Release Notes for TRITON® Mobile Security

Topic 40017 / Updated: 11-Jul-2012

Applies To:	TRITON Mobile Security

Use the Release Notes to find information about TRITON® Mobile Security and how to get it set up.

What is TRITON Mobile Security

Topic 40018 / Updated: 13-Jul-2012

Applies To:	Websense TRITON Mobile Security

TRITON Mobile Security is a cloud-based service that brings comprehensive and flexible protection against Web threats and remote device management features to your organization's mobile devices. Mobile Security is managed from the **Mobile Security** tab of the Cloud Security portal.

With TRITON Mobile Security you can:

- Use Cloud Web Security or Web Security Gateway Anywhere policies to regulate Web traffic on mobile devices used outside of your corporate network (over cellular data networks and Wi-Fi).
- Configure security requirements, allowed device and application functions, and Wi-Fi and email settings for registered mobile devices.
- Wipe, lock, and clear passwords for registered mobile devices.
- View reports on trends and statistics for mobile users, devices, and administrative actions.

Supported mobile devices

Topic 40019 / Updated: 2-Jul-2012

Applies To:	TRITON Mobile Security

All Apple iPhone and iPad models running iOS v4.3.5 or later are supported.

Supported Web browsers

Topic 40019 / Updated: 11-Jul-2012

Applies To:	TRITON Mobile Security

The Cloud Security portal supports the following Web browsers:

- Microsoft Internet Explorer v7, 8, and 9. To upload the Apple push notification certificate file, however, you must use one of the other supported browsers.
- Mozilla Firefox v3.x, 4.x, and 5.x
- Safari v4 and 5 (Mac and Windows)

Setting up Mobile Security

Topic 40021 / Updated: 1-Aug-2012

Applies To:	TRITON Mobile Security

Follow these steps to set up TRITON Mobile Security in your organization:

Acquire logon credentials for the Cloud Security portal, if needed

TRITON Mobile Security is administered through the Cloud Security portal, the same portal used for Cloud Web Security and Cloud Email Security. If you don't have logon credentials for this portal—for example, if you are a Web Security Gateway Anywhere customer—you must request credentials through Websense Technical Support. See this knowledgebase article for the details you'll require when making the request.

Generate and upload an Apple Push Notification (APN) certificate

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

In TRITON - Mobile Security, select **General > Push Notification Certificate**, and then click **Create and Upload Certificate**.

Click **Help** for instructions.

Synchronize your user directory information

Cloud Security and Web Security Gateway Anywhere 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 Cloud 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 Security 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 Web Security Gateway Anywhere synchronizes user directory data with the hybrid service on the **Settings > Hybrid Configuration > Shared User Data** page in TRITON - Web Security.

Select specific contexts from the Active Directory global catalogs already configured for on-premises filtering. Only directory entries in the specified contexts are sent to the hybrid service. See "Configure Directory Agent settings for hybrid filtering" in the TRITON - Web Security Help for details.

Define your Web security policies

Web traffic on mobile devices is governed by Web security policies configured in the Web Security tab of the Cloud Security portal, or on the **Policy Management > Policies** page in TRITON - Web Security.

Note

Very restrictive policies are not recommended for use with Mobile Security, as 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: Adult Material, Drugs, Extended Protection, Gambling, Illegal and Questionable, Militancy and Extremist, Racism and Hate, Security, Tasteless, Violence, and Weapons.

Be aware that such an action affects both desktop and mobile-device filtering for the users associated with the policy.

For more information on Web policy configuration in the Cloud Security portal, see "Defining Web Policies" in the TRITON Cloud Security Help.

For more information about policy configuration in TRITON - Web Security, see "Working with policies" in the TRITON - Web Security Help.

Customize mobile user policies and device profiles

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

TRITON Mobile Security includes a predefined policy template that can be customized to meet your needs. To view or edit the policy template settings and profiles, click the policy name on the **General** > **Policies** page.

For best practice, apply only security filters to your profiles. If you apply all Web policies to devices, many apps will be blocked. For example, if your Web Security policy applies productivity filters (such as Shopping), the Amazon and eBay apps won't work on users mobile devices.

By default, only security filters are applied to personal profiles, but all Web policies are applied to corporate profiles. To change the setting:

1. Click a policy name on the **General** > **Policies** page.
2. Click the corporate profile.
3. Scroll to the **Restrictions > Traffic and Filtering** section.
4. Deselect **Apply all Web policies**.

You can also create your own custom policies. To do so, select **General > Policies**, and then click **Add**.

Click **Help** on either of these pages for instructions.

Register mobile devices

To be protected from Web threats and managed by TRITON Mobile Security, mobile devices must first be registered with the system.

Select **General** > **Devices** > **Register New Device** to get started. Here you select users and email them an invitation to register.

Users click a button in the email message and then follow a registration wizard to complete the process.

Note that some users may be unable to receive the message on their mobile device—for example, if they don't have Microsoft Exchange configured on the device.

For these cases, you can customize the email invitation that you send. For example, you can instruct 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. Refer to this knowledgebase article for more information.

Javascript must be enabled on users' i-devices to go through the registration process.

Known issues

Topic 40099 / Updated: 2-Jul-2012

Applies To:	TRITON Mobile Security

A list of resolved and known issues is available in the Technical Library. You must log on to MyAccount to view the list.