WEBROOT®

an opentext™ company

Webroot Business Mobile Protection Admin Guide

Copyright

WSAB Mobile Protection Admin Guide

Table of Contents

Chapter 1: WSA Business Mobile Protection Admin Guide

To get started using Business Mobile Protection, see the following topic:

WSA Business - Mobile Protection Admin Guide Overview

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. For more information, see the WSA Endpoint Protection Admin Guide.

Chapter 2: Getting Started With Mobile Protection

To get started with Mobile Protection, see the following topics:

System Requirements for Mobile Protection

The following describes the system requirements for using Mobile Protection functionality on Windows and on Mac and on Android and iOS devices.

System Requirements for Android Devices

Operating Systems

- Android operating system version 4.4 (Kit Kat) or higher.

Devices

- Android-compatible phones and tablets, including Kindle and Nook.

Note: Requires an active internet connection for some features. For a list of these features, click here.

System Requirements for iOS Devices

Operating Systems

- iOS 10 or later.

Devices

- Compatible with iPhone®, iPod Touch®, and iPad® mobile digital devices.

System Requirements for Windows

Operating Systems

- Windows 10 (32-bit and 64-bit).
- Windows 8 and 8.1 (32-bit and 64-bit).
- Windows 7 (32-bit and 64-bit) , Windows 7 SP1 (32-bit and 64-bit).
- Windows Vista® (32-bit), Windows Vista SP1, SP2 (32-bit and 64-bit).

RAM

- Intel Pentium®/Celeron® family, or AMD® K6™/Athlon®/AMD Duron™ family, or other compatible processor.
- 128 MB RAM (minimum).
- 2 GB RAM recommended (minimum).

Hard Disk Space

- 15 MB

Internet/Browser

- Internet access is required.
- Internet Explorer® 9.0 and higher (32-bit and 64-bit).
- Mozilla Firefox® (32-bit and 64-bit); current and most recent versions.
- Google Chrome® (32-bit and 64-bit); current and most recent versions.

System Requirements for Mac

Operating System

- Mac OS X 10.7 (Lion®)
- Mac OS X 10.8 (Mountain Lion®)
- OS X 10.9 (Mavericks®)
- OS X 10.10 (Yosemite®)
- OS X 10.11 (El Capitan®)
- macOS 10.12 (Sierra®)
- macOS 10.13 (High Sierra®)

Memory

- 128 MB RAM (minimum)

Storage

- 15 MB

Internet/Browser

- Internet access is required.
- Apple Safari® 7.0 or higher.
- Mozilla Firefox®; current and most recent versions.
- Google Chrome®; current and most recent versions.

After Logging In

Before completing the procedures described in this manual, follow the instructions in SecureAnywhere Business Mobile Protection Getting Started to install the software, set up your account and log in.

Workflow of Tasks

Once you have logged in to your Mobile Protection account, follow these steps:

- Create policies for Android and iOS. For more information, see *Adding Policies on page 70*.
- Create groups and assign one Android and one iOS policy to each group. For more information, see *Adding Groups on page 61*.
- Add users and enroll their devices. For more information, see *Adding Users on page 45* and *Adding Devices to Your Account on page 15* and *Adding Admin Users on page 48*.
- Optionally, change the default group assigned to each user. For more information, see *Moving Users Between Groups on page 65*.

  Note: Each device inherits the policies assigned to that user's group.

- Optionally, add additional devices and assign to users. For more information, see *Adding Devices to Your Account on page 15*.
- Optionally, override a group policy with a policy specific to a device. For more information, see *Changing Policy and Ownership Attributes on page 29*.
- Configure alerts to notify you when a device needs attention. For more information, see *Configuring Alert Notifications on page 38*.

When you have gone through the above steps for all your users and devices, you can assign policies on a group or device basis that control the following:

- The level of protection on the device
- Block malicious text messages from a device.
- Block a device from browsing on malicious websites.
- Require a password and specify password formats for the device.
  - For a detailed description of policy options, see:
  - *Android Policy Options on page 72*

- *iOS Policy Options on page 78*

You can also perform the following device management functions remotely:

- View alerts and work with the user to remove threats.
- Run scans and force a virus definition update.

  Note: If you have Mobile Protection software that is version 3.7.1 or greater, cloud definitions are always up to date, and you will not need to push them. However, if you have software that is version 3.7.0 or older, the Scan Now and Force Definitions Update buttons will be available and you will still be able to schedule and push updates.

- Depending on your OS, locate, lock, unlock, wipe devices, and issue a scream.

If You Are Upgrading

- If you are upgrading from a previous version of Mobile Protection, your users will be assigned to the Default Group, which is assigned the Default Android policy and Default iOS policy.
- If you want to move users to a different group, see *Moving Users Between Groups on page 65*.

Editing Administrator Account Settings

The Account Settings described in this section define details for admin users who have access to the Mobile Protection website console. You can add or change any of the account settings, except the email address specified for your login name.

To edit administrator account settings:

1. Log in to the SecureAnywhere website.
2. Click the **Go to Mobile Protection** button.

   The Mobile Protection console displays, with the Status tab active.

   The system displays the Account Settings page.

3. Next to the information you want to edit, click the **Change** link.
4. Use the table below for guidance to make your changes:

FIELD	DESCRIPTION
Name	Your name.
Display Name	Alternate name
Email	Not modifiable.

FIELD	DESCRIPTION
Password	To change your password, enter a minimum of nine characters for your new password. Your password: • Must contain at least six alphabetic characters and three numeric characters. • Can include special characters, except for angle brackets: < and >. • Is case sensitive. As you type, the Strength meter displays how secure your password is. For optimum security, you should make your password as strong as possible.
Security Code	You defined a security code when you created the account. • As an extra security step, the SecureAnywhere website prompts you for this code right after you log in. • Every time you log in, you must also enter two random characters of this code. For example, if your code is *123456* and it prompts you for the fourth and sixth character, you would enter **4** and **6**.
Security Question	The security question allows Webroot to identify your account if you forget your user name, password, or security code. • If you answer the question correctly, we can retrieve the login information for you. • You can select a new question from the New Security Question field, then type your answer along with your password.

FIELD	DESCRIPTION
2-factor Authentication (2FA)	If you enabled 2-factor authentication (2FA), follow the steps to log in using your mobile authenticator app. • Once you have enabled 2FA and downloaded an authenticator app, you have to open the app and enter the code that is presented each time you log in.
Office Phone	Enter or change your office phone number.
Mobile Phone	Enter or change your mobile phone number.
Time Zone	Select your timezone.
Access & Permissions	The SecureAnywhere permissions control the ability to add and delete users. The Mobile Protection permission defines whether or not this user has access to the Mobile Protection website.

5. When you're done, click the **Save Details** button to save your changes.

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 manage keycodes:

1. Log in to the SecureAnywhere website.
2. Click the **Go to Mobile Protection** button.

   The Mobile Protection console displays, with the Status tab active.

3. Do either of the following:
   - From the Account Snapshot panel on the Status tab, click **Manage Licenses**.
   - In the upper-right corner that displays your login ID, from the drop-down menu, select **Manage Keycodes**.

   The list displays the following information:

   - Your keycodes
   - Their affiliated product editions
   - The number of devices, also called seats, for each keycode
   - The number of days remaining on each license
   - Each time you add a user or device, a seat is assigned whether or not the user completes enrollment.
4. You can do any of the following:
   - To include new mobile licenses, in the upper right corner, click **Add Product Keycode**.
   - To display the Webroot home page and purchase a new keycode, in the upper left corner, click **Buy a Keycode Now**.
   - To extend the time limit on the license, in the Renew column, click the **Renew** link.
   - To purchase additional mobile protection, in the Upgrade column, click the **Upgrade** link.

Viewing Account Statuses

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.
2. Click the **Go to Mobile Protection** button.

   The Mobile Protection console displays, with the Status tab active.

3. The Status page is divided into the panels described below:
   - **Status Snapshot Panel** — Displays the number of devices that are secure, infected, or otherwise needing attention.
   - **Device Activity Snapshot Panel** — Displays The number of devices that have and have not connected to Mobile Protection within the selected period. It also displays the number of devices that are registered, but have not enrolled in the website.
   - **Devices Needing Attention Panel** — Displays any vulnerable devices. Double-click a device entry to see a detailed view.

     For information about how to fix any problems, see *Viewing Device Statuses on page 18*.

   - **Account Snapshot Panel** — Displays the number of seats used in your license, the total seats available, and the number of days before the earliest license expires.
     - To update license keycodes, click **Manage Licenses**. For more information, see **Managing Keycodes**.
     - Each time you add a user or device, a seat is assigned whether or not the user completes enrollment.
   - **Help and Support** — Provides links to Webroot's publications and Technical Support.
   - **Reports Panel** — Provides quick access to reports for high-level statistics.

Chapter 3: Managing Devices

To manage devices, see the following topics:

Adding Devices to Your Account

Normally, you will add devices to your account by sending users an enrollment invitation when you add the user. A user might have more than one device so you can also add and enroll devices for a user using the steps below. The steps to initiate the enrollment differ but the process is basically the same — the user receives an email or text invitation and follows the provided instructions to access the link and type in the password. In order for you to add a device using this procedure, the user must already exist in the account.

Note: If you have Apple devices, be sure to first install the Apple MDM certificate. For more information, see Installing Apple MDM Certificates. in the WSA Business - Mobile Protection Getting Started Guide.

To add a device:

1. Log in to the SecureAnywhere website.
2. Click the **Go to Mobile Protection** button.

   The Mobile Protection console displays with the Status tab active.

3. Click the **Devices** tab.

   The Devices tab displays.

4. Click the **Add a Device icon**.

   The Add a Device window displays.

5. Specify the device information as described in the following table.

FIELD	DESCRIPTION
Device Details	
Ownership	From the Ownership drop-down, select the device owner: • **Company** • **Employee** • **Not Specified**
Phone Number	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 to the account information 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	
Existing User	Select the checkbox to email enrollment instructions to the user.
Email Enrollment Instructions to User	Select the checkbox to email enrollment instructions to the user.

FIELD	DESCRIPTION
SMS Enrollment Instructions to User	Select the checkbox to send enrollment instructions to the user with SMS. **Note:** This option is only available if you have entered a phone number in the Phone Number field.
Email Enrollment Instructions to Me	At the bottom of the panel, select one or more ways to communicate enrollment instructions: send email to the user of the device, send email to yourself, or send a text to the user.

6. When you're done, click the **Save** button 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.
- At that time, information from the device is uploaded to the account information, including device type, phone number, OS, and so on. Until that occurs, the device information remains blank or uses default data.

Viewing Device Statuses

From the Devices page, you can access a list of all devices. Each entry displays the user's name and contact information; device phone number, make, model, and OS; policy, and the last time the device checked in.

The timezone for Last Check In is set in Account Settings. For more information, see *Editing Administrator Account Settings on page 9*.

To view the status of a device:

1. Log in to the SecureAnywhere website.
2. Click the **Go to Mobile Protection** button.

   The Mobile Protection console displays, with the Status tab active.

3. Click the **Devices** tab.

   The Devices tab displays.

4. Double-click on the device for which you want to view a status.

   The Device Details window displays with the Security Status tab active.

5. Each device has a color-coded status icon associated with it. The table below describes what each color represents.

ICON COLOR	DEFINITION
Grey	Either of the following: • Enrolled but not confirmed. • Enrolled and deleted.
Green	Enrolled, confirmed, and protected.

ICON COLOR	DEFINITION
Red	Enrolled, confirmed, in a vulnerable state needing attention.
Orange	Enrolled, confirmed, in a possibly vulnerable state.

6. If there is a problem, this panel describes the problem and displays information about what action should be taken to resolve it. You can do either of the following:
   - **Run a remote scan** — In the upper right corner, click the **Scan Now** button.
   - **Force a virus definitions update to the device** — In the upper right corner, click the **Force Definitions Update** button.

   Note: If you have Mobile Protection software that is version 3.7.1 or greater, cloud definitions are always up to date, and you will not need to push them. However, if you have software that is version 3.7.0 or older, the Scan Now and Force Definitions Update buttons will be available and you will still be able to schedule and push updates.

7. Click any of the tabs at the top of the panel to view the following information:
   - **History** — See *Viewing Device Histories on page 22*
   - **Lost Device Protection** — See either of the following topics:
     - *Sending Lost Device Protection Commands to Android Devices on page 23*
     - *Sending Lost Device Protection Commands to iOS Devices on page 26*
   - **Device Attributes** — See *Changing Policy and Ownership Attributes on page 29*.
   - **Protection Policy** — This tab displays the policy assigned to this device, either via the user's group policy or via the Device Attributes tab.

Scanning Devices

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

Note: If you have Mobile Protection software that is version 3.7.1 or greater, cloud definitions are always up to date, and you will not need to push them. However, if you have software that is version 3.7.0 or older, the Scan Now and Force Definitions Update buttons will be available and you will still be able to schedule and push updates.

To scan a device:

1. Log in to the SecureAnywhere website.
2. Click the **Go to Mobile Protection** button.

   The Mobile Protection console displays with the Status tab active.

3. Click the **Devices** tab.

   The Devices tab displays.

4. Double-click on the device you want to scan.

   The Device Details window displays with the Security Status tab active.

5. In the upper right corner, click the **Scan Now** button.

   When the scan completes, the updated device status displays on the Security Status page and the scan is added to the History tab.

Pushing Updates to Devices

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

Note: If you have Mobile Protection software that is version 3.7.1 or greater, cloud definitions are always up to date, and you will not need to push them. However, if you have software that is version 3.7.0 or older, the Scan Now and Force Definitions Update buttons will be available and you will still be able to schedule and push updates.

To push updates to a device:

1. Log in to the SecureAnywhere website.
2. Click the **Go to Mobile Protection** button.

   The Mobile Protection console displays with the Status tab active.

3. Click the **Devices** tab.

   The Devices tab displays.

4. Double-click on a device for which you want to push an update.

   The Device Details window displays with the Security Status tab active.

5. In the upper right corner of the Device Details window, click the **Force Definitions Update** button.

Viewing Device Histories

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.
2. Click the **Go to Mobile Protection** button.

   The Mobile Protection console displays with the Status tab active.

3. Click the **Devices** tab.

   The Devices tab displays.

4. From the Devices panel, double-click on the device for which you want to view a history.

   The Device Details window displays with the Security Status tab active.

5. Click the **History** tab.
   - The History tab displays activity on the device, such as a completed scan or a quarantined threat.
   - The page displays activity date and description.
6. Click the **Refresh** button in the upper right corner of the Device Details window to fetch any activity completed since you accessed this display.

Sending Lost Device Protection Commands to Android Devices

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 Lost Device Protection Commands to iOS Devices on page 26*.

To send a lost device protection command to an Android device:

1. Log in to the SecureAnywhere website.
2. Click the **Go to Mobile Protection** button.

   The Mobile Protection console displays with the Status tab active.

3. Click the **Devices** tab.

   The Devices tab displays.

4. Double-click on the Android device to which you want to send a Lost Device Protection command.

   The Device Details window displays with the Security Status tab active..

5. Click the **Lost Device Protection** tab.

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

COMMAND	DESCRIPTION
Locate This Device	This device responds with a link to a Google Maps page displaying the current location. If the device happens to be turned off and cannot receive the command, then it will detect the pending command next time it checks in with the console. The device is set to check for pending commands every 30 minutes. **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 you must log into the Android Marketplace.
Scream	Locks the device, the same as the Lock command described 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, the same as the Lock command described below, then performs a factory reset to remove everything, including personal data, apps, and the account. 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. **Note:** Do not use this command unless you are absolutely sure that the device is permanently lost and you want to completely wipe it!

COMMAND	DESCRIPTION
Lock	Remotely locks the device and prevents its unauthorized use. Once the device is locked, the user must enter the account password to unlock it. Unlock allows you to unlock the device using the password.
Unlock	Remotely unlocks the device.
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 Lost Device Protection Commands to iOS Devices

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

For information on using Lost Device Protection with Android devices, see *Sending Lost Device Protection Commands to Android Devices on page 23*.

To issue Lost Device Protection commands to an iOS device:

1. Log in to the SecureAnywhere website.
2. Click the **Go to Mobile Protection** button.

   The Mobile Protection console displays with the Status tab active.

3. Click the **Devices** tab.

   The Devices tab displays.

4. Double-click on the iOS device for which you want to send a Lost Device Protection command.

   The Device Details window displays with the Security Status tab active.

5. Click the **Lost Device Protection** tab.

   The Lost Device Protection tab displays.

6. Select any of the following:

COMMAND	DESCRIPTION
Locate This Device	Responds with a link to a Google Maps page displaying the current location. **Note:** For the Locate command to work, the device must have either a GPS, Wi-Fi, or a telephony connection. Also, this feature requires device to have iOS 7 and higher.
Scream	Locks the device, and prevents its unauthorized use, then performs a factory reset to remove everything, including personal data, apps, and the account. Then it blasts a loud screaming noise from the phone to help locate it or scare a thief. To suppress the sound, user must push the up or down volume buttons on device.
Wipe	Immediately locks the device and prevents its unauthorized use, then performs a factory reset to remove everything, including personal data, apps, and the account. Once it's locked, the user must enter the account password to unlock it. **Note:** Do not use this command unless you are absolutely sure that the device is permanently lost and you want to completely wipe it!

COMMAND	DESCRIPTION
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 Policy and Ownership Attributes

From the Devices page, you can change the policy and ownership attributes for each device.

To change the policy or ownership attributes:

1. Log in to the SecureAnywhere website.
2. Click the **Go to Mobile Protection** button.

   The system displays the Mobile Protection console with the Status tab active.

3. Click the **Devices** tab.

   The Devices tab displays.

4. From the Devices panel, double-click on the device whose attributes you want to change.

   The Device Details window displays with the Security Status tab active.

5. Click the **Device Attributes** tab.

   The Device Attributes tab displays.

6. Do either or both of the following:
   - From the Policy drop-down menu, select a new policy.
   - From the Ownership drop-down menu, select a new owner.
7. When you're done, click the **Update Device** button.

Deleting Devices

To delete a device:

1. Log in to the SecureAnywhere website.
2. Click the **Go to Mobile Protection** button.

   The system displays the Mobile Protection console with the Status tab active.

3. Click the **Devices** tab.

   The Devices tab displays.

4. Do either of the following:
   - Select a device in the list.
   - Use the **Shift** or **Control** keys to select multiple devices.
5. Click the **Delete Device** button.
6. At the prompt, click **Yes**.
   - When you delete a device from the website, the user's app displays as deactivated.
   - All the functions will be deactivated except for an Uninstall button, which will display once the delete device command has been received by the device.

About Updates

If you have a version of the Mobile Protection software that is newer than 3.7.0, updates are made automatically, and you will not need to push them.

However, if you have an earlier version of the software other than 3.7.0, the Force Deletes Update button will be available and you will still be able to push updates.

Chapter 4: Managing Alerts

To manage alerts, see the following topics:

Alert Notification Descriptions

This topic contains descriptions of all the alert notifications in Mobile Protection.

Those marked with an asterisk (*) are alerts you will see with Android clients running 3.3.0.5561 or older.

Newer versions of client are policy driven, and user cannot change setting on device. Please ensure users are running latest version of both Android application and iOS application posted within Google Play and Apple iTunes stores respectively.

PORTAL ALERT	CAUSES	HOW TO FIX IT
% threat(s) found on your device	Android – If malware is found during scan	Remove or quarantine application.
Install Shield disabled*	Android – Install Shield setting on device is turned off	Work with user to enable this setting within app.
Execution Shield disabled*	Android – Execution Shield setting on device is turned off	Work with user to enable this setting within app.
File System Shield disabled*	Android – File System Shield setting on device is turned off	Work with user to enable this setting within app.
Current scan out of date	Android – Last scan is more than a week old	Ensure device has internet connectivity. Scans are on a scheduler, but can be manually triggered from device.

PORTAL ALERT	CAUSES	HOW TO FIX IT
Current definitions out of date	Android – Local definition file is more than a week old Ensure device has internet connectivity.	Ensure device has internet connectivity. Definition downloads are on a scheduler, but can be manually triggered from device. **Note:** If you have Mobile Protection software that is version 3.7.1 or greater, cloud definitions are always up to date, and you will not need to push them. However, if you have software that is version 3.7.0 or older, the Scan Now and Force Definitions Update buttons will be available and you will still be able to schedule and push updates.
Scheduled scans disabled*	Android – Scheduled scan setting on device is turned off	Work with user to enable this setting within app.

PORTAL ALERT	CAUSES	HOW TO FIX IT
Automatic definitions updates disabled*	Android – Automatic definition update setting on device is turned off	Work with user to enable this setting within app. **Note:** If you have Mobile Protection software that is version 3.7.1 or greater, cloud definitions are always up to date, and you will not need to push them. However, if you have software that is version 3.7.0 or older, the Scan Now and Force Definitions Update buttons will be available and you will still be able to schedule and push updates.
Secure Browsing disabled*	Android – Secure Web Browsing setting on device is turned off	Work with user to enable this setting within app.
Lost Device Protection disabled*	Android – Lost Device setting on device is turned off	Work with user to enable this setting within app.
Insecure option enabled: Unknown sources	Android – Unknown sources is enabled in Android security settings	Work with user to enable this setting within OS.
Insecure option enabled: USB debugging	Android – USB debugging is enabled in Android security settings	Work with user to enable this setting within OS.

PORTAL ALERT	CAUSES	HOW TO FIX IT
Unknown Source Shield disabled*	Android – Unknown Source setting on device is turned off	Work with user to enable this setting within app.
USB Debugging Shield disabled*	Android – USB Debugging setting on device is turned off	Work with user to enable this setting within app.
Passcode is not set on device	iOS Passcode not set on device iOS	User must set passcode on device which adheres to policy requirements.
Device authorization requirements not met	Android – Device screen lock authorization does not meet minimum policy setting	User must set password on device which adheres to policy requirements.
Device idle timeout before screen lock requirements are not met	Android – Screen Lock timeout value on device does not meet minimum policy setting	User must set screen lock timeout on device which adheres to policy requirements.
The user did not grant Device Administration to the client application	Android – Device Administration is turned off for Webroot application in Android security settings	User must enable Device Administrator privileges for Webroot app within OS Security settings.
The device has not responded to communication requests	Device has not responded to server commands for over a period of x days	Ensure device has internet connectivity.

PORTAL ALERT	CAUSES	HOW TO FIX IT
The device has push notifications disabled	iOS app requires push notifications to be enabled	User must allow push notifications for Webroot app.
The device has locations services disabled	iOS app requires location services to be enabled	User must enable location services for Webroot app.
User removed MDM profile from the device	iOS app recognized user removed MDM profile from device	User must re-enroll by going to Webroot app and following onscreen directions.
Webroot iOS agent is not running	iOS app is not running on device	Work with user to make sure Webroot app is running in background on device.
User removed Webroot iOS agent	iOS app was uninstalled by user on device or application was never installed	Send re-enrollment instructions to user from portal to re-install Webroot app.

Configuring Alert Notifications

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

To configure an alert notification:

1. Log in to the SecureAnywhere website.
2. Click the **Go to Mobile Protection** button.

   The Mobile Protection console displays with the Status tab active.

3. From your email-drop-down menu, select **Alerts**.

   The Alert Subscriptions window displays.

4. Click the **Add Subscription** icon..

   The the Add Alert window displays.

5. Specify the alert information in the Add Alert panel, as described in the following table.

FIELD	DESCRIPTION
Recipient Details	Do either of the following: • To send by email, type the recipient's email address. • To send by text, type the device phone number for the text alert. You can also specify a language for the alert.
Subscription Details	Select one or more types of alerts you want sent to the user. The Send Daily Summary Email displays only if you select Email for the address type. If you select Send Daily Summary Email, you must enter a time of day to send the email and select the number of days for devices that have not reported status. For example, to see devices that have not reported status in 2 weeks, enter 14.

6. When you're done, click the **Save** button.

- 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.

Managing Alert Subscriptions

After you configure alerts, use this procedure to do either or both of the following:

- Viewing Alert Subscriptions
- Deleting Alert Subscriptions

Viewing Alert Subscriptions

Follow this procedure to view subscription details, which includes how to resend an address verification by email or text.

To view an alert subscription:

1. Log in to the SecureAnywhere website.
2. Click the **Go to Mobile Protection** button.

   The Mobile Protection console displays with the Status tab active.

3. From your email drop-down menu, select **Alerts**.

   The Alert Subscriptions page displays your alerts and their attributes:

   - 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 — Indicates whether or not the user has responded to the alert verification message:
     - **Yes** — The user has responded.
     - **No** — The user has not responded.
   - The following columns indicate whether the alert is set up for the various conditions:
     - Daily Summary
     - Device Critical
     - Device Warning
     - Device Cleared
     - Device Enrolled

- For users who have not responded, you can select the user and click **Resend Address Verification** to send the message again.

Deleting Alert Subscriptions

Follow this procedure to delete alert subscriptions.

To delete an alert subscription:

1. Log in to the SecureAnywhere website.
2. Click the **Go to Mobile Protection** button.

   The Mobile Protection console displays with the Status tab active.

3. From your email drop-down menu, select **Alerts**.

   The Alert Subscriptions page displays your alerts and their attributes:

   - 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 — Indicates whether or not the user has responded to the alert verification message:
     - **Yes** — The user has responded.
     - **No** — The user has not responded.
   - The following columns indicate whether the alert is set up for the various conditions:
     - Daily Summary
     - Device Critical
     - Device Warning
     - Device Cleared
     - Device Enrolled
   - For users who have not responded, you can select the user and click **Resend Address Verification** to send the message again.

4. Select a subscription and click the **Delete Subscription** icon.

Chapter 5: Managing Users and Groups

To manage users and groups, see the following topics:

Users and Groups Overview

Your Mobile Protection account consists of two types of users:

- **End User** — Someone who receives an invitation to install and register the Mobile Protection app on their device from the administrator of the Mobile Protection account website. That device can then be monitored by the admin user from the website. The end user does not have access to the Mobile Protection website.
- **Admin User** — Someone who has access to the Mobile Protection website, where they monitor, add, and enroll users and their devices. The admin user might also be a Mobile Protection end user, and might also be an admin user for other SecureAnywhere applications.

The procedures for setting up these two user types differs. For more information, see:

- *Adding Admin Users on page 48*
- *Adding Users on page 45*
- *Enrolling Devices on page 47*

Keep in mind the following:

- Because policies are assigned to groups, each user must belong to a group. For more information about defining policies, see *Policies Overview on page 69*.
- Assigning policies to groups allows you to create policies for specific departments. For example, you may want to require all members of one department to enter a pass code when they access their device. New users are always added to the Default Group; however, you can drag users to a different group on the Users & Groups display.
- You can add users and groups in any order. For a recommended procedure for setting up, see *After Logging In on page 7*.

Below is a sample Users & Groups display:

- The Groups panel allows you view, add, edit and delete groups. You can also assign users to a group by clicking and dragging the user entry onto the group name.
- The Users panel displays users that belong to the group selected in the Groups panel.
  - To move users to a different group, drag the user name to the new group.
  - To customize what columns are displayed, click the **Down** arrow for that column, select **Columns**, and enable or disable the columns you want displayed or removed, respectively.
  - For more information, see *Viewing User Details on page 54*.

- The Policies panel displays the policies for the group selected in the Groups panel. Each group might have an Android policy, an iOS policy, or both.

Adding Users

This procedure describes how to add end users, that is, non-admin users.

- To add admin users, see *Adding Admin Users on page 48*.
- You can also import users from your Active Directory. For more information, see *Importing Active Directory Users on page 52*.

To add a user:

1. Log in to the SecureAnywhere website.
2. Click the **Go to Mobile Protection** button.

   The Mobile Protection console displays with the Status tab active.

3. Click the **Users & Groups** tab.

   The Users & Groups tab displays.

4. In the left panel, highlight the group to which you want to add this user.

   If you do not select a group, the user is assigned by default to the Default Group.

5. Click the **Add a user** icon.

   The Add User window displays.

6. In the First Name field, enter the user's first name.
7. In the Last Name field, enter the user's last name.
8. In the Email field, enter the user's email address.
   - All users require a valid email address or they will not be enrolled.
   - Each email address must be unique within Mobile Protection.
9. From the Group drop-down menu, select the group to which you want to add this user.

   If you do not select a group, the user is assigned by default to the Default Group.

10. Do not select the **Administrator** checkbox.
11. When you're done, click the **Save** button.
12. Continue with *Enrolling Devices on page 47*.

Enrolling Devices

This procedure describes how to enroll a device for an end user.

To enroll a user:

1. Log in to the SecureAnywhere website.
2. Click the **Go to Mobile Protection** button.

   The Mobile Protection console displays with the Status tab active.

3. Click the **Users & Groups** tab.

   The Users & Groups tab displays.

4. From the main user panel, highlight the user whose device you want to enroll, and click **Enroll**.

   The user receives a confirmation email that includes a link to the app, a temporary password, and instructions for installing the app on the device and getting enrolled.

5. Once the user has installed the app on the device and enrolled, you can change the default group assigned to that user.

   Each device inherits the policies assigned to that user's group. For more information, see *Moving Users Between Groups on page 65*.

6. If a user has more than one device, you can add and enroll additional devices from the Devices tab and assign them to the appropriate user.

   For more information, see *Adding Devices to Your Account on page 15*.

Adding Admin Users

Adding an admin user differs slightly from adding an end user. If your admin user is also an end user, that is, the admin user's devices will be secured under Mobile Protection, an extra step is needed, as described below.

In order to add admin users and assign permissions, you must be an admin user with full permissions.

This procedure describes the two methods that are available for adding an admin user:

- To create an admin user with permissions within Mobile Protection, see *Adding Admin Users From the Users & Groups Tab on page 48*.
- To create an admin user with permissions within Mobile Protection and in other SecureAnywhere applications, see *Adding Admin Users From the Drop-Down Menu on page 49*.

Adding Admin Users From the Users & Groups Tab

Using this method creates an admin user who has admin permissions only within SecureAnywhere Mobile Protection.

To add an admin user from the Users & Groups tab:

1. Log in to the SecureAnywhere website.
2. Click the **Go to Mobile Protection** button.

   The Mobile Protection console displays with the Status tab active.

3. Click the **Users & Groups** tab.

   The Users & Groups tab displays.

4. Click the **Add a user** icon.

   The Add User window displays.

5. In the First Name field, enter the admin's first name.
6. In the Last Name field, enter the admin's last name.
7. In the Email field, enter the admin's email.
   - All users require a valid email address or they will not be enrolled.
   - Each email address must be unique within SecureAnywhere.

8. From the Group drop-down menu, select the group to which the user will be added.
9. Select the **Administrator** checkbox.
10. Click the **Save** button.
    - The new admin user receives a confirmation email with instructions and a link that they must click on to complete the registration.
    - Once the new user has been confirmed, they display in your list of users.
    - By default, the new admin user has access to the Mobile Protection console, but cannot remove users, add admin users, or change permissions.
11. To change this admin user's permissions, from the drop-down menu select **Manage Users**, display the user, and make your changes on the Access & Permissions tab.
12. To enroll a device for this admin user, highlight the user name and click the **Enroll** button.

    The user receives another confirmation email, which includes a link to the app, a temporary password, and instructions for installing the app on the device.

13. Once the user has confirmed, you can change the default group assigned to that user.
    - Each device inherits the policies assigned to that user's group.
    - For more information, see *Moving Users Between Groups on page 65*.
14. If a user has more than one device, you can add and enroll additional devices from the Devices tab and assign them to the appropriate user.

    For more information, see *Adding Devices to Your Account on page 15*.

Adding Admin Users From the Drop-Down Menu

Using this method creates an admin user who has admin permissions within all SecureAnywhere products associated with this account.

To add an admin user from the drop-down menu:

1. Log in to the SecureAnywhere website.
2. Click the **Go to Mobile Protection** button.

   The Mobile Protection console displays with the Status tab active.

3. Click the **Users & Groups** tab.

   The Users & Groups tab displays.

4. From your drop-down menu, select **Manage Admins**.

   The admin user panel displays, displaying the initial admin user with full permissions.

5. Click the **Create New Admins** button.

   The Create New Admin panel displays.

6. In the Email address field, enter the admin's email address.
7. From the Time Zone drop-down menu, select the time zone for this admin.

   Additional permissions fields display.

   - The SecureAnywhere permissions control the ability to add and delete users.
   - The Mobile Protection permission defines whether or not this user has access to the Mobile Protection website.

8. Select the **Do you wish to give this user console access** checkbox.

   Two additional fields display.

9. From the SecureAnywhere drop-down menu, select one of the following permission levels:
   - **Basic**
   - **Admin**
10. From the Mobile Protection drop-down menu, select one of the following access levels:
    - **No Access**
    - **Access**
11. Click the **Create Admin** button.

    The new user receives an email providing a link and a temporary password.

12. When the new user clicks on the link, they are asked to complete a registration form, using the temporary password.

13. The new admin user enters a new password, populates the other fields, then clicks **Confirm**.
    - The new admin user's name will now display in the list of users under Mobile Protection.
    - By default, the new admin user does not include a name.
14. To add a name to this admin user, from the drop-down menu, select **Manage Users**,
15. Click the **Edit** button for that user entry, and make your changes on the User Details tab.
16. To enroll a device for this admin user, highlight the user name and click **Enroll**.

    The user receives another confirmation email, which includes a link to the app, a temporary password, and instructions.

17. Once the user has confirmed, you can change the default group assigned to that user. Each device inherits the policies assigned to that user's group.

    For more information, see *Moving Users Between Groups on page 65*.

18. If a user has more than one device, you can add and enroll additional devices from the Devices tab and assign them to the appropriate user.

    For more information, see *Adding Devices to Your Account on page 15*.

Importing Active Directory Users

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

To import an Active Directory user:

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.
3. Click the **Go to Mobile Protection** button.

   The Mobile Protection console displays with the Status tab active..

4. Click the **Users & Groups** tab.

   The Users & Groups tab displays.

5. In the All Users area, click the **Import Users** icon.

   The Import Users window displays.

6. Browse to the CSV file you created and select it.
7. Click the **Import** button.

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

8. Do either of the following:
   - To add a single user, highlight the name and click **Enroll** in the toolbar.
   - To add multiple users, press **Ctrl-Click** to highlight multiple users and click **Enroll** in the toolbar.

   Each user receives a confirmation email that includes instructions, a temporary password, and a link to install the app on the device and enroll.

   Once the user has installed the app on the device and enrolled, you can change the default group assigned to that user.

   Each device inherits the policies assigned to that user's group. For more information, see *Moving Users Between Groups on page 65*.

If a user has more than one device, you can add and enroll additional devices from the Devices tab and assign them to the appropriate user. For more information, see *Adding Devices to Your Account on page 15*.

Viewing User Details

You can view a list of users from the Users & Groups tab.

To view a user's details:

1. Log in to the SecureAnywhere website.
2. Click the **Go to Mobile Protection** button.

   The Mobile Protection console displays with the Status tab active.

3. Click the **Users & Groups** tab.

   The Users & Groups tab displays.

4. In the Groups pane, click on a group name..

   The Users pane displays the users in that group.

5. Do either of the following:
   - In the Users area, click on a single user..
   - In the Groups pane, select **All Groups** to view all users or a specific groups of users.
6. The User Details window displays with the Details tab active.

   The following table describes the information on the All Users pane.

FIELD	DESCRIPTION
First Name	User's first name.
Last Name	User's last name.
Email	User's email address; must be unique.

FIELD	DESCRIPTION
Devices	Number of devices associated with this user.
Administrator	Whether or not this user has administrator privileges.
Group	Name of group this user is assigned to. • Displays only if All Groups is selected in the Groups panel. • Each user must be assigned to one group. • By default, new users are initially assigned to the Default Group. • If needed, you can click-and-drag a user to a new group.

7. To add or remove columns from the display by clicking the down-arrow on a column, selecting **Columns**, and enabling/disabling one or more columns.

8. To display device details associated with each user record by double clicking on the user name.

   The User Details window displays with two tabs.

   - **Details** — Mirrors the User list, see table above. If needed, you can select a different group from the drop-down menu.
   - **Devices** — Provides details about each device associated with this user. The table below describes each field:

FIELD	DESCRIPTION
Operating System	Operating system of this device. Either Android or iOS. Informational only.
Manufacturer	Manufacturer of device. Informational only.
Model	Model name of this device. Informational only.
Device Phone Number	If applicable, the phone number associated with this device. This number is used by Mobile Protection to communicate with the device.
Policy	Name of policy assigned to this device. • The default is the policy assigned to the group this device's user belongs to. • You can associate a different policy with this device by double-clicking the policy name. • You can also design a custom policy for this device only. • A drop-down menu displays from which you can select the new policy. • When you're done, click the **Save** button.
Last Check-in	System-supplied, the date this device last sent information to the Mobile Protection administration app. Set the time zone from the **Account Settings** drop-down menu.

9. To view the status of a device, double-click it. For more information, see *Viewing Device Statuses on page 18*.

Managing User Data

The list of users displays when you click the Users & Groups tab and, from the Groups panel, select either of the following:

- A specific group whose users you want to view.
- All Groups to display all users.

You can drag a column to a new location, and sort the items in the columns. To change the sorting, hover your cursor over a column header to open the drop-down menu. 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.

This topic contains the following procedures:

Adding Users to Your Account

Click any of the following links to display information about adding users to your account.

- *Importing Active Directory Users on page 52*.
- *Adding Users on page 45*.
- *Adding Admin Users on page 48*

Deleting Users From Your Account

Use the following procedure to remove users from your account.

To remove a user from your account:

1. Log in to the SecureAnywhere website.
2. Click the **Go to Mobile Protection** button.

   The Mobile Protection console displays with the Status tab active.

3. Click the **Users & Groups** tab.

   The Users & Groups tab displays.

4. Select one or more users in the list.

   Note: You can only remove non-admin users.

5. Click the **Delete User** icon.

Resetting User Passwords for Android Devices

Use the following procedure to reset user passwords for Android devices.

To reset a password for an Android device:

1. Log in to the SecureAnywhere website.
2. Click the **Go to Mobile Protection** button.

   The Mobile Protection console displays with the Status tab active.

3. Click the **Users & Groups** tab.

   The Users & Groups tab displays.

4. Select a user in the list.

   Note: For admin users, you must reset the password from the Account Settings option in the drop-down menu.

5. Click the **Reset Password** icon.

   The system displays a Rest User Password window.

6. In the Password field, enter the new password.
7. In the Confirm Password field, enter the new password again.

8. Click the **Save** button.

   The system saves the new password.

Enrolling Users in Mobile Protection

Use the following procedure to reset user passwords for android devices.

To reset a password:

1. Log in to the SecureAnywhere website.
2. Click the **Go to Mobile Protection** button.

   The Mobile Protection console displays with the Status tab active.

3. Click the **Users & Groups** tab.

   The Users & Groups tab displays.

4. Do either of the following:
   - Select a user from the list.
   - Press **Ctrl-Click** to select multiple users.
5. Click the **Enroll** icon.

   The system displays a confirm message.

6. Click the **OK** button.

   Users receive email instructions to complete the enrollment.

Adding Groups

A group is a collection of users to which you assign a common set of policies. For example, you might want to create groups based on the different departments of your company.

Each group has up to two policies associated with it, one for Android devices and another for iOS devices.

- If a member of the group has an Android device, that policy is applied to that user's device.
- If a member of the group has an iOS device, the iOS policy is applied to the user's device.

To add a group:

1. Log in to the SecureAnywhere website.
2. Click the **Go to Mobile Protection** button.

   The Mobile Protection console displays with the Status tab active.

3. Click the **Users & Groups** tab.

   The Users & Groups tab displays.

4. In the Groups panel, click the **Add** icon.

   The Add Group window displays.

   - By default, new users are assigned to the Default Group.
   - You can move users into your new group by clicking and dragging the users from the Users panel onto the Group name.

5. Populate the fields using the information in the following table.

FIELD	DESCRIPTION
Name	The name of the group.
Description	Description for the group.
Domain	Informational only.
Android Policy	The default policy to be applied to all Android devices belonging to users in this group.
iOS Policy	The default policy to be applied to all iOS devices belonging to users in this group.

6. When you're done, click the **Save** button.

Editing and Deleting Groups

In the Users & Groups tab, you can *To edit a group: on page 63*and *To delete a group: on page 63*.

To edit a group:

1. Log in to the SecureAnywhere website.
2. Click the **Go to Mobile Protection** button.

   The Mobile Protection console displays with the Status tab active.

3. Click the **Users & Groups** tab.

   The Users & Groups tab displays.

4. Click on one or more users and drag them to the new group under the Groups panel.

   A message displays, describing how the new group's policies will now be applied to any devices associated with this user.

5. Do either of the following:
   - Double-click the group name.
   - Highlight the group name.
6. Click **Edit**.
7. Make your changes and click the **Save** button.

To delete a group:

1. Log in to the SecureAnywhere website.
2. Click the **Go to Mobile Protection** button.

   The Mobile Protection console displays with the Status tab active.

3. Click the **Users & Groups** tab.

   The Users & Groups tab displays.

4. Click on one or more users and drag them to the new group under the Groups panel.

   A message displays, describing how the new group's policies will now be applied to any devices associated with this user.

5. Highlight the group you want to delete.
6. Click **Delete**.

   If there are any users assigned to the group, the system prompts you to select a new group for them

---

Moving Users Between Groups

Each user is added to the group that is highlighted when you added the user record. If you had no group highlighted, new users are added to the Default Group.

You can click and drag one or more users to a different group, as described in this procedure..

To move a user between groups:

1. Log in to the SecureAnywhere website.
2. Click the **Go to Mobile Protection** button.

   The Mobile Protection console displays with the Status tab active.

3. Click the **Users & Groups** tab.

   The Users & Groups tab displays.

4. Click on one or more users and drag them to the new group under the Groups panel.

   A message displays, describing how the new group's policies will now be applied to any devices associated with this user.

5. When you're ready, click the **Move Users** button to complete.

Viewing Group Details

The list of groups displays when you click the **Users & Groups** tab. The Group panel displays the group name and number of members.

When you select a group name, the Users panel displays users that belong to that group and the Policies panel displays policies associated with that group or with members in the group.

Follow this procedure to view details about a group.

To view group details:

1. Log in to the SecureAnywhere website.
2. Click the **Go to Mobile Protection** button.

   The Mobile Protection console displays with the Status tab active.

3. Click the **Users & Groups** tab.

   The Users & Groups tab displays with the group name and number of members.

4. In the Groups pane, select a group.
   - The Users panel displays users that belong to that group.
   - The Policies panel displays policies associated with that group.
5. To display additional details about each group record, double-click on the group name.

   The Group Details window displays.

FIELD	DESCRIPTION
Name	The name of the group.
Description	Description for the group.

FIELD	DESCRIPTION
Domain	Informational only.
Android Policy	The default policy to be applied to all Android devices belonging to users in this group.
iOS Policy	The default policy to be applied to all iOS devices belonging to users in this group.

6. From the Group Details window, you can do either or both of the following:

   - *Editing and Deleting Groups on page 63*.
   - Select a new policy for *Android Policy Options on page 72* or *iOS Policy Options on page 78*.

Chapter 6: Managing Policies

To manage policies, see the following topics:

Policies Overview

A policy is a set of behavior definitions that the administrator assigns to a group of users.

For example, you might want to require passwords on devices for users in a high-security group but not for other types of users. For some groups of users, you might need extremely stringent security requirements such as high-strength password formats and frequent automatic scans. Other groups might require lost device protection but no passwords.

When you enroll a device for a user, that device inherits the policies associated with the group to which the user belongs. If necessary, you can override the group policy with a device-specific policy.

SecureAnywhere Mobile Protection installs with the following policies:

- Default Group
- Default Android Policy
- Default iOS Policy

Adding Policies

To add a policy:

1. Log into the SecureAnywhere website.
2. Click the **Go to Mobile Protection** button.

   The Mobile Protection console displays with the Status tab active.

3. Click the **Policies** tab.

   The Policies tab displays.

4. Click the **Add a policy** icon.

   The Policy Details window displays with the General tab active.

5. In the Policy name field, enter a name for the policy.
6. In the Description field, enter a description for the policy.
7. From the Operating system drop-down field, select one of the following:
   - **Android**
   - **iOS**

   > **Note:** The contents of the Protection and Communication tabs differ depending on the operating environment. The default layout is Android. For more information about policy options and tab-specific instructions, see *Android Policy Options on page 72* and *iOS Policy Options on page 78*.

8. As you define your policy, you can save it in draft form by clicking the **Save Changes to Draft** button.
9. When you are finished defining the entire policy, click **Promote Draft to Live**.
10. Once you have created the policy, follow the *Adding Groups on page 61* procedure to assign the policy to a group.

Viewing Policies

In the Policies tab, you can view a list of all defined policies. Two default policies are provided with the product:

- Default Android Policy
- Default iOS Policy

> **Note:** For more information on policy options, see *Android Policy Options on page 72* and *iOS Policy Options on page 78*.

To view a policy:

1. Log in to the SecureAnywhere website.
2. Click the **Go to Mobile Protection** button.

   The Mobile Protection console displays with the Status tab active.

3. Click the **Policies** tab.
   - The Policies tab displays the list of policies.
   - The Groups area below displays groups associated with the policy selected in the top panel.
4. To **Add**, **Delete**, and **Duplicate** policies, click the appropriate button.
5. To search for a specific policy name, enter that policy name in the **Search** field.
6. To export policy information to a CSV file, in the upper right corner, click the **Export** button.
7. To refresh the screen, in the upper right corner, click the **Refresh** button.
8. To view details about a policy, double-click the name of the policy.
9. To change policies assigned to a group, double-click the name of the group.

Android Policy Options

General Tab

The table below describes policy options in the General tab.

FIELD	DESCRIPTION
Policy Name	User-supplied name for this policy.
Description	User-supplied description.
Operating System	OS of mobile device; must be Android.

Protection Tab

The tables below describes security settings defined in the Protection tab.

Antivirus Shields

FIELD	DESCRIPTION
Install Shield	Select **On** to prevent apps identified as threats from installing on the device. On is the default.
File System Shield	Select **On** to display an alert if a threat is detected on the mobile's memory card. On is the default.
Execution Shield	Select **On** to prevent an app identified as a threat from installing or executing on the mobile. On is the default.
Unknown Sources Shield	Select **On** to warn if the device has Unknown Sources enabled. On is the default.
USB Debugging Shield	Select **On** to warn if the device has USB Debugging setting enabled. On is the default.

Antivirus Schedule

FIELD	DESCRIPTION
Automatic scan frequency	Select how often you want an automatic scan to run on the device. Options: • **Never** • **Hourly** • **Daily** — This is the default. • **Weekly**
Automatic threat definition update frequency	Select how often you want threat definitions updated. Options: • **Never** • **Hourly** • **Daily** — This is the default. • **Weekly**

Lost Device Protection

FIELD	DESCRIPTION
Lost Device Protection	Select **On** to enable lost device protection features such as lock, wipe, locate, and scream. On is the default.
SIM Card Lock	Select **On** to lock the device if someone removes or exchanges the SIM card. On is the default.

SMS Blocking

FIELD	DESCRIPTION
Block malicious SMS messages	Select **On** to block SMS messages deemed malicious according to current threat definitions. On is the default.

Secure Web Browsing

FIELD	DESCRIPTION
Block known malicious websites	Select **On** (default) to prevent access to known malicious websites.

Device Lock

FIELD	DESCRIPTION
Require a passcode	Select **On** to require a password to access the device. On is the default.
Minimum passcode length	Select the minimum required length of password. Options: • **4 through 16**. • **4** is the default.

FIELD	DESCRIPTION
Idle time before automatic device lock	Amount of idle time before the device is locked and requires a password to unlock. Options: • **Off** • **15 or 13 seconds** • **1 minute** — This is the default. • **2 minutes** • **3 minutes** • **4 minutes** • **5 minutes** • **10 minutes** • **15 minutes** • **30 minutes** • **60 minutes**
Minimum passcode strength	Required format of passwords. Options: • **Off** • **Alphabetic, PIN or Pattern** — This is the default. • **Alphanumeric or PIN** • **Alphabetic** — At least letters. • **Alphanumeric** — Letters and numbers.

iOS Policy Options

Described below are the policy options for iOS devices.

General Tab

The table below describes policy options in the General tab.

FIELD	DESCRIPTION
Policy Name	User-supplied name for this policy.
Description	User-supplied description.
Operating System	OS of mobile device. Must be iOS.

Protection Tab

The table below describes policy options in the Protection tab.

FIELD	DESCRIPTION
Require a passcode	Select **On** to require a password to access the device. On is the default.
Allow simple passcode	Select **Yes** to allow simple passcodes. Yes is the default. A simple passcode is one that repeats or uses ascending or descending sequences, such as *111*, *123* or *abc*.
Require at least one letter	Select **Yes** to require that passcodes include at least one alphabetic character. No is the default.
Minimum passcode length	Select the minimum required length of password. Options: • **4** — This is the default. • **1 through 16**
Minimum number of non-alphanumeric characters	Allows you to require one or more special characters such as # or % in the password. Options: • **None** — This is the default. • **1 through 4**

FIELD	DESCRIPTION
Require passcode change every__days	Type or select a number from 0 to 730 to specify the number of days that a password remains valid, after which the user is prompted for a new password. Zero (0) means the password remains valid indefinitely.
Idle time before automatic device lock	Amount of idle time in minutes before the device is locked and requires a password to unlock. Options: • **Off** • **1** — This is the default. • **2 minutes** • **3 minutes** • **4 minutes** • **5 minutes** • **10 minutes** • **15 minutes**
Prevent passcode re-use for passcodes	Select a number from **0** (**zero**) to **50** to specify the number of password changes that must occur before the user can re-use a password. Zero (0) means the user can re-use passwords any time.

FIELD	DESCRIPTION
After locking, require passcode to unlock device	Select the amount of time that can elapse before a password is required to unlock the device. Options: • **Immediately** • **1 minute** • **5 minute** • **15 minutes** • **1 hour** • **4 hours**
Erase device after__ failed login attempts	Select an option that enables an automatic erase after the number of failed sign-on attempts. Options: • **Off** means the device will not be erased. This is the default. • 4 through 10 mean the device will be erased after that number of failed attempts.

Adding Email Profiles

The Communication tab allows you to create profiles defining communication settings for iOS devices. Supported communication methods are Email, Wi-Fi, and VPN.

To add an email profile:

1. Log in to the SecureAnywhere website.
2. Click the **Go to Mobile Protection** button.

   The Mobile Protection console displays with the Status tab active.

3. Click the **Policies** tab.

   The Policies tab displays.

4. Double-click the policy to which you want to add an Email profile.

   The Policy Details window displays with the General tab active.

5. Click the **Communication** tab.
6. In the Category column, select **Email**.
7. In the upper right of the Policy Details window, click the **+ (plus)** button to create a new profile.

   The New panel displays.

8. Populate the fields using the information in the following table.

FIELD	DESCRIPTION
Display name of email account	Enter the name of the email profile. This is a free-form text field and is required.
Account type	From the drop-down menu, select the type of email account: • **IMAP** • **POP**
Path prefix	Enter the path prefix. This is a free-form field and is required with IMAP.
User display name	This is a free-form field and is optional.
User email address	Free-form text, optional.
Allow user to move messages to other email accounts	Select either **Yes** or **No**. Yes is the default.
Incoming Mail Server	This is a free-form field, and is optional.

FIELD	DESCRIPTION
Incoming Mail Port	Enter or select a port number.
Incoming Mail Username	This is a free-form field, and is optional.
Incoming Mail Authentication Type	Type of authentication used for incoming messages. Options: • **None** • **Password** — This is the default. • **MD5 challenge-response** • **NTLM** • **HTTP MD5 digest**
Incoming Mail Password	This is a free-form field, and is optional.
Incoming Mail Use SSL	Defines whether or not SSL will be used for incoming mail. Yes or No. No is the default.
Outgoing Mail Server	This is a free-form field, and is optional.
Outgoing Mail Port	Type or select the outgoing port number.

FIELD	DESCRIPTION
Outgoing Mail Username	This is a free-form field, and is optional.
Outgoing Mail Authentication Type	Type of authentication used for outgoing messages. Options: • **None** • **Password** — This is the default. • **MD5 challenge-response** • **NTLM** • **HTTP MD5 digest**
Outgoing Mail Use same password as Incoming Mail	Specifies whether to use the same password for incoming and outgoing messages. No is the default.
Outgoing Mail Password	If the above is No, enter the outgoing mail password. Free-form text, optional.
Outgoing Mail Use SSL	Defines whether or not SSL will be used for outgoing mail. No is the default.
Outgoing Mail Allow recent address syncing in iOS with this account	No is the default.

FIELD	DESCRIPTION
Outgoing Mail Only allow Mail app to use this outgoing mail account	No is the default.
Outgoing Mail Use S/MIME encryption	No is the default.
Outgoing Mail Signing certificate	If S/MIME is Yes, lists the detected certificates.
Outgoing Mail Encryption certificate	If S/MIME is Yes, lists the detected certificates.

9. When you're done, click the **Save Changes** button.
10. When you are ready to go live with this policy, click **Promote Draft to Live**.

Adding Exchange Active Sync Profiles

To add an Exchange ActiveSync profile:

1. Log in to the SecureAnywhere website.
2. Click the **Go to Mobile Protection** button.

   The Mobile Protection console displays with the Status tab active.

3. Click the **Policies** tab.

   The Policies tab displays.

4. Double-click the policy to which you want to add an ActiveSync profile.

   The Policy Details window displays with the General tab active.

5. Click the **Communication** tab.

   The Communication tab displays.

6. In the Category column, select **Exchange ActiveSync**.
7. In the upper right of the Policy Details window, click the **+ (plus)** button to create a new profile.

   The New panel displays.

8. Complete the fields using the information in the following table:

FIELD	DESCRIPTION
Account Name	Name for the Exchange ActiveSync account. Free-form text field; this is a required field.
Exchange ActiveSync Host	Microsoft Exchange Server. Free-form text field; this is a required field.
Use SSL	Send all communication through secure socket layer. Select **Yes** or **No**.
Allow Move	Allow user to move messages from this account. Select **Yes** or **No**.
Allow Recent Address Syncing	Include this account in recent address syncing. Select **Yes** or **No**.
Use Only in Mail	Send outgoing mail from this account only from Mail app. Select **Yes** or **No**.

FIELD	DESCRIPTION
Use S/MIME	Send outgoing mail using S/MIME encryption. Select **Yes** or **No**.
Signing certificate	Credentials for signing MIME data. If S/MIME is yes, lists the detected certificates.
Encryption certificate	Credentials for encrypting MIME data. If S/MIME is yes, lists the detected certificates.
User	User for the account, including domain. Free-form text field; this is a required field.
Email Address	The address of the account. Free-form text field; this is a required field.
Password	The password for the account. Free-form text field; this is a required field.

FIELD	DESCRIPTION
Identity Certificate	Credentials for connection to ActiveSync. Lists detected credentials. This is a required field.
Past Days of Mail to Sync	Options: • **Unlimited** — This is the default. • **One day** • **Three days** • **One week** • **Two weeks** • **One month**

9. When you're done, click the **Save Changes** button.
10. When you are finished and ready to go live with this policy, click **Promote Draft to Live**.

Adding VPN Profiles

To add a VPN profile:

1. Log in to the SecureAnywhere website.
2. Click the **Go to Mobile Protection** button.

   The Mobile Protection console displays with the Status tab active.

3. Click the **Policies** tab.

   The Policy tab displays.

4. Double-click the policy where you want to add a VPN profile.

   The Policy Details window displays with the General tab active.

5. Click the **Communication** tab.

   The Communication tab displays.

6. In the Category column, click **VPN** .

   The New panel displays.

7. In the upper right of the Policy Details window, click the **+ (plus)** button to create a new profile.

   The New panel displays.

8. In the Connection name field, enter the name of the connection. This free-form field is required.
9. From the Connection type drop-down menu, select one of the following VPN connections:
   - **L2TP** — This is the default.
   - **PPTP**
   - **Ipsec (Cisco)**
   - **Cisco AnyConnect**
   - **Juniper SSL**
   - **F5 SSL**
   - **SonicWALL Mobile Connect**

- **Check Point Mobile VPN**
- **Aruba VIA**
- **OpenVPN**
- **Custom SSL**

10. Based on your selection in the previous step, use the appropriately associated table below for guidance to complete the fields.

(Server Account Details) If Connection type = L2TP

FIELD	DESCRIPTION
Server hostname/IP address	Free-form text field; this is a required field.
Account username (leave blank if username is set on the device)	Free-form text field; this is an optional field.
User authentication type	Options: • **Password** — This is the default. • **RSA SecureID**
Password for connection authentication	If authentication type = password.

FIELD	DESCRIPTION
Shared secret	Free-form text field; this is an optional field.
Route all network traffic through VPN connection	Select **Yes** or **No**. No is the default.

(Server Account Details) If Connection type = PPTP

FIELD	DESCRIPTION
Server hostname/IP address	Free-form text field; this is a required field.
Account username (leave blank if username is set on the device)	Free-form text field; this is an optional field.
User authentication type	Options: • **Password** — This is the default. • **RSA SecureID**
Password for connection authentication	If authentication type = password.

FIELD	DESCRIPTION
Encryption level	Options: • **None** - This is the default. • **Automatic, Maximum (128 bit)**
Route ALL network traffic through VPN connection	Select **Yes** or **No**. No is the default.

(Server Account Details) If Connection type = IPsec (Cisco)

FIELD	DESCRIPTION
Server hostname/IP address	Free-form text field; this is a required field.
Account username (leave blank if username is set on the device)	Free-form text field; this is an optional field.
Account password (leave blank if password is set on the device)	Free-form text field; this is an optional field.

FIELD	DESCRIPTION
Machine authentication type	Options: • **Shared Secret/Group Name** — This is the default. • **Certificate**
Group name	If Machine Authentication type = Shared Secret/Group Name, free-form text, optional.
Shared secret	If Machine Authentication type = Shared Secret/Group Name, free-form text, optional.
Use hybrid identification (Authenticate with secret, name and server-side authentication)	If Machine Authentication type = Shared Secret/Group Name, Yes or No. No is the default.
Prompt user for password on device	If Machine Authentication type = Shared Secret/Group Name, Yes or No. No is the default.
Credentials for authenticating connection	If Machine Authentication type = Certificate, a list of detected certificates.

FIELD	DESCRIPTION
Include user PIN. Request PIN during connection and send with authentication	If Machine Authentication type = Certificate, Yes or No. No is the default.
Enable VPN On Demand. Domain and host names that will establish a VPN	If Machine Authentication type = Certificate, Yes or No.

(Server Account Details) If Connection type = Cisco AnyConnect

FIELD	DESCRIPTION
Server hostname/IP address	Free-form text field; this is a required field.
Account username (leave blank if username is set on the device)	Free-form text field; this is an optional field.
Group	Free-form text field; this is an optional field.
User authentication	Options: • **Password** — This is the default. • **Certificate**

FIELD	DESCRIPTION
Password for connection authentication	If authentication type = password.
Credentials for authenticating connection	If User authentication type = Certificate, a list of detected certificates.
Include user PIN. Request PIN during connection and send with authentication	If User authentication type = Certificate, Yes or No. No is the default.
Enable VPN On Demand. Domain and host names that will establish a VPN	If User authentication type = Certificate. Yes or No.

(Server Account Details) If Connection type = Juniper SSL

FIELD	DESCRIPTION
Server hostname/IP address	Free-form text field; this is a required field.
Account username (leave blank if username is set on the device)	Free-form text field; this is a required field.

FIELD	DESCRIPTION
Realm for authenticating the connection (leave blank if realm is set on the device)	Free-form text field; this is an optional field.
Role for device authentication (leave blank if realm is set on the device)	Free-form text field; this is an optional field.
User authentication	Options: • **Password** — This is the default • **Certificate**
Password for connection authentication	If authentication type = password.
Credentials for authenticating connection	If User authentication type = Certificate, a list of detected certificates.
Include user PIN. Request PIN during connection and send with authentication	If User authentication type = Certificate, Yes or No. No is the default.
Enable VPN On Demand. Domain and host names that will establish a VPN	If User authentication type = Certificate. Yes or No.

(Server Account Details) If Connection type = F5 SSL

FIELD	DESCRIPTION
Server hostname/IP address	Free-form text field; this is a required field.
Account username (leave blank if username is set on the device)	Free-form text field; this is an optional field.
User authentication	Options: • **Password** — This is the default • **Certificate**
Password for connection authentication	If authentication type = password.
Credentials for authenticating connection	If User authentication type = Certificate, a list of detected certificates.
Include user PIN. Request PIN during connection and send with authentication	If User authentication type = Certificate, Yes or No. No is the default.
Enable VPN On Demand. Domain and host names that will establish a VPN	If User authentication type = Certificate. Yes or No.

(Server Account Details) If Connection type = SonicWALL Mobile Connect

FIELD	DESCRIPTION
Server hostname/IP address	Free-form text field; this is a required field.
Account username (leave blank if username is set on the device)	Free-form text field; this is an optional field.
Login group or domain (leave blank if group/domain is set on the device)	Free-form text field; this is an optional field.
User authentication	Options: • **Password** — This is the default • **Certificate**
Password for connection authentication	If authentication type = password.
Credentials for authenticating connection	If User authentication type = Certificate, a list of detected certificates.

FIELD	DESCRIPTION
Include user PIN. Request PIN during connection and send with authentication.	If User authentication type = Certificate, Yes or No. No is the default.
Enable VPN On Demand. Domain and host names that will establish a VPN	If User authentication type = Certificate, Yes or No.

(Server Account Details) If Connection type = Check Point Mobile VPN

FIELD	DESCRIPTION
Server hostname/IP address	Free-form text field; this is a required field.
Account username (leave blank if username is set on the device)	Free-form text field; this is an optional field.
User authentication	Options: • **Password** — This is the default • **Certificate**
Password for connection authentication	If authentication type = password.

FIELD	DESCRIPTION
Credentials for authenticating connection	If User authentication type = Certificate, a list of detected certificates.
Include user PIN. Request PIN during connection and send with authentication	If User authentication type = Certificate, Yes or No. No is the default.
Enable VPN On Demand. Domain and host names that will establish a VPN	If User authentication type = Certificate, Yes or No.

(Server Account Details) If Connection type = Aruba VIA

FIELD	DESCRIPTION
Server hostname/IP address	Free-form text field; this is a required field.
Account username (leave blank if username is set on the device)	Free-form text field; this is an optional field.

FIELD	DESCRIPTION
User authentication	Options: • **Password** — This is the default • **Certificate**
Password for connection authentication	If authentication type = password.
Credentials for authenticating connection	If User authentication type = Certificate, a list of detected certificates.
Include user PIN. Request PIN during connection and send with authentication	If User authentication type = Certificate, Yes or No. No is the default.
Enable VPN On Demand. Domain and host names that will establish a VPN	If User authentication type = Certificate, Yes or No.

(Server Account Details) If Connection type = OpenVPN

FIELD	DESCRIPTION
Server hostname/IP address	Free-form text field; this is a required field.
Account username (leave blank if username is set on the device)	Free-form text field; this is an optional field.
User authentication	Options: • **Password** — This is the default • **Certificate**
Password for connection authentication	If authentication type = password.
Credentials for authenticating connection	If User authentication type = Certificate, a list of detected certificates.
Include user PIN. Request PIN during connection and send with authentication	If User authentication type = Certificate, Yes or No. No is the default.
Enable VPN On Demand. Domain and host names that will establish a VPN	If User authentication type = Certificate, Yes or No.

(Server Account Details) If Connection type = Custom SSL

FIELD	DESCRIPTION
Identifier. Reverse DNS format identifier for custom SSL VPN	Free-form text field; this is a required field.
Server hostname/IP address	Free-form text field; this is a required field.
Account username (leave blank if username is set on the device)	Free-form text field; this is an optional field.
Custom data	User-managed list of Key/Value pairs. • To add a key/value pair, click the **+** (**Plus**) sign. • To delete an entry, highlight the entry and click the **-** (**Minus**) sign. • Key Column: Free-form text • Value Column: Free-form text
User authentication	Options: • **Password** — This is the default. • **Certificate**
Password for connection authentication	If authentication type = password.

FIELD	DESCRIPTION
Credentials for authenticating connection	If User authentication type = Certificate, a list of detected certificates.
Include user PIN. Request PIN during connection and send with authentication	If User authentication type = Certificate, Yes or No. No is the default.
Enable VPN On Demand. Domain and host names that will establish a VPN.	If User authentication type = Certificate, Yes or No.

11. Complete the following proxy settings:

FIELD	DESCRIPTION
Proxy	Options: • **None** — This is the default. • **Manual** • **Automatic**
Proxy server URL. Server from which to get proxy settings.	• If Proxy = Automatic. • Free-form text field; this is a required field.

FIELD	DESCRIPTION
Proxy server. Fully qualified address and port of proxy server.	• If Proxy = Manual. • Free-form text field; this is a required field.
Proxy port. Fully qualified port of proxy server.	• If Proxy = Manual. • Free-form text field; this is a required field.
Proxy username	• If Proxy = Manual. • Free-form text field; this is a required field.
Proxy password	• If Proxy = Manual. • Free-form text field; this is a required field.

12. When you're done, click the **Save Changes** button.
13. When you are finished and ready to go live with this policy, click **Promote Draft to Live.**

Adding Wi-Fi Profiles

To add a wi-fi profile:

1. Log in to the SecureAnywhere website.
2. Click the **Go to Mobile Protection** button.

   The Mobile Protection console displays with the Status tab active.

3. Click the **Policies** tab.

   The Policy tab displays.

4. Double-click on the policy to which you want to add a wi-fi profile.

   The Policy Details window displays with the General tab active.

5. Click the **Communication** tab.

   The Communication tab displays.

6. In the Category column, select **Wi-Fi.**
7. In the upper right of the Policy Details window, click the **+ (plus)** button to create a new profile.

   The New panel displays.

8. Use the following table to complete the fields in the New panel.

FIELD	DESCRIPTION
Service Set Identifier (SSID)	Enter the network name. This is a free-form field.
Auto join	From the drop-down menu, select either **Yes** or **No** to determine whether to automatically join when this network is detected. Yes is the default.
Hidden network	From the drop-down menu, select either **Yes** or **No** to determine whether the target network is open for broadcasting. No is the default.
Security type	From the drop-down men, select one of the following to determine the preferred type of encryption: • **None** — This is the default. • **WEP (personal)** • **WPA/WPA2 (personal)** • **Any (personal)** • **WEP (enterprise)** • **WPA/WPA2 (enterprise)** • **Any (enterprise)**

FIELD	DESCRIPTION
Password	Enter the password for this profile. This field only displays if the Security type field displays one of the following: • WEP (personal) • WPA/WPA2 (personal) • Any (personal)
Protocols Accepted EAP types. Authentication protocols accepted on the target network	Select one of the following checkboxes to select accepted protocols: • **TLS** • **TTLS** • **LEAP** • **PEAP** • **EAP-FAST** • **EAP-SIM** This field only displays if the Security type field displays one of the following: • WEP (enterprise) • WPA/WPA2 (enterprise) • Any (enterprise)

FIELD	DESCRIPTION
Protocols EAP-FAST. Configuration of Protected Access Credentials (PAC)	Select one of the following checkboxes: • **Use PAC. If Use PAC=enabled, Provision PAC** • **If Provision PAC = enabled, Provision PAC anonymously** This field only displays if the Security type field displays one of the following: • WEP (enterprise) • WPA/WPA2 (enterprise) • Any (enterprise)
Authentication Username	Enter the authentication user name. This is a free-form field. This field only displays if the Security type field displays one of the following: • WEP (enterprise) • WPA/WPA2 (enterprise) • Any (enterprise)

FIELD	DESCRIPTION
Authentication. Use per-connection password. User provides password during connection request	From the drop-down menu, select either **Yes** or **No**. No is the default. This field only displays if the Security type field displays one of the following: • WEP (enterprise) • WPA/WPA2 (enterprise) • Any (enterprise)
Authentication password	Enter the authentication password. This is a free-form field. This field only displays if the Security type field displays one of the following: • WEP (enterprise) • WPA/WPA2 (enterprise) • Any (enterprise)
Authentication Identity certificate. Credentials for connection to wireless network	Credentials for connection to wireless network. This field only displays if the Security type field displays one of the following: • WEP (enterprise) • WPA/WPA2 (enterprise) • Any (enterprise)

FIELD	DESCRIPTION
Authentication Outer Identity. Externally visible identification (for TTLS, PEAP, and EAP-FAST)	Enter the externally visible identity. This is a free-form field. This field only displays if the Security type field displays one of the following: • WEP (enterprise) • WPA/WPA2 (enterprise) • Any (enterprise)
Trusted certificates. Certificates trusted/expected for authentication	Lists detected certificates. This field only displays if the Security type field displays one of the following: • WEP (enterprise) • WPA/WPA2 (enterprise) • Any (enterprise)
Trusted server certificate names. Certificate names expected from authentication server	User-managed list of server certificate names. You can add or remove names using the + (plus) and - (minus) buttons.

FIELD	DESCRIPTION
Proxy setup	From the drop-down menu, select one of the following to configure a proxy to be used with the network: • **None** — This is the default. • **Automatic** • **Manual** This is an optional field.
Proxy Server URL	Enter the URL of the proxy server. This field only displays if the Proxy setup field is set to Automatic.
Proxy server	Enter the host name or IP address of the proxy server. This field only displays if the Proxy setup field is set to Manual.
Proxy port	Enter the port number for the proxy server. This field only displays if the Proxy setup field is set to Manual.

FIELD	DESCRIPTION
Authentication	Enter the username to be used to connect to the proxy server. This field only displays if the Proxy setup field is set to Manual.
Password	Enter a password to be used to connect to proxy server. This field only displays if the Proxy setup field is set to Manual.

9. When you're done, click the **Save Change**s button.
10. When you are finished and ready to go live with this policy, click the **Promote Draft to Live** button.

Exporting Policy Results

To export a policy to CSV file:

1. Log in to the SecureAnywhere website.
2. Click the **Go to Mobile Protection** button.

   The Mobile Protection console displays with the Status tab active.

3. Click the **Policies** tab.

   The Policies tab displays.

4. In the Policy Name column, click the policy you want to export.
5. In the upper right corner of the Policies tab, click the **Export** button.

   The CSV file downloads to your Downloads folder.

Deleting Policies

To delete a policy:

1. Log in to the SecureAnywhere website.
2. Click the **Go to Mobile Protection** button.

   The Mobile Protection console displays with the Status tab active.

3. Click the **Policies** tab.

   The Policies tab displays.

4. Select the policy you want to delete.

   The lower panel displays any groups associated with this policy.

   Note: Before deleting the policy, you should assign replacement policies to any groups associated with it.

5. Click the **Delete Policy** icon.

   The system checks to see if this policy is assigned to any groups or devices.

   - If the policy isn't assigned, the system displays a Delete confirmation window. Click the **OK** button.
   - If the policy isn't assigned, the system prompts you to select a different policy for those groups and devices. From the drop-down menu, select the policy you want to delete and click **Apply**.

Chapter 7: Working With Reports

To get started working with reports, see the following topics:

Generating 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.
2. Click the **Go to Mobile Protection** button.

   The Mobile Protection console displays with the Status tab active.

3. Click the **Reports** tab.

   The Reports tab displays.

4. Select **Inventory Management**. If needed, click the **Down** arrow to expand the Inventory Management tree.
5. Select any of the following 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.

   The results of the generated report display in the lower panel. Device status is displayed using color-coded icons. For more information on color-coded icons, see *Viewing Device Statuses on page 18*.

6. Do either or both of the following:
   - To display specific devices, enter your query in the **Search** field at the top of the list.
   - To see more information about a specific item, double-click the entry.
7. When you're done, click a different tab to exit out of the Reports tab.

Generating 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.
2. Click the **Mobile Protection** tab.

   The Mobile Protection console displays with the Status tab active.

3. Click the **Go to Mobile Protection** button.

   The Reports tab displays.

4. Select Device Status. If needed, click the **Down** arrow to expand the Device Status tree.
5. Select any of the following 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.
6. Do either of the following, as needed:
   - To display specific devices, enter your query in the **Search** field at the top of the list.
   - To see more information about a specific item, double-click the entry.
7. When you're done, click the **Close** button in the Report tab to exit.

Generating Alerts and Infection Reports

You can generate reports that display the following:

- All devices needing attention
- All infections found on devices
- Devices currently infected
- Threats blocked with website filtering
- All the Lost Device Protection commands sent

To generate an Alerts and Infections report:

1. Log in to the SecureAnywhere website.
2. Click the **Go to Mobile Protection** button.

   The Mobile Protection console displays with the Status tab active.

3. Click the **Reports** tab.

   The Reports tab displays.

4. Select **Alerts and Infections**. If needed, click the **Expand** arrow to expand the Alerts and Infections tree.
5. Select any of the following reports:
   - **Devices Needing Attention** — View all devices that may be compromised with malware or need administrative attention; these devices do not display in green.
   - **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 displays a breakdown of Lock, Scream, Locate, and Wipe commands.

6. Do either of the following, as needed:
   - To display specific devices, enter your query in the **Search** field at the top of the list.
   - To see more information about a specific item, double-click the entry.
7. When you're done, click the **Close** button in the Report tab to exit.

Generating App Reputation Reports

You can generate reports that display information about the breakdown of all apps reported within the organization.

To generate an App Reputation report:

1. Log in to the SecureAnywhere website.
2. Click the **Go to Mobile Protection** button.

   The Mobile Protection console displays with the Status tab active.

3. Click the **Reports** tab.

   The Reports tab displays.

4. In the Select your report column, select **App Reputation**.

   If needed, click the **Expand** arrow to expand the Alerts and Infections tree.

5. Select any of the following reports:
   - **App Reputation Distribution** — View the status of each app, broken down by reputation, as described in the following table.
   - **Android - Top Installed Apps** — View the top ten installed Android apps, including its reputation.
   - **iOS - Top Installed Apps** — View the top ten installed iOS apps, including its reputation.

   The following table describes the app reputation definitions. You can rearrange the order of the distributions, as needed.

FIELD	DESCRIPTION
Benign	The application is non-whitelisted, contains no dangerous permissions and has received favorable scores from machine classifiers.
Malicious	The application was detected as a threat such as Trojan, Rootkit, etc., by Webroot definitions.
Moderate	The application does not seem to be suspicious, but contains dangerous permissions such as Send, SMS, Call Phone, etc.
Moderate**	This value is returned in a special case when reputation is computed based on package name, that is, no md5 information is available, and means that both malicious and whitelisted application have been found with the same package name.
Suspicious	The application has not triggered any definitions but has received machine classifiers in the malicious and unwanted range.
Trustworthy	The application displays in our whitelist and is safe to use.
Unknown	The application is detected as a Potentially Unwanted Application, or PUA. A PUA is not malware but has unwanted characteristics which may include, aggressive ads and popups, intrusive privacy policies, marketing to contacts, etc.

6. Do either of the following, as needed:
   - To display specific devices, enter your query in the **Search** field at the top of the list.
   - To see more information about a specific item, double-click the entry.
7. When you're done, click the **Close** button in the Report tab to exit.

Working With Report Results

You can work with reports in the following ways:

- Filtering Report Results
- Refreshing Report Data
- Changing Report Orientation
- Hiding Report Details

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.
2. Click the **Go to Mobile Protection** button.

   The Mobile Protection console displays with the Status tab active.

3. Click the **Reports** tab.

   The Reports tab displays.

4. From the left panel, select a report.

   The selected report displays.

5. Filter the results, in any of the following ways:
   - To re-sort the order of rows, click in the column head and select a new sorting method.
   - In the Columns filter, to remove a column from the display, deselect the appropriate checkbox.
   - To display specific entries, enter your query in the Search field at the top of the report data. As you type characters in the Search field, the columns below display only the content that matches your search criteria.

Refreshing Report Data

You can receive the most up-to-date report results by refreshing the display.

To refresh report data:

1. In the upper right corner, click the **Refresh** button.

Changing Report Orientation

To change orientation:

1. To switch report orientation between portrait and landscape, click the **Switch report orientation** button.

Hiding Report Details

To hide report details:

1. To hide details and display only the graph, click the **Right Arrow**.

Exporting Report Results

You can export the report data to a spreadsheet.

To export report results:

1. Log in to the SecureAnywhere website.
2. Click the **Go to Mobile Protection** button.

   The Mobile Protection console displays with the Status tab active.

3. Click the **Reports** tab.

   The Reports tab displays.

4. Select any report to open it.
5. In the upper right corner of the report, click the **Export to CSV** button.

   The system creates and downloads a spreadsheet to your computer.

Chapter 8: WSA Business Mobile Protection Support

To learn more about Webroot's support options and other resources, see the following topics:

Accessing Technical Support

Webroot offers a variety of support options. You can do any of the following:

- Look for the answer in our knowledgebase.
- Look for the answer in our online documentation.
- Enter a help ticket.
- Obtain general customer support information.
- Connect to the Webroot Online Business Forum.

Index

A

B

C

D

E

M

O

P

R

S

T

U

V

W