

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

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
- <u>Step 2 Administration Access</u>
- <u>Step 3 Site Details</u>

Secure Anyw	eeroor ecure/Anywhere. Cosada - Q - O - Janooagaraat cor													eğgmal.com ~	
Dashboard Sites Ad	shboard Bites Admins Broops Pulicies Overrides Alerts Reports Detrings Security Awarenees Training														
SRes 4 Resds 11 Shis Accessible 11 Total												Q, Search		+	≂0 ¢
Status +	Site e									Devices a	Site Seats +	DNS Protection @		Security Awareness Training o	
Protected	Cafe Disco							Manage	Gu	11	11	Ø Active	\$	Ø Active	80
Protected	Down! The Pet 8	imporium						Manage	80	0 🔘	4	Ø Active	۲	Ø Active	\$ Ø
Protected	Haymont Tires							Manage	60	3 🗇	9	Ø Active	۲	Ø Active	* Ø
Protected Prestige Direct Sales Solutions Manuge Bu 9 ① 25									25	Ø Active	۰	S Active	\$ Ø		
2									22 Antive Devices 0 Trial Active Devices	49 Stie Seale 9 Stiel Ste Seale					

Step 1 – Site Setup

Secure Anywhere.				Console - D - S - JaneDoe&gmail.com -
Dashboard Siles Admins Groups 7	Policies Overrides Alerts Reports Settings	Security Awareness Training		
< Back Add Site				
O Details	Permissions	Endpoint Protection	O DNS Protection	Security Awareness Training
Site / Company Name ③				
Site Type ()				
Contraction Contraction Contractions				
Please select one of the following				
Company Industry (7)				
Please select one of the following				
Billing Cycle ()				
Annually				
Billing Date ③				
Jan + Tst +				
Comments ③				
Tags ()				Å
Add Tag + Add				
Next				
	# 301	Webrootine, Privacy Statement, Website Terms of Service, License Agreem	eri	

- 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 <u>Adding Sites</u>.

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.

Secure Any	where	2.								~
Dashboard Sites	Admins	Groups	Policies	Overrides	Alerts	Reports	Settings	Security Awareness Training		
Summary Details Permi	ression	Pro	tected	otection Secu	rity Awaren	ess Training	Downloads			
Admin							(🔿 Admin	O View Only	O No Access
								 Admin 	O View Only	O No Access
								 Admin 	View Only	O No Access
								 Admin 	O View Only	O No Access

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 <u>Updating Site Admin Permissions</u>.

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 <u>Recommended</u> <u>Defaults</u>.
- 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.

SecureAn	ywher	e.									 ¢~ ⊙~
Dashboard Sites	Admins	Groups	Policies	Overrides	Alerts	Reports	Settings	Security Awareness Training			
< Back Add Sit	e										
	0									0	0
	Details				Permiss	ions		Endpoint Protectio	ion	DNS Protection	Security Awareness Training
C Endpoint Protection	i is required to t	itial or purch	ane any of We	broofs addition	al products	and services	including DN	S Protection and Security Awareness Trai	aining.		
Keycode Type 💿											
⊙ Full ◯ 30 day trial											
Site Seats ①											
Detault Endpoint Policy (D										
Recommended Defaults											-
Report Distribution List	0										
cpitzgwebroot.com											
Include Global Polici	m7 📥										
Include Global Overs	des? 🛆										
Data Filler 🛞											
Inherit the GSM data filts	r setting										
Previces 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 indepth explanation will focus on recommended changes to policies for user endpoints, not servers.

- Polling Interval
- Potentially Unwanted Applications (PUAs)
- <u>Scan Schedule</u>
- 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.

lame	
Workstation Defaults	
escription	
Copy of the Recommended Defaults Policy	
olicy Section	
Basic Configuration	
Setting	
Favor low disk usage over verbose logging (fewer details stored in logs)	🛈 Off 🔾 On
🙀 Lower resource usage when intensive applications or games are detected	🔾 Off 💿 On
K Allow SecureAnywhere to be shut down manually	💿 Off 🔾 On
Force non-critical notifications into the background	🔿 Off 💿 On
Fade out warning messages automatically	🔿 Off 💿 On
Store Execution History details	🔿 Off 💿 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.

Management Console Best Practices Guide

Server Defaults										
Name										
Server Defaults										
Description										
Copy of the Recommended Server Defaults Policy	Copy of the Recommended Server Defaults Policy									
Policy Section										
Scan Settings	-									
Setting	4	•								
Automatically reboot during cleanup without prompting	⊙ Off ◯ On									
Never reboot during malware cleanup	⊙ Off ◯ On									
Automatically remove threats found during background scans	🔿 Off 💿 On									
Automatically remove threats found on the learning scan	⊙ Off ◯ On									
Enable Enhanced Support	🔾 Off 💿 On									
Show Infected Scan Results	⊙ Off ◯ On									
Detect Possibly Unwanted Applications (PUAs) as malicious	⊖ Off ⊙ On	r.								
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	Off 💿 On
Hide the scan progress window during scheduled scans	⊖ Off ⊙ On
Only notify me if an infection is found during a scheduled scan	🔿 Off 💿 On
Do not perform scheduled scans when on battery power	⊖ Off ⊙ On
Do not perform scheduled scans when a full screen application or game is open	⊙ 0ff ◯ 0n
Randomize the time of scheduled scans up to one hour for distributed scanning	○ 0ff ⊙ 0n
Perform a scheduled Quick Scan instead of a Deep Scan	⊙ Off ◯ 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		*
octang		
Enable Web Shield	🔾 Off 💿 On	
Activate browser extensions	🔾 Off 💿 On	
Block malicious websites	🔿 Off 💿 On	
Enable realtime anti-phishing	🔿 Off 💿 On	
📫 Show safety ratings when using search engines	🔾 Off 💿 On	
Enable web filtering driver	🔾 Off 💿 On	
Suppress the user's ability to bypass blocked websites	🔿 Off 💿 On	$\mathbf{)}$.
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.

Secur	Secure Anywhere.											
Dashboard	Sites	Admins	Groups	Policies	Overrides	Alerts	Reports	Settings	Security Awareness Training			
File Whitelist F	ile Blacklis	t Web Block	k / Allow List	Web Block	Page Settings							
	Drag an image file or click here to upload your logo											
	Website not allowed											
					The	catego	ry <categ< th=""><th>ory> is re</th><th>stricted.</th><th></th><th></th><th></th></categ<>	ory> is re	stricted.			
			Your or	ganizatior	n's Interne	t usage	policy re	stricts acc	ess to this website at	this time.		
		в /	Ξ	ΞΞ	≡ .	٩.						
	Please contact your network administrator if you have any questions. Submit a request to review category here											

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.

Serve	er Defaults									
Name	e									
Sen	ver Defaults									
Desc	Description									
Сор	by of the Recommended Server Defaults Policy									
Polic	y Section									
Fire	wall	*								
	Setting									
	Enabled	⊖ Off ⊙ On								
	Firewall level	Warn unknown and infected 👻								
	Show firewall management warnings	⊙ Off ◯ On								
	Show firewall process warnings	⊙ Off ◯ On								
Sav	re l									
Polic; Fire	y Section wall Setting Enabled Firewall level Show firewall management warnings Show firewall process warnings	 Off ⊙ On Warn unknown and infected ▼ Off ○ On Off ○ On Off ○ On 								

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

Management Console Best Practices Guide



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.

Secur	eAn	ywhe	ere.						
Dashboard	Sites	Admins	Groups	Policies	Overrides	Alerts	Reports	Settings	
Endpoint DN	S								
🕀 Add	🗋 Сору	× Delet	e						
Policies							Selec	t a policy to y	iew its settings
A Recommen	nded Defa	ults						a ponej to i	ien no oettingo
A Recomme	nded DNS	Enabled							
A Recommen	t	er Defaults							

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.

Secure Anywhere	0		
Home Endpoint Protection Admin	s (Downloads	
Status Policies Group Management	Rep	orts Overrides Alerts Settings Lo	ogs Resources
Select your report	End	points with undetermined software on las	st scan (Apr 02 09:55) 🗵
Report Type:	🔥 E	indpoints with Undetermined Software	
Endpoints with undetermined soft 💙		Hostname	Policy
All Threats Seen	1	AWS-GVALM86HXF	Silent Audit View
All Undetermined Software Seen	2	AWS-P57NAKGR2C	111222 View
All URLs Blocked	3	IP-AC10013E	111222 View
Endpointe with throate on last ccan	4	IP-AC10013E-79AA72BA	111222 View
Endpoints with undetermined soft)	5	IP-AC100147-C6727143	111222 View
Threat History (Daily)	6	IP-AC10014A	111222 View
Threat History (Collated)	7	IP-AC10014A	111222 View
Blocked URL History (Daily)	8	IP-AC10014F	111222 View
Agent Version Spread	9	IP-AC1001BA-C73636EF	111222 View
Agents Installed			

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.

Report Type: @ Endpoints anth Understands forhume Endpoints with understands for the set of the set	
Reget Traje: Endpoints with Moderninand Software Endpoints with windowning (with) Printy Orage Bidan Last Seen	
Report Type: Independent with Understanded Galbauer Endpoints with understand Galbauer Product with Understand Galbauer Endpoints with understand Galbauer Product with Understand Galbauer Index and with and the set of the set	
Argust Type © Endpoints with Undetermined Software Endpoints with undetermined soft as Medicance Endpoints with undetermined soft as Medicance I holds flact-out and hole 1 and Software I holds flact-out and hole 2 and Software(000 million) See Land Software 5 and Software(000 million)	
Angen Tope @ Endpoints with Undetermined Software Endpoints with undetermined soft yr Maximum Pality Droug State Last Seen Last Thread	
Asport Type 🔒 Endpoints with Undetonised Suffware	
2 federal year report () Talquarts with addressment withwards as (pr 0.001) ²	
State Address Grag Nangareet Regards Counties Advis Setting Laps Resources	G, Advanced Sear

Note: For more information, see <u>Generating Endpoints With Undetermined Software on Last Scan</u> 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.

RANSIMDLL.	DLL WRDEMOEP14					? X
Propagation Tir	meline			File Information		Treate override
				Determination:	Undetermined	
			6	Global Popularity:		
	6		T	Console Popularity:	and t	
	T			Filename:	RANSIMDLL.DLL	
	6			MD5:	7CECC603850EB123E	34F38492E518236
FS				Pathname:	%documents%\ransim\	
HONE TO THE HONE T	and work and a state of the state of	e3210 De5210 De12	to of 19 2910 of 12 2910 of 14 2910	File Size:	498.5 KB	
	E First Seen	Last Seen 😥 Date	Determined	Endpoints encour	ntering this file	
				WRDEMOEP14	Dec 14 201	6, 5:52
Perspective	First Seen	Last Seen	Dwell Time			
🔁 📕 Globally	Nov 25 2016, 6:03					
🔁 📕 Console	Nov 30 2016, 11:20	Dec 14 2016, 5:52				
🕑 📕 Endpoint	Nov 30 2016, 11:20	Dec 14 2016, 5:52	13 day 18 hr 32 min 45 sec			
			OK		, E	adpoint <i>Forensics</i>

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	?	×
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		

Devices needing attention (Now)	Apex Technology						
Devices			File Information: APEX-PROCUREMENT				
Device Name	Last Infected	Cleanup	Filename	Pathname	Malware Group	Last Seen	Actions
APEX-WEBDESIGN	Apr 10th 2017, 15:04	4	WEBROOTTESTFILE.EXE	%desktop%/webroottestfile/	W32.Webroottestfile	Apr 10th 2017, 11:42	
APEX-PROCUREMENT	Apr 10th 2017, 11:42	-	SETHASHBUSTED.EXE	%desktop%l	W32.Adware.Gen	Apr 10th 2017, 11:42	3 2
APEX-WAREHOUSE	Apr 10th 2017, 03:07	4	SET.EXE	%desktop%l	W32.Adware.Gen	Apr 10h 2017, 11:42	6 2

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

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

	i All	thr	eats ever seen on thi	is endpoint			BOX
G	Cr	reat	e override 📑 Show a	II PCS which have encountere	d this file 📑 Restore from	n Quarantine	
	-	V	Filename	Pathname	Malware Group	Last Seen	Dwell Time
	1		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		

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

New Whitelist Entry	?	×
(i) Please note: File / Folder overrides will only be supported by endpoints running version 9.0.1 and higher		
Name / Description		
Enter a name or description to help identify this entry		
Override Type		
MD5 📀 Folder / File		
File Mask (Optional)		0
e.g. notepad.exe		
Path / Folder Mask		0
%		
%AllUsersProfile%\ %CommonProgramFiles%\ %CommonProgramFiles(x86)%\ %CommonProgramW6432%\ %ProgramData%\ %ProgramFiles(x86)%\ %ProgramW6432%\ %Public%\ %SystemDrive%\ %SystemDrive%\ %SystemDrive%\ %WinDir%\ Create Cancel		Þ

New Whitelist Entry	?	×
() Please note: File / Folder overrides will only be supported by endpoints running version 9.0.1 and higher		
Name / Description		
Enter a name or description to help identify this entry		
Override Type		
MD5 • Folder / File		
File Mask (Optional)		0
e.g. notepad.exe		
Path / Folder Mask		0
%AllUsersProfile%\		
Include Sub-folders		
Detect if Malicious		0
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.

	Hostname	Current User	Polic	·	St
1	AB-WIN10-DEMO	1 Sort Ascending	nma	anaged	0
2	BCOFF3571LBRM	Z Sed Deconding	nma	anaged	
3 🔳 💐	WRDemoDC01	A+ son bescending	raci	mell_Policy	0
4	WRDemoEP01	Columns		Platform	
5	WRDEMOEP05	DemoAdmin_01		Current User	
6	WRDemoEP05	DemoUser_05		Policy	
7 🔳 🚦	WRDemoEP06	DemoUser_06	1	Group	-)
8	WRDEMOEP08			Group	
9	WRDEMOEP11-W8-L	wradmin	<u>د</u>	Status	
10 🔳 📑	WRDEMOEP14		, 🖻	First Seen	
11 🔳 📑	WRDEMOEP15		5 🔽	Last Seen	
12 🕅 💐	WRDemoSVR01	DemoAdmin_01	F 🔽	Last Threat	
				Agent Version	
				Keycode	
				Operating System	
Policies	used in Default Group			Device MID	
100000				Device MID	
a save Ch	anges 🔁 Undo Changes		V	Instance MID	
olicy Name)			VM	
tandard W	orkstation Policy			Agent Language	
o Remedia	ation			IP Address	
nmanaged				Internal IP Address	
emo Policy	y (Do Not Edit)			MAC Address	
ecomment	ded Server Defaults			Active Directory Domain	
racknell_P	olicy			Active Directory Domain	
				Active Directory OU	

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.

Datus	Policies Group Managem	ert Reports Overrides	Alerta Betlings L	ogs Resources						Search for hostnam
Whitefal	Backlet									
Whitefall										
O Create	Ovinia 🕤 Import									Filter by Policy
	Override Name	MD5	Path Mask	File Mask	Common Filename	Common Pathname	Detect if Malicious	Determination	Last modified +	Last modified by
1 []	Sample with File		SProgramFiles(x06(%))	mahware.exe			Yes	NA	Nov 8th 2016, 14:58	webrockonsole@gmail.
10	Good file	796001/1028545245828			WEBROOTPLUGIN DLL	Titworkingmaphetripec		Undetermined	Nov 8th 2016, 11:24	webroctonacie@gnal
10	Verified file with threat	75090345C724ECD5/E			(01506882-8A40-4740	Sapplata/Vinicrosoftwi.		Bell	Oct 27th 2016, 12:40	webroctoneole@gnal
4 🖂	My test machine		SProgramFiles)dd(Nig	12			No	NA	Aug 24th 2016, 09.11	aconper@webrootsalead.
100	Centraetage		SprogramfieeVcentrast.				No	NA	Jul 28th 2018, 10-48	aconper@webrochaiesd.
• [2]	test opera	73COMBA3DA7FCSFBA.			OPERA.EXE.NEW	NampNopers autoupd		Undetermined	May 27th 2016, 04:49	SGrangwebrox.com
10	test opera	809985768AA87A8C8F			OPERA.EXE.NEW	KerpNopes autoupd		Undetermined	May 27th 2016, 04.49	5Grangwebrox.com
	Custom Software Absolu		C/CustomSoftware/Dire				No	NA	Jul 280-2015, 10:57	khamison@webroot.com
	Custom Software Byste		MPogan/leeNCuto				No	NA	Jul 28th 2015, 10:56	khanlasn@webrool.com
1000	Contern Deliver a Concer-	PRECOMPLEXITING.						- C	AV 280-2112, 1241	A REAL PROPERTY.
0	Media Center	GABC32A5147A708880			MICROSOFT MEDIACE.	Nassambly%).		Good	May 27th 2015, 11.11	broweli@webroot.com
of Lat.		WHERE A PRODUCT OF CE			CORE EXE	PROPERTY OF A STREET, SALES		0.00	002002014 1420	N IS NO GROUP TO LOSS
0	à	800534E46882F70870			OPERA_1216_INT_SET	%cache%/		Geod	May 8th 2014, 1849	BLee-Price@webroot.com
H []	à	FF825F4A81080608EE						Geod	Oct 15th 2013, 04:22	jinclaughtin@webroot.com
4 []	à	1A0251835F43134F086			WSASME.SFX.EXE	%desktop%i		Good	Mar 7th 2013, 20:40	shalework@webroot.com
4 []	a de la companya de la	24/54/642E2E7148788			XLCONV2007 #826673	SpogranflerNirumara.		Undetermined	Nov 15th 2012, 12:04	khamleon@webroot.com
9 🖂	h i i i i i i i i i i i i i i i i i i i	\$379C320A30F0E6AD8			NOP205P2 #82729450	SpogramfierVirumara.		Good	Nov 15th 2012, 12:04	khamison@webroot.com
10	1	40061873C2/A6832C8			NDP205P2 #82729450	SpogranfierVirunera.		Good	Nov 15th 2012, 12:04	khamlaon@webroot.com
19 [1]	a	7960601948250487820			EXCEL2007-K82687307	SpogranfierVirunera.		Undetermined	Nov 15th 2012, 12:04	khamison@webroot.com
20	1	D1C1AE40068DA8874			EXCEL2007-482087307	SpogranfierNirumara.		Undetermined	Nov 15th 2012, 12:04	khamison@webroot.com
21 []	h i	6453E7840000065A77			EXCEL2007-480487307	SpogranfierNirumara.		Undetermined	Nov 15th 2012, 12:04	Khamison@webroot.com
22	1	BAD?40081027YAE757			XLCONV20074826673	SpogramfierNirumana.		Undetermined	Nov 15th 2012, 12:04	khamison@webroot.com
() inform	ation									

Chapter 2: Management Console Support

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

Capturing Logs	
Tickets	
Deployment Options	

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.

5	All Endp	points					
	ave Ch	anges 눌 Undo Changes 🚪	Move endpoints to another group	Apply policy to endpoints	📢 Agent Commands 🔹 🤤 Deactivate		
		Hostname	Policy	Group	Agent	Þ	Last Seen La
1		AWS-GVALM86HXF	Silent Audit	Default Group	🙆 Clear Data	Þ	Oct 2nd 2017, 13:41
2		AWS-P57NAKGR2C	111222	SkyGSMAuthTest10	Keycode	Þ	Oct 4th 2017, 12:50
3		IP-AC10013E	111222	Default Group	Power & User Access	Þ	Oct 3rd 2017, 09:49
- 4		IP-AC10013E	111222	Default Group	💼 Antimakuana Tanin		Oct 3rd 2017, 15:47
5		IP-AC10013E-79AA72BA	111222	SkyGSMAuthTest10	Characterization in the second	1	Oct 3rd 2017, 18:35
0		IP-AC100147-C6727143	111222	Default Group	Files & Processes	P.	Oct 3rd 2017, 22:59
7		IP-AC10014A	111222	Default Group	Identity Shield	÷	Oct 3rd 2017, 15:58
		IP-AC10014A	111222	Default Group	Advanced	Þ	Run Customer Support script
		IP-AC10014F	111222	Default Group	Manual and the selected as desired.	(Customer Support Diagnostics
10		IP-AC10014F	111222	Default Group	wew commands for selected endpoints		Download and run a file
11		IP-AC10014F-58646990	111222	Default Group	Expired		
12	0	IP-AC1001BA-C73636EF	111222	Default Group	Expired		Run a DOS command
13		IP-AC158046	111222	Default Group	🔹 Expired		Run a registry command

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.

Customer Support Diagno	stics
URL:	http://download.webroot.com/wsablogs.exe
Email address:	scooper@webrootsalesdemo.com
- Advanced (optiona)

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.

Console 🗸 🎝 🗸 🍞 🏠	JaneDoe@gmail.com ~
(i) Help Documentation	
DNS Help Documentation	
	ψ÷φ
₁⇔ Product Training	
Service Status	
🕆 Spotlight Tour	57 40
🗞 Support	
🖏 🐨 macuve	Re-enable

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.

WEBROOT	
Contact Support	
Login To contact support please click the button below to log in. Login	Create ticket now If you don't have an account with us, start here and we'll create one for you. Start new ticket
CS 2.1.0.183 @ Copyright 2004 - 2018 Webroot Inc.	About Contact Us Privacy Legal

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

Status Policies Group Management Reports Overrides Alerts Settings Logs Resources
A 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 kaypooles / downloads; XXXX.XXXX.XXXX Devices Purchased 28 Windows Download Imail template for Windows Mac users can download the Webroot BeoursAnywhere software from here: Imail template for Windows
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. Hun be resulter hom a command line, using the commands listed in the depoyment, nept. Unick new to view.
Download the Webroot SecureAnywhere MSI installer. Click here to download. 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

С

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

Е

entering tickets 30

F

file overrides 20 firewall policy 12 folder overrides 21

G

group management 25

L

logs, capturing 29

М

management, group 25 management, policy 6

N

new sites, creating 2

0

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

Р

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

\mathbf{S}

scan schedule policy 8 setup, site 3 silent audits, using 17 site details 4 site setup 3 suggestions, user interface 25

Т

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