WEBROOT®

Managed Service Provider
Global Site Manager
Getting Started Guide

Table of Contents

Webroot SecureAnywhere – Business

While deploying Webroot SecureAnywhere Business – Endpoint Protection (WSAB) using our Global Site Manager (GSM) console is extremely easy, we recognize that your environment can vary greatly, and that each deployment has their own particular requirements. 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 deployment environments and security policies.

Requirements

Management Console Access Requirements

- Internet access is required.
- Google Chrome® (32-bit and 64-bit); current and previous two versions
- Internet Explorer® (32-bit and 64-bit); version 11
- Microsoft Edge® (32-bit and 64-bit; current and previous two versions
- Mozilla® Firefox® (32-bit and 64-bit; current and previous two versions
- Safari; current and previous two versions
- Opera; current and previous two versions

WSAB Agent - System Requirements

Workstations

- Windows 10 (32-bit and 64-bit)
- Windows 8 and 8.1 (32-bit and 64-bit)
- Windows 7 (32-bit and 64-bit), Windows 7 SP1 (32-bit and 64-bit)
- Windows Vista® (32-bit), Windows Vista SP1, SP2 (32-bit and 64-bit)
- Mac OS X 10.7 (Lion®)
- Mac OS X 10.8 (Mountain Lion®)
- OS X 10.9 (Mavericks®)
- OS X 10.10 (Yosemite®)
- OS X 10.11 (El Capitan®)
- macOS 10.12 (Sierra®)
- macOS 10.13 (High Sierra®)

Server

- Windows Server 2003 Standard, Enterprise, 32-bit and 64-bit
- Windows Server 2008 R2 Foundation, Standard, Enterprise
- Windows Small Business Server 2008 and 2011
- Windows Small Business Server 2012

Virtual Server Platforms

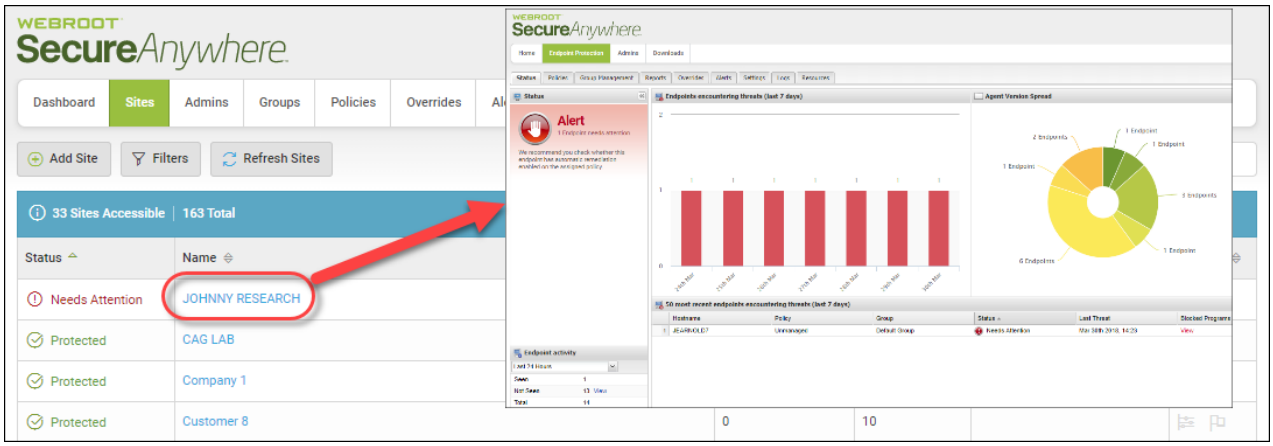
- VMware vSphere 4 (ESX/ESXi 3.0, 3.5, 4.0, 4.1), Workstation 6.5, 7.0, & Server 1.0, 2.0
- Citrix XenDesktop 5 and XenServer 5.0, 5.5, 5.6
- Microsoft Hyper-V Server 2008, 2008 R2

Service Configurations

Webroot's Global Site Manager (GSM) is a cloud-hosted, hierarchical management tool, providing you with an intuitive interface for administering multiple entities such as geographical locations, sites and user groups.

Each entity within Global Site Manager may be uniquely identified by its own keycode and may also be individually administered, if required, through its own separate WSAB Endpoint Protection management console.

Global Site Manager is also able to enforce global policies, overrides, and alerting over all endpoint entities.



The standard WSAB Endpoint Protection management console is a cloud-hosted solution that provides remote endpoint management including policy and group assignment, reporting, audit logs, and alerts.

Several assumptions are made in respect to this document:

- You have received your Welcome Email. For more information, see the Endpoint Protection Small and Medium Business Getting Started Guide.

  Note: If you have not received your Welcome Email, please contact your Webroot Partner, or notify your Webroot Channel Account Manager.

- You have set up your management console user login.
- You have direct access to the Webroot SecureAnywhere Global Site Manager.

General Setup

There are several ways to configure the WSAB service, depending on your needs and requirements:

Scenario 1: All managed entities within a single WSAB Endpoint Protection console.

- This is ideal for multiple entities that do *not* need individual administrative access via their own personal console.
- Each entity is then simply set-up under an individual group name. The group name being specified at the time of installation.

Scenario 2: All entities within the WSAB Global Site Manager console.

- This approach is suited to large deployments for many different entities at many locations and a large number of endpoints needing tailored management.
- Where individual entities require some level of local administrative access to their local console.
- For situations where you need to restrict administrator access to particular local functions.

Scenario 3: Hybrid approach.

- Some grouped entities within a single WSAB Endpoint Protection console
- Some customers in the Global Site Manager, separated by location

Note: How you manage WSAB is extremely flexible, allowing you to tailor management to suit your deployment, entity identification (keycode) and administration needs.

Deployment

Use the following table to determine the appropriate steps in your deployment process.

If you are…	Then do this…
Selecting the **All Entities** in a single WSAB Endpoint Protection console.	See the WSAB-EP Getting Started Guide.
Selecting all entities in Global Site Manager.	Continue reading.
Selecting a hybrid approach.	Continue reading.

General Deployment Process

- GSM site creation
  - One site for each entity
  - One site for multiple entities, if applicable
- Policy creation/assignment
- Create additional administrators and assign permissions, if applicable
- Permit WSAB URLs, if applicable
- Configure Global Alerts, if applicable
- Deploy WSAB agent

Note: For more information, see the GSM Admin Guide.

Policies

Policies give an administrator centralized control over an endpoint's WSAB settings. Policies can be configured at the GSM and/or entity level. For more information, see the Working With Policies section of the GSM Admin Guide.

Policies can be configured from several locations within SecureAnywhere:

- GSM or Global Policies can be configured at the GSM level and can be applied to one or more entities.
  - Policies are configured under the Policies tab.
  - A default policy can be assigned to a GSM Site entity at the time of Site creation or by editing a Site's settings.
- Site Policies can be configured at the Site level.
  - Policies are configured under the Policies tab.
  - A default policy can be set.
  - Policies can be assigned to groups under the Group Management tab.
  - Endpoints in these groups will inherit the assigned Group Policy.

Webroot SecureAnywhere comes with four customizable security policies:

- **Recommended Defaults** – Recommended settings with endpoint protection and remediation enabled.
- **Recommended Server Defaults** – Recommended settings for use in Servers, with protection and remediation enabled.
- **Silent Audit** – Non-remediation, just security audit reporting only.
- **Unmanaged** – Provides agent policy control to the endpoint user.

Note: When an endpoint is covered by any policy other than Unmanaged then it is automatically locked down, tamper-proofing the agent and preventing any changes or uninstallation. Default policies cannot be edited or deleted, they can, however, be copied and edited to create new custom policies.

Poll Interval Considerations

The WSAB-EP agent checks in with the console when the following events occur:

- The configurable, policy-assigned poll interval expires.
- Scans are run, both scheduled and manual.
- A new file is being determined.
- The endpoint is rebooted.
- Right-clicking the WSAB agent in the System Tray and selecting Refresh Configuration.
- An agent poll is triggered by using the remote agent command line. For more information on remote commands see Command Line Switches.

Installer Options

- Windows
  - EXE package
  - MSI package
- Mac
  - DMG package

Note: Only individual entity/site 'child' keycodes should be used for deployment. The 'parent' GSM account keycode should never be used.

- A customized EXE package is available at the Site child keycode level, under the Resources > Windows Download link. The site EXE package is then renamed using the keycode provided. When it runs, it then imbeds the keycode into the silent, unattended installation process.
- The MSI can be edited directly to include a Site's keycode and deployed using Windows Group Policy, RMM, or any software distribution method that supports a MSI package.

Installing on VMs/Citrix Considerations

Some architectures can cause duplicates in the WSAB console. This can occasionally occur because of improperly configured endpoint images or virtual machines.

If duplicates occur in your Webroot console during your testing, please uninstall Webroot SecureAnywhere Business Endpoint Protection from the affected endpoints. Then, reinstall it with the command line option *-clone*, which causes SecureAnywhere to create a unique identification for that system.

For example, enter the following command line:

WSABsme.exe /key=xxxx-xxxx-xxxx-xxxx-xxxx /silent -clone

Note: X's represent the numerals in your license key.

After installation, a new hostname appears in the Webroot console. For example, hostname *PCHOSTNAME* might become *PCHOSTNAME-C8137921*.

When an agent is uninstalled or reinstalled, this value persists so that existing agents won't move to other IDs. However, if the OS is reinstalled, the ID will change.

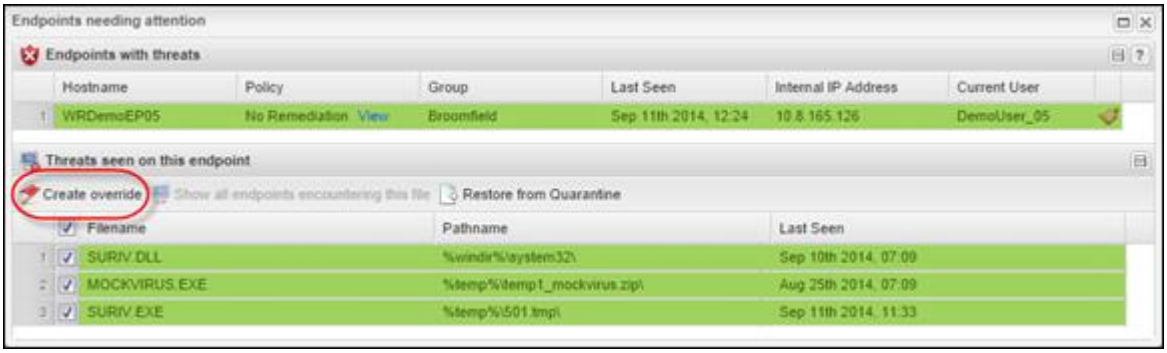
Overrides

Overrides give an administrator centralized control over the files that are allowed to run on endpoints, with the ability to override files as *Good* or *Bad*. Overrides can be configured at the GSM console and/or Site console levels.

For more information see the Working With Overrides chapter in the Global Site Manager Admin Guide.

Overrides can be configured from several locations within SecureAnywhere:

- GSM or Global Overrides can be configured at the GSM level and can be applied to one or more sites:
  - Located under Global Settings > Overrides.
  - Overrides can be configured using a file's MD5.
  - Overrides can be imported from a site's existing overrides.
- Site Overrides can be configured at the site level and can be applied to an entire site or a single policy:
  - Located under the Overrides tab.
  - Overrides can also be configured under the Status, Group Management, and Reports tabs, utilizing the Create override button:



Support

Gathering Logs

The process of opening a Support Ticket can usually be expedited by first collecting log files from the affected endpoint.

Customer Support Diagnostics Agent Command

Utilizing the WSAB agent command `Customer Support Diagnostics` is the preferred method.

This agent command gathers all of the necessary diagnostic information needed by Webroot's Support Team to help you with your issue.

To speed this process even further, click the **Refresh Configuration** button on the endpoint, instead of waiting for the Poll Interval to expire for the endpoint to check-in and pick-up the agent command.

Log File Locations

WSAB-EP log files are located in the WRData folder:

- Windows XP Systems: C:\Documents and Settings\All Users\WRData
- Windows Vista and Newer: C:\ProgramData\WRData

Opening Support Tickets

Support can be obtained via the web or the phone:

http://www.webroot.com/us/en/support/support-business

Communications

The WSAB agent communicates over port 80 and 443, to the Webroot Intelligence Network and your management console. These communications are encrypted via a proprietary form of obfuscation. If you are utilizing a web content filter or a proxy server, you will want to consider the following to ensure that the WSAB agent can communicate to the Webroot Intelligence Network and your console.

WSAB-Needed URLs

When configuring firewalls or any network access layer that can block WSAB 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 whatsoever.

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.
***.webrootanywhere.com**	Port 443 (https)	Agent file downloading and uploading.
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 80 (http) & 443 (https)	Required for agent Web Filtering, elasticbeanstalk is an amazon AWS domain.
WSAWebFilteringPortal.elasticbeanstalk.com	Port 80 (http) & 443 (https)	Management portal and support ticket logs upload.

Mobile Protection URL

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

- *.webrootmobile.com

System Email Addresses

To ensure you receive emails from the addresses below, it is recommended that they be added to your Allowed/White Lists:

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

Proxy Settings

1. By using the `–autoproxy` switch during install, the WSAB agent auto-detects an endpoint's proxy settings.
2. However, you can manually specify those settings as needed. The syntax is listed under Command Line Switches.

Command Line Switches

Command Line	Description
/key	Install with a specific keycode. Example: `WSABsme.exe /key=xxxx-xxxx-xxxx-xxxx-xxxx`
/silent	Install silently without showing any prompts. Example: `WSABsme.exe /key=xxxx-xxxx-xxxx-xxxx-xxxx /silent`

Command Line	Description

/group=GROUPCODE	Command line switch for deploying directly into groups.
	Example:
	`WSABsme.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:\WSABsme.msi" GUILIC="XXXX-XXXX-XXXX-XXXX" CMDLINE="SME,quiet,Group=-135260017840748808" /qn /l*v %windir%\WSAB_install_log.txt`
	For MSI installs you can use command line and an MSI editor.
	Example for MSI Editor in CMDLINE field: Group=-135260017840748808

-clone	For use when InstanceMID's are matching causing duplicates in the console or endpoints replacing endpoints at each poll interval, usually found in imaged/cloned environments. Example: `WSABsme.exe /key=xxxx-xxxx-xxxx-xxxx-xxxx /silent -clone`
-uniquedevice	For use when DeviceMID's are matching causing duplicates in the console or endpoints replacing endpoints at each poll interval. Typically used for virtual environments like Citrix Provisioning or VDI where the use of -clone is not effective due to Device MIDs being the same. Example: WSABsme.exe /key=xxxx-xxxx-xxxx-xxxx-xxxx /silent -uniquedevice

Command Line	Description
-poll	Poll via a command line option. Example: `"c:\program files\webroot\wrsa.exe" –poll`
-autoproxy	Use the automatic proxy configuration.

-proxy	Proxy settings.
	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
	Example:
	`WSABsme.exe /key=xxxx-xxxx-xxxx-xxxx-xxxx /silent -proxyhost=nn.nn.nn.nn -proxyauth=n -proxyuser="proxyuser" -proxypass="password" -proxyport=port_number`

Uninstall Tips

Option #1 - Uninstall Using Agent Commands

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

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

   To remove a listing completely, select the red **Deactivate** button, which frees up the license seat taken by the endpoint. This endpoint will no longer check in with your console unless you reactivate it.

Option #2 - 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 press 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 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 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 press **Enter** on your keyboard.
   - **Windows Vista and Newer** – Click **Start**, or the **Windows** icon. In the Search field, type **appwiz.cpl**, then press **Enter** on your keyboard.
7. Select **Webroot SecureAnywhere**, then click **Uninstall/Remove**.
8. Confirm any messages regarding uninstalling the program.

   Once the uninstall process has finished, restart the computer.

   If Webroot SecureAnywhere is not visible in the Control Panel, the software can be uninstalled from the command line by running the following: *C:\Program Files\Webroot\WRSA.exe –uninstall*

Resources

Links

- WSAB Console
- Ask Webroot
- Open Support Ticket
- Business Community
- Admin Guide
- Webroot YouTube Channel
- WSAB Trial

Canned Demos

- http://detail.webrootanywhere.com/gsmdemo_sites.asp
- http://detail.webrootcloudav.com/Endpoint_demo.asp