Release Notes for Websense® TRITON® Mobile Security Integration with AirWatch MDM, Release 1

Topic 65048 / Updated: 1-July-2014

Applies To:	Cloud Web Security Gateway and TRITON Mobile Security integrated with AirWatch MDM Cloud Security 2014 Release 4

Use the release notes to find information about Websense® TRITON® Mobile Security integration with AirWatch Mobile Device Management (MDM). The release notes include:

What's new in Websense TRITON Mobile Security?

Topic 65049 / Updated: 1-July-2014

Applies To:	Cloud Web Security Gateway and TRITON Mobile Security integrated with AirWatch MDM Cloud Security 2014 Release 4

This release introduces the following:

TRITON Mobile Security integration with AirWatch MDM

You can now integrate TRITON Mobile Security with AirWatch® Mobile Device Management (MDM). When integrated with AirWatch MDM, you can provision iOS and Android mobile devices to send traffic to Websense Cloud Web Security for analysis and policy enforcement. You can also enroll devices in your enterprise

environment quickly, configure and update device settings over the air, create different policies for corporate versus personal devices, and secure mobile devices through actions such as locking and wiping them.

> **Important**
> TRITON Mobile Security integrated with AirWatch MDM is currently available only to a select group of early adopters, until further notice is given by Product Management. For additional information about this feature, contact your support representative.

For the integration process, you need access to the TRITON Cloud Security portal, the AirWatch Admin Console server (version 7.1 or later), the AirWatch Device Services server, and the AirWatch API server. New actions you can perform in the Cloud Security portal related to the integration are described in the following sections:

- *Device Management*
- *Exceptions tab*

For an overview of the integration process, see the Getting Started Guide.

Device Management

If you are a TRITON Mobile Security user, set up your account to integrate with AirWatch MDM by going to **Account Settings** > **Device Management > Mobile Device Management Account Setup**. Enter the following details:

Field	Description
API URL	This is the AirWatch application programming interface URL.
API key	This is the AirWatch application programming interface key.
User name	This is the name you use to log on to your AirWatch account.
Password	This is the password you use to log on to your AirWatch account.

The connection URL that AirWatch needs to integrate with Cloud Web Security is also provided at the bottom of the Mobile Device Management Account Setup page.

Click **Save** when done.

Exceptions tab

Use the Exceptions tab to create exceptions for a specific mobile device profile that block or allow access to certain web categories or web application controls, overriding default settings.

Note

Exceptions configured in the Web Categories and Application Control tabs take precedence over exceptions set for device profiles. For example, if you have the category Job Search set to **Allow** under Web Application Control Exceptions but set to **Block** under Mobile Device Profile Exceptions, the Job Search category will still be allowed.

If you set up an Allow exception for a category, this overrides only the Block action on URL categories. It does not bypass any other actions, including user authentication and antivirus analysis.

On the Exceptions tab, the exceptions to the default analysis action are listed at the bottom of the page. The device profiles you may choose include the following:

Device profile	Description
Corporate (individual)	Owned by an organization or company and used exclusively by one employee.
Corporate (shared)	Owned by an organization or company and used by more than one employee.
Personal	Owned by an employee for that employee's personal use.
Unknown	Ownership status is unknown.

The exceptions table provides the following summary information about each exception:

- The name assigned to the exception.
- The web categories and web application controls that you are blocking or allowing for this exception. Mouse over the links to view the list of categories and application controls if more than one is selected.
- The device profile(s) to which the exception applies, such as Corporate or Personal.
- The action for the exception, such as Block access or Allow access.
- The state of the exception – on or off. You can change the exception's state in this table by clicking the State switch.

To create an exception:

1. On the **Exceptions** tab, under **Mobile Device Profile Exceptions,** click **Add**.
2. The exception **State** is set to ON by default, meaning the exception will be enabled for the device profile(s) you select. If you want to set up an exception but not enable it immediately, click the State switch to set it to OFF.

3. Enter a **Name** for the exception.
4. Select the **Action** to apply, such as Allow access or Block Access.
5. Select the device profile(s) to which the rule applies. Your choices are Corporate (individual), Corporate (shared), Personal, and Unknown.
6. Under **Web Categories > Available web categories**, select the categories you wish to include in your exception. Then, click the right-facing arrow, so that your choices appear under **Selected web categories**.
7. Repeat this process under **Web Application Controls** if there are controls you wish to select.
8. Click **Save**.

Note that while you add one exception at a time, you can delete multiple exceptions at a time from the Exceptions tab landing page.

To edit an exception:

1. On the **Exceptions** tab, click on the exception name**.** This brings you to the **Edit Mobile Device Profile Exception** page for that exception.
2. Make your changes.
3. Click **Save**.

As an example, here are the steps an administrator would take to create an exception named Social Media for an organization that wants its users of non-shared corporate devices to take advantage of news, information-sharing, and networking sites, which are not allowed under its default policy:

1. Click **Add** under Mobile Device Profile Exceptions.
2. On the Add Mobile Device Profile Exception page, leave the State set to **ON**, so that the exception will be enabled for the device profile(s) selected.
3. Enter “Social Media” as the name of thee xception.
4. Select **Allow access** as the action.
5. For the device profile, select **Corporate (individual)**.
6. Under **Web Categories > Available web categories**, select News, and click the right arrow, so that News shows up under **Selected web categories.**
7. Under **Web Application Controls > Available web application controls**, select Facebook Chat, Facebook Comments, and LinkedIn (all), so that these show up under **Selected web application controls.**
8. Click **Save**.

A new exception should display under Mobile Device Profile Exceptions called Social Media with 1 web category and 3 web application controls for devices with a Corporate (individual) profile. The action should be Allow access with the status of ON.

TRITON Mobile Security app

The Websense TRITON Mobile Security app offers valuable tools that enhance your device users' experience with TRITON Mobile Security. For Android device users, the app is required to receive TRITON Mobile Security protection. You add the app in the AirWatch Console, and indicate how you want to deploy it to users' devices.

Important

This app is meant to be used in conjunction with an active corporate license of Websense TRITON Mobile Security. To benefit from all the app's features, device users must have TRITON Mobile Security with AirWatch MDM on their devices.

App Features

- Ensures ongoing protection by checking that TRITON Mobile Security has a VPN connection.
- Offers easy-to-use diagnostic tools and system information about your users' devices that helps your IT department address potential issues.
- Lets device users analyze a website or IP address in real time before they visit it to determine potential threat risk, using Websense CSI: ACE Insight.

Keeps users up to date on the latest online threats with direct access to the Websense Security Labs™ blog—from the leader in global threat intelligence. This feature is only available on the tablet.

Known issues

Topic 65050 / Updated: 22-Aug-2014

Applies To:	Cloud Web Security Gateway and TRITON Mobile Security integrated with AirWatch MDM Cloud Security 2014 Release 4

A list of resolved and known issues is available in the Websense Technical Library. You must log onto MyWebsense to view the list.