



Check Point[®]
SOFTWARE TECHNOLOGIES LTD.

26 May 2020

SandBlast Mobile for Microsoft Intune

Integration Guide

[Classification: None]

Check Point Copyright Notice

© 2020 Check Point Software Technologies Ltd.

All rights reserved. This product and related documentation are protected by copyright and distributed under licensing restricting their use, copying, distribution, and decompilation. No part of this product or related documentation may be reproduced in any form or by any means without prior written authorization of Check Point. While every precaution has been taken in the preparation of this book, Check Point assumes no responsibility for errors or omissions. This publication and features described herein are subject to change without notice.

RESTRICTED RIGHTS LEGEND:

Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and FAR 52.227-19.

TRADEMARKS:

Refer to the [Copyright page](#) for a list of our trademarks.

Refer to the [Third Party copyright notices](#) for a list of relevant copyrights and third-party licenses.

Table of Contents

About Check Point SandBlast Mobile	5
General Workflow	5
Introduction to the SandBlast Mobile Integration Guide	6
Solution Architecture	7
Preparing UEM Platform for Integration	9
Prerequisites.....	9
Creating a User Group for SandBlast Mobile.....	10
Creating Security Group for your Devices.....	10
Adding User Licenses to the Security Group.....	11
Adding Users to the Security Group	13
Enrolling Devices to Microsoft Intune.....	15
Creating Administrator Account for Integration with the SandBlast Mobile	15
Configuring the Check Point SandBlast Mobile Dashboard UEM Integration Settings ...	17
Prerequisites.....	17
Configuring UEM Integration Settings.....	17
Configuring UEM to Deploy the SandBlast Mobile Protect app	25
Enabling the MTD Connector in Microsoft Intune Portal	26
Adding the SandBlast Mobile Protect app to your App Catalog	28
Configuring the Application Configuration Settings	37
Connecting the SandBlast Mobile Protect app to your Device.....	43
Creating a Compliance Policy for the Organization Devices	44
Using Android Enterprise with SandBlast Mobile	46
Android Enterprise Deployment Scenarios	46
Configuring SandBlast Mobile Protect app to Protect your Devices.....	46
Policies.....	49

Risk Handling	50
Applying the SandBlast Mobile Protect app on Devices	53
Deploying the SandBlast Mobile Protect app on the iOS Devices	53
Deploying the SandBlast Mobile Protect app on Android Devices	54
Testing High Risk Activity Detection and Policy Enforcement.....	57
Blacklisting a Test App	57
View of a Non-Compliant Device	58
Administrator View on the SandBlast Mobile Dashboard.....	60
Administrator View on the Microsoft Intune Console.....	61

About Check Point SandBlast Mobile

Check Point SandBlast Mobile is the most complete threat defense solution that prevents emerging fifth generation cyber-attacks and allows workers to safely conduct their businesses. This technology prevents threats to the OS, apps, and network. It scores the highest threat catch rate in the industry and does not hit performance or user experience.

SandBlast Mobile delivers threat prevention technology that:

- Performs advanced app analysis to detect known and unknown threats.
- Prevents man-in-the-middle attacks on both cellular and Wi-Fi networks.
- Blocks phishing attacks on all apps: email, messaging, social media.
- Prevents sensitive data distribution from infected devices to botnets.
- Blocks infected devices from accessing corporate applications and data.
- Mitigates threats independently from user action or mobile management platforms.

SandBlast Mobile uses machine learning algorithms and state-of-the-art detection techniques to identify mobile device risks, and triggers proper defense responses that protect business and personal data.

- The SandBlast Mobile solution ("the Solution") includes these components:
- SandBlast Mobile Behavioral Risk Engine ("the Engine").
- SandBlast Mobile Gateway ("the Gateway").
- SandBlast Mobile Management Dashboard ("the Dashboard").
- SandBlast Mobile Protect app ("the App") for iOS and Android.

SandBlast Mobile integrates with UEM systems and provides integral risk assessment of the device which the UEM can use to quarantine, or activate a set of policies until the device is no longer at risk.

This policy enforcement can disable certain capabilities of a device, for example, block access to corporate assets, such as email, internal websites, and more. It provides protection of the corporation's network and data from mobile-based threats.

This guide describes how to integrate the SandBlast Mobile Dashboard with your UEM. It provides a quick tour through the interface of the UEM and the SandBlast Mobile Dashboard to enable integration, alerting, and policy enforcement. This includes activation and protection of a new device, malware detection, and mitigation (including mitigation flow).

General Workflow

1. Prepare your Microsoft Intune UEM platform for the Check Point SandBlast Mobile Protect app integration. See ["Preparing UEM Platform for Integration"](#) on page 9.
2. Configure the Check Point SandBlast Mobile Dashboard for integration with the Microsoft Intune. See ["Configuring the Check Point SandBlast Mobile Dashboard Integration Settings"](#) on page 17.
3. Configure your Microsoft Intune UEM to deploy the Check Point SandBlast Mobile Protect app. See ["Configuring UEM to Deploy the SandBlast Mobile Protect app"](#) on page 25.
4. Apply the Check Point SandBlast Mobile Protect app configuration and policy enforcement to your Microsoft Intune devices. See ["Applying the SandBlast Mobile Protect app Configuration and Policy Enforcement"](#) on page 53.
5. Test the Check Point SandBlast Mobile Protect app on your protected Microsoft Intune devices. See ["Testing High Risk Activity Detection and Policy Enforcement"](#) on page 57.

Introduction to the SandBlast Mobile Integration Guide

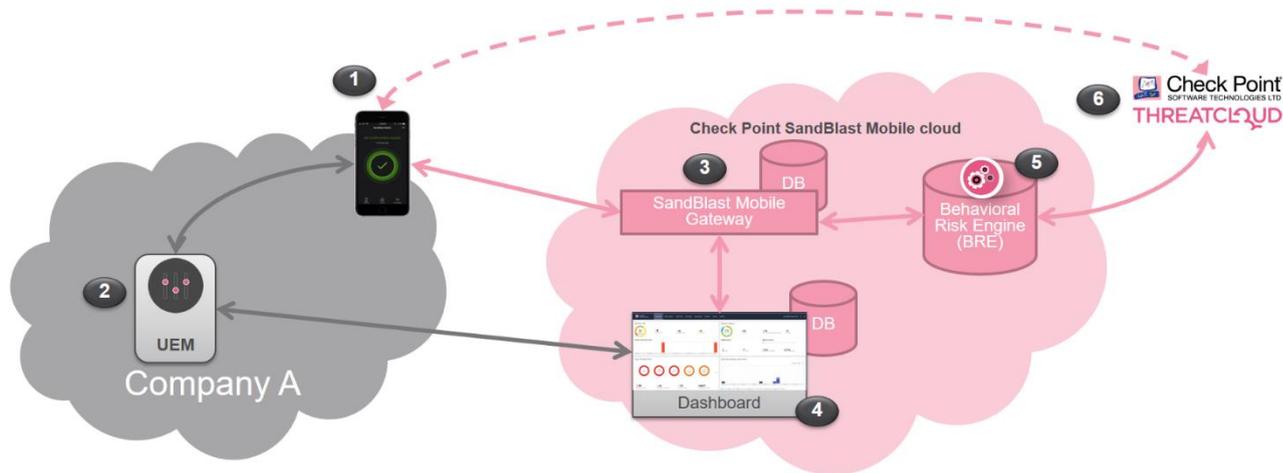
The SandBlast Mobile Protect app is an app for iOS® and Android™ that gathers data and helps analyze threats to mobile devices in an Enterprise environment. It monitors operating systems and information about apps and network connections and provides data to the Solution which it uses to identify suspicious or malicious behavior.

To protect user privacy, the App examines critical risk indicators found in the anonymized data it collects.

The App performs some analysis on the device while resource-intensive analysis is performed in the cloud. This approach minimizes impact on device performance and battery life without changing the end-user experience.

This Guide explains how to integrate the Check Point SandBlast Mobile Protect app with the company's mobile device management systems.

Solution Architecture



Component	Description
1 SandBlast Mobile Protect app	<ul style="list-style-type: none"> The SandBlast Mobile Protect app is a lightweight app for iOS® and Android™ that gathers data and helps analyze threats to devices in an Enterprise environment. It monitors operating systems and information about apps and network connections and provides data to the Solution which it uses to identify suspicious or malicious behavior. To protect user privacy, the App examines critical risk indicators found in the anonymized data it collects. The App performs some analysis on the device while resource-intensive analysis is performed in the cloud. This approach minimizes impact on device performance and battery life without changing the end-user experience.
2 UEM	<ul style="list-style-type: none"> Unified Endpoint Management (generalized term replacing MDM/EMM) Device Management and Policy Enforcement System
3 SandBlast Mobile Gateway	<ul style="list-style-type: none"> The cloud-based Check Point SandBlast Mobile Gateway is a multi-tenant architecture to which mobile devices are registered. The Gateway handles all Solution communications with enrolled mobile devices and with the customer's (organization's) Dashboard instance. No Personal Information is processed by or stored in the Gateway.

	Component	Description
4	SandBlast Mobile Management Dashboard	<ul style="list-style-type: none"> ▪ The cloud-based web-GUI SandBlast Mobile Management Dashboard enables administration, provisioning, and monitoring of devices and policies and is configured as a per-customer instance. ▪ The Dashboard can be integrated with an existing Unified Endpoint Management (UEM) solution for automated policy enforcement on devices at risk. ▪ When using this integration, the UEM serves as a repository with which the Dashboard syncs enrolled devices and identities.
5	Behavioral Risk Engine	<ul style="list-style-type: none"> ▪ The cloud-based SandBlast Mobile Behavioral Risk Engine (BRE) uses data it receives from the App about network, configuration, and operating system integrity data, and information about installed apps to perform in-depth mobile threat analysis. ▪ The Engine uses this data to detect and analyze suspicious activity, and produces a risk score based on the threat type and severity. ▪ The risk score determines if and what automatic mitigation action is needed to keep a device and its data protected. ▪ No Personal Information is processed by or stored in the Engine.
6	ThreatCloud	<ul style="list-style-type: none"> ▪ Check Point’s ThreatCloud is the world largest incidence of compromise database that incorporates real-time threat intelligence from hundreds of thousand Check Point gateways and from millions of endpoints across the globe. ▪ ThreatCloud powers the Anti-Phishing, Safe Browsing, URL Filtering and Anti-bot technologies for SandBlast Mobile on-device Network Protection. ▪ ThreatCloud exchanges threat intelligence with the Behavioral Risk Engine for app analysis.

Preparing UEM Platform for Integration

Microsoft Intune deploys SandBlast Mobile Protect app on a device to upgrade the device enrollment.

Prerequisites

SandBlast Mobile service integrates with Microsoft Intune through Azure Portal.

To enable integration:

1. Configure a Microsoft Intune for MDM Authority. For more information, see the [MDM Authority Configuration Guide](#).
2. Configure Microsoft Intune with an Apple Push Certificate (APNS). For more information, see [Get an Apple MDM push certificate](#).

Microsoft Intune Console view:

The screenshot shows the Microsoft Intune console interface. At the top, there is a search bar and navigation icons. Below the search bar, the breadcrumb path is 'Home > Microsoft Intune | Overview'. The main heading is 'Microsoft Intune | Overview'. On the left, there is a navigation menu with options like 'Overview', 'Quick start', and 'Manage' (which includes 'Device enrollment', 'Device compliance', 'Device configuration', 'Device security', 'Devices', 'Client apps', 'E-books', 'Conditional access', 'Exchange access', 'Users', and 'Groups'). The main content area is divided into two sections: 'Status' and 'Top app installation failures'. The 'Status' section shows 'Device assignment error' with a count of 1 and a warning icon, and 'Device assignment failure' with a count of 0 and a warning icon. The 'Top app installation failures' section contains a table with the following data:

App name	Platform	Device Failures
SandBlast Mobile Protect	iOS/iPadOS	1
Gett - Worldwide Grou...	iOS/iPadOS	0
SandBlast Mobile Protect	Android device adminis...	0
Microsoft Authenticator	Android device adminis...	0
Gmail - Email by Google	iOS/iPadOS	0



Best Practice - For integration with the Check Point SandBlast Mobile, use Security groups to set up the same UEM hierarchy as in your organization's internal hierarchy, or set up groups based on Microsoft Intune features and content.

General Workflow

1. Create Security Group(s) for the SandBlast Mobile users to organize users and devices and connect them to the SandBlast Mobile. See "[Creating a User Group for SandBlast Mobile](#)" on page 10. For more information, see [this guide](#).
2. Assign Microsoft Intune licenses to the SandBlast Mobile users to enroll the devices in Microsoft Intune. For more information see [this guide](#).
3. Add the SandBlast Mobile users to Microsoft Intune and create Administrator accounts. For more information see [this guide](#).
4. Enroll devices to Microsoft Intune. For more information see [this guide](#).
5. Create an Administrator account for integration between the SandBlast Mobile Protect app and Microsoft Intune. See "[Creating Administrator Account for Integration with the SandBlast Mobile \(Optional\)](#)" on page 15.
6. Configure the UEM to deploy the SandBlast Mobile Protect app. See "[Configuring UEM to Deploy the SandBlast Mobile Protect app](#)" on page 25.

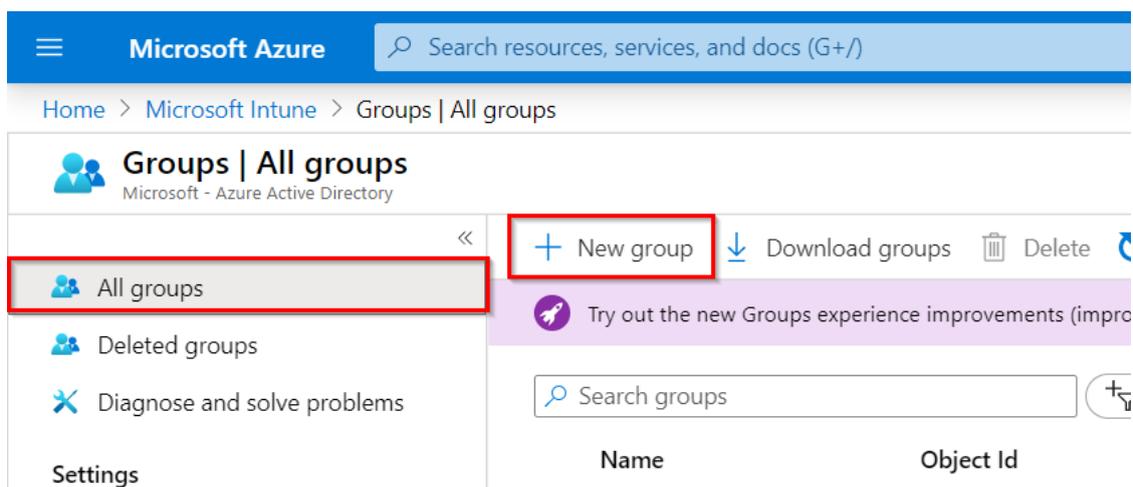
Creating a User Group for SandBlast Mobile

To deploy the SandBlast Mobile policies, configurations, apps, and more in Microsoft Intune, you must create special Security Group(s) for the SandBlast Mobile users and add these users to the SandBlast Mobile.

Creating Security Group for your Devices

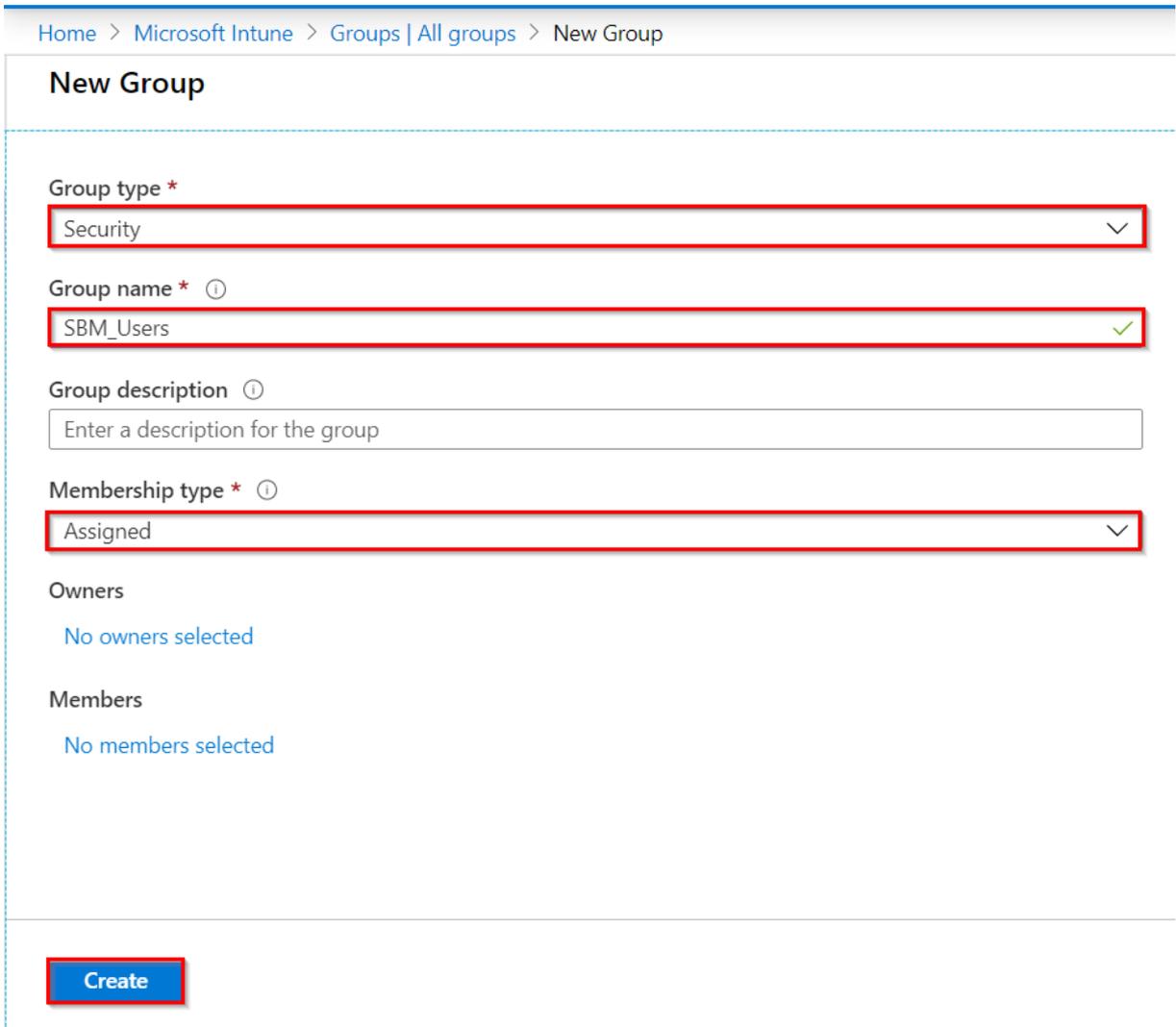
1. On your Microsoft Intune portal, go to **Groups > All groups** and click **+New Group**.

Example:



2. On the **New Group** tab, enter this information:
 - **Group type** - *Security*
 - **Group name** - *SBM_Users*
 - **Membership type** - *Assigned*
3. Click **Create**.

Example:



Home > Microsoft Intune > Groups | All groups > New Group

New Group

Group type *
Security

Group name * ⓘ
SBM_Users

Group description ⓘ
Enter a description for the group

Membership type * ⓘ
Assigned

Owners
No owners selected

Members
No members selected

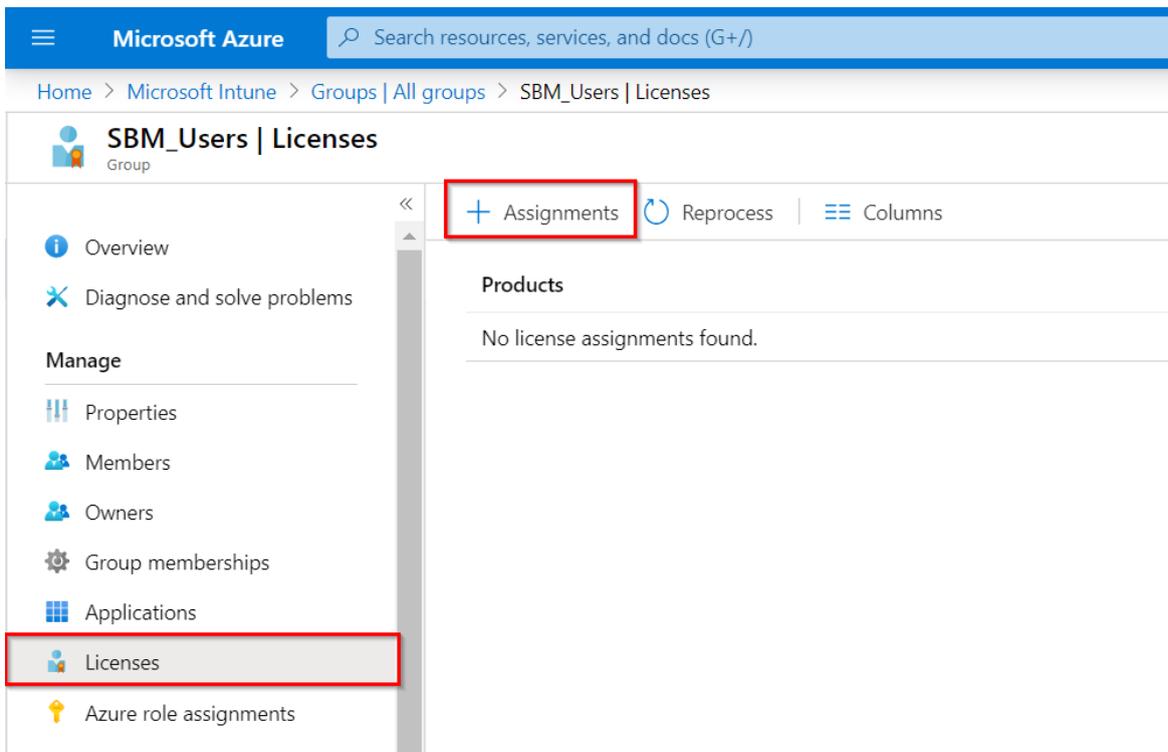
Create

For more information see the [online guide](#).

Adding User Licenses to the Security Group

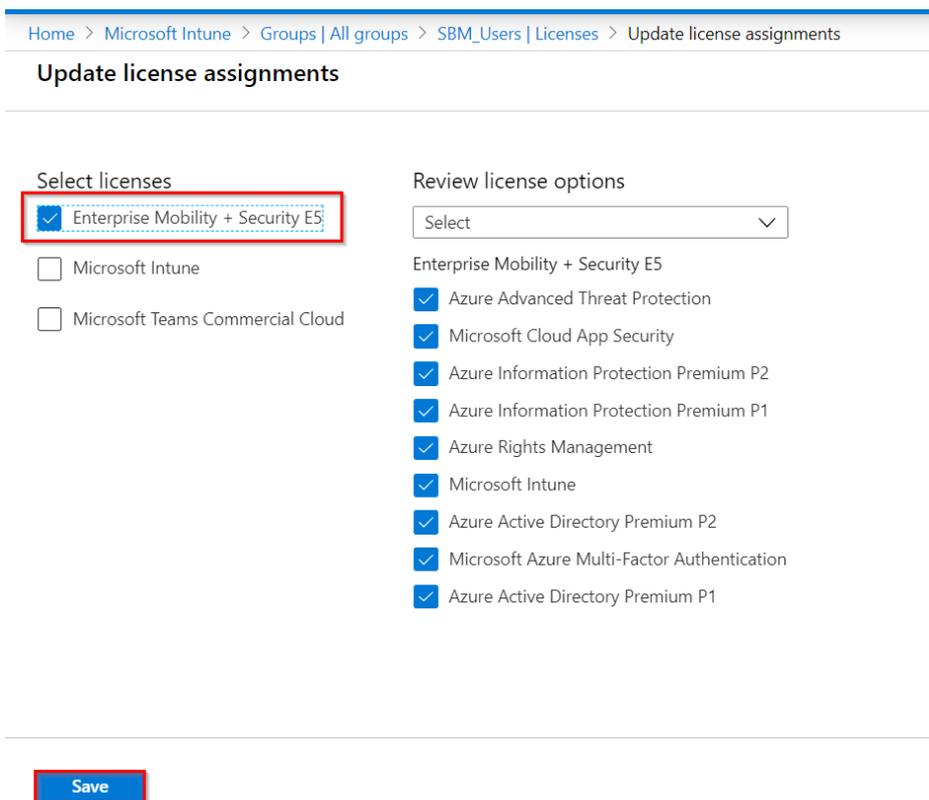
1. On your Microsoft Intune Console, go to the group created above: **Groups > All groups > SBM_Users > Licenses** and click **+Assign**.

Example:



2. On the **Assign Licenses** pane, select **Products** tab and **Enterprise Mobility + Security ES** tab.
3. Review the License options and click **Save**.

Example:



For more information see the [online guide](#).

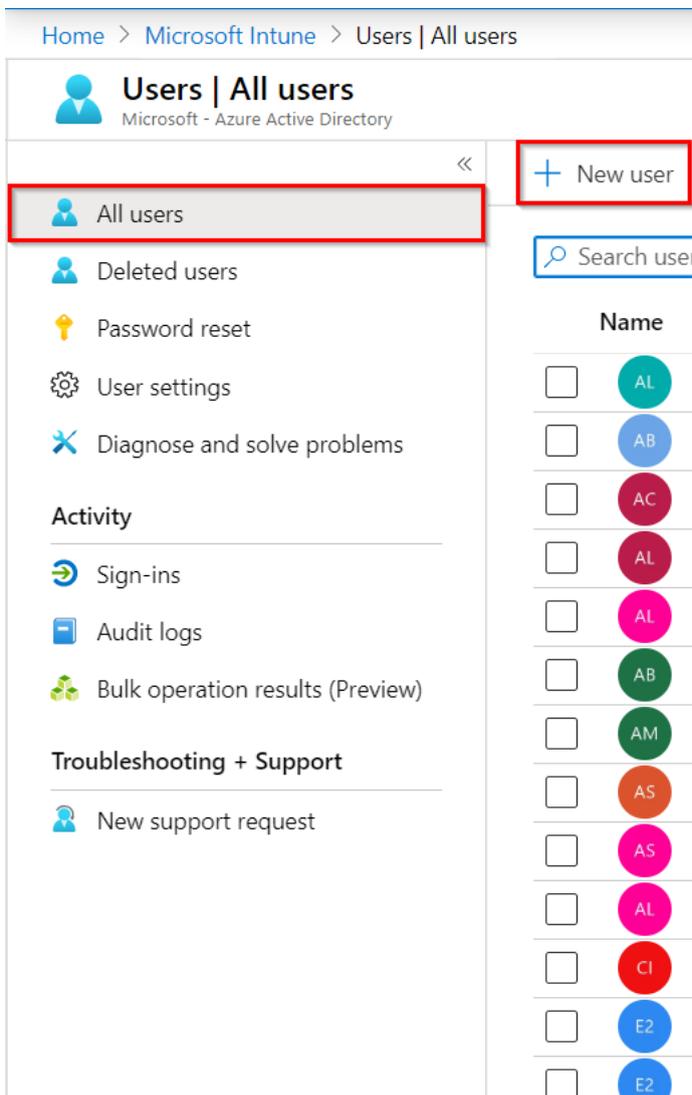
Adding Users to the Security Group



Note - Repeat these steps to add additional users.

1. On your Microsoft Intune Console, go to **All Users** and click **+New User**.

Example:



The screenshot shows the Microsoft Intune console interface for managing users. The breadcrumb path is 'Home > Microsoft Intune > Users | All users'. The page title is 'Users | All users' with the subtitle 'Microsoft - Azure Active Directory'. In the left-hand navigation pane, the 'All users' option is highlighted with a red box. In the top right corner, the '+ New user' button is also highlighted with a red box. Below the navigation pane, there is a search bar labeled 'Search users'. The main content area displays a list of users under the heading 'Name'. Each user entry consists of a checkbox, a colored circular avatar, and a name. The users listed are: AL (teal), AB (blue), AC (red), AL (red), AL (pink), AB (green), AM (green), AS (orange), AS (pink), AL (pink), CI (red), E2 (blue), and E2 (blue).

2. In the **User** window, enter this information:
 - **Name** - free text
 - **User Name** - an email address
 - **First Name** and **Last Name** - (optional)

Example:

Home > Microsoft Intune > Users | All users > New user

New user
Microsoft

Got feedback?

Identity

User name * ⓘ Example: chris @ [Domain dropdown]

Name * ⓘ Example: 'Chris Green'

First name [Text box]

Last name [Text box]

Groups and roles

Groups 0 groups selected

Roles User

The domain name I need isn't shown here

3. Go to the **Groups and roles** tab, and select the **Security** group created before.
4. Click **Select**.
5. Click **Create**.

Example:

Microsoft Azure | Search resources, services, and docs (G+J) | ilanta@checkpointtestc... MICROSOFT

Home > Microsoft Intune > Users | All users > New user

New user
Microsoft

Got feedback?

Initial password [Text box] [Show Password]

Groups and roles

Groups 0 groups selected

Roles User

Settings

Block sign in Yes No

Usage location [Dropdown]

Job info

Job title [Text box]

Department [Text box]

Create

Groups
Select groups in which this user is to be a member

SBM_user [Text box]

SBM_Users

Selected groups
No groups selected

Select

For more information see the [online guide](#).

Enrolling Devices to Microsoft Intune

To manage your devices and apps and their access to your company data you must enroll them in the Microsoft Intune service.

For more information see the [online guide](#).

Creating Administrator Account for Integration with the SandBlast Mobile



Best Practice - For the interaction with SandBlast Mobile create a dedicated Administrator account user in your Microsoft Intune with Global Admin role.

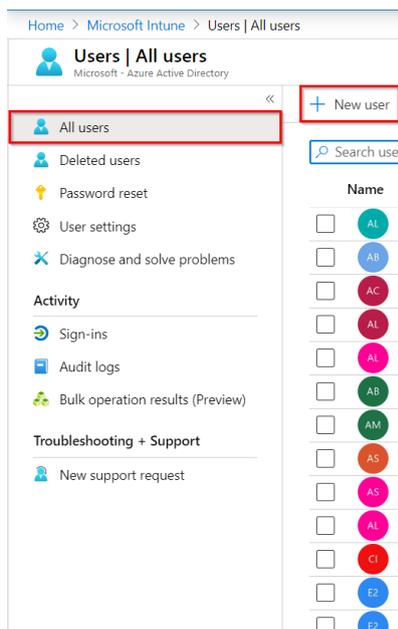
For more information see the [online guide](#).

To create an Administrator Account for the SandBlast Mobile:

Set a new Administrator account.

1. On the Microsoft Intune Console, go to **All Users** and click **+New User**.

Example:



2. In the **User** window, enter this information:
 - **Name** - free text
 - **User Name** - an email address (for example, sbm_admin@checkpointtrial.onmicrosoft.com).
3. Go to **Groups and roles** tab, click **Roles > User**
4. Select **Global administrator** on the right pane.
5. Click **Select**.
6. Click **Create**.

Example:

The screenshot shows the Microsoft Azure portal interface for creating a new user. The page is titled "New user" and includes sections for "Groups and roles" and "Directory roles".

Groups and roles:

- Groups:** 0 groups selected
- Roles:** A dropdown menu is open, showing "User" selected.

Directory roles:

Role	Description
<input type="checkbox"/> Desktop Analytics administrator	Can access and manage Desktop management tool
<input type="checkbox"/> Directory readers	Can read basic directory information. Commonly us
<input type="checkbox"/> Dynamics 365 administrator	Can manage all aspects of the Dynamics 365 produ
<input type="checkbox"/> Exchange administrator	Can manage all aspects of the Exchange product.
<input type="checkbox"/> External Identity Provider administ...	Can configure identity providers for use in direct fe
<input checked="" type="checkbox"/> Global administrator	Can manage all aspects of Azure AD and Microsof
<input type="checkbox"/> Global reader	Can read everything that a global administrator can
<input type="checkbox"/> Groups administrator	Can manage all aspects of groups and group settin
<input type="checkbox"/> Guest inviter	Can invite guest users independent of the 'member
<input type="checkbox"/> Helpdesk administrator	Can reset passwords for non-administrators and He
<input type="checkbox"/> Intune administrator	Can manage all aspects of the Intune product.
<input type="checkbox"/> Kaizala administrator	Can manage settings for Microsoft Kaizala.
<input type="checkbox"/> License administrator	Ability to assign, remove and update license assign
<input type="checkbox"/> Message center privacy reader	Can read Message Center posts, data privacy mess
<input type="checkbox"/> Message center reader	Can read messages and updates for their organizat
<input type="checkbox"/> Office apps administrator	Can manage Office apps cloud services, including p
<input type="checkbox"/> Password administrator	Can reset passwords for non-administrators and Pa
<input type="checkbox"/> Power BI administrator	Can manage all aspects of the Power BI product.
<input type="checkbox"/> Power platform administrator	Can create and manage all aspects of Microsoft Dy

At the bottom of the "New user" form is a "Create" button. At the bottom of the "Directory roles" list is a "Select" button.

Configuring the Check Point SandBlast Mobile Dashboard UEM Integration Settings

The following section includes all necessary configuration steps for SandBlast Mobile Dashboard that will enable the integration with Microsoft Intune UEM.

Prerequisites

You need these details from your Microsoft Intune Deployment:

- **Server:** The URL of your Microsoft Intune System. Usually - the same as the Microsoft Intune Console.
- **User name and Password:** credentials that the SandBlast Mobile Dashboard uses to connect to the Microsoft Intune UEM. See "[Creating Administrator Account for Integration with the SandBlast Mobile](#)" on page 15.
- **Security Group(s):** The Microsoft Intune Azure AD mobile device / user groups to which the devices are registered and then integrated with the SandBlast Mobile Dashboard. You can integrate several groups in the same SandBlast Mobile Dashboard instance. Separate each group name separated with a semicolon (;). See. "[Creating a User Group for SandBlast Mobile](#)" on page 10



Notes:

Before you start configuring the integration in SandBlast Mobile dashboard, delete any existing devices.

Configuring UEM Integration Settings

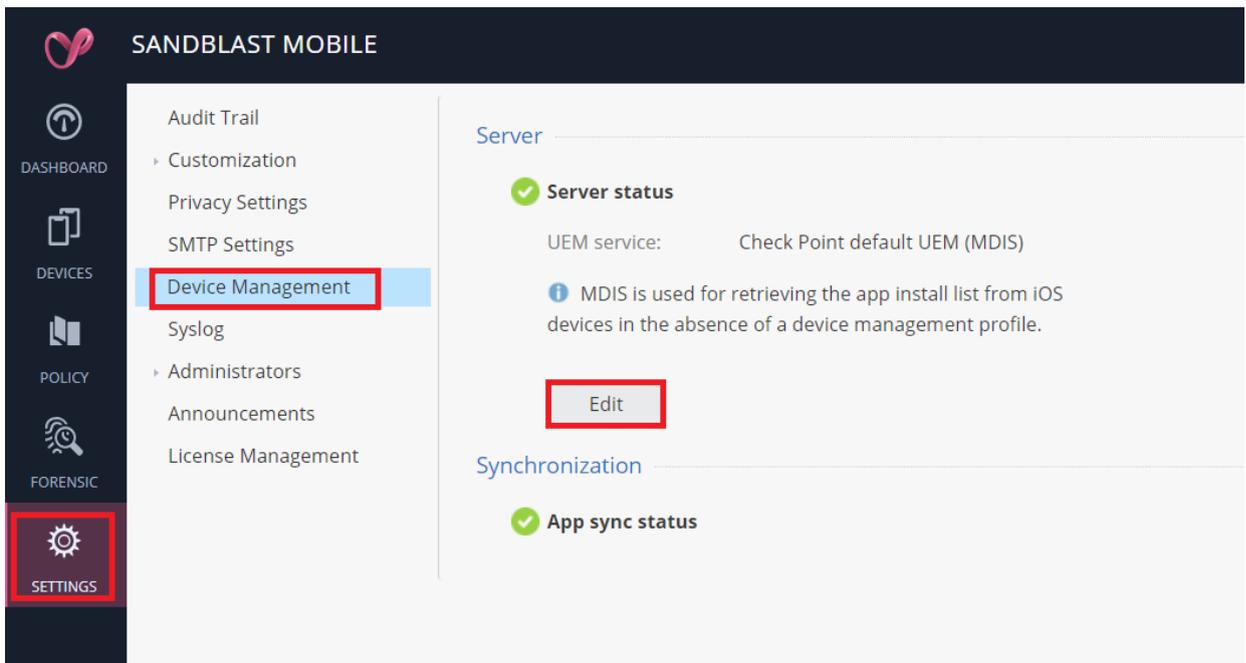
After you complete the necessary steps, the **Device Management** pane on the Infinity portal shows the detailed status of the settings.

Procedure:

1. On the SandBlast Mobile Dashboard, go to **Settings > Device Management**. Click **Edit** on the Server section.

The Integration Wizard opens.

Example:



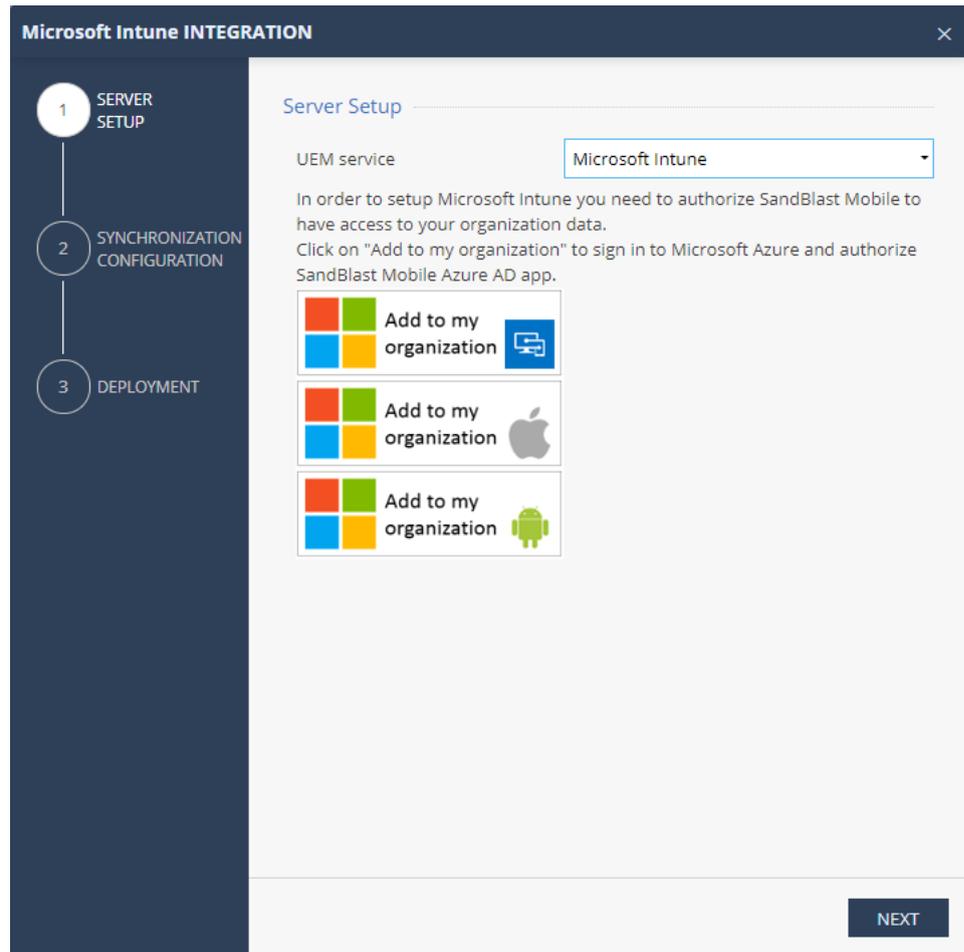
2. Configure the settings for your Microsoft Intune Deployment.

For information about the settings see "[Preparing UEM Platform for Integration](#)" on page 9.

- **Server Setup**

Configure your UEM to integrate with the created Microsoft Intune devices:

- a. In **Server Setup** section, select:
 - **UEM service** - Microsoft Intune.



- b. Click “Add to my organization” Microsoft Intune, login with the Admin credentials you created for the SBM integration, and accept to add SandBlast Mobile to your organization.
- c. Click “Add to my organization” iOS devices, login with the Admin credentials you created for the SBM integration, and accept to add SandBlast Mobile to your organization.

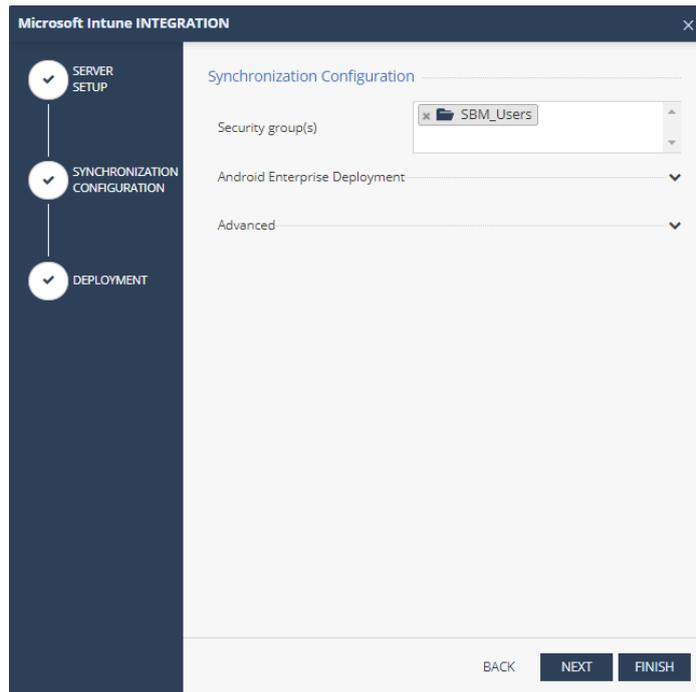
Click “Add to my organization” Android devices, login with the Admin credentials you created for the SBM integration, and accept to add SandBlast Mobile to your organization.
- d. Click **Next**.

▪ **Synchronization Configuration**

Configure the devices and security groups in Intune that you want to synchronize with SandBlast Mobile Dashboard. The dropdown list will automatically populate.

- a. In the **Group(s)** field:
 - i. Click Security **Group(s)**.

A dropdown with list of the available groups opens.
 - ii. Select the group(s) you need for integration with Microsoft Intune.

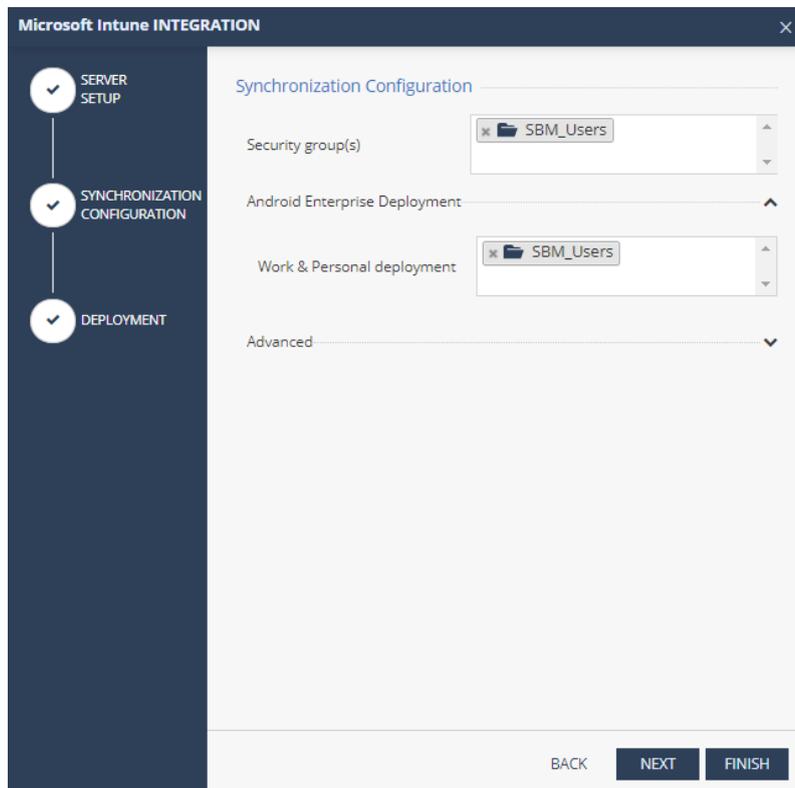


b. In the **Android Enterprise Deployment** field:

If you use Android Enterprise and have two different profiles in your devices, select the groups for two deployed applications as part of the Microsoft Intune Android Enterprise deployment. See "[Using Android Enterprise with SandBlast Mobile](#)" on page 46.

Note that this step is relevant if your devices are fully managed on Intune with two profiles work and personal.

Example:



- c. In the **Advanced** section:
 - i. Import Personally Identifiable Information (PII) and set the synchronization intervals.

You can limit the import of the PII devices (users) to SandBlast Mobile.



Note - If all entries are OFF, the placeholder information set for the email address is placed in the Device Owner’s Email, in form of "UEMDevice UDID@vendor.mdm".

Example:

Setting	Description	Value
Device sync interval	Interval to connect with UEM to sync devices.	10-1440 minutes, in 10 minute intervals.
Device deletion threshold	Percentage of devices allowed for deletion after UEM device sync (in %).	0-100% ; use 100% for no threshold.
Deletion delay interval	Delay device deletion after sync – device is not deleted if it is re-synchronized from UEM during the threshold interval.	0-48 hours.

App sync interval	Interval to connect with UEM to sync applications.	10-1440 minutes, in 10 minute intervals.
-------------------	--	--

d. Click **Next**.

▪ **Deployment configuration**

Check the “Allow auto device addition prior to device sync” option in case you require a faster device enrollment. Without this option checked, the device will not be able to connect to the SandBlast Mobile Dashboard not until a complete sync step has created the device in the dashboard. This option generates a unique dashboard token to be used in the UEM configuration that will tell the device which dashboard it needs to register to.



Note - use the “copy to clipboard” button to set the Token value in the Application configuration step in the UEM. Section [Configuring the Application Configuration settings](#) Page 37

Example:



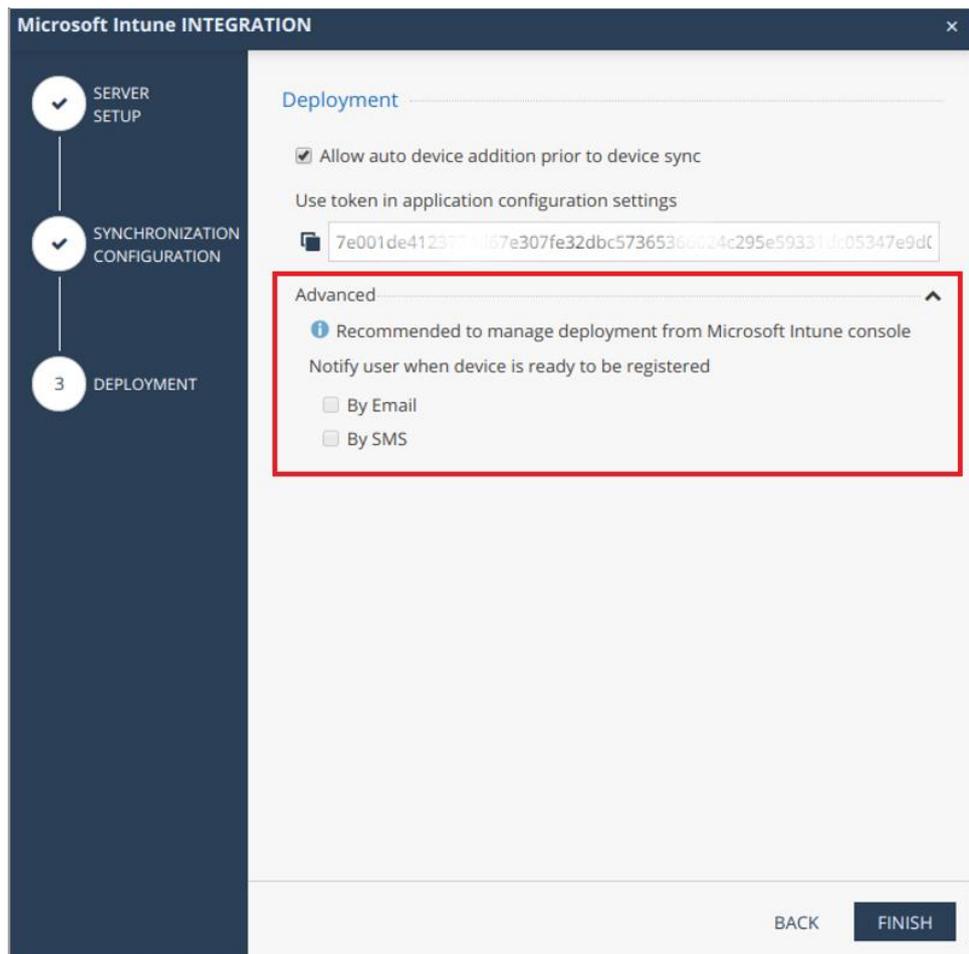
Note – The token is the hashed unique identifier of your dashboard.
We will use it in a later step, when we will configure application configurations on Intune.

If you use SandBlast Mobile to manage the deployment instead of the UEM:

In the **Advanced** section:

- a. Enable options to have SandBlast Mobile Dashboard send email and/or SMS notification to the new users with instructions to download and install the SandBlast Mobile Protect app. Usually when the UEM is configured it will notify the end user itself to install the app so this option is disabled by default.
- b. Click **Finish**.

Example:



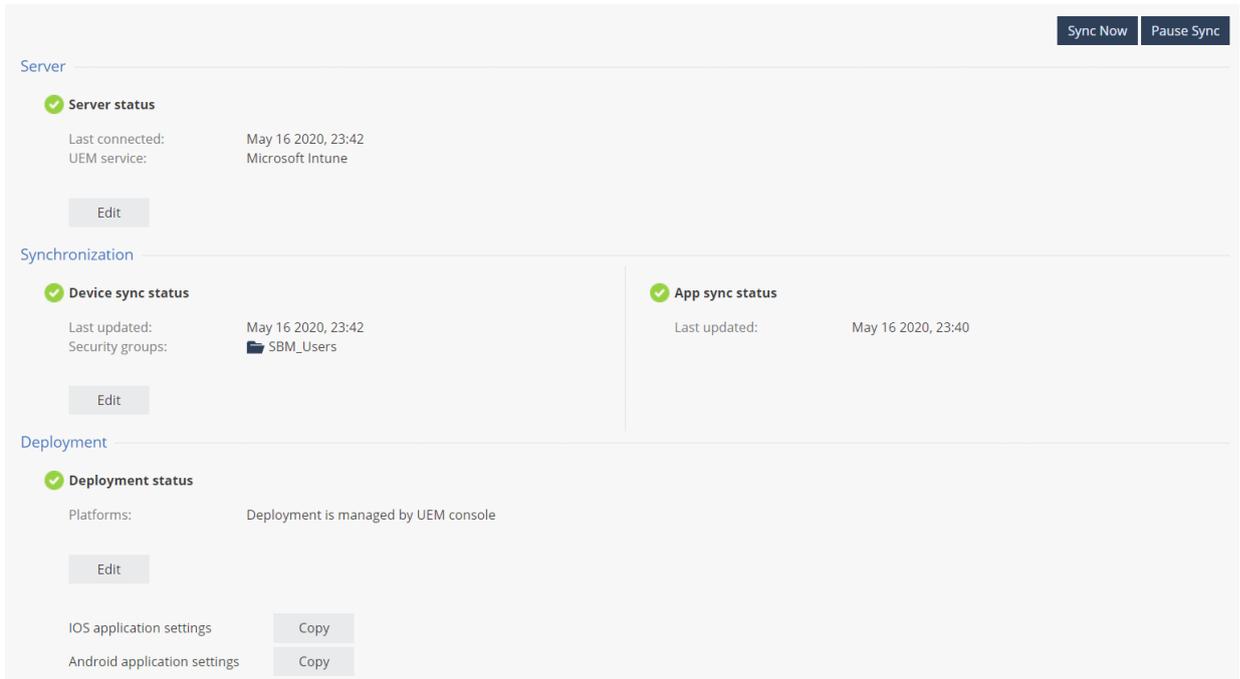
3. View the Integration Status.

In **Settings > Device Management** menu.

The Device Management pane shows this information:

- **Server** – The latest server configuration status.
 - **Synchronization** – The synchronized groups and the sync status time stamp.
 - **Deployment** – Deployment Configuration and Deployment Status.
4. Click Pause Sync / Resume Sync to temporarily stop/resume the device sync process
 5. Click Sync Now to force an immediate device sync call and not wait to the next auto sync cycle

Example:



The screenshot displays the configuration page for the Check Point SandBlast Mobile MDM integration. At the top right, there are two buttons: "Sync Now" and "Pause Sync". The page is divided into three main sections:

- Server:** Shows "Server status" with a green checkmark. It lists "Last connected: May 16 2020, 23:42" and "UEM service: Microsoft Intune". An "Edit" button is located below this section.
- Synchronization:** Contains two sub-sections:
 - Device sync status:** Shows "Last updated: May 16 2020, 23:42" and "Security groups: SBM_Users". An "Edit" button is below it.
 - App sync status:** Shows "Last updated: May 16 2020, 23:40".
- Deployment:** Shows "Deployment status" with a green checkmark. It lists "Platforms: Deployment is managed by UEM console". Below this, there are "Copy" buttons for "IOS application settings" and "Android application settings".

6. Click Edit in each section to edit the settings.

Configuring UEM to Deploy the SandBlast Mobile Protect app

If SandBlast Mobile Protect app is not installed or removed from device, then the device is marked as not protected.

You must add your devices the SandBlast Mobile Protect group and associate the SandBlast Mobile Protect app to the created Policy.

To prompt the SandBlast Mobile Protect app installation on your devices:

1. Create a Protect app Application Group for both iOS and Android apps.
2. Assign this group to your organization.
3. Create a compliance policy that uninstalls and, or removes all corporate apps from the device until the user installs the SandBlast Mobile Protect app on the device.



Notes:

- If you configured Microsoft Intune for **Whitelisting Apps**, you must add the SandBlast Mobile Protect app to the white list.
- You can only synchronize devices from the UEM to the SandBlast Mobile Dashboard. You cannot synchronize users.
- You must add the SandBlast Mobile Protect app for the iOS and for the Android operating systems.

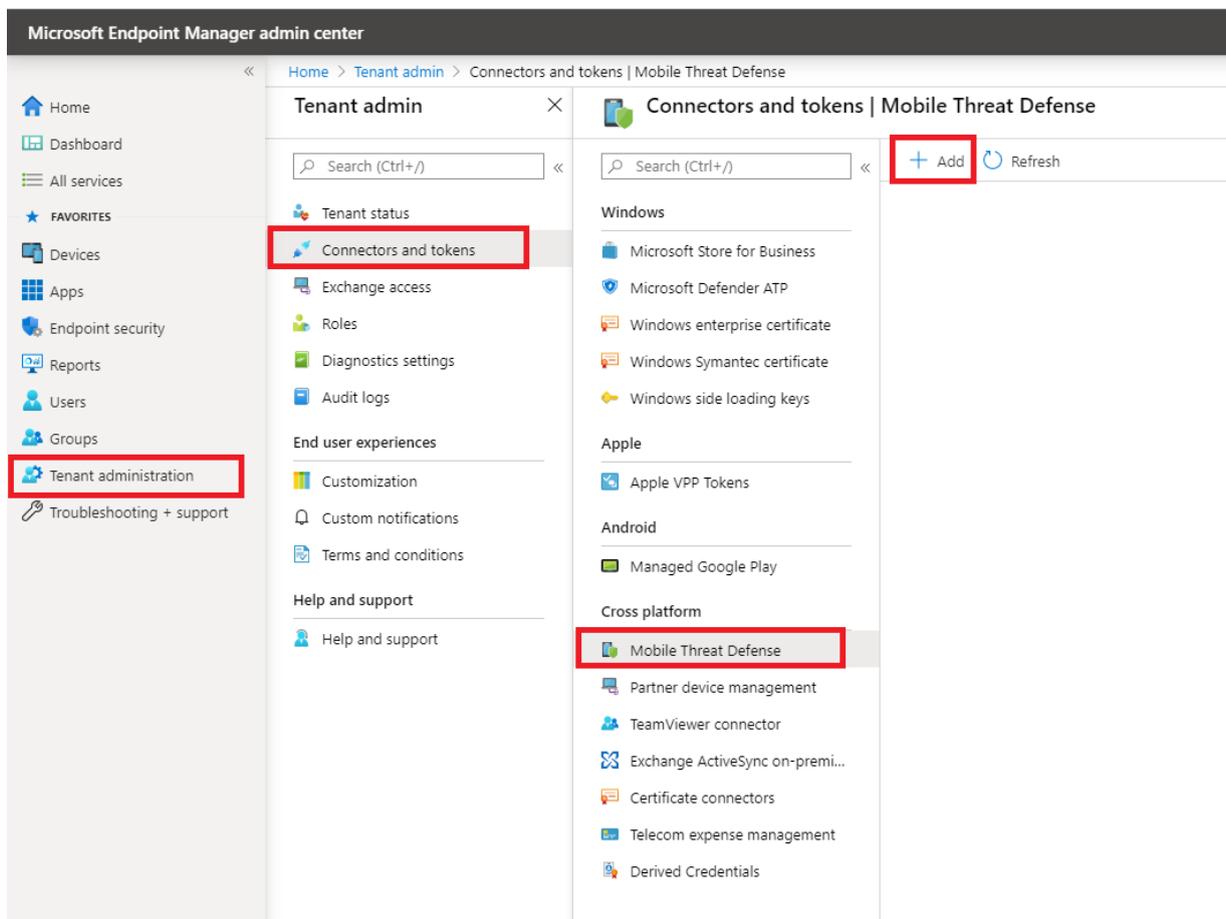
General Workflow:

1. Add the SandBlast Mobile Protect app to your App Catalog. See "[Adding the SandBlast Mobile Protect app to your App Catalog](#)" on page 28.
2. Connect the app to your devices. See "[Connecting the SandBlast Mobile Protect app to your Device](#)" on page 43.

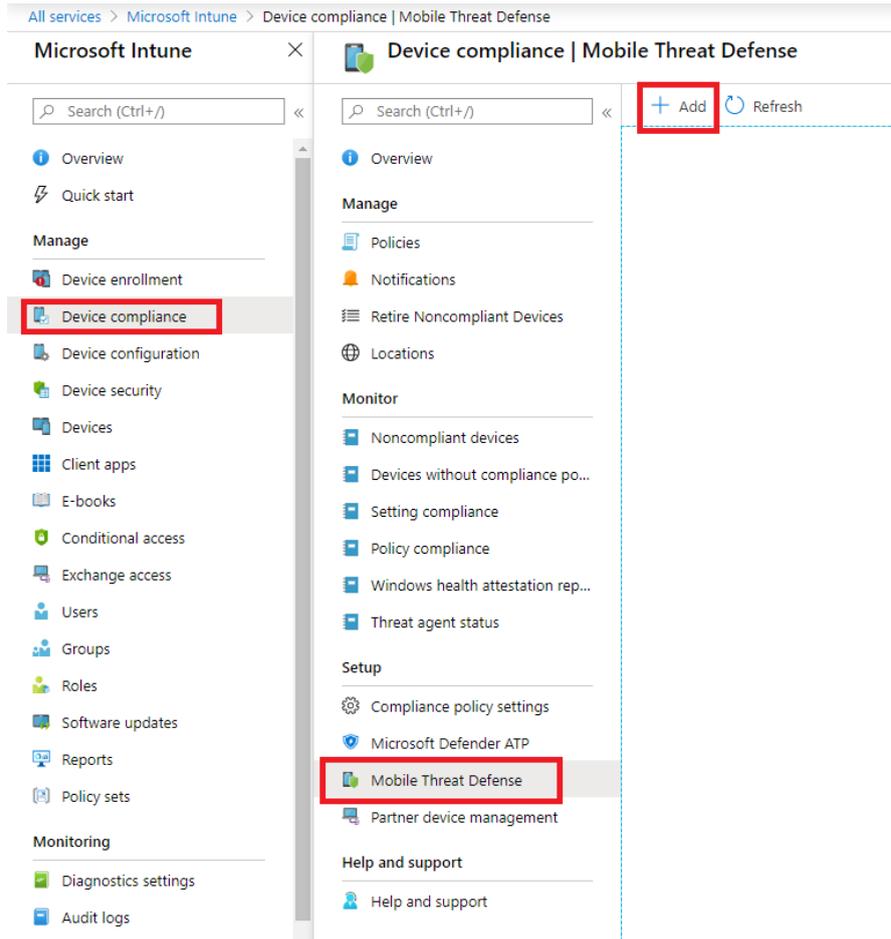
Enabling the MTD Connector in Microsoft Intune Portal

In this step we will define the Check Point Mobile Threat Defense connector in Microsoft Intune. For more information see [MTD connector guide](#)

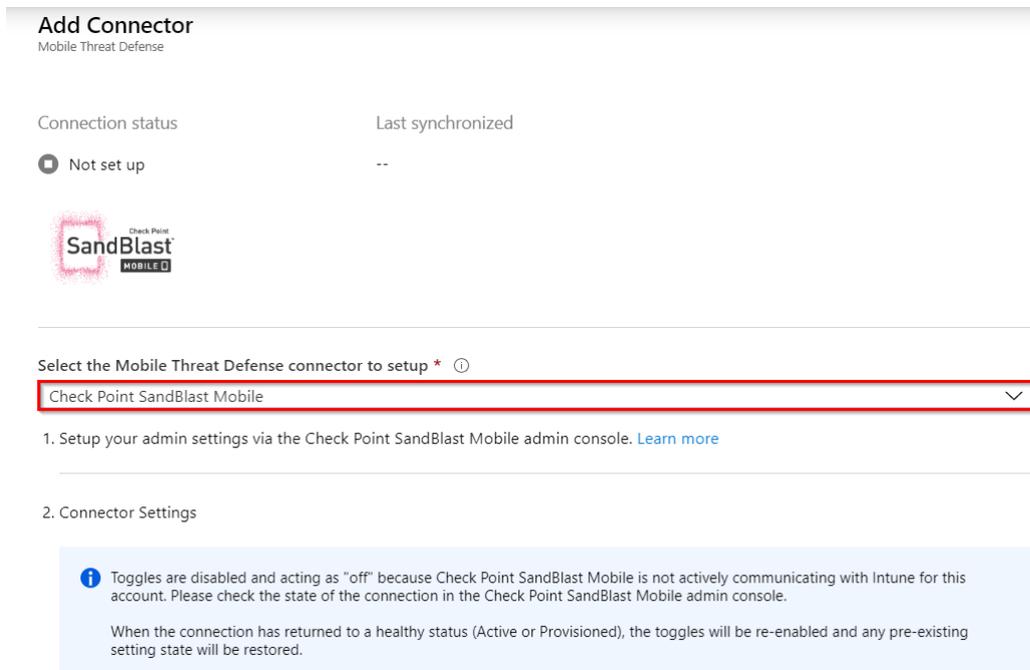
1. If you are using the Microsoft Endpoint Manager Admin center select **Tenant administration > Connectors and tokens > Mobile Threat Defense**.



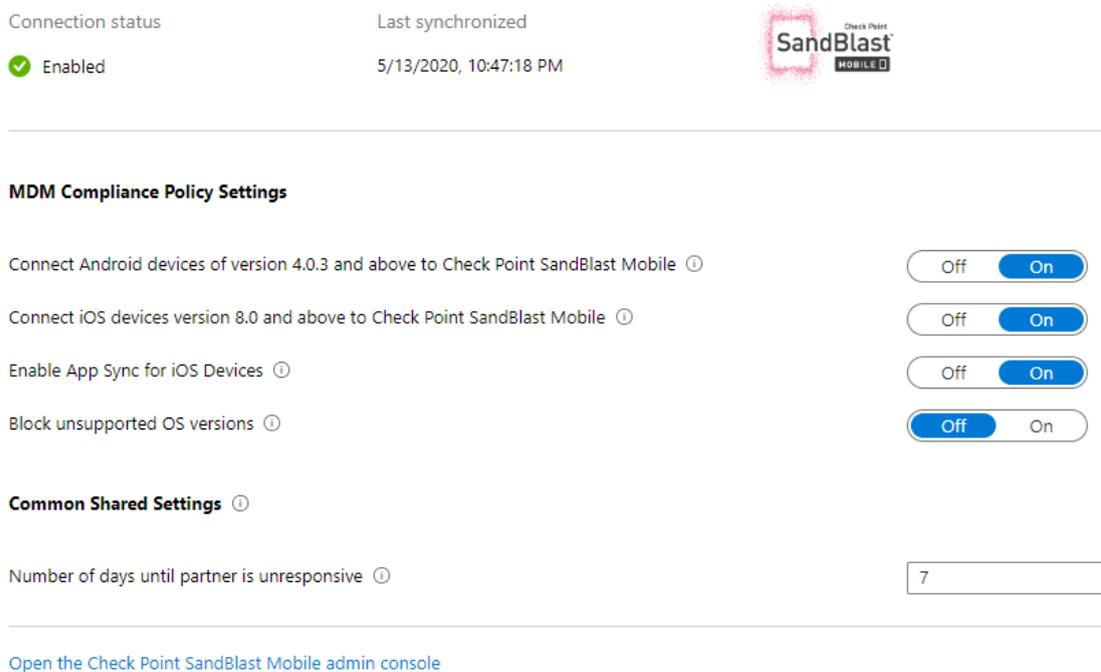
2. Alternatively if you are using the Microsoft Intune Portal, select **Device Compliance > Mobile Threat Defense**.



3. On the **Mobile Threat Defense** pane, choose **Add**.
4. In the drill down menu, select the connector Check Point SandBlast Mobile



5. Make sure it is configured to connect Android devices, iOS Devices and enable app sync for iOS (first three options are ON) like in the following screenshot:



Connection status: Enabled (Green checkmark icon)

Last synchronized: 5/13/2020, 10:47:18 PM

MDM Compliance Policy Settings

- Connect Android devices of version 4.0.3 and above to Check Point SandBlast Mobile (On)
- Connect iOS devices version 8.0 and above to Check Point SandBlast Mobile (On)
- Enable App Sync for iOS Devices (On)
- Block unsupported OS versions (Off)

Common Shared Settings

- Number of days until partner is unresponsive:

[Open the Check Point SandBlast Mobile admin console](#)

6. Click on Save.

Adding the SandBlast Mobile Protect app to your App Catalog

To protect your devices, deploy the SandBlast Mobile Protect app from the public stores to the devices that are protected by Check Point SandBlast Mobile.

You must add the Protect app for both iOS and Android operating systems.

For more information about adding apps to the Microsoft Intune App Catalog, see the [online guide](#).

Notes:



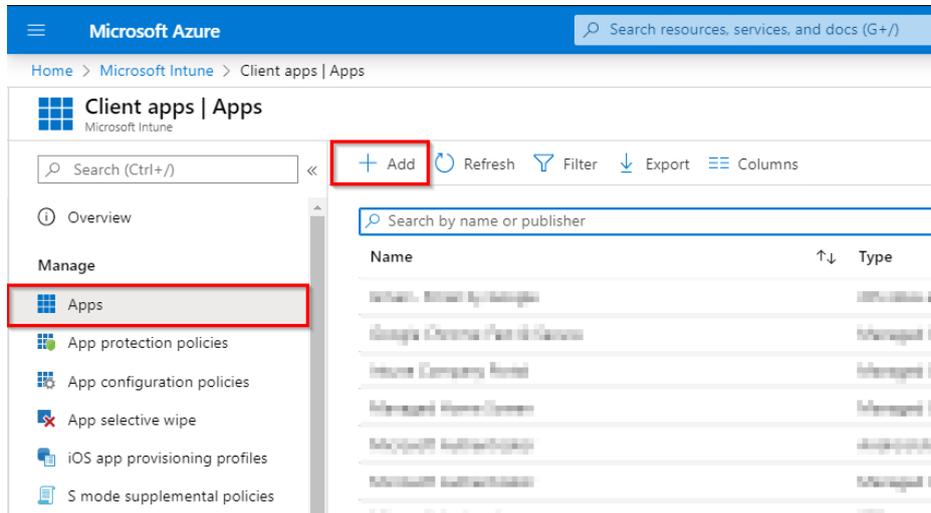
- As you add the SandBlast Mobile Protect app to your catalog, rename this **New Mobile Device App** to **SandBlast Mobile Protect app**.
- For Android, approve the **SandBlast Mobile Protect app** in the managed Google Play account.

To import the SandBlast Mobile Protect app:

1. On the Microsoft Intune portal, go to **Client apps > Apps** and click **+ Add**.
2. Click **+Add Application**.

An **Add App** window opens.

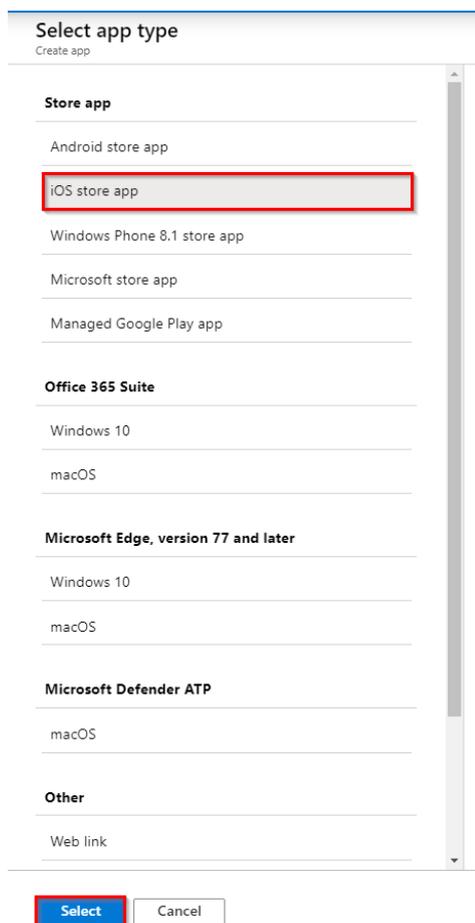
Example:



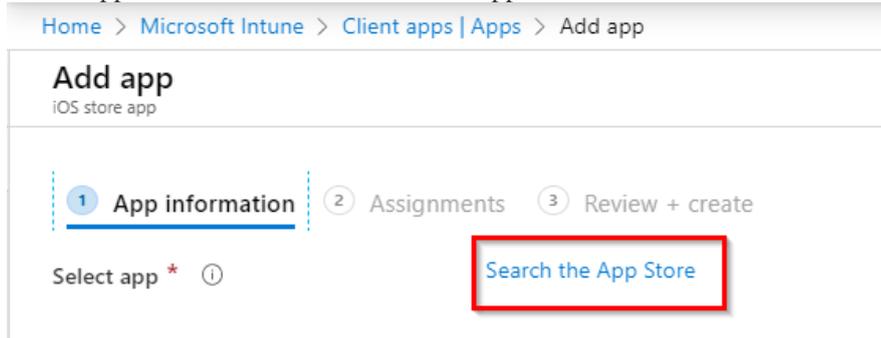
Note - The data fields are similar for both iOS and Android users. The examples below are applicable for both platforms.

- **For iOS Devices**

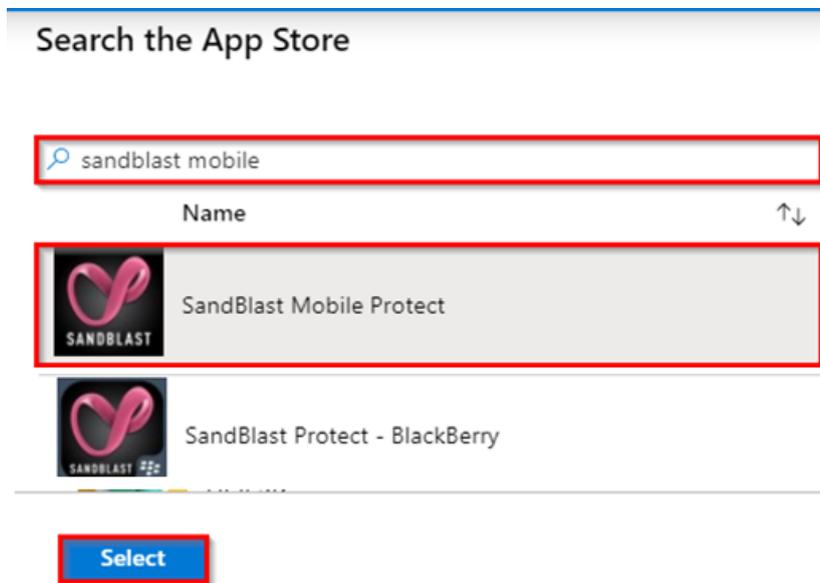
- a. Select App type **iOS store app** and click **Select**.



- b. In the App information select Search the App Store



- c. Search for SandBlast Mobile application and click on Select.



- d. Click **Next**.
- e. Under Assignments, **Required**, select **+Add Group**
- Select the security group created before and click **Select** and then **Next**

Home > Microsoft Intune > Client apps | Apps > Add app

Add app

iOS store app

✓ App information 2 Assignments 3 Review + create

Required

GROUP	MODE	VPN
No assignments		

+ Add group + Add all users + Add all devices

Available for enrolled devices

GROUP	MODE	VPN
No assignments		

+ Add group + Add all users

Available with or without enrollment

GROUP	MODE
No assignments	

+ Add group + Add all users

Previous **Next**

Select groups

Azure AD groups

sbm

- SBM_Chadfield
- sbm_pm_test
- SBM_PMs
- SBM_Users Selected**

Selected items

- SBM_Users

Select

f. Review and click **Create**

Home > Microsoft Intune > Client apps | Apps > Add app

Add app

iOS store app

✓ App information ✓ Assignments 3 **Review + create**

Summary

App information

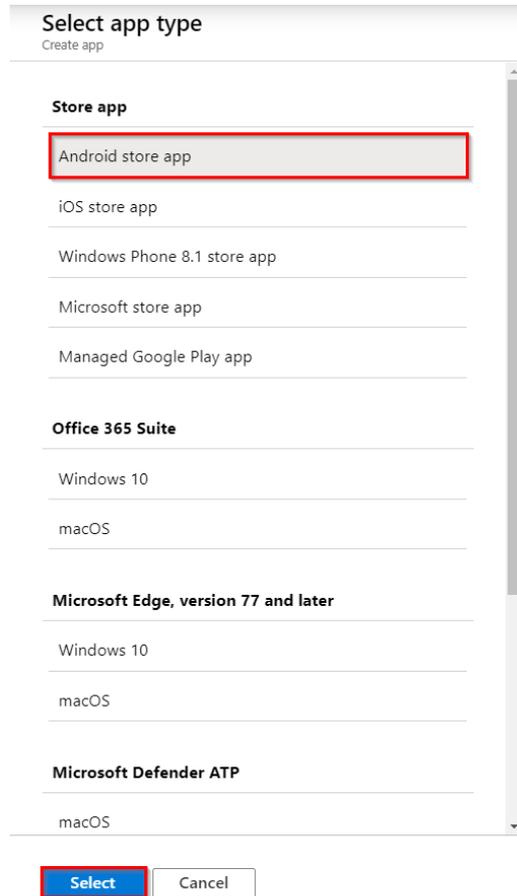
Assignments

Previous **Create**

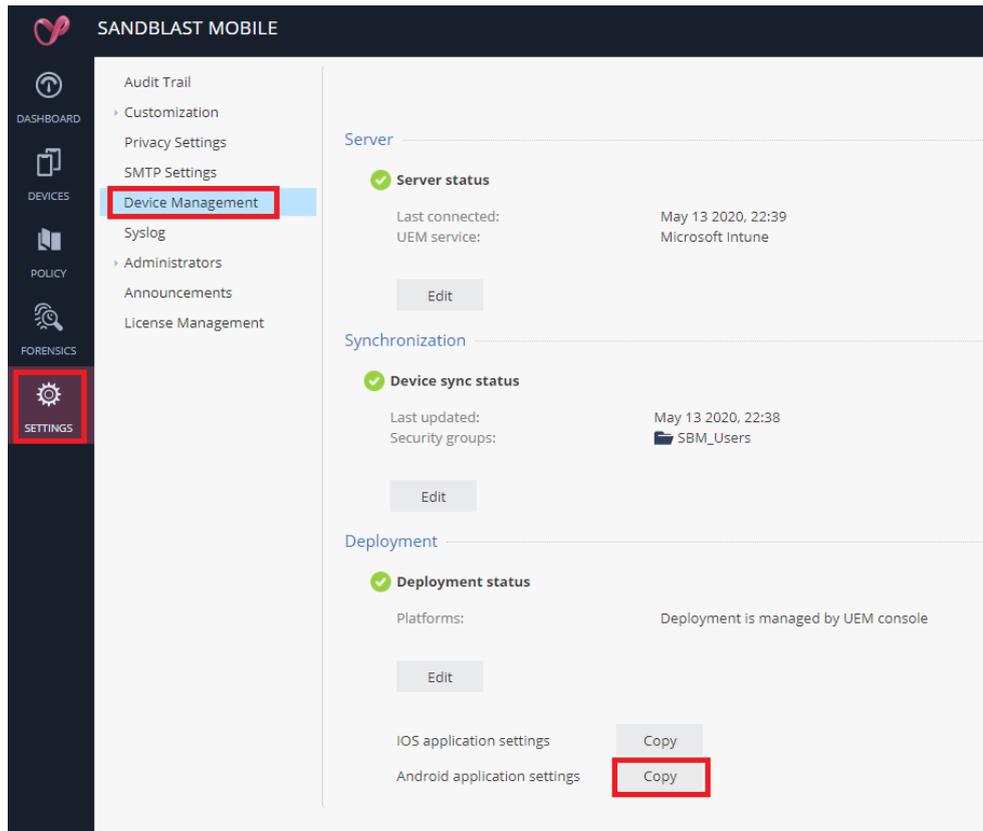
▪ **For Android Legacy Devices**

- a. Select App type Android Store App and click Select.

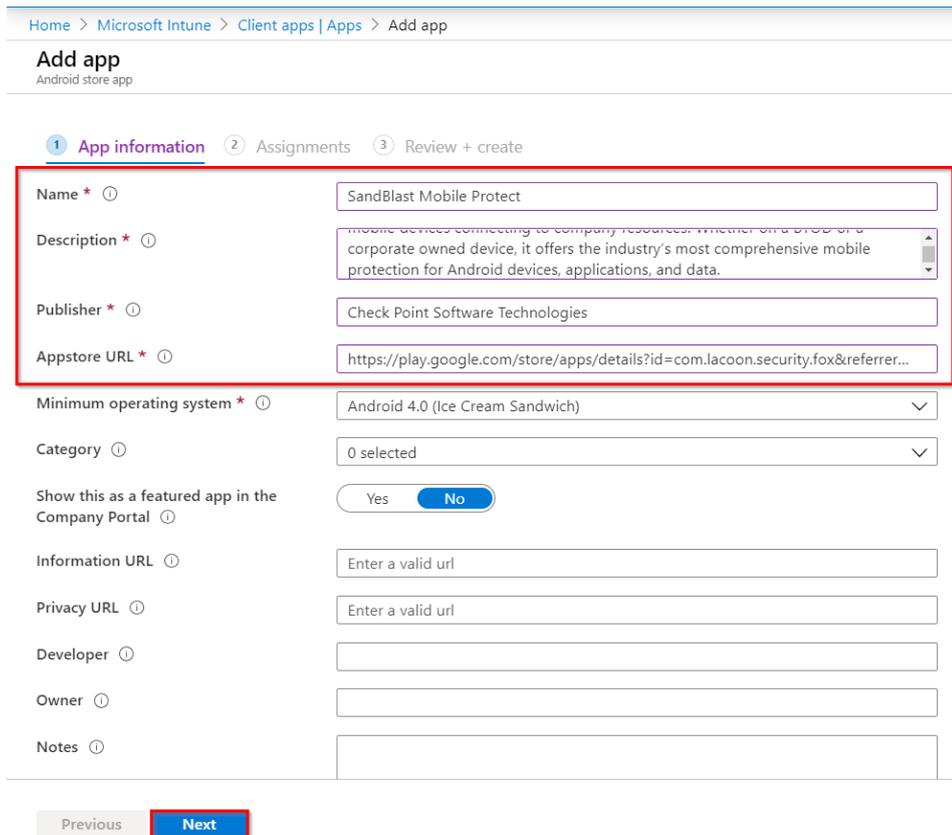
Example:



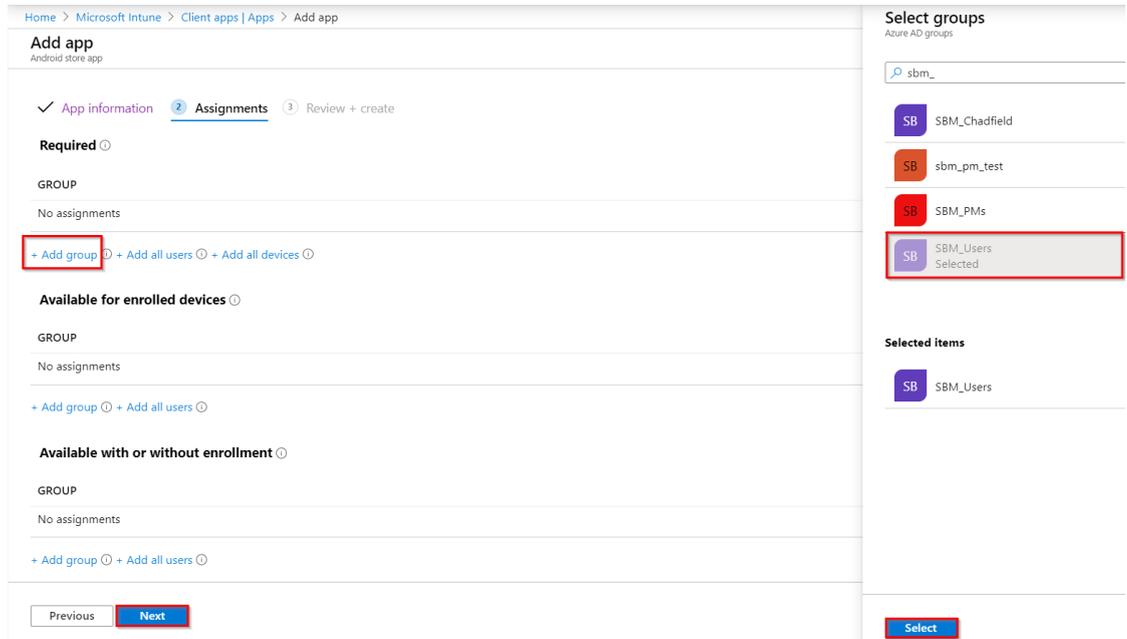
- b. In the App information tab Enter SandBlast Mobile Protect as the name.
- c. Enter a description, as listed in the app store description.
- d. Set the Publisher to Check Point Software Technologies.
- e. Get the URL for SandBlast Mobile Protect Android link from the **SandBlast Mobile Dashboard** go to **Settings > Device Management** Click "Copy" next to "Android application settings" under the **Deployment** section:



f. Paste this URL under **App-Store URL** on the **Add App** pane



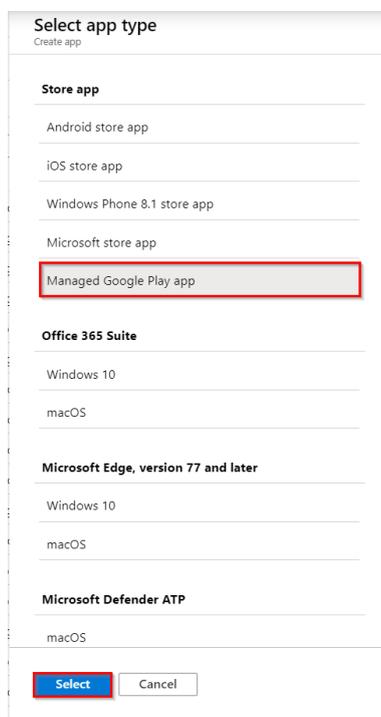
- g. Click **Next**.
- h. Under Assignments, **Required**, select **+Add Group**
Select the security group created before and click **Select** and then **Next**



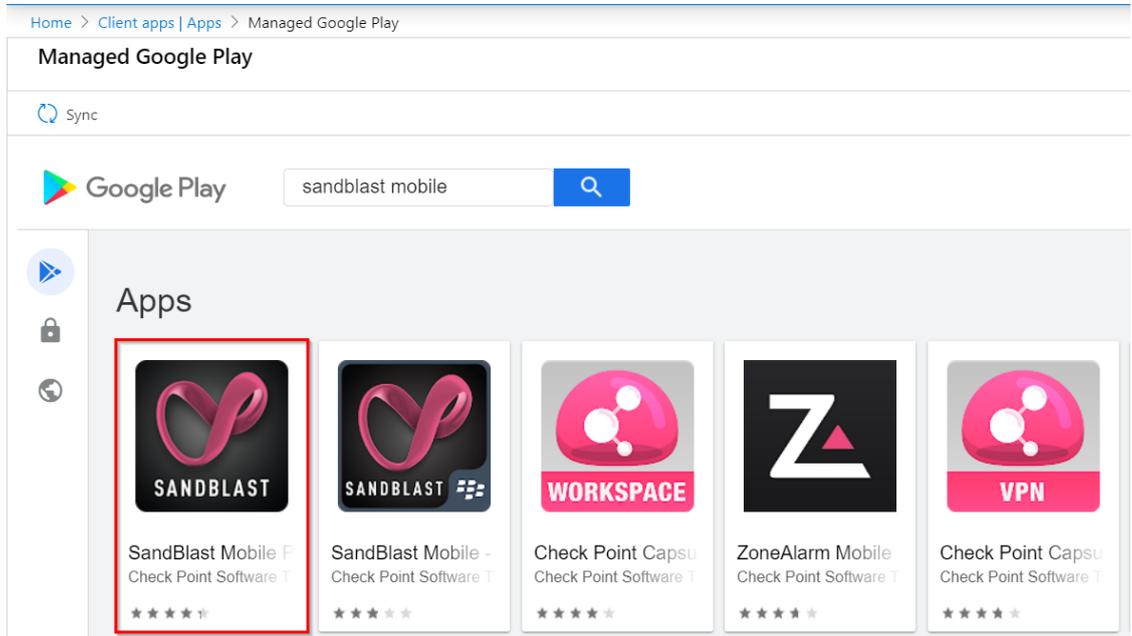
- i. Review and click **Create**

▪ **For Android Enterprise Devices**

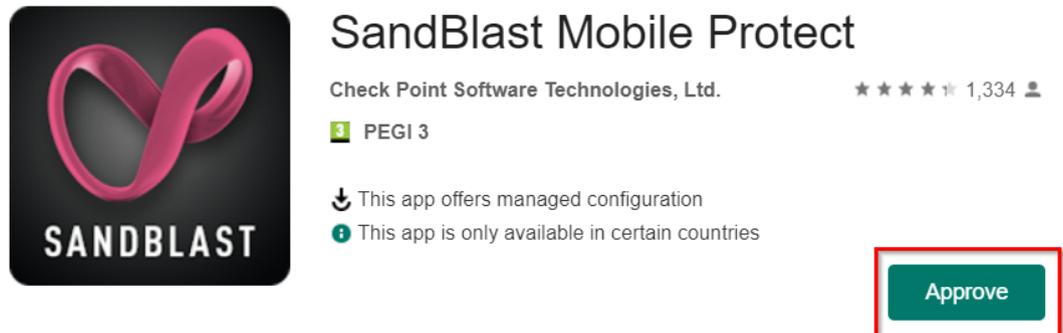
- a. Select App type Managed Google Play App and click Select.



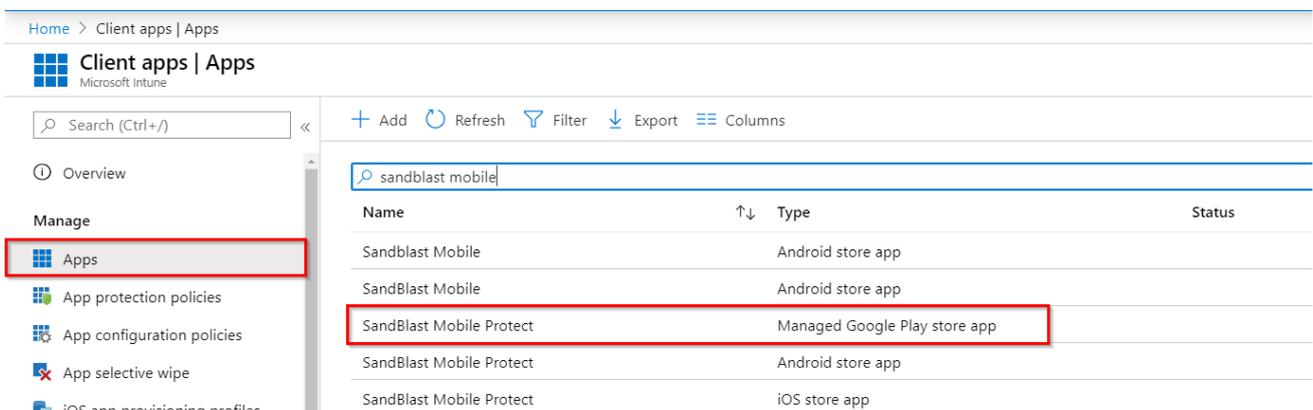
b. Search SandBlast Mobile Protect App and select it



c. Click Approve



d. Go to Apps, and select **SandBlast Mobile Protect** app from the Managed Google Play store app



e. Go to **Properties > Assignments**, click **Edit**

Home > Client apps | Apps > SandBlast Mobile Protect | Properties

SandBlast Mobile Protect | Properties
Client Apps

Search (Ctrl+/) <<

Overview

Manage

Properties

Monitor

Device install status

User install status

App information Edit

Name SandBlast Mobile Protect

Description SandBlast Mobile Protect helps secure your mobile phone or tablet.

Publisher Check Point Software Technologies, Ltd.

Appstore URL <https://play.google.com/store/apps/details?id=com.lacoon.security.fox&hl=US>

Logo

Available licenses 0

Total licenses 0

Assignments Edit

f. Under Assignments, **Required**, select **+Add Group**

g. Select the relevant security group you want to install the app on and click **Select**

h. Click **Review + save**

i. Review and click **Create**

Home > Client apps | Apps > SandBlast Mobile Protect | Properties > Edit application

Edit application
Managed Google Play store app

Assignments Review + save

Required

GROUP

caso_dynamic

ItemGroup

List_group

ofo_ja_cope

QIR_SBM_users

SBM_qualified

+ Add group + Add all users + Add all devices

Available for enrolled devices

Review + save Cancel

Select groups
Azure AD groups

SBM_user

SB SBM_Users Selected

Selected items

SB SBM_Users

Select

f. Click **Next**.

g. Under **Configuration Settings format**, select “Use configuration designer”

Use the table below for the configurations

Configuration Key	Value Type	Configuration Value
DEVICE_UDID	String	{{aaddeviceid}}
token	String	** Dashboard ID Hash **
Lacoon Server Address	String	gw.locsec.net

Notes: It is highly recommended to Copy & Paste the Configuration Key and Configuration Value directly from the table above where applicable

h. ** for the key “token” value use SandBlast Mobile dashboard go to Settings > Device Management, under the Deployment section click Edit:

Copy the token of your dashboard – See section “*Configuring UEM Integration Settings*” page 22

Example:

All services > Microsoft Intune > Client apps | App configuration policies > Create app configuration policy

Create app configuration policy

Basics
 Settings
 3 Assignments
 4 Review + create

Configuration settings format * ⓘ

ⓘ Once the policy is created, the format cannot be changed

Enter values for the XML property list. The values in the list will vary depending on the app you are configuring. Contact the supplier of the app to learn the values you can use.

[Learn more about XML property lists](#)

Configuration key	Value type	Configuration value
DEVICE_UDID	String	{{aaddeviceid}} ...
token	String	cc1e99b621ec3181fbaf3021b8883d... ...
<input type="text" value="Lacoon Server Address"/> ✓	<input type="text" value="String"/> v	<input type="text" value="gw.locsec.net"/> ✓ ...
<input type="text"/>	<input type="text" value="Select one"/> v	<input type="text"/>

- i. When done click **Next**
- j. Under Assignments click on +Select groups to include
- k. Select the security group you want to associate the app configuration with
- l. Click Select
- m. Click Next

Home > Client apps | App configuration policies > Create app configuration policy

Create app configuration policy

✓ Basics ✓ Settings **3 Assignments** 4 Review + create

Included groups
Assign to: Selected groups

Selected groups
No groups selected

+ Select groups to include

Excluded groups

ⓘ When excluding groups, you cannot mix user and device groups across include and exclude. [Click here to learn more.](#)

Selected groups
No groups selected

[+ Select groups to exclude](#)

Previous **Next**

Select groups to include
Azure AD Groups

SBM_Users

SB SBM_Users
Selected

Selected items

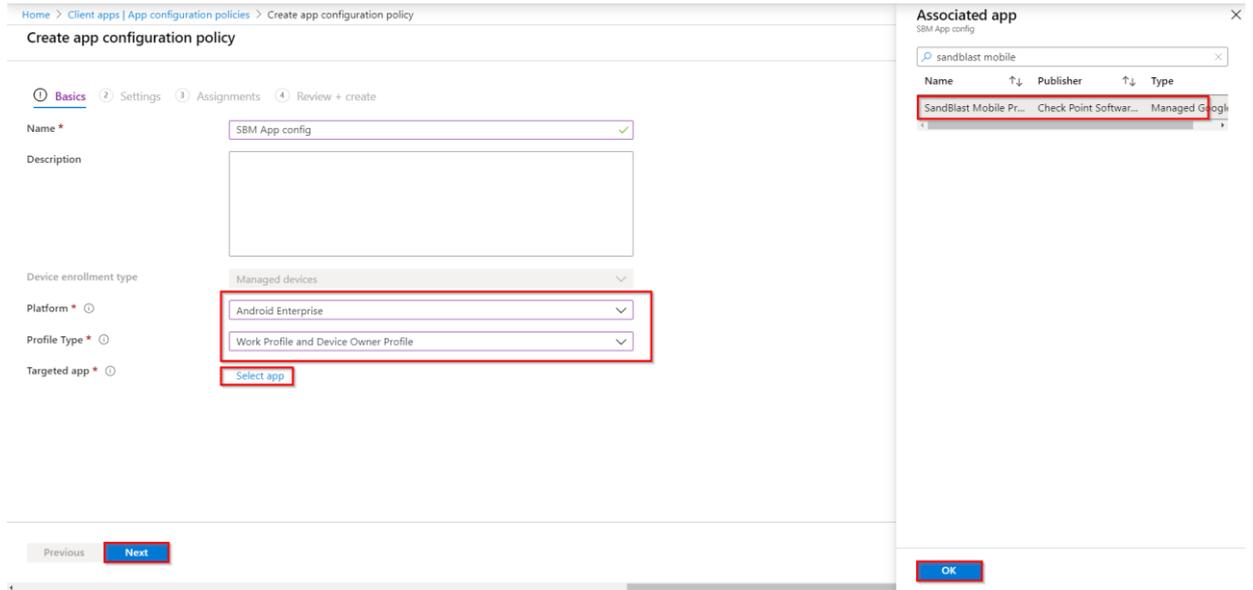
SB SBM_Users

Select

n. Review your configuration and click Create.

For Android Enterprise App:

- a. Give your configuration a **Name** (e.g. “SBM App Config AE”)
- b. **Platform** select Android Enterprise
- c. Profile Type select **Work Profile and Device Owner Profile**
- d. Click on Select App and choose SandBlast Mobile app from the Managed Google Play
- e. Click OK
- f. Click Next:



g. Under **Configuration Settings format**, select “Use configuration designer” click **+Add**

Use the table below for the configurations (check the key to populate, rest of configuration keys can stay empty)

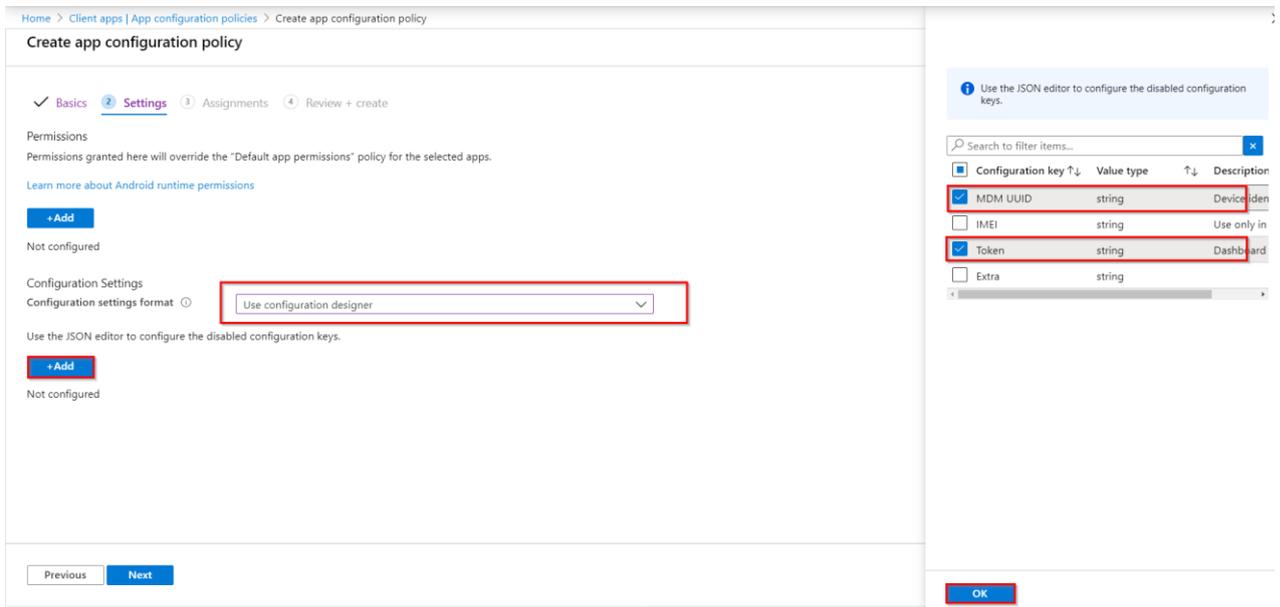
Configuration Key	Value Type	Configuration Value
MDM UDID	String	{{aaddeviceid}}
Token	String	** Dashboard ID Hash **



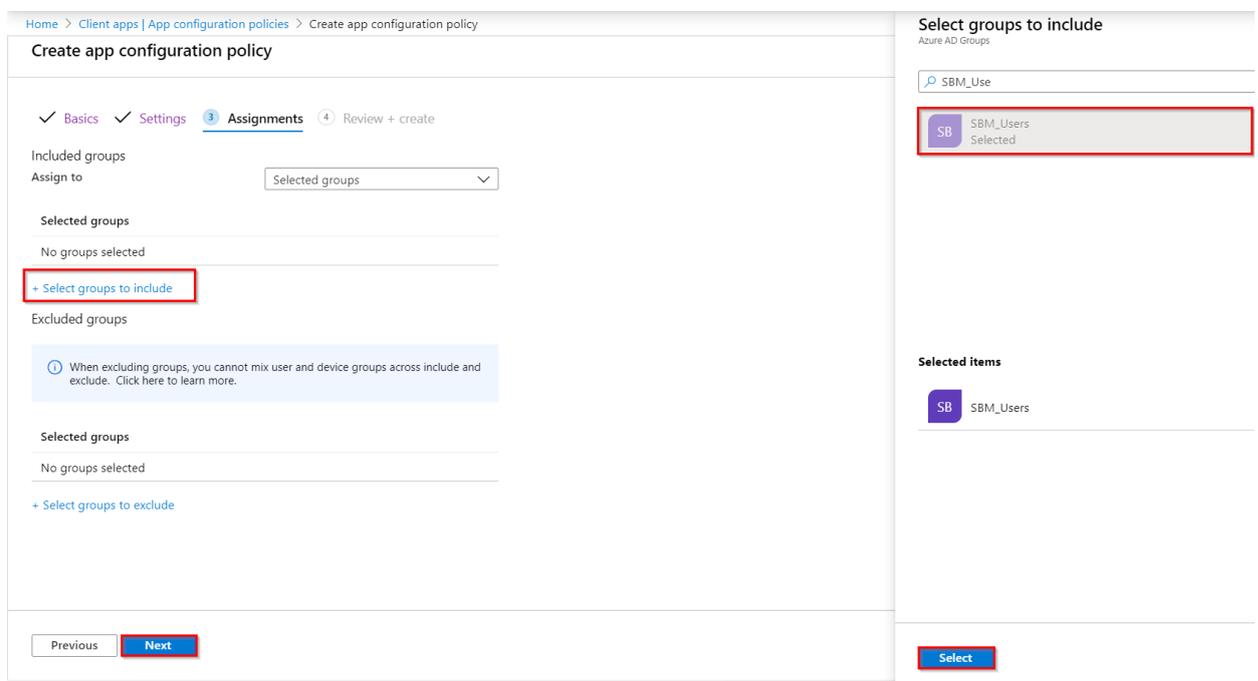
Notes: It is highly recommended to Copy & Paste the Configuration Value directly from the table above where applicable

h. ** for the key “token” value use **SandBlast Mobile dashboard** go to **Settings > Device Management**, under the **Deployment** section click **Edit**:

Copy the token of your dashboard – See section “*Configuring UEM Integration Settings*” page 22
Example:



- i. When done click **Next**
- j. Under **Assignments** click on **+Select groups to include**
- k. Select the security group you want to associate the app configuration with
- l. Click **Select**
- m. Click **Next**



- n. Review you configuration and click **Create**:

Home > Microsoft Intune > Client apps | App configuration policies > Create app configuration policy

Create app configuration policy

✓ Basics ✓ Settings ✓ Assignments **4 Review + create**

Summary

Basics

Name	SBM App config
Description	--
Device enrollment type	Managed devices
Platform	Android Enterprise
Profile Type	Work Profile and Device Owner Profile
Targeted app	SandBlast Mobile Protect

Settings

Permissions

Not configured

Configuration Settings

Configuration key	Value type	Configuration value
Token	string	cd39b7c22c9f39767a5a7f4b1887a24d2c...
MDM UUID	string	{{deviceid}}

Connecting the SandBlast Mobile Protect app to your Device

To install the SandBlast Mobile Protect app on your devices in your organization, you must first configure them to require the SandBlast Mobile Protect app. This is a dynamic group assignment according to the associated tag. Microsoft Intune calls these dynamic Assignment Groups “Smart Groups”.

Add all the devices marked with the Status labels to a group that indicates that the devices are registered in SandBlast Mobile Dashboard.

Create a mitigation process.

General Workflow:

1. Create a compliance policy to uninstall / remove corporate apps from the device until the user installs the required apps on the device.
2. Create a Mitigation Process for devices-at-risk through the Smart Group Risk labels.

Creating a Compliance Policy for the Organization Devices

The Compliance Policies are activated on the devices that did not install the required apps. SandBlast Mobile Protect app defines the security levels for the devices. You select the security level that marks the device as Not Compliant with company policy.

You must create separate compliance policies for specific OS types, such as iOS and Android.



Note - In every organization, the customer configures the compliance policies according to the production environment, needs, and the internal security policy.

For more information about Intune compliance policy see the [online guide](#) where you can explore the details of creating compliance policies for iOS, Android and Android Enterprise.

To create a Compliance Policy:

1. Go to **Device compliance > Policies** and click **Create Policy**.
2. On the **Compliance Policy** panel select a platform to start.



Note - The data fields are similar for both iOS and Android settings.

Example for *Android Enterprise* with *Device Owner*:

The screenshot shows the Microsoft Intune console interface. On the left, the navigation pane is open to 'Device compliance > Policies'. The 'Policies' option is highlighted. In the main content area, the 'Create a policy' form is displayed. The 'Platform' dropdown is set to 'Android Enterprise' and the 'Policy type' dropdown is set to 'Device owner'. A 'Create' button is located at the bottom right of the form. The background shows a list of existing policies, including 'aaaaa', 'Android_test_mp', 'Android_testMP_policy', 'Chadfield', 'Elad_IT_Policy', 'Gil Compliance Policy', 'IlanAndroidWorkProfil', 'Max Policy', 'Mobile_QA_Policy_And', 'Mobile_QA_Policy_iOS', 'mtp', and 'Ofir Compliance'.

3. On the **basis** tab, give your policy a name
4. On the Compliance Settings tab, go to **Device health**, and require the device to be at or under the Device Threat Level of **Medium** (recommended). This will turn your device to be not compliant if its risk level determined by Check Point SandBlast Mobile (MTD) is **High**. See below details for all options:

Device Health Level	Description
Secured:	This is the most secure. The device cannot have any threats present and still access company resources. If any threats are found, the device is evaluated as non-compliant.
Low:	The device is compliant if only low level threats are present. Anything higher puts the device in a non-compliant status.
Medium:	The device is compliant if the threats found on the device are low or medium level. If high level threats are detected, the device is determined as non-compliant.
High:	This is the least secure. This allows all threat levels, and uses Mobile Threat Defense for reporting purposes only. Devices are required to have the MTD app activated with this setting.

Home > Microsoft Intune > Device compliance | Policies > Device owner

Device owner

Android Enterprise

✓ Basics
2 Compliance settings
3 Actions for noncompliance
4 Scope tags
5 Assignments
6 Review + create

∨ Microsoft Defender ATP

∧ Device Health

Require the device to be at or under the Device Threat Level ⓘ Medium ∨

Google Play Protect

SafetyNet device attestation ⓘ Not configured ∨

∨ Device Properties

∨ System Security

Previous
Next

Note that you can configure actions for noncompliance and Scope tags (not covered on this guide).

5. Go to Assignments and assign this policy to the relevant security group to apply this policy to
6. Review and create your policy.

Using Android Enterprise with SandBlast Mobile

Android Enterprise is a Google-led initiative that enables the operation of Android devices and apps in the workplace. The program offers APIs and other tools for developers to integrate support for Android into their enterprise mobility management (EMM) solutions.

For example, through one or more API(s) your UEM platform can disable a camera, Bluetooth, or prevent an access to system settings.

For information about configuring Android Enterprise on your device, see [online guide](#).

Android Enterprise Deployment Scenarios

Android Enterprise supports these deployment scenarios:

- Company-owned fully managed devices (COBO)
- Company-owned fully managed devices with a work profile (COPE)
- Company-owned devices for dedicated use (COSU)
- Employee-owned devices (BYOD)

COBO and COSU devices have a single profile. Follow integration guide instructions for Android Enterprise devices to deploy SandBlast Mobile Protect app on your devices. For more information see the [online guide](#).

COPE and BYOD devices have Work and Personal profiles. With SandBlast Mobile Protect app you can protect one profile or both profiles.

For the highest protection level we recommend to protect both Work and Personal Profiles. See "[Configuring SandBlast Mobile Protect app to Protect your Devices](#)" on page 46.



Note - If you protect only the Work profile, skip the next section.

Configuring SandBlast Mobile Protect app to Protect your Devices



Note -The deployment of the SandBlast Mobile Protect app on the Personal profile of BYOD device cannot be automated by Android design (Personal profile of BYOD device is not managed).

With the Android Enterprise, you can protect the whole device or part(s) of it.

If you protect the whole device, install the SandBlast Mobile Protect app to both Work and Personal Profiles.

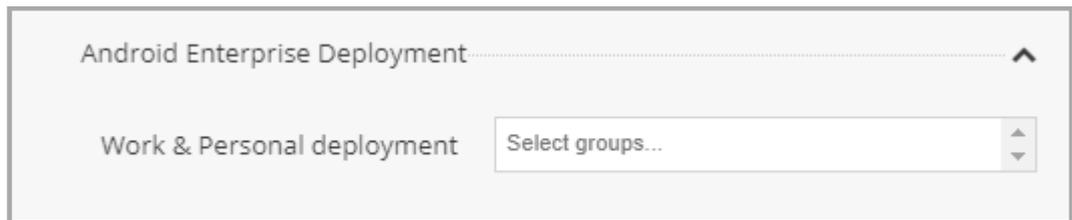


Note - If you protect only the Personal profile, skip this section.

To protect both profiles:

1. On the SandBlast Mobile Dashboard, go to **Settings > Device Management**.
2. Enable the SandBlast Mobile Protect app (for both profiles).
 - For a new UEM configurations:
 - a. Go to **Settings > Device Management > Edit Settings**
 - b. In the **Android Enterprise Deployment** section, select and add the device groups for both profiles.

Example:



Notes:

- Only the synced groups in the upper groups' section are available for Android Enterprise deployment.
- If one or more devices in the selected group have SandBlast Mobile Protect app Version earlier than 3.6.4.4348, the operation stops until the devices are upgraded.
- If you add a group of devices for Android Enterprise deployment, make sure to configure the devices with both Personal and Work profiles.
- If you remove a group of devices from the Android Enterprise deployment, the SandBlast Mobile Protect app deletes the Personal profile record on every device in this group.
- iOS devices are ignored in the Android Enterprise context.

3. Click **Finish**.



Note - If a device belongs to more than one group, one group selected in Android Enterprise deployment, and one group is not selected, the deployment is both Work and Personal.

General View on the Check Point Dashboard (Example):

Time	Severity Level	Attack Vector	Threat Factors	Event	Event Details	OS	Device ID
Feb 11 2020, 09:52:01	Information	Device	Personal profile inactive	Compliant		Android Enterprise	58052
Feb 11 2020, 01:15:00	Critical	Device	Personal profile inactive	Noncompliant		Android Enterprise	58052
Feb 09 2020, 17:11:57	Information	Device	Personal profile compromised	Compliant		Android Enterprise	58052
Feb 09 2020, 17:10:50	Critical	Device	Personal profile compromised	Noncompliant		Android Enterprise	58052
Feb 09 2020, 17:09:26	Information	Device	Personal profile inactive	Compliant		Android Enterprise	58052
Feb 09 2020, 17:08:14	Critical	Device	Personal profile inactive	Noncompliant		Android Enterprise	58052
Feb 09 2020, 17:08:14	Information	Device	Connectivity	Active		Android Enterprise	58052
Feb 09 2020, 16:59:48	Information	Device	Personal profile inactive	Compliant		Android Enterprise	58046
Feb 09 2020, 16:58:50	Critical	Device	Personal profile inactive	Noncompliant		Android Enterprise	58046
Feb 09 2020, 16:58:50	Information	Device	Connectivity	Active		Android Enterprise	58046
Feb 09 2020, 16:21:03	Information	Device	Connectivity	Active		Android Enterprise	58040
Feb 09 2020, 16:08:13	Critical	Device	Personal profile inactive	Noncompliant		Android Enterprise	58031
Feb 09 2020, 16:08:13	Information	Device	Connectivity	Active		Android Enterprise	58031
Feb 09 2020, 15:40:39	Information	Device	Personal profile inactive	Compliant		Android Enterprise	58018
Feb 09 2020, 15:39:21	Critical	Device	Personal profile inactive	Noncompliant		Android Enterprise	58018
Feb 09 2020, 15:39:20	Information	Device	Connectivity	Active		Android Enterprise	58018
Feb 09 2020, 15:29:13	Information	Device	Connectivity	Active		Android Enterprise	58015
Feb 09 2020, 14:35:10	Information	Device	Personal profile inactive	Compliant		Android Enterprise	58003

To view and filter the devices:

1. On the SandBlast Mobile Dashboard, go to **Devices > Groups > Devices**.

Example:

ID	Name	Email	Device Number	Device Type	OS Version	Device Details	Client Version
20	John Doe	john@domain.com	No number	Android Enterprise	Unknown	unknown / unknown	
19	John Doe	john@domain.com	No number	Android	Unknown	unknown / unknown	

2. In the **Device Type** column, filter the devices in the list according to their protection profile.

Profile	Icon	Filter
Work		Device Type OS - Android Enterprise
Personal		Device Type OS - Android

Policies

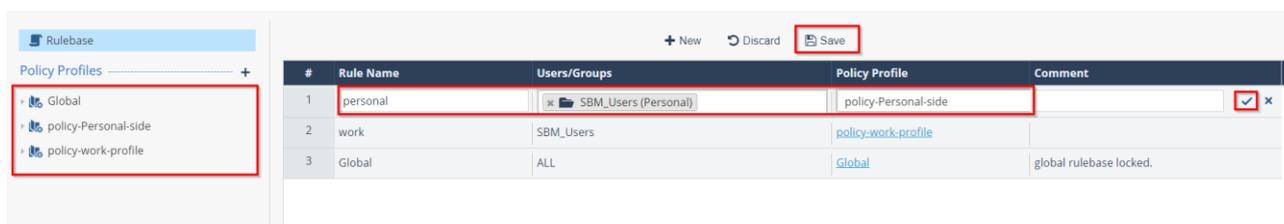
Check Point recommends creating different policies for personal side and working profile of the device.

1. To create a new policy, go to Policy and click the + next to Policy Profiles



2. Create a policy called Policy-Personal side and a second one called Policy-Work Profile.
3. Then you have to apply these policies to the different groups.
4. At the top of the Rule-base click +New.
5. Give your new rule a name, choose the relevant group (work or personal), and select the relevant policy you just created.
6. Confirm your changes and click on Save.

Example:

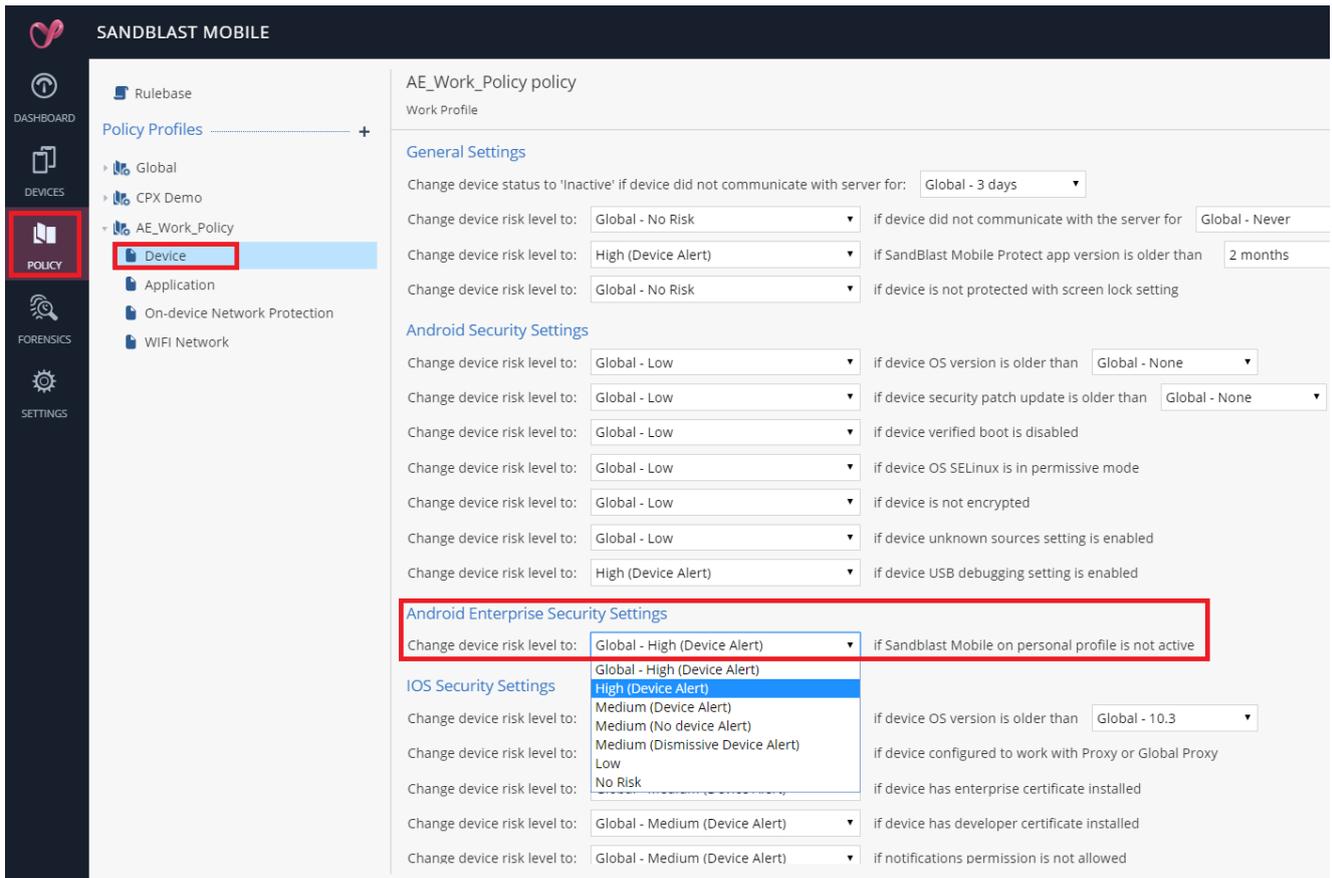


To change policy for inactive personal profile:

You can raise the risk level of the Work Profile if the personal side of the device is not protected with SandBlast mobile, or if SandBlast Mobile on the personal side has detected a risk with a level of High:

1. On the SandBlast Mobile Dashboard, go to **Policy > The policy applied to the Work Profile, or the local one > Device**
2. Go to **Android Enterprise Security Settings**. And select the risk level you want to give to the Work Profile is the personal side of the device is compromised or not protected:

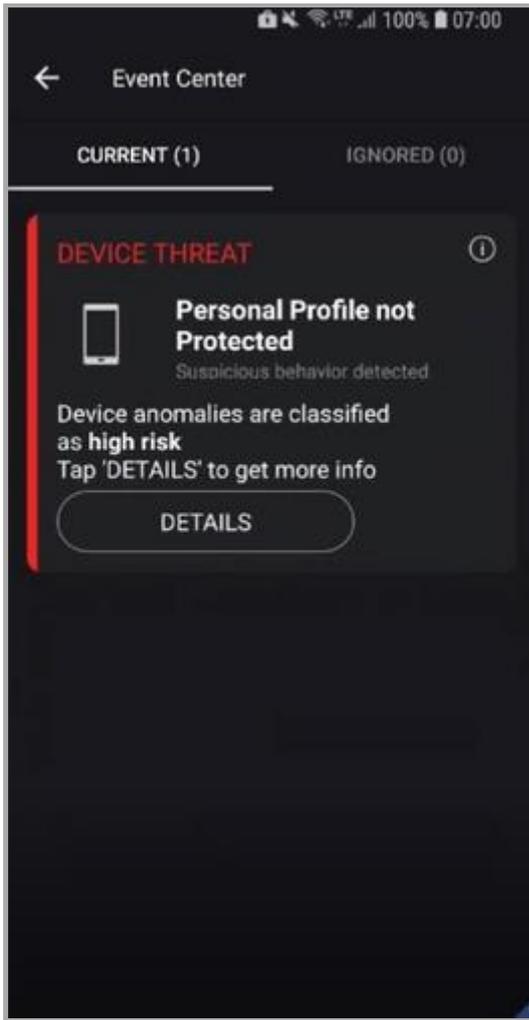
Example:



Risk Handling

- If the SandBlast Mobile protection is inactive on the Personal profile, the risk level is raised according to the Android Enterprise Security Settings policy on the Work profile (see "*Policies*" on page 49).

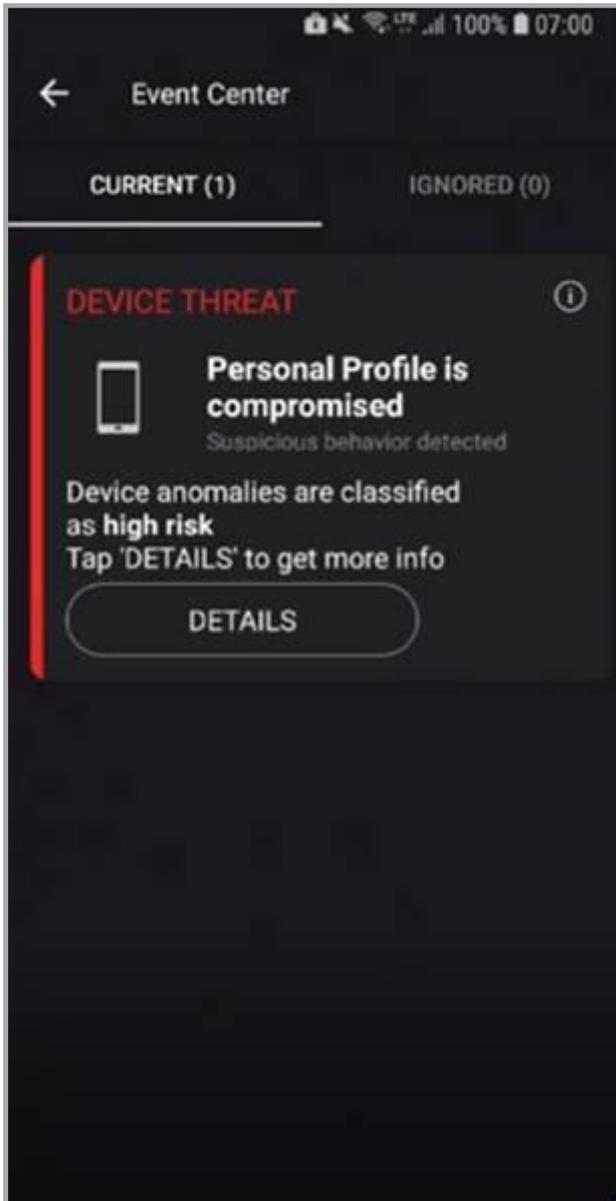
Example:



Time	Severity Level	Attack Vector	Threat Factors	Event	Event Details	OS	Device ID
Feb 09 2020, 17:09:26	Information	Device	Personal profile inactive	Compliant			58052
Feb 09 2020, 17:09:26	Information	Device	Connectivity	Active			58054
Feb 09 2020, 17:08:14	Critical	Device	Personal profile inactive	Noncompliant			58052

- If the Personal profile has the High Risk status, the risk level is raised to **High** on the Work profile. The SandBlast Mobile informs the user that the personal profile is at risk.

Example:



Time	Severity Level	Attack Vector	Threat Factors	Event	Event Details	OS	Device ID
Feb 09 2020, 17:11:57	Information	Device	Personal profile compromised	Compliant		Android	58052
Feb 09 2020, 17:11:57	Information	Application	Malware	Removed	App: Test Virus	Android	58054
Feb 09 2020, 17:10:50	Critical	Device	Personal profile compromised	Noncompliant		Android	58052
Feb 09 2020, 17:10:49	Critical	Application	Malware	Installed	App: Test Virus	Android	58054

- You can enable mitigation by UEM on the work profile, if you raise device health to high risk on the work profile. To configure incomppliance action, see [Creating a Compliance Policy on Devices](#) see [page 44](#).

Applying the SandBlast Mobile Protect app on Devices

The following section describes the user experience of device install and registration process with SandBlast Mobile. After following all the configurations in previous chapters the registration process of the SandBlast Mobile Protect app with the SandBlast Mobile Dashboard is automatic using the UEM deployment.

Deploying the SandBlast Mobile Protect app on the iOS Devices

With the deployment settings for SandBlast Mobile Protect app for iOS configured in section [Configuring Microsoft Intune Integration Settings on the SandBlast Mobile](#) on page 17, the App is automatically deployed to the devices that belong to the defined groups (see ["Configuring UEM to Deploy the SandBlast Mobile Protect app"](#) on page 25).

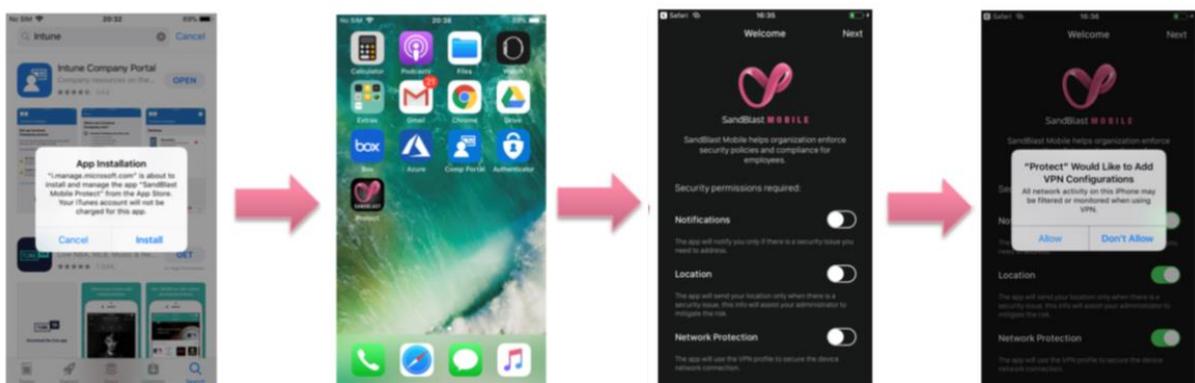


Note - It can take up to 10 minutes for Microsoft Intune to sync with the SandBlast Mobile Dashboard, and several more minutes for Microsoft Intune to push the App to the user device.

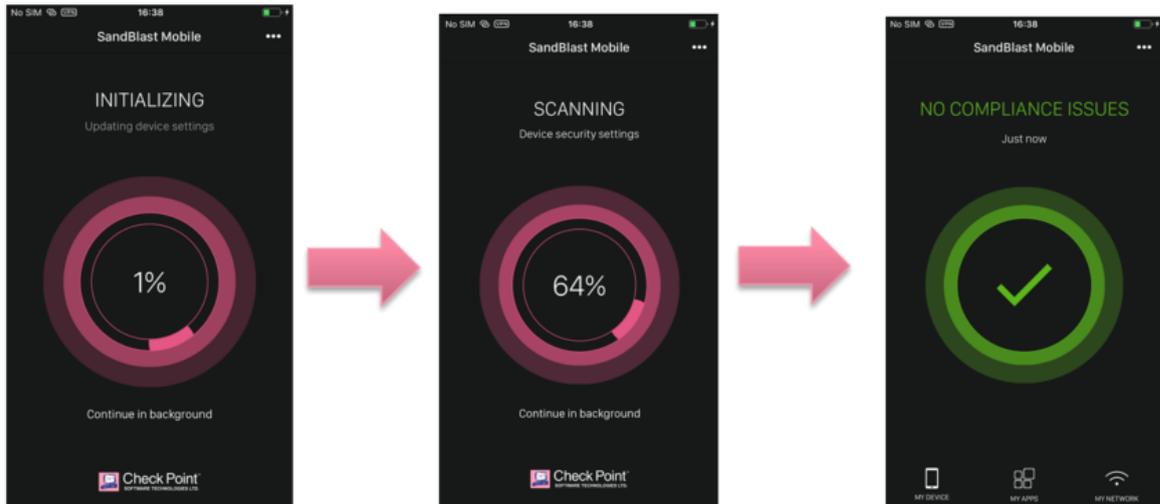
After you register your device in the Microsoft Intune and attach it to the defined groups, the system prompts the user to install the SandBlast Mobile Protect app.

▪ iOS Device Process

1. The user taps "INSTALL"
2. After the App has been deployed on the iOS Device, the user only needs to launch the App to finish the registration.
3. The user is prompted to enable Notifications, Location, and Network Protection.



4. Once the installation is done, the App scans the system.



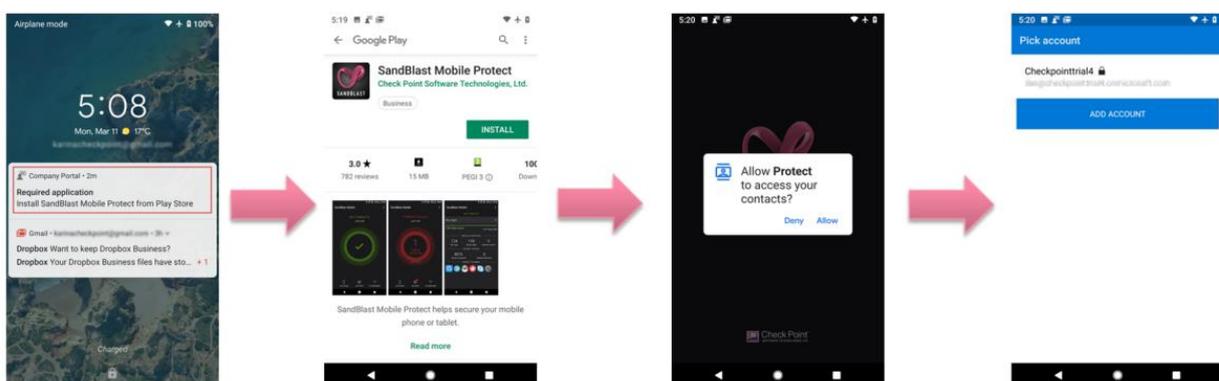
- Once the App is done scanning the system, it will display the state of the device. In this case, the device is without malicious or high risk apps, network and OS threats.

Deploying the SandBlast Mobile Protect app on Android Devices

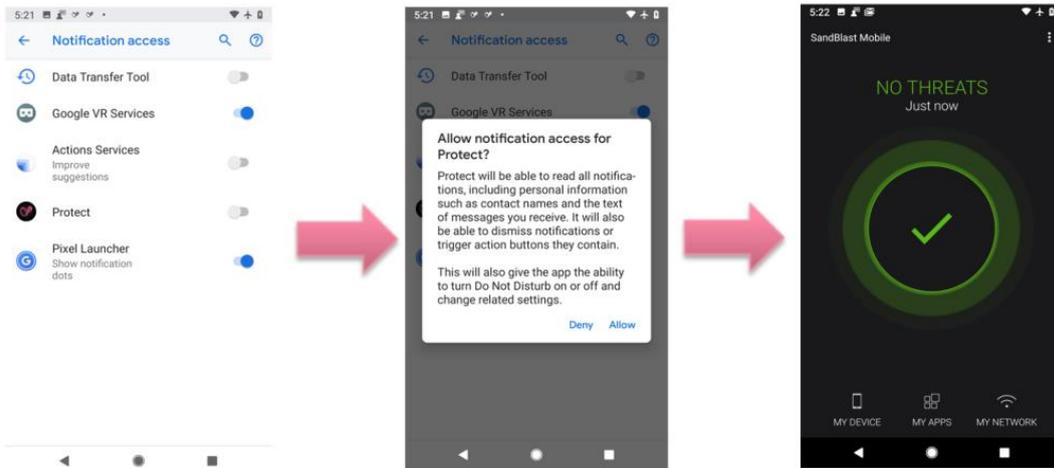
Legacy Android Device Process

After the device is enrolled to the Microsoft Intune and the device is synchronized to SandBlast Mobile, the user will be prompted to install the SandBlast Mobile Protect app. The user is automatically taken to the Google Play Store.

- The user taps "INSTALL".
- The user taps "Allow" to accept access to the device's contacts.
- The user selects the SSO credentials.
- The user allows the app to make phone calls and access device location (Android 9 and below).



- Once the App is done scanning the system, it will display the state of the device. In this case, the device is without malicious or high risk apps, network and OS threats.

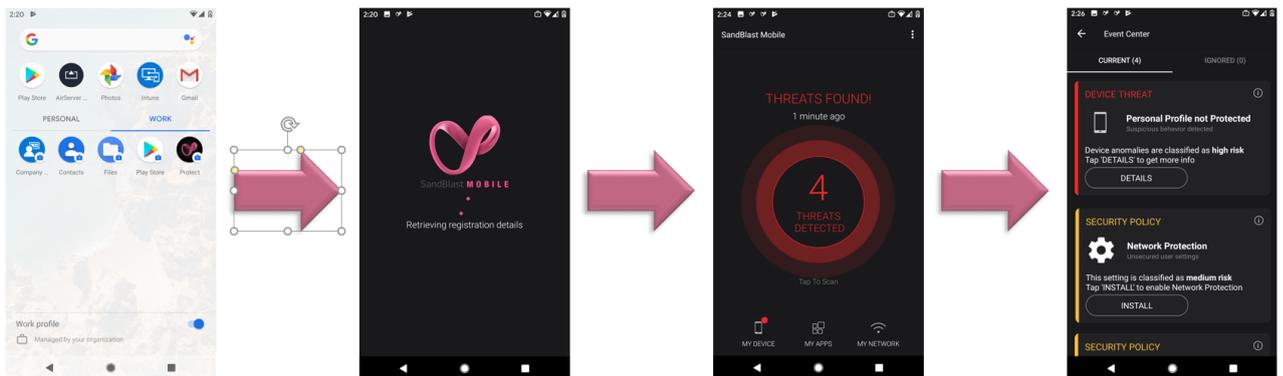


The registration server and the key are automatically configured in the App by the Microsoft Intune system. See ["Configuring UEM to Deploy the SandBlast Mobile Protect app"](#) on page 25

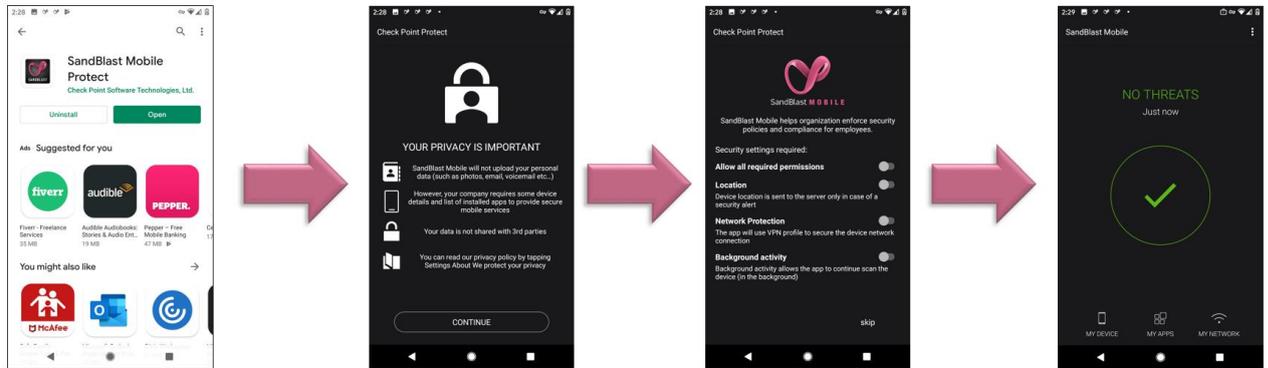
▪ **Android Enterprise Device Process**

After the device is enrolled to the Microsoft Intune and the work profile is activated, SandBlast Mobile Protect app will be pushed and installed automatically since it is a managed and a required app.

1. When the user opens the app it will register in the SandBlast Mobile Dashboard and become active
2. Depends on the policy defined for the device the user might need to approve few permissions for example Allowing Notification access or Location
3. SandBlast Mobile Protect app might show the device at high risk because it is configured to alert when the personal side is not protected See [Using Android Enterprise with SandBlast Mobile](#) on page 46



- Once the user installs the SandBlast Mobile Protect app on the personal side via his google play (relevant for COPE or BYOD modes) the app will automatically registers to the dashboard and becomes fully active.



Testing High Risk Activity Detection and Policy Enforcement

If the user's device is determined to be at risk either due to a malicious app or malicious activity, the SandBlast Mobile system notifies the User through in-app notifications, and also updates the device health **risk level** in Microsoft Intune system for that device. Microsoft Intune receives the risk state change, and upon recognizing the **risk level** value tied to a Configuration Profile, enacts that policy.

In this example, the Administrator blacklists an app, for example, "Box". As a result, the user's device is identified to be at High Risk due to the blacklisted app installed on the device. The SandBlast Mobile Dashboard notifies the user, and mark the device as High Risk to the Microsoft Intune system. The Microsoft Intune system then enforces policy actions specified in the Configuration Profile.

Blacklisting a Test App



Note - When you blacklist an app, all release versions and OS types of this app are blacklisted. Select **Apply only to this version** option to blacklist the specified version only.

1. Log into the **SandBlast Mobile Dashboard**.
2. Go to **App Analysis** tab and select for the app you wish to blacklist.

Example:

The screenshot displays the SandBlast Mobile Dashboard interface for the 'Box' app. The app is identified as legitimate with a 'Risk None' status. A dialog box titled 'CHANGING APPLICATION POLICY - GLOBAL' is open, allowing the user to change the application policy. The 'New policy' is set to 'Black Listed', and the 'Apply only to this version' checkbox is checked. The dialog also includes an 'Audit Trail note' field with the text 'Test compliance policy' and 'OK' and 'CANCEL' buttons.

THREAT SUMMARY
This application was identified as legitimate.

POLICY

Name	Risk	Action
Global	None	Edit
Fatih Test Profile	None	Edit
YS_Policy	None	Edit
test	None	Edit

MARKET DATA

Developer:	Box, Inc.
Website:	http://www.box.com/ref/ios_appstore_companylink
Genre:	Business
Market URL:	https://apps.apple.com/app/box-cloud-content-management/id290853822?uo=5
Platform:	iOS
Price:	Free
Publisher:	Box, Inc.
Release date:	2019-02-12T08:00:00Z

3. Go to **Global Policy** and click **Edit**.

A **Changing application policy-Global** window pops up.

4. From the **New Policy** drop-down menu, select **Black Listed**.
5. In the **Audit Trail note** field, enter a reason for this change.
6. Click **OK**.

The user receives a SandBlast Mobile Protect app notification to indicate that the blacklisted app (for example, Waze) is not allowed by the Corporate Policy.

View of a Non-Compliant Device

To see the non-compliant device in Intune:

1. Go to **Devices > All devices** and locate the relevant device.
2. Click **View**.

The device is displayed.

If you configured an email notification, you receive an email from Microsoft Intune.



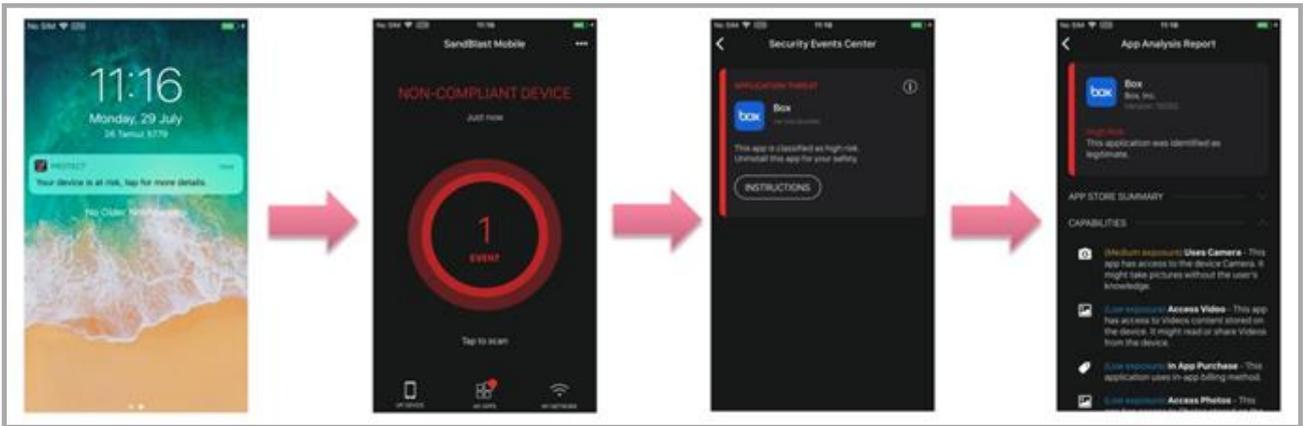
Note - The data fields are similar for both iOS and Android users. The examples below are applicable for both platforms.

The user is not allowed to use the app until the user removes the blacklisted app, or changes the compliance policy settings.

SandBlast Mobile Protect app Notifications

The user receives SandBlast Mobile Protect app notifications.

Example:



Microsoft Intune Company Portal Notifications

The user receives Microsoft Intune Agent notifications. The device is NO compliant with the company policy. The user must open the SandBlast Mobile Protect app for the solution.

Example:



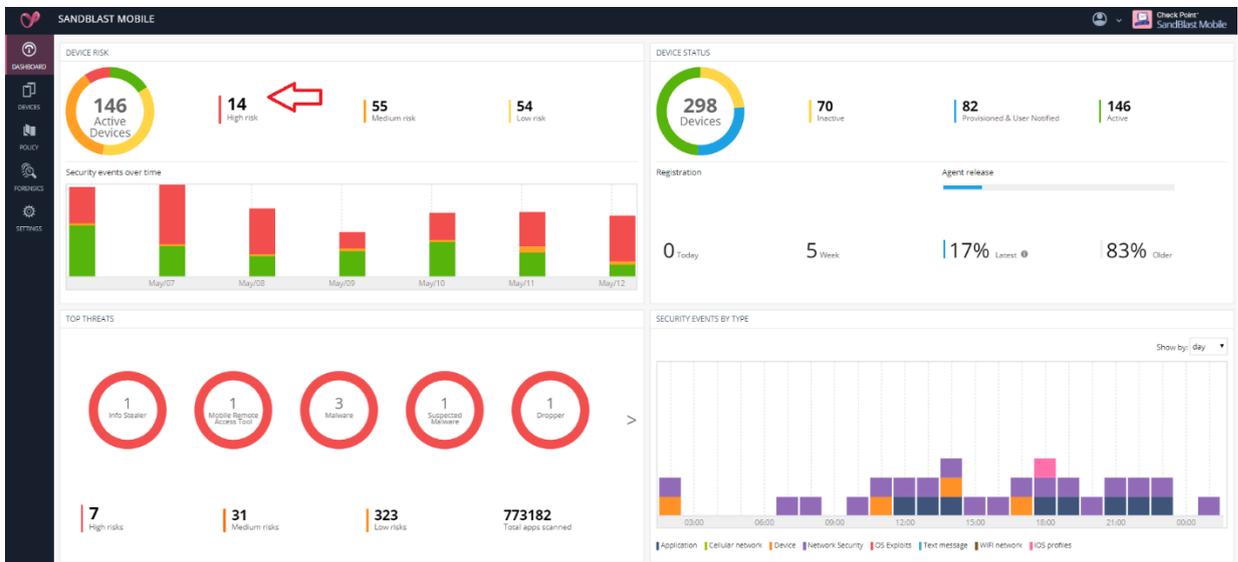
Administrator View on the SandBlast Mobile Dashboard

On the SandBlast Mobile Dashboard the Administrator can see the devices at High Risk.

1. Go to **Device Risk > High Risk** menu.

A list of the Devices At Risk is displayed in the **Device Risk** section.

Example:



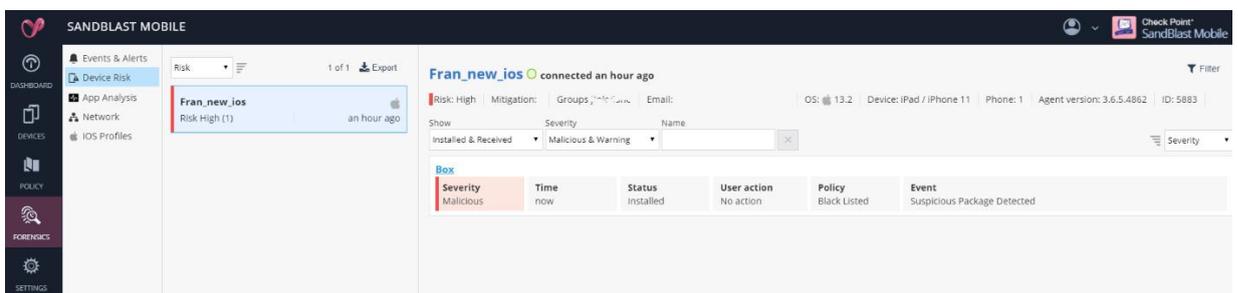
2. Click **High Risk**.

The list of devices at High Risk state is displayed.

3. Select the specified device on the left-side list.

You can see that the blacklisted app causes the High Risk state.

Example:



Administrator View on the Microsoft Intune Console

On the Microsoft Intune Console:

1. Go to **Microsoft Intune Overview > Device Compliance**.

You can see the devices that have compliance violations, or violate some policies, or both.

Example:

The screenshot shows the 'Device compliance' page in the Microsoft Intune console. On the left, there is a navigation menu with sections for 'Manage' (Policies, Notifications, Retire Noncompliant Devices, Locations) and 'Monitor' (Noncompliant devices, Devices without compliance..., Setting compliance, Policy compliance, Windows health attestation r..., Threat agent status). The main area displays 'Policy compliance' with a table:

Policy	Compliant devices	Noncompliant devices
BaselineConfigurationProfile	0	1
AE Compliance Policy	0	0
...	0	0
...	0	0
...	0	0

A callout box on the left indicates 'Devices without...' with a large '8' and a red 'x' icon, corresponding to the non-compliant devices in the table.

2. You can see the devices in the Out of Compliance state and click on the specified device with the Status **Non-Compliant**.

Example:

The screenshot shows the 'Device status' page in the Microsoft Intune console. It displays a table with the following data:

Device	User Principal Name	Compliance status	Last status update
ffnappc_andr04@intuneil_4/5/2020_3:32 PM	ffnappc@checkpoint.com	Not Compliant	4/26/20, 11:14 AM