Secure Anywhere. Business — Mobile Protection

Administrator's Guide

Copyright

SecureAnywhere Mobile Protection Administrator's Guide

November, 2012

© 2012 Webroot Software, Inc. All rights reserved. Webroot is a registered trademark and SecureAnywhere is a trademark of Webroot Software, Inc. All other product and company names mentioned may be trademarks or registered trademarks of their respective owners.

Table of Contents

Getting Started	1
Creating an account	2
Logging in to Mobile Protection	3
Adding a keycode to your account	4
Installing the Apple MDM certificate	5
Managing accounts	7
Viewing account status	8
Managing keycodes	10
Managing devices	11
Viewing details for all devices	12
Viewing status of a device	13
Scanning a device	15
Forcing updates to a device	17
Viewing the history of a device	19
Sending Android devices Lost Device Protection commands	
Sending Apple (iOS) devices Lost Device Protection commands	24
Changing settings for an Android device	
Adding a device to your account	
Managing alerts	
Configuring alert notifications	34
Managing alert subscriptions	
Managing users	
Managing users	40
Managing users	40
Managing users	40 41 42
Managing users	40 41 42 45
Managing users Importing users into your account Adding new users Managing user data Generating reports Viewing Inventory Management reports	40 41 42 45 46
Managing users Importing users into your account Adding new users Managing user data Generating reports Viewing Inventory Management reports Viewing Device Status reports	40 41 42 45 46 48
Managing users Importing users into your account Adding new users Managing user data Generating reports Viewing Inventory Management reports Viewing Device Status reports Viewing Alerts and Infections reports	40 41 42 45 46 48 50

Refreshing the report data	. 53
Exporting report results to a CSV file	. 54
Index	55

Getting Started

Webroot[®] SecureAnywhere[™] Business – Mobile Protection secures devices from malware, malicious websites and application hijacks. Leveraging the cloud, it protects both corporate and user data against accidental loss or theft. Mobile Protection does not require on-premise management hardware or software. Administration is delivered by the Webroot SecureAnywhere Business website, dramatically simplifying management of mobile devices, PCs, and network server endpoints through a unified experience.

To get started with SecureAnywhere Mobile Protection:

- Create a Webroot account and log in. See "Creating an account" on page 2 and "Logging in to Mobile Protection" on page 3.
 If you already have a Webroot account, you must add the Mobile Protection keycode to your account. See "Adding a keycode to your account" on page 4.
- 2. Add devices to your account. See "Adding a device to your account" on page 30.
- 3. If you have Apple devices, be sure to first install the Apple MDM certificate. See "Installing the Apple MDM certificate" on page 5.
- 4. Configure alerts to notify you when a device needs attention. See "Configuring alert notifications" on page 34.
- 5. Add users to your account. See "Importing users into your account" on page 40 and "Adding new users" on page 41.

Creating an account

By creating a Webroot account, you can view the overall security status of your devices in the SecureAnywhere website. This site shows if your devices are secure, infected, or require administrative attention. If you already have a Webroot account, see "Adding a keycode to your account" on page 4.

To create an account:

- 1. On the Webroot SecureAnywhere website: my.webrootanywhere.com.
- 2. Click Sign up now in the Create an account panel.

Becure Anywhere.	
Log in	Create an account
Email Address Password Log in Can't log in?	Security & Convenience Creating an account helps you manage your security across multiple devices, with any Webroot product. It also makes it easy to add new devices and help other people protect theirs. Sign up now

3. Complete the registration information in the Create an account panel.

4. Click Register Now.

SecureAnywhere sends a confirmation message to the email address you specified.

- Open your email application. Click the link in the confirmation email message to open the Confirm Registration page.
 SecureAnywhere requests two randomly selected characters of the security code you specified when you created the account.
- 6. Type the two requested characters of your security code and click Confirm Registration Now.

Logging in to Mobile Protection

After you create a Webroot account, log in to the SecureAnywhere website to view information about your account.

To log in to Mobile Protection:

- 1. On the Webroot SecureAnywhere website: my.webrootanywhere.com.
- 2. Enter the email address and password you specified when you registered. Your email address is your user name for the account.

Tip: If you forget your password or security code, click the *Can't log in*? link, then click **I forgot my password** or **I forgot my security code**. SecureAnywhere prompts you to enter your email address, and sends you an email message containing a link for resetting your login information.

- 3. Click Log in.
- 4. Type the requested characters of your security code, and click Login to view your account.

Adding a keycode to your account

If you already have a Webroot account, add the keycode you received when you purchased Mobile Protection.

To add a keycode to your account:

- 1. Log in to the SecureAnywhere website.
- 2. Open the drop-down menu in the upper right corner, and click Manage Keycodes.



3. Click Add Product Keycode.

Secure Anywhere.				
Home	PC Security	Mobile Security		
Manage	e Keycodes			
Add Pro	duct Keycode)		

4. Type the keycode into the **Product Keycode** field and click **Add**.

Installing the Apple MDM certificate

Before you enroll Apple devices in Mobile Protection, you must load an Apple Mobile Device Management (MDM) certificate. If the MDM certificate is not imported into Webroot's Mobile Protection, the Lost Device Protection commands will not work properly on Apple devices.

To install the Apple MDM certificate:

- 1. Log in to the SecureAnywhere website.
- 2. Open the drop-down menu in the upper right corner, and click **Mobile Protection Settings**. (You may also see a yellow warning message on the main dashboard that instructs you to install the MDM certificate. If you see this message, you can also click the **Set up iOS Management** button to begin.)



3. Follow the steps in the Mobile Protection Settings dialog to create and download the certificate:

Mobile Protection Settings				
iOS Device Management Certificate				
To create this iOS device management SSL certificate:				
1. Download the certificate signing request (CSR) file: Download Download				
2. Sign in with your Apple ID at identity.apple.com/pushcert/				
3. Click "Create a Certificate" or "Renew", and upload the CSR file that you downloaded in Step 1.				
4. Download the certificate from the Apple website.				
5. Upload the certificate file that you downloaded in Step 4:				
Browse				
For more information about certificates and mobile device management, go to www.apple.com/iphone/business/integration/mdm/				
Save Cancel				

4. When you're done, be sure to click the Save button.

Managing accounts

To manage your Mobile Protection account, see the following topics:

Viewing account status	8
Managing keycodes	10

Viewing account status

From the Status page, you can see an overview of all your managed devices in one quick glance.

To view your account status:

- 1. Log in to the SecureAnywhere website, then click Mobile Protection (or Go to Mobile Protection).
- 2. Make sure the Status tab is selected.

Secure Anywhere.				user@fakemail.c	om 🝷
Home Endpoint Protection Mobil	e Protection				
Status Devices Users Reports	1				_
Status Snapshot	Devices Needing Attention		8	Account Snapshot	
· · · · ·	* Device Owner	Device Type	Alert Summary	Seats used: 115 of 50/	0
Vulnerable	650	Android Tablet	Threats detected	Earliest expiration: 364 days	
113 Devices Protected 5 Infected	😧 Kam	Android Phone	Threats detected	Manage Licenses	
8 Need Attention	0 MMM	Android Phone	Threats detected		
	O SM	Android Phone	Threats detected	Reports	
	MMM2	Android Phone	Threats detected	Protocol and a finite of	
	😝 Dj	Android Phone	Multiple alert conditions	URL Filtering	
	😝 GSD	Android Phone	Insecure option enabled: Unknown Sources	Devices Needing Attention	
	😛 Major	Android Phone	Multiple alert conditions		
	😛 Shine	Android Phone	Multiple alert conditions	Help and Support	
	😛 joan	Android Phone	Multiple alert conditions	map and support	
	😧 Driver	Android Phone	Multiple alert conditions	Getting Started Guide Administrator Guide	
	😛 pam	Android Phone	Multiple alert conditions	Support	
Device Activity Snapshot	😣 Mori	Android Phone	Multiple alert conditions		
Last 24 Hours 💌	-			News and Updates	
Seen: 8 Not Seen: 105 Total: 113				Latest Threats News from Webroot	

The Status page is divided into the following panels:

- The **Status Snapshot** panel shows the number of devices that are secure, infected, or otherwise needing attention.
- The **Device Activity Snapshot** panel shows the number of devices that have connected to Mobile Protection. It also shows the number of devices that are registered, but have not checked into the website.
- The **Devices Needing Attention** panel lists any vulnerable devices. Double-click a device entry to see a detailed view.

- The Account Snapshot panel shows the number of licenses used in your account, the total licenses available, and the number of days before the earliest license expires. Click Manage Licenses to update license keycodes. See "Managing keycodes" on page 10.
- The **Reports** panel provides quick access to reports for high-level statistics.
- Help and Support opens Webroot's publications and Technical Support.
- News and Updates opens the Webroot Threat Blog and the Webroot Press Room.

Managing keycodes

A keycode is the license number for a purchased Webroot product. As the SecureAnywhere administrator, you can view existing keycodes and add new ones.

To view license keycodes:

- 1. Log in to the SecureAnywhere website, then click Mobile Protection (or Go to Mobile Protection).
- 2. From the Account Snapshot panel, click **Manage Licenses**. (You can also open the drop-down Mobile Protection menu and click **Manage Keycodes**.)

Account Snapshot		\$
Seats used: Earliest expiration:	136 of 500 347 days	
Manage Licenses		

The list shows your keycodes and their affiliated product editions, the number of devices for each keycode, and the number of days remaining on each license.

Manage Keycodes					
Add Product Keycode				Buy a K	eycode now
Keycode	Edition	Devices	Days Remaining	Renew	Upgrade
SA32-TEST	Endpoint Protection	100	348 (Jun 22 2013)	Renew	Upgrade
ADE5-TEST	Mobile Protection	500	347 (Jun 22 2013)	Renew	Upgrade

From here, you can:

- Click Add Product Keycode (upper left button) to include new mobile licenses.
- Click **Buy a Keycode now** (upper right button) to go to the Webroot home page and purchase a new keycode.
- Click the **Renew** link under the Renew column to extend the time limit on the license.
- Click the Upgrade link under the Upgrade column to purchase additional mobile protection.

Managing devices

To manage devices, see the following topics:

Viewing details for all devices	12
Viewing status of a device	13
Scanning a device	15
Forcing updates to a device	17
Viewing the history of a device	19
Sending Android devices Lost Device Protection commands	21
Sending Apple (iOS) devices Lost Device Protection commands	24
Changing settings for an Android device	26
Adding a device to your account	30

Viewing details for all devices

From the Devices page, you can view a summary of each Android or iOS device managed in your account.

To view all devices:

- 1. Log in to the SecureAnywhere website, then click Mobile Protection (or Go to Mobile Protection).
- 2. Click the **Devices** tab.



3. From the Devices panel, double-click on a device entry to open more details. For more information, see "Viewing status of a device" on page 13.

Viewing status of a device

From the Devices page, you can access status details about an individual device. For example, if a yellow or red status icon appears next to the device name, you can view exactly what issues are associated with it.

To view the status of a device:

- 1. Log in to the SecureAnywhere website, then click Mobile Protection (or Go to Mobile Protection).
- 2. Click the **Devices** tab.



3. From the Devices panel, double-click on the device.

Home	E	ndpoint	t Protecti	ion	Mobile F	Protection	۱.
Status	D	evices	Users	Repor	rts		
havices							
Devices	a Devi	ce 🖨		vice 🕕			
Devices	a Devi	ce 🤤 User En	Delete Dev nail	rice 🕒	Resend	Enrollment	: Invite Name

4. In the next panel, make sure the **Security Status** tab is selected at the top.

The middle panel provides more information about the device status.

evice Details		2
Jolie Gallagher's Android Phor	e	LGE LS670 Android 2.3 Added Oct 19 2012 12:03 Last check in Nov 1 2012 09:58
Security Status History Lost Device Protection	Device Settings	
Webroot SecureAnywhere Det SecureAnywhere Mobile version: 3.0.0.4084 Security definitions version: 378 Last security scan: Oct 29 2012 18:29	ails	Scan Now Force Definitions Update
The device is experiencing the following pro 1 threat(s) found on the device Malware was detected on this device. The user should run th	blems: e Webroot client and select Remove All to clean the infect	ion.
	Close	

5. From this panel, you can resolve some issues by running a scan (click the **Scan Now** button in the upper right corner) or forcing a definitions update (click the **Force Definitions Update** button in the upper right corner).

Note: Only devices running SecureAnywhere Mobile version 3.0 and above show the Scan Now and Force Definitions Updates buttons.

You can also use the tabs at the top of the panel to check the following information:

- History. See "Viewing the history of a device" on page 19.
- Lost Device Protection. See "Sending Android devices Lost Device Protection commands" on page 21 or "Sending Apple (iOS) devices Lost Device Protection commands" on page 24.
- Device Settings. See "Changing settings for an Android device" on page 26. Note: Apple (iOS) devices do not include the Device Settings tab.

Scanning a device

From the Devices page, you can run a remote scan on a device.

To scan a device:

- 1. Log in to the SecureAnywhere website, then click Mobile Protection (or Go to Mobile Protection).
- 2. Click the **Devices** tab.



3. From the Devices panel, double-click on the device you want.

Home	E	ndpoint Pr	otection	м	obile	Protec	ction	
Status	D	evices U	Isers	Report	5			
evices	a Devi	ce 🤤 Dele		B R				
Add a	a Devi	ce 😑 Dele User Email	te Device	🕒 R	esen (i Enrolir	ment Ir Last Na	ivite me

4. In the next panel, make sure the Security Status tab is selected at the top.

5. Click the Scan Now button in the upper right corner.



Note: Only devices running SecureAnywhere Mobile version 3.0 and above show the Scan Now button.

Forcing updates to a device

From the Devices page, you can push updated threat definitions to a device.

To push updates to a device:

- 1. Log in to the SecureAnywhere website, then click Mobile Protection (or Go to Mobile Protection).
- 2. Click the **Devices** tab.



3. From the devices panel, double-click on a device entry to open more details.

Add 🧧	•	User Em	nail	First N	ame	Last	Name
Add a							
	a Devi	ce 😑 i		ice 🕒			
evices							
itatus	D	evices	Users	Repor	rts		
		napoint	Protocol		NOUNC	FIOLOGUO	<u> </u>
	E	ndpoint	Protecti	on 🗾	lobile	Protection	

4. In the next panel, make sure the Security Status tab is selected at the top.

5. Click the Force Definitions Update button in the upper right corner.

Webroot	SecureAnywhere Det	ails	Scan Now
SecureAnywhere	Mobile version: 3.0.0.4084		
Security definition	ns version: 309		Force Definitions Update
Last security scar	n: Oct 8 2012 23:42		
При ты	is device needs attention		
	is device needs attendon		
The The	device is experiencing the following pro	blems:	
		Close	

Note: Only devices running SecureAnywhere Mobile version 3.0 and above show the **Force Definitions Update** button.

Viewing the history of a device

From the Devices page, you can view a history of security activity on each device.

To view the history of a device:

- 1. Log in to the SecureAnywhere website, then click Mobile Protection (or Go to Mobile Protection).
- 2. Click the **Devices** tab.



3. From the Devices panel, double-click on the device.

Home	E	ndpoin	t Protecti	on	Mobile	Protection	
Status	De	vices	Users	Repo	rts		
Devices							
Devices	a Devic	ie 😑		ice 🕒			
Devices	Devic	:e 😑 User Er	Delete Dev mail	fice 🕒 First N	Resend	Enroliment I	nvite ame

4. In the next panel, click the **History** tab.

The History tab shows activity on the device, such as a completed scan or a quarantined threat. The page also shows activity date and description.

Administrator's Guide

Security Status	History	Lost Device Prote	ection	Device Settings
History				æ
Date 👻	Activity		Descrip	ation
Jun 11 2012 08:02	Scan Cor	mpleted	Scan co	ompleted. 0 threats found. 169 apps scanned. 88 files scanned.
Jun 11 2012 07:36	Threat Q	uarantined	The fol	llowing threat was quarantined: /mnt/sdcard/download/4bbb53f8ebcd0b363f354e13ffaa8c87_com.choopc
Jun 11 2012 07:36	Scan Det	tection	A scan	found the following threat: /mnt/sdcard/download/4bbb53f8ebcd0b363f354e13ffaa8c87_com.choopchee
Jun 11 2012 07:36	Scan Cor	mpleted	Scan co	ompleted. 1 threats found. 169 apps scanned. 88 files scanned.
Jun 11 2012 04:21	Scan Det	tection	A scan	found the following threat: /mnt/sdcard/download/4bbb53f8ebcd0b363f354e13ffaa8c87_com.choopchee
Jun 11 2012 04:21	Scan Cor	mpleted	Scan co	ompleted. 1 threats found. 169 apps scanned. 88 files scanned.
Jun 11 2012 04:19	Scan Det	tection	A scan	found the following threat: /mnt/sdcard/download/4bbb53f8ebcd0b363f354e13ffaa8c87_com.choopchee
Jun 11 2012 04:19	Scan Cor	mpleted	Scan co	ompleted. 1 threats found. 169 apps scanned. 88 files scanned.
Jun 11 2012 04:11	File Syste	em Shield Detection	File Sys	stem Shield detected the following threat: /mnt/sdcard/download/4bbb53f8ebcd0b363f354e13ffaa8c87_c
Jun 11 2012 03:48	LDP Scre	am Received	A screa	am command was received from Portal
Jun 11 2012 03:27	Scan Cor	mpleted	Scan co	ompleted. 0 threats found. 169 apps scanned. 87 files scanned.
Jun 11 2012 03:26	Definition	ns Updated	Definiti	ions updated. New version: 278

Sending Android devices Lost Device Protection commands

You can send Android devices a variety of Lost Device Protection commands. These commands allow you to locate a missing phone, activate a Scream alarm to scare a thief, lock or unlock the device, or send a Wipe command to permanently remove data.

For instructions on using Lost Device Protection with iOS devices, see "Sending Apple (iOS) devices Lost Device Protection commands" on page 24.

To issue Lost Device Protection commands to an Android device:

- 1. Log in to the SecureAnywhere website, then click Mobile Protection (or Go to Mobile Protection).
- 2. Click the **Devices** tab.



3. From the Devices panel, double-click on the device.



4. In the next panel, click the Lost Device Protection tab.

The Lost Device Protection tab shows the available commands under Device Recovery Actions.



Lost Device Protection includes the commands described in the following table.

Lost Device Protection	n commands for Android
Locate This Device	Responds with a link to a Google Maps page showing the current location. Note : For the Locate command to work, the device must have either a GPS, Wi-Fi, or a telephony connection. Also, if the device does not support SMS or if Webroot does not support your carrier, then the user must log into the Android Marketplace.
Scream	Locks the device (see the description for the Lock command, below) and then blasts a loud screaming noise from the phone to help locate it or scare a thief. The noise will continue for up to two minutes or until the device is unlocked with the account password.
Wipe	Immediately locks the device (see the description for the Lock command, below), then performs a factory reset to remove everything, including personal data, apps, and the account. Do not use this command unless you are absolutely sure that the device is permanently lost and you want to completely wipe it! Note : Before wiping Android device data, SecureAnywhere turns off the Auto-sync function. This means it won't delete anything previously uploaded to Gmail servers, such as contacts or calendar entries.

Lost Device Protection	commands for Android
Lock	Remotely locks the device and prevents its unauthorized use. Once it's locked, the user must enter the account password to unlock it.
Unlock	Allows you to unlock the device using the password.
Lock with Message	Locks your phone (same as the Lock command, described above) and displays a text message on its panel. When you use this command, you might want to enter instructions for returning the phone, such as "If found, call 555-5555."

Sending Apple (iOS) devices Lost Device Protection commands

You can send iOS devices a variety of Lost Device Protection commands. These commands allow you to lock or unlock the device, or send a Wipe command to permanently remove data.

For instructions on using Lost Device Protection with Android devices, see "Sending Android devices Lost Device Protection commands" on page 21.

To issue Lost Device Protection commands to an iOS device:

- 1. Log in to the SecureAnywhere website, then click Mobile Protection (or Go to Mobile Protection).
- 2. Click the **Devices** tab.



3. From the Devices panel, double-click on the device.



4. In the next panel, click the Lost Device Protection tab.

The Lost Device Protection tab shows the available commands under Device Recovery Actions.

Device Details	×
Jolie Gallagher's iPhone	Apple, Inc. iPhone IOS 5.0 Added Sep 28 2012 13:14 Last check in Oct 29 2012 21:43
Security Status History Lost Device Protection	
Device Recovery Actions	
Wipe Lock Clear Passcode	

Lost Device Protection includes the commands described in the following table.

Lost Device Protection	commands for iOS
Wipe	Immediately locks the device (see the description for the Lock command, below), then performs a factory reset to remove everything, including personal data, apps, and the account. Do not use this command unless you are absolutely sure that the device is permanently lost and you want to completely wipe it!
Lock	Remotely locks the device and prevents its unauthorized use. Once it's locked, the user must enter the account password to unlock it.
Clear Passcode	Allows you to unlock the device. The user will have 60 minutes to enter a new passcode.

Changing settings for an Android device

From the Devices page, you can change the settings for each Android device.

Note: Apple (iOS) devices do not include a method for changing device settings.

To change settings:

- 1. Log in to the SecureAnywhere website, then click Mobile Protection (or Go to Mobile Protection).
- 2. Click the **Devices** tab.



3. From the Devices panel, double-click on the device.

Home	E	ndpoint	t Protect	ion	Mobile	Protect	tion
Status	De	vices	Users	Repo	rts		
evices							
evices	Devic	e 😑		vice 🕒	Resent		
Add a	Devic	e 😑 User En	Delete De	vice 🕒 First f	Resent	f Enrollm	ent Invito ast Name

- 4. In the next panel, click the **Device Settings** tab.
- 5. In the Device Settings tab, you can click the settings category to the left, which displays the individual settings on the right. You can change a setting from the left panel by clicking on it and making a new selection. When you're done, click **Update Device**. (If you make a mistake, you can switch back to the original settings by clicking **Revert Changes**.)

Security Status History Lost De	evice Protection Device Settings		
Category	Settings		
Antivirus Shields	Install Shield	(DFF	~
Antivirus Schedule	File System Shield	ON	
Lost Device Protection	Execution Shield	ON	
Call & SMS Blocking	Unknown Sources Shield	ON	
Secure Web Browsing	USB Debugging Shield	ON	
		Update Device Revert Change	ges

The following tables describe device settings.

Antivirus Shields	
Install Shield	Opens an alert if a new or updated application contains a potential threat, and blocks it from installing. SecureAnywhere Mobile provides options for either removing it (sending it to quarantine) or ignoring it and continuing with the download.
File System Shield	Opens an alert if the memory card in the device contains a potential threat, including threats that may launch when you restart or power on the device. If it detects a threat, it provides options for removing it (sending it to quarantine) or ignoring it.
Execution Shield	Opens an alert if a suspicious application or file tries to install or start on the device. If it detects a threat, it provides options for preventing the item from running (sending it to quarantine) or ignoring the warning and allowing the item to run.

Antivirus Shields	
Unknown Sources Shield	Opens an alert if the Unknown Sources setting is enabled. The Unknown Sources setting is a feature of the mobile device, available from Settings. If enabled, it allows the user to download applications that are not part of the Android Market. (Note : On AT&T devices, the Unknown Sources setting always appears secure, which means the setting is disabled.)
USB Debugging Shield	Opens an alert if the USB Debugging setting is enabled. The USB Debugging setting is a feature of the mobile device, available from Settings, which allows you to communicate with a computer over a USB port. Connecting via USB can make the mobile device vulnerable to malware that could be downloaded over this port.

Antivirus Schedule	
Schedule Scan Frequency	Adjusts the frequency of the scan.
Schedule Definitions Update Frequency	Adjusts the frequency of the threat definition updates.

Lost Device Protection	
Lost Device Protection	Enables the features for locating a missing phone or tablet, and locking it down if necessary.
SIM Card Lock	(For GSM-standard phones.) Locks the phone if someone removes the SIM card. The phone can only be unlocked with the user password.

Call & SMS Blocking	
Call & SMS Block List	Enables the Call & SMS Blocking list, which allows the user to filter calls and text messages from undesirable or unknown sources. Once the user enters a phone number into the blocked list, calls from that number are sent directly to voicemail and text messages are simply blocked. If it blocks a call or text, SecureAnywhere Mobile displays a notification.
Block Unidentified Numbers	Enables the Block Unidentified Numbers feature, which sends calls from unknown contacts directly to voicemail. Texts from unknown contacts are blocked.

Secure Web Browsing	
Block Known Threats	Enables Secure Web Browsing, which allows the user to safely surf the Internet by blocking malicious websites from loading before they are accessed. When the user attempts to visit a website that is known for spreading malware, an alert opens and provides the following options: continue blocking the site, ignore the alert and proceed to the site, or permanently ignore the warning and always proceed to the site. You should keep Secure Web Browsing enabled and choose to continue blocking any sites that it categorized as potentially malicious.

Adding a device to your account

You can add devices to your account by sending users an enrollment invitation. The invitations can be sent by SMS or an email.

To add a device:

- 1. Log in to the SecureAnywhere website, then click Mobile Protection (or Go to Mobile Protection).
- 2. Click the **Devices** tab.
- 3. Click Add a Device.



The Add a Device panel opens.

Device Deta	lls
Ownership:	Company Owned
Phone Number:	+ ()
User Details	
Existing User	New User
First Name:	
Last Name:	
Email:	
✓ Email Enrollme ○ Email Enrollme	nt Instructions to User SMS Enrollment Instructions to User nt Instructions to Me

4. In the Add a Device panel, specify the device information as described in the table below.

Add a Device set	tings
Device Details	From the Ownership drop-down, select the device owner (Company, Employee, or Not Specified). For the Phone Number , you can optionally enter the phone number if you plan to send the user an enrollment invitation by SMS. (When the phone checks in for the first time, the phone number is added at that time.) For tablets and other devices that do not have phone numbers, you can enter another contact number for the user.
User Details	Select either Existing User or New User . For existing users in your account, enter a name or phone number in the User field. The field is automatically populated as you type. For new users, enter the owner's name and email address in the fields. At the bottom of the panel, choose one or more ways to communicate enrollment instructions: send email to the owner of the device, send email to yourself, or send a text to the owner.

5. When you're done, click **Save** to send the enrollment invitation to the user.

The user must follow the enrollment instructions from the device before the device can report its status

to the Mobile Protection website.

Managing alerts

To manage alerts, see the following topics:

Configuring alert notifications	34
Managing alert subscriptions	37

Configuring alert notifications

When you subscribe to alerts, you specify whether to deliver them by email or text. You can choose to send instant alerts whenever a device enters a specific state, or (for email only) you can choose to send a summary of alerts generated in the last 24 hours.

To configure alert notifications:

- 1. Log in to the SecureAnywhere website, then click Mobile Protection (or Go to Mobile Protection).
- 2. Open the drop-down menu in the upper right corner, and click Alerts.



Add Alert		×				
Recipient D	etails					
First Name:						
Last Name:						
Address Type:	Email 👻					
Email:						
Subscription	1 Details					
Send Alert Wh	on Device Enters Critical State					
Send Alert When Device Enters Varning State						
Send Alert When Device Returns To Protected State						
Send Alert When a New Device Has Completed Enrollment						
	Save Cancel					

3. In the Alert Subscriptions panel, click Add Subscription to open the Add Alert panel.

4. Specify the alert information in the Add Alert panel, as described in the table below. When you're done, click **Save**.

A message notifies you that a confirmation email was sent to the recipient email address you entered. The alert recipient must open the confirmation link in the email message to activate alerts.

Add Alert fields	
Recipient Details	Type the name of the alert recipient, and specify whether alerts are to be sent by email or text. If you choose to send by email, type the recipient's email address. If you choose to send by text, type the device phone number for the text alert.
Subscription Details	Choose one or more methods of alerting the device owners. Note : The Send Daily Summary Email appears only if you select Email for the address type. The Send Daily Summary Email selection also requires that you enter a time of day to send the email and select the number of days for devices that have not reported status. For example, if you want to see devices that have not reported status in 2 weeks, enter 14.

Managing alert subscriptions

After you configure alerts, you can view their subscription details, delete subscriptions, and resend an address verification by email or text.

To view alert subscriptions:

- 1. Log in to the SecureAnywhere website, then click Mobile Protection (or Go to Mobile Protection).
- 2. Open the drop-down menu in the upper right corner, and click Alerts.



The Alert Subscriptions page lists your alerts and their attributes.

Alert Subscriptions									
🔂 Add Sub	😌 Add Subscription 🤤 Delete Subscription 🔯 Resend Address Verification								
First Name	Last Name	Address Type	Address	Verified	Daily Summary	Device Critical	Device Warning	Device Cleared	Device Enrolled
Andrea	Beltrando	Email	aBeltrando	Yes	Subscribed	No	Subscribed	No	No
Manoi C	Complet	Empil	manaicomolo	Vee	Me	Me	No	Mo	Subscribed

The Alert Subscriptions list shows:

- First Name and Last Name of the device user.
- Address Type, which is either email or SMS.
- Address, which is either the email address or the device phone number for SMS.
- Verified, which is either Yes if the user has responded to the alert verification message or No if the user has not responded. For users who have not responded, you can select the user and click **Resend** Address Verification to send the message again.

Administrator's Guide

Alert Subscription	ons				_
🔂 Add Subscrip	ition 😑 Delete Si	ubscription	🕒 Res	end Address Verificatio	•
First Name Last Name		Addres	sType	Adda	

• Daily Summary, Device Critical, Device Warning, Device Cleared, and Device Enrolled show whether the alert is set up for these conditions.

To delete alert subscriptions:

1. Open the drop-down menu in the upper right corner, and click Alerts.



2. Select a subscription and click **Delete Subscription**.



Managing users

To manage users, see the following topics:

Importing users into your account	. 40
Adding new users	. 41
Managing user data	. 42

Importing users into your account

You can add your Active Directory users by importing them from a file containing a comma-separated list.

To import Active Directory users from a list:

- 1. Create the file to import by running this command on your Active Directory server: csvde -f export.csv -l "DN, mail, sn, givenName, objectClass, cn" -r objectClass=user
- 2. Log in to the SecureAnywhere website, then click Mobile Protection (or Go to Mobile Protection).
- 3. Make sure the Users tab is selected.
- 4. Click Import Users.

Status Devic	ces Users Reports	8				
Users						8
🔂 Add a User (Remove Selected User	🙆 Reset Password 🛛 📴 Enrol 🤇 🤤	Import Users		Search	
First Name	Last Name	Email 🔺	Devices	Administrator		
A	SunnyDay	SunnyDay@fakemail.com	1	Yes		<u>~</u>
Alba	Fresca	Fresca@fakemail.com	2	No		_
Andrea	Beltrando	aBeltrando@fakemail.com	1	Yes		=
16.16	10.10.1	6 161 m 161 6 1				

- 5. Browse to the file you created and select it.
- 6. Click Import.

When the import completes, the users appear in the Users list.

7. Select the newly added users and click Enroll in the toolbar.

Adding new users

In addition to importing users from your Active Directory (see "Importing users into your account" on page 40), you can add users individually.

To add a user from the Users tab:

- 1. Log in to the SecureAnywhere website, then click Mobile Protection (or Go to Mobile Protection).
- 2. Make sure the Users tab is selected.
- 3. Click Add a User.

Status Dev	ices Users Reports					
Users						= ≠
Add a User	😑 Remove Selected User 🛛 🧕	Reset Password 🛛 📴 Enroll 🛛 🧲	Import Users		Search	
First Name	Last Name	Email 🔺	Devices	Administrator		
A	SunnyDay	SunnyDay@fakemail.com	1	Yes		<u>^</u>
Alba	Fresca	Fresca@fakemail.com	2	No		-
Andrea	Beltrando	aBeltrando@fakemail.com	1	Yes		=
10.10	10.10.1					

4. In the Add User panel, specify the user information. Select the **Administrator** checkbox if your are adding an administrative user.

Add User		X
First Name:		
Last Name:		
Email:		
Administrator:		
	Cours Course	
	Save Cancel	

5. Click Save.

The user will receive a confirmation email that includes a temporary password and a link to activate the account.

Managing user data

In the Users tab, you can view user details in Mobile Protection, remove them from the active user list, reset passwords for Android devices, and enroll them in Mobile Protection.

To view users in your account:

- 1. Log in to the SecureAnywhere website, then click Mobile Protection (or Go to Mobile Protection).
- 2. Open the **Mobile Protection Users** tab. The Users page lists your alerts and their attributes.

Status Devices	Users Reports				
Users					8
🔁 Add a User 🛛 🤤 R	emove Selected User – 🙆 Res	et Password 🛛 📴 Enroli 🛛 🧿	Import Users		Search
First Name	Last Name	Email 🔺	Devices	Administrator	
A	SunnyDay	SunnyDay@fakemail.com	1	Yes	<u>^</u>
Alba	Fresca	Fresca@fakemail.com	2	No	
Andrea	Beltrando	aBeltrando@fakemail.com	1	Yes	
10.10	16.16.1		0		

The Users list shows the personal information of the device owners and whether they have administrative functions.

You can also add or delete columns in the user list, and sort the items in the columns. To do this, hover your cursor over a column header to open the drop-down menu for these functions. The two icons in the upper right of the Users page enable you to export the user list to a CSV file, and refresh the user list.

Adding users to your account:

See:

- "Importing users into your account" on page 40
- "Adding new users" on page 41

Removing users from your account:

- 1. Select one or more users in the list.
- 2. Click Remove Selected User.

Resetting user passwords for Android devices:

- 1. Select a user in the list.
- 2. Click Reset Password.

3. Type the new password, confirm it, and click Save.

Enrolling a user in Mobile Protection:

- 1. Select one or more users in the list.
- 2. Click Enroll.

The users will receive email instructions to complete the enrollment.

Generating reports

To generate reports, see the following topics:

Viewing Inventory Management reports	46
Viewing Device Status reports	
Viewing Alerts and Infections reports	50
Filtering report results	52
Refreshing the report data	53
Exporting report results to a CSV file	54

Viewing Inventory Management reports

You can view device inventories in a detailed view, or by OS version, manufacturer, or owner.

To generate an Inventory Management report:

- 1. Log in to the SecureAnywhere website, then click Mobile Protection (or Go to Mobile Protection).
- 2. Click the **Reports** tab.
- 3. If necessary, click to expand the Inventory Management tree.

Home Mobile Protection	on
Status Devices Users	Reports
Select your report	**
Inventory Management	
Device Details	
OS Versions	
Manufacturers	
Device Ownership	
Device Status	
Alerts and Infections	

- 4. Select one of these reports:
 - **Device Details**: View a list of all devices, including the device owner, make and model, phone number, and the time the device last checked into the site.
 - **OS Versions**: View the operating system versions of all devices.
 - Manufacturers: View the manufacturers of all devices.
 - **Device Ownership**: View the owners of all devices, and whether the device is company owned or employee owned.
- 5. To display specific devices, use the **Search** box at the top of the list.

Report	Details
Search	

- 6. To see more information about a specific item, double-click the entry.
- 7. When you're done, exit from the report by selecting the **Close** B button in the report tab.

Viewing Device Status reports

You can view device status by pending check-in, last check-in time, and the Webroot SecureAnywhere version.

To generate a Device Status report:

- 1. Log in to the SecureAnywhere website, then click Mobile Protection (or Go to Mobile Protection).
- 2. Click the Reports tab.
- 3. If necessary, click to expand the Device Status tree.

Home	Mobile Protec	tion:
Status	Devices Use	Reports
Select you	r report	
Inventory	/ Management	
Device St	tatus	
Device	es Pending Enrollm	nent
Last C	checked In	
Secur	eAnywhere Version	n
	d Infactions	

- 4. Select one of these reports:
 - **Devices Pending Enrollment**: View which devices have received an enrollment invitation, but have not responded by checking into Mobile Protection.
 - Last Checked In: View the dates and times that devices reported into SecureAnywhere. When you select this report, you can filter the results by entering a "Before" date.
 - SecureAnywhere Version: View the versions of the Webroot apps on each device.
- 5. To display specific devices, use the **Search** box at the top of the list.

Report	Details
Search	

- 6. To see more information about a specific item, double-click the entry.
- 7. When you're done, exit from the report by selecting the **Close** B button in the report tab.

Viewing Alerts and Infections reports

You can view reports that show all devices needing attention, all infections found on devices, devices currently infected, threats blocked with website filtering, and all the Lost Device Protection commands sent.

To generate an Alerts and Infections report:

- 1. Log in to the SecureAnywhere website, then click Mobile Protection (or Go to Mobile Protection).
- 2. Click the **Reports** tab.
- 3. If necessary, click to expand the Alerts and Infections tree.

Home	Mobile Protection
Status	Devices Users Reports
Select you	ur report 🔍
> Inventor	y Management
Device S	tatus
Alerts an	d Infections
Devic	es Needing Attention
All In	fections Found
Devic	es Currently Infected
URL F	Filtering
	Davise Destastion

- 4. Select one of these reports:
 - **Devices Needing Attention**: View all devices that may be compromised with malware or need administrative attention (any devices not in a green state).
 - All Infections Found: View all threats that Webroot's shields and scans detected. When you select this report, you can filter the results by entering a date range.
 - **Devices Currently Infected**: View only the devices that are compromised by threats or potentially unwanted items.
 - URL Filtering: View all threats or other items detected in web filtering, as well as infected text messages. When you select this report, you can filter the results by entering a date range.

- Lost Device Protection: View all Lost Device Protection commands sent to devices. When you select this report, you can filter the results by entering a date range. The report graph shows a breakdown of Lock, Scream, Locate, and Wipe commands.
- 5. To display specific devices, use the **Search** box at the top of the list.

Report	Details
Search	

- 6. To see more information about a specific item, double-click the entry.
- 7. When you're done, exit from the report by selecting the **Close** button in the report tab.

Filtering report results

To filter report results, you can sort report data and search for specific data.

To generate a report and filter the results:

- 1. Log in to the SecureAnywhere website, then click Mobile Protection (or Go to Mobile Protection).
- 2. Click the Reports tab.
- 3. Select a report from the left panel.
- 4. You can then filter the results, as follows:
 - To re-sort the order of rows, click in the column head and select a new sorting method. In the Columns filter, you can remove a column from the display by clicking on a box (so the checkmark is removed).

Status Devices Users Rep	ports			
Select your report	Device Details			
▲ Inventory Management	Report Details			
Device Details	Search			
OS Versions Manufacturers	User Email	 First Name 	Last Name Operating S	System
Device Ownership Device Status Devices Pending Enrollment Last Checked In SecureAnywhere Version Alerts and Infections Devices Needing Attention All Infections Found Devices Currently Infected URL Filtering Lost Device Protection	sfoley@webroot.com	☆↓ Sort Ascending	oley Android 2.3	1
	kgoguen@webroot.com	Z↓ Sort Descending	oguen Android 2.3	
	dbrendan@webroot.com			
	jcarl@webroot.com	Columns	_ ⊻ •	
	sfoley@webroot.com	Filter Data	Alert Summary	
	obrowell@webroot.com	Bob	User Email	
	salesdemo@webroot.com	Sales	First Name	
	CMartinez@syseng2.com	Cris	Last Name	
			Operating System	

• To display specific entries, use the **Search** box at the top of the report data:

Report Details		
Search		

As you type characters in the Search box, the columns below display only the content that matches your search criteria.

Refreshing the report data

You can receive the most up-to-date report results by refreshing the display. To do this, click the **Refresh** button in the upper right corner:

Dev	vice Details				
Rep	ort Details				
Sear	rch				Defrech
•	User Email	First Name	Last Name	Operating System	Manufacture

Exporting report results to a CSV file

You can export the report data to a spreadsheet. To do this, click the **Export** button in the upper right corner:

Dev	ice Details				
Repo	ort Details				
Sear	ch				Export to CSV
•	User Email	First Name	Last Name	Operating System	Manufacturer

Index

A

account 8 adding devices 30 adding or renewing keycodes 10 creating 2 logging in 3 viewing status 8 Active Directory, importing 40 alerts 37 configuring notifications 34 deleting subscriptions 38 managing subscriptions 37 resending address verification 37 Alerts and Infections report 50 Antivirus schedule 28 Apple MDM certificate 5

B

Block Known Threats 29 Block Unidentified Numbers 28

С

Call & SMS Block List 28 certificate for Apple MDM 5 Clear Passcode 25 CSV file, exporting reports to 54

D

definitions, adjusting updates 28 Device Status report 48 devices 12 adding 30 changing settings 26 determing which need attention 50 forcing an update to 17 scanning 15 using Lost Device Protection (Android) 21 using Lost Device Protection (iOS) 24 viewing details 13 viewing history 19 viewing summary 12

E

Execution Shield 27

F

File System Shield 27 forcing updates 17

Η

history of devices 19

I

Infections report 50 Install Shield 27 Internet surfing, protecting 29 Inventory Management reports 46

K

keycode adding 4 managing 10

L

licenses, adding or renewing 10 Locate This Device command 22 Lock command Android 23 iOS 25 Lock with Message command 23 login 3 Lost Device Protection Android commands 21 Apple (iOS) commands 24 determing commands sent from each device 51 disabling 28

M

malware, determining which devices are infected 50
Manage Keycodes 10
Manage Licenses 10
manufacturer, determining 46
MDM certificate 5
Mobile Protection settings 5

0

OS versions, determining 46 ownership of a device, determining 46

P

passwords, resetting 42 pending enrollment 48 product keycode 4

R

reports Alerts and Infections 50 Device Status 48 exporting data 54 filtering data 52 Inventory Management 46 refreshing data 53

S

scanning a device 15 Schedule Definitions Update Frequency 28 Schedule Scan Frequency 28 Scream command for Android 22 Secure Web Browsing 29 settings for a device 26 shields 27 SIM Card Lock 28 spreadsheet, exporting reports to 54 status of a device 13 Status tab 8 subscriptions configuring alert notifications 34 managing alert notifications 37

Т

texts, blocking 28 threat definition updates, adjusting 28

U

unidentified calls, blocking 28 Unknown Sources Shield 28 Unlock command 23 updates, forcing 17 URL threats, determining which devices are infected with 50 USB Debugging Shield 28 users 42 adding 41 enrolling 43 importing into account 40 removing 42 resetting passwords 42

V

version of SecureAnywhere, determining 48

W

web browsing, protecting 29 Wipe command Android 22 iOS 25