# 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 personalowned 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 (<u>http://testdatabasewebsense.com/</u>) 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**.

General	Devices				
Alerts Reporting	Search	Options d Search Device Name •		Search Show All	
Policies	Viewing:	All devices			1-2 (
Registered Mobile Users		Device Name	Device Type	User	X Status
ush Notification Certificate ob Queue		endvonapena1@websense.com_Phone3 _1	iPhone	endyongpeng1@websense.com	Normal
redentials ind-user Settings polication Management	Wipe	endyongpeng2@websense.com_Pad2_1	Pad Lock F	endyongpeng2@websense.com	Normal move Profile
echnical Support	1	1	1		

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**.

(C) Control (C)	Policies > Edit Policy > Edit Personal Profile	
General     Alarts	Device Functionality	Applications
Reporting	Select functions the device can perform.	Select applications the device can access.
Policies	Addition of Game Center friends	ITunes Store
Devices	App installation	V Safari
Registered Mobile Users	Automatic sync while roaming	Enable autofil
Push Notification Certificate	🖉 Camera	Force fraud warnings
Credentials	V FaceTime	Enable JavaScript
End-user Settings	Force encrypted backups	Block popups
Application Management	In-app purchases	Accept cookies Always
	Wultiplayer gaming	When Safari accepts cookies
	Passbook notifications while device is locked	🖉 Siri
	Require Apple ID password for each install	V While device is locked
	Screen capture	VouTube
	Voice daling	
	Media Content Ratings	iCloud Storage
	Region: United States -	Enable or disable access to iCloud services.
	Select the ratings to allow for each media:	Backup data to iCloud
	Movies: Allow All Movies	Share photos via Photo Stream
	TV shows: Allow All TV shows	Disabling this feature can cause data loss.
		Shared photo streams
	Apps: Allow All Apps •	Users can invite others to view their streams and can view shared photo streams.
	Allow explicit music and podcasts downloads and purchases	Sync documents to iCloud
	App Installation	
Version: Websense MDM 7.8-278		Save Cancel

# **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.

<u>Reporting</u> > Jailbroken Devices					
< Return to Report Catalog					PSF 145
					2013-04-03 13:29:52
	Jailbroke Displays jailbr	n Dev	ices		
	Date Range: 2012-	08-01 - 2013	3-04-03		
Number of Jailbroken Devices: 1					
Device	User Name	Group	Туре	OS	Time Stamp
endzhi1@websense.com_iPad2_1	Mr End Zhi1		iPad2	5.1.1	2013-03-28 23:39:46

# 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 <u>Getting Started Guide</u> 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.

General	Device	15					
Alerts Reporting Policies	Keyw	Search Options Keyword Search Device Name  Show All					
Devices	Viewing	g: All devices			1-2 of 2	e e Page 1 Go	
Registered Mobile Users	(E)	Device Name	<ul> <li>Device Type</li> </ul>	User	I Status	Policy/Profile	
Job Queue	10	endyongpeng1@websense.com Phone3	Phone	endyangpeng1@websense.com	Normal	updating_test/Personal	
Credentials		endvonapeng2@websense.com Pad2_1	Pad	endyangpeng2@websense.com	Normal	updwting_test/Personal	
End-user Settings Application Nanagement Technical Support	Wp	Clear Passcode	Lock	Register New Device(s)	lemove Profile		

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.

General	A POINTED > CONT	oncy				
lerts	Policy name	default_policy				
eporting	Policy description	The default po	olicy	*		
licies						
vices						
stered Mobile Users						
stered Mobile Users 1 Notification Certificate						
istered Mobile Users h Notification Certificate Queue				*		
gistered Mobile Users sh Notfication Certificate I Queue Identials	Use device profile	s to define accepta	able settings, restrictions,	+ and email and Wi-Fi accounts	s for devices. Click Deploy to	o update the devices.
istered Mobile Users h Notification Certificate Queue fentials -user Settings	Use device profile Profiles:	s to define accepta	able settings, restrictions,	+ and email and Wi-Fi accounts Descrip	s for devices. Click Deploy to	o update the devices.
istered Mobile Users h Notification Certificate Queue dentals I-user Settings Silication Management	Use device profiles Profiles:	s to define accepta Profile Name	able settings, restrictions,	+ and email and Wi-Fi accounts Descrip	s for devices. Click Deploy to	o update the devices. Status Drabled

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.

Devices > E Device name	dit Device enduser1@ntpr.com_	IPad2_5	
Current user	enduser1@ntpr.com		
User policy		•	
	Device profile		<u>Customize Selected Profile</u>
Details	Applications		
Mobile Secu	ity has not yet retrievo	ed details from	n the device.

#### **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.

-	C End-User Settings
() General	
Alerts	Configure settings for end-user notifications, agreements, and device management.
Reporting	Registration Email
Policies	Enter text for the email message sent to end users prompting them to register their device with Websense Mobile Security.
Devices	
Registered Mobile Users	H1 <username>,</username>
Push Notification Certificate	Please start your device registration process based on the steps below.
Job Queue	
End-user Settings	
End-user Settings	Content in brackets (<>) is not editable.
rippinanser managements	IIsane Anroements
	Upload end-user usage agreements for your device profiles. End users are prompted to review and accept agreements uploaded here when registering new devices.
	Agreement Title
	E datab
	Add Delete
	End-User Device Management Portal
	Define which device management features are available to end users in the End-user Device Management Portal.
	Wipe device feature
	V LOCK device readure
	Clear passode feature
	Exchange Server Settings
	If you are running Microsoft Exchange 2003 or before, enter the URL of your Exchange server so users can use domain credentials to register their devices and access the End-User Device Management portal. Users can provide Cloud Security credentials as well.
	Exchange server URL
	OK Cancel

The end-user Device Management portal can be accessed by navigating to <u>https://</u><u>mobile.websense.net/hosted/selfservice.html</u>. 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.

ts	Reporting Catalog	Report Settings
porting Ices vices gistared Mobile Users sh Notification Certificate 2 Quaue identals d-user Settings plication Management	User Summary  Mobile users per user group  Dexices per user  Sandwidth use trends  Top bandwidth users Dexices per yoe  Dexice details by user  Dexice details by user  Libbroken dexices Actions Summary  Actions Summary  Actions per dexice	Report title: Jaibroken devices Displays jaibroken devices. © Display for all user groups © Fiker results Filter User Groups Select users to include in the report. Group •

For more information on generating reports, see the <u>Reporting</u> 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.

A former l	S dot	ueue				
General Jerts Jeporting Volcies Jevices Jacistered Mohile Users	View of Sear	or delete administrative jobs sched ch Options vord search: Device Name	uled for users and dev	Search Show Al	1.20 of 24	
ish Notification Certificate	11	Device Name	User	Job Type	Status	Last Modified Time
dentials	10	endyongpeng1@websense.com_Phone3 _1	endyongpang1@websen se.com	Get device information	Sent to device	Wednesday, April 03, 2013 1:35:51 PM(UTC - 07:00)
I-user Settings	10	endyongpeng2@websense.com_Pad2_1	endyongpeng2@websen se.com	Get device information	Sent to device	Wednesday, April 03, 2013 1:35:51 PM(UTC - 07:00)
hnical Support	13	endyongpang1@websense.com_Phone3 _1	endyongpeng1@websen se.com	Get device installed applications information	Sent to device	Wednesday, April 03, 2013 1:35:51 PM(UTC - 07:00)
		endyongpeng2@websense.com_Pad2_1	endyongpeng2@websen se.com	Get device installed applications information	Sent to device	Wednesday, April 03, 2013 1:35:51 PM(UTC - 07:00)
		endyongpeng1@websense.com_Phone3 _1	endyongpang1@websen se.com	Get Managed Applications	Sent to device	Wednesday, April 03, 2013 1:35:51 PM(UTC - 07:00)
		endyongpeng2@websense.com_Pad2_1	endyongpeng2@websen	Get Managed Applications	Sent to device	Wednesday, April 03, 2013 1:35:51 PM(UTC - 02:00)

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.