websense®

TRITON Mobile Security Help

Websense® TRITON® Mobile Security

Release 10.1

Websense TRITON Mobile Security

September 2013

10900 Stonelake Boulevard, 3rd Floor, Austin, TX 78759, USA

Published 2013
Printed in the United States of America

Every effort has been made to ensure the accuracy of this manual. However, Websense, Inc., makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. Websense, Inc., shall not be liable for any error or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or the examples herein. The information in this documentation is subject to change without notice.

Contents

1 Introduction

TRITON Mobile Security Help | Mobile Security Solutions

Related topics:

Welcome to Websense® TRITON® Mobile Security. Mobile Security is a cloud-based service that brings comprehensive and flexible protection against Web threats to your organization's mobile devices.

You configure and manage Mobile Security using the Cloud TRITON Manager or portal. The portal provides a central, graphical interface for the general configuration, policy management, and reporting functions of your cloud-based service, making defining and enforcing mobile security an easy, straightforward process.

Mobile Security is simple to use and works "out of the box" with a default policy. To make full use of its features, however, you should customize the Default policy or add new policies.

Once you've set things up in the portal, end users must register their devices with the system to be protected.

This chapter explains the steps necessary to get TRITON Mobile Security managing mobile devices for your organization. For additional details about initial configuration, refer to the TRITON Mobile Security Getting Started Guide.

Supported mobile devices

TRITON Mobile Security Help | Mobile Security Solutions

TRITON Mobile Security supports:

- Apple iPhone, iPad, and iPad mini models running v5 and later of the iOS operating system.

Administrator Help overview

TRITON Mobile Security Help | Mobile Security Solutions

Related topics:

- *Logging on and portal security*, page 5
- *Navigating in the Cloud TRITON Manager*, page 6
- *Further Information*, page 23

Mobile Security Help includes the following topics:

Topic	Title	Description
1	Getting Started	Includes a brief introduction to Mobile Security, steps for configuring a new account, administrator Help contents, and Websense Technical Support contact information.
2	Policy Management	Provides an overview of user policy and device profile configuration, the policy template, and the Default policy.
3	Managing Devices	Includes details for registering new devices, administrative actions you can perform on devices, and viewing and updating device details.
4	Reporting	Provides descriptions of user, device and administrative actions-based reporting tools available in the Mobile tab of the Cloud TRITON Manager.
5	End-user Self Service	Contains an overview of the end-user Device Management portal.

Logging on and portal security

TRITON Mobile Security Help | Mobile Security Solutions

Related topics:

- *New account configuration*, page 8
- *Alerts*, page 18
- *Navigating in the Cloud TRITON Manager*, page 6
- *Job Queue*, page 21
- *Further Information*, page 23

To access the portal, visit https://admin.websense.net/portal.

The logon process uses cookies where possible. For the best user experience, we recommend that you accept cookies from the Cloud TRITON Manager. If your Web browser is unable to, or is configured not to accept cookies from the portal, an additional screen appears during logon reminding you of the benefits of securing your session.

If the portal cannot use cookies to secure the session, it falls back to ensuring that all requests for the session come from the same IP address. This may cause problems for you if your company has several load-balanced Web proxies, because the portal perceives requests coming from several sources as a security breach. Companies with a single Web proxy or a cooperating Web proxy farm should not be affected.

To avoid problems, we recommend enabling cookies on your Web browsers. To use the portal, your browser must be Javascript-enabled.

Note

If you don’t have logon credentials for this portal—for example, if you are a customer using TRITON AP-WEB with the Web Hybrid module—you can request credentials through Websense Technical Support. See this knowledgebase article for the details you’ll require when making the request.

Supported Web browsers

Refer to the TRITON Mobile Security Getting Started Guide for a list of supported web browsers that you may use to access the Cloud TRITON Manager.

Privacy statement

The portal uses 2 cookies during logon. The first is used to identify whether the user’s Web browser is willing to accept and store cookies for the portal; it contains no information. If the first cookie is successfully stored, a second cookie is stored containing temporary information about the session. No personal information is stored in either cookie, and both cookies are used only for the duration of the session.

Idle timeout

For security reasons, if you are logged on to your account and are inactive for 30 minutes, you are automatically logged off. When you next attempt to perform an action, you are asked to log on again.

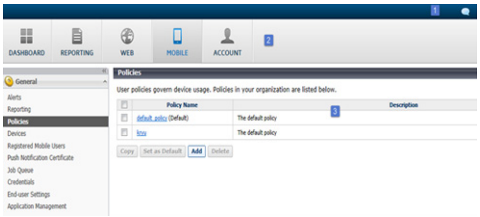
Navigating in the Cloud TRITON Manager

TRITON Mobile Security Help | Mobile Security Solutions

Related topics:

- *Logging on and portal security*, page 5
- *Navigating in the Cloud TRITON Manager*, page 6
- *Further Information*, page 23

The cloud portal interface can be divided into the following main areas:



User policies govern device usage. Policies in your organization are listed below.

	Policy Name	Description
□	default policy (Default)	The default policy
□	kny	The default policy

1. Banner
2. Toolbar
3. Content pane

The **banner** shows:

- Any Alerts that are available for your account
- Your current **logon account**. When you're ready to end your administrative session, click the arrow next to the administrator name and select **Log Off**.
- The **Help** menu, from which you can access assistance for the page you are currently viewing, further product information, and Websense Technical Support resources.

  The Help menu also includes the **Support PIN**. You must authenticate yourself with this PIN when calling Websense Technical Support.

Each PIN is unique per portal user, and is generated when a user logs on. The PIN is then valid for 24 hours after logon. After a 24-hour period has expired, a new PIN is generated at the next portal logon.

> **Important**
>
> In order to preserve and maintain the security of your data, Support representatives will not be able to provide customer support without an accurate, up-to-date PIN.

The **toolbar** indicates which part of the cloud portal is currently active:

- **Dashboard** provides access to the threat, productivity, and bandwidth dashboard for Web Filter & Security with the Web Filter Security Cloud module, and dashboards for TRITON AP-EMAIL with the Email Cloud module.
- **Reporting** gives access to all reporting options, including email reports, account service reports, your saved reports, and the cloud web solution Report Catalog and Report Builder.
- **Email** contains all configuration settings relating to the cloud email solution including account-wide email settings, policy management, and the Message Center.
- **Web** contains all configuration settings relating to the cloud web solution including account-wide web settings, policy management, access to endpoint and single sign-on configuration, and management of devices in your network that connect to the cloud service. To manage appliances, your subscription must include the i-Series appliance.
- **Mobile** contains all configuration settings relating to Mobile Security, including policy management, device management, and mobile reports.
- **Account** provides access to configuration options that apply to the cloud web solution and cloud email solution. This includes administrator management, directory synchronization, licenses, and groups.

When you select an item in the toolbar, a **navigation pane** drops down, containing the available navigation choices for that item. Click the toolbar item again to close the navigation pane.

The **content pane** varies according to the selection you make in the navigation pane

New account configuration

TRITON Mobile Security Help | Mobile Security Solutions

Related topics:

- *Generate an Apple Push Notification certificate*, page 8
- *Customize user policies and device profiles*, page 17
- *Register mobile devices*, page 18

Complete these 3 steps to enable TRITON Mobile Security to manage devices in your organization:

1. *Generate an Apple Push Notification certificate*, page 8
2. *Customize user policies and device profiles*, page 17 (optional step)
3. *Register mobile devices*, page 18

Generate an Apple Push Notification certificate

TRITON Mobile Security Help | Mobile Security Solutions

Related topics:

- *Creating a new certificate*, page 9
- *Renewing a certificate*, page 12
- *Replacing a certificate*, page 14
- *New account configuration*, page 8
- *Customize user policies and device profiles*, page 17
- *Register mobile devices*, page 18
- *Navigating in the Cloud TRITON Manager*, page 6

To install mobile security profiles on devices, your organization must request an Apple Push Notification (APN) certificate from Apple and then upload it to Mobile Security.

This certificate allows Mobile Security to connect to devices so it can send administrative updates and receive reporting feedback.

Important

To avoid service interruption, do not let your APN certificate expire. If your certificate expires, Mobile Security can no longer manage your devices, and they must be re-registered to restore the service.

For instructions on creating, renewing, and replacing APN certificates, see the following topics:

- *Creating a new certificate*, page 9
- *Renewing a certificate*, page 12
- *Replacing a certificate*, page 14

Creating a new certificate

TRITON Mobile Security Help | Mobile Security Solutions

Related topics:

- *Renewing a certificate*, page 12
- *Replacing a certificate*, page 14

1. In the Mobile tab of the Cloud TRITON Manager, select **General > Push Notification Certificate**.
2. Click **Create and Upload Certificate**. This process consists of three main steps.
3. In the Step 1: Create Signed Certificate box:
   a. Enter information about your organization. This information will be used when generating a certificate specific to your organization.

Field Name	Description
Certificate name	Enter a friendly name that you would like to assign to your organization's signed certificate, such as "Acme Corp Certificate".
Organization	Enter the name of your organization, such as "Acme Corp".
Organization unit	If applicable, enter the name of the organizational unit that will be using this mobile security certificate, such as "Accounting".
Email address	Enter the email address of a system administrator responsible for this certificate.
City/locality	Enter the city or locality where your organization is located.
State/Province	Enter the state or province where your organization is located.
Country	Enter the country where your organization is located.

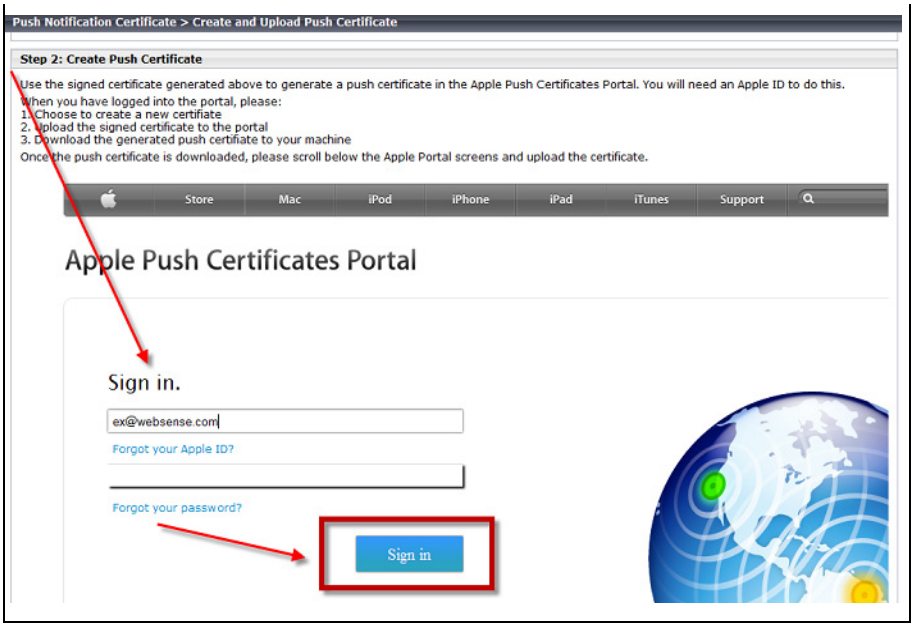
   b. Click **Create Signed Certificate**.
   c. When the certificate is available, a link appears next to the **Create Signed Certificate** button, "The signed certificate is available for download."
   d. Click the link. The signed certificate is available as a .plist file for download. You may change the filename, but do not change the filename extension.
   e. Indicate where to save the file on your computer.

4. In the Step 2: Create Push Certificate box, sign onto the Apple Push Certificates Portal where you create a push certificate using the signed certificate that you just generated.

Note

Use a Safari or Firefox browser to complete this section.

a. Sign onto the Apple Push Certificate Portal by entering your organization’s Apple ID and password in the fields provided. You can also sign onto the portal by navigating to https://identity.apple.com/pushcert/.



Push Notification Certificate > Create and Upload Push Certificate

Step 2: Create Push Certificate

Use the signed certificate generated above to generate a push certificate in the Apple Push Certificates Portal. You will need an Apple ID to do this.
When you have logged into the portal, please:
1. Choose to create a new certifiate
2. Upload the signed certificate to the portal
3. Download the generated push certifiate to your machine
Once the push certificate is downloaded, please scroll below the Apple Portal screens and upload the certificate.

Apple Push Certificates Portal

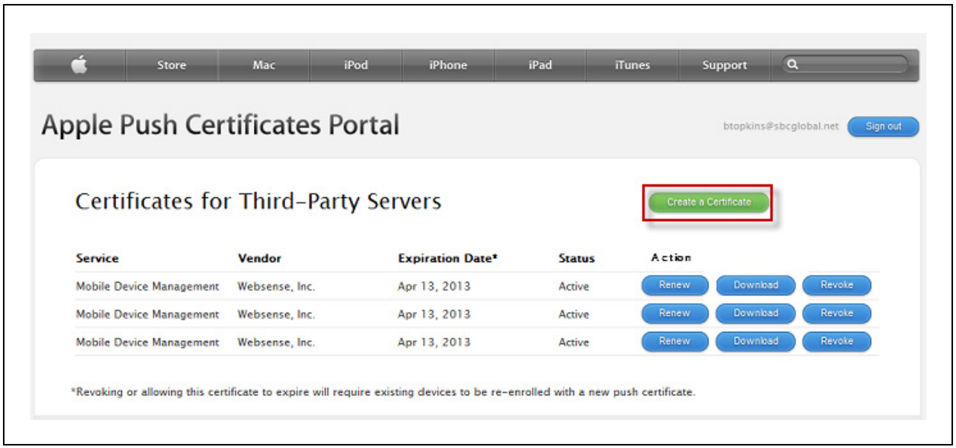
Sign in.

ex@websense.com

If your organization does not have an Apple ID, go to https://appleid.apple.com/ and create one. This can be any Apple ID, and does not have to be associated with an Apple Developer account. However, it is recommended that you create a new Apple ID for your organization that can be used to manage your Apple Push Notification certificates. For best practice, the ID should be corporate-owned to avoid renewal issues in case your administrator leaves the company.

b. Read and accept the Terms of Use document.

c. Select **Create a Certificate**.



Apple Push Certificates Portal

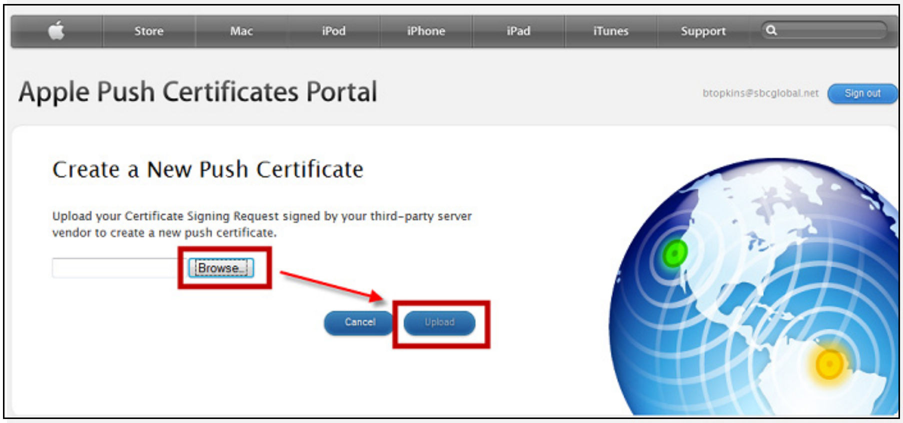
Certificates for Third-Party Servers

Service	Vendor	Expiration Date*	Status	Action
Mobile Device Management	Websense, Inc.	Apr 13, 2013	Active	Renew Download Revoke
Mobile Device Management	Websense, Inc.	Apr 13, 2013	Active	Renew Download Revoke
Mobile Device Management	Websense, Inc.	Apr 13, 2013	Active	Renew Download Revoke

*Revoking or allowing this certificate to expire will require existing devices to be re-enrolled with a new push certificate.

d. Click **Browse** and select the file you downloaded in step 3e. Do not change the filename extension.

e. Click **Upload**. The certificate is now listed in the Certificates for Third-Party Servers list.

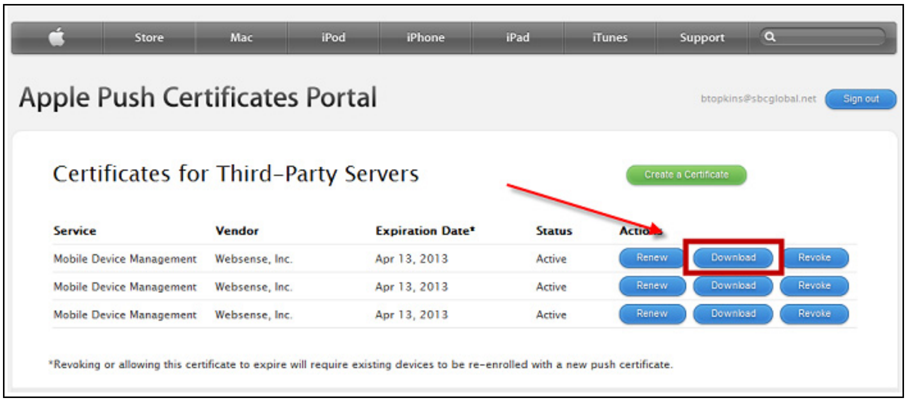


Apple Push Certificates Portal

Create a New Push Certificate

Upload your Certificate Signing Request signed by your third-party server vendor to create a new push certificate.

f. Click **Download** next to the certificate you just created.



Apple Push Certificates Portal

Certificates for Third-Party Servers

Service	Vendor	Expiration Date*	Status	Action
Mobile Device Management	Websense, Inc.	Apr 13, 2013	Active	Renew Download Revoke
Mobile Device Management	Websense, Inc.	Apr 13, 2013	Active	Renew Download Revoke
Mobile Device Management	Websense, Inc.	Apr 13, 2013	Active	Renew Download Revoke

*Revoking or allowing this certificate to expire will require existing devices to be re-enrolled with a new push certificate.

g. Save the file to your computer.

5. In the Step 3: Upload Push Certificate to Mobile Security box, browse to the APN file.

a. Click **Upload Certificate**.

Renewing a certificate

TRITON Mobile Security Help | Mobile Security Solutions

Related topics:

- *Creating a new certificate*, page 9
- *Replacing a certificate*, page 14

Apple push notification (APN) certificates have expiration dates. To maintain connection with the mobile devices in your organization, you must renew your certificates periodically. When your certificate approaches it expiration date or expires, an alert displays on the Alerts page when you log on and you are sent a notification by email.

If your certificate expires, your devices are no longer managed by Mobile Security, and they must be re-registered to restore the service.

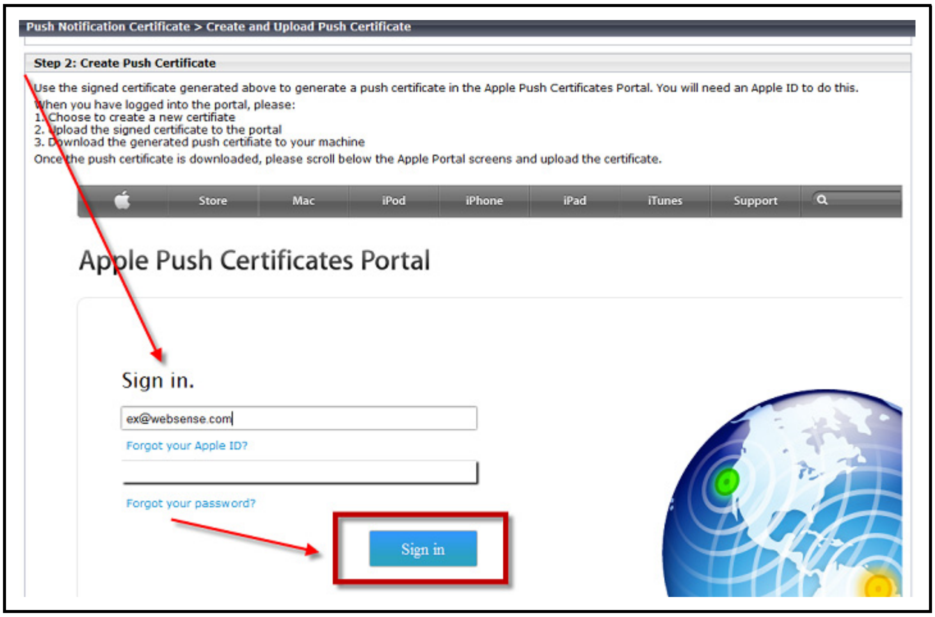
To see your certificate's expiration date, select **General > Push Notification Certificate**. This page shows details about your certificate, including the issued and expiration dates.

To renew your certificate:

1. Click **Renew Certificate**.
2. Locate the original signed certificate for your organization on your computer, or download it again. To download it:
   a. In the Download Signed Certificate box, information about your current/original signed certificate appears. This includes your organization name, organization unit, email address, and physical address.
   b. Scroll to the bottom of this box and locate the message, "The signed certificate is available for download." Click **download** and save a copy of your signed certificate to your computer.
3. Renew the push notification certificate on the Apple Push Certificates portal.

Note
Use a Safari or Firefox browser to complete this section.

a. Sign onto the Apple Push Certificate Portal by entering the Apple ID and password used to create the APN certificate originally. You can also sign onto the portal by navigating to https://identity.apple.com/pushcert/.



Push Notification Certificate > Create and Upload Push Certificate

Step 2: Create Push Certificate

Use the signed certificate generated above to generate a push certificate in the Apple Push Certificates Portal. You will need an Apple ID to do this.

When you have logged into the portal, please:
1. Choose to create a new certifiate
2. Upload the signed certificate to the portal
3. Download the generated push certifiate to your machine

Once the push certificate is downloaded, please scroll below the Apple Portal screens and upload the certificate.

Apple Push Certificates Portal

Sign in.

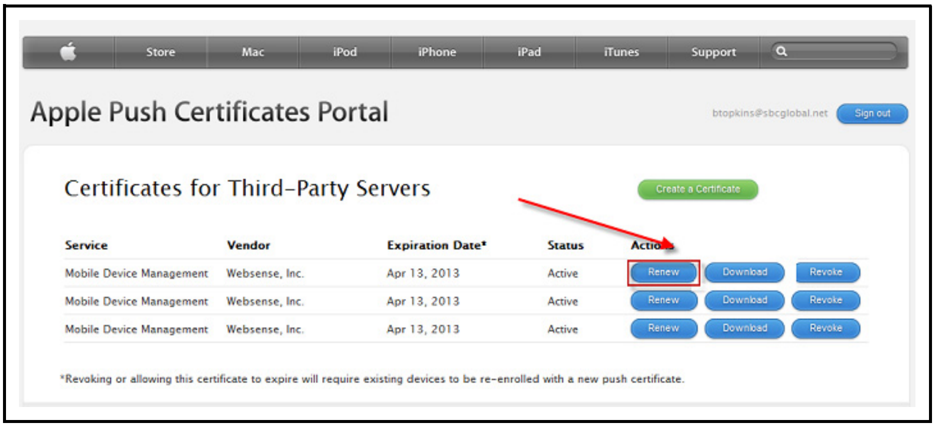
ex@websense.com

b. Read and accept the Terms of Use document.

c. A list of all the APN certificates for your organization shows in the Certificates for Third-Party Servers list.

d. Select the **Renew** button next to the certificate currently being used by the Websense MDM service. To view the serial number of a certificate, hover over the **Renew** button and look at the bottom of the page.

If you select the wrong certificate, you will receive an error when uploading the renewed certificate to the Mobile Security system.



Apple Push Certificates Portal

btopkins@sbcglobal.net

Certificates for Third-Party Servers

Service	Vendor	Expiration Date*	Status	Actions		
Mobile Device Management	Websense, Inc.	Apr 13, 2013	Active	Renew	Download	Revoke
Mobile Device Management	Websense, Inc.	Apr 13, 2013	Active	Renew	Download	Revoke
Mobile Device Management	Websense, Inc.	Apr 13, 2013	Active	Renew	Download	Revoke

*Revoking or allowing this certificate to expire will require existing devices to be re-enrolled with a new push certificate.

e. When prompted, click **Browse** and select the original signed certificate from step 1.

f. Click **Upload**. Confirm that the expiration date for the certificate is updated in the Certificates for Third-Party Servers list.

g. Click **Download** next to the renewed certificate.

h. Save the file to your computer.

4. Upload the renewed Apple certificate to Mobile Security.

   a. Scroll to the bottom of the Mobile tab's Renew Certificate page.

   b. In the section, Upload Renewed Push Certificate to Mobile Security, browse to the APN file.

   c. Click **Upload Renewed Certificate**.

   The certificate that you upload must match the certificate signing request of the original certificate in Mobile Security. The topic of the certificate must match the original topic. If you receive an error that these 2 conditions have not been met, you may have selected the wrong certificate in the Apple portal.

Replacing a certificate

TRITON Mobile Security Help | Mobile Security Solutions

Related topics:

- *Creating a new certificate*, page 9
- *Renewing a certificate*, page 12

If your Apple push notification certificate stops working or has become corrupted, Websense Technical Support may instruct you to replace it and re-register your devices.

Warning

If you replace the push notification certificate associated with your account, device owners must re-register all their devices with Mobile Security.

1. In the Mobile tab of the Cloud TRITON Manager, select **General > Push Notification Certificate**.
2. Click **Replace Certificate**.
3. Create a new signed certificate for your organization.

   a. In the Create New Signed Certificate box, enter information about your organization. Do not use the same information that you used in previous signed certificates.

Field Name	Description
Certificate name	Enter a friendly name that you would like to assign to your organization's signed certificate, such as "Acme Corp Certificate".
Organization	Enter the name of your organization, such as "Acme Corp".

Field Name	Description
Organization unit	If applicable, enter the name of the organizational unit that will be using this mobile security certificate, such as “Accounting”.
Email address	Enter the email address of a system administrator responsible for this certificate.
City/locality	Enter the city or locality where your organization is located.
State/Province	Enter the state or province where your organization is located.
Country	Enter the country where your organization is located.

b. Scroll to the bottom of this box and click **Create New Certificate**. A warning appears:

```
Are you sure you want to generate a new signed
certificate? If you continue, you must complete the steps
to replace the APN certificate or the signed certificate
will be invalid. Once the push certificate is replaced,
users must re-register all of their devices with Mobile
Security.
```

If you are willing to re-register every mobile device in your organization, click **Yes**.

c. When the certificate is available, a link appears next to the **Create Signed Certificate** button, “This certificate is available for download.”

d. Click the link.

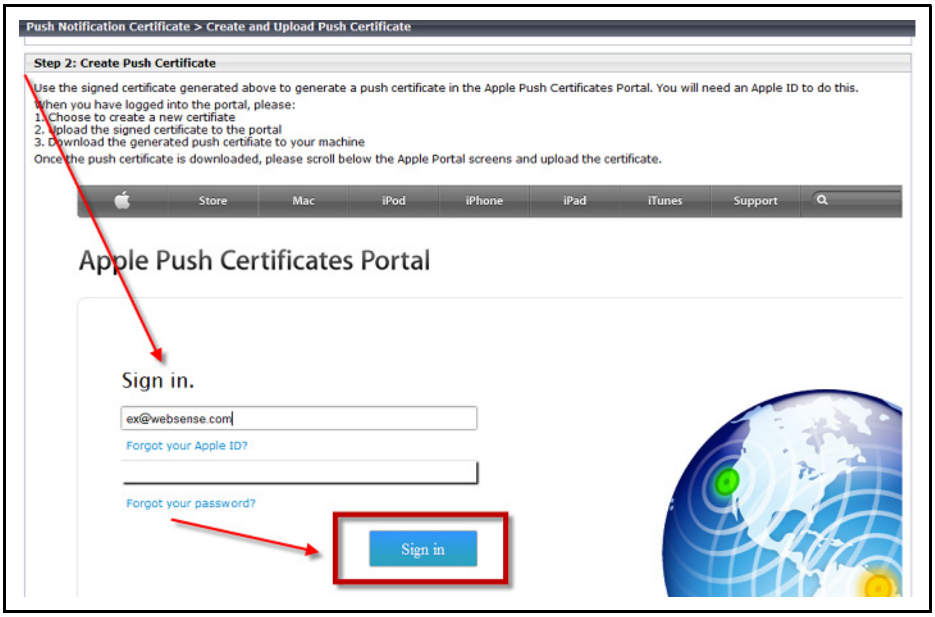
e. Indicate where to save the file on your computer.

4. Create a new push notification certificate on the Apple Push Certificates portal.

✓ **Note**

Use a Safari or Firefox browser to complete this section.

a. Sign onto the Apple Push Certificate Portal by entering your organization's Apple ID and password in the fields provided. You can also sign onto the portal by navigating to https://identity.apple.com/pushcert/.



Push Notification Certificate > Create and Upload Push Certificate

Step 2: Create Push Certificate

Use the signed certificate generated above to generate a push certificate in the Apple Push Certificates Portal. You will need an Apple ID to do this.
When you have logged into the portal, please:
1. Choose to create a new certifiate
2. Upload the signed certificate to the portal
3. Download the generated push certifiate to your machine
Once the push certificate is downloaded, please scroll below the Apple Portal screens and upload the certificate.

Apple Push Certificates Portal

Sign in.

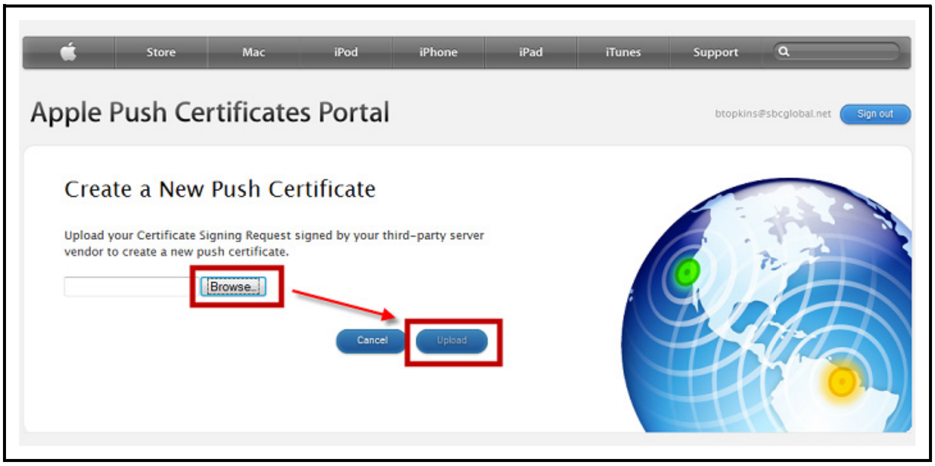
ex@websense.com

b. Read and accept the Terms of Use document.

c. Select **Create a Certificate**.

d. Click **Browse** and select the file you downloaded in step 1.

e. Click **Upload**. The certificate is now listed in the Certificates for Third-Party Servers list.



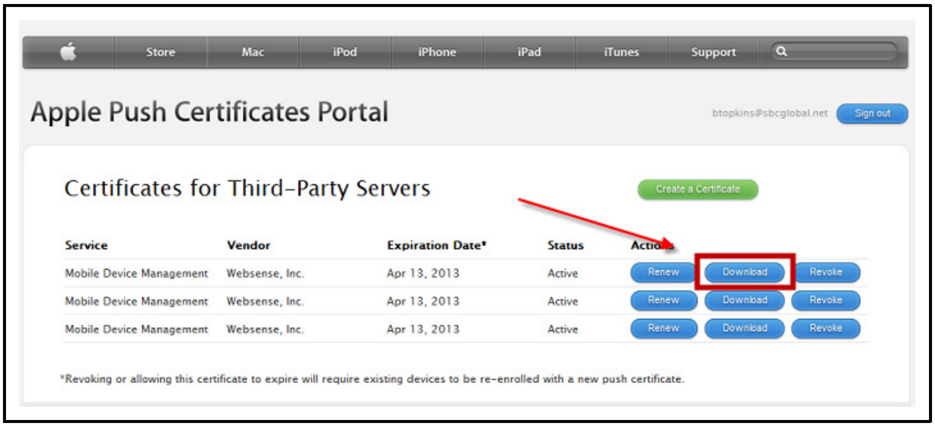
Apple Push Certificates Portal

btopkins@sbcglobal.net

Create a New Push Certificate

Upload your Certificate Signing Request signed by your third-party server vendor to create a new push certificate.

f. Click **Download** next to the certificate you just created.



Apple Push Certificates Portal

Certificates for Third-Party Servers

Service	Vendor	Expiration Date*	Status	Actions		
Mobile Device Management	Websense, Inc.	Apr 13, 2013	Active	Renew	Download	Revoke
Mobile Device Management	Websense, Inc.	Apr 13, 2013	Active	Renew	Download	Revoke
Mobile Device Management	Websense, Inc.	Apr 13, 2013	Active	Renew	Download	Revoke

*Revoking or allowing this certificate to expire will require existing devices to be re-enrolled with a new push certificate.

g. Save the file to your computer.

5. Upload the new Apple certificate to Mobile Security.
   a. Scroll to the bottom of the Mobile tab’s Replace Certificate page.
   b. In the section, Upload Push Certificate to Mobile Security, browse to the APN file.
   c. Click **Upload New Certificate**.

Customize user policies and device profiles

TRITON Mobile Security Help | Mobile Security Solutions

Related topics:

- *Generate an Apple Push Notification certificate*, page 8
- *New account configuration*, page 8
- *Register mobile devices*, page 18

Policies govern end users’ device usage. A policy is made up of 2 device profiles where you can configure security requirements, allowed device and application functions, and Wi-Fi and email settings. For more information on policies, see *Policy Management*, page 25.

The Mobile tab of the Cloud TRITON Manager includes a predefined policy template that can be customized to meet your needs, see *The Default policy*, page 26. You can also create your own custom policies, see *Adding a policy*, page 26.

Register mobile devices

TRITON Mobile Security Help | Mobile Security Solutions

Related topics:

- *Generate an Apple Push Notification certificate*, page 8
- *New account configuration*, page 8
- *Customize user policies and device profiles*, page 17

To protect devices from Web threats and enable device management features, mobile devices must first be registered with TRITON Mobile Security.

When the setup process is complete, you send email messages asking end users to register their mobile devices with Mobile Security. For step-by-step instructions for registering devices, see *Registering new devices*, page 41.

Alerts

TRITON Mobile Security Help | Mobile Security Solutions

Related topics:

- *Logging on and portal security*, page 5
- *Navigating in the Cloud TRITON Manager*, page 6
- *Further Information*, page 23
- *Job Queue*, page 21

The Mobile tab provides alerts for some important events on the **General** > **Alerts** page:

Alert	Description
You have not uploaded an Apple Push Notification (APN) certificate to the Mobile tab of the Cloud TRITON Manager. An APN certificate is required to manage devices with Mobile Security.	An Apple Push Notification (APN) certificate is required to utilize Mobile Security mobile device management features. Because you have not uploaded one, your organization's mobile devices are not managed by the system. For information on generating an APN certificate and uploading it to the Mobile tab of the Cloud TRITON Manager, see *Creating a new certificate*, page 9.
Your Apple Push Notification (APN) Certificate expires in 5 days.	The Apple Push Notification (APN) certificate you uploaded in the Mobile tab will expire in 5 days. To maintain connection with the mobile devices in your organization, you must renew your certificate. If your certificate expires, your devices are no longer managed by Mobile Security, and every one of them must be re-registered to restore the service. Please generate a new certificate and upload it to the Mobile tab of the Cloud TRITON Manager. For more information, see *Renewing a certificate*, page 12.
Your Apple Push Notification (APN) Certificate has expired.	The Apple Push Notification (APN) certificate you uploaded in the Mobile tab of the Cloud TRITON Manager has expired. Your devices are no longer managed by Mobile Security. Please generate a new certificate and upload it to the Mobile tab. When you are done, every device in your organization must re-register with the system. For more information, see *Renewing a certificate*, page 12.
Mobile Security was unable to deliver a device registration request message to the listed email address.	The registration request email message you sent to the listed email address could not be delivered. This user doesn't know he should register his devices with the system. For information on sending these messages, see *Registering new devices*, page 41.

Alert	Description
Users have been removed from your organization’s directory service, but you have not removed their profiles or wiped their devices.	Sometimes users are deleted from the directory service—for example, when they leave the company. In these cases, you should remove the Mobile Security profile from the users’ devices and consider wiping the devices. You have not done either yet. This is a security risk. Their devices are still managed by the system, and company resources are still on their devices. For information on resolving this alert, see *Removing users’ profiles*, page 20.
Some mobile devices in your network are jailbroken. Take action to protect your corporate data.	Some users have hacked the iOS operating system on their mobile devices and have full control over them. If desired, they could circumvent the device management controls and policy enforcement supplied by TRITON Mobile Security. Take action to ensure that the jailbroken device is not a risk to your organization. To see which devices are compromised, view the *Jailbroken devices*, page 56 report.
The certificate used by your ActiveSync server cannot be validated by Certificate Authority. Users cannot be authenticated for registration or device management.	If the security certificate used by your ActiveSync server is not recognized by CA, users are unable to log onto the end-user Device Management portal or use network credentials to register their device.

Removing users’ profiles

TRITON Mobile Security Help | Mobile Security Solutions

If a user was removed from your directory service, but you have not removed the cloud web solution profile from their device or wiped their device, an alert appears on the portal Alert page. To remove the profile or wipe the device, click the **Resolve** button next to the alert.

The Resolve Devices For Removed Users page lists the users who have been removed, along with their devices, device types, and profile types.

Select the devices to act upon, then click **Remove Profile From Device** or **Wipe Device**. A message appears asking you to confirm your action. Click **Confirm** to complete the operation.

Wipe actions require 2 confirmations, because when you wipe a device, all data is deleted from it (corporate and personal) and the device is returned to its factory settings.

When you remove a profile from a device, it is no longer protected by TRITON Mobile Security.

Requests for action are immediately sent to the device. If the device is off or out of range, it is wiped or its profile is removed the next time it is powered on. The request for action times out after 7 days.

Job Queue

TRITON Mobile Security Help | Mobile Security Solutions

Related topics:

- *Logging on and portal security*, page 5
- *Navigating in the Cloud TRITON Manager*, page 6
- *Further Information*, page 23
- *Alerts*, page 18

The **General** > **Jobs Queue** page lists the currently scheduled jobs (or, administrative actions) for users and devices. From this page you can view and delete scheduled jobs.

You can search for a particular job by Device Name, User, or Job Type. Enter a search term and click **Search** to begin the search. Click **Show all** to remove the current search term.

The list provides the following information on each job:

Data Item	Description
Device Name	The name of the device on which the administrative action is performed.
User	The user the device is registered to

Data Item	Description
Job Type	One of the following kinds of jobs: • Install settings profile • Remote wipe • Remote lock • Get device information • Get device installed applications information • Remote passcode clear • Install VPN profile • Remove VPN profile • Remove MDM profile • Install email settings • Install Exchange settings • Install WiFi settings • Remove email settings • Remove Exchange settings • Remove WiFi settings
Status	Indicates whether the job is: • New: the task has been created, but has not yet been sent to the device. • Send notification: The task has been sent to the device and is pending completion. • Notified: The task cannot be executed at this time; the device has been notified to complete this task. • Pending: The task is pending completion. • Failed: The task could not be executed.

Jobs are automatically deleted from the queue after 7 days. When a high-priority job is deleted, whether by the system or another administrator, you are sent a notification message by email. High-priority jobs include:

- Remote lock
- Remote wipe
- Clear passcode
- Remove MDM profile
- Remove VPN profile
- Install/update Settings profile
- Install/remove email profile
- Install/remove Exchange profile
- Install/update WiFi profile

Further Information

TRITON Mobile Security Help | Mobile Security Solutions

Related topics:

- *Logging on and portal security*, page 5
- *Navigating in the Cloud TRITON Manager*, page 6
- *Further Information*, page 23

Technical information about Websense software and services is available 24 hours a day at support.websense.com, including:

- the searchable Websense Knowledge Base (made up of a Solution Center, Technical Library, and customer forums)
- Webinars and show-me videos
- product documents and in-depth technical papers
- answers to frequently asked questions

If you are a cloud solution customer, you can access these resources by navigating to **Home > Support**.

The **Home > Support > Summary** page tells you how to contact Technical Support with a support question. You can visit the Support website, send an email to Support, or call one of the telephone numbers that are listed. We ask that you take a few minutes to review the material on the Support pages first, to see if your question has already been answered.

Password Maintenance

Go to **Home > Support > Password** if you need to change your password or generate a new one. Enter and confirm a password, then click **Submit** when done. The password must conform to your password policy, as described on the screen.

2 Policy Management

TRITON Mobile Security Help | Mobile Security Solutions

Related topics:

- *The policy template*, page 25
- *The Default policy*, page 26
- *Adding a policy*, page 26
- *Defining a profile*, page 27
- *Editing a policy*, page 39

Policies govern end users' device usage. A policy is made up of 2 device profiles where you can configure security requirements, allowed device and application functions, and Wi-Fi and email settings.

Use the **General** > **Policies** page to:

- Add, delete, or copy policies.
- Review and edit policies.
- Select a default policy.

The policy template

TRITON Mobile Security Help | Mobile Security Solutions

Related topics:

- *The Default policy*, page 26
- *Adding a policy*, page 26
- *Adding a Wi-Fi access account*, page 34

The Mobile tab of the Cloud TRITON Manager includes a predefined policy template that can be customized to meet your needs. You can also create your own custom policies, see *Adding a policy*, page 26.

The provided policy template includes two device profiles: one profile intended for corporate-owned devices and one for personal devices. To view or edit the policy template settings and profiles, click the policy name on the **General** > **Policies** page. See *Defining a profile*, page 27 for information on profile configuration.

This policy is also set as your default policy when you first log on to the Mobile tab of the Cloud TRITON Manager. See *The Default policy*, page 26 for more information.

The Default policy

TRITON Mobile Security Help | Mobile Security Solutions

Related topics:

- *The policy template*, page 25
- *Adding a policy*, page 26
- *Adding a Wi-Fi access account*, page 34

The Default policy acts as a safety net, enforcing a basic security policy for any users not governed by another policy. In the Mobile tab of the Cloud TRITON manager, one policy must be designated as the Default policy. The Default policy cannot be deleted.

When you first log on to the Mobile tab, the provided policy template is selected as your Default policy (see *The policy template*, page 25). However, you can select any user policy as your Default policy, to suit the needs of your organization. To make a policy the Default policy, select a policy on the **General** > **Policies** screen and click **Set as Default**.

Adding a policy

TRITON Mobile Security Help | Mobile Security Solutions

Related topics:

- *Defining a profile*, page 27
- *The Default policy*, page 26
- *Adding a Wi-Fi access account*, page 34

The Mobile tab of the Cloud TRITON Manager includes one predefined (and customizable) policy template. For more information, see *The policy template*, page 25.

You can also create custom policies. To do so:

1. Click **Add** on the **General** > **Policies** page to open the **Add policies** page.

2. Enter a unique and descriptive name for your policy in the **Policy name** field.
3. Optionally, enter a description of your policy in the **Policy Description** field.
4. Click **Save** and you're returned to the Policies screen.
5. To configure the policy, click the policy name, and then edit both the corporate and personal profiles. See *Defining a profile*, page 27.

If you would like to disable the personal profile in this policy, click **Disable** next to the profile in the **Profile list** table.

If you disable a profile in this policy, it does not appear as an option when users in this profile register new devices. However, users assigned to a disabled profile must be manually reassigned to another profile (otherwise they retain the disabled profile's settings).

Defining a profile

TRITON Mobile Security Help | Mobile Security Solutions

Each user policy consists of two device profiles. Profiles allow you to enforce device usage restrictions based on how the device is used (for example, a corporate device or personal device).

Click the name of a profile on the **General** > **Policies** > **Edit Policy** screen to open the **Edit Profile** screen.

The **General** > **Policies** > **Edit Policy > Edit Profile** screen consists of the following sections:

- *General settings*
- *Traffic and filtering*
- *Restrictions*
- *Credentials*
- *Wi-Fi settings*
- *Email and Exchange settings*
- *Web clip settings*

General settings

Use **General** settings to define the organization affiliated with the profile, when the end user can remove the profile from the device, and the usage agreement affiliated with the profile.

The following fields are displayed in the **General** settings section:

Field Name	Description
Organization	Enter the name of your organization. The Cloud service uses this information to know which policy to apply to each device.
Usage agreement	Select the end-user usage agreement users are asked to agree to when registering devices assigned to this profile. Here you can select from usage agreements uploaded on the **General** > **End-user Settings** screen (see *End-user self service*, page 59 for more information).

Traffic and filtering

Select how you want Web requests from devices with this profile to be routed, and the level of security to apply to these devices.

This section can be used to improve the performance of devices experiencing latency.

Field Name	Description
Send traffic through the Websense cloud service via VPN	This option is enabled by default for both corporate and personal profiles. To protect devices with the TRITON Mobile Security system, you must leave this option as enabled, and you must enter a PAC file URL. (See below) Deselect this option to bypass security on devices with this profile. When VPN is disabled, user requests for data go directly to the Internet as unfiltered traffic. **Tip:** If you want to bypass security on user devices, but track Web usage for the user, enable VPN but clear the PAC file URL below. With no PAC file URL, the system doesn’t know which policy to apply, so Web traffic is unfiltered.
Use a PAC file to apply your company Web policy	Select this box if you want devices with this profile to be protected by TRITON Mobile Security. If this box is deselected, all Web traffic is unfiltered, because the system doesn’t know whose device is making the requests or what policy to apply. Neither security or productivity filters are applied. To enable filtering, you must also enter the PAC file URL (see below).

PAC file URL	Enter the URL of a Proxy Auto-Configuration (PAC) file to configure auto-proxy settings. This PAC file should be configured according to the Web security policy you want to enforce. For Cloud Security, copy the PAC file URL from the General tab for that policy. To get to this tab, go to **Web Security** > **Policy Management** > **Policies**, and click on the policy you want. For TRITON AP-WEB with the Web Hybrid module, retrieve it on the Hybrid User Identification page under **Settings** > **Hybrid Configuration**. Use a PAC file to specify the appropriate proxy for fetching a given URL and to specify exclusions (URLs that should not be accessed through the Websense Cloud Security proxy). For a description of PAC files, see What is a PAC file? If you leave this field blank, the system doesn't know which policy to apply, so Web traffic is unfiltered. For more information about the PAC file you should deploy, see the Help for your Web Security product.
Apply all Web policies	When selected, browser traffic from devices with this profile has all corporate Web security policies applied. This includes security filters (such as phishing and malware) and productivity filters (such as social networking). By default, only security filters are applied to browser traffic. Only security filters are applied to app traffic regardless of this setting.
Log all traffic	Select this option to log all Web requests from the user's devices. Disabling logging improves device performance. By default, logging is enabled for corporate profiles, but disabled for personal profiles. For more information about logging, see the Help for your Web Security product.

Passcode settings

Use **Passcode** settings to define passcode-related security requirements for devices assigned to the profile.

You can configure the following settings in this section:

Field Name	Description
Require passcode on device	Select this option to require the user to configure a passcode to access the device.
Simple value	Select this option to allow users to choose passcodes containing ascending, descending, or repeating sequences.
Alphanumeric value	Select this option to require users to choose passcodes containing at least one letter.
Minimum code length	The minimum character length for a passcode.
Minimum number of non-alphanumeric characters	The minimum number of non-alphanumeric characters (not numbers or letters) allowed in the passcode.
Passcode expires after	Number of days before the user must choose a new passcode.
Auto-Lock (minutes)	Number of minutes a device can be idle before it is automatically locked.
Passcodes can be reused after	The number of unique passcodes that must be used before a previously used passcode can be used again.
Require passcode to unlock device after	Number of minutes a device can be locked without prompting the user for a passcode to unlock the device.
Maximum number of failed logon attempts	Number of incorrect password attempts allowed before the device is wiped of all personal data and restored to factory settings.

Restrictions

Use **Restrictions** settings to define which device functions and applications can be used on the device.

Device functionality

You can enable or disable the following functions for devices assigned to the profile (select the check box next to the feature to enable it).

Field Name	Description
App installation	Select this option to allow the user to install apps from the iTunes Store on the device. Select **Require Apple ID password for each install** if you want users to authenticate with Apple before installing apps.
Camera	Select this option to allow the user to use the camera on the device. Select **FaceTime** to allow the user to use the FaceTime feature on the device.
Screen capture	Select this option to allow the user to use the screen capture feature on the device.
Automatic sync while roaming	Select this option to enable the device to automatically sync data while the device is roaming.
Voice dialing	Select this option to allow the user to use the voice dialing command feature to place calls on the device.
In-app purchases	Select this option to allow the user to make purchases in applications on the device.
Receive Passbook notifications while locked	Passbook is an iOS app that allows merchants to develop Passes to be stored in the user's Passbook. Select this option if you want to allow Passbook notifications to be displayed while the device is locked. This option is selected by default.
Multiplayer gaming	Select this option to allow the user to play multiplayer games in the Game Center application.
Addition of Game Center friends	Select this option to allow the user to add friends in the Game Center application.
Force encrypted backups	Select this option to require that backups of the device are encrypted.

Applications

You can enable or disable access to the following applications (and application features) for devices assigned to the profile.

Field Name	Description
YouTube	Select this setting to allow the user to use the YouTube app.
iTunes Store	Select this setting to allow the user to use the iTunes Store on the device.
Siri,	Select this setting to allow the user to use the Siri app. Select **While device is locked** to allow Siri usage when the device is locked.
Safari	Select this setting to allow the user to use the Safari Web browser on the device. ◆ **Enable AutoFill** - Select this setting to enable the AutoFill (auto populate form) feature in Safari. ◆ **Force fraud warnings** - Select this option to force the Safari fraud warning option to remain on. ◆ **Enable JavaScript** - Select this option to enable JavaScript in Safari. ◆ **Block popups** - Select this option to force the Safari block popups option to remain on. ◆ **Accept cookies** - Select when the device accepts cookies while browsing in Safari: Never, From visited sites (only from sites directly accessed), or Always.

Media Content Ratings

You can specify the ratings you will allow for various forms of media content. For example, you can allow or disallow adult content.

Field Name	Description
Region	Select the region whose rating system you want to use.
Movies	Select which movies users with this profile can view.
TV shows	Select which TV shows users with this profile can view.

Field Name	Description
Apps	Select which apps users with this profile can use.
Allow explicit music and podcast downloads and purchases	Select this option to allow explicit music and podcasts (containing potentially offensive content) on the device.

iCloud Storage

You can enable or disable access to iCloud services.

Field Name	Description
Data backup	Select this option to allow users to back up data to iCloud.
Document sync	Select this option to allow users to sync documents to iCloud.
Photo Stream	Select this option to allow users to use Photo Stream to share photos with other Apple devices. If you disable this feature, Photo Stream photos will be erased from the user’s device and photos from the Camera Roll will be prevented from being sent to Photo Stream. If there are no other copies of the photos, they may be lost.
Shared photo streams	When this option is selected, users can invite others to view their photo streams and can view photo streams shared by others.

Credentials

To access Wi-Fi and Exchange accounts, mobile devices must have the proper credentials. To define the credentials to use for devices with this profile:

1. Click **Manage Credentials** in the Credentials section.
2. Select the credentials to apply.
3. Click the right arrow.
4. Click **OK**.

The credentials you select are sent to all devices with this profile.

To add credentials to the system, select **General** > **Credentials**. See *Adding credentials* for more information.

Wi-Fi settings

You can add Wi-Fi access accounts to the profile to allow users automatic access to your organization’s wireless networks.

Use the **Wi-Fi** section of the **Edit Profile** screen to add, edit, or delete available Wi-Fi access accounts for the profile.

Click **Add** to open the **Add Wi-Fi Account** screen (See *Adding a Wi-Fi access account*, page 34).

Email and Exchange settings

Use the **Email and Exchange** settings section of the **Edit Profile** screen to define email and Microsoft Exchange ActiveSync accounts to install on devices in the profile. See *Adding an email account*, page 36 and *Adding an Exchange ActiveSync account*, page 37 for more information.

Web clip settings

Web clips are shortcut links to URLs that appear on the iOS Home screen, just like apps. When a Web clip is added to the iOS profile, it is displayed on the Home screen of all iOS devices in the profile.

Use the **Web clip** section of the **Edit Profile** screen to manage Web clips in the profile. Click **Add** in the **Web clip** section of the **Edit Profile** screen to navigate to the **Add Web Clip Item** screen (See *Adding a Web clip*, page 38 for more information).

Adding apps to a profile

TRITON Mobile Security Help | Mobile Security Solutions

Apps can be automatically installed on devices during registration and profile update deployment. To install an app, you must add it to a profile:

1. Click **Add** in the **App Installation** section of the **Edit Profile** screen.
2. From the “Available apps” list, select the apps that you want installed on devices with this profile.
3. Click the right arrow to move the app to the “Apps included in this profile” pane.
4. Click **OK**.

To add apps to the “Available apps” list, see *Adding apps*, page 63.

Adding a Wi-Fi access account

TRITON Mobile Security Help | Mobile Security Solutions

Click **Add** in the **Wi-Fi** section of the **Edit Profile** screen to open the **Add Wi-Fi Account** screen.

Configure the following fields to add a Wi-Fi access account to the profile:

Field Name	Description
Service set identifier (SSID)	The identifier for the wireless network.
Automatically join the target network	Select this option to enable the device to automatically connect to your corporate network.
Network is hidden or not broadcasting	Select this option if the network is hidden.
Security type	The type of security encryption to use when connecting to the network. The following encryption options are available: ◆ None ◆ WEP: Use only WEP authentication. ◆ WPA/WPA2: Use only WPA authentication. ◆ Any (Personal): Also called pre-shared key mode (PSK). Devices can use WEP or WPA authentication, but can't connect to non-authenticated networks. ◆ WEP (Enterprise): Use only WEP authentication with a centralized authentication protocol. ◆ WPA/WPA2 (Enterprise): Same as WPA/WPA2 option above, but also supports EAP-TLS, EAP-TTLS, EAP-FAST, EAP-SIM, PEAP v0/v1, and LEAP 802.1X authentication methods. ◆ Any (Enterprise): Use either WEP or WPA (personal or enterprise) authentication and don't connect to non-authenticated networks.
Password	The password required to authenticate with the wireless network. (This field appears only when **WEP**, **WPA/WPA2**, or **Any (Personal)** encryption type is selected.)
Proxy type	Select how the Proxy settings are configured (none, manually or automatically).
Proxy server URL	(Note: This field is displayed only if Automatic is selected as the Proxy type.) The URL for the server from which to get proxy settings for this connection.
Server IP address	(Note: This field is displayed only if Manual is selected as the Proxy type.) The IP address of the proxy server to retrieve settings from.

Field Name	Description
Port	(Note: This field is displayed only if Manual is selected as the Proxy type.) The port to use when accessing the proxy server.
Username	(Note: This field is displayed only if Manual is selected as the Proxy type.) The user name to use when connecting to the proxy server.
Password	(Note: This field is displayed only if Manual is selected as the Proxy type.) The password to use when connecting to the proxy server.

Adding an email account

TRITON Mobile Security Help | Mobile Security Solutions

Use the **Add Email Account** screen to configure POP and IMAP email accounts. See *Adding an Exchange ActiveSync account*, page 37 to configure Microsoft Exchange email accounts.

Users are prompted for any information you do not provide here when they access the account on their device for the first time. They can also edit the account name, password, and SMTP server information later on their device.

Configure the following fields to add an email account to the profile:

Field Name	Description
Account name	The label that is displayed for the account.
Account type	The protocol used to access the email account (POP or IMAP).
Incoming Mail	
Mail server	Enter the host name or IP address for the incoming mail server.
Port	Enter the port number for the incoming mail server.
Authentication type	Select the authentication method the device should use to connect with the incoming mail server. • None • Password • MD5 Challenge-Response • NTLM • HTTP MD5 Digest For all options except None, supply the password to use.

Field Name	Description
Use SSL	Optional. Select this option to force the device to use Secure Sockets Layer when retrieving mail from the server.
Outgoing Mail	
Mail server	Enter the host name or IP address for the outgoing mail server.
Port	Enter the port number for the outgoing mail server.
Authentication type	Select the authentication method the device should use to connect with the outgoing mail server. ◆ None ◆ Password ◆ MD5 Challenge-Response ◆ NTLM ◆ HTTP MD5 Digest For all options except None, supply the password to use.
Outgoing password same as incoming	Select this option if the credentials you want to use for connecting to the outgoing mail server are the same as those for the incoming mail server.
Use SSL	Select this option to force the device to use Secure Sockets Layer when retrieving mail from the server.
Prevent email from within an app	Optional. Select this option to prevent this account from sending email from within third-party applications. This option is disabled by default.

Adding an Exchange ActiveSync account

TRITON Mobile Security Help | Mobile Security Solutions

Use the **Add Exchange ActiveSync Account** screen to configure Microsoft Exchange server settings for devices in the profile. Microsoft Exchange ActiveSync synchronizes users' email, contacts, tasks, and calendar information to the device from a Microsoft Exchange server. See *Adding an email account*, page 36 to configure other email accounts.

Users are prompted for any information you do not provide here when they access the account on their device.

Configure the following fields to add a Microsoft Exchange Server account to the profile:

Field Name	Description
Account name	Enter the label to be displayed for the account.
Exchange ActiveSync Host	Enter the name of the Microsoft Exchange Server the account is hosted on. • **Use SSL** - Select this option to force the device to use Secure Sockets Layer when connecting with this host. • **Use S/MIME** - Select this option to force the device to use Secure/ Multipurpose Internet Mail Extensions to send and receive MIME data. • **Prevent moving email into another account** - Select this option to prevent outbound messages in this email account from being moved into another account or forwarded or replied to from a different account. This option is disabled by default. • **Prevent email from within an app** - Select this option to prevent this account from sending email from within third-party applications. This option is disabled by default.
Domain	Enter the domain name for the account.
Synchronize mail for past	Select the number of days for which you want to sync email.
Authentication credential name	Select the credential to use for connecting to your ActiveSync server. If no options are listed, you have not uploaded a credential yet. Do this in the Credentials section of the Edit Profile page.
Include authentication credential passphrase	Select this option to install the account with the authentication credential passphrase. If you do not include the passphrase with the profile, users are prompted for it when they first access the account on their device.

Adding a Web clip

TRITON Mobile Security Help | Mobile Security Solutions

Click **Add** in the **Web clip** section of the **Edit Profile** screen to navigate to the **Add Web Clip Item** screen.

Configure the following fields to add a Web clip item to the profile:

Field Name	Description
Label	The label that is displayed below the icon on the iOS Home screen.
URL	The URL the Web clip links to (for example: http://www.websense.com).
Icon	Browse to an image file that you want to serve as an icon for the Web clip on the iOS Home screen. Click **OK** to upload the file to the system. The Web clips feature supports GIF, JPEG, and PNG image formats (the file should be less than 400 KB).
Allow user to remove Web clip	Select this option to allow the user to delete the Web clip on their device.
Remove shine effect from Web clip icon	Select this option to remove the shine effect automatically applied to icons in iOS.
Launch URL as full-screen Web app	Select this option to make the Web clip open the URL as a full-screen app (removes the browser address and toolbar).

Editing a policy

TRITON Mobile Security Help | Mobile Security Solutions

Related topics:

- *The policy template*, page 25
- *Adding a policy*, page 26
- *The Default policy*, page 26

Click the name of a policy on the **General** > **Policies** screen to open the **Edit Policy** screen. Use the **Edit Policy** screen to edit, enable, and disable profiles in the policy and enter a description for the policy.

After making changes to a policy, click **Save** on the **Policies** > **Edit Policy** screen to apply the changes to devices assigned to the policy going forward, then click **Deploy** to apply saved changes to all devices currently assigned to the selected policy.

✓ **Note**

To apply policy changes to all devices currently assigned to a policy, you must click **Save** and then **Deploy**. If you click only **Save**, the changes will not be applied to devices currently assigned to the policy, only to devices assigned to the policy after that time.

Editing a profile

Click the name of a profile on the **General** > **Policies > Edit Policy** screen to open the **Edit Profile** screen. See *Defining a profile*, page 27 for more information on the configuration options.

Disabling a profile

You can disable the personal profile in a policy so that end users cannot select that profile option when registering a device. Click **Disable** in the status column of the **Profile list** on the **Policies** > **Edit Policy** screen to disable that profile in the policy. You can enable the profile again at any time by clicking **Enable** in the status column.

Disabling a profile will not affect devices currently assigned to that profile. If you want to remove all devices from this profile, navigate to the **General** > **Devices** screen, search by policy and assign the devices listed with that profile to another profile.

Managing users

TRITON Mobile Security Help | Mobile Security Solutions

Use the **General > Registered Mobile Users** page to search for users and view assigned policies and the registered devices associated with the users. From this page, click a device name in the **Devices** column to edit device details, or click a policy name in the **Policies** column to edit the policy. Policies are assigned when devices are registered. Device users select the policy to apply based on whether the device is for their personal or corporate use.

See *Editing a policy*, page 39 and *Update device information*, page 46 for detailed instructions on editing policies and device information.

3 Managing devices

TRITON Mobile Security Help | Mobile Security Solutions

Related topics:

- *Registering new devices*, page 41
- *Editing device details*, page 45
- *Customize profile*, page 48
- *Wiping a device*, page 48
- *Locking a device*, page 49
- *Clearing the passcode on a device*, page 50
- *Removing a profile from a device*, page 50

Use the **General** > **Devices** screen to:

- Register new mobile devices with Mobile Security. (See *Registering new devices*, page 41.)
- Wipe, lock, and delete mobile devices. (See *Wiping a device*, page 48, *Locking a device*, page 49, and *Removing a profile from a device*, page 50.)
- Clear the password on mobile devices. (See *Clearing the passcode on a device*, page 50.)
- View device information, including the device type, user, status, and the assigned policy and profile. (See *Viewing device details*, page 44.)
- Access the Edit Device screen. Click the name of a device to view and edit device details. (See *Editing device details*, page 45.)

Registering new devices

TRITON Mobile Security Help | Mobile Security Solutions

Related topics:

- *Editing device details*, page 45

To protect devices from web threats and enable device management features, mobile devices must first be registered with Mobile Security.

The following steps must be completed to register a new mobile device with Mobile Security.

1. An administrator sends the end user an email message from the Mobile tab of the Cloud TRITON Manager requesting that they register their mobile device.
2. The end user opens the email message on the device to be registered and follows the link to the Device Registration portal.
3. The end user logs on to the Device Registration portal and selects the appropriate profile for the device (For example, personal or corporate).
4. The device profile is pushed out to the device.

Sending registration messages

Administrators must send email messages asking end users to register mobile devices from the Mobile tab of the Cloud TRITON Manager. You can also customize the text in this message (see *End-user settings*, page 43). Use the **General** > **Devices** > **Register New Device** screen to send these messages.

To send device registration requests to end users:

1. Search for the user or user group of interest. These are pulled from your user directory service.
2. Select the check box next to the users you want to register.
3. Click the right arrow (>) to move the selected end users into the right pane.
4. If you want to resend the email to selected users who have previously been sent a device registration request, select the **Send multiple requests** check box.
5. Select a policy to apply to the device when it is enrolled (if you do not select a policy here, the default policy is applied to the user).
6. Click **OK** to send a device registration request email message to the selected users.

End-user device registration

End users receive an email message prompting them to register their device with Mobile Security. You can customize this message on the **General** > **End-user Settings** screen (See *End-user settings*, page 43). .

✓ **Note**

- Users must open the registration request email message on the device they intend to register, so that the user profile can be pushed onto the device.
- Users can use the same device registration request message to register multiple devices.

In the Device Registration portal, users are prompted to enter their network or Websense Cloud Security email address and password. The Cloud Security password was created by end users if they were previously asked to register with Cloud Security. They must select the appropriate device profile and agree to their organization's end-user license agreement (see *End-user settings*, page 43).

After the end user clicks **Install**, the Mobile Security user profile is pushed to the mobile device. The end user is then notified that the registration process is complete. Once the registration process is complete, the end user's device appears in the Mobile tab of the Cloud TRITON Manager with **Initial registered** status.

If a required profile fails to install on a device, you are sent a notification by email.

Javascript must be enabled on users' mobile devices to complete the registration process.

End-user settings

TRITON Mobile Security Help | Mobile Security Solutions

Use the **General** > **End-user Settings** screen to:

- Edit the text included in the device registration request email message sent to users.
- Upload usage agreements for device profiles.
- Configure which device management features are available to end users in the end-user Device Management portal.
- Configure Exchange server settings so that users can log on with their domain credentials.

Editing the registration email

Use the **Registration Email** section to customize the text included in the device registration request message. The text you input here is included at the top of the message.

If Exchange is not yet configured on their device, tell users how to access the message in the registration email that you send. For example, tell users to open the message in Webmail or forward it to their personal accounts, and then open the message on the device they want to register.

Edit the message in the text field to change the text content of the email message sent to end users, then click **OK** to save your changes.

Uploading end-user usage agreements

Use the **Usage Agreements** section to upload end-user usage agreements to appear when end users register new devices. To add a usage agreement, click **Add** and upload a text file containing the desired usage agreement, then click **OK** to save your changes. You can define which device profile the usage agreement is associated with on the **Edit Profile** screen (see *Defining a profile*, page 27).

End-user Device Management portal functionality

As an administrator, you can define which device management features are available to end users. If you select to enable a feature on the **End-user Settings** screen, users have access to that feature in the end-user Device Management portal. The following features can be enabled for end users to manage their registered devices in the portal:

Management Feature	Description
Wipe	Wiping a device restores the device to factory settings and permanently deletes all data, including personal data.
Lock	The lock feature locks the device and requires the device passcode to unlock it.
Clear passcode	Clearing the passcode on a device unlocks the device and prompts the user to define a new passcode (if a passcode is required by the assigned device profile).

Configuring Exchange for domain credential use

Users are prompted for user name and password in two places:

- When prompted in the Device Registration portal while registering their device with Mobile Security
- When logging onto the end-user Device Management portal

Normally users log on with their Cloud Security credentials, but not all users have these.

To enable users to log on with their domain credentials (network user name and password), enter the URL of your Exchange server in the space provided. Mobile Security will connect to your Exchange server to authenticate users.

✓ **Note**

This feature is available with Microsoft Exchange Server version 2003 or later, but you need to enter the URL of your Exchange server only if you are using version 2003.

Viewing device details

TRITON Mobile Security Help | Mobile Security Solution

Select **General** > **Devices** to view or manage the mobile devices in your organization. A list of devices appears, along with the following information:

Column	Description
Device Name	Name given to the device when it was registered
Device Type	Type of device: iPad, iPad mini, or iPhone
User	Name of device owner
Status	Device status, such as registered or jailbroken
Policy/Profile	The policy and profile assigned to the device

On this page, you can search for devices by these categories. For example, you can search by **Device Type > iPad** to list only iPads, or by **Status > Jailbroken** to locate devices that have been compromised.

You can also lock a device, clear its passcode, wipe a device, delete a device, or invite users to register their devices.

Editing device details

TRITON Mobile Security Help | Mobile Security Solutions

Related topics:

- *Customize profile*, page 48
- *Registering new devices*, page 41
- *Removing a profile from a device*, page 50
- *Wiping a device*, page 48
- *Locking a device*, page 49
- *Clearing the passcode on a device*, page 50

Click the name of a device on the **General** > **Devices** page to view and edit device details.

On the **Devices** > **Edit Device** screen, you can view and update device and application information, view and edit the user policy and profile assigned to the device, and delete the device. You can also customize the device profile for the selected device (See *Customize profile*, page 48).

Editing the policy and profile assigned to a device

Mobile devices are associated with a user policy and device profile during the registration process. However, you can edit these settings later on the **Devices** > **Edit Device** screen.

- To change the user policy, select a policy from the **User policy** drop-down menu. Click **OK** to save your changes.
- To change the device profile, select a profile for the device from the **Policy profile** drop-down menu. Click **OK** to save your changes. You can also customize the profile for this specific device by selecting Customize Selected Profile (see *Customize profile*, page 48).

For more information on policies and profiles, see *Policy Management*, page 25.

Update device information

Mobile Security queries each device daily for some basic information.

On the **Details** tab of the **Devices** > **Edit Device** screen, the following information is displayed, as reported by the device.

Field Name	Description
Identifier	The Unique Device Identifier (UDID) associated with the device.
OS version	The version of the operating system running on the mobile device.
Phone number	The phone number associated with the device (if applicable).
Model name	The model name of the mobile device.
Model number	The model number of the mobile device.
Product name	The model code of the mobile device.
Serial number	The serial number of the device.
Device capacity	Memory available on the device (in GBs).
Cellular technology	The cellular technology standard used by the device (GSM, CDMA, etc.).
IMEI	The International Mobile Equipment Identity (IMEI) number associated with the device.
MEID	The Mobile equipment identifier (MEID) number associated with the device.
Modem firmware version	The version of the firmware used by the device's modem.
Bluetooth MAC	The MAC address associated with the bluetooth feature on the device.
Wi-Fi MAC	The MAC address associated with the Wi-Fi address on the device.
Current carrier network	The wireless network currently in use by the device.
SIM carrier network	The wireless network associated with the SIM card in use by the device.

Field Name	Description
Carrier settings version	The version of the carrier settings file currently installed on the device.
Subscriber MCC	The subscriber’s home Mobile Country Code (MCC).
SIM MCC	The Mobile Country Code (MCC) associated with the installed SIM card.
SIM MNC	The Mobile Network Code (MNC) associated with the installed SIM card.
Current MCC	The current Mobile Country Code (MCC) associated based on the device’s current location.
Current MNC	The current Mobile Network Code (MNC) based on the wireless network currently in use by the device.

To request updated device information from the device, click **Update Device Information** (this information is automatically updated once per day when the device is available).

Update device applications

Mobile Security queries each device daily for information about the applications installed on the device.

On the **Applications** tab of the **Devices** > **Edit Device** page, you can view information about all apps on the device.

The following information is shown for each app.

Field Name	Description
Name	The name of the installed application.
Identifier	The unique identifier for this application.
Version	The version number of the application installed on the mobile device.
App Size	The static size of the application bundle (in megabytes). This includes the executable file and all related resources.
Cache Size	The amount of disk space used by the application when it is running, including documents, folders, and other data (in megabytes). Cache size varies according to the processes that are being run.

You can use this information to assess risk when a device is lost. Once you know the apps installed on the device, you can generate reports on app usage. (Use the reporting functions of your Web Security product.)

To request updated application information from the device, click **Update Device Applications** (this information is automatically updated once per day when the device is available).

If desired, you can export this data to a PDF or Microsoft Excel spreadsheet.

Customize profile

TRITON Mobile Security Help | Mobile Security Solutions

On the **Edit Device** screen, you can customize the device profile for the selected device. Click **Customize Selected Profile** to open the **Customize profile** page.

Changes you make on the **Customize profile** page will affect only the selected device. The new customized profile is not available to assign to other devices.

See *Defining a profile*, page 27 for more information on profile settings.

Adding credentials

TRITON Mobile Security Help | Mobile Security Solutions

Select **General > Credentials** to upload X.509-compliant credential certificates necessary for accessing your organization’s network resources. Certificates uploaded here are installed on devices when relevant profiles are deployed.

To upload a new certificate:

1. Click **Add** to open the **Add Credential** screen.
2. Enter a name for the certificate in the **Credential Name** field.
3. Click **Browse** and upload a certificate file in the **File** field (.cer, .crt, .der, .p12, and .pfx certificate file types are supported).
4. Click **OK** to save your changes and upload the certificate.

To define which credentials to use for each profile, see *Defining a profile*, page 27.

Wiping a device

TRITON Mobile Security Help | Mobile Security Solutions

Related topics:

- *Locking a device*, page 49
- *Clearing the passcode on a device*, page 50
- *Removing a profile from a device*, page 50
- *Editing device details*, page 45

The wipe feature in Mobile Security restores devices to default factory settings and permanently deletes all personal data.

To wipe a device, select the device and click **Wipe Device** on the **General** > **Devices** screen. A message appears asking you to confirm that you would like to wipe the selected device. Click **Confirm** to complete the operation. You can monitor the status of the wipe operation on the **General** > **Jobs Queue** page.

If you have given end users the ability to wipe data from their devices, they can do this from the end-user Device Management portal. See *End-user self service*, page 59 for more information. For configuration instructions, see *End-user settings*, page 43.

The system notifies users and administrators by email when a device has been wiped, regardless of who wiped it.

Locking a device

TRITON Mobile Security Help | Mobile Security Solutions

Related topics:

- *Wiping a device*, page 48
- *Clearing the passcode on a device*, page 50
- *Removing a profile from a device*, page 50
- *Editing device details*, page 45

The lock feature in Mobile Security locks the device and requires the device passcode to unlock it.

To lock a device, select the device on the **General** > **Devices** screen and click **Lock**. A message appears asking you to confirm that you would like to lock the selected device. Click **Yes** to complete the operation. You can monitor the status of the lock operation on the **General** > **Jobs Queue** page.

If you have given end users the ability to lock their devices, they can do this from the end-user Device Management portal. See *End-user self service*, page 59 for more information. For configuration instructions, see *End-user settings*, page 43.

The system notifies users and administrators by email when a device has been locked, regardless of who locked it.

Clearing the passcode on a device

TRITON Mobile Security Help | Mobile Security Solutions

Related topics:

- *Wiping a device*, page 48
- *Locking a device*, page 49
- *Removing a profile from a device*, page 50
- *Editing device details*, page 45

Mobile Security allows you to clear the passcode on a device, effectively unlocking the device.

To clear the passcode on a device, select the device on the **General** > **Devices** screen and click **Clear Passcode**. A message appears confirming that you would like to clear the passcode on the selected device. Click **Yes** to complete the operation. You can monitor the status of the operation on the **General** > **Jobs Queue** page.

If you have given end users the ability to clear passcodes on their devices, they can do this from the end-user Device Management portal. See *End-user self service*, page 59 for more information. For configuration instructions, see *End-user settings*, page 43.

Removing a profile from a device

TRITON Mobile Security Help | Mobile Security Solutions

Related topics:

- *Wiping a device*, page 48
- *Clearing the passcode on a device*, page 50
- *Locking a device*, page 49
- *Editing device details*, page 45

Select a device on the **General** > **Devices** screen and click **Remove Profile** when you want to remove a device from Mobile Security but not wipe it entirely.

This operation generates a task to remove the Mobile Security profile from the device and updates the device status in the management portal to “Deleted.”

The relationship between Mobile Security and the device ends as a result. All settings, profiles, and accounts installed by Mobile Security are removed from the device and your organization’s security policies are no longer enforced.

The system notifies users and administrators by email when a profile has been deleted from a device, regardless of who deleted it.

Device jailbreaking

TRITON Mobile Security Help | Mobile Security Solution

Occasionally users want to remove the limitations imposed on their devices by the iOS operating system or circumvent security features on their devices. One way to do so is by hacking into their device operating system using hardware or software exploits. This is known as jailbreaking.

Jailbreaking gives users root access to the operating system so they can configure their Exchange or corporate VPN access privileges or erase the TRITON Mobile Security profile if they want. They can also download apps, extensions, and themes that are unavailable through the Apple App Store.

Jailbroken devices compromise your enterprise security.

To safeguard your information assets, Mobile Security prevents jailbroken devices from registering with the system.

In addition, if it detects that a registered device becomes jailbroken, it does several things:

1. It alerts you by email.
2. It adds an alert to the **General > Alerts** page on the Cloud Security portal. On this page, it lists the number of compromised devices and gives a link to a filtered device view.
3. It logs the incident for reporting purposes. You can view reports to see who has jailbroken (**General > Reporting > Jailbroken Devices)**. Once you see which devices have been compromised, you may choose to perform a remote wipe to protect your assets. The system resets devices when they are wiped so they can reregister with the system.

4 Reporting

TRITON Mobile Security Help | Mobile Security Solutions

Related topics:

- *User summary reports*, page 53
- *Device summary reports*, page 54
- *Administrative actions summary reports*, page 57

Mobile Security provides several reporting tools for viewing trends and statistics for registered users, devices, and administrative actions. On the **General** > **Reporting** screen you can generate reports based on users, devices, and administrative actions.

- **User Summary** reports: User reports display information about users with registered mobile devices. With user reports, you can generate summaries of mobile users per user group, top bandwidth users, and bandwidth use trends by user and user group.
- **Device Summary** reports: Use device reports to review summaries of registered devices. With device summary reports, you can generate reports on devices by type, the most installed applications, and device details by user.
- **Actions Summary** reports: Use actions reports to generate summaries of administrative actions (for example: wiping or locking a device, or clearing the passcode on a device) completed per device or user group over time, top devices for a specific administrative action, and completed action details.

User summary reports

TRITON Mobile Security Help | Mobile Security Solutions

Related topics:

- *Device summary reports*, page 54
- *Administrative actions summary reports*, page 57

Use the **User Summary** reports section on the **General** > **Reporting** page to generate reports about users with registered mobile devices.

1. Select the report you would like to generate.

Report	Description	Output
Mobile users per user group	Displays the number of users with registered mobile devices in each user group in your organization.	Text table and bar graph
Devices per user	Displays the number of devices registered to each user for selected users and user groups.	Text table
Bandwidth use trends	Displays bandwidth use over the specified time period for selected user groups or for all registered mobile users.	Text table and chart
Top bandwidth users	Displays users consuming the most bandwidth. You can display top bandwidth users in selected user groups or from all registered mobile users.	Text table and bar graph

2. Select the users you would like to include in the report in the **Report Settings** pane (if applicable):
    a. Select **Display for all users** to include all users with registered mobile devices in your organization, or select **Filter results** to run the report on specific users or user groups.
    b. To select specific users or user groups to include in the report, select the check box next to users and user groups you would like to include in the search results box and click the right arrow (>**).**
3. Some reports let you specify the device type to report on. Choose iPhone or iPad depending on your needs. (iPad includes iPad mini.)
4. Some reports let you group results by day or week. Indicate your preference in the **Group by** field.
5. Click **Generate Report**.

Device summary reports

TRITON Mobile Security Help | Mobile Security Solutions

Related topics:

- *User summary reports*, page 53
- *Administrative actions summary reports*, page 57

Use the **Device Summary** section of the **General** > **Reporting** page to generate reports about registered devices.

Select the report you would like to generate. You can generate the following device-based reports:

Report	Description	Output
Devices by type	Displays how many devices of each type (for example, iPads or iPhones) are registered in your organization.	Text table and bar graph
Device details by user	Displays details for all devices registered to selected users. Device details include: group name, user name, device OS, device type, policy, profile, and device status.	Text table
Top applications	Displays how many of the most popular applications (apps) are installed on registered devices.	Text table and bar graph
Jailbroken devices	Displays the number of jailbroken devices in your organization by device and user name, group, type, and operating system.	Text table

Devices by type

TRITON Mobile Security Help | Mobile Security Solution

This report displays how many devices of each type (for example, iPads or iPhones) are registered in your organization.

To generate a Devices by Type report:

1. Select **General** > **Reporting** > **Devices by type**.
2. Click **Generate Report**.

Device details by user

TRITON Mobile Security Help | Mobile Security Solution

This report displays details for all devices registered to selected users. Device details include: group name, user name, device operating system, device type, policy, profile, and device status.

To generate a Devices Details by User report:

1. Select **General** > **Reporting** > **Device details by user**.
2. Select the users you would like to include in the report in the Report Settings pane:
   a. Select **Display for all users** to include all users with registered mobile devices in your organization, or select **Filter results** to run the report on specific users or user groups.
   b. If you select **Filter results**, enter a search term then click **Search**. In the results window, select the users and user groups you would like to include and click the right arrow (>**).**
3. Click **Generate Report**.

Top applications

TRITON Mobile Security Help | Mobile Security Solution

This report displays how many of the most popular applications (apps) are installed on registered devices.

To generate a Top Applications report:

1. Select **General** > **Reporting** > **Top applications**.
2. Specify the device type to report on. Choose iPhone or iPad. (iPad includes iPad mini.)
3. Select applications to exclude from the report.
   a. Click **Search** to find all applications, or enter a search term to filter the results.
   b. In the results window, select the applications you would like to exclude and click the right arrow (>**).**
4. Specify how many applications to include in the report. You can choose between 5 and 20.
5. Click **Generate Report**.

Jailbroken devices

TRITON Mobile Security Help | Mobile Security Solution

This report displays the number of jailbroken devices in your organization by device and user name, group, type, and operating system.

To generate a Jailbroken Devices report:

1. Select **General** > **Reporting** > **Jailbroken devices**.
2. Select the users you would like to include in the report in the **Report Settings** pane:
   a. Select **Display for all users** to include all users with registered mobile devices in your organization, or select **Filter results** to run the report on specific users or user groups.
   b. To select specific users or user groups to include in the report, select the check box next to users and user groups you would like to include in the search results box and click the right arrow (>**)**.
3. Specify the device type to report on. Choose iPhone or iPad. (iPad includes iPad mini.)
4. Specify a date range for the report.
5. Click **Generate Report**.

For more information on jailbreaking and the way the system handles it, see *Device jailbreaking*, page 51.

Administrative actions summary reports

TRITON Mobile Security Help | Mobile Security Solutions

Related topics:

- *User summary reports*, page 53
- *Device summary reports*, page 54

Use the **Actions Summary** section of the **General** > **Reporting** page to generate reports about administrative actions — for example, wiping or locking a device, or clearing the passcode on a device.

1. Select the report, **Administrative actions per device**. This report displays the number of administrative actions performed on selected devices and devices registered to selected users.
2. Search for the users or groups of interest.
3. Select the users you would like to include in the report and click the right arrow (**>**).
4. Select the devices you would like to include in the report and click the right arrow (**>**).
5. Specify a date range to include in the report in the **From** and **To** fields.
6. Select the administrative actions to include in the report. You can select actions by name.

Administrative Action	Description
Application information updated	Display devices that had their application information updated by an administrator. This action is performed on the **Devices** > **Edit Device** screen.
Device information updated	Display devices that had their device information updated by an administrator. This action is performed on the **Devices** > **Edit Device** screen.
Email profile installed	Display devices that had a Mobile Security email profile installed.
Email profile removed	Display devices that had their Mobile Security email profile removed.
Exchange profile installed	Display devices that had a Mobile Security Exchange profile installed.
Exchange profile removed	Display devices that had their Mobile Security Exchange profile removed.
Locked	Display the devices that were locked by an administrator or user. See *Locking a device*, page 49 for more information.

Administrative Action	Description
MDM profile removed by administrator	Display devices that had the Mobile Security MDM profile removed by an administrator.
MDM profile removed by user	Display devices that had the Mobile Security MDM profile removed by a user.
Passcode cleared	Display devices whose passwords were cleared. This operation can be initiated by either a user or an administrator. See *Clearing the passcode on a device*, page 50 for more information.
Registered	Display the devices registered with Mobile Security.
Settings profile installed	Display devices that had the Mobile Security Settings profile installed.
VPN profile installed	Display devices that had the Mobile Security VPN profile installed.
VPN profile removed	Display devices that had the Mobile Security VPN profile removed.
Wi-Fi profile installed	Display devices that had a Mobile Security Wi-Fi profile installed.
Wi-Fi profile removed	Display devices that had their Mobile Security Wi-Fi profile removed.
Wiped	Display the devices that were wiped by an administrator or user. See *Wiping a device*, page 48 for more information.

7. Click **Generate Report**.

5 End-user self service

TRITON Mobile Security Help | Mobile Security Solutions

Related topics:

- *Accessing the portal*, page 59
- *End-user portal features*, page 60
- *End-user settings*, page 43

The end-user Device Management portal allows end users to monitor device status, wipe and lock devices, and clear the passcode for devices they register with Mobile Security. As an administrator, you can configure which device management features are available to end users in the portal.

Use the **General** > **End-user Settings** screen in the Mobile tab of the Cloud TRITON Manager to set up the end-user Device Management portal environment for your end users.

Accessing the portal

TRITON Mobile Security Help | Mobile Security Solutions

Related topics:

- *End-user portal features*, page 60
- *End-user settings*, page 43

End users receive the URL for the end-user Device Management portal in an email message sent by Mobile Security when a device has been successfully registered.

The logon credentials for the end-user Device Management portal are the same as the Device Registration Portal (the end user's corporate email address and their Cloud Security password). A **Forgot your password?** link is provided on the End-user Device Registration Portal logon page if end users need to look up their password.

End-user portal features

TRITON Mobile Security Help | Mobile Security Solutions

Related topics:

- *Accessing the portal*, page 59
- *End-user settings*, page 43

The end-user Device Management portal displays the following information about the devices registered to the user:

Field Name	Description
Device Name	The device name specified in the Mobile tab of the Cloud TRITON Manager.
Model	The device model (for example, iPad or iPhone).
Status	The status column displays device updates when device management operations are completed on the device (for example, Locked, Wiped, etc.).
Device Type	The device profile assigned to the device.

The portal can also be configured to allow end users to wipe or lock their devices and clear the passcode on their devices.

You can configure which device management features are available to end users on the **General** > **End-user Settings** screen (see *End-user settings*, page 43 for configuration instructions).

For instructions on using the portal, see the Mobile Device User's Guide. These instructions are available to end users when they click **Help** in the portal.

6 Application Management

TRITON Mobile Security Help | Mobile Security Solutions

Related topics:

- *Viewing apps*, page 24
- *Adding apps*, page 26
- *Adding apps to a profile*, page 34
- *Deleting apps*, page 27

TRITON Mobile Security lets you automatically install apps on devices when they register with the system or when you deploy profile updates. You can install:

- Free Apple Store apps like Concur or Salesforce
- Apps that have been purchased with Apple's volume purchase program (VPP)

To do so:

1. Add apps to the Application Management repository. See *Adding apps*, page 26.
2. Add apps to specific policy profiles. See *Adding apps to a profile*, page 34.

When profiles are pushed to devices, the apps are installed.

✓ **Note**
This feature works only with iOS 5 and above.

Viewing apps

TRITON Mobile Security Help | Mobile Security Solutions

Related topics:

- *Adding apps*, page 26
- *Deleting apps*, page 27

Select **General > Application Management** to view a list of the apps in your system. Click a tab to view the free apps or purchased apps that have been added.

✓ **Note**

These apps are managed by the system, but may or may not be installed on any devices. To install a managed app on a device, you must add it to a device profile, and update or register the device.

Free apps

The Free Apps tab lists free apps that you've added to the system. Free apps are those that do not need to be purchased, such as Concur or Salesforce. In the app list, you can see the following information:

Column	Description
Application	Name of the app
Description	Description of the app
Genre	Type of app, such as productivity or games
Version	Version of the app
Device Type	Type of device the app applies to
Policies/Profiles	Click a link to view a list of all the policies and profiles that include this app.

Click an application name to view details about it, including the URL of the app.

Purchased apps

The Purchased Apps tab lists apps that you've purchased by a volume purchase pack (VPP) and added to the system. In the app list, you can see the following information:

Column	Description
Application	Name of the app
Description	Description of the app
Genre	Type of app, such as productivity or games
Version	Version of the app
Device Type	Type of device the app applies to

Column	Description
Price	The price of the app per user
Redemption Details	Click a link to view an estimate of the number of app downloads remaining in the volume purchase pack. Listed are the number of redemption codes purchased and an estimate of the number redeemed and remaining. If you need to upload a new redemption file, return to the Purchased Applications main page, click the application name, and then browse to the redemption file in the field provided.
Policies/Profiles	Click a link to view a list of all the policies and profiles that include this app.

Click an application name to view details about it and to upload a redemption file.

Redemption files are provided by Apple when you purchase apps. If you purchase apps in volume, such as with the VPP, the file contains multiple redemption codes. Mobile Security can manage your redemption codes to ensure that you are using the apps as licensed.

Click **Browse** to locate your redemption file, and then click **OK**. Only **.xls** files are supported.

Adding apps

TRITON Mobile Security Help | Mobile Security Solutions

Related topics:

- *Viewing apps*, page 24
- *Deleting apps*, page 27

To add an app to the system’s app repository:

1. Navigate to the **General > Application Management** page.
2. Click the tab pertaining to the type of app you want to add: Free Apps or Purchased Apps.
3. Click **Add Apps**.
4. You can add free and purchased apps 2 ways:
   a. You can search the App Store for the app you want to add to the system and then click **Add App** when you find it. (Do this on the Search App Store tab.)

b. You can enter the URL of the app from the Apple Store. (Do this on the Enter iTunes URL tab.) If you are not sure how to obtain the URL, click **Need help finding the application URL?**

   When you've entered the URL, click **Get App Details**. A popup displays the name, genre, version, device type and URL for the app that you entered. If this is the app you want to add, click **Add App**. If this is a purchased app, upload the redemption file provided by Apple first.

5. Click **OK** when done.

The app now appears on the **General > Application Management** page where you can add more apps if desired.

If an app has already been added to the system, an error message displays.

To install the app on devices, you must add it to a profile, and then the profile must be pushed to the device through registration or profile update.

Deleting apps

TRITON Mobile Security Help | Mobile Security Solutions

Related topics:

- ◆ *Viewing apps*, page 24
- ◆ *Adding apps*, page 26

To delete an app from the system's app repository, first remove it from all the profiles that include it or an error message displays when you attempt to delete it. If the error message displays, remove the app from all the profiles that include it, and then try again. Select it on the **General > Application Management** page and then click **Delete Apps**. You can select multiple apps if desired.

If the app is not in a profile, you are asked to confirm the operation and notified when the operation is successful.

When an app is deleted from this page, it can no longer be added to profiles, but the app is not deleted from devices where it is already installed.