

WEBROOT®

an **opentext™** company

Management Console Best Practices Guide

Copyright

Copyright 2019 Webroot. All rights reserved.

Management Console Best Practices 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: Management Console Best Practices Guide	1
Creating New Sites	2
Step 1 – Site Setup	3
Step 2 – Administration Access	4
Step 3 – Site Details	4
Policy Management	6
Default Policies and Recommendations	6
Polling Interval	7
Potentially Unwanted Applications (PUAs)	7
Scan Schedule	8
Web Threat Shield	9
Unblocking Sites	10
Firewall	12
User Interface	13
Using Silent Audits	17
Undetermined Report	17
Undetermined Application	19
Working With Overrides	20
Path Overrides	20
File Overrides	20
Folder Overrides	21
User Interface Suggestions	25
Columns	25
Group Management	25
Cloud Determinations	26
Chapter 2: Management Console Support	28
Capturing Logs	29
Tickets	30
Deployment Options	31
Index	i

Chapter 1: Management Console Best Practices Guide

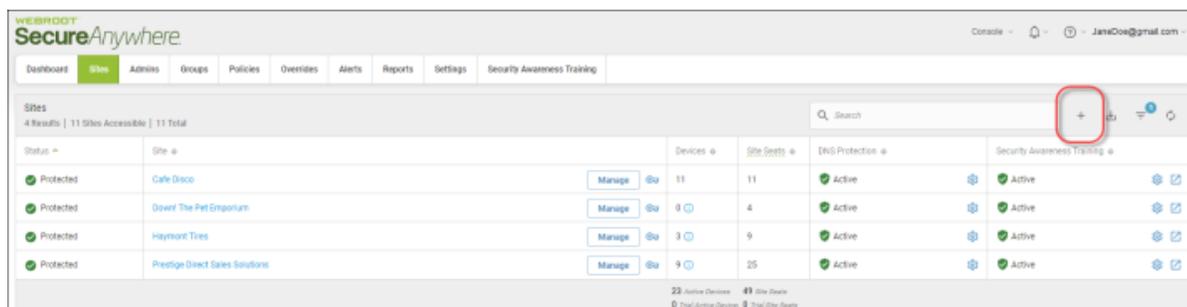
For information about best practices for the management console, see the following topics:

Creating New Sites	2
Step 1 – Site Setup	3
Step 2 – Administration Access	4
Step 3 – Site Details	4
Policy Management	6
Default Policies and Recommendations	6
Polling Interval	7
Potentially Unwanted Applications (PUAs)	7
Scan Schedule	8
Web Threat Shield	9
Unblocking Sites	10
Firewall	12
User Interface	13
Using Silent Audits	17
Undetermined Report	17
Undetermined Application	19
Working With Overrides	20
Path Overrides	20
File Overrides	20
Folder Overrides	21
User Interface Suggestions	25
Columns	25
Group Management	25
Cloud Determinations	26

Creating New Sites

Adding a New Site has a three step wizard for configuration. All settings can be modified after the site is created.

- [Step 1 – Site Setup](#)
- [Step 2 – Administration Access](#)
- [Step 3 – Site Details](#)



Step 1 – Site Setup

The screenshot displays the 'Add Site' configuration page in the Webroot SecureAnywhere Management Console. The interface includes a top navigation bar with options like Dashboard, Sites, Admins, Groups, Policies, Overrides, Alerts, Reports, Settings, and Security Awareness Training. A progress indicator at the top shows five steps: 1. Details (active), 2. Permissions, 3. Endpoint Protection, 4. DNS Protection, and 5. Security Awareness Training. The 'Details' section contains the following fields:

- Site / Company Name:** A text input field.
- Site Type:** Radio buttons for 'External Company' (selected) and 'Internal Site'.
- Company Size:** A dropdown menu with the text 'Please select one of the following...'.
- Company Industry:** A dropdown menu with the text 'Please select one of the following...'.
- Billing Cycle:** A dropdown menu with 'Annually' selected.
- Billing Date:** A calendar picker showing 'Jan' and '1st'.
- Comments:** A large text area for additional notes.
- Tags:** An input field with an 'Add' button.

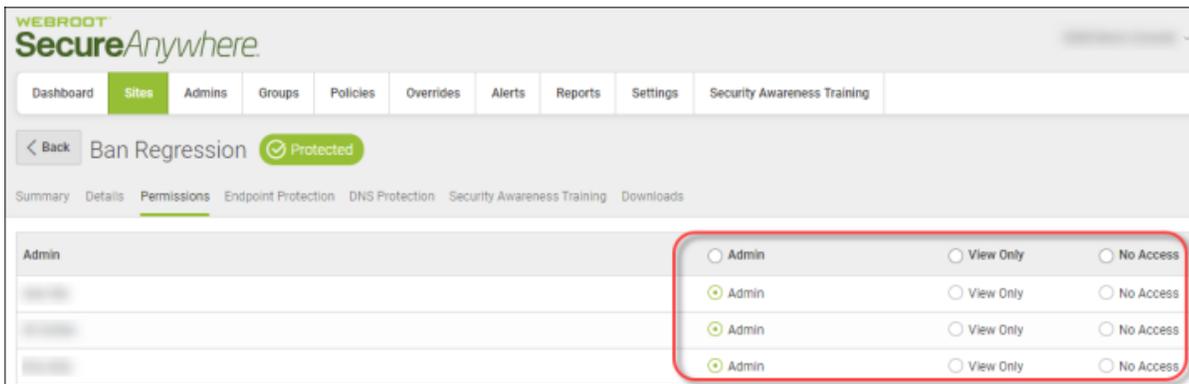
A green 'Next' button is located at the bottom left of the form. The footer of the page includes the text: © 2019 Webroot Inc. Privacy Statement Website Terms of Service License Agreement.

- **Site / Company Name** – Customer name.
- **Site Type** – Either External or Internal.
- **Company Industry** – For informational demographic purposes only.

Note: The rest of the fields, Billing Cycle, Billing Date and Comments, are for informational purposes, and do not affect licensing, billing or any other system, and are strictly for your internal information only. For more information, see [Adding Sites](#).

Step 2 – Administration Access

- **Global Administrators** – Grant admins access to various sites. Great for teams who manage different customer accounts:
 - **Admin** – Full access to the respective site.
 - **View Only** – Admins can see the site information and access the endpoints, but cannot make any changes.
 - **No Access** – Admins have no access to this site, and are not even aware it exists.



Note: You can assign site only admins for local customers separately. This site permission step in the initial creation is for admins only. For more information, see [Updating Site Admin Permissions](#).

Step 3 – Site Details

- **Include Global Policy** – We recommend that you allow Global Policies to be accessible at the site level, as this feature has little impact on endpoint and site management. It’s good for setting up golden master policies and assigning them to endpoints and groups of endpoints.
- **Default Policy** – When an endpoint is installed, it will pick up the site default policy. We recommend that you use either your own workstation default policy copied from our default, or the built-in [Recommended Defaults](#).
- **Include Global Overrides** – Global Overrides are great for exceptions that need to be used across multiple customers with similar industry focus. However, in some cases, it might not make sense to have global overrides turned On for every site. For example, legal focused overrides may not make sense for a medical practice.
- **Report Distribution List** – Set default email to distribution list, as this can be changed later.
- **Data Filter** – Leave as default.

WEBROOT
SecureAnywhere

Dashboard Sites Admins Groups Policies Overrides Alerts Reports Settings Security Awareness Training

< Back Add Site

1 Details 2 Permissions 3 Endpoint Protection 4 DNG Protection 5 Security Awareness Training

Endpoint Protection is required to trial or purchase any of Webroot's additional products and services - including DNG Protection and Security Awareness Training.

Keycode Type ⓘ
 Full 30 day trial

Site Seats ⓘ

Default Endpoint Policy ⓘ
Recommended Defaults

Report Distribution List ⓘ
gpi@webroot.com

Include Global Policies? ⚠

Include Global Overrides? ⚠

Data Filter ⓘ
Inherit the GDM data filter setting

Previous Next

Note: Including Global Policy and Global Overrides cannot be undone. The best practice is to turn Global Policies On and leave Global Overrides turned Off, unless it's prudent to change later.

Policy Management

Default Policies and Recommendations

Default policies should be used as templates and should not be assigned to endpoints, as they cannot be edited. We recommend that you make a copy and modify the copy, according to your needs.

- **Recommended Default** – This policy covers the majority of endpoint requirements for general users working on workstations or laptops. User interface and PUAs are turned Off.
- **Recommended Server Default** – This policy covers the majority of server environments with the primary focus on resource utilization. Designed for server environments. Difference is around resource management for zero impact on a server.
- **Silent Audit** – This policy is a derivative of Recommended Defaults and purposefully has the remediation function suppressed so as to not effect production. This policy should be used for short duration during initial site/endpoint setup to capture potential production false positives. See section below on how to utilize the [Silent Audit policy, and review Unknown Applications](#).
- **Unmanaged** – Designed for troubleshooting and/or no policy management where necessary. This is not a manageable or editable policy, rather it turns the agent into a local, unmanaged application to be controlled directly by the endpoint user. Primary recommended use is for technical support, but it's highly recommended to not be used in production, as it moves the management responsibility to the endpoint user which could cause a network vulnerability.

Note: For more information, see [Working With Policies](#).

Various policy settings are either not configured or should be reviewed before using all default settings. An in-depth explanation will focus on recommended changes to policies for user endpoints, not servers.

- [Polling Interval](#)
- [Potentially Unwanted Applications \(PUAs\)](#)
- [Scan Schedule](#)
- [Web Threat Shield](#)
- [Unblocking Sites](#)
- [Firewall](#)
- [User Interface](#)

Polling Interval

Our agent will check in with our console based upon this Poll Interval. The default is set to Daily (24 hours). We recommend that you change this to 15 minutes.

The screenshot shows the 'Workstation Defaults' configuration page. It includes fields for 'Name' (Workstation Defaults) and 'Description' (Copy of the Recommended Defaults Policy). The 'Policy Section' is set to 'Basic Configuration'. A list of settings is shown, with 'Poll interval' highlighted by a red circle and set to '15 Mins'. A 'Save' button is located at the bottom left.

Setting	Value
Favor low disk usage over verbose logging (fewer details stored in logs)	Off
Lower resource usage when intensive applications or games are detected	On
Allow SecureAnywhere to be shut down manually	Off
Force non-critical notifications into the background	On
Fade out warning messages automatically	On
Store Execution History details	On
Poll interval	15 Mins

Potentially Unwanted Applications (PUAs)

By default, Detect Possibly Unwanted Applications as malicious is turned Off. Given the number of attack vectors that come through Adware and other various utilities and browser add-ons, we recommend, in most environments, that you turn this On. The caveat is, it could catch more false positives and be chatty, but the agent will identify more malicious code with this turned On.

Server Defaults

Name
Server Defaults

Description
Copy of the Recommended Server Defaults Policy

Policy Section
Scan Settings

Setting	Off	On
Automatically reboot during cleanup without prompting	<input checked="" type="radio"/>	<input type="radio"/>
Never reboot during malware cleanup	<input checked="" type="radio"/>	<input type="radio"/>
Automatically remove threats found during background scans	<input type="radio"/>	<input checked="" type="radio"/>
Automatically remove threats found on the learning scan	<input checked="" type="radio"/>	<input type="radio"/>
Enable Enhanced Support	<input type="radio"/>	<input checked="" type="radio"/>
Show Infected Scan Results	<input checked="" type="radio"/>	<input type="radio"/>
Detect Possibly Unwanted Applications (PUAs) as malicious	<input type="radio"/>	<input checked="" type="radio"/>

Save

Scan Schedule

Daily scans can be set at an appropriate time based upon your environment and customer needs. By default, there is a Randomize setting, which will tell the agent to scan at various times close to the scheduled scan. If you want to have the machines scan at an exact time, turn this setting Off.

Server Defaults

Name
Server Defaults

Description
Copy of the Recommended Server Defaults Policy

Policy Section
Scan Schedule

Setting

Scan on bootup if the computer is off at the scheduled time	<input type="radio"/> Off <input checked="" type="radio"/> On
Hide the scan progress window during scheduled scans	<input type="radio"/> Off <input checked="" type="radio"/> On
Only notify me if an infection is found during a scheduled scan	<input type="radio"/> Off <input checked="" type="radio"/> On
Do not perform scheduled scans when on battery power	<input type="radio"/> Off <input checked="" type="radio"/> On
Do not perform scheduled scans when a full screen application or game is open	<input checked="" type="radio"/> Off <input type="radio"/> On
Randomize the time of scheduled scans up to one hour for distributed scanning	<input type="radio"/> Off <input checked="" type="radio"/> On
Perform a scheduled Quick Scan instead of a Deep Scan	<input checked="" type="radio"/> Off <input type="radio"/> On

Save

Web Threat Shield

By default, the agent will install extensions for all browsers and a driver for Edge on Windows 10. It will also suppress the user's ability to override a blocked website. If you are interested in allowing users to bypass the block, which may be needed in some cases, turn this setting Off.

Server Defaults

Name
Server Defaults

Description
Copy of the Recommended Server Defaults Policy

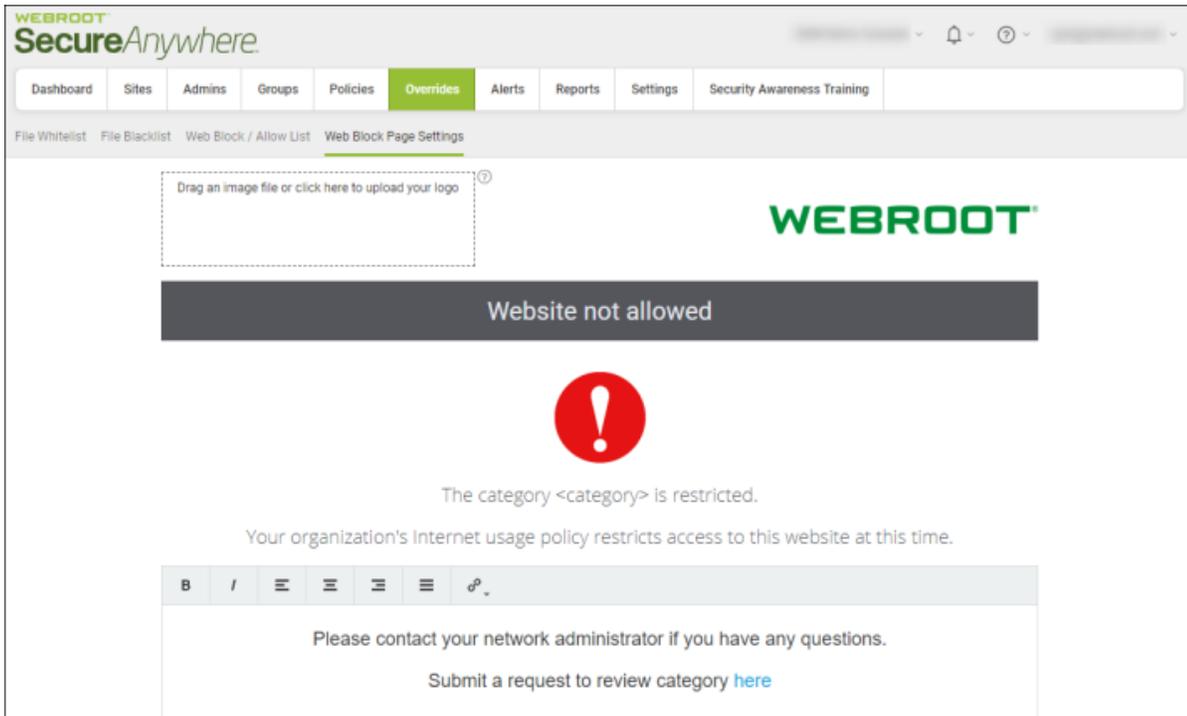
Policy Section
Web Threat Shield

Setting	Off	On
Enable Web Shield	<input type="radio"/>	<input checked="" type="radio"/>
Activate browser extensions	<input type="radio"/>	<input checked="" type="radio"/>
Block malicious websites	<input type="radio"/>	<input checked="" type="radio"/>
Enable realtime anti-phishing	<input type="radio"/>	<input checked="" type="radio"/>
Show safety ratings when using search engines	<input type="radio"/>	<input checked="" type="radio"/>
Enable web filtering driver	<input type="radio"/>	<input checked="" type="radio"/>
Suppress the user's ability to bypass blocked websites	<input type="radio"/>	<input checked="" type="radio"/>

Save

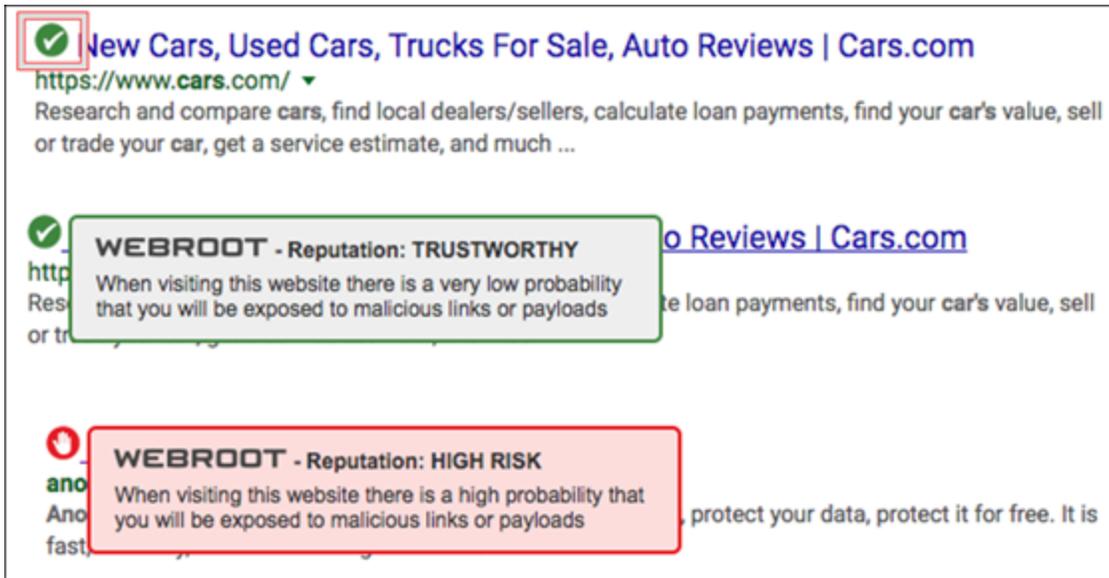
Unblocking Sites

With the Suppress Users ability to make local overrides setting turned Off, the user will get a blocked page, along with a message indicating that they should contact their network administrator with any questions.



Search Reputation

With the extensions enabled in the Web Threat Shield policy, users will see various reputation indicators when performing a web search. Mouse over the icon to get a review of what Webroot thinks about this sites reputation.



Firewall

This setting is actually an outbound port monitor, not an inbound/outbound port manager with rules, like a traditional firewall. It should be left On, as it's not manageable. It does, however, provide behavior information about an unknown process being monitored and is valuable to the agent in making a decision about the monitored process.

Server Defaults	
Name	Server Defaults
Description	Copy of the Recommended Server Defaults Policy
Policy Section	Firewall
Setting	
Enabled	<input checked="" type="radio"/> Off <input checked="" type="radio"/> On
Firewall level	Warn unknown and infected
Show firewall management warnings	<input checked="" type="radio"/> Off <input type="radio"/> On
Show firewall process warnings	<input checked="" type="radio"/> Off <input type="radio"/> On

Save

User Interface

GUI

By default, the User Interface is hidden. If you'd like your users to be able to see the Webroot application, turn this to Show.

Users can only perform a scan, and cannot turn any other settings On/Off or manage the agent application in any way. To leave the GUI hidden and only show a system tray icon, set this at Hide. Best practice is to turn it to Show.

Server Defaults

Name
Server Defaults

Description
Copy of the Recommended Server Defaults Policy

Policy Section
User Interface

Setting

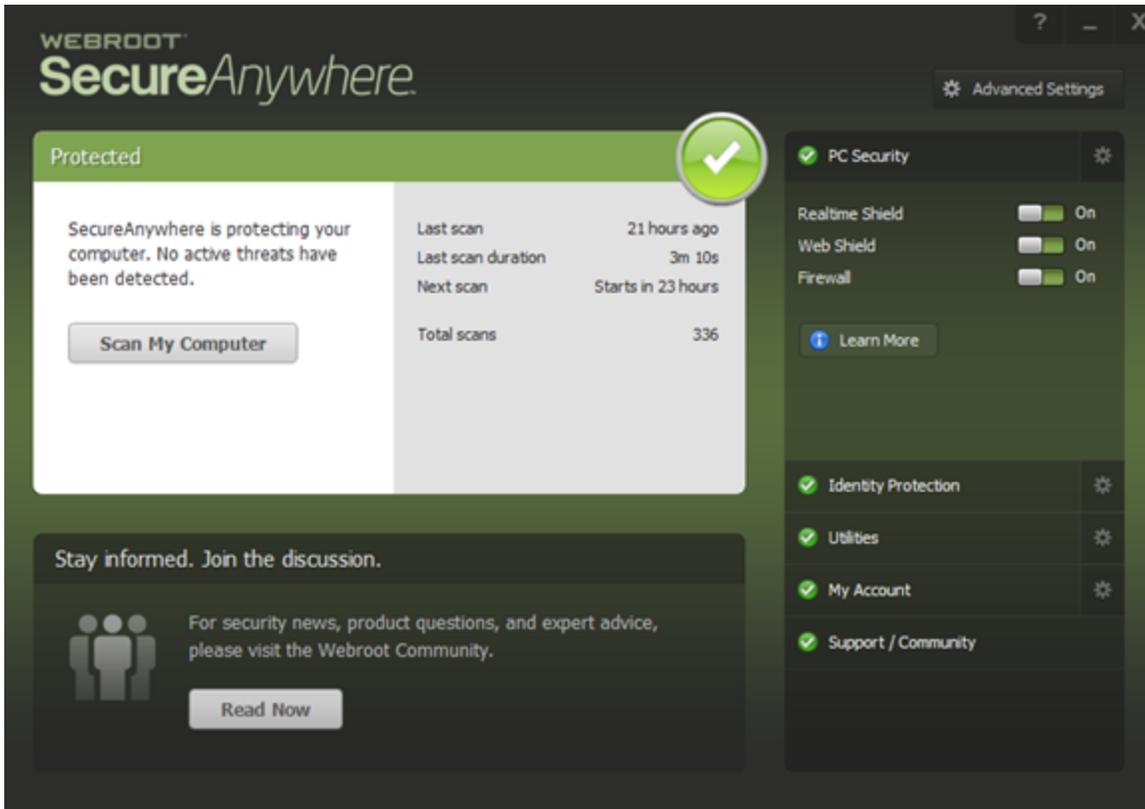
GUI Show Hide

Save

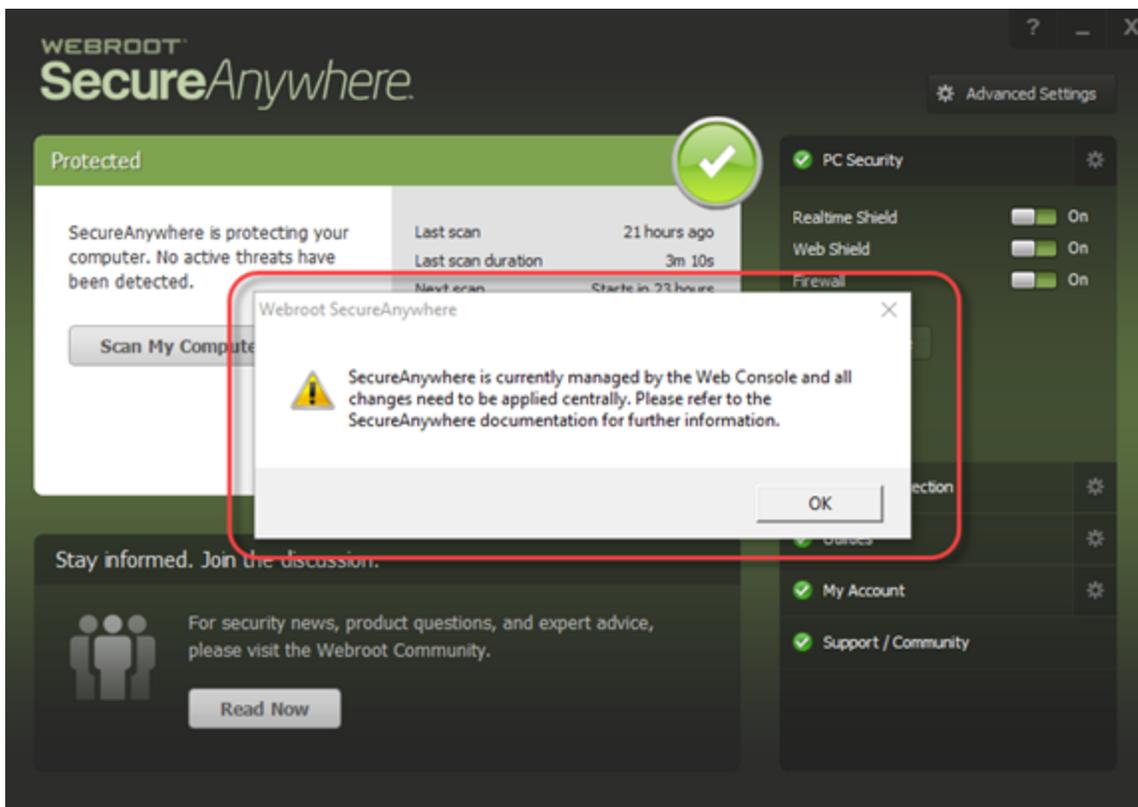
Agent GUI

The local GUI cannot be managed or changed by the user. However, they will see the settings and know protection is turned On and is working.

Normal View

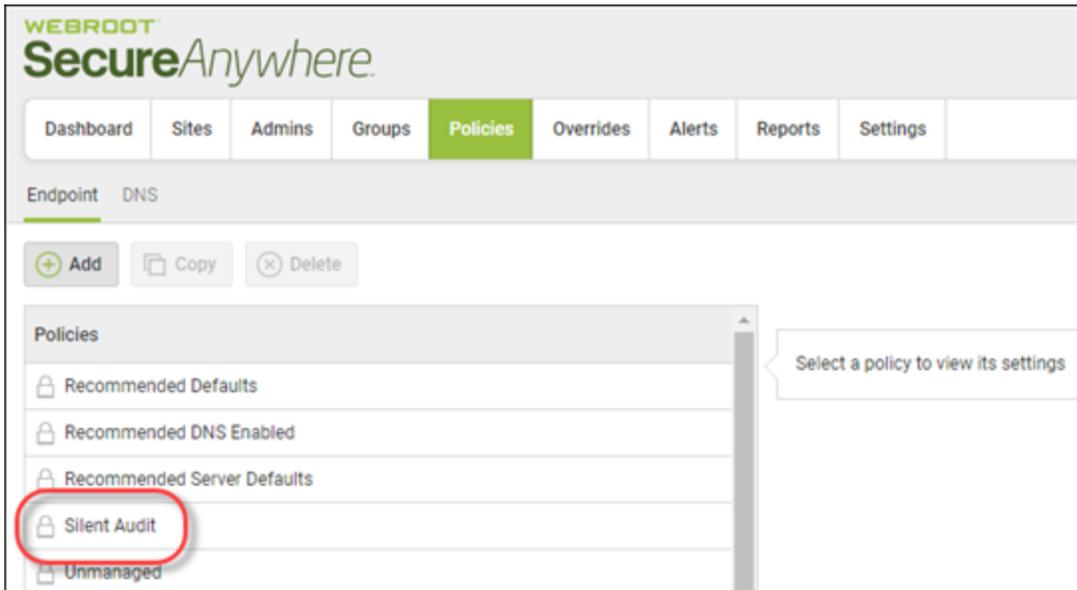


Alert on Change Attempt



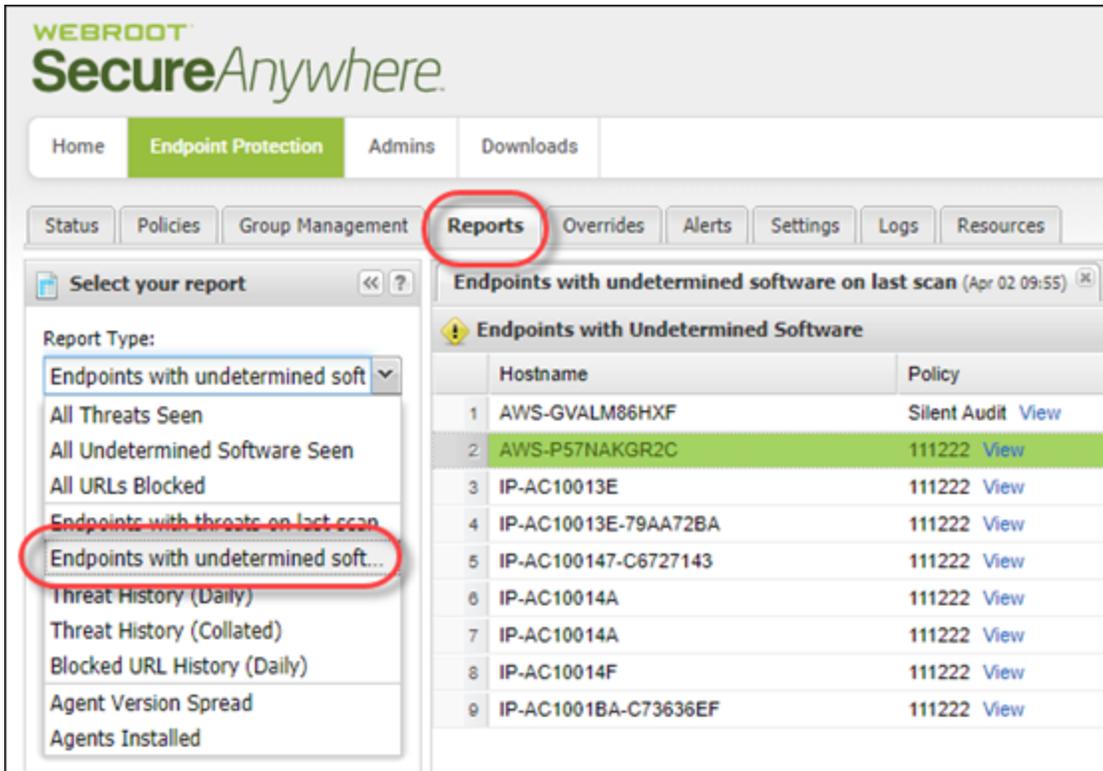
Using Silent Audits

Consider taking a conservative approach when rolling out to new environments and use the Silent Audit policy. This is a policy that will not remediate monitored undetermined applications, but will remediate known files. It will help you learn what is undetermined, so you can proactively configure whitelist overrides.

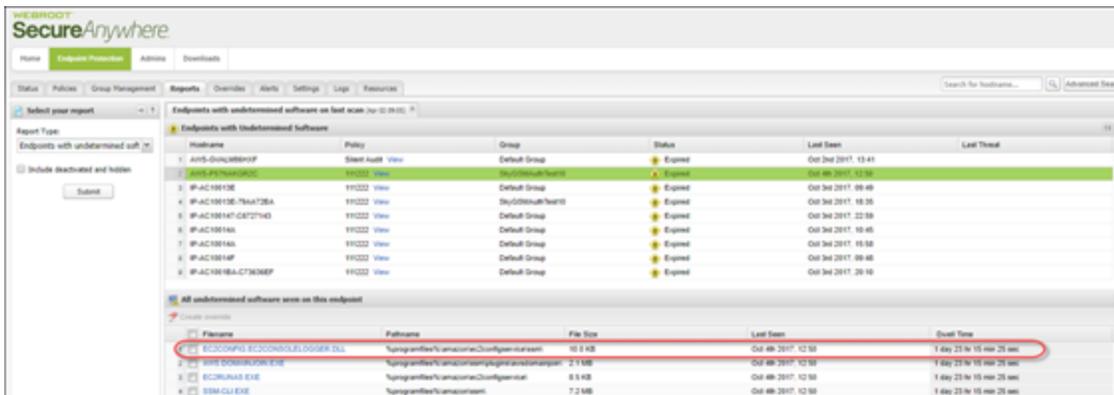


Undetermined Report

Once you've assigned the Silent Audit policy to a specific endpoint, test endpoints that represents a sample of users' environments or all endpoints on a site, let it run a few days, and then pull an Undetermined Report by going to the Site and selecting the Reports tab.



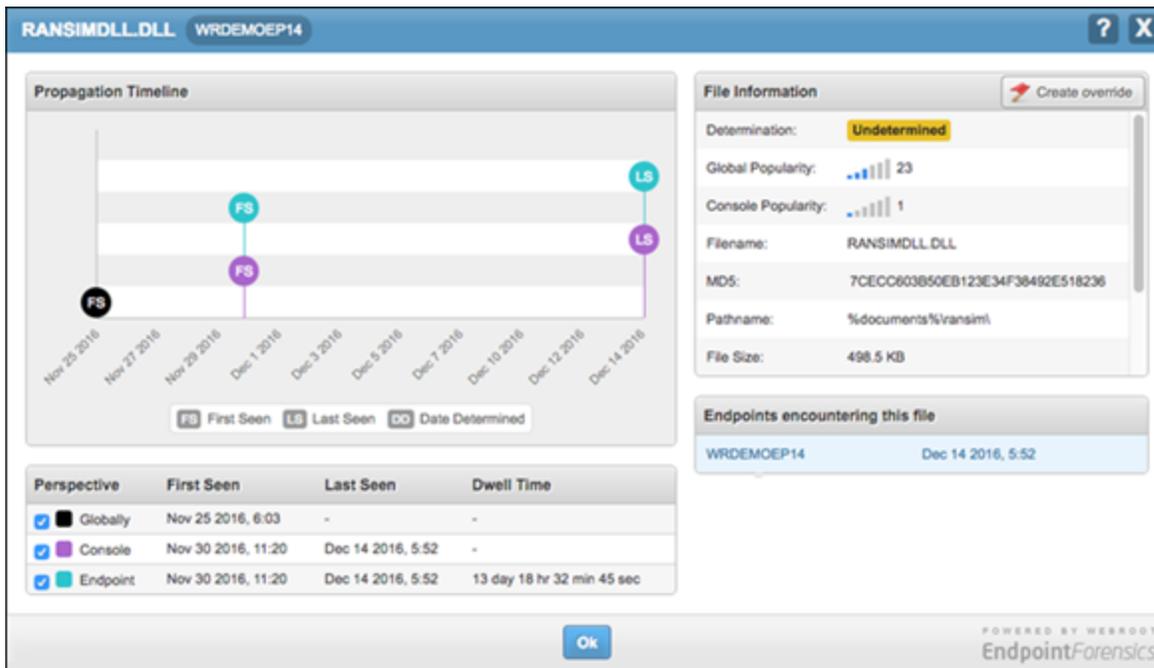
The report will list the endpoints with undetermined software being monitored, and list each application below when you select an endpoint host. You can export this list or review it, and use the information for whitelist override configurations.



Note: For more information, see [Generating Endpoints With Undetermined Software on Last Scan report](#).

Undetermined Application

For additional review, you can select the file in question and see detailed forensics related to what Webroot's Threat intelligence knows about this file.



Working With Overrides

File Overrides can be captured in various ways when presented:

- On the management console, you can take action and establish a file override.
- When viewing the endpoint at the Site and Group Management level.
- You can override a file manually.

Note: For more information, see [Working With Overrides](#).

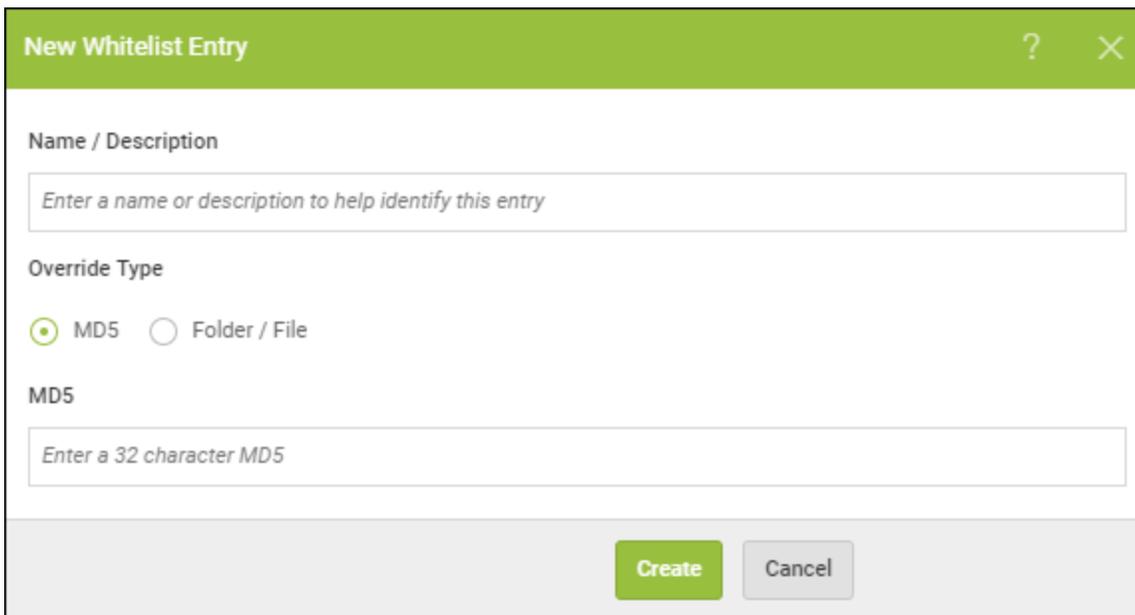
Path Overrides

- Locate path in Undetermined report
- Manual

File Overrides

A file based override can be generated manually and/or through several areas displayed in the management console and at a Site.

Manually - Overrides Tab



New Whitelist Entry ? X

Name / Description

Enter a name or description to help identify this entry

Override Type

MD5 Folder / File

MD5

Enter a 32 character MD5

Create Cancel

GSM Sites – Generate Threats Seen and Review -> Select Endpoint -> Select Make Override Icon

Devices			File Information: APEX-PROCUREMENT				
Device Name	Last Infected	Cleanup	Filename	Pathname	Malware Group	Last Seen	Actions
APEX-WEBDESIGN	Apr 10th 2017, 15:04		WEBROOTTESTFILE.EXE	%desktop%\webrootestfile	W32.Webrootestfile	Apr 10th 2017, 11:42	
APEX-PROCUREMENT	Apr 10th 2017, 11:42		SETHASHBUSTED.EXE	%desktop%\	W32.Adware.Gen	Apr 10th 2017, 11:42	
APEX-WAREHOUSE	Apr 10th 2017, 03:07		SET.EXE	%desktop%\	W32.Adware.Gen	Apr 10th 2017, 11:42	

Site and Endpoint Level – View Blocked File -> Select Checkbox -> Create Override Button

All threats ever seen on this endpoint					
<input checked="" type="checkbox"/>	Filename	Pathname	Malware Group	Last Seen	Dwell Time
<input checked="" type="checkbox"/>	LAUNCHER.EXE	%documents%\ransim\	W32.Ransomsimul...	Dec 14th 2016, 05:52	13 Days 18 hr 32 ...

Folder Overrides

Folder overrides can only be created or configured manually through the Override policy editor. Anywhere that an undetermined application is reported, you can copy the path location where it's launching and use that directory structure for creating the override.

Manually - Overrides Tab

Explicit or dynamic directories can be configured.

New Whitelist Entry

Name / Description

Enter a name or description to help identify this entry

Override Type

MD5 Folder / File

MD5

Enter a 32 character MD5

Create Cancel

Dynamic directories are listed within the registry and no driver letter is explicitly declared.

New Whitelist Entry

Please note: File / Folder overrides will only be supported by endpoints running version 9.0.1 and higher

Name / Description

Override Type
 MD5 Folder / File

File Mask (Optional) ⓘ

Path / Folder Mask ⓘ

%AllUsersProfile%\
%CommonProgramFiles%\
%CommonProgramFiles(x86)%\
%CommonProgramW6432%\
%ProgramData%\
%ProgramFiles%\
%ProgramFiles(x86)%\
%ProgramW6432%\
%Public%\
%SystemDrive%\
%SystemRoot%\
%WinDir%\

New Whitelist Entry

Please note: File / Folder overrides will only be supported by endpoints running version 9.0.1 and higher

Name / Description

Override Type
 MDS Folder / File

File Mask (Optional) ⓘ

Path / Folder Mask ⓘ

Include Sub-folders

Detect if Malicious ⓘ

Create **Cancel**

User Interface Suggestions

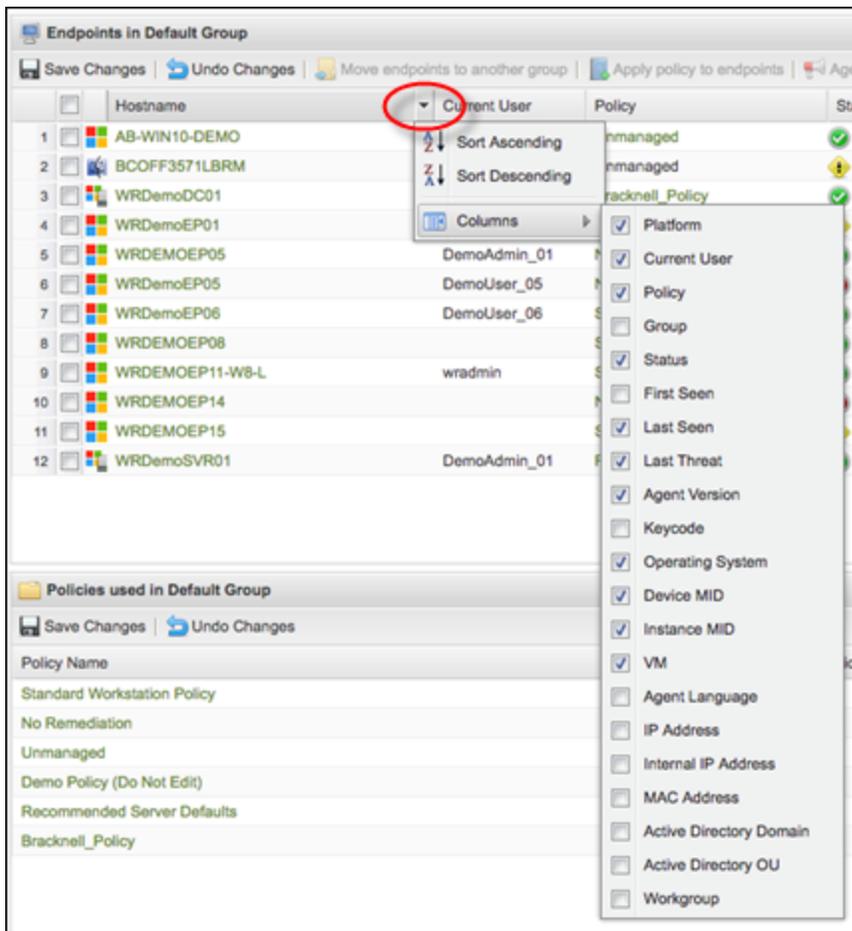
Columns

In various locations, we display information in columns. There are additional columns that are not turned On by default. We recommend that you display specific columns you're interested in by selecting the **Down** arrow next to the Current User column.

Group Management

In group management under a particular site, there are several useful columns that can be exposed by selecting the column checkbox when the list is shown.

In this example, Current User is not displayed by default. You can also turn on IP Address, Machine ID, and several other informational fields captured by the endpoint agent.



Note: Columns can be sorted and moved around based upon visual needs. Also, column settings are user based, so each user account can have different columns exposed and will persist across sessions. So, once they're turned On, they will be exposed during each management session until turned Off.

Cloud Determinations

When working with overrides, understanding what is in our central threat intelligence, or Cloud Determination, will be helpful when configuring file overrides. Turning this column On will help with initial configurations as well as on-going management of overrides.

If the determination status has the Green (Good) indicator, we recommend that you remove this local override in the GSM or Site console so as to minimize the agent's performance.

Override Name	MCS	Path Mask	File Mask	Common Filename	Common Pathname	Detect if Malicious	Determination	Last modified -	Last modified by
1	Sample with File	79C21FC26542452B...	%ProgramFiles%/*	mls.exe	WEBROOT\PLUGIN.DLL	Yes	Not Determined	Nov 8th 2016, 14:58	web@incontrol.com
2	Good file	79C21FC26542452B...	%ProgramFiles%/*	mls.exe	WEBROOT\PLUGIN.DLL	Yes	Not Determined	Nov 8th 2016, 14:58	web@incontrol.com
3	Verified file with threat	79C21FC26542452B...	%ProgramFiles%/*	mls.exe	WEBROOT\PLUGIN.DLL	Yes	Not Determined	Nov 8th 2016, 14:58	web@incontrol.com
4	My test machine	79C21FC26542452B...	%ProgramFiles%/*	mls.exe	WEBROOT\PLUGIN.DLL	Yes	Not Determined	Nov 8th 2016, 14:58	web@incontrol.com
5	Centrality	79C21FC26542452B...	%ProgramFiles%/*	mls.exe	WEBROOT\PLUGIN.DLL	Yes	Not Determined	Nov 8th 2016, 14:58	web@incontrol.com
6	test opera	79C21FC26542452B...	%ProgramFiles%/*	mls.exe	WEBROOT\PLUGIN.DLL	Yes	Not Determined	Nov 8th 2016, 14:58	web@incontrol.com
7	test opera	79C21FC26542452B...	%ProgramFiles%/*	mls.exe	WEBROOT\PLUGIN.DLL	Yes	Not Determined	Nov 8th 2016, 14:58	web@incontrol.com
8	Custom Software Alias...	79C21FC26542452B...	%ProgramFiles%/*	mls.exe	WEBROOT\PLUGIN.DLL	Yes	Not Determined	Nov 8th 2016, 14:58	web@incontrol.com
9	Custom Software Syste...	79C21FC26542452B...	%ProgramFiles%/*	mls.exe	WEBROOT\PLUGIN.DLL	Yes	Not Determined	Nov 8th 2016, 14:58	web@incontrol.com
10	Custom Software Syste...	79C21FC26542452B...	%ProgramFiles%/*	mls.exe	WEBROOT\PLUGIN.DLL	Yes	Not Determined	Nov 8th 2016, 14:58	web@incontrol.com
11	Mailx Center	79C21FC26542452B...	%ProgramFiles%/*	mls.exe	WEBROOT\PLUGIN.DLL	Yes	Not Determined	Nov 8th 2016, 14:58	web@incontrol.com
12	Mailx Center	79C21FC26542452B...	%ProgramFiles%/*	mls.exe	WEBROOT\PLUGIN.DLL	Yes	Not Determined	Nov 8th 2016, 14:58	web@incontrol.com
13	Mailx Center	79C21FC26542452B...	%ProgramFiles%/*	mls.exe	WEBROOT\PLUGIN.DLL	Yes	Not Determined	Nov 8th 2016, 14:58	web@incontrol.com
14	Mailx Center	79C21FC26542452B...	%ProgramFiles%/*	mls.exe	WEBROOT\PLUGIN.DLL	Yes	Not Determined	Nov 8th 2016, 14:58	web@incontrol.com
15	Mailx Center	79C21FC26542452B...	%ProgramFiles%/*	mls.exe	WEBROOT\PLUGIN.DLL	Yes	Not Determined	Nov 8th 2016, 14:58	web@incontrol.com
16	Mailx Center	79C21FC26542452B...	%ProgramFiles%/*	mls.exe	WEBROOT\PLUGIN.DLL	Yes	Not Determined	Nov 8th 2016, 14:58	web@incontrol.com
17	Mailx Center	79C21FC26542452B...	%ProgramFiles%/*	mls.exe	WEBROOT\PLUGIN.DLL	Yes	Not Determined	Nov 8th 2016, 14:58	web@incontrol.com
18	Mailx Center	79C21FC26542452B...	%ProgramFiles%/*	mls.exe	WEBROOT\PLUGIN.DLL	Yes	Not Determined	Nov 8th 2016, 14:58	web@incontrol.com
19	Mailx Center	79C21FC26542452B...	%ProgramFiles%/*	mls.exe	WEBROOT\PLUGIN.DLL	Yes	Not Determined	Nov 8th 2016, 14:58	web@incontrol.com
20	Mailx Center	79C21FC26542452B...	%ProgramFiles%/*	mls.exe	WEBROOT\PLUGIN.DLL	Yes	Not Determined	Nov 8th 2016, 14:58	web@incontrol.com
21	Mailx Center	79C21FC26542452B...	%ProgramFiles%/*	mls.exe	WEBROOT\PLUGIN.DLL	Yes	Not Determined	Nov 8th 2016, 14:58	web@incontrol.com
22	Mailx Center	79C21FC26542452B...	%ProgramFiles%/*	mls.exe	WEBROOT\PLUGIN.DLL	Yes	Not Determined	Nov 8th 2016, 14:58	web@incontrol.com

Chapter 2: Management Console Support

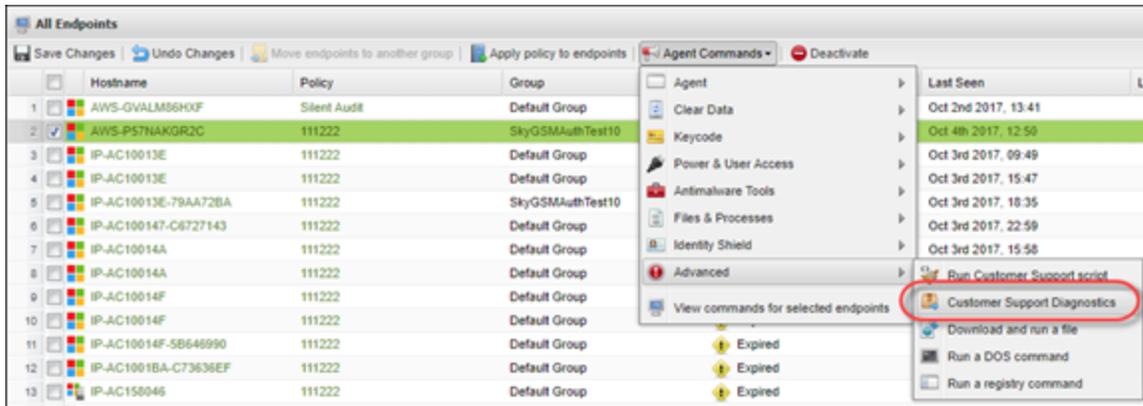
For information about support for the management console, see the following topics:

Capturing Logs	29
Tickets	30
Deployment Options	31

Capturing Logs

Rather than requiring a technician to remote access an endpoint having issues, the agent gathers a variety of logs, puts them into a zip file, and pushes them up through our backend infrastructure for a support agent's review.

Simply select the endpoint, and from the Agent Commands menu, select **Advanced > Customer Support Diagnostics**, and the agent will do the work.



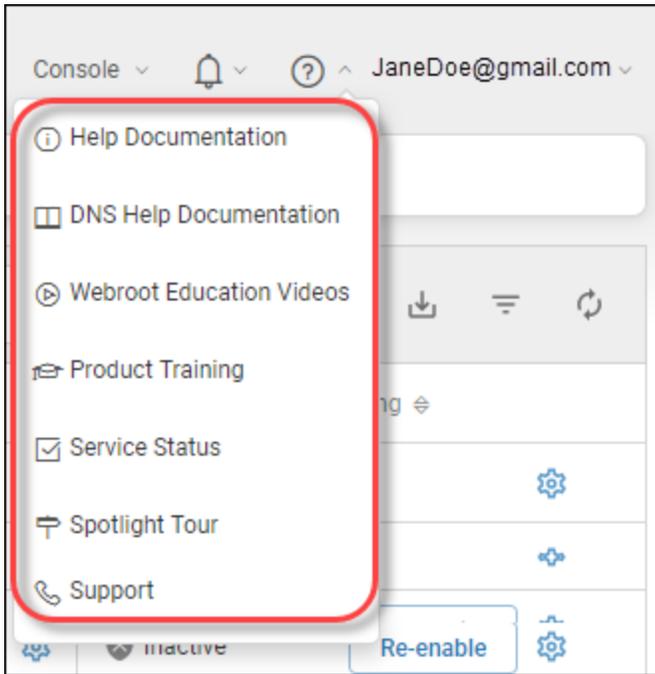
Note: The email address entered is for reference by the Webroot Support Technician. The agent or our console will not send an email when the logs are finished. This is a fairly silent activity.

The 'Customer Support Diagnostics' dialog box is shown. It has a title bar with a close button. The main area contains the following fields and options:

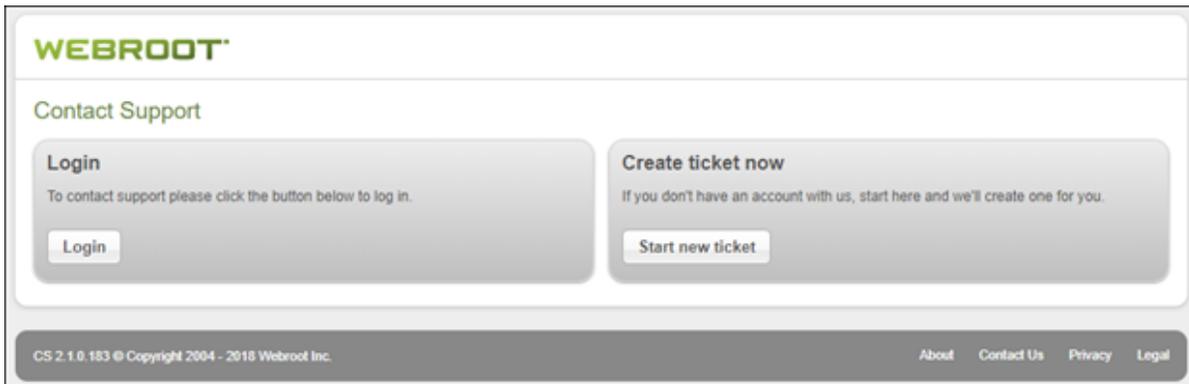
- Customer Support Diagnostics
- URL:
- Email address:
- Advanced (optional)
- Submit button
- Cancel button

Tickets

At both the management console and Site level, there is always a Support button at the top right, where a technician or admin can open a support ticket. These tickets are instantly displayed to Webroot support technicians, and are not fed into another system. The ticket system is custom built as part of the backend support system all technicians' access, and is live and dynamic.



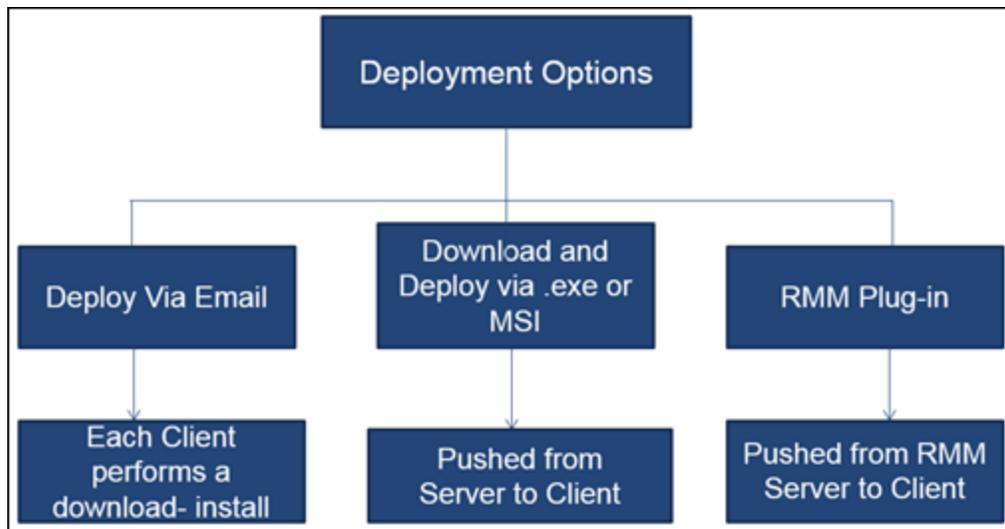
The fastest and best way to contact support is directly from within the management console. All tickets, both open and closed, are available to all administrators for review.



Deployment Options

Common deployment options for various scenarios include but not limited to the following:

- Custom Deployments via MSI and EXE:
 - RMM solutions deploy through their respective agent.:
 - GPO within Active Directory:
 - Login Scripts:
 - Third party deployment tools like: SCOM, PDQ Deploy, AutoMox
- Via Email



To support these types of installations, locate the Resource tab on the respective client site, and download the EXE or MSI, depending on installation requirements.

Management Console Best Practices Guide

The screenshot shows the 'Resources' tab in the Management Console. The 'Resources' tab is highlighted with a red circle. The page content is organized into two main sections: 'Simple Deployment Options' and 'Advanced Deployment Options: (Windows Only)'. The 'Simple Deployment Options' section explains that the easiest way to get endpoints reporting is by downloading software with a keycode. It provides a table of available keycodes and download links for Windows and Mac. The 'Advanced Deployment Options' section provides instructions for running the installer in the background from a command line and installing using MSI.

Status Policies Group Management Reports Overrides Alerts Settings Logs **Resources** Search for hostname... Advanced Search

Resources

Simple Deployment Options

The quickest and easiest way to get endpoints reporting into the console is by downloading a copy of the Webroot SecureAnywhere software which has one of your keycodes automatically applied. The user then simply needs to run the file, and their endpoint will automatically report into the console.

Your available keycodes / downloads:

XXXX-XXXX-XXXX-XXXX-XXXX	Devices Purchased: 28	Windows Download	Email template for Windows
--------------------------	-----------------------	------------------	----------------------------

Mac users can download the Webroot SecureAnywhere software from here: [Mac Download](#)

Advanced Deployment Options: (Windows Only)

Run the installer in the background from a command line

1. On the endpoint, download the Webroot SecureAnywhere installer. [Click here to download.](#)
2. Run the installer from a command line, using the commands listed in the deployment help. [Click here to view.](#)

Install using MSI

1. Download the Webroot SecureAnywhere MSI installer. [Click here to download.](#)
2. Run the installer from a command line, using the commands listed in the deployment help. [Click here to view.](#)

For further details about these deployment options, see the Deploying Webroot SecureAnywhere help guide. [Click here to view.](#)

Index

A

about
 tickets 30
access, admin 4
admin access 4
application, undetermined 19

C

capturing logs 29
cloud determinations 26
columns, user interface 25
creating new sites 2

D

default policies 6
deployment, options 31
details, site 4
determinations, cloud 26

E

entering tickets 30

F

file overrides 20
firewall policy 12
folder overrides 21

G

group management 25

L

logs, capturing 29

M

management, group 25
management, policy 6

N

new sites, creating 2

O

options, deployment 31
overrides
 file 20
 folder 21
 path 20
overrides, working with 20

P

path overrides 20
policies, default and recommendations 6
policy
 firewall 12
 polling interval 7
 potentially unwanted applications 7
 PUA 7
 scan schedule 8
 unblocking sites 10
 user interface 13
 web threat shield 9
policy management 6
polling interval policy 7
potentially unwanted application policy 7
PUA policy 7

R

recommendations for policies 6
report, undetermined 17

S

scan schedule policy 8
setup, site 3
silent audits, using 17

site details 4
site setup 3
suggestions, user interface 25

T

tickets, entering 30

U

unblocking sites policy 10
undetermined
 application 19
 report 17
user interface
 columns 25
user interface policy 13
user interface suggestions 25
using silent audits 17

W

web threat shield policy 9
working with overrides 20