1 TRITON Mobile Security Evaluation Guide

Why TRITON Mobile Security

Evaluation Guide | Mobile Security Solutions

Websense® TRITON® Mobile Security enables the safe and secure use of mobile devices in your organization. It helps protect against data loss and the theft of intellectual property. Mobile Device Management features let you control mobile devices to keep them secure, minimize risk, and maintain compliance. It extends your Web Security policies to mobile devices whether they are used on your network or outside your corporate network on 3G/4G and wireless networks you don't own. And you get real-time contextual security provided by Websense Advanced Classification Engine (ACE), the technology that powers all TRITON security solutions.

Key Features

- Global protection against mobile malware, malicious apps, SMS spoofing, phishing, data theft and web threats.
- Flexible and granular policy controls support both enterprise-issued and personal-owned devices.
- Reporting on web traffic through corporate mobile devices, with logging disabled for personal devices by default.
- Integrated Mobile Device Management (MDM) features such as password enforcement, encryption, jailbreak detection, remote wipe and lock, selective wipe, and more.
- Detailed inventory of devices, operating system versions, and installed apps.
- Support for Apple® iPhone®, iTouch®, iPad®, and iPad mini models running iOS version 5 or higher.

During Your Evaluation

In this guide, you will be introduced to the key features of the TRITON Mobile Security solution. The purpose of this guide is not to provide instructions on how to administrate Mobile Security, but to highlight the value of the Mobile Security solution, and to ensure you get the most out of your evaluation.

For detailed information on how to get started with your evaluation, refer to the TRITON Mobile Security Getting Started Guide.

About Websense

www.websense.com

About Websense, Inc.

Websense, Inc. is a global leader in protecting organizations from advanced cyberattacks and data theft. Websense TRITON APX comprehensive security solutions unify web, email, data and endpoint security at the lowest total cost of ownership. Tens of thousands of enterprises rely on Websense TRITON security intelligence to stop advanced persistent threats, targeted attacks and evolving malware. Websense prevents data breaches, intellectual property theft and enforces security compliance and best practices. A global network of channel partners distributes scalable, unified appliance- and cloud-based Websense TRITON APX solutions.

Mobile Device Protection

Evaluation Guide | Mobile Security Solutions

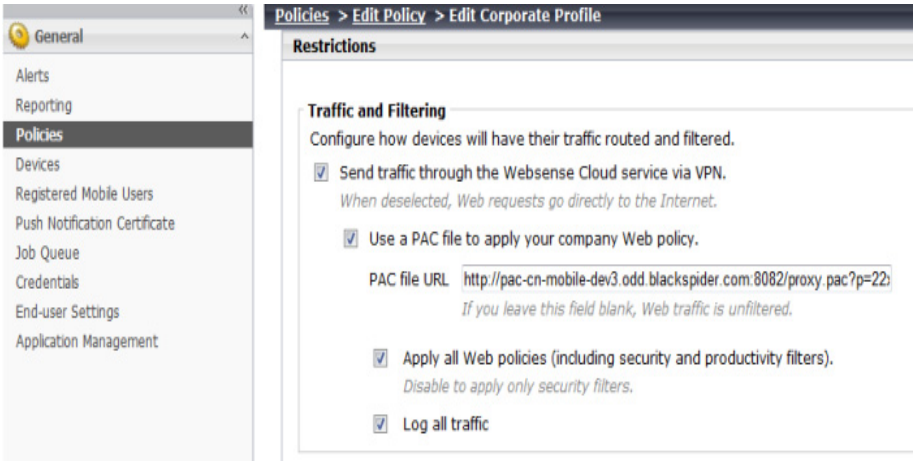
TRITON Mobile Security protects mobile devices in your organization from malware and data loss by providing security filtering and real-time content classification for all traffic through your mobile devices, protecting users from risky activity, detecting jailbroken devices, and allowing immediate action to be taken when a device is compromised by wiping or locking the device, ensuring your proprietary data is safe.

Threat Protection

Unlike other solutions, Mobile Security protects users from threats targeted at mobile devices through all avenues, web, app, email, and SMS.

Security filtering is always in effect when traffic is routed through the Websense cloud service, and always-on VPN ensures that users and corporate data are always protected by Mobile Security. To enable this feature:

1. Navigate to **General > Policies** and select a policy.
2. Select a profile.
3. Under Traffic and Filtering, ensure that Send traffic through the Websense cloud service via VPN is selected. This should be enabled by default.
4. Select **Use a PAC file to apply your company Web policy**.
5. Enter the URL of your PAC file. (Click Help on this page for information on retrieving the URL.)



6. Websense offers industry-leading threat protection. Safely test threats based on the policies you have devised by attempting to access category test pages (http://testdatabasewebsense.com/) using a device with a Mobile Security profile installed.

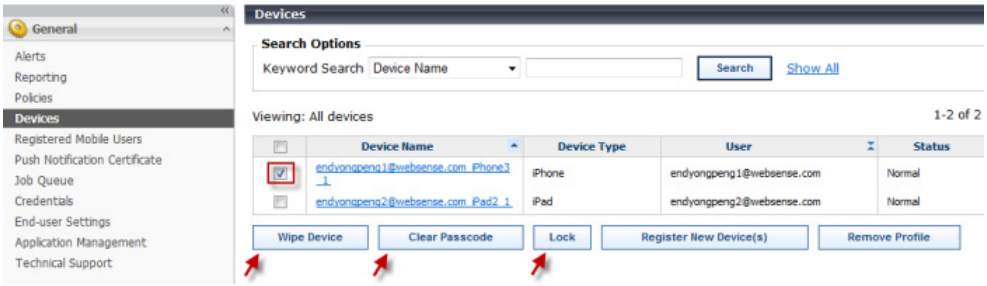
Data Protection

In the event a mobile device becomes infected, lost, or stolen, you can remotely wipe all information from the device. A remote wipe will return the device to factory settings. To wipe a device, select the device and click **Wipe Device** on the **General > Devices** screen.

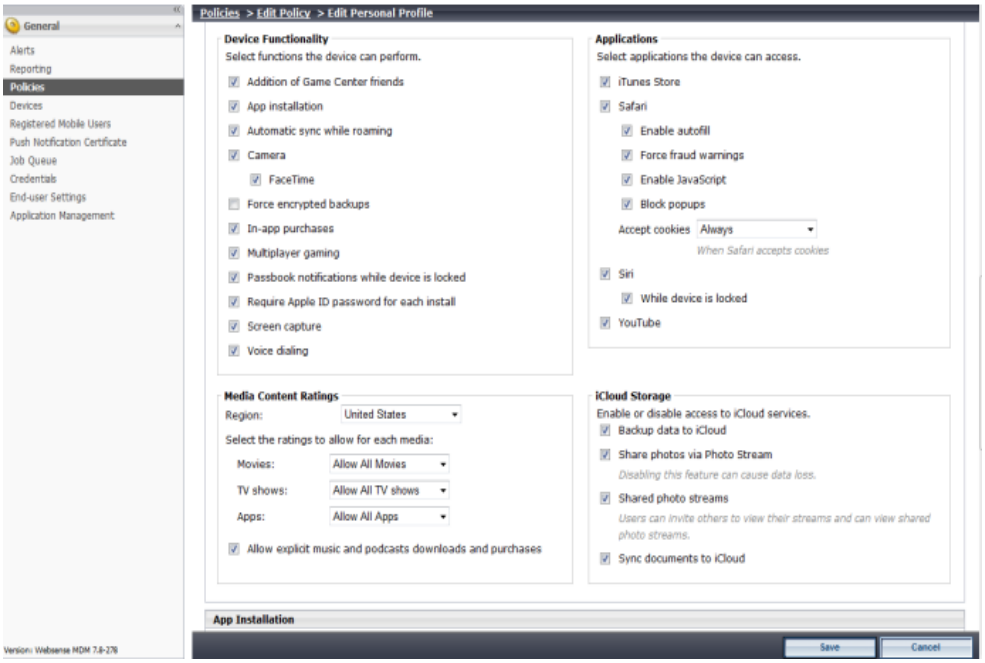
When employees who have brought their own devices leave the company and no longer need to be protected by Mobile Security, their device can be deleted from the system. The relationship between Mobile Security and the device ends as a result. This triggers a **selective wipe**, removing all corporate calendars, contacts, and emails from the device and your organization's security policies are no longer enforced. Select a device on the **General > Devices** screen and click **Remove Profile** to remove a device from the system.

If a lost device can potentially be recovered, you may choose to simply lock the device. This feature triggers the default locking mechanism for iOS devices and can be unlocked using the device passcode. To lock a device, select the device on the **General > Devices** screen and click **Lock**.

In the event users forget their passcode, you can clear the passcode from the device, effectively unlocking the device. The user can then access their device and reset their device passcode. To clear the passcode on a device, select the device on the **General > Devices** screen and click **Clear Passcode**.



TRITON Mobile Security allows you to configure device management capabilities to ensure that you are maintaining compliance regulations, and allowing you to minimize the potential loss of data. These settings can be configured in **General > Policies > Policy Name > Profile Name > iOS**.



Jailbreak Detection

Occasionally users want to remove the limitations imposed on their devices by the iOS operating system. This is known as jailbreaking.

The TRITON Mobile Security system does not allow jailbroken devices to register. In addition, when the system detects that an already registered device is 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 provides a link to a filtered device view.
3. It logs the incident for reporting purposes. You can view reports to see who has jailbroken their device (**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.

Mobile Device Management (MDM)

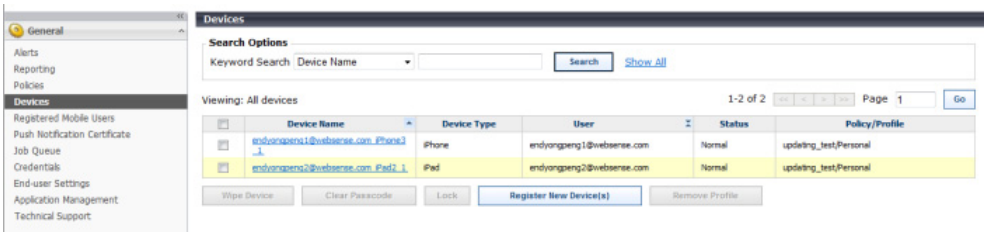
Evaluation Guide | Mobile Security Solutions

With Mobile Security, you can view the device type and operating system of registered devices, customize logging and filtering for corporate and personal devices, allow end users to remotely wipe, lock, or clear the passcode from their mobile devices, and device controls for compliance and data loss/theft prevention.

Managing Devices

Devices must first be registered with Mobile Security before they can be managed. Users register their devices by clicking a link on a notification email message they receive and following a wizard on a registration portal. See the Getting Started Guide for complete instructions.

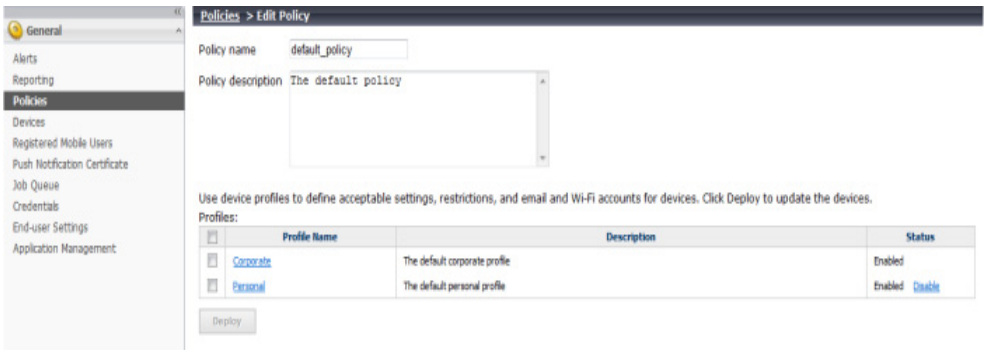
After devices are registered, you can view information about the device by clicking on the **Devices** tab. This page lists all your devices, as well as some basic information about the device, user, and policy currently associated with that device.



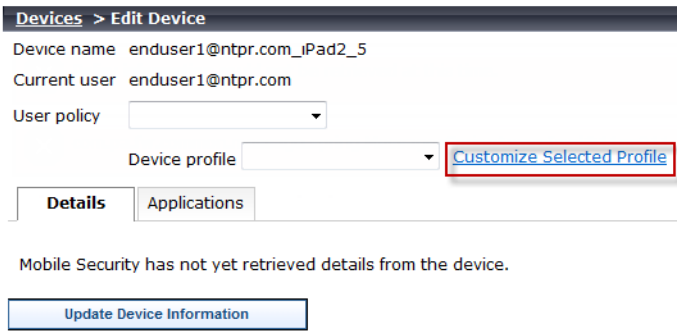
You can view more detailed information by clicking on the device name. This information is updated daily when the device is available, but can also be refreshed by clicking **Update Device Information** on this page.

Customizing Profiles

Mobile Security allows the option to use separate profiles for corporate and personal devices (BYOD). These can be managed by navigating to **Policies > [policy name] > Corporate/Personal Profile**. Profiles are installed on the device at the time of registration.



If you need to be more granular in how you manage policies for different devices, you can customize the profile for individual devices. On the **Devices > Edit Device** page, click **Customize Selected Profile** to open the Customize profile page. Changes you make on the Customize profile page will only affect the selected device and the new customized profile is not available to assign to other devices.



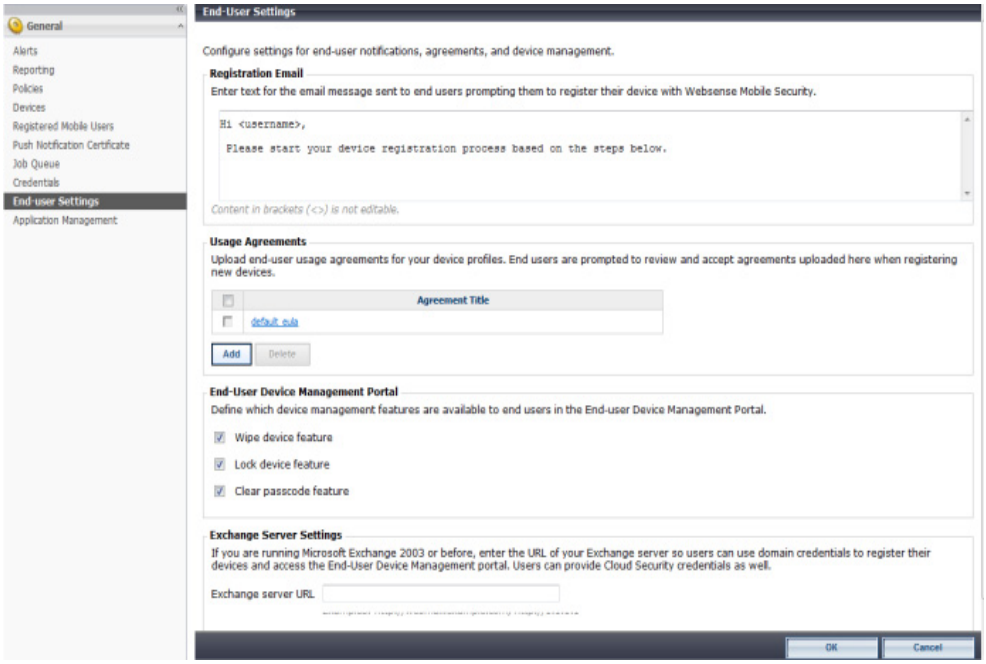
End-User Device Management

End users can be allowed to perform a remote wipe, lock, and clear passcode from the end-user Device Management portal.

These settings are configured on the **General > End-User Settings** page. The features that can be enabled are:

- Lock
- Wipe
- Clear Passcode

Here you can also modify the text for the registration email, as well as upload a custom end-user usage agreement. After adding a custom usage agreement, you must select the agreement on the edit profile page.



The end-user Device Management portal can be accessed by navigating to https://mobile.websense.net/hosted/selfservice.html. Users can log on with either their Cloud Security or network credentials.

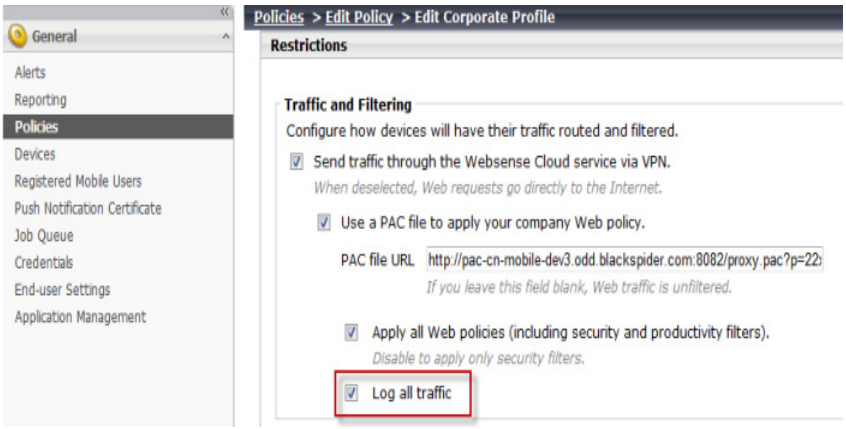
Administration

Evaluation Guide | Mobile Security Solutions

Mobile Security provides extensive logging and reporting, and can track events that may require your immediate attention, alerting you when necessary.

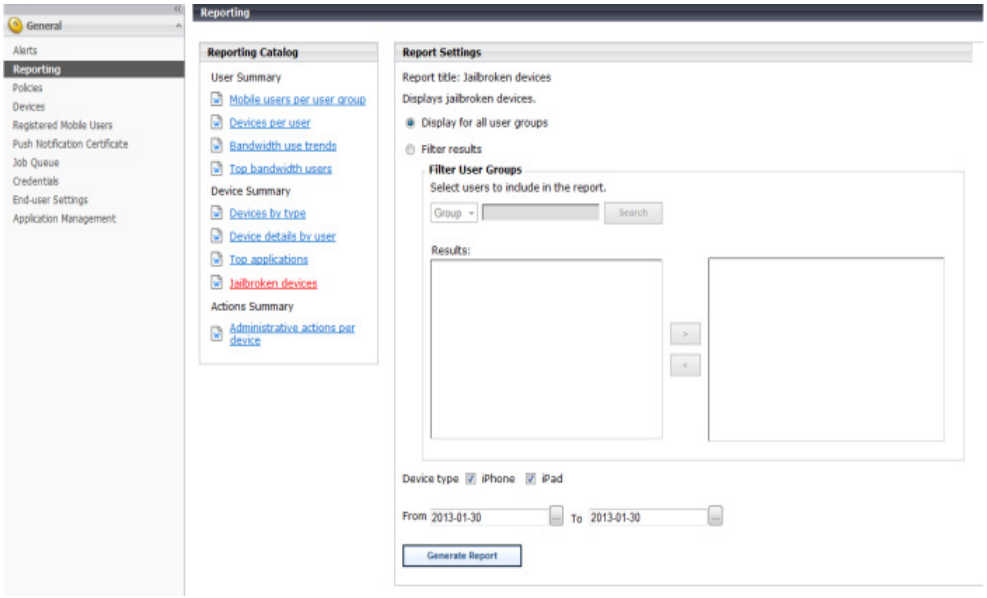
Logging and Reporting

You may have a privacy policy that forbids the logging of traffic from personal owned devices. By default, logging is enabled for devices with the corporate profile, but is disabled for devices with the personal profile. This can be configured by navigating to **General > Policies > [policy name] > Corporate/Personal profile** and selecting or deselecting **Log all traffic**.



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.

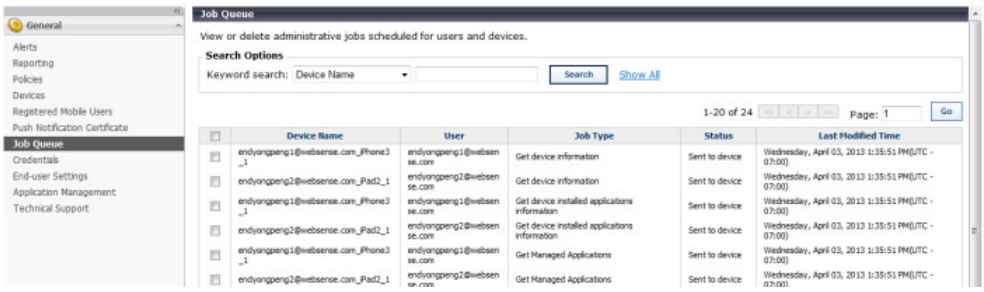
- **User Summary reports**: User reports display information about users with registered mobile devices. With user reports, you can generate summaries of mobile users per user group, top bandwidth users, and bandwidth use trends by user and user group.
- **Device Summary reports**: Use device reports 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.



For more information on generating reports, see the Reporting section of the TRITON Mobile Security Help document.

Job Queue and Alerts

The **General > Job 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.



You are also notified via email of events that may adversely affect your enterprise security. For example, email notifications are sent:

- When high priority jobs are deleted from the job queue, including:
  - Install VPN profile
  - Install Settings profile
  - Remote wipe
  - Remove VPN profile

  - Remove MDM profile
  - Remote lock
  - Clear Passcode

  The notification includes details about the job. You can verify the device status and decide to ignore the tasks or re-initiate them.
- When an Apple Push Notification (APN) certificate is about to expire
- When profile installation fails
- When profile updates fail
- When a jailbroken device is detected

Thanks for evaluating TRITON Mobile Security

Evaluation Guide | Mobile Security Solutions

We hope you've enjoyed evaluating the many features Websense has to offer as a mobile security solution—from blocking users from risky activity, locking and wiping devices, and protecting devices from malware and jailbreaking, we hope you've completed your evaluation confident that TRITON Mobile Security provides you with the tools you need to help protect and manage your mobile devices.