# 1 Getting Started with TRITON Mobile Security



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.

TRITON Mobile Security requires either a subscription to Web Filter & Security with the Web Filter Security Cloud module or TRITON AP-WEB with the Web Hybrid module.

This guide explains how to set up the Mobile Security add-on for the first time.

To get started with Mobile Security, do the following.



## Device operating systems

TRITON Mobile Security supports Apple® iPhone®, iPad®, and iPad mini models running the following operating systems:

- iOS v5 and later

## Step 1: Request a cloud service account



TRITON Mobile Security is managed through the Mobile tab in the Cloud TRITON Manager, also referred to here as the "portal." If you are a Websense customer using Web Filter & Security with the Web Filter Security Cloud module, you already have a cloud service account with logon credentials to the portal.

If you are a customer using TRITON AP-WEB with the Web Hybrid module, you must request credentials to the portal through Websense Technical Support.

See Knowledge Base article 6112 for details you'll require when making the request.

Once you have a cloud service account, proceed to *Step 2: Log onto the administrator portal*.

## Step 2: Log onto the administrator portal

Getting Started Guide | Mobile Security Solutions

To manage and configure TRITON Mobile Security, you use the Mobile tab in the Cloud TRITON Manager.

To access the portal, visit https://admin.websense.net/portal/ using one of the following browsers:

- Microsoft Internet Explorer (Windows platform only), versions 8 through 11
- Mozilla Firefox (Windows and MAC platforms)
- Google Chrome (Windows and MAC platforms)
- Apple Safari (MAC platform only)
  - Safari 3.1 on MacOS X 10.4
  - Safari 5.x on MacOS X 10.6 and 10.7
  - Safari 6.x on MacOS X 10.8
  - Safari 7.x on MacOS X 10.9
  - Safari 8.x on MacOS X 10.10.

While the portal supports Microsoft Internet Explorer, Apple requires that you use either Firefox or Safari to upload the Apple Push Notification certificate file.

To use the portal, your browser must be Javascript-enabled. For the best user experience, your browser should also be enabled to accept cookies from the portal.

Once you're logged on, proceed to *Step 3: Synchronize your user directory information*.

## Step 3: Synchronize your user directory information

Getting Started Guide | Mobile Security Solutions

The cloud web solution and the hybrid solution allow you to make use of existing LDAP directories, such as Active Directory, so you don't have to recreate user accounts and groups for your mobile services or manage users and groups in two places.

Although Web Filter & Security is a cloud-based service, it synchronizes with LDAP directories via a client-resident application known as the Directory Synchronization Client.

If you are not already a cloud service customer, you must install a new instance of the Directory Synchronization Client and synchronize your directory entries. For step-by-step instructions, see the Directory Synchronization Client Administrator's Guide.

Configure how the hybrid solution synchronizes user directory data with the hybrid service in the Web tab of the TRITON Manager. Go to the **Settings > Hybrid Configuration > Shared User Data** page.

Select specific contexts from the Active Directory global catalogs already configured for on-premises user identification. Only directory entries in the specified contexts are sent to the hybrid service. For more details, see "Configure Directory Agent settings for hybrid filtering" in the Administrator Help for the Web module.

Once you've synchronized your user directory information, proceed to *Step 4: Define web security policies*.

# Step 4: Define web security policies

Getting Started Guide | Mobile Security Solutions

If you have not done so already, define your web security policies in one of the following locations:

- In the Web tab of the Cloud TRITON Manager, on the **Policy Management** > **Policies** page.
- In the Web tab of the TRITON Manager on the **Policy Management > Policies** page.

These policies will govern web traffic on mobile devices. To create a new policy in either the Cloud TRITON Manager or the TRITON Manager, click **Add** on the Policies page. Very restrictive policies are not recommended for use with Mobile Security, since blocking access to web categories also blocks app-based web requests associated with those categories.

For your initial deployment, consider relaxing existing policies to block only high-risk categories such as Gambling, Illegal and Questionable, Militancy and Extremist, Racism and Hate, Security, Extended Protection, Tasteless, Violence, and Weapons.

Be aware that your policies affect both desktop and mobile-device Internet access management for the users assigned to the policy.

For more information on web policy configuration in the Cloud TRITON Manager, see "Defining Web Policies" in the cloud web Help.

For more information about policy configuration in the Web tab of the TRITON Manager, see "Working with policies" in the Administrator Help for the Web module.

Once you've created your web policy, proceed to *Step 5: Generate an Apple Push Notification certificate*.

# Step 5: Generate an Apple Push Notification certificate

Getting Started Guide | Mobile Security Solutions

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

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

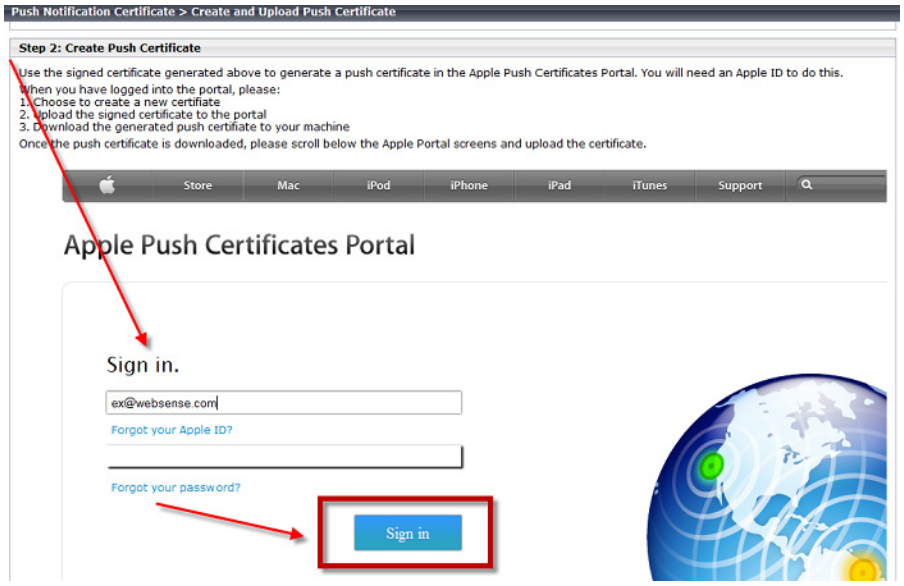
1. In the Mobile tab, select **General > Push Notification Certificate**.
2. Click **Create and Upload Certificate**. This process consists of three main steps.
3. In the Step 1: Create Signed Certificate box:
   a. Enter information about your organization. This information will be used when generating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

| Field Name | Description |
|---|---|
| Certificate name | Enter a name that you would like to assign to your organization's signed certificate. |
| Organization | Enter the name of your organization, such as your company name. |
| Organization unit | If applicable, enter the name of the organizational unit that will be using this mobile security certificate. |
| 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.

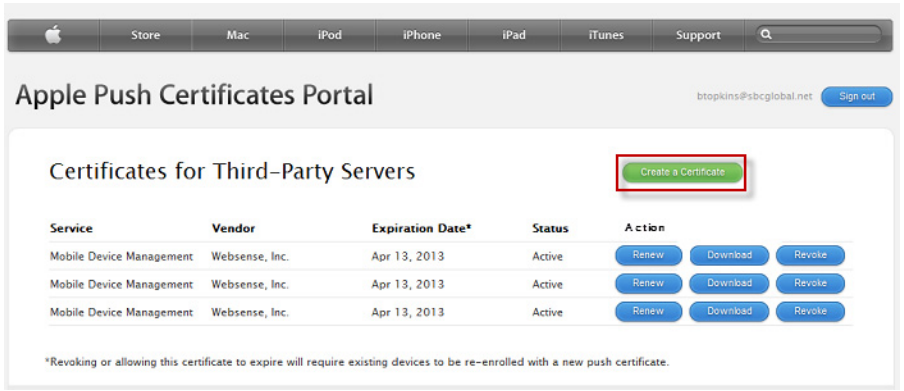
   a. Sign onto the Apple Push Certificate Portal by entering your organization's Apple ID and password in the fields provided. You can also sign into the portal by navigating to https://identity.apple.com/pushcert/.




   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.

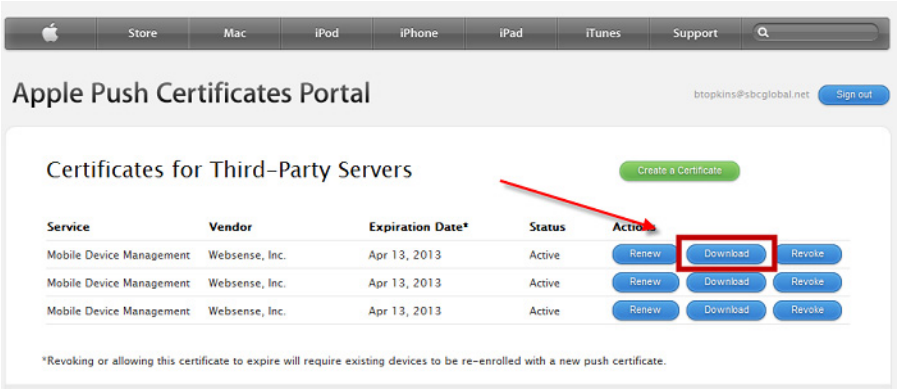
   c. Select **Create a Certificate**.




   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.


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




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**.

Once you've uploaded the APN certificate, proceed to *Step 6: Customize policies and device profiles*.

# Step 6: Customize policies and device profiles

Getting Started Guide | Mobile Security Solutions

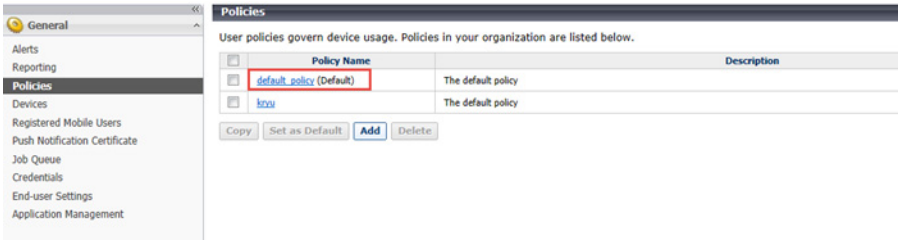
Policies govern end users' device usage. TRITON Mobile Security includes a predefined policy template that can be customized to meet your needs. You can also create your own custom policies.

Policies are made up of corporate and personal device profiles. These govern what functions will be allowed or blocked on each device as well as things like Wi-Fi and email settings.

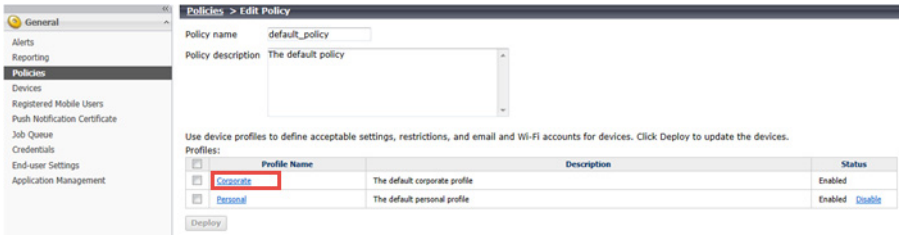
Corporate profiles are typically more strict than personal profiles. By default, corporate profiles are assigned to corporate devices and personal profiles to personal devices.

Before you get started, configure the corporate and personal profiles used by your policies.

1. In the Mobile tab, select **General > Policies**.
2. Click the policy name, such as **default_policy**.




3. In the Device Profile table, click **Corporate**.




4. Under **Restrictions > Traffic and Filtering**:
   a. Select **Use a PAC file to apply your company Web policy**.
   b. Enter the URL of the Proxy Auto-Configuration (PAC) file used by your web security policies.

      For the cloud service, if you want to copy the policy-specific PAC file URL, go to the General tab for that policy.

      - Go to **Web Security** > **Policy Management** > **Policies**.
      - Click on the policy you want, then view its General tab.

      For the hybrid solution, retrieve the PAC file URL from the Hybrid User Identification page under **Settings** > **Hybrid Configuration**.

5. Scroll through the Edit Corporate Profile screen and customize options as needed. For example, indicate whether or not a passcode is required for devices with this profile and what apps the devices can access. Also configure credentials and accounts that the devices can use to access network resources. Click **Help** on the screen for details about each field.
6. Click **Save**.
7. On the Edit Policy screen, click **Personal**.
8. Repeat steps 4 and 5.

When you're done, proceed to *Step 7: Register mobile devices with the system*.

**Note**

If you use a third-party authentication option or Form Login authentication, you must override the authentication settings in the policy, by deploying a PAC file URL that uses the parameter "a=n." Otherwise, your end users will be prompted twice for credentials when they try to browse the Web from their mobile devices.

Example for a policy-specific PAC file:

```
http://webdefence.global.blackspider.com:8082/
proxy.pac?p=22zz73bh&a=n
```

When the "a=n" parameter is applied, NTLM identification or basic authentication is used, depending on the policy settings and the browser or application capability.

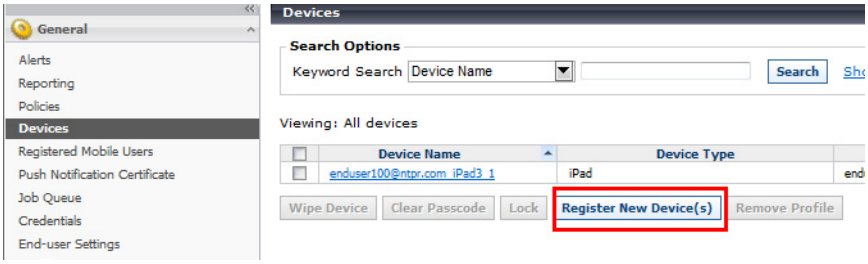
# Step 7: Register mobile devices with the system

Getting Started Guide | Mobile Security Solutions

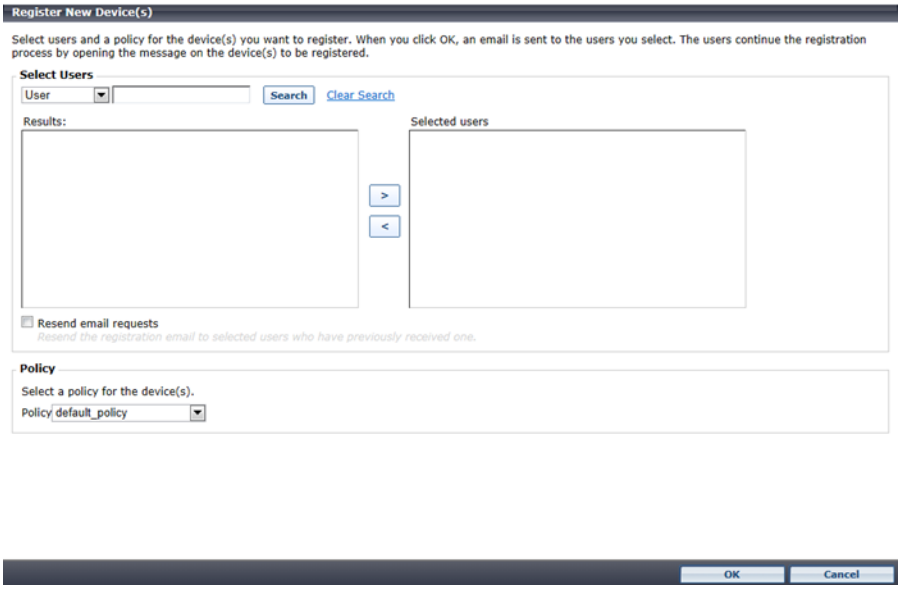
End users must register their devices with the system in order to be protected by it. To assist with this, you can send an email message inviting them to register their mobile devices.

## Inviting users to register their devices

1. Select **General** > **Devices.**
2. Click **Register New Device (s)**.



3. Search for the user or user group of interest. These are pulled from your user directory service.
4. Select the check box next to the users you want to register.
5. Click the right arrow (>) to move the selected end users into the right pane.




6. If you want to resend the email to selected users who have previously been sent a device registration request, select the **Resend email requests** check box.
7. 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 or group). Click **OK** to send a device registration request email message to the selected users.

## Running the registration wizard (end users)

End users receive an email message prompting them to register their device or devices with Mobile Security. The registration request message includes a link to start the registration process.

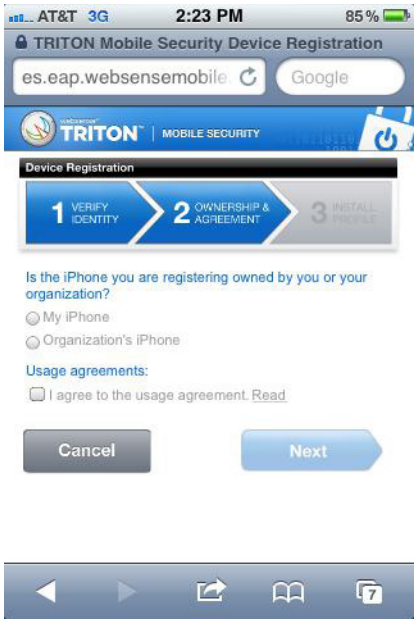
Here is the procedure end users perform:

1. Open the invitation to register on their mobile device. If they don't receive corporate email on their device, they can use Webmail or forward the message to a personal account in order to access it. See knowledgebase article 6125 for best practices handling this issue.

2. Click **Start Registration**.


3. Provide a user name and password when prompted. These are the end user's network or cloud service credentials.

4. Indicate whether the device is owned by the user or their organization. A personal profile is applied to personal devices; and a corporate profile is applied to corporate devices. You can change these settings later if desired.



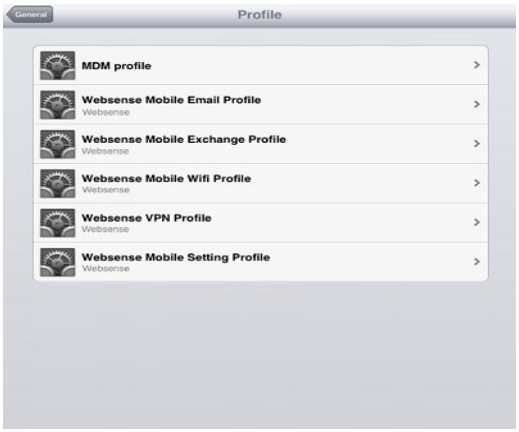

5. Click **Install**.


The following iOS configuration profiles are deployed to the device:

- **Websense Mobile Email Profile** – If enabled, contains information for defining email accounts to install on the device.
- **Websense Mobile Exchange Profile** – If enabled, contains information for defining Microsoft Exchange ActiveSync accounts to install on the device.

- **Websense Mobile Wifi Profile** – If enabled, contains information that allows user devices to automatically connect to your wireless networks.
- **Websense VPN Profile** – If enabled, contains information and certificates required to establish a VPN connection to the cloud service server.
- **Websense Mobile Setting Profile** – Contains mobile device manager policies that secure the mobile device.

All installed profiles are shown in your iOS device under **Settings** > **General** > **Profiles**.




When the devices are registered, they are monitored and protected by the TRITON Mobile Security system!

For information on configuring and using the product after it is running, see the TRITON Mobile Security Help.

To access information on the self-help functions device users can perform, see the Mobile Device User's Guide. We recommend that you provide this document to your device users.