Check Point SandBlast Mobile

MDM Integration Guide with IBM MaaS360

Check Point
SOFTWARE TECHNOLOGIES LTD.

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

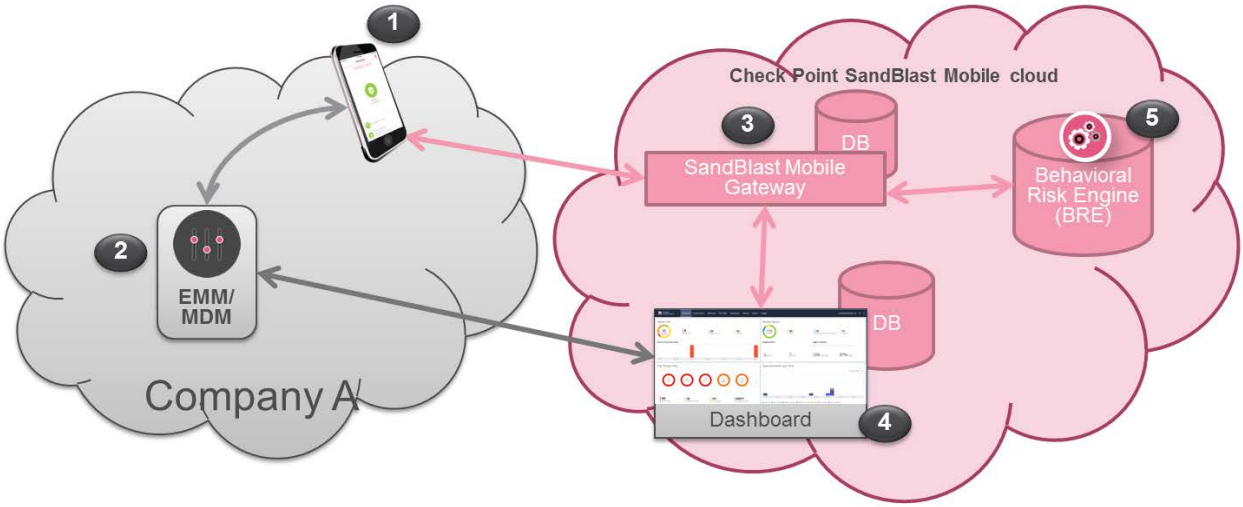
6 TESTING HIGH RISK ACTIVITY DETECTION AND POLICY ENFORCEMENT 67

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

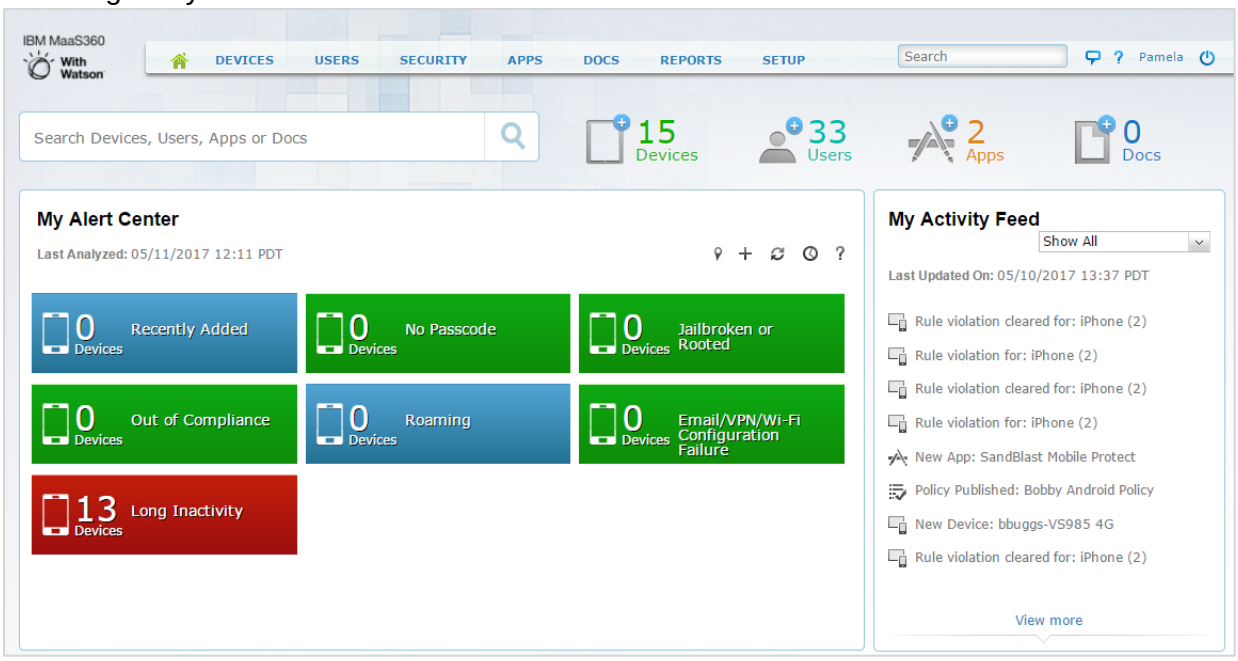
2.1 Prerequisites

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 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.

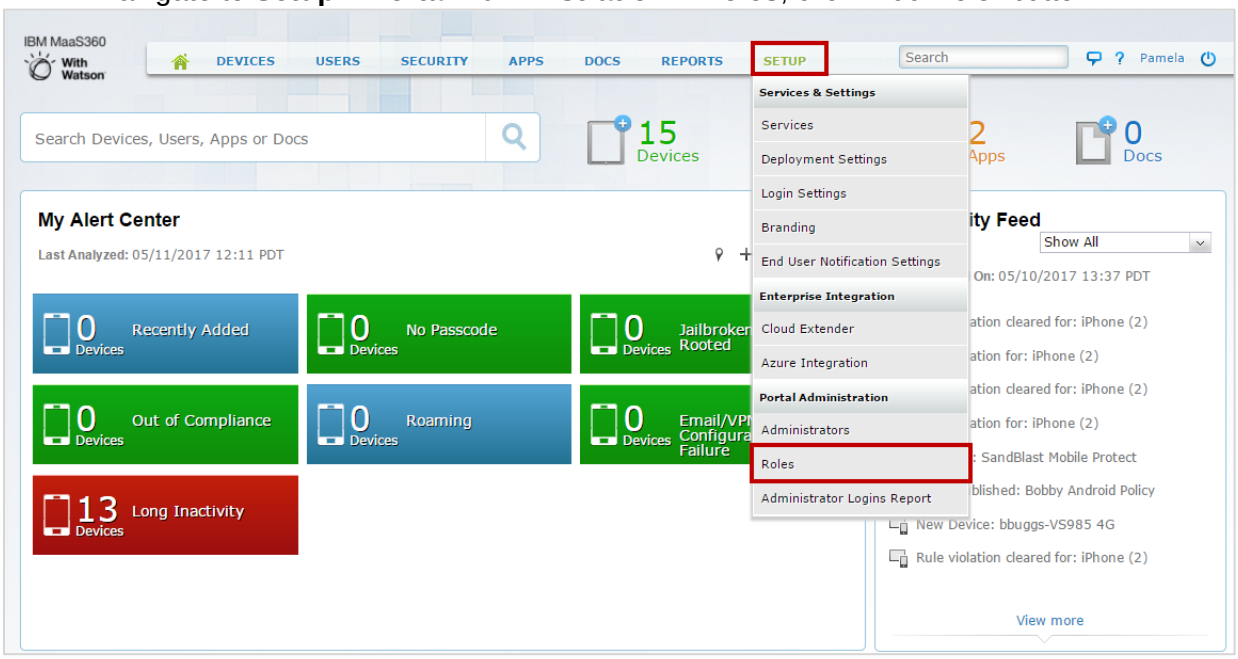
Note:	It is a best practice to create such an admin account and highly recommended, but is optional.

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

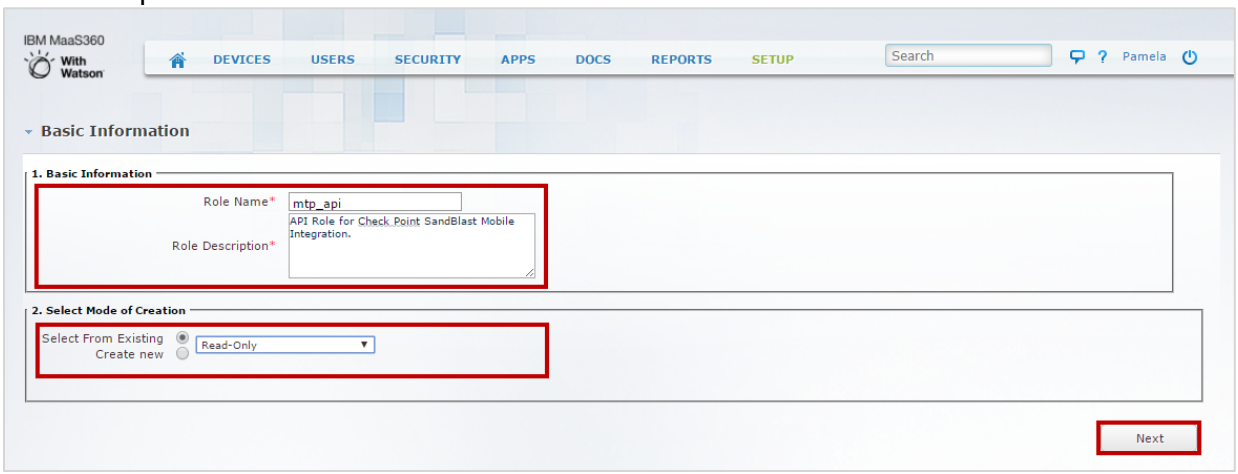
To create an “API” Administrator Account, follow this process.

2.3.1 Create a New API Only Administrator Role

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



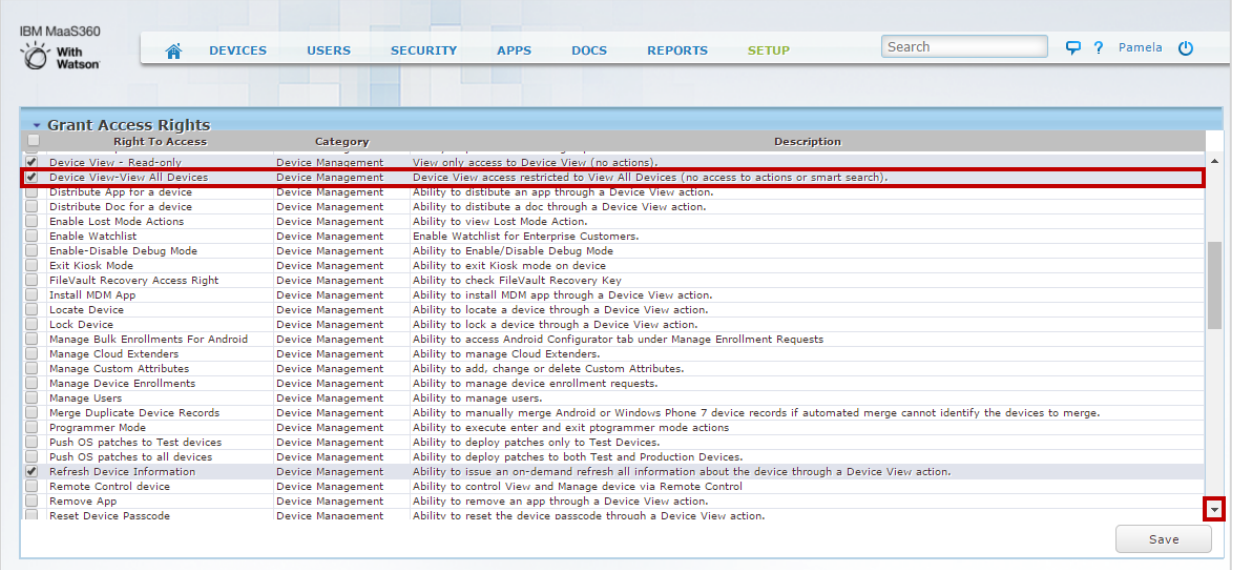
2.3.1.2. Enter in a Role Name, such as “mtp_api”, and a description, select the “Select From Existing” radio button for “Select Mode of Creation”, and choose “Read-Only” from the drop-down menu.

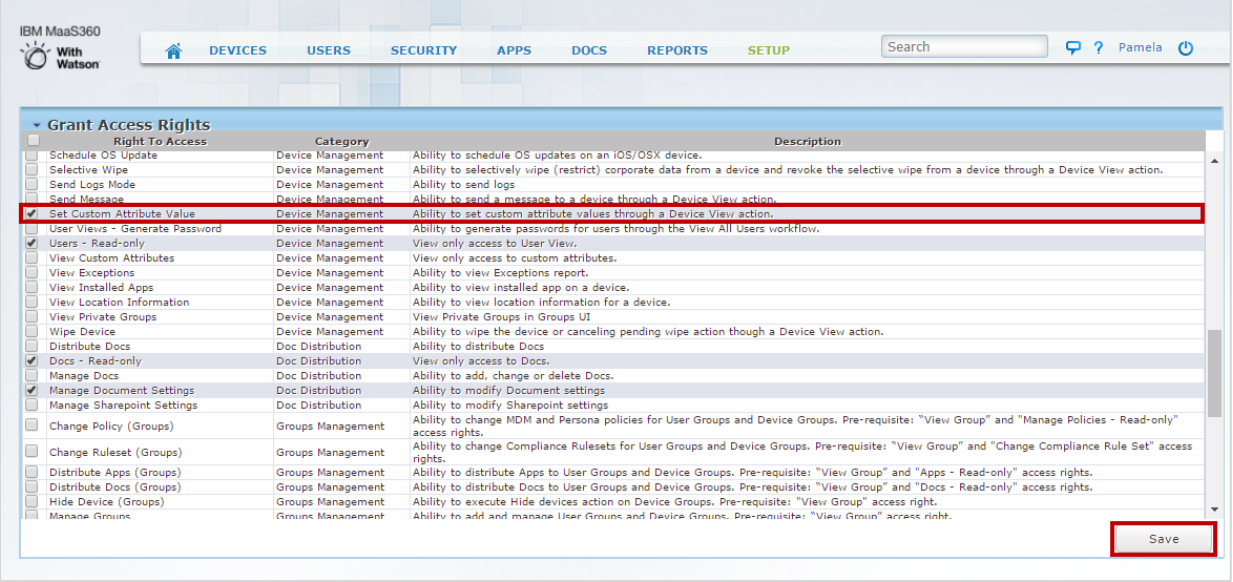


2.3.1.3. Click the “Next” button. The “Grant Access Rights” window is displayed.

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:

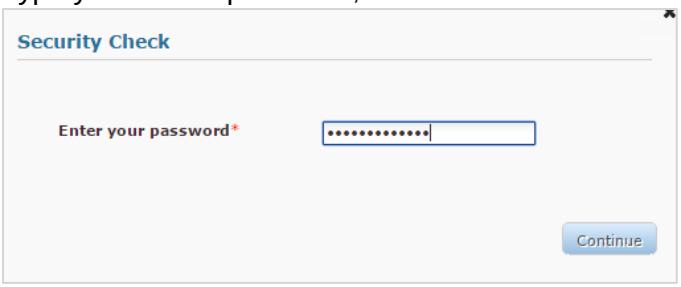
+ Device View – All Devices
+ Set Custom Attribute Value



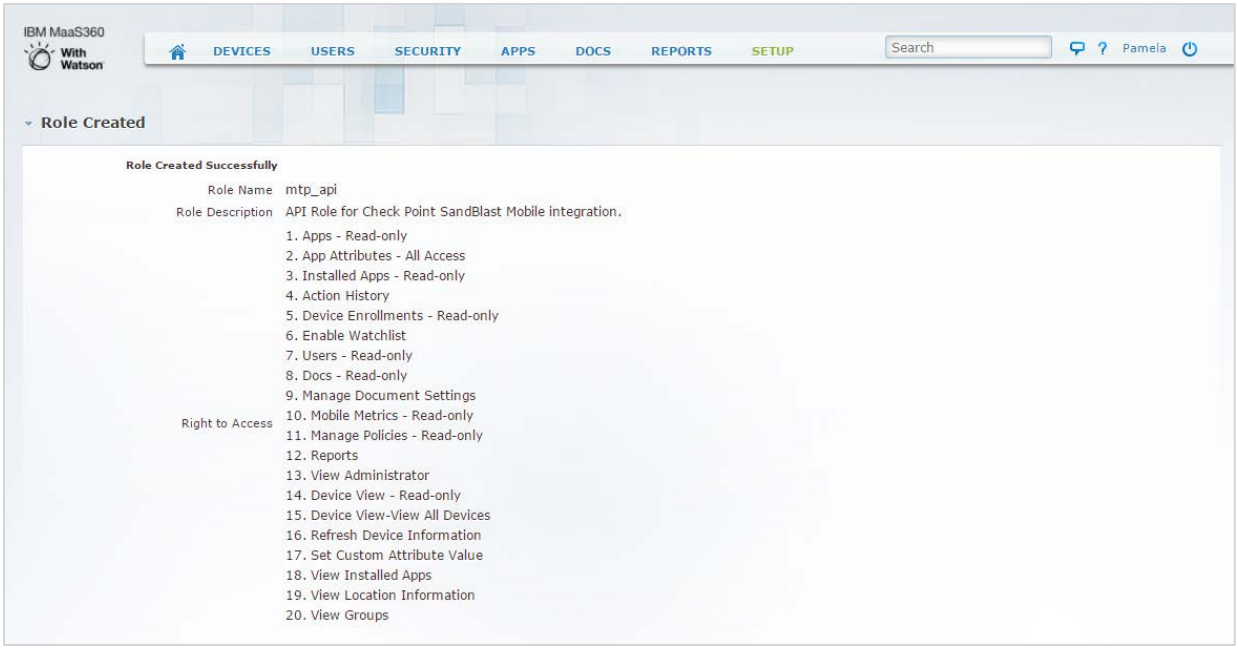


2.3.1.5. Click the “Save” button.

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

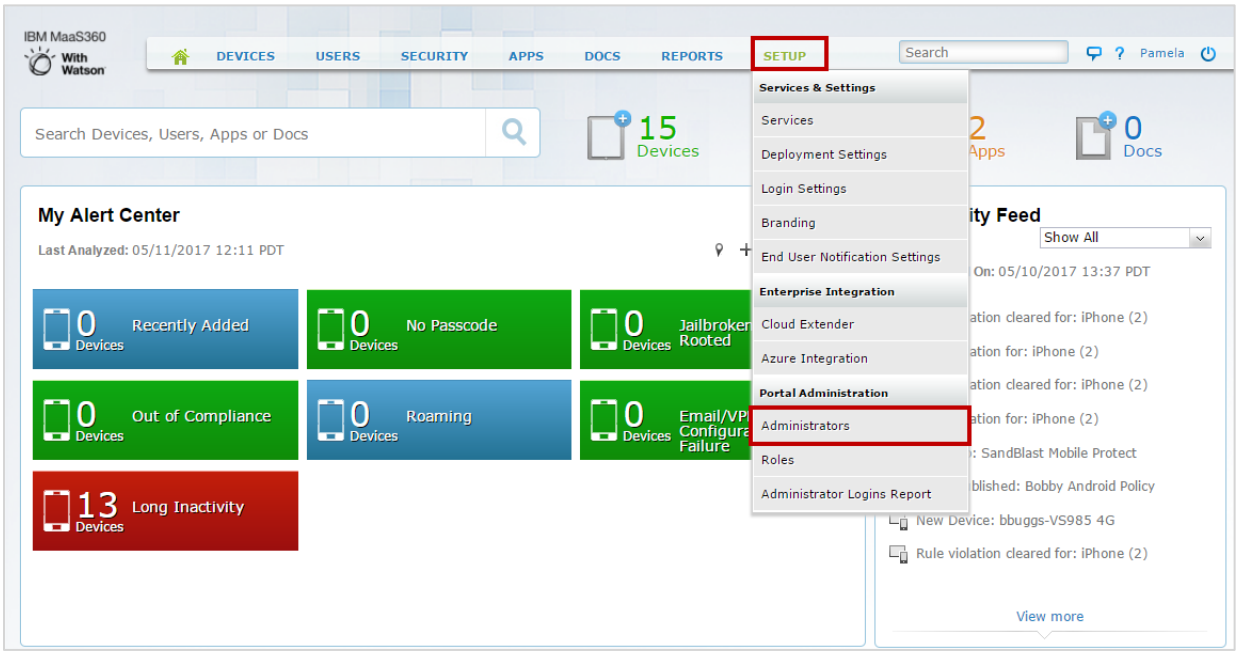


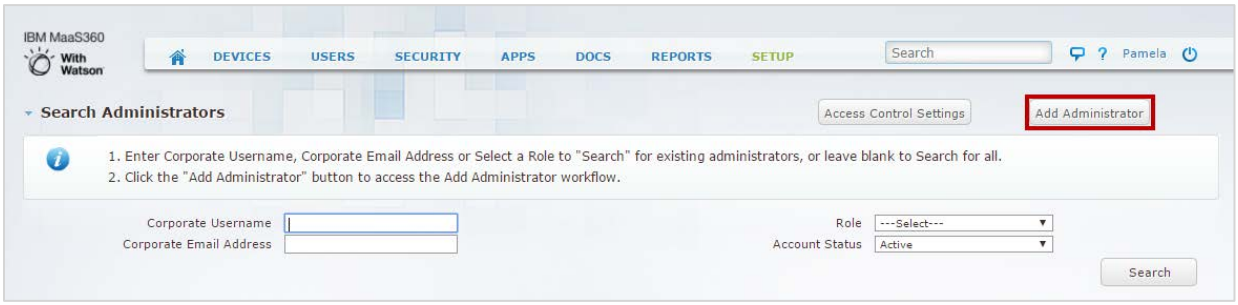
2.3.1.7. A confirmation message is displayed.



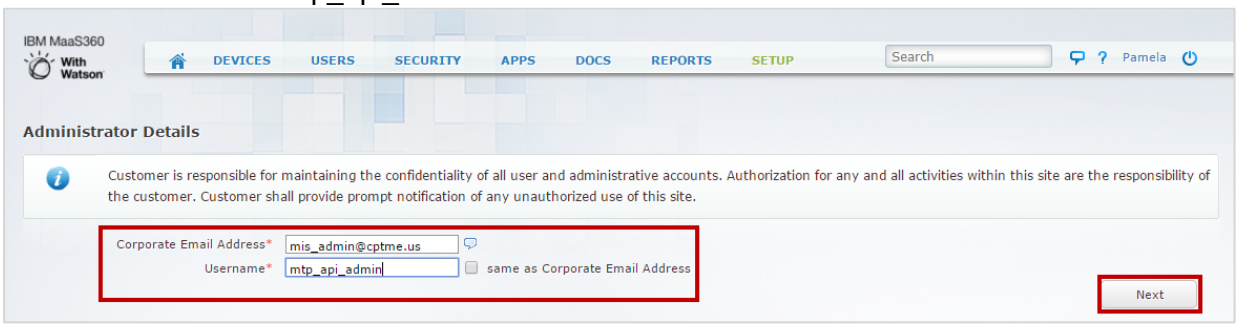
2.3.2 Create a New Administrator Account

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



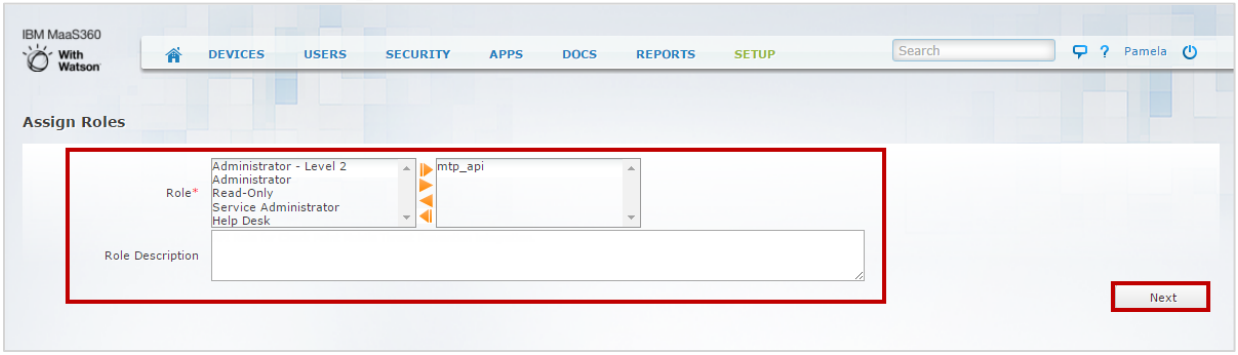


2.3.2.2. On the Administrator Details window, fill in the email address and the user name for the new administrator. If the user name is the same as the email address, select the “same as Corporate Email Address” checkbox. In our example, we will create an admin username of “mtp_api_admin”.



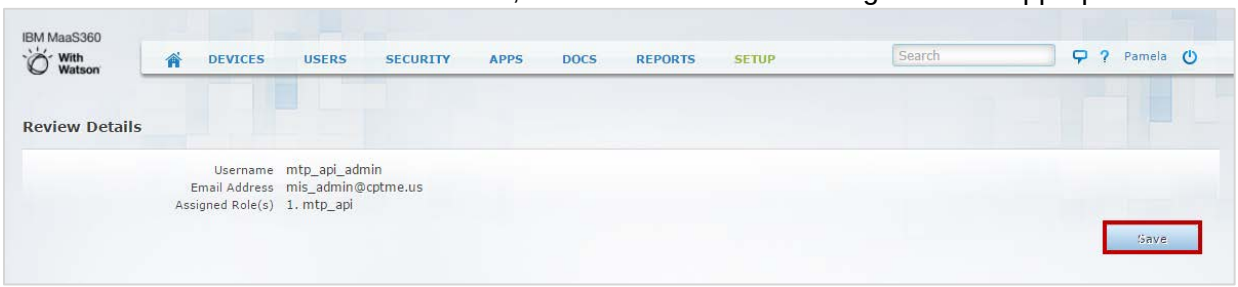
2.3.2.3. Click the “Next” button.

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”.



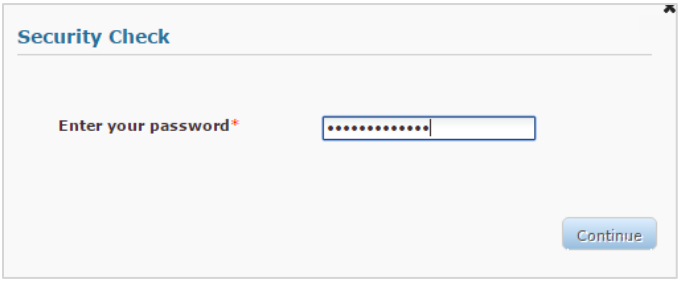
2.3.2.5. Click the “Next” button.

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

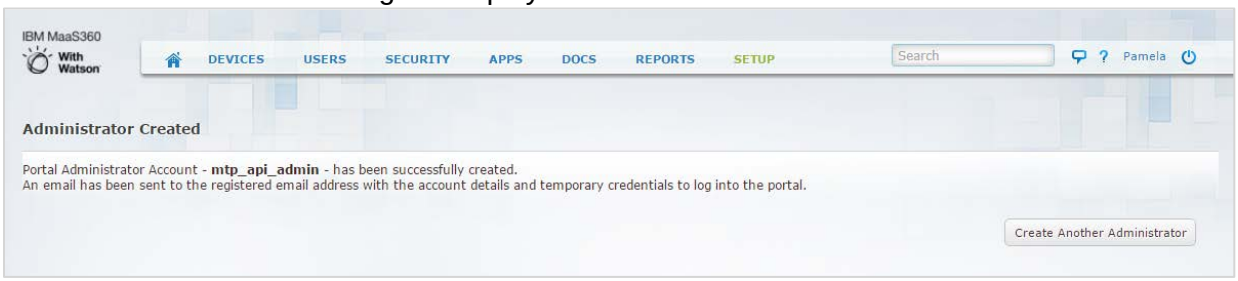


2.3.2.7. Click the “Save” button.

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

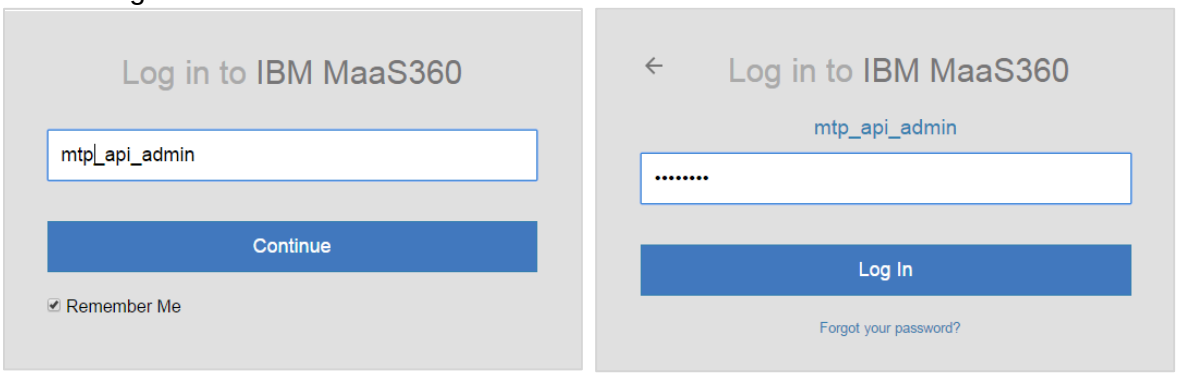


2.3.2.9. A confirmation message is displayed.

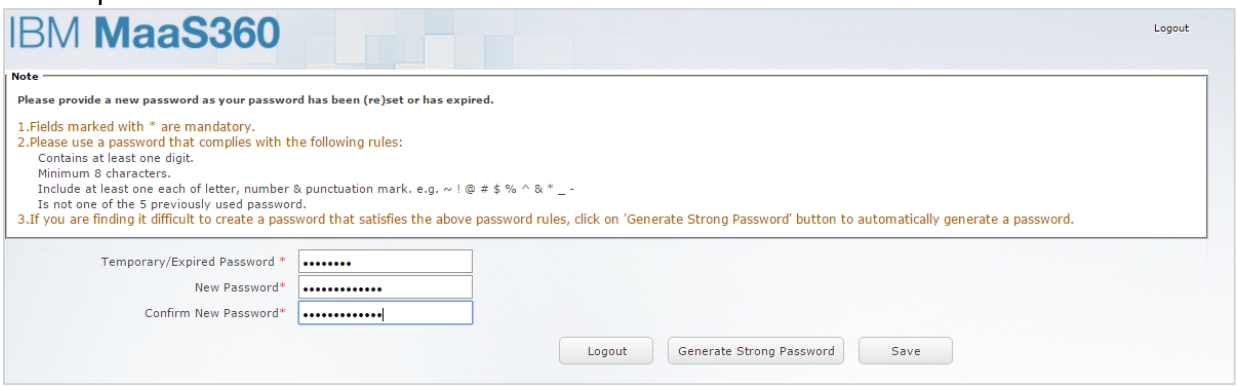


2.3.2.10. Finish the creation of the new admin account by logging out of the MaaS360 portal, and then logging back in using the credentials sent to the email address used for mtp_api_admin. This will force you to select a new unique password.

2.3.2.11. Log into MaaS360 Portal with the above credentials.

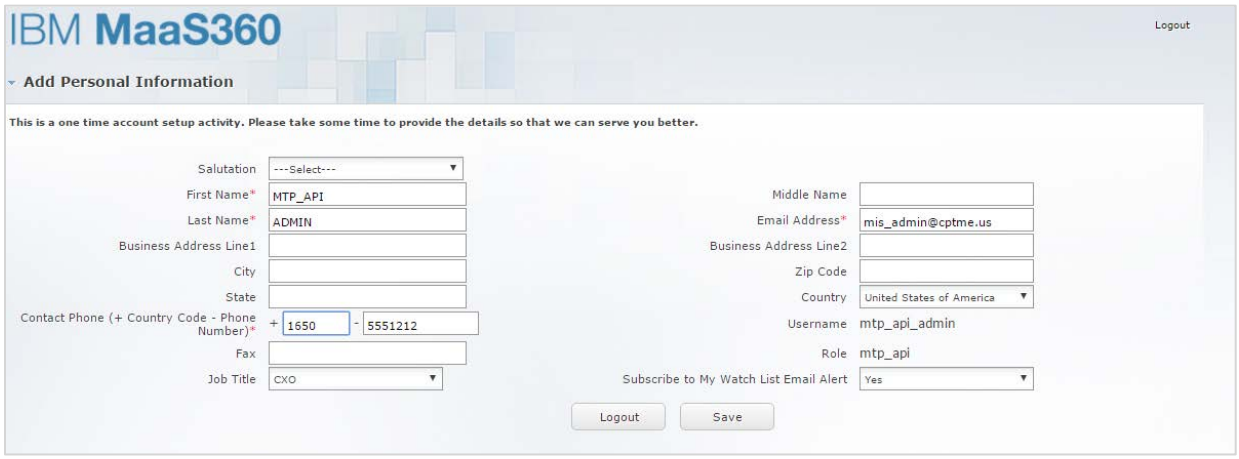


2.3.2.12. You are then prompted to select a new password. Enter a password that satisfies the password rules.

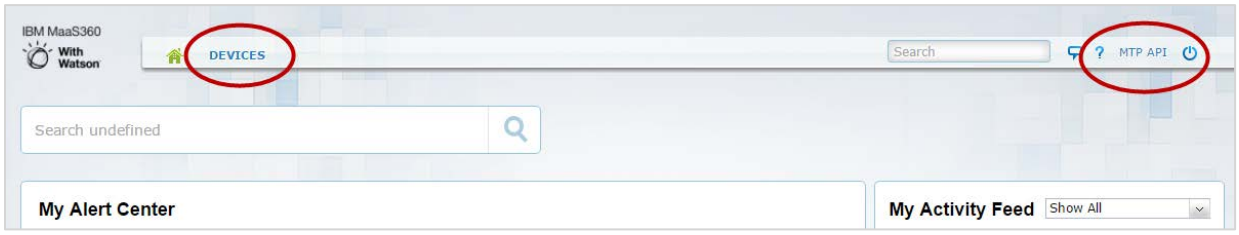


2.3.2.13. Click the “Save” button.

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.

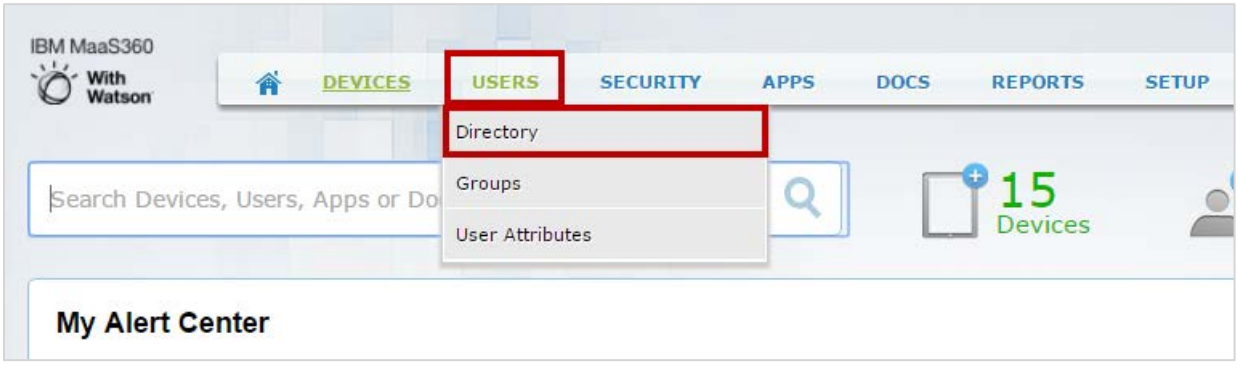
2.4 Adding a User

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

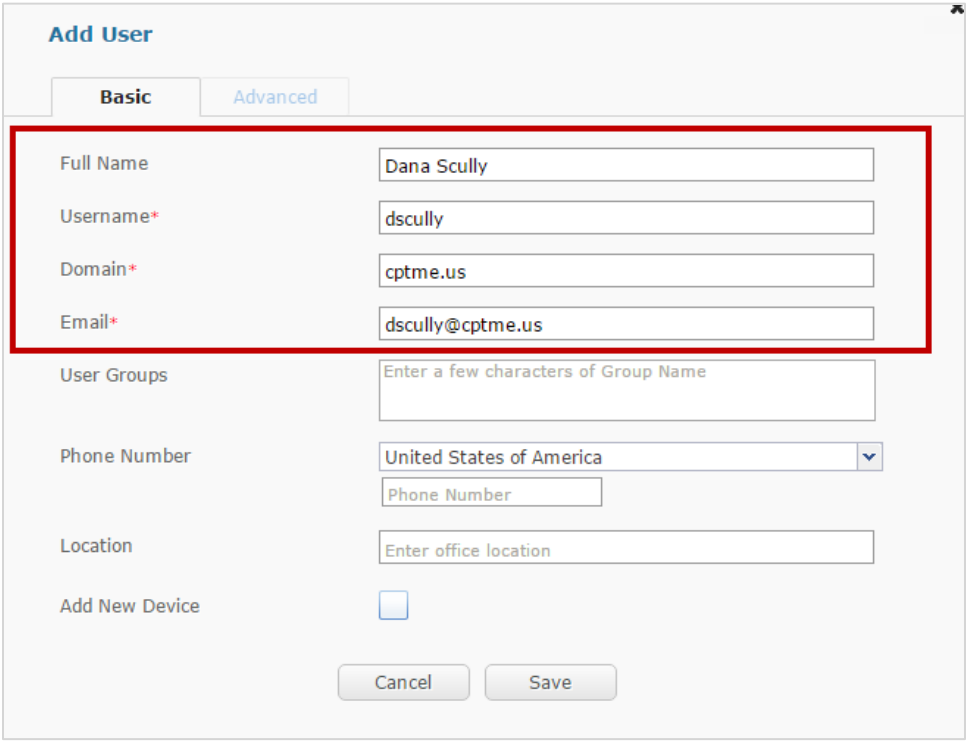
Note:	Use the Cloud Extender or Azure AD Integration to integrate with your Corporate User Directory to import group and associated user information. Cloud Extender is available for download on the Services enablement workflow. Azure AD Integration is available as part of Enterprise Integration. Imported 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.



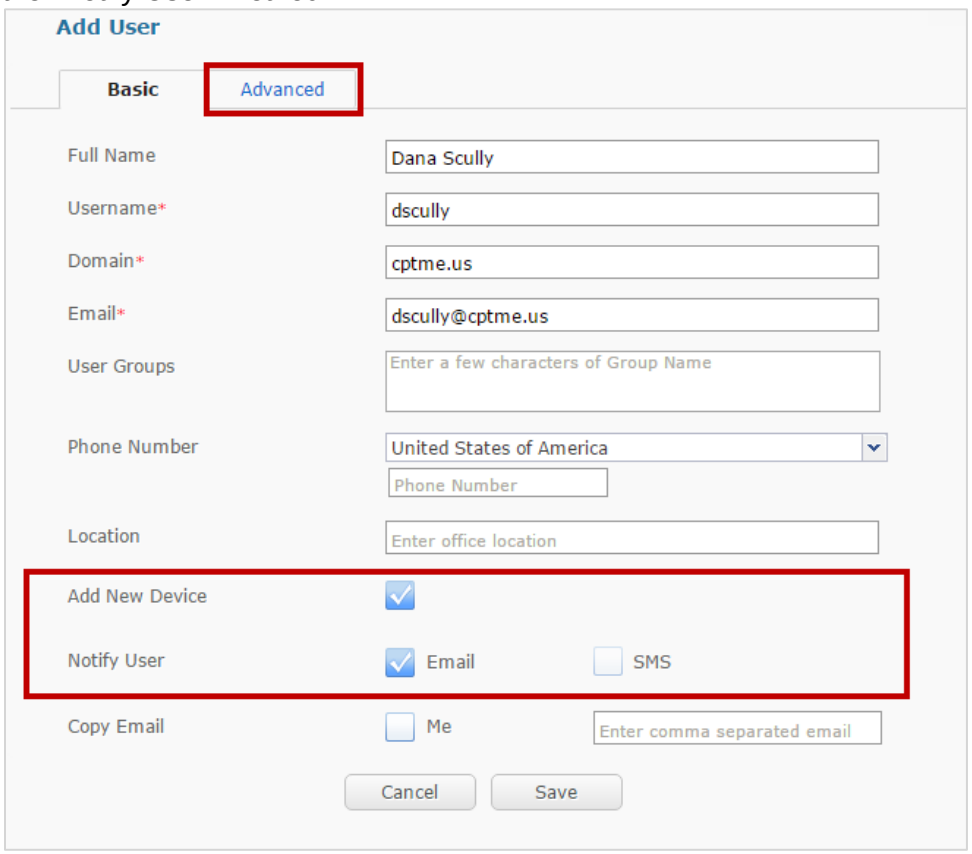
2.4.0.2. On the “Add User” pop-up window “Basic” tab, fill in all the required (*) fields with the appropriate information, such as in the example below.



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.

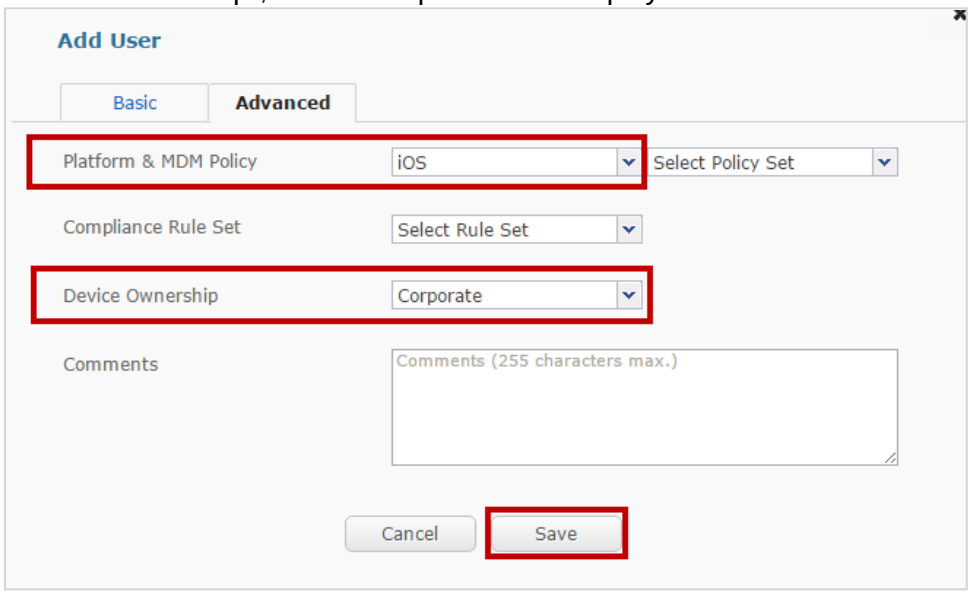
2.4.1 Adding a Device While Adding the User

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



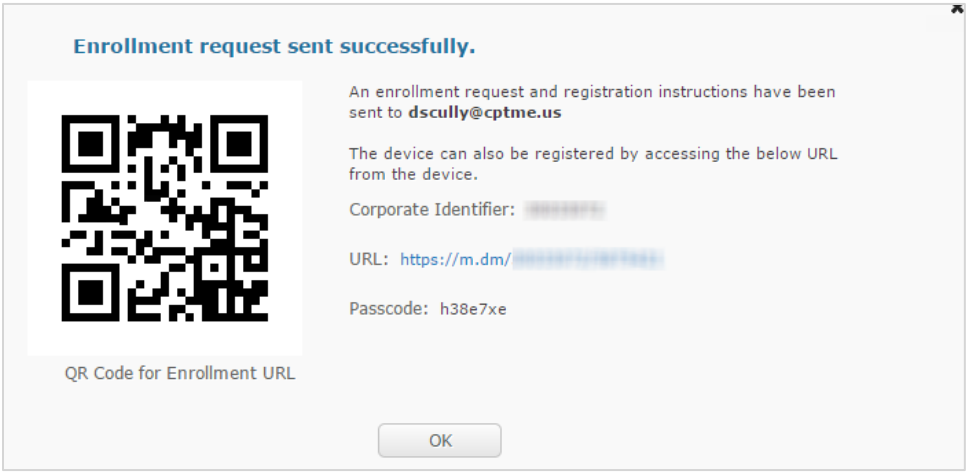
2.4.1.2. On the “Add User” pop-up window, click the “Advanced” tab.

2.4.1.3. On the “Advanced” tab, under “Platform”, select “iOS” or “Android”, and under the “Device Ownership”, select “Corporate” or “Employee Owned”.



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.

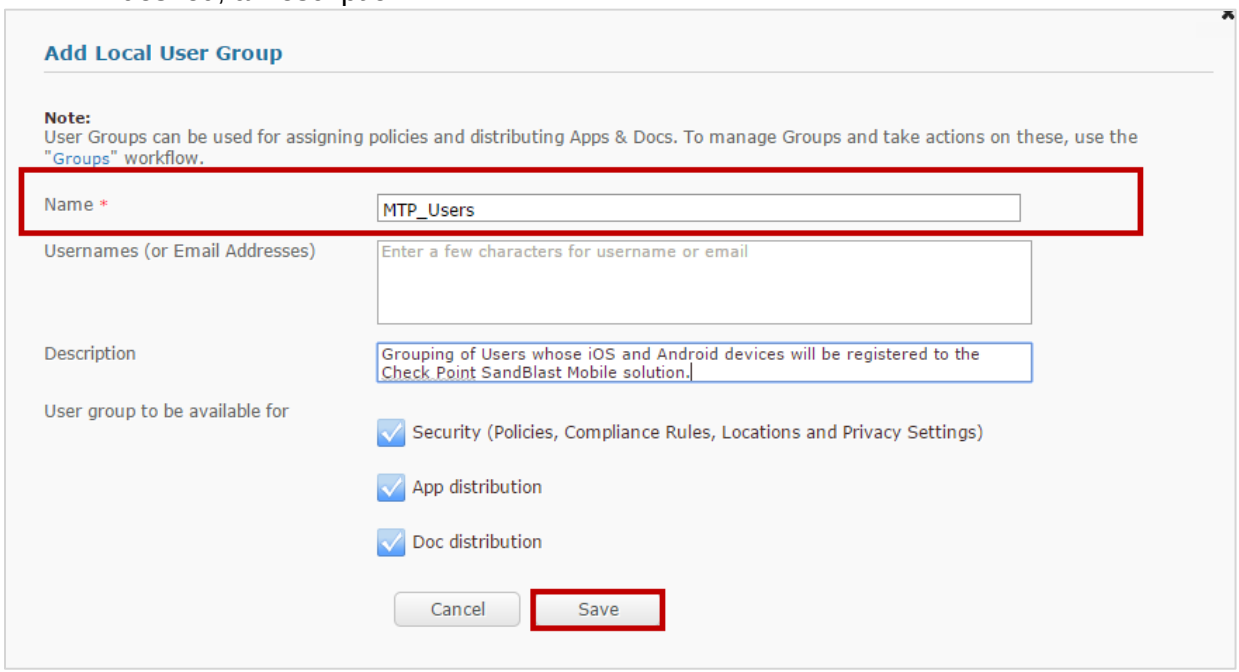
2.5 Creating a User Groups

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).

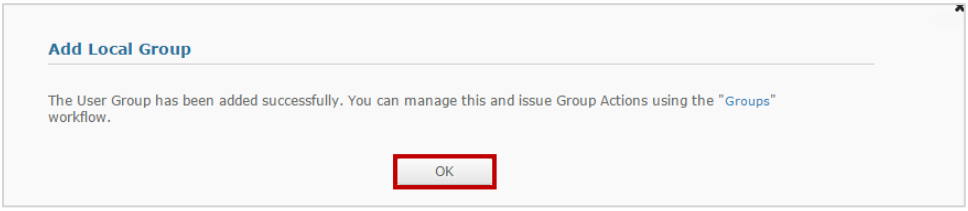
2.5.1 Creating a User Group

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

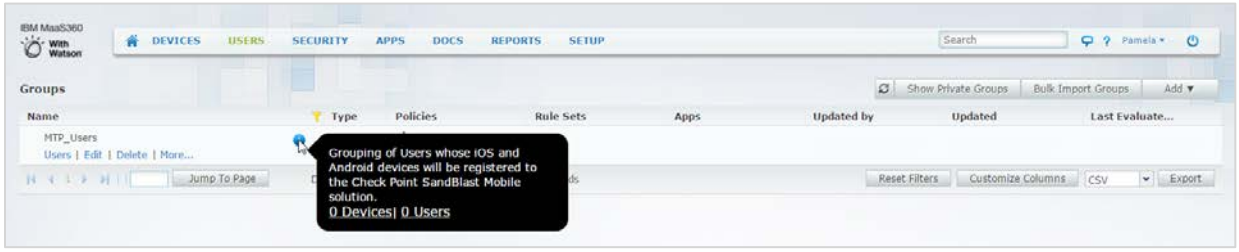
2.5.1.2. On the “Add Local Group pop-up window, enter in a Name, such as “MTP_Users”, and, if desired, a Description.



2.5.1.3. Click the “Save” button.



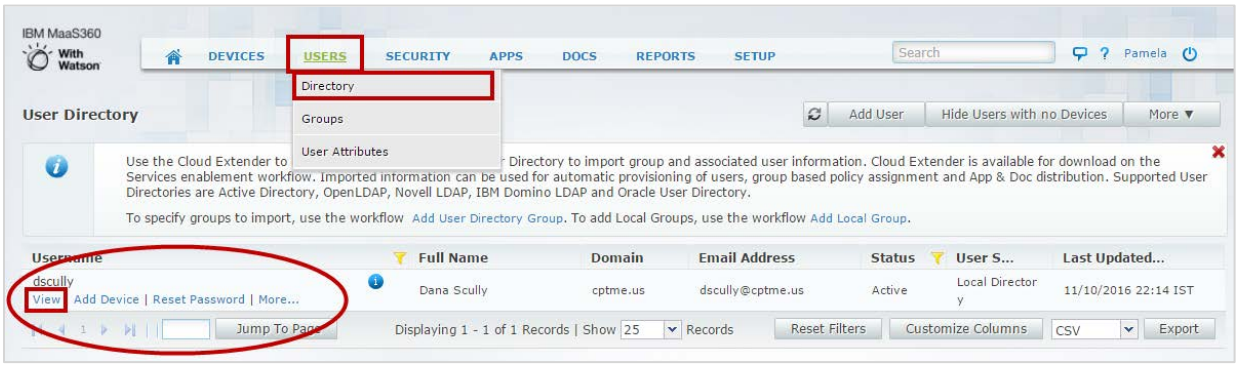
2.5.1.4. Click the “OK” button.



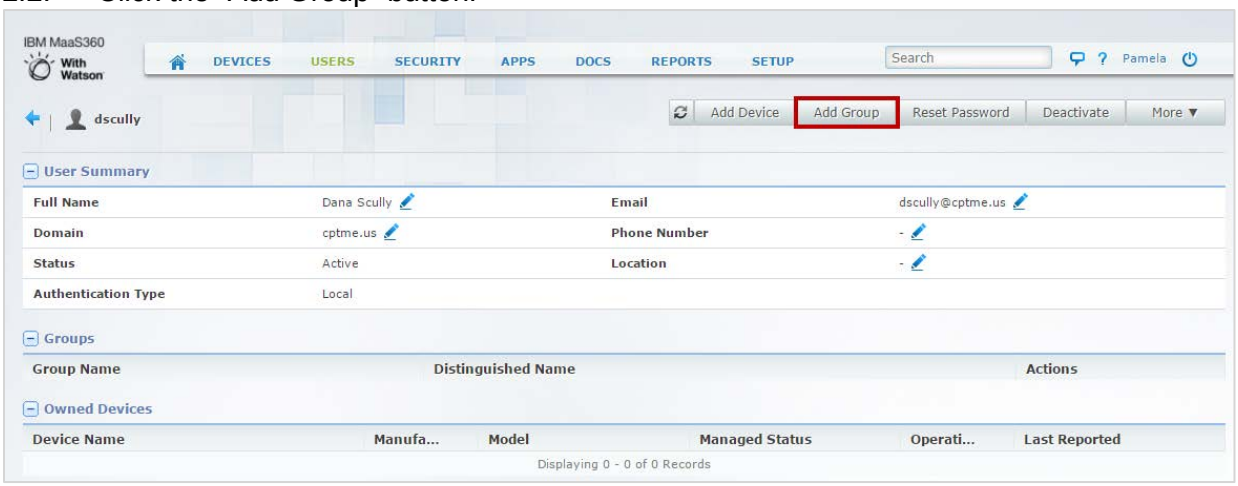
2.5.2 Adding an Existing User to a User Group

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

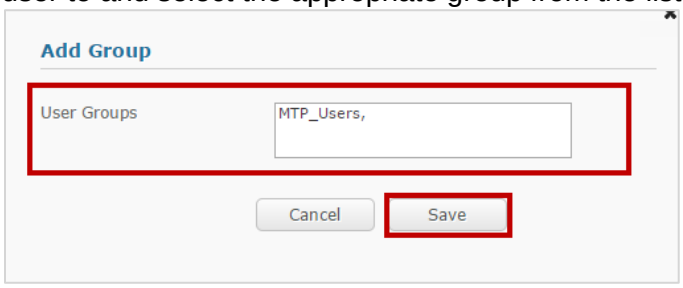
2.5.2.1. Navigate to **Users > Directory**, scroll to the user you want to add to a user group, and click the "View" link.



2.5.2.2. Click the "Add Group" button.

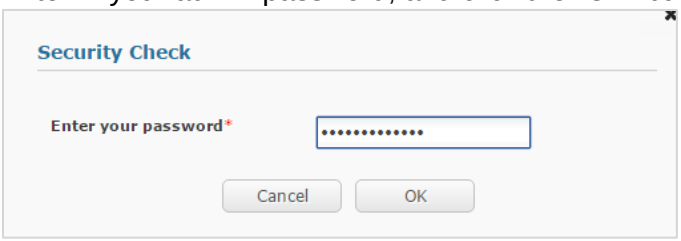


2.5.2.3. In the "Add Group" pop-up window, start typing the User Group you want to add the user to and select the appropriate group from the list, in our example "MTP_Users".

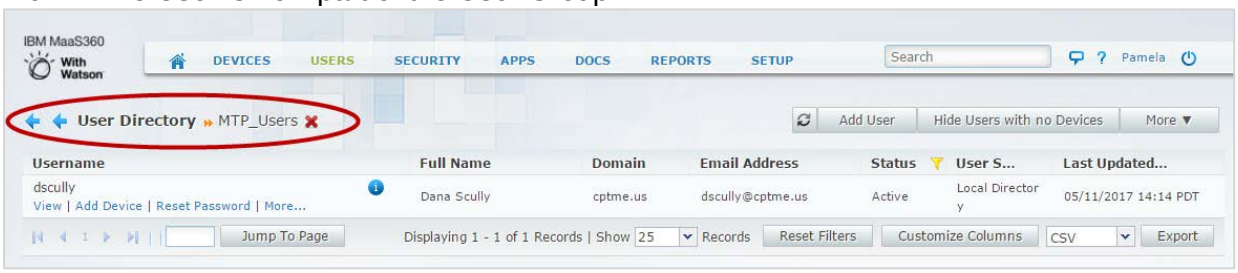


2.5.2.4. Click the "Save" button.

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



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



2.5.3 Adding a New User to an Existing User Group

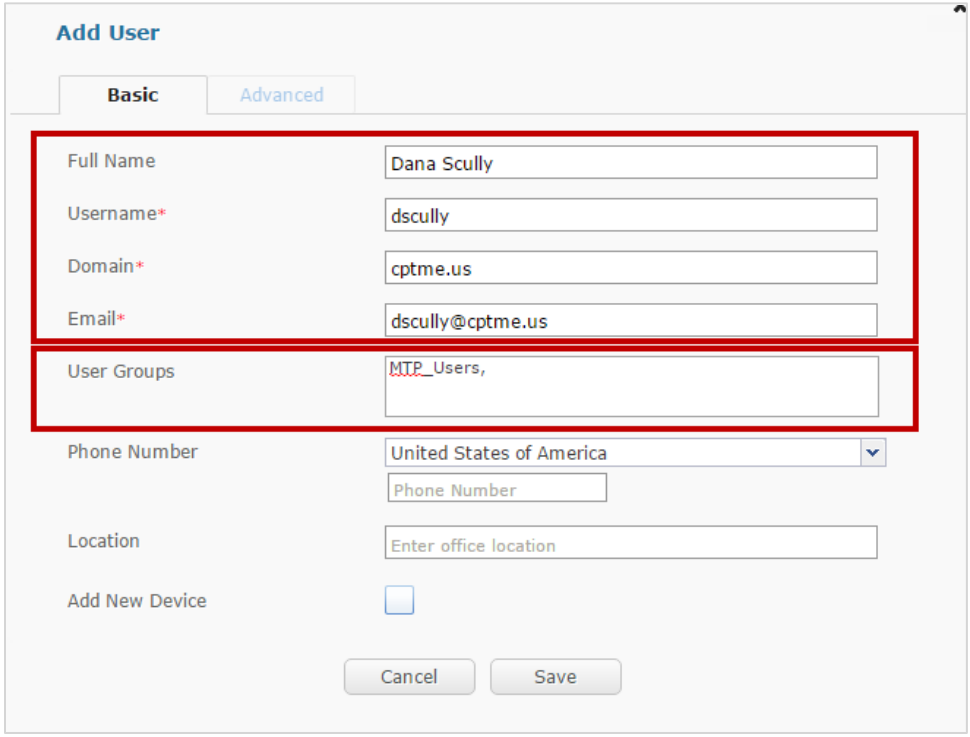
Adding a new user to an existing user group is close to the same procedure in Section 2.4.

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.

2.5.3.2. Click the “Add User” button.

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.

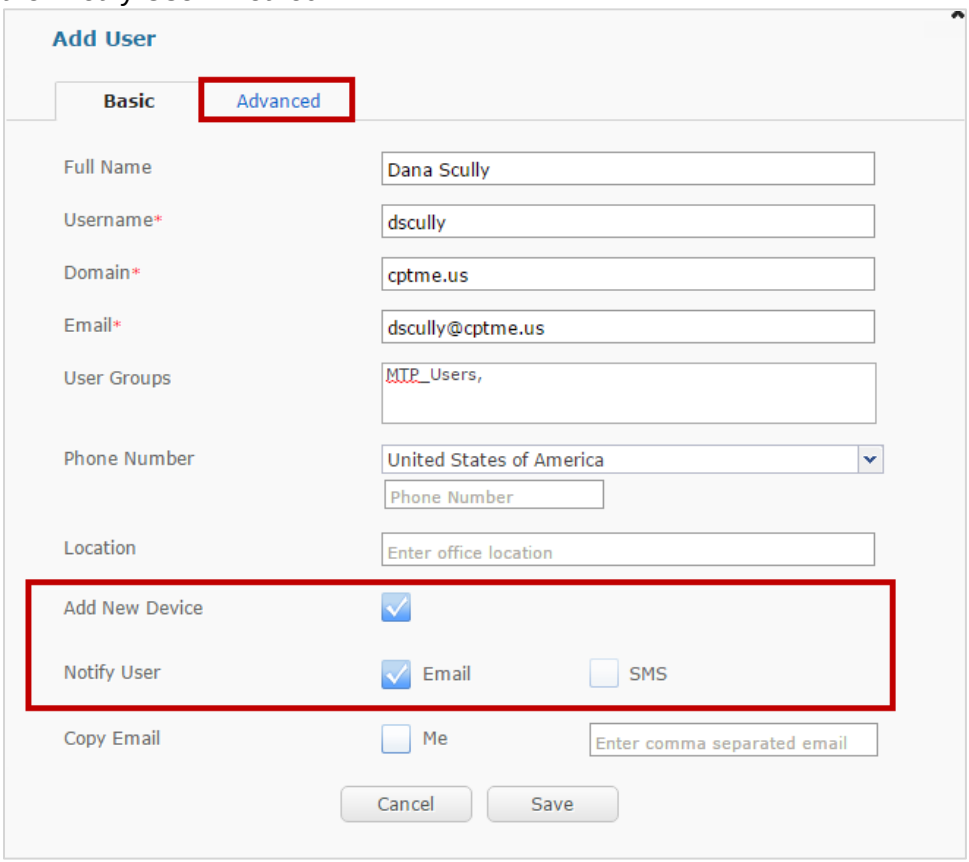
2.5.3.4. Also, enter in the user group in the “Users Groups” field, in our example “MTP_Users”



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.

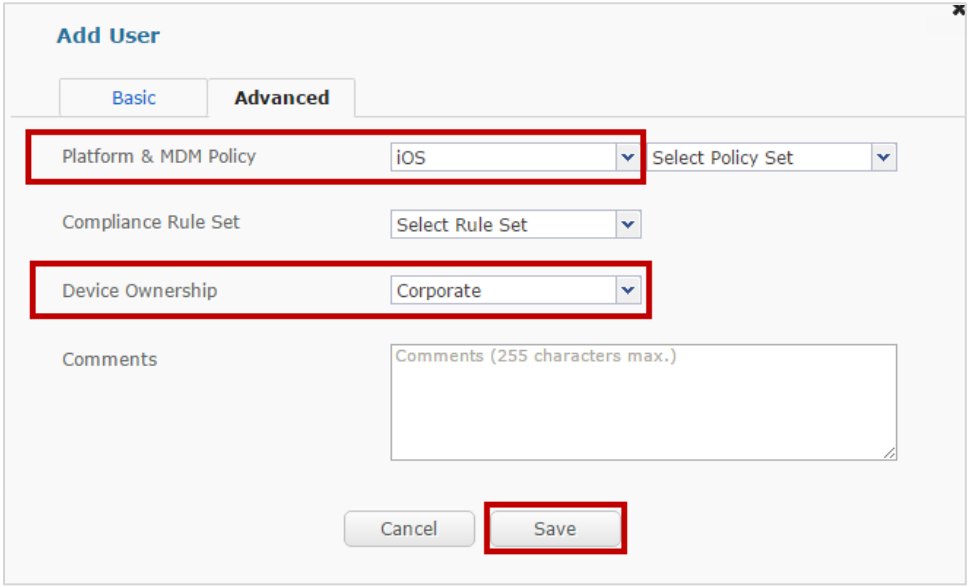
2.5.3.1 Adding a Device While Adding the User

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.



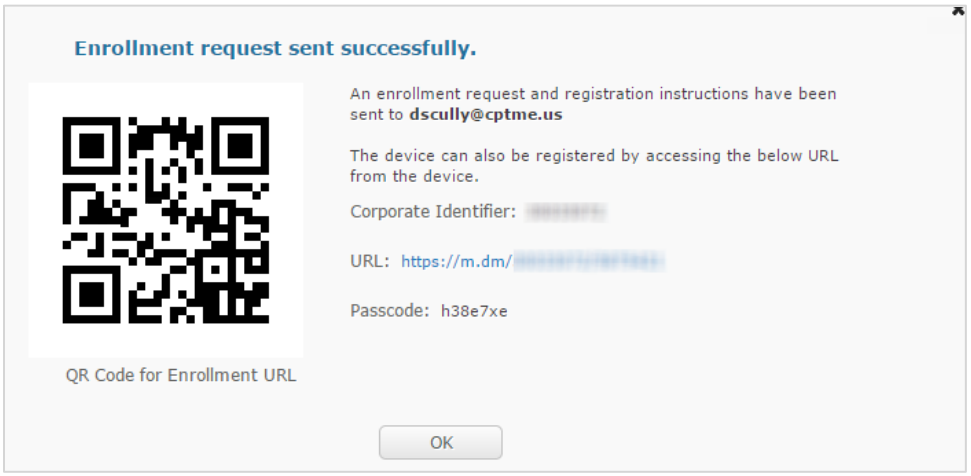
2.5.3.1.2. On the “Add User” pop-up window, click the “Advanced” tab.

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”.



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.



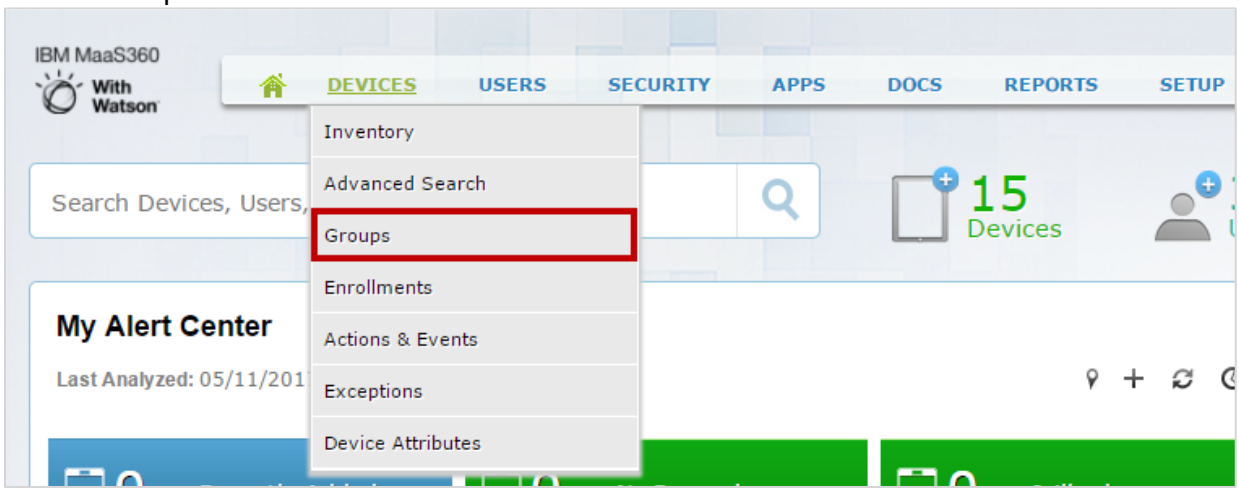
2.5.3.1.6. Click the “OK” button.

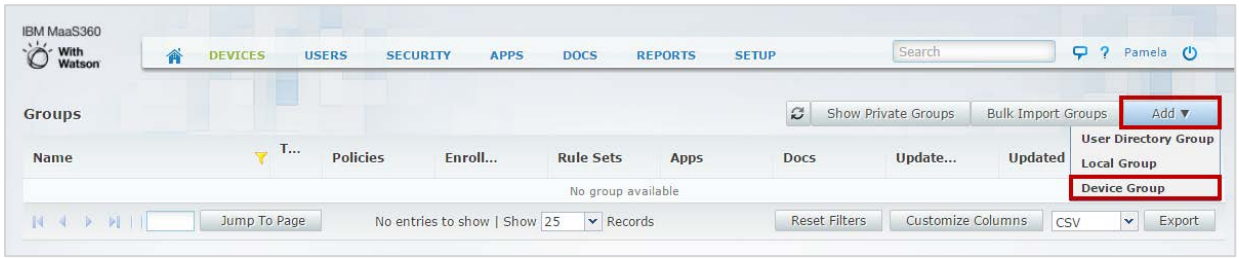
2.6 Creating a Device Provisioning Group

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

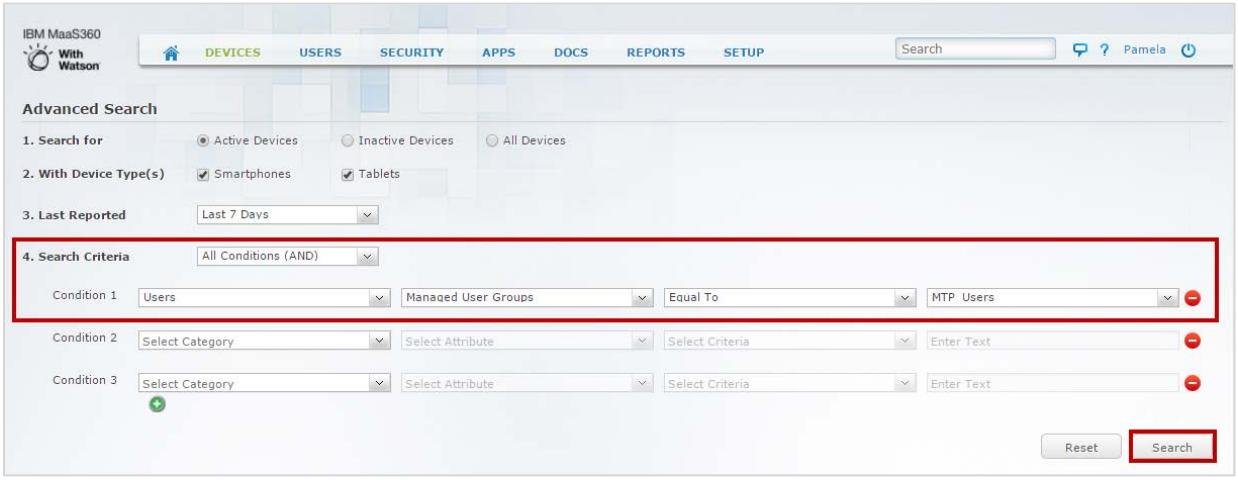
2.6.1.1. Navigate to **Devices > Groups**, click the “Add” drop-down button, and select “Device Group”.





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

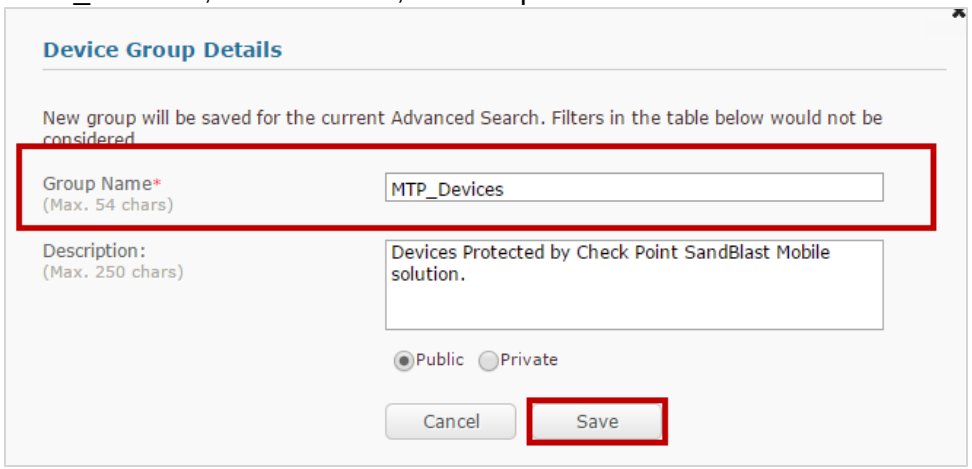
devices assigned to all “Users” in the “Managed User Groups” “Equal To” the User Group we created in the previous section, in our example “MTP_Users”.



2.6.1.3. Click the “Search” button.

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

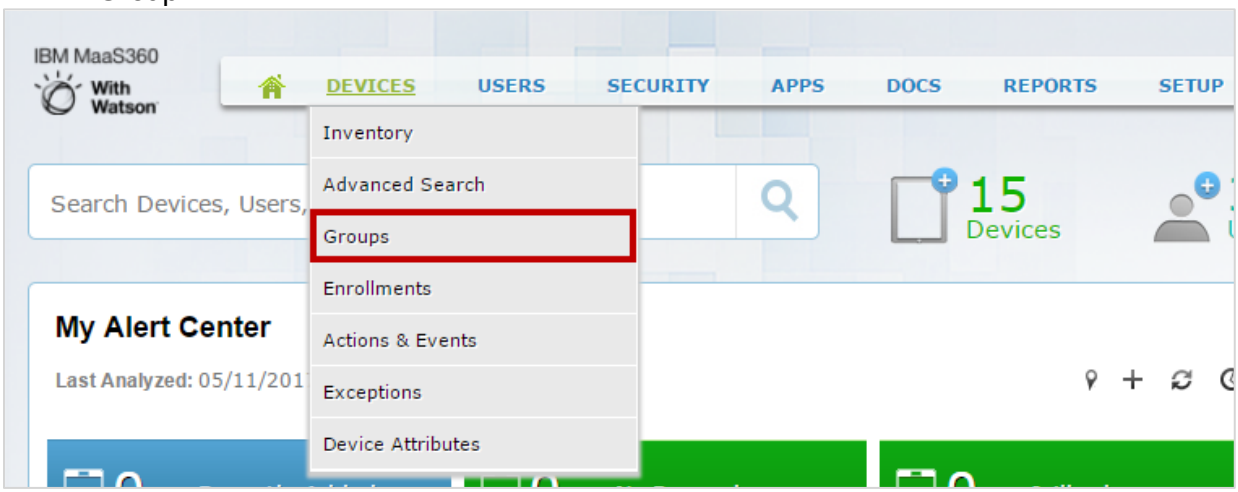
2.6.1.5. On the “Device Group Details” pop-up window, enter a Group Name, such as “MTP_Devices”, and if desired, a Description.

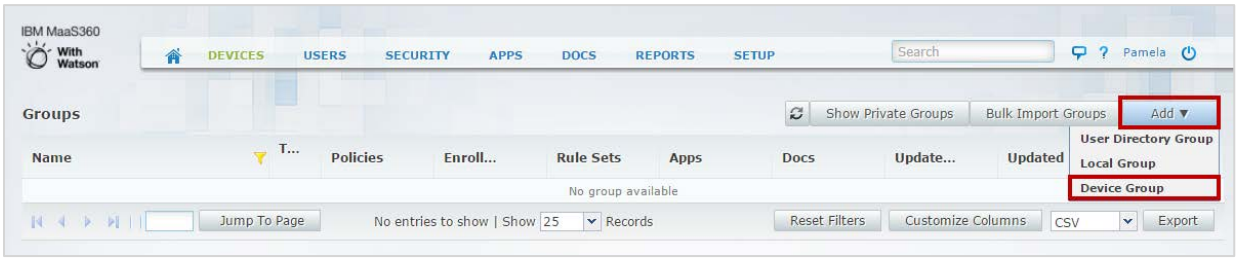


2.6.1.6. Click the “Save” button.

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.

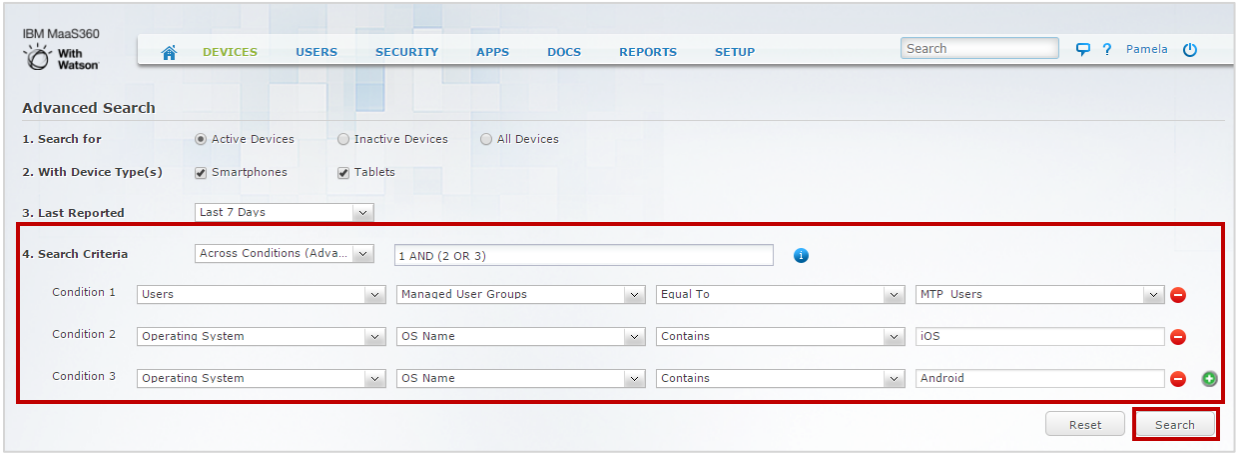
2.6.2.2.1. In our example, we will group all the devices assigned to all “Users” in the “Managed User Groups” “Equal To” the User Group we created in the previous section, in our example “MTP_Users”, then

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)”

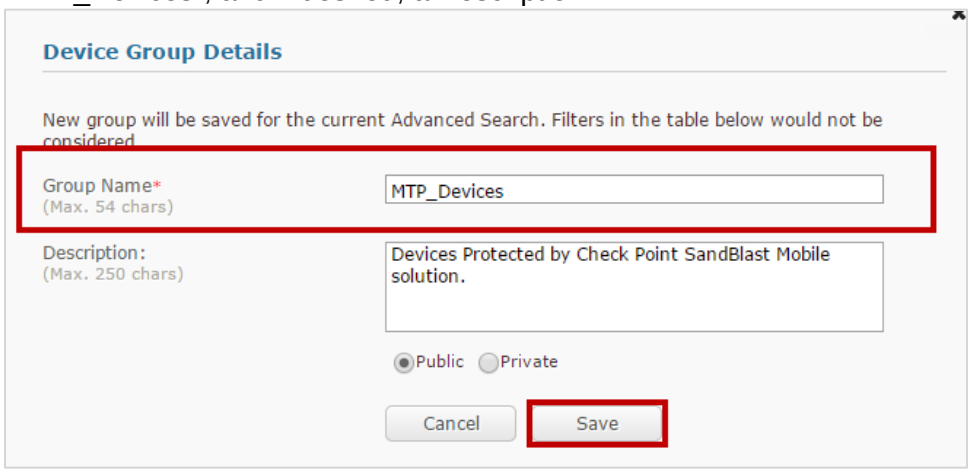
2.6.2.3. These criteria will match all iOS or Android devices belonging to the users that belong to the user group “MTP_Users”.



2.6.2.4. Click the “Search” button.

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

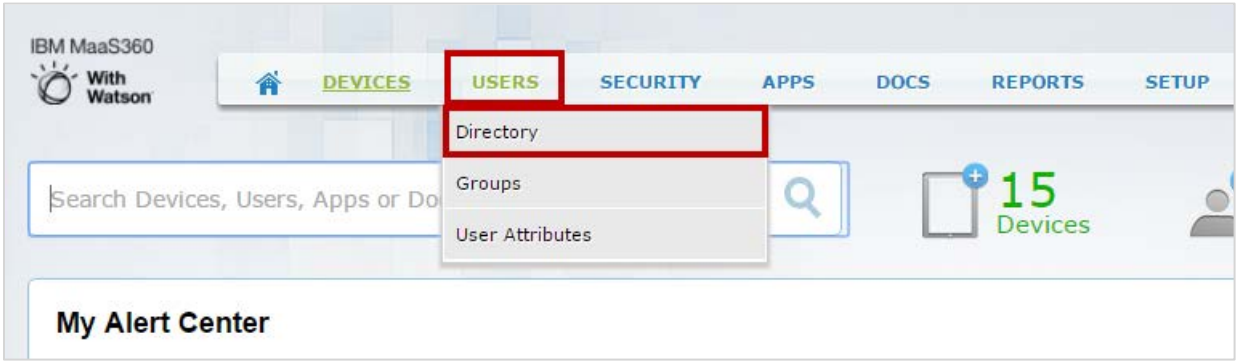
2.6.2.6. On the “Device Group Details” pop-up window, enter a Group Name, such as “MTP_Devices”, and if desired, a Description.



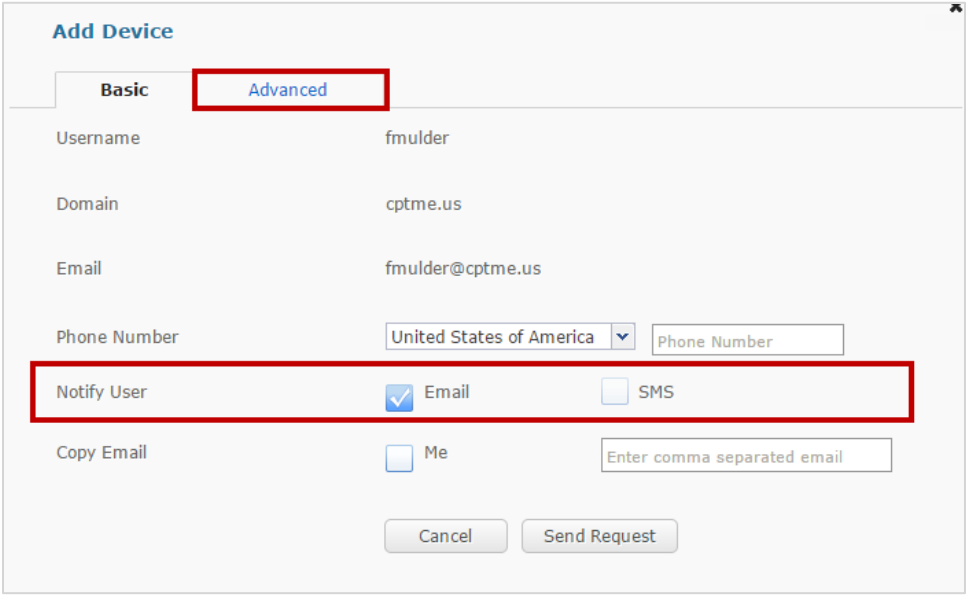
2.6.2.7. Click the “Save” button.

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.

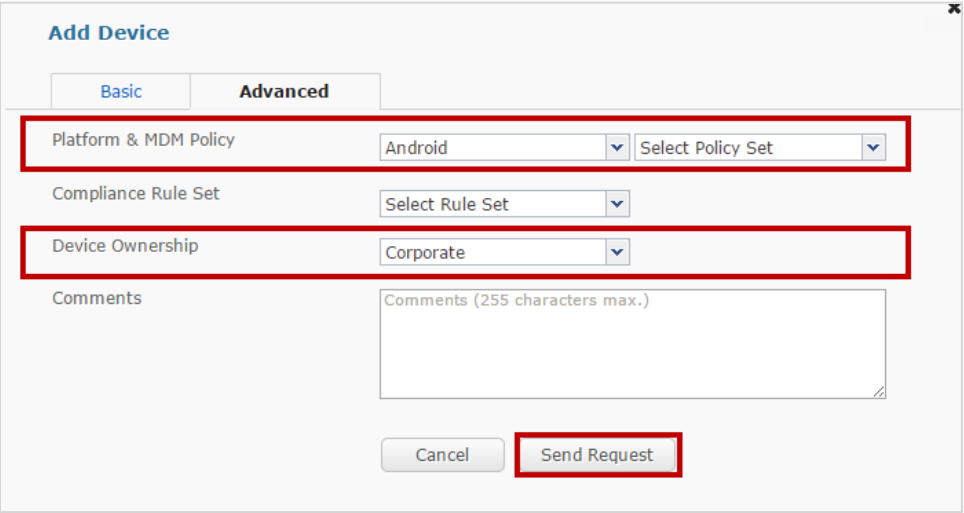


2.7.0.2. On the “Add Device” pop-up window “Basic” tab, select the “Notify User” method.



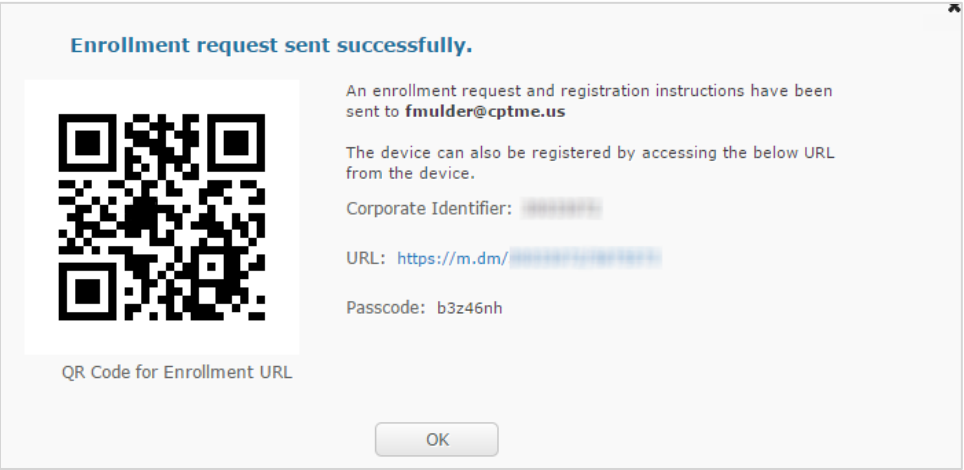
2.7.0.3. Click the “Advanced” tab.

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”.



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.

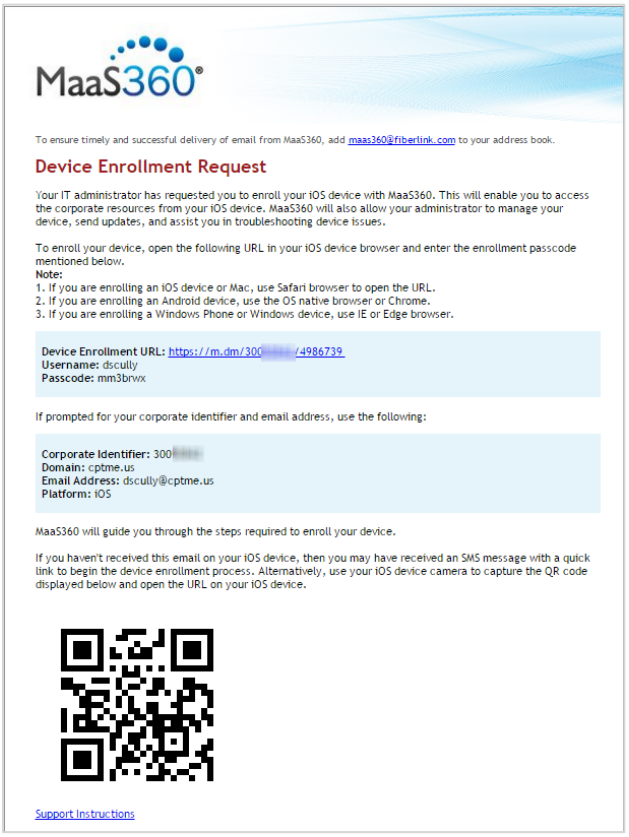


2.7.0.7. Click the “OK” button.

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.



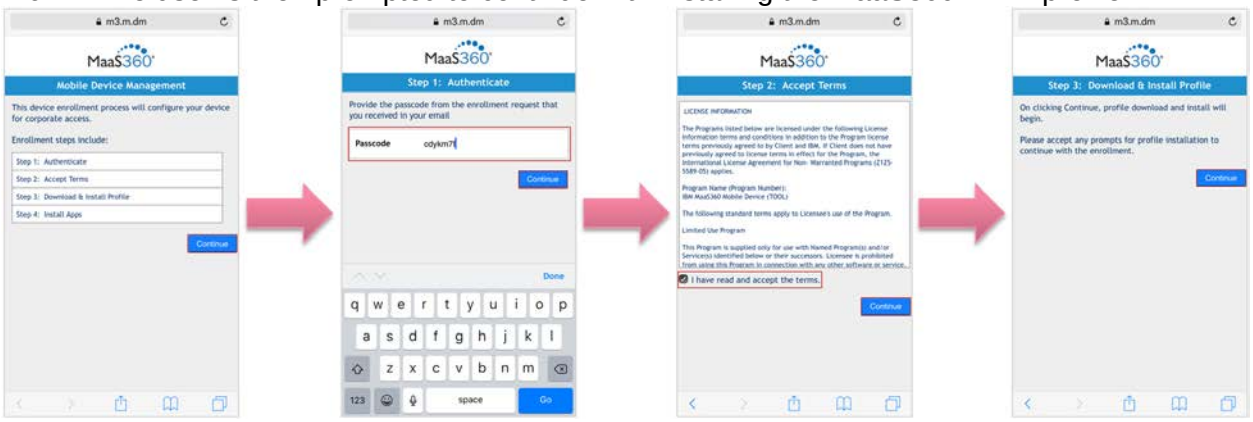
2.7.1.2. The user will open the “Device Enrollment URL” link in their device’s browser.

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.

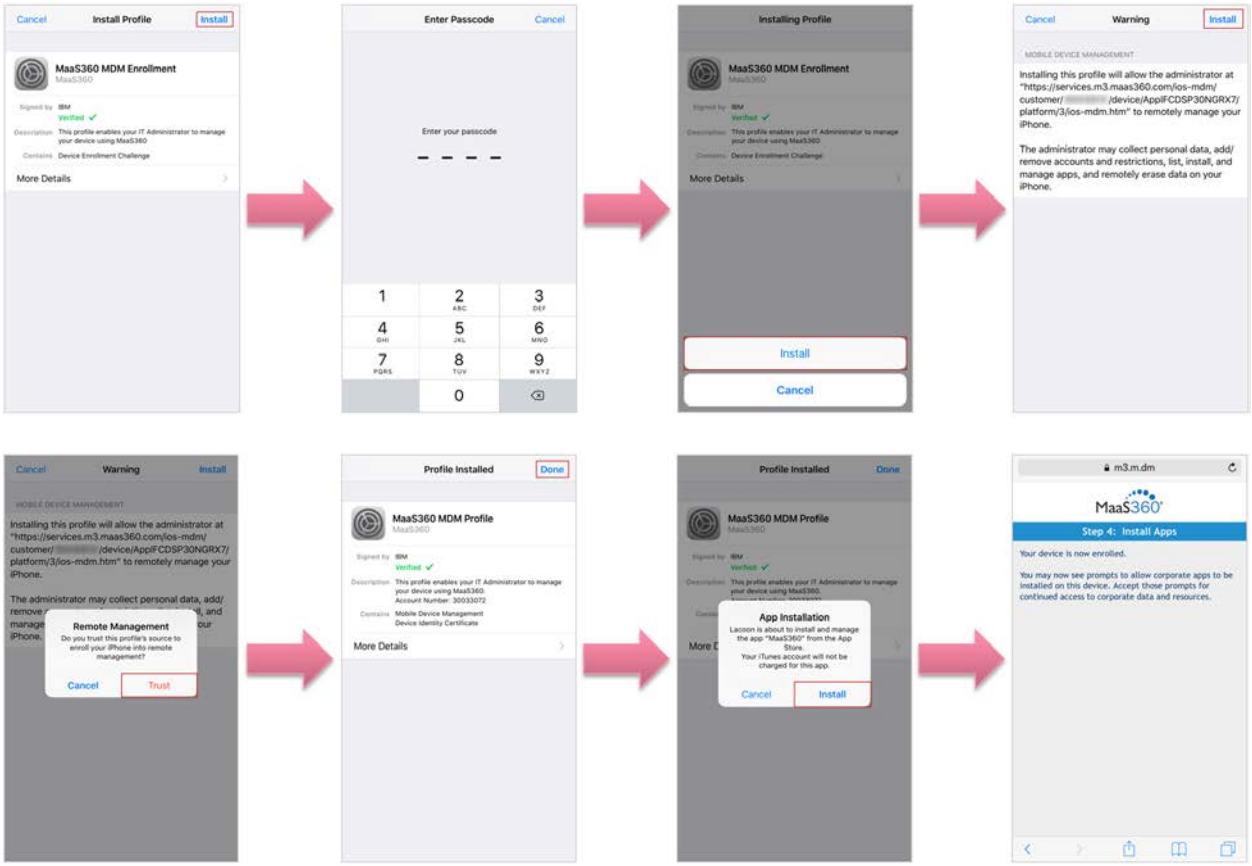
2.7.1.5. The user will be prompted to accept the “Terms of Use” by selecting the “I have read and accept the terms” checkbox, and tapping the “Continue” button.

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.



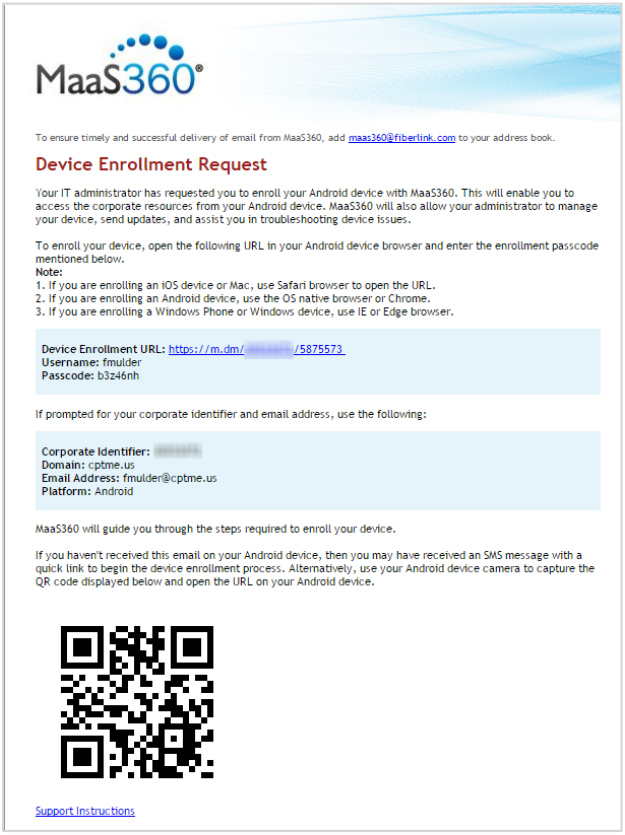
2.7.1.8. Once the profile is installed, the user will be prompted to install the MaaS360 app.

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

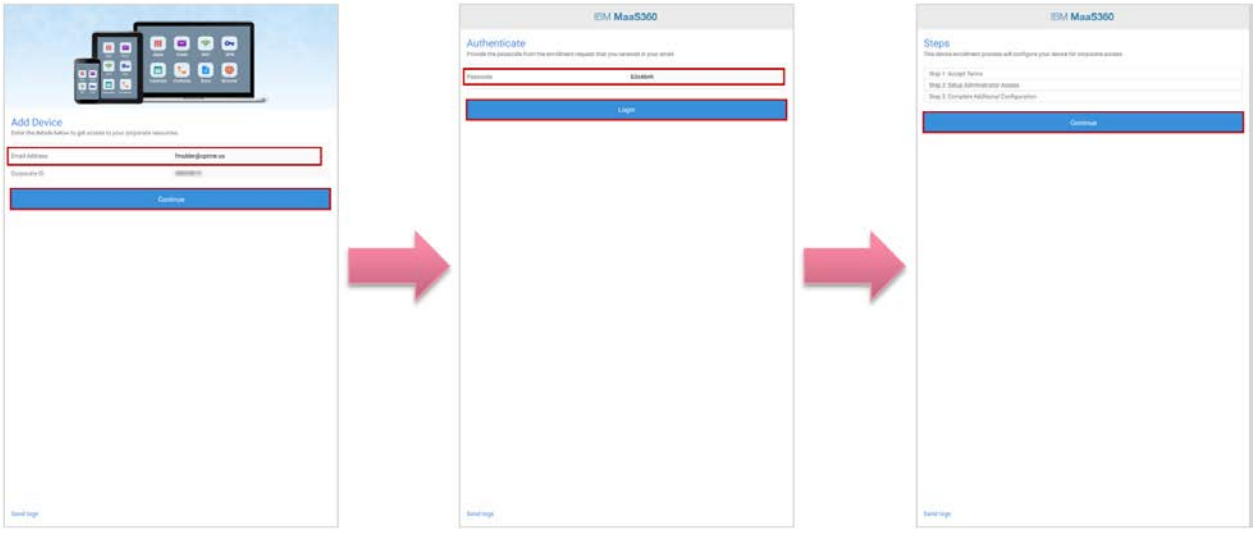
2.7.2.1. The user will receive an enrollment email from the MaaS360 system.



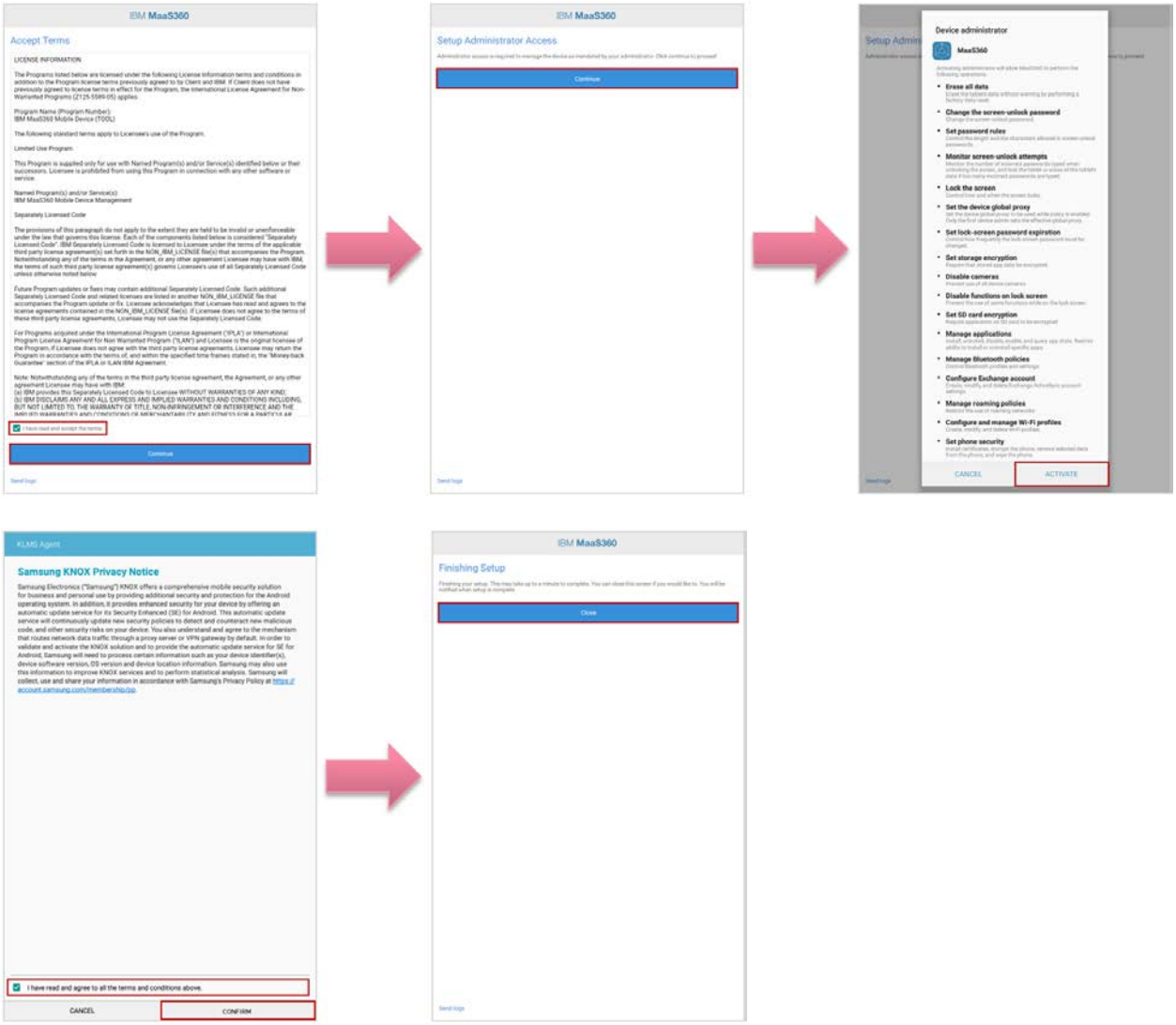
2.7.2.2. The user will open the MaaS360 link in their device's browser. This will prompt the user to go to the Google Play Store to download/install the MaaS360 app.

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.

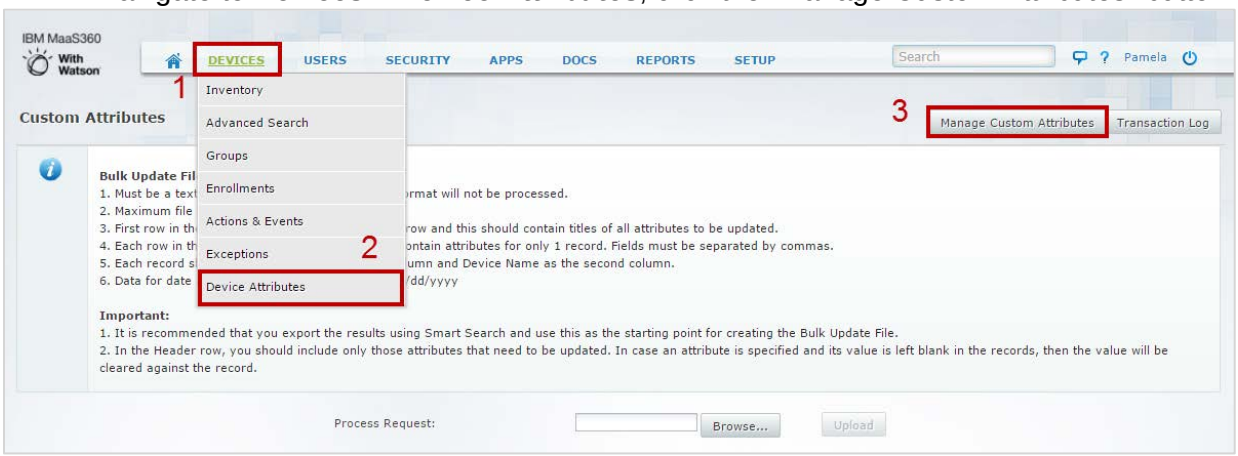
2.8 Creating a Mitigation Process

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.

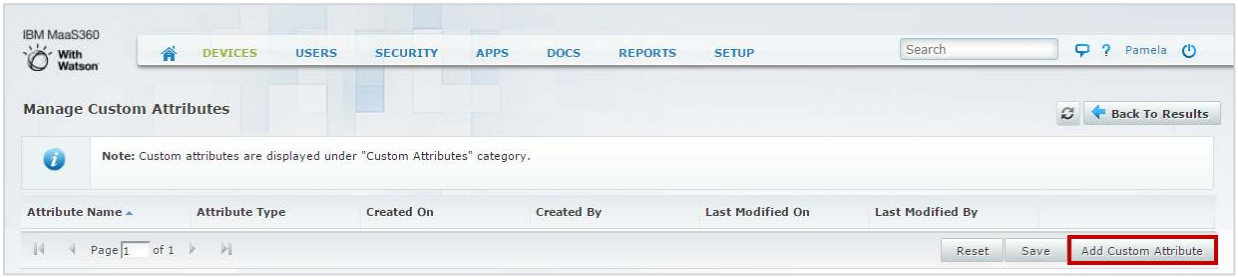
2.8.1 Creating a Mitigation Label

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.

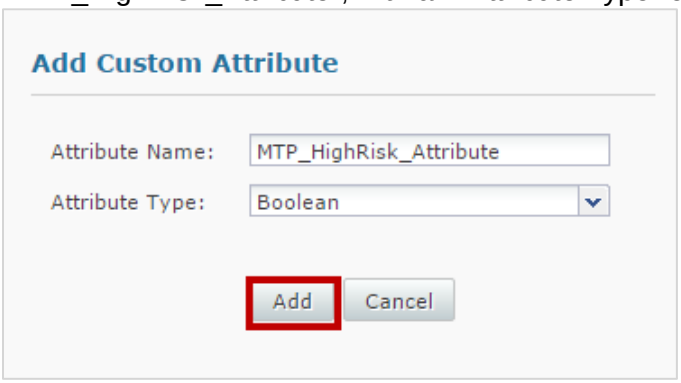
2.8.1.1. Navigate to **Devices > Device Attributes**, click the “Manage Custom Attributes” button.



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”.

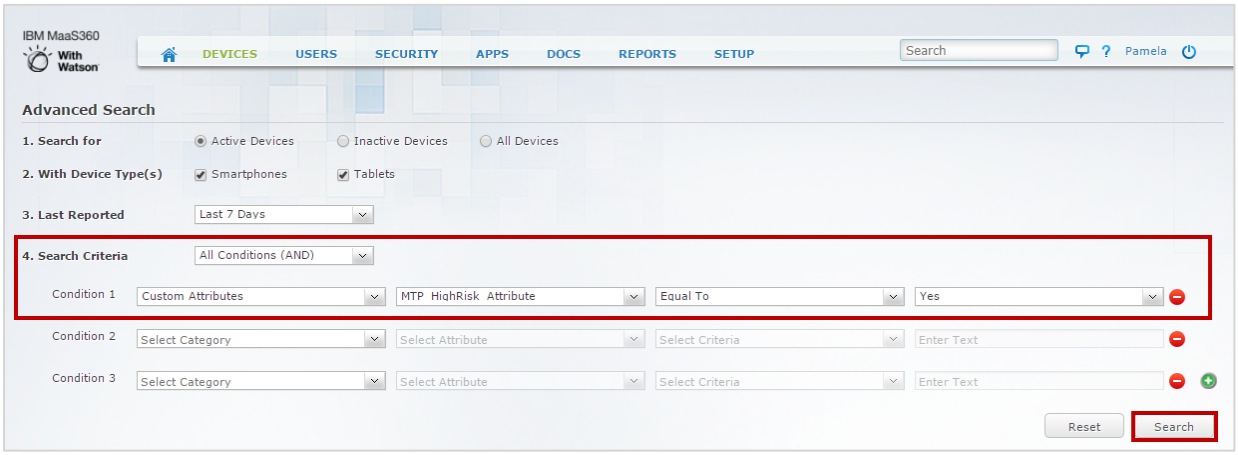


2.8.1.4. Click the “Add” button.

2.8.2 Creating a Device Mitigation Group

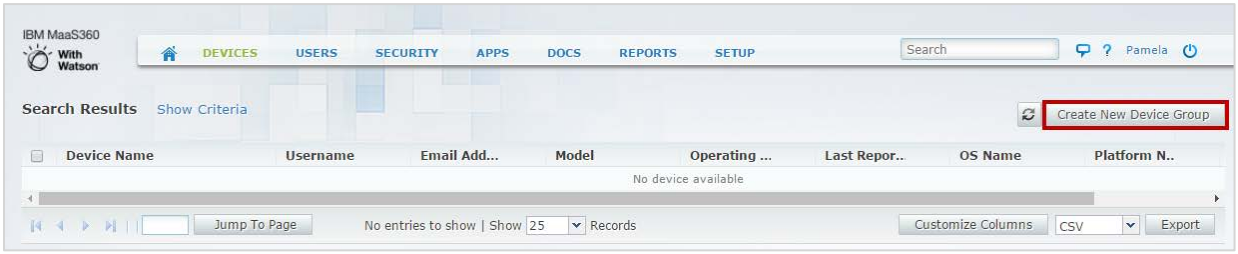
Now that we have a mitigation label ("MTP_HighRisk_Attribute"), we will create a Device Mitigation Group (device group) based on this custom attribute.
For this example, we will call this device mitigation group, "Devices_At_High_Risk". This group will contain all the devices in which the custom attribute, 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"

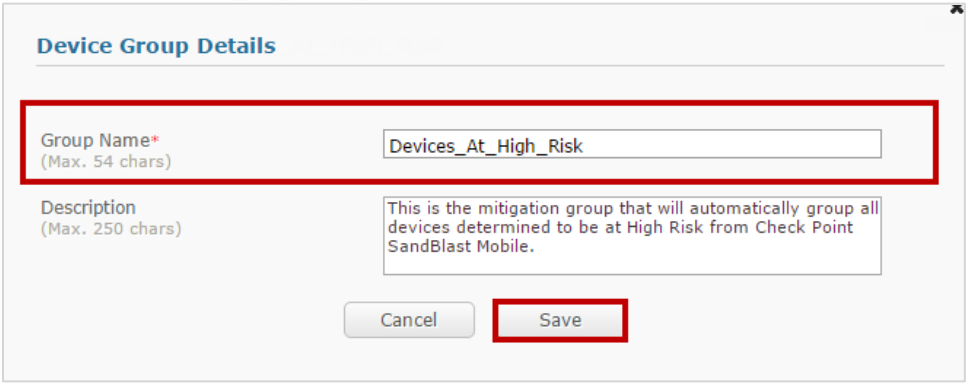


2.8.2.3. Click the "Search" button.

2.8.2.4. Click the "Create New Device Group" button.



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.



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.

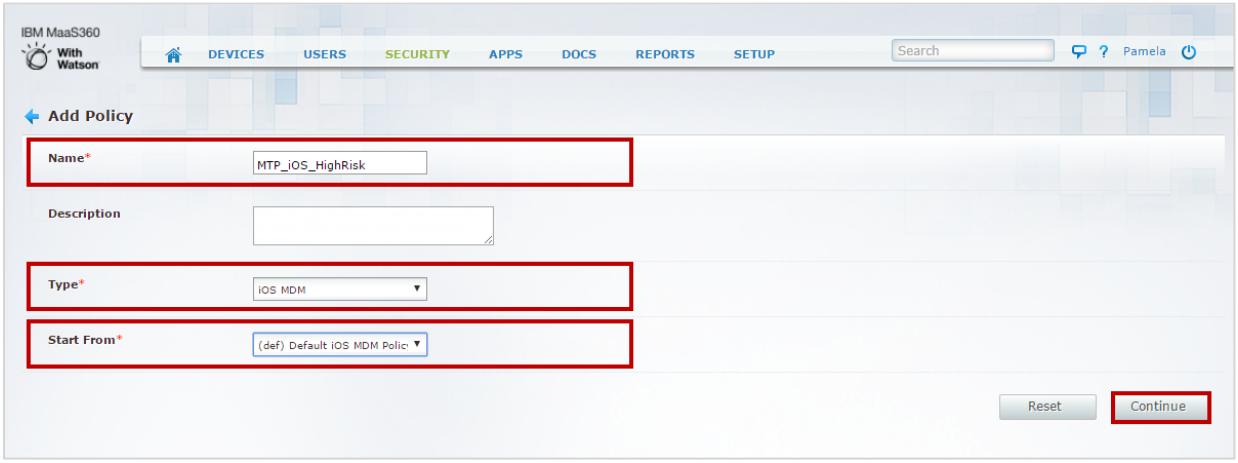
2.8.3.1 Security Policy (Examples)

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.

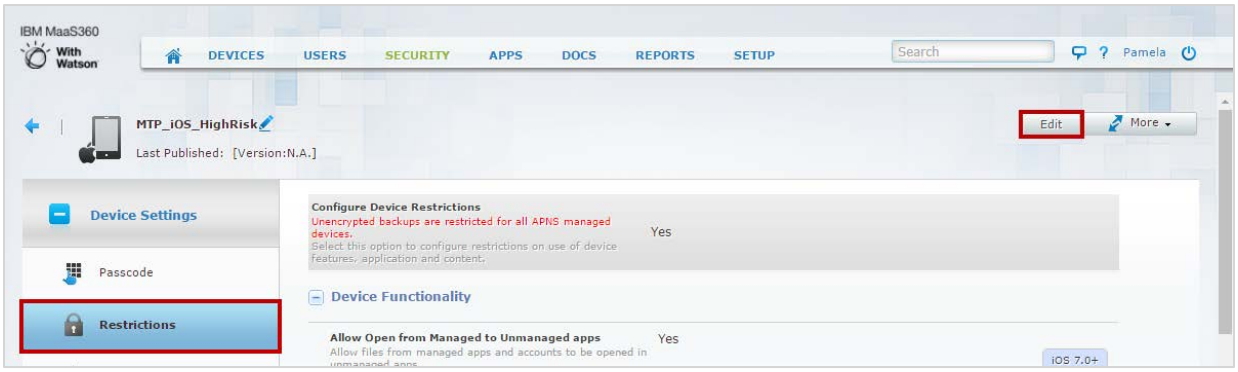
2.8.3.1.1.2. Enter a Name for the policy, such as “MTP_iOS_HighRisk”, select a “Type” of “iOS MDM”, and select “Start From” equal to “Default iOS MDM Policy”.



2.8.3.1.1.3. Click the “Continue” button.

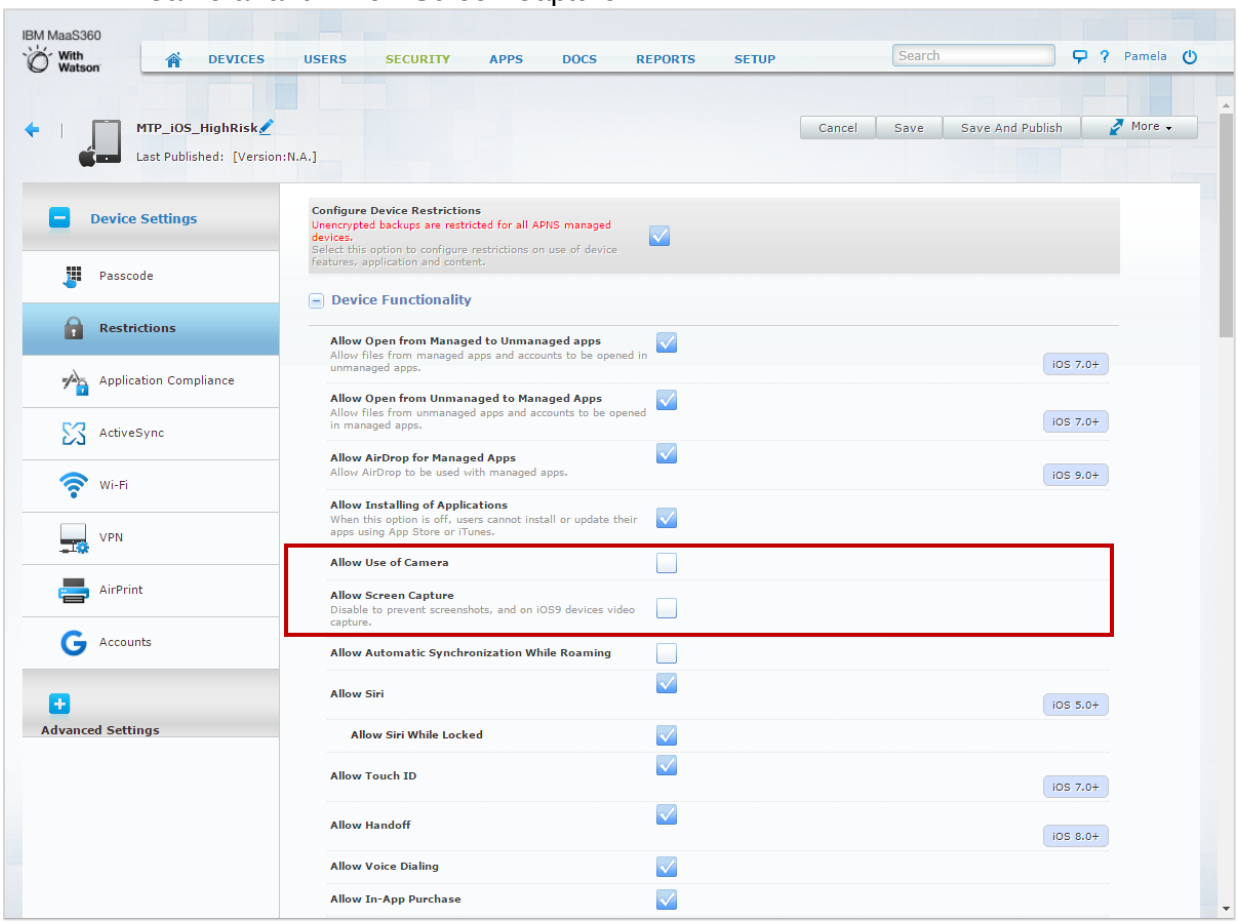
2.8.3.1.1.4. There are several sections for policy sets, such as “Passcode, Restrictions, Application Compliance, etc. We will make our modifications in the Restrictions section.

2.8.3.1.1.5. Select the “Restrictions” tab.

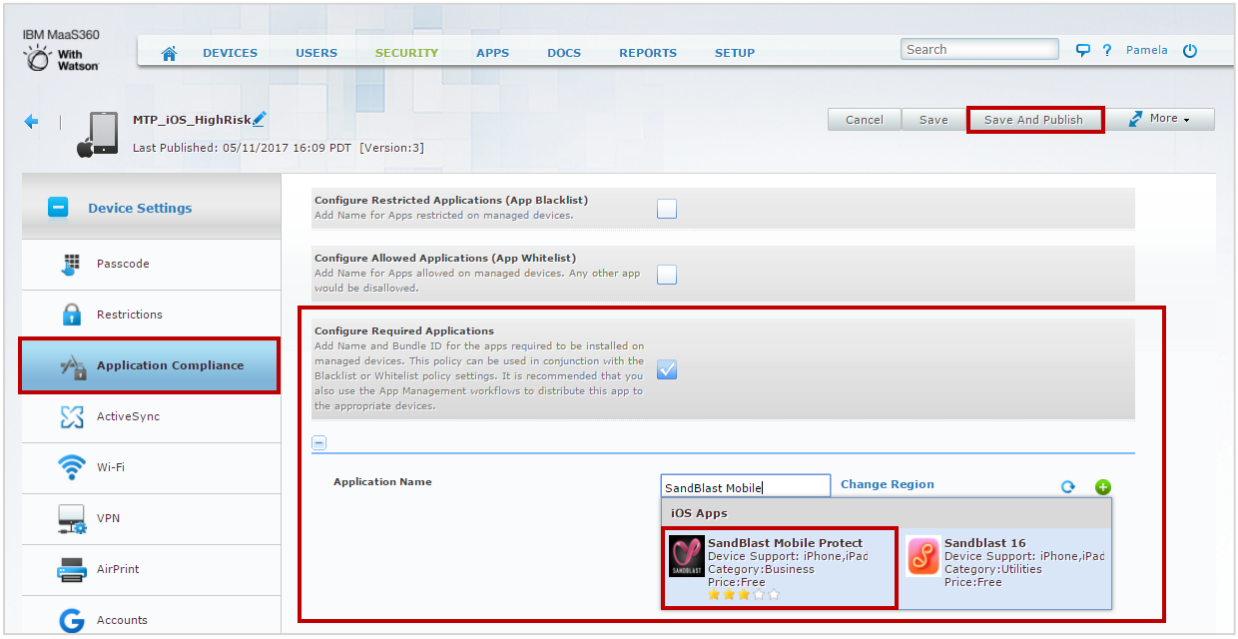


2.8.3.1.1.6. Click the “Edit” button.

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.



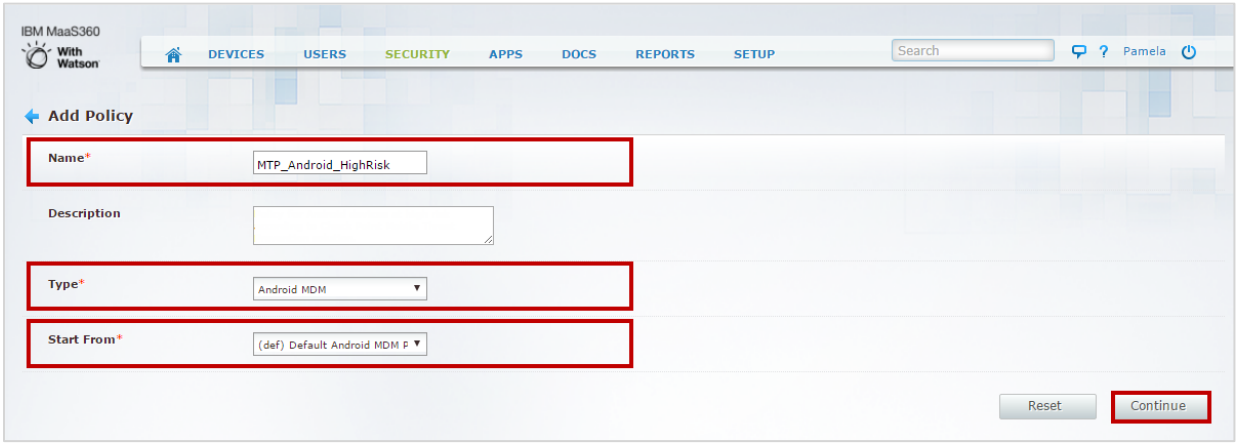
2.8.3.1.1.11. Click the “Save and Publish” button.

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.

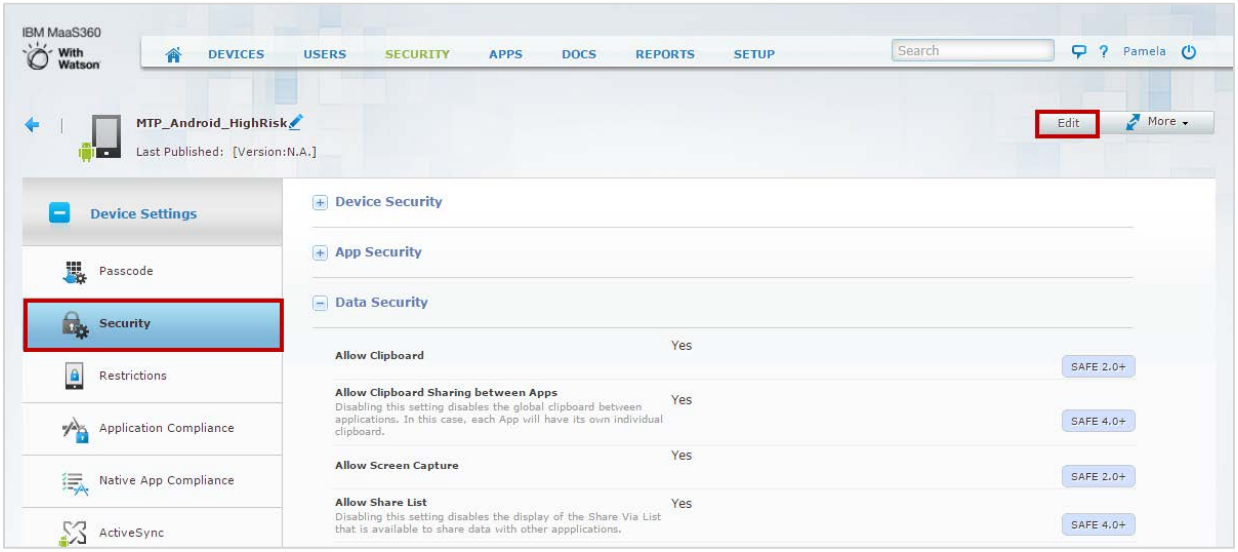
2.8.3.1.2.2. Enter a Name for the policy, such as “MTP_Android_HighRisk”, select a “Type” of “Android MDM”, and select “Start From” equal to “Default Android MDM Policy”.



2.8.3.1.2.3. Click the “Continue” button.

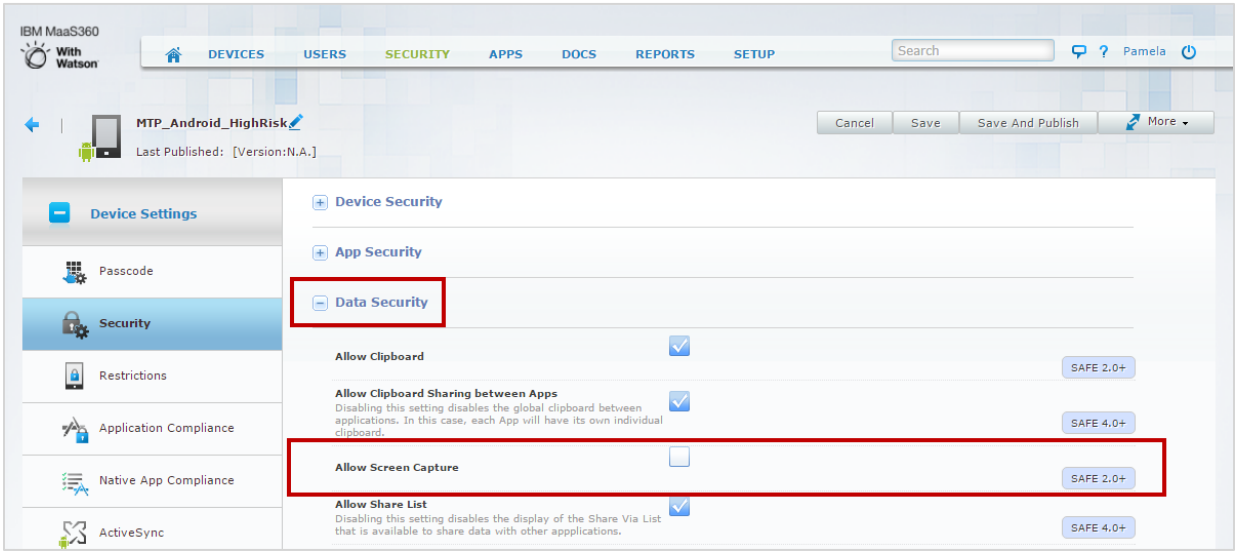
2.8.3.1.2.4. There are several sections for policy sets, such as “Passcode, Security, Restrictions, Application Compliance, etc. We will make our modifications in the Security, Application Compliance, and Restrictions sections.

2.8.3.1.2.5. Select the “Security” tab.



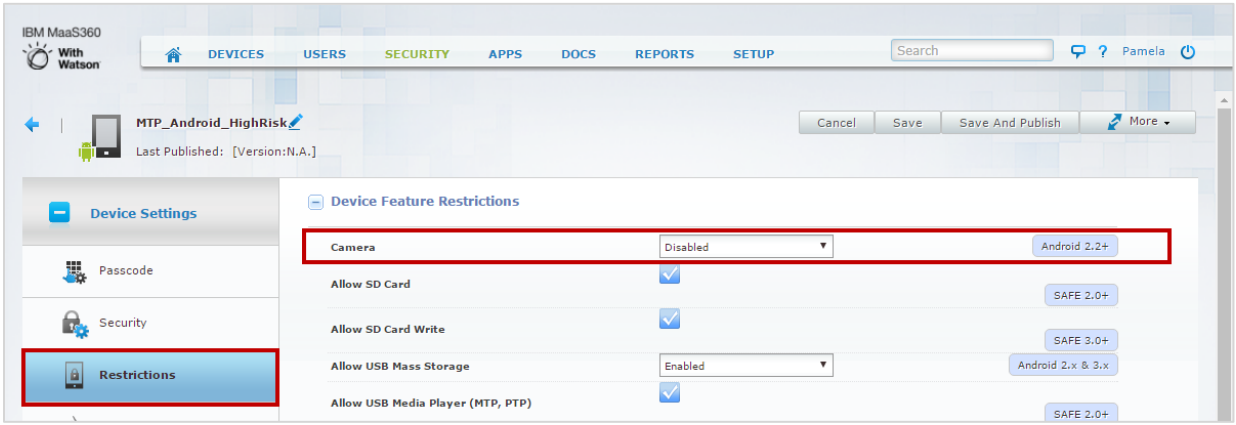
2.8.3.1.2.6. Click the “Edit” button.

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

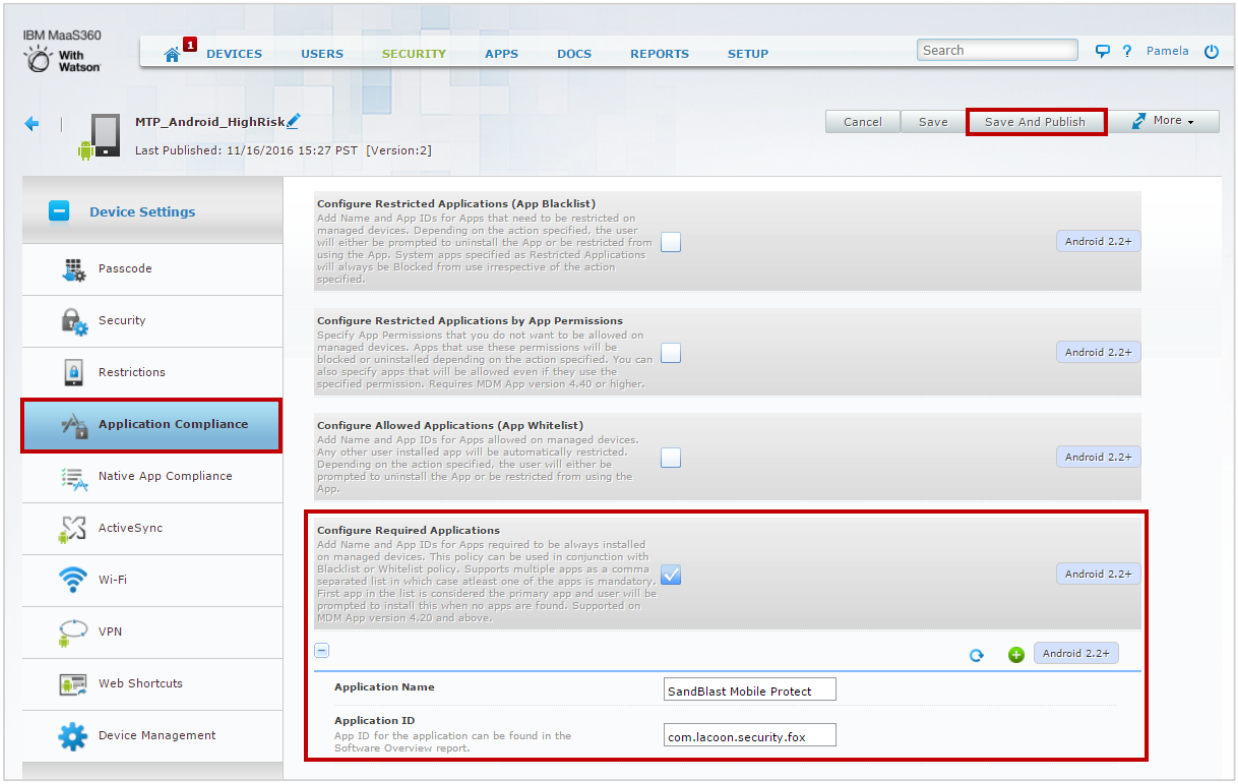


2.8.3.1.2.8. Select the “Restrictions” tab.

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”

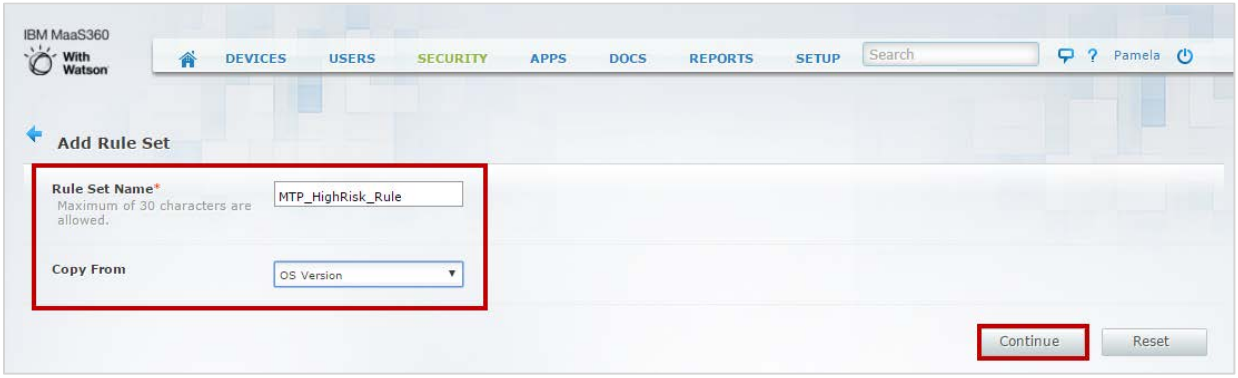


2.8.3.1.2.12. Click the “Save And Publish” button.

2.8.3.2 Creating Security Compliance Rule (Enforcement)

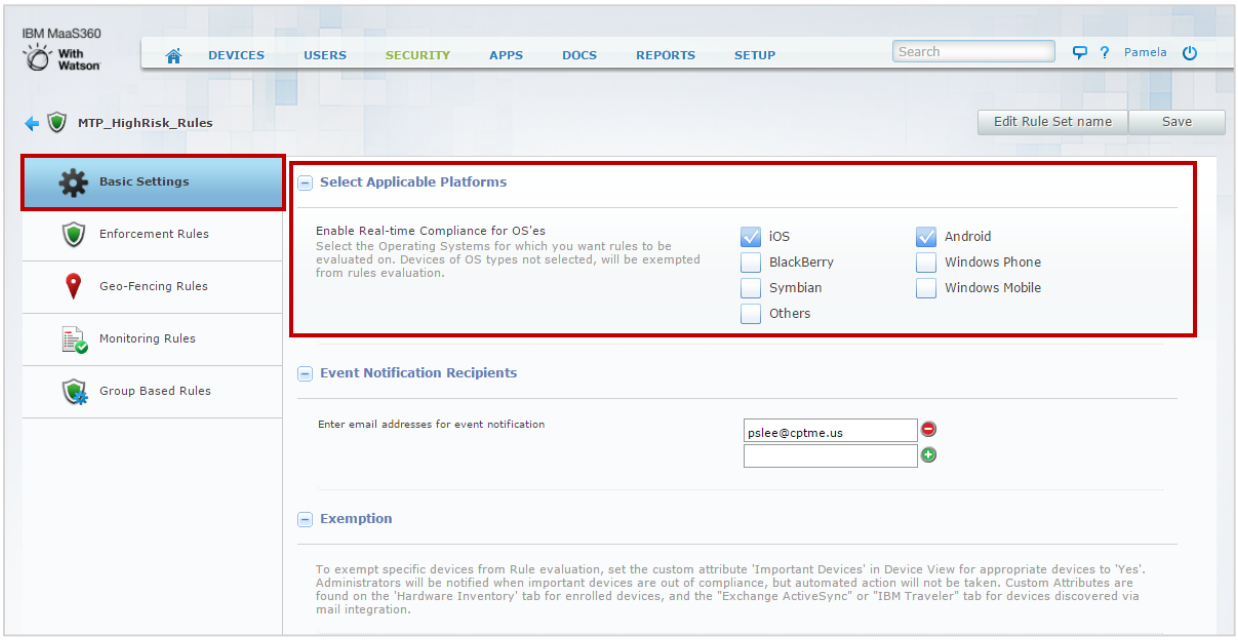
This compliance rule will be used to enforce the policies created in the previous section.
2.8.3.2.1. Navigate to **Security > Compliance Rules**, and click the “Add Rule Set” button.

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”



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”.



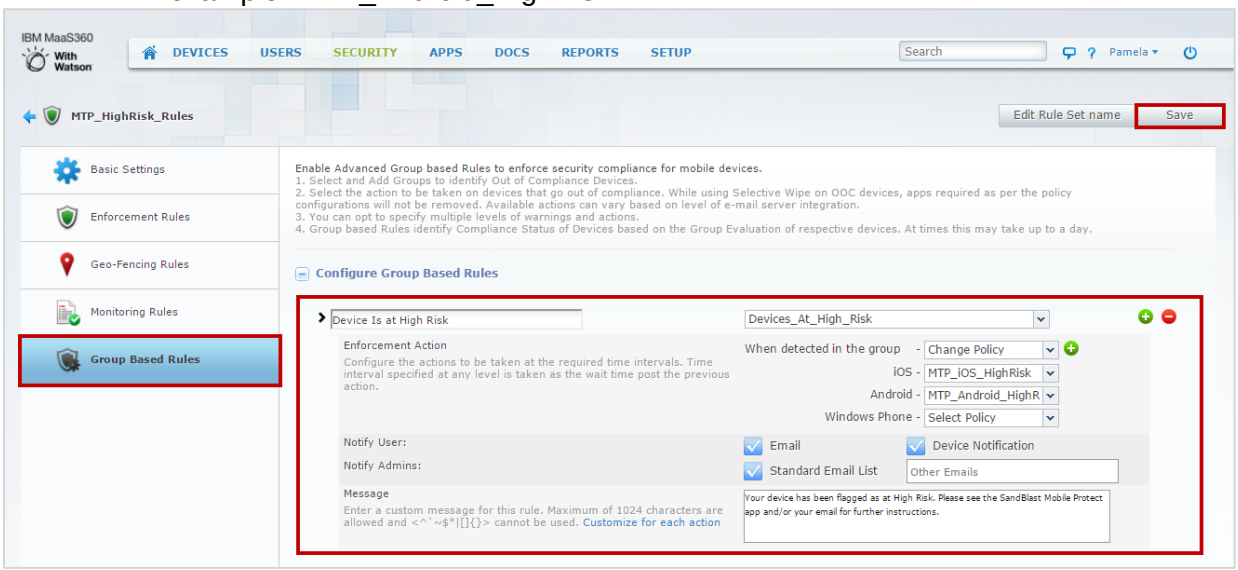
2.8.3.2.5. Select “Group Based Rules” tab, and click the “Add a New Rule” button.

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.

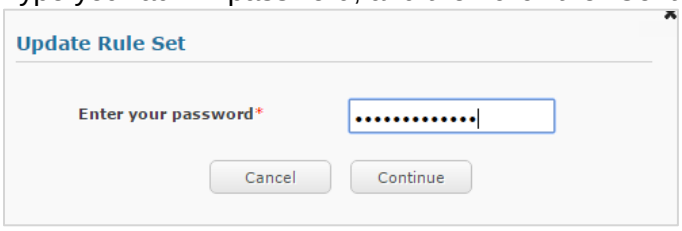
2.8.3.2.6.1.1. Set iOS policy to the compliance policy we created in Section 2.8.3.1.1, in our example “MTP_iOS_HighRisk”.

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”



2.8.3.2.7. Click the “Save” button.

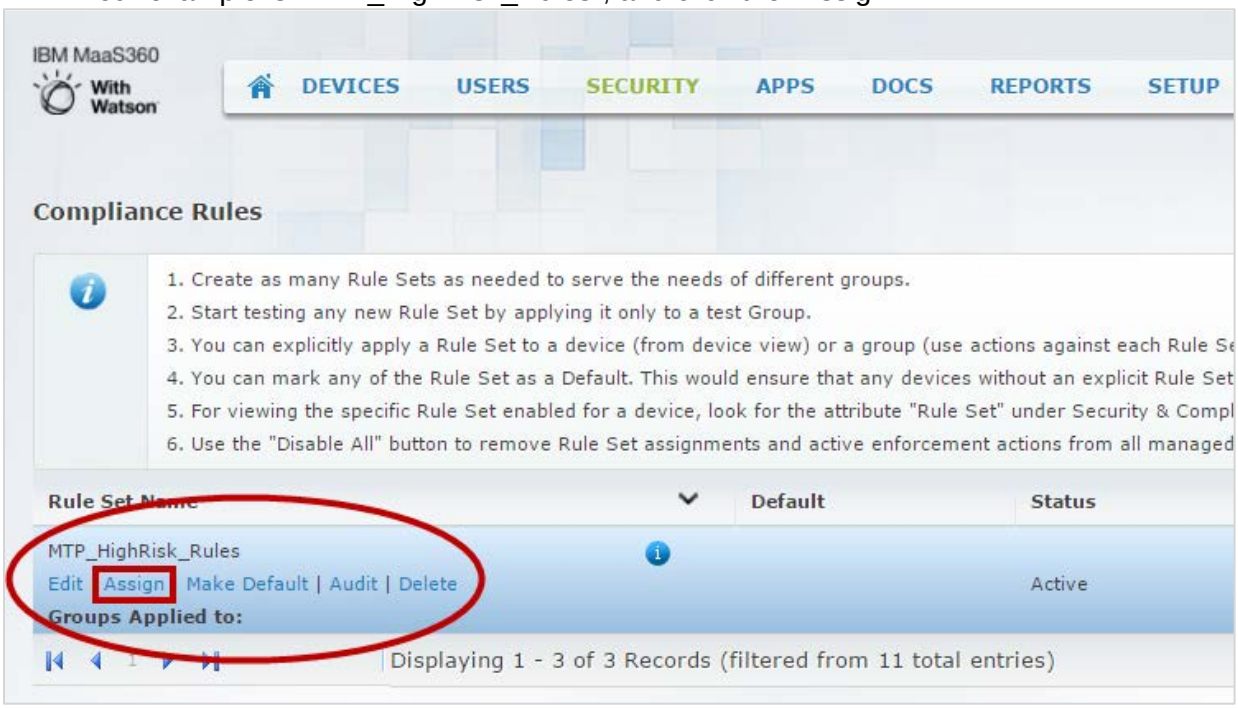
2.8.3.2.8. Type your admin password, and then click the “Continue” button.



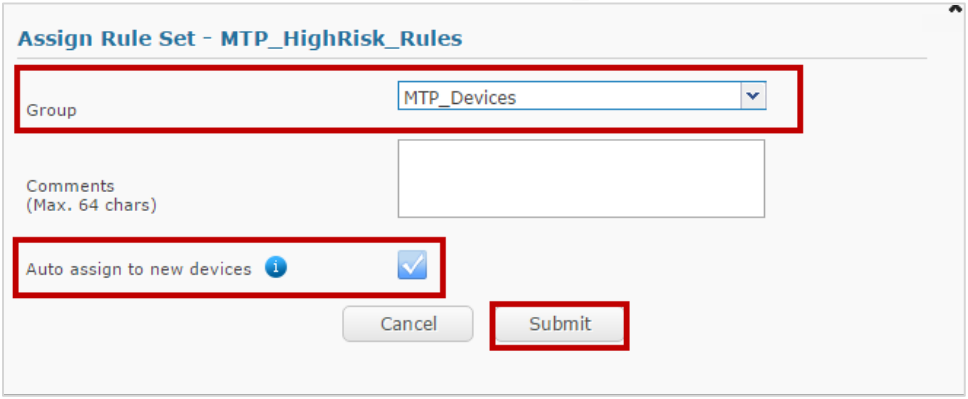
2.8.4 Applying the Compliance Policy to the Device Provisioning Group

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.

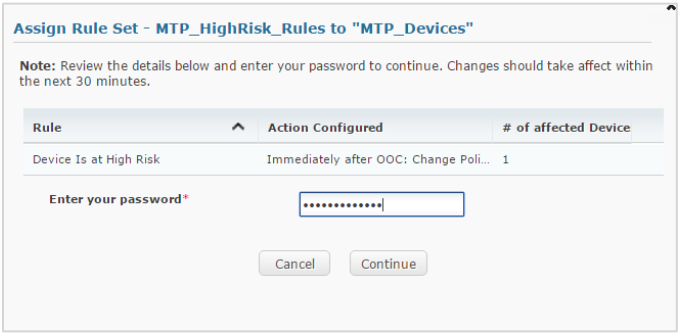


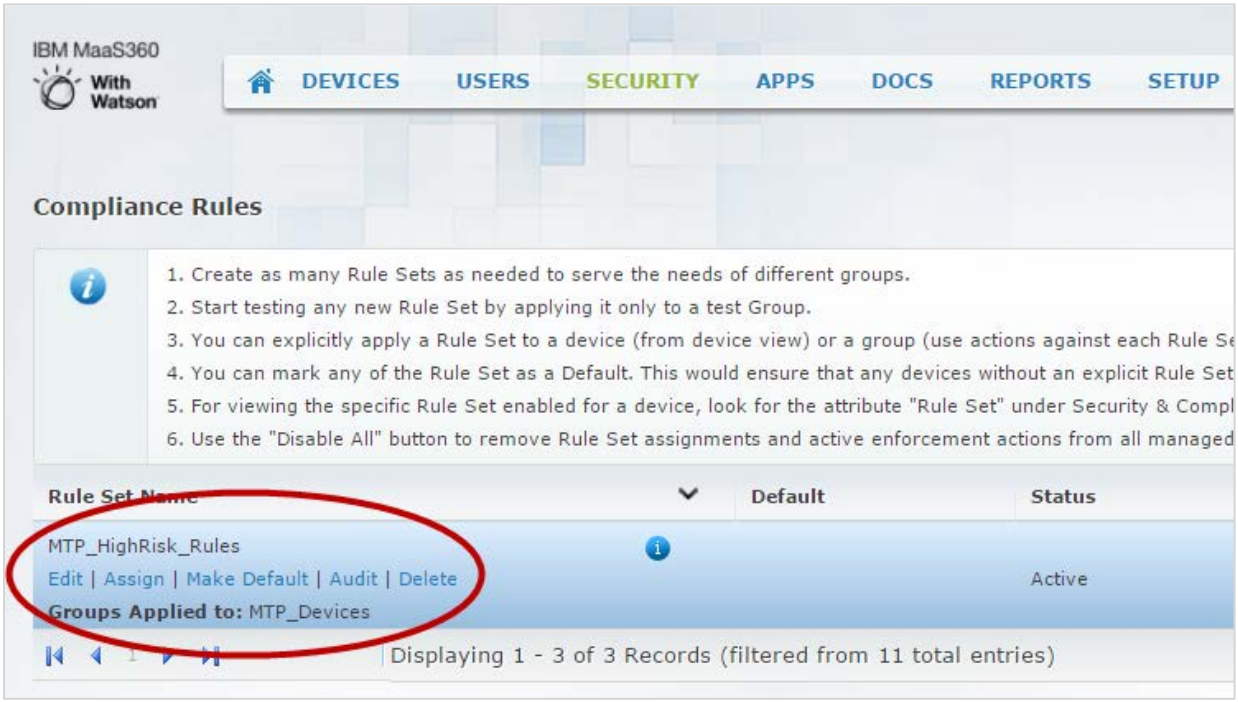
2.8.4.2. On the Assign Rule Set pop-up window, select the Device Provisioning Group we created in Section 2.6, in our example "MTP_Devices".



2.8.4.3. Click the “Submit” button.

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





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.

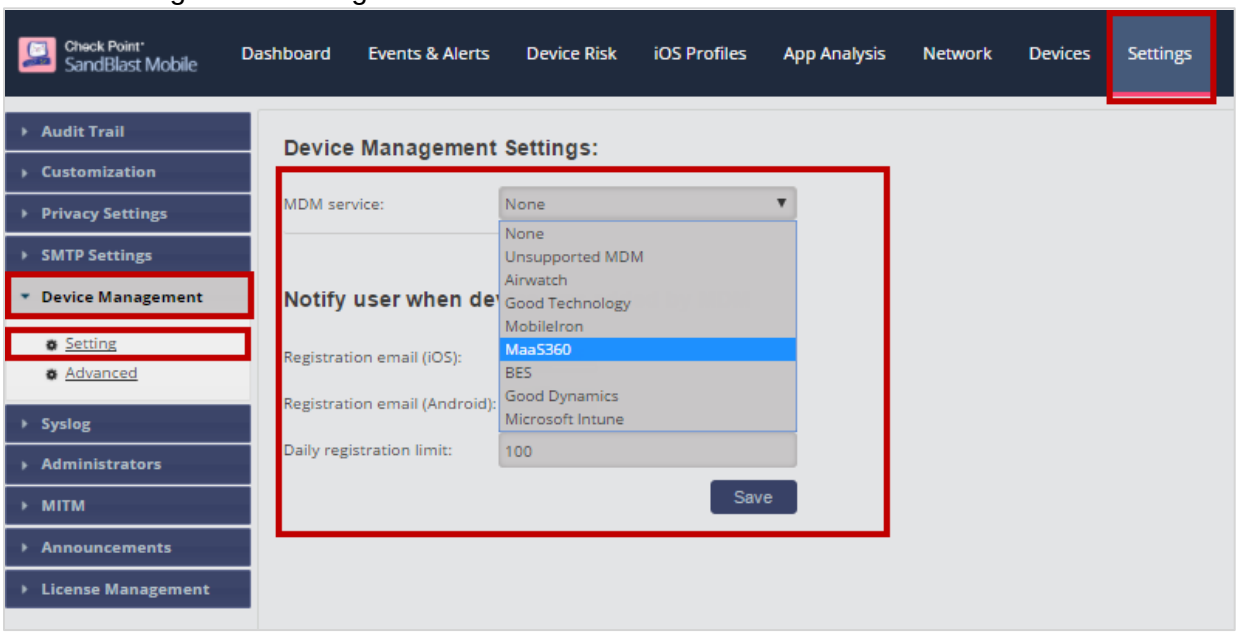
3.1.3. Delete any existing devices in the SandBlast Mobile Dashboard.

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

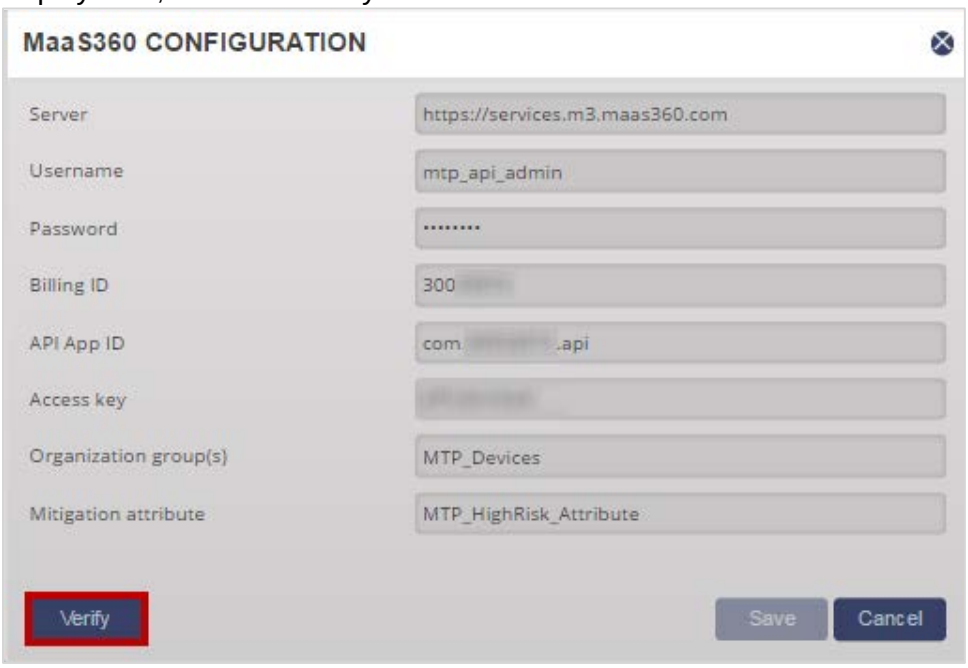
3.2 Configuring MDM Integration Settings

3.2.0.1. Navigate to **Settings > Device Management > Setting**.

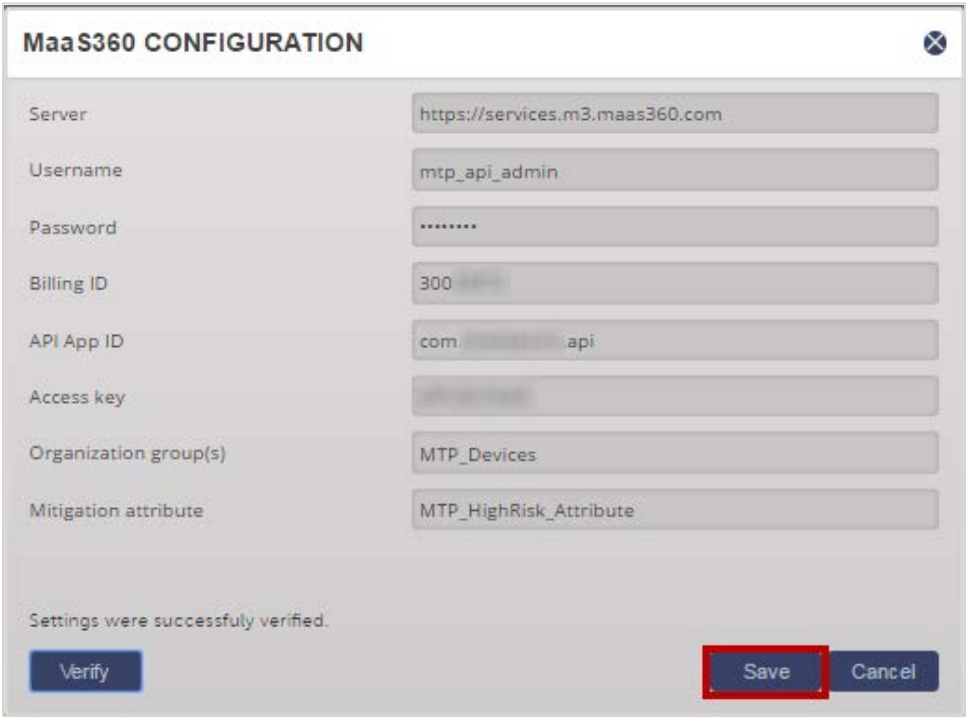
3.2.0.2. Select “MaaS360” from the “MDM service” drop-down menu under the Device Management Settings area.



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.

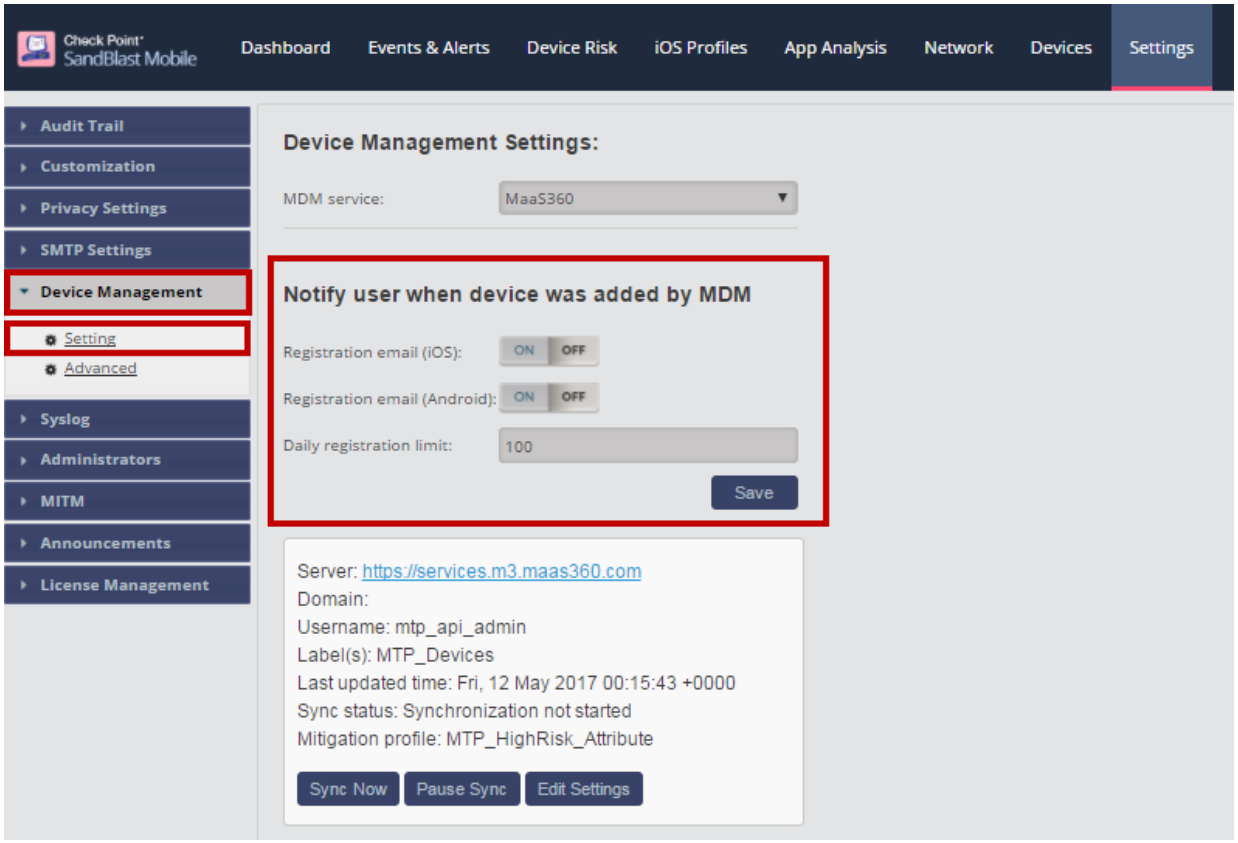


3.2.0.4. Click the “VERIFY” button. If the settings are correct, and the SandBlast Mobile Dashboard can communicate with the MaaS360 system, you will be able to click the “SAVE” button to finish configuration.



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.



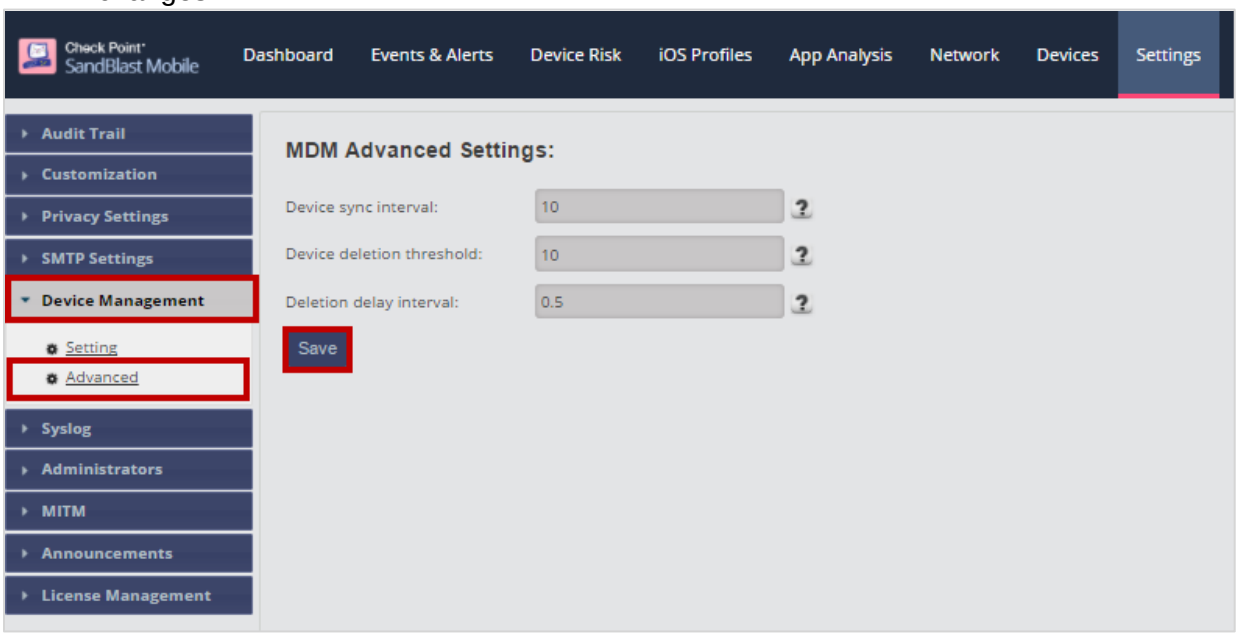
Setting	Description
Registration email (iOS)	Should the system send Registration email to iOS devices?
Registration email (Android)	Should the system send Registration email to Android devices?
Daily registration limit	The number of devices that can register within a 24 hour period.

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.



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.

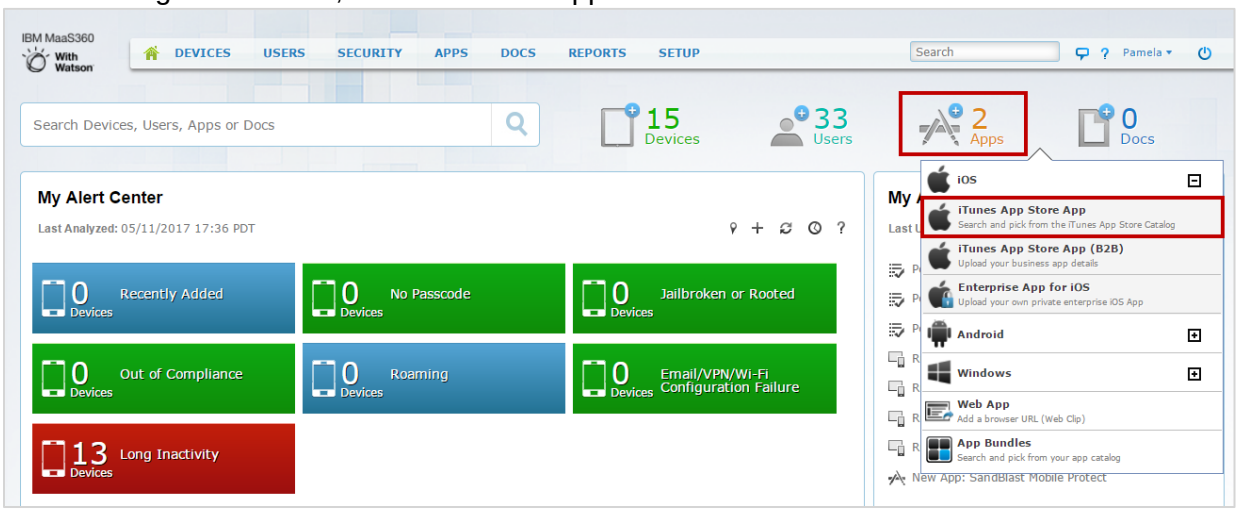
4.2 Adding the SandBlast Mobile Protect App to Your App Catalog

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

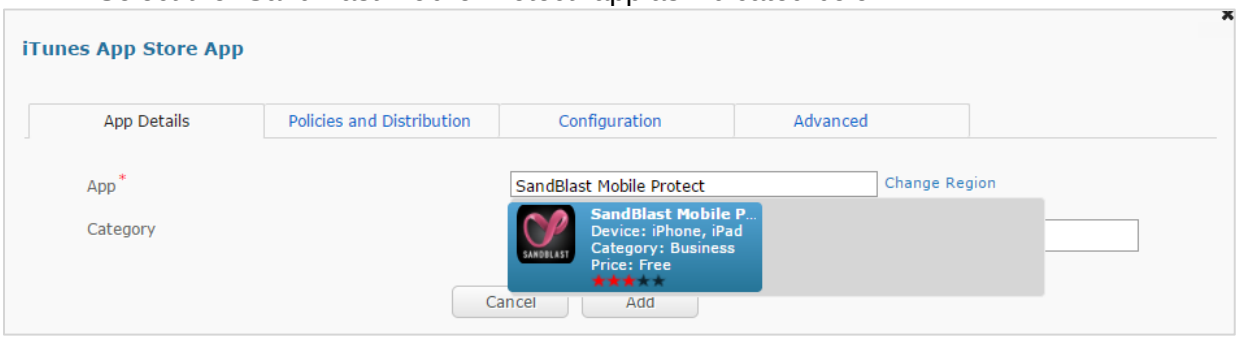
The SandBlast Mobile Protect App for iOS can be automatically configured and deployed. The user only needs to accept the installation, and then launch the app once it is installed to finish activation and registration.

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.

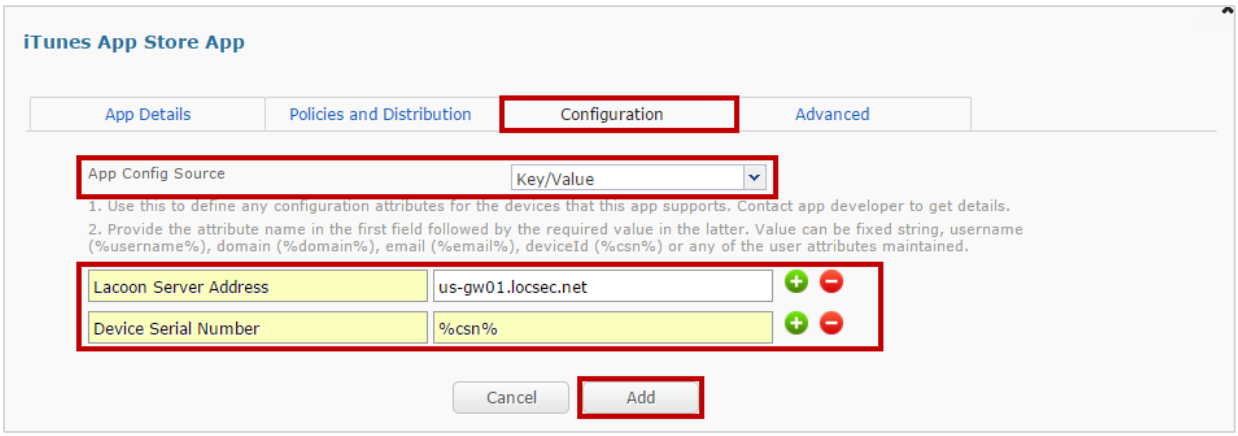


4.2.1.4. Navigate to the "Configuration" tab, and select "Input Type" of "Key/Value".

4.2.1.5. Add the following Key/Value pairs:

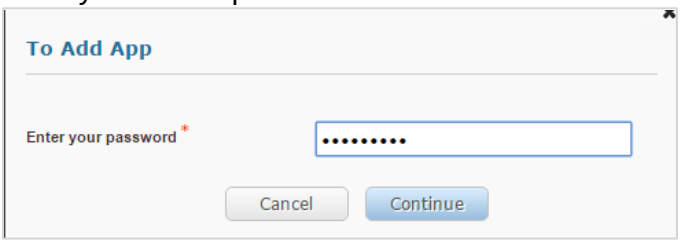
4.2.1.5.1. Lacoon Server Address = us-gw01 (this value should be **your** SandBlast Mobile gateway)

4.2.1.5.2. Device Serial Number = %csn%



4.2.1.6. Click the “Add” button.

4.2.1.7. Enter your admin password.

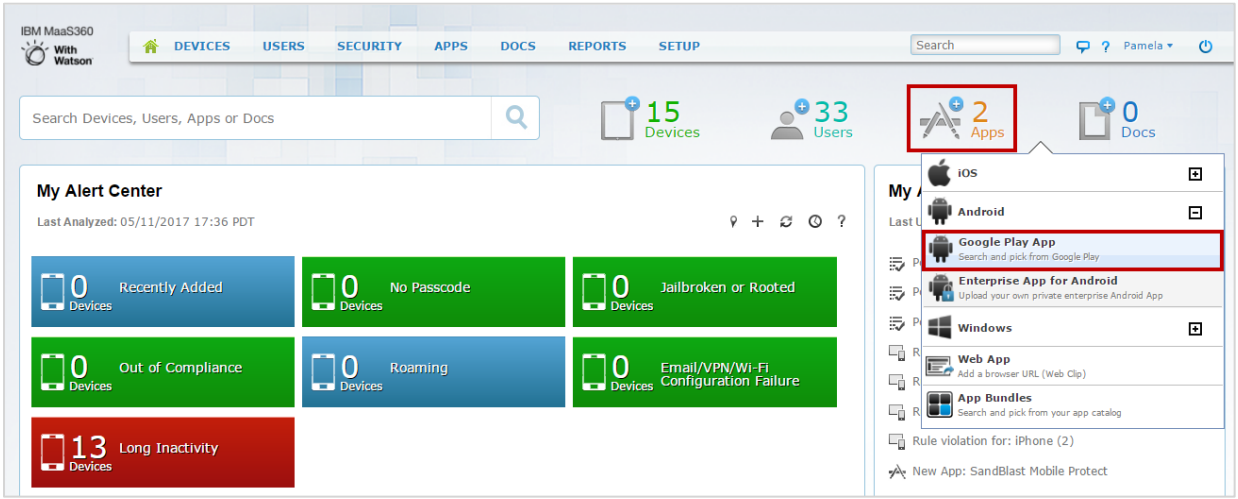


4.2.1.8. Click the “Continue” button.

4.2.2 Android App – Add to Catalog

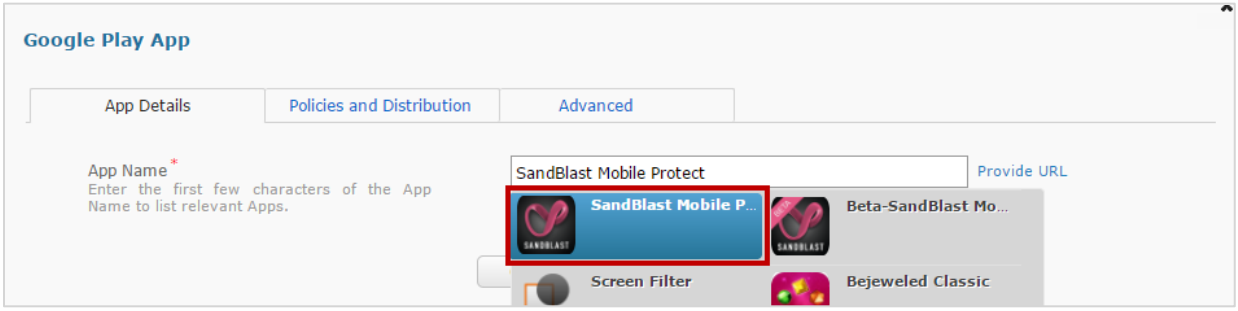
The Android SandBlast Mobile Protect App can be automatically configured and deployed. The user only needs to accept the installation, and then launch the app once it is installed to finish activation and registration.

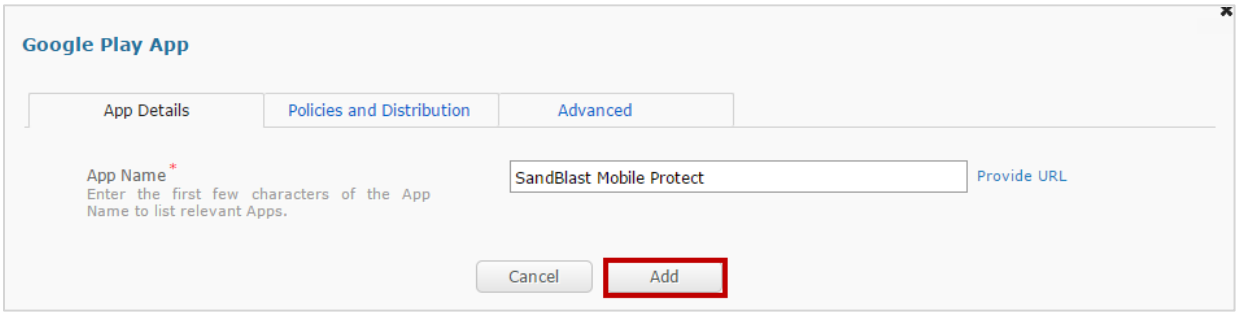
4.2.2.1. Navigate to **Home**, and select the “Apps” button.



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.



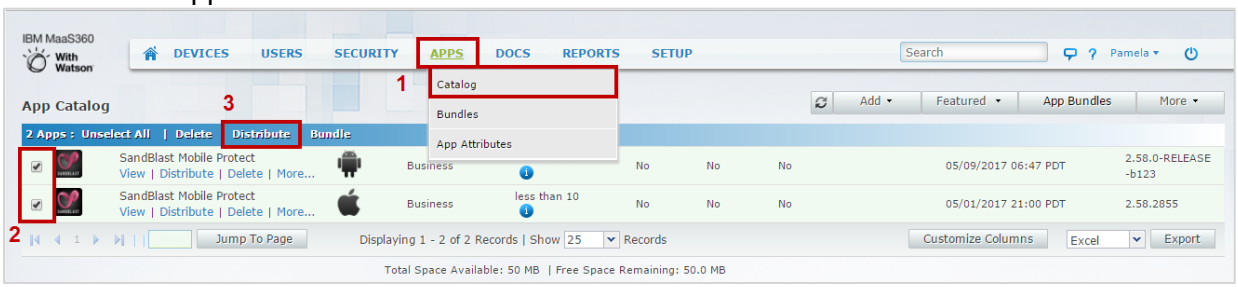


4.2.2.4. Click the “Add” button.

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.

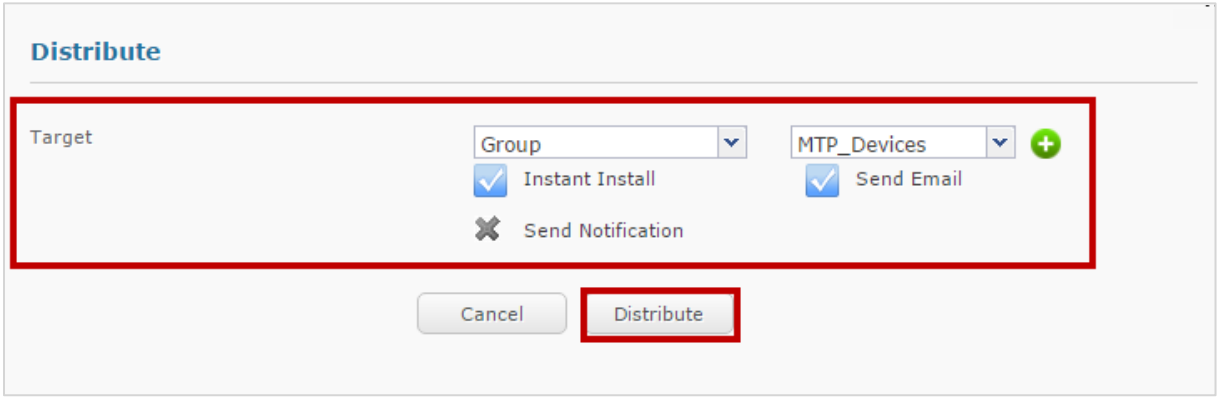
4.3.1. Navigating to **Apps > App Catalog**, select both the iOS and Android SandBlast Mobile Protect apps.



4.3.2. Click the “Distribute” link.

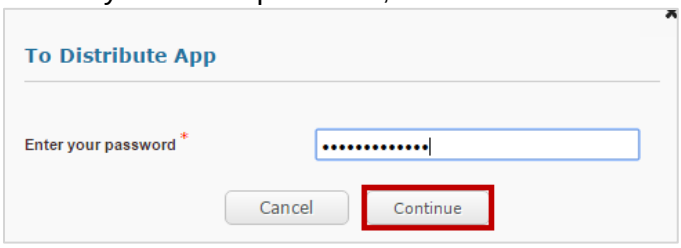
4.3.3. On the “Distribute” pop-up window, set “Target” equal to “Group” and choose the device provisioning group you created in Section 2.6, in our example “MTP_Devices”.

4.3.3.1. Select “Instant Install” and “Send Email” checkboxes.



4.3.4. Click the “Distribute” button.

4.3.5. Enter your admin password, and click the “Continue” button.



4.4 Setting Policy to Require SandBlast Mobile Protect to be Installed

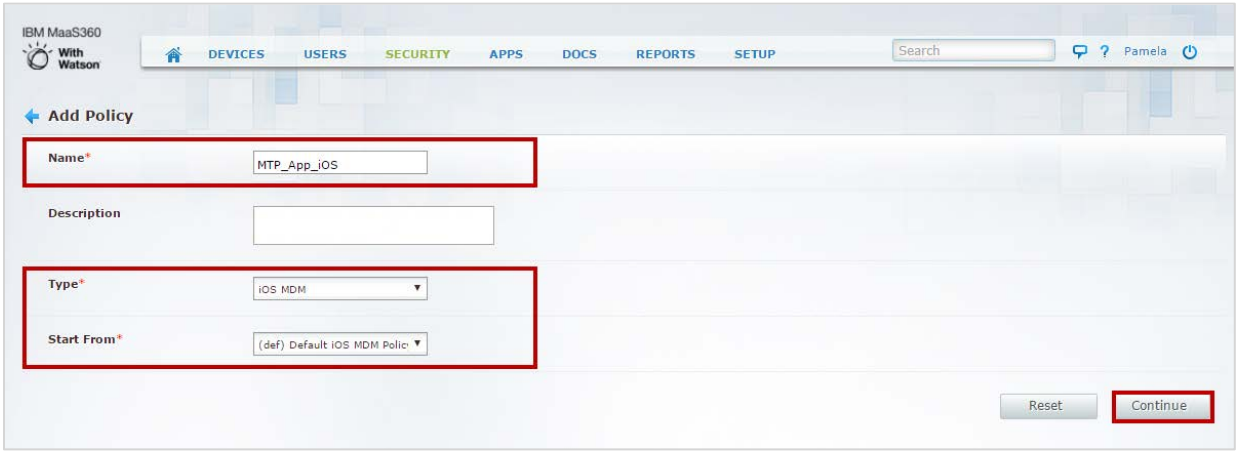
The SandBlast Mobile Protect app is required by creating a Security Policy for iOS and Android devices, then creating a compliance rule set to the Device Provisioning Group we created in Section 2.6, and apply the compliance policy to the Device Provisioning Group.

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.

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”.



4.4.1.3. Click the “Continue” button.

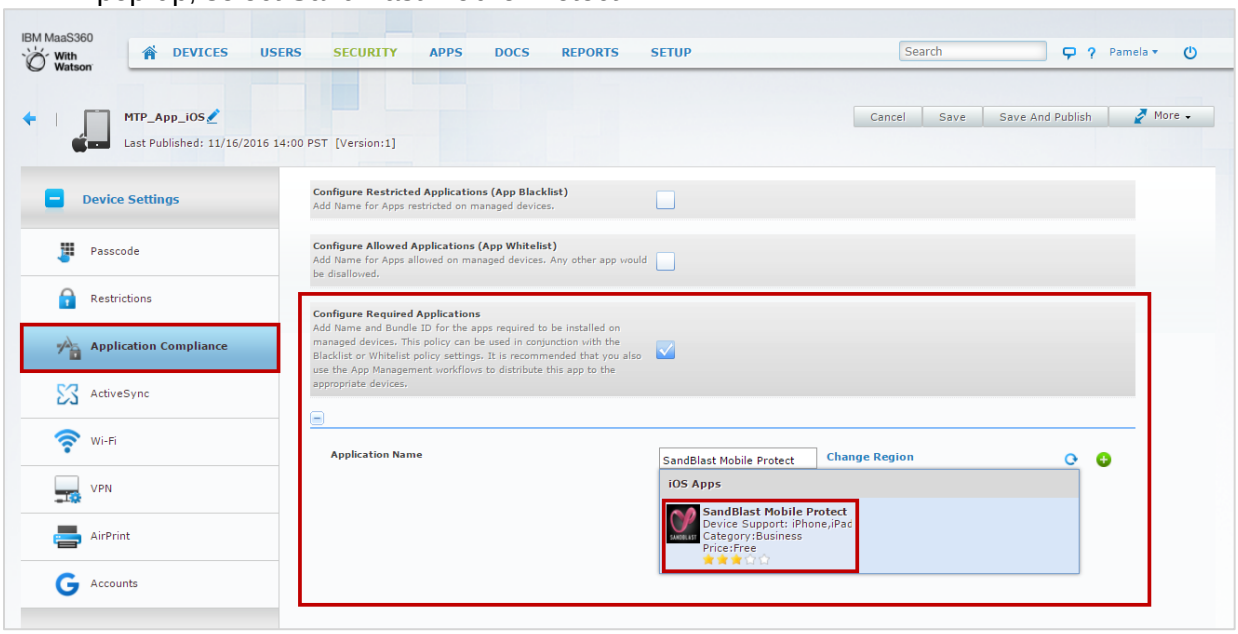
4.4.1.4. There are several sections for policy sets, such as “Passcode, Restrictions, Application Compliance, etc. We will make our modifications in the Restrictions section.

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.

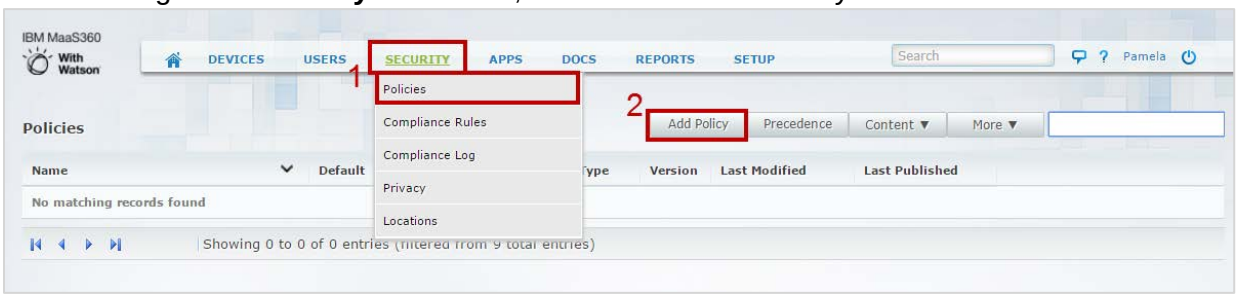


4.4.1.9. Click the “Save and Publish” button.

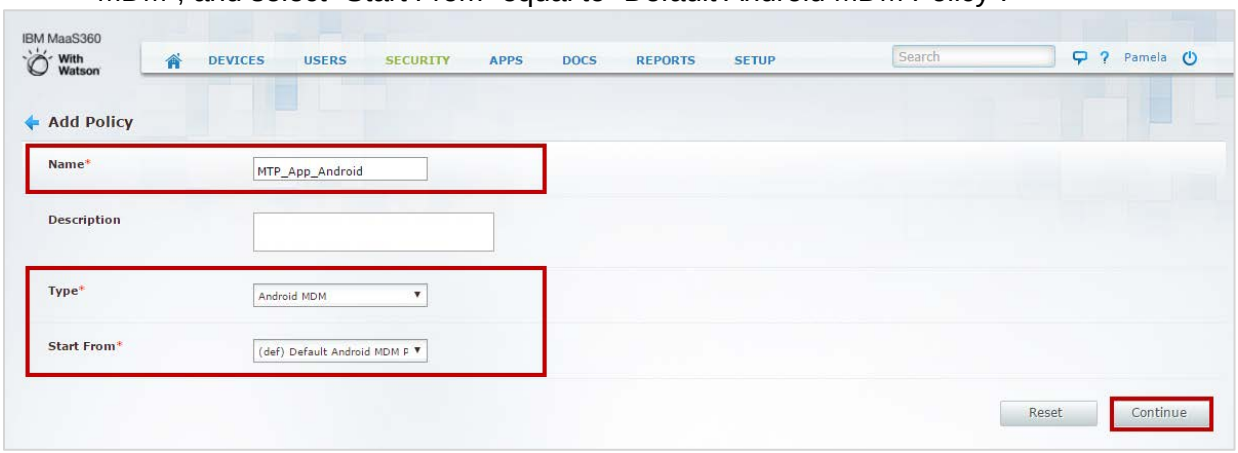
4.4.2 Creating Compliance Actions for Android Devices (Policy)

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.

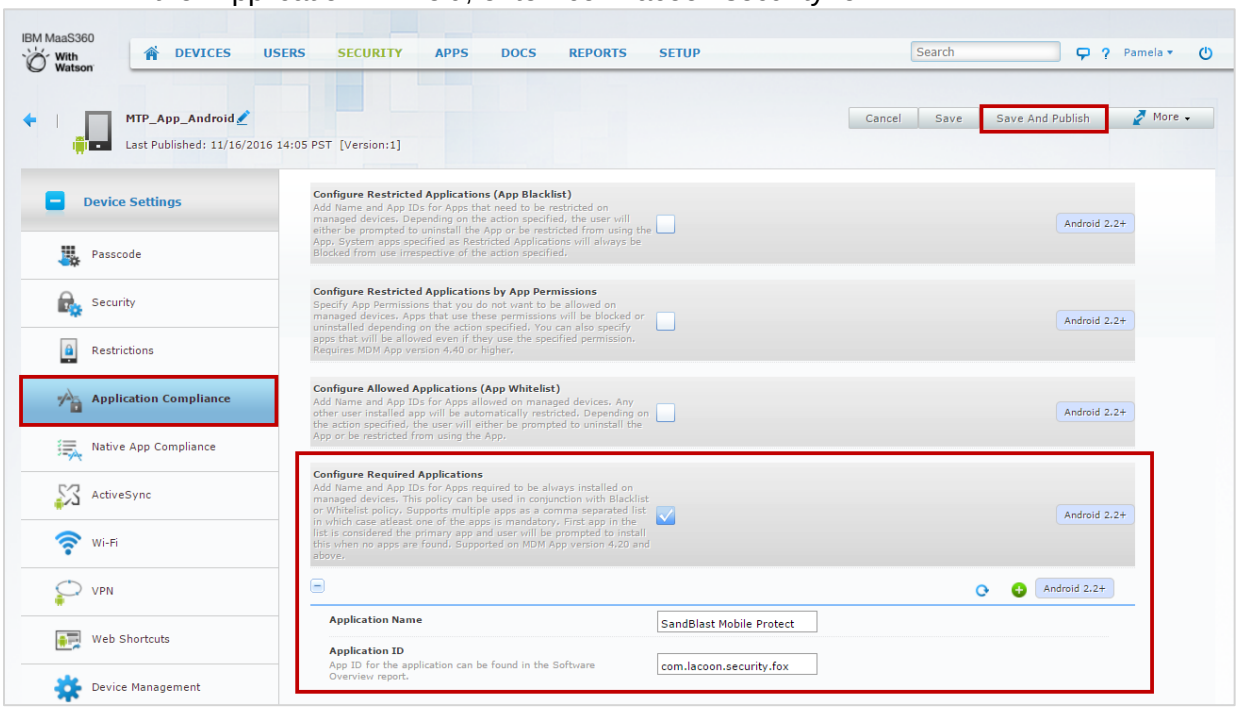


4.4.2.2. Enter a Name for the policy, such as “MTP_App_Android”, select a “Type” of “Android MDM”, and select “Start From” equal to “Default Android MDM Policy”.



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”

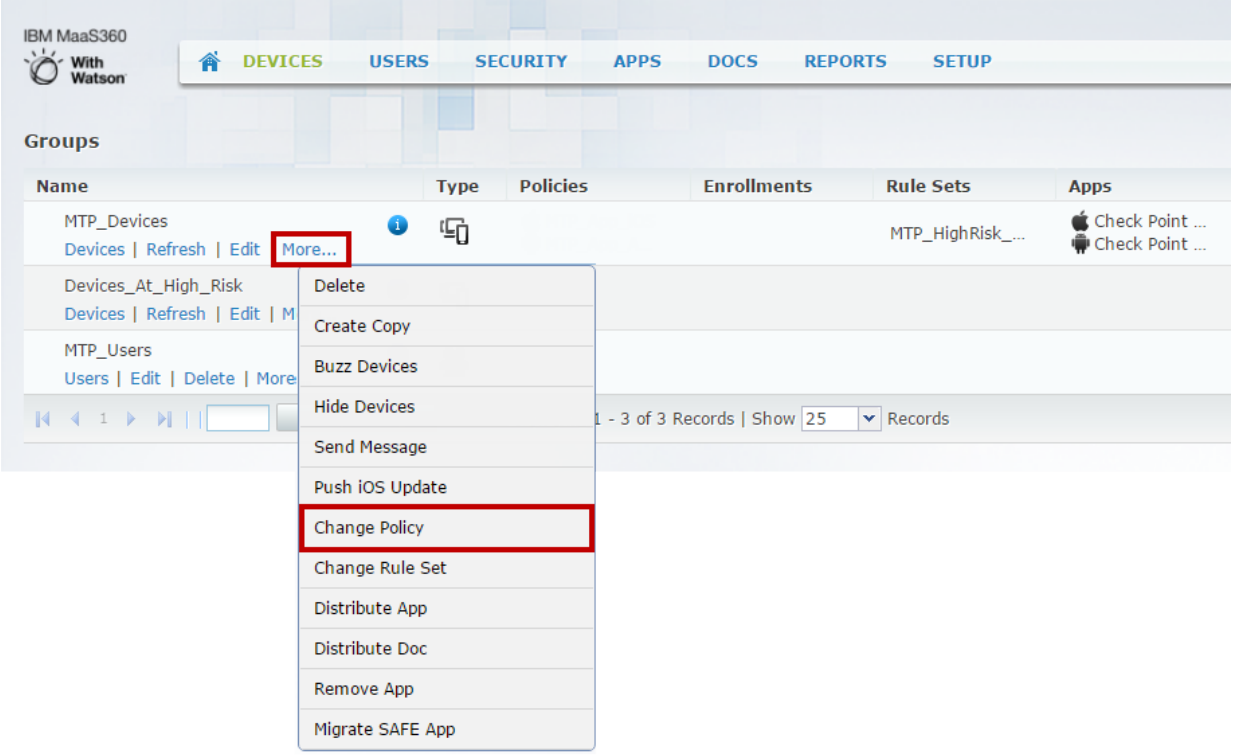


4.4.2.8. Click the “Save And Publish” button.

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”.

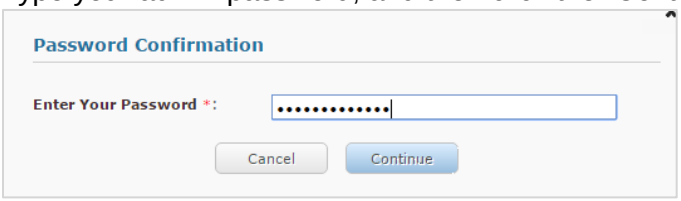


4.4.3.2. Set iOS Policy to the compliance policy we created in Section 4.4.1, in our example “MTP_App_iOS”.

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

4.4.3.4. Click the “Submit” button.

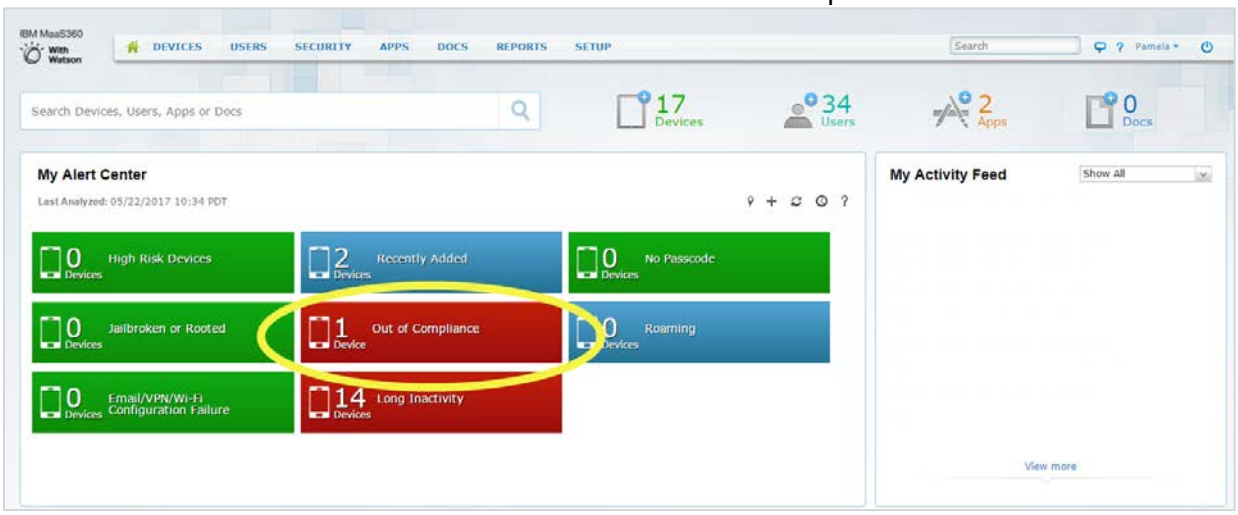
4.4.3.5. Type your admin password, and then click the “Continue” button.



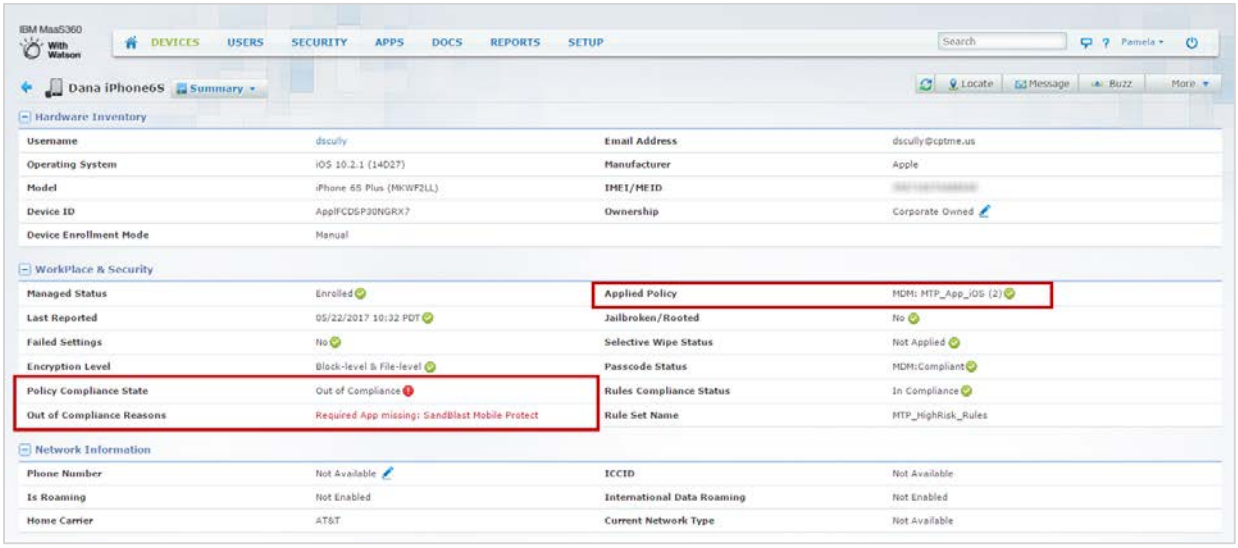
Note: Any device that belongs to the Device Provisioning Group (“MTP_Devices”) that hasn’t installed the SandBlast Mobile Protect app will be out of compliance.

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.



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



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

5 Deploying SandBlast Mobile Protect App to the Devices

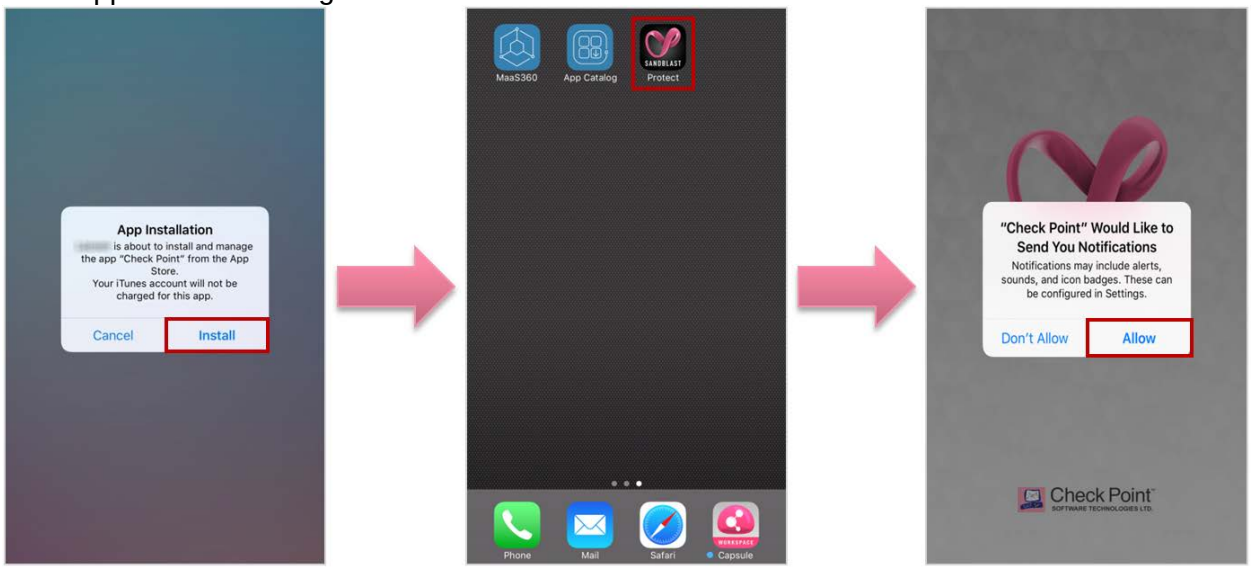
This section describes the user experience during the deployment of the SandBlast Mobile Protect app.

5.1 Registration of an iOS Device

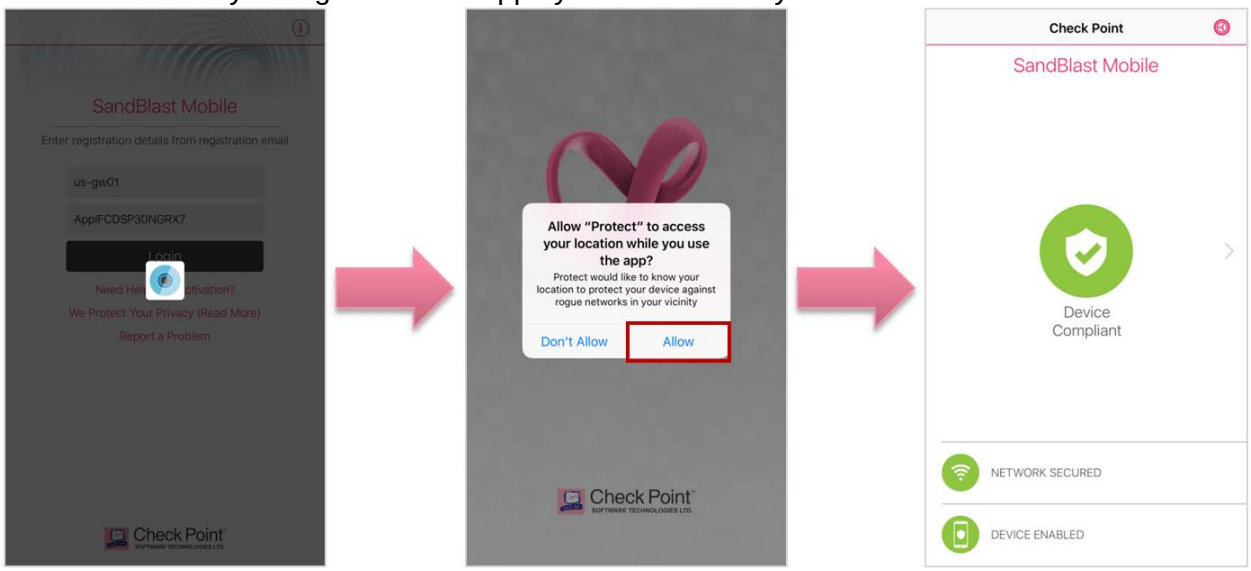
After the device is registered to the MaaS360 system and the SandBlast Mobile Protect app has been "Distributed" to the Device Provisioning Group ("MTP_Devices"), the user will be prompted to install the SandBlast Mobile Protect App.

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.

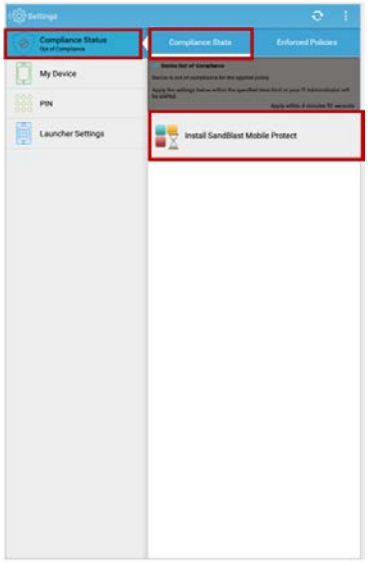
5.2 Registration of an Android Device

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.

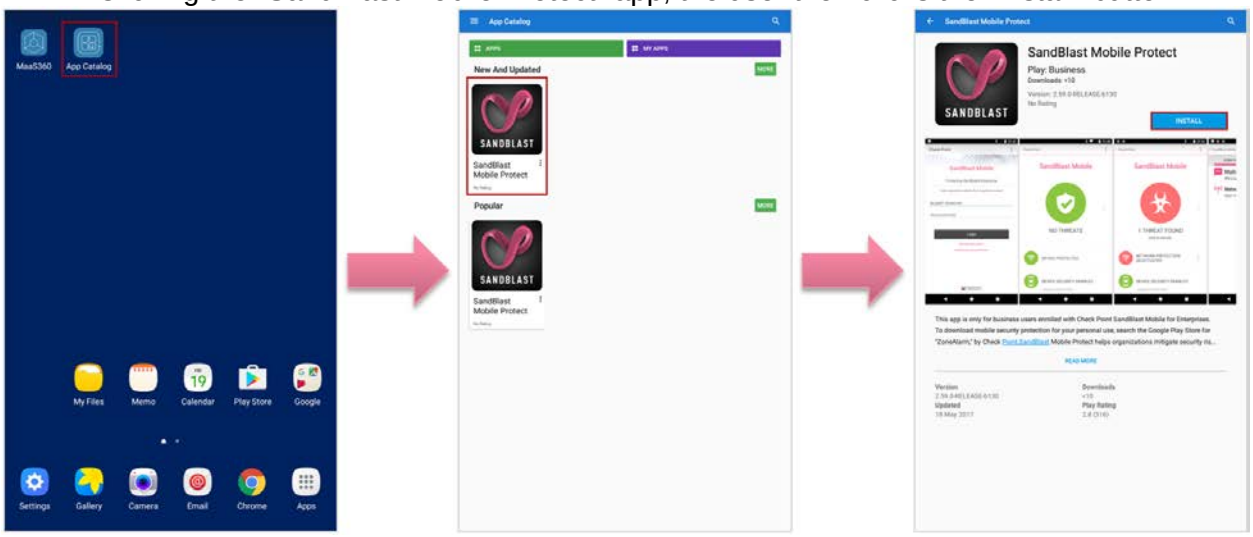


5.2.1.3. Skip to Section 5.2.3 to continue with the app installation.

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.

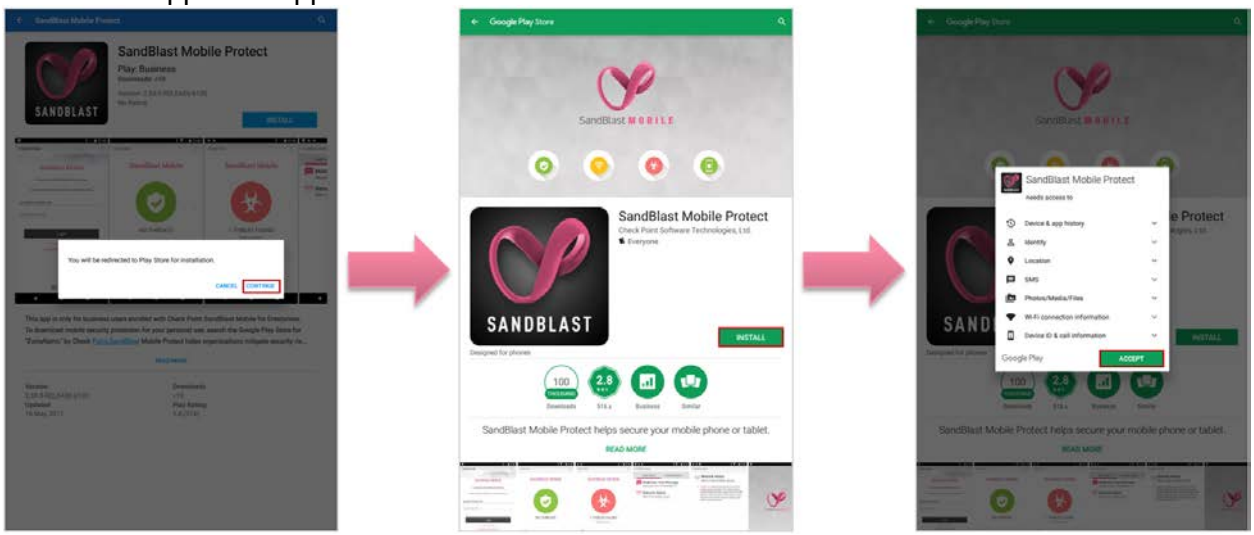


5.2.2.3. Proceed to Section 5.2.3 to continue with the app installation.

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.

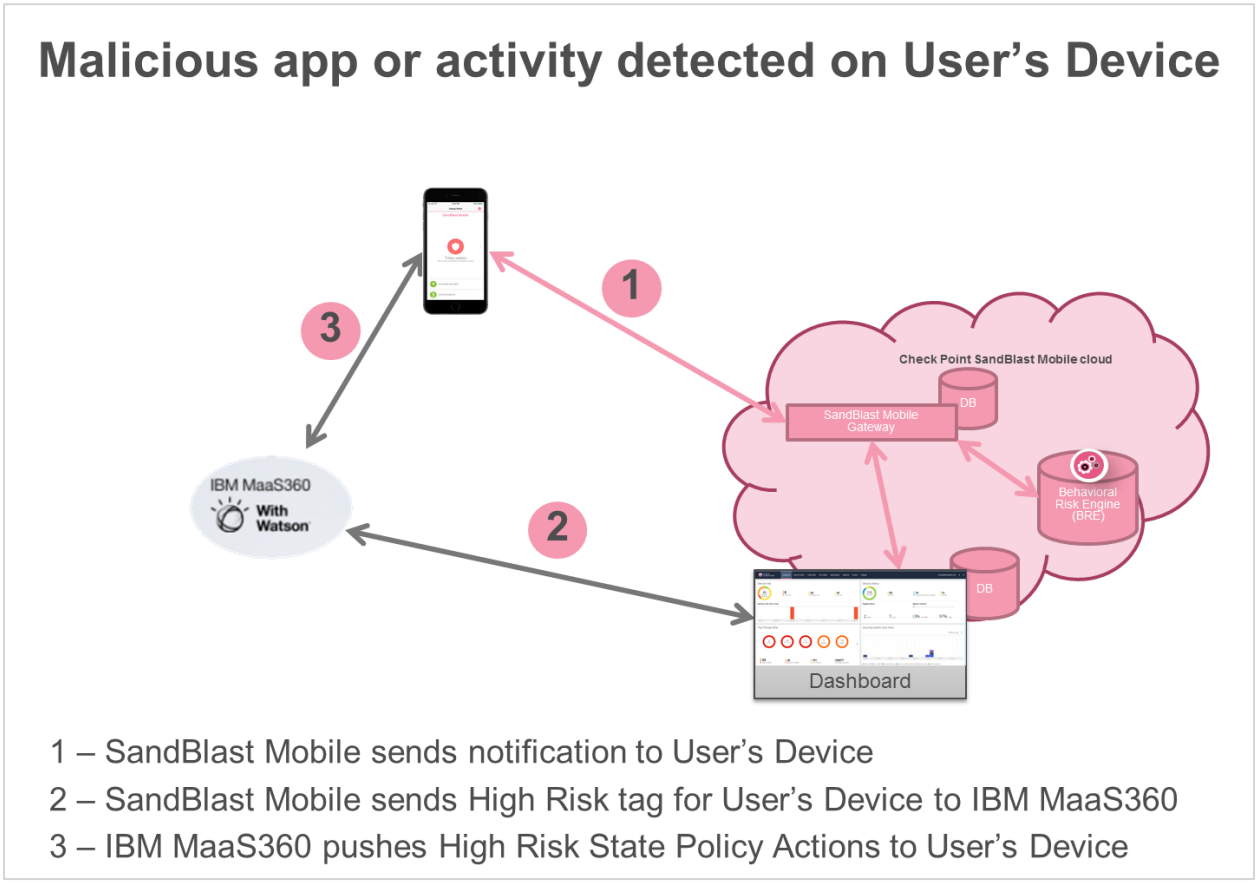


5.2.3.3. After the App is installed, the user must launch the App to finish its deployment and registration to SandBlast Mobile.

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



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.

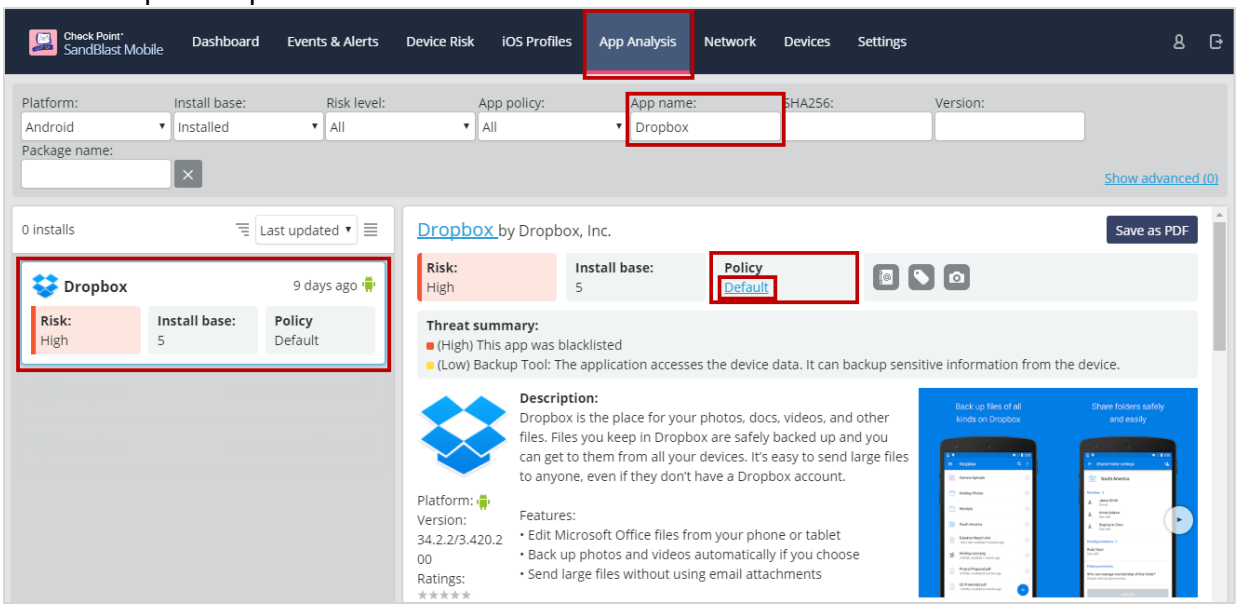
In the following example, the Administrator will blacklist an app, such as in our example "Dropbox". As a result, the user's device will be identified to be at High Risk due to the blacklisted app, "Dropbox", being installed on the device. The SandBlast Mobile Dashboard will notify the user, and mark 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”.

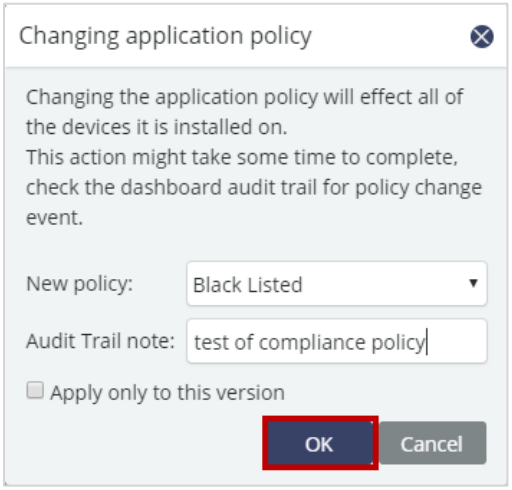
6.1.1. Log into the SandBlast Mobile Dashboard.

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”.

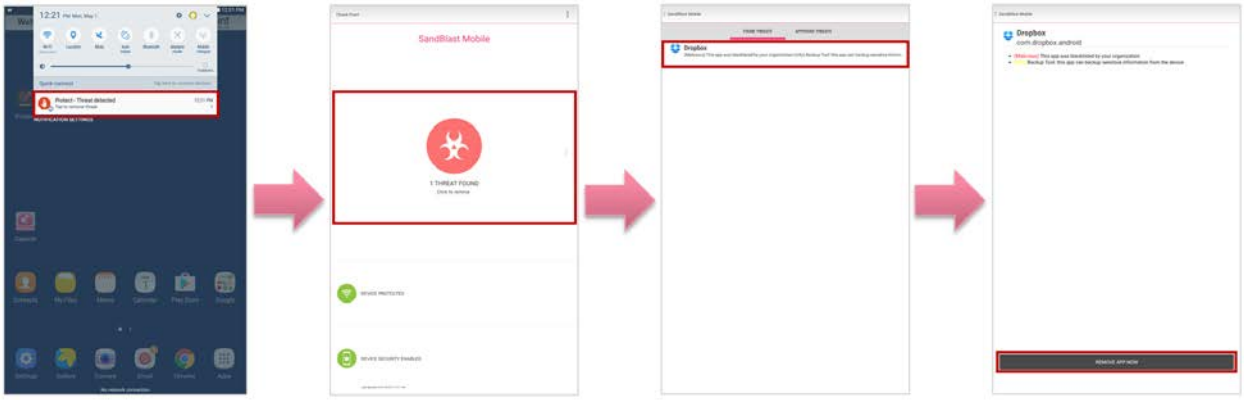


6.1.5. Click the “OK” button.

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".

To ensure timely and successful delivery of email from MaaS360, add maas360@fiberlink.com to your address book.

Policy Violation Alert

Device Name: fmulder-SM-T567V
Username: fmulder (fmulder@cptme.us)
Policy Violation: Device is at High Risk

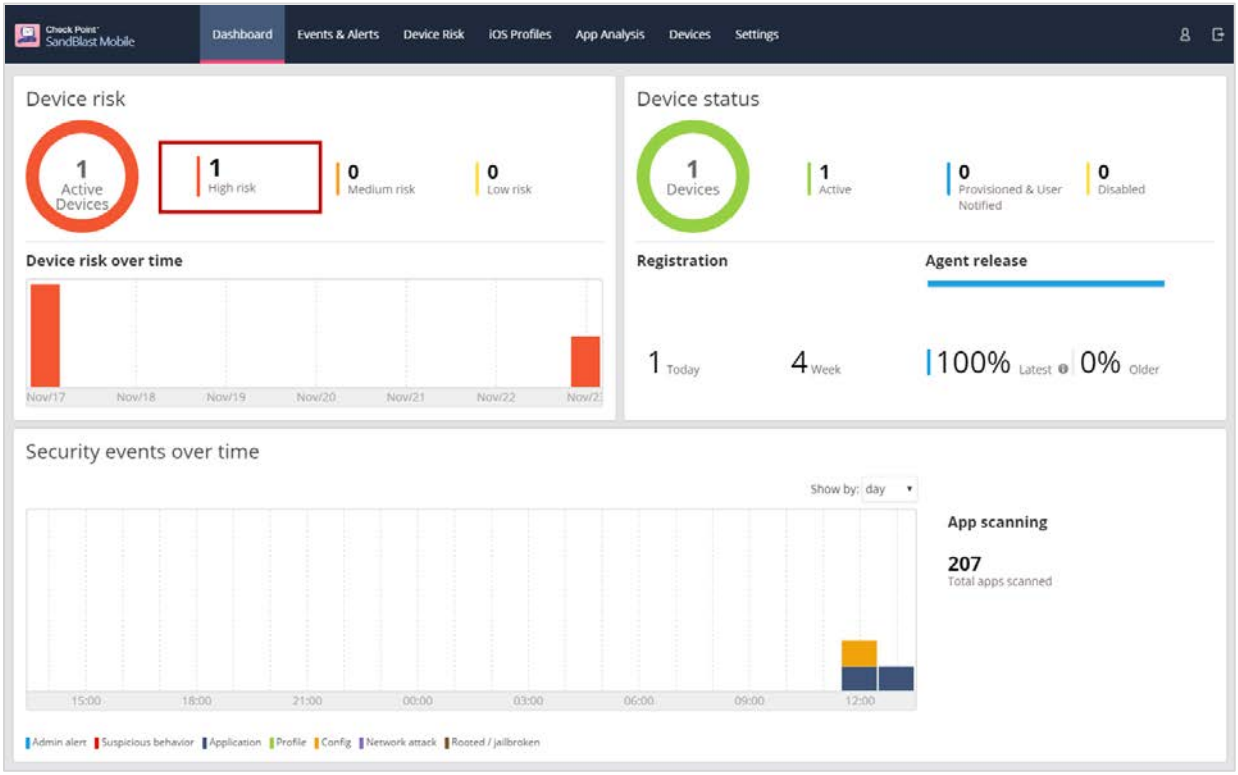
Review executed and planned enforcement actions below:

Action(s) Performed:
Change Policy. MDM Policy will be changed on your device.
Action(s) Planned: None

Instructions from Admin: Your device has been flagged as High Risk. Please see the SandBlast Mobile Protect app and/or your email for further instructions to remediate the issues.

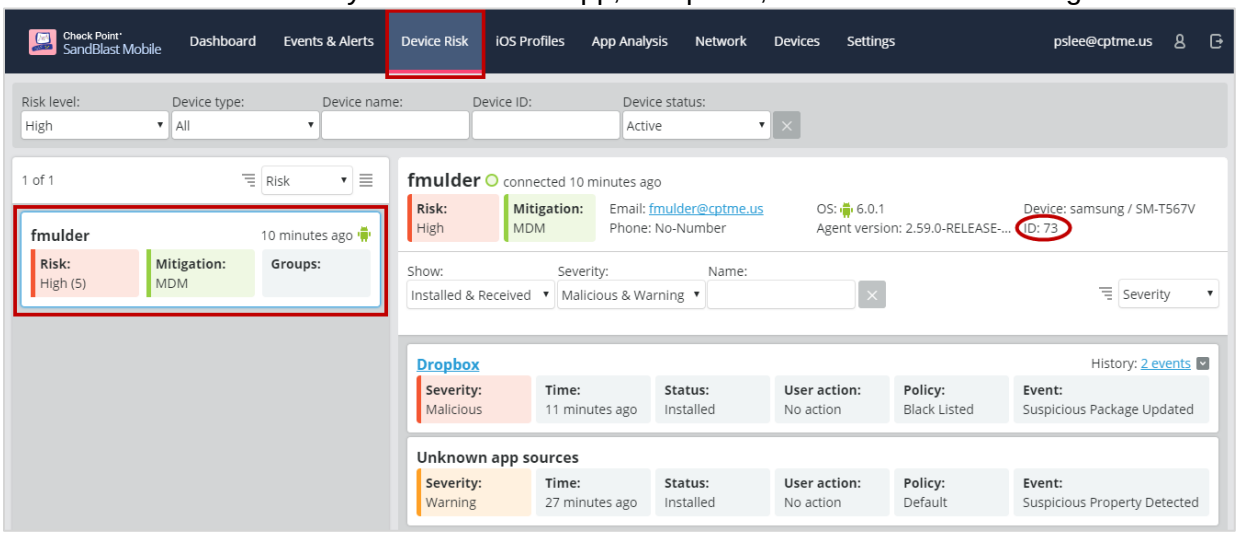
6.3 Administrator View on the SandBlast Mobile Dashboard

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



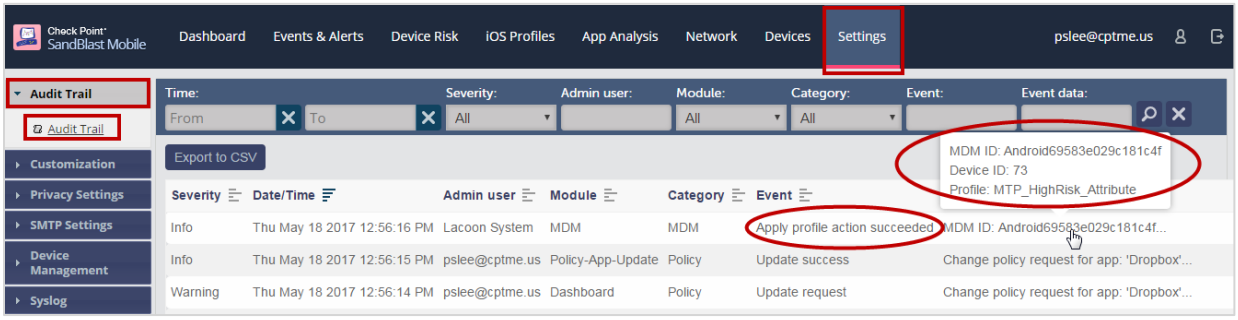
6.3.2. Clicking the High Risk will display a list of devices at high risk.

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.



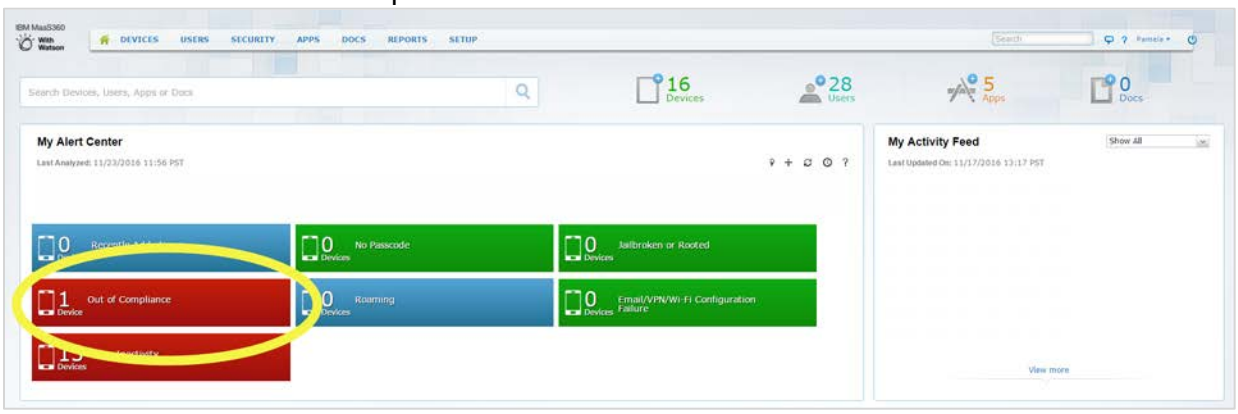
6.3.4. Navigating to **Settings > Audit** Trail, the Administrator will see that there was an alert sent to the MDM, and hovering over the Event Data information, it will pop-up the Event that was sent.

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.



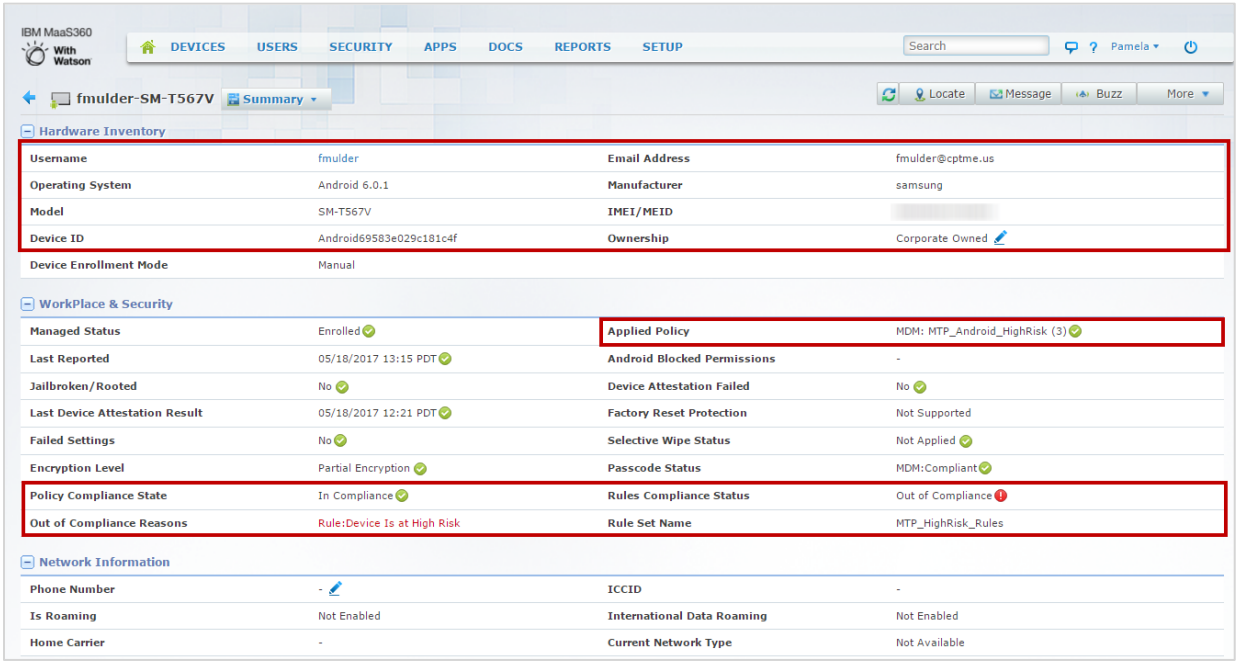
6.4 Administrator View on the MaaS360 Portal

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

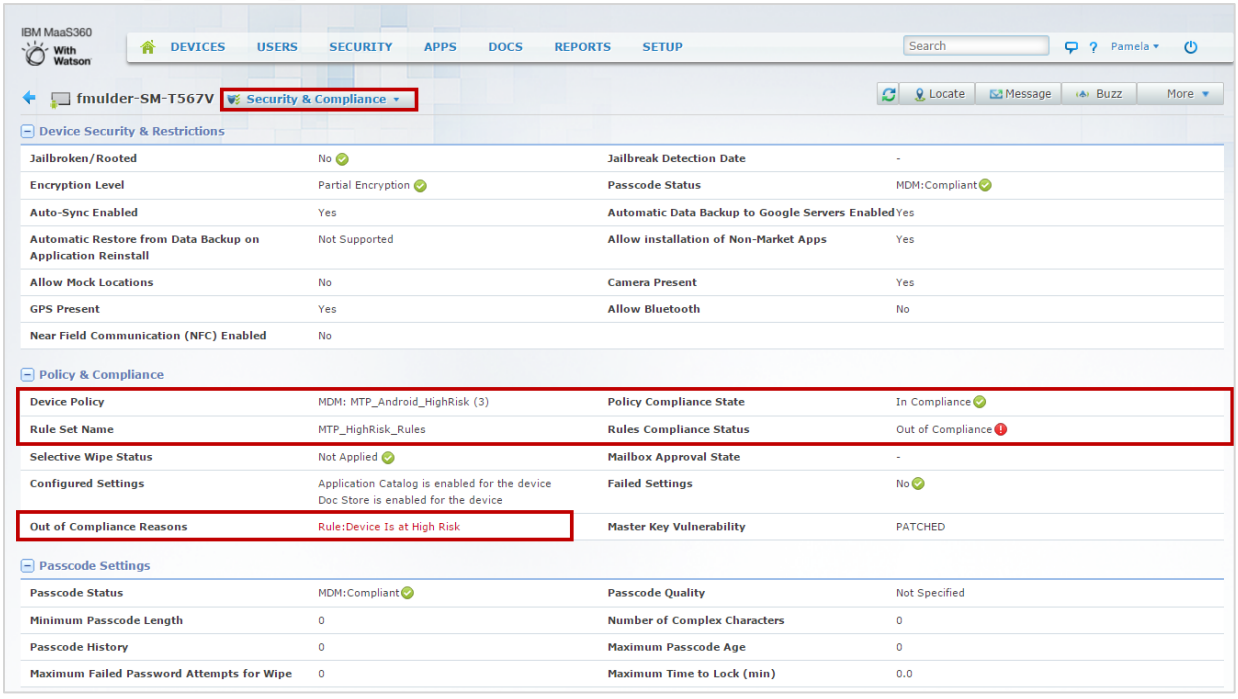


6.4.2. Clicking the “Out of Compliance” button, the Administrator is presented with a list of the devices currently “Out of Compliance”.

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

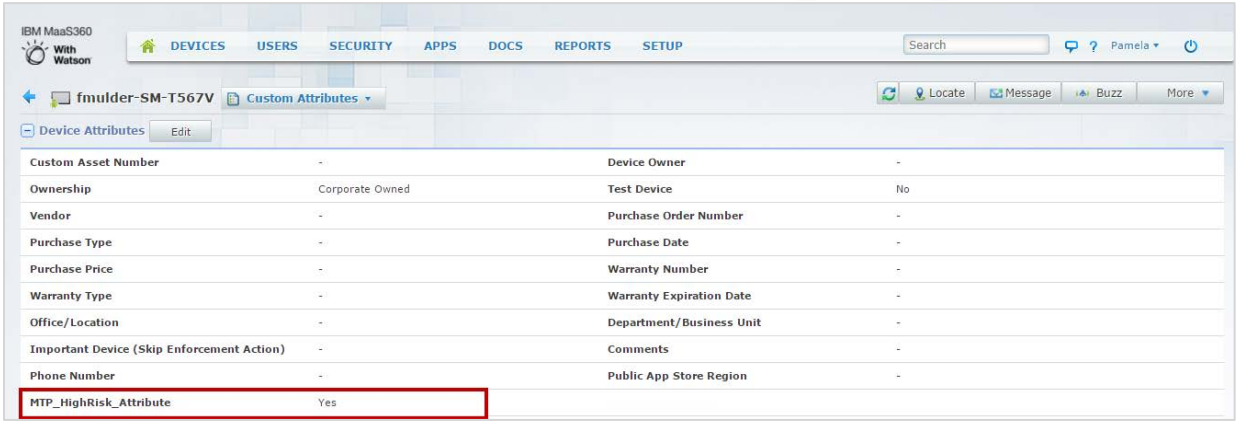


6.4.4. Clicking on the “Summary” drop-down menu, the Administrator can choose “Security & Compliance” details. The Administrator can see that the device is “Out of Compliance” because of the device belongs to the “MTP_Android_HighRisk” policy, with the compliance rule of “Device is at High Risk” under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

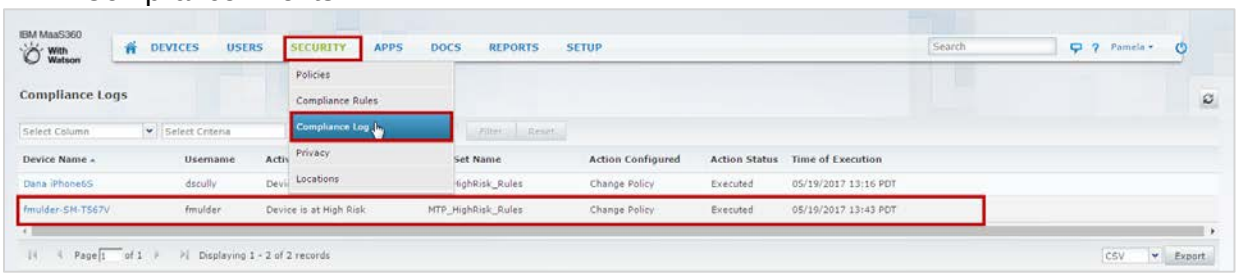


6.4.5. Clicking on the “Security & Compliance” drop-down menu, the Administrator can choose “Custom Attributes” details. The Administrator can see which custom attributes are currently set.

6.4.6. The Administrator can see that the device has the “MTP_HighRisk_Attribute” set to “Yes”.



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



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 mtp-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

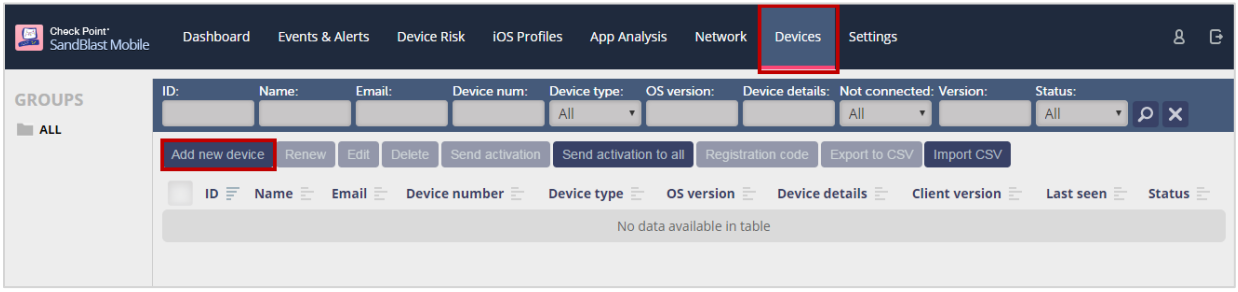
In order to prevent spam filters from blocking SandBlast Mobile's emails, the following IP address should be allowed as a sender: 167.89.59.134.

7.2 Discovering your SandBlast Gateway Name and Region

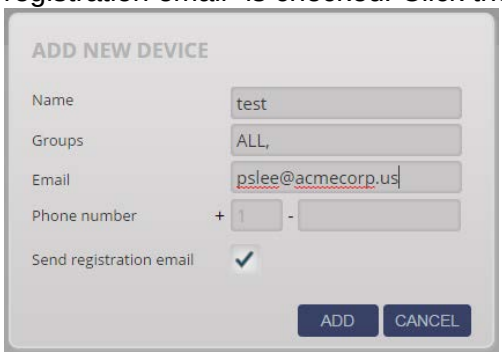
If you do not know your SandBlast Mobile Dashboard's region, please follow these instructions.

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.3333300.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

