

Check Point SandBlast Mobile

MDM Integration Guide with IBM MaaS360

Classification: none



Check Point
SOFTWARE TECHNOLOGIES LTD.

© 2017 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 is a registered trademark 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. MaaS360 is registered trademark of IBM and/or its affiliates.

About This Guide

Only Check Point provides a complete mobile security solution that protects devices from threats on the device (OS), in apps, in SMS messages, and in the network, and delivers the industry's highest threat catch rate for iOS and Android. Check Point SandBlast Mobile uses malicious app detection to find known and unknown threats by applying threat emulation, advanced static code analysis, app reputation and machine learning.

- Perform advanced app analysis to detect known and unknown threats
- Monitor network activity for suspicious or malicious behavior
- Monitor SMS messages received for malicious URLs
- Assess device-level (OS) vulnerabilities to reduce the attack surface

It 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 Check Point SandBlast Mobile solution ("the Solution") includes the following components:

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

In cooperation with an MDM, the SandBlast Mobile Solution provides integral risk assessment of the device to which the MDM can use to quarantine or enforce a set of policies that are in effect until the device is no longer at High 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 Check Point SandBlast Mobile Dashboard with the IBM MaaS360 MDM. It provides a quick tour through the interface of the MaaS360 Portal and the SandBlast Mobile Dashboard in order enable integration, alerting, and policy enforcement.

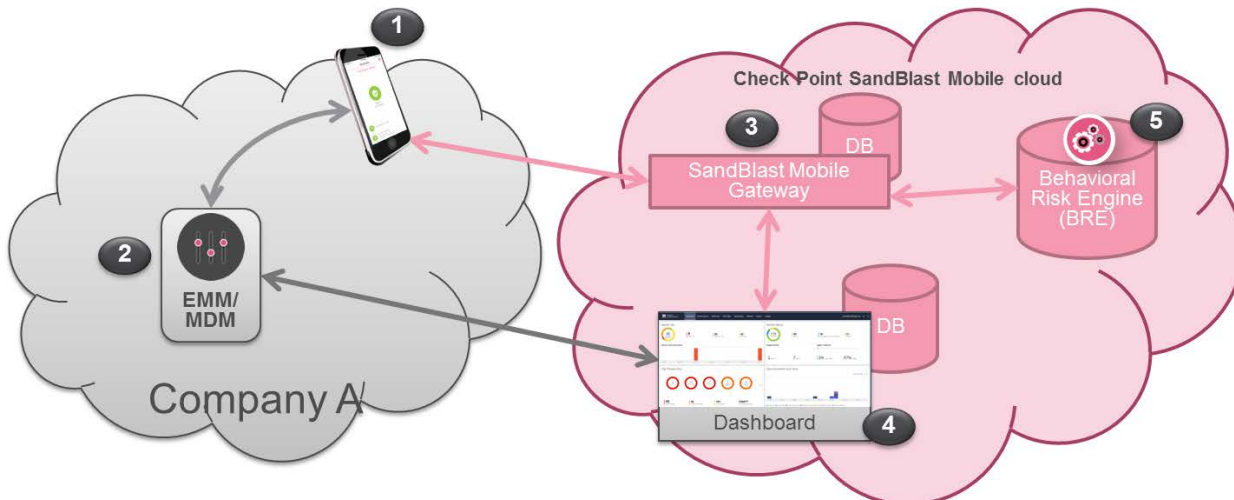
This includes activation and protection of a new device, malware detection, and mitigation (including mitigation flow).

Note: During the procedures in this this document there a quite a few pieces of information that you will need to gather or create. There is a form in Section 7.3 that you can record your settings for easy reference.

Contents

1	SOLUTION ARCHITECTURE	5
1.1	COMPONENTS	5
2	PREPARING MDM PLATFORM FOR INTEGRATION	6
2.1	PREREQUISITES	6
2.2	MAAS360 PORTAL.....	6
2.3	CREATING AN API ONLY ADMINISTRATOR ACCOUNT (OPTIONAL)	6
2.4	ADDING A USER	14
2.5	CREATING A USER GROUPS	17
2.6	CREATING A DEVICE PROVISIONING GROUP	23
2.7	ADDING A DEVICE TO AN EXISTING USER.....	28
2.8	CREATING A MITIGATION PROCESS	35
3	CONFIGURING THE SANDBLAST MOBILE DASHBOARD MDM INTEGRATION SETTINGS.....	48
3.1	PREREQUISITES	48
3.2	CONFIGURING MDM INTEGRATION SETTINGS	49
4	CONFIGURING MDM TO DEPLOY SANDBLAST MOBILE PROTECT APP	53
4.1	PREREQUISITES	53
4.2	ADDING THE SANDBLAST MOBILE PROTECT APP TO YOUR APP CATALOG.....	53
4.3	DEPLOYING SANDBLAST MOBILE PROTECT APP	55
4.4	SETTING POLICY TO REQUIRE SANDBLAST MOBILE PROTECT TO BE INSTALLED.....	56
5	DEPLOYING SANDBLAST MOBILE PROTECT APP TO THE DEVICES.....	63
5.1	REGISTRATION OF AN IOS DEVICE.....	63
5.2	REGISTRATION OF AN ANDROID DEVICE	64
6	TESTING HIGH RISK ACTIVITY DETECTION AND POLICY ENFORCEMENT	67
6.1	BLACKLISTING A TEST APP	68
6.2	VIEW OF NON-COMPLIANT DEVICE.....	69
6.3	ADMINISTRATOR VIEW ON THE SANDBLAST MOBILE DASHBOARD	71
6.4	ADMINISTRATOR VIEW ON THE MAAS360 PORTAL.....	72
7	APPENDICES.....	75
7.1	SANDBLAST MOBILE COMMUNICATION INFORMATION.....	75
7.2	DISCOVERING YOUR SANDBLAST GATEWAY NAME AND REGION.....	76
7.3	INTEGRATION INFORMATION	77

1 Solution Architecture



1.1 Components

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 EMM/MDM	- Enterprise Mobility Management/Mobile Device Management - 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") SandBlast Mobile Dashboard instance.
4 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 SandBlast Mobile Dashboard can be integrated with an existing Mobile Device Management (MDM)/Enterprise Mobility Management (EMM) solution for automated policy enforcement on devices at risk. - When using this integration, the MDM/EMM serves as a repository with which the SandBlast Mobile 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.

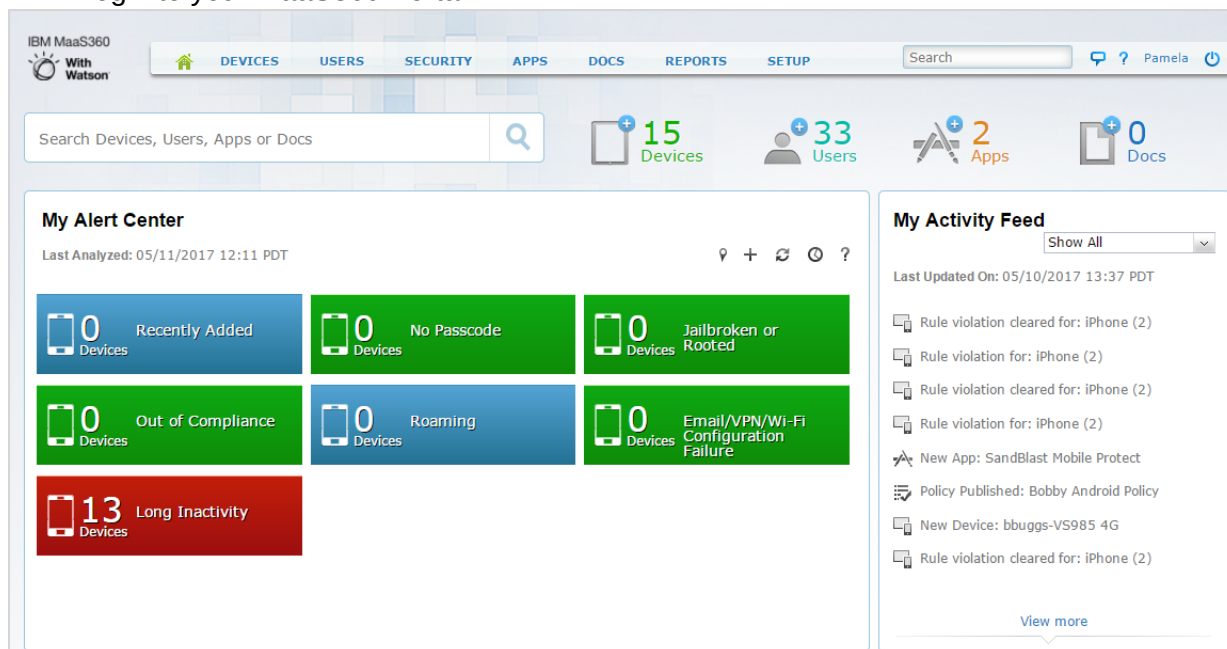
2 Preparing MDM Platform for Integration

2.1 Prerequisites

- 2.1.1. MaaS360 version 10.0 or higher with REST API access enabled.
- 2.1.2. For on-premise MaaS360 Deployments, the port used for the API must be accessible remotely through your firewall before trying to connect.

2.2 MaaS360 Portal

- 2.2.1. Login to your MaaS360 Portal.



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 Section 7.3 that you can record your settings for easy reference.

2.3 Creating an API Only Administrator Account (optional)

For the interaction at the API, we will create an API admin user in the MaaS360 Portal that you use to limit the capability of the admin credentials used between the SandBlast Mobile Dashboard and the MaaS360 system.

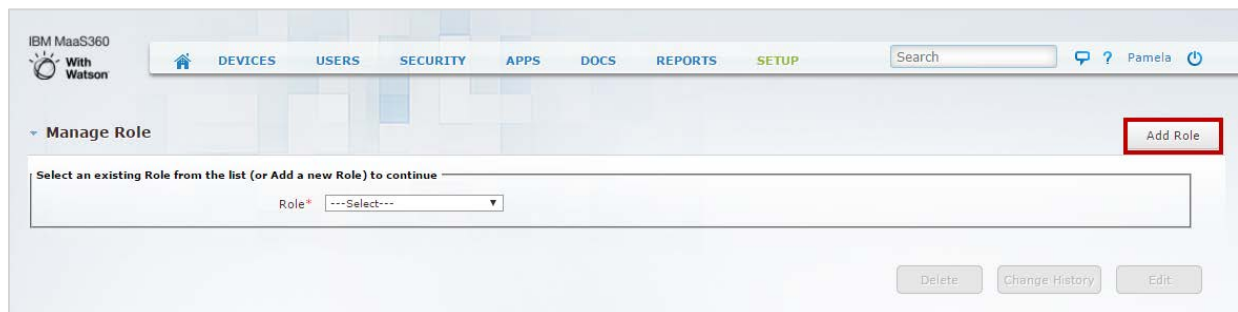
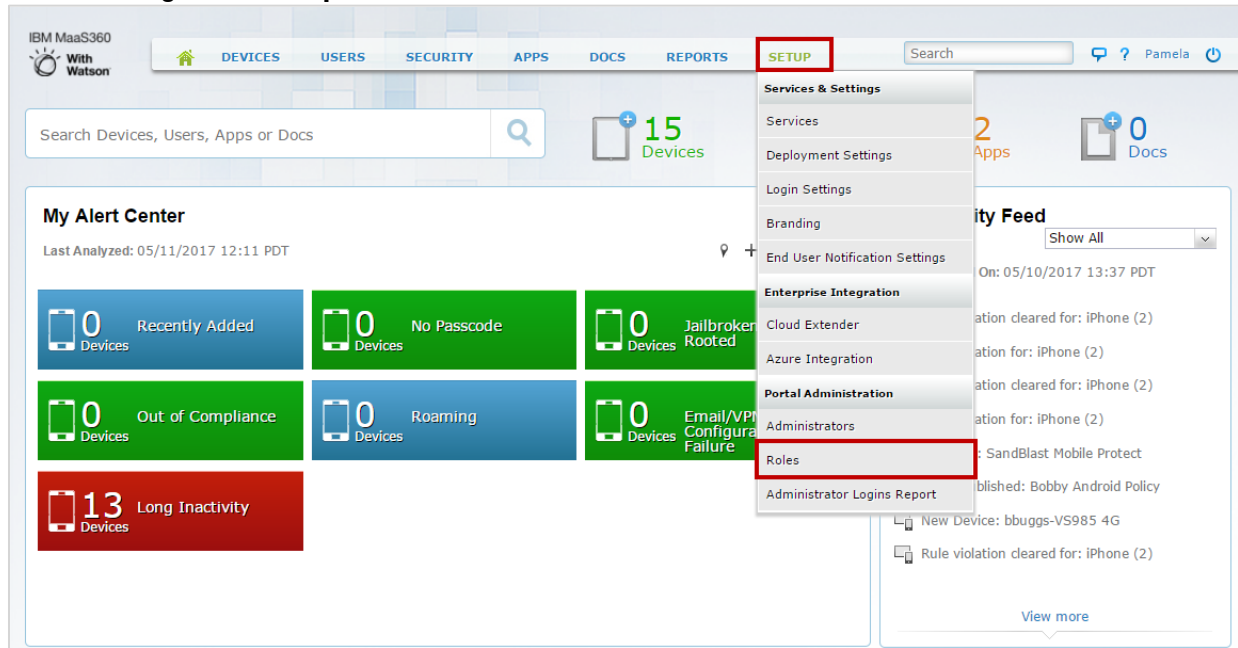
Note: It is a best practice to create such an admin account and highly recommended, but is optional.

Note: Creating an administrator account and administrator role requires a “Services Administrator” level role.

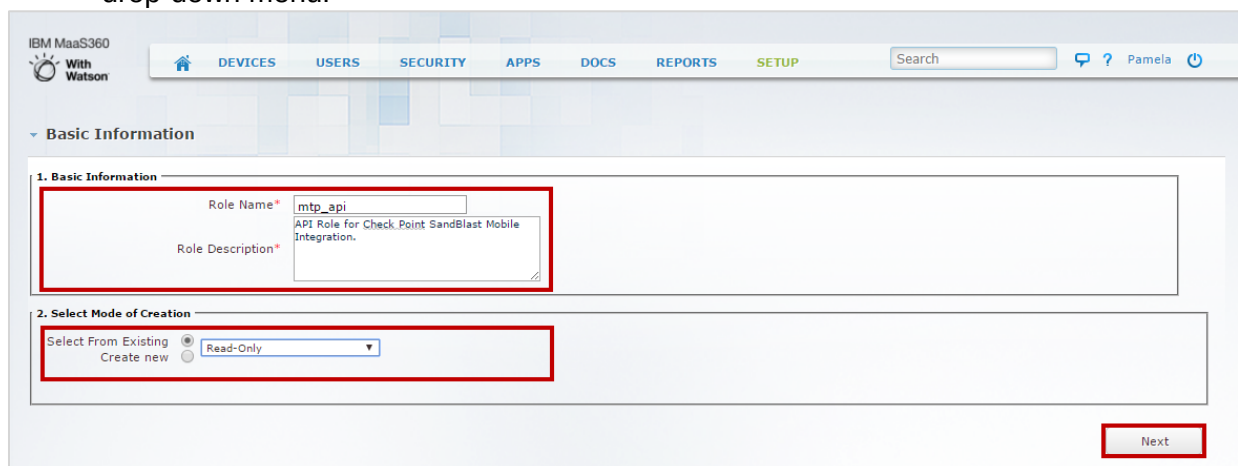
To create an “API” Administrator Account, follow this process.

2.3.1 Create a New API Only Administrator Role

2.3.1.1. Navigate to **Setup > Portal Administration > Roles**, click “Add Role” button.

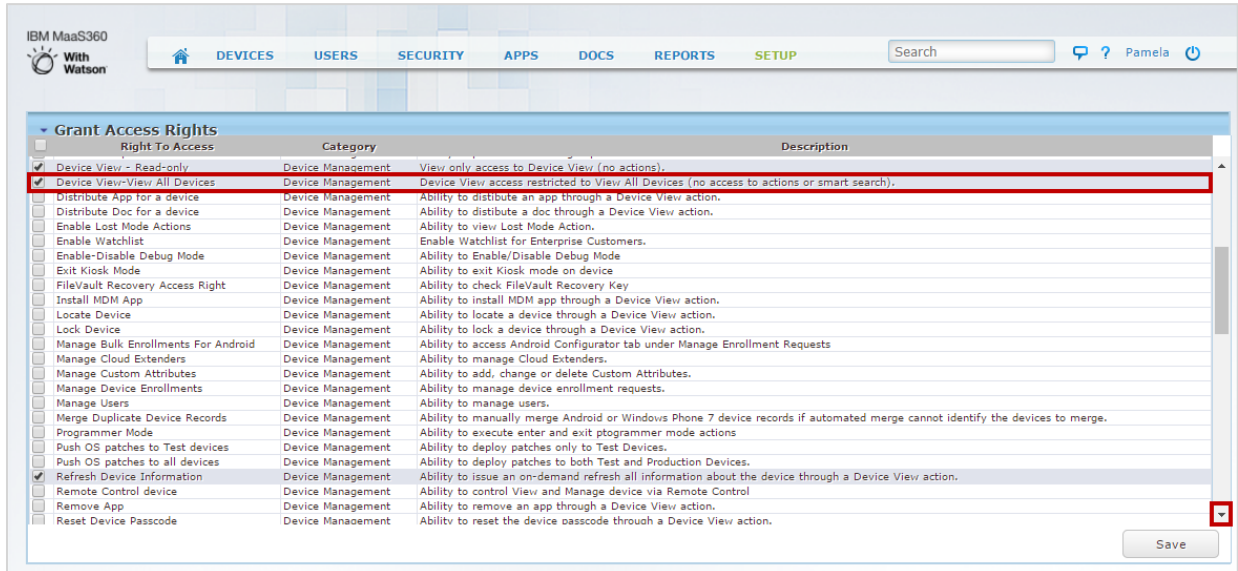


2.3.1.2. Enter in a Role Name, such as “mtp_api”, and a description, select the “Select From Existing” radio button for “Select Mode of Creation”, and choose “Read-Only” from the drop-down menu.

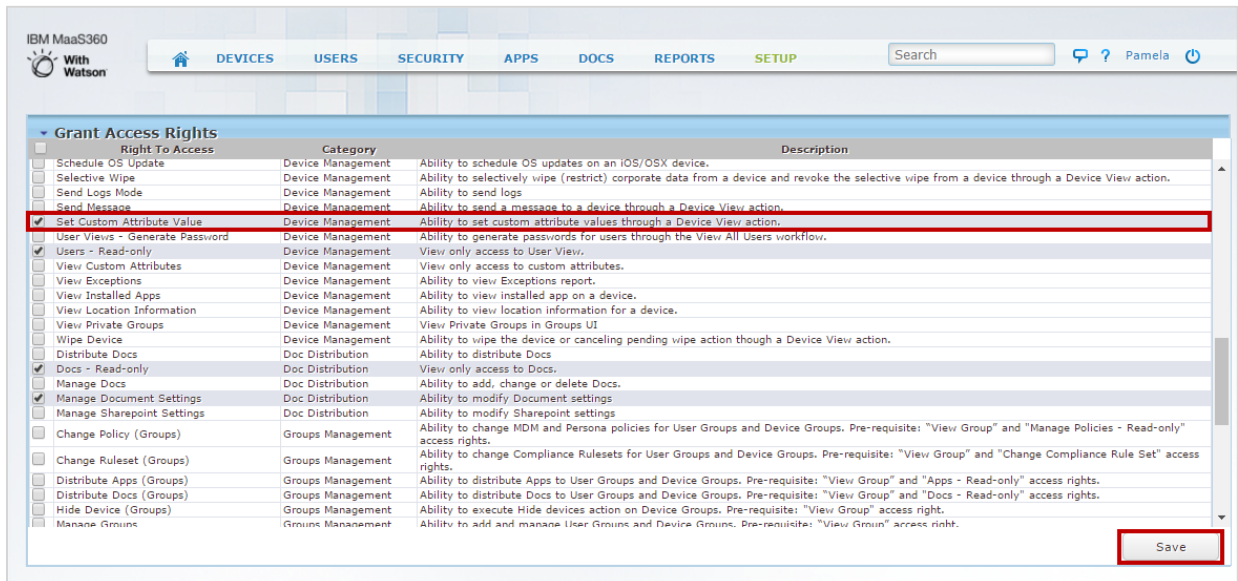


2.3.1.3. Click the “Next” button. The “Grant Access Rights” window is displayed.

- 2.3.1.4. On the “Grant Access Rights” screen, scroll down the list and select the following additional access rights for the new role:
- + Device View – All Devices
 - + Set Custom Attribute Value



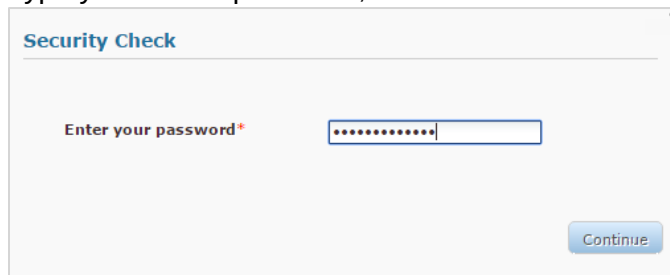
Right To Access	Category	Description
☒ Device View - Read-only	Device Management	View only access to Device View (no actions).
☒ Device View-View All Devices	Device Management	Device View access restricted to View All Devices (no access to actions or smart search).
☐ Distribute App for a device	Device Management	Ability to distribute an app through a Device View action.
☐ Distribute Doc for a device	Device Management	Ability to distribute a doc through a Device View action.
☐ Enable Lost Mode Actions	Device Management	Ability to view Lost Mode Action.
☐ Enable Watchlist	Device Management	Enable Watchlist for Enterprise Customers.
☐ Enable-Disable Debug Mode	Device Management	Ability to Enable/Disable Debug Mode.
☐ Exit Kiosk Mode	Device Management	Ability to exit Kiosk mode on device.
☐ FileVault Recovery Access Right	Device Management	Ability to check FileVault Recovery Key.
☐ Install MDM App	Device Management	Ability to install MDM app through a Device View action.
☐ Locate Device	Device Management	Ability to locate a device through a Device View action.
☐ Lock Device	Device Management	Ability to lock a device through a Device View action.
☐ Manage Bulk Enrollments For Android	Device Management	Ability to access Android Configurator tab under Manage Enrollment Requests.
☐ Manage Cloud Extenders	Device Management	Ability to manage Cloud Extenders.
☐ Manage Custom Attributes	Device Management	Ability to add, change or delete Custom Attributes.
☐ Manage Device Enrollments	Device Management	Ability to manage device enrollment requests.
☐ Manage Users	Device Management	Ability to manage users.
☐ Merge Duplicate Device Records	Device Management	Ability to manually merge Android or Windows Phone 7 device records if automated merge cannot identify the devices to merge.
☐ Programmer Mode	Device Management	Ability to execute enter and exit programmer mode actions.
☐ Push OS patches to Test devices	Device Management	Ability to deploy patches only to Test Devices.
☐ Push OS patches to all devices	Device Management	Ability to deploy patches to both Test and Production Devices.
☒ Refresh Device Information	Device Management	Ability to issue an on-demand refresh all information about the device through a Device View action.
☐ Remote Control Device	Device Management	Ability to control View and Manage device via Remote Control.
☐ Remove App	Device Management	Ability to remove an app through a Device View action.
☐ Reset Device Passcode	Device Management	Ability to reset the device passcode through a Device View action.



Right To Access	Category	Description
☐ Schedule OS Update	Device Management	Ability to schedule OS updates on an iOS/OSX device.
☐ Selective Wipe	Device Management	Ability to selectively wipe (restrict) corporate data from a device and revoke the selective wipe from a device through a Device View action.
☐ Send Logs Mode	Device Management	Ability to send logs.
☐ Send Message	Device Management	Ability to send a message to a device through a Device View action.
☒ Set Custom Attribute Value	Device Management	Ability to set custom attribute values through a Device View action.
☐ User Views - Generate Password	Device Management	Ability to generate passwords for users through the View All Users workflow.
☒ Users - Read-only	Device Management	View only access to User View.
☐ View Custom Attributes	Device Management	View only access to custom attributes.
☐ View Exceptions	Device Management	Ability to view Exceptions report.
☐ View Installed Apps	Device Management	Ability to view installed app on a device.
☐ View Location Information	Device Management	Ability to view location information for a device.
☐ View Private Groups	Device Management	View Private Groups in Groups UI.
☐ Wipe Device	Device Management	Ability to wipe the device or canceling pending wipe action through a Device View action.
☐ Distribute Docs	Doc Distribution	Ability to distribute Docs.
☐ Docs - Read-only	Doc Distribution	View only access to Docs.
☒ Manage Docs	Doc Distribution	Ability to add, change or delete Docs.
☐ Manage Document Settings	Doc Distribution	Ability to modify Document settings.
☐ Manage Sharepoint Settings	Doc Distribution	Ability to modify Sharepoint settings.
☐ Change Policy (Groups)	Groups Management	Ability to change MDM and Persona policies for User Groups and Device Groups. Pre-requisite: "View Group" and "Manage Policies - Read-only" access rights.
☐ Change Ruleset (Groups)	Groups Management	Ability to change Compliance Rulesets for User Groups and Device Groups. Pre-requisite: "View Group" and "Change Compliance Rule Set" access rights.
☐ Distribute Apps (Groups)	Groups Management	Ability to distribute Apps to User Groups and Device Groups. Pre-requisite: "View Group" and "Apps - Read-only" access rights.
☐ Distribute Docs (Groups)	Groups Management	Ability to distribute Docs to User Groups and Device Groups. Pre-requisite: "View Group" and "Docs - Read-only" access rights.
☐ Hide Device (Groups)	Groups Management	Ability to execute Hide devices action on Device Groups. Pre-requisite: "View Group" access right.
☐ Manage Groups	Groups Management	Ability to add and manage User Groups and Device Groups. Pre-requisite: "View Group" access right.

- 2.3.1.5. Click the “Save” button.

- 2.3.1.6. Type your admin password, and then click the “Continue” button.



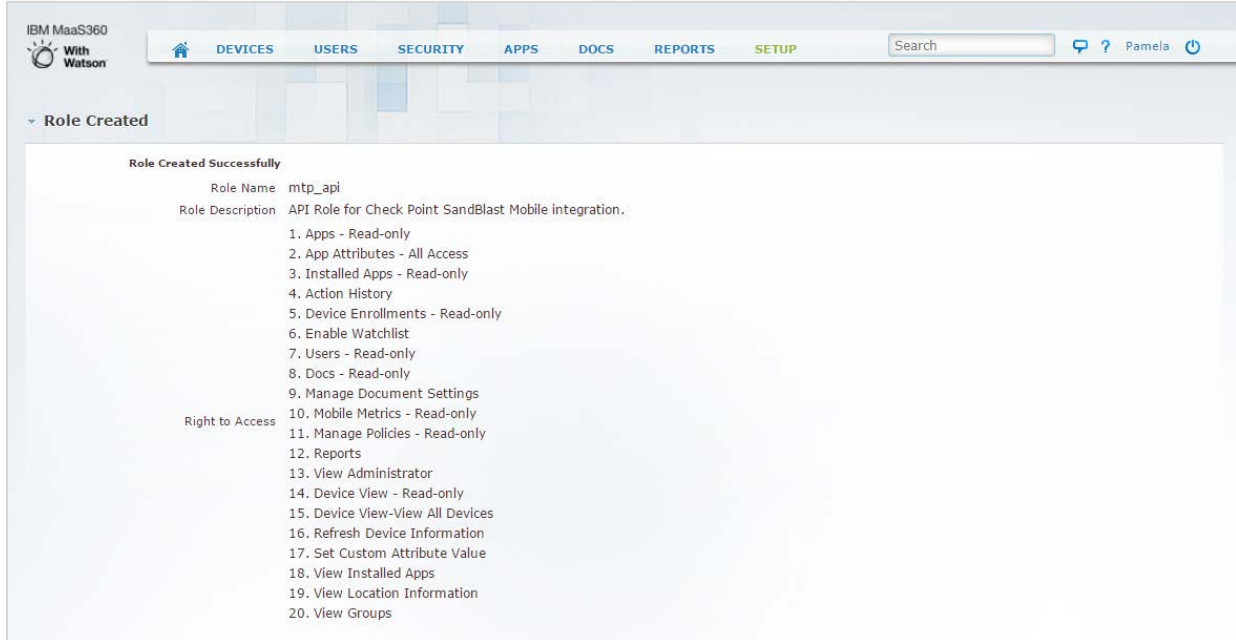
Security Check

Enter your password*

.....

Continue

2.3.1.7. A confirmation message is displayed.

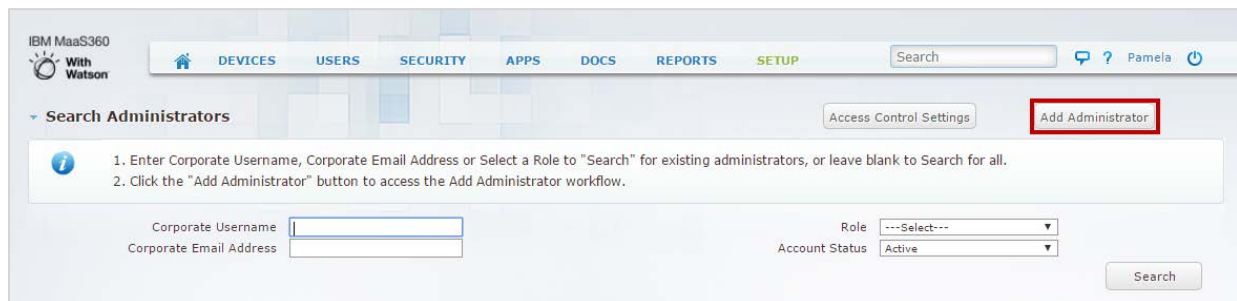
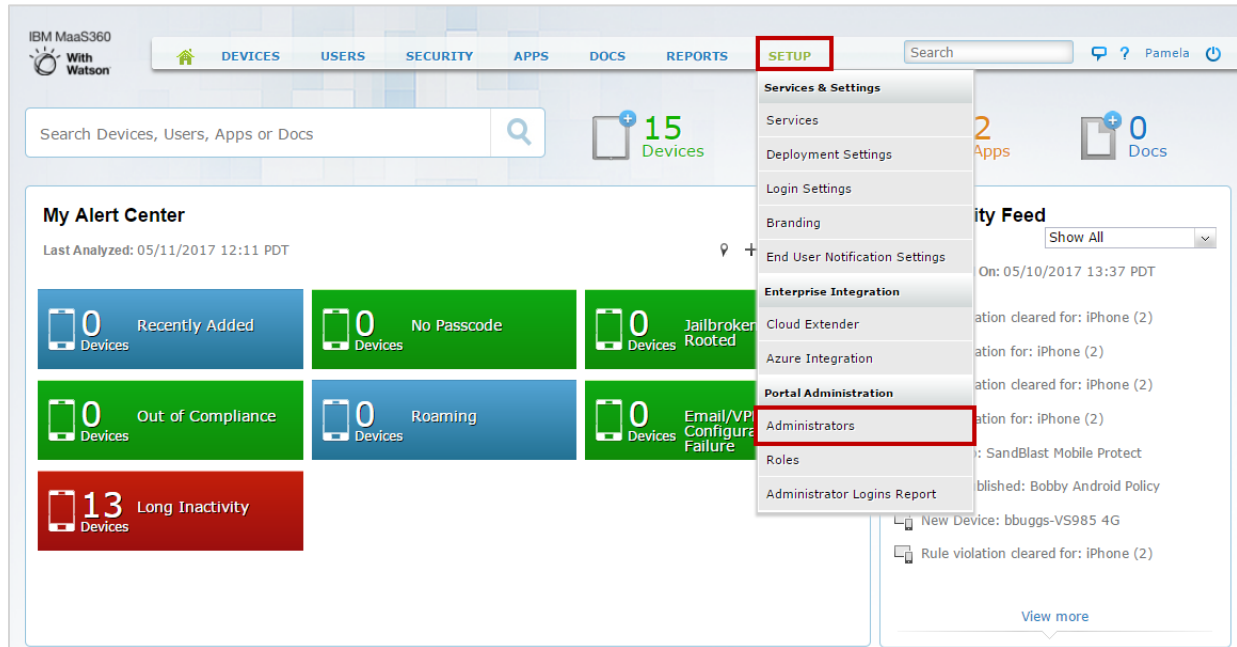


The screenshot shows the IBM MaaS360 console interface. At the top, there is a navigation bar with tabs for DEVICES, USERS, SECURITY, APPS, DOCS, REPORTS, and SETUP. A search bar and user profile (Pamela) are also visible. Below the navigation bar, a message box titled 'Role Created' is displayed, indicating that a role named 'mtp_api' has been successfully created. The role description is 'API Role for Check Point SandBlast Mobile integration.' and it lists 20 specific rights to access.

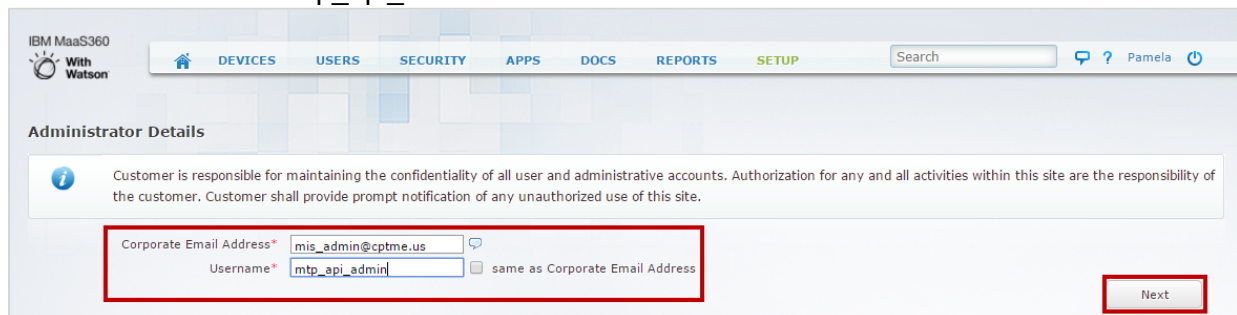
Role Name	Role Description	Right to Access
mtp_api	API Role for Check Point SandBlast Mobile integration.	1. Apps - Read-only 2. App Attributes - All Access 3. Installed Apps - Read-only 4. Action History 5. Device Enrollments - Read-only 6. Enable Watchlist 7. Users - Read-only 8. Docs - Read-only 9. Manage Document Settings 10. Mobile Metrics - Read-only 11. Manage Policies - Read-only 12. Reports 13. View Administrator 14. Device View - Read-only 15. Device View-View All Devices 16. Refresh Device Information 17. Set Custom Attribute Value 18. View Installed Apps 19. View Location Information 20. View Groups

2.3.2 Create a New Administrator Account

2.3.2.1. Navigate to **Setup > Portal Administration > Administrators**, click the “Add Administrator” button.



2.3.2.2. On the Administrator Details window, fill in the email address and the user name for the new administrator. If the user name is the same as the email address, select the “same as Corporate Email Address” checkbox. In our example, we will create an admin username of “mtp_api_admin”.



2.3.2.3. Click the “Next” button.

- 2.3.2.4. On the “Assign Roles” window, select the Role created in the previous section (2.3.1), in our example “mtp_api”.

- 2.3.2.5. Click the “Next” button.

- 2.3.2.6. On the “Review Details” window, review to ensure the configuration is appropriate.

- 2.3.2.7. Click the “Save” button.

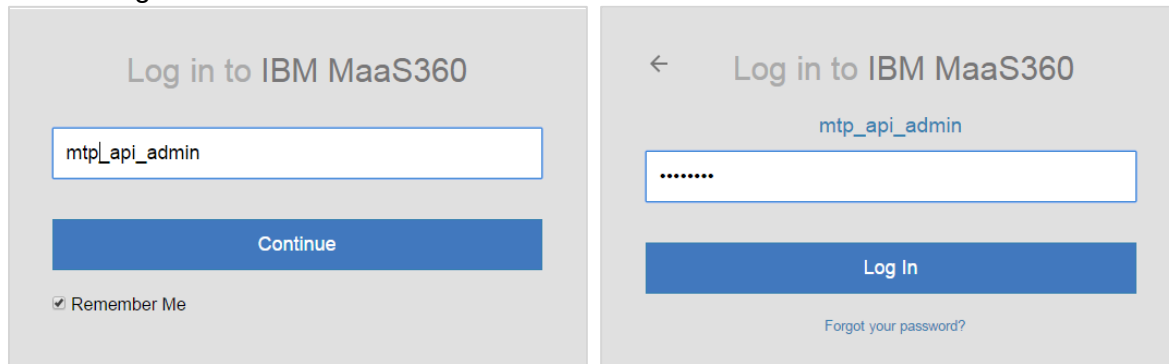
- 2.3.2.8. Type your admin password, and then click the “Continue” button.

- 2.3.2.9. A confirmation message is displayed.

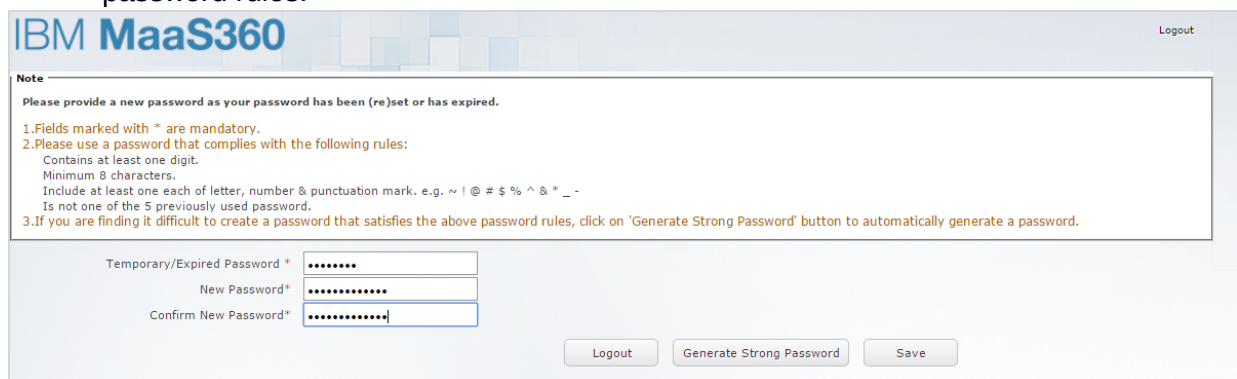
- 2.3.2.10. Finish the creation of the new admin account by logging out of the MaaS360 portal, and then logging back in using the credentials sent to the email address used for mtp_api_admin. This will force you to select a new unique password.



- 2.3.2.11. Log into MaaS360 Portal with the above credentials.



- 2.3.2.12. You are then prompted to select a new password. Enter a password that satisfies the password rules.



- 2.3.2.13. Click the “Save” button.

2.3.2.14. Enter in a First Name, Last Name, and Contact Phone Number in the “Add Personal Information” form.

2.3.2.15. Click the “Save” button.

Note: Log out and log back into the MaaS360 Portal with your Service Administrator credentials to continue with the configuration.

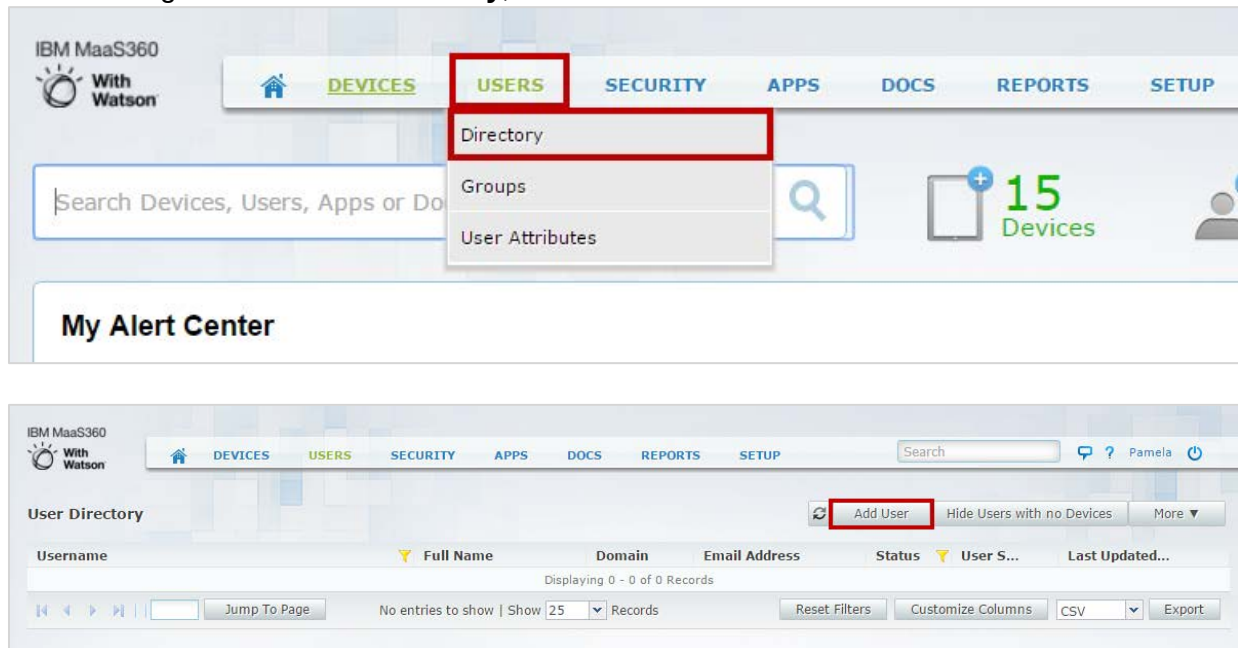
2.4 Adding a User

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

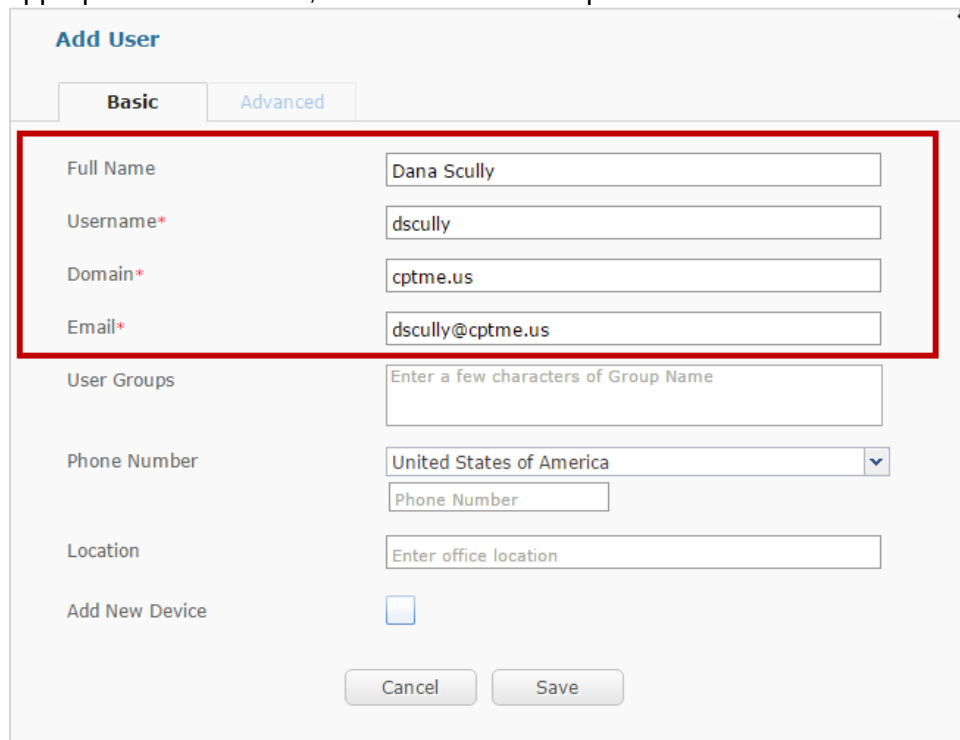
Note: Use the Cloud Extender or Azure AD Integration to integrate with your Corporate User Directory to import group and associated user information. Cloud Extender is available for download on the Services enablement workflow. Azure AD Integration is available as part of Enterprise Integration. Imported information can be used for automatic provisioning of users, group based policy assignment and App & Doc distribution. Supported User Directories for Cloud Extender are Active Directory, OpenLDAP, Novell LDAP, IBM Domino LDAP and Oracle User Directory.

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

2.4.0.1. Navigate to **Users > Directory**, click the “Add User” button.



- 2.4.0.2. On the “Add User” pop-up window “Basic” tab, fill in all the required (*) fields with the appropriate information, such as in the example below.



Add User

Basic Advanced

Full Name Dana Scully

Username* dscully

Domain* cptme.us

Email* dscully@cptme.us

User Groups Enter a few characters of Group Name

Phone Number United States of America
Phone Number

Location Enter office location

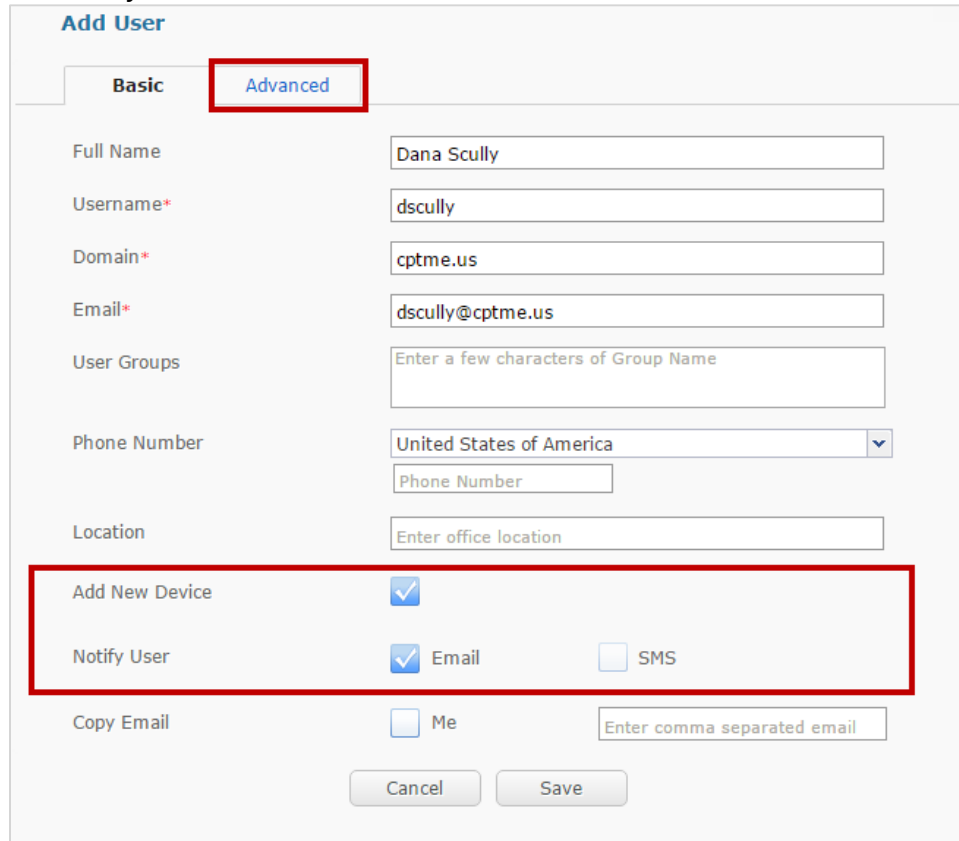
Add New Device ☐

Cancel Save

Note: You can either add a new device right now by following the instructions in the next section, or you can click the “Save” button now, and add a new device later using the instructions in Section 2.7.

2.4.1 Adding a Device While Adding the User

- 2.4.1.1. To add a new device to this new user, select “Add New Device” checkbox, and select the “Notify User” method.



Add User

Basic **Advanced**

Full Name: Dana Scully

Username*: dscully

Domain*: cptme.us

Email*: dscully@cptme.us

User Groups: Enter a few characters of Group Name

Phone Number: United States of America (dropdown), Phone Number (input)

Location: Enter office location

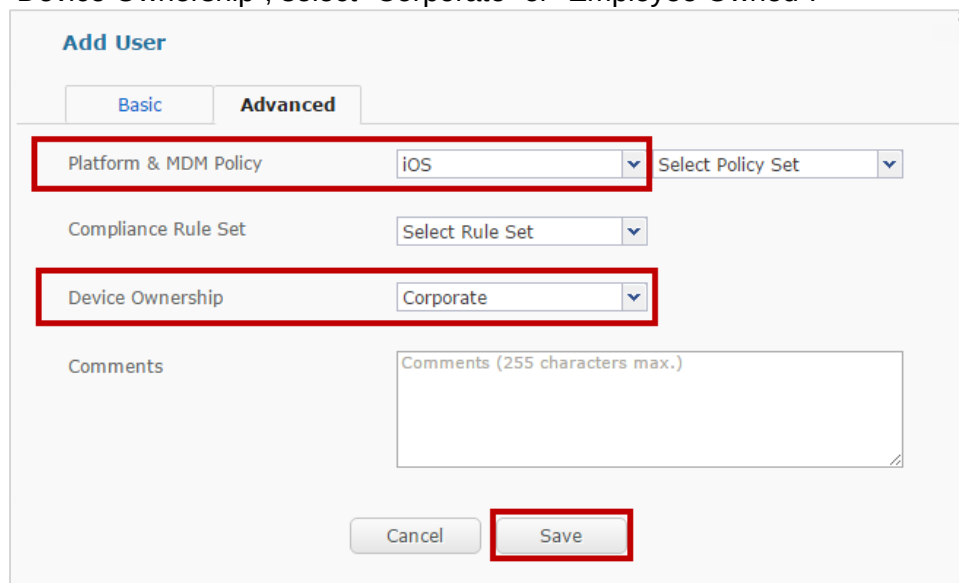
Add New Device: ☒

Notify User: ☒ Email ☐ SMS

Copy Email: ☐ Me

Cancel Save

- 2.4.1.2. On the “Add User” pop-up window, click the “Advanced” tab.
- 2.4.1.3. On the “Advanced” tab, under “Platform”, select “iOS” or “Android”, and under the “Device Ownership”, select “Corporate” or “Employee Owned”.



Add User

Basic **Advanced**

Platform & MDM Policy: iOS (dropdown), Select Policy Set (dropdown)

Compliance Rule Set: Select Rule Set (dropdown)

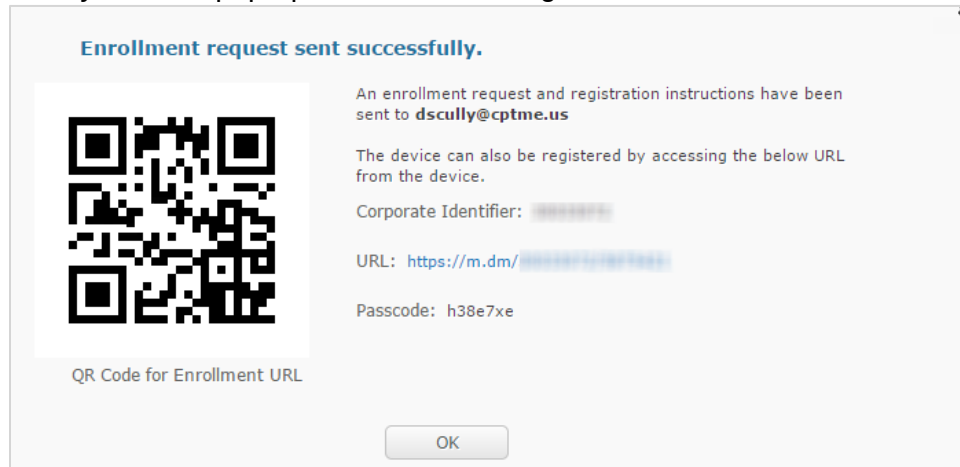
Device Ownership: Corporate (dropdown)

Comments: Comments (255 characters max.)

Cancel **Save**

- 2.4.1.4. Click the “Save” button.

2.4.1.5. The system will pop-up a success message with the enrollment details sent to the user.



2.4.1.6. Click the “OK” button.

2.5 Creating a User Groups

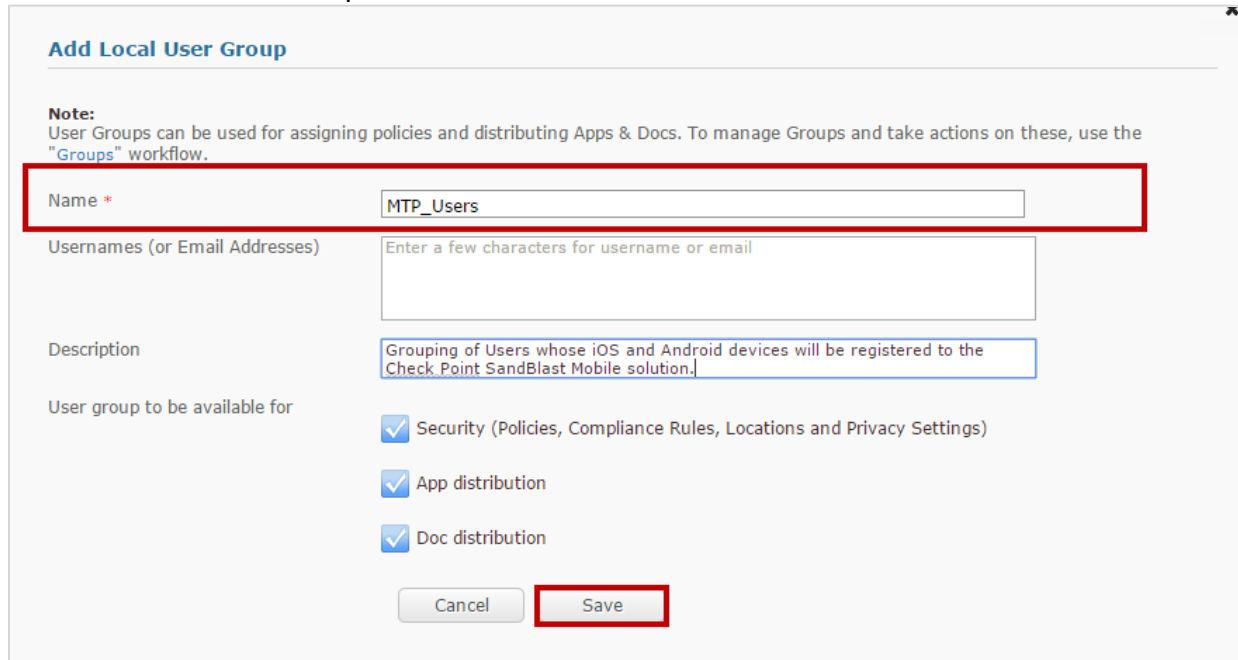
To create a group of users whose devices will be registered to the SandBlast Mobile solution, follow this procedure. Although this can be an optional step, it is used in the creation of the dynamic Device Provisioning Group in the next section (2.6.1).

2.5.1 Creating a User Group

2.5.1.1. Navigate to **Users > Groups**, click the “Add” drop-down button, and select “Local Group”.



- 2.5.1.2. On the “Add Local Group pop-up window, enter in a Name, such as “MTP_Users”, and, if desired, a Description.



Add Local User Group

Note:
User Groups can be used for assigning policies and distributing Apps & Docs. To manage Groups and take actions on these, use the "Groups" workflow.

Name *

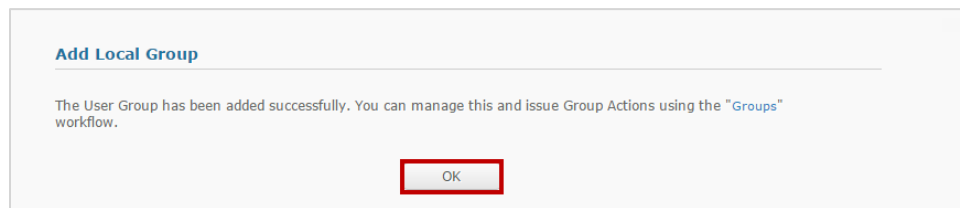
Username (or Email Addresses)

Description

User group to be available for

- ☒ Security (Policies, Compliance Rules, Locations and Privacy Settings)
- ☒ App distribution
- ☒ Doc distribution

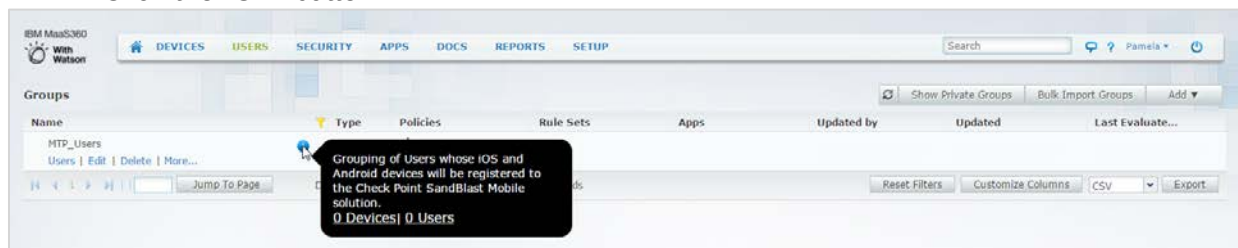
- 2.5.1.3. Click the “Save” button.



Add Local Group

The User Group has been added successfully. You can manage this and issue Group Actions using the "Groups" workflow.

- 2.5.1.4. Click the “OK” button.



IBM MaaS360

DEVICES USERS SECURITY APPS DOCS REPORTS SETUP

Search

Groups

Name	Type	Policies	Rule Sets	Apps	Updated by	Updated	Last Evaluate...
MTP_Users	Users						

Grouping of Users whose iOS and Android devices will be registered to the Check Point SandBlast Mobile solution. 0 Devices| 0 Users

2.5.2 Adding an Existing User to a User Group

To add an existing user to the User Group we created in the previous section (2.5.1), follow this procedure.

- 2.5.2.1. Navigate to **Users > Directory**, scroll to the user you want to add to a user group, and click the “View” link.

IBM MaaS360 With Watson

DEVICES **USERS** SECURITY APPS DOCS REPORTS SETUP

Directory

User Directory

Use the Cloud Extender to... Directory to import group and associated user information. Cloud Extender is available for download on the Services enablement workflow. Imported information can be used for automatic provisioning of users, group based policy assignment and App & Doc distribution. Supported User Directories are Active Directory, OpenLDAP, Novell LDAP, IBM Domino LDAP and Oracle User Directory.

To specify groups to import, use the workflow [Add User Directory Group](#). To add Local Groups, use the workflow [Add Local Group](#).

Username	Full Name	Domain	Email Address	Status	User S...	Last Updated...
dscully	Dana Scully	cptme.us	dscully@cptme.us	Active	Local Director y	11/10/2016 22:14 IST

View Add Device | Reset Password | More...

Jump To Page

Displaying 1 - 1 of 1 Records | Show 25 Records | Reset Filters | Customize Columns | CSV | Export

- 2.5.2.2. Click the “Add Group” button.

IBM MaaS360 With Watson

DEVICES **USERS** SECURITY APPS DOCS REPORTS SETUP

dscully

Add Device **Add Group** Reset Password Deactivate More

User Summary

Full Name	Dana Scully	Email	dscully@cptme.us
Domain	cptme.us	Phone Number	-
Status	Active	Location	-
Authentication Type	Local		

Groups

Group Name	Distinguished Name	Actions
------------	--------------------	---------

Owned Devices

Device Name	Manufa...	Model	Managed Status	Operati...	Last Reported
-------------	-----------	-------	----------------	------------	---------------

Displaying 0 - 0 of 0 Records

- 2.5.2.3. In the “Add Group” pop-up window, start typing the User Group you want to add the user to and select the appropriate group from the list, in our example “MTP_Users”.

Add Group

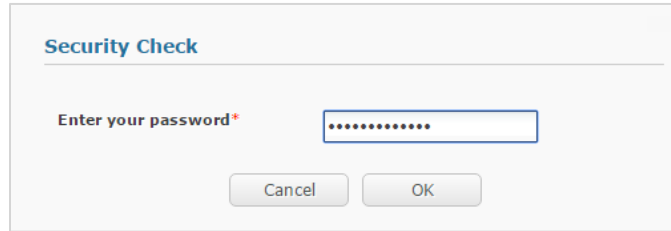
User Groups

MTP_Users,

Cancel Save

- 2.5.2.4. Click the “Save” button.

2.5.2.5. Enter in your admin password, and click the “OK” button.



A dialog box titled "Security Check" with a text input field labeled "Enter your password*" containing masked characters (dots). Below the input field are two buttons: "Cancel" and "OK".

2.5.2.6. The User is now part of the User Group.

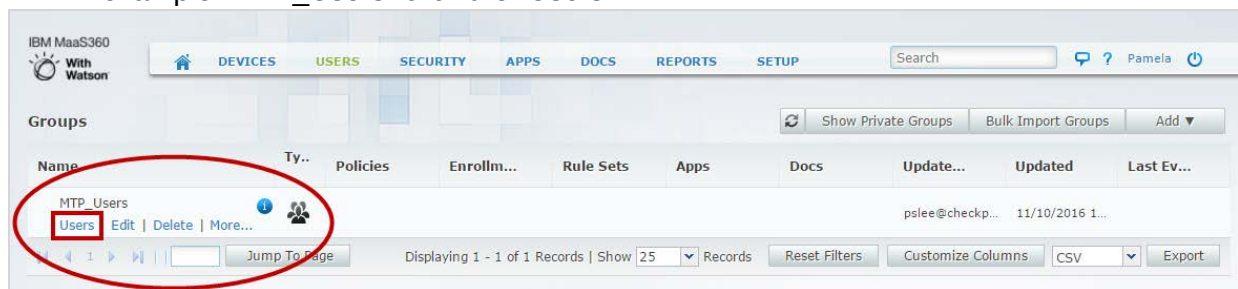


The IBM MaaS360 interface shows the "USERS" tab selected. A red circle highlights the "User Directory" link and the "MTP_Users" group name. Below, a table lists users with columns: Username, Full Name, Domain, Email Address, Status, User S..., and Last Updated... The first user listed is dscully, Dana Scully, cptme.us, dscully@cptme.us, Active, Local Director y, and 05/11/2017 14:14 PDT.

2.5.3 Adding a New User to an Existing User Group

Adding a new user to an existing user group is close to the same procedure in Section 2.4.

2.5.3.1. Navigate to **Users > Groups**, under the User Group you created in Section 2.5.1, in our example “MTP_Users” click the “Users” link.



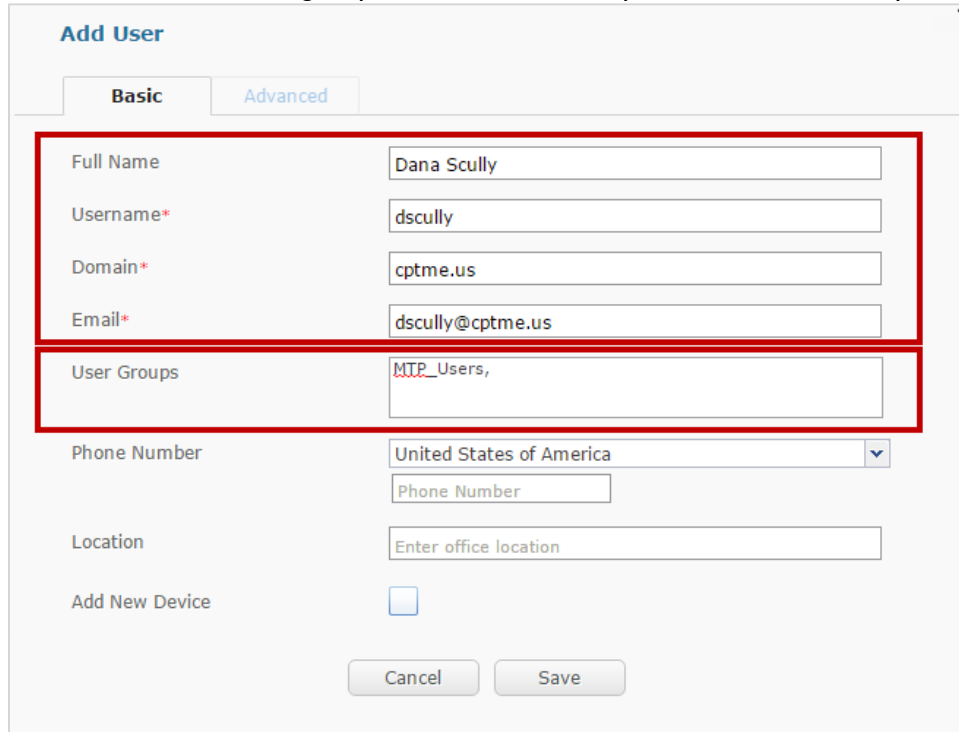
The IBM MaaS360 interface shows the "GROUPS" tab selected. A red circle highlights the "MTP_Users" group name and the "Users" link below it. The table below shows group details with columns: Name, Ty..., Policies, Enrollm..., Rule Sets, Apps, Docs, Update..., Updated, and Last Ev... The first group listed is MTP_Users, with a user count of 1.

2.5.3.2. Click the “Add User” button.



The IBM MaaS360 interface shows the "USERS" tab selected. A red circle highlights the "Add User" button. Below, the table is empty, showing "Displaying 0 - 0 of 0 Records" and "No entries to show".

- 2.5.3.3. On the “Add User” pop-up window “Basic” tab, fill in all the required (*) fields with the appropriate information, such as in the example below.
- 2.5.3.4. Also, enter in the user group in the “Users Groups” field, in our example “MTP_Users”



Add User

Basic Advanced

Full Name Dana Scully

Username* dscully

Domain* cptme.us

Email* dscully@cptme.us

User Groups MTP_Users,

Phone Number United States of America
Phone Number

Location Enter office location

Add New Device ☐

Cancel Save

Note: You can either add a new device right now by following the instructions in the next section, or you can click the “Save” button now and add a new device later using the instructions in Section 2.7.

2.5.3.1 Adding a Device While Adding the User

- 2.5.3.1.1. To add a new device to this new user, select “Add New Device” checkbox, and select the “Notify User” method.

Add User

Basic **Advanced**

Full Name: Dana Scully

Username*: dscully

Domain*: cptme.us

Email*: dscully@cptme.us

User Groups: MTP_Users,

Phone Number: United States of America
Phone Number

Location: Enter office location

Add New Device: ☒

Notify User: ☒ Email ☐ SMS

Copy Email: ☐ Me

Cancel Save

- 2.5.3.1.2. On the “Add User” pop-up window, click the “Advanced” tab.
- 2.5.3.1.3. On the “Advanced” tab, under “Platform”, select “iOS” or “Android”, and under the “Device Ownership”, select “Corporate” or “Employee Owned”.

Add User

Basic **Advanced**

Platform & MDM Policy: iOS Select Policy Set

Compliance Rule Set: Select Rule Set

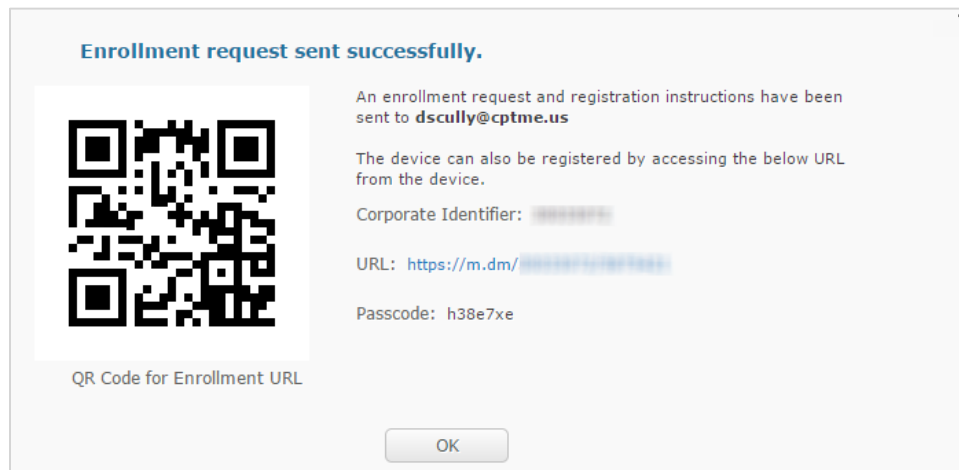
Device Ownership: Corporate

Comments: Comments (255 characters max.)

Cancel **Save**

- 2.5.3.1.4. Click the “Save” button.

- 2.5.3.1.5. The system will pop-up a success message with the enrollment details sent to the user.



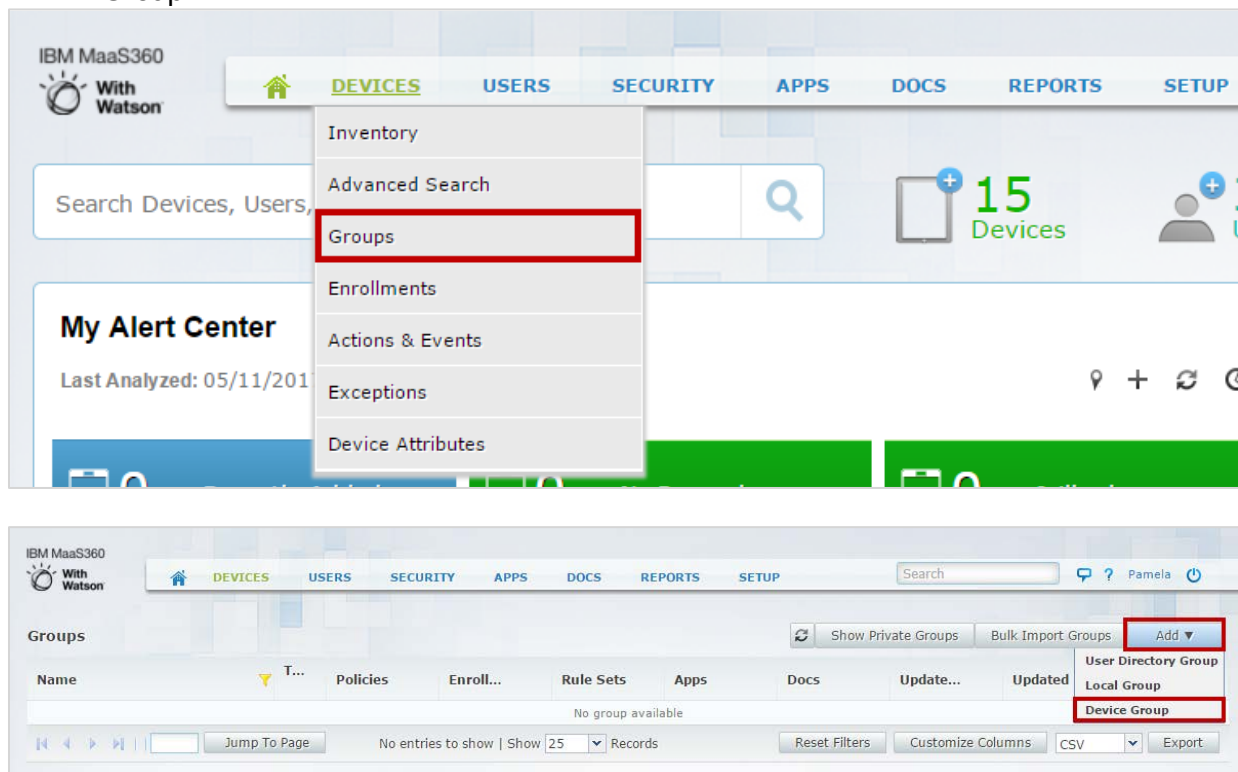
- 2.5.3.1.6. Click the “OK” button.

2.6 Creating a Device Provisioning Group

A device provisioning group is used to tie devices, apps, and app configurations together for deployment. MaaS360 calls a device provisioning group a “device group”. This group will be used in the SandBlast Mobile Protect app deployment process discussed in Section 4.

2.6.1 Creating a Simple Device Provisioning Group

- 2.6.1.1. Navigate to **Devices > Groups**, click the “Add” drop-down button, and select “Device Group”.



- 2.6.1.2. On the “Advanced Search” screen, you will need to build a query that will group all devices matching the criteria into the device group. In our example, we will group all the

devices assigned to all “Users” in the “Managed User Groups” “Equal To” the User Group we created in the previous section, in our example “MTP_Users”.

IBM MaaS360
With Watson

DEVICES USERS SECURITY APPS DOCS REPORTS SETUP

Advanced Search

1. Search for ☒ Active Devices ☐ Inactive Devices ☐ All Devices

2. With Device Type(s) ☒ Smartphones ☒ Tablets

3. Last Reported

4. Search Criteria

Condition 1

Condition 2

Condition 3

Reset Search

2.6.1.3. Click the “Search” button.

2.6.1.4. Click the “Create New Device Group” button.

IBM MaaS360
With Watson

DEVICES USERS SECURITY APPS DOCS REPORTS SETUP

Search Results Show Criteria

Create New Device Group

Device Name	Username	Email Add...	Model	Operating ...	Last Repor...	OS Name	Platform N...
No device available							

Jump To Page No entries to show | Show 25 Records Customize Columns CSV Export

2.6.1.5. On the “Device Group Details” pop-up window, enter a Group Name, such as “MTP_Devices”, and if desired, a Description.

Device Group Details

New group will be saved for the current Advanced Search. Filters in the table below would not be considered

Group Name* (Max. 54 chars)

Description: (Max. 250 chars)

☒ Public ☐ Private

Cancel Save

2.6.1.6. Click the “Save” button.

IBM MaaS360
With Watson

DEVICES USERS SECURITY APPS DOCS REPORTS SETUP

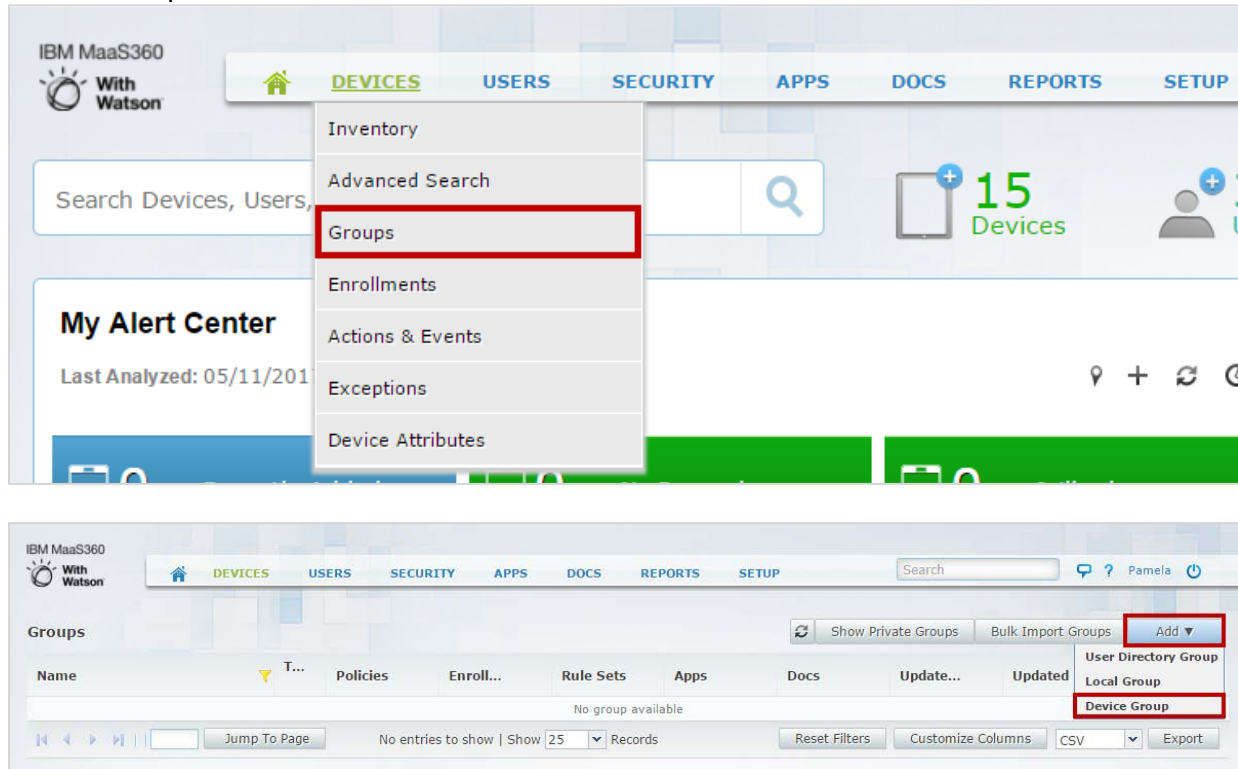
Groups Show Private Groups Bulk Import Groups Add

Name	Ty...	Policies	Enrollm...	Rule Sets	Apps	Docs	Updated...	Updated	Last Eva...
MTP_Devices	Devices							11/15/2016 12...	05/10/2017 18...

Jump To Page Displaying 1 - 1 of 1 Records | Show 25 Records Reset Filters Customize Columns CSV Export

2.6.2 Creating a Specific Device Provisioning Group

- 2.6.2.1. Navigate to **Devices > Groups**, click the “Add” drop-down button, and select “Device Group”.



- 2.6.2.2. On the “Advanced Search” screen, you will need to build a query that will group all devices matching the criteria into the device group.
- 2.6.2.2.1. In our example, we will group all the devices assigned to all “Users” in the “Managed User Groups” “Equal To” the User Group we created in the previous section, in our example “MTP_Users”, then
- 2.6.2.2.2. we will add additional conditions for “Operating System” “OS Name” “Contains” “iOS” and
- 2.6.2.2.3. “Operating System” “OS Name” “Contains” “Android”. Then,
- 2.6.2.2.4. change the “Search Criteria” to “Across Conditions (Advanced)” with the formula of “1 AND (2 OR 3)”
- 2.6.2.3. These criteria will match all iOS or Android devices belonging to the users that belong to the user group “MTP_Users”.

IBM MaaS360
With Watson

DEVICES USERS SECURITY APPS DOCS REPORTS SETUP

Advanced Search

1. Search for ☐ Active Devices ☐ Inactive Devices ☐ All Devices

2. With Device Type(s) ☒ Smartphones ☒ Tablets

3. Last Reported

4. Search Criteria

Condition 1

Condition 2

Condition 3

Reset Search

- 2.6.2.4. Click the “Search” button.
- 2.6.2.5. Click the “Create New Device Group” button.

IBM MaaS360
With Watson

DEVICES USERS SECURITY APPS DOCS REPORTS SETUP

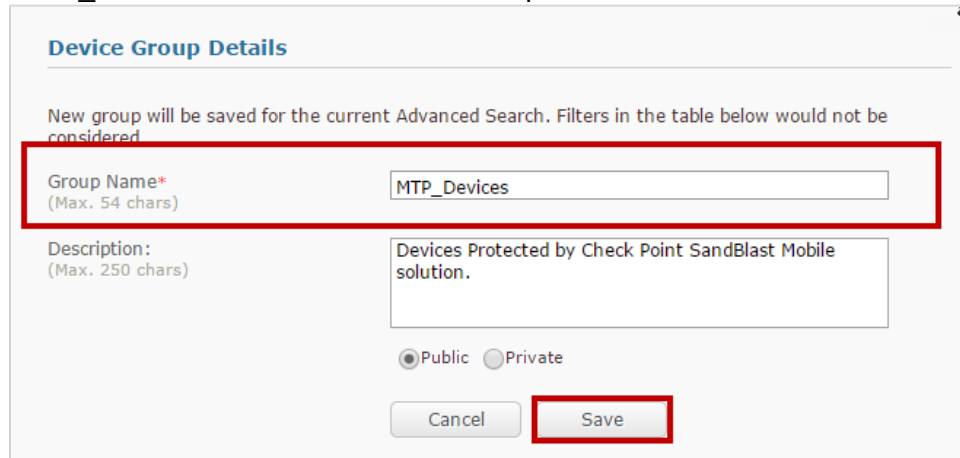
Search Results [Show Criteria](#)

[Create New Device Group](#)

Device Name	Username	Email Address	Model	Operating System	Last Reported	OS Name	Platform Name
No device available							

Jump To Page No entries to show | Show Records [Customize Columns](#) [Export](#)

- 2.6.2.6. On the “Device Group Details” pop-up window, enter a Group Name, such as “MTP_Devices”, and if desired, a Description.



Device Group Details

New group will be saved for the current Advanced Search. Filters in the table below would not be considered

Group Name*
(Max. 54 chars)

Description:
(Max. 250 chars)

☒ Public ☐ Private

- 2.6.2.7. Click the “Save” button.



IBM MaaS360 With Watson

DEVICES USERS SECURITY APPS DOCS REPORTS SETUP

Search Pamela

Groups

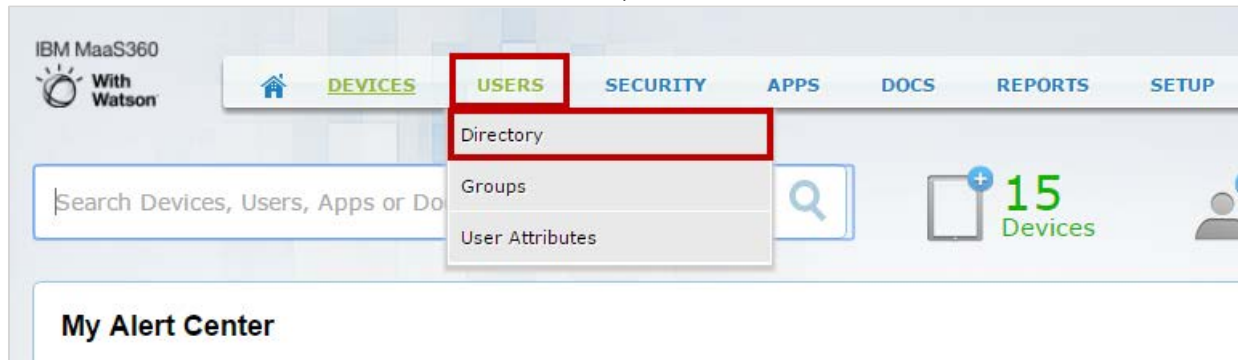
Show Private Groups Bulk Import Groups Add

Name	Ty...	Policies	Enrollm...	Rule Sets	Apps	Docs	Updated...	Updated	Last Eva...
MTP_Devices	Devices						11/15/2016 12...	05/10/2017 18...	

Jump To Page Displaying 1 - 1 of 1 Records | Show 25 Records | Reset Filters Customize Columns CSV Export

2.7 Adding a Device to an Existing User

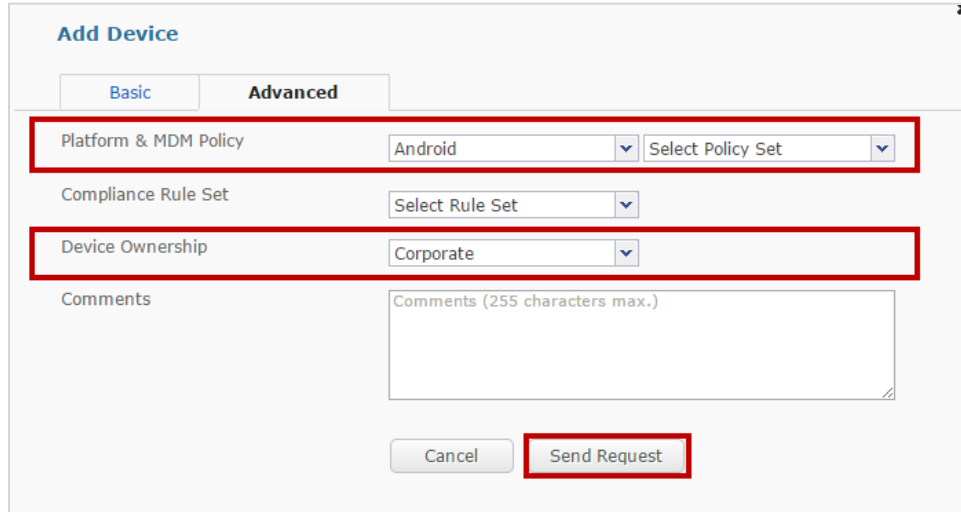
- 2.7.0.1. You can add a device to an existing user by navigating to **Users > Directory**, scroll to or search for the user to add a device to, and click the “Add Device” link.



- 2.7.0.2. On the “Add Device” pop-up window “Basic” tab, select the “Notify User” method.

- 2.7.0.3. Click the “Advanced” tab.

- 2.7.0.4. On the “Add Device” pop-up window “Advanced” tab, under “Platform” select “iOS” or “Android”, and under “Device Ownership” select “Corporate” or “Employee Owned”.



Add Device

Basic Advanced

Platform & MDM Policy Android Select Policy Set

Compliance Rule Set Select Rule Set

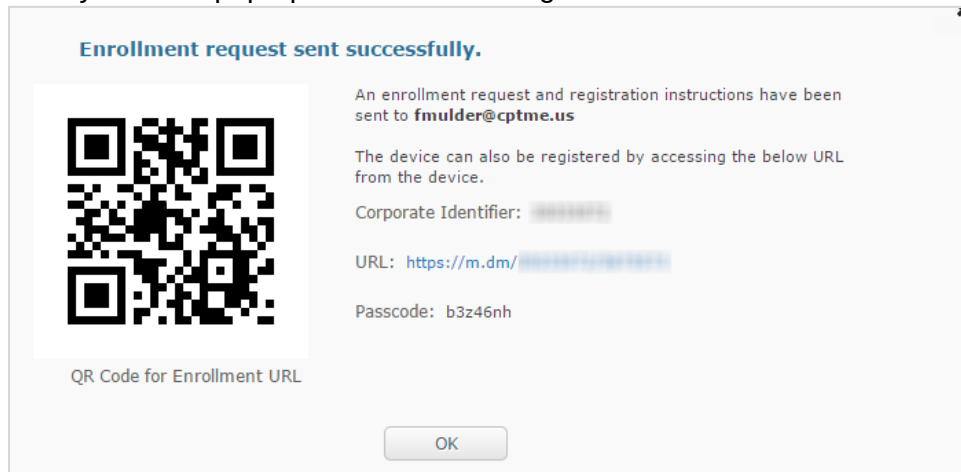
Device Ownership Corporate

Comments (255 characters max.)

Cancel Send Request

- 2.7.0.5. Click the “Send Request” button.

- 2.7.0.6. The system will pop-up a success message with the enrollment details sent to the user.



Enrollment request sent successfully.

An enrollment request and registration instructions have been sent to **fmulder@cptme.us**

The device can also be registered by accessing the below URL from the device.

Corporate Identifier: [redacted]

URL: [https://m.dm/\[redacted\]](https://m.dm/[redacted])

Passcode: b3z46nh

QR Code for Enrollment URL

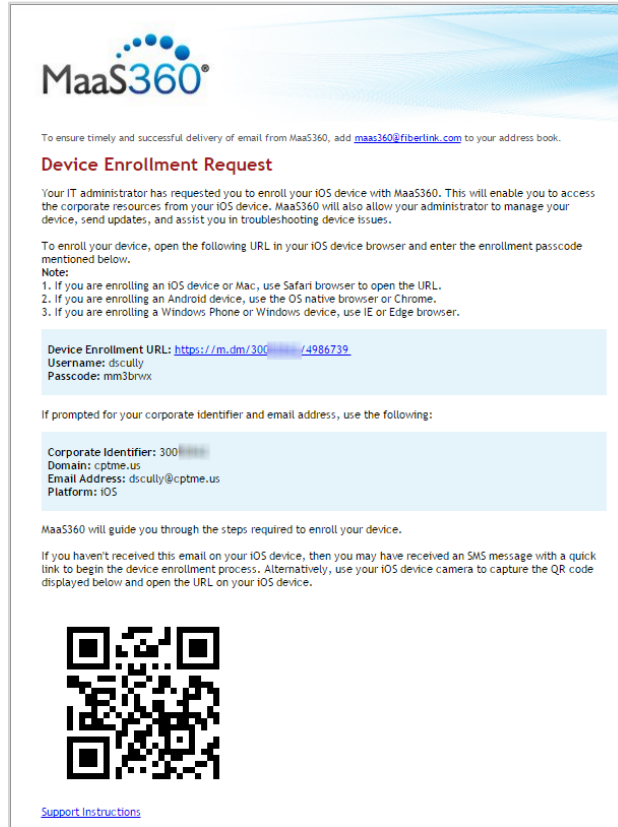
OK

- 2.7.0.7. Click the “OK” button.

Note: Repeat these steps to add another device.

2.7.1 Enrolling an iOS Device to MaaS360

2.7.1.1. The user will receive an enrollment email from the MaaS360 system.



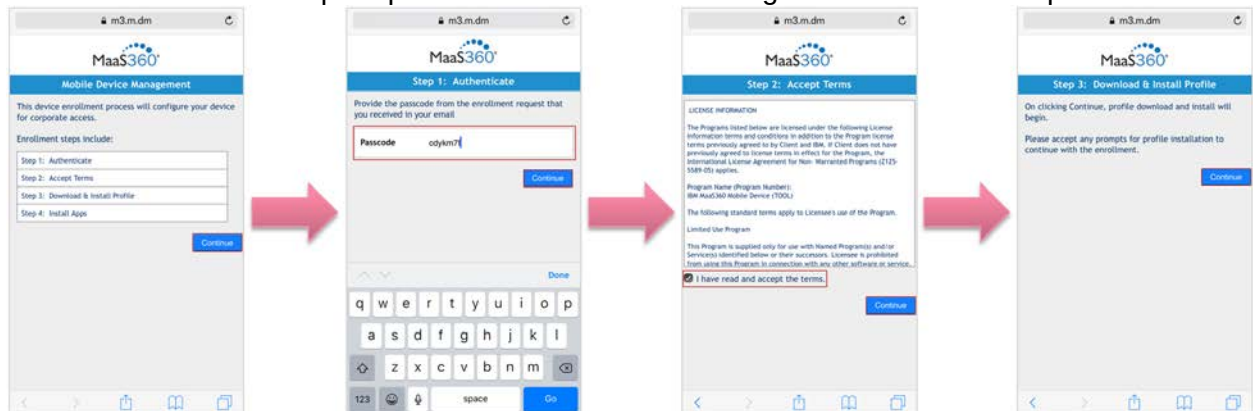
2.7.1.2. The user will open the “Device Enrollment URL” link in their device's browser.

2.7.1.3. The user will be prompted to continue with the install by tapping the “Continue” button.

2.7.1.4. The user will be prompted to enter the passcode they received in the Device Enrollment Request email, and tapping the “Continue” button.

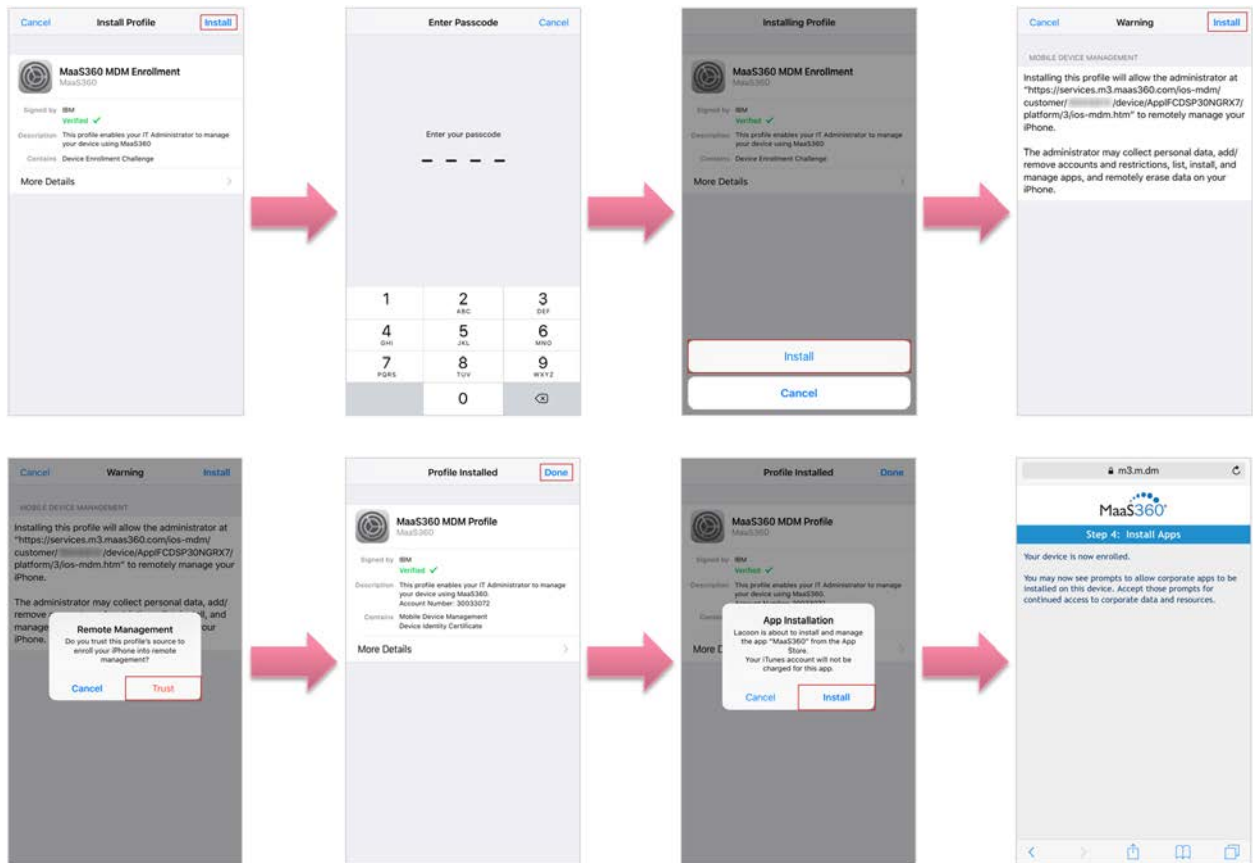
2.7.1.5. The user will be prompted to accept the “Terms of Use” by selecting the “I have read and accept the terms” checkbox, and tapping the “Continue” button.

2.7.1.6. The user is then prompted to continue with installing the MaaS360 MDM profile.



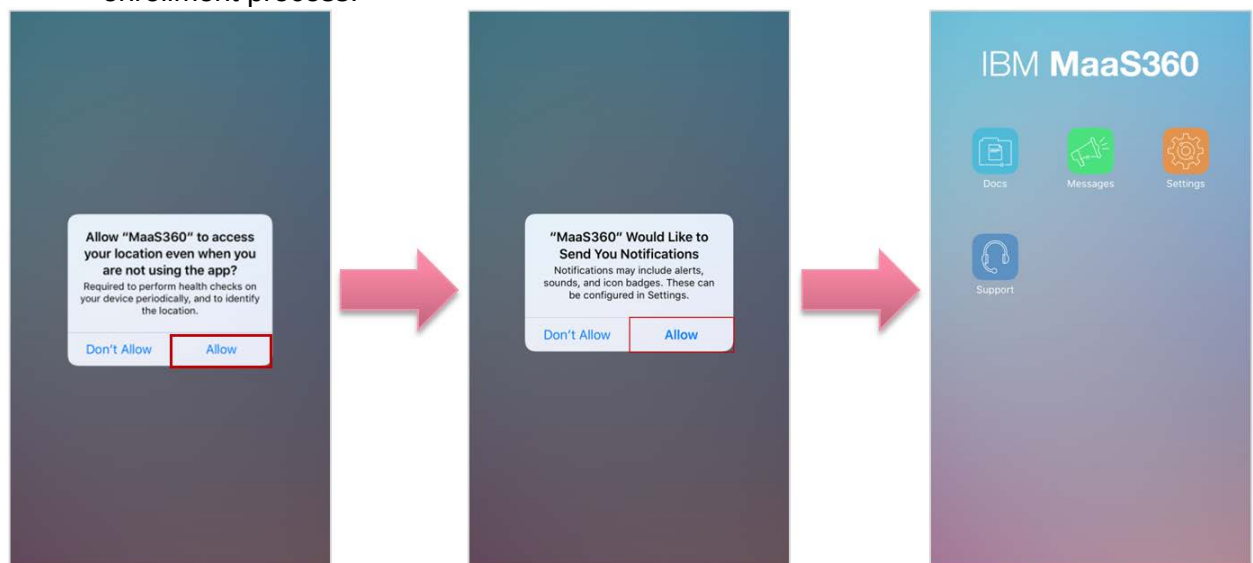
2.7.1.7. The user must tap “Install” through this procedure.

Note: If there is already a device management profile installed, the user must uninstall the existing profile and then continue with the MaaS360 MDM profile installation.



2.7.1.8. Once the profile is installed, the user will be prompted to install the MaaS360 app.

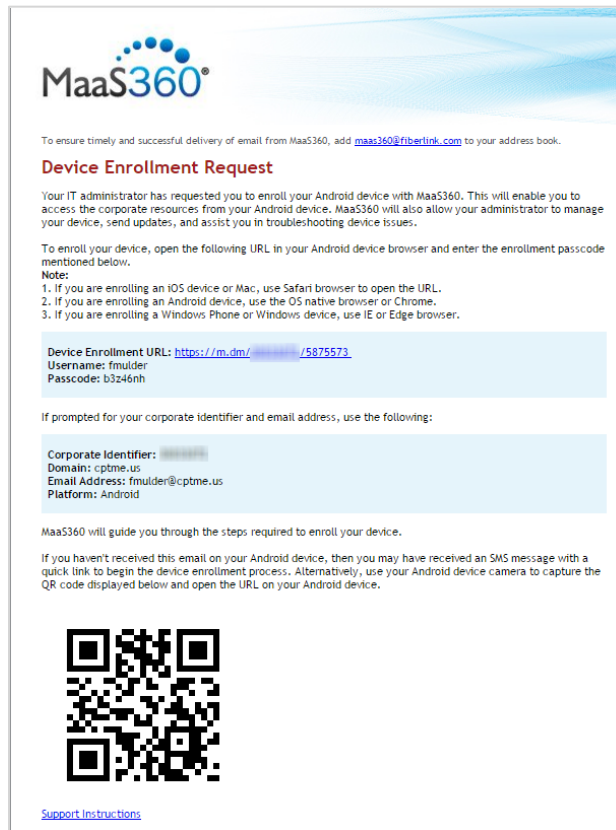
2.7.1.9. After the MaaS360 app is installed, the user must launch the app to continue the enrollment process.



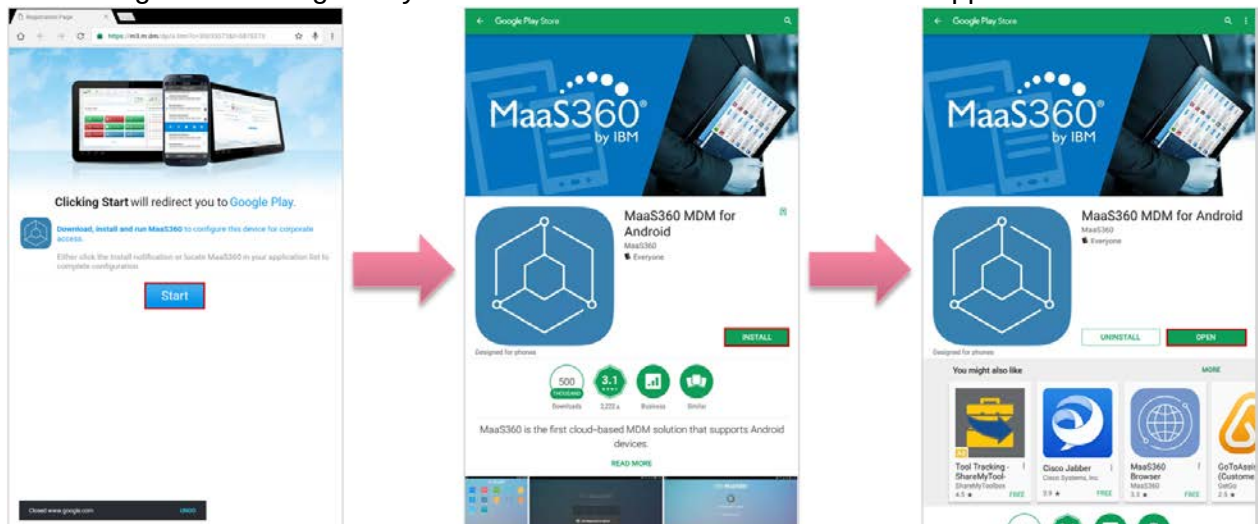
2.7.1.10. The device has been successfully enrolled to the MaaS360 system.

2.7.2 Enrolling an Android Device to MaaS360

2.7.2.1. The user will receive an enrollment email from the MaaS360 system.

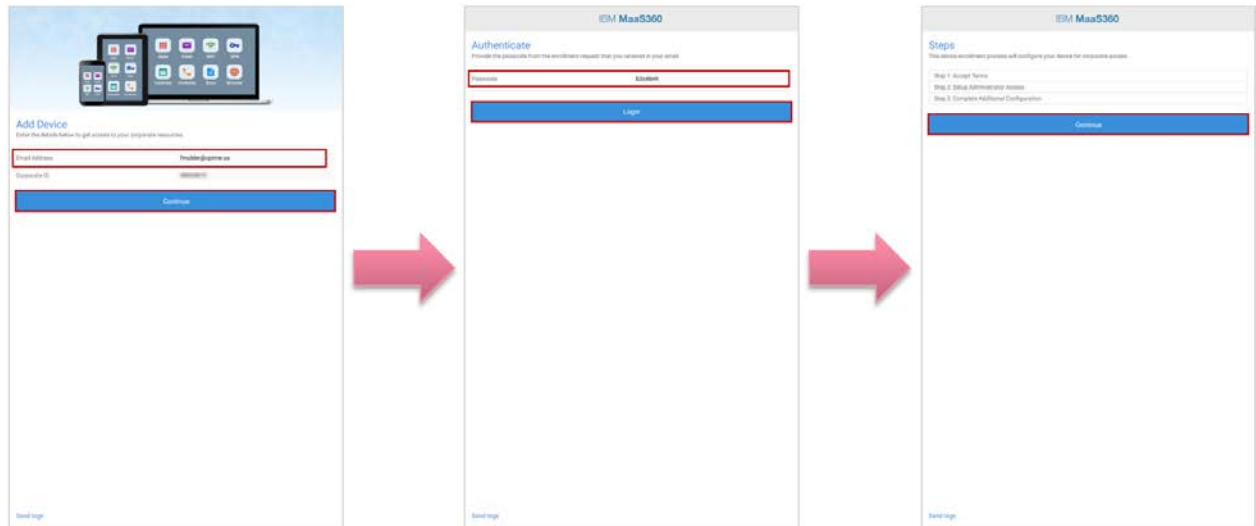


2.7.2.2. The user will open the MaaS360 link in their device's browser. This will prompt the user to go to the Google Play Store to download/install the MaaS360 app.

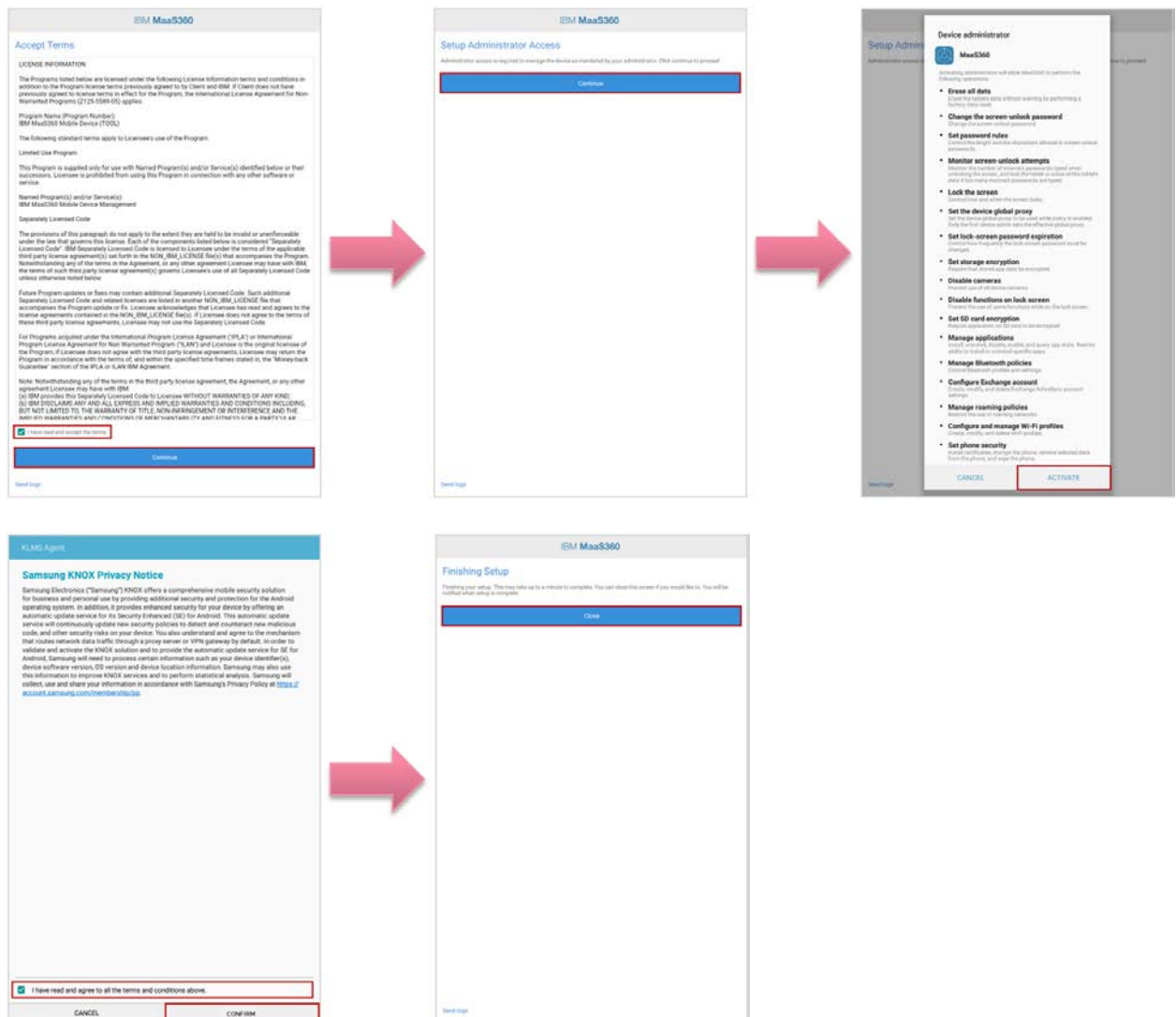


2.7.2.3. Once the MaaS360 app is installed, the user must launch the app to continue the enrollment process.

2.7.2.4. The user is prompted for the Corporate Identifier as provided in the email and their email address.



2.7.2.5. The user must accept the Terms of Use, and Activate the MaaS360 app to be a device administrator.



- 2.7.2.6. After the setup is finished, the device has been successfully enrolled to the MaaS360 system.



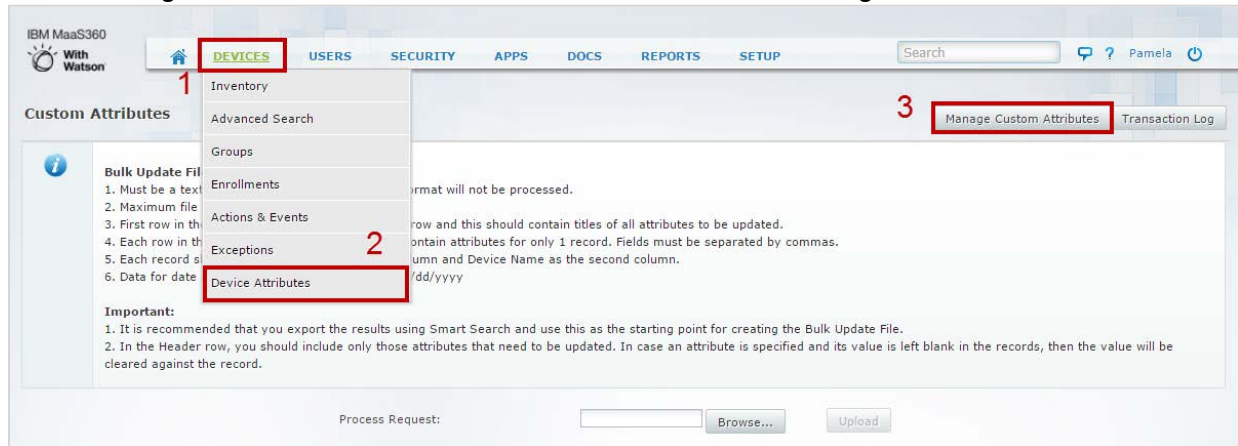
2.8 Creating a Mitigation Process

In this procedure, you will create a mitigation label that the SandBlast Mobile Dashboard will use to label any device in High Risk as determined by the SandBlast Mobile Analysis. This label will allow the MaaS360 system to identify which devices are at High Risk and to enforce configured compliance and mitigation policies against those devices.

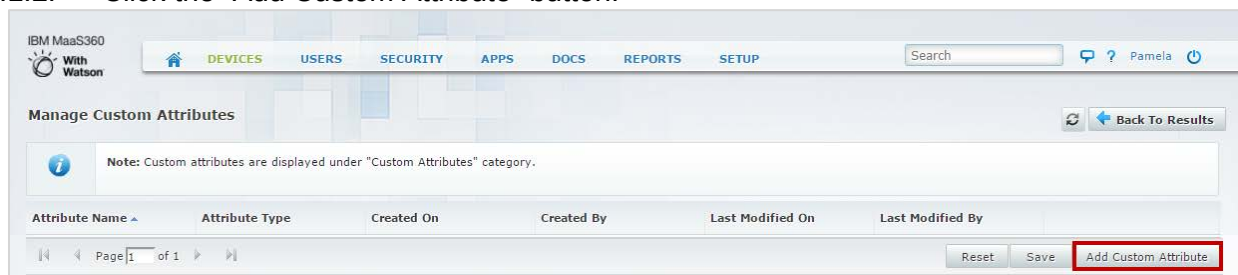
2.8.1 Creating a Mitigation Label

In MaaS360 the mitigation label is called a custom device attribute. This section describes how to create the custom device attribute, and the next section (2.8.2) will use this custom attribute to create a device mitigation group on which compliance and mitigation policies can be applied.

2.8.1.1. Navigate to **Devices > Device Attributes**, click the “Manage Custom Attributes” button.



2.8.1.2. Click the “Add Custom Attribute” button.



2.8.1.3. On the “Add Custom Attribute” pop-up window, enter the “Attribute Name”, such as “MTP_HighRisk_Attribute”, with an “Attribute Type” of “Boolean”.

The screenshot shows the 'Add Custom Attribute' pop-up window. It has a title 'Add Custom Attribute' in blue. Below the title, there are two input fields: 'Attribute Name' with the value 'MTP_HighRisk_Attribute' and 'Attribute Type' with a dropdown menu showing 'Boolean'. At the bottom, there are two buttons: 'Add' and 'Cancel'. The 'Add' button is highlighted with a red box.

2.8.1.4. Click the “Add” button.

2.8.2 Creating a Device Mitigation Group

Now that we have a mitigation label (“MTP_HighRisk_Attribute”), we will create a Device Mitigation Group (device group) based on this custom attribute.

For this example, we will call this device mitigation group, “Devices_At_High_Risk”. This group will contain all the devices in which the custom attribute, for our example “MTP_HighRisk_Attribute”, is set to “Yes”.

- 2.8.2.1. Navigating to **Devices > Groups**, click the “Add” drop-down button, and select “Device Group”.
- 2.8.2.2. On the Advanced Search screen, configure the following settings:
 - 2.8.2.2.1. Search for = “Active Devices”
 - 2.8.2.2.2. With Device Type(s) = “Smartphones” and “Tablets”
 - 2.8.2.2.3. Last Reported = “Last 7 Days”
 - 2.8.2.2.4. Search Criteria = “All Conditions (AND)”
 - 2.8.2.2.5. Condition 1 = “Custom Attributes”, “MTP_HighRisk_Attribute”, “Equal To”, “Yes”

IBM MaaS360 With Watson

DEVICES USERS SECURITY APPS DOCS REPORTS SETUP

Search Pamela

Advanced Search

1. Search for ☒ Active Devices ☐ Inactive Devices ☐ All Devices

2. With Device Type(s) ☒ Smartphones ☒ Tablets

3. Last Reported Last 7 Days

4. Search Criteria All Conditions (AND)

Condition 1 Custom Attributes MTP_HighRisk_Attribute Equal To Yes

Condition 2 Select Category Select Attribute Select Criteria Enter Text

Condition 3 Select Category Select Attribute Select Criteria Enter Text

Reset Search

- 2.8.2.3. Click the “Search” button.

- 2.8.2.4. Click the “Create New Device Group” button.

IBM MaaS360 With Watson

DEVICES USERS SECURITY APPS DOCS REPORTS SETUP

Search Pamela

Search Results Show Criteria

Create New Device Group

Device Name	Username	Email Add...	Model	Operating ...	Last Repor...	OS Name	Platform N..
No device available							

Jump To Page No entries to show | Show 25 Records Customize Columns CSV Export

- 2.8.2.5. On the “Devices Group Details” pop-up window, enter the Group Name, such as in our example “Devices_At_High_Risk”, and a Description, if desired.

Device Group Details

Group Name*
(Max. 54 chars)

Description
(Max. 250 chars)

- 2.8.2.6. Click the “Save” button.



2.8.3 Creating Compliance Policies

Now that we have a Device Mitigation Group, we can create Compliance Policies that will be enforced on devices that are at High Risk using the Mitigation Label. In this section, we will create Security Policies and Compliance Rules that will be used to enforce these actions.

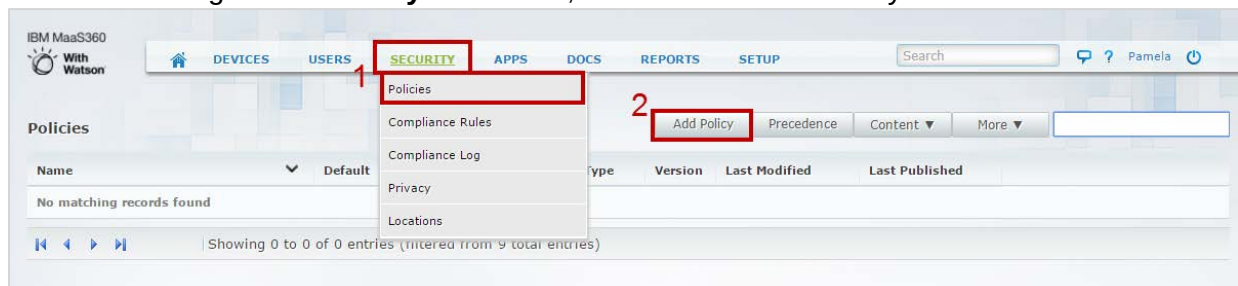
Note: We will show a couple of different compliance policies, but these enforcement policies are something that the customer should create for their environment and needs. In a production environment, the customer should configure the compliance policies according to their internal security policy.

2.8.3.1 Security Policy (Examples)

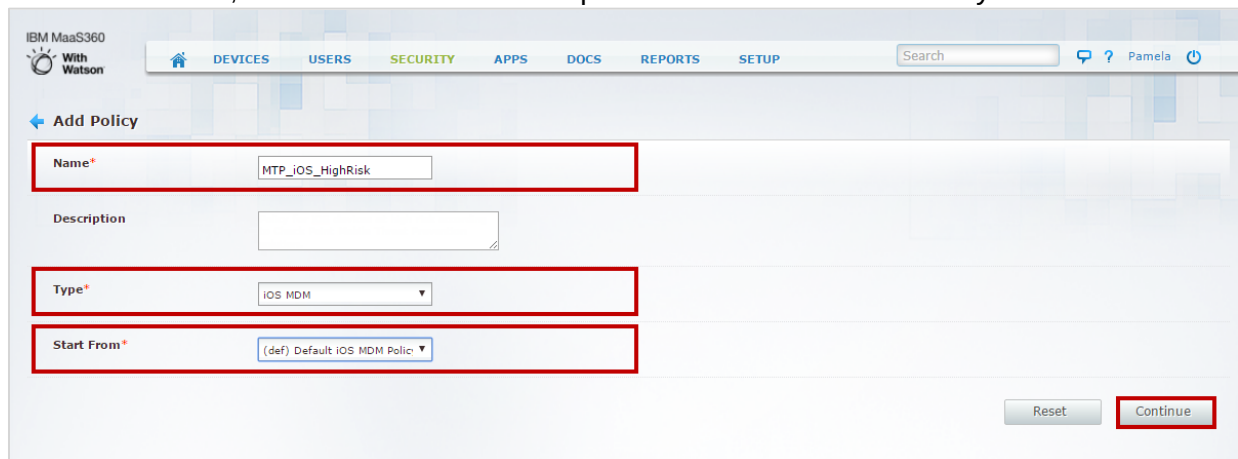
2.8.3.1.1 Creating Compliance Actions for iOS Devices (Policy)

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

- 2.8.3.1.1.1. Navigate to **Security > Policies**, and click the “Add Policy” button.



- 2.8.3.1.1.2. Enter a Name for the policy, such as “MTP_iOS_HighRisk”, select a “Type” of “iOS MDM”, and select “Start From” equal to “Default iOS MDM Policy”.



IBM MaaS360
With Watson

DEVICES USERS SECURITY APPS DOCS REPORTS SETUP

Search ? Pamela

← Add Policy

Name* MTP_iOS_HighRisk

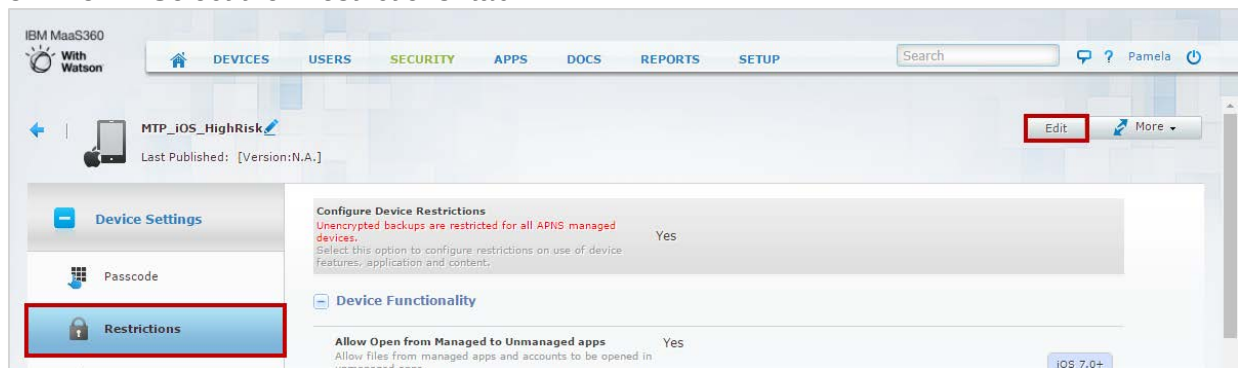
Description

Type* iOS MDM

Start From* (def) Default iOS MDM Policy

Reset Continue

- 2.8.3.1.1.3. Click the “Continue” button.
- 2.8.3.1.1.4. There are several sections for policy sets, such as “Passcode, Restrictions, Application Compliance, etc. We will make our modifications in the Restrictions section.
- 2.8.3.1.1.5. Select the “Restrictions” tab.



IBM MaaS360
With Watson

DEVICES USERS SECURITY APPS DOCS REPORTS SETUP

Search ? Pamela

← MTP_iOS_HighRisk

Last Published: [Version:N.A.] Edit More

Device Settings

Passcode

Restrictions

Configure Device Restrictions

Unencrypted backups are restricted for all APNS managed devices. Select this option to configure restrictions on use of device features, application and content. Yes

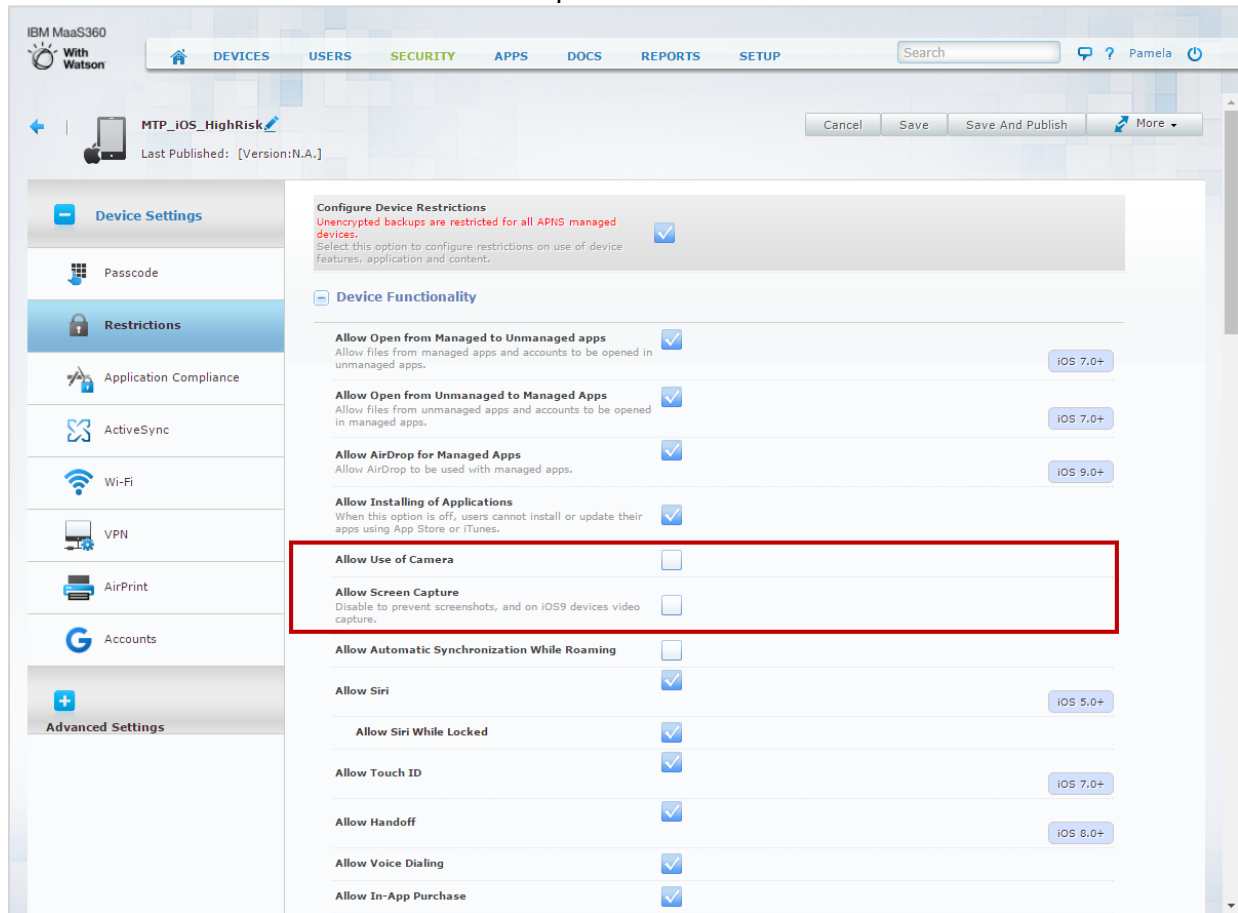
Device Functionality

Allow Open from Managed to Unmanaged apps Allow files from managed apps and accounts to be opened in unmanaged apps. Yes

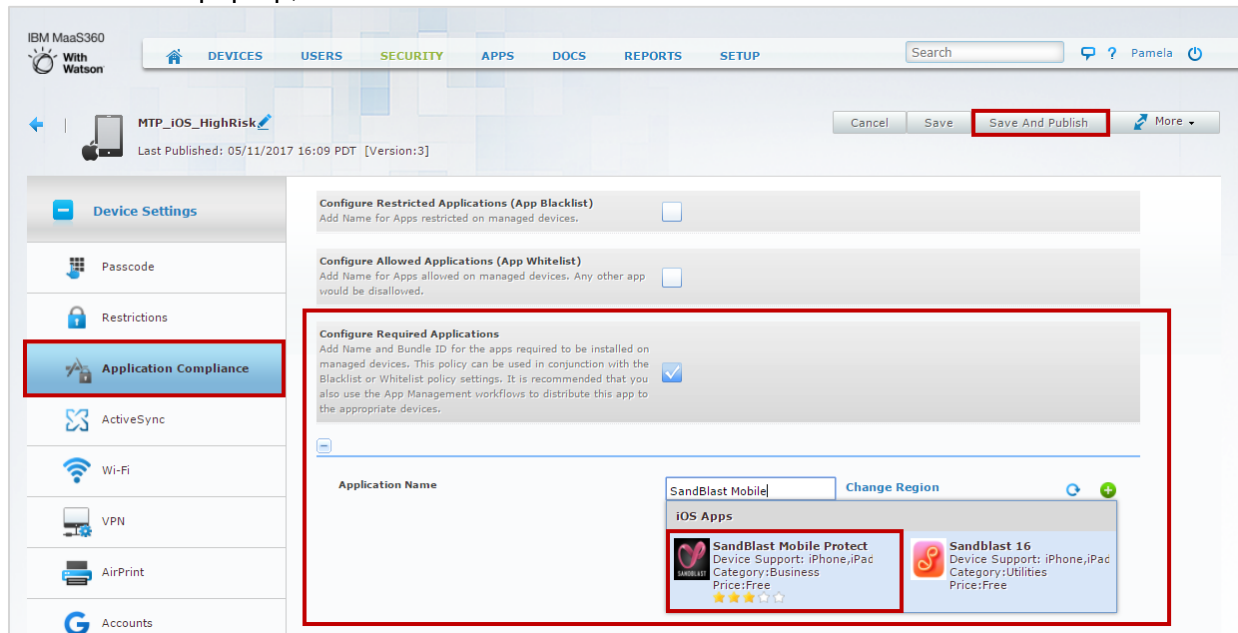
iOS 7.0+

2.8.3.1.1.6. Click the “Edit” button.

2.8.3.1.1.7. Under the **Restrictions > Device Functionality** section, unselect “Allow Use of Camera” and “Allow Screen Capture”.



- 2.8.3.1.1.8. Select the “Application Compliance” tab.
- 2.8.3.1.1.9. Under the **Application Compliance** section, select “Configure Required Applications”.
- 2.8.3.1.1.10. In the “Application Name” field, start typing “SandBlast Mobile Protect” and the app will pop-up, select SandBlast Mobile Protect.



- 2.8.3.1.1.11. Click the “Save and Publish” button.

2.8.3.1.2 Creating Compliance Actions for Android Devices (Policy)

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

- 2.8.3.1.2.1. Navigate to **Security > Policies**, and click the “Add Policy” button.



- 2.8.3.1.2.2. Enter a Name for the policy, such as “MTP_Android_HighRisk”, select a “Type” of “Android MDM”, and select “Start From” equal to “Default Android MDM Policy”.

IBM MaaS360
With Watson

DEVICES USERS SECURITY APPS DOCS REPORTS SETUP

Search ? Pamela

← Add Policy

Name* MTP_Android_HighRisk

Description

Type* Android MDM

Start From* (def) Default Android MDM P

Reset Continue

- 2.8.3.1.2.3. Click the “Continue” button.

- 2.8.3.1.2.4. There are several sections for policy sets, such as “Passcode, Security, Restrictions, Application Compliance, etc. We will make our modifications in the Security, Application Compliance, and Restrictions sections.

- 2.8.3.1.2.5. Select the “Security” tab.

IBM MaaS360
With Watson

DEVICES USERS SECURITY APPS DOCS REPORTS SETUP

Search ? Pamela

← MTP_Android_HighRisk Last Published: [Version:N.A.] Edit More

Device Settings

- Passcode
- Security
- Restrictions
- Application Compliance
- Native App Compliance
- ActiveSync

Device Security

App Security

Data Security

Allow Clipboard Yes SAFE 2.0+

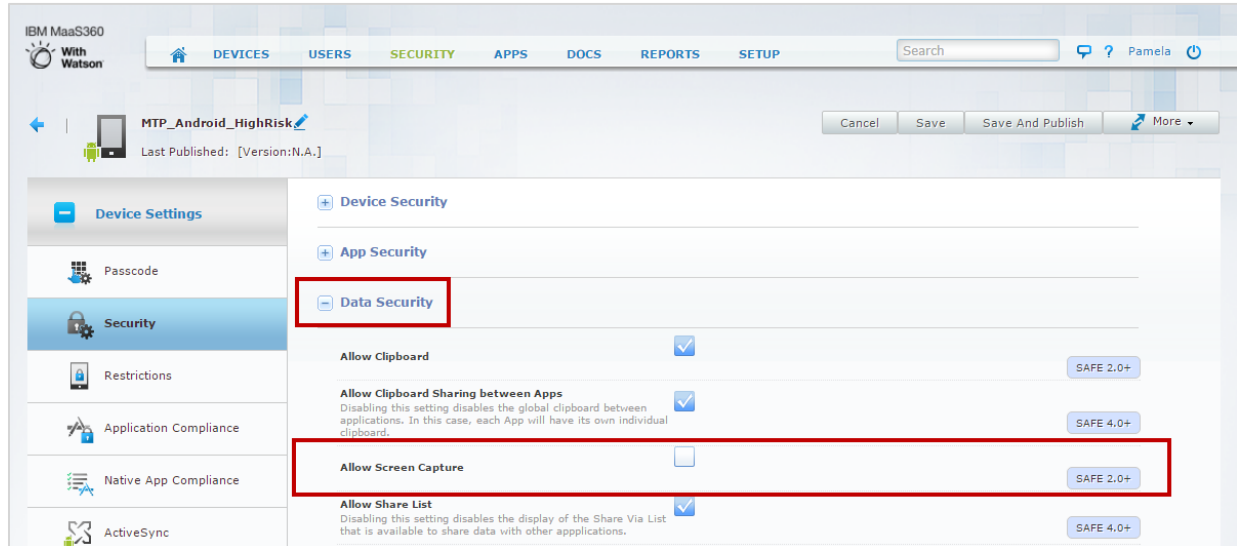
Allow Clipboard Sharing between Apps Yes SAFE 4.0+
Disabling this setting disables the global clipboard between applications. In this case, each App will have its own individual clipboard.

Allow Screen Capture Yes SAFE 2.0+

Allow Share List Yes SAFE 4.0+
Disabling this setting disables the display of the Share Via List that is available to share data with other applications.

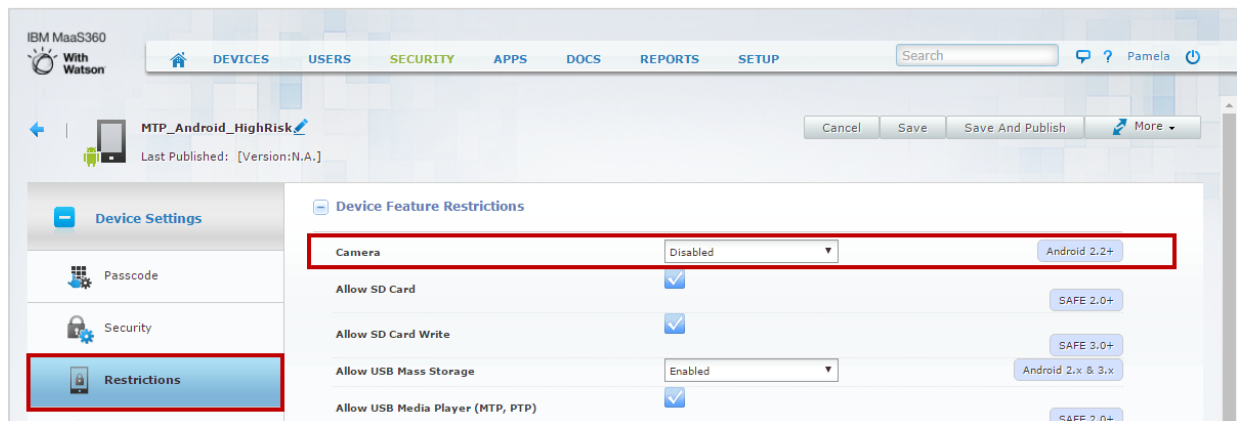
- 2.8.3.1.2.6. Click the “Edit” button.

2.8.3.1.2.7. Under the **Security > Data Security** section, unselect “Allow Screen Capture”.



2.8.3.1.2.8. Select the “Restrictions” tab.

2.8.3.1.2.9. Under the **Restrictions > Device Feature Restrictions** section, change Camera to “Disabled”.



- 2.8.3.1.2.10. Select the “Application Compliance” tab.
- 2.8.3.1.2.11. Under the **Application Compliance** section, select “Configure Required Applications”.
- 2.8.3.1.2.11.1. In the “Application Name” field, enter “SandBlast Mobile Protect”
- 2.8.3.1.2.11.2. In the “Application ID” field, enter “com.lacoon.security.fox”

IBM MaaS360 With Watson

DEVICES USERS **SECURITY** APPS DOCS REPORTS SETUP

Search Pamela

Cancel Save **Save And Publish** More

MTP_Android_HighRisk
Last Published: 11/16/2016 15:27 PST [Version:2]

Device Settings

- Passcode
- Security
- Restrictions
- Application Compliance**
- Native App Compliance
- ActiveSync
- Wi-Fi
- VPN
- Web Shortcuts
- Device Management

Configure Restricted Applications (App Blacklist)
Add Name and App IDs for Apps that need to be restricted on managed devices. Depending on the action specified, the user will either be prompted to uninstall the App or be restricted from using the App. System apps specified as Restricted Applications will always be blocked from use irrespective of the action specified.

Configure Restricted Applications by App Permissions
Specify App Permissions that you do not want to be allowed on managed devices. Apps that use these permissions will be blocked or uninstalled depending on the action specified. You can also specify apps that will be allowed even if they use the specified permission. Requires MDM App version 4.40 or higher.

Configure Allowed Applications (App Whitelist)
Add Name and App IDs for Apps allowed on managed devices. Any other user installed app will be automatically restricted. Depending on the action specified, the user will either be prompted to uninstall the App or be restricted from using the App.

Configure Required Applications
Add Name and App IDs for Apps required to be always installed on managed devices. This policy can be used in conjunction with Blacklist or Whitelist policy. Supports multiple apps as a comma separated list in which case at least one of the apps is mandatory. First app in the list is considered the primary app and user will be prompted to install this when no apps are found. Supported on MDM App version 4.20 and above.

Application Name: SandBlast Mobile Protect

Application ID: com.lacoon.security.fox

- 2.8.3.1.2.12. Click the “Save And Publish” button.

2.8.3.2 Creating Security Compliance Rule (Enforcement)

This compliance rule will be used to enforce the policies created in the previous section.

- 2.8.3.2.1. Navigate to **Security > Compliance Rules**, and click the “Add Rule Set” button.

IBM MaaS360 With Watson

DEVICES USERS **SECURITY** APPS DOCS REPORTS SETUP

Search Pamela

Compliance Rules

1 Policies
2 **Compliance Rules**
3 Compliance Log
4 Privacy
5 Locations

Add Rule Set Precedence Disable All Show All

1. Create as many Rule Sets as needed to set up your compliance policy.
2. Start testing any new Rule Set by applying it to a group of devices.
3. You can explicitly apply a Rule Set to a device or a group of devices.
4. You can mark any of the Rule Set as a Default Rule Set.
5. For viewing the specific Rule Set enabled for a device, look for the attribute "Rule Set" under Security & Compliance Section in Device View.
6. Use the "Disable All" button to remove Rule Set assignments and active enforcement actions from all managed devices.

Rule Set Name	Default	Status	Precedence	Last Updated By	Last Updated On
No matching records found					

Showing 0 to 0 of 0 entries (filtered from 8 total entries)

- 2.8.3.2.2. Enter in a Rule Set Name, such as “MTP_HighRisk_Rules”, and if desired to copy from an existing rule, such as “OS Version”

IBM MaaS360
With Watson

DEVICES USERS SECURITY APPS DOCS REPORTS SETUP Search ? Pamela

← Add Rule Set

Rule Set Name*
Maximum of 30 characters are allowed. MTP_HighRisk_Rule

Copy From OS Version

Continue Reset

- 2.8.3.2.3. Click the “Continue” button.

- 2.8.3.2.4. Because SandBlast Mobile supports iOS and Android only, under **Basic Settings > Select Applicable Platforms** section, we will unselect all OS'es other than “iOS” and “Android”.

IBM MaaS360
With Watson

DEVICES USERS SECURITY APPS DOCS REPORTS SETUP Search ? Pamela

← MTP_HighRisk_Rules Edit Rule Set name Save

Basic Settings

Enforcement Rules

Geo-Fencing Rules

Monitoring Rules

Group Based Rules

Select Applicable Platforms

Enable Real-time Compliance for OS'es
Select the Operating Systems for which you want rules to be evaluated on. Devices of OS types not selected, will be exempted from rules evaluation.

☒ iOS ☒ Android
☐ BlackBerry ☐ Windows Phone
☐ Symbian ☐ Windows Mobile
☐ Others

Event Notification Recipients

Enter email addresses for event notification

pslee@cptme.us

Exemption

To exempt specific devices from Rule evaluation, set the custom attribute 'Important Devices' in Device View for appropriate devices to 'Yes'. Administrators will be notified when important devices are out of compliance, but automated action will not be taken. Custom Attributes are found on the 'Hardware Inventory' tab for enrolled devices, and the "Exchange ActiveSync" or "IBM Traveler" tab for devices discovered via mail integration.

- 2.8.3.2.5. Select “Group Based Rules” tab, and click the “Add a New Rule” button.

- 2.8.3.2.6. Enter in a Name, such as “MTP_HighRisk”, select the Device Mitigation Group we created in Section 2.8.2 to put all our SandBlast Mobile Devices into, in our example “Devices_At_High_Risk”.
- 2.8.3.2.6.1. Under Enforcement Action section, the first action “When detected in the group” is already set to “Alert”. Change “Alert” to “Change Policy” action. This will create additional fields for setting the policies to enforce on iOS, Android, and Windows Phone.
- 2.8.3.2.6.1.1. Set iOS policy to the compliance policy we created in Section 2.8.3.1.1, in our example “MTP_iOS_HighRisk”.
- 2.8.3.2.6.1.2. Set Android policy to the compliance policy we created in Section 2.8.3.1.2, in our example “MTP_Android_HighRisk”

IBM MaaS360

With Watson

DEVICES USERS SECURITY APPS DOCS REPORTS SETUP

Search [] ? Pamela []

MTP_HighRisk_Rules

Edit Rule Set name Save

- Basic Settings
- Enforcement Rules
- Geo-Fencing Rules
- Monitoring Rules
- Group Based Rules**

Enable Advanced Group based Rules to enforce security compliance for mobile devices.

- Select and Add Groups to identify Out of Compliance Devices.
- Select the action to be taken on devices that go out of compliance. While using Selective Wipe on OOC devices, apps required as per the policy configurations will not be removed. Available actions can vary based on level of e-mail server integration.
- You can opt to specify multiple levels of warnings and actions.
- Group based Rules identify Compliance Status of Devices based on the Group Evaluation of respective devices. At times this may take up to a day.

Configure Group Based Rules

> Device Is at High Risk

Enforcement Action

When detected in the group - Change Policy +

iOS - MTP_IOS_HighRisk

Android - MTP_Android_HighR

Windows Phone - Select Policy

Notify User: ☒ Email ☒ Device Notification

Notify Admins: ☒ Standard Email List

Message

Enter a custom message for this rule. Maximum of 1024 characters are allowed and <^~\$*![]{}> cannot be used. [Customize for each action](#)

Your device has been flagged as at High Risk. Please see the SandBlast Mobile Protect app and/or your email for further instructions.

- 2.8.3.2.7. Click the “Save” button.
- 2.8.3.2.8. Type your admin password, and then click the “Continue” button.

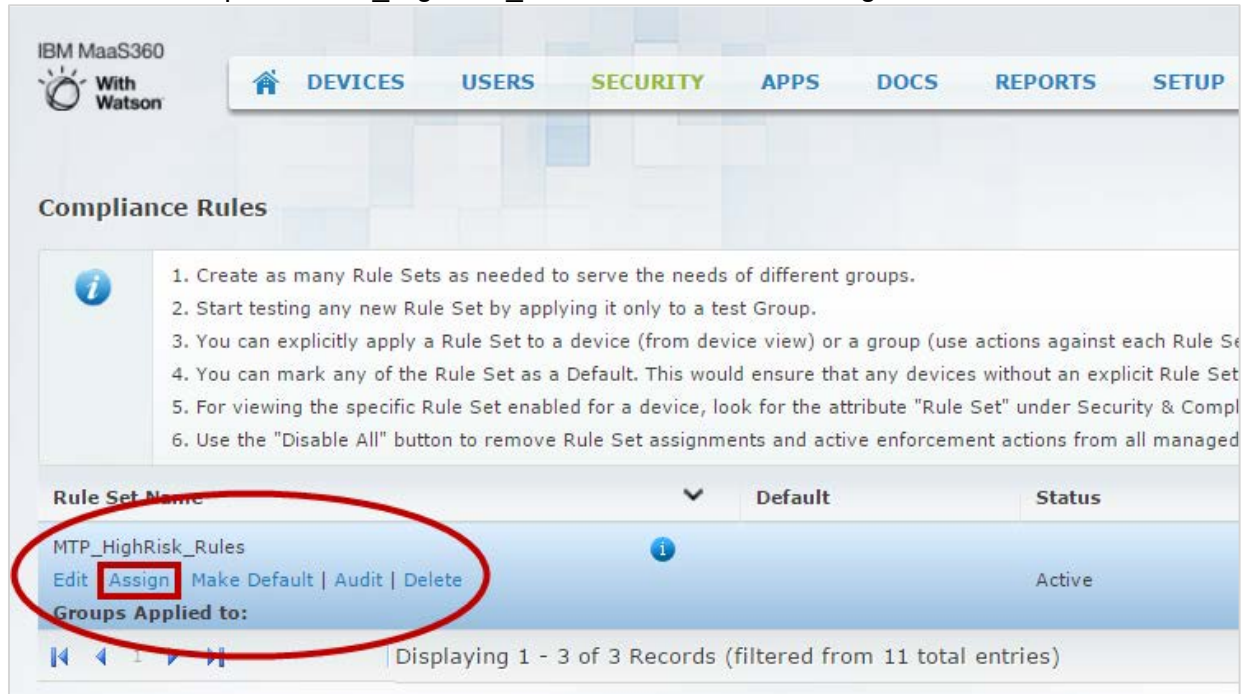
Update Rule Set

Enter your password*

2.8.4 Applying the Compliance Policy to the Device Provisioning Group

Now that we have created the compliance rule ("MTP_HighRisk_Rules") we want to enforce, we need to link those rules to our Device Provisioning Group ("MTP_Devices") we created in Section 2.6.

- 2.8.4.1. Navigate to **Security > Compliance Rules**, find the rule you created in Section 2.8.3.2, our example is "MTP_HighRisk_Rules", and click the "Assign" link.



IBM MaaS360
With Watson

DEVICES USERS **SECURITY** APPS DOCS REPORTS SETUP

Compliance Rules

i

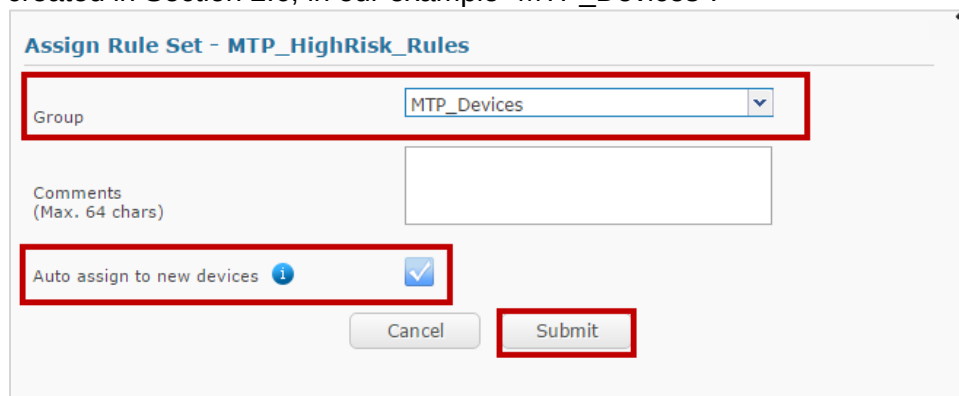
1. Create as many Rule Sets as needed to serve the needs of different groups.
2. Start testing any new Rule Set by applying it only to a test Group.
3. You can explicitly apply a Rule Set to a device (from device view) or a group (use actions against each Rule Set).
4. You can mark any of the Rule Set as a Default. This would ensure that any devices without an explicit Rule Set.
5. For viewing the specific Rule Set enabled for a device, look for the attribute "Rule Set" under Security & Compliance.
6. Use the "Disable All" button to remove Rule Set assignments and active enforcement actions from all managed devices.

Rule Set Name	Default	Status
MTP_HighRisk_Rules		Active

Groups Applied to:

Displaying 1 - 3 of 3 Records (filtered from 11 total entries)

- 2.8.4.2. On the Assign Rule Set pop-up window, select the Device Provisioning Group we created in Section 2.6, in our example "MTP_Devices".



Assign Rule Set - MTP_HighRisk_Rules

Group: MTP_Devices

Comments (Max. 64 chars):

Auto assign to new devices ☒

Cancel Submit

2.8.4.3. Click the “Submit” button.

2.8.4.4. Type your admin password, and then click the “Continue” button.

Assign Rule Set – MTP_HighRisk_Rules to “MTP_Devices”

Note: Review the details below and enter your password to continue. Changes should take affect within the next 30 minutes.

Rule	Action Configured	# of affected Device
Device Is at High Risk	Immediately after OOC: Change Poli...	1

Enter your password*

.....

Cancel Continue

IBM MaaS360
With Watson

DEVICES USERS **SECURITY** APPS DOCS REPORTS SETUP

Compliance Rules

i

1. Create as many Rule Sets as needed to serve the needs of different groups.
2. Start testing any new Rule Set by applying it only to a test Group.
3. You can explicitly apply a Rule Set to a device (from device view) or a group (use actions against each Rule Set).
4. You can mark any of the Rule Set as a Default. This would ensure that any devices without an explicit Rule Set.
5. For viewing the specific Rule Set enabled for a device, look for the attribute “Rule Set” under Security & Compliance.
6. Use the “Disable All” button to remove Rule Set assignments and active enforcement actions from all managed devices.

Rule Set Name	Default	Status
MTP_HighRisk_Rules		Active

Edit | Assign | Make Default | Audit | Delete

Groups Applied to: MTP_Devices

Displaying 1 - 3 of 3 Records (filtered from 11 total entries)

Note: Now any device in the Device Provisioning Group (“MTP_Devices”) that has their custom attribute (“MTP_HighRisk_Attribute”) set to “Yes” by the SandBlast Mobile system will be placed in the Device Mitigation Group (“Devices_At_High_Risk”), which in turn will have the compliance actions in the Compliance Rule (“MTP_HighRisk_Rules”) acted upon it.

- For iOS, this policy is named “MTP_iOS_HighRisk”, and
- For Android, this policy is named “MTP_Android_HighRisk”.

Note: At this point, we have all the information we will need to configure the MDM integration settings in the SandBlast Mobile Dashboard. We are going to do that and then return to the MaaS360 Portal to configure the SandBlast Mobile Protect app deployment settings.

From Our Examples:

- Server = <https://services.m3.maas360.com>
- API Admin Username/Password = mtp_api_admin/<hidden>
- Device Provisioning Group(s) = MTP_Devices
- Mitigation Label = MTP_HighRisk_Attribute

3 Configuring the SandBlast Mobile Dashboard MDM Integration Settings

3.1 Prerequisites

3.1.1. You will need the following details from your MaaS360 Deployment:

Note: There is a table in Section 7.3 that you can record your settings for easy reference.

- 3.1.1.1. **Server:** The root URL to your MaaS360 Web Services API including the leading https://, such as https://services.m3.maas360.com
- 3.1.1.2. **MaaS360 API Administrator Username and Password:** These are the Admin credentials that the SandBlast Mobile Dashboard will use to connect to the MDM. You may have created a special API Admin account in Section 2.3 for this purpose.
- 3.1.1.3. **Billing ID:** This is the Corporate Identifier and can be located on **Setup > Deployment Settings**.
- 3.1.1.4. **API App ID:** com.[Billing ID or Corporate Name].api (This information needs to be obtained from IBM MaaS360 Support)
- 3.1.1.5. **Access Key:** This key needs to be obtained from IBM MaaS360 Support.
- 3.1.1.6. **Organization Groups(s):** This is the MaaS360 device provisioning group to which the 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 label name separated with a semicolon (;). This is the Device Provisioning Group we created in Section 2.6 ("MTP_Devices").

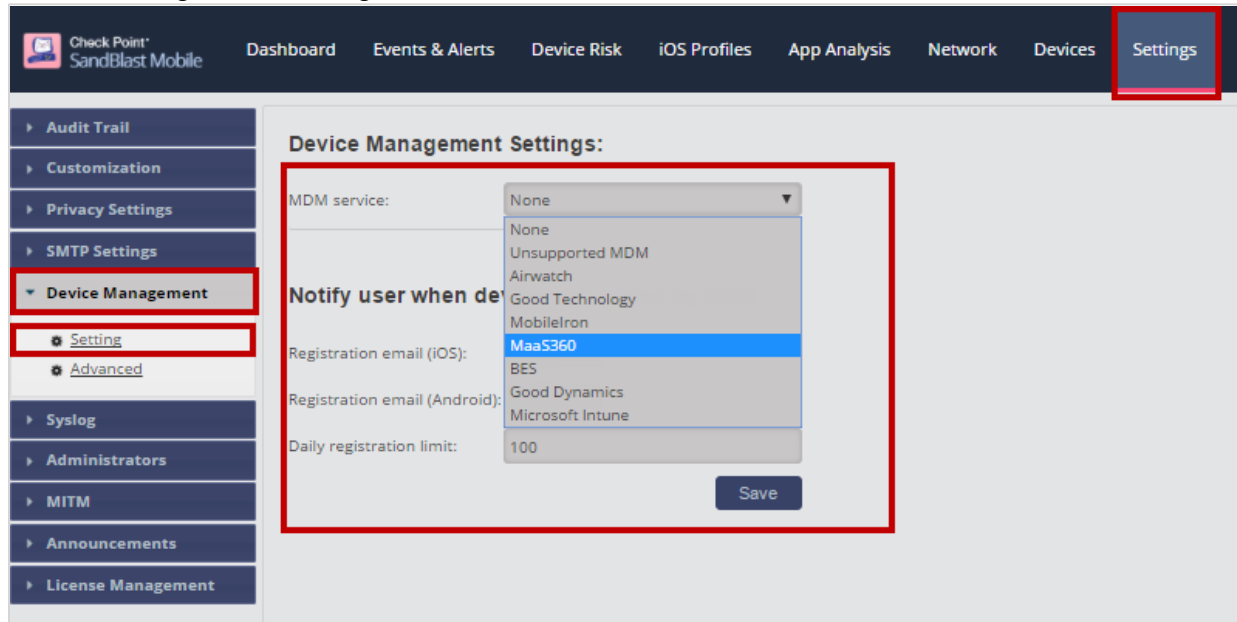
Note: Multiple SandBlast Mobile Dashboards can be integrated to one MaaS360 instance by separating the devices into different "Device Provisioning Groups", such as creating a device provisioning group for All EU Devices (i.e. "MTP_EU_Devices") and a device provisioning group for All US Devices (i.e. "MTP_US_Devices"). Then, the SandBlast Mobile Dashboard in the EU would be integrated to "MTP_EU_Devices" and the SandBlast Mobile Dashboard in the US would be integrated to "MTP_US_Devices".

- 3.1.1.7. **Mitigation Attribute:** This is the custom attribute that will be set to "Yes" when the device is in High Risk. This is the custom attribute that you created in Section 2.8.1 ("MTP_HighRisk_Attribute").
- 3.1.2. For on-premise MDM environments, port 443 (HTTPS) must be remotely accessible through your firewall from the SandBlast Mobile Dashboard to the MDM system before trying to connect.
 - 3.1.2.1. See Section 7.1 for the SandBlast Mobile Dashboard IP addresses for your region.
 - 3.1.2.2. If you do not know your SandBlast Mobile Dashboard's region, follow the instructions in Section 7.2 to find out.
- 3.1.3. Delete any existing devices in the SandBlast Mobile Dashboard.

Note: Only the devices are synchronized from the MDM to the SandBlast Mobile Dashboard, not users.

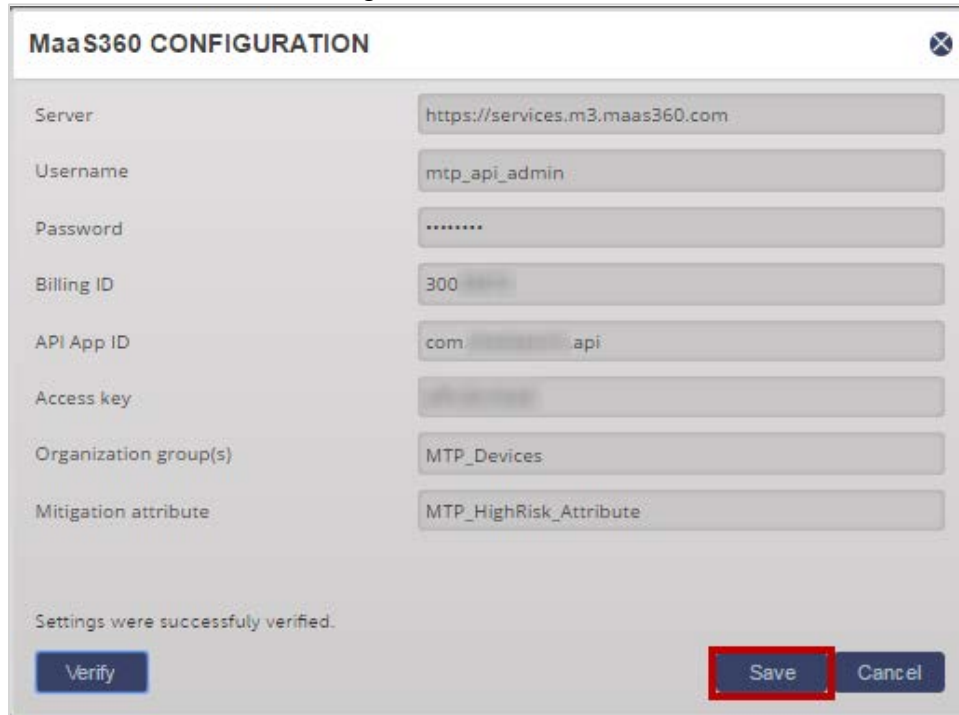
3.2 Configuring MDM Integration Settings

- 3.2.0.1. Navigate to **Settings > Device Management > Setting**.
- 3.2.0.2. Select “MaaS360” from the “MDM service” drop-down menu under the Device Management Settings area.



- 3.2.0.3. A pop-up window will open. Configure the settings as are appropriate for your MaaS360 Deployment, such as those you have created in Section 2.

- 3.2.0.4. Click the “VERIFY” button. If the settings are correct, and the SandBlast Mobile Dashboard can communicate with the MaaS360 system, you will be able to click the “SAVE” button to finish configuration.



The image shows a configuration window titled "MaaS360 CONFIGURATION" with a close button in the top right corner. It contains several input fields for configuration data. Below the fields, a message states "Settings were successfully verified." At the bottom, there are three buttons: "Verify", "Save", and "Cancel". The "Save" button is highlighted with a red rectangular border.

Field	Value
Server	https://services.m3.maas360.com
Username	mtp_api_admin
Password	*****
Billing ID	300
API App ID	com. api
Access key	
Organization group(s)	MTP_Devices
Mitigation attribute	MTP_HighRisk_Attribute

Settings were successfully verified.

3.2.1 Registration Email and Registration Limit Settings

- 3.2.1.1. Navigate to **Settings > Device Management > Setting**, under the “Notify user when device was added by MDM” section, when a MDM Service is configured, these settings are configured automatically. Registration emails are turned off. Daily registration limit is set to 100.

Setting	Description
Registration email (iOS)	Should the system send Registration email to iOS devices?
Registration email (Android)	Should the system send Registration email to Android devices?
Daily registration limit	The number of devices that can register within a 24 hour period.

- 3.2.1.2. If you make changes to the default settings, click the “Save” button to have changes take effect.

3.2.2 MDM Advanced Settings

When a MDM Service is configured, the Device Management Advanced Settings are automatically configured based on recommendations of the selected MDM provider, in this case from MaaS360. If you wish to change these settings follow this process.

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

The screenshot shows the 'Settings' page in the Check Point SandBlast Mobile interface. The left sidebar contains a menu with the following items: Audit Trail, Customization, Privacy Settings, SMTP Settings, Device Management (expanded), Setting, Advanced (selected), Syslog, Administrators, MITM, Announcements, and License Management. The main content area is titled 'MDM Advanced Settings:' and contains three settings: 'Device sync interval' with a value of 10, 'Device deletion threshold' with a value of 10, and 'Deletion delay interval' with a value of 0.5. Each input field has a help icon (question mark) to its right. A 'Save' button is located below the settings.

Setting	Description
Device sync interval	Interval to connect with MDM to sync devices. Values: 10-1440 minutes, in 10 minute intervals.
Device deletion threshold	Percentage of devices allowed for deletion after MDM 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 MDM during the threshold interval. Values: 0-48 hours

- 3.2.2.2. If you make changes to the default settings, click the “Save” button to have changes take effect.

4 Configuring MDM to Deploy SandBlast Mobile Protect app

4.1 Prerequisites

- 4.1.1. **SandBlast Mobile Gateway/Server** – Server name of the SandBlast Mobile gateway/server, which should be us-gw01 or eu-gw01. If you don't know your SandBlast Mobile server name, follow the instructions in Section 7.2 to find out.

4.2 Adding the SandBlast Mobile Protect App to Your App Catalog

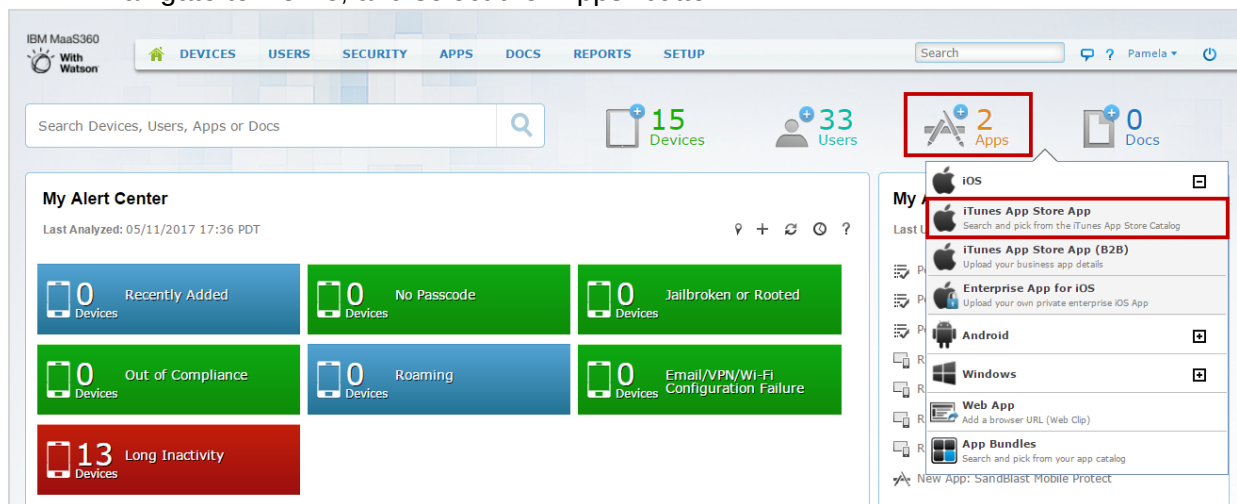
Now that the MDM and SandBlast Mobile Dashboard are communicating, we can now start deploying the SandBlast Mobile Protect app from the public stores to those devices that will be protected by SandBlast Mobile.

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

4.2.1 iOS App – Add to Catalog

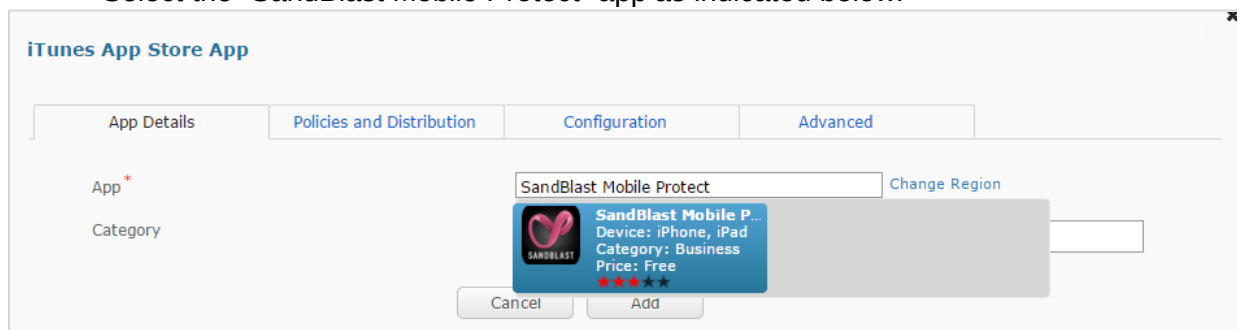
The SandBlast Mobile Protect App for iOS can be automatically configured and deployed. The user only needs to accept the installation, and then launch the app once it is installed to finish activation and registration.

- 4.2.1.1. Navigate to **Home**, and select the “Apps” button.



- 4.2.1.2. Select “iTunes App Store App” from the Store List.

- 4.2.1.3. In the “App” field, enter “SandBlast Mobile Protect” to start actively searching the store. Select the “SandBlast Mobile Protect” app as indicated below.



- 4.2.1.4. Navigate to the “Configuration” tab, and select “Input Type” of “Key/Value”.

4.2.1.5. Add the following Key/Value pairs:

4.2.1.5.1. Lagoon Server Address = us-gw01 (this value should be **your** SandBlast Mobile gateway)

4.2.1.5.2. Device Serial Number = %csn%

iTunes App Store App

App Details Policies and Distribution **Configuration** Advanced

App Config Source: Key/Value

1. Use this to define any configuration attributes for the devices that this app supports. Contact app developer to get details.
2. Provide the attribute name in the first field followed by the required value in the latter. Value can be fixed string, username (%username%), domain (%domain%), email (%email%), deviceId (%csn%) or any of the user attributes maintained.

Lagoon Server Address	us-gw01.locsec.net	+ -
Device Serial Number	%csn%	+ -

Cancel Add

4.2.1.6. Click the “Add” button.

4.2.1.7. Enter your admin password.

To Add App

Enter your password *

Cancel Continue

4.2.1.8. Click the “Continue” button.

4.2.2 Android App – Add to Catalog

The Android SandBlast Mobile Protect App can be automatically configured and deployed. The user only needs to accept the installation, and then launch the app once it is installed to finish activation and registration.

4.2.2.1. Navigate to **Home**, and select the “Apps” button.

IBM MaaS360 With Watson

DEVICES USERS SECURITY **APPS** DOCS REPORTS SETUP

Search Devices, Users, Apps or Docs

15 Devices 33 Users **2 Apps** 0 Docs

My Alert Center
Last Analyzed: 05/11/2017 17:36 PDT

0 Devices Recently Added	0 Devices No Passcode	0 Devices Jailbroken or Rooted
0 Devices Out of Compliance	0 Devices Roaming	0 Devices Email/VPN/Wi-Fi Configuration Failure
13 Devices Long Inactivity		

My Apps

- Android
 - Google Play App** (highlighted)
 - Enterprise App for Android
- Windows
- Web App
- App Bundles

Rule violation for: iPhone (2)
New App: SandBlast Mobile Protect

4.2.2.2. Select “Google Play App” from the Store List.

- 4.2.2.3. In the “App” field, enter “SandBlast Mobile Protect” to start actively searching the store. Select the “SandBlast Mobile Protect” app as indicated below.

The first screenshot shows the Google Play App search interface. The 'App Name' field contains 'SandBlast Mobile Protect'. Below the field, there are search results. The first result is 'SandBlast Mobile P...' with a red box highlighting its icon. Other results include 'Beta-SandBlast Mo...' and 'Bejeweled Classic'.

The second screenshot shows the same interface. The 'App Name' field still contains 'SandBlast Mobile Protect'. At the bottom, there are 'Cancel' and 'Add' buttons. The 'Add' button is highlighted with a red box.

- 4.2.2.4. Click the “Add” button.

4.3 Deploying SandBlast Mobile Protect app

To deploy the SandBlast Mobile Protect app to devices that will be registered to the SandBlast Mobile solution we need to link the SandBlast Mobile Protect app in our app catalog to the Device Provisioning Group we created in Section 2.6.

- 4.3.1. Navigating to **Apps > App Catalog**, select both the iOS and Android SandBlast Mobile Protect apps.

The screenshot shows the IBM MaaS360 App Catalog interface. The top navigation bar has tabs for DEVICES, USERS, SECURITY, APPS, DOCS, REPORTS, and SETUP. The 'APPS' tab is selected and highlighted with a red box. Below the navigation bar, there is a search bar and a 'Pamela' dropdown. The main content area shows a table of apps. There are two apps listed, both named 'SandBlast Mobile Protect'. The first app is for Android and the second is for iOS. Both apps have a 'Distribute' link highlighted with a red box. A red box also highlights the 'APPS' tab in the top navigation bar.

App	Platform	Version	Release Date	Release ID
SandBlast Mobile Protect	Android	2.58.0-RELEASE-b123	05/09/2017 06:47 PDT	2.58.0-RELEASE-b123
SandBlast Mobile Protect	iOS	2.58.2855	05/01/2017 21:00 PDT	2.58.2855

- 4.3.2. Click the “Distribute” link.

- 4.3.3. On the “Distribute” pop-up window, set “Target” equal to “Group” and choose the device provisioning group you created in Section 2.6, in our example “MTP_Devices”.
- 4.3.3.1. Select “Instant Install” and “Send Email” checkboxes.

Distribute

Target: Group (dropdown) | MTP_Devices (dropdown) +

☒ Instant Install ☒ Send Email ☐ Send Notification

Cancel Distribute

- 4.3.4. Click the “Distribute” button.
- 4.3.5. Enter your admin password, and click the “Continue” button.

To Distribute App

Enter your password *

Cancel Continue

4.4 Setting Policy to Require SandBlast Mobile Protect to be Installed

The SandBlast Mobile Protect app is required by creating a Security Policy for iOS and Android devices, then creating a compliance rule set to the Device Provisioning Group we created in Section 2.6, and apply the compliance policy to the Device Provisioning Group.

4.4.1 Creating Compliance Actions for iOS Devices (Policy)

The policy will specify the actions taken on all SandBlast Mobile iOS devices.

- 4.4.1.1. Navigate to **Security > Policies**, and click the “Add Policy” button.

IBM MaaS360 With Watson

DEVICES USERS **SECURITY** APPS DOCS REPORTS SETUP

Policies

Compliance Rules

Compliance Log

Privacy

Locations

2 Add Policy Precedence Content More

Name Version Last Modified Last Published

No matching records found

Showing 0 to 0 of 0 entries (filtered from 9 total entries)

- 4.4.1.2. Enter a Name for the policy, such as “MTP_App_iOS”, select a “Type” of “iOS MDM”, and select “Start From” equal to “Default iOS MDM Policy”.

IBM MaaS360
With Watson

DEVICES USERS SECURITY APPS DOCS REPORTS SETUP

Search ? Pamela

← Add Policy

Name* MTP_App_iOS

Description

Type* iOS MDM

Start From* (def) Default iOS MDM Policy

Reset Continue

- 4.4.1.3. Click the “Continue” button.
- 4.4.1.4. There are several sections for policy sets, such as “Passcode, Restrictions, Application Compliance, etc. We will make our modifications in the Restrictions section.
- 4.4.1.5. Click the “Edit” button.
- 4.4.1.6. Select the “Application Compliance” tab.
- 4.4.1.7. Under the **Application Compliance** section, select “Configure Required Applications”.
- 4.4.1.8. In the “Application Name” field, start typing “SandBlast Mobile Protect” and the app will pop-up, select SandBlast Mobile Protect.

IBM MaaS360
With Watson

DEVICES USERS SECURITY APPS DOCS REPORTS SETUP

Search ? Pamela

← MTP_App_iOS

Last Published: 11/16/2016 14:00 PST [Version:1]

Cancel Save Save And Publish More

Device Settings

Passcode

Restrictions

Application Compliance

ActiveSync

Wi-Fi

VPN

AirPrint

Accounts

Configure Restricted Applications (App Blacklist)
Add Name for Apps restricted on managed devices.

Configure Allowed Applications (App Whitelist)
Add Name for Apps allowed on managed devices. Any other app would be disallowed.

Configure Required Applications
Add Name and Bundle ID for the apps required to be installed on managed devices. This policy can be used in conjunction with the Blacklist or Whitelist policy settings. It is recommended that you also use the App Management workflows to distribute this app to the appropriate devices.

Application Name

SandBlast Mobile Protect Change Region

iOS Apps

SandBlast Mobile Protect
Device Support: iPhone,iPad
Category:Business
Price:Free

- 4.4.1.9. Click the “Save and Publish” button.

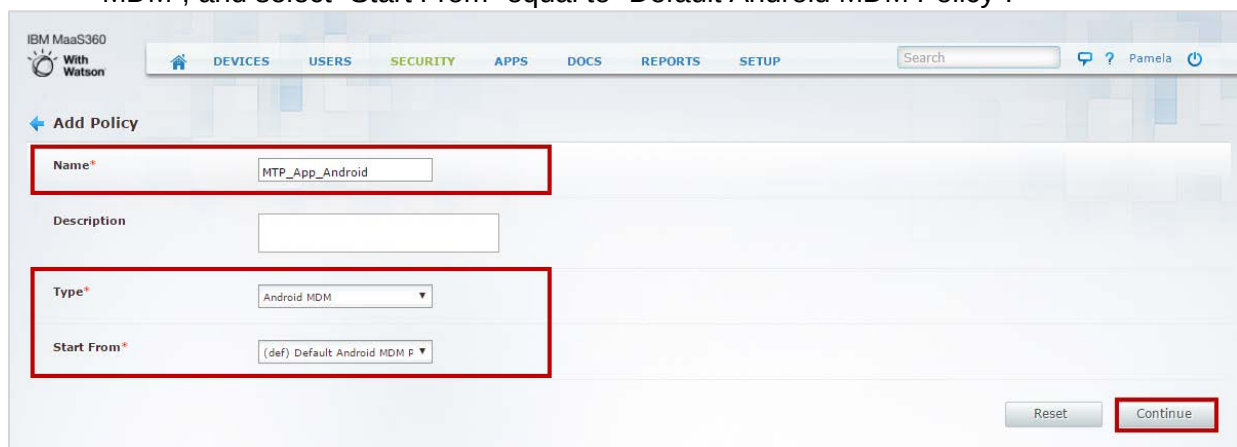
4.4.2 Creating Compliance Actions for Android Devices (Policy)

The policy will specify the actions taken on all SandBlast Mobile Android devices.

4.4.2.1. Navigate to **Security > Policies**, and click the “Add Policy” button.



4.4.2.2. Enter a Name for the policy, such as “MTP_App_Android”, select a “Type” of “Android MDM”, and select “Start From” equal to “Default Android MDM Policy”.



4.4.2.3. Click the “Continue” button.

- 4.4.2.4. There are several sections for policy sets, such as “Passcode, Security, Restrictions, Application Compliance, etc. We will make our modifications in the Restrictions section.
- 4.4.2.5. Select the “Application Compliance” tab.
- 4.4.2.6. Click the “Edit” button.
- 4.4.2.7. Under the **Application Compliance** section, select “Configure Required Applications”.
- 4.4.2.7.1. In the “Application Name” field, enter “SandBlast Mobile Protect”
- 4.4.2.7.2. In the “Application ID” field, enter “com.lacoon.security.fox”

IBM MaaS360
With Watson

DEVICES USERS SECURITY APPS DOCS REPORTS SETUP

Search Pamela

MTP_App_Android
Last Published: 11/16/2016 14:05 PST [Version:1]

Cancel Save **Save And Publish** More

Device Settings

- Passcode
- Security
- Restrictions
- Application Compliance**
- Native App Compliance
- ActiveSync
- Wi-Fi
- VPN
- Web Shortcuts
- Device Management

Configure Restricted Applications (App Blacklist)
Add Name and App IDs for Apps that need to be restricted on managed devices. Depending on the action specified, the user will either be prompted to uninstall the App or be restricted from using the App. System apps specified as Restricted Applications will always be Blocked from use irrespective of the action specified.

Configure Restricted Applications by App Permissions
Specify App Permissions that you do not want to be allowed on managed devices. Apps that use these permissions will be blocked or uninstalled depending on the action specified. You can also specify apps that will be allowed even if they use the specified permission. Requires MDM App version 4.40 or higher.

Configure Allowed Applications (App Whitelist)
Add Name and App IDs for Apps allowed on managed devices. Any other user installed app will be automatically restricted. Depending on the action specified, the user will either be prompted to uninstall the App or be restricted from using the App.

Configure Required Applications
Add Name and App IDs for Apps required to be always installed on managed devices. This policy can be used in conjunction with Blacklist or Whitelist policy. Supports multiple apps as a comma separated list in which case atleast one of the apps is mandatory. First app in the list is considered the primary app and user will be prompted to install this when no apps are found. Supported on MDM App version 4.20 and above.

Application Name: SandBlast Mobile Protect

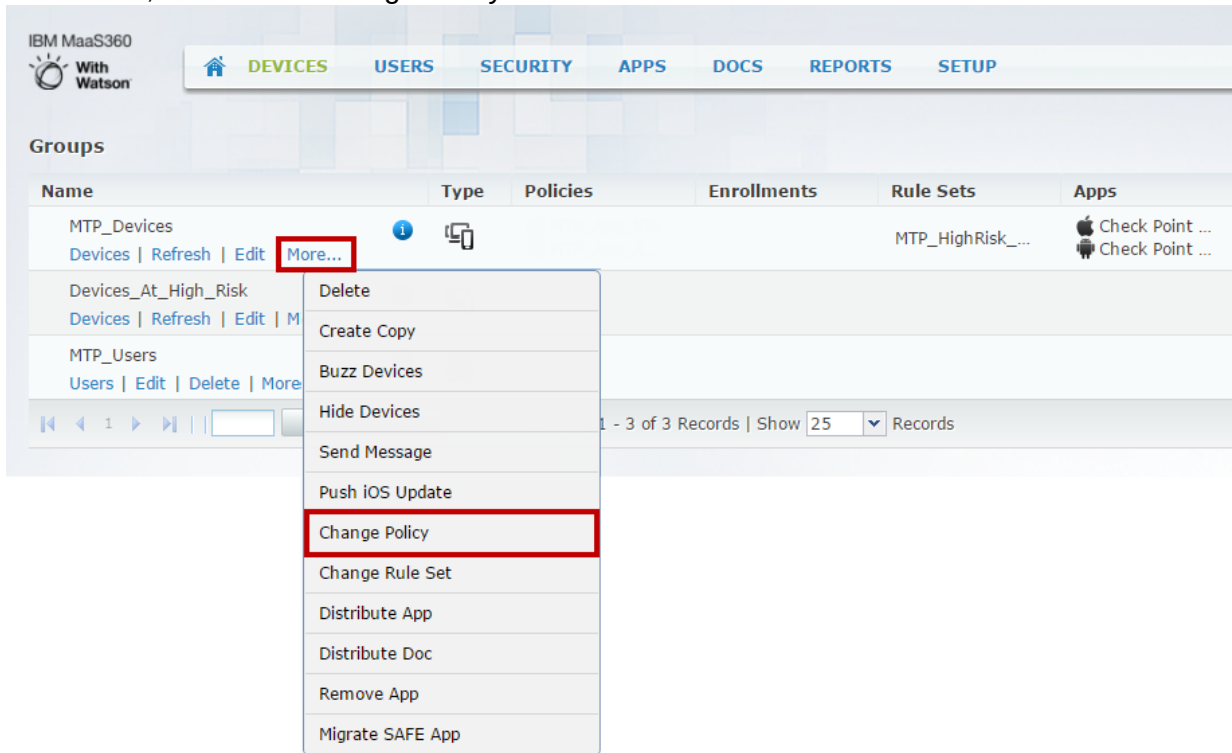
Application ID: com.lacoon.security.fox

- 4.4.2.8. Click the “Save And Publish” button.

4.4.3 Applying App Required Policy to Device Provisioning Group

The policies created in the previous section are assigned to the device provisioning group created in Section 2.6, in our example “MTP_Devices”.

- 4.4.3.1. Navigate to **Devices > Groups**, locate the device provisioning group, click the “More...” link, and select “Change Policy”.

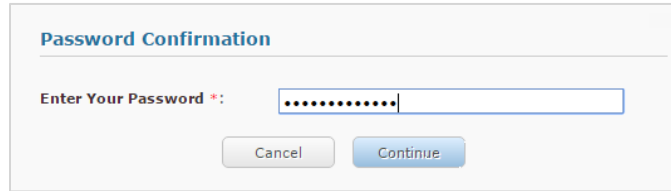


- 4.4.3.2. Set iOS Policy to the compliance policy we created in Section 4.4.1, in our example “MTP_App_iOS”.
- 4.4.3.3. Set Android Policy to the compliance policy we created in Section 4.4.2, in our example “MTP_App_Android”

The screenshot shows the 'Change Policy - MTP_Devices' dialog box. It contains three dropdown menus: 'iOS Policy' (set to 'MTP_App_iOS'), 'Android Policy' (set to 'MTP_App_Android'), and 'Windows MDM Policy' (set to 'Select a Policy Set'). Below these, there is a checkbox for 'Auto assign to new devices' which is checked. At the bottom, there are 'Cancel' and 'Submit' buttons. The 'Submit' button is highlighted with a red box.

- 4.4.3.4. Click the “Submit” button.

4.4.3.5. Type your admin password, and then click the “Continue” button.



Password Confirmation

Enter Your Password *:

.....

Cancel Continue



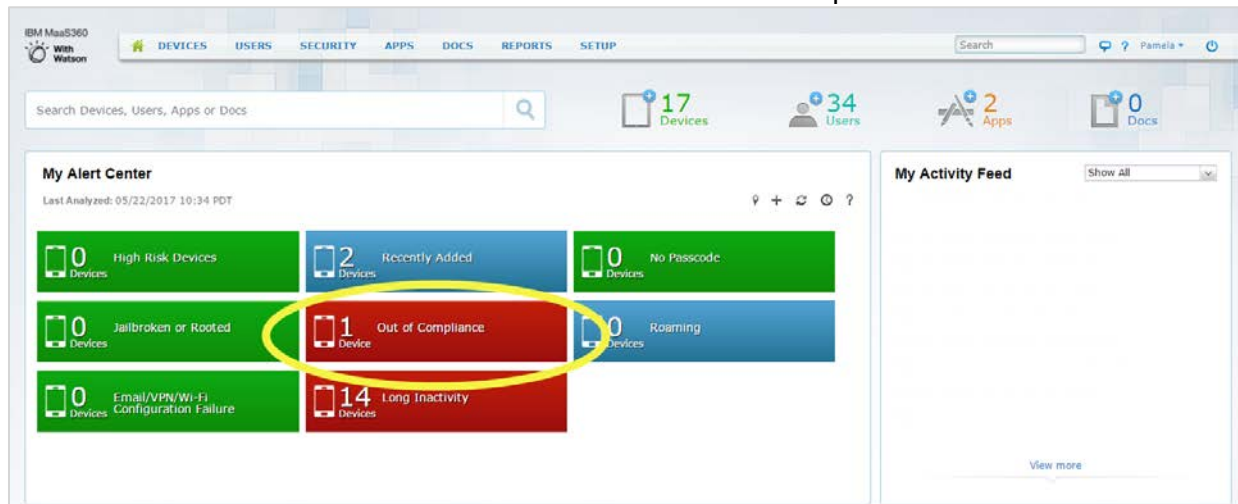
Name	Ty...	Policies	Enrollme...	Rule Sets	Apps	Docs	Updated ...	Updated	Last Eval...
Devices_At_High_Risk	Devices Refresh Edit More...						05/11/2017 15:...	05/10/2017 18:...	
MTP_Devices	Devices Refresh Edit More...	MTP_App_i...		MTP_HighRis...			11/15/2016 12:...	05/10/2017 18:...	
MTP_Users	Users Edit Delete More...						11/10/2016 12:...		

Jump To Page: Displaying 1 - 3 of 3 Records | Show 25 Records Reset Filters Customize Columns CSV Export

Note: Any device that belongs to the Device Provisioning Group (“MTP_Devices”) that hasn’t installed the SandBlast Mobile Protect app will be out of compliance.

4.4.4 Device Out of Compliance – Missing SandBlast Mobile Protect App

4.4.4.1. MaaS360 Portal Home Screen indicates an “Out of Compliance” issue.



Search Devices, Users, Apps or Docs

17 Devices 34 Users 2 Apps 0 Docs

My Alert Center
Last Analyzed: 05/22/2017 10:34 PDT

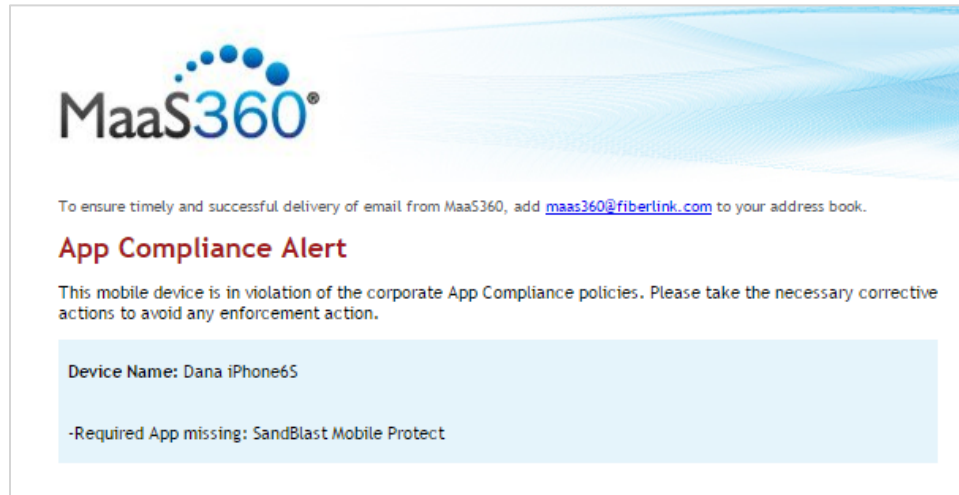
0 High Risk Devices	2 Recently Added Devices	0 No Passcode Devices
0 Jailbroken or Rooted Devices	1 Out of Compliance Device	0 Roaming Devices
0 Email/VPN/Wi-Fi Configuration Failure Devices	14 Long Inactivity Devices	

View more

4.4.4.2. Device Details View indicates an “Out of Compliance” issue.

IBM MaaS360			
DEVICES USERS SECURITY APPS DOCS REPORTS SETUP			
Dana iPhone6S Summary			
Hardware Inventory			
Username	dscully	Email Address	dscully@cptme.us
Operating System	iOS 10.2.1 (14D27)	Manufacturer	Apple
Model	iPhone6S Plus (M16W2LL)	IMEI/MEID	Not Available
Device ID	AppICD5P3JNGRX7	Ownership	Corporate Owned
Device Enrollment Mode	Manual		
WorkPlace & Security			
Managed Status	Enrolled	Applied Policy	MDM: MTP_App_iOS (2)
Last Reported	05/22/2017 10:32 PDT	Jailbroken/Rooted	No
Failed Settings	No	Selective Wipe Status	Not Applied
Encryption Level	Block-level & File-level	Passcode Status	MDM: Compliant
Policy Compliance State	Out of Compliance	Rules Compliance Status	In Compliance
Out of Compliance Reasons	Required App missing: SandBlast Mobile Protect	Rule Set Name	MTP_highRisk_Rules
Network Information			
Phone Number	Not Available	ICCID	Not Available
Is Roaming	Not Enabled	International Data Roaming	Not Enabled
Home Carrier	AT&T	Current Network Type	Not Available

4.4.4.3. The user and the admin will receive an alert email.



5 Deploying SandBlast Mobile Protect App to the Devices

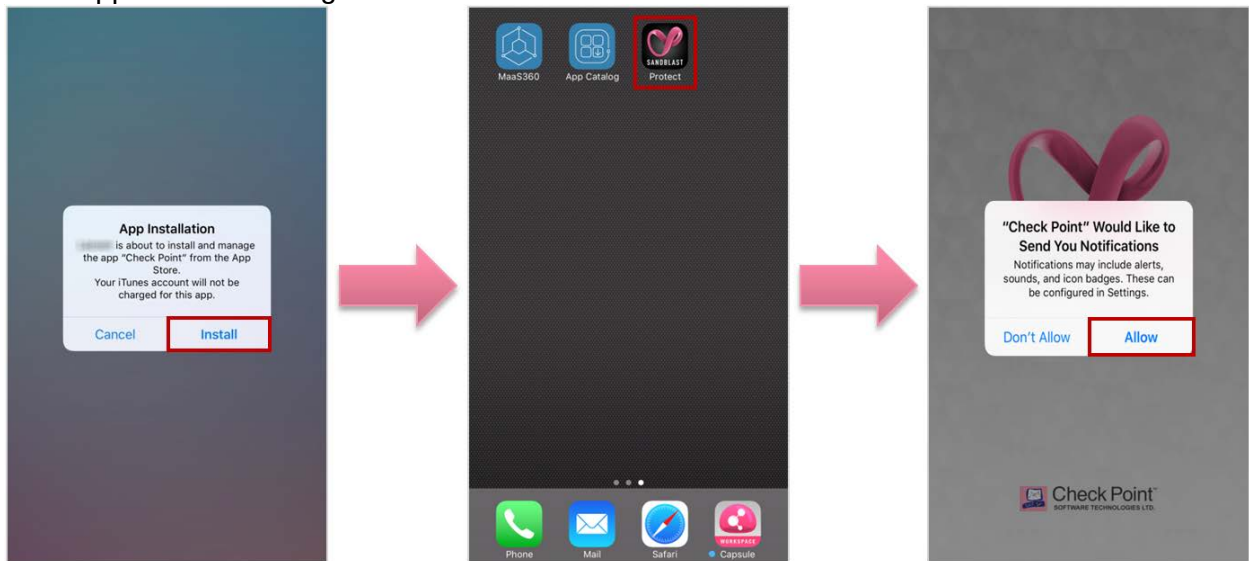
This section describes the user experience during the deployment of the SandBlast Mobile Protect app.

5.1 Registration of an iOS Device

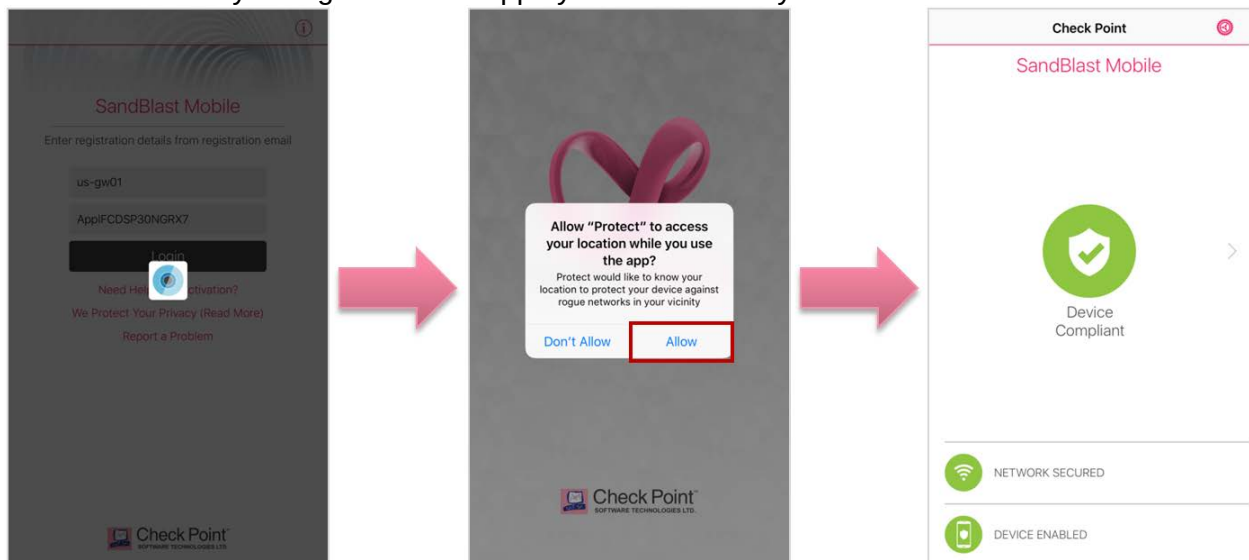
After the device is registered to the MaaS360 system and the SandBlast Mobile Protect app has been “Distributed” to the Device Provisioning Group (“MTP_Devices”), the user will be prompted to install the SandBlast Mobile Protect App.

5.1.1. The user taps “INSTALL”.

5.1.2. After the App has been installed on the iOS Device, the user only needs to launch the App to finish the registration.



5.1.3. After the overview, the App will automatically register. The registration server and key are automatically configured in the App by the MaaS360 system.



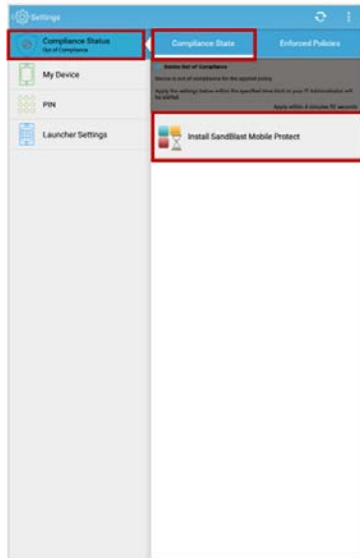
5.1.4. Once the App is done scanning the system, it will display the state of the device. In this case, the device is without malicious or high risk apps, network and OS threats.

5.2 Registration of an Android Device

After the device is registered to the MaaS360 system, the user will navigate in the MaaS360 App Catalog app or the user will receive a policy error.

5.2.1 SandBlast Mobile Protect Install Prompted by Compliance Violation

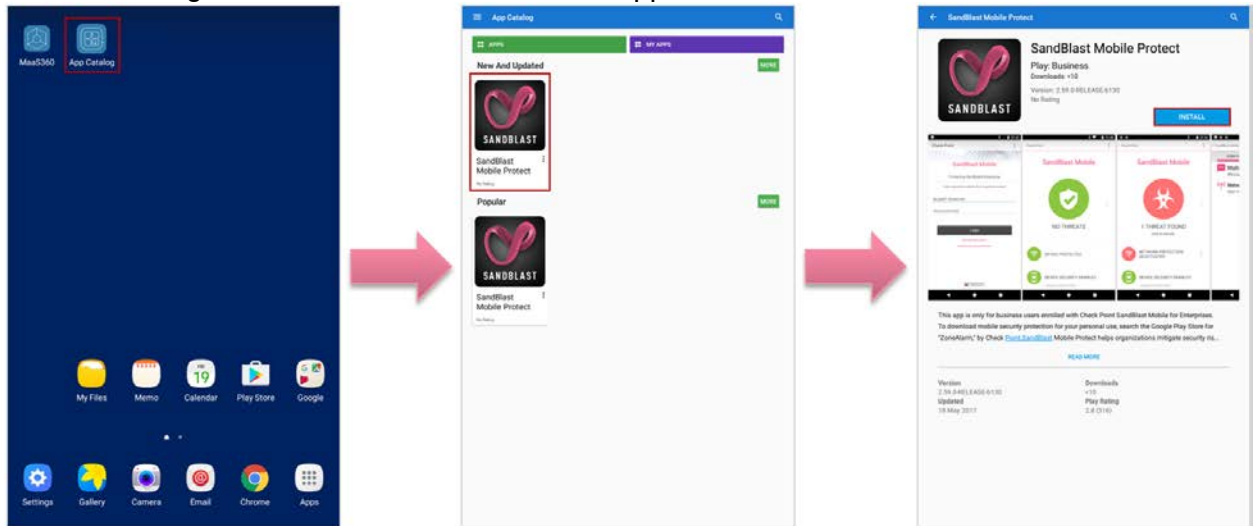
- 5.2.1.1. The user is prompted through notifications that their device is out of compliance. Clicking that notification will launch the MaaS360 app, opening the Compliance Status screen.
- 5.2.1.2. Clicking the “Install SandBlast Mobile Protect” button will launch the SandBlast Mobile Protect app in the Google Play Store.



- 5.2.1.3. Skip to Section 5.2.3 to continue with the app installation.

5.2.2 SandBlast Mobile Protect Install Initiated by User in MaaS360 App Catalog

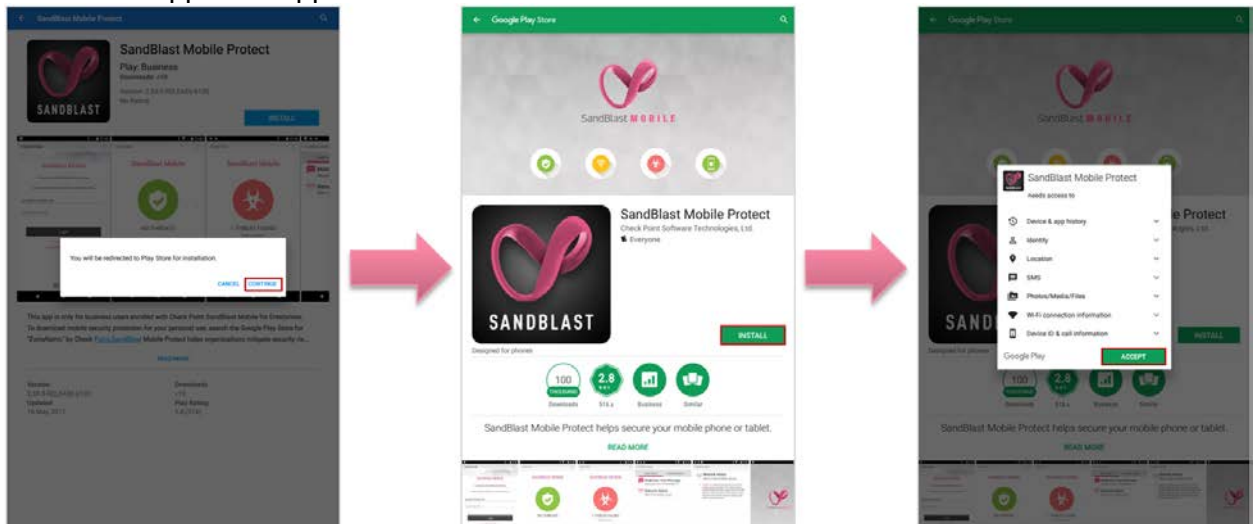
- 5.2.2.1. When the user opens the MaaS360 App Catalog, the app opens to the Apps list.
- 5.2.2.2. Clicking the “SandBlast Mobile Protect” app, the user then clicks the “Install” button.



- 5.2.2.3. Proceed to Section 5.2.3 to continue with the app installation.

5.2.3 Continuation of SandBlast Mobile Protect App

- 5.2.3.1. At the prompt to open within the Google Play Store, the user clicks the “Continue” button.
- 5.2.3.2. The user taps the “INSTALL” button, and taps “ACCEPT” to accept the permissions of the App. The App installs.

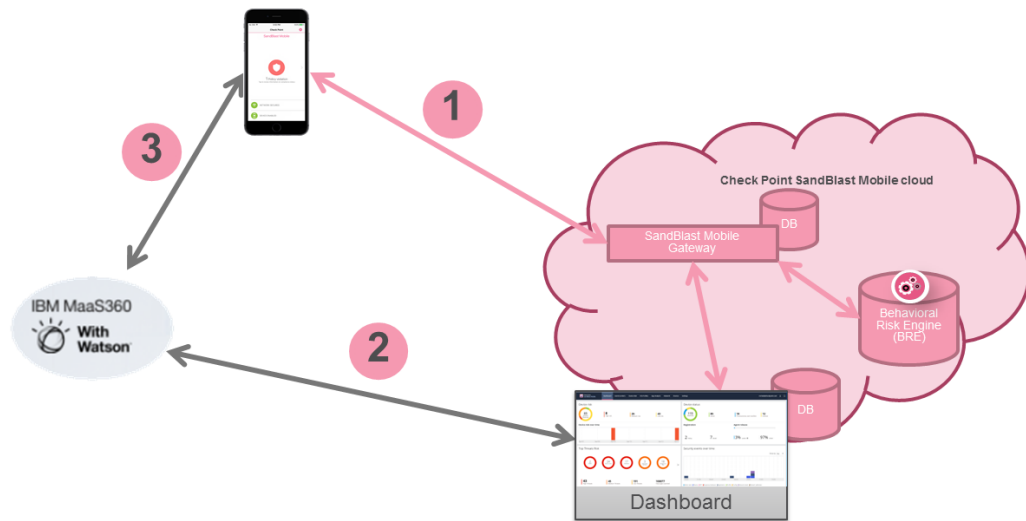


- 5.2.3.3. After the App is installed, the user must launch the App to finish its deployment and registration to SandBlast Mobile.
- 5.2.3.4. The user is prompted to allow the SandBlast Mobile Protect app to be a device administrator. They must tap “Activate”.
- 5.2.3.5. Once the App is done scanning 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.



6 Testing High Risk Activity Detection and Policy Enforcement

Malicious app or activity detected on User's Device



- 1 – SandBlast Mobile sends notification to User's Device
- 2 – SandBlast Mobile sends High Risk tag for User's Device to IBM MaaS360
- 3 – IBM MaaS360 pushes High Risk State Policy Actions to User's Device

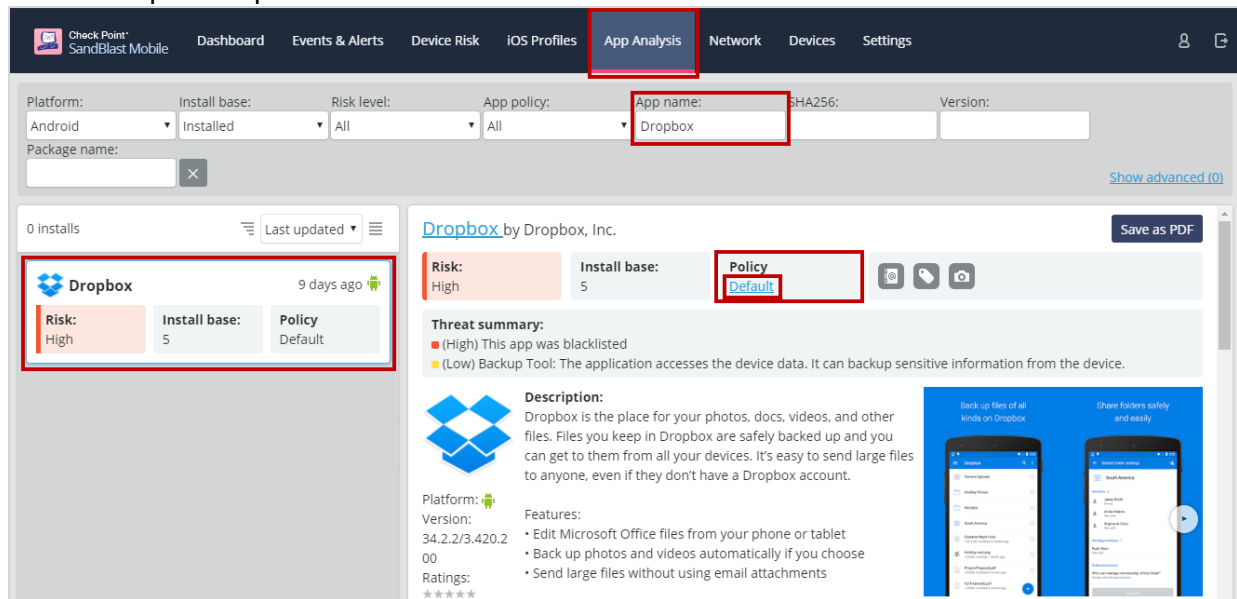
If the user's device is determined to be at a High Risk state either due to a malicious app or malicious activity, the SandBlast Mobile system notifies the User via in-app notifications as well as updates the High Risk state to the MaaS360 system for that device. MaaS360 receives the state change, and upon recognizing the custom attribute being tied to a compliance policy, enacts the policy actions.

In the following example, the Administrator will blacklist an app, such as in our example "Dropbox". As a result, the user's device will be identified to be at High Risk due to the blacklisted app, "Dropbox", being installed on the device. The SandBlast Mobile Dashboard will notify the user, and mark the device as High Risk to the MaaS360 system. The MaaS360 System will then enforce policy actions specified in the compliance policy, in our example "MTP_Android_HighRisk" based on the compliance rules specifying that the custom attribute set to "yes" groups this device in the device mitigation group, "Devices_At_High_Risk". This mitigation process was the one we created in Section 2.8.

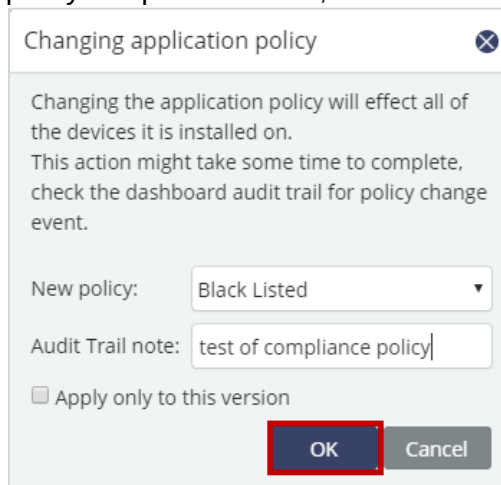
6.1 Blacklisting a Test App

The first step is to blacklist an app, in our example “Dropbox”.

- 6.1.1. Log into the SandBlast Mobile Dashboard.
- 6.1.2. Navigate to **App Analysis** tab, and search for the app you wish to blacklist, in our example “Dropbox”.



- 6.1.3. Click the “Policy” link of “Default”.
- 6.1.4. 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”.

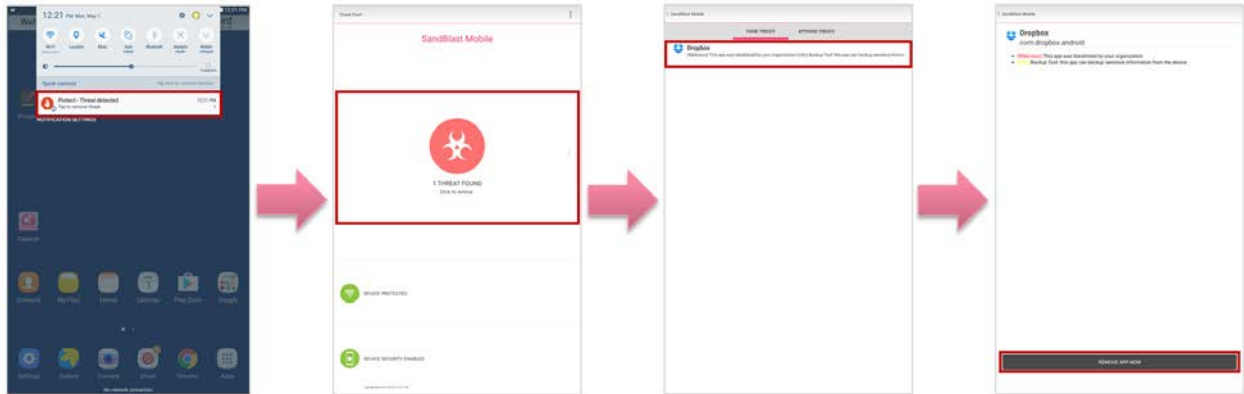


- 6.1.5. Click the “OK” button.

6.2 View of Non-Compliant Device

6.2.1 SandBlast Mobile Protect App Notifications

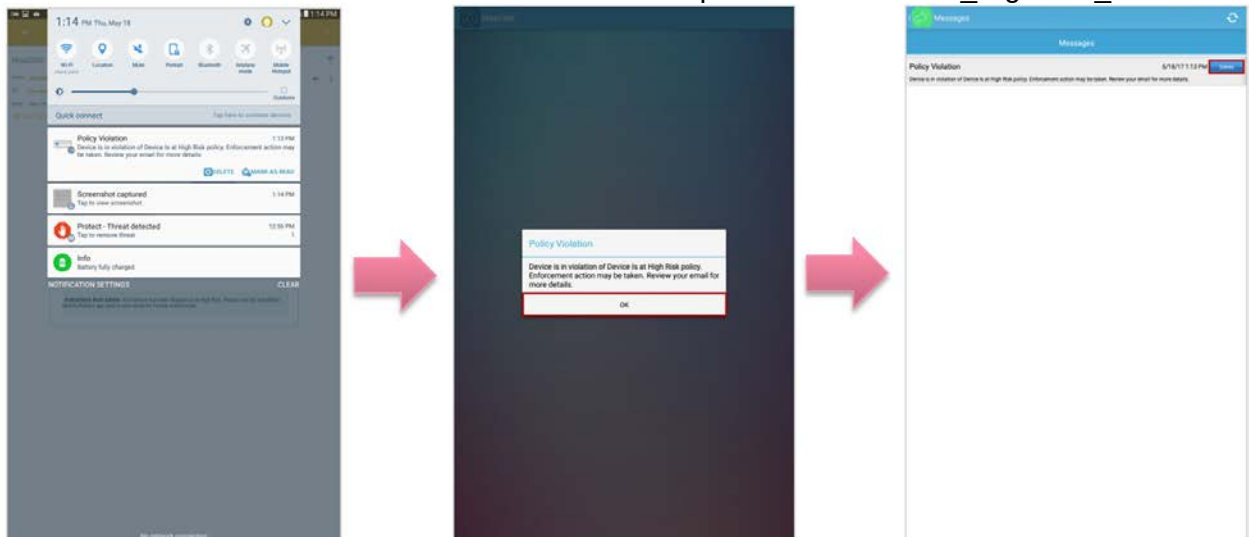
- 6.2.1.1. The user receives a SandBlast Mobile Protect notification indicating that the blacklisted app is not allowed by Corporate Policy, in our example “Dropbox”.



- 6.2.1.2. The user will not be able to use the device's camera, as specified in the compliance actions (policy) we created in Section 2.8.3.1.2, in our example “MTP_Android_HighRisk” until the user removes the blacklisted app.

6.2.2 MaaS360 App Notifications

- 6.2.2.1. The user receives a MaaS360 notification as specified in the “MTP_HighRisk_Rules”.



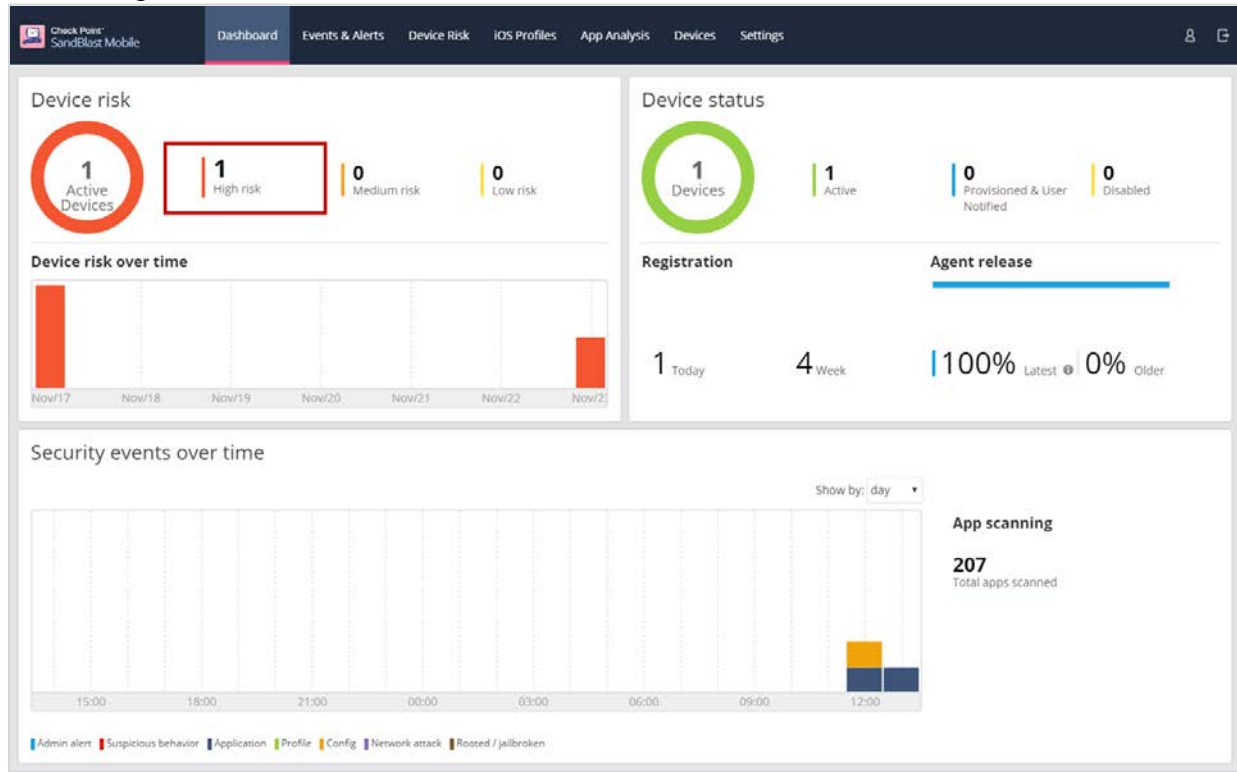
6.2.3 MaaS360 Email Notification

- 6.2.3.1. The user receives an email from the MaaS360 system, as specified in the “MTP_HighRisk_Rules”.



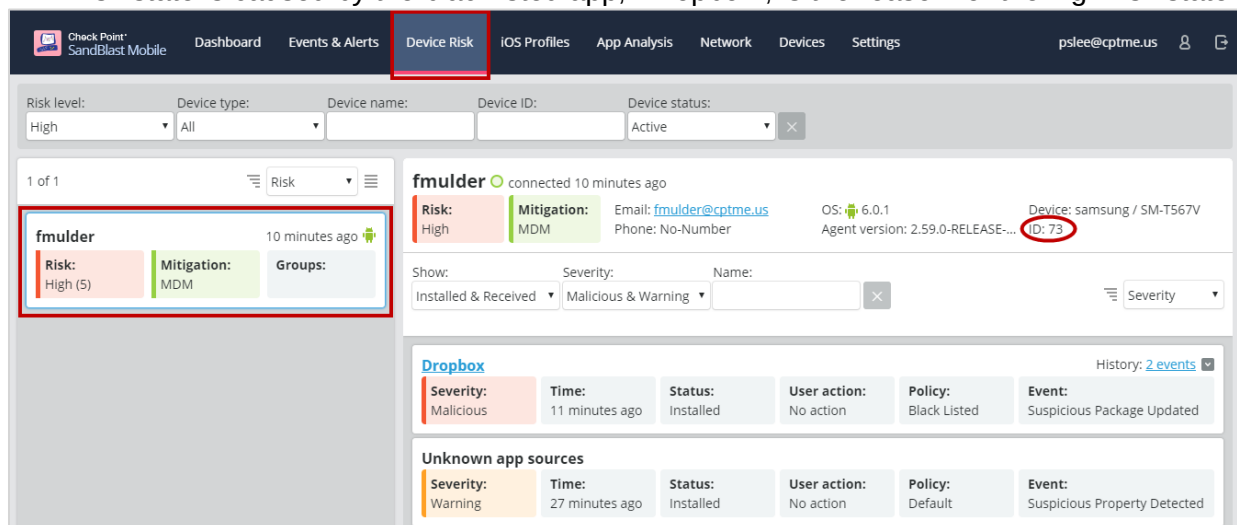
6.3 Administrator View on the SandBlast Mobile Dashboard

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

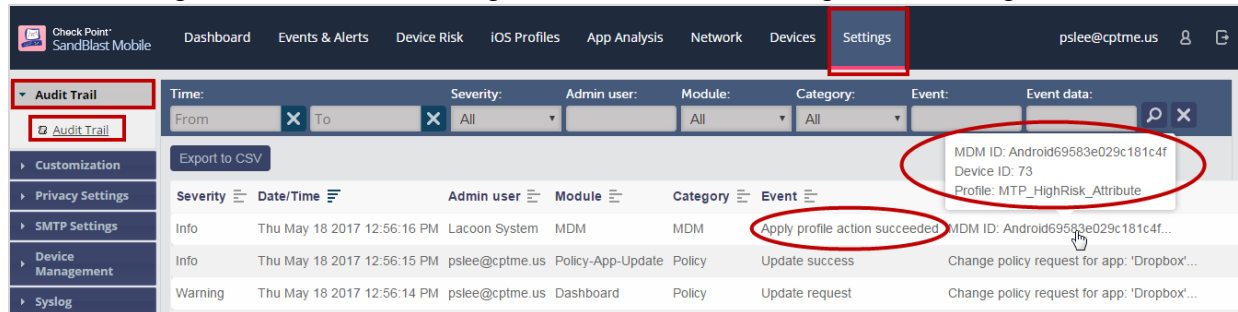


- 6.3.2. Clicking the High Risk will display a list of devices at high risk.

- 6.3.3. Selecting the desired device from the left-side list, the Administrator can see that the high risk state is caused by the blacklisted app, "Dropbox", is the reason for the high risk state.

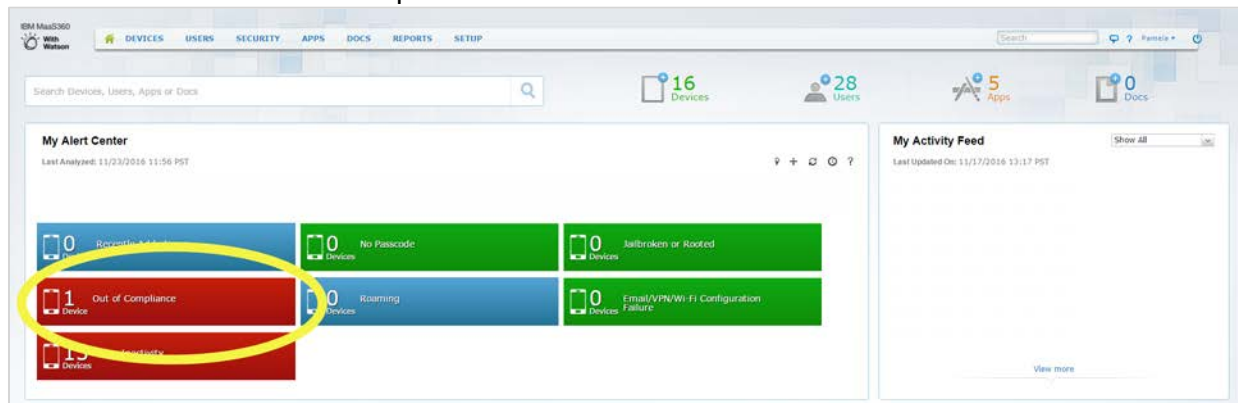


- 6.3.4. Navigating to **Settings > Audit Trail**, the Administrator will see that there was an alert sent to the MDM, and hovering over the Event Data information, it will pop-up the Event that was sent.
- 6.3.5. In this example Device ID of 73 was moved to Profile “MTP_HighRisk_Attribute” which is the Mitigation Attribute we configured in the Device Management Settings for MaaS360.

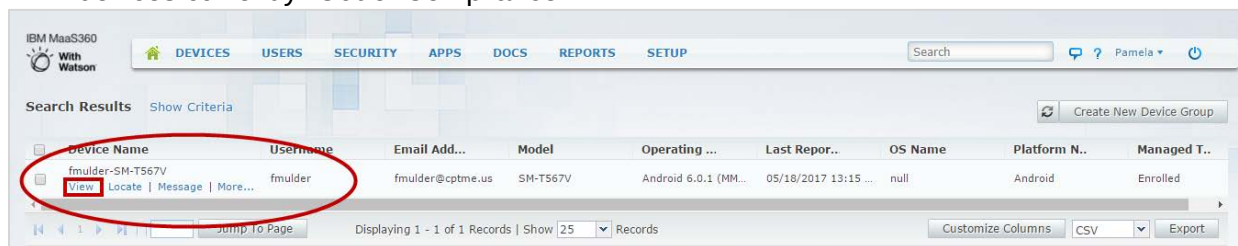


6.4 Administrator View on the MaaS360 Portal

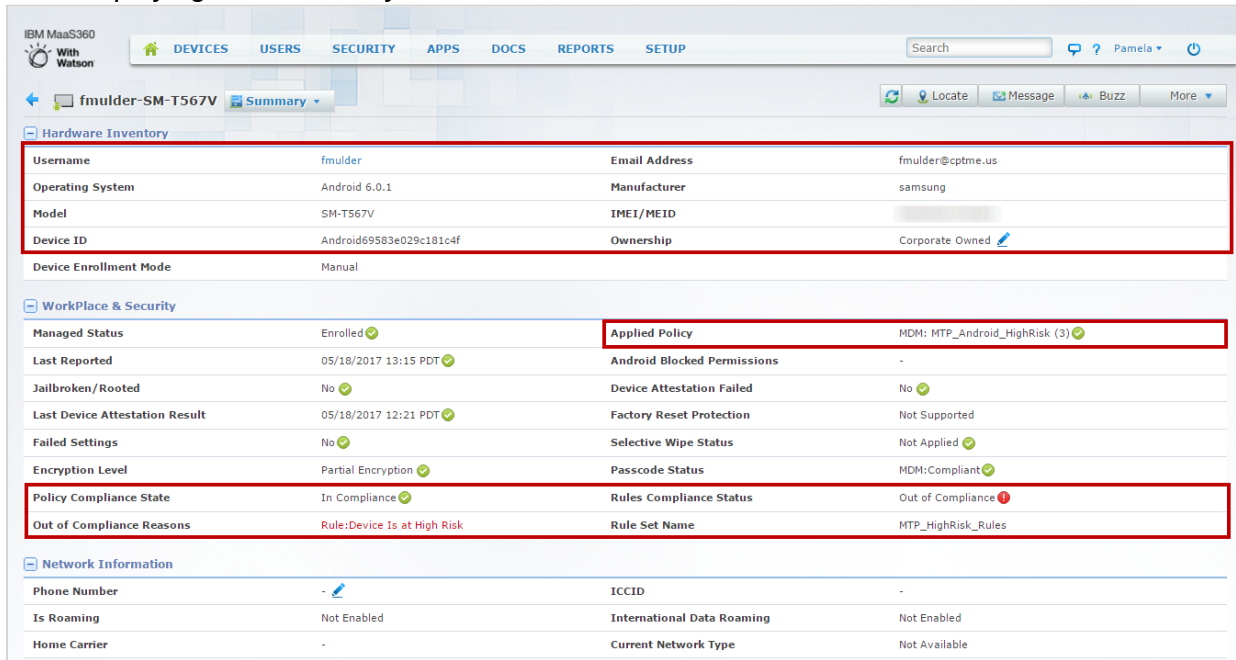
- 6.4.1. In the MaaS360 Portal from the **Home** tab, the Administrator can that one or more devices are “Out of Compliance”.



- 6.4.2. Clicking the “Out of Compliance” button, the Administrator is presented with a list of the devices currently “Out of Compliance”.



- 6.4.3. Clicking the “View” link under the device of interest will open the Device Details view displaying the “Summary” screen.



Hardware Inventory

Username	fmulder	Email Address	fmulder@cptme.us
Operating System	Android 6.0.1	Manufacturer	samsung
Model	SM-T567V	IMEI/MEID	
Device ID	Android69583e029c181c4f	Ownership	Corporate Owned
Device Enrollment Mode	Manual		

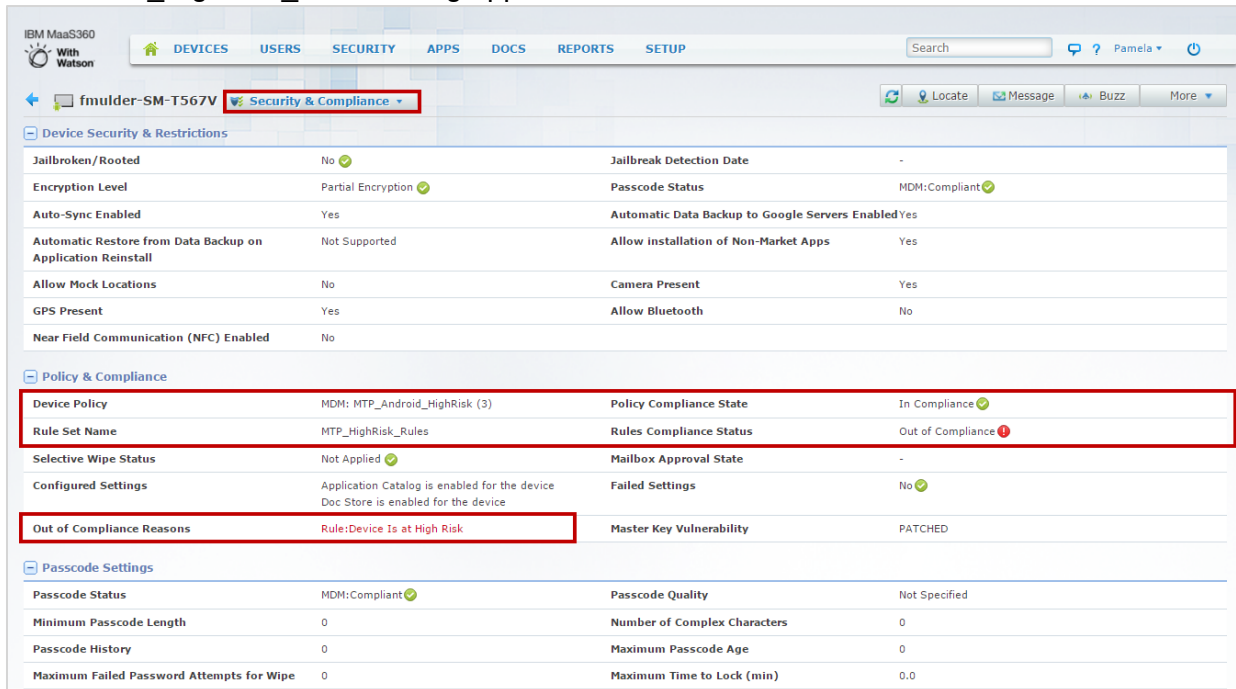
WorkPlace & Security

Managed Status	Enrolled	Applied Policy	MDM: MTP_Android_HighRisk (3)
Last Reported	05/18/2017 13:15 PDT	Android Blocked Permissions	-
Jailbroken/Rooted	No	Device Attestation Failed	No
Last Device Attestation Result	05/18/2017 12:21 PDT	Factory Reset Protection	Not Supported
Failed Settings	No	Selective Wipe Status	Not Applied
Encryption Level	Partial Encryption	Passcode Status	MDM:Compliant
Policy Compliance State	In Compliance	Rules Compliance Status	Out of Compliance
Out of Compliance Reasons	Rule: Device Is at High Risk	Rule Set Name	MTP_HighRisk_Rules

Network Information

Phone Number	-	ICCID	-
Is Roaming	Not Enabled	International Data Roaming	Not Enabled
Home Carrier	-	Current Network Type	Not Available

- 6.4.4. Clicking on the “Summary” drop-down menu, the Administrator can choose “Security & Compliance” details. The Administrator can see that the device is “Out of Compliance” because of the device belongs to the “MTP_Android_HighRisk” policy, with the compliance rule of “Device is at High Risk” under the compliance rule set “MTP_HighRisk_Rules” being applied.



Device Security & Restrictions

Jailbroken/Rooted	No	Jailbreak Detection Date	-
Encryption Level	Partial Encryption	Passcode Status	MDM:Compliant
Auto-Sync Enabled	Yes	Automatic Data Backup to Google Servers Enabled	Yes
Automatic Restore from Data Backup on Application Reinstall	Not Supported	Allow installation of Non-Market Apps	Yes
Allow Mock Locations	No	Camera Present	Yes
GPS Present	Yes	Allow Bluetooth	No
Near Field Communication (NFC) Enabled	No		

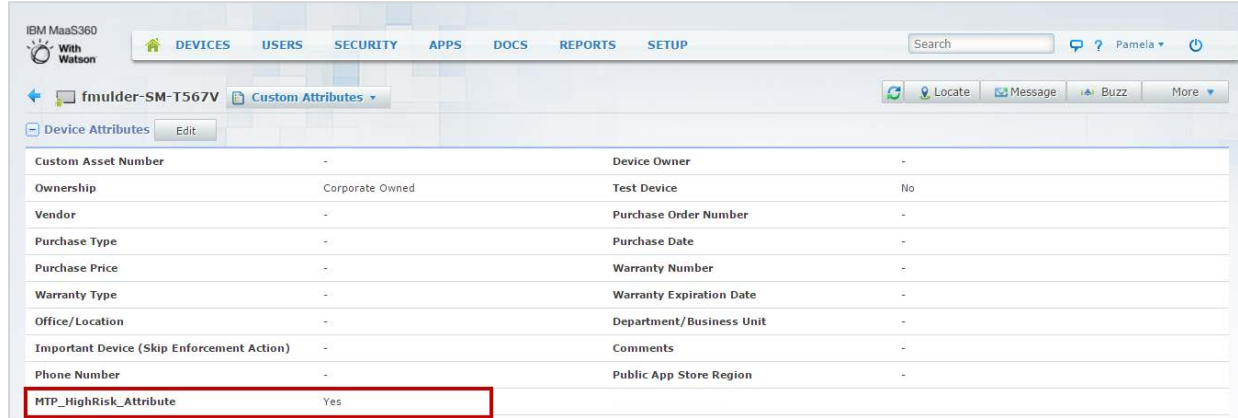
Policy & Compliance

Device Policy	MDM: MTP_Android_HighRisk (3)	Policy Compliance State	In Compliance
Rule Set Name	MTP_HighRisk_Rules	Rules Compliance Status	Out of Compliance
Selective Wipe Status	Not Applied	Mailbox Approval State	-
Configured Settings	Application Catalog is enabled for the device Doc Store is enabled for the device	Failed Settings	No
Out of Compliance Reasons	Rule: Device Is at High Risk	Master Key Vulnerability	PATCHED

Passcode Settings

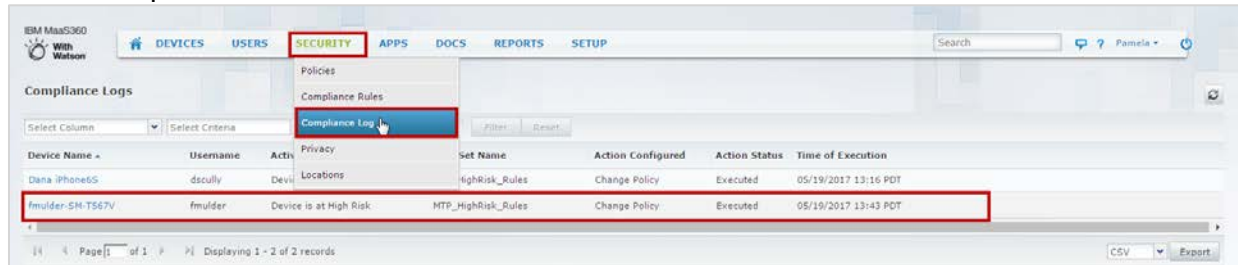
Passcode Status	MDM:Compliant	Passcode Quality	Not Specified
Minimum Passcode Length	0	Number of Complex Characters	0
Passcode History	0	Maximum Passcode Age	0
Maximum Failed Password Attempts for Wipe	0	Maximum Time to Lock (min)	0.0

- 6.4.5. Clicking on the “Security & Compliance” drop-down menu, the Administrator can choose “Custom Attributes” details. The Administrator can see which custom attributes are currently set.
- 6.4.6. The Administrator can see that the device has the “MTP_HighRisk_Attribute” set to “Yes”.



Device Attributes	
Custom Asset Number	-
Ownership	Corporate Owned
Vendor	-
Purchase Type	-
Purchase Price	-
Warranty Type	-
Office/Location	-
Important Device (Skip Enforcement Action)	-
Phone Number	-
MTP_HighRisk_Attribute	Yes
Device Owner	-
Test Device	No
Purchase Order Number	-
Purchase Date	-
Warranty Number	-
Warranty Expiration Date	-
Department/Business Unit	-
Comments	-
Public App Store Region	-

- 6.4.7. Navigating to **Security > Compliance Logs**, the Administrator can view the active “Compliance Events”.



Device Name	Username	Action	Set Name	Action Configured	Action Status	Time of Execution
Dana iPhone6S	dscully	Locations	HighRisk_Rules	Change Policy	Executed	05/19/2017 13:16 PDT
fmulder-SM-T567V	fmulder	Device is at High Risk	MTP_HighRisk_Rules	Change Policy	Executed	05/19/2017 13:43 PDT

7 Appendices

7.1 SandBlast Mobile Communication Information

The following table describes the networking rules required to configure your security systems in order to allow the Solution's integration with your on premise systems (MDMs, syslog, etc.). If you do not know your SandBlast Mobile Dashboard's region, please contact alm@checkpoint.com, or alternatively, perform the procedure in Section 7.2.

Description	Source	Destination	Port	Region
Connection to customer's MDM (EU)	52.51.115.5 52.31.98.20 52.30.229.13 52.51.47.83	Customer MDM and/or UDM	443	EU
Connection to customer's MDM (US)	54.84.231.79 54.84.219.180 52.6.231.218 52.0.129.11 52.71.46.86 52.203.42.126 52.202.99.13	Customer MDM and/or UDM	443	US
Connection to Customer's ArcSight/Syslog (EU)	52.51.115.5 52.31.98.20 52.30.229.13 52.51.47.83	Customer ArcSight/Syslog	Protocol and port as configured in the Dashboard Settings > Syslog screen	EU
Connection to Customer's ArcSight/Syslog (US)	54.84.231.79 54.84.219.180 52.6.231.218 52.0.129.11 52.71.46.86 52.203.42.126 52.202.99.13	Customer ArcSight/Syslog	Protocol and port as configured in the Dashboard Settings > Syslog screen	US
UDM connection to SandBlast Mobile (EU)	Customer UDM server	52.17.79.161	443	EU
UDM connection to SandBlast Mobile (US)	Customer UDM server	54.84.231.79 54.84.219.180 52.6.231.218 52.0.129.11 52.21.154.72	443	US
Connection to the customer's SMTP server if configured in SandBlast Mobile Dashboard (Settings > SMTP Settings)	52.1.198.108 52.7.158.188 52.202.99.13 52.71.46.86 52.203.42.126	Customer SMTP server	SMTP port configured in the Dashboard SMTP screen	Any

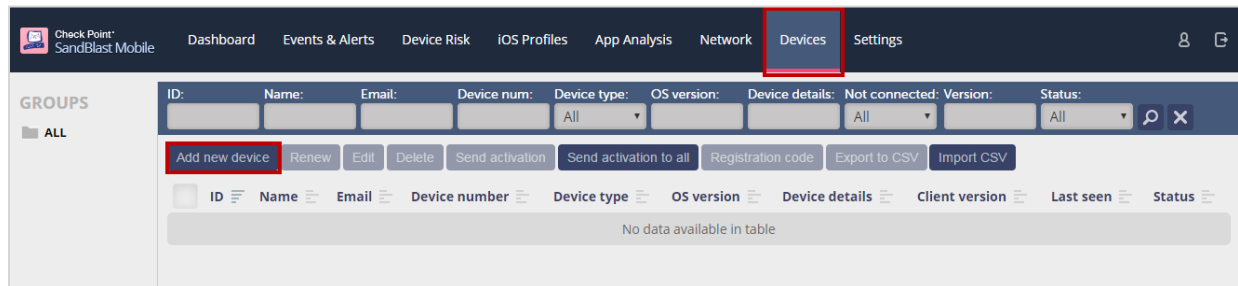
In order to prevent spam filters from blocking SandBlast Mobile's emails, the following IP address should be allowed as a sender: 167.89.59.134.

7.2 Discovering your SandBlast Gateway Name and Region

If you do not know your SandBlast Mobile Dashboard's region, please follow these instructions.

Note: These instructions must be done prior to configuring the Device Management Settings in the SandBlast Mobile Dashboard.

- 7.2.1. Login to your SandBlast Mobile Dashboard.
- 7.2.2. Navigate to **Devices**.
- 7.2.3. Click the “Add new device” button to add a new device.



- 7.2.4. In the pop-up window, enter a name, enter your email address, and ensure that “Send registration email” is checked. Click the “ADD” button.

- 7.2.5. Retrieve your email. In the Device Registration email from mtp-register@checkpoint.com the Server Address will be listed.
 - 7.2.5.1. EU Region = eu-gw01.locsec.net
 - 7.2.5.2. US Region = us-gw01.locsec.net
- 7.2.6. Go back into the SandBlast Mobile Dashboard > **Devices**, select the device you just created, and click the “Delete” button. Confirm deletion of device.

7.3 Integration Information

MaaS360 API URL (Server)	
MaaS360 API Admin Username	
MaaS360 API Admin Password	
MaaS360 Billing ID (Corporate Identifier)	
MaaS360 API App ID (com.[Billing ID].api (such as com.33333300.api))	
MaaS360 API Access Key	
MaaS360 Device Group(s)	
MaaS360 Device Custom Attribute	
SandBlast Mobile Gateway	
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