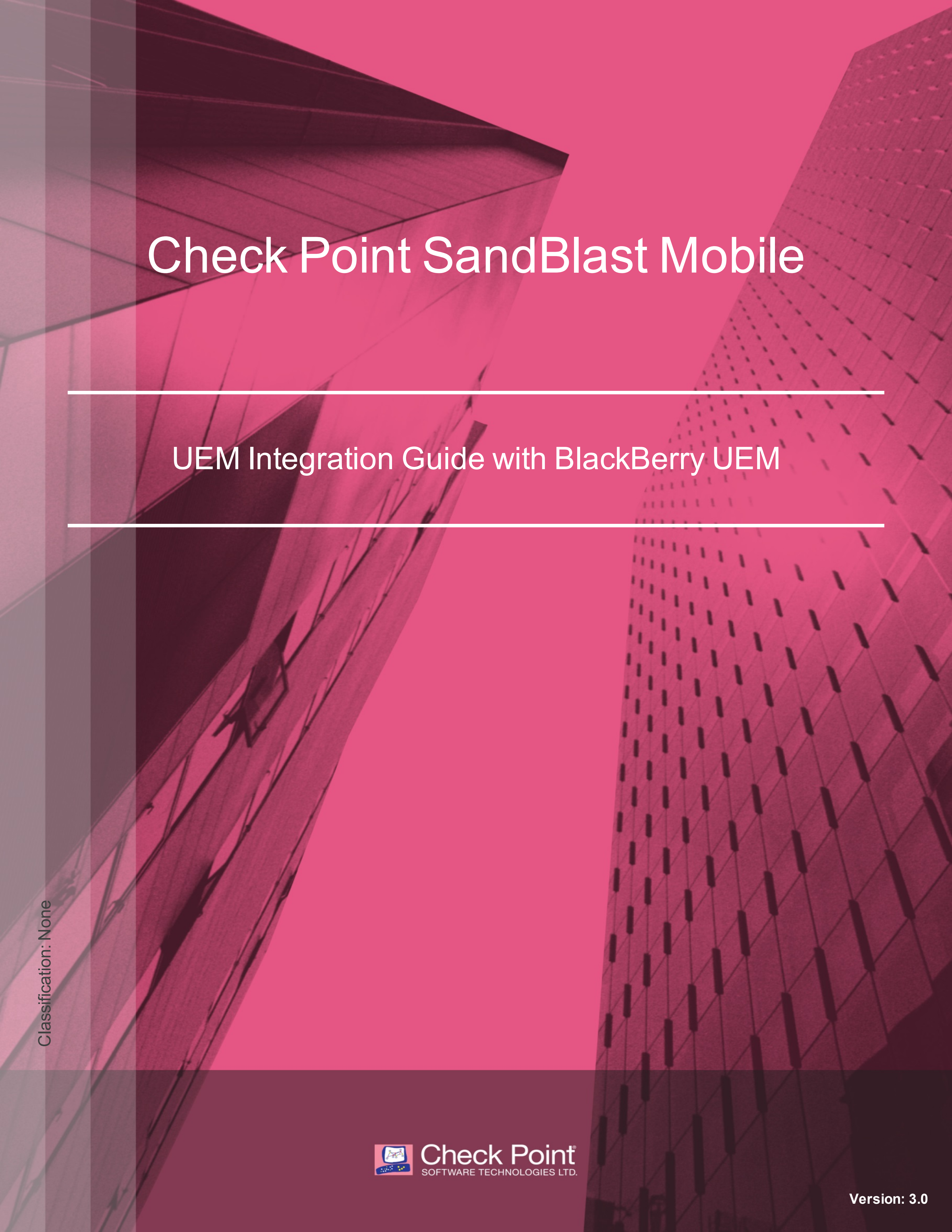


Check Point SandBlast Mobile

UEM Integration Guide with BlackBerry UEM

Classification: None

Check Point
SOFTWARE TECHNOLOGIES LTD.

Version: 3.0

© 2018 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 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. BlackBerry, BES, BES12, UEM, and UEM Client are registered trademarks of BlackBerry Limited and/or its subsidiaries.

About This Guide

Check Point SandBlast Mobile 3.0 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 3.0 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 3.0 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:

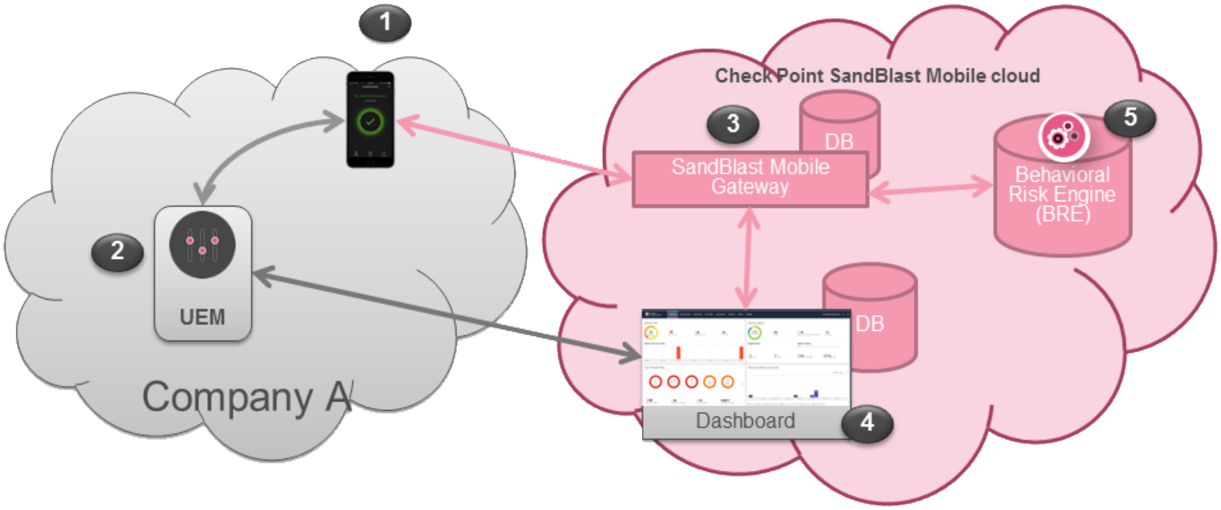
- SandBlast Mobile Behavioral Risk Engine ("the Engine")
- SandBlast Mobile Gateway ("the Gateway")
- SandBlast Mobile Management Dashboard ("the Dashboard")
- SandBlast Mobile Protect app ("the App") for iOS and Android

When used with an Unified Endpoint Management (UEM) system, such as BlackBerry UEM, 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 BlackBerry UEM. It provides a quick tour through the interface of the BlackBerry UEM Console 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


1
2
UEM
Company A
Check Point SandBlast Mobile cloud
3
DB
SandBlast Mobile Gateway
5
Behavioral Risk Engine (BRE)
DB
Dashboard
4

	Component	Description
1	**SandBlast Mobile Protect app**	» 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**	» Unified Endpoint Management (generalized term replacing MDM/EMM) » Device Management and Policy Enforcement System
3	**SandBlast Mobile Gateway**	» The cloud-based 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.
4	**SandBlast Mobile Dashboard**	» 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**	» 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. » 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.

Contents

© 2018 Check Point Software Technologies Ltd. All rights reserved.

Chapter 1

Preparing the UEM Platform for Integration

This chapter discusses the following:

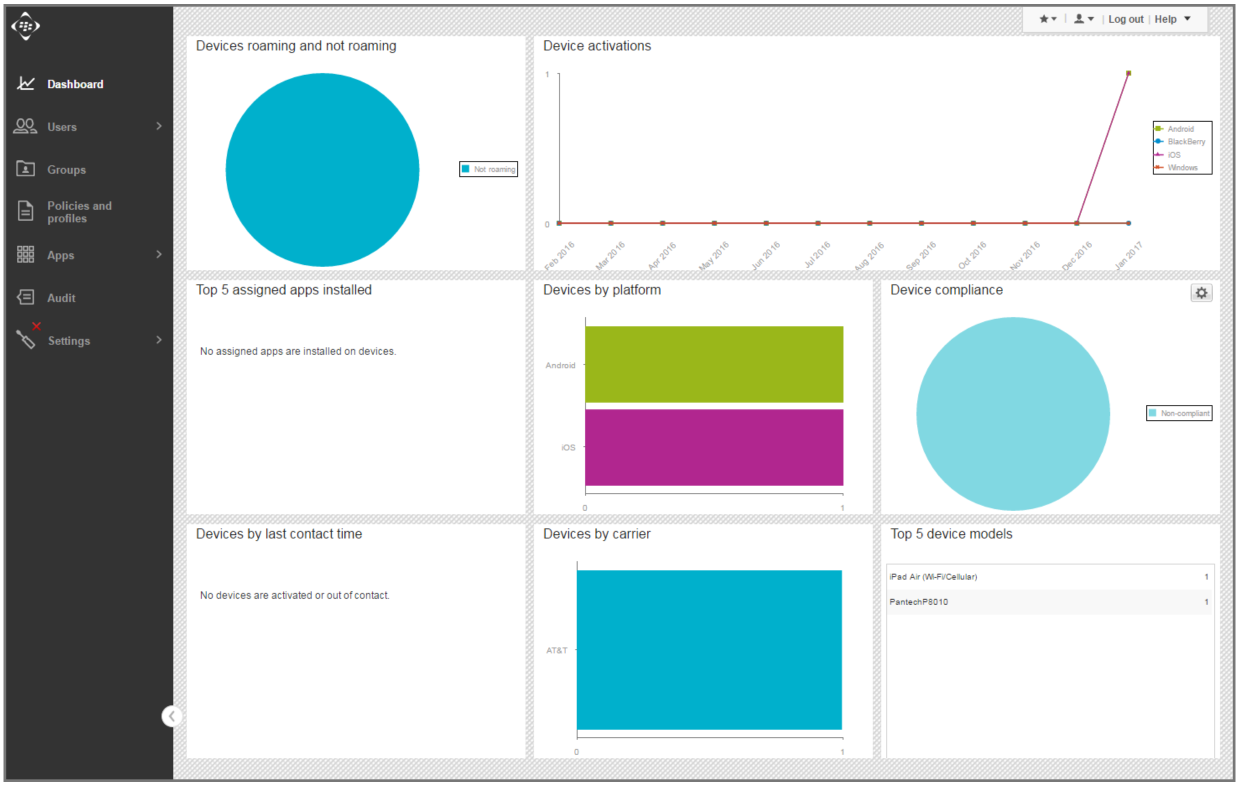
Prerequisites

1. BlackBerry UEM 12.6 or higher.
2. For **on-premise BlackBerry UEM Deployments**, the port used for the UEM Web Services API (default: TCP 18084) must be accessible remotely by the SandBlast Mobile servers through your firewall before trying to connect.

BlackBerry UEM Console

For more or updated information regarding BlackBerry UEM, please see http://help.blackberry.com/en/blackberry-uem/current/

1. Login to your BB Console.



No assigned apps are installed on devices.

No devices are activated or out of contact.

iPad Air (Wi-Fi/Cellular)	1
PantechP8010	1

> **Note:** During the procedures in this document there are quite a few pieces of information that you will need to gather or create. There is a form in "Integration Information" on page 70 that you can record your settings for easy reference.

Creating an API Administrator Account (optional)

For the interaction at the API, we will create an API admin user in the BlackBerry UEM Console that you use to limit the capability of the admin credentials used between the SandBlast Mobile Dashboard and the BlackBerry UEM system.

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

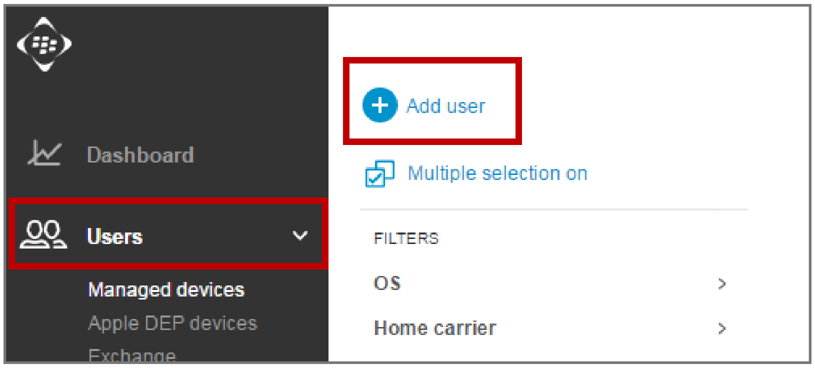
> **Note:** Creating an administrator account and administrator role requires a "Security Administrator" level role.

To create an "API" Administrator Account, follow this process.

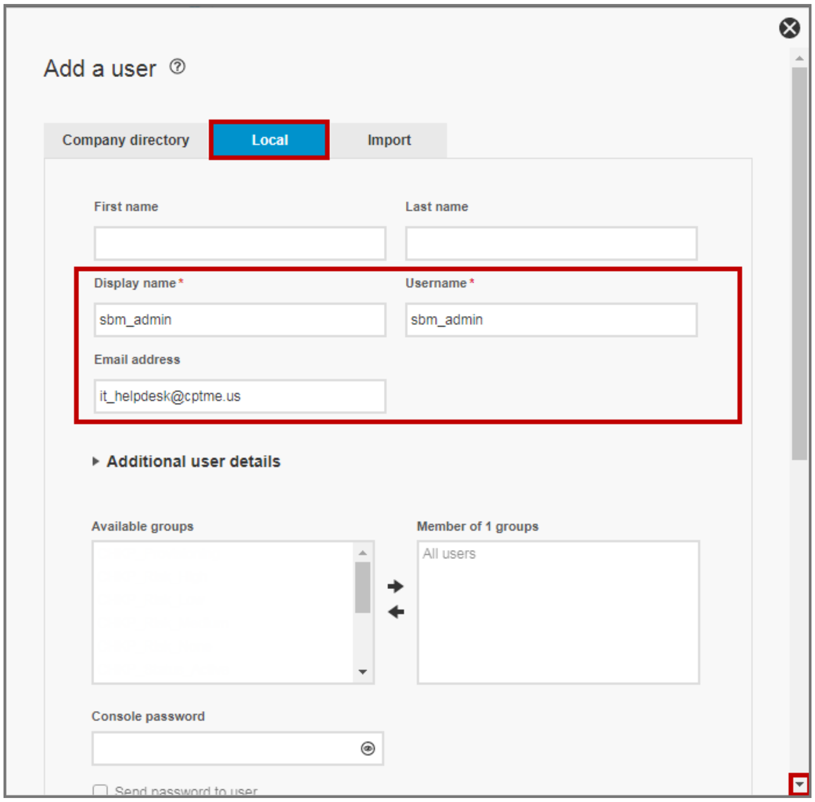
For more or updated information, please see BlackBerry's documentation at http://help.blackberry.com/en/blackberry-uem/current/administration/create-administrator.html

Create a New Administrator User Account

1. Navigate to **Users**, click "Add user".

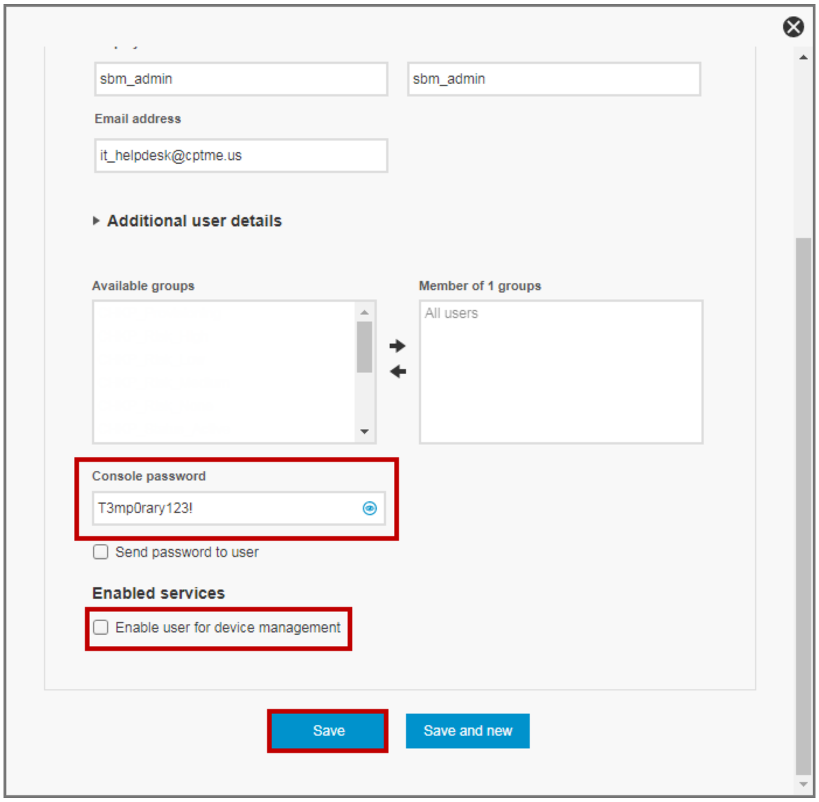


2. On the "Add a user" pop-up window "Local" tab, fill in the "Display name", "Username", and an "Email address" for the new user. In our example, we will create an admin username of "sbm_admin".


Add a user

Display name* sbm_admin
Username* sbm_admin
Email address it_helpdesk@cptme.us

3. Enter in a temporary console password for this user. When you login the first time with these credentials, you will be prompted to set a new password.
4. Scroll down and deselect the "Enable user for device management" checkbox.



sbm_admin | sbm_admin

Email address: it_helpdesk@cptme.us

▸ Additional user details

Available groups

Member of 1 groups: All users

Console password: T3mp0rary123!

□ Send password to user

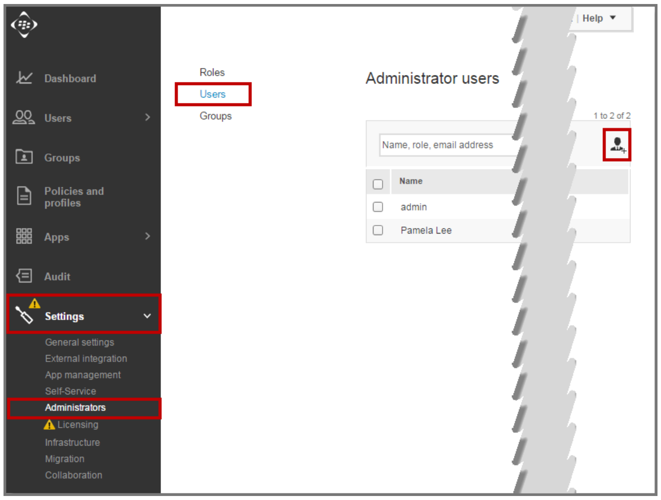
Enabled services

□ Enable user for device management

5. Click "Save".

Assign New User to Administrator Role

1. Navigate to **Settings > Administrators > Users**, click "Add Admin".



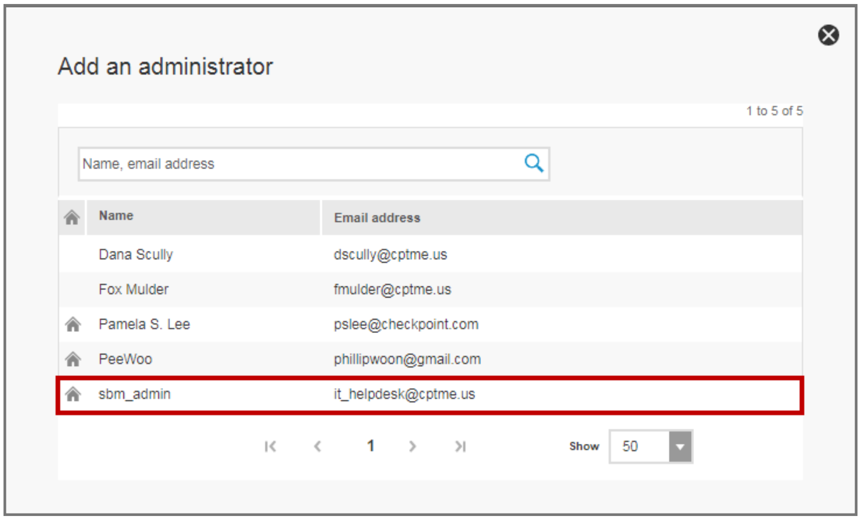
Administrator users

1 to 2 of 2

Name, role, email address

	Name
□	admin
□	Pamela Lee

2. On the "Add an Administrator" pop-up window, search/select the user you created in "Create a New Administrator User Account" on page 3.



Add an administrator

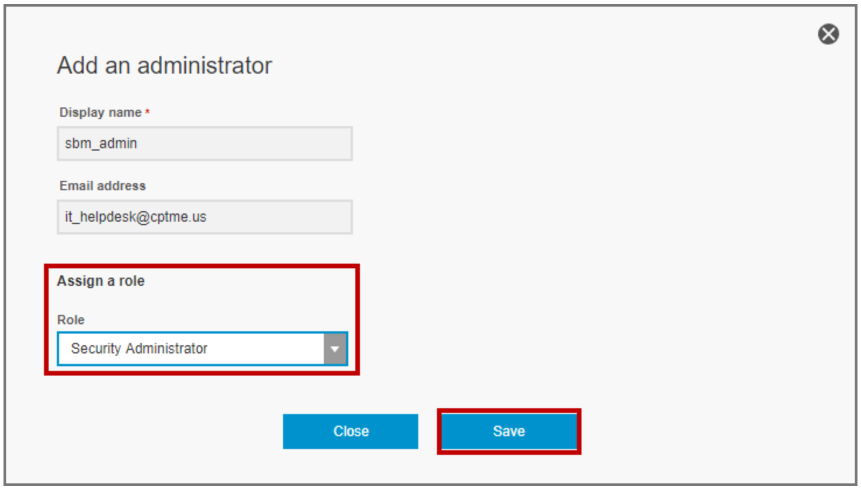
1 to 5 of 5

Name, email address

Name	Email address
Dana Scully	dscully@cptme.us
Fox Mulder	fmulder@cptme.us
Pamela S. Lee	pslee@checkpoint.com
PeeWoo	phillipwoon@gmail.com
sbm_admin	it_helpdesk@cptme.us

3. Click the user’s "Name".

4. Under "Assign a role" select the "Security Administrator" role.



Add an administrator

Display name *
sbm_admin

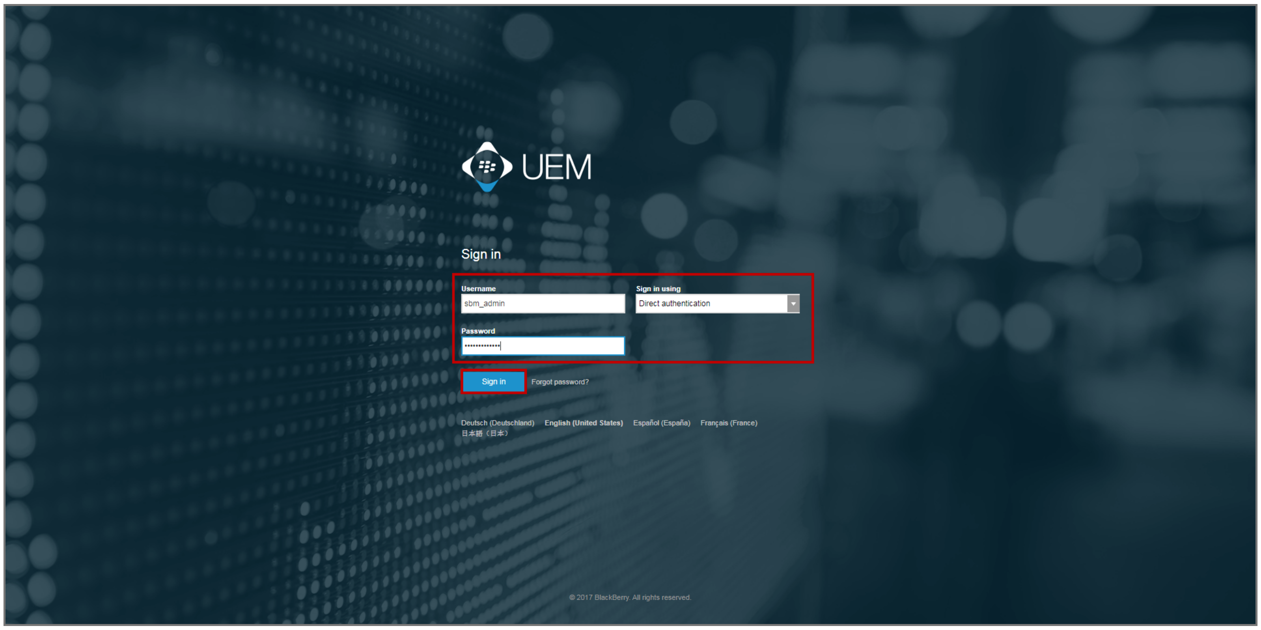
Email address
it_helpdesk@cptme.us

Assign a role

Role
Security Administrator

5. Click "Save".

6. Finish the creation of the new admin account by logging out of the BlackBerry UEM Console, and then logging back in using the temporary credentials you assigned to this new admin, in our example "sbm_admin / T3mp0rary123!". This will force you to select a new unique password.



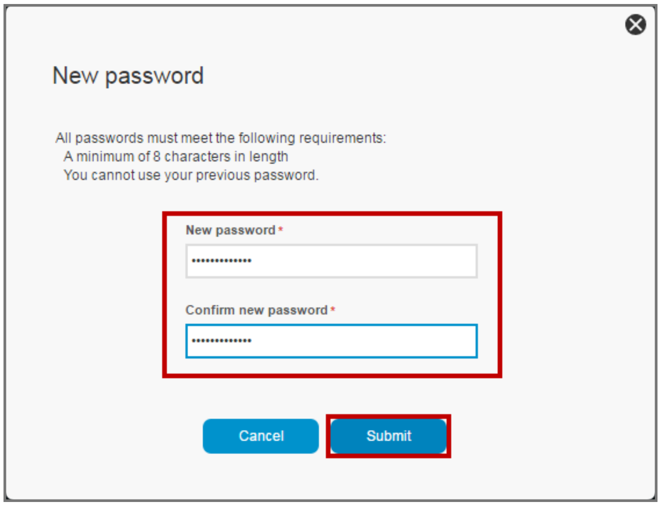
Username: sbm_admin

Sign in using: Direct authentication

Password: ••••••••••••••

7. Click "Sign In".

8. On the "New password" pop-up window, enter in a new password.



New password

All passwords must meet the following requirements:
A minimum of 8 characters in length
You cannot use your previous password.

New password *: ••••••••••••••

Confirm new password *: ••••••••••••••

9. Click "Submit".
10. On the "Find out about…" pop-up window, select "Do not show this again".
11. Click "Start".
12. Click "Log out".

> **Note:** Log out and log back into the BlackBerry UEM Console with your original Admin credentials to continue with the configuration.

Adding a User

There are two ways to add a user, "Add a Local User", or sync with a corporate user directory.

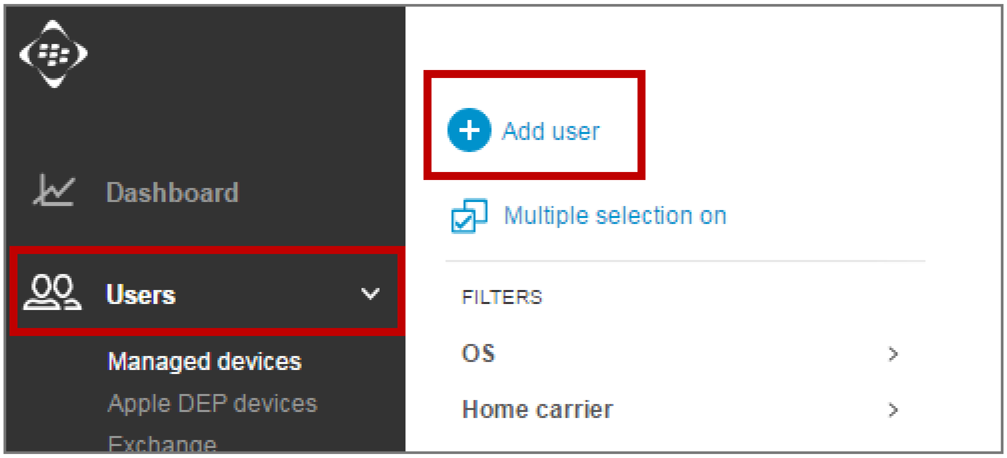
> **Note:** You can integrate with your Corporate User Directory to import group and associated user information. Imported information can be used for automatic provisioning of users, group based policy assignment and App distribution. Supported User Directories are Microsoft Active Directory and LDAP.

For more or updated information, please see BlackBerry's documentation at http://help.blackberry.com/en/blackberry-uem/current/getting-started-blackberry-uem-and-blackberry-dynamics/hse1372277059163.html

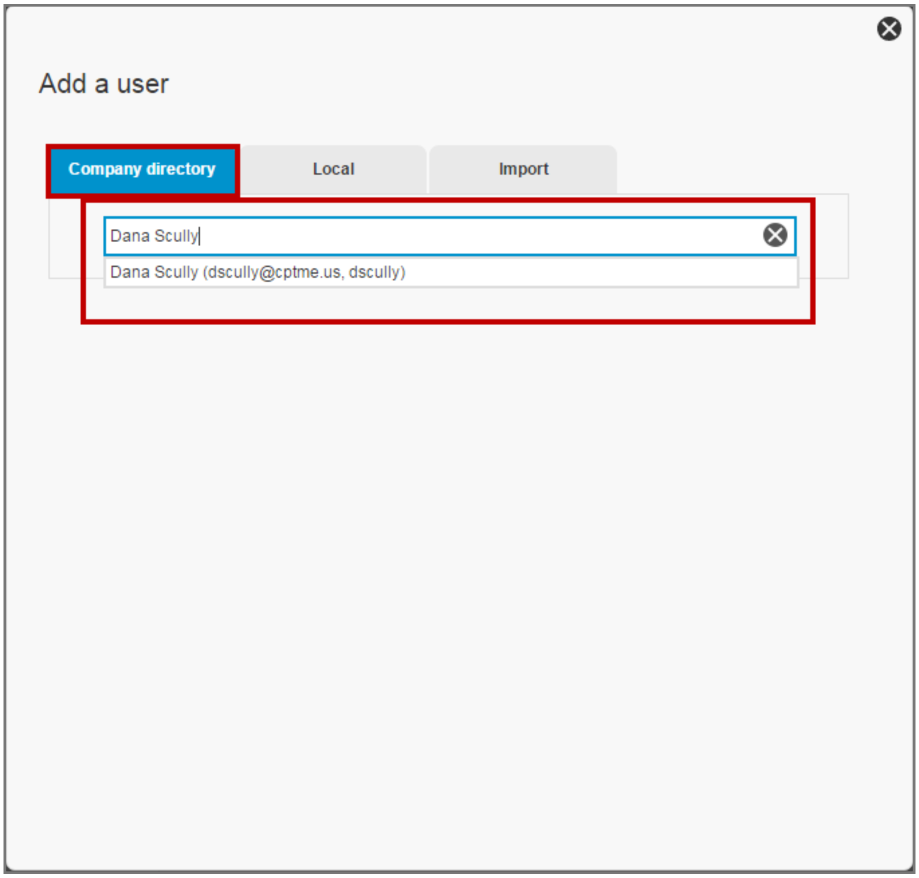
Adding a User from Corporate Directory

If you have configured your BlackBerry UEM Console to integrate with your company user directory, follow these steps to add a user to the BlackBerry UEM Console.

1. Navigate to **Users**, click "Add user".



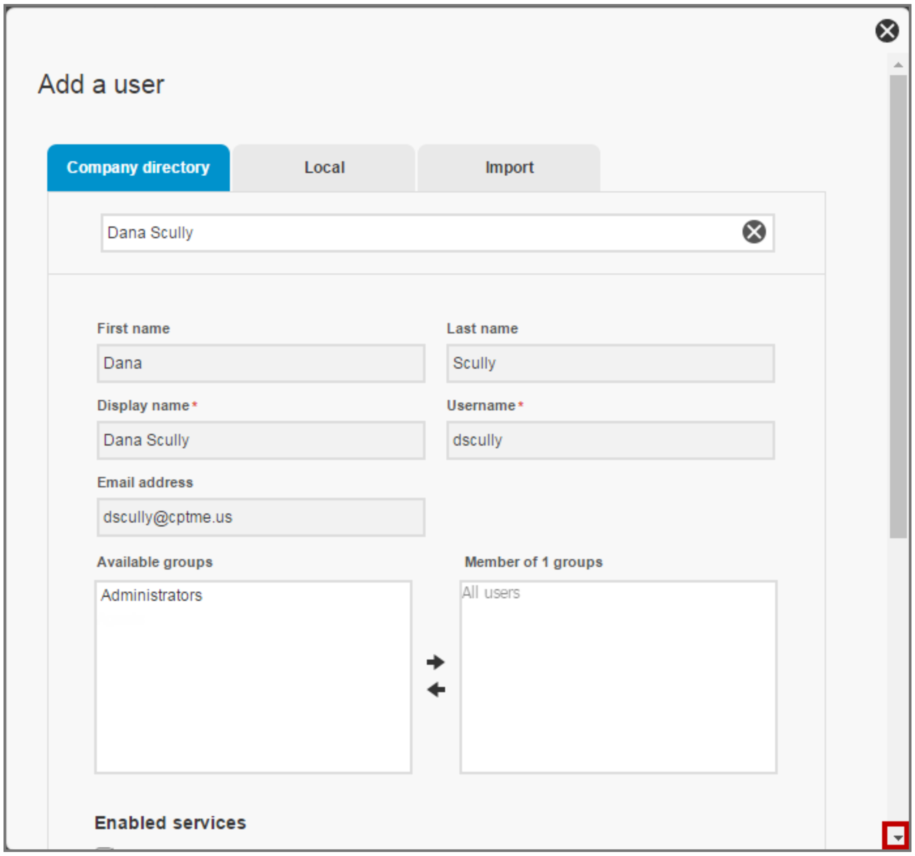
2. On the "Add a user" pop-up window "Company directory" tab, start typing the name of the user you want to add. When the name is displayed, select it from the drop-down list.



Dana Scully

Dana Scully (dscully@cptme.us, dscully)

3. The required (*) user information such as Display Name, Username, and Email address will be filled in from the company directory entry.



Add a user

Dana Scully

First name: Dana

Last name: Scully

Display name*: Dana Scully

Username*: dscully

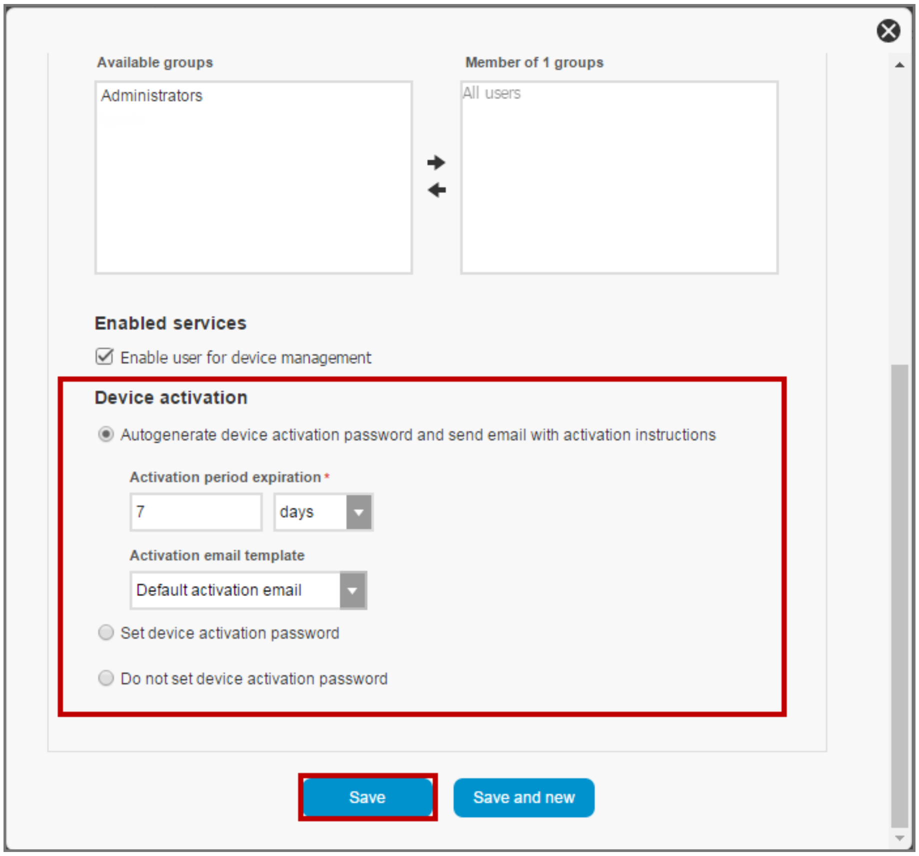
Email address: dscully@cptme.us

Available groups: Administrators

Member of 1 groups: All users

Enabled services

4. Scroll down to the bottom on the pop-up window and set the "Device activation" settings as required for your company.



Available groups

Administrators

Member of 1 groups

All users

Enabled services

☑ Enable user for device management

Device activation

● Autogenerate device activation password and send email with activation instructions

Activation period expiration *

7 days

Activation email template

Default activation email

○ Set device activation password

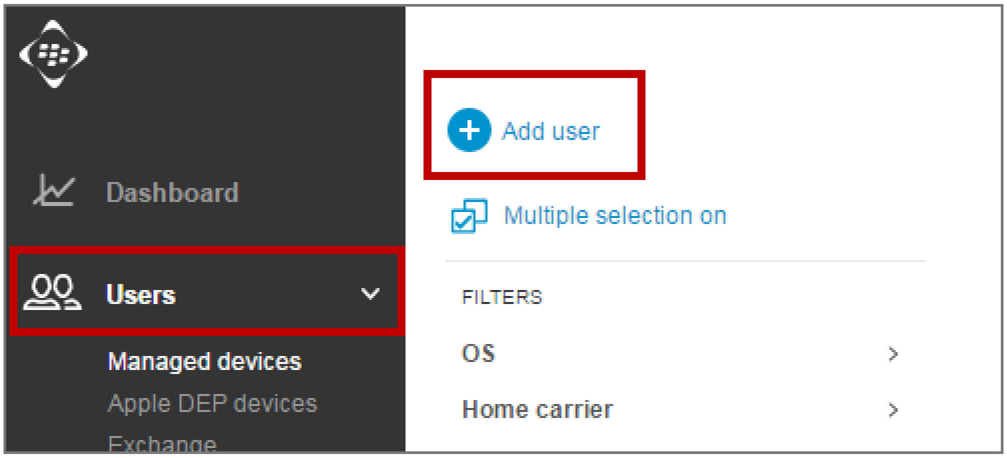
○ Do not set device activation password

5. Click "Save".

Adding a Local User

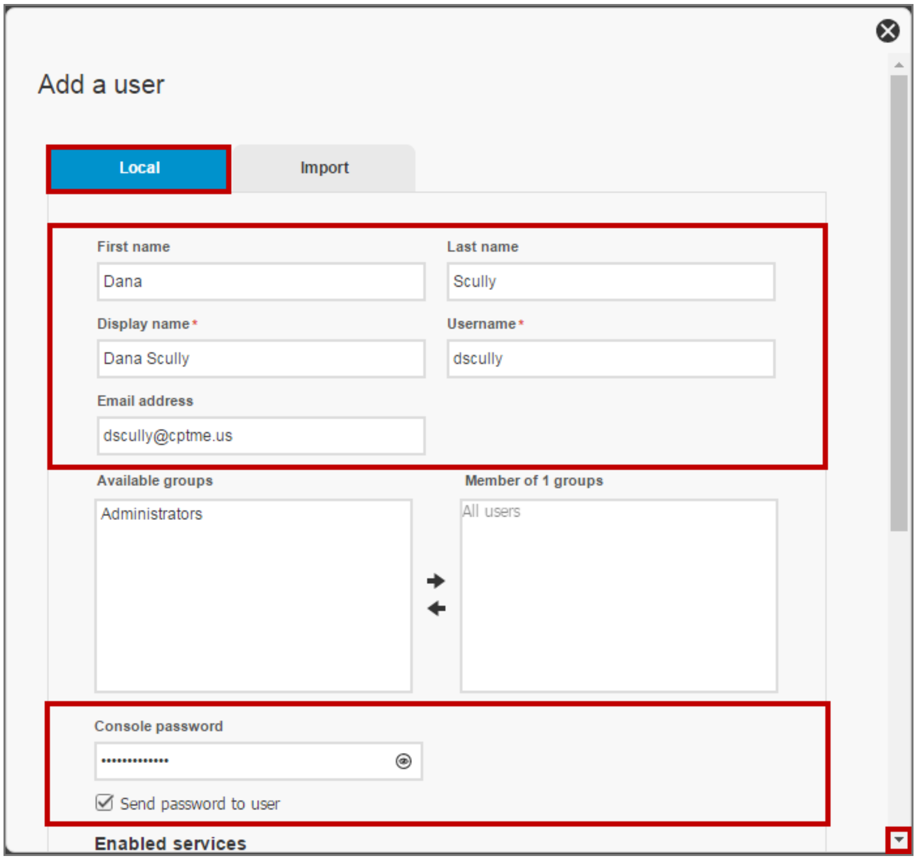
We are going to show how to add a local user using the "Add User" method.

1. Navigate to **Users**, click "Add user".



© 2018 Check Point Software Technologies Ltd. All rights reserved.

2. On the "Add a user" pop-up window "Local" tab, fill in all the required (*) fields with the appropriate information, such as in the example below.
3. Enter in a temporary console password for this user and select "Send password to user".



Add a user

Local | Import

First name: Dana
Last name: Scully
Display name*: Dana Scully
Username*: dscully
Email address: dscully@cptme.us

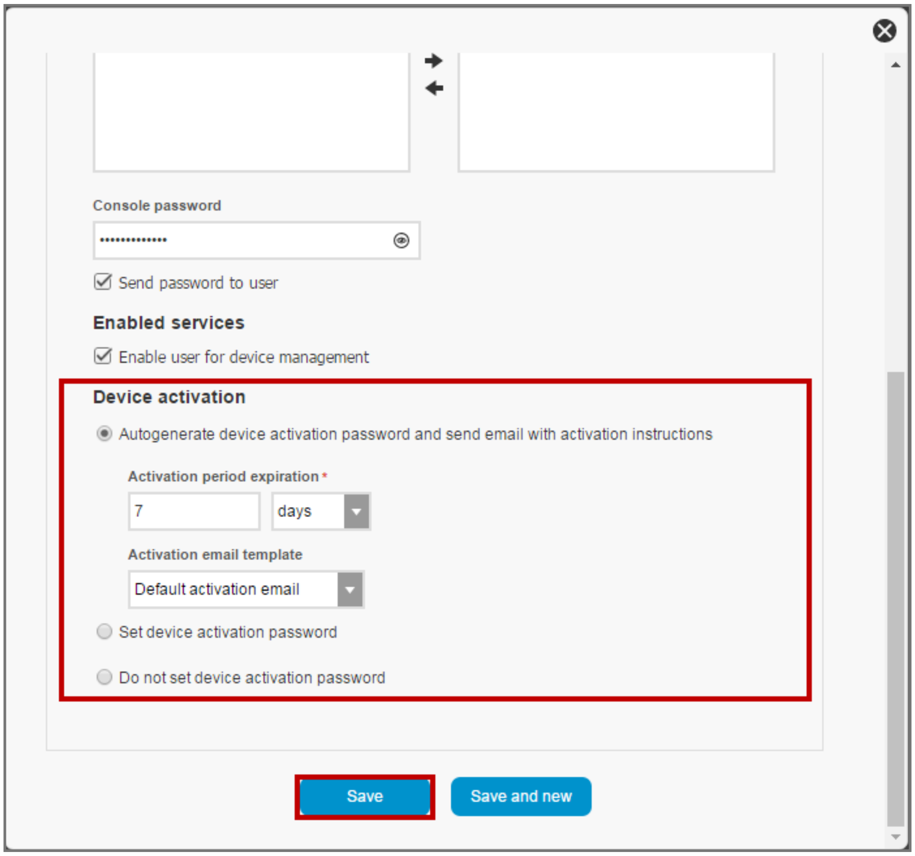
Available groups: Administrators
Member of 1 groups: All users

Console password: •••••••••••••

☑ Send password to user

Enabled services

4. Scroll down to the bottom on the pop-up window and set the "Device activation" settings as required for your company.



Console password
•••••••••••••

☑ Send password to user

Enabled services

☑ Enable user for device management

Device activation

● Autogenerate device activation password and send email with activation instructions

Activation period expiration *
7 days

Activation email template
Default activation email

○ Set device activation password

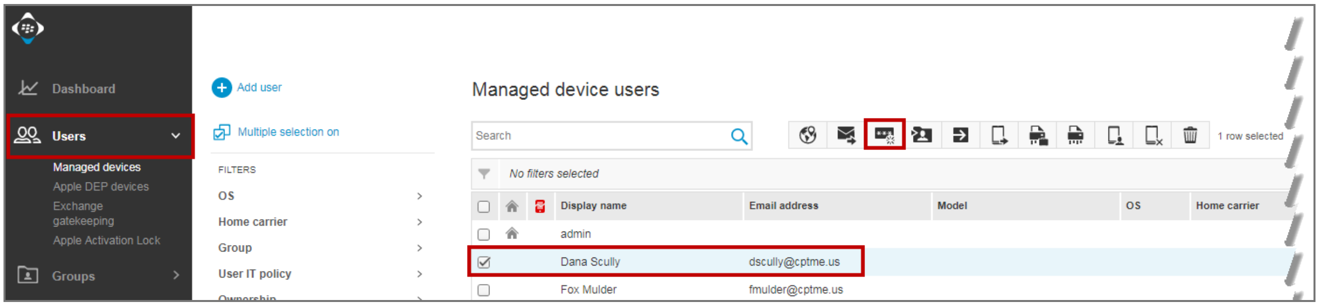
○ Do not set device activation password

5. Click "Save".

> **Note:** The user is already notified with device enrollment procedures upon the creation of the user.

Adding a Device to an Existing User

1. Navigate to **Users**, scroll to or search for the user, and select that user.
2. Click "Send activation email".



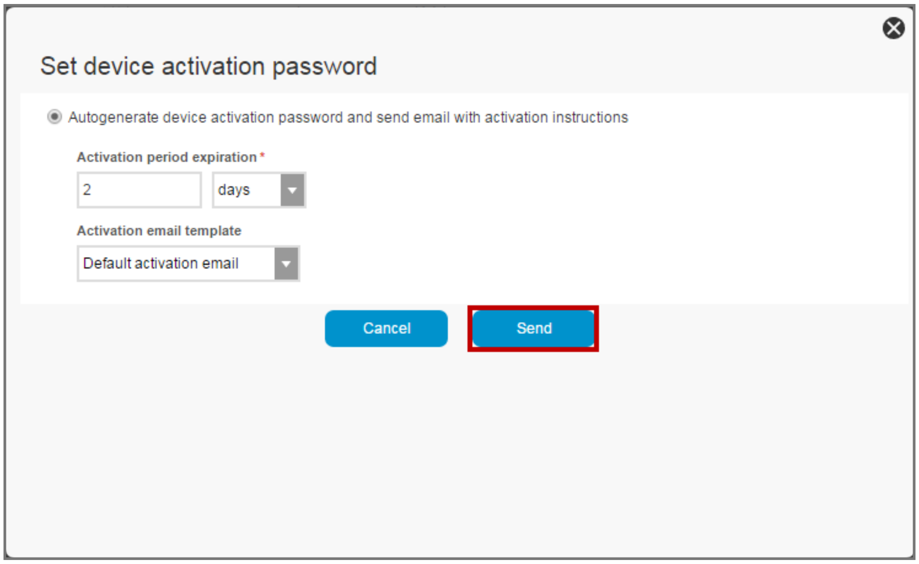
Managed device users

No filters selected

			Display name	Email address	Model	OS	Home carrier
□			admin				
☑			Dana Scully	dscully@cptme.us			
□			Fox Mulder	fmulder@cptme.us			

© 2018 Check Point Software Technologies Ltd. All rights reserved.

3. On the "Set device activation password" pop-up window, Set the "Device activation" settings as required for your company.



Set device activation password

● Autogenerate device activation password and send email with activation instructions

Activation period expiration *: 2 days

Activation email template: Default activation email

4. Click "Send".

> **Note:** Repeat these steps to add another device.

Creating User Provisioning Groups

To create a group of users whose devices will be registered to the Check Point SandBlast Mobile solution, follow this procedure.

Information about Device Risk & Status tags and BlackBerry UEM user groups

User groups are how BlackBerry UEM applies policies and assigns/deploys apps.

For more or updated information about adding user groups, see BlackBerry's documentation at:

http://help.blackberry.com/en/blackberry-uem/current/getting-started-blackberry-uem-and-blackberry-dynamics/managing_user_groups_and_user_accounts.html

SandBlast Mobile utilizes these groups to move devices in and out of 7 pre-defined groups, and one freeform mitigation group.

There are 3 pre-defined status groups:

- CHKP_Status_Provisioned
- CHKP_Status_Active
- CHKP_Status_Inactive

When a device is provisioned in SandBlast Mobile Dashboard, this device is placed in the CHKP_Status_ Provisioned group.

After the user has installed and registered to SandBlast Mobile, this device is moved from the CHKP_Status_ Provisioned group to the CHKP_Status_Active group.

If the device hasn't checked-in with SandBlast Mobile for X number of days (configured by the SandBlast Mobile Admin), then the device is moved from CHKP_Status_Active to CHKP_Status_Inactive.

There are 4 pre-defined risk groups:

- CHKP_Risk_None
- CHKP_Risk_Low
- CHKP_Risk_Medium
- CHKP_Risk_High

If a device is determined to be at High, Medium, or Low risk, the device is placed in the respective group. If the device has no risks, then it is placed in the CHKP_Risk_None group.

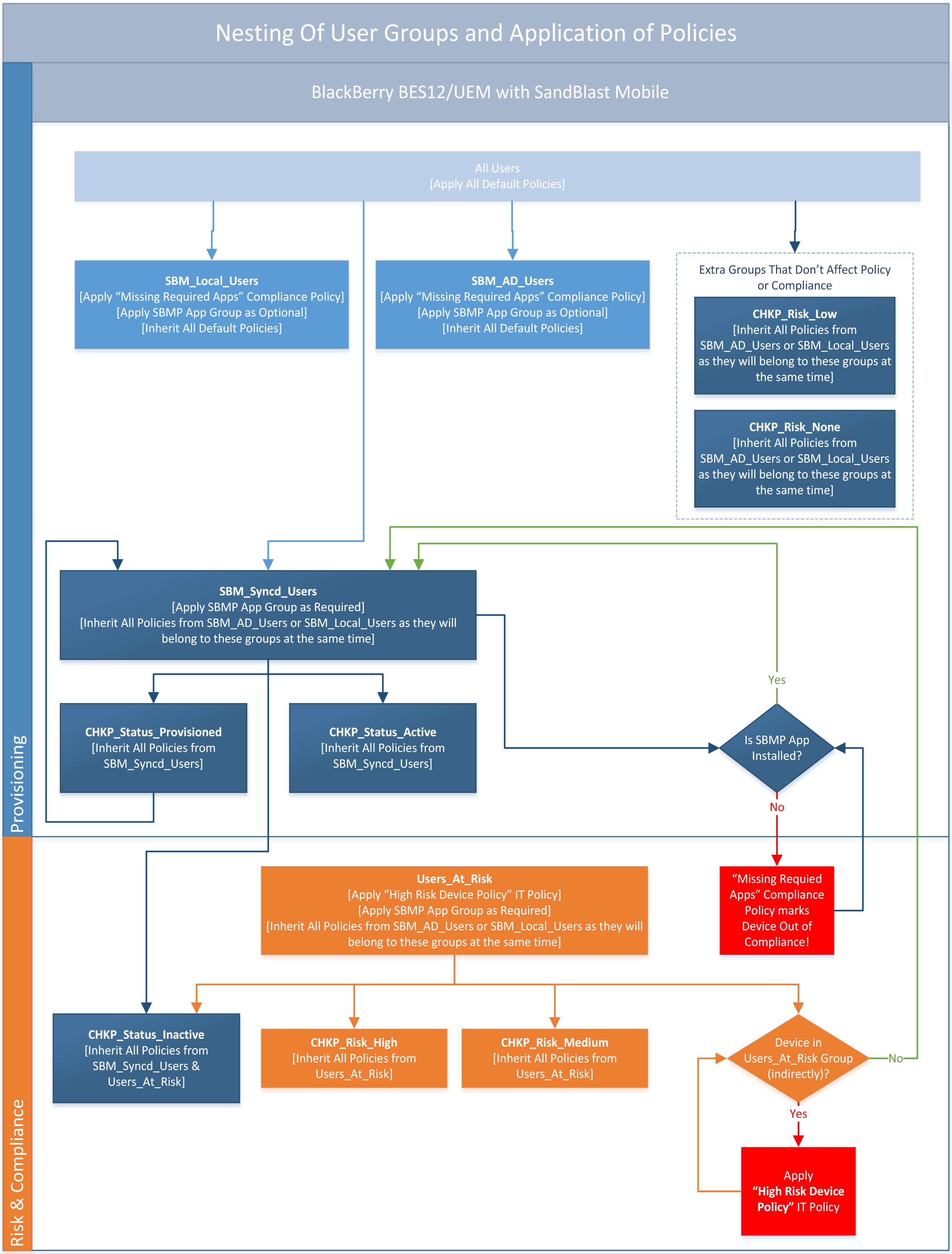
For example, if the device has a Low risk app and a High risk (malicious) SMS URL, then the device will appear in both the CHKP_Risk_Low and CHKP_Risk_High groups.

The freeform mitigation group is any unique name, such as "Users_At_High_Risk", that SandBlast Mobile will place only devices determined to be at High Risk. It does not provided the granularity of the different risk levels of the device, just high risk state. This method was the original way to group devices at high risk, and it is strongly recommended that you implement the CHKP Risk and Status groups instead of using the freeform group.

In "Creating Local User Group(s)" on page 18, we will create these pre-defined SandBlast Mobile groups and nest them according to how we want our corporate policies to be applied.

In our example, devices that are members of CHKP_Risk_High, CHKP_Risk_Medium, or CHKP_Status_Inactive will be considered to be "Users_At_Risk", and have the appropriate Mitigation Policies applied as defined later in "Creating a Mitigation Process" on page 55. Devices that are members of CHKP_Risk_None or CHKP_Risk_Low, will not have the mitigation policies applied.

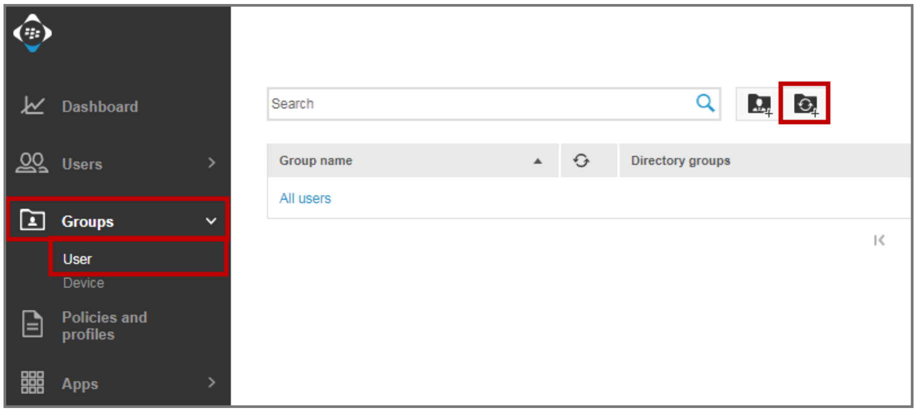
See the following diagram on how polices and group nesting are applied.


Nesting Of User Groups and Application of Policies
BlackBerry BES12/UEM with SandBlast Mobile
Provisioning
Risk & Compliance
All Users
[Apply All Default Policies]
SBM_Local_Users
[Apply "Missing Required Apps" Compliance Policy]
[Apply SBMP App Group as Optional]
[Inherit All Default Policies]
SBM_AD_Users
[Apply "Missing Required Apps" Compliance Policy]
[Apply SBMP App Group as Optional]
[Inherit All Default Policies]
Extra Groups That Don't Affect Policy or Compliance
CHKP_Risk_Low
[Inherit All Policies from SBM_AD_Users or SBM_Local_Users as they will belong to these groups at the same time]
CHKP_Risk_None
[Inherit All Policies from SBM_AD_Users or SBM_Local_Users as they will belong to these groups at the same time]
SBM_Syncd_Users
[Apply SBMP App Group as Required]
[Inherit All Policies from SBM_AD_Users or SBM_Local_Users as they will belong to these groups at the same time]
CHKP_Status_Provisioned
[Inherit All Policies from SBM_Syncd_Users]
CHKP_Status_Active
[Inherit All Policies from SBM_Syncd_Users]
Yes
Is SBMP App Installed?
No
"Missing Requied Apps" Compliance Policy marks Device Out of Compliance!
Users_At_Risk
[Apply "High Risk Device Policy" IT Policy]
[Apply SBMP App Group as Required]
[Inherit All Policies from SBM_AD_Users or SBM_Local_Users as they will belong to these groups at the same time]
CHKP_Status_Inactive
[Inherit All Policies from SBM_Syncd_Users & Users_At_Risk]
CHKP_Risk_High
[Inherit All Policies from Users_At_Risk]
CHKP_Risk_Medium
[Inherit All Policies from Users_At_Risk]
Device in Users_At_Risk Group (indirectly)?
No
Yes
Apply "High Risk Device Policy" IT Policy

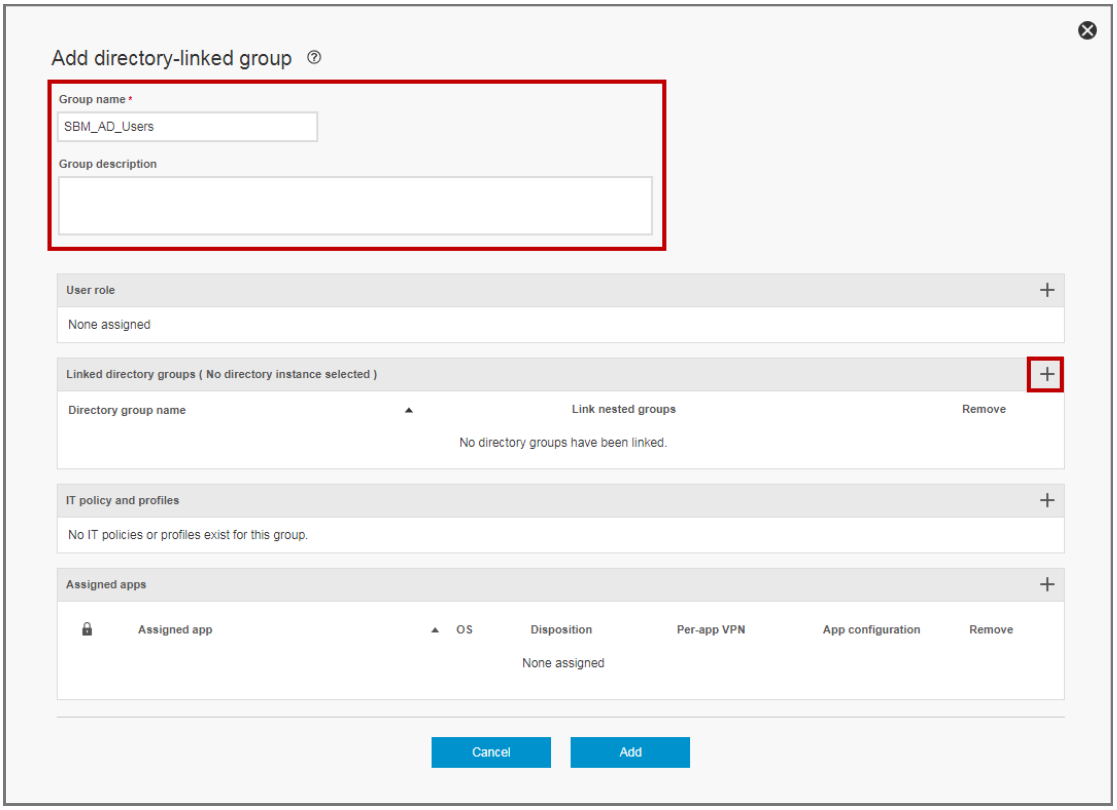
Creating a User Group based on Corporate User Directory

In this section we will create a User Group that is tied to Active Directory.

1. Navigate to **Groups > User**, click "Add a directory-linked group" icon.



2. On the "Add directory-linked group" pop-up window, enter in a Group Name, such as "SBM_AD_Users", and, if desired, a Group Description.


Add directory-linked group

Group name *: SBM_AD_Users

Group description:

User role: None assigned

Linked directory groups (No directory instance selected)

Directory group name	Link nested groups	Remove
No directory groups have been linked.		

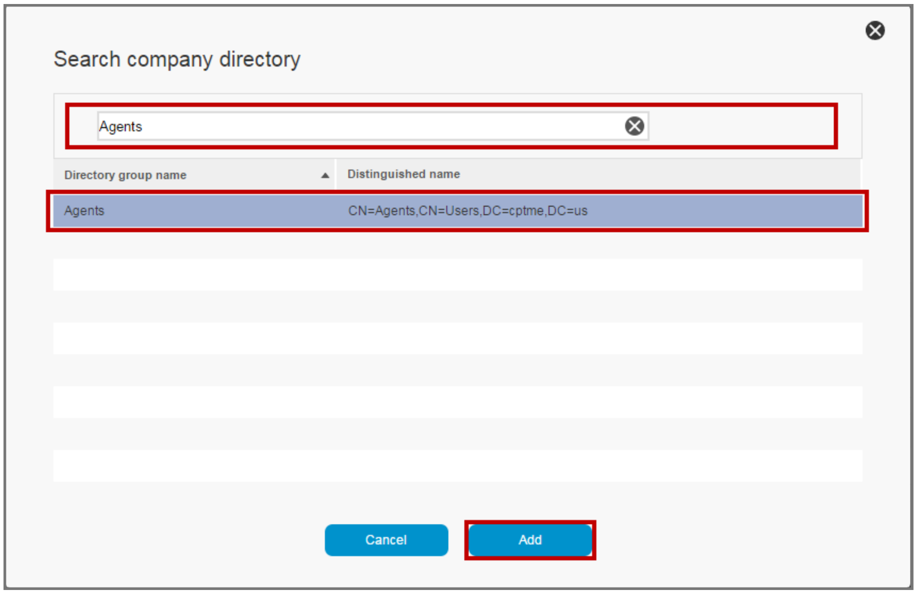
IT policy and profiles: No IT policies or profiles exist for this group.

Assigned apps

	Assigned app	OS	Disposition	Per-app VPN	App configuration	Remove
None assigned						

3. Click "+" sign to add a Linked directory group.

4. On the "Search company directory" pop-up window, enter in the first few letters of the corporate directory group you want to link, and hit enter.



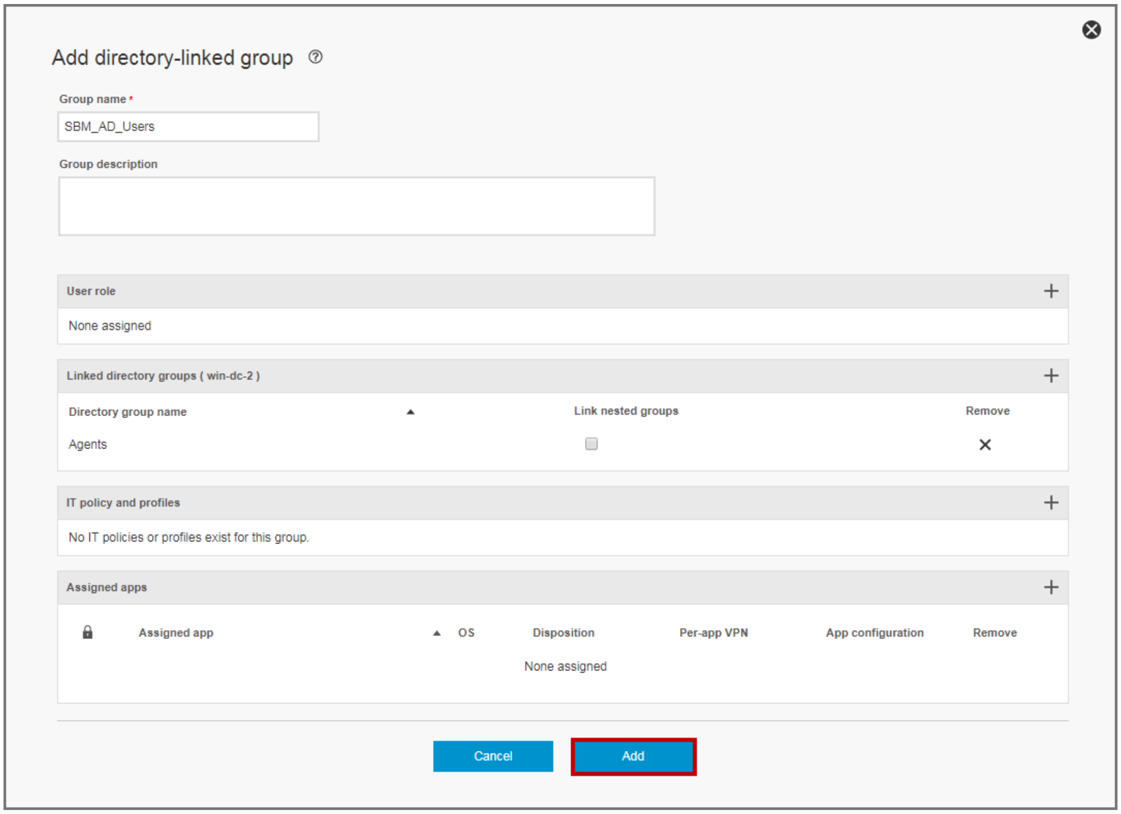
Search company directory

Agents

Directory group name	Distinguished name
Agents	CN=Agents,CN=Users,DC=cptme,DC=us

5. Click "Add".

6. We haven’t created any IT policies and profiles or added Apps to our App Catalog as of yet, so we will add those in subsequent sections.



Add directory-linked group

Group name *
SBM_AD_Users

Group description

User role
None assigned

Linked directory groups (win-dc-2)

Directory group name	Link nested groups	Remove
Agents	☐	✕

IT policy and profiles
No IT policies or profiles exist for this group.

Assigned apps

🔒	Assigned app	OS	Disposition	Per-app VPN	App configuration	Remove
			None assigned			

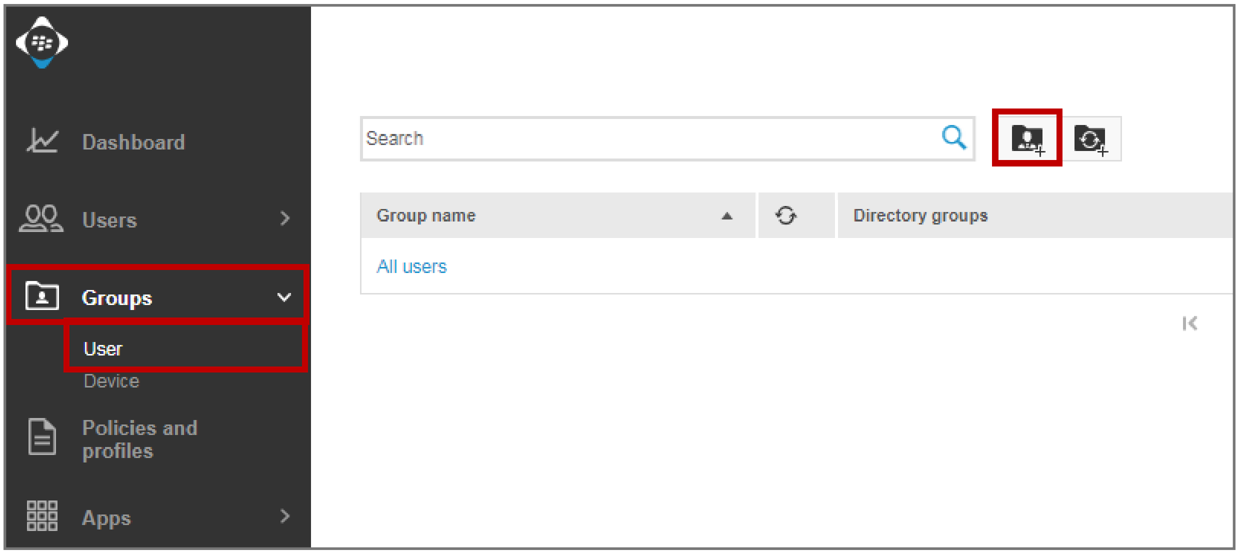
7. Click "Add".

Creating Local User Group(s)

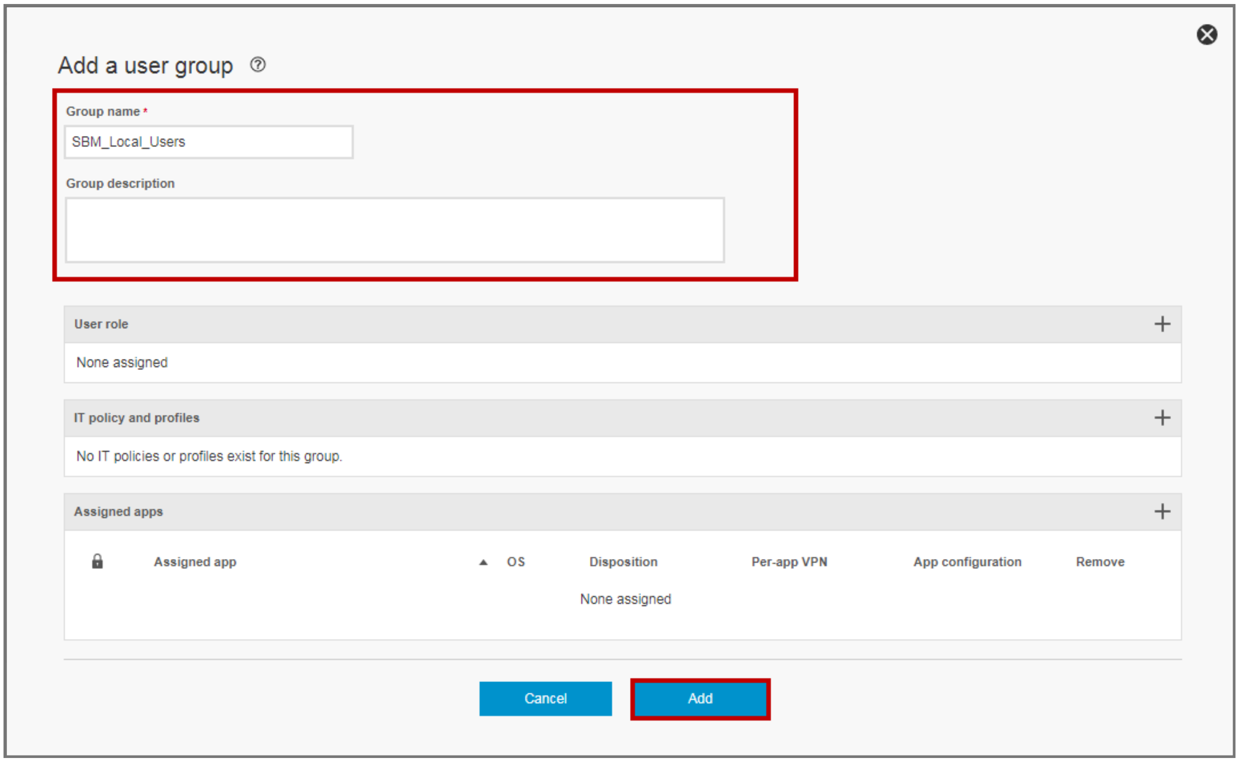
In this section, we will create all of the User Groups we need for Provisioning, Monitoring, and Mitigation. These groups are:

- **Optional User Groups**, but recommended in order to simplify applying policies, deploying apps, and mitigating risks. Some of the required user groups will be nested under these groups as discussed further in "Information about Device Risk & Status tags and BlackBerry UEM user groups" on page 13 and in "Nesting User Groups (Optional)" on page 23.
  - SBM_Syncd_Users
  - Users_At_Risk
- **Required User Group** if not using AD User Group
  - SBM_Local_Users
- **Required User Groups for Integration** if using Tag Device Status and Tag Device Risk
  - CHKP_Status_Provisioned
  - CHKP_Status_Active
  - CHKP_Status_Inactive
  - CHKP_Risk_None
  - CHKP_Risk_Low
  - CHKP_Risk_Medium
  - CHKP_Risk_High

1. Navigate to **Groups > User**, click "Add a user group" icon.



2. On the "Add a user group" pop-up window, enter in a Group Name, such as "SBM_Local_Users", and, if desired, a Group Description.



Add a user group

Group name * SBM_Local_Users

Group description

User role

None assigned

IT policy and profiles

No IT policies or profiles exist for this group.

Assigned apps

	Assigned app	OS	Disposition	Per-app VPN	App configuration	Remove
			None assigned			

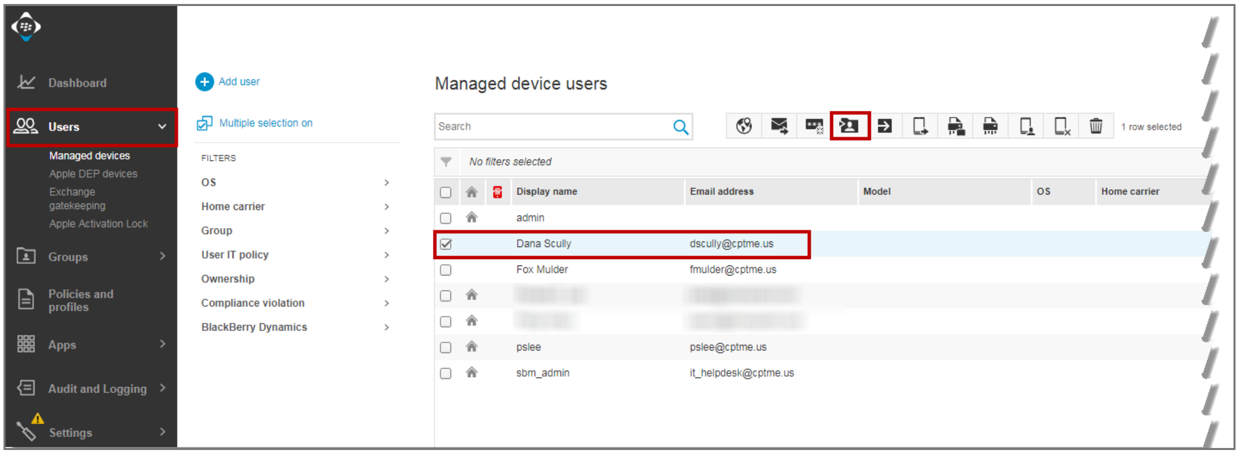
3. We haven't created any IT policies and profiles or added Apps to our App Catalog as of yet, so we will add those in subsequent sections.
4. Click "Add".

Note: Repeat these steps to add all the user groups listed above.

Adding an Existing User to the Local User Group

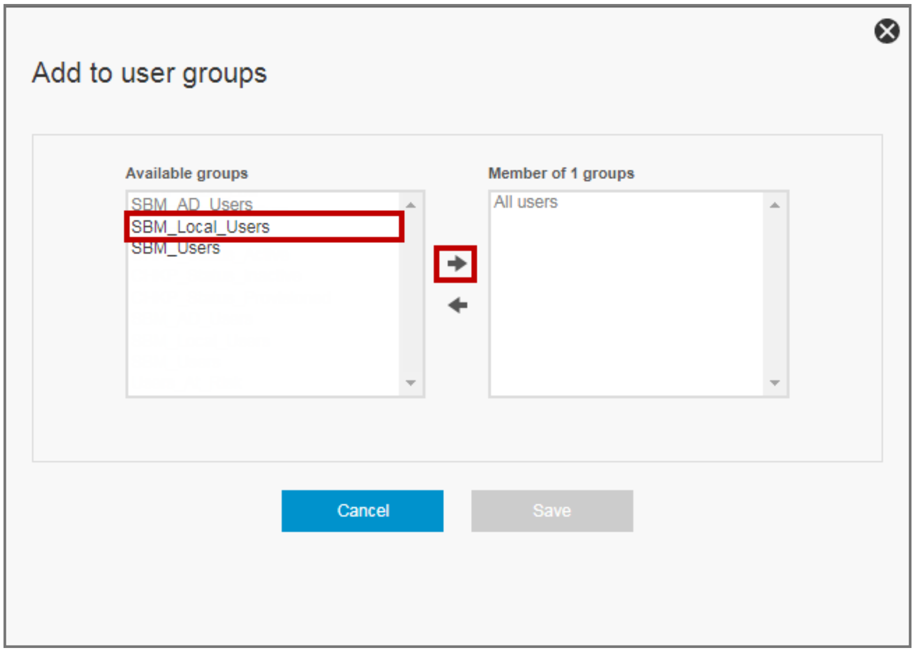
To add an existing user to the User Group we created in "Creating a User Group based on Corporate User Directory" on page 16 or "Creating Local User Group(s)" on the previous page, follow this procedure. Our example will be using the Local User group ("SBM_Local_Users").

1. Navigate to **Users**, scroll and select the user you want to add to the user group, and click the "Add to user groups" icon.

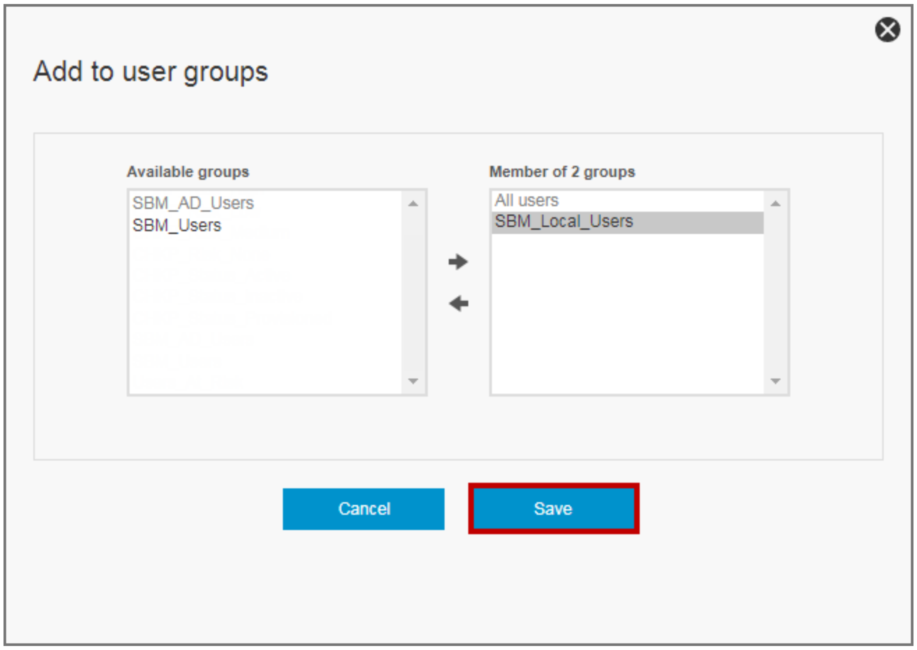


			Display name	Email address	Model	OS	Home carrier
□			admin				
☑			Dana Scully	dscully@cptme.us			
□			Fox Mulder	fmulder@cptme.us			
□			[redacted]	[redacted]			
□			[redacted]	[redacted]			
□			pslee	pslee@cptme.us			
□			sbm_admin	it_helpdesk@cptme.us			

2. On the "Add to user groups" pop-up window, select the SBM_Local_Users from the "Available groups" list, can click right arrow.



3. Click "Save".


Add to user groups

Available groups
- SBM_AD_Users
- SBM_Users

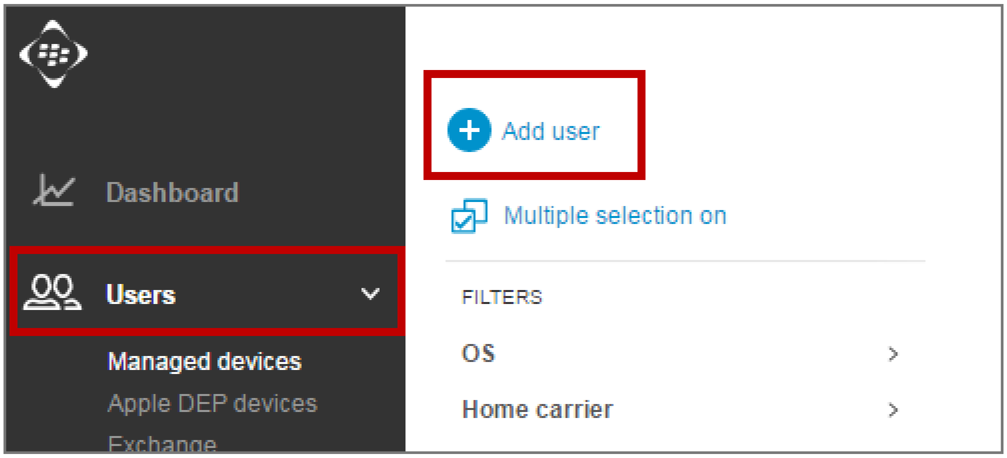
Member of 2 groups
- All users
- SBM_Local_Users

4. The User is now part of the User Group "SBM_Local_Users".

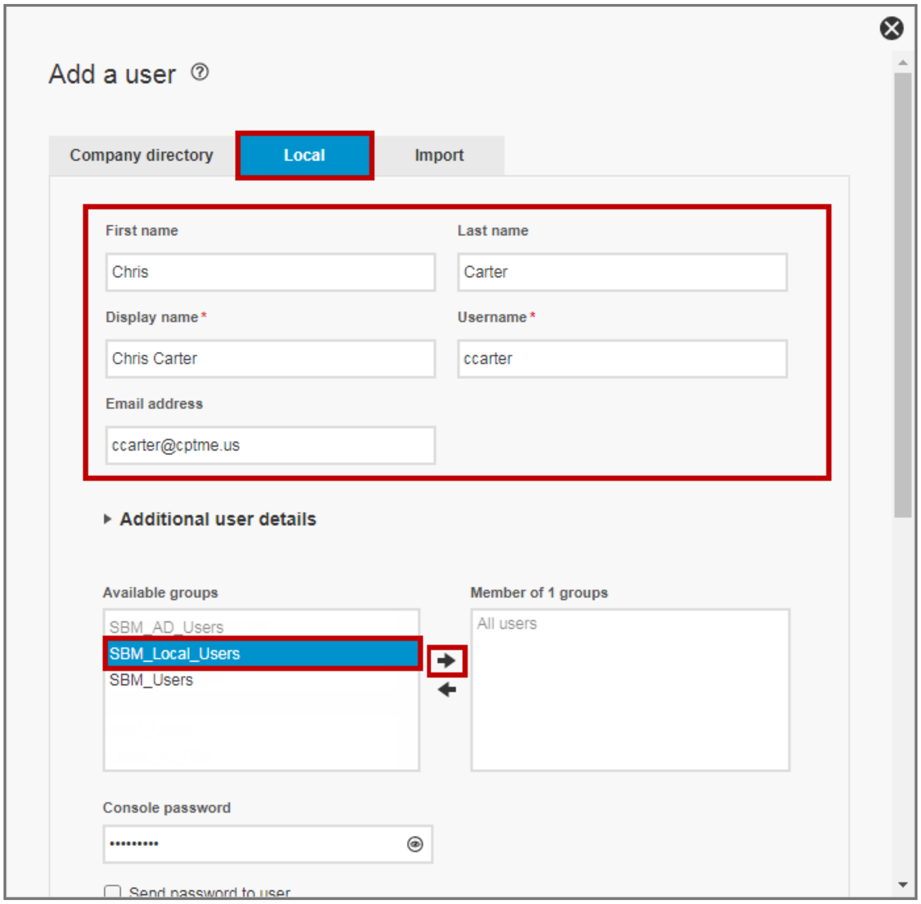
Adding a New User to an Existing Local User Group

Adding a new user to an existing user group is close to the same procedure in "Adding a User" on page 7.

1. Navigate to **Users**, click "Add user".



2. On the "Add a user" pop-up window "Local" tab, fill in all the required (*) fields with the appropriate information, such as in the example below.
3. Select the User Group from the "Available groups" list and click right arrow.


Add a user ⓘ

First name: Chris
Last name: Carter
Display name*: Chris Carter
Username*: ccarter
Email address: ccarter@cptme.us

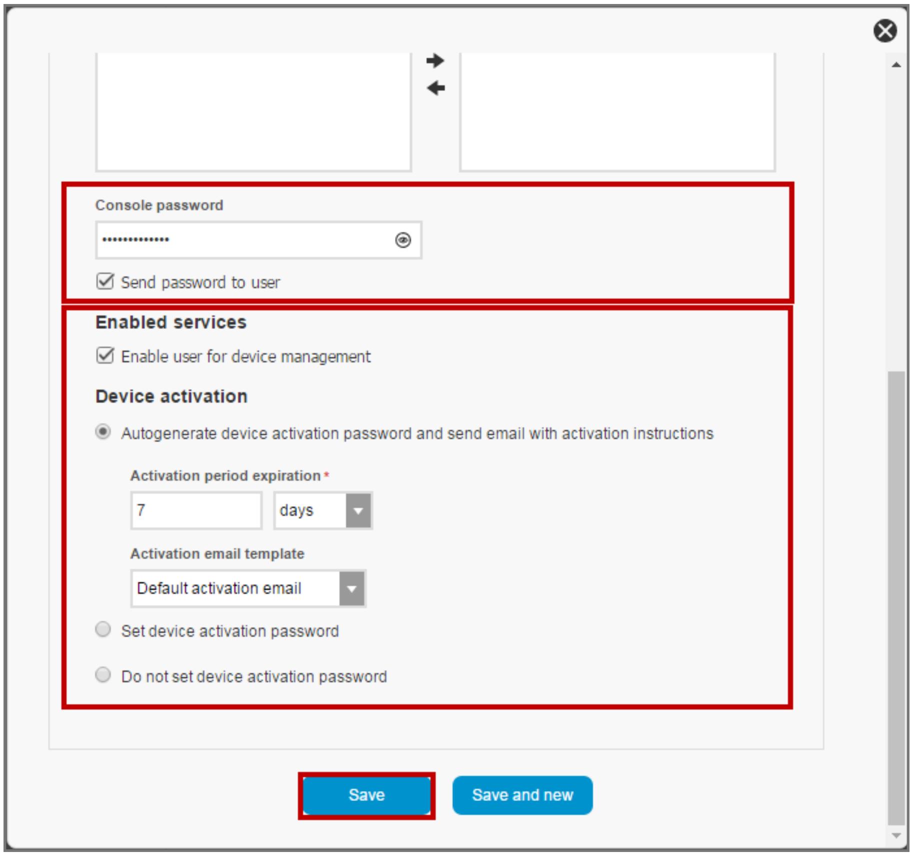
Available groups:
SBM_AD_Users
SBM_Local_Users
SBM_Users

Member of 1 groups:
All users

Console password: •••••••••

□ Send password to user

4. Scroll down to the bottom on the pop-up window, and enter in a temporary console password for this user and select "Send password to user".
5. Set the "Device activation" settings as required for your company.



Console password: ••••••••••••

☑ Send password to user

Enabled services

☑ Enable user for device management

Device activation

● Autogenerate device activation password and send email with activation instructions

Activation period expiration *: 7 days

Activation email template: Default activation email

○ Set device activation password

○ Do not set device activation password

6. Click "Save".

> **Note:** The user is already notified with device enrollment procedures upon the creation of the user.

Nesting User Groups (Optional)

We will be nesting the user groups that we created in "Creating Local User Group(s)" on page 18 and as discussed in "Information about Device Risk & Status tags and BlackBerry UEM user groups" on page 13.

This will simplify the policy enforcement.

> **Note:** If you do not want to create nested user groups, then you must apply the appropriate policies, apps, etc to each group individually as inheritance only occurs from parent group to child group.

In our example, we will nest our groups as follows:

- SBM_Syncd_Users
  - CHKP_Status_Provisioned
  - CHKP_Status_Active

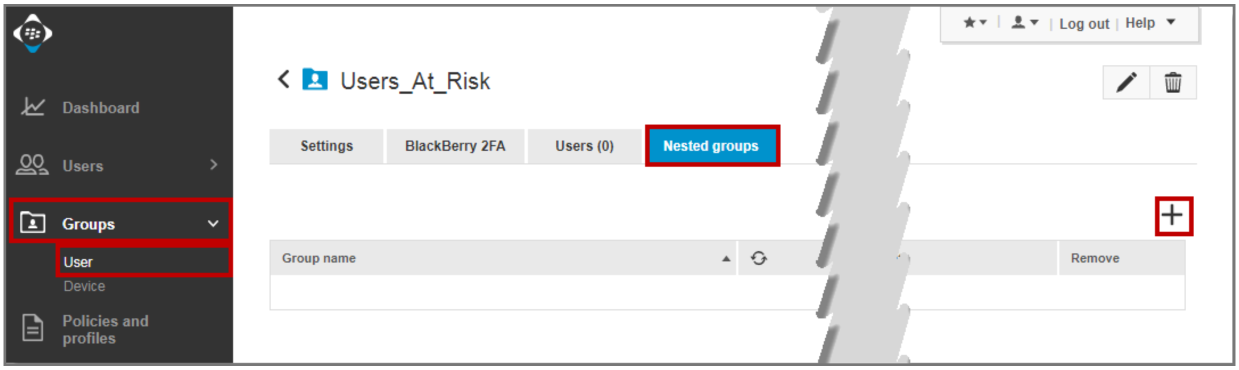
© 2018 Check Point Software Technologies Ltd. All rights reserved.

  - CHKP_Status_Inactive
- Users_At_Risk
  - CHKP_Risk_High
  - CHKP_Risk_Medium
  - CHKP_Status_Inactive

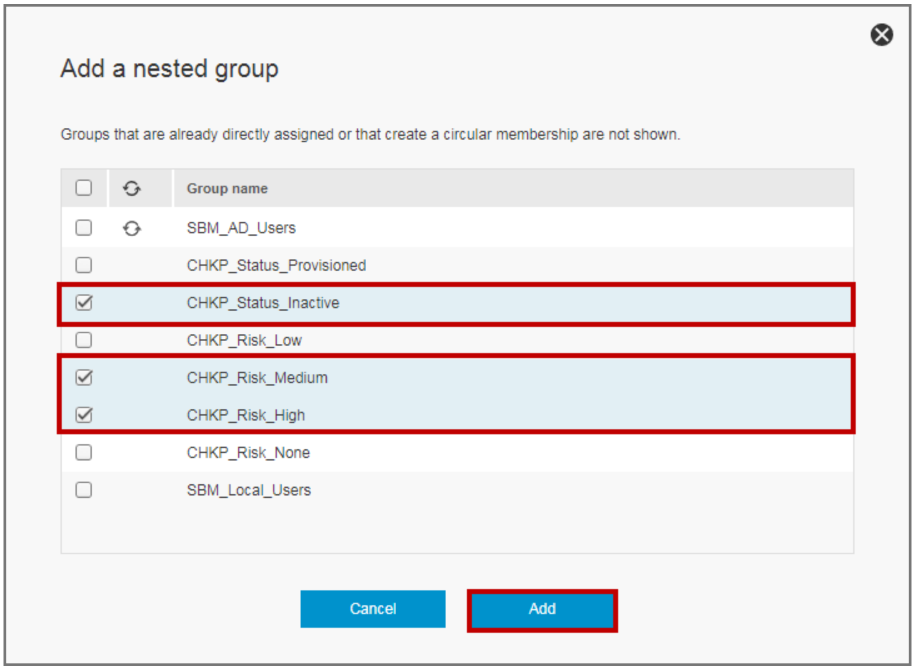
Also, if you want devices at Low Risk to be subject to the same Non-Compliant policies as those at High Risk, simply nest CHKP_Risk_Low under Users_At_Risk.

For more or updated information about nested groups in BlackBerry UEM, see http://help.blackberry.com/en/blackberry-uem/current/administration/jth1410530746516.html

1. Navigate to **Groups > User**, and select "Users_At_Risk" to edit it.
2. Select "Nested groups" tab, and click "+".



3. On the "Add a nested group" pop-up window, select CHKP_Status_Inactive, CHKP_Risk_Medium, and CHKP_Risk_High.


Add a nested group

Groups that are already directly assigned or that create a circular membership are not shown.

□		Group name
□		SBM_AD_Users
□		CHKP_Status_Provisioned
☑		CHKP_Status_Inactive
□		CHKP_Risk_Low
☑		CHKP_Risk_Medium
☑		CHKP_Risk_High
□		CHKP_Risk_None
□		SBM_Local_Users

4. Click "Add".

Note: Repeat these steps for adding the appropriate nested groups for SBM_Syncd_Users.

Enrolling Devices to BlackBerry UEM

For iOS device, see **http://help.blackberry.com/en/blackberry-uem/current/getting-started-blackberry-uem-and-blackberry-dynamics/adr1451941812493.html** for more details.

For Android device, see **http://help.blackberry.com/en/blackberry-uem/current/getting-started-blackberry-uem-and-blackberry-dynamics/adr1451941820349.html** for more details.

Note: At this point, we have all the information we will need to configure the UEM integration settings in the SandBlast Mobile Dashboard.

From Our Examples:

- **Server URL** = https://<FQDN of BlackBerry UEM Server>:<port to Web Services API> (ie. https://uem.acme.us:18084)
- **SandBlast Mobile API Admin Username/Password** = sbm_admin/<hidden>
- **User Provisioning Group(s)** = SBM_Local_Users; SBM_AD_Users

© 2018 Check Point Software Technologies Ltd. All rights reserved.

Chapter 2

Configuring the SandBlast Mobile Dashboard UEM Integration Settings

This chapter discusses the following:

Prerequisites

You will need the following details from your BlackBerry UEM Deployment:

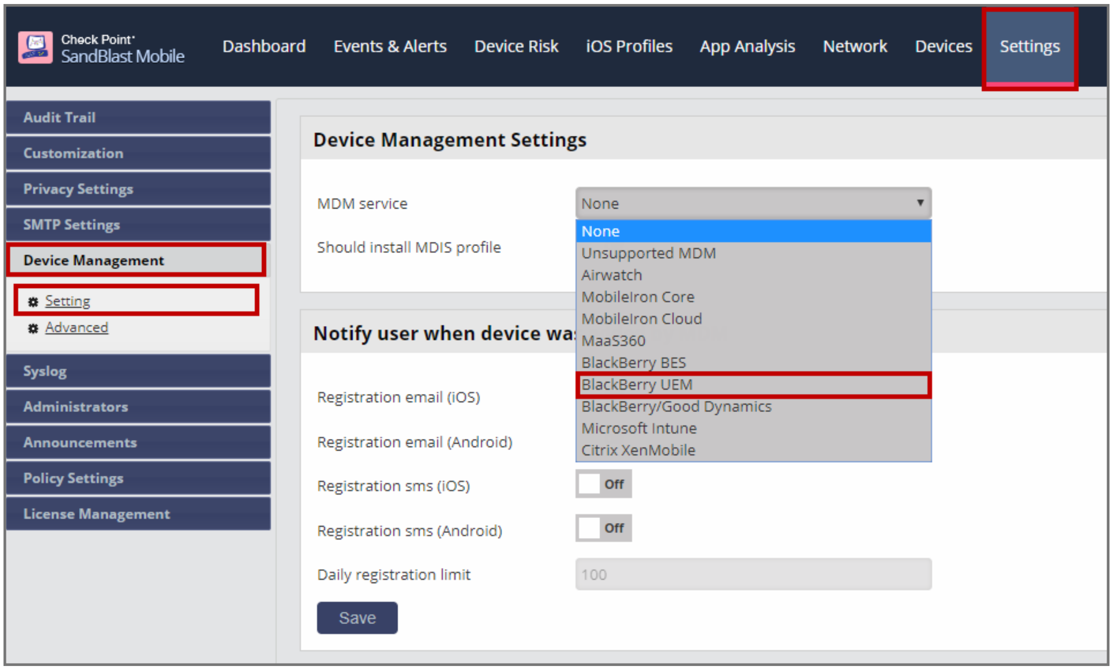
Note: There is a table in "Integration Information" on page 70 that you can record your settings for easy reference.

1. **Server:** The root URL to your BlackBerry UEM Web Services API including the leading https://, such as https://uem.acme.us:18084
2. **SRP ID:** This is the SRP ID from BlackBerry licensing registered to your instance, in the form of S12345678. This value can be found by going to **BlackBerry UEM Console > Help > About BlackBerry UEM**.
3. **BlackBerry UEM SandBlast Mobile Administrator 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 API Admin account in "Creating an API Administrator Account (optional)" on page 2 for this purpose.
4. **Groups(s):** These are the BlackBerry UEM user provisioning groups to which the users/devices to be registered to SandBlast Mobile are grouped, and 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 (;). These are the User Provisioning Groups we created in "Creating User Provisioning Groups" on page 13 ("SBM_Local_Users; SBM_AD_Users").
5. **Mitigation Group:** This field will not be used as we will be using the CHKP Risk and Status tags, as defined in "Creating Local User Group(s)" on page 18.
6. For **on-premise UEM environments**, the BlackBerry UEM Web Services port (TCP 18084) must be remotely accessible through your firewall from the SandBlast Mobile Dashboard to the UEM system before trying to connect.
7. Delete any existing devices in the SandBlast Mobile Dashboard, and ensure that any devices that are to be enrolled via BlackBerry UEM integration are removed from other SandBlast Mobile Dashboards.

Note: Only the devices are synchronized from BlackBerry UEM 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.

Configuring Device Management Settings

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



Device Management Settings

MDM service: None

Should install MDIS profile

Notify user when device wa

Registration email (iOS)

Registration email (Android)

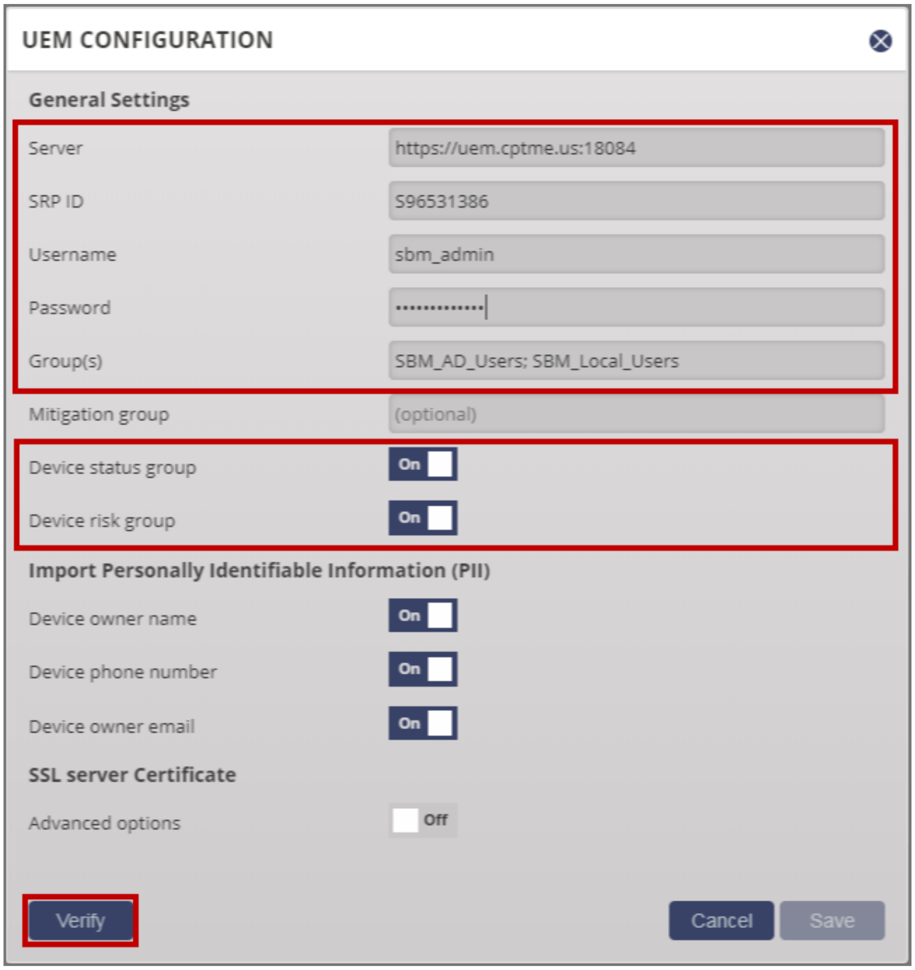
Registration sms (iOS): Off

Registration sms (Android): Off

Daily registration limit: 100

3. A pop-up window will open.

4. Configure the settings as are appropriate for your BlackBerry UEM Deployment, such as those you have created in "Preparing the UEM Platform for Integration" on page 1.
5. Turn ON the "Tag Device Status" and "Tag Device Risk" toggles. Additional information regarding these tags can be found in "Information about Device Risk & Status tags and BlackBerry UEM user groups" on page 13 and in "Multi-tags in SandBlast Mobile and Usage in BlackBerry UEM" on page 31.
6. If your organization does not want to import any of the Personally Identifiable Information (PII), these toggles can be turned OFF for Owner Name, Phone Number, and/or Owner Email address. See additional information in "Controlling the Importing of Personally Identifiable Information (PII) from the UEM" on page 32.



UEM CONFIGURATION

General Settings

Server: https://uem.cptme.us:18084

SRP ID: S96531386

Username: sbm_admin

Password: •••••••••••••

Group(s): SBM_AD_Users; SBM_Local_Users

Mitigation group: (optional)

Device status group: On

Device risk group: On

Import Personally Identifiable Information (PII)

Device owner name: On

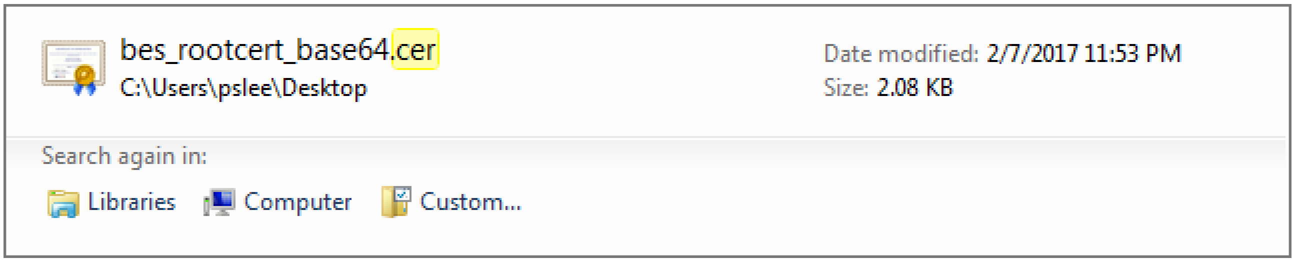
Device phone number: On

Device owner email: On

SSL server Certificate

Advanced options: Off

7. If the BlackBerry UEM instance is self-signed, you can upload the 64Base Certificate information to the SandBlast Mobile server by turning on "Advanced options", by click "Upload Certificate" and selecting the Base64 certificate you saved from your UEM instance's Web Services page (i.e. https://uem.acmecorp.us:18084).

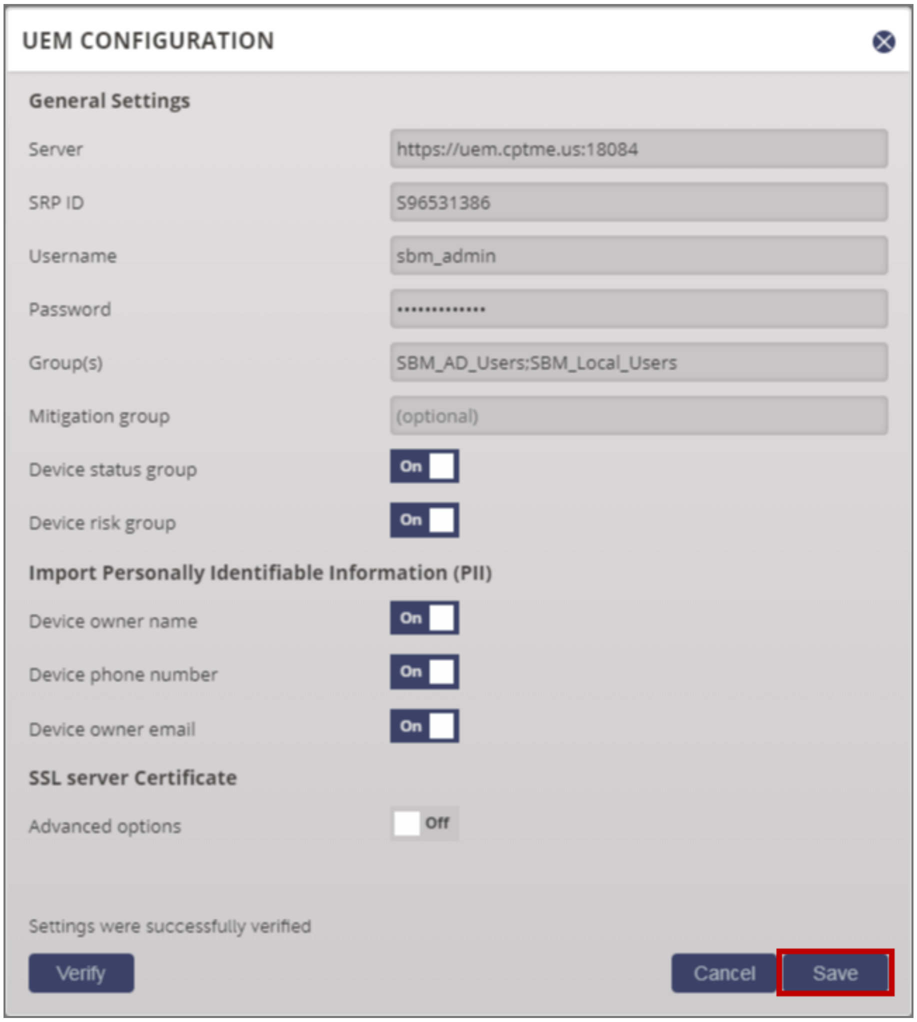


bes_rootcert_base64.cer
C:\Users\pslee\Desktop

Date modified: 2/7/2017 11:53 PM
Size: 2.08 KB

Search again in:

8. Click "Verify". If the settings are correct, and the SandBlast Mobile Dashboard can communicate with the BlackBerry UEM system, you will be able to click "Save" to finish configuration.



UEM CONFIGURATION

General Settings

Server	https://uem.cptme.us:18084
SRP ID	S96531386
Username	sbm_admin
Password	•••••••••••••
Group(s)	SBM_AD_Users;SBM_Local_Users
Mitigation group	(optional)
Device status group	On
Device risk group	On

Import Personally Identifiable Information (PII)

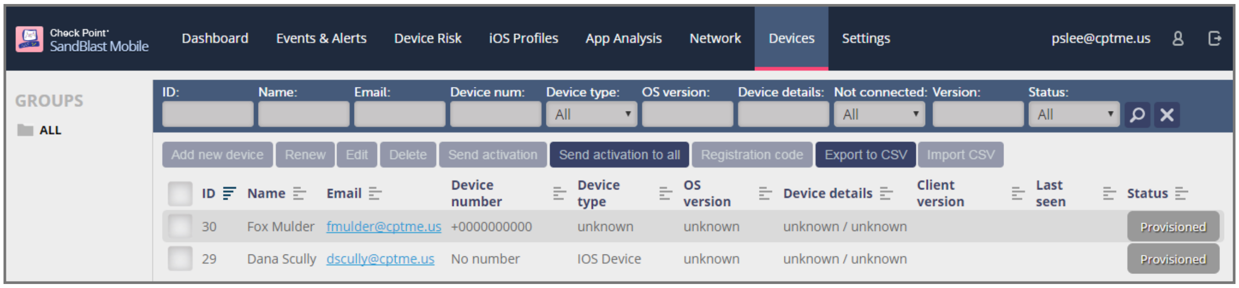
Device owner name	On
Device phone number	On
Device owner email	On

SSL server Certificate

Advanced options	Off

Settings were successfully verified

9. After successful configuration and sync, the "Devices" tab will show the devices added to SandBlast Mobile and their status as "Provisioned" which indicates that they have not yet tried to register to the SandBlast Mobile Dashboard.



ID	Name	Email	Device number	Device type	OS version	Device details	Client version	Last seen	Status
30	Fox Mulder	fmulder@cptme.us	+0000000000	unknown	unknown	unknown / unknown			Provisioned
29	Dana Scully	dscully@cptme.us	No number	IOS Device	unknown	unknown / unknown			Provisioned

Multi-tags in SandBlast Mobile and Usage in BlackBerry UEM

Recently added to SandBlast Mobile Dashboard for UEM integrations is the concept of multi-tags.

The multi-tags are built-in tags that SandBlast Mobile will use to indicate the different registration states (CHKP_Status) and the different risk levels (CHKP_Risk) to which the devices can be marked. This allows the Administrators on the UEM to configure granular compliance policies based on device registration status or risk level. These tags are created as "user groups" in BlackBerry UEM.

There are 3 Status states:

Status	Description
CHKP_Status_Provisioned	When a device is synchronized for the first time in SandBlast Mobile Dashboard
CHKP_Status_Active	After the user has installed and registered to SandBlast Mobile
CHKP_Status_Inactive	If the device hasn't checked-in with SandBlast Mobile for X number of days (configured by the SandBlast Mobile Admin)

There are 4 pre-defined Risk levels:

- CHKP_Risk_None
- CHKP_Risk_Low
- CHKP_Risk_Medium
- CHKP_Risk_High

For example, if the device has a Low risk app and a High risk (malicious) SMS URL, then the device will be marked as at High Risk (CHKP_Risk_High = 1) and at Low Risk (CHKP_Risk_Low = 1). Once the High Risk issue has been remediated (SMS deleted), then the CHKP_Risk_High will be set to 0. Once the Low Risk issue has been remediated, the CHKP_Risk_Low will be set to 0.

Tag Device Status

For integration with BlackBerry UEM, the Device Status Tag are interpreted as "user groups" of "CHKP_Status_Provisioned", "CHKP_Status_Active", or "CHKP_Status_Inactive" which will have an either "0" or "1" when set.

We will use the CHKP_Status user groups to determine when to prompt the user to install the SandBlast Mobile Protect app on their device. If the none of CHKP_Status user groups haven't been set yet for a device, then the device has not been synced with SandBlast Mobile Dashboard.

Tag Device Risk

For integration with BlackBerry UEM, the Device Risk tags are interpreted as "user groups" of "CHKP_Risk_None", "CHKP_Risk_Low", "CHKP_Risk_Medium", and "CHKP_Risk_High" with the values of "0" or "1".

We will use the CHKP_Risk user groups to determine when to enact certain policies or actions on the device. As an example, if CHKP_Risk_High is set to "1", then the device will be sent an in-app notification and blocked from running corporate apps or connecting to corporate assets.

Mitigation Group

The free-form Mitigation group is any unique name, such as "SBM_HighRisk", that SandBlast Mobile will place only devices determined to be at High Risk.

> **Note:** This mitigation group must be created as a "user group" in BlackBerry UEM prior to using.

Please note that the Mitigation group does not provided the granularity of the different risk levels of the device, just high risk.

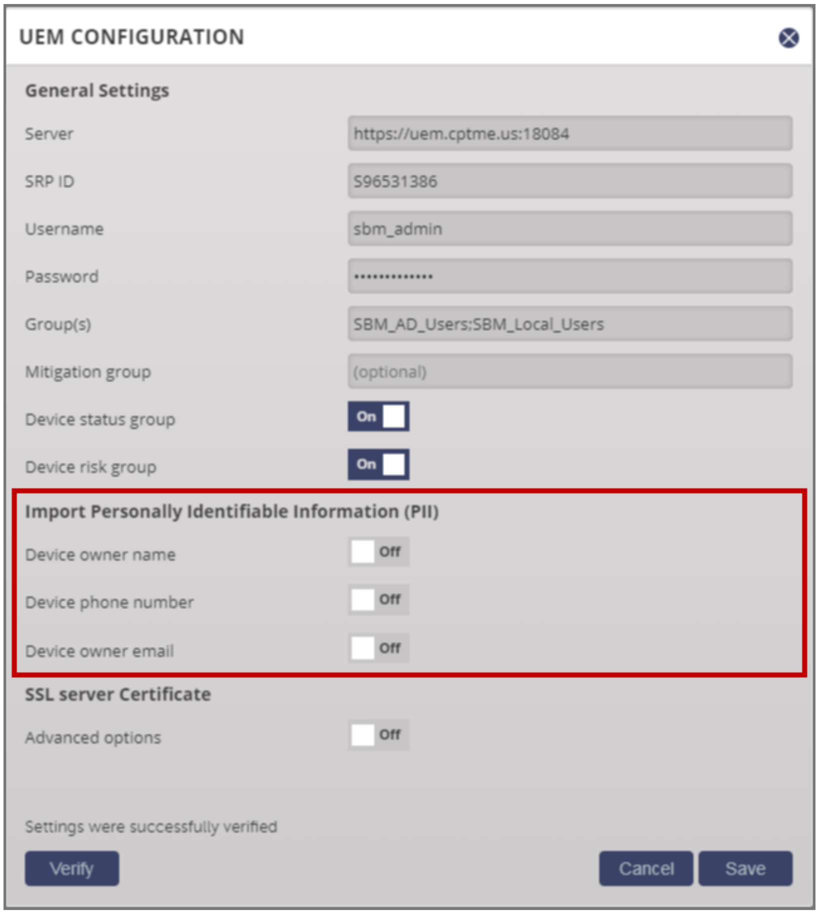
This method was the original way to group devices at high risk, and it is strongly recommended that you implement the CHKP_Risk and CHKP_Status user groups instead of using the free-form Mitigation group.

Controlling the Importing of Personally Identifiable Information (PII) from the UEM

The PII for devices (users) can be limited from being imported to SandBlast Mobile by configuring the "Import Personally Identifiable Information (PII)" section.

If all entries are turned off, then a placeholder information set for the email address will be placed in the Device Owner's Email, in the form of "Device UDID@mdm_vendor", such as bb30f0ab-92dd-4b84-ba02-351bbaaacc22@uem.mdm.

1. PII Control is configured in the **Settings > Device Management > Setting > MDM** service pop-up window.



UEM CONFIGURATION

General Settings

Server	https://uem.cptme.us:18084
SRP ID	S96531386
Username	sbm_admin
Password	•••••••••••••
Group(s)	SBM_AD_Users;SBM_Local_Users
Mitigation group	(optional)
Device status group	On
Device risk group	On

Import Personally Identifiable Information (PII)

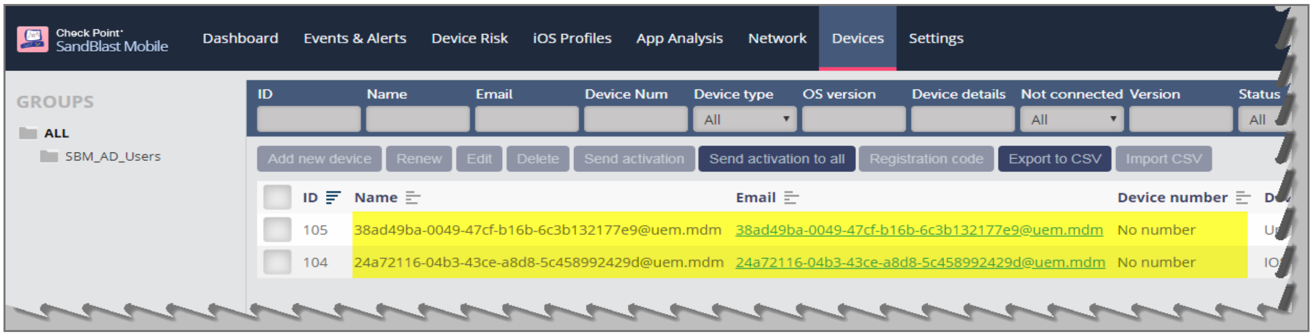
Device owner name	Off
Device phone number	Off
Device owner email	Off

SSL server Certificate

Advanced options	Off

Settings were successfully verified

2. Turning off PII Import, will result in the following Devices display in SandBlast Mobile.

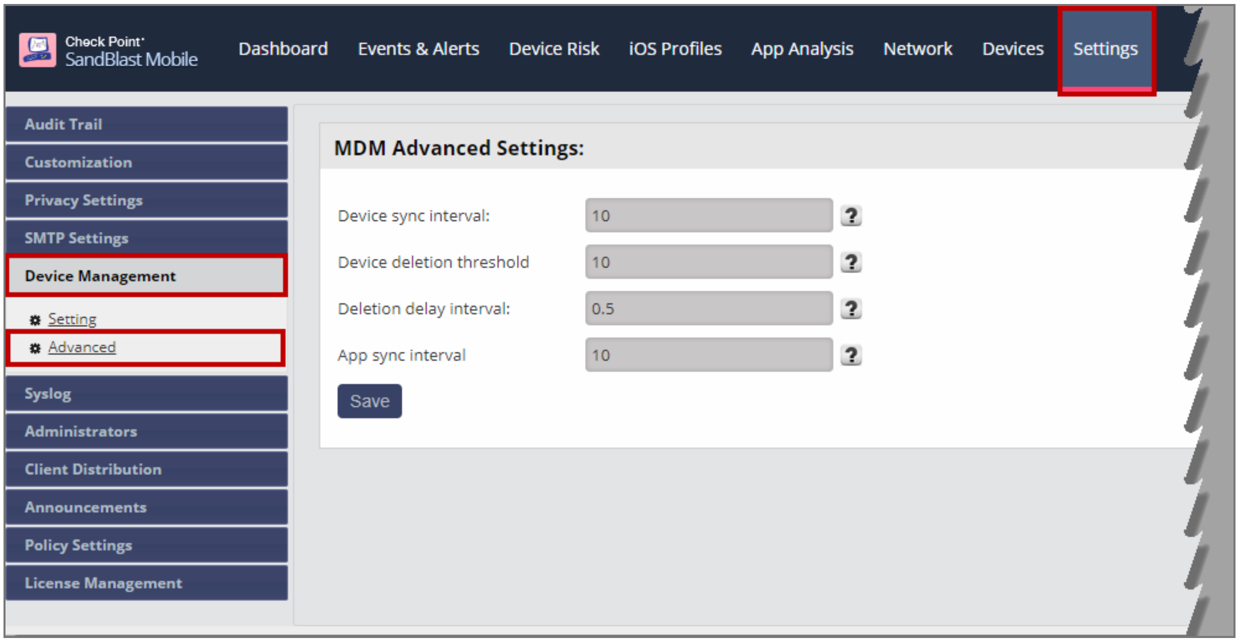


	ID	Name	Email	Device number	D
□	105	38ad49ba-0049-47cf-b16b-6c3b132177e9@uem.mdm	38ad49ba-0049-47cf-b16b-6c3b132177e9@uem.mdm	No number	U
□	104	24a72116-04b3-43ce-a8d8-5c458992429d@uem.mdm	24a72116-04b3-43ce-a8d8-5c458992429d@uem.mdm	No number	IO

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 BlackBerry UEM.

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



MDM Advanced Settings:

Device sync interval: 10

Device deletion threshold 10

Deletion delay interval: 0.5

App sync interval 10

Setting	Description
Device sync interval	Interval to connect with UEM to sync devices. Values: 10-1440 minutes, in 10 minute intervals
Device deletion threshold	Percentage of devices allowed for deletion after UEM device sync. 100% for no threshold
Deletion delay interval	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
App sync interval	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.

Chapter 3

Configuring the UEM Platform

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

For this process we will return to the BlackBerry UEM Console to complete the configuration.

This chapter discusses the following:

Prerequisites

1. BlackBerry UEM 12.6 or higher.
2. For **on-premise BlackBerry UEM Deployments**, the port used for the UEM Web Services API (default: TCP 18084) must be accessible remotely by the SandBlast Mobile servers through your firewall before trying to connect.

Configuring UEM to Deploy SandBlast Mobile Protect app

For more or updated information, please see BlackBerry's documentation at http://help.blackberry.com/en/blackberry-uem/current/getting-started-blackberry-uem-and-blackberry-dynamics/zfd1473950276026.html

Adding the SandBlast Mobile Protect App to Your App Catalog

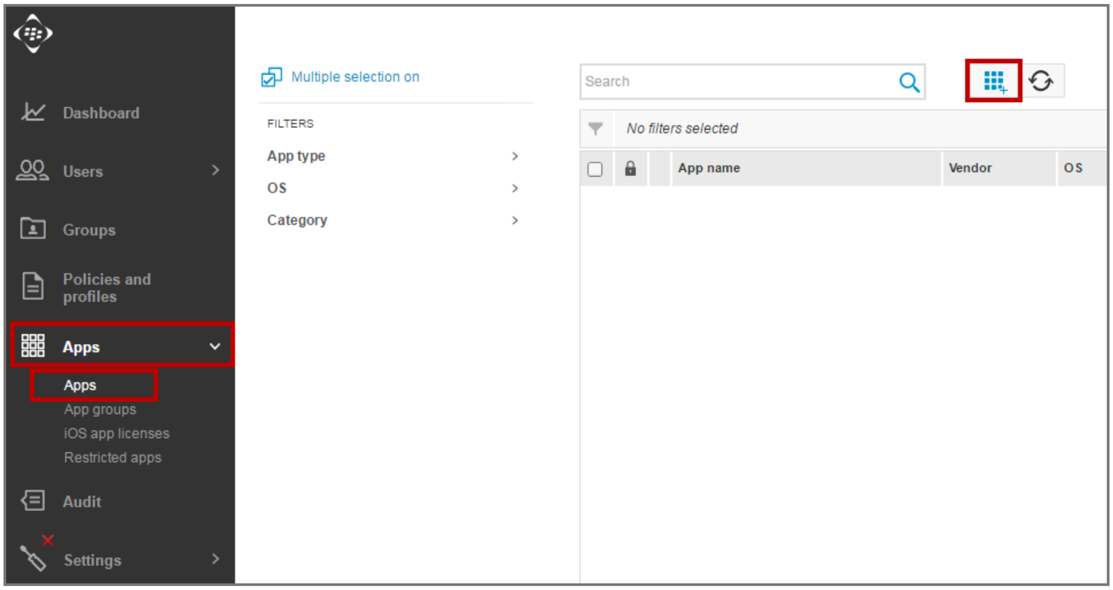
Now that BlackBerry UEM and Check Point SandBlast Mobile Dashboard are communicating, we can now start deploying the SandBlast Mobile Protect app to those devices that will be protected by Check Point SandBlast Mobile.

We will need to add the App for both iOS and Android operating systems.

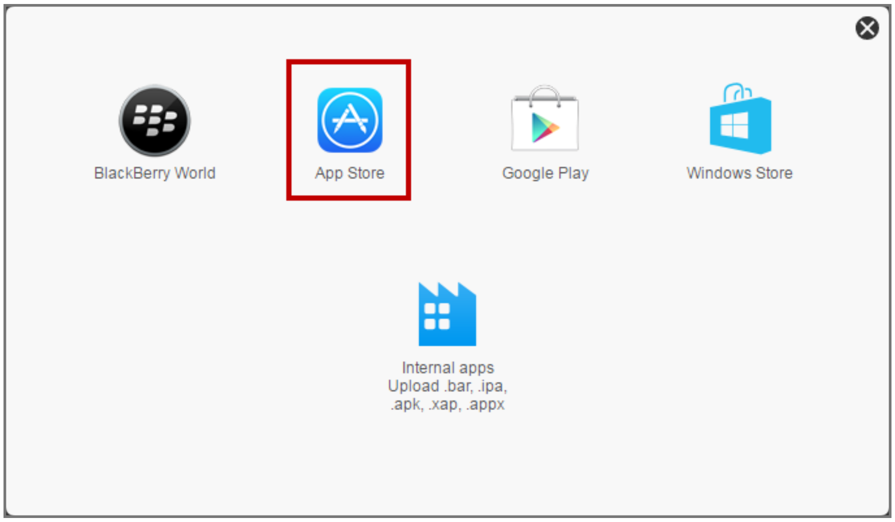
AppStore iOS App – Add to Catalog

For the iOS app, BlackBerry UEM can automatically deploy and configure the SandBlast Mobile Protect app registration server and key on an iOS device. It does require the user to launch the SandBlast Mobile Protect app to finish device registration. There are two possible deployment scenarios for iOS, using the Apple App Store app or the Enterprise iOS app that has been signed by your organization. This procedure describes deploying the Apple App Store app.

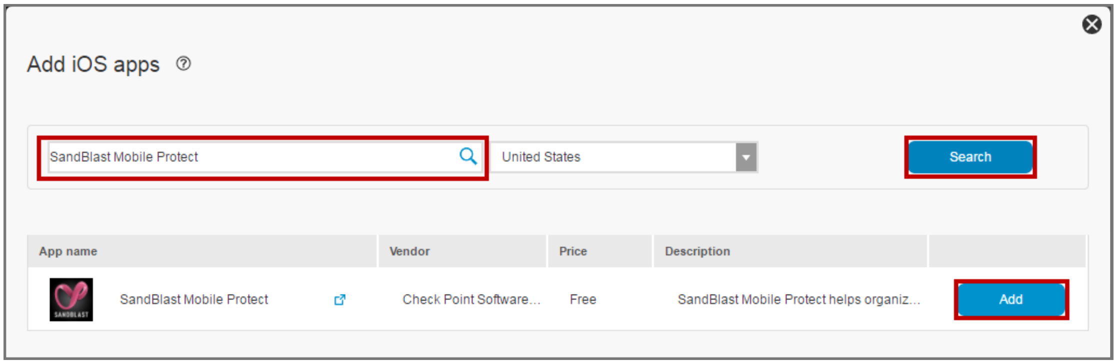
1. Navigate to **Apps > Apps**, and click the ⊞ icon.



2. Select "iTunes" from the Store List.



3. In the "App" field, enter "SandBlast Mobile Protect", select the appropriate store for your country, and click "Search" to search the store.
4. Select SandBlast Mobile Protect app as indicated below by clicking the "Add".

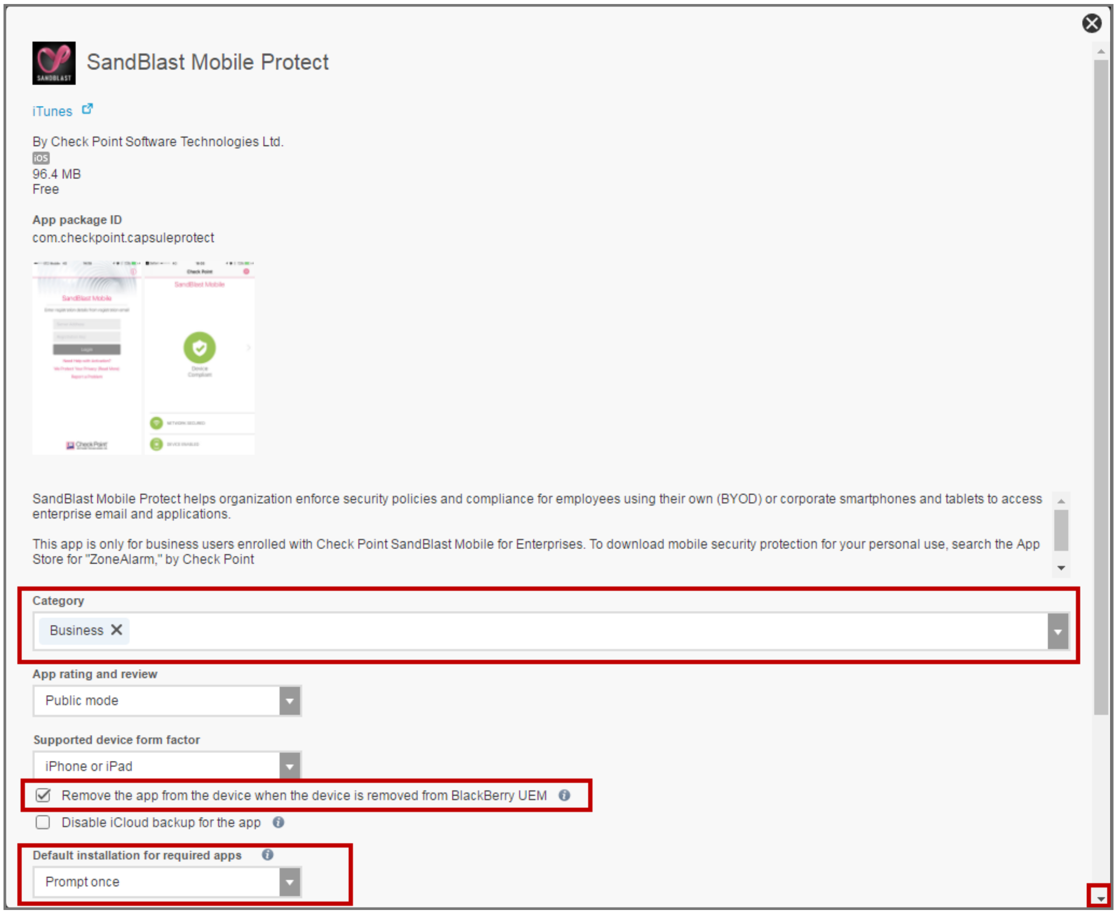

Add iOS apps

SandBlast Mobile Protect

United States

App name	Vendor	Price	Description	
SandBlast Mobile Protect	Check Point Software...	Free	SandBlast Mobile Protect helps organiz...	Add

5. A pop-up an App Configuration window for "SandBlast Mobile Protect" will open.



SandBlast Mobile Protect

iTunes

By Check Point Software Technologies Ltd.
iOS
96.4 MB
Free

App package ID
com.checkpoint.capsuleprotect

SandBlast Mobile Protect helps organization enforce security policies and compliance for employees using their own (BYOD) or corporate smartphones and tablets to access enterprise email and applications.

This app is only for business users enrolled with Check Point SandBlast Mobile for Enterprises. To download mobile security protection for your personal use, search the App Store for "ZoneAlarm," by Check Point

Category
Business ✕

App rating and review
Public mode

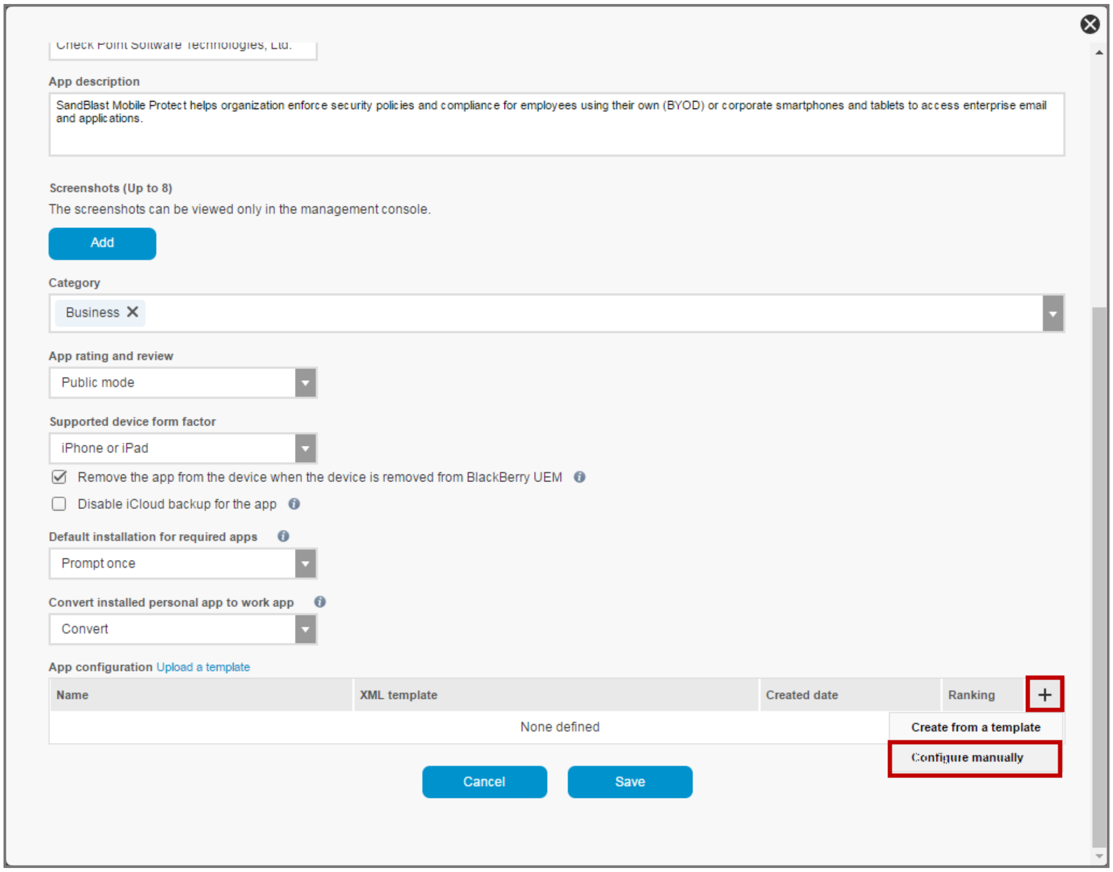
Supported device form factor
iPhone or iPad

☑ Remove the app from the device when the device is removed from BlackBerry UEM

☐ Disable iCloud backup for the app

Default installation for required apps
Prompt once

6. Scroll down to bottom of the screen, and click "+" on the right-hand side of the "App configuration" table.
7. Select "Configure manually" from the drop-down.



Check Point Software Technologies, Ltd.

App description

SandBlast Mobile Protect helps organization enforce security policies and compliance for employees using their own (BYOD) or corporate smartphones and tablets to access enterprise email and applications.

Screenshots (Up to 8)

The screenshots can be viewed only in the management console.

Add

Category: Business ✕

App rating and review: Public mode

Supported device form factor: iPhone or iPad

☑ Remove the app from the device when the device is removed from BlackBerry UEM

☐ Disable iCloud backup for the app

Default installation for required apps: Prompt once

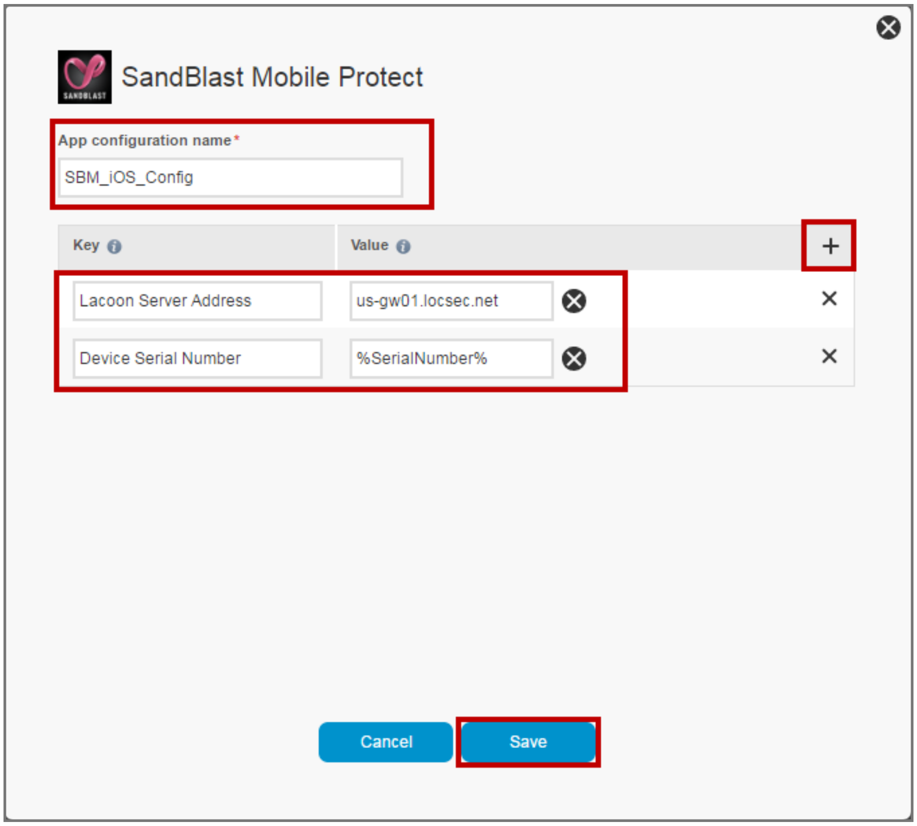
Convert installed personal app to work app: Convert

App configuration Upload a template

Name	XML template	Created date	Ranking
None defined			

8. On the "SandBlast Mobile Protect" configuration pop-up window, enter in an App configuration name.
9. Click "+" and select "String" twice.
10. Add the following Key/Value pairs:

Key	Type	Value
Lacoon Server Address	string	gw.locsec.net
Device Serial Number	string	%SerialNumber%



SandBlast Mobile Protect

App configuration name*: SBM_iOS_Config

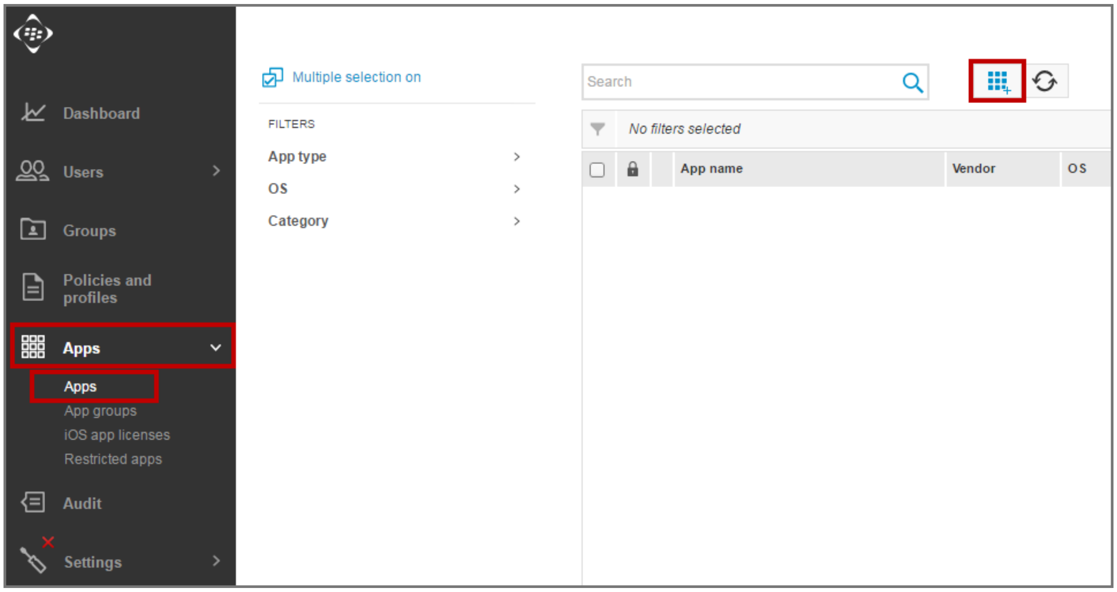
Key	Value
Lacoon Server Address	us-gw01.locsec.net
Device Serial Number	%SerialNumber%

11. Click "Save".
12. Click "Add" to finish adding the app to the app catalog.

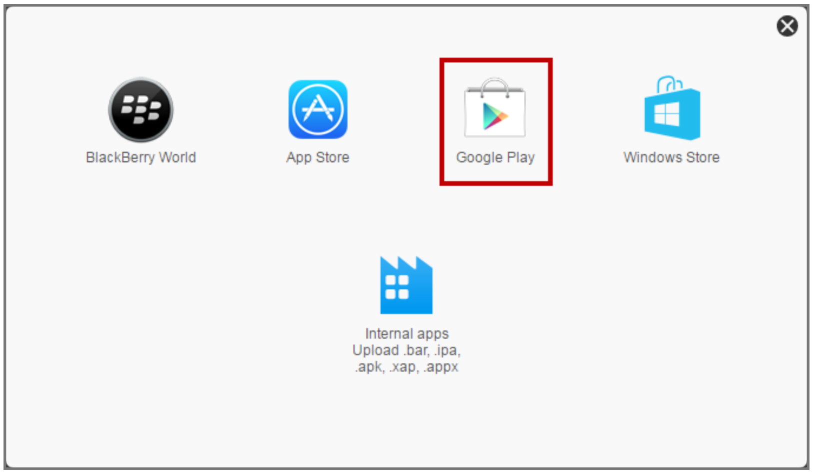
Android App – Add to Catalog

BlackBerry UEM can automatically deploy, but not configure the SandBlast Mobile Protect app registration server and key on an Android device. Completing deployment requires the user to launch the SandBlast Mobile Protect app to finish device registration, by entering the registration server and registration key the user received via email.

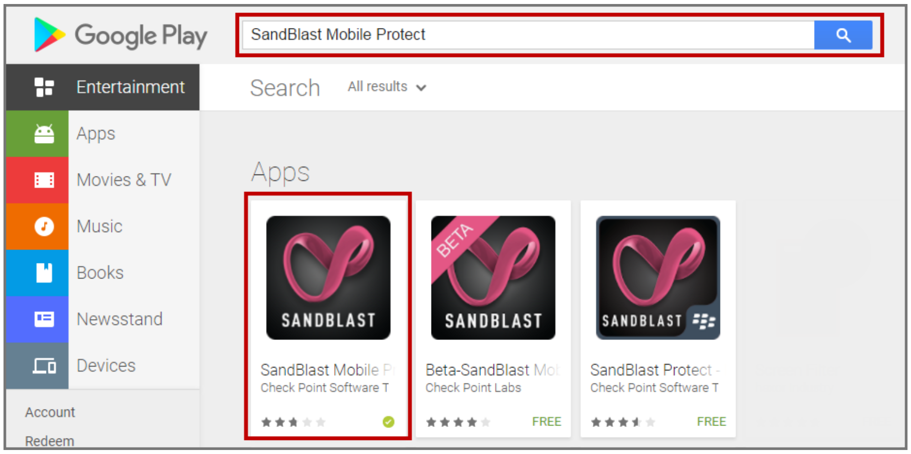
1. Navigate to **Apps > Apps**, and click the ▦ icon.



2. Select "Google Play App" from the Store List.



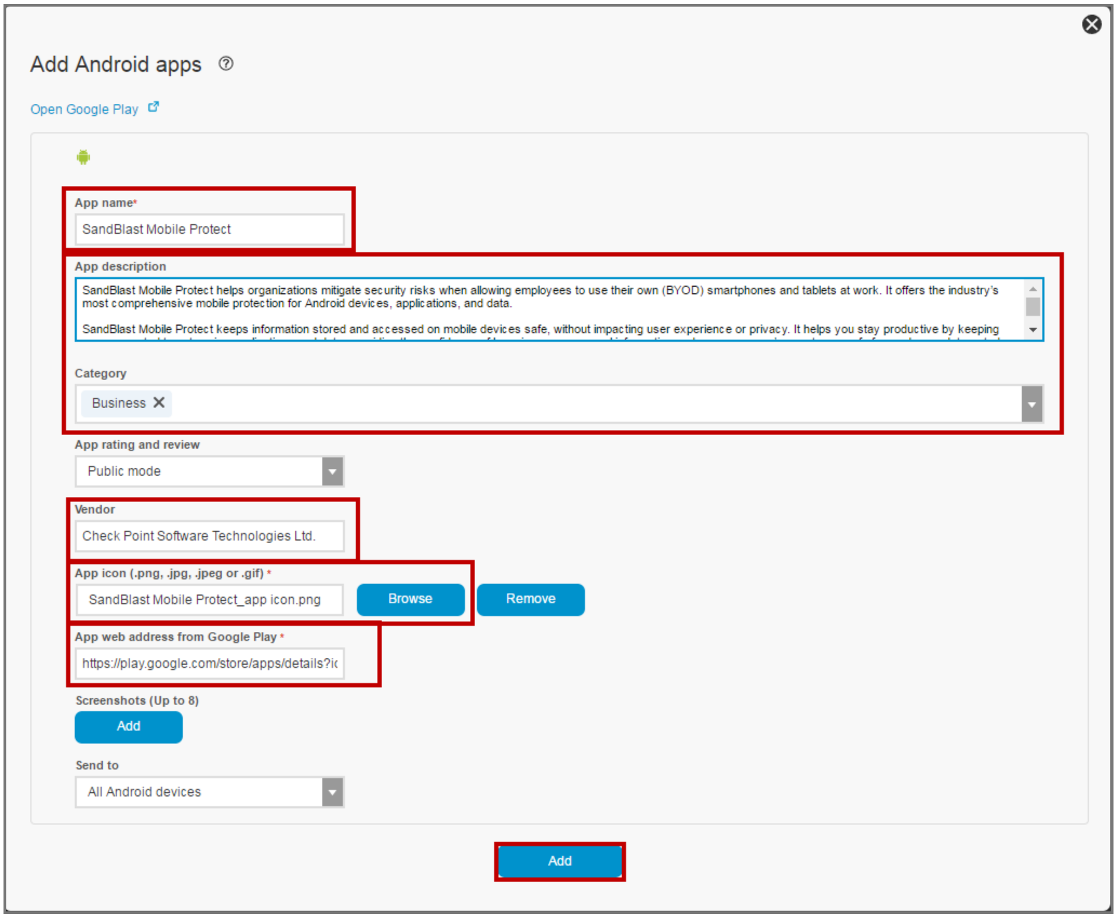
3. Click "Open Google Play" and search for the app that you want to add. You can then copy and paste information from Google Play in the following steps and also download icons and screen shots.



4. In the App name field, type the app name, "SandBlast Mobile Protect".
5. In the App description field, type a description for the app.
6. In the Vendor field, type the name of the app vendor, "Check Point Software Technologies, Ltd."
7. In the App icon field, click Browse. Locate and select an icon for the app. The supported formats are .png, .jpg, .jpeg, or .gif.

> **Note:** Do not use Google Chrome to download the icon because an incompatible .webp image is downloaded.

8. In the App web address from Google Play field, type the web address of the app in Google Play.
   a. https://play.google.com/store/apps/details?id=com.lacoon.security.fox



Add Android apps

Open Google Play

App name*
SandBlast Mobile Protect

App description
SandBlast Mobile Protect helps organizations mitigate security risks when allowing employees to use their own (BYOD) smartphones and tablets at work. It offers the industry's most comprehensive mobile protection for Android devices, applications, and data.

SandBlast Mobile Protect keeps information stored and accessed on mobile devices safe, without impacting user experience or privacy. It helps you stay productive by keeping

Category
Business

App rating and review
Public mode

Vendor
Check Point Software Technologies Ltd.

App icon (.png, .jpg, .jpeg or .gif) *
SandBlast Mobile Protect_app icon.png

App web address from Google Play *
https://play.google.com/store/apps/details?ic

Screenshots (Up to 8)

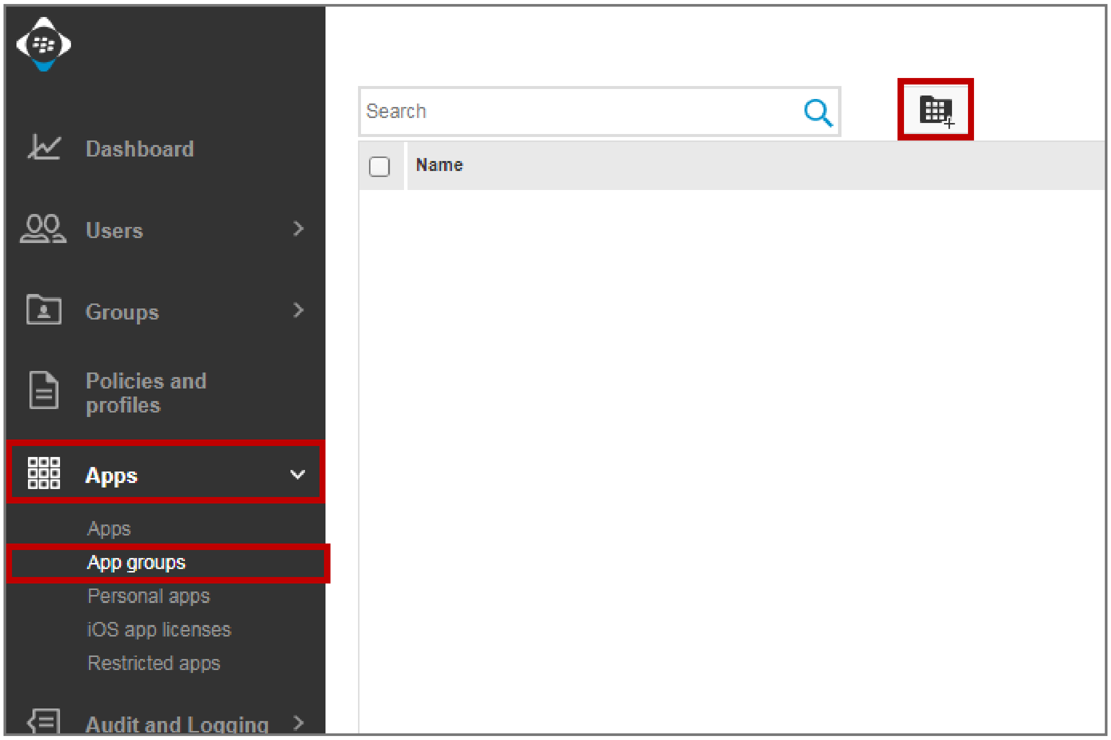
Send to
All Android devices

9. Click "Add".

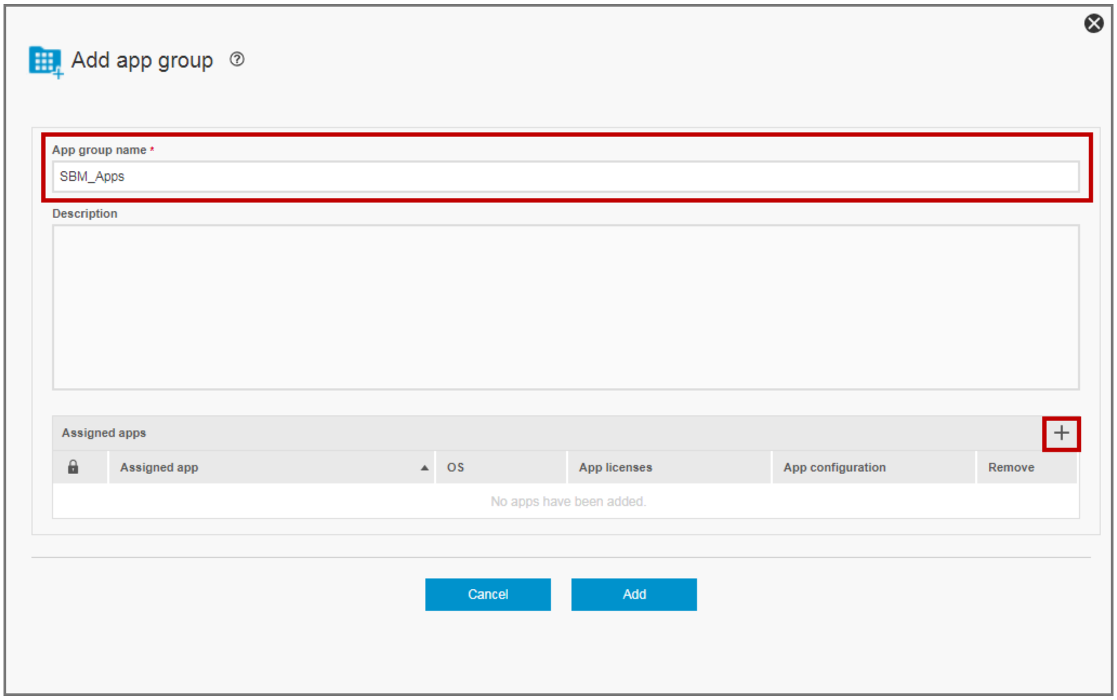
Creating an App Group (Optional)

This is an optional step, but does provide a method of organizing Apps.

1. Navigating to **Apps > App groups**, click the ▦ icon.



2. On the "Add app group" pop-up window, enter in a name for the App group.
3. Click "+" on the "Assigned apps" section.



Add app group

App group name *

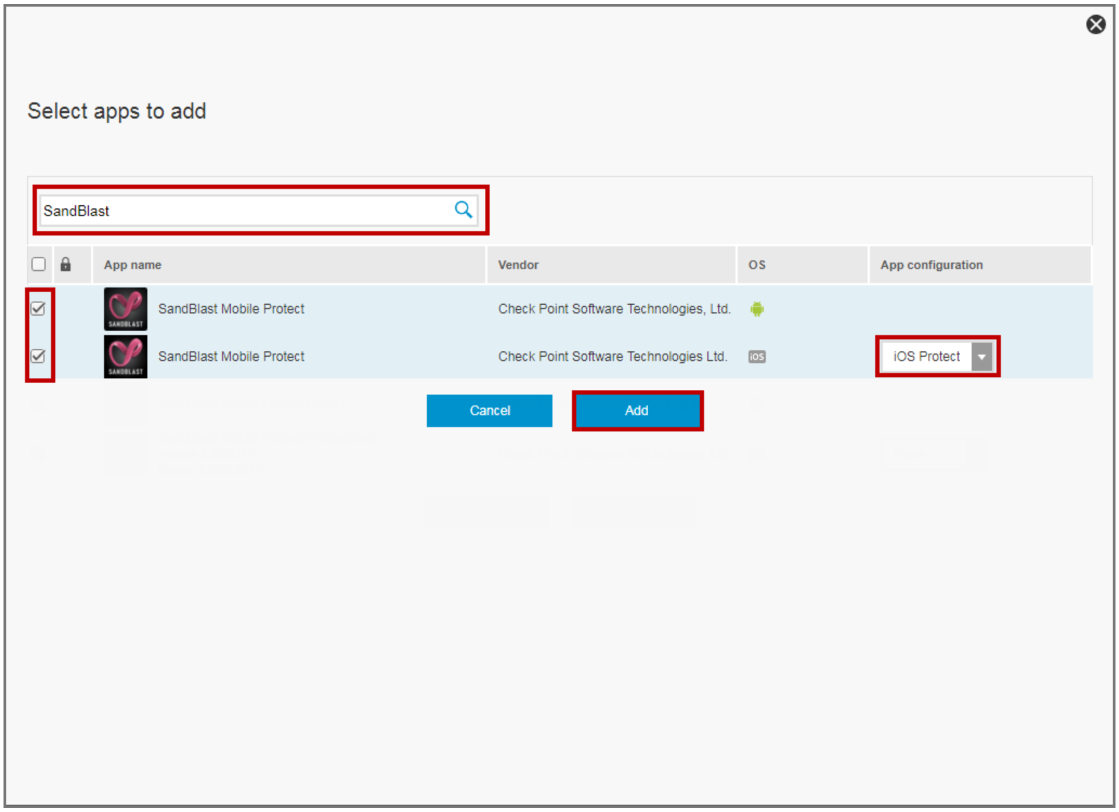
SBM_Apps

Description

Assigned apps

🔒	Assigned app ▲	OS	App licenses	App configuration	Remove
		No apps have been added.			

4. Enter in SandBlast into the Search box, and select the Android and iOS versions of the SandBlast Mobile Protect app.
5. Set the App configuration to "iOS Protect" for the iOS app.



Select apps to add

SandBlast

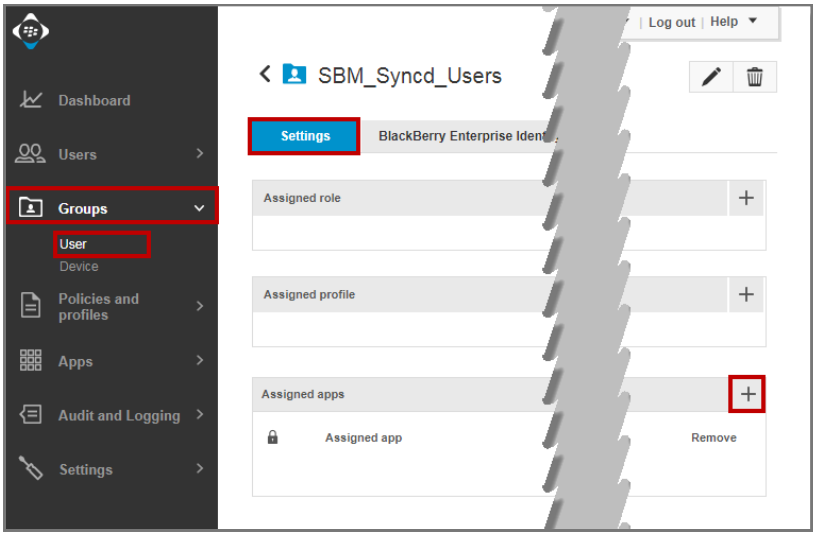
□	App name	Vendor	OS	App configuration
☑	SandBlast Mobile Protect	Check Point Software Technologies, Ltd.	🤖	
☑	SandBlast Mobile Protect	Check Point Software Technologies Ltd.	iOS	iOS Protect

6. Click "Add".

Deploying SandBlast Mobile Protect app

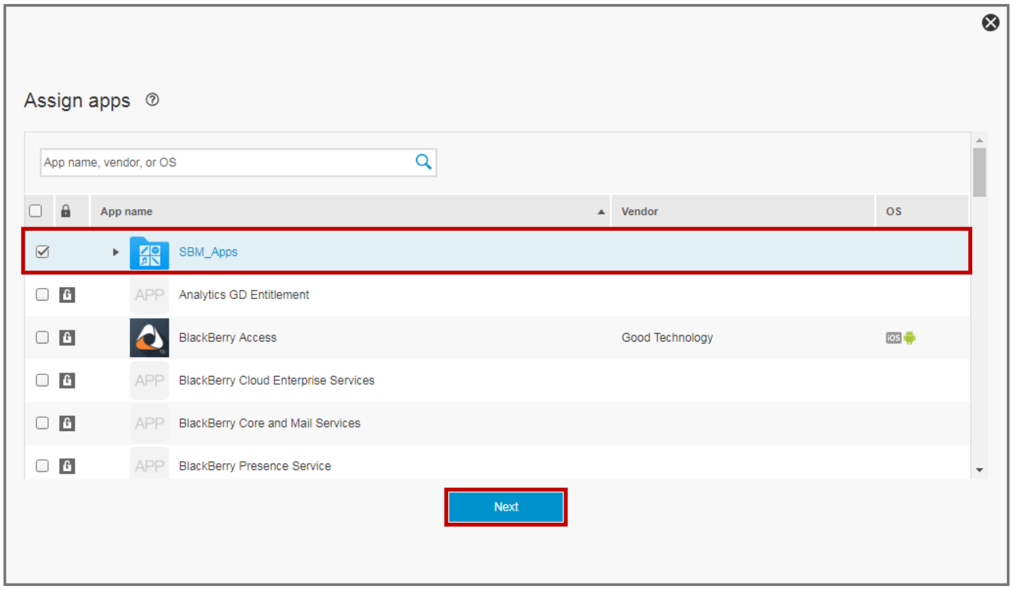
To deploy the SandBlast Mobile Protect app to devices that will be registered to the Check Point SandBlast Mobile solution we need to link the SandBlast Mobile Protect app in our app catalog to the User Groups we created in "Creating User Provisioning Groups" on page 13.

1. Navigating to **Groups > User**, click name of the User Provisioning Group, in our example "SBM_Syncd_Users".
2. Click Settings tab.



3. Click "+" on the "Assigned apps" section.

4. On the "Assign app" pop-up window, select the App Group we created in "Creating an App Group (Optional)" on page 44. If you didn't create an App Group, you would select both SandBlast Mobile Protect apps and assign them directly, selecting the iOS Configuration.

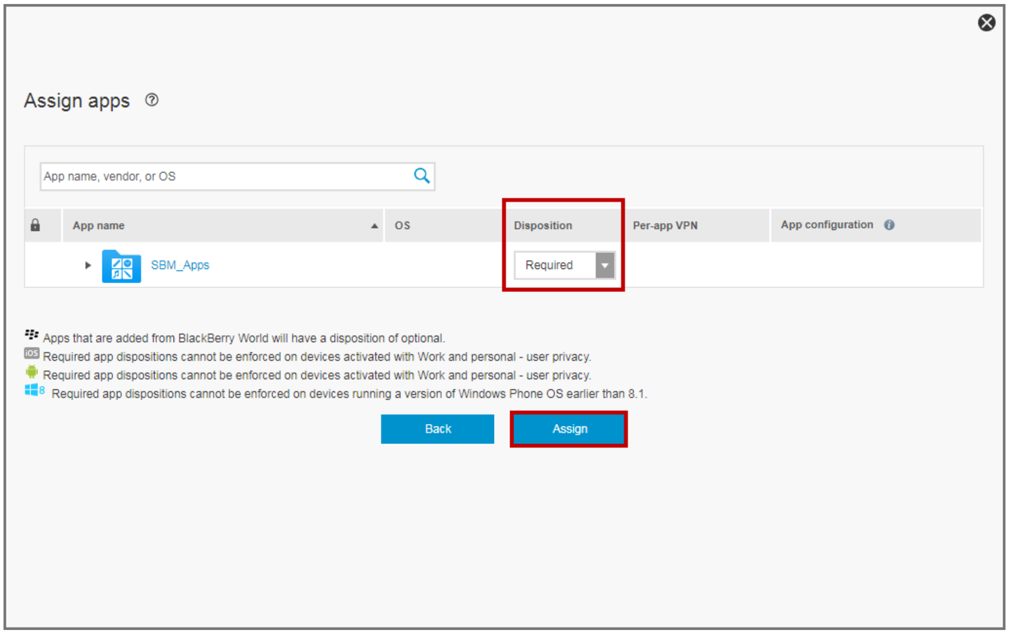

Assign apps

App name, vendor, or OS

☐		App name	Vendor	OS
☑		SBM_Apps		
☐		Analytics GD Entitlement		
☐		BlackBerry Access	Good Technology	iOS
☐		BlackBerry Cloud Enterprise Services		
☐		BlackBerry Core and Mail Services		
☐		BlackBerry Presence Service		

5. Click "Next".

6. Set the "Disposition" to "Required" for the App Group.



App name	OS	Disposition	Per-app VPN	App configuration
SBM_Apps		Required		

Apps that are added from BlackBerry World will have a disposition of optional.
iOS Required app dispositions cannot be enforced on devices activated with Work and personal - user privacy.
Required app dispositions cannot be enforced on devices activated with Work and personal - user privacy.
8 Required app dispositions cannot be enforced on devices running a version of Windows Phone OS earlier than 8.1.

7. Click "Assign".

Note: Repeat the steps in this section for "Users_At_Risk". This will prompt the users who belong to "SBM_Syncd_Users" to install the SandBlast Mobile Protect app. Also, those users who are in the "Users_At_Risk" who uninstall the SandBlast Mobile Protect app will be out of compliance.

Note: Repeat the steps in this section for "SBM_AD_Users" and "SBM_Local_Users", but change the **"Disposition"** to **"Optional"** instead of "Required".

Requiring the SandBlast Mobile Protect App to be Installed

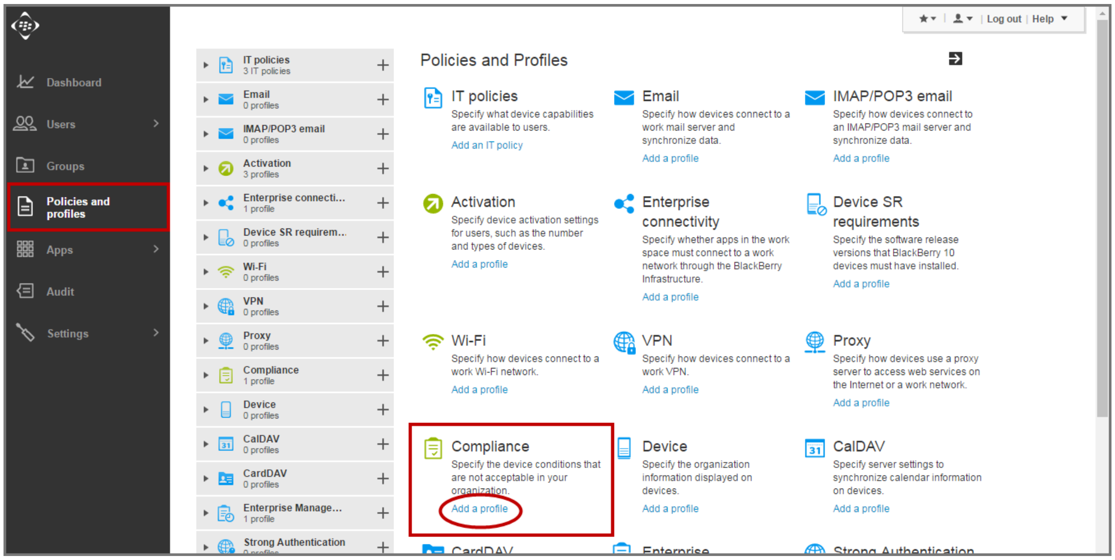
The SandBlast Mobile Protect app is required by creating a Compliance Policy for iOS and Android devices, then assigning this compliance policy to the User Provisioning Group we created in "Creating User Provisioning Groups" on page 13.

Creating a Compliance Policy

The policy will specify the actions taken on all SandBlast Mobile devices that do not have required apps, such as SandBlast Mobile Protect, installed.

© 2018 Check Point Software Technologies Ltd. All rights reserved.

1. Navigate to **Policies and profiles**, and click the "Add a profile" link under "Compliance".



Policies and Profiles

IT policies
Specify what device capabilities are available to users.
Add an IT policy

Email
Specify how devices connect to a work mail server and synchronize data.
Add a profile

IMAP/POP3 email
Specify how devices connect to an IMAP/POP3 mail server and synchronize data.
Add a profile

Activation
Specify device activation settings for users, such as the number and types of devices.
Add a profile

Enterprise connectivity
Specify whether apps in the work space must connect to a work network through the BlackBerry Infrastructure.
Add a profile

Device SR requirements
Specify the software release versions that BlackBerry 10 devices must have installed.
Add a profile

Wi-Fi
Specify how devices connect to a work Wi-Fi network.
Add a profile

VPN
Specify how devices connect to a work VPN.
Add a profile

Proxy
Specify how devices use a proxy server to access web services on the Internet or a work network.
Add a profile

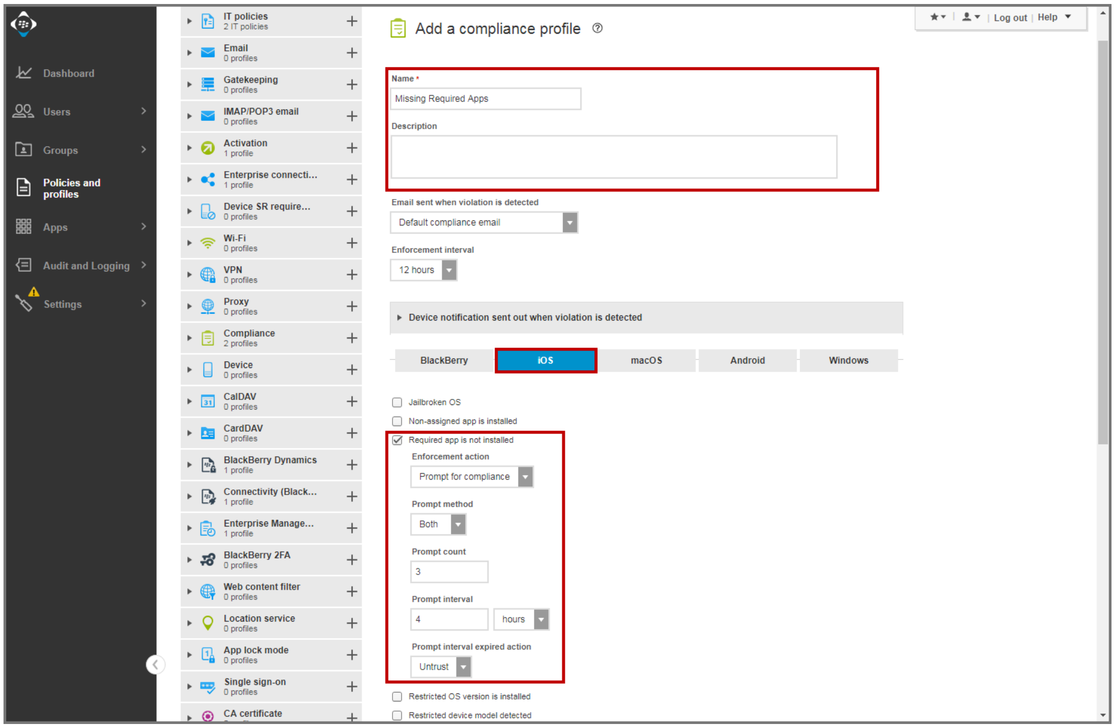
Compliance
Specify the device conditions that are not acceptable in your organization.
Add a profile

Device
Specify the organization information displayed on devices.
Add a profile

CalDAV
Specify server settings to synchronize calendar information on devices.
Add a profile

CardDAV
Enterprise
Strong Authentication

2. Enter a Name for the policy, such as "Missing Required Apps", enter a description, and select the "iOS" tab.
3. Select "Required app is not installed" and set appropriate actions to be taken if the user doesn’t install the app.



Add a compliance profile

Name *: Missing Required Apps

Description:

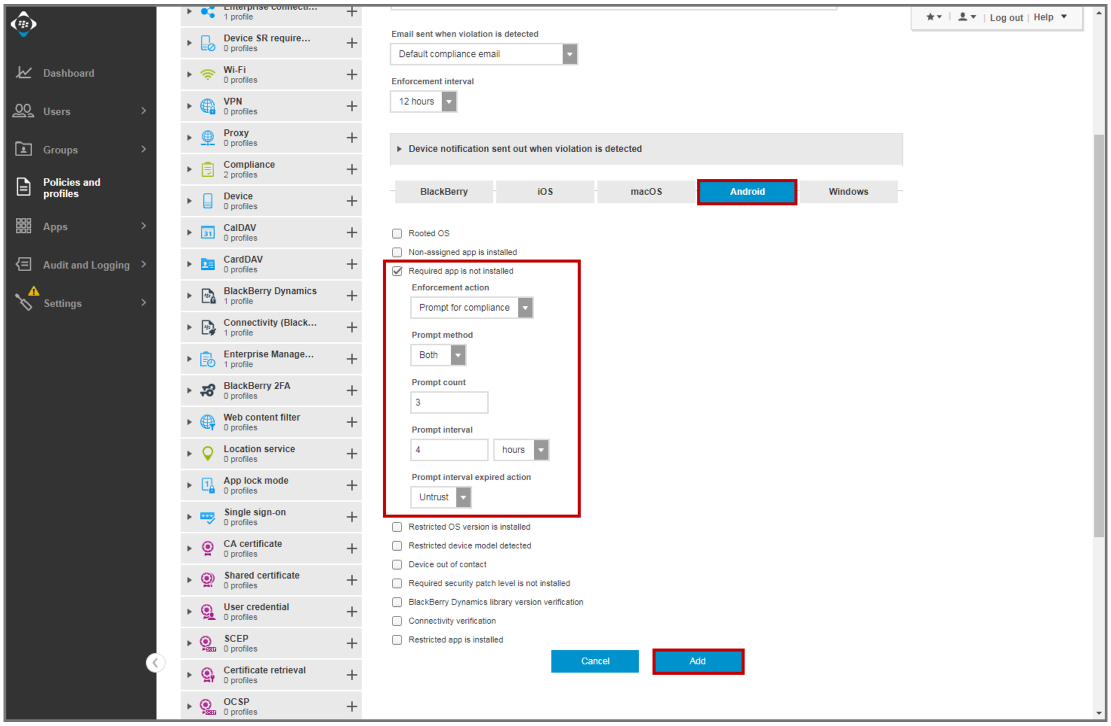
Email sent when violation is detected: Default compliance email

Enforcement interval: 12 hours

Device notification sent out when violation is detected

□ Jailbroken OS
□ Non-assigned app is installed
☑ Required app is not installed
Enforcement action: Prompt for compliance
Prompt method: Both
Prompt count: 3
Prompt interval: 4 hours
Prompt interval expired action: Untrust
□ Restricted OS version is installed
□ Restricted device model detected

4. Select the "Android" tab.
5. Select "Required app is not installed" and set appropriate actions to be taken if the user doesn’t install the app.


Dashboard
Users
Groups
Policies and profiles
Apps
Audit and Logging
Settings
Enterprise connecti... 1 profile
Device SR require... 0 profiles
Wi-Fi 0 profiles
VPN 0 profiles
Proxy 0 profiles
Compliance 2 profiles
Device 0 profiles
CalDAV 0 profiles
CardDAV 0 profiles
BlackBerry Dynamics 1 profile
Connectivity (Black... 1 profile
Enterprise Manage... 1 profile
BlackBerry 2FA 0 profiles
Web content filter 0 profiles
Location service 0 profiles
App lock mode 0 profiles
Single sign-on 0 profiles
CA certificate 0 profiles
Shared certificate 0 profiles
User credential 0 profiles
SCEP 0 profiles
Certificate retrieval 0 profiles
OCSP 0 profiles
Log out
Help

Email sent when violation is detected: Default compliance email

Enforcement interval: 12 hours

Device notification sent out when violation is detected

BlackBerry | iOS | macOS | **Android** | Windows

☐ Rooted OS
☐ Non-assigned app is installed
☑ Required app is not installed
Enforcement action: Prompt for compliance
Prompt method: Both
Prompt count: 3
Prompt interval: 4 hours
Prompt interval expired action: Untrust
☐ Restricted OS version is installed
☐ Restricted device model detected
☐ Device out of contact
☐ Required security patch level is not installed
☐ BlackBerry Dynamics library version verification
☐ Connectivity verification
☐ Restricted app is installed

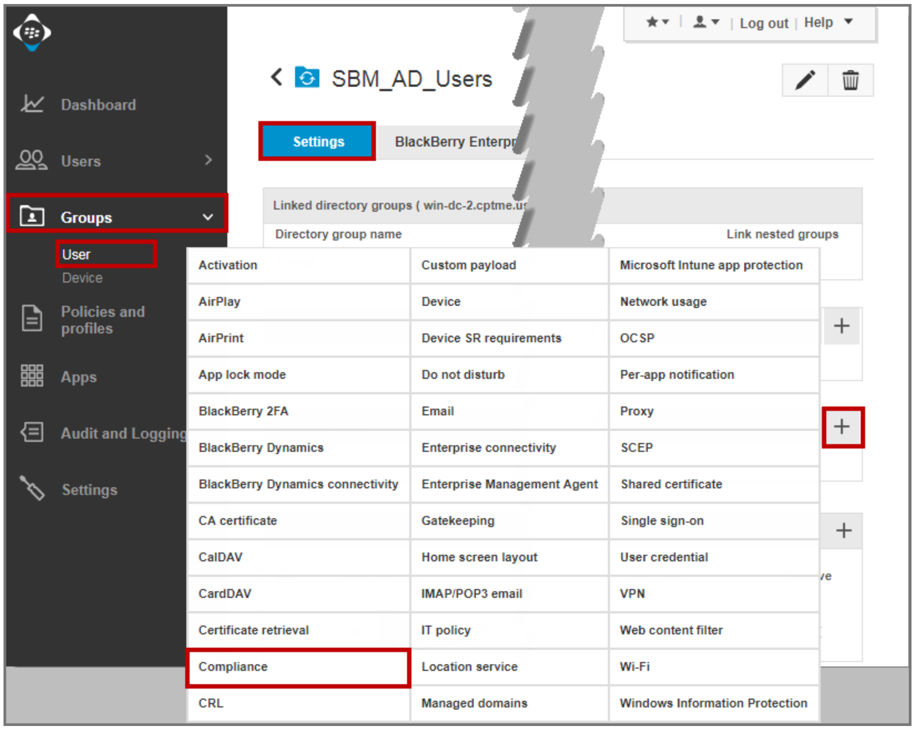
Cancel | Add

6. Click "Add".

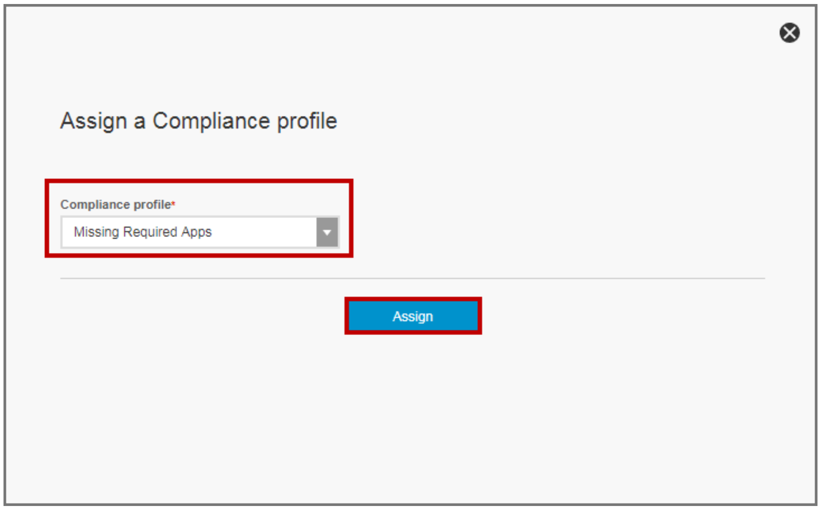
Applying App Required Compliance Policy to User Provisioning Group

The policies created in the previous section are assigned to the user provisioning group created in "Creating User Provisioning Groups" on page 13, in our example "SBM_AD_Users" and "SBM_Local_Users". Because the users will remain in the "SBM_AD_Users" or "SBM_Local_Users" group while their devices are synchronized with SandBlast Mobile, the policies will remain in effect for all other user groups they belong to as long as they are not removed from this group.

1. Navigate to **Groups > User**, locate the user provisioning group, click group's name link.
2. Select the "Settings" tab, and click "+" in the "IT policy and profiles" section.
3. Select "Compliance" from the pop-up list.



4. On the "Assign a Compliance profile" pop-up window, select the "Compliance Policy" we created in the previous section.
5. Click "Assign".


Assign a Compliance profile

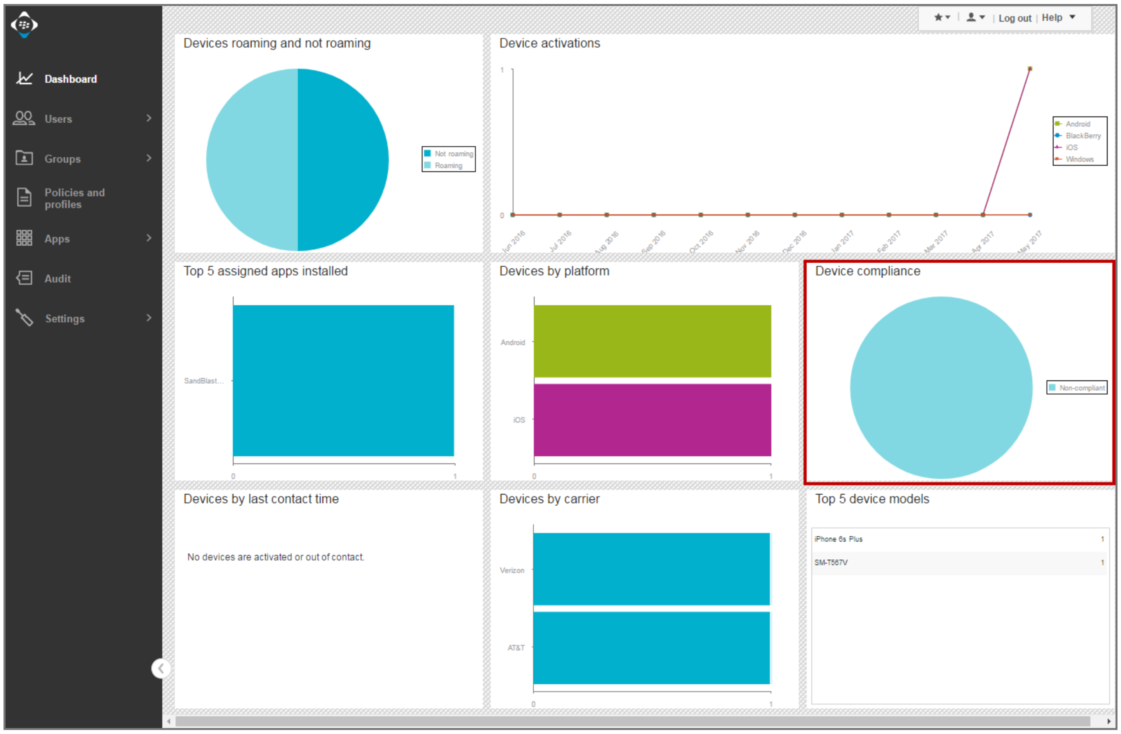
Compliance profile*: Missing Required Apps

Note: Repeat these steps for "SBM_Local_Users", if you are using it.

Note: Any device that belongs to the User Provisioning Group(s) which require the SandBlast Mobile Protect apps to be installed ("SBM_Syncd_Users" and "Users_At_Risk") that hasn’t installed the SandBlast Mobile Protect app will be out of compliance.

Device Out of Compliance – Missing SandBlast Mobile Protect App

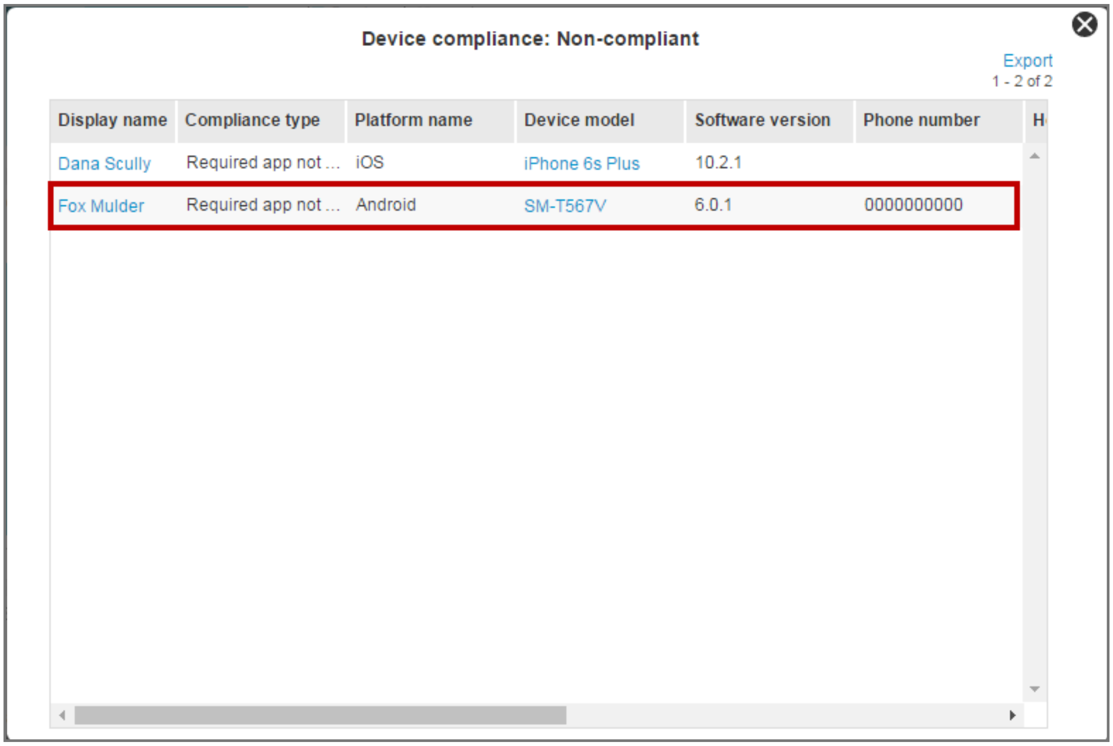
1. BlackBerry UEM Console Home Screen indicates an "Out of Compliance" issue.



No devices are activated or out of contact.

iPhone 6s Plus	1
SM-T567V	1

2. Clicking on the "Non-compliant" pie piece, opens a reporting window.

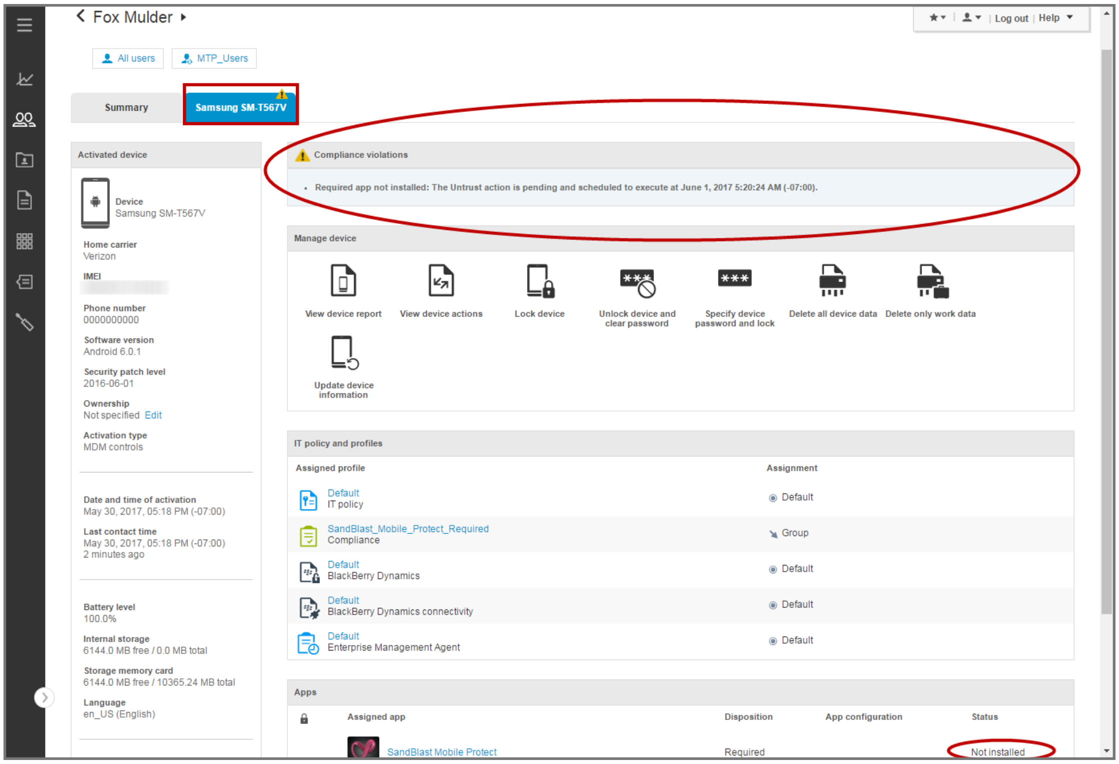


Device compliance: Non-compliant

Export
1 - 2 of 2

Display name	Compliance type	Platform name	Device model	Software version	Phone number	H
Dana Scully	Required app not ...	iOS	iPhone 6s Plus	10.2.1		
Fox Mulder	Required app not ...	Android	SM-T567V	6.0.1	0000000000	

3. Device Details View indicates an "Out of Compliance" issue.



Fox Mulder

Activated device

Device
Samsung SM-T567V

Home carrier
Verizon

IMEI
[redacted]

Phone number
0000000000

Software version
Android 6.0.1

Security patch level
2016-06-01

Ownership
Not specified Edit

Activation type
MDM controls

Date and time of activation
May 30, 2017, 05:18 PM (-07:00)

Last contact time
May 30, 2017, 05:18 PM (-07:00)
2 minutes ago

Battery level
100.0%

Internal storage
6144.0 MB free / 0.0 MB total

Storage memory card
6144.0 MB free / 10365.24 MB total

Language
en_US (English)

Compliance violations

- Required app not installed: The Untrust action is pending and scheduled to execute at June 1, 2017 5:20:24 AM (-07:00).

Manage device

IT policy and profiles

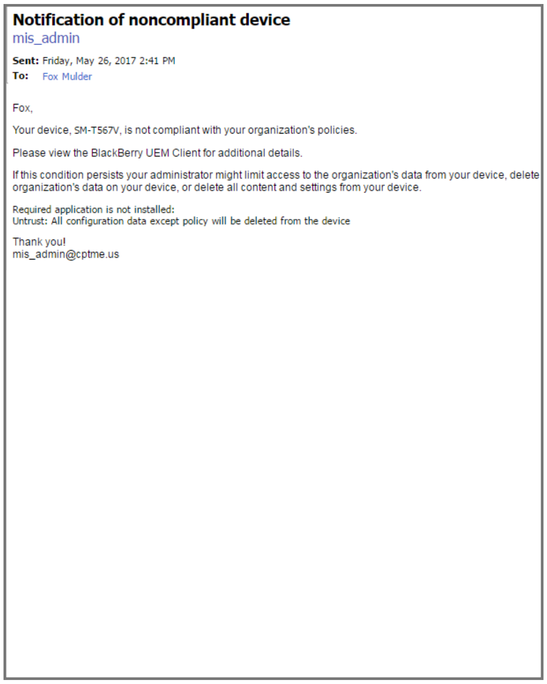
Assigned profile	Assignment
Default IT policy	Default
SandBlast_Mobile_Protect_Required Compliance	Group
Default BlackBerry Dynamics	Default
Default BlackBerry Dynamics connectivity	Default
Default Enterprise Management Agent	Default

Apps

Assigned app	Disposition	App configuration	Status
SandBlast Mobile Protect	Required		Not installed

© 2018 Check Point Software Technologies Ltd. All rights reserved.

4. The user will receive an alert email as well as an in-app notification.



Notification of noncompliant device
mis_admin

Sent: Friday, May 26, 2017 2:41 PM
To: Fox Mulder

Fox,

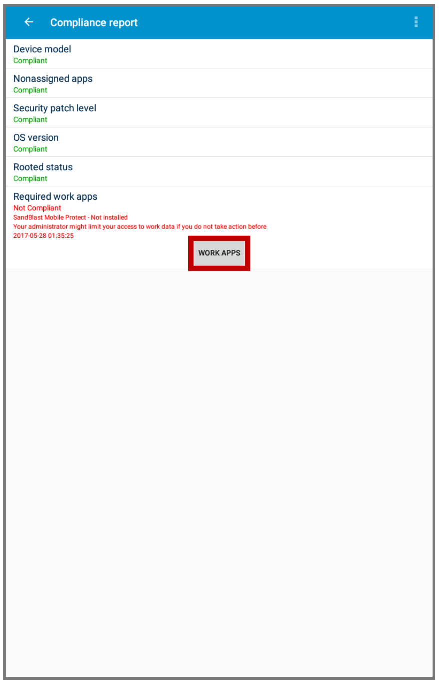
Your device, SM-T567V, is not compliant with your organization's policies.

Please view the BlackBerry UEM Client for additional details.

If this condition persists your administrator might limit access to the organization's data from your device, delete organization's data on your device, or delete all content and settings from your device.

Required application is not installed:
Untrust: All configuration data except policy will be deleted from the device

Thank you!
mis_admin@cptme.us



Compliance report

Device model
Compliant

Nonassigned apps
Compliant

Security patch level
Compliant

OS version
Compliant

Rooted status
Compliant

Required work apps
Not Compliant
SandBlast Mobile Protect - Not installed
Your administrator might limit your access to work data if you do not take action before
2017-05-28 01:35:25

Creating a Mitigation Process

In this procedure, you will create a mitigation policy set to enforce compliance and mitigation policies against those devices that belong to the Users_At_Risk group.

For more or updated information regarding IT Policies, please see BlackBerry's documentation at **http://help.blackberry.com/en/blackberry-uem/current/administration/ksa1373387706292.html** and **http://help.blackberry.com/en/blackberry-uem/current/administration/it-policies.html**

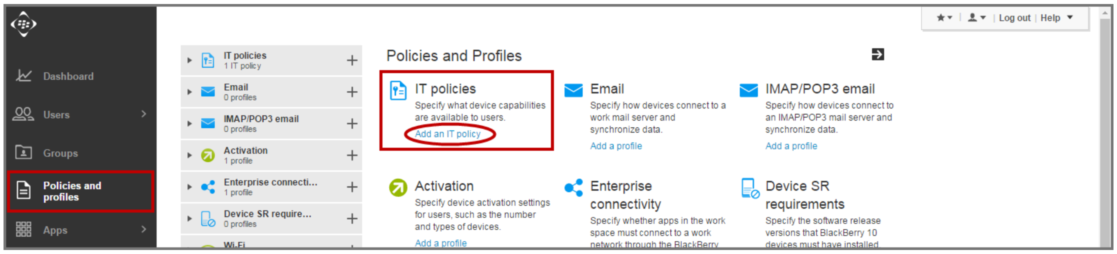
Creating IT Policies

We will create IT Policies that will be enforced on devices that are at risk. In this section, we will create an IT Policy that will be used to enforce restrict the At Risk device in some manner.

> **Note:** We will show a example policy, but these enforcement policies are something that the customer should create for their environment and needs. In a production environment, the customer should configure the compliance and IT policies according to their internal security policy.

The policy will specify the actions taken on At Risk devices. In our example, we will disable the camera, but you might create a policy that disables access to the corporate network or assets.

1. Navigate to **Policies and profiles**, and click the "Add an IT policy" link under "IT policies".



Policies and Profiles

IT policies
Specify what device capabilities are available to users.
Add an IT policy

Email
Specify how devices connect to a work mail server and synchronize data.
Add a profile

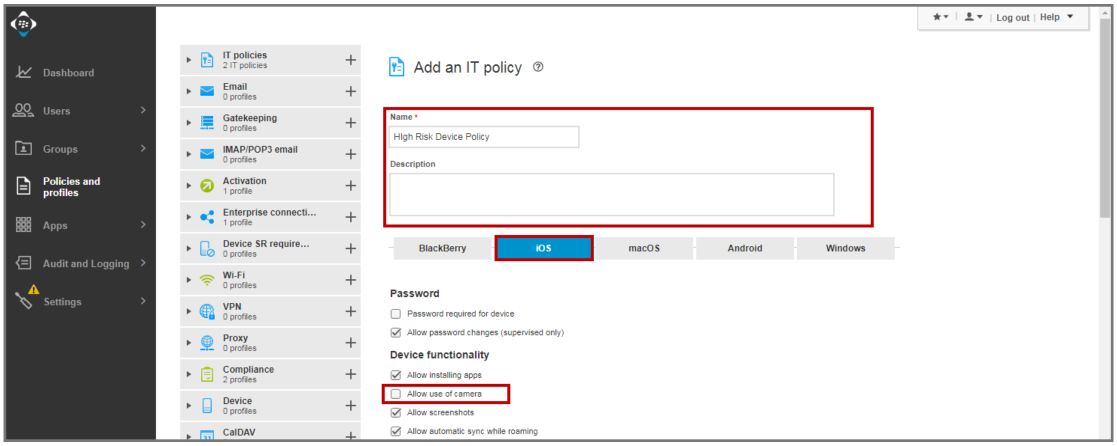
IMAP/POP3 email
Specify how devices connect to an IMAP/POP3 mail server and synchronize data.
Add a profile

Activation
Specify device activation settings for users, such as the number and types of devices.
Add a profile

Enterprise connectivity
Specify whether apps in the work space must connect to a work network through the BlackBerry

Device SR requirements
Specify the software release versions that BlackBerry 10 devices must have installed

2. Enter a Name for the policy, such as "High Risk Device Policy", select the "iOS" tab.
3. Under "Device functionality", unselect "Allow use of camera".



Add an IT policy

Name *
HIgh Risk Device Policy

Description

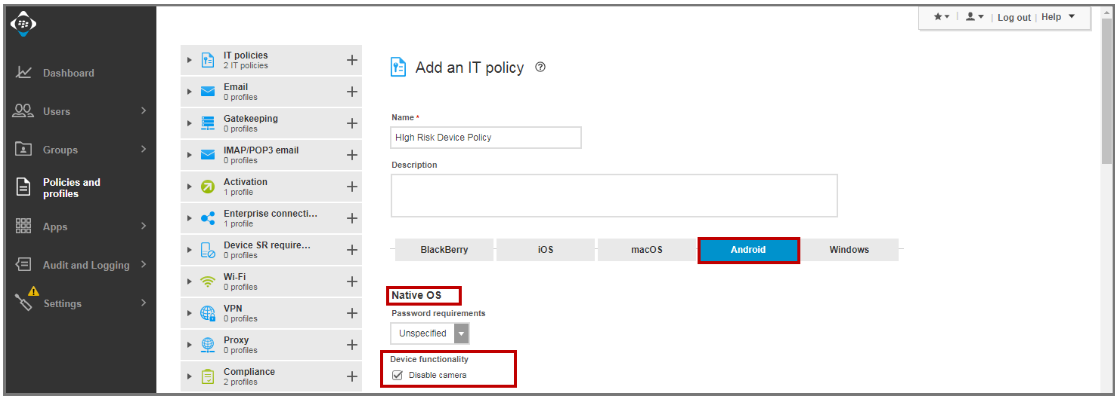
Password

☐ Password required for device
☑ Allow password changes (supervised only)

Device functionality

☑ Allow installing apps
☐ Allow use of camera
☑ Allow screenshots
☑ Allow automatic sync while roaming

4. Select the "Android" tab.
5. Under "Native OS > Device functionality", select "Disable camera".



Name * HIgh Risk Device Policy

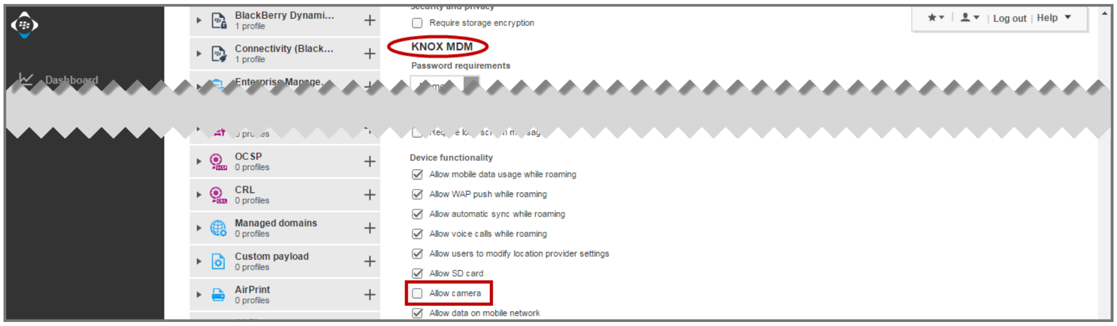
Description

Native OS

Password requirements: Unspecified

Device functionality
☑ Disable camera

6. Scroll to "KNOX MDM > Device functionality", unselect "Allow camera".



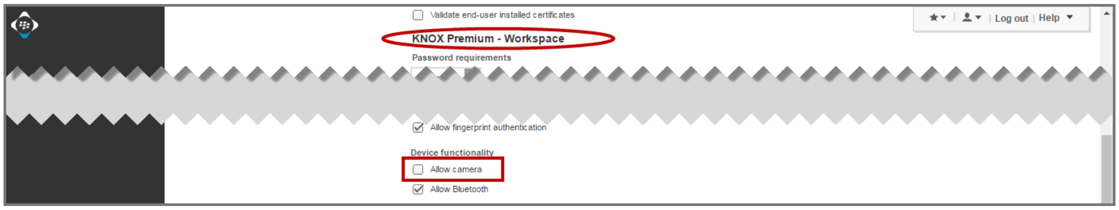
Security and privacy
□ Require storage encryption

KNOX MDM

Password requirements

Device functionality
☑ Allow mobile data usage while roaming
☑ Allow WAP push while roaming
☑ Allow automatic sync while roaming
☑ Allow voice calls while roaming
☑ Allow users to modify location provider settings
☑ Allow SD card
□ Allow camera
☑ Allow data on mobile network

7. Scroll to "KNOX Premium – Workspace > Device functionality", unselect "Allow camera".



□ Validate end-user installed certificates

KNOX Premium - Workspace

Password requirements

☑ Allow fingerprint authentication

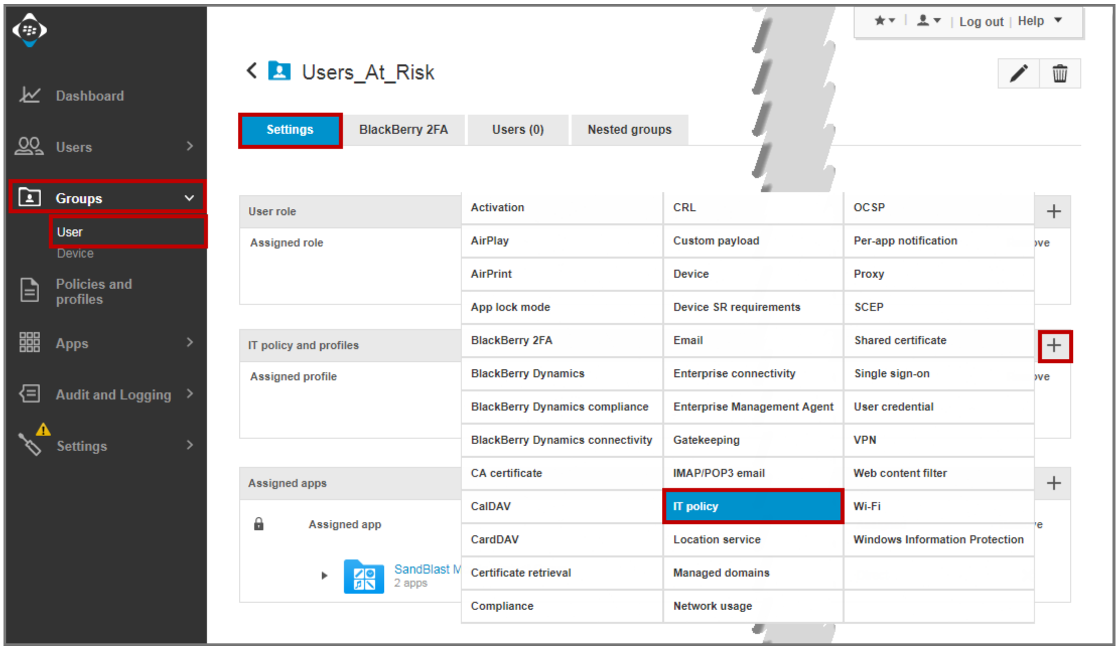
Device functionality
□ Allow camera
☑ Allow Bluetooth

8. Scroll to the bottom of the screen and click "Add".

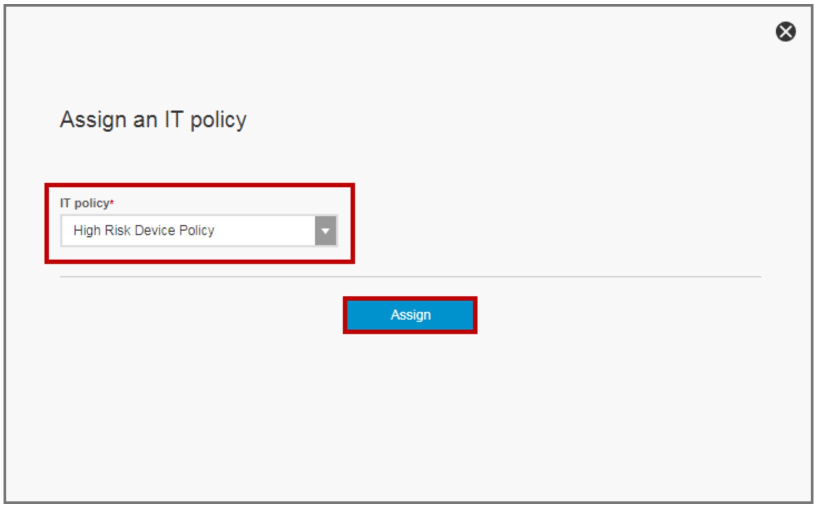
Applying the Policy to the User Mitigation Group

Now that we have created the policy ("High Risk Device Policy") we want to enforce, we need to link this policy to our User Mitigation Group ("Users_At_Risk") we created in "Creating Local User Group(s)" on page 18.

1. Navigate to **Groups > User groups**, find the user mitigation group you created in "Creating Local User Group(s)" on page 18, in our example "Users_At_Risk", and click group name link.
2. On the user mitigation group detailed view, click the "Settings" tab.
3. On the "Settings" tab, click "+" on the "IT policy and profiles" section.
4. Select "IT policy".



5. On the "Assign an IT policy" pop-up window, select the IT policy we created in "Creating IT Policies" on page 55, in our example "High Risk Device Policy".

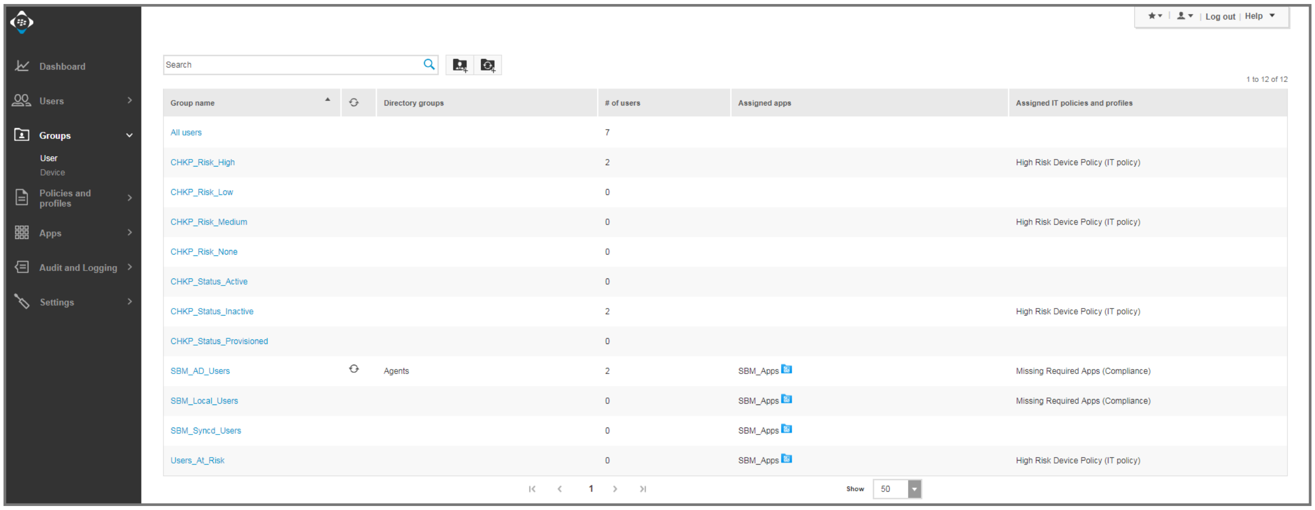

Assign an IT policy

IT policy*: High Risk Device Policy

6. Click "Assign".

Note: Now any device placed into the user groups, CHKP_Risk_High, CHKP_Risk_Medium or CHKP_Status_Inactive, which are nested under Users_At_Risk will have the policy actions in the IT Policy ("High Risk Device Policy") acted upon it.

7. When all of these steps have been completed, your User Groups will look something like this:



Group name	⟳	Directory groups	# of users	Assigned apps	Assigned IT policies and profiles
All users			7		
CHKP_Risk_High			2		High Risk Device Policy (IT policy)
CHKP_Risk_Low			0		
CHKP_Risk_Medium			0		High Risk Device Policy (IT policy)
CHKP_Risk_None			0		
CHKP_Status_Active			0		
CHKP_Status_Inactive			2		High Risk Device Policy (IT policy)
CHKP_Status_Provisioned			0		
SBM_AD_Users	⟳	Agents	2	SBM_Apps	Missing Required Apps (Compliance)
SBM_Local_Users			0	SBM_Apps	Missing Required Apps (Compliance)
SBM_Syncd_Users			0	SBM_Apps	
Users_At_Risk			0	SBM_Apps	High Risk Device Policy (IT policy)

© 2018 Check Point Software Technologies Ltd. All rights reserved.

Check Point
SOFTWARE TECHNOLOGIES LTD

Chapter 4

Registering Devices to SandBlast Mobile

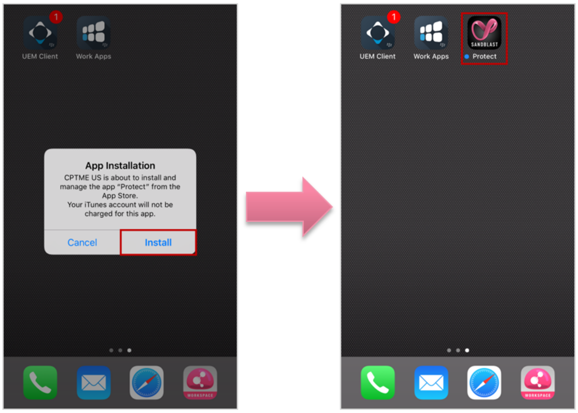
In this chapter we will cover the user experience of device registration with SandBlast Mobile.

This chapter discusses the following:

Registration of an iOS Device

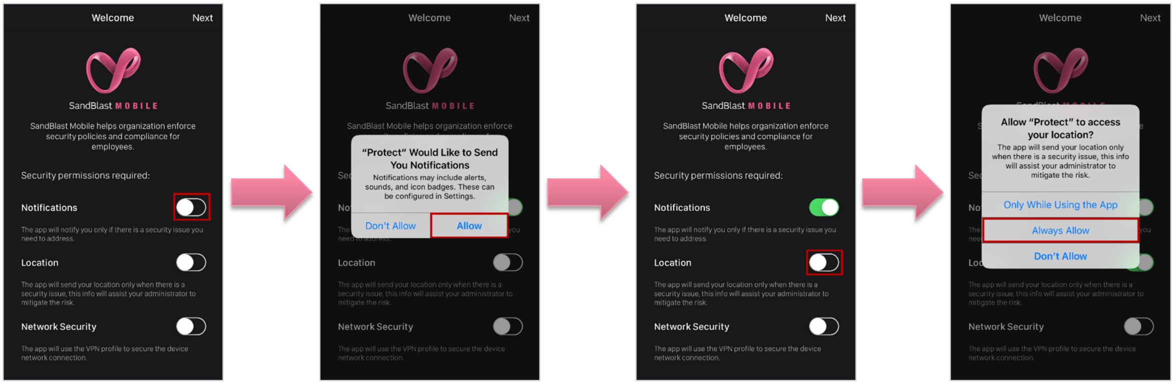
After the device is registered to the BlackBerry UEM system and the SandBlast Mobile Protect app has been "Assigned" to the User Provisioning Group ("SBM_Syncd_Users"), the user will be prompted to install the SandBlast Mobile Protect App. Users will be automatically assigned to "SBM_Syncd_Users" when their device has been provisioned within SandBlast Mobile. This keeps the users of experiencing registration issues if there is a time lag between device enrollment to BlackBerry UEM and that device being synchronized to the SandBlast Mobile Dashboard.

1. The user is prompted to install SandBlast Mobile Protect.
2. The user taps "INSTALL".
3. After the App has been installed on the iOS Device, the user only needs to launch the App to finish the registration.



App Installation
CPTME US is about to install and manage the app "Protect" from the App Store.
Your iTunes account will not be charged for this app.

4. The user will be prompted to install the SandBlast Mobile Protect App. The user taps "INSTALL".
5. After the App has been deployed on the iOS Device, the user only needs to launch the App to finish the registration. The registration server and key are automatically configured in the App by BlackBerry UEM.
6. The user is prompted to enable Notifications, Location, and Network Security.



Welcome — Next

SandBlast MOBILE

SandBlast Mobile helps organization enforce security policies and compliance for employees.

Security permissions required:

Notifications
The app will notify you only if there is a security issue you need to address.

Location
The app will send your location only when there is a security issue, this info will assist your administrator to mitigate the risk.

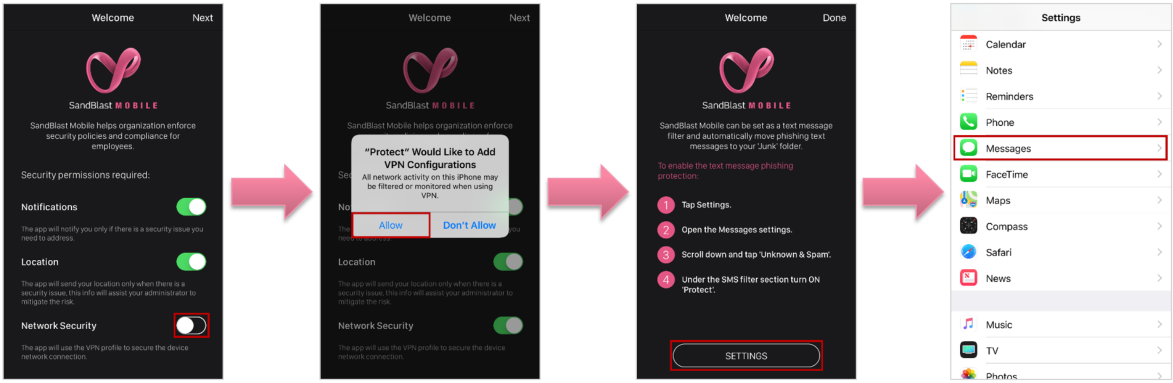
Network Security
The app will use the VPN profile to secure the device network connection.

"Protect" Would Like to Send You Notifications
Notifications may include alerts, sounds, and icon badges. These can be configured in Settings.
Don't Allow | Allow

Allow "Protect" to access your location?
The app will send your location only when there is a security issue, this info will assist your administrator to mitigate the risk.
Only While Using the App
Always Allow
Don't Allow

7. Continue with enabling Network Security, and tap "Allow" to allow SandBlast Mobile Protect to add the needed VPN Configuration profile.

8. The user is prompted to enable SMS Phishing Protection.



Welcome Next

SandBlast MOBILE

SandBlast Mobile helps organization enforce security policies and compliance for employees.

Security permissions required:

Notifications

The app will notify you only if there is a security issue you need to address.

Location

The app will send your location only when there is a security issue, this info will assist your administrator to mitigate the risk.

Network Security

The app will use the VPN profile to secure the device network connection.

"Protect" Would Like to Add VPN Configurations

All network activity on this iPhone may be filtered or monitored when using VPN.

Allow Don't Allow

Welcome Done

SandBlast MOBILE

SandBlast Mobile can be set as a text message filter and automatically move phishing text messages to your 'Junk' folder.

To enable the text message phishing protection:

1 Tap Settings.

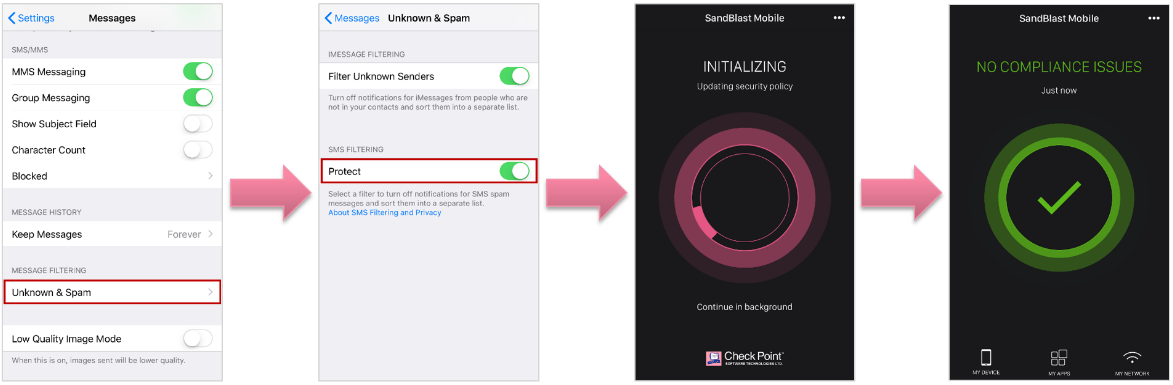
2 Open the Messages settings.

3 Scroll down and tap 'Unknown & Spam'.

4 Under the SMS filter section turn ON 'Protect'.

SETTINGS

9. Continue through Settings > Messages > Unknown & Spam, and make sure that SMS Phishing > Protect is enabled.
10. Returning to SandBlast Mobile Protect, tap "Done" to initialize the scanning of the device.
11. 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.



Settings Messages

SMS/MMS

MMS Messaging

Group Messaging

Show Subject Field

Character Count

Blocked

MESSAGE HISTORY

Keep Messages Forever

MESSAGE FILTERING

Unknown & Spam

Low Quality Image Mode

When this is on, images sent will be lower quality.

Messages Unknown & Spam

IMESSAGE FILTERING

Filter Unknown Senders

Turn off notifications for iMessages from people who are not in your contacts and sort them into a separate list.

SMS FILTERING

Protect

Select a filter to turn off notifications for SMS spam messages and sort them into a separate list.
About SMS Filtering and Privacy

SandBlast Mobile

INITIALIZING

Updating security policy

Continue in background

SandBlast Mobile

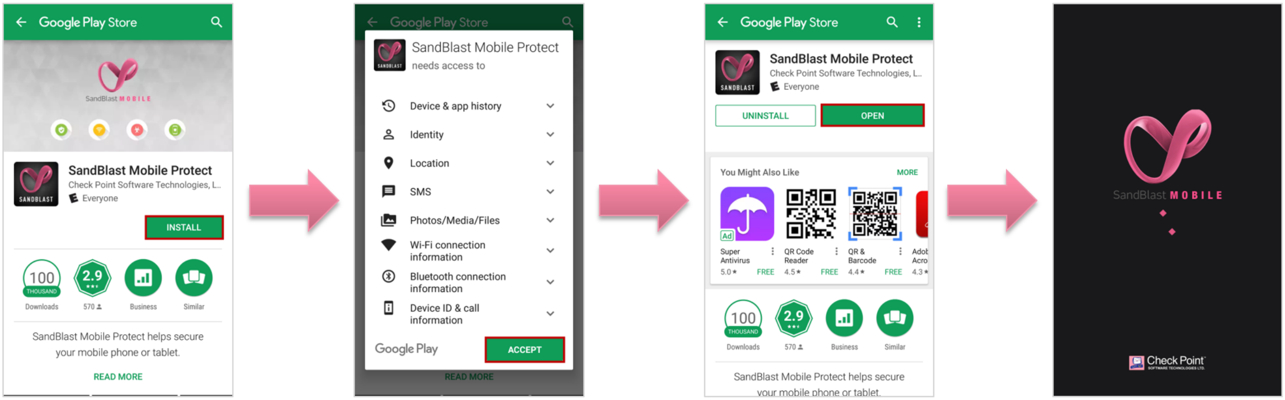
NO COMPLIANCE ISSUES

Just now

Registration of an Android Device

After the device is registered to the BlackBerry UEM system and the SandBlast Mobile Protect app has been "Assigned" to the User Provisioning Group ("SBM_Syncd_Users"), the user will be prompted to install the SandBlast Mobile Protect App.

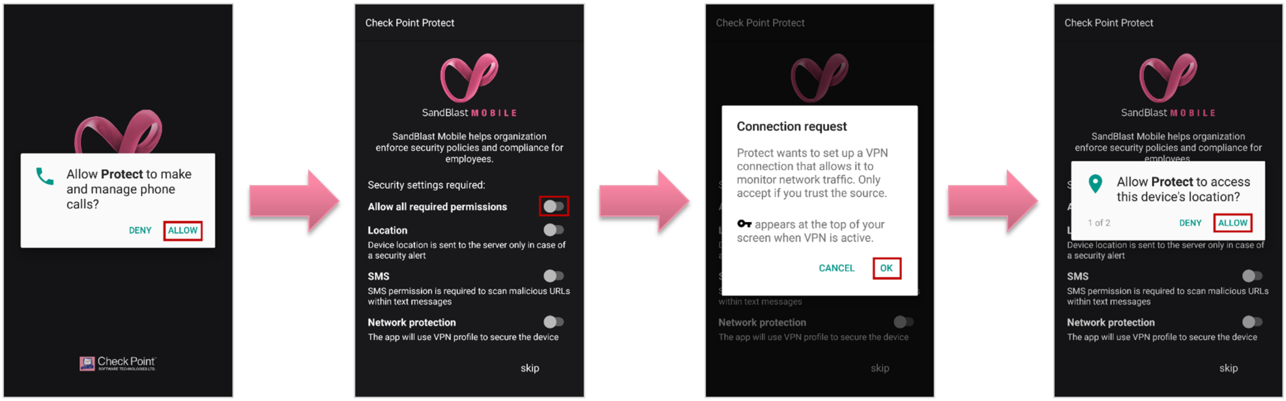
1. The user is prompted by the UEM client to install the SandBlast Mobile Protect app, tapping "OK".
2. The user taps the "INSTALL", and taps "ACCEPT" to accept the permissions of the App. The App installs.
3. After the App is installed, the user must launch the App to finish its deployment and registration to Check Point SandBlast Mobile.
4. The App will automatically register.



SandBlast Mobile Protect helps secure your mobile phone or tablet.

SandBlast Mobile Protect needs access to

5. The user is prompted to allow SandBlast Mobile Protect to make and manage phone calls. Tap "Allow".
6. The user is prompted to turn on Location, SMS, and Network Protection features. Tap "Allow all required permissions".
7. Tap "OK" to allow SandBlast Mobile Protect to configure a VPN connection. This is necessary for the Network Security Protection features of Safe Browsing and Anti-Phishing to work.
8. Tap "Allow" to allow SandBlast Mobile Protect to access this device's location.



Allow **Protect** to make and manage phone calls?

DENY ALLOW

Check Point Protect

SandBlast Mobile helps organization enforce security policies and compliance for employees.

Security settings required:

Allow all required permissions

Location
Device location is sent to the server only in case of a security alert

SMS
SMS permission is required to scan malicious URLs within text messages

Network protection
The app will use VPN profile to secure the device

skip

Connection request

Protect wants to set up a VPN connection that allows it to monitor network traffic. Only accept if you trust the source.

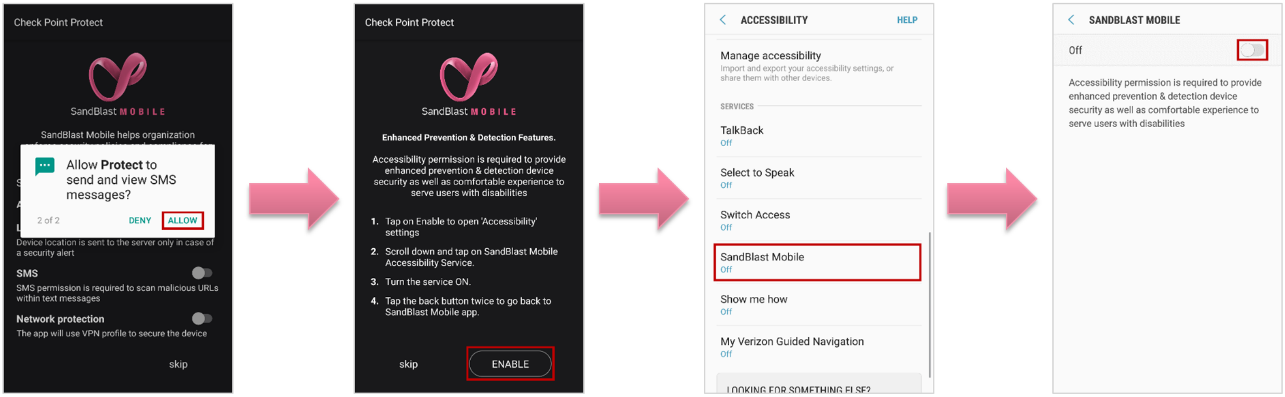
appears at the top of your screen when VPN is active.

CANCEL OK

Allow **Protect** to access this device's location?

1 of 2 DENY ALLOW

9. Tap "Allow" to allow SandBlast Mobile Protect to provide SMS protection.
10. Tap "Enable" to configure Accessibility permissions for SandBlast Mobile Protect.
11. Scroll down and tap "SandBlast Mobile". and tap the toggle to turn Accessibility ON.



Allow **Protect** to send and view SMS messages?

Device location is sent to the server only in case of a security alert

SMS permission is required to scan malicious URLs within text messages

The app will use VPN profile to secure the device

Enhanced Prevention & Detection Features.

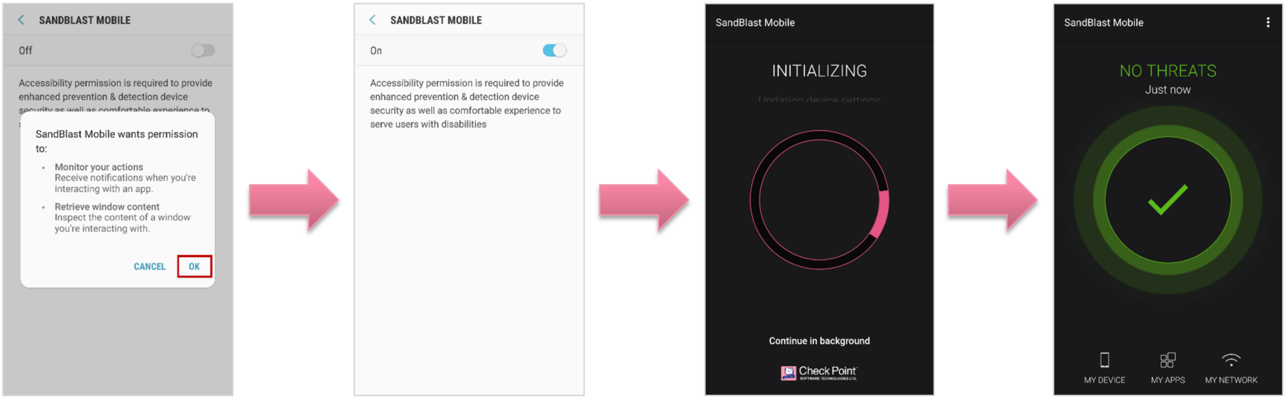
Accessibility permission is required to provide enhanced prevention & detection device security as well as comfortable experience to serve users with disabilities

1. Tap on Enable to open 'Accessibility' settings
2. Scroll down and tap on SandBlast Mobile Accessibility Service.
3. Turn the service ON.
4. Tap the back button twice to go back to SandBlast Mobile app.

Import and export your accessibility settings, or share them with other devices.

Accessibility permission is required to provide enhanced prevention & detection device security as well as comfortable experience to serve users with disabilities

12. Continue with configuring the Accessibility permissions for SandBlast Mobile Protect. Tap "OK".
13. Return to SandBlast Mobile Protect.
14. 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.



Accessibility permission is required to provide enhanced prevention & detection device security as well as comfortable experience to

SandBlast Mobile wants permission to:

- **Monitor your actions**
  Receive notifications when you're interacting with an app.
- **Retrieve window content**
  Inspect the content of a window you're interacting with.

Accessibility permission is required to provide enhanced prevention & detection device security as well as comfortable experience to serve users with disabilities

Redeployment of the SandBlast Mobile Protect App – iOS

If the user removes the SandBlast Mobile Protect app, the device will be out of compliance. Because the iOS app is auto-configured, the user only needs to open the BlackBerry UEM client App Catalog, and choose to install SandBlast Mobile Protect.

> **Note:** The instructions for installing and registration of the SandBlast Mobile Protect app are described in "Registration of an iOS Device" on page 60.

Redeployment of the SandBlast Mobile Protect App - Android

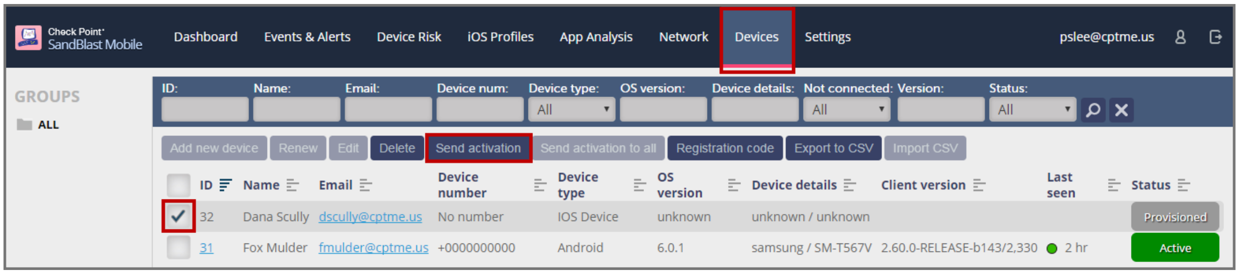
If the user removes the SandBlast Mobile Protect app, the device will be out of compliance. Because the Android app is auto-configured, the user only needs to open the BlackBerry UEM client App Catalog, and choose to install SandBlast Mobile Protect.

Note: The instructions for installing and registration of the SandBlast Mobile Protect app are described in "Registration of an Android Device" on page 62.

Resending SandBlast Mobile Activation Code

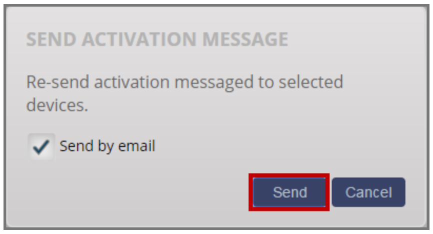
If the user requires the activation registration email/SMS to be resent to them, the administrator will log into the SandBlast Mobile Dashboard.

1. Navigating to the Devices tab, select the device to which to send activation code, and click "Send activation".



	ID	Name	Email	Device number	Device type	OS version	Device details	Client version	Last seen	Status
☑	32	Dana Scully	dscully@cptme.us	No number	IOS Device	unknown	unknown / unknown			Provisioned
□	31	Fox Mulder	fmulder@cptme.us	+0000000000	Android	6.0.1	samsung / SM-T567V	2.60.0-RELEASE-b143/2,330	● 2 hr	Active

2. On the pop-up "Send Activation Message" window, select the type of message, and click "Send". If the device has a phone number assigned, the message could be sent via SMS text message as well.

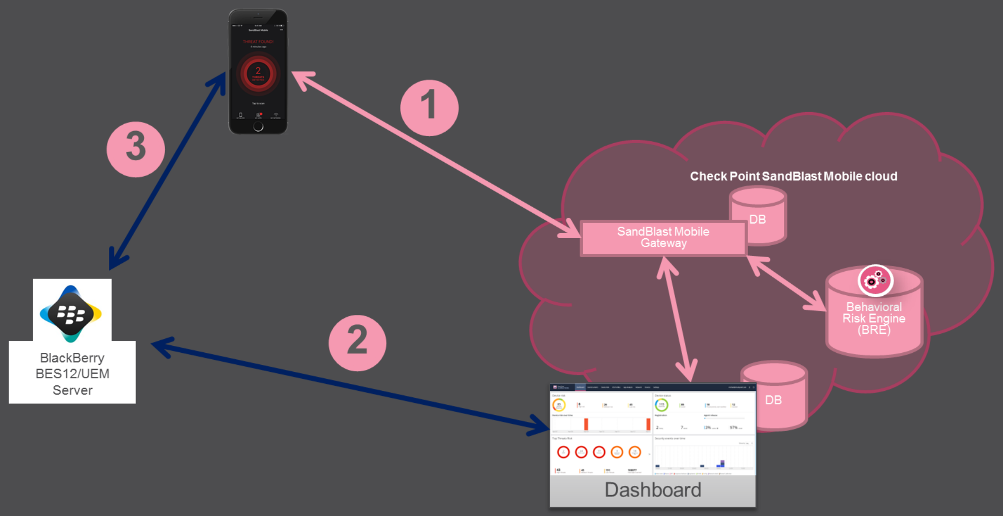

SEND ACTIVATION MESSAGE

Re-send activation messaged to selected devices.

☑ Send by email

Chapter 5

Testing High Risk Activity Detection and Policy Enforcement


1
3
Check Point SandBlast Mobile cloud
DB
SandBlast Mobile Gateway
Behavioral Risk Engine (BRE)
BlackBerry BES12/UEM Server
2
DB
Dashboard

1 – SandBlast Mobile sends risk notification to User’s Device

2 – SandBlast Mobile sends the risk level for User’s Device to BlackBerry BES12/UEM

3 – BlackBerry BES12/UEM activates the appropriate compliance policy for User’s Device based on security risk level

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 BlackBerry UEM system for that device.

BlackBerry UEM receives the group assignment change, and applies any policies belonging to that group (either by direct or indirect assignment).

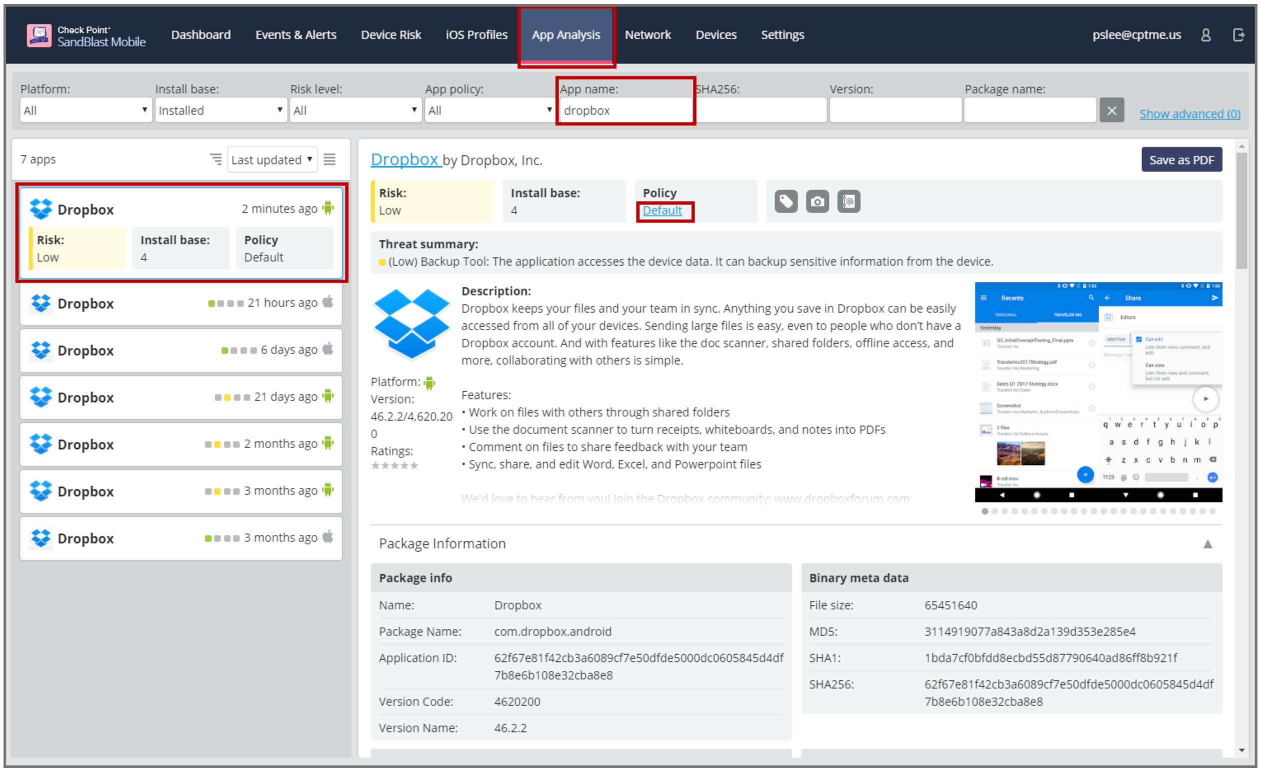
In the following example, the Administrator will blacklist an app, such as in our example "Dropbox". As a result, all the devices with the app, "Dropbox", installed will be identified to be at High Risk (CHKP_Risk_High) due to the blacklisted app, "Dropbox". The SandBlast Mobile Dashboard will notify the user, and mark the device as belonging to the CHKP_Risk_High group to the BlackBerry UEM system. The BlackBerry UEM System will then enforce policy actions specified in the IT policy, in our example "High Risk Device Policy". This mitigation process was the one we created in "Creating a Mitigation Process" on page 55.

This chapter discusses the following:

Blacklisting a Test App

The first step is to blacklist an app, in our example "Dropbox". By blacklisting this app, all release version and OS types will also be blacklisted. In our example, Dropbox for Android will be blacklisted which will result in all Dropbox numbered release versions for Android 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 "Dropbox".



Platform: All
Install base: Installed
Risk level: All
App policy: All
App name: dropbox
SHA256:
Version:
Package name:

7 apps

Dropbox 2 minutes ago
Risk: Low | Install base: 4 | Policy Default

Dropbox 21 hours ago

Dropbox 6 days ago

Dropbox 21 days ago

Dropbox 2 months ago

Dropbox 3 months ago

Dropbox 3 months ago

Dropbox by Dropbox, Inc.

Risk: Low | Install base: 4 | Policy Default

Threat summary:
(Low) Backup Tool: The application accesses the device data. It can backup sensitive information from the device.

Description:
Dropbox keeps your files and your team in sync. Anything you save in Dropbox can be easily accessed from all of your devices. Sending large files is easy, even to people who don't have a Dropbox account. And with features like the doc scanner, shared folders, offline access, and more, collaborating with others is simple.

Platform:
Version: 46.2.2/4,620,200
Ratings: ★★★★★

Features:
• Work on files with others through shared folders
• Use the document scanner to turn receipts, whiteboards, and notes into PDFs
• Comment on files to share feedback with your team
• Sync, share, and edit Word, Excel, and Powerpoint files

We'd love to hear from you! Join the Dropbox community: www.dropboxforum.com

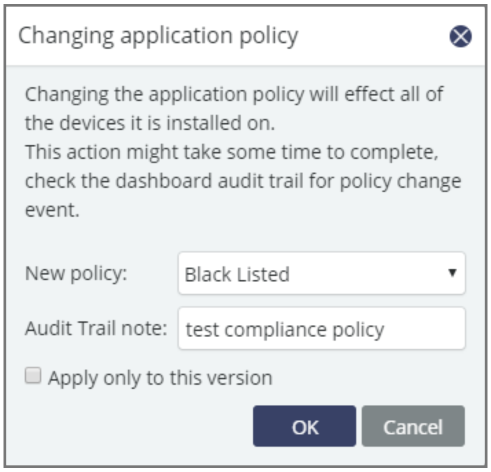
Package Information

Package info	
Name:	Dropbox
Package Name:	com.dropbox.android
Application ID:	62f67e81f42cb3a6089cf7e50dfde5000dc0605845d4df7b8e6b108e32cba8e8
Version Code:	4620200
Version Name:	46.2.2

Binary meta data	
File size:	65451640
MD5:	3114919077a843a8d2a139d353e285e4
SHA1:	1bda7cf0bfdd8ecbd55d87790640ad86ff8b921f
SHA256:	62f67e81f42cb3a6089cf7e50dfde5000dc0605845d4df7b8e6b108e32cba8e8

3. Click "Policy" link of "Default".

4. On the "Changing application policy" pop-up window, select "Black Listed" from the "New policy" drop-down menu, and enter a reason for this change in the "Audit Trail note".



Changing application policy

Changing the application policy will effect all of the devices it is installed on.
This action might take some time to complete, check the dashboard audit trail for policy change event.

New policy: Black Listed ▾

Audit Trail note: test compliance policy

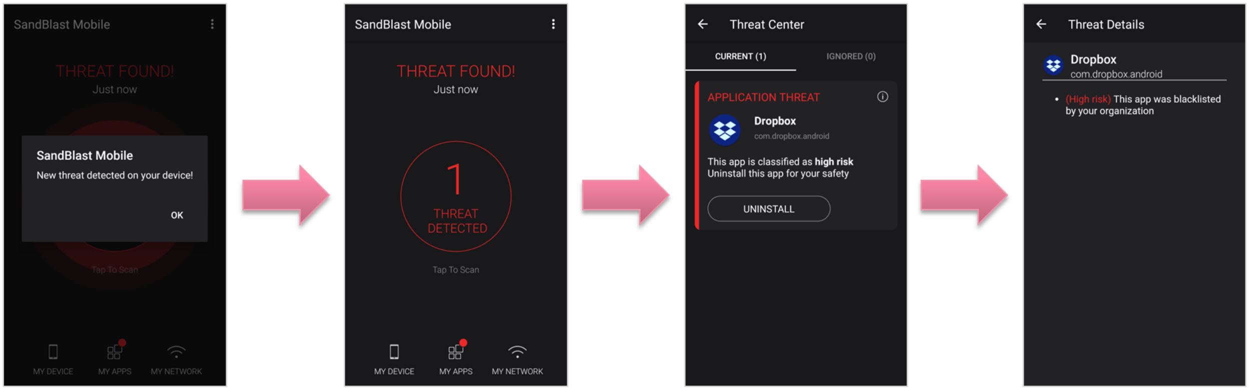
☐ Apply only to this version

5. Click "OK".

View of Non-Compliant Device

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 "Dropbox".



SandBlast Mobile

THREAT FOUND!
Just now

SandBlast Mobile
New threat detected on your device!

1 THREAT DETECTED

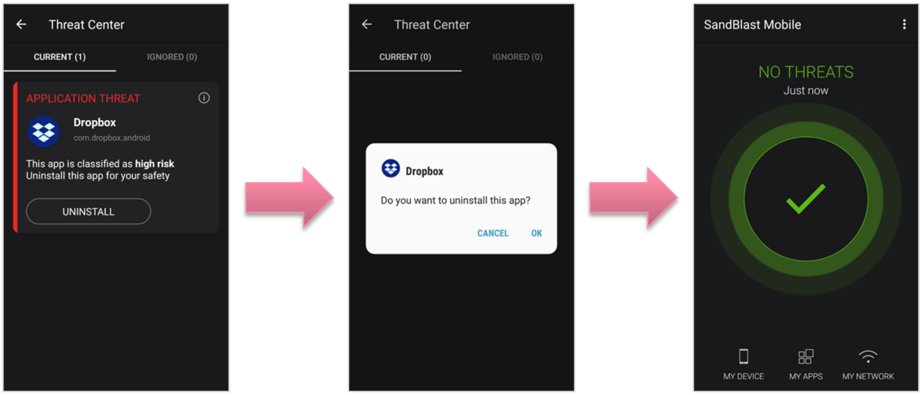
Threat Center

APPLICATION THREAT
Dropbox
com.dropbox.android
This app is classified as **high risk**
Uninstall this app for your safety

Threat Details

Dropbox
com.dropbox.android
- (High risk) This app was blacklisted by your organization

2. Once the issue has been remediated by the user, the system will update the security posture.



Threat Center

APPLICATION THREAT
Dropbox
com.dropbox.android
This app is classified as **high risk**
Uninstall this app for your safety

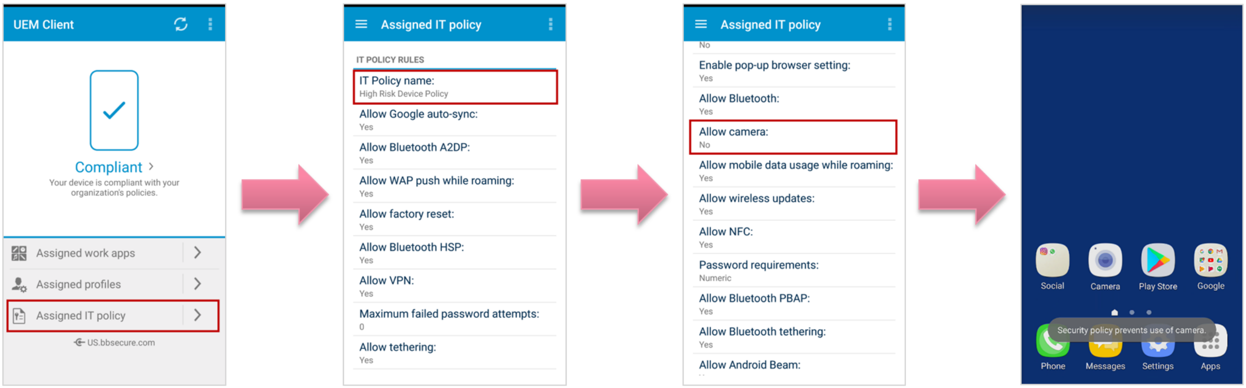
Dropbox
Do you want to uninstall this app?

SandBlast Mobile

NO THREATS
Just now

UEM Client App Notifications

1. The user will not be able to use the device's camera, as specified in the compliance actions (policy) we created in "Creating IT Policies" on page 55, in our example "High Risk Device Policy" until the user removes the blacklisted app.
2. Your policy will probably block the device's access to corporate networks and data by disabling VPN profiles, connections to email, and/or connecting to the Corporate Wi-Fi, until the issue is remediated.



UEM Client

Compliant >
Your device is compliant with your organization's policies.

Assigned work apps >
Assigned profiles >
Assigned IT policy >

US.bbsecure.com

Assigned IT policy

IT POLICY RULES

IT Policy name:
High Risk Device Policy

Allow Google auto-sync:
Yes

Allow Bluetooth A2DP:
Yes

Allow WAP push while roaming:
Yes

Allow factory reset:
Yes

Allow Bluetooth HSP:
Yes

Allow VPN:
Yes

Maximum failed password attempts:
0

Allow tethering:
Yes

Assigned IT policy

No

Enable pop-up browser setting:
Yes

Allow Bluetooth:
Yes

Allow camera:
No

Allow mobile data usage while roaming:
Yes

Allow wireless updates:
Yes

Allow NFC:
Yes

Password requirements:
Numeric

Allow Bluetooth PBAP:
Yes

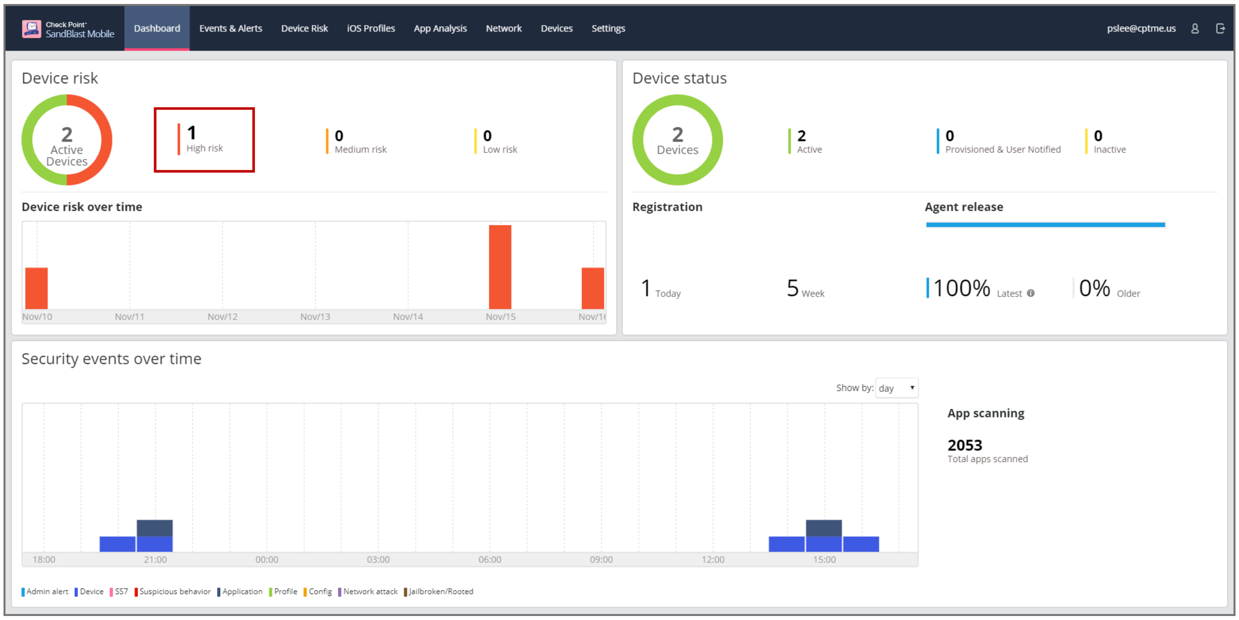
Allow Bluetooth tethering:
Yes

Allow Android Beam:

Security policy prevents use of camera.

Administrator View on the SandBlast Mobile Dashboard

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



Device risk

2 Active Devices

1 High risk

0 Medium risk

0 Low risk

Device risk over time

Device status

2 Devices

2 Active

0 Provisioned & User Notified

0 Inactive

Registration

1 Today

5 Week

Agent release

100% Latest

0% Older

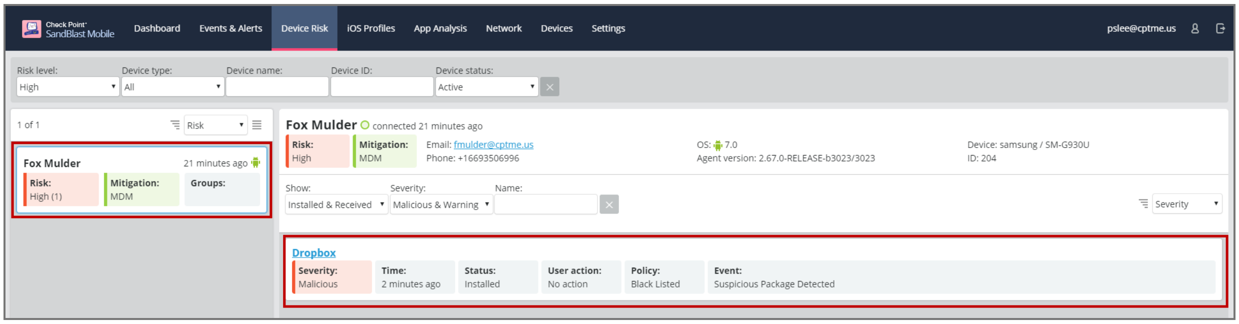
Security events over time

Show by: day

App scanning

2053
Total apps scanned

2. Clicking the High Risk will display a list of devices at high risk.
3. 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, "Dropbox".



Risk level: High | Device type: All | Device name: | Device ID: | Device status: Active

Fox Mulder 21 minutes ago
Risk: High (1) | Mitigation: MDM | Groups:

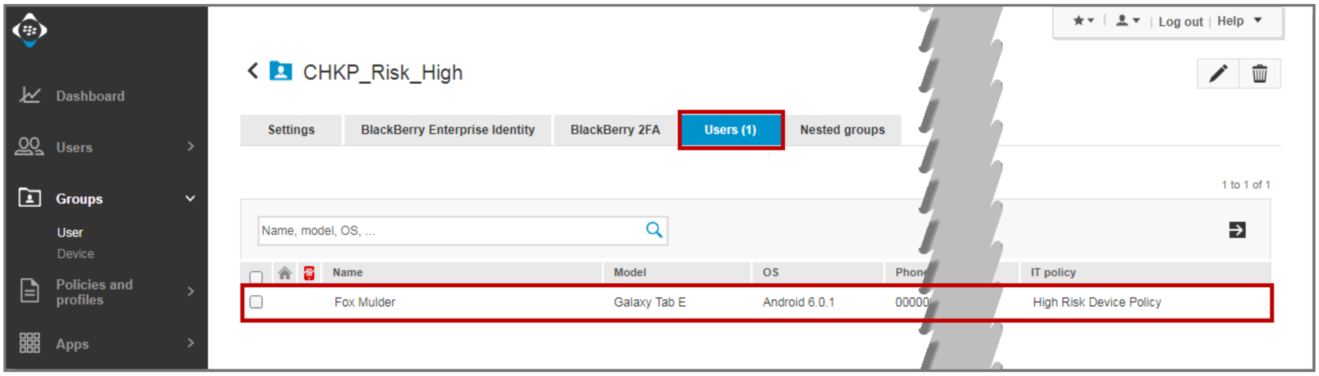
Fox Mulder connected 21 minutes ago
Risk: High | Mitigation: MDM | Email: fmulder@cptme.us | Phone: +16693506996 | OS: 7.0 | Agent version: 2.67.0-RELEASE-b3023/3023 | Device: samsung / SM-G930U | ID: 204

Show: Installed & Received | Severity: Malicious & Warning | Name:

Dropbox
Severity: Malicious | Time: 2 minutes ago | Status: Installed | User action: No action | Policy: Black Listed | Event: Suspicious Package Detected

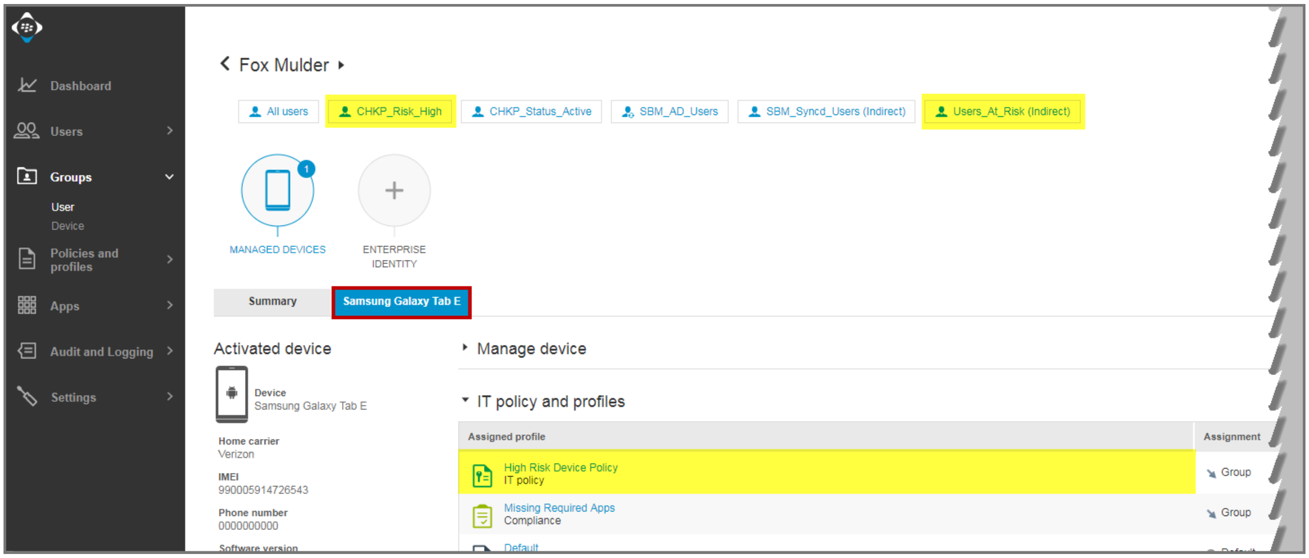
Administrator View on the BlackBerry UEM Console

1. In the BlackBerry UEM Console, in the User Device Detail screen the Administrator can see that the user is now a member of the "CHKP_Risk_High" group and indirectly a member of the "Users_At_Risk" group, and that the IT policy "High Risk Device Policy" has been assigned.



CHKP_Risk_High

Name	Model	OS	Phon	IT policy
Fox Mulder	Galaxy Tab E	Android 6.0.1	00000	High Risk Device Policy



Fox Mulder

All users | CHKP_Risk_High | CHKP_Status_Active | SBM_AD_Users | SBM_Syncd_Users (Indirect) | Users_At_Risk (Indirect)

Activated device

Device
Samsung Galaxy Tab E

Home carrier
Verizon

IMEI
990005914726543

Phone number
0000000000

Software version

IT policy and profiles

Assigned profile	Assignment
High Risk Device Policy IT policy	Group
Missing Required Apps Compliance	Group
Default	Default

Appendix

Integration Information

Information Name	Value
UEM Server URL	
UEM Web Services URL	
UEM SRP ID	
UEM SandBlast Mobile Admin Username	
UEM SandBlast Mobile Admin Password	
UEM Group(s)	
UEM Mitigation Group	
Tag Device Status (Boolean tags) become user groups in UEM	CHKP_Status_Provisioned, CHKP_Status_Active, CHKP_Status_Inactive
Tag Device Risk (Boolean tags) become user groups in UEM	CHKP_Risk_None, CHKP_Risk_Low, CHKP_Risk_Medium, CHKP_Risk_High
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

CONTACT US

Worldwide Headquarters | 5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: 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