



Endpoint Protection Getting Started Guide

Table of Contents

Getting Started Guide.....	2
Console Registration.....	2
SecureAnywhere Agent: System Requirements.....	2
Communications.....	3
Necessary URLs.....	3
Mobile Protection.....	4
System Email Addresses.....	4
Proxy Settings.....	4
Deployment.....	5
General Deployment Process.....	5
Policies.....	5
Poll Interval Considerations.....	5
Installer Options.....	7
Installing on Terminal (RDS) Servers and Citrix XenApp.....	7
Installing on Duplicated Images or VMs.....	7
Command Line Switches.....	10
Overrides.....	11
Uninstall Tips.....	12
Option 1 – Agent Commands.....	12
Option 2 – Local Uninstall in Safe Mode With Networking.....	12
Support.....	13
Gathering Logs.....	13
Opening Support Tickets.....	13
Resources.....	15

Getting Started Guide

While Webroot SecureAnywhere® Business Endpoint Protection is extremely easy to deploy and manage, we recognize that enterprise environments can vary greatly. With that in mind, this Getting Started Guide covers some common deployment scenarios and settings. As always, this information should be balanced against your specific environment and security policies.

Console Registration

The first step is registering your new console. This ensures that you can modify any policy settings prior to installing the SecureAnywhere agent.

System Requirements

The system requirements can be found here: [System Requirements section of the Business Endpoint Protection webpage](#).

Communications

The SecureAnywhere agent uses ports 80 and 443 to communicate with the Webroot® Threat Intelligence Platform and your management console. These communications are encrypted using a proprietary form of obfuscation. If you are utilizing a web content filter or a proxy server, you will need to consider the following to ensure the agent can communicate correctly.

Necessary URLs

When configuring firewalls or any network access layer that can block SecureAnywhere traffic, the following URL masks need to be considered. These URLs can also be used to lock down any systems that would otherwise have no internet access.

- *.webrootcloudav.com
- *.webroot.com
- https://wrskynet.s3.amazonaws.com/*
- https://wrskynet-eu.s3-eu-west-1.amazonaws.com/*
- https://wrskynet-oregon.s3-us-west-2.amazonaws.com/*WSAWebFilteringPortal.elasticbeanstalk.com
- *.webrootanywhere.com

Path	Port	Information
*.webrootcloudav.com	Port 443 (https)	Agent communication and updates. Note: 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.
*.webroot.com	Port 443 (https)	Agent messaging.
https://wrskynet.s3.amazonaws.com/*	Port 443 (https)	Agent file downloading and uploading.
https://wrskynet-eu.s3-eu-west-1.amazonaws.com/*	Port 443 (https)	Agent file downloading and uploading.
https://wrskynet-oregon.s3-us-west-2.amazonaws.com/*	Port 443 (https)	Agent file downloading and uploading.
WSAWebFilteringPortal.elasticbeanstalk.com	Port 80 (http) & 443 (https)	Required for agent Web Filtering, elasticbeanstalk is an amazon AWS domain.

*.webrootanywhere.com	Port 80 (http) & 443 (https)	Management portal and support ticket logs upload.
-----------------------	------------------------------	---

Mobile Protection

If you have Mobile Protection, you should permit the following URLs:

- *.webrootmobile.com
- *.wrproxy.com

System Email Addresses

- Welcome Email – noreply@webroot.com
- Alerts/Summaries – noreply@webrootanywhere.com
- Support Notifications – noreply@webrootcloudav.com

Proxy Settings

By using the -autoproxy switch during install, the SecureAnywhere agent automatically detects an endpoint's proxy settings. You can also specify those settings manually, as needed. The syntax is listed in the Command Line Switches section on page 10.

Deployment

General Deployment Process

- Trial Initiation and Welcome Email
- User Creation and Console Registration
- Default Policy Selection
- Create Additional Admins, if applicable
- Permit SecureAnywhere URLs, if applicable
- Configure Alerts (optional)
- Deploy SecureAnywhere Agent
- Review Unknowns and Create Overrides (optional)

As mentioned, the first step is registering your new console. This ensures that you can modify any policy settings prior to installing the SecureAnywhere agent.

After the trial has been initiated, you will receive an email from noreply@webroot.com, which will contain the following:

- A link to start the registration process
- Your keycode
- Additional helpful information

Policies

The SecureAnywhere console comes with the following default policies:

- **Recommended Defaults** – Recommended settings, with protection and remediation enabled.
- **Recommended Server Defaults** – Recommended settings for servers, with protection and remediation enabled.
- **Silent Audit** – Non-remediation/Security audit.
- **Unmanaged** – Provides agent control to the endpoint's local user.

Note: When an endpoint is covered by any policy other than Unmanaged, it is automatically locked down, preventing changes and uninstallation. Default policies cannot be edited or deleted. They can, however, be used to create new policies by copying and editing.

Poll Interval Considerations

The SecureAnywhere agent checks for updates when the following events occur:

- Scans are run, scheduled or manual
- A new file is being determined
- The endpoint is rebooted
- Refresh Configuration is run by right-clicking the agent icon in the System Tray
- The poll interval expires
- The poll is triggered by command line; for more information, see Command Line Switches on page 10.

The poll interval is controlled by policy. The default settings are:

- **Daily** – For the Recommended Defaults policy
- **1 Hour** – For the Recommended Server Defaults policy

The possible Poll Interval settings are:

- Daily
- 12 hours
- 6 hours
- 4 hours
- 3 hours
- 2 hours
- 1 hour
- 30 minutes
- 15 minutes

If you are testing or making numerous policy changes, consider shortening the polling interval so that the endpoints receive these changes sooner.

Installer Options

The SecureAnywhere agent comes in two installer formats: EXE and MSI. Both are located under the Resources tab in the management console.

- **EXE** – The EXE file format can be downloaded and installed using either the generic EXE file, [wsasme.exe](#), or the Windows download link. This is the EXE file renamed using your SecureAnywhere keycode. When run, the installer automatically embeds the keycode into the installation process, and installs silently.
- **MS** – The MSI format can be downloaded utilizing the [wsasme.msi](#) link under the Install using MSI section of the console. The MSI can be edited to customize the installation to include the keycode in the GUILIC property and Command-Line options in the CMDLINE property, and may be deployed using GPO. This [video](#) outlines that process.

Installing on Terminal (RDS) Servers and Citrix XenApp

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

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 reused without sys prepping, or if 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. This may also generate duplicates in the management console.

If you encounter duplicates in the management console, uninstall Webroot SecureAnywhere Business Endpoint Protection from the affected endpoints. Be sure to remove or rename the WRDATA folder located in %PROGRAMDATA% to ensure no configuration files remain. Afterward, you can reinstall the agent with the -uniquedevic command line option. For example:

Executable Method

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

MSI Method

CMDLINE	-uniquedevic
---------	--------------

This will cause the SecureAnywhere agent 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 machine’s OS or hardware are cloned but the hostnames are always different. In this case, the unique hostname will enable unique instances of devices to report into the management console. The hostname remains untouched, so it will be reported into the console exactly as it exists within the OS.

For this reason, we do not recommend installing 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, be sure to use the -clone install switch as illustrated below.

Executable Method

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

MSI Method

CMDLINE	-clone
---------	--------

This creates a registry key in:

`HKLM\System\CurrentControlSet\Control\CloneTimeStampFlags`

Use this to make the agent create a persistent, unique value on the PC, which will change how the machine IDs and the PC hostname are displayed in the console.

The scan log will indicate this flag so admins can identify PCs more easily, for example, "Applied unique machine ID: C8137921" where C8137921 matches the hostname reported in the Webroot management console, such as PCHOSTNAME-C8137921. This value will persist if the agent is uninstalled/reinstalled so that existing agents don't move to other IDs. If the OS is reinstalled, the ID will change.

For more information on deploying within a Citrix environment, see [this document](#).

Command Line Switches

Command Line	Description
/key	Install with a specific keycode. <i>e.g. wsasme.exe /key=xxxx-xxxx-xxxx-xxxx-xxxx</i>
/silent	Install silently without showing any prompts. <i>e.g. wsasme.exe /key=xxxx-xxxx-xxxx-xxxx-xxxx /silent</i>
/group=GROUPCODE	<p>Command line switch for deploying directly into groups. <i>e.g. wsasme.exe /key=xxxxxxxx /group=-135260017840748808 /silent</i></p> <p>Assign endpoints to a specific group by selecting that group in the console > Actions drop-down menu > Deploy Endpoints to this Group. Note the GROUPCODE.</p> <p>Other requirements:</p> <ul style="list-style-type: none"> 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. <p>Command line. <i>e.g. msixexec /i "C:\wsasme.msi" GUILIC="XXXX-XXXX-XXXX-XXXX" CMDLINE="SME,quiet,Group=-135260017840748808" /qn /!*v %windir%\wsa_install_log.txt</i></p> <p>For MSI installs, you can use command line and an MSI editor. <i>MSI Editor in CMDLINE field: Group=-135260017840748808</i></p>
-clone	Use when InstanceMIDs match and cause duplicates in the console, or when endpoints replace others at each poll interval; this is usually found in imaged/cloned environments. <i>e.g. wsasme.exe /key=xxxx-xxxx-xxxx-xxxx-xxxx /silent -clone</i>
-uniquedevice	Use when InstanceMIDs match and cause duplicates in the console, or when endpoints replace others at each poll interval; this is typically used for virtual environments like Citrix Provisioning or VDI, where -clone is not effective because Device MIDs are the same. <i>e.g. wsasme.exe /key=xxxx-xxxx-xxxx-xxxx-xxxx /silent -uniquedevice</i>
-poll	Poll via a command line option. <i>e.g. "c:\program files\webroot\wrsa.exe" -poll</i>
-autoproxy	Use the automatic proxy configuration.
-proxy	<p>Proxy settings. Always use all parameters and blank out any value you don't need with double quotes, i.e., proxypass="" proxyauth #s: 0 = Any authentication 1 = Basic 2 = Digest 3 = Negotiate 4 = NTLM <i>e.g. wsasme.exe /key=xxxx-xxxx-xxxx-xxxx-xxxx /silent -proxyhost=nn.nn.nn.nn -</i></p>

```
proxyauth=n -proxyuser="proxyuser" -proxypass="password" -proxyport=port_number
```

Overrides

Overrides give administrative control over files on endpoints. Admins can override Webroot determinations as Good or Bad, and apply them globally or to individual policies. Use cases might include benign executables that do not comply with an organization’s acceptable use policies, or proprietary software that might otherwise have been classified as unwanted or malicious due to certain behaviors.

Admins can deploy Overrides from several locations within the management console, including the following tabs:

- **Overrides**
- **Group Management**
- **Reports**

Overrides can also be deployed from any area of the management console that displays the **Create override** button.



- When an administrator adds overrides from the Group Management or Reports tabs, the MD5 values have already been saved in the console and are available for use.
- When overrides are added from the Overrides tab, the administrator will need to scan the endpoint first and save the endpoint log to find and use the MD5 values.
- Overrides may be applied to all managed endpoints’ policies globally or within individual policies.
- Overrides may also have different settings at the global and individual policy levels. For example, an MD5 file might be treated as Bad at the global level and Good at the individual policy level.

Note: For more information, see the [Override](#) chapter in the [Endpoint Protection Admin Guide](#).

Uninstall Tips

Option 1 – Agent Commands

1. Open the Group Management tab and select the desired group from the Groups panel.
2. Do either one of the following:
 - Select an individual endpoint on which to run the command.
 - Select **Hostname** to run the command on all endpoints in the group.
3. Open the Agent Commands menu and select **Agent > Uninstall**.

The SecureAnywhere agent will be removed; however, the listing for the workstation remains. We recommend that you create a group called Uninstalled Clients into which these can be moved.

To remove a listing completely, click the red **Deactivate** button, which frees up the license seat taken by the endpoint.

Note: These endpoints will no longer check in with your console unless you reactivate them.

Option 2 – Local Uninstall in Safe Mode With Networking

Use the following steps to boot the computer into Safe Mode with Networking.

1. Shut down the computer.
2. Turn the computer on and tap the **F8** key repeatedly.
3. Use the **Up** and **Down** arrows to select **Safe Mode with Networking**.
4. On your keyboard, press **Enter**.
5. Do either one of the following:
 - If the endpoint was managed by a policy, Select **Safe Mode with Networking**. This is the default.
 - If the endpoint was not managed by a policy, select **Safe Mode**.
6. Do either one of the following, depending on your operating system:
 - **Windows XP** – Click **Start**, and then click **Run**. In the Run window, type **appwiz.cpl**, then, on your keyboard, press **Enter**.
 - **Windows Vista/Windows 7** – Click **Start**, or the **Windows** icon. In the Search field, type **appwiz.cpl**, then, on your keyboard, press **Enter**.
7. Select **Webroot SecureAnywhere**, then click **Uninstall/Remove**.
8. Confirm any messages regarding uninstalling the program.
9. Once the uninstall process has finished, restart the computer.

If the Webroot SecureAnywhere program is not visible in the Control Panel, the software can be uninstalled from the command line by running the following:

```
C:\Program Files\Webroot\WRSAs.exe -uninstall
```

Support

Gathering Logs

The process of opening a Support Ticket can be expedited by first collecting log files from the affected endpoint using the SecureAnywhere agent command **Customer Support Diagnostics**.

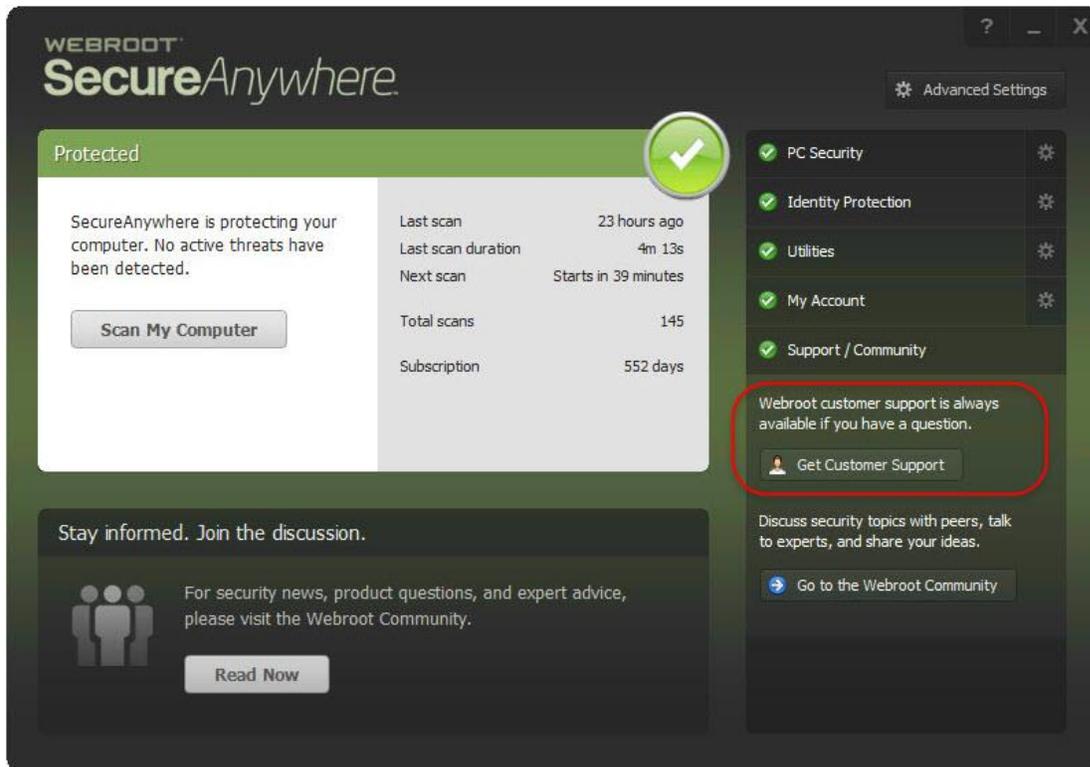
This agent command gathers all of the necessary diagnostic information for the Webroot Support Team to help you with the issue.

To speed this process even further, click **Refresh Configuration** on the endpoint instead of waiting for the Poll Interval to expire. This causes the SecureAnywhere agent to check in and receive the agent command sooner.

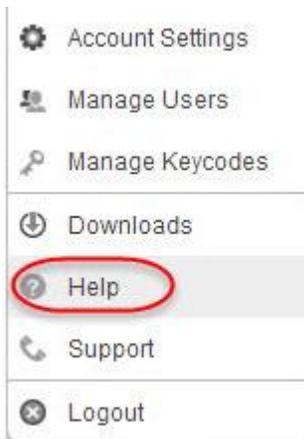
Opening Support Tickets

Admins can open a support ticket from several locations.

- **Agent** – Click the **Get Customer Support** button in the SecureAnywhere agent interface.



- **Agent** – Right-click the SecureAnywhere system tray icon and select **Help**.



- **Console** – Select your email address to open the drop-down menu in the upper right corner of the management console interface, then click **Support**.
- **Online** – Visit the [Webroot Support website](#).

With each method, you will be prompted for your email address. You will be notified via email when Webroot Support has responded to your ticket, and you will need to log back in to the Support page to retrieve the reply.

- If this is the first time you have contacted Webroot Support via online ticket, you can open your ticket immediately. A password will be sent to you automatically for future conversations.
- If you are a returning Support customer, enter the password that was sent to you previously. If you have forgotten that password, use the password recovery link.

Resources

- [Management Console](#)
- [Ask Webroot Knowledge Base](#)
- [Support Ticket Home](#)
- [Business Community](#)
- [Admin Guide](#)
- [Webroot YouTube Channel](#)
- [SecureAnywhere Free Trials](#)

© 2018 Webroot Inc. All rights reserved. Webroot, BrightCloud, SecureAnywhere, Webroot SecureAnywhere, and Smarter Cybersecurity are trademarks or registered trademarks of Webroot Inc. in the United States and/or other countries. All other trademarks are properties of their respective owners.