

# Check Point SandBlast Mobile

---

## UEM Integration Guide with Microsoft Intune

---

Classification: None

© 2019 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 recompilation. 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 <http://www.checkpoint.com/copyright.html> for a list of our trademarks.

Refer to the Third Party copyright notices [http://www.checkpoint.com/3rd\\_party\\_copyright.html](http://www.checkpoint.com/3rd_party_copyright.html) for a list of relevant copyrights and third-party licenses.

Check Point and SandBlast are registered trademarks of Check Point Software Technologies Ltd. All rights reserved. Android and Google Play are trademarks of Google, Inc. App Store is a registered trademark of Apple Inc. iOS is a registered trademark of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. iOS® is used under license by Apple Inc. Microsoft, Azure, Microsoft Intune, and Microsoft Authenticator are registered trademarks of Microsoft Corporation and/or its subsidiaries.

## About This Guide

Check Point SandBlast Mobile 3.4 is the most complete threat defense solution designed to prevent emerging fifth generation cyber attacks and allow workers to safely conduct business. Its technology protects against threats to the OS, apps, and network, scoring the industry's highest threat catch rate without impacting performance or user experience.

Only SandBlast Mobile 3.4 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 WiFi networks
- » Blocks phishing attacks on all apps: email, messaging, social media
- » Prevents infected devices from sending sensitive data to botnets
- » Blocks infected devices from accessing corporate applications and data
- » Mitigates threats without relying on user action or mobile management platforms

SandBlast Mobile 3.4 uses a variety of patent-pending algorithms and detection techniques to identify mobile device risks, and triggers appropriate defense responses that protect business and personal data.

The SandBlast Mobile solution ("the Solution") includes the following components:

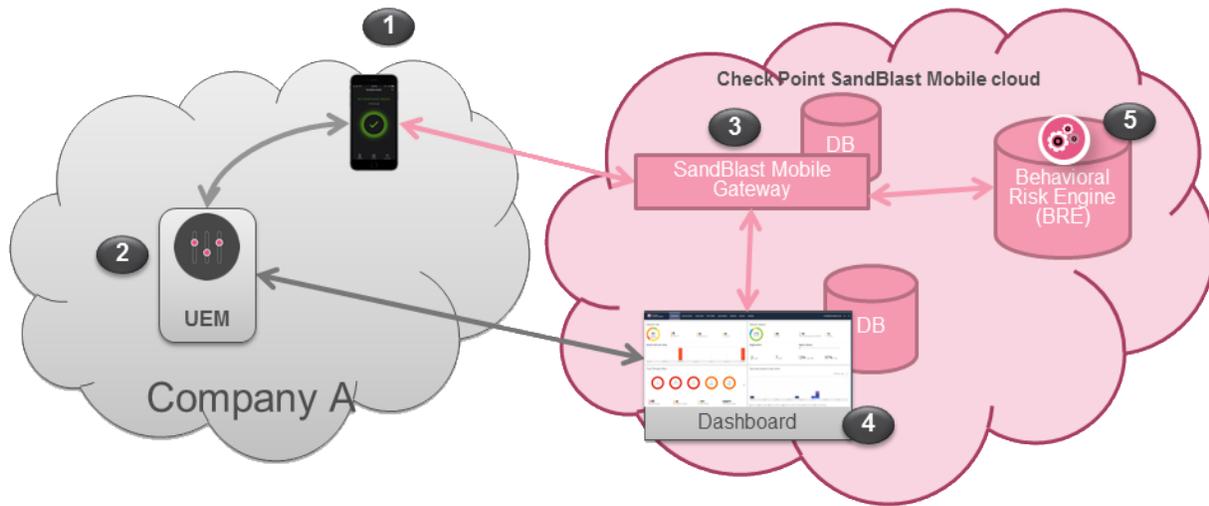
- » SandBlast Mobile Behavioral Risk Engine ("the Engine")
- » SandBlast Mobile Gateway ("the Gateway")
- » SandBlast Mobile Management Dashboard ("the Dashboard")
- » SandBlast Mobile Protect app ("the App") for iOS and Android

When used with an Unified Endpoint Management (UEM) system, such as Microsoft Intune, SandBlast Mobile provides integral risk assessment of the device to which the UEM can use to quarantine or enforce a set of policies that are in effect until the device is no longer at risk. Such policy enforcement could be to disable certain capabilities of a device, such as blocking access to corporate assets, such as email, internal websites, etc., thus, providing protection of the corporation's network and data from mobile-based threats.

This guide first describes how to integrate the SandBlast Mobile Dashboard with Microsoft Intune. It provides a quick tour through the interface of the Microsoft Azure Intune Portal and the SandBlast Mobile Dashboard in order enable integration, alerting, and policy enforcement.

This includes activation and protection of a new device, malware detection, and mitigation (including mitigation flow).

## Solution Architecture



Component	Description
1 SandBlast Mobile Protect app	<ul style="list-style-type: none"> <li>» 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.</li> <li>» To protect user privacy, the App examines critical risk indicators found in the anonymized data it collects.</li> <li>» 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.</li> </ul>
2 UEM	<ul style="list-style-type: none"> <li>» Unified Endpoint Management (generalized term replacing MDM/EMM)</li> <li>» Device Management and Policy Enforcement System</li> </ul>
3 SandBlast Mobile Gateway	<ul style="list-style-type: none"> <li>» The cloud-based SandBlast Mobile Gateway is a multi-tenant architecture to which mobile devices are registered.</li> <li>» The Gateway handles all Solution communications with enrolled mobile devices and with the customer's (organization's) Dashboard instance.</li> </ul>
4 SandBlast Mobile Dashboard	<ul style="list-style-type: none"> <li>» 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.</li> <li>» The Dashboard can be integrated with an existing Unified Endpoint Management (UEM) solution for automated policy enforcement on devices at risk.</li> <li>» When using this integration, the UEM serves as a repository with which the Dashboard syncs enrolled devices and identities.</li> </ul>
5 Behavioral Risk Engine	<ul style="list-style-type: none"> <li>» The cloud-based SandBlast Mobile Behavioral Risk Engine 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.</li> <li>» The Engine uses this data to detect and analyze suspicious activity, and produces a risk score based on the threat type and severity.</li> <li>» The risk score determines if and what automatic mitigation action is needed to keep a device and its data protected.</li> <li>» No Personal Information is processed by or stored in the Engine.</li> </ul>

## Contents

<b>Chapter 1 Preparing the UEM Platform for Integration</b>	<b>1</b>
<i>Prerequisites</i>	1
<i>Microsoft Azure Intune Portal</i>	2
<i>Creating a User Group</i>	2
<i>Adding Users</i>	8
<i>Enrolling Devices to Microsoft Intune</i>	11
<i>Creating an Administrator Account (optional)</i>	11
<i>Creating a Mitigation Process</i>	13
Creating an Android Compliance Policy	13
<b>Chapter 2 Configuring the SandBlast Mobile Dashboard UEM Integration Settings</b>	<b>17</b>
<i>Prerequisites</i>	17
<i>Configuring Device Management Integration Settings</i>	18
MDM Advanced Settings	21
<b>Chapter 3 Configuring the UEM Platform</b>	<b>23</b>
<i>Enabling the MTD Connector in Microsoft Intune Portal</i>	24
<i>Configuring the UEM to Deploy the SandBlast Mobile Protect app</i>	26
Prerequisites	26
Adding the SandBlast Mobile Protect App to Your App Catalog	26
<i>Adding SandBlast Mobile Protect app for Android Devices</i>	26
<i>Adding SandBlast Mobile Protect app for iOS Devices</i>	34
Adding Microsoft Authenticator app for iOS Devices	40
Adding an iOS Configuration Policy for SandBlast Mobile Protect	45
<b>Chapter 4 Registering Devices to SandBlast Mobile</b>	<b>51</b>
<i>Registration of an iOS Device</i>	52
<i>Registration of an Android Device</i>	55
<b>Chapter 5 Testing High Risk Activity Detection and Policy Enforcement</b>	<b>57</b>
<i>Blacklisting a Test App</i>	58
<i>View of Device at Risk</i>	59
SandBlast Mobile Protect App Notifications	59
Microsoft Intune Company Portal Notification	59
<i>Administrator View on the SandBlast Mobile Dashboard</i>	60
<i>Administrator View on the Microsoft Intune Portal</i>	61
<b>Appendices</b>	<b>63</b>
<i>Integration Information</i>	63



## Preparing the UEM Platform for Integration

This chapter discusses the following:

Prerequisites .....	1
Microsoft Azure Intune Portal .....	2
Creating a User Group .....	2
Adding Users .....	8
Enrolling Devices to Microsoft Intune .....	11
Creating an Administrator Account (optional) .....	11
Creating a Mitigation Process .....	13
<i>Creating an Android Compliance Policy .....</i>	<i>13</i>

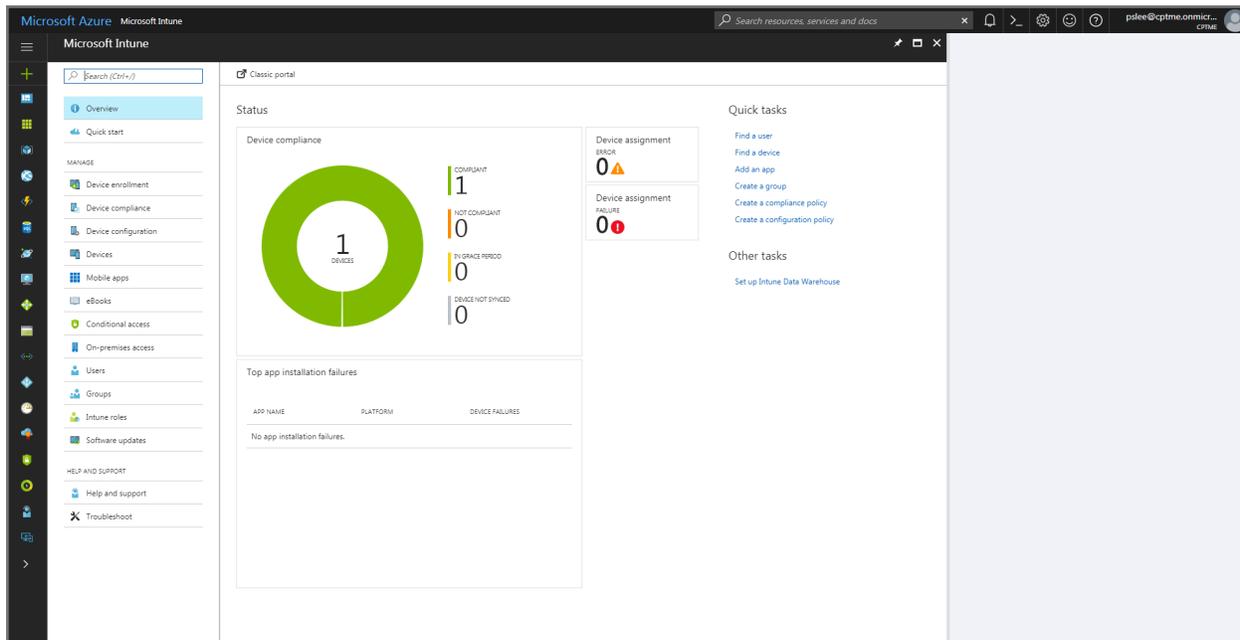
### Prerequisites

1. Microsoft Intune in Azure Portal
2. Configure Intune for MDM Authority  
<https://docs.microsoft.com/en-us/intune/mdm-authority-set#set-mdm-authority-to-intune>
3. Microsoft Intune must be configured with an Apple Push Certificate (APNS)  
<https://docs.microsoft.com/en-us/intune/apple-mdm-push-certificate-get>
4. For Active Directory integration, users to be registered to SandBlast Mobile must belong to Security Group(s) to be tied to SandBlast Mobile. See "Creating a User Group" on the next page

# Chapter 1

## Microsoft Azure Intune Portal

1. Login to your Microsoft Azure Portal and launch Microsoft Intune.



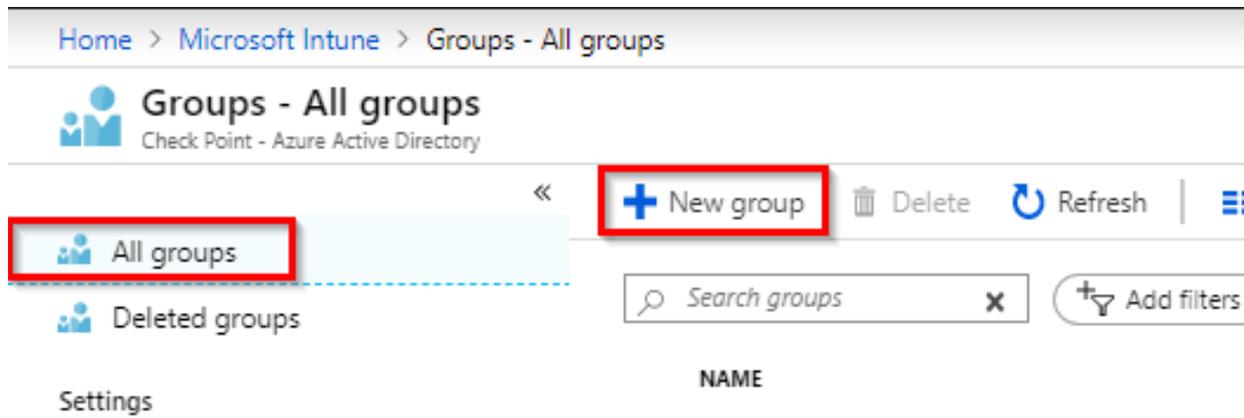
### Creating a User Group

To deploy policies, configurations, apps, etc. in Microsoft Intune, we must create a delivery group that will contain the users whose devices will be registered to SandBlast Mobile.

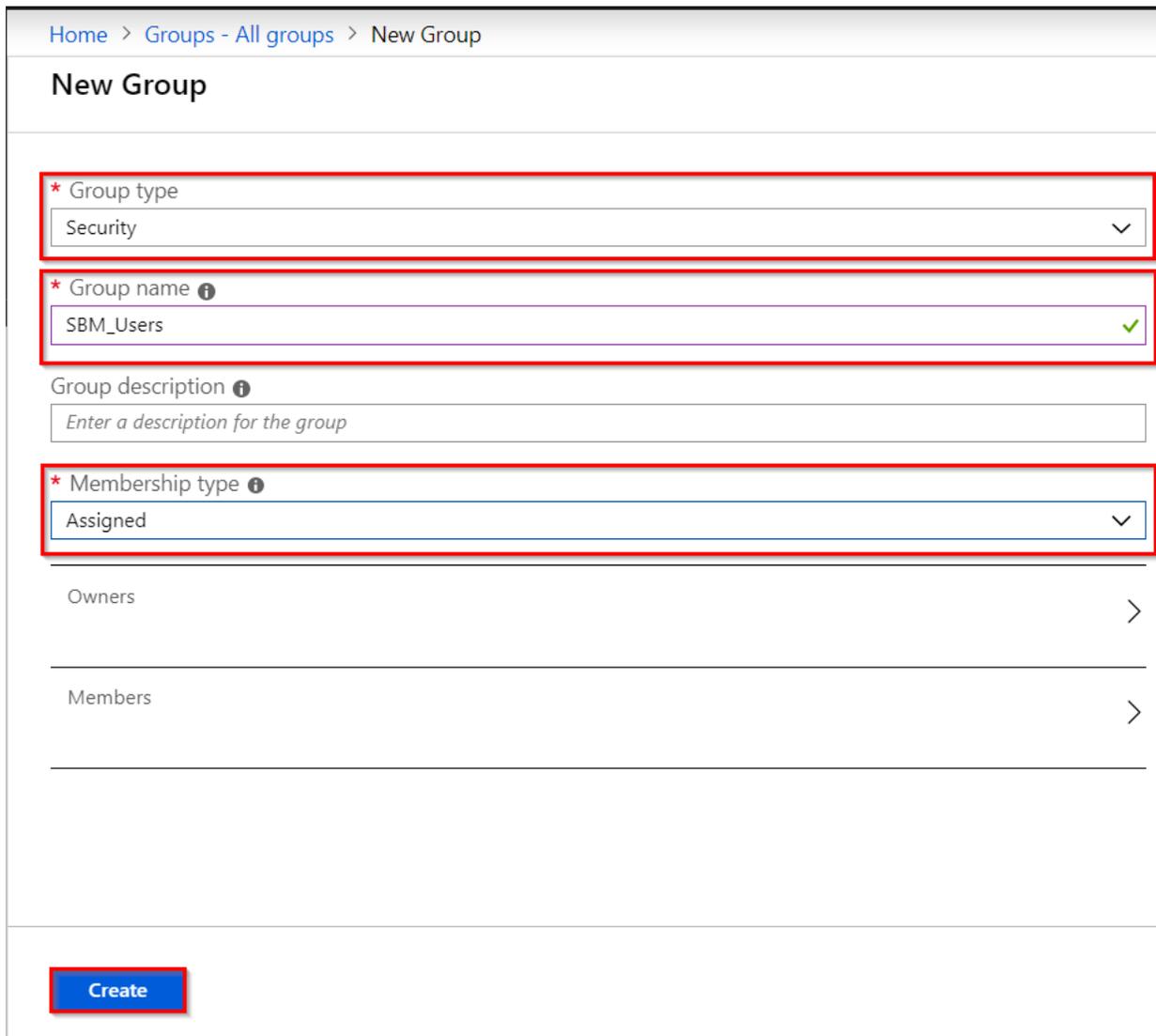
For more information about User Groups and License assignment in Microsoft Intune, please see the following links:

- >> <https://docs.microsoft.com/en-us/intune/groups-add>
- >> <https://docs.microsoft.com/en-us/intune/licenses-assign>

1. Navigate to **Groups > All groups**, and click "+ New group".



2. Select a Group type of Security, type a name for the group, and select a Membership type of Assigned.



Home > 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

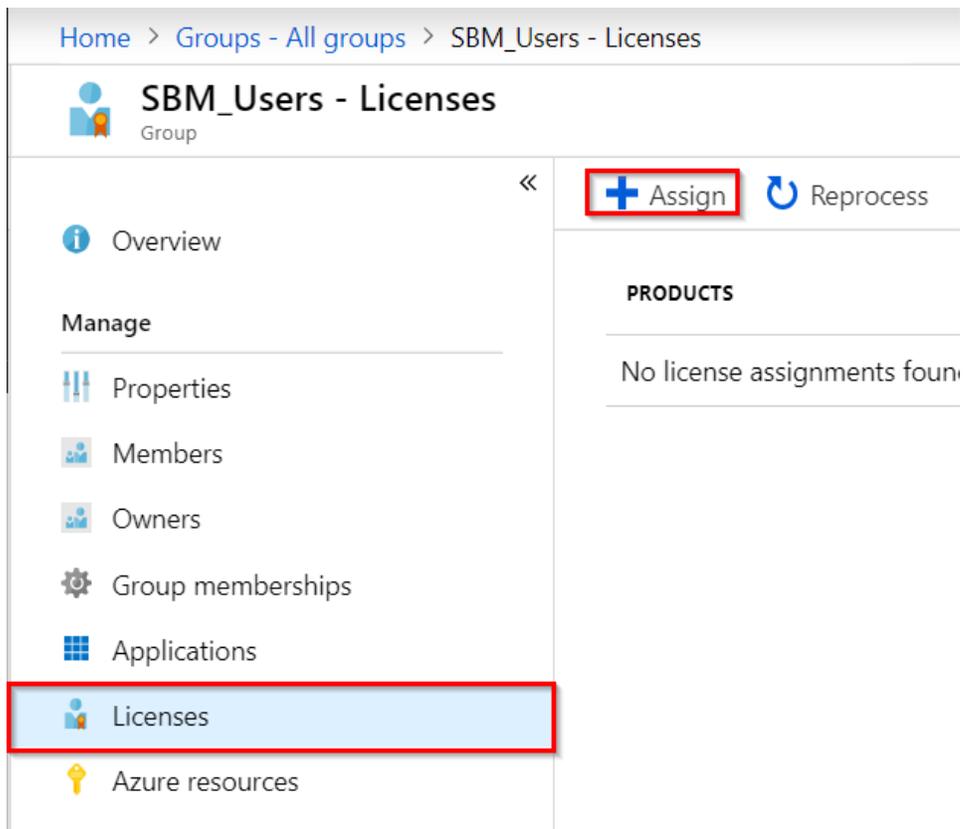
Owners >

Members >

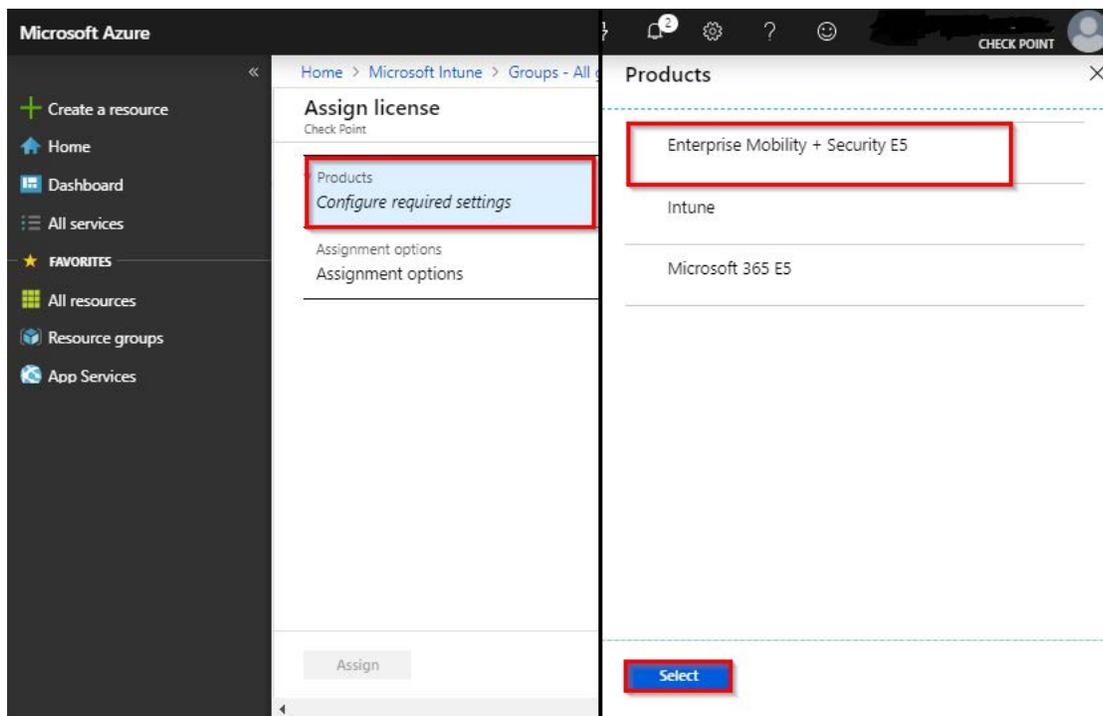
**Create**

3. Click "Create".

- Now we need to assign the EM+S license to this group so that any user added to this group will automatically be eligible to enroll their device to Microsoft Intune.
- Select the "Licenses" tab, and click "+ Assign".

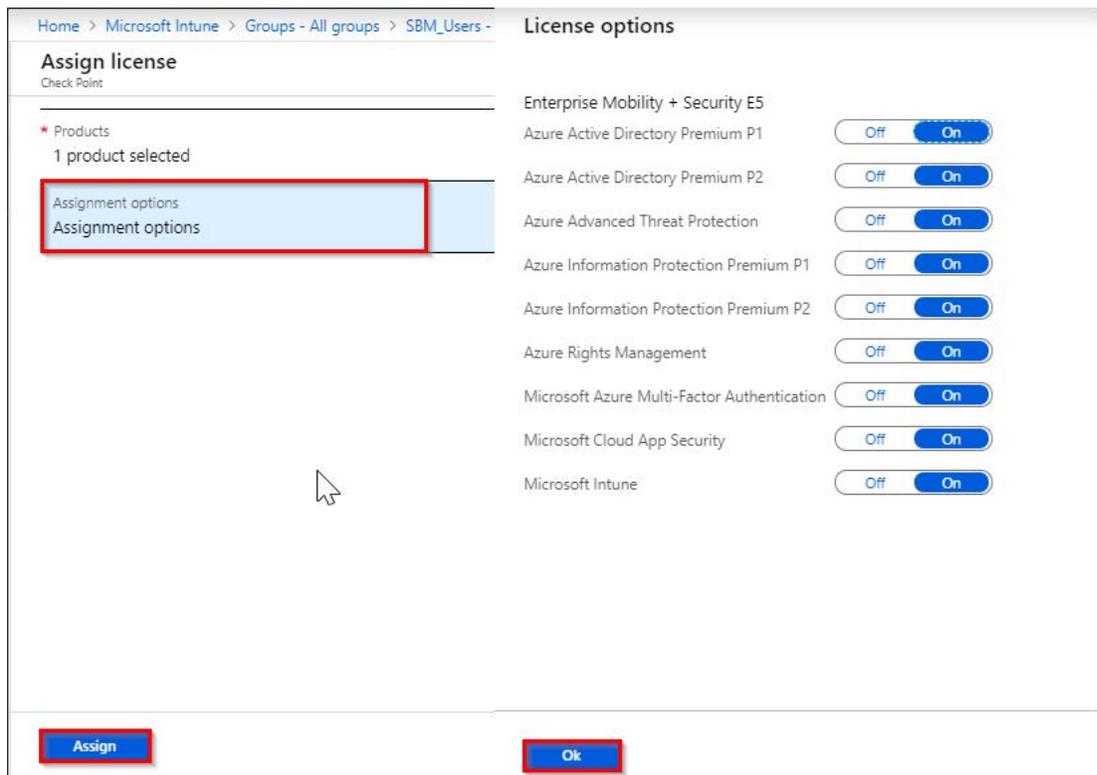


6. Select the "Products" tab, and select "Enterprise Mobility + Security".



7. Click "Select".

8. Select the "Assignment options" tab, and click "Ok".

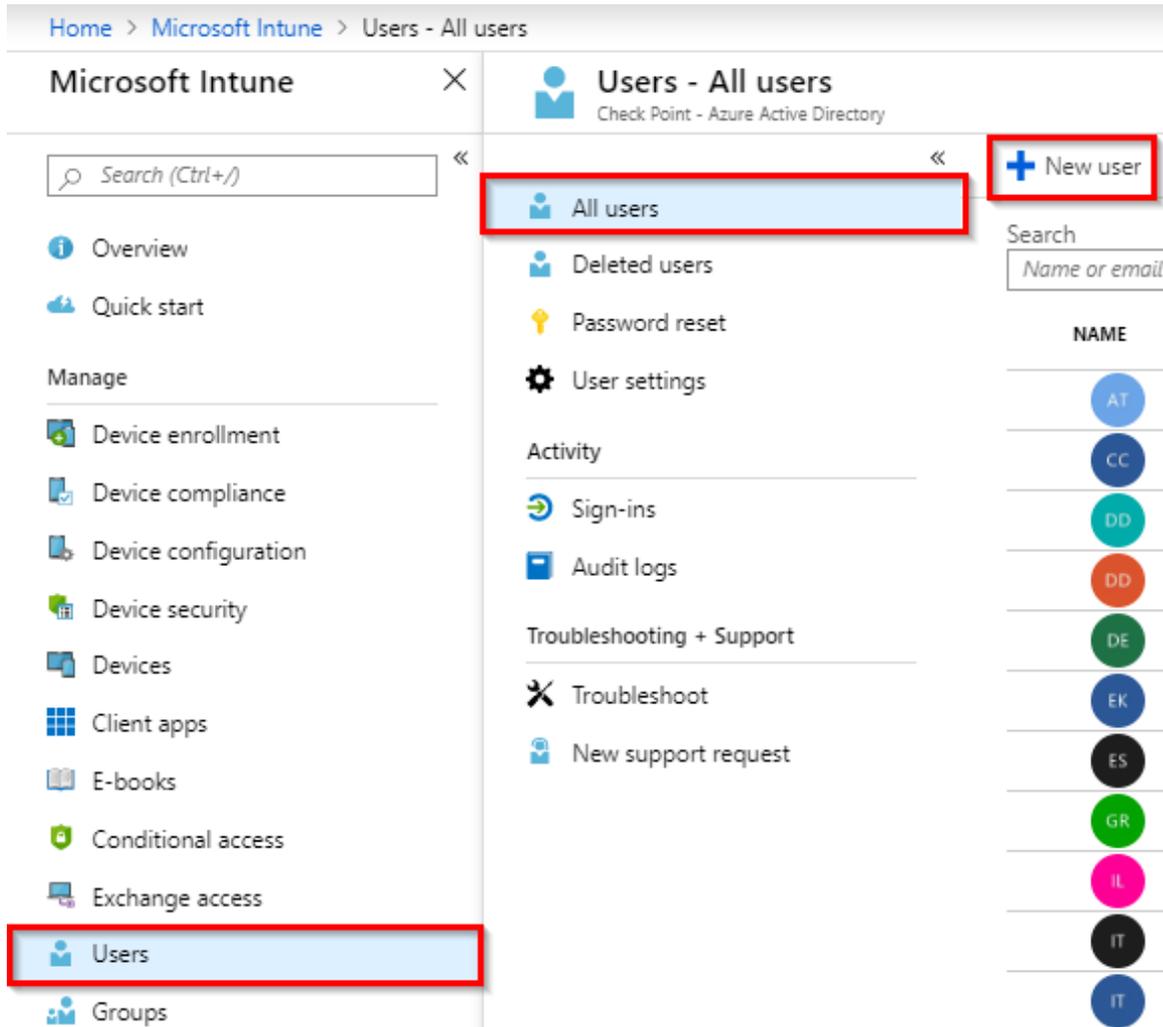


9. Click "Assign".

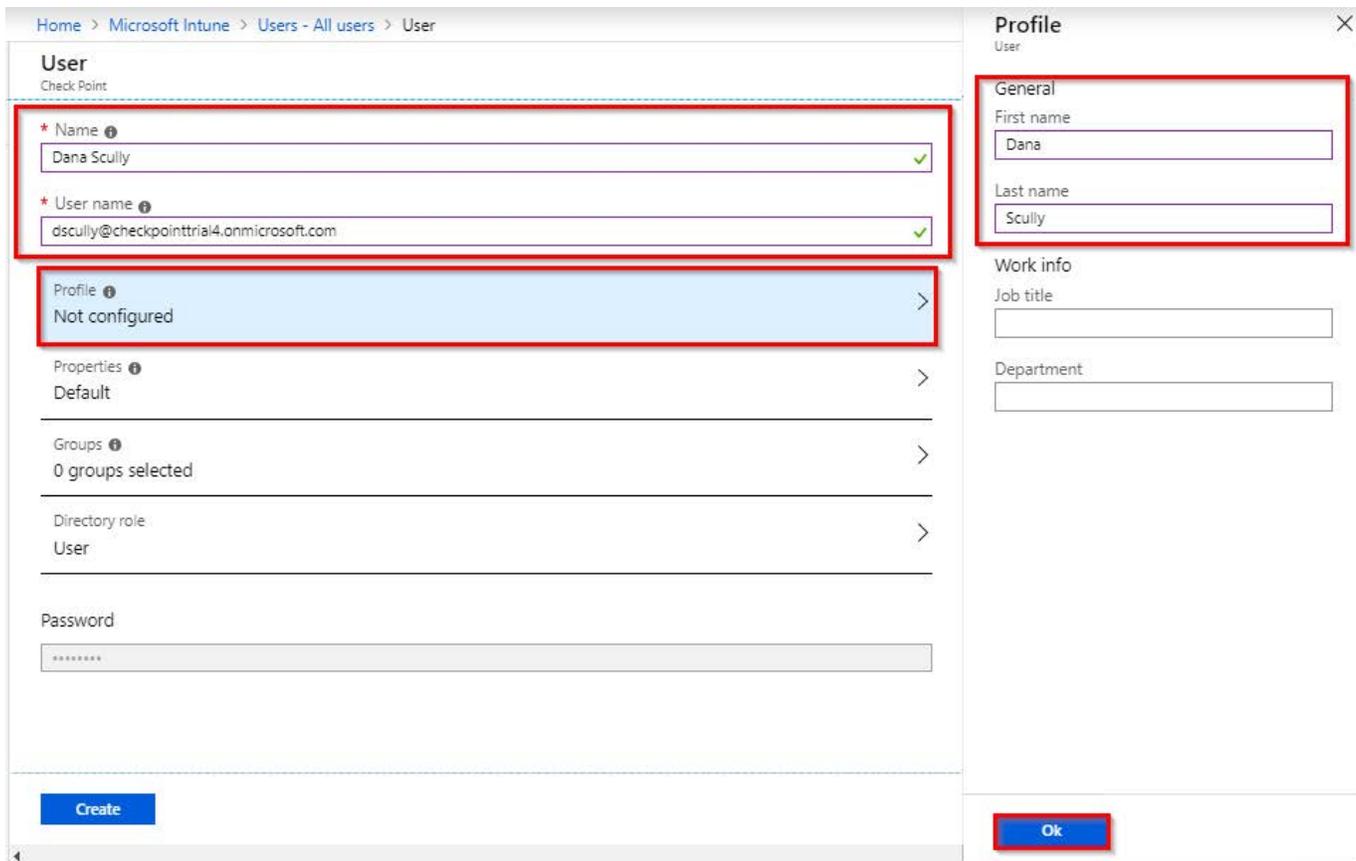
## Adding Users

For more information about Adding Users in Microsoft Intune, please see <https://docs.microsoft.com/en-us/intune/users-add>.

1. Navigate to **Users > All users**, and click "+ New user".



2. Enter in a name and the user name in the form of an email address.
3. Select the Profile tab, and enter in a First name and Last name, if desired.



Home > Microsoft Intune > Users - All users > User

### User

Check Point

\* Name   
Dana Scully ✓

\* User name   
dscully@checkpointtrial4.onmicrosoft.com ✓

Profile   
Not configured >

Properties   
Default >

Groups   
0 groups selected >

Directory role   
User >

Password  
\*\*\*\*\*

**Create**

### Profile

User

General

First name  
Dana

Last name  
Scully

Work info

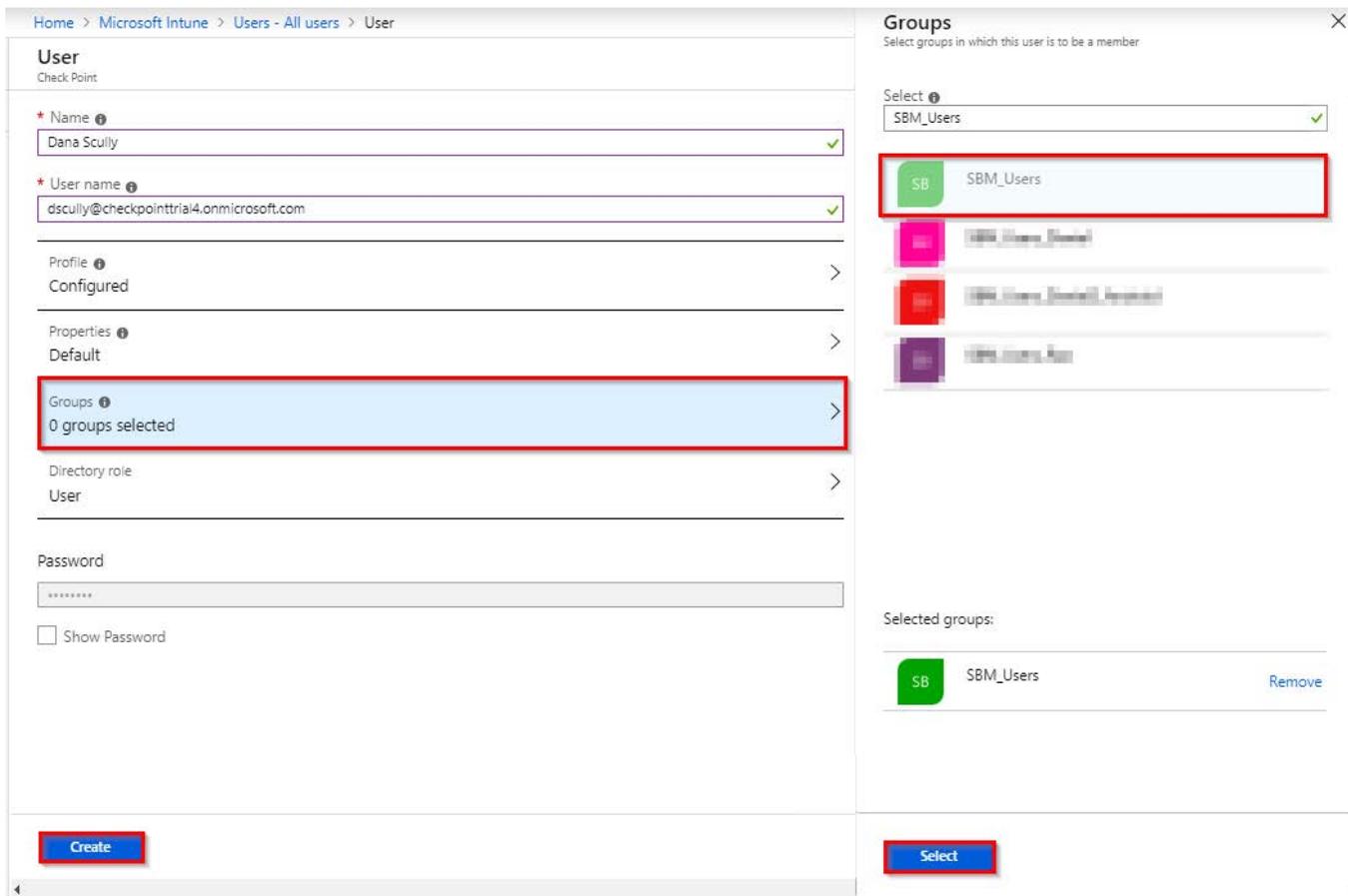
Job title  
\_\_\_\_\_

Department  
\_\_\_\_\_

**Ok**

4. Click "Ok".

5. Select the "Groups" tab, and select the group we created in "Creating a User Group" on page 2.



- 6. Click "Select"
- 7. Click "Create"

**Note:** Repeat these steps to add additional users.

## Enrolling Devices to Microsoft Intune

Visit <https://docs.microsoft.com/en-us/intune/device-enrollment> for details on device enrollment to Microsoft Intune.

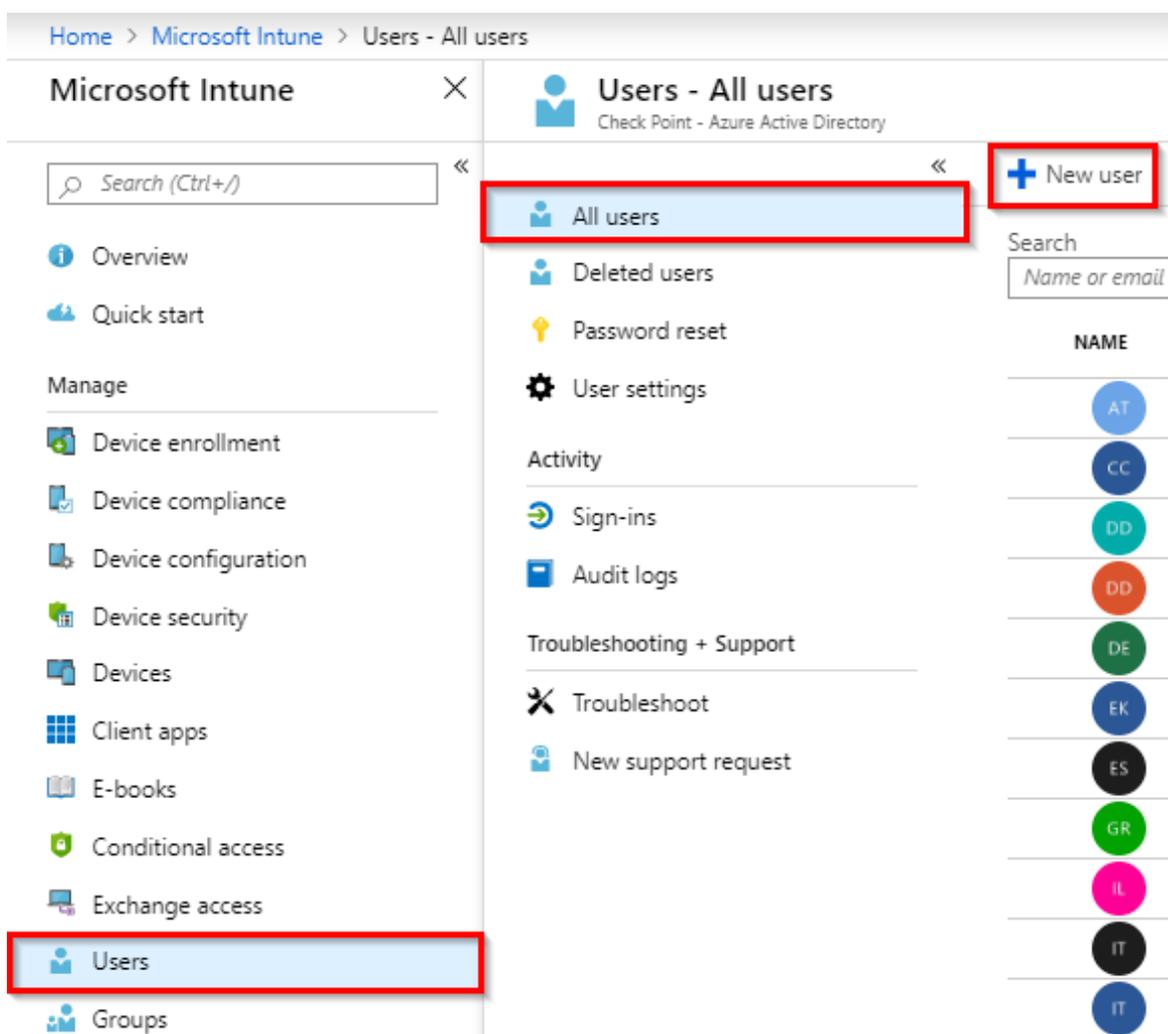
### Creating an Administrator Account (optional)

For integration from SandBlast Mobile to Microsoft Intune, we will create an administrator account for use for integration.

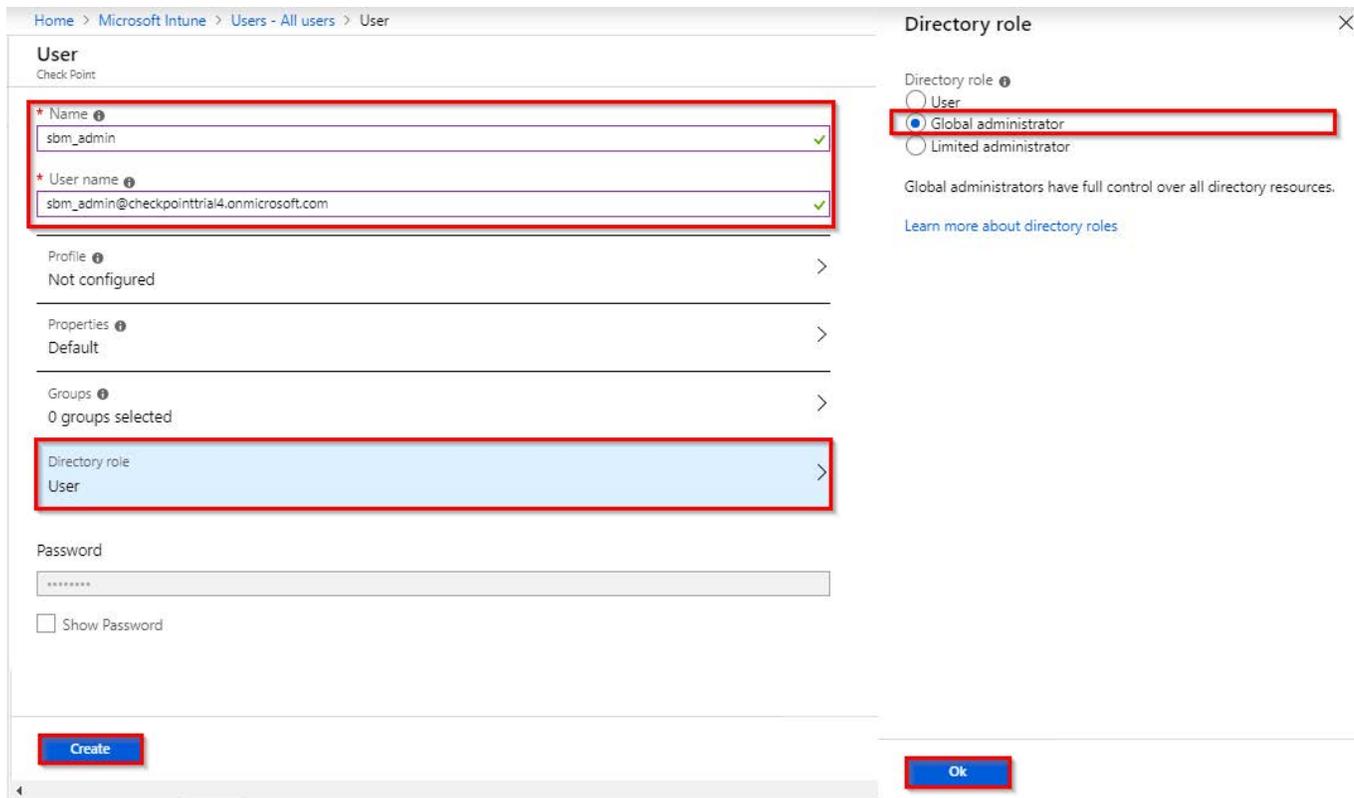
For more information about adding Admin accounts to Microsoft Intune, please see <https://docs.microsoft.com/en-us/intune/users-add#grant-admin-permissions>.

**Note:** It is a best practice to create such an admin account, but is optional.

1. Navigate to **Users > All users**, click "+ New user".



2. Enter in a username, such as sbm\_admin and the email address, such as in our example sbm\_admin@checkpointtrial4.onmicrosoft.com.
3. Click "Directory role" tab, and select "Global administrator".



Home > Microsoft Intune > Users - All users > User

### User

Check Point

\* Name  ✓

\* User name  ✓

Profile  >

Properties  >

Groups  >

Directory role  >

Password

Show Password

### Directory role

Directory role  >

User

Global administrator

Limited administrator

Global administrators have full control over all directory resources.

[Learn more about directory roles](#)

4. Click "Ok".
5. Click "Create".

## Creating a Mitigation Process

In this last step, we will create the start of a compliance policy.

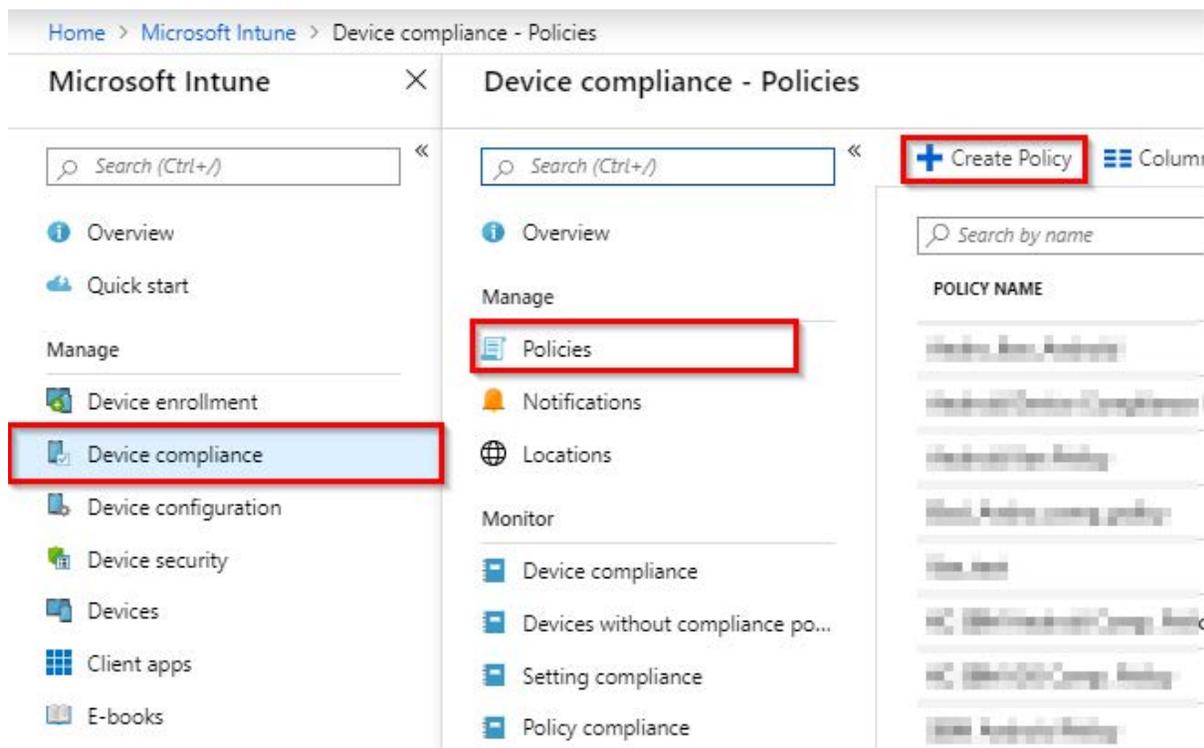
For more information about Compliance Policies in Microsoft Intune, please visit:

- » <https://docs.microsoft.com/en-us/intune/mtd-device-compliance-policy-create>
- » <https://docs.microsoft.com/en-us/intune/device-compliance-get-started>
- » <https://docs.microsoft.com/en-us/intune/compliance-policy-create-android>
- » <https://docs.microsoft.com/en-us/intune/compliance-policy-create-ios>

This policy will key off the state change as reported by SandBlast Mobile, and if the level matches, the user's device will be marked as non-compliant. Additional actions can be created within the policy to limit or block the device's access to the corporate network and data when the device is not compliant.

### Creating an Android Compliance Policy

1. Navigate to **Device compliance > Policies**, and click "Create Policy".



2. Fill in the Name field and select the platform to which this policy will be applied.
3. This policy will be for Android devices.
4. Select the Settings tab, and then select the Device Health tab, in the "Require the device to be at or under the Mobile Threat Level" pull-down menu select the level that devices must be at in order to be considered compliant.

The screenshot shows the 'Create Policy' interface for an Android compliance policy. The 'Device Health' section is highlighted, showing the 'Require the device to be at or under the Device Threat Level' dropdown menu set to 'Secured'. Other settings include 'Rooted devices' (Not configured), 'Google Play Protect' (Not configured), 'Google Play Services is configured' (Not configured), 'Up-to-date security provider' (Not configured), 'Threat scan on apps' (Not configured), and 'SafetyNet device attestation' (Not configured).

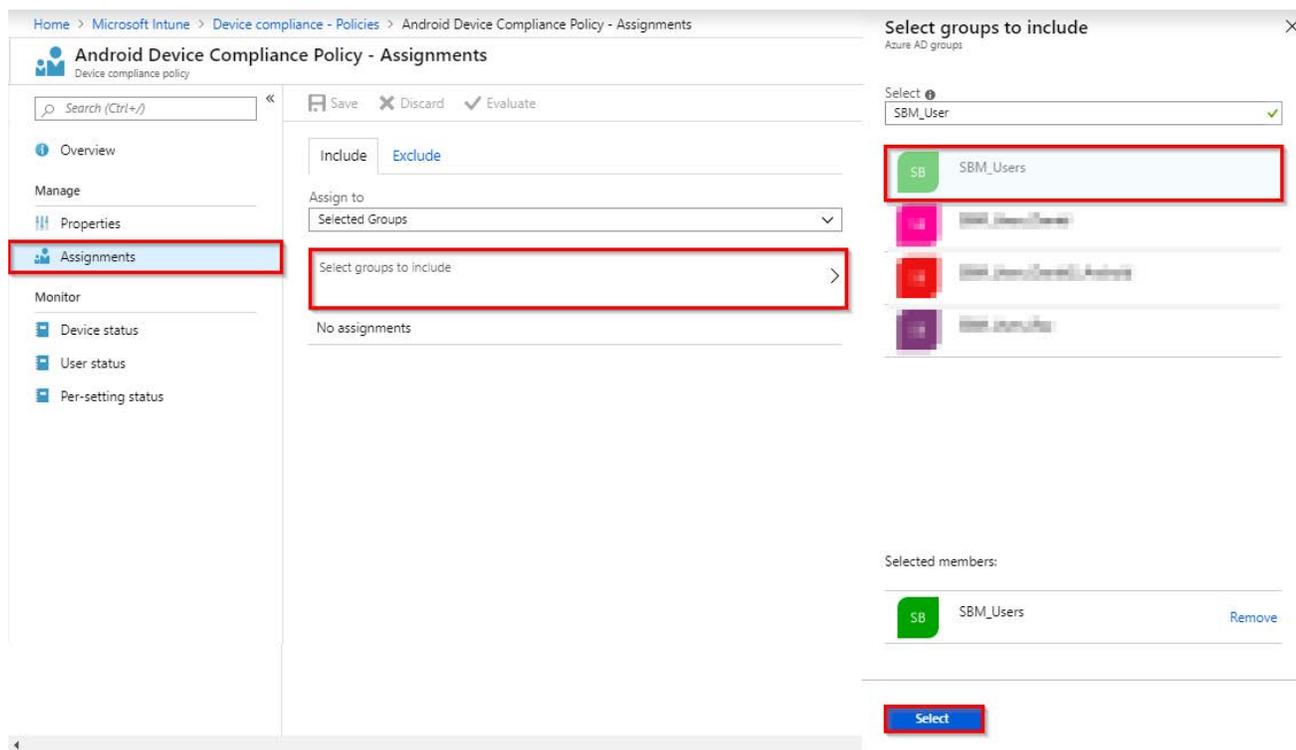
Your choices are: **Secured, Low, Medium, and High.**

The definitions are as follows:

<b>Secured:</b>	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.
<b>Low:</b>	The device is compliant if only low level threats are present. Anything higher puts the device in a non-compliant status.
<b>Medium:</b>	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.
<b>High:</b>	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.

5. We will select Secured.
6. Click "OK".
7. There are additional settings that can be configured under the Device Properties and System Security panels.
8. Click "OK".
9. Then click "Create".

10. While still on the Compliance Policy's panel, select the Assignments tab, and click "Select groups to include" arrow.
11. Select the group you created in "Creating a User Group" on page 2.



12. Click "Select".
13. Click "Save".

**Note:** Repeat these steps to create a similar policy for iOS devices.

**Note:** Now any device in the Security Group ("SBM\_Users") that has any risk level (Low, Medium, or High) set by the SandBlast Mobile system will be Non-Compliant.



## Configuring the SandBlast Mobile Dashboard UEM Integration Settings

This chapter discusses the following:

Prerequisites .....	17
Configuring Device Management Integration Settings .....	18
MDM Advanced Settings .....	21

### Prerequisites

You will need the following details from your Microsoft Intune Deployment:

**Note:** There is a table in "Integration Information" on page 63 that you can record your settings for easy reference.

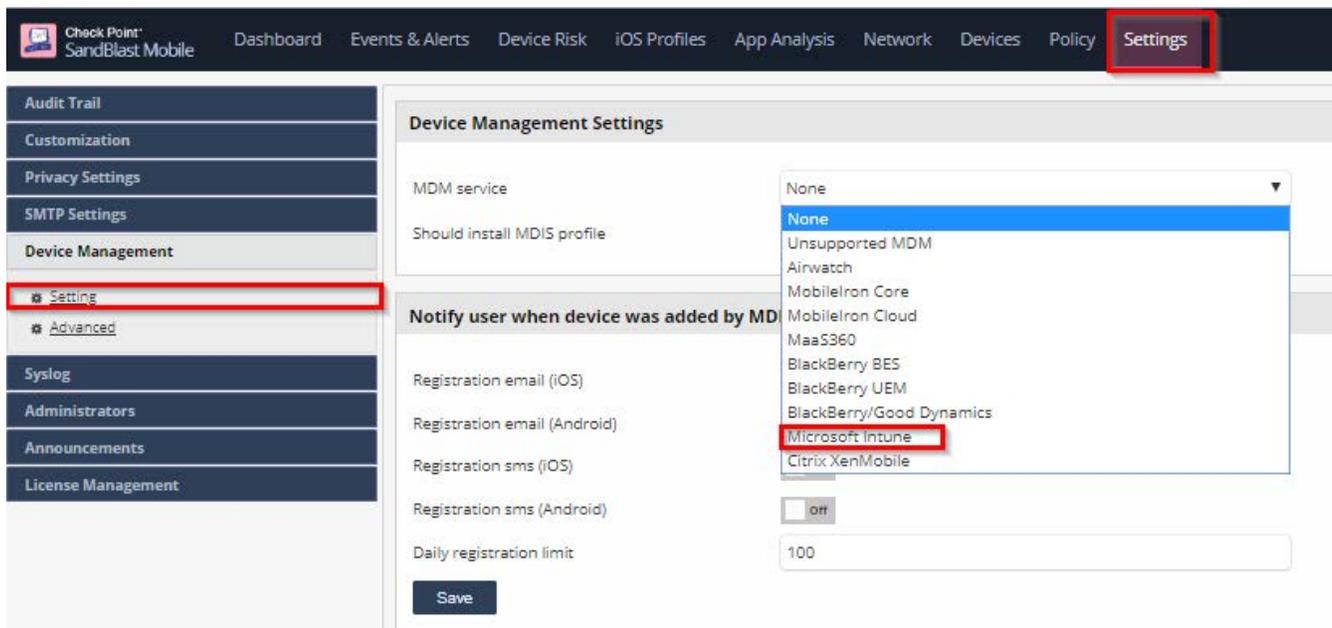
1. **Microsoft Intune Administrative Username and Password:** These are the Admin credentials that the SandBlast Mobile Dashboard will use to connect to the UEM. You may have created a special Admin account in "Creating an Administrator Account (optional)" on page 11 for this purpose.
2. **Security Group(s):** This is the Microsoft Azure AD group(s) to which the users/devices are members, and whose devices will be integrated with the SandBlast Mobile Dashboard. Multiple groups can be integrated with the one SandBlast Mobile Dashboard instance by entering each group name separated with a semicolon (;).
3. Delete any existing devices in the SandBlast Mobile Dashboard.

**Note:** Only the devices are synchronized from Microsoft Intune to the SandBlast Mobile Dashboard, not users. If a user doesn't have a device enrolled, their information will not be synchronized to the SandBlast Mobile Dashboard.

# Chapter 2

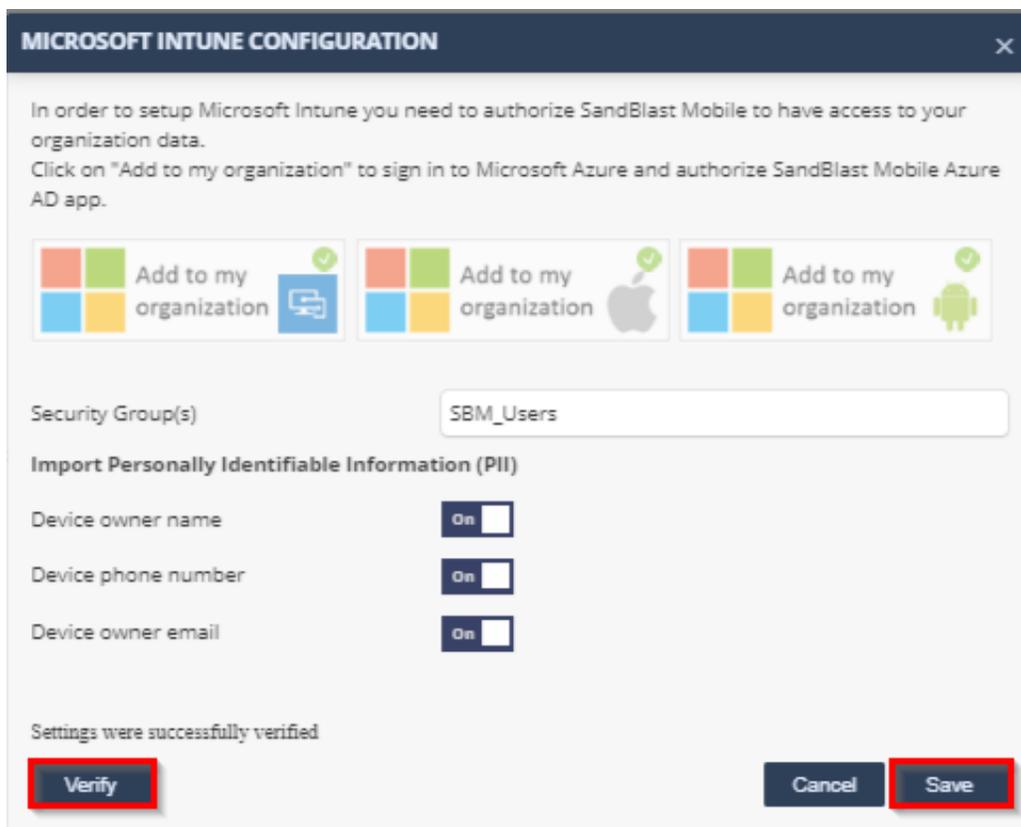
## Configuring Device Management Integration Settings

1. Navigate to **Settings > Device Management > Setting**.
2. Select "Microsoft Intune" from the "MDM service" drop-down menu under the Device Management Settings area.



3. A pop-up window will open.

4. 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.
5. 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..
6. 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..
7. Enter in the Azure Active Directory Security Group(s).



**MICROSOFT INTUNE CONFIGURATION** [X]

In order to setup Microsoft Intune you need to authorize SandBlast Mobile to have access to your organization data.  
Click on "Add to my organization" to sign in to Microsoft Azure and authorize SandBlast Mobile Azure AD app.

 Add to my organization   Add to my organization   Add to my organization 

Security Group(s)

**Import Personally Identifiable Information (PII)**

Device owner name  On

Device phone number  On

Device owner email  On

Settings were successfully verified

8. Click "VERIFY". If the settings are correct, and the SandBlast Mobile Dashboard can communicate with the Microsoft Intune system, you will be able to click "SAVE" to finish configuration.
9. Click "Sync Now" to initiate the MTD Connector association on the Microsoft Intune Portal.

The screenshot displays the 'Device Management Settings' interface. On the left is a navigation menu with options like Audit Trail, Customization, Privacy Settings, SMTP Settings, Device Management (with sub-items Setting and Advanced), Syslog, Administrators, Announcements, and License Management. The main content area is divided into sections:

- Device Management Settings:** Includes a dropdown for 'MDM service' set to 'Microsoft Intune' and a toggle for 'Should install MDIS profile' which is currently 'off'.
- Notify user when device was added by MDM:** Contains several notification toggles (Registration email for iOS and Android, Registration sms for iOS and Android) all set to 'off', and a 'Daily registration limit' input field set to '100'. A 'Save' button is located below these settings.
- Application deployment for MS Intune:** Provides status information (Security Groups: SBM\_Users, Last updated time: Sun, 28 Jul 2019 08:17:41 +0000, Last Microsoft Intune service heartbeat, Sync Status: Synchronization not started) and instructions on how to use the 'Copy' buttons for iOS and Android application settings.

At the bottom of the settings area, there are three buttons: 'Sync Now' (highlighted with a red border), 'Pause Sync', and 'Edit Settings'.

## MDM Advanced Settings

When a UEM Service is configured, the Device Management Advanced Settings are automatically configured based on recommendations of the selected UEM provider, in this case from Microsoft Intune.

1. Navigate to **Settings > Device Management > Advanced**, and make any appropriate changes.

The screenshot shows the Check Point SandBlast Mobile web interface. The top navigation bar includes 'Settings', which is highlighted with a red box. On the left sidebar, under 'Device Management', the 'Advanced' option is also highlighted with a red box. The main content area is titled 'MDM Advanced Settings' and contains four input fields with values: 'Device sync interval' (10), 'Device deletion threshold' (10), 'Deletion delay interval' (0.5), and 'App sync interval' (10). Each field has a help icon (question mark) to its right. A 'Save' button is located below the input fields.

Setting	Description
<b>Device sync interval</b>	Interval to connect with UEM to sync devices. Values: 10-1440 minutes, in 10 minute intervals
<b>Device deletion threshold</b>	Percentage of devices allowed for deletion after UEM device sync. 100% for no threshold
<b>Deletion delay interval</b>	Delay device deletion after sync – device will not be deleted if it will be re-sync from UEM during the threshold interval. Values: 0-48 hours
<b>App sync interval</b>	Interval to connect with UEM to sync app list. Values: 10-1440 minutes, in 10 minute intervals

**Note:** If you make changes to the default settings, click "Save" to have changes take effect.



## Configuring the UEM Platform

Now that we have completed the integration steps, we can continue with the configuration of the UEM platform.

For this process we will return to the Microsoft Azure Intune Portal to complete the configuration.

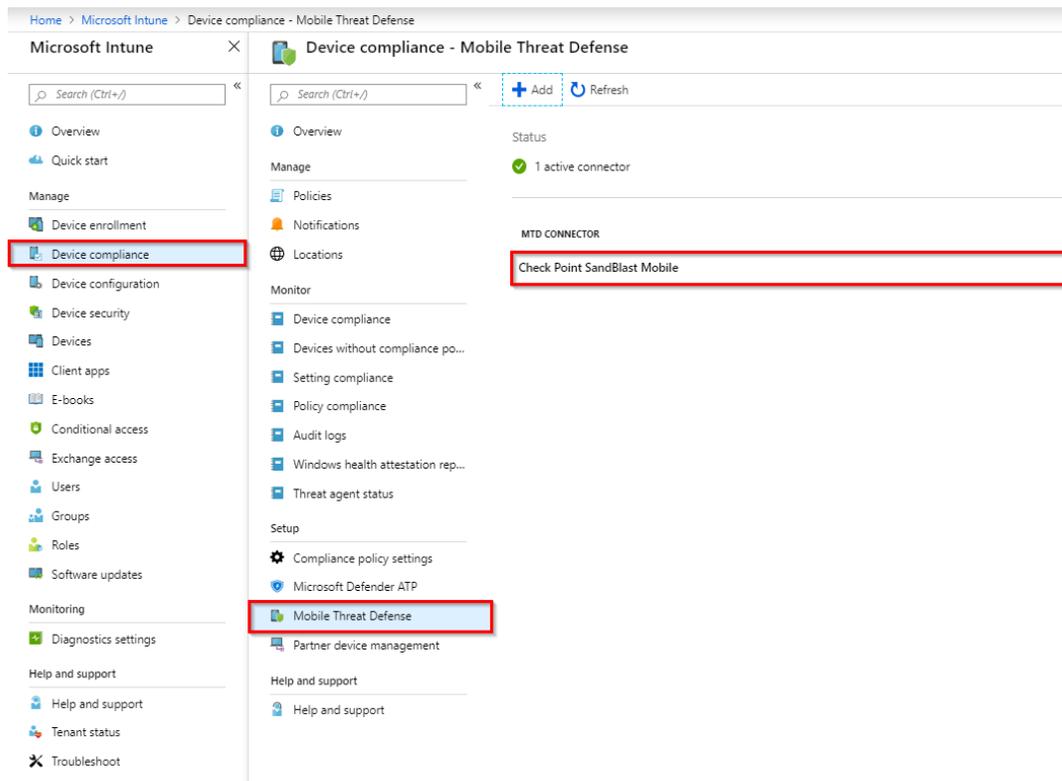
This chapter discusses the following:

<b>Enabling the MTD Connector in Microsoft Intune Portal</b> .....	<b>24</b>
<b>Configuring the UEM to Deploy the SandBlast Mobile Protect app</b> .....	<b>26</b>
<i>Prerequisites</i> .....	<b>26</b>
<i>Adding the SandBlast Mobile Protect App to Your App Catalog</i> .....	<b>26</b>
Adding SandBlast Mobile Protect app for Android Devices .....	<b>26</b>
Adding SandBlast Mobile Protect app for iOS Devices .....	<b>34</b>
<i>Adding Microsoft Authenticator app for iOS Devices</i> .....	<b>40</b>
<i>Adding an iOS Configuration Policy for SandBlast Mobile Protect</i> .....	<b>45</b>

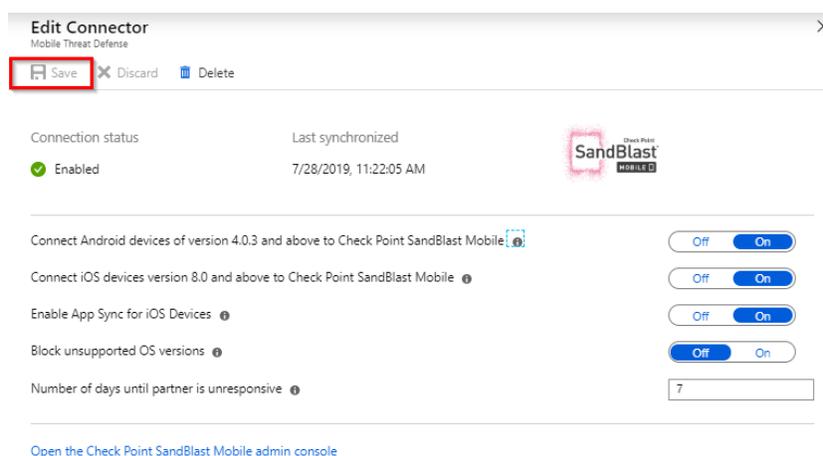
# Chapter 3

## Enabling the MTD Connector in Microsoft Intune Portal

1. In the Microsoft Intune Portal, navigate to **Device Compliance > Mobile Threat Defense**.



2. Click on the "Check Point SandBlast Mobile" entry and turn on "Connect Android devices to Check Point SandBlast Mobile", "Connect iOS devices to Check Point SandBlast Mobile", and "Enable App Sync for iOS Devices".



3. Click "Save".

#### 4. Check Point SandBlast Mobile MTD Connector is now enabled.

**Device compliance - Mobile Threat Defense**

Search (Ctrl+/) « + Add Refresh

**Overview**

Status

✔ 1 active connector

MTD CONNECTOR	STATUS	ENABLED PLATFORMS
Check Point SandBlast Mobile	✔ Enabled	Android, iOS

**Manage**

- Policies
- Notifications
- Locations

**Monitor**

- Device compliance
- Devices without compliance po...
- Setting compliance
- Policy compliance
- Audit logs
- Windows health attestation rep...
- Threat agent status

## Configuring the UEM to Deploy the SandBlast Mobile Protect app

### Prerequisites

1. SandBlast Mobile Dashboard configured integration with Microsoft Intune without errors.
2. SandBlast Mobile Protect app logo/icon from Google Play saved locally on your hard drive  
<https://play.google.com/store/apps/details?id=com.lacoon.security.fox>

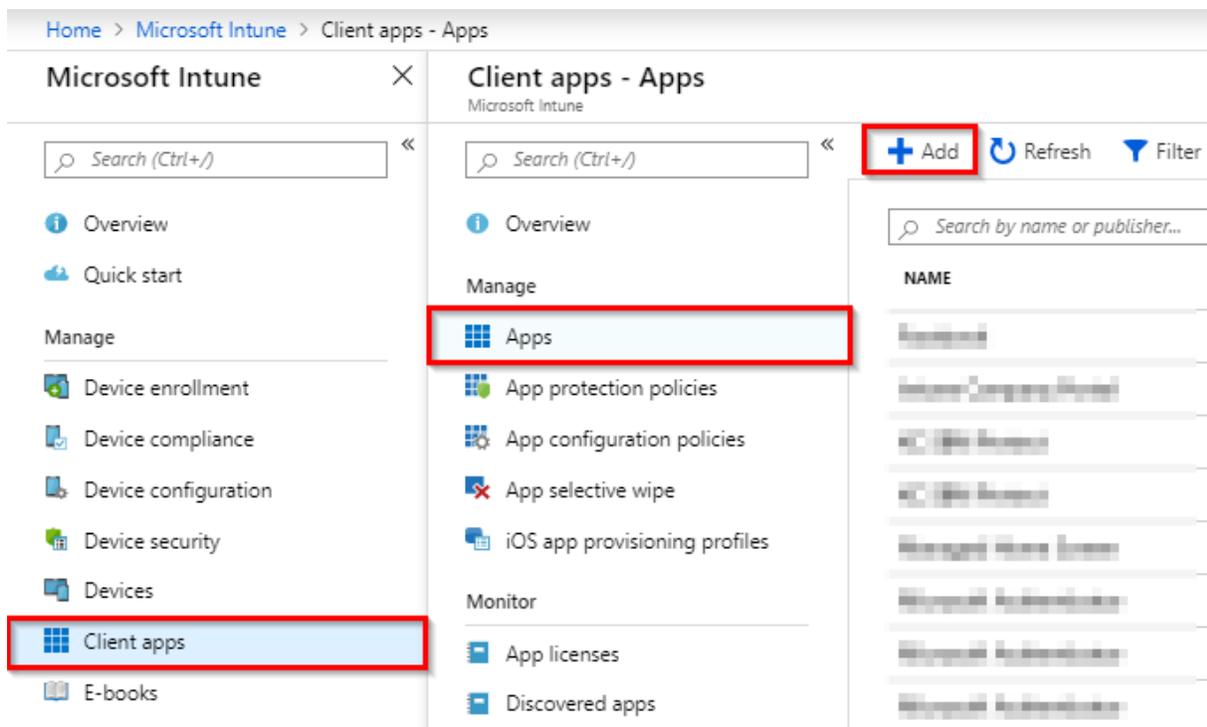
### Adding the SandBlast Mobile Protect App to Your App Catalog

We will need to add the Protect App for both iOS and Android operating systems, as well as the Microsoft Authenticator app for iOS devices, which is needed to provide Single Sign-On (SSO) functionality to SandBlast Mobile Protect on iOS devices.

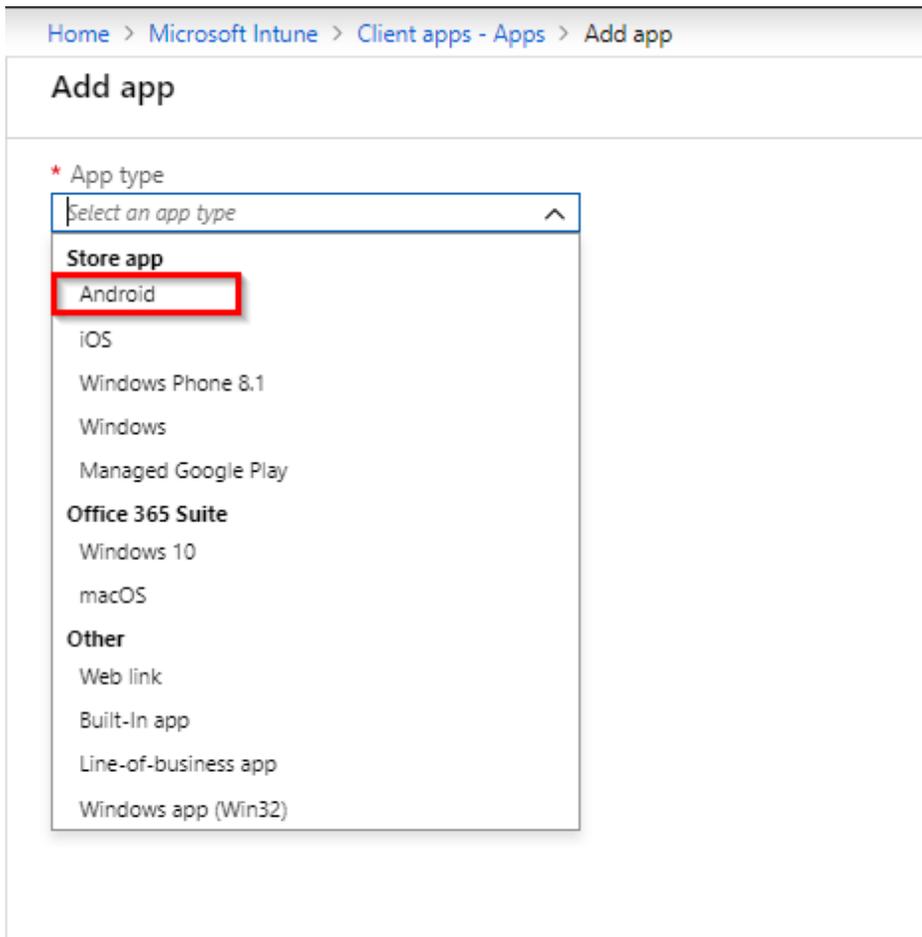
For more information about Adding Apps to the Microsoft Intune App Catalog, please visit:  
<https://docs.microsoft.com/intune/deploy-use/deploy-apps-in-microsoft-intune>

### Adding SandBlast Mobile Protect app for Android Devices

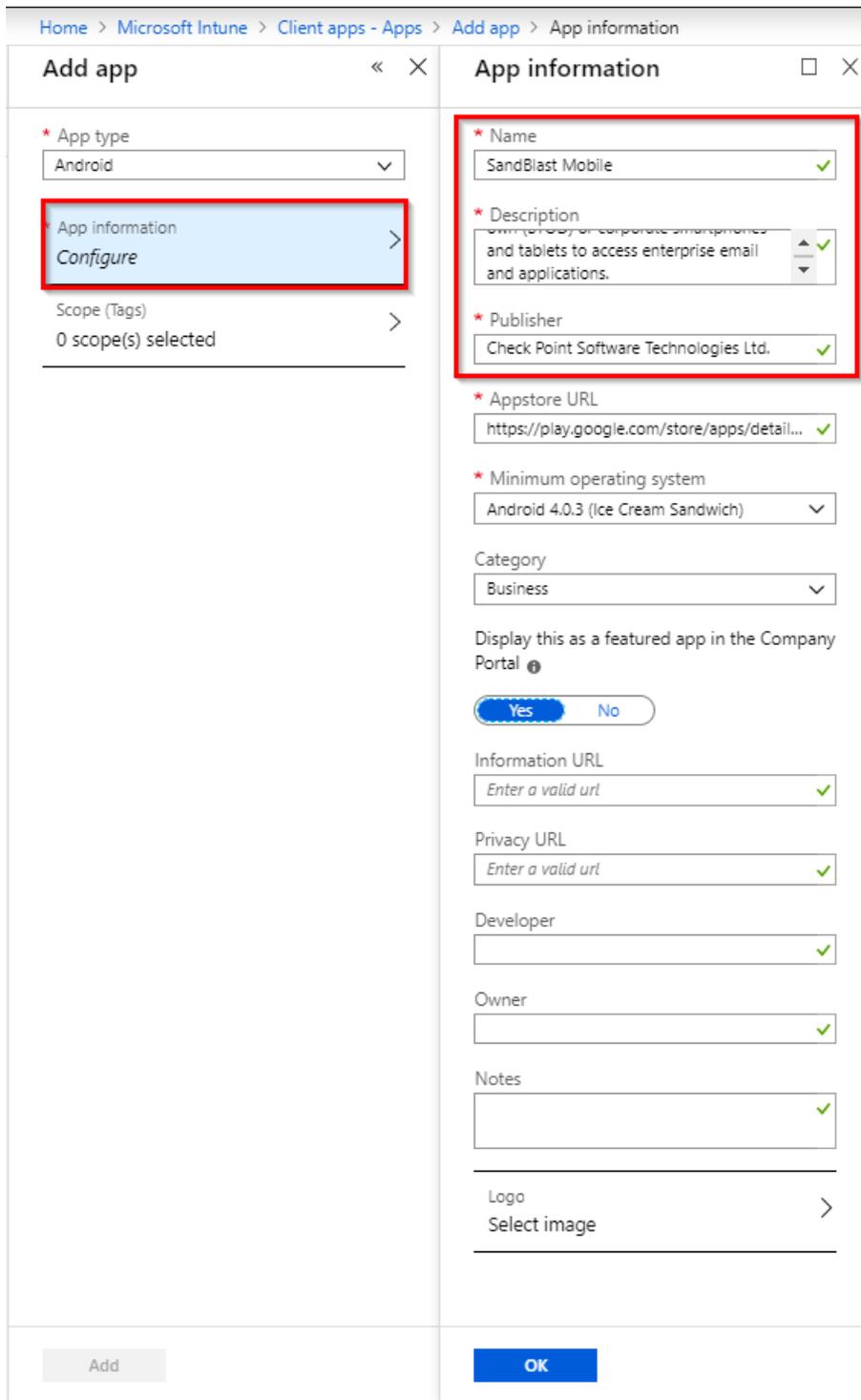
1. Navigate to **Client apps > Apps**, and click "+ Add".



2. In the Add App panel, select the type of "Store app > Android".



3. Select the App information tab.
4. Enter SandBlast Mobile Protect as the name.
5. Enter a description, such what is listed in the app store description.
6. Set the Publisher to Check Point Software Technologies.



Home > Microsoft Intune > Client apps - Apps > Add app > App information

**Add app** « ×

\* App type  
Android ▾

**App information** >  
Configure

Scope (Tags)  
0 scope(s) selected >

**App information** □ ×

\* Name  
SandBlast Mobile ✓

\* Description  
SandBlast Mobile Protect for Android  
and tablets to access enterprise email  
and applications. ✓

\* Publisher  
Check Point Software Technologies Ltd. ✓

\* Appstore URL  
https://play.google.com/store/apps/detail... ✓

\* Minimum operating system  
Android 4.0.3 (Ice Cream Sandwich) ▾

Category  
Business ▾

Display this as a featured app in the Company Portal ⓘ  
**Yes** No

Information URL  
Enter a valid url ✓

Privacy URL  
Enter a valid url ✓

Developer  
✓

Owner  
✓

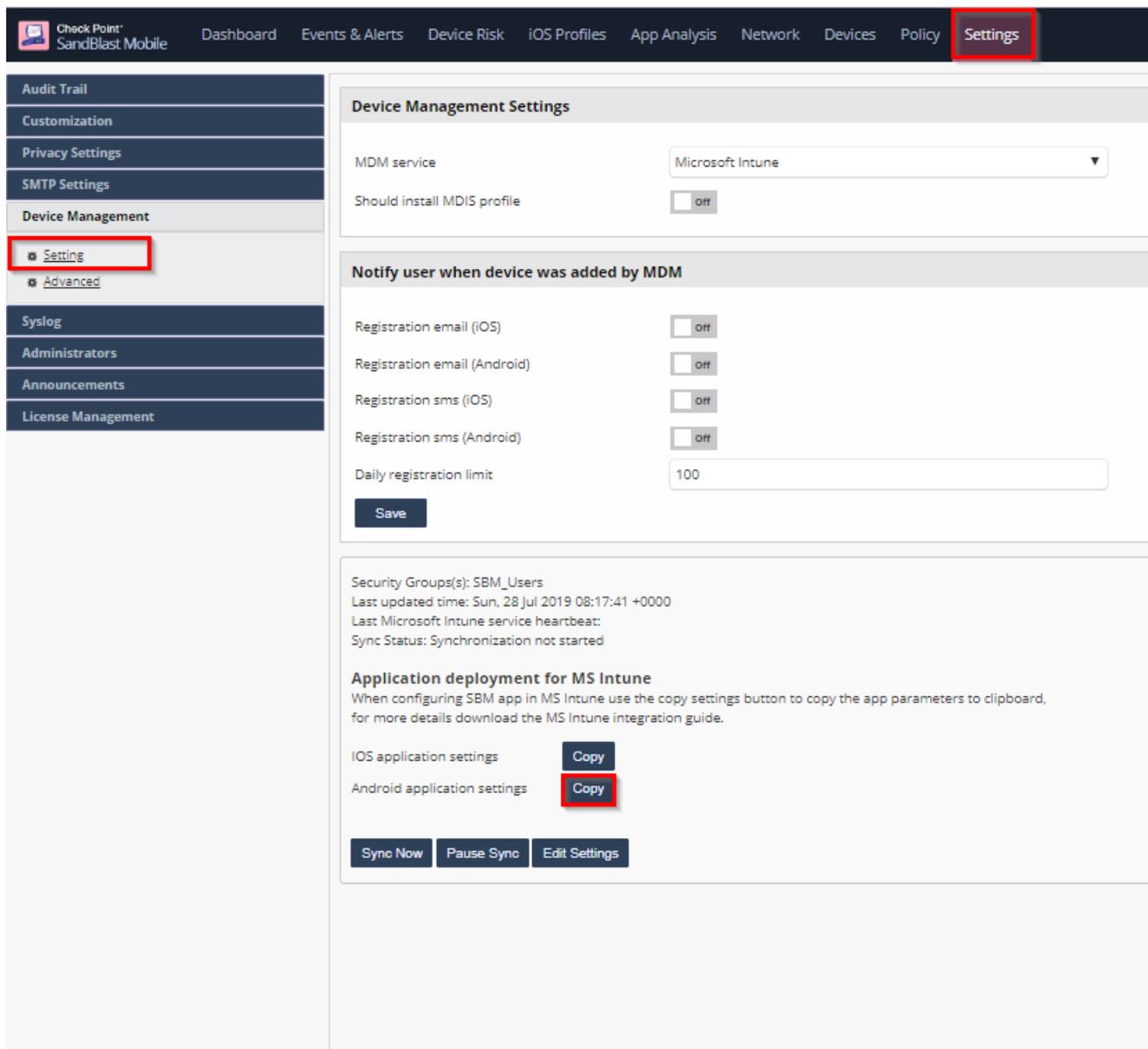
Notes  
✓

Logo  
Select image >

Add

**OK**

7. Get the URL for SandBlast Mobile Protect Android link from the SandBlast Mobile Dashboard under **Settings > Device Management > Setting**.
8. Click "Copy" next to "Android application settings".



Check Point SandBlast Mobile Dashboard

**Settings**

**Device Management Settings**

MDM service: Microsoft Intune

Should install MDIS profile:  off

**Notify user when device was added by MDM**

Registration email (iOS):  off

Registration email (Android):  off

Registration sms (iOS):  off

Registration sms (Android):  off

Daily registration limit: 100

Save

Security Groups(s): SBM\_Users  
Last updated time: Sun, 28 Jul 2019 08:17:41 +0000  
Last Microsoft Intune service heartbeat:  
Sync Status: Synchronization not started

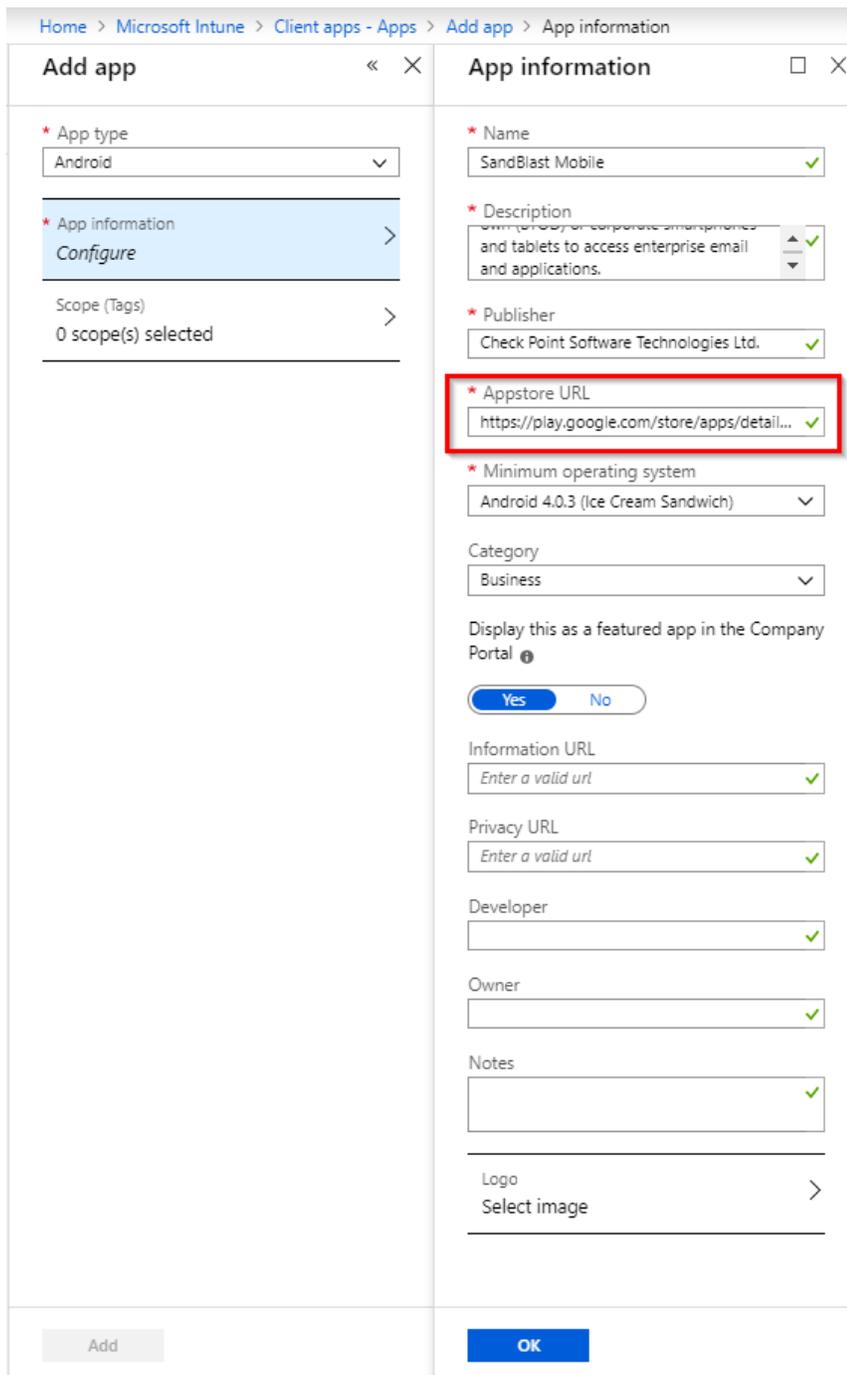
**Application deployment for MS Intune**  
When configuring SBM app in MS Intune use the copy settings button to copy the app parameters to clipboard, for more details download the MS Intune integration guide.

IOS application settings: Copy

Android application settings: **Copy**

Sync Now | Pause Sync | Edit Settings

9. Paste it into the URL field.



Home > Microsoft Intune > Client apps - Apps > Add app > App information

**Add app** « ×

- \* App type: Android
- \* App information: **Configure**
- Scope (Tags): 0 scope(s) selected

**App information** □ ×

- \* Name: SandBlast Mobile ✓
- \* Description: Configure SandBlast Mobile on corporate smartphones and tablets to access enterprise email and applications. ✓
- \* Publisher: Check Point Software Technologies Ltd. ✓
- \* Appstore URL: **https://play.google.com/store/apps/detail...** ✓
- \* Minimum operating system: Android 4.0.3 (Ice Cream Sandwich)
- Category: Business
- Display this as a featured app in the Company Portal: **Yes** No
- Information URL: Enter a valid url ✓
- Privacy URL: Enter a valid url ✓
- Developer: ✓
- Owner: ✓
- Notes: ✓
- Logo: Select image >

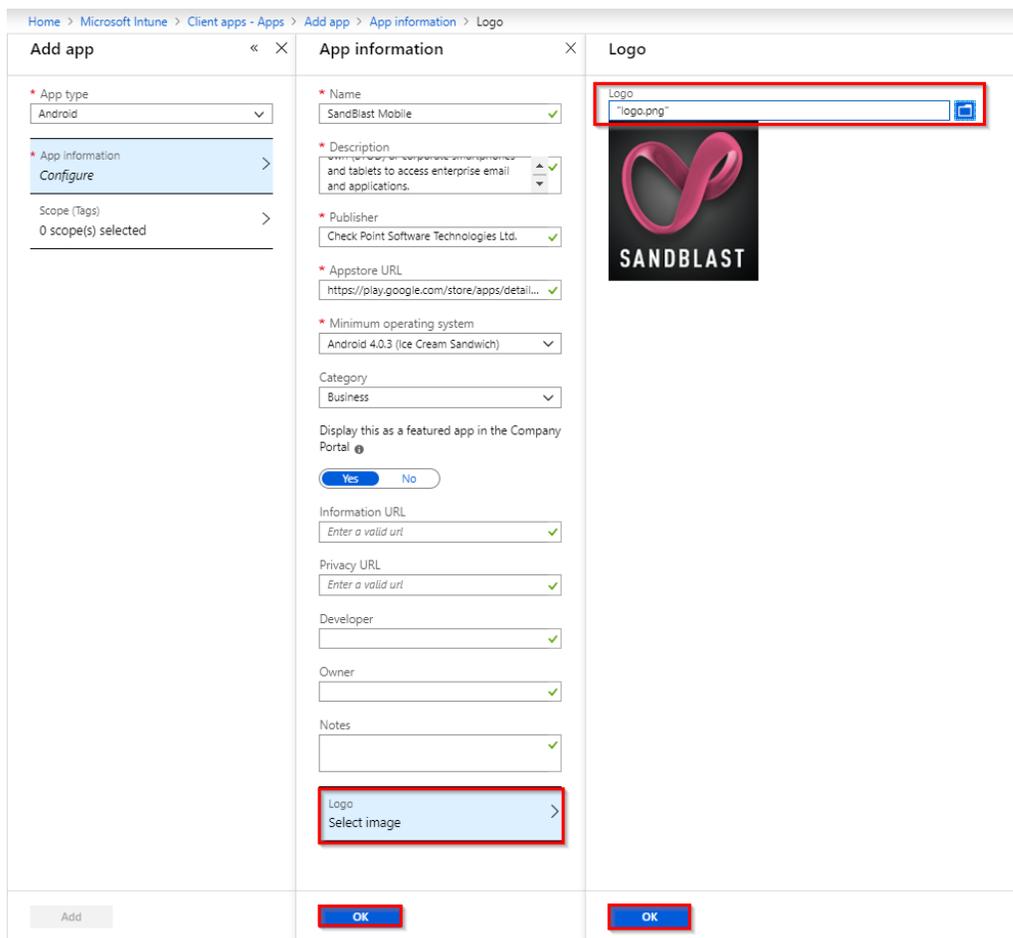
Add OK

10. Select the minimum operating system of Android 4.0.3.

The screenshot shows the 'Add app' configuration interface in Microsoft Intune. The left pane shows the 'Add app' sidebar with 'App information' selected. The right pane shows the 'App information' configuration for 'SandBlast Mobile'. The 'Minimum operating system' dropdown is highlighted with a red box and set to 'Android 4.0.3 (Ice Cream Sandwich)'. Other fields include Name, Description, Publisher, Appstore URL, Category, Information URL, Privacy URL, Developer, Owner, and Notes. The 'Display this as a featured app in the Company Portal' toggle is set to 'Yes'. The 'Add' button is visible at the bottom left, and the 'OK' button is at the bottom right.

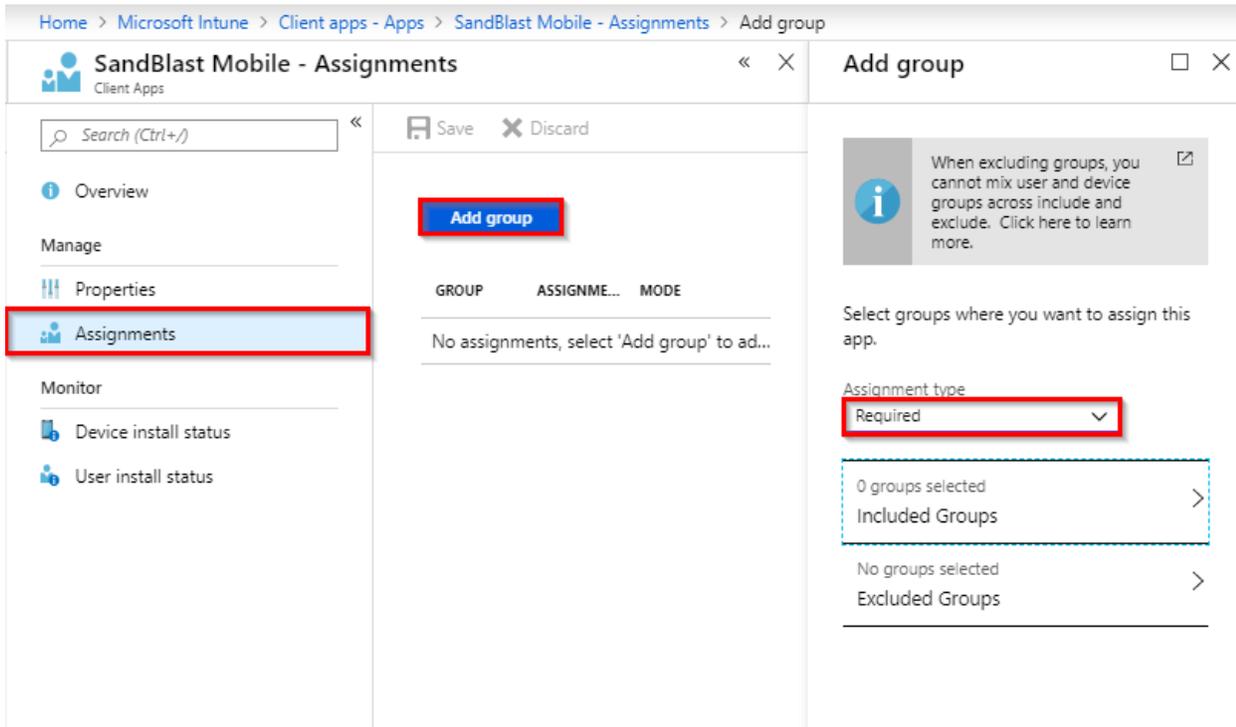
11. Scroll down to Add the logo image.

12. Browse to a local file on your hard drive.

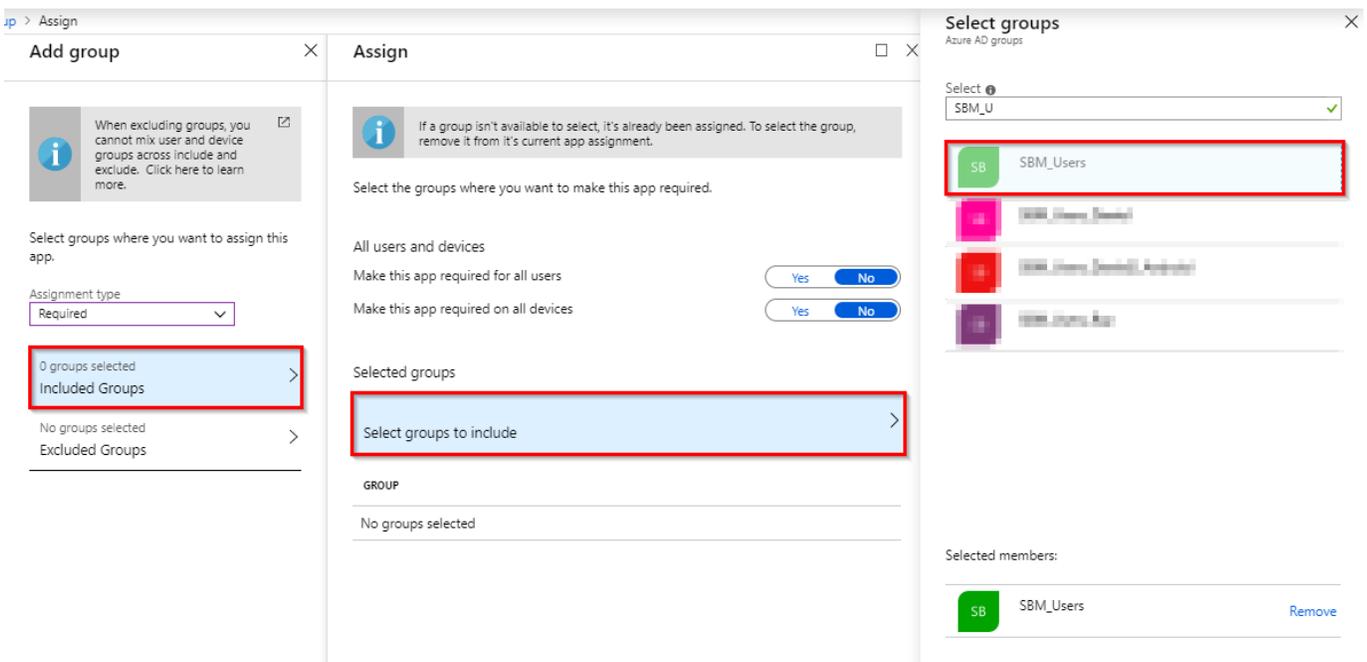


- 13. Click "OK".
- 14. Click "OK".
- 15. Click "Add".

16. Select the Assignments tab, and click "Add group".
17. Set the type to "Required" from the pull-down menu.



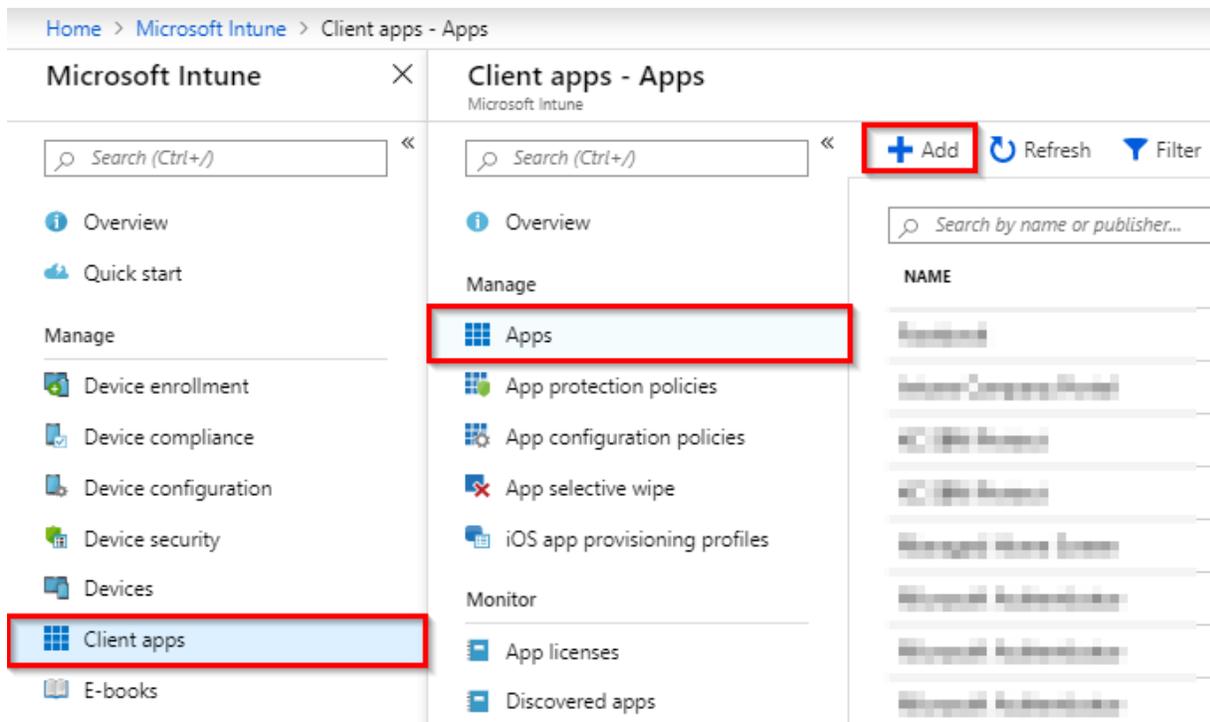
18. Select the appropriate Users Group.



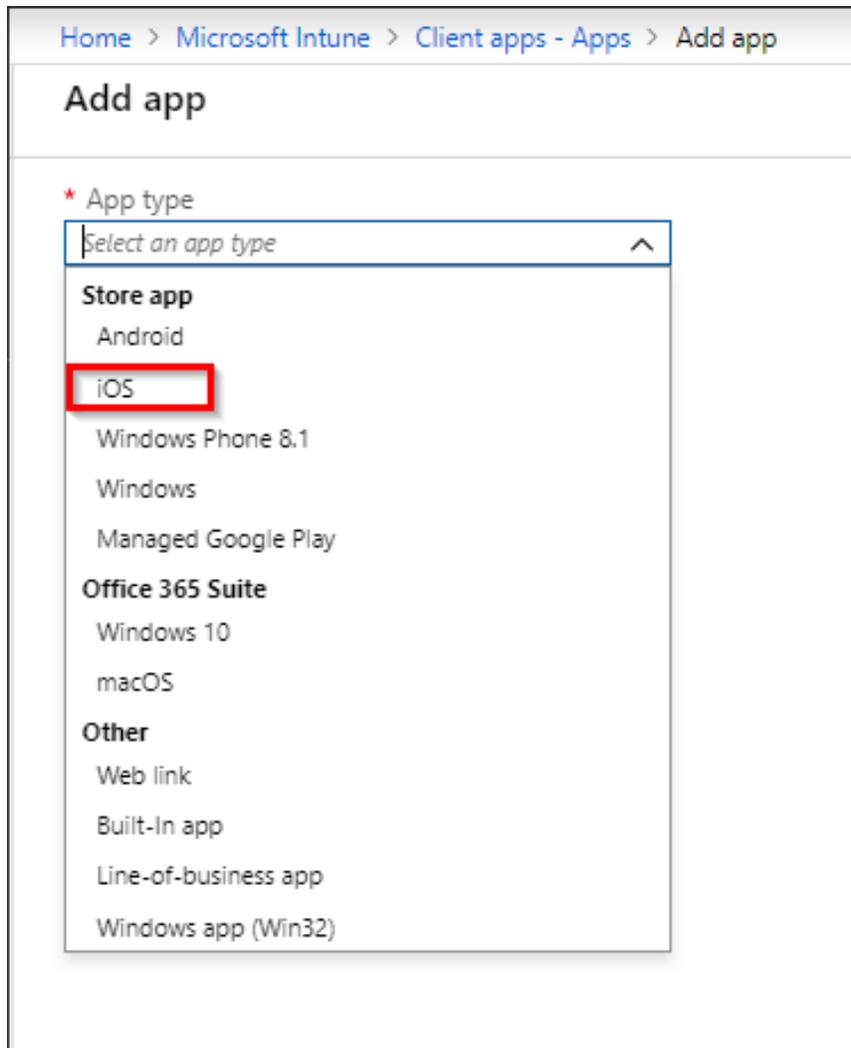
19. Click "Select" and "Save".

## Adding SandBlast Mobile Protect app for iOS Devices

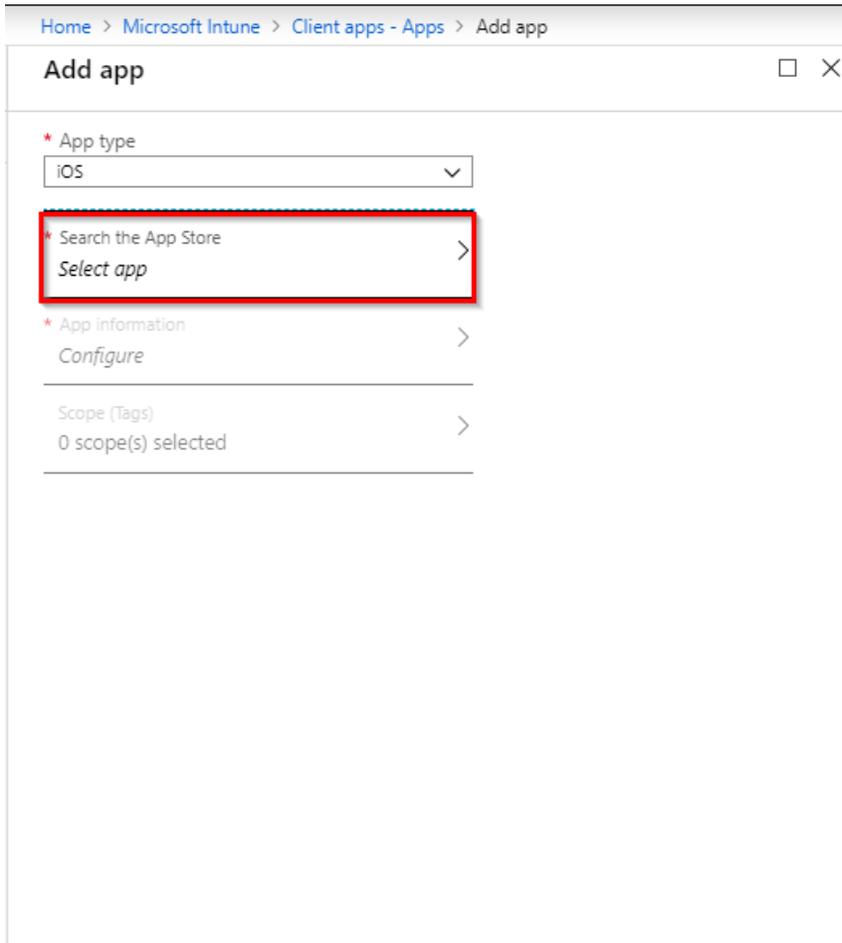
1. Navigate to **Client apps > Apps**, and click "+ Add".



2. In the add app panel, select the type of "Store app > iOS".



3. Select the "Search the App Store" tab



4. Enter in "SandBlast Mobile Protect", and select it from the list.

Search the App Store

---

SandBlast Mobile Protect

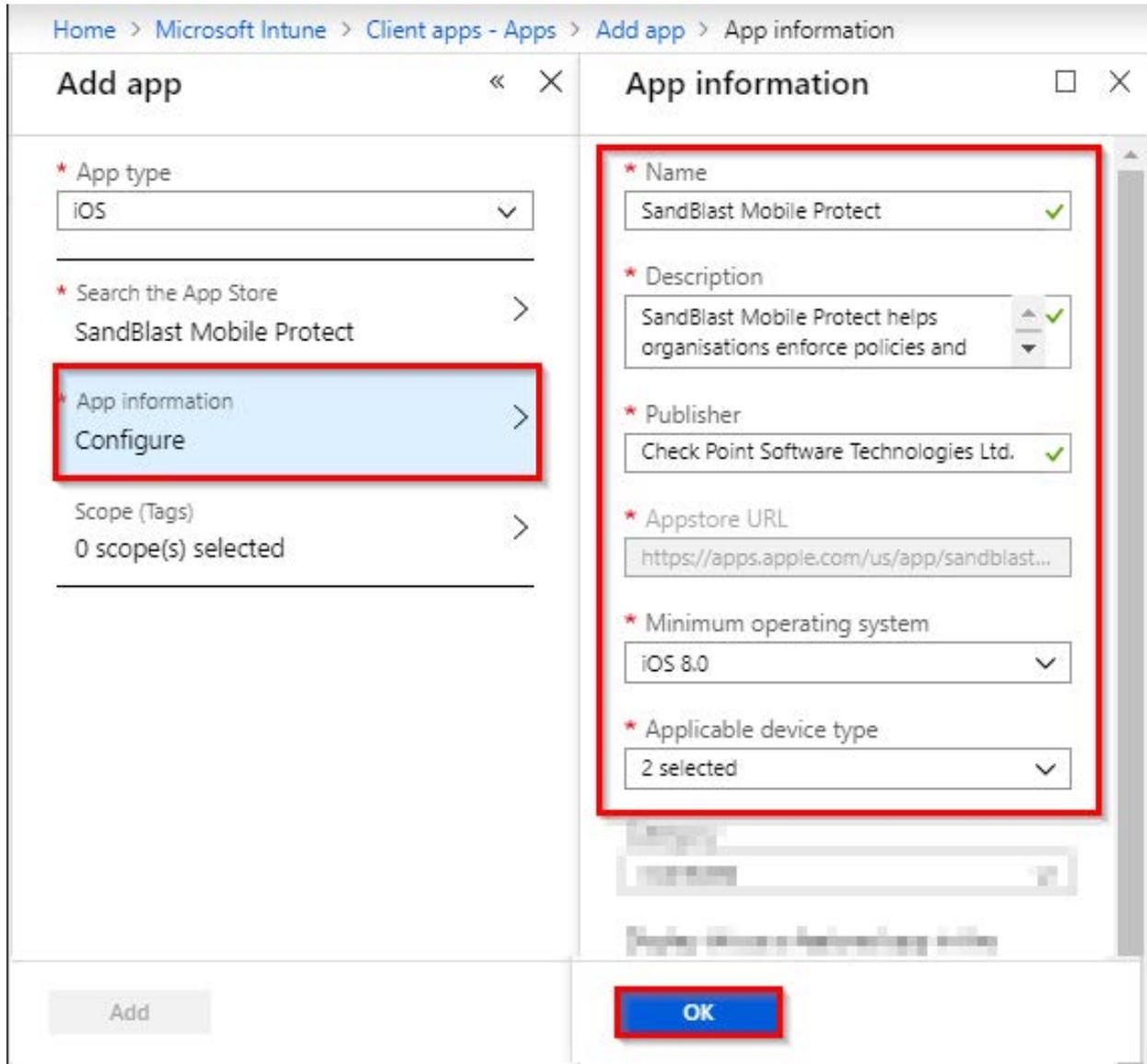
---

Found 2 apps

NAME	PUBLISHER
 SandBlast Mobile Protect	Check Point Software Technologies Ltd.
	Check Point Software Technologies Ltd.

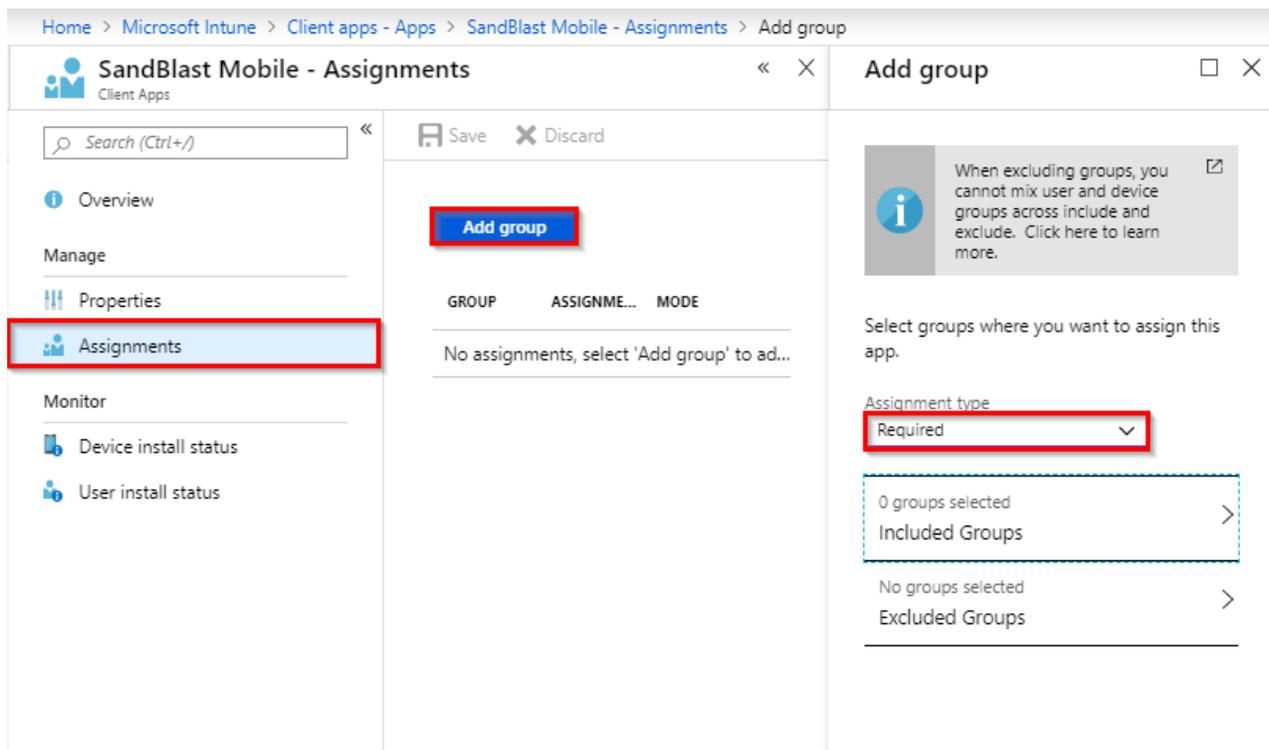
5. Click "Select".

6. In the add app panel, select the App information tab.

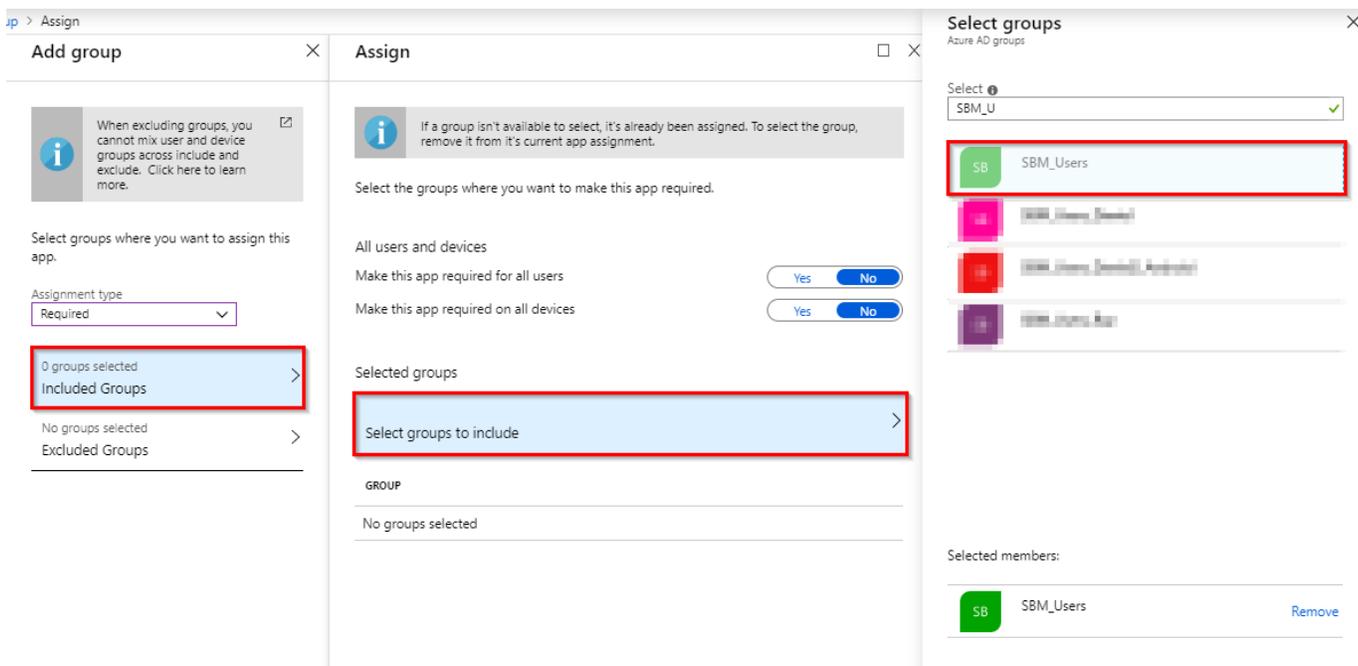


- 7. Click "OK".
- 8. Click "Add".

9. Select the Assignments tab, and click "Add group".
10. Set the type to "Required" from the pull-down menu.



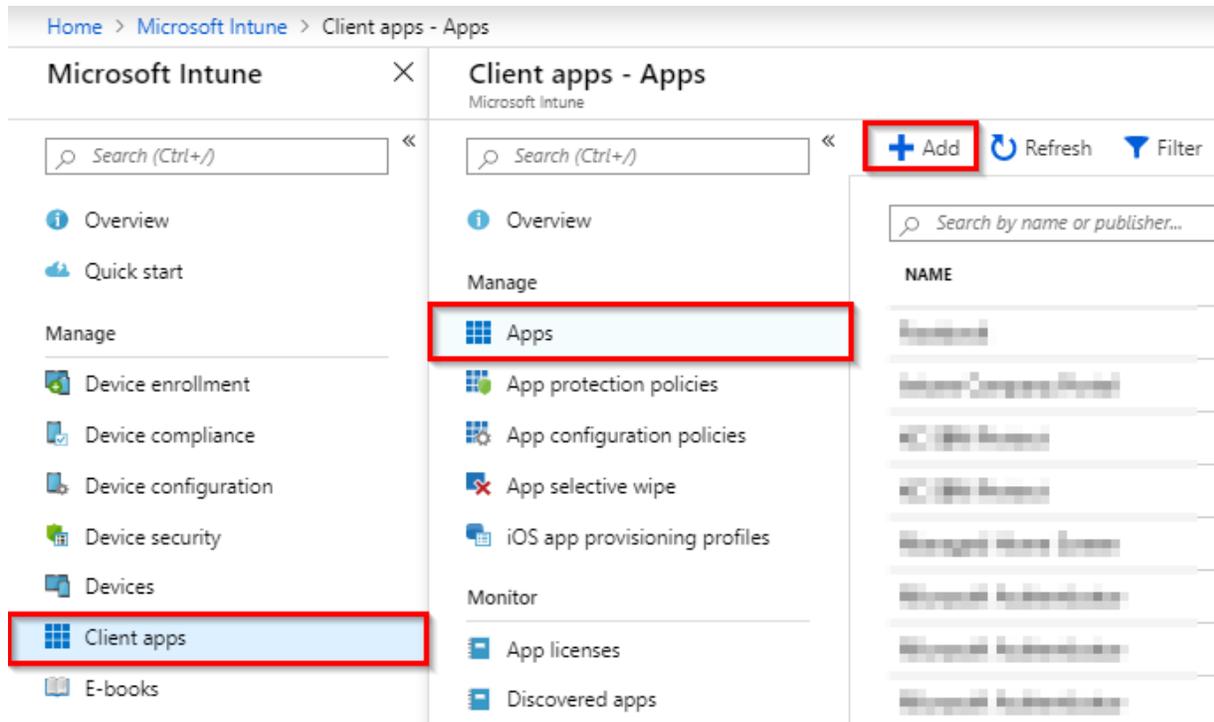
11. Select the appropriate Users Group.



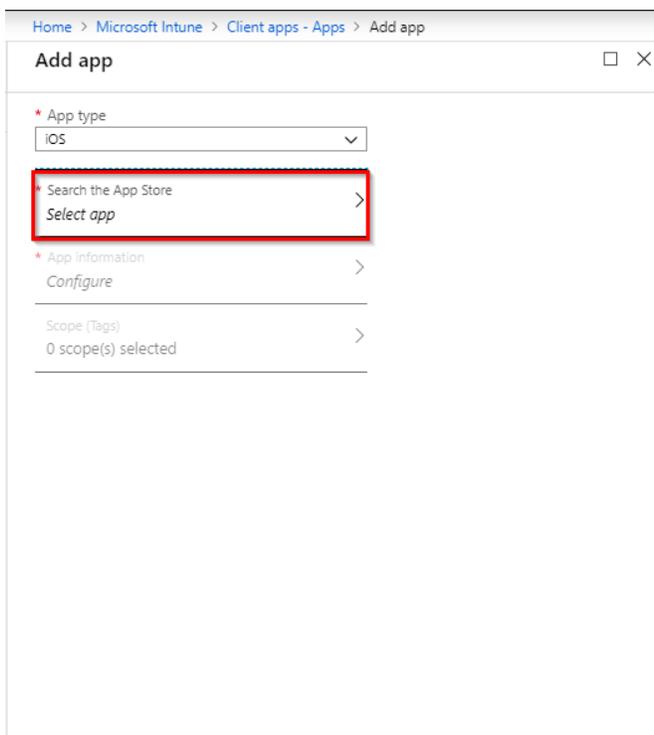
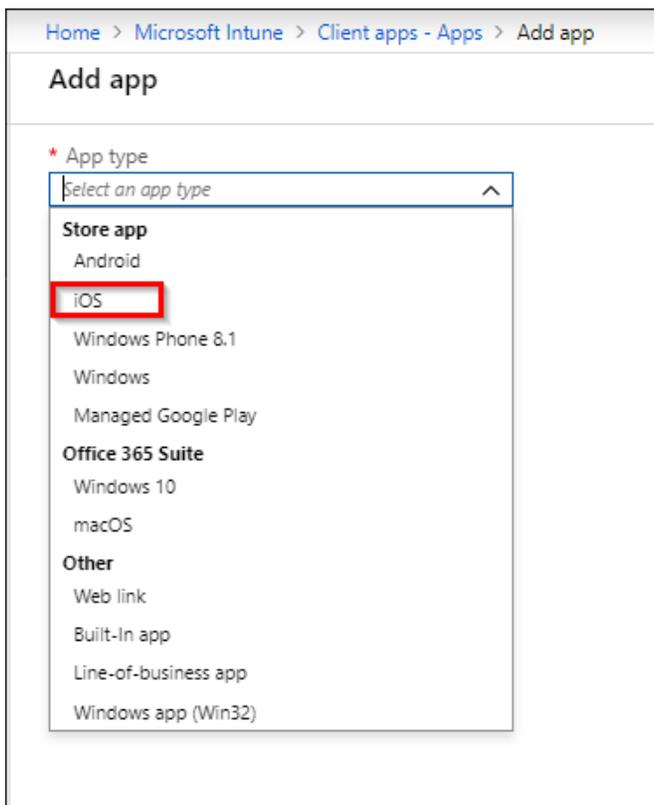
12. Click "Select" and "Save".

## Adding Microsoft Authenticator app for iOS Devices

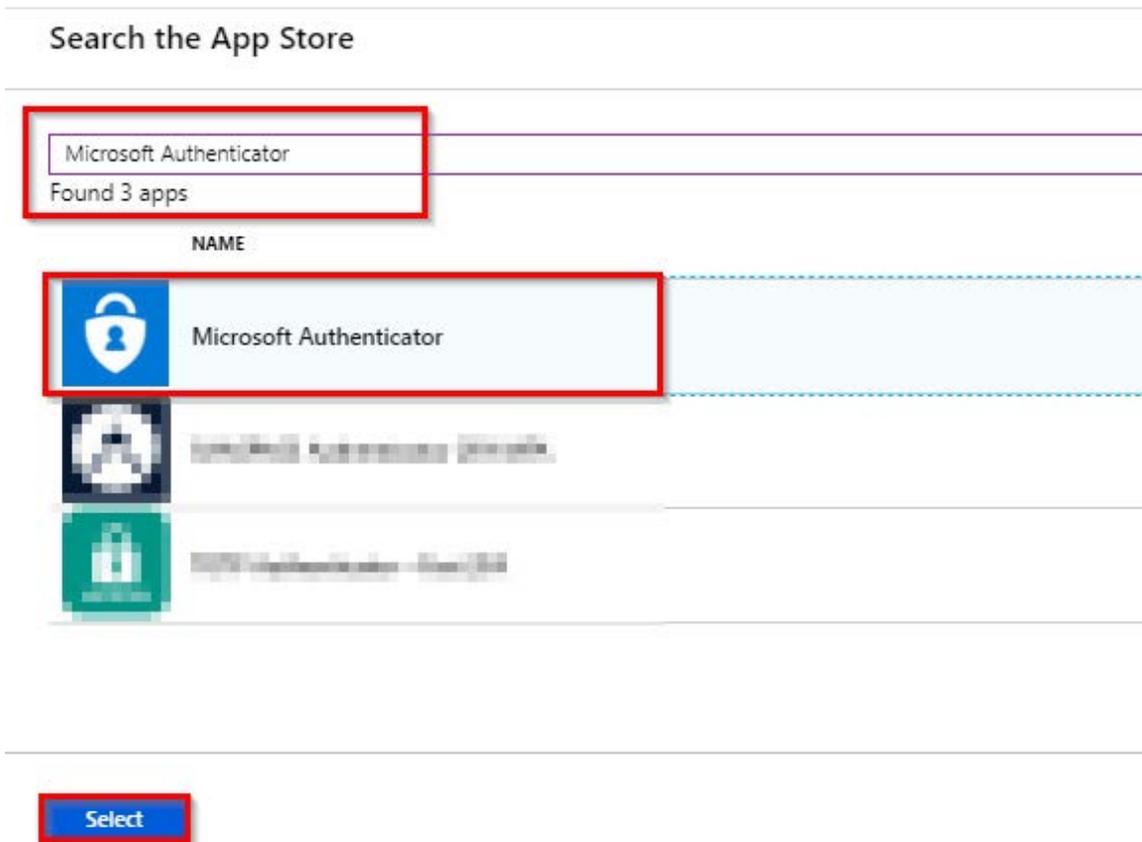
1. Navigate to **Client apps > Apps**, and click "+ Add".



2. In the add app panel, select the type of "iOS store app".
3. Select the "Search the App Store" tab.

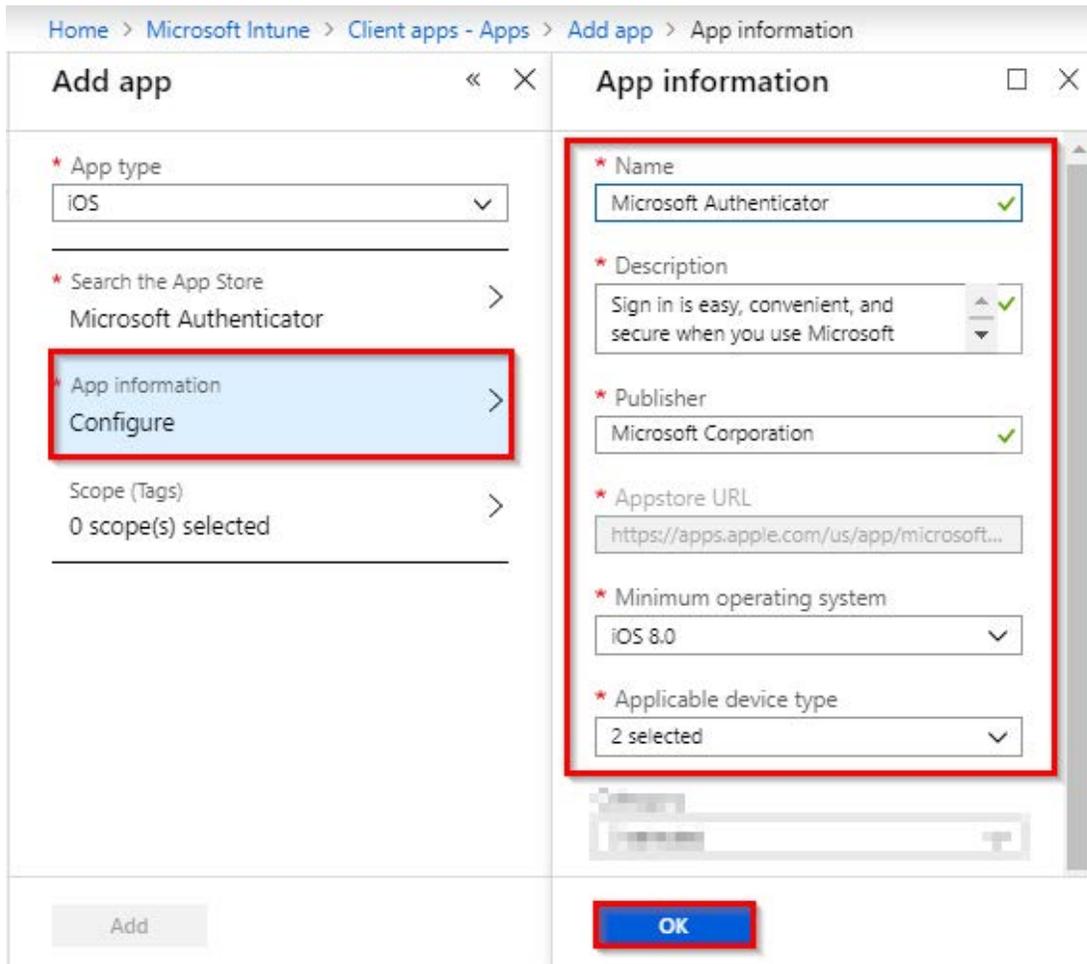


4. Enter in Microsoft Authenticator, and select it from the list.



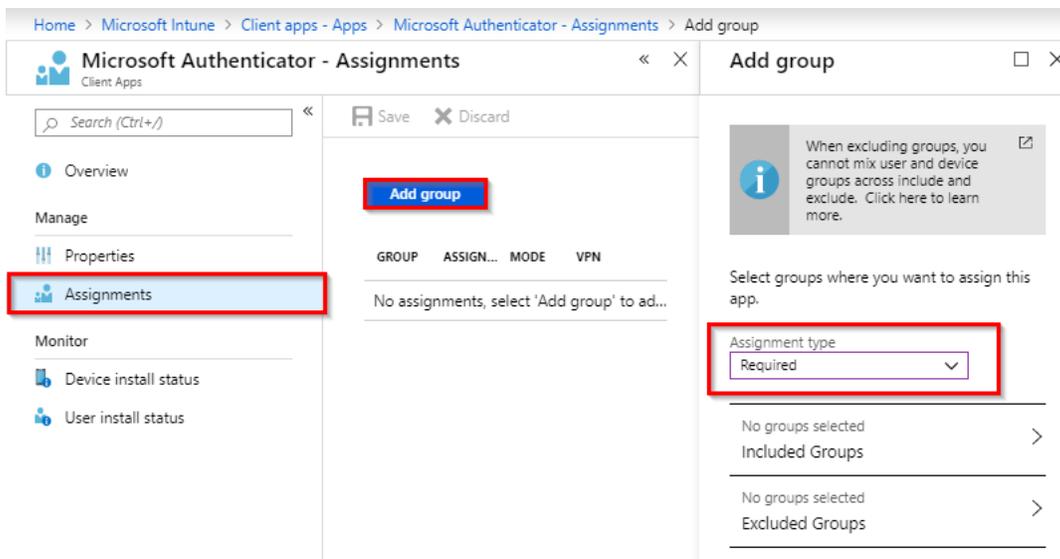
5. Click "Select".

6. In the add app panel, select the App information tab.

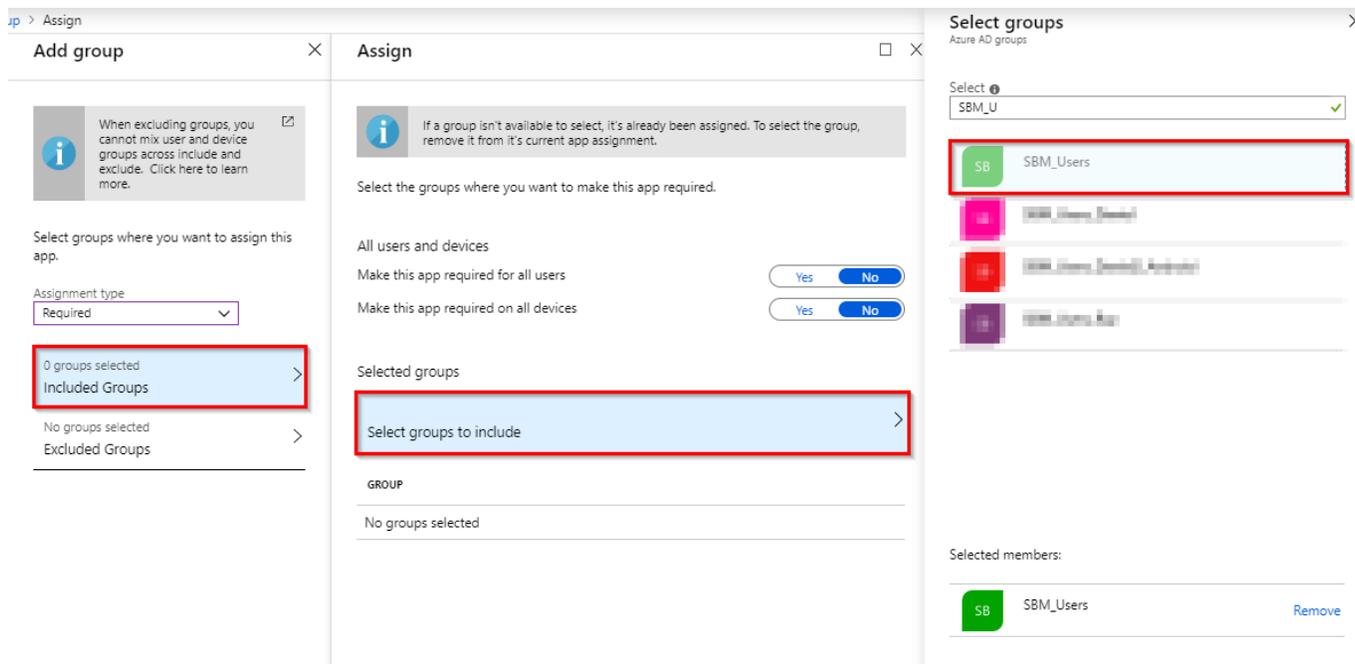


- 7. Click "OK".
- 8. Click "Add".

9. On the Microsoft Authenticator – Overview panel, select the Assignments tab.
10. Click "Add group".
11. Set the type to "Required" from the pull-down menu.



12. Select the appropriate Users Group.



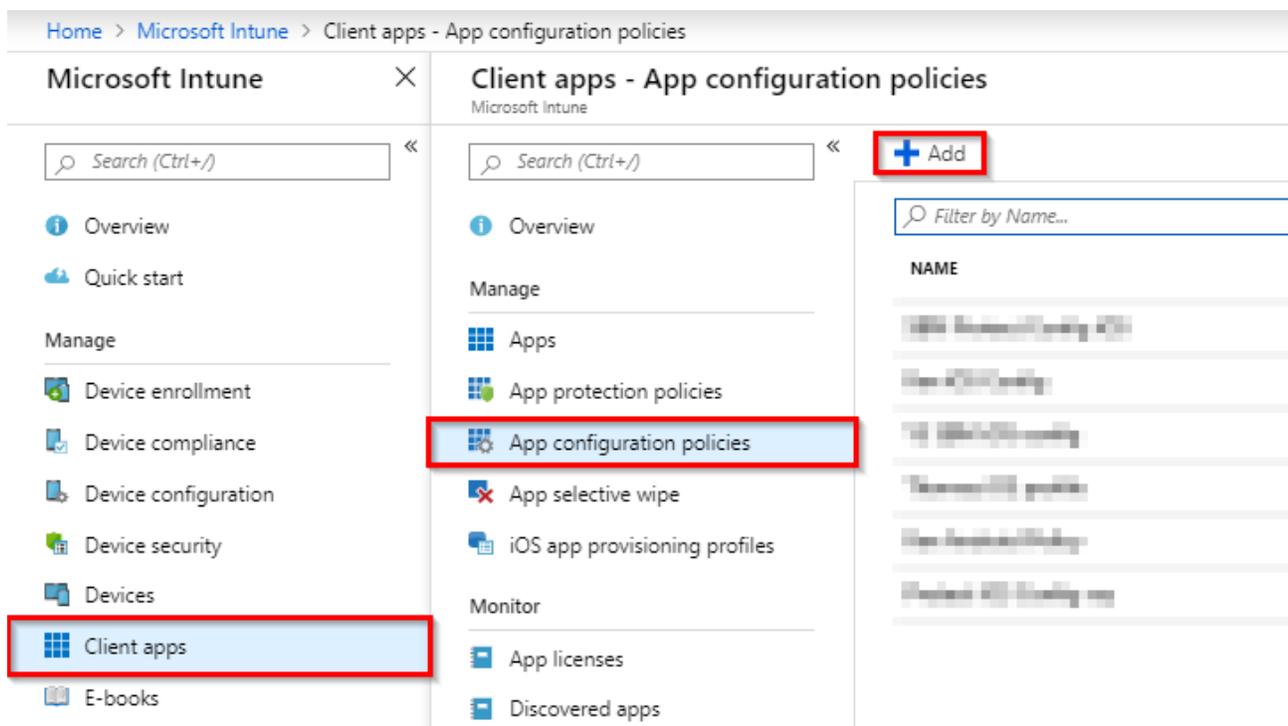
13. Click "Select" and "Save".

## Adding an iOS Configuration Policy for SandBlast Mobile Protect

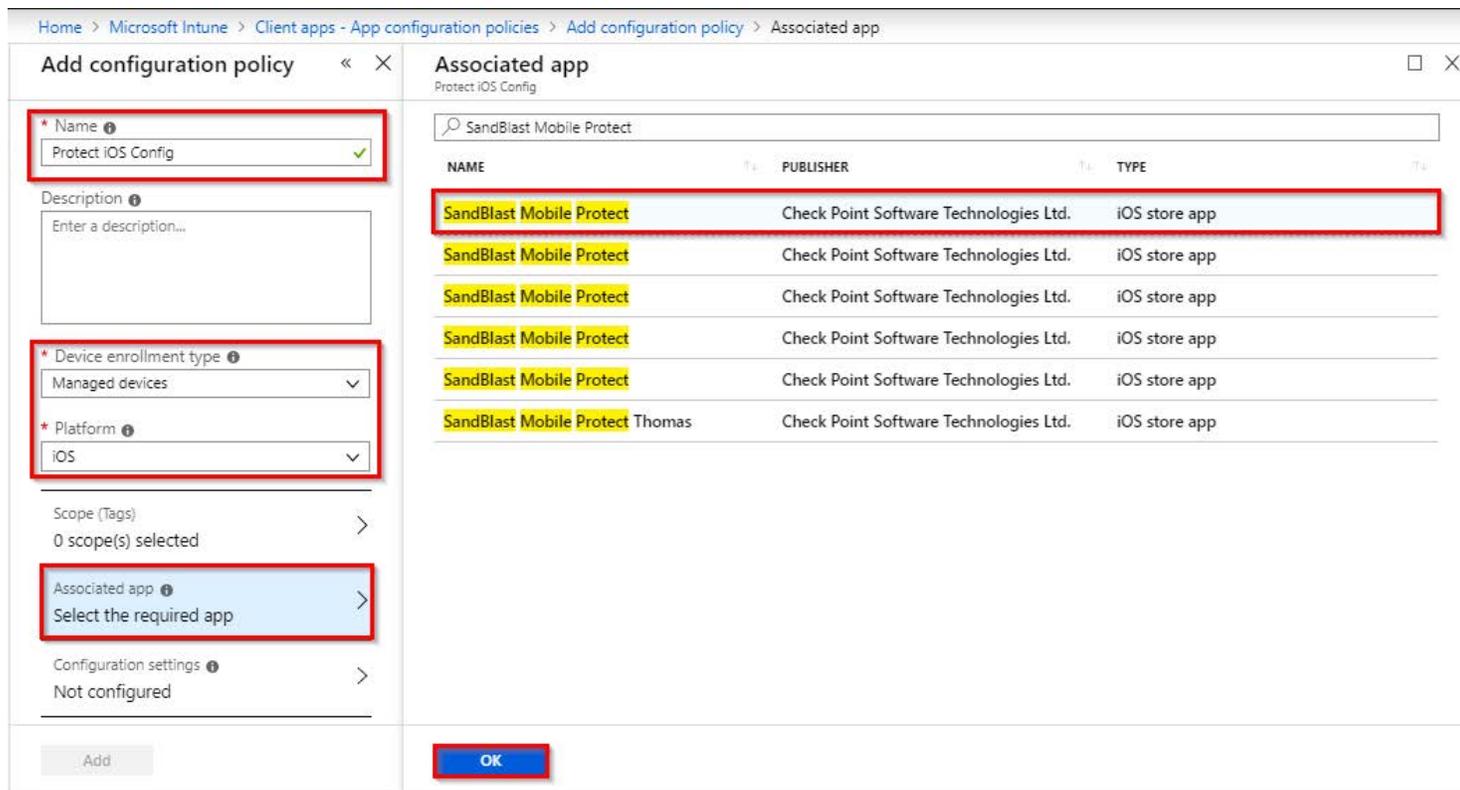
To auto-register iOS devices to SandBlast Mobile, we need to configure an iOS Configuration Policy.

For more information about "iOS Configuration Policies" in Microsoft Intune, please visit:  
<https://docs.microsoft.com/intune/deploy-use/deploy-apps-in-microsoft-intune>

1. Navigate to **Client apps > App configuration policies**, and click "+ Add".



2. Enter in a name and select "Managed devices" from the "Device enrollment type" pull-down menu.
3. Select "iOS" from the "Platform" pull-down menu.
4. Select the Associated app tab, and select SandBlast Mobile Protect.



Home > Microsoft Intune > Client apps - App configuration policies > Add configuration policy > Associated app

### Add configuration policy

**Name**  
Protect iOS Config ✓

**Description**  
Enter a description...

**Device enrollment type**  
Managed devices

**Platform**  
iOS

Scope (Tags)  
0 scope(s) selected

**Associated app**  
Select the required app

Configuration settings  
Not configured

Add

### Associated app

Protect iOS Config

SandBlast Mobile Protect

NAME	PUBLISHER	TYPE
SandBlast Mobile Protect	Check Point Software Technologies Ltd.	iOS store app
SandBlast Mobile Protect	Check Point Software Technologies Ltd.	iOS store app
SandBlast Mobile Protect	Check Point Software Technologies Ltd.	iOS store app
SandBlast Mobile Protect	Check Point Software Technologies Ltd.	iOS store app
SandBlast Mobile Protect	Check Point Software Technologies Ltd.	iOS store app
SandBlast Mobile Protect Thomas	Check Point Software Technologies Ltd.	iOS store app

OK

5. Click "OK".

6. Get the URL for SandBlast Mobile Protect Android link from the SandBlast Mobile Dashboard under **Settings > Device Management > Setting**.
7. Click "Copy" next to "iOS application settings".

The screenshot displays the Check Point SandBlast Mobile management console. The top navigation bar includes 'Dashboard', 'Events & Alerts', 'Device Risk', 'iOS Profiles', 'App Analysis', 'Network', 'Devices', 'Policy', and 'Settings' (highlighted with a red box). The left sidebar contains various configuration categories, with 'Device Management' expanded and 'Setting' highlighted with a red box. The main content area is titled 'Device Management Settings' and includes the following sections:

- Device Management Settings:** MDM service (Microsoft Intune), Should install MDIS profile (off).
- Notify user when device was added by MDM:** Registration email (iOS) (off), Registration email (Android) (off), Registration sms (iOS) (off), Registration sms (Android) (off), Daily registration limit (100). A 'Save' button is present.
- Application deployment for MS Intune:** When configuring SBM app in MS Intune. Includes 'Copy' buttons for 'iOS application settings' (highlighted with a red box) and 'Android application settings'.
- Buttons at the bottom: 'Sync Now', 'Pause Sync', and 'Edit Settings'.

8. In Microsoft Azure Intune Portal, select the Configuration Settings tab, and select "Enter XML data" from the Configuration Settings format pull-down menu.
9. Paste the copied text into the "Dictionary content" field.

Home > Microsoft Intune > Client apps - App configuration policies > Add configuration policy > Configuration settings

**Add configuration policy** < X

**Configuration settings** □ X

\* Name ⓘ  
Protect iOS Config ✓

Description ⓘ  
Enter a description...

\* Device enrollment type ⓘ  
Managed devices ▾

\* Platform ⓘ  
iOS ▾

Scope (Tags)  
0 scope(s) selected >

Associated app ⓘ  
SandBlast Mobile Protect >

Configuration settings ⓘ  
Not configured >

Once the policy is created, the format cannot be changed

Configuration settings format ⓘ Enter XML data ▾

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.

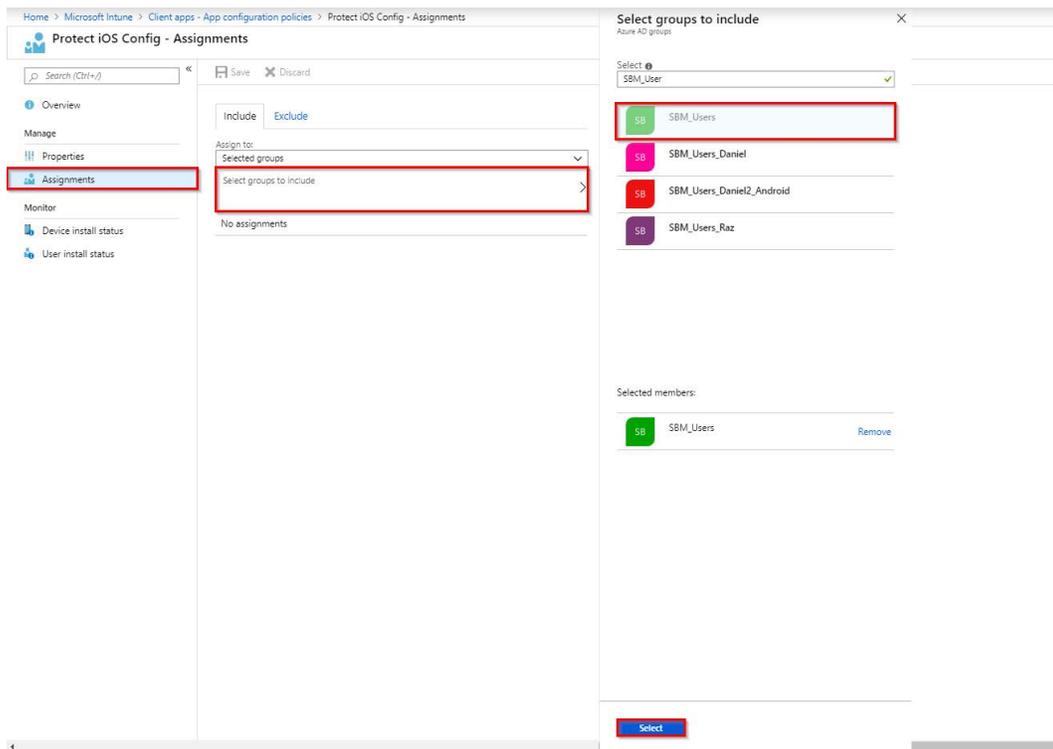
[Learn more about XML property lists](#)

```
<dict><key>MDM</key><string>INTUNE</string><key>UserEmail</key><string>userprincipalname</string><key>managedId</key><string>d7261dc8f7f4b4232827e6ab2c72a0ac4767d314ee0ad54d877fbc97087f18</string></dict>
```

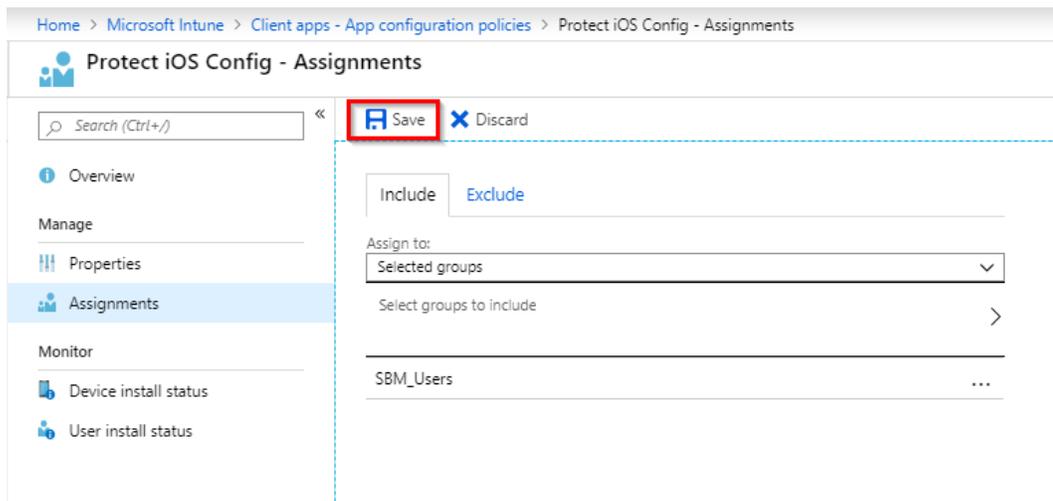
Add OK

10. Click "OK".
11. Click "Add".

- 12. Select the Assignments tab, and click "Select groups".
- 13. Select the appropriate Users Group.



- 14. Click "Select".



- 15. Click "Save".



## Registering Devices to SandBlast Mobile

In this chapter we will cover the user experience of device registration with SandBlast Mobile.

This chapter discusses the following:

Registration of an iOS Device .....	52
Registration of an Android Device .....	55

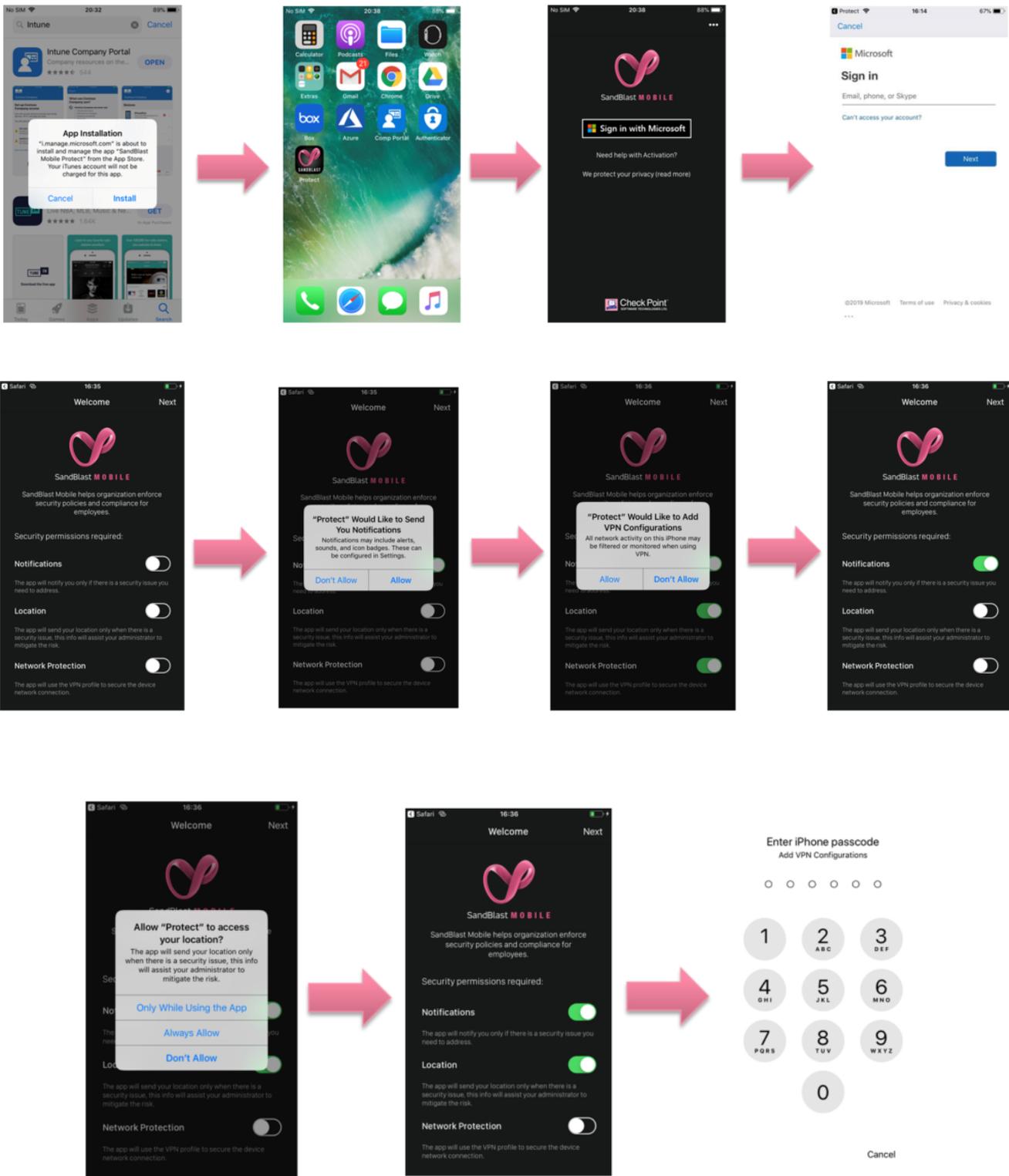
# Chapter 4

## ***Registration of an iOS Device***

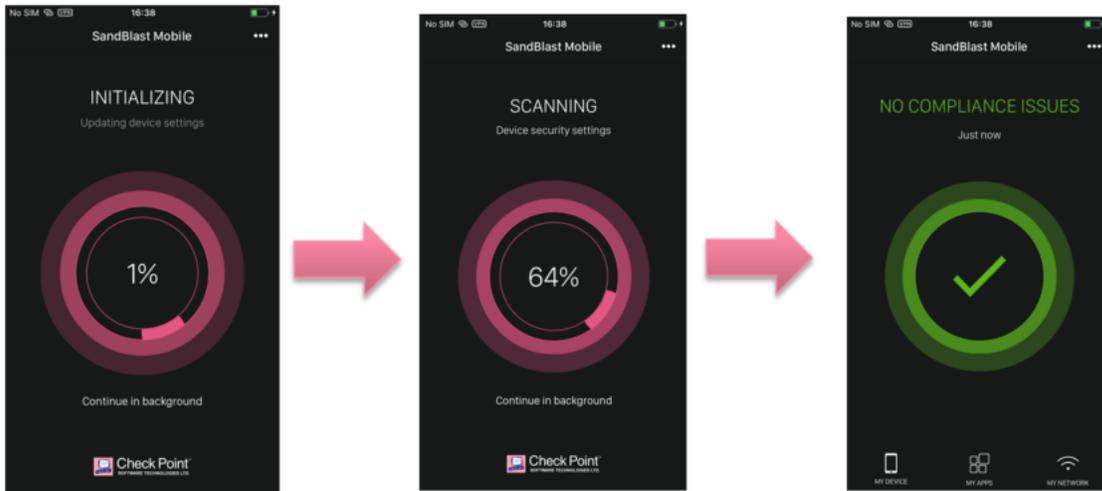
After the device is enrolled to the Microsoft Intune and the device is synchronized to SandBlast Mobile, the user will be prompted to install the SandBlast Mobile Protect App.

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 taps "Sign in with Microsoft" and Microsoft Authenticator is launched.
4. The user enters in their email address and password.

5. The user is prompted to enable Notifications, Location, and Network Protection.



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

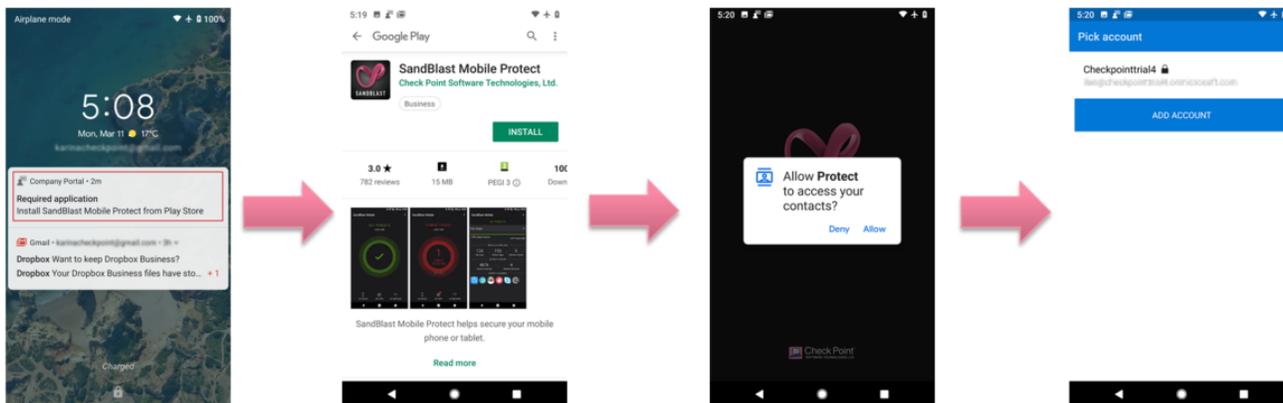


7. Once the App is done scanning the system, it will display the state of the device. In this case, the device is without malicious or high risk apps, network and OS threats.

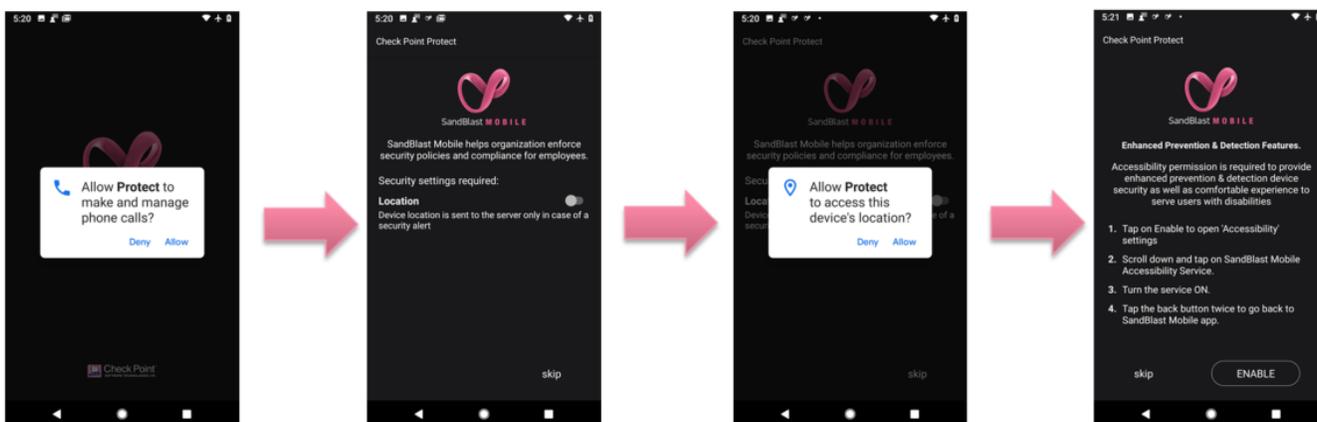
## Registration of an Android Device

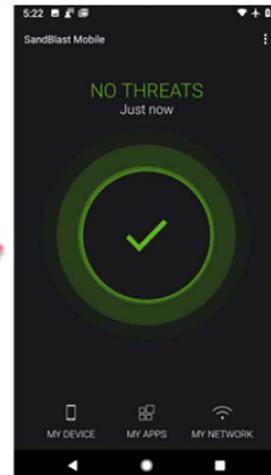
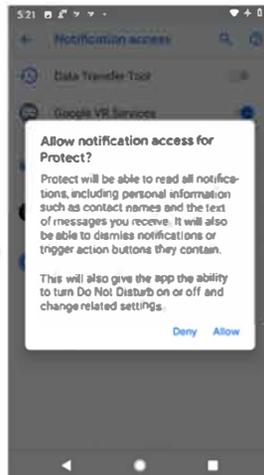
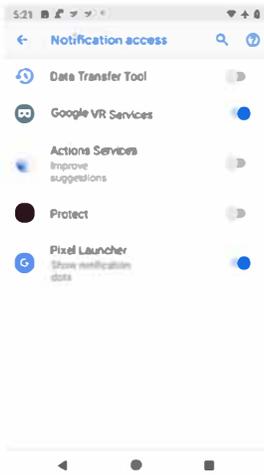
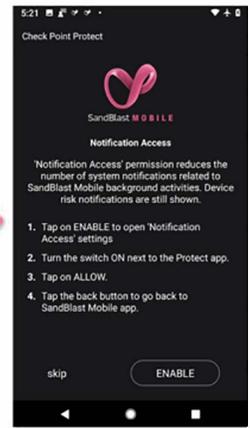
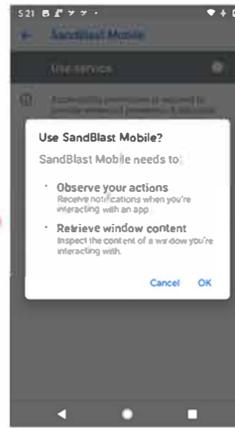
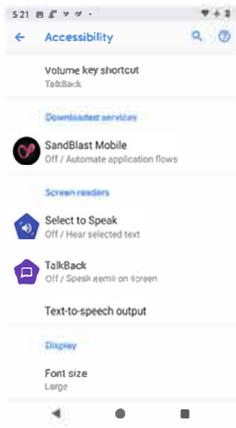
After the device is enrolled to the Microsoft Intune and the device is synchronized to SandBlast Mobile, the user will be prompted to install the SandBlast Mobile Protect app. The user is automatically taken to the Google Play Store.

1. The user taps "INSTALL".
2. The user taps "Allow" to accept access to the device's contacts.
3. The user selects the SSO credentials.
4. The user allows the app to make phone calls and access device location.

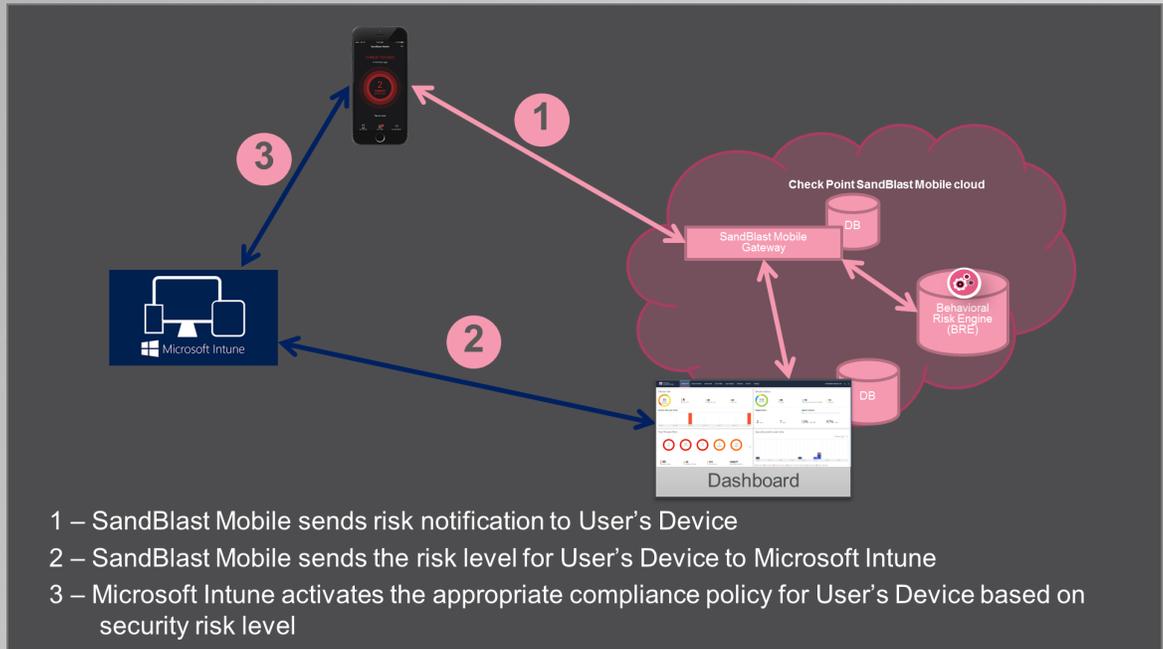


5. The user enables accessibility and notifications from the app.
6. Once the App is done scanning the system, it will display the state of the device. In this case, the device is without malicious or high risk apps, network and OS threats.





## 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 via in-app notifications as well as updates the risk state to the Microsoft Intune system for that device.

Microsoft Intune receives the state change, and upon recognizing the risk state level as being above acceptable risk, and marks the device as Not Compliant and enacts any conditional access policies imposed on Not Compliant devices.

In the following example, the Administrator will blacklist an app, such as in our example "Box". As a result, all devices with "Box" installed will be identified to be at High Risk due to the blacklisted app being installed on the device. The SandBlast Mobile Dashboard will notify the user, and mark the device as High Risk to the Microsoft Intune system. This mitigation process was the one we created in "Creating a Mitigation Process" on page 13

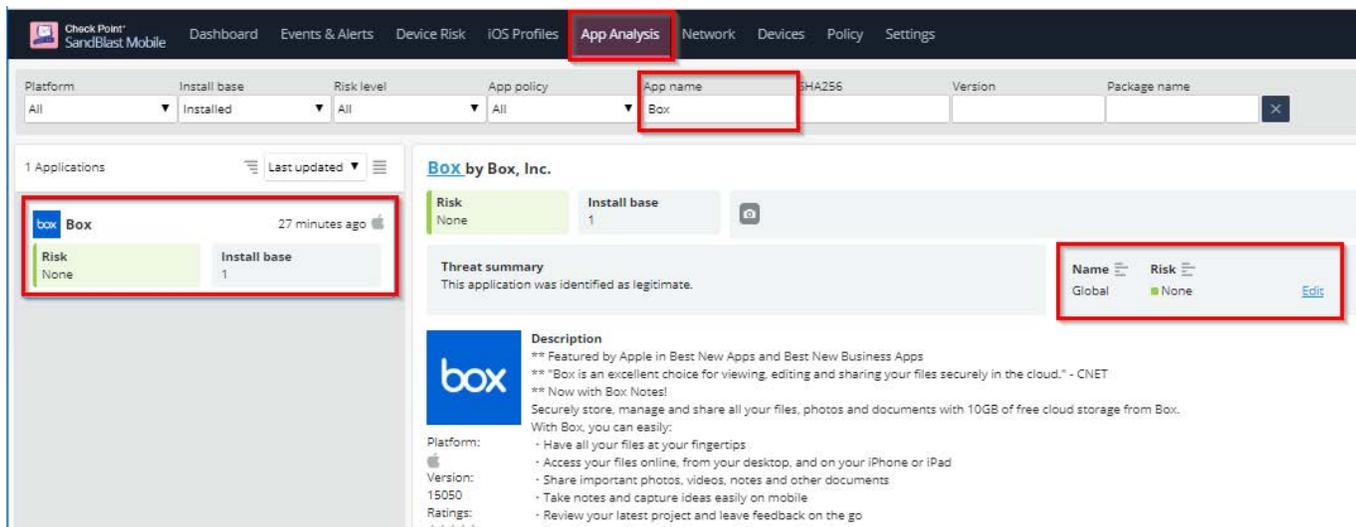
This chapter discusses the following:

<b>Blacklisting a Test App</b> .....	<b>58</b>
<b>View of Device at Risk</b> .....	<b>59</b>
<i>SandBlast Mobile Protect App Notifications</i> .....	<b>59</b>
<i>Microsoft Intune Company Portal Notification</i> .....	<b>59</b>
<b>Administrator View on the SandBlast Mobile Dashboard</b> .....	<b>60</b>
<b>Administrator View on the Microsoft Intune Portal</b> .....	<b>61</b>

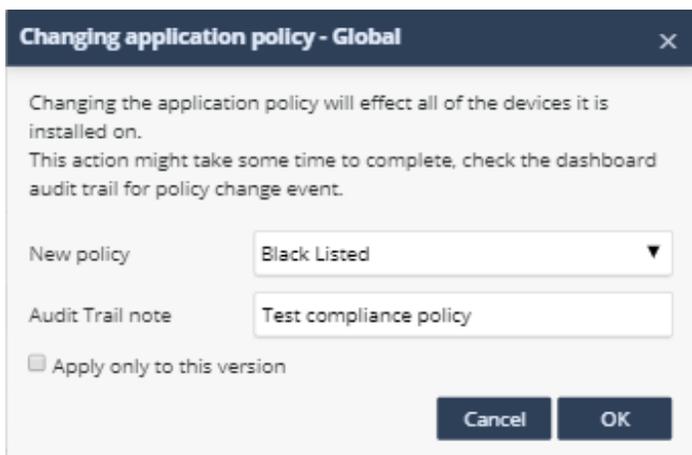
## Blacklisting a Test App

The first step is to blacklist an app, in our example "Box". By blacklisting this app, all release version and OS types will also be blacklisted. In our example, Box for iOS will be blacklisted which will result in all Box numbered release versions for iOS to be blacklisted as well, unless the "Apply only to this version" checkbox is selected.

1. Log into the SandBlast Mobile Dashboard.
2. Navigate to **App Analysis** tab, and search for the app you wish to blacklist, in our example "Box".



3. Click "Policy" link of "None".
4. On the "Changing application policy" pop-up window, select "Black Listed" from the "New policy" drop-down menu.
5. Enter a reason for this change in the "Audit Trail note".

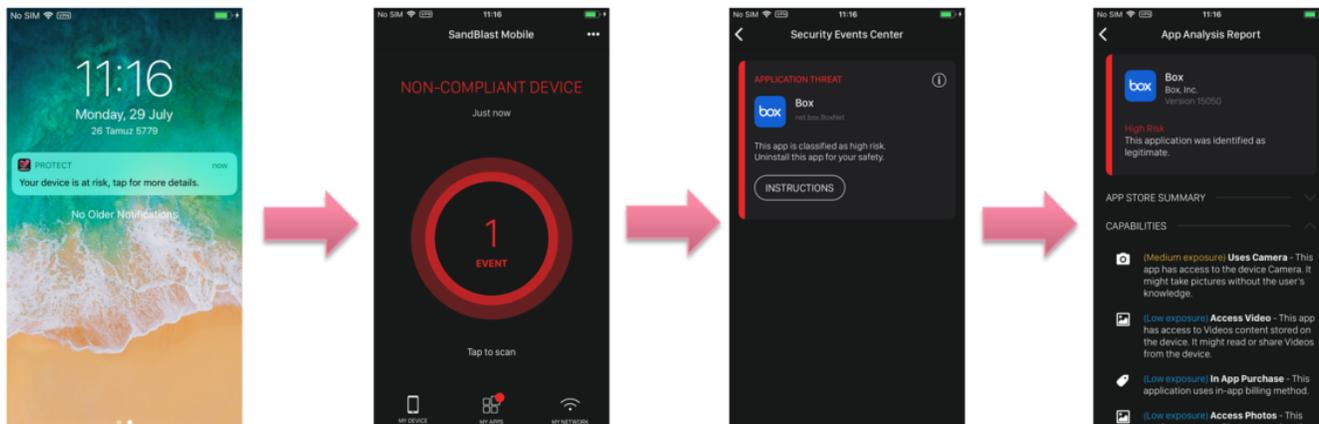


6. Click "OK".

## View of Device at Risk

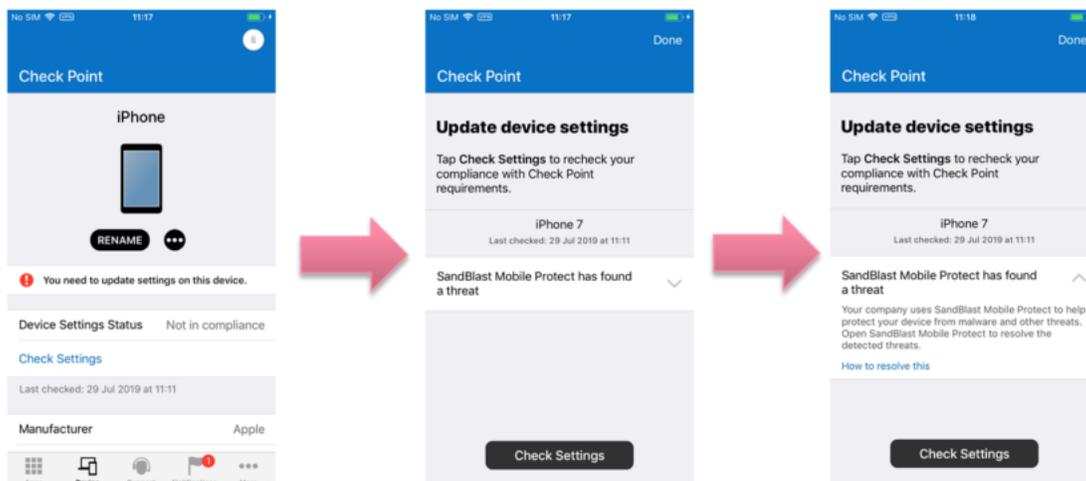
### SandBlast Mobile Protect App Notifications

1. The user receives a SandBlast Mobile Protect notification indicating that the blacklisted app is not allowed by Corporate Policy, in our example "Box".



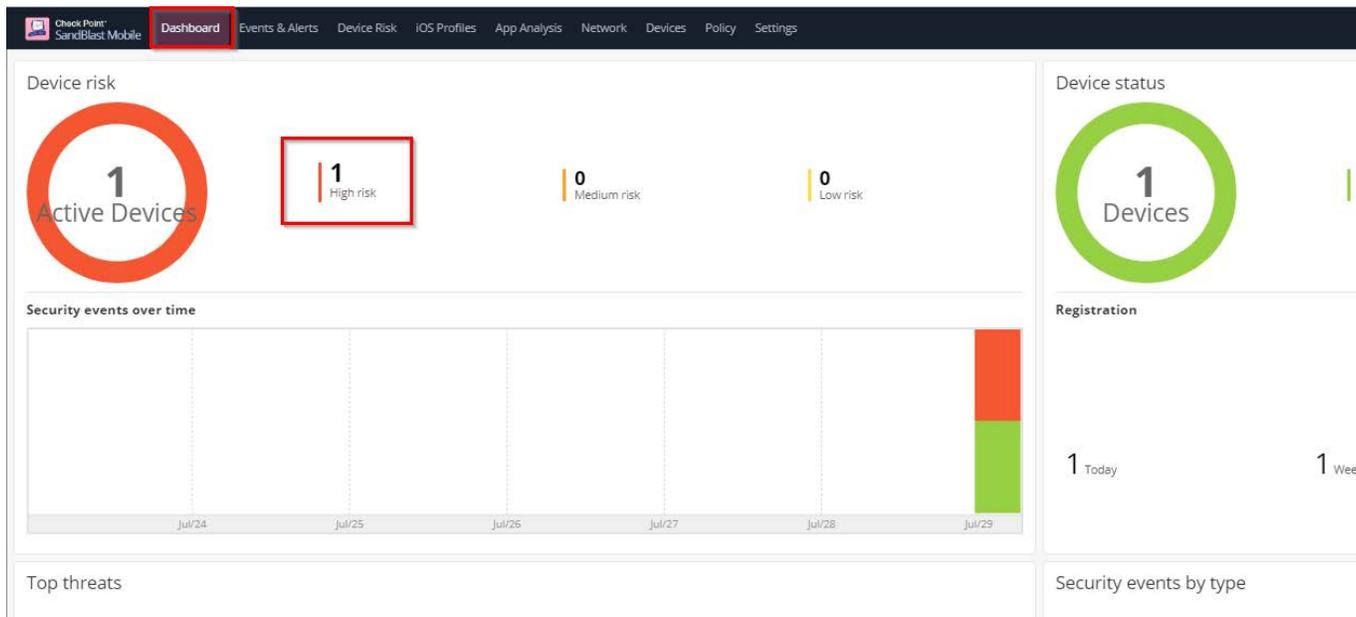
### Microsoft Intune Company Portal Notification

1. The user receives an in-app notification from the Microsoft Intune system, notifying the user that their device is not compliant with company policies, and that they should open the Protect app to view further details to rectify the issue.

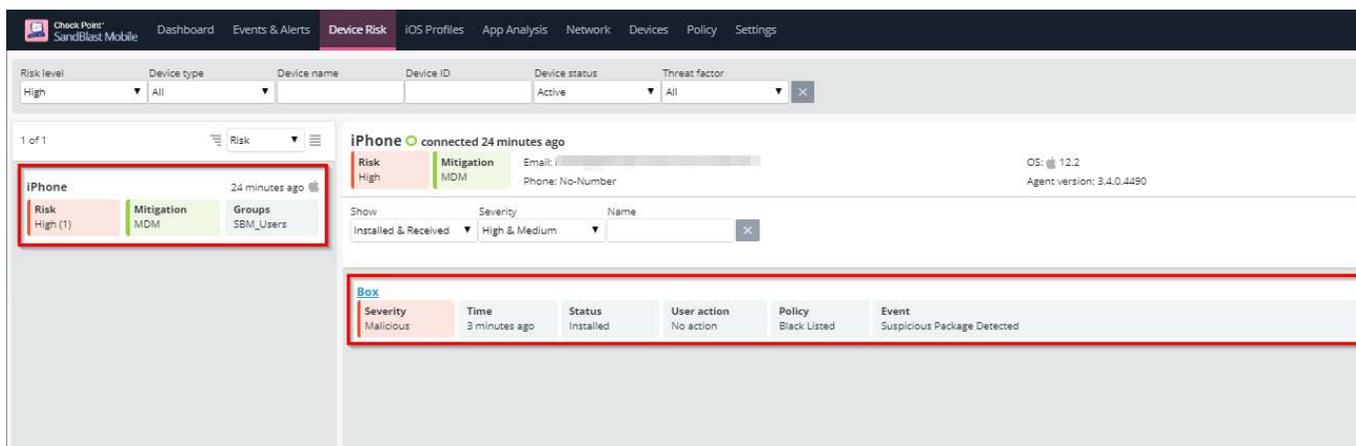


## Administrator View on the SandBlast Mobile Dashboard

- From the SandBlast Mobile Dashboard, the Administrator will see that there are devices at high risk.



- Clicking the High Risk will display a list of devices at high risk.
- Selecting the desired device from the left-side list, the Administrator can see that the high risk state is caused by the existence of the blacklisted app, "Box".



## Administrator View on the Microsoft Intune Portal

1. In the Microsoft Intune Portal on the **Device Compliance** overview screen, the Administrator can see that one or more devices are Not Compliant.

Home > Microsoft Intune - Overview > Device compliance

**Device compliance**

Search (Ctrl+/) Sync Report

Data in this view was last refreshed on 7/29/2019 at 10:56:10 AM.

Tenant name : [redacted] MDM  
Tenant location : Europe 0102 Acc

STATUS	DEVICES
Compliant	1
In grace period	0
Not evaluated	2
<b>Not compliant</b>	<b>4</b>
<b>Total</b>	<b>7</b>

Devices without com... 0

Policy compliance

2. In the Microsoft Intune Portal from **Device compliance > Device Compliance**, the Administrator can see that Fox's device is Out of Compliance.

Home > Microsoft Intune - Overview > Device compliance - Device compliance

**Device compliance - Device compliance**

Search (Ctrl+/) Refresh Filter Columns Export Delete

Data in this view is live.

Filters applied: Managed by, Compliance

Search by IMEI, Serial number, Email, UPN, Device name or Management name

0 Devices selected (100 max)

DEVICE NAME	USER PRINCIPAL NAME	MANAGED BY	COMPLIANCE	OS	OS VERSION	DEVICE STATE	COMPLIANCE GRACE PERIOD EXPIRATION	DEVICE THREAT LEVEL
iPhone	[redacted]	MDM	Not Compliant	iOS	12.2	Managed	7/29/2019, 11:15:54 AM	High
[redacted]	[redacted]	MDM	Not Compliant	iOS	12.2	Retire issued	5/1/2019, 6:06:35 PM	Unknown
[redacted]	[redacted]	MDM	Not Compliant	iOS	12.3	Managed	6/3/2019, 11:27:21 AM	Deactivated
[redacted]	[redacted]	MDM	Not Compliant	iOS	12.1.4	Managed	4/17/2019, 6:19:22 PM	Deactivated
[redacted]	[redacted]	MDM	Not Compliant	iOS	11.1.2	Managed	5/28/2019, 3:11:28 PM	Deactivated



## Appendices

### Integration Information

Information Name	Value
Microsoft Intune API Admin Username	
Microsoft Intune API Admin Password	
Microsoft Intune AD Security Group(s)	
Device Risk Levels	None, Low, Medium, or High
Device Status Levels	Provisioned, Active, or Inactive
SandBlast Mobile Gateway	gw.locsec.net
SandBlast Mobile App Name (iOS)	SandBlast Mobile Protect
SandBlast Mobile App ID (iOS)	com.checkpoint.capsuleprotect
SandBlast Mobile App Name (Android)	SandBlast Mobile Protect
SandBlast Mobile App ID (Android)	com.lacoon.security.fox





**For more information, visit [checkpoint.com/mobilesecurity](https://checkpoint.com/mobilesecurity)**

---

**CONTACT US**

**Worldwide Headquarters** | 5 Ha'Soleim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: [info@checkpoint.com](mailto:info@checkpoint.com)

**U.S. Headquarters** | 959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233 | [www.checkpoint.com](http://www.checkpoint.com)