Release Notes for TRITON® Mobile Security 2012 Release 9

Topic 42521 / Updated: 3-Dec-2012

Applies To:	TRITON Mobile Security

Use the release notes to find information about TRITON® Mobile Security 2012 Release 9. The release notes include:

- *What's new in TRITON Mobile Security?*
- *Resolved and known issues*

What's new in TRITON Mobile Security?

Topic 42522 / Updated: 3-Dec-2012

Applies To:	TRITON Mobile Security

Release 9 introduces several new features:

- *iOS jailbreak detection, alerting, and reporting*
- *Automatically install free app store apps on devices*
- *Control Siri access*
- *Manage media content ratings*
- *Prevent device iCloud sync*

In addition, it addresses several customer issues and offers stability and performance improvements.

iOS jailbreak detection, alerting, and reporting

Occasionally users want to remove the limitations imposed on their devices by the iOS operating system or circumvent the device management controls and policy enforcement of TRITON Mobile Security. This is known as jailbreaking.

When the TRITON Mobile Security system detects that a 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 give a link to a filtered device view.
3. It logs the incident for reporting purposes. You can view reports to see who has jailbroken (**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.
4. You can also search by Status on devices page to find compromised devices.

Automatically install free app store apps on devices

If desired, you can configure the system to push one or more free Apple Store apps to users' devices when they register them or when profile updates are deployed. For example, you can install Concur or Salesforce on their devices at these times.

To accommodate this feature, there is a new option on General menu: **Application Management**. On this page, you add or delete apps to the system. Then on the Edit Profile page, you can add or delete apps to specific profiles.

Email notifications are sent in the event that apps fail to be pushed.

Please note, this feature works only for devices running iOS 5 and above.

Control Siri access

You can control whether users have access to Siri, a natural language app designed iOS devices.

On the Edit Profile page, there are new Siri options under Applications. You can enable or disable access to Siri for users with the profile.

Manage media content ratings

You can specify the ratings you will allow for various forms of media content that users might try to access. For example, you can allow or disallow access to movies rated R and above.

On the Edit Profile page, there are new Media Content Ratings options. Here you specify ratings for movies, TV shows, apps, music, and podcasts, and you select the rating system to use (by region).

Prevent device iCloud sync

It is common for mobile users to sync their devices with iCloud. iCloud is a popular cloud service that stores music, photos, apps, calendars, documents, and more.

For corporate profiles, this can be security issue, because data is being backed up to storage outside of your control.

On the Edit Profile page, there is a new iCloud Storage section for preventing iCloud sync.

Resolved and known issues

Topic 42523 / Updated: 3-Dec-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.