do either or both of the following:
   - Select one of the following to sort that column in a different order:
     - Sort Ascending
     - Sort Descending
- Select **Columns**, and do one of the following:
  - Select a checkbox to display that column.
  - Deselect a checkbox to hide that column.

For more information about the data in the columns, see *Sorting Data in Tables and Reports on page 44.*
Moving Endpoints Between Policies

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

**Note:** To move an individual endpoint to a policy, see *Applying Policies to Endpoint Groups on page 316.*

To move endpoints between policies:

1. Log in to your Endpoint Protection console.

The Endpoint Protection console displays, with the Status tab active.
2. Click the **Policies** tab.

The Policies tab displays.
3. From the Policy Name column, select the policy you want to move.

The bottom panel lists which groups use this policy.
4. Click the **Move all endpoints on this policy to another policy** button.

![Image of the Move all endpoints on this policy to another policy window]

The Move all endpoints to another policy window displays.

![Image of the Move all endpoints to another policy window]

5. From the **Policy** drop-down menu, select from a list of policies the policy where you want to move the endpoints to.
The Policy field reflects the policy you have selected.

6. Click the Save button.

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

For more information, see Viewing Endpoints Assigned to Policies on page 293.
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. Log in to your Endpoint Protection console.

   The Endpoint Protection console displays, with the Status tab active.
2. Click the **Policies** tab.

The Policies tab displays.
3. From the Policy Name column, select the policy you want to delete.

The Delete button becomes active.
4. Click the **Delete** button.

The system displays the Delete Policy window.

5. Click the **Yes** button.
The Replacement Policy window displays.

6. From the Policy drop-down menu, select a new policy to associate with any group or endpoint that the prior policy was associated with.

7. Click the **Save** button
The deleted policy is moved to a Deleted Policies list.

8. To view any deleted policies, select the Show Deleted Policies checkbox in the upper right corner of the Policies tab.

The Deleted policies display in gray.
Chapter 7: Managing Groups

To manage groups, see the following topics:

- Adding New Groups .......................................................... 311
- Renaming Groups ............................................................. 313
- Applying Policies to Endpoint Groups ................................... 316
  - Applying Policies to a Group of Endpoints .......................... 316
  - Applying Policies to a Single Endpoint ............................... 317
- Moving Endpoints Between Groups ...................................... 320
- Organizing Endpoints Into Groups ...................................... 322
- Using the Activity Directory Tab in Views ............................. 324
- Using the IP Range Tab in Views ......................................... 326
- Using the Workgroup Tab in Views ..................................... 328
- Deleting Groups ............................................................. 330
Adding New Groups

When you first deploy SecureAnywhere to endpoints, Endpoint Protection assigns them all to the Default group. If needed, 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. From the Command bar, click the Create icon.
3. In the Create Group window that displays, enter a group name and description, then click the Create Group button.

The new group displays 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.

   Note: You can select all endpoints within the selected group by clicking the Hostname checkbox at the top of the list.

6. From the Command bar, click the Move endpoints to another group button.

   The Move endpoints to which group? window displays.

7. From the Group drop-down menu, select your new group and click the Save button.

8. You can now apply policies to the entire group or to individual endpoints; for more information, see Applying Policies to Endpoint Groups on page 316.
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. From the Endpoint console, click the **Group Management** tab.
2. From the left panel, select the group you want to rename.
3. From the Actions drop-down menu, select Edit Group.

The Edit Group window displays.
4. In the Group Name field, enter a new name for the group.
5. When you're done, click the Save button.
Applying Policies 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 then follow the instructions below to apply that policy to a group. For more information, see *Implementing Policies on page 215.*

This topic contains the following procedures:

- Applying Policies to a Group of Endpoints
- Applying Policies to a Single Endpoint

Applying Policies to a Group of Endpoints

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 endpoints you want.
3. From the Endpoints panel on the right, select one or more endpoints.

**Note:** You can select all endpoints within the selected group by clicking the Hostname checkbox at the top of the list.
4. From the Command bar, click the **Apply policy to endpoints** button.

   **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.

The Apply Policy window displays.

5. From the Policy drop-down menu, select the new policy for the group, and click the **Apply** button.

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

   **Applying Policies to a Single Endpoint**

   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 endpoint.
3. From the Endpoints panel on the right, select the endpoint.

![Image of Webroot Endpoint Protection Admin Guide](image)

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

![Image of Webroot Endpoint Protection Admin Guide](image)

5. Select the policy and press the **Enter** key.

The new policy name displays in the upper left corner, in the column with a red flag. 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 needed, you can continue making other changes in this panel until you are ready to save the changes.
6. To apply the change, click the **Save Changes** button.

The system removes the red flag from the row.
Moving Endpoints Between Groups

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 between groups 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.
   
   **Note:** You can select all endpoints within the selected group by selecting the Hostname checkbox at the top of the list.

4. From the Command bar, click the Move endpoints to another group icon.
   
   **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.

The Move endpoints to which groups? window displays.
5. From the Group drop-down arrow, select the group and click the **Save** button.

6. Click the group you selected from the left panel. Make sure all the endpoints are displayed in the Endpoints panel on the right.
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. For more information, see Setting Console User Permissions on page 74.

To organize endpoints into groups:

1. You can view all groups in the Group Management tab.
2. 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 displayed on the top; policies are displayed on the bottom.
Note: All endpoints are assigned to the Default group, unless you used the /groupname switch in the command line during a silent installation. For more information, see Deploying SecureAnywhere to Endpoints on page 110.

To create more groups and move endpoints, do any of the following:

1. Add one or more new groups, as described in Adding New Groups on page 311.
2. Move endpoints to the newly created groups, as described in Moving Endpoints Between Groups on page 320.
3. Assign a policy to the new group of endpoints, as described in Applying Policies to Endpoint Groups on page 316.
Using the Activity Directory Tab in Views

When you install SecureAnywhere on endpoints, the agent runs an initial scan to report the endpoint status and gather information to identify it in the Management Portal. Once these endpoints report back to the Management Console, you can then view the data collected by the agent in the Views tab under Group Management.

For more information, see Using the IP Range Tab in Views on page 326 and Using the Workgroup Tab in Views on page 328.

To view the Active Directory lists in the Management Portal:

1. Click the Group Management tab.
2. On the left, click the Views tab, then click the Active Directory tab.
3. From here you can view your endpoints by their Active Directory. For more information on descriptions of the data in the columns, see Sorting Data in Tables and Reports on page 44.

Note: The endpoints listed here cannot be moved as the organization is based on the data collected by the agent on its last scan. This information will change if the data is different on any subsequent scan.

4. You can also send commands and change the polices to the endpoints listed. You can only send these changes by individual endpoint or page, not by the entire view.
Note: You can select all endpoints on the page within the selected view by selecting the Hostname checkbox at the top of the list.

You cannot send commands or change the assigned policy to Groups from the Management tab; go the Groups tab instead. For more information, see Issuing Commands to Endpoints on page 140 and Applying Policies to Endpoint Groups on page 316.
Using the IP Range Tab in Views

When you install SecureAnywhere on endpoints, the agent runs an initial scan to report the endpoint status and gather information to identify it in the Management Portal. Once these endpoints report back to the Management Console, you can then view the data collected by the agent in the Views tab under Group Management.

For more information see Using the Activity Directory Tab in Views on page 324 and Using the Workgroup Tab in Views on page 328.

To view the IP Range lists in the Management Portal:

1. Click the Group Management tab.
2. On the left, click the Views tab, then click the IP Range tab.
3. From here you can view your endpoints by their IP Range. For more information on descriptions of the data in the columns, see Sorting Data in Tables and Reports on page 44.

Note: The endpoints listed here cannot be moved as the organization is based on the data collected by the agent on its last scan. This information will change if the data is different on any subsequent scan.

4. You can also send commands and change the polices to the endpoints listed. You can only send these changes by individual endpoint or page, not by the entire view.
Note: You can select all endpoints on the page within the selected view by selecting the Hostname checkbox at the top of the list.

You cannot send commands or change the assigned policy to Groups from the Management tab; go the Groups tab instead. For more information, see Issuing Commands to Endpoints on page 140 and Applying Policies to Endpoint Groups on page 316.
Using the Workgroup Tab in Views

When you install SecureAnywhere on endpoints, the agent runs an initial scan to report the endpoint status and gather information to identify it in the Management Portal. Once these endpoints report back to the Management Console, you can then view the data collected by the agent in the Views tab under Group Management.

For more information, see Using the IP Range Tab in Views on page 326 and Using the Workgroup Tab in Views.

To view the Workgroup lists in the Management Portal:

1. Click the Group Management tab.
2. On the left, click the Views tab, then click the Workgroup tab.
3. From here you can view your endpoints by their Workgroup. For more information on the data in the columns, see Sorting Data in Tables and Reports on page 44.

Note: The endpoints listed here cannot be moved as the organization is based on the data collected by the agent on its last scan. This information will change if the data is different on any subsequent scan.

4. You can also send commands and change the polices to the endpoints listed. You can only send these changes by individual endpoint or page, not by the entire view.
**Note:** You can select all endpoints on the page within the selected view by selecting the Hostname checkbox at the top of the list.

You cannot send commands or change the assigned policy to Groups from the Management tab; go the Groups tab instead. For more information, see *Issuing Commands to Endpoints on page 140* and *Applying Policies to Endpoint Groups on page 316.*
Dealing with 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. From the Group Name column, select the group you want to delete.
3. From the Command bar, click the Delete icon.
4. At the prompt, click the Yes button.

If endpoints are assigned to this group, another window displays and asks you to select a group where you want the endpoints moved.
5. Select the target group, then click the Save button.
Chapter 8: Working With Reports

To work with reports, see the following topics:

- Generating Endpoint Protection Reports ................................................................. 332
- Generating All Threats Seen Reports ...................................................................... 334
- Generating All Undetermined Software Seen Reports ............................................. 341
- Generating All URLs Blocked Reports ..................................................................... 348
- Generating Endpoints With Threats On Last Scan Reports ...................................... 353
- Generating Endpoints With Undetermined Software On Last Scan Reports ............. 357
- Generating Daily Threat History Reports ................................................................. 360
- Generating Collated Threat History Reports ......................................................... 368
- Generating Daily Blocked URL History Reports ..................................................... 377
- Generating Agent Version Spread Reports ............................................................ 381
- Generating Agents Installed Reports ....................................................................... 386
- Downloading Report Spreadsheets ......................................................................... 393
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.

<table>
<thead>
<tr>
<th>TO DO THIS...</th>
<th>USE THIS REPORT...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Locate endpoints with different SecureAnywhere versions installed</td>
<td>Generating Agent Version Spread Reports on page 381</td>
</tr>
<tr>
<td>Locate endpoints with newly installed SecureAnywhere software</td>
<td>Generating Agents Installed Reports on page 386</td>
</tr>
<tr>
<td>Locate and manage detected threats</td>
<td>Generating All Threats Seen Reports on page 334</td>
</tr>
<tr>
<td></td>
<td>or</td>
</tr>
<tr>
<td></td>
<td>Generating Endpoints With Threats On Last Scan Reports on page 353</td>
</tr>
<tr>
<td>Locate files classified as Undetermined</td>
<td>Generating All Undetermined Software Seen Reports on page 341</td>
</tr>
<tr>
<td></td>
<td>or</td>
</tr>
<tr>
<td></td>
<td>Generating Endpoints With Undetermined Software On Last Scan Reports on page 357</td>
</tr>
<tr>
<td>TO DO THIS...</td>
<td>USE THIS REPORT...</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>--------------------------------------------------------</td>
</tr>
<tr>
<td>View a summary of detected threats</td>
<td>Generating Collated Threat History Reports on page 368</td>
</tr>
<tr>
<td>View a summary of threats detected on a daily basis</td>
<td>Generating Daily Threat History Reports on page 360</td>
</tr>
</tbody>
</table>
Generating All Threats Seen Reports

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 display 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. From the Endpoint Protection console, click the **Reports** tab.

2. From the Report Type drop-down menu, select **All Threats Seen**.

3. If needed, select a specific policy and group. Otherwise, the report data displays all policies and groups, and may take a long time to generate, depending on your environment.
4. To enter a date range for the data, select the **Select time period** checkbox. This is an optional step.

5. To include deactivated and hidden endpoints in the report, select the **Include deactivated and hidden** checkbox. This is an optional step.
6. Click the **Submit** button.

The report opens in the right panel. Each threat is listed by its file name, along with where and when SecureAnywhere detected and removed it.
7. From this panel, do either of the following as needed:
   - **Create override** — To bypass Endpoint Protection and designate the file as Good (allow the file to run) or Bad (detect and quarantine the file), click the **Create override** icon in the command bar. For more information, see *Applying Overrides to Files From Reports*.
   - **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. To display or hide additional data for the report, click a column header to open the drop-down menu, then select the checkboxes to select the columns to add or remove. For more information, see *Sorting Data in Tables and Reports on page 44*.

9. To download a report spreadsheet, see *Downloading Report Spreadsheets on page 393*. 
Generating All Undetermined Software Seen Reports

SecureAnywhere may sometimes detect a file that displays legitimate, but also exhibits questionable behavior. In these cases, it classifies the file as Undetermined.

To locate files that SecureAnywhere classified as Undetermined, generate the All Undetermined Software Seen report. The All Undetermined Software Seen report displays all undetermined software, typically executable files, that SecureAnywhere cannot classify as either safe or as malware.

This report lists items by file name, along with when and where SecureAnywhere detected them. This report might display 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: For information on how to view the most recent endpoints with undetermined software, see Generating Endpoints With Threats On Last Scan Reports on page 353.

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. From the Endpoint Protection console, click the **Reports** tab.

2. From the Report Type drop-down menu, select **All Undetermined Software Seen**.

3. If needed, select a specific policy and group. Otherwise, the report data displays all policies and groups, and may take a long time to generate, depending on your environment.
4. To enter a date range for the data, select the Select time period checkbox. This is an optional step.

5. To include deactivated and hidden endpoints in the report, select the Include deactivated and hidden checkbox. This is an optional step.
6. Click the **Submit** button.

The report displays in the right pane.

7. Select a file and click the **Create override** button to reclassify it in one of the following ways:
   - **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. To display or hide additional data for the report, click a column header to display the drop-down menu, then select checkboxes to add, or remove columns. For more information, see *Sorting Data in Tables and Reports on page 44*.

9. To download a report spreadsheet, see *Downloading Report Spreadsheets on page 393*.
Generating All URLs Blocked Reports

To view all the URLs that have been blocked by Webroot’s SecureAnywhere Web Threat Shield, generate the All URLs Blocked Report. You can also generate this report to see which endpoints have visited sites that have been classed as Bad URLs and have been blocked.

You can modify the report data as follows:

- View all Blocked URLs within a selected group, which is helpful if you need to narrow search results to a specific set of endpoints.
- View all Blocked URLs within a selected Policy, so that you can see which Policy settings may need amending.

To generate the All URLs Blocked report:

1. From the Endpoint Protection console, click the Reports tab.
2. From the Report Type drop-down menu, select All URLs Blocked.
3. To include a specific time period or to include deactivated and hidden endpoints in the report, select the **Time Period** and **Include deactivated and hidden** checkboxes.

4. If you have selected a Time Period, enter the specific date that you want the report to be run against. This is an optional step.
**Note:** This report can now be un for any period up to 90 days.
5. When you’re done, click the **Submit** button to generate the report.

The report results display on the right side with the following information:

- URLs that have blocked
- Category of the block
- Reputation
- Hostname
- User action
- Date/Time of the block.
Generating Endpoints With Threats On Last Scan Reports

To locate and manage detected threats from the last scan, you can generate the Endpoints with Threats on Last Scan report. This report displays 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. From the Endpoint Protection console, click the Reports tab.
2. From the Report Type drop-down menu, select Endpoints with Threats on Last Scan.
3. To include deactivated and hidden endpoints in the report, select the Include deactivated and hidden checkbox. This is an optional step.
4. Click the **Submit** button.

The report displays in the right pane, with the following options:
- View and change the policy — To open the policy settings for that endpoint and change the settings, 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.

5. To view more details about threats found on an endpoint, click an item in the Hostname column. Details display in the bottom panel.

6. From the bottom panel, you can perform one of the following actions on a selected threat:
   - Create override — To bypass Endpoint Protection and designate the file as Good (allow the file to run) or Bad (detect and quarantine the file), from the command bar, click the Create override icon. For more information, see Applying Overrides To Files From Reports on page 444.
   - Restore from Quarantine — If the file is safe, to restore it to the original location on the endpoint, from the command bar, click the Restore from Quarantine icon.

7. To display or hide additional data for the report, click a column header to display the drop-down menu, then select the checkboxes to add or remove columns. For more information about the columns, see
Sorting Data in Tables and Reports on page 44.

For information on downloading a report spreadsheet, see Downloading Report Spreadsheets on page 393.
Generating Endpoints With Undetermined Software On Last Scan Reports

SecureAnywhere may sometimes detect a file that seems 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, 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. In the Endpoint Protection console, click the Reports tab.
2. From the Report Type drop-down menu, select Endpoint with undetermined software on last scan.

3. To include deactivated and hidden endpoints in the report, select the Include deactivated and hidden
checkbox. This is an optional step.

4. Click the **Submit** button.

The report displays in the right pane, displaying all the endpoints.
5. To view more details about the undetermined software found, click an endpoint's row to see details in the bottom.

6. 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.

7. To display or hide additional data for the report, click a column header to display the drop-down menu, then select checkboxes to add, or remove columns. For information on the columns, see *Sorting Data in Tables and Reports on page 44*.

   For information on how to download a report spreadsheet, see *Downloading Report Spreadsheets on page 393*. 
Generating Daily Threat History Reports

To view a summary of threats detected on a daily basis, you can generate the Threat History (Daily) report. This report displays 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. From the Endpoint Protection console, click the **Reports** tab.

2. From the Report Type drop-down menu, select **Threat History (Daily)**.

3. If needed, select a specific policy or group. If you do not select a policy or group, the report data displays all policies and groups, and, depending on your environment, may take a long time to generate.
4. In the Between and And fields, enter a start and end date for the report data.

5. To include deactivated and hidden endpoints in the report, select the **Include deactivated and hidden** checkbox. This is an optional step.
6. Click the **Submit** button.

The report displays in the right pane.
7. To view more details about threats, click on a bar to see details for a specific day.

The bottom panel displays details about the endpoints with the detected threats.
8. To view more information about a block program, in the Blocked Programs column, click a View link.

9. To display or hide additional data for the report, click a column header to display the drop-down menu, then select checkboxes to select, add, or remove columns. For more information about the descriptions of the data in the columns, see Sorting Data in Tables and Reports on page 44.
Generating Collated Threat History Reports

To view a summary of detected threats, you can generate the Threat History (Collated) report. This report displays 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 Daily Threat History Reports on page 360*. The Threat History (Daily) report provides 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. From the Endpoint Protection console, click the **Reports** tab.
2. From the Report Type drop-down menu, select **Threat History (Collated)**.

   ![Report Selection Screenshot]

3. If needed, select a specific policy or group. Otherwise, the report data displays all policies and groups, and may take a long time to generate, depending on your environment.
4. In the Between and And fields, enter a start and end date for the report data.

5. To include deactivated and hidden endpoints in the report, select the **Include deactivated and hidden** checkbox. This is an optional step.
6. Click the **Submit** button.

The report displays in the right pane.
7. 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 displays details about the programs.

8. 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.

![Endpoints which have seen this Program](image1)

The View link under All Versions displays this panel.

![All versions encountered of this program](image2)

9. 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.

![Endpoints with threats](image3)

10. Locate the row for the endpoint that has the blocked program and select the View link in the Blocked Programs column.

The following window displays.
11. In this window, you can do either of the following:
   - **Create override** — 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 more information, see *Applying Overrides To Files From Reports on page 444*.
   - **Restore from Quarantine** — If the file is safe, 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. To display or hide additional data for the report, click a column header to open the drop-down menu, then select checkboxes to add or remove columns. For more information about the descriptions of the data in the columns, see *Sorting Data in Tables and Reports on page 44*. 

---

- 376 -
Generating Daily Blocked URL History Reports

To view a history of the URLs that have been blocked by Webroot’s SecureAnywhere Web Threat Shield, generate the Block URLs History (Daily) Report.

To generate a Blocked URLs History (Daily) report:

1. From the Endpoint Protection console, click the Reports tab.
2. From the Report Type drop-down menu, select Block URLs History (Daily).
3. Do one of the following:
   - Select to view results from all policies and groups.
   - Select a specific policy or group to view Blocked URLs from.
4. Select the **Include deactivated and hidden** checkbox to display deactivated and hidden URLs that have been blocked. This is an optional step.
5. When you’re done, click **Submit** to generate the report.

The report results display on the right side with the following information:

- URLs that have blocked
- Category of the block
- Reputation
- Hostname
- User action
- Date/Time of the block
Generating Agent Version Spread Reports

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.

Use this report to locate endpoints that should be upgraded. The report displays a bar chart displaying 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, although this chart is less detailed than the Agent Version Spread report. For more information, see Viewing Agent Version Overviews on page 205.

To generate the Agent Version Spread report:
1. From the Endpoint Protection console, click the **Reports** tab.

2. From the Report Type drop-down menu, select **Agent Version Spread**.

3. To include deactivated and hidden endpoints in the report, select the **Include deactivated and hidden** checkbox. This is an optional step.
4. Click the Submit button.
A list of groups opens along with the Agent Version Spread report.

5. Do either or both of the following:
   - To view data for a specific group, click the group name on the left. The bar chart re-displays the data with only the selected group.
   - To view the endpoints using the version, click a bar to see details. The bottom panel displays data about each endpoint.
6. To display or hide additional data for the report, click a column header to display the drop-down menu, then select checkboxes to select, add, or remove columns.

For more information about the data in the columns, see *Sorting Data in Tables and Reports on page 44.*
Generating Agents Installed Reports

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 displaying 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. From the Endpoint Protection console, click the **Reports** tab.

2. From the Report Type drop-down menu, select **Agents Installed**.

3. If needed, select a specific policy or group.

   If you do not specify a policy or group, the report data displays all policies and groups, and may take a long time to generate, depending on your environment.
4. In the Between and And fields, enter a start and end date for the report data.

5. To include deactivated and hidden endpoints in the report, select the **Include deactivated and hidden** checkbox. This is an optional step.
6. Click the **Submit** button.

The report displays in the right pane.
7. 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.

8. To display or hide additional data for the report, click a column header to display the drop-down menu, then select checkboxes to select, add, or remove columns. For more information, see Sorting Data in Tables and Reports on page 44.
Chapter 8: Working With Reports

Downloading Report Spreadsheets

After you run a report, you might want a spreadsheet, or CSV file, that you can email or save. Follow this procedure to download a report spreadsheet, as needed.

The following reports support spreadsheet downloads:

- All Threats Seen
- All Undetermined Software Seen
- Endpoints With Threats on Last Scan
- Endpoints With Undetermined Software

To download a report spreadsheet:

1. After you've run the report, in the upper right corner of a report, click the CSV icon.

2. When the message displays at the bottom of the window, click the Open button.

The system displays a spreadsheet, which is populated with the data based on your report settings.
3. Sort and format the spreadsheet as needed, then save to your computer.
Chapter 9: Managing Alerts

To manage alerts, see the following topics:

- Implementing Alerts ................................................................. 396
- Creating Distribution Lists ...................................................... 397
- Creating Customized Alerts ..................................................... 399
- Viewing Defined Alert Messages ............................................. 410
- Suspending or Deleting Alerts ................................................ 412
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, such as 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. For information and instructions on changing access permissions, see [Setting Console User Permissions on page 74](#).

To implement an alert:

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. For more information, see [Creating Distribution Lists on page 397](#).
2. Create alert messages that are sent to the distribution list whenever endpoints report an infection or SecureAnywhere is installed on an endpoint. For more information, see [Creating Customized Alerts on page 399](#).

All your customized alerts display in the Alerts tab.

![Alerts Tab](image-url)
Creating Distribution Lists

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. For more information, see *Creating Customized Alerts on page 399.*

To create a distribution list:

1. Click the Alerts tab.
2. In the Distribution Lists column, from the Command bar, click Create.

The Create Distribution window displays

3. In the List Name field, enter a name for the list.
4. In the Email Addresses field, enter the email addresses of the recipients, with each address separated by a comma.
5. When you're done, click the **Save** button.

The new list is added to the Distribution Lists panel.

To delete the list later, highlight the name of the list and from the Command bar, click the **Delete** icon.
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 in this topic. You can also define a distribution list separately; for more information, see Creating Distribution Lists on page 397.

**To create a customized alert:**

1. From the main console, click the Alerts tab.

   ![Alerts Tab](image)

   The Alerts panel displays.
2. From the Command bar, click the Create icon.

The Create Alert window displays.
3. From the Alert Type drop-down menu, select an alert type.

4. In the Alert Name field, enter a name for this alert.

5. If you selected Threat Summary or Install Summary as the alert type, the Frequency field displays. Select a frequency to determine how often you want the system to send alerts.
   - Daily
   - Weekly
   - Monthly
6. Click the **Next** button.

The Step 2 window displays.

7. Select one of the following radio buttons to determine the list of recipients that you want to alert:
   - If you already created a distribution list, select the **Use existing list** radio button.
If you have not yet created a distribution list, select the **Create new list** radio button, enter a list name, then enter the email addresses.

8. When you're done, click the **Next** button.

   The Step 3 window displays.
9. In the Email title field, enter the subject head for the message.
10. In the Email message body field, enter the text for the message.

![Create Alert](image)

11. 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 displayed in brackets.

To add your own data inputs, click inside the text where you want a variable to display, then click the drop-down arrow for one of the Data Inputs buttons. There is one button for the email title and one for the email body.
12. Select from the data inputs, which are all described in the following table.

**Note:** Depending on the type of alert message you are defining, only the applicable data inputs display in the drop-down menu.
<table>
<thead>
<tr>
<th><strong>DATA INPUT</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>The name of the endpoint triggering the alert.</td>
</tr>
<tr>
<td>Group Name</td>
<td>The group assigned to the endpoint triggering the alert.</td>
</tr>
<tr>
<td>Group Description</td>
<td>A description of the group assigned to the endpoint triggering the alert.</td>
</tr>
<tr>
<td>Policy Name</td>
<td>The policy assigned to the endpoint triggering the alert.</td>
</tr>
<tr>
<td>Keycode</td>
<td>The keycode used for the endpoint triggering the alert.</td>
</tr>
<tr>
<td>Current User</td>
<td>The user of the endpoint triggering the alert.</td>
</tr>
<tr>
<td>Console Name</td>
<td>The name of the Console where the endpoint is included.</td>
</tr>
<tr>
<td>First Seen</td>
<td>The date and time when this event was first detected.</td>
</tr>
<tr>
<td>Last Seen</td>
<td>The date and time when this event was last detected.</td>
</tr>
<tr>
<td>Last Infected</td>
<td>The date and time the endpoint triggering the alert was last infected.</td>
</tr>
<tr>
<td>DATA INPUT</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Operating System</td>
<td>The operating system version on the endpoint triggering the alert.</td>
</tr>
<tr>
<td>Agent Version</td>
<td>The version number of the SecureAnywhere software installed on the endpoint triggering the alert.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>The Media Access Control (MAC) address on the network where the endpoint triggering the alert is installed.</td>
</tr>
<tr>
<td>Workgroup</td>
<td>The network workgroup where the endpoint is located, if any.</td>
</tr>
<tr>
<td>Active Directory</td>
<td>The name of the Active Directory.</td>
</tr>
<tr>
<td>Infection List</td>
<td>A list of infections.</td>
</tr>
<tr>
<td>Infection Summary</td>
<td>A summary of the infections.</td>
</tr>
<tr>
<td>Install Summary</td>
<td>A summary of the SecureAnywhere installations.</td>
</tr>
</tbody>
</table>

Note: Both the Workgroup and Active Directory data points are unsupported in the Mac agent.

13. To view the email message, click Preview.
14. When you are done creating the message, click Finish.
Viewing Defined Alert Messages

All your customized alerts are listed 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 needed, you can display or hide additional data about the alert messages.

To view a defined alert message:

1. Click a column header to open the drop-down menu, then do either of the following:
   - Select a checkbox to add a column.
   - Deselect a checkbox to remove a column.

The information in the columns is described in the following table.
## Column Description

<table>
<thead>
<tr>
<th>COLUMN</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert Name</td>
<td>The name defined in the Create Alert wizard. This column is static and cannot be hidden.</td>
</tr>
<tr>
<td>Alert Type</td>
<td>Displays one of the following alert types:</td>
</tr>
<tr>
<td></td>
<td>• Infection Detected</td>
</tr>
<tr>
<td></td>
<td>• Endpoint Installed</td>
</tr>
<tr>
<td></td>
<td>• Infection Summary</td>
</tr>
<tr>
<td></td>
<td>• Install Summary</td>
</tr>
<tr>
<td>Distribution List</td>
<td>The email recipients for this alert.</td>
</tr>
<tr>
<td>Date Created</td>
<td>The date the alert message was defined.</td>
</tr>
<tr>
<td>Created By</td>
<td>The administrator who created the alert message.</td>
</tr>
<tr>
<td>Date Edited</td>
<td>The date, if any, that the alert message was modified.</td>
</tr>
<tr>
<td>Edited By</td>
<td>The administrator who modified the alert message, if applicable.</td>
</tr>
<tr>
<td>Status</td>
<td>The alert status, which is either Active or Suspended.</td>
</tr>
</tbody>
</table>
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. From the Alert Name column, select an alert.
3. From the Command menu bar, click either the Delete or Suspend icon.

   ![Alerts tab with options](image)

   - If you selected Suspend, the alert is grayed out in the column, and Suspended displays in the Status column. Later, you can select the alert again and click Resume.
   - If you selected Delete, click Yes at the prompt. The alert is permanently removed from Endpoint Protection.
# Chapter 10: Using Overrides

To use overrides, see the following topics:

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Implementing Overrides</td>
<td>414</td>
</tr>
<tr>
<td>Creating Blacklist Overrides</td>
<td>416</td>
</tr>
<tr>
<td>Creating Whitelist Overrides</td>
<td>422</td>
</tr>
<tr>
<td>Applying Overrides From the Overrides Tab</td>
<td>429</td>
</tr>
<tr>
<td>Applying Overrides to Files From Groups</td>
<td>436</td>
</tr>
<tr>
<td>Applying Overrides To Files From Reports</td>
<td>444</td>
</tr>
<tr>
<td>Applying Overrides From Dwell Time Popups</td>
<td>449</td>
</tr>
<tr>
<td>Viewing Overrides</td>
<td>456</td>
</tr>
<tr>
<td>Exporting Overrides to Spreadsheets</td>
<td>461</td>
</tr>
<tr>
<td>Deleting Overrides</td>
<td>463</td>
</tr>
</tbody>
</table>
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.
- 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.

**Note:** To fully manage overrides, you must have access permissions for Overrides: MD5 and Overrides: Determination Capability. To change permissions, see [Setting Console User Permissions on page 74](#).

To change how a file is detected and managed, 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:

- **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 429](#).

- **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 436](#).

- **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 444.*

- **Dwell Time Popup** — You can create an override for an MD5 from within this popup.
  
  For more information, see *Applying Overrides From Dwell Time Popups on page 449.*
Creating Blacklist Overrides

You can create blacklist overrides in the Overrides panel in the Endpoint Protection console.

To create a blacklist override:

1. Log in to your Endpoint Protection console.

   The Endpoint Protection console displays, with the Status tab active.
2. Click the **Overrides** tab.

The system displays the Overrides panel, with the Whitelist tab active.

The system displays the Overrides panel, with the Whitelist tab active.
3. Click the **Blacklist** tab.

The system displays the Blacklist tab.
4. Click the **Create** button.

The system displays the Create override window.
5. In the Override Name field, enter a name for the override.

6. In the MD5 field, enter the 32-character unique identifier for the file.
7. Select either the **No** or **Yes Apply to Policy** radio button.

8. When you're done, click the **Save** button.
Creating Whitelist Overrides

Global whitelist overrides can now be set on a file or folder level as well as the traditional MD5 (Message-Digest algorithm 5) level in Endpoint Protection. This upgrade allows greater flexibility in the deployment of overrides and means that multiple related MD5 overrides no longer have to be whitelisted individually, instead the whole associated directory can simply be whitelisted.

**Note:** If you detect or remove a file before an exclusion or override is in place, you will need to uninstall then reinstall or ensure that the detected files are restored from quarantine. If the files are still located locally in the quarantine or block/allow tab, the exclusion does not work.

To create a whitelist override:

1. Log in to your [Endpoint Protection console](#).

   The Endpoint Protection console displays, with the Status tab active.

![Endpoint Protection Console](image)

Webroot Endpoint Protection Admin Guide
2. Click the **Overrides** tab.

3. The system displays the Overrides panel, with the Whitelist tab active.
4. Click the **Create** button.

The system displays the Create override window.
5. In the Override Name field, enter a name for the override.

6. Do one of the following:
   - If you're done, click the **Save** button.
   - To create a Folder/File override, continue with this procedure.

   **Note:** To use File/Folder overrides please make sure endpoints are running version 9.0.1 or higher of Webroot SecureAnywhere Endpoint Protection. Earlier versions support MD5 overrides only.

7. In the New Whitelist Entry window, select the **Path/File** radio button.

   The system displays the Create override window with the relevant fields.
8. Use the information in the following table to populate the fields.

<table>
<thead>
<tr>
<th>FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Override Name</td>
<td>Enter a name for the override.</td>
</tr>
<tr>
<td>Override Type</td>
<td>You have already selected the Path/File radio button.</td>
</tr>
<tr>
<td>File Mask</td>
<td>Target a file or group of files by specifying a file mask with optional wildcards, for example, *.exe to target all executable files in the selected folder. This will default to all files in the selected folder/path if not specified.</td>
</tr>
<tr>
<td>FIELD</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>-----------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Path/Folder Mask      | The folder to target with the override. You can specify an absolute path, for example, x:\myfolder\ or a system variable with optional path, for example, %SystemDrive%\myfolder.  
Default supported environment variables are displayed when you type % (percent)however you may choose to use any variable you have setup on the target machine with the exception of user variables which are not supported. You may not use %temp% for example as this refers to a specific users temp directory (‘username/temp’). Wildcards are not supported. |
| Include Sub-folders   | Select this checkbox to apply the override to all sub-folders within this folder.                                                             |
| Detect if Malicious   | If this setting is enabled Webroot will continue to protect the user against threats originating from the selected file/folder whitelist override but will disable monitoring and journaling. This is primarily used to improve performance when monitoring and journaling is being applied to a large number of files with an unknown determination. Disabling this setting will provide a true whitelisting, allowing files to run without Webroot protection. |
### FIELD | DESCRIPTION
--- | ---
Global (GSM) Override | Selecting this will make the Override global for every site under the current GSM Console.
Apply to Policy | Do either of the following:

- Select **Yes** to apply the Override to a specific policy, global policies included.
- Select **No** to apply to all policies on the selected site.

9. When you're done, click the **Save** button.
Applying Overrides From the Overrides Tab

When you apply 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.

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

This procedure has two parts:

- **Locating and Saving MD5 Values**
- **Adding MD5 Values**

**Note:** This procedure only be done on a Windows computer.

**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. For more information, see *Issuing Commands to Endpoints on page 140*.

2. On the endpoint, such as a PC or other device, open SecureAnywhere.
3. Click the **System Tools** tab.
4. In the left pane, select **Reports**.
5. In the Scan Log section of the page, click the Save as button and specify a name and location for the log.

6. Open the scan log and locate the MD5 value to the right of the filename.

The following example display the MD5 value for a file named csrss.exe.

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

To add an MD5 override from the Overrides tab:

1. Log in to your [Endpoint Protection console](#).

   The Endpoint Protection console displays, with the Status tab active.
2. Click the **Overrides** tab.

The Overrides tab displays, with the File & Folder Overrides tab active.
3. Click the Create icon.

The Create override window displays.
4. In the Override Name field, enter a name for the override.

5. In the Override Type area, select the **MD5** radio button.
6. In the MD5 field, paste the copied **MD5 value**

![Create override dialog box](image)

7. In the Apply to a policy area, do either of the following:
   - To not apply a policy, select the **No** radio button.

![Create override dialog box](image)

   - To apply the override to a single policy, select the **Yes** radio button. Then, from the Select a policy drop-down menu, select the policy you want to apply the override to.

![Create override dialog box](image)
Note: You can apply an override globally or you can apply it to a single policy; you cannot do both.

8. When you're done, click the Save button.

9. To test how SecureAnywhere will detect the file, send the endpoint a Reverify all files and processes command. For more information, see Issuing Commands to Endpoints on page 140.
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. Log in to your Endpoint Management console.

   The Endpoint Protection console displays, with the Status tab active.
2. Click the **Group Management** tab.

The Group Management tab displays, with the Groups tab active.
3. In the left pane, select the group for the endpoint where the file was detected.

A list of endpoints displays.
4. In the right pane, select the endpoint where the file was detected.

5. In the Scan History list at the bottom, do either of the following:
   - Click **View all threats seen on this endpoint**
   - Click **View** in the Status column for the date when the threat was detected.
6. In the dialog, select the checkbox for the filename you want to create an override for and click the Create override icon.

The Create override window displays.

7. From the Determination drop-down menu, select one of the following:
   - **Good** — Always allow the file to run.
   - **Bad** — Always send the file to quarantine.
8. In the Description field, enter a description for the override.

9. Apply the override in one of the following ways:
   - To apply the override to all policies, do not select the **Assign to a policy?** checkbox.
   - To apply the override to an individual policy, select the **Apply to a policy?** checkbox. When the Policy field displays, select a policy from the drop-down menu.
10. When you're done, click the **Save** button.

11. To test the file's detection, send the endpoint a Reverify all files and processes command. For more information, see *Issuing Commands to Endpoints on page 140*. 
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 the following reports:

- Generating All Threats Seen Reports on page 334
- Generating All Undetermined Software Seen Reports on page 341
- Generating Endpoints With Threats On Last Scan Reports on page 353, in the panel for Threats Seen on this Endpoint panel; individual endpoints only.
- Generating Endpoints With Undetermined Software On Last Scan Reports on page 357, in the panel for All Undetermined Software Seen on this Endpoint; individual endpoints only.

To apply an override from reports:

1. Log in to your Endpoint Protection console.
   
The Endpoint Protection console displays, with the Status tab active.
2. Click the **Reports** tab.

The Reports tab displays.
3. From the **Report Type** drop-down menu, select one of the reports listed above and click the **Submit** button to generate a report.

4. In the All Threats Seen area, select the filename and from the command bar, click the **Create override** icon.

The Create override window displays.
5. From the Determination drop-down menu, select one of the following:
   - **Good** — Always allow the file to run.
   - **Bad** — Always send the file to quarantine.

6. Apply the override in one of the following ways:
   - To apply the override to all policies, do not select the **Apply to a policy?** checkbox.
   - To select an individual policy for the override, deselect the **Apply to a policy?** checkbox. When the Policy field displays, from the Policy drop-down menu, select a policy.
7. When you're done, click the **Save** button.

8. To test the file's detection, send the endpoint a **Reverify all files and processes** command. For more information, see *Issuing Commands to Endpoints on page 140*. 
Applying Overrides From Dwell Time Popups

From a the dwell time popup, 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 a dwell time popup:

1. Log in to your Endpoint Protection console.

   The Endpoint Protection console displays, with the Status tab active.

2. In the 50 Most Recent Endpoints Encountering Threats area, for the item for which you want to create an override, click the View link.
The All Threats Ever Seen On This Endpoint window displays.

3. In the Filename column, select the link for the item for which you want to create an override.

The Dwelltime Popup window displays.
Chapter 10: Using Overrides

![Image of a computer interface showing propagation timeline, file information, and endpoints encountering the file.]

- SURIV.DLL WRDemoEP95

**Propagation Timeline**
- Jan 31 2012
- Jul 1 2012
- Nov 30 2012
- May 2 2013
- Oct 1 2013

**File Information**
- **Determination:** Bad
- **Malware Group:** Win32.Suric Test
- **Global Popularity:** 155
- **Console Popularity:** 3
- **Determined:** Oct 9 2014, 8:45
- **Filename:** SURIV.DLL
- **MD5:** DAA8E95610027DC3960C3196A19BD5EF

**Endpoints encountering this file**
- GAGPTEST11-13914952 Aug 12 2013, 17:35
- FHAL-3277-W7 Jan 6 2014, 7:26
- WRDemoEP95 Jun 3 2010, 5:09

**Endpoints**
- **First Sees**
  - Globally: Aug 31 2011, 14:05
  - Console: Oct 29 2012, 9:49
  - Endpoint: Dec 17 2013, 9:47
- **Last Seen**
  - Globally: -
  - Console: Jan 15 2015, 5:07
  - Endpoint: Jun 3 2015, 5:09
- **Dwell Time**
  - 552 days 20 hours 1 min 37 secs

[Powered by Dragroot]
4. Click the **Create Override** button.

The Create Override window displays.

5. From the Determination drop-down menu, select one of the following:
   - **Good** — Always allow the file to run.
   - **Bad** — Always send the file to quarantine.
6. In the Description field, enter information about the override.

7. Do one of the following to apply the override:
   - If you don't want to apply the override to a specific policy, do not select the Assign to a policy checkbox.
   - If you want to apply the override to a specific policy, select the Assign to a policy checkbox.

If you selected the checkbox, the Policy drop-down menu displays.
8. Select the policy you want to apply the override to.

**Note:** You can apply an override globally or you can apply it to a single policy; you cannot do both.
9. When you're done, click the **Save** button.

![Create override form]

10. To test how SecureAnywhere will detect the file, send the endpoint a **Reverify all files and processes** command. For more information, see *Issuing Commands to Endpoints on page 140.*
Viewing Overrides

After you add overrides to Endpoint Protection, you can view them in the Overrides tab.

To view an override:

1. Log in to your Endpoint Protection console.

   The Endpoint Protection console displays, with the Status tab active.
2. Click the **Overrides** tab.

The Overrides tab displays, with the File & Folder Overrides tab active.

3. Select a policy from the left panel to narrow the results displayed on the right.

Your selected overrides display in the Manual Determination column.
4. To display or hide additional data about the overrides, click a column header to open the drop-down menu, then select or deselect a checkbox to add or remove a column.

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

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. Log in to your Endpoint Protection console.

   The Endpoint Protection console displays, with the Status tab active.

   ![Endpoint Protection console with Status tab active]

2. In the Site console, click the Overrides tab.

3. To narrow the results in the right panel, select a specific policy from the left.

4. In the Command menu bar, click the Export to CSV icon.
5. 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.
Deleting Overrides

Use this procedure to delete either whitelist or blacklist overrides.

To delete an override:

1. Log in to your Endpoint Protection console.

The Endpoint Protection console displays, with the Status tab active.
2. From the Site console, click the **Overrides** tab.

![Image of the user interface showing the Overrides tab highlighted]

The system displays the Overrides panel, with the Whitelist tab active.
3. On either the Whitelist or the Blacklist tab, highlight the override that you want to delete.
The system displays the Delete button.

![Image of the Webroot SecureAnywhere interface with the Delete button highlighted.](image-url)
4. Click the **Delete** button.

The system displays the Delete Whitelist/Blacklist Entry confirmation window.

![Confirm Delete Window](image)
5. Click the **Yes** button.

The system deletes the override.
Chapter 11: Using Web Overrides

To use web overrides, see the following topics:

- Creating Web Overrides ................................................................. 470
- Creating Web Overrides From Group Management ........................... 475
- Creating Web Overrides From Reports ........................................... 484
- Editing Web Overrides .................................................................... 492
- Deleting Web Overrides .................................................................... 496
Creating Web Overrides

Follow this procedure to create web overrides from the Web Overrides tab.

To create a web override:

1. Log in to your Endpoint Protection console.

   The Endpoint Protection console displays, with the Status tab active.
2. Click the **Overrides** tab.

The Overrides tab displays, with the File & Folder Overrides tab active.
3. Click the **Web Overrides** tab.

![Web Overides tab](image)

The Web Overides tab displays.
4. Click the **Create** button.

![Web Override window](image1)

The Web Override window displays.

![Web Override](image2)

5. In the URL field, enter the URL for the website you want to create an override for.
6. When you're done, click the **Save** button.

The system creates the web override.
Creating Web Overrides From Group Management

Follow this procedure to create web overrides from the Group Management tab.

To create a web override from the Group Management tab:

1. Log in to your Endpoint Protection console.

   The Endpoint Protection console displays, with the Status tab active.
2. Click the **Group Management** tab.

The Group Management tab displays.
3. In the Group Name column, select All Endpoints.

In the All Endpoints area, all endpoints display.
### Chapter 11: Using Web Overrides

#### Webroot SecureAnywhere

**Groups**
- All Endpoints: 14
- Deactivated Endpoints: 78
- Default Group: 9
- Bracknell: 0
- Broomfield: 0
- Dublin: 0
- Mac OS X Systems: 0
- RemoteUS: 0
- Server: 0
- Servers: 0
- Sydney: 3
- Tokyo: 0
- TradeShow: 2
- Workstations: 0

**Policy**
- AB-WIN10-DEMO: Unmanaged
- TRADE3-7185-BRM: Unmanaged
- TRADE4-7184-RRM: Unmanaged
- WRDemoEP01: Demo Policy (Do Not Edit)
- WRDemoEP03: Demo Policy (Do Not Edit)
- WRDemoEP04: Demo Policy (Do Not Edit)
- WRDemoEP05: No Remediation
- WRDemoEP06: No Remediation
- WRDemoEP07: Standard Workstation Policy
- WRDemoEP11-W8-L: Standard Workstation Policy
- WRDemoEP14: No Remediation
- WRDemoEP15: Standard Workstation Policy
- WRDemoSVR31: Recommended Server Default

---

- 479 -
4. Select the endpoint that you want to create a web override for.
5. Click the **Blocked URLs** tab.

The **Blocked URLs** tab displays.

<table>
<thead>
<tr>
<th>URL</th>
<th>Category</th>
<th>Reputation</th>
<th>User Action</th>
<th>Date</th>
</tr>
</thead>
</table>
6. Select the URL that you want to create a web override for.

The Create Override icon becomes active.
7. Click the **Create Override** icon.

The Web Override window displays, with the URL you selected displayed in the URL field.

8. Click the **Save** button.

The URL is added to your Allow list.
Creating Web Overrides From Reports

Follow this procedure to create web overrides from the Reports tab.

To create a web override from the Reports tab:

1. Log in to your [Endpoint Protection console](#).

The Endpoint Protection console displays, with the Status tab active.
2. Click the **Reports** tab.

The Reports tab displays.
3. From the Report Type drop-down menu, select **All URLs Blocked**.
4. Click the **Submit** button.

In the All URLs Blocked area, a list of blocked URLs displays.
5. In the All URLs Blocked area, select the URL that you want to allow.

The Create override icon becomes active.
6. Click the **Create override** icon.

The Create Override window displays, with the URL that you have selected.
7. Click the **Save** button.

![Web Override dialog box with URL set to `ww1.see-password.com` and a highlighted `Save` button.]

The URL is added to your allow list.
Editing Web Overrides

Follow this procedure to edit a web override.

To edit a web override:

1. Log in to your [Endpoint Protection console](#).

   The Endpoint Protection console displays, with the Status tab active.
2. Click the **Overrides** tab.

The Overrides tab displays, with the File & Folder Overrides tab active.
3. Click the **Web Overrides** tab.

The Web Overrides tab displays.
4. From the Allow List, select the web override that you want to edit, and double-click.

The Web Override window displays.

5. Edit the web override, as needed.

6. When you're done, click the Save button.

The system saves your edits.
Deleting Web Overrides

Follow this procedure to delete web overrides.

To delete a web override:

1. Log in to your Endpoint Protection console.

   The Endpoint Protection console displays, with the Status tab active.
2. Click the **Overrides** tab.

The Overrides tab displays, with the File & Folder Overrides tab active.
3. Click the **Web Overrides** tab.

The Web Overrides tab displays.
4. In the Allow List area, select the web override that you want to delete.

The Delete icon becomes active.
5. Click the **Delete** icon.

A confirm message displays.

6. Click the **Yes** button.

The web override is deleted from the system.
Chapter 12: Managing Settings

To manage settings, see the following topic:

| Setting Data Filters | 502 |
Setting Data Filters

Within the Endpoint Protection management console, you can remove endpoints from your data which have not been seen for a set period of time giving you the most accurate data for the current state-of-play of your site.

Select to hide all endpoints from data sets which have not been seen for 1 month, 2 months, 3 months, 6 months, 12 months, or inherit GSM data filter setting if your EP console is managed under a GSM. You may also decide to display all data.

To set data filters:

1. Log in to the [Endpoint Protection console](#).

   The Endpoint Protection panel displays, with the Status tab active.
2. Click the **Settings** tab.

![Settings Panel](image)

The Settings panel displays.

![Data Filter](image)

3. From the Data Filter drop-down menu, select one of the following:
   - Hide all data for endpoints not seen for 1 month
   - Hide all data for endpoints not seen for 2 months
   - Hide all data for endpoints not seen for 3 months
   - Hide all data for endpoints not seen for 6 months
   - Hide all data for endpoints not seen for 12 months
   - Show all data; this is the default setting
   - Inherit the GSM data filter setting
4. Click the **Save** button.

The system displays a **Save Successful** message.

![Save Successful Message](image-url)
5. Click the **OK** button.

![Save Successful](image)

Your console data will now be updated, with endpoints and their associated data shown or hidden depending on your selection. Please note that dependent on deployment size, it may take a few minutes until all data has been filtered.

The system updates the setting and creates a log entry. For more information, see *Viewing Data Filter Logs on page 514.*
Chapter 13: Viewing Logs

To view logs, see the following topics:

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Viewing Change Logs</td>
<td>507</td>
</tr>
<tr>
<td>Viewing Command Logs</td>
<td>510</td>
</tr>
<tr>
<td>Viewing Data Filter Logs</td>
<td>514</td>
</tr>
</tbody>
</table>
Viewing Change Logs

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** — Any commands that were 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 a change log:**

1. From the Endpoint portal, click the **Logs** tab.

   The Change Log displays by default. It lists change events, and provides filters for narrowing the list.
2. Use the Filter Change Log options in the left pane to narrow the data. You can decide to filter the data, as follows:
   - **Between and And** — In these two fields, enter the time frame in the *mm/dd/yyyy* format, or by clicking the calendar icons to determine dates.
   - **Event Type** — From the drop-down list, select an event. Events include changes in groups, endpoints, or policies, as well as overrides and user logons.
   - **Involving User** — From the drop-down list, select a user.
   - **Involving Group** — From the drop-down list, select a group.
   - **Involving Policy** — From the drop-down list, select a policy.

3. When you have selected the filtering criteria, click **Submit**.

4. Do either or both of the following:
   - If the data exceeds 50 items, click the **Left** and **Right** arrows at the bottom to move between additional pages.
• Click the **Refresh** icon to update the data.
Viewing Command Logs

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 a command log:

1. From the Endpoint portal, click the **Logs** tab.

The Logs panel displays with the Change Log tab active.
### Change Log

<table>
<thead>
<tr>
<th>Date</th>
<th>Event Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jul 7th 2014, 08:30</td>
<td>Logon</td>
<td><a href="mailto:swilson@emailaddress.com">swilson@emailaddress.com</a> logged on</td>
</tr>
<tr>
<td>Jul 4th 2014, 06:25</td>
<td>Logon</td>
<td><a href="mailto:swilson@emailaddress.com">swilson@emailaddress.com</a> logged on</td>
</tr>
<tr>
<td>Jun 28th 2014, 10:30</td>
<td>Logon</td>
<td><a href="mailto:swilson@emailaddress.com">swilson@emailaddress.com</a> logged on</td>
</tr>
<tr>
<td>Jun 25th 2014, 05:15</td>
<td>Logon</td>
<td><a href="mailto:swilson@emailaddress.com">swilson@emailaddress.com</a> logged on</td>
</tr>
<tr>
<td>Jul 6th 2014, 23:48</td>
<td>Group</td>
<td><a href="mailto:swilson@emailaddress.com">swilson@emailaddress.com</a> deleted Marketing</td>
</tr>
<tr>
<td>Jul 11th 2014, 00:34</td>
<td>Group</td>
<td><a href="mailto:swilson@emailaddress.com">swilson@emailaddress.com</a> created Sales</td>
</tr>
<tr>
<td>Jul 8th 2014, 10:12</td>
<td>Policy</td>
<td><a href="mailto:swilson@emailaddress.com">swilson@emailaddress.com</a> created Recommended Server Defaults</td>
</tr>
<tr>
<td>Jul 10th 2014, 21:07</td>
<td>Policy</td>
<td><a href="mailto:swilson@emailaddress.com">swilson@emailaddress.com</a> created Recommended Defaults</td>
</tr>
<tr>
<td>Jun 30th 2014, 12:30</td>
<td>Logon</td>
<td><a href="mailto:jsmith@emailaddress.com">jsmith@emailaddress.com</a> logged on</td>
</tr>
<tr>
<td>Jul 16th 2014, 13:32</td>
<td>Override</td>
<td><a href="mailto:jsmith@emailaddress.com">jsmith@emailaddress.com</a> added Override MDS:a743d0b6ebba852e27567af1ec</td>
</tr>
<tr>
<td>Jun 28th 2014, 13:20</td>
<td>Endpoint</td>
<td><a href="mailto:djones@emailaddress.com">djones@emailaddress.com</a> moved NancyJackson_PC74 (Policy: Recommended)</td>
</tr>
<tr>
<td>Jul 12th 2014, 16:35</td>
<td>Endpoint</td>
<td><a href="mailto:djones@emailaddress.com">djones@emailaddress.com</a> moved ArthurVazquez_PC48 (Policy: Recommended)</td>
</tr>
<tr>
<td>Jun 24th 2014, 13:19</td>
<td>Override</td>
<td><a href="mailto:djones@emailaddress.com">djones@emailaddress.com</a> added Override MDS:a743d0b6ebba852e27567af1ec</td>
</tr>
</tbody>
</table>
2. Click the **Command Log** tab.

The Command Log panel displays.
3. If the data exceeds 50 items, use the navigation buttons at the bottom to move between pages.

4. To update data, click the **Refresh** icon.
Viewing Data Filter Logs

All changes made to the data filter setting are captured in the data filter log.

To view a data filter log:

1. Log in to the Endpoint Protection console.

The Endpoint Protection panel displays with the Status tab active.
2. Click the **Logs** tab.

The Logs panel displays with the Change Log tab active.
3. Click the **Data Filter Log** tab.

The Data Filter Log panel displays with the following information for each change that you made:

- **Setting** — The filter option that was selected.
- **User** — The name of the user who made the change.
- **Date** — The date the change was made.
<table>
<thead>
<tr>
<th>Setting</th>
<th>User</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Hide all data for endpoints not seen for more than 6 months</td>
<td><a href="mailto:JaneDoe@webroot.com">JaneDoe@webroot.com</a></td>
<td>Nov 11th 2015, 13:36</td>
</tr>
<tr>
<td>2 Hide all data for endpoints not seen for more than 3 months</td>
<td><a href="mailto:JaneDoe@webroot.com">JaneDoe@webroot.com</a></td>
<td>Nov 11th 2015, 12:44</td>
</tr>
<tr>
<td>3 Hide all data for endpoints not seen for more than 1 month</td>
<td><a href="mailto:JaneDoe@webroot.com">JaneDoe@webroot.com</a></td>
<td>Nov 11th 2015, 10:34</td>
</tr>
<tr>
<td>4 Inhibit the CSM data filter setting</td>
<td><a href="mailto:JaneDoe@webroot.com">JaneDoe@webroot.com</a></td>
<td>Nov 11th 2015, 10:34</td>
</tr>
<tr>
<td>5 Show all data</td>
<td><a href="mailto:JaneDoe@webroot.com">JaneDoe@webroot.com</a></td>
<td>Nov 5th 2015, 00:15</td>
</tr>
<tr>
<td>6 Hide all data for endpoints not seen for more than 1 month</td>
<td><a href="mailto:JaneDoe@webroot.com">JaneDoe@webroot.com</a></td>
<td>Nov 5th 2015, 00:17</td>
</tr>
</tbody>
</table>
Chapter 14: Accessing Usage Data

For information about accessing usage data, see the following topic:

About Accessing Usage Data ................................................................. 520
About Accessing Usage Data

With the usage console that includes detailed breakdowns of your Webroot products and services, you can now access your usage data for Security Awareness Training.

For more information, see the Accessing Usage Data topic in the Working With Settings section of the GSM Admin Guide.
Chapter 15: WSA Business Endpoint Protection Support

To learn more about Webroot's support options and other resources, see the following topic:

Accessing Technical Support ........................................................................................................ 522
Accessing Technical Support

Webroot offers a variety of support options. You can do any of the following:

- Look for the answer in our knowledgebase.
- Look for the answer in our online documentation.
- Enter a help ticket.
- Connect to the Webroot Online Business Forum.
Index

A

about
  accessing usage data 520
about dwell time 207
accessing
  management console 51
  product information 42
  technical support 522
  usage data 520
account settings, editing yours 54
accounts
  renewing 89
  upgrading 89
active directory tab, using 324
adding
  consoles 82
  keycodes 79
  groups 311
  site admins 91
advanced commands 153
agent commands 143
agent version overviews, viewing 205
agent version spread reports, generating 381
agents installed reports, generating 386
alerts
  deleting 412
  implementing 396
  suspending 412
all threats seen reports, generating 334
all undetermined software seen reports, generating 341
all URLs blocked reports, generating 348
antimalware commands 149
applying overrides
  from dwell time popups 449
  from groups 436
  from overrides tab 429
  from reports 444
applying policies
  to groups 316
  to single endpoints 317
B

basic configuration settings 252
behavior shield settings 270
blacklist overrides, creating 416

C

change logs, viewing 507
changing
  endpoint keycodes 131
  hardware on endpoints 157
checking scan results 166
collapsing panels 40
collated threat history reports, generating 368
command logs, viewing 510
commands
  advanced 153
  agent 143
  antimalware 149
  file 151
  identity shield 152
  issuing to endpoints 140
  power 149
  process 151
  running at endpoints 188
  user access 149
communicating through firewalls 6, 158
configuring environments 5
consoles
  adding 82
  renaming 88
  switching between 88
copying policies 230
core system shield settings 272
creating
  blacklist overrides 416
  customized alerts 399
  distribution lists 397
  policies 226
  portal users 67
  web overrides 470
  web overrides from group management 475
  web overrides from reports 484
Webroot accounts 11
whitelist overrides 422
CSV files, exporting 209
customized alerts, creating 399

D
daily blocked URL history reports, generating 377
daily threat history reports, generating 360
data filter logs, viewing 514
data filters, setting 502
data in reports, sorting 44
data in tables, sorting 44
deactivating endpoints 192
default policies, selecting 27, 220
defined alert messages, viewing 410
deleting
alarms 412
groups 330
policies 304
site admins 105
web overrides 496
deploying SecureAnywhere 110
deployment methods, selecting 29
descriptions
endpoint protection tabs 37
distribution lists, creating 397
downloading
report spreadsheets 393
updates 171
duplicated images, installing SecureAnywhere on 128
dwell time popups, applying overrides from 449
dwell time, about 207

E
editing
site admin settings 96
user information 71
web overrides 492
your account settings 54
endpoint keycodes, changing 131
endpoint protection menu, opening 38
endpoint protection overview 2
endpoint protection reports, generating 332
endpoint protection tabs description 37
endpoint statuses, viewing 197
endpoint updates, managing 157
endpoints
  changing hardware on 157
deactivating 192
  moving to subnets 157
reactivating 193
endpoints assigned to policies, viewing 293
endpoints with threats on last scan reports, generating 353
endpoints with undetermined software on last scan reports, generating 357
endpoints, changing keycodes 131
endpoints, issuing commands to 140
endpoints, moving between groups 320
endpoints, moving between policies 299
endpoints, organizing into groups 322
endpoints, renaming 134
endpoints, searching for 135
entering
  proxy bypasses 8
  proxy information on endpoints 9
  proxy information within installer 8
environments, configuring 5
exporting
  CSV files 209
  data to spreadsheets 41
  overrides to spreadsheets 461

F

file commands 151
file overrides, setting 169
firewall settings 280
firewalls, communicating through 6, 158
first time logging in 24
forcing
  immediate updates 174
  updates 171

G

generating
  agent version spread reports 381
  agents installed reports 386
  all threats seen reports 334
  all undetermined software seen reports 341
  all URLs blocked reports 348
  collated threat history reports 368
  daily blocked URL history reports 377
daily threat history reports 360
endpoint protection reports 332
endpoints with threats on last scan reports 353
endpoints with undetermined software on last scan reports 357
reports 332
GPO, installing SecureAnywhere 127
groups
   adding 311
   applying overrides from 436
   applying policies to 316
   deleting 330
   renaming 313

H

hardware, changing on endpoints 157
help files, opening 41
heuristic settings 263

I

identity shield
   commands 152
   settings 277
immediate updates, forcing 174
implementing
   alerts 396
   overrides 414
   policies 215
installer options 128
installing
   SecureAnywhere on duplicated images 128
   SecureAnywhere on terminal RDS servers 128
   SecureAnywhere on VMs 128
   SecureAnywhere with GPO 127
   SecureAnywhere with MSI 126
IP range tab, using 326
issuing commands to endpoints 140

K

keycodes, adding 79

L

logging in, first time 24
Mac SecureAnywhere menu 163
Mac tools drop-down menu 164
Mac, using SecureAnywhere installer for 114
Macs, opening SecureAnywhere 162
management console, accessing 51
management portal, using 33
managing
   endpoint updates 157
   portal users 67
   threats 166
menu, Mac SecureAnywhere 163
migrating systems 157
moving endpoints
   between groups 320
   between policies 299
   to subnets 157
MSI, installing SecureAnywhere with 126

opening
   endpoint protection menu 38
   help files 41
   panels 40
   SecureAnywhere on Macs 162
   SecureAnywhere on Windows 160
   video tutorials 41
options, installer 128
organizing endpoints into groups 322
overrides
   exporting to spreadsheets 461
   implementing 414
   viewing 456
overrides tab, applying overrides from 429
overview, Endpoint protection 2

panels
   collapsing 40
   opening 40
performing test installs 29
policies
   copying 230
creating 226
deleting 304
implementing 215
renaming 235
portal user permissions, setting 74
portal users
  creating 67
  managing 67
power commands 149
preparing for setup 5
process commands 151
product information, accessing 42
proxy bypasses, entering 8
proxy information on endpoints, entering 9
proxy information, entering within installer 8

Q

quarantine files, restoring 168

R

reactivating endpoints 193
realtime shield settings 267
recent threat statuses, viewing 201
renaming
  consoles 88
  endpoints 134
  groups 313
  policies 235
renewing accounts 89
report spreadsheets, downloading 393
reports
  agent version spread 381
  agents installed 386
  all threats seen 334
  all undetermined software seen 341
  all URLs blocked 348
  applying overrides from 444
  collated threat history 368
  daily blocked URL history 377
  daily threat history 360
  endpoints with threats on last scan 353
  endpoints with undetermined software on last scan 357
  generating 332
requirements, systems 4
restoring quarantine files 168
running commands at endpoints 188

S

scan histories
viewing 166
scan results
checking 166
scan schedule settings 255
scan settings 257
searching for endpoints 135
SecureAnywhere
deploying 110
installing with GPO 127
installer for Mac, using 114
installer for Windows, using 113
installer, using 113
installing on duplicated images 128
installing on terminal RDS servers 128
installing on VMs 128
installing with MSI 126
uninstalling 195
selecting default policies 27, 220
selecting deployment methods 29
self-protection settings 262
setting
data filters 502
file overrides 169
portal user permissions 74
settings
basic configuration 252
behavior shield 270
core system shield 272
firewall 280
heuristic 263
identity shield 277
realtime shield 267
scan 257
scan schedule 255
self protection 262
system optimizer 283
user interface 282
web threat shield 274
setup, preparing for 5
single endpoints, applying policies to 317
site admin
    settings, editing 96
site admins
    adding 91
    deleting 105
sorting data
    in reports 44
    in tables 44
spreadsheets, exporting data to 41
suspending alerts 412
switching between consoles 88
system optimizer settings 283
system requirements 4
systems, migrating 157

T

technical support, accessing 522
terminal RDS servers, installing SecureAnywhere on 128
test installs, performing 29
threats, managing 166
tools drop-down menu, Mac 164

U

uninstalling SecureAnywhere 195
updates
    downloading 171
    forcing 171
upgrading accounts 89
user access commands 149
user information, editing 71
user interface settings 282
using
    active directory tab 324
    IP range tab 326
    management portal 33
    SecureAnywhere installer 113
    SecureAnywhere installer for Mac 114
    SecureAnywhere installer for Windows 113
    workgroup tab 328

V

video tutorials, opening 41
viewing
  agent version overviews 205
  change logs 507
  command logs 510
  data filter logs 514
  defined alert messages 410
  endpoint statuses 197
  endpoints assigned to policies 293
  overrides 456
  recent threat statuses 201
  scan histories 166
VMs, installing SecureAnywhere on 128

W
web overrides
  creating 470
    creating from group management 475
    creating from reports 484
    deleting 496
    editing 492
web threat shield settings 274
Webroot accounts, creating 11
whitelist overrides, creating 422
Windows
  opening SecureAnywhere 160
    using SecureAnywhere installer for 113
workgroup tab, using 328