Lookout® Mobile Endpoint Security

Deploying Lookout with IBM MaaS360

February 2018

Lookout

Copyright and disclaimer

Table of contents

Preface

Lookout Mobile Endpoint Security (MES) provides comprehensive risk management across iOS and Android devices to secure against app, device, and network-based threats while providing visibility and control over data leakage. With a seamless integration to your EMM solution, Lookout empowers your organization to adopt secure mobility without compromising productivity.

About this guide

This guide describes how to deploy and integrate Lookout MES with your existing MaaS360 environment. It covers initial deployment for both the Lookout MES Console and the Lookout for Work mobile app.

Note that some screenshots may differ from your own MaaS360 configuration.

Audience

This guide is for administrators, business users, and mobile security engineers who administer and support Lookout with IBM MaaS36.

Typographic conventions

The following table describes the typographic conventions used in this document.

Typeface	Meaning
User interface elements	This formatting is used for graphical user interface elements such as pages, dialog boxes, buttons, and field labels.
`Code sample`	This formatting is used for sample code segments.
<*Variable*>	This formatting is used for variable values. For variables within a code sample the formatting is <*`Variable`*>.
`File/path`	This formatting is used for filenames and paths.
>	The right angle bracket, or greater-than sign, indicates menu item selections in a graphic user interface, e.g., **File > New > Tag**.

Overview

1. Create an API user in MaaS360.
2. Create MaaS360 Custom Attributes to indicate device states.
3. Configure the MaaS360 Connector from the MES Console.
4. Add the Lookout for Work app to MaaS360 App Catalog and deploy it to your users.
5. Monitor device status in Lookout MES to see when users activate Lookout for Work on their devices.
6. Create iOS and Android Security Policies.
7. Create Device Groups in MaaS360 for each of the MES threat levels (Low, Moderate, and High Risk).
8. Create a Compliance Policy Rule Set to apply your iOS and Android Security Policies to devices in the corresponding Device Group.

Requirements

See the Lookout Mobile Endpoint Security Supported Platforms document for supported platform information.

MaaS360 requirements:

- **MaaS360** On-premises or SaaS, tenant version **10.x**
- **Administrator - Level 2** access to the MaaS360 Admin Portal

Lookout requirements:

- If you are deploying Lookout for Work on Android, contact Lookout Enterprise Support to request an `.apk` app file with the embedded Global Enrollment Code for your Lookout MES tenant. If you are running multiple Lookout MES tenants, you must request a separate `.apk` for each tenant.

Preparing MaaS360 for Integration

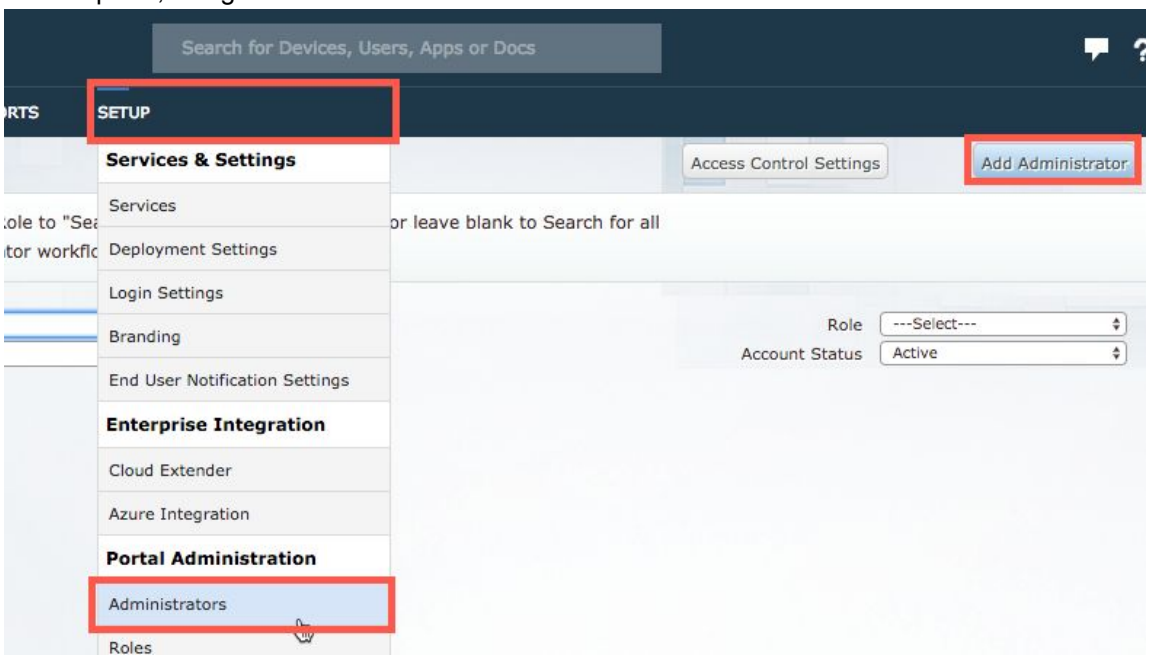
Before creating a MaaS360 Connector in the Lookout Mobile Endpoint Security (MES) Console, you must login to your MaaS360 Admin Portal and do the following:

1. Create an API User to act as the connection between Lookout and MaaS360.
2. Add custom attributes to communicate device status between Lookout and MaaS360.

Creating an API User

As a best practice, you should create an API User for use solely between Lookout and MaaS360. This ensures that communication between Lookout MES and MaaS360 is restricted to a single set of credentials.

1. Log in to your MaaS360 Admin Portal.
2. In the top bar, navigate to **SETUP > Administrators** and click **Add Administrator**:



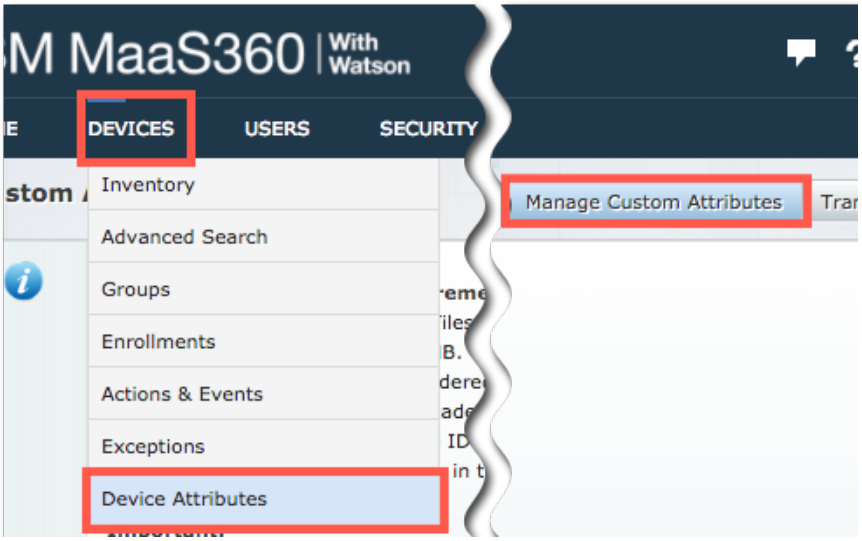
3. Fill out the email address and username information and click **Next**.
4. Grant the **Administrator** role and click **Next**:

5. Click **Save**.
6. Log in to the MaaS360 Admin portal as the new API User to verify that you have access.

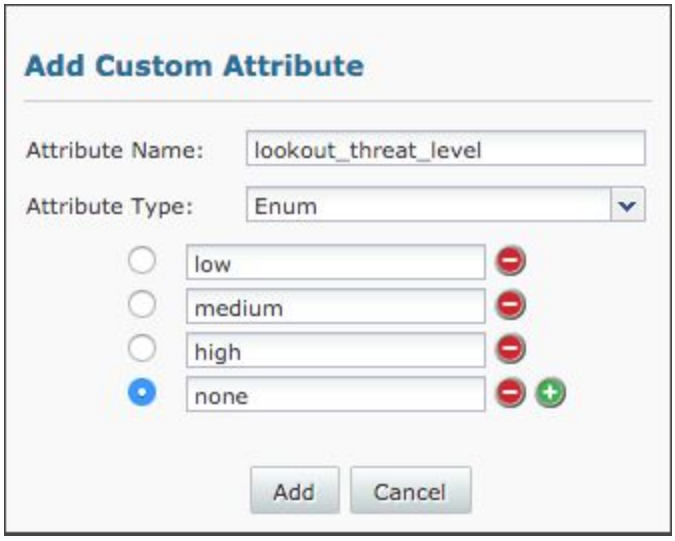
Creating Custom Attributes for Device State Sync

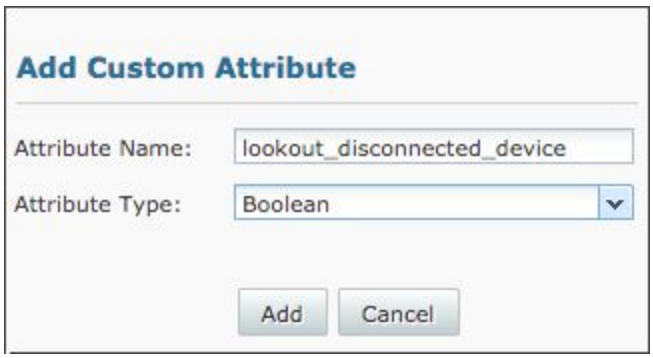
Lookout uses MaaS360 Custom Attributes to synchronize device state to MaaS360. These attributes are required to configure the MaaS360 Connector in the Lookout MES Console. To add them:

1. In the MaaS360 Admin Portal, navigate to **DEVICES > Device Attributes** and click **Manage Custom Attributes**:



2. Click **Add Custom Attribute** and create the following attributes:





Attribute Name	Attribute Type	Values

`lookout_device_state`	Enum	`secured`
		`threats_detected`
		`deactivated`
		`none` (default)
		
		IMPORTANT: These values are case-sensitive.

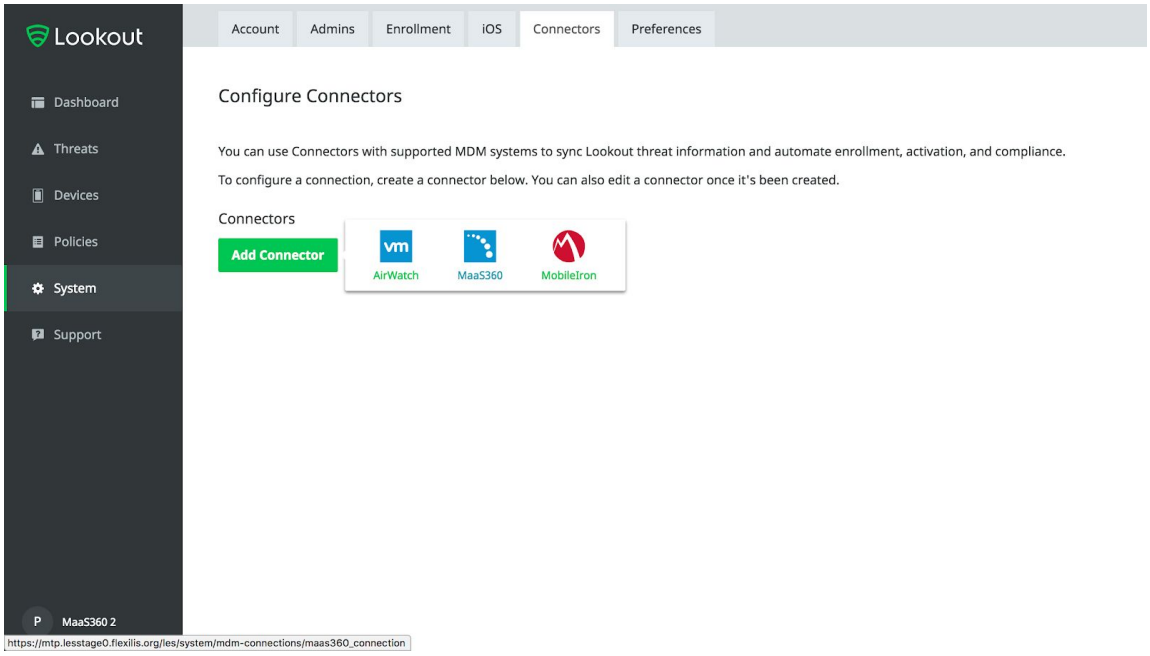
`lookout_threat_level`	Enum	`low`
		`medium`
		`high`
		`none` (default)
		
		IMPORTANT: These values are case-sensitive.

`lookout_disconnected_device`	Boolean	

Setting up your MaaS360 Connector in the Lookout Mobile Endpoint Security Console

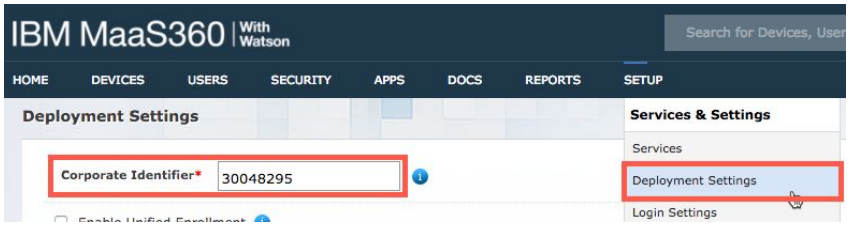
Once you have configured MaaS360, you can set up a connector in the Lookout MES Console.

1. Log in to the Lookout MES Console at https://app.lookout.com.
2. In the left sidebar, click **System > Connectors** then click **Add Connector**.
3. Click **MaaS360**:



4. Enter the following:

Field	Value
MaaS360 URL	The API Root URL for your MaaS360 server. This varies by the MaaS360 instance on which your account exists: • M1: https://services.fiberlink.com/ • M2: https://services.m2.maas360.com/ • M3: https://services.m3.maas360.com/ Your administrator should have an email from IBM with this information.
Admin Email	Enter the MaaS360 Username (which may not necessarily be an email address) and Password from Creating an API User.
Admin Password	

Access Key **App ID**	Your administrator should have an email from IBM with this information. If you still do not know your MaaS360 API Key or Application ID, refer to the IBM developerworks wiki. **IMPORTANT:** According to the article above, for MaaS360 SaaS customers, estimated completion time for this request is one week.
Billing ID	Your corporate identifier. In MaaS360, navigate to **SETUP > Deployment Settings**:  Your **Corporate Identifier** is listed at the top of the page.

5. Click **Create Connector**.
   If creation is successful, the other configuration tabs become enabled.
6. Click **State Sync** and enter the custom attributes you created in Creating Custom Attributes for Device State Sync:

Field	Value	Enabled?
Custom attribute used to set device state	`lookout_device_state`	**ON**
Custom attribute set when device is disconnected	`lookout_disconnected`	**ON**
Custom attribute with issue state level, if any	`lookout_threat_level`	**ON**

   If you choose not to synchronize a specific state, toggle off the corresponding item.

7. Click **Save Changes**.
8. Click **Error Management** and enter an email address for error reporting.
9. Click **Save Changes**.
   Once configured, you can view connector settings in MES on the **System > Connectors** page.

Configuring Threat Classification in Lookout Mobile Endpoint Security

MES classifies mobile threats of various types, so that you can match different classifications to the risk levels they represent for your organization. All threat classifications initially reflect the default threat levels assigned by Lookout. Users with Full Access to the MES Console can modify the settings from the

Policies page:

MES sets the `lookout_threat_level` custom attribute to reflect the risk level of a device based on the settings in the Policies page.

Adding Lookout for Work to MaaS360

Adding the Lookout for Work iOS and Android applications to the MaaS360 App Catalog makes it easy for users to download and install the Lookout mobile app. It also allows you to push updates automatically to ensure users are always on the latest version.

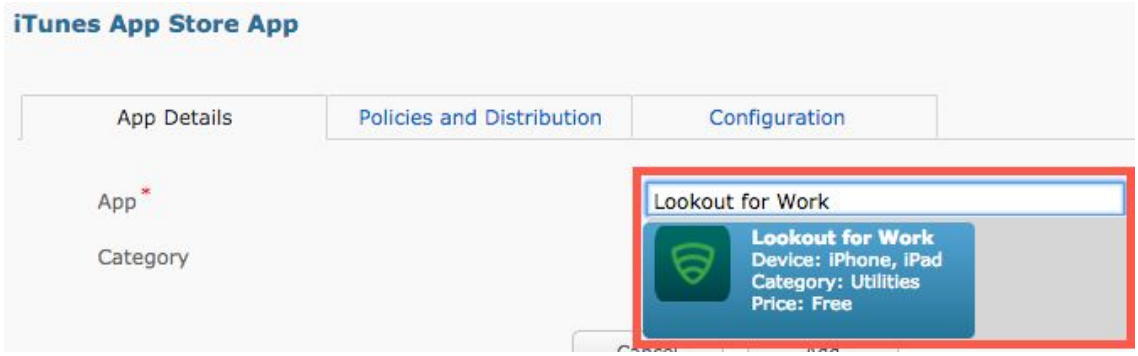
Follow the steps below for the version(s) of Lookout for Work that your organization uses.

Adding and Deploying the iOS App Store Lookout for Work App

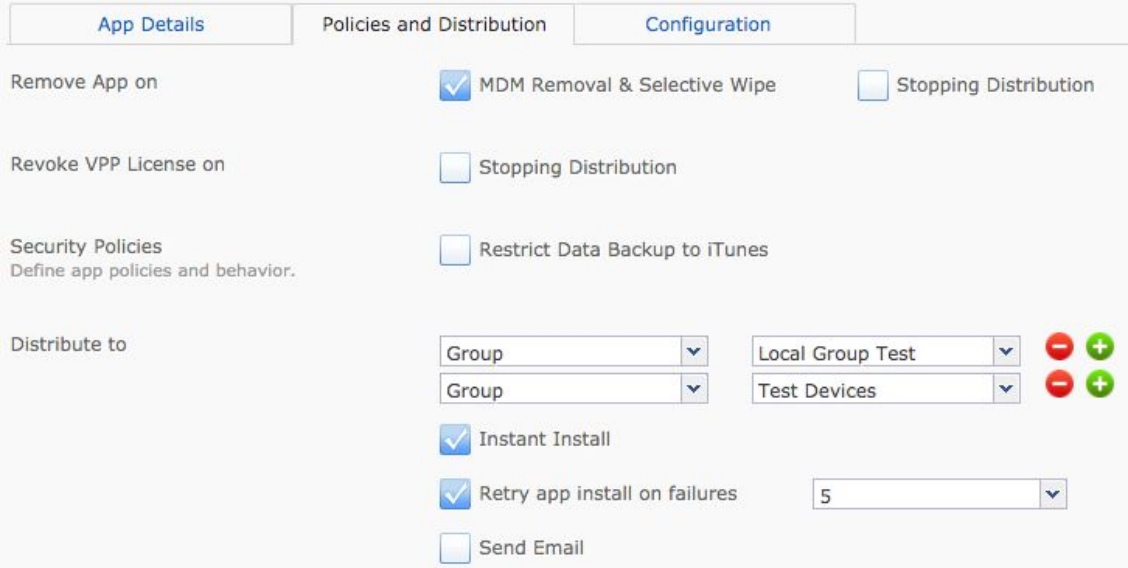
1. Log in to the MaaS360 Admin Portal.
2. Navigate to **APPS > Catalog** and click **Add > iOS > iTunes App Store App:**

The iTunes App Store App window appears.

3. From the App Details tab, in the **App** field, enter `Lookout For Work` and click the **Lookout for Work** app:



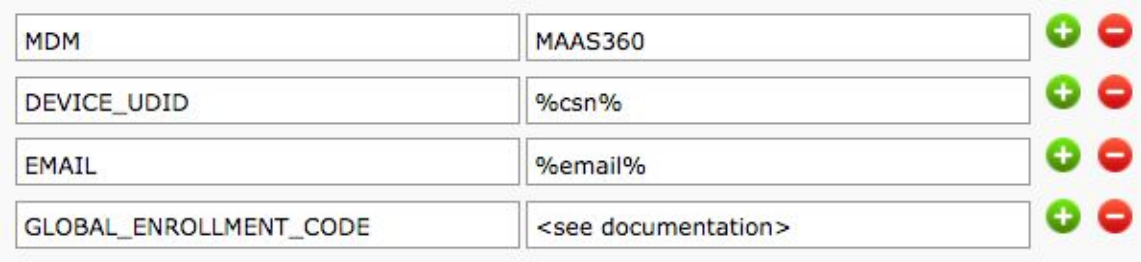
4. Click the **Policies and Distribution** tab, then set the following:

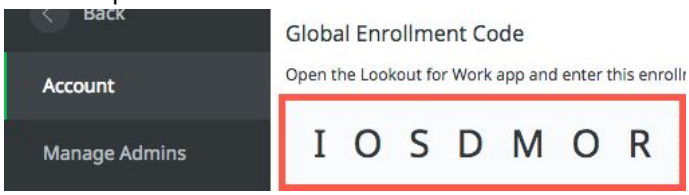


Setting	Value
Remove App on	MDM Removal & Selective Wipe
Distribute to	Set to **Group** and select your test user group. Add additional groups or individual devices if necessary.
Instant Install	Enabled
Retry app install on failures	Enabled, **5**

5. Click the **Configuration** tab, then in the **App Config Source** dropdown select **Key/Value**:

6. Click the **+** button to add more key/value pairs and create the following entries:



Key	Value
MDM	MAAS360
DEVICE_UDID	%csn%
EMAIL	%email%
GLOBAL_ENROLLMENT_CODE	Enter the 7 letter Enrollment Code from the **System > Account** screen in your Lookout MES Console. For example: 

7. Click **Add**, then enter your password and click **Continue**.
   MaaS360 adds the app.

Adding and Deploying the iOS In-House Lookout for Work App

Lookout distributes an In-House edition of the Lookout for Work iOS app outside of the Apple App Store. Before distributing this version of the app, you must sign it using your iOS Enterprise Developer Certificate.

> **NOTE:** You must use a Mac device to complete this task.

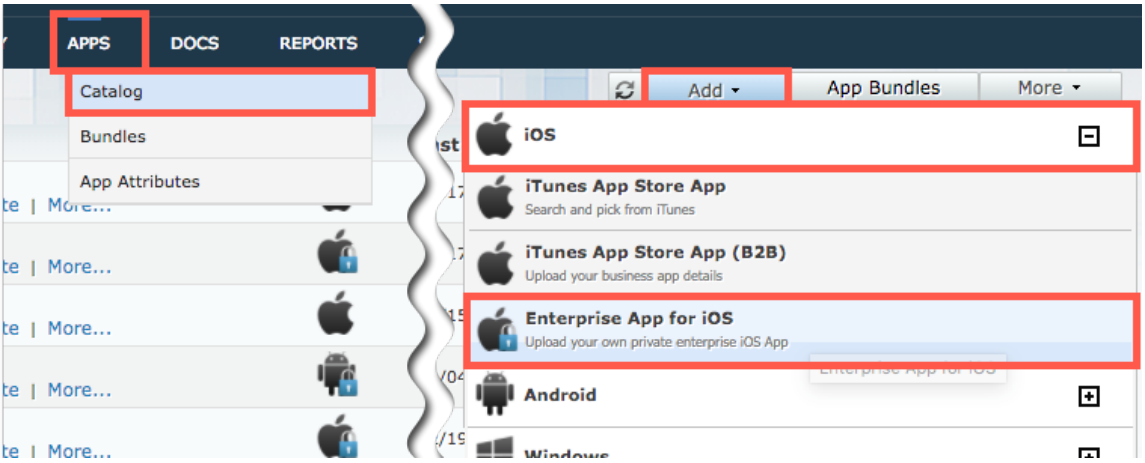
For details, see iOS App Re-Signing Process on the Lookout Enterprise Support Portal. Make note of your new Bundle ID (for example, `com.lookout.enterprise.AcmeInc`), as you'll need it to configure MaaS360.

> **NOTE:** It is important to upload the Lookout for Work IPA to the Mobile Endpoint Security Console (Step 6 in the document linked above), even though you are using MaaS360 to distribute the app. This step validates that the app was re-signed correctly and also helps set up your iOS Sideloaded App Whitelist by automatically whitelisting apps that were signed with your iOS

Enterprise Developer Certificate. This reduces the number of sideloaded app detections you see when you first roll out Lookout Mobile Endpoint Security (MES) to your test devices.

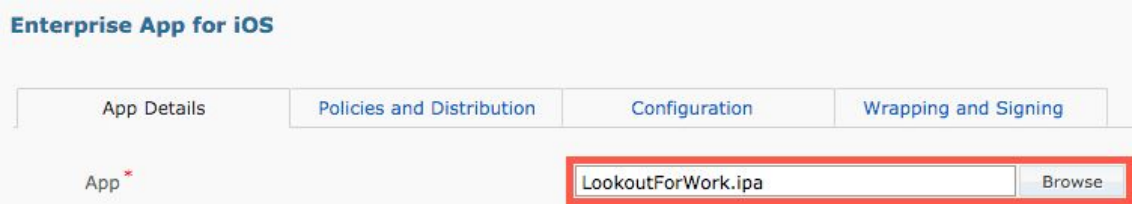
Once you have re-signed the app, you can add it to the MaaS360 App Catalog:

1. In the MaaS360 Admin Portal, navigate to **APPS > Catalog** and click **Add > iOS > Enterprise App for iOS:**

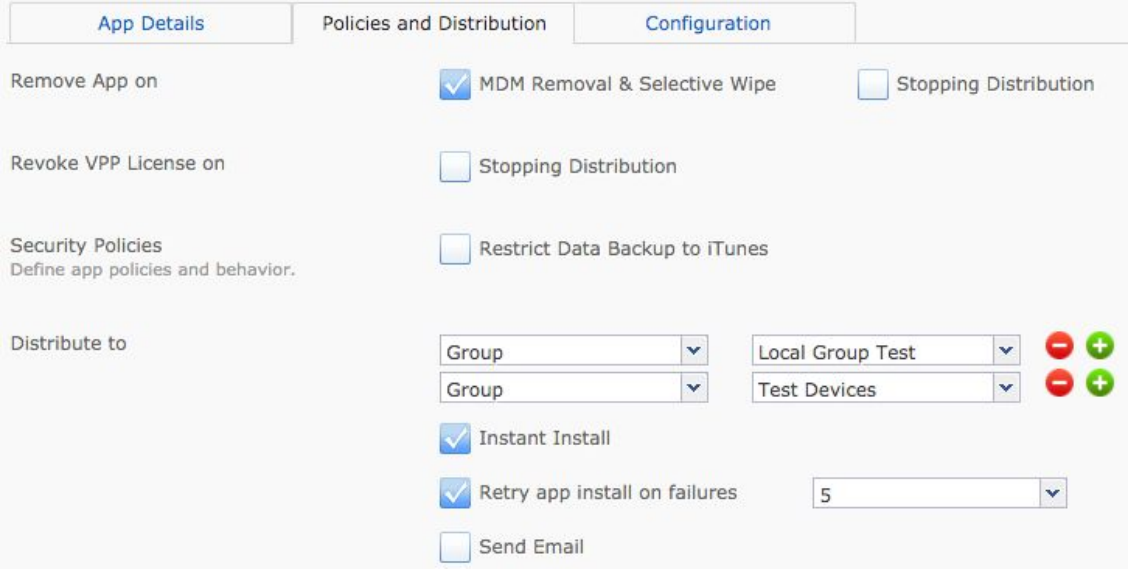


The Enterprise App for iOS window appears.

2. From the App Details tab, click **Browse** to upload the resigned `.ipa` file:



3. Click the **Policies and Distribution** tab, then set the following:



Setting	Value
Remove App on	MDM Removal & Selective Wipe
Distribute to	Set to **Group** and select your test user group. Add additional groups or individual devices if necessary.
Instant Install	Enabled
Retry app install on failures	Enabled, **5** (maximum)

4. Click **Add**, then enter your password and click **Continue**.
   MaaS360 uploads the app.

Adding and Deploying the Android Lookout for Work App

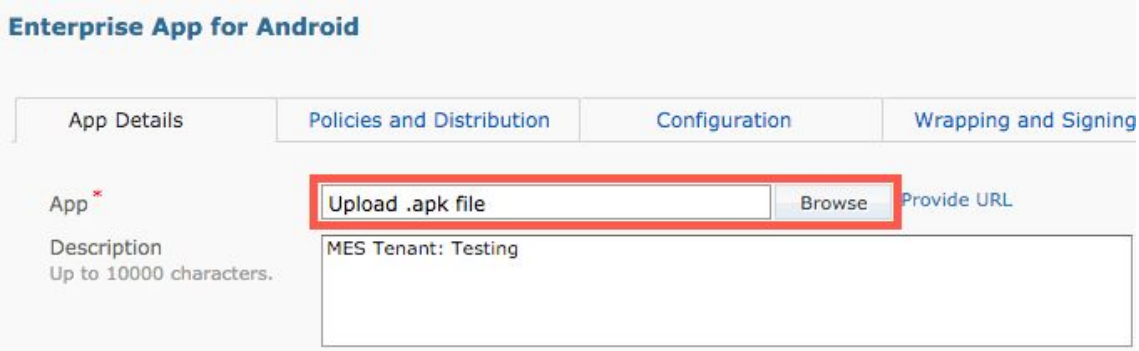
The Lookout Enterprise Support team embeds the Global Enrollment Code for your Lookout MES tenant in the Lookout for Work `.apk` file.

> **IMPORTANT:** Because this code is tenant specific, if you are running more than one Lookout MES tenant, repeat the steps below for each of them and be careful to assign the app to the correct set of devices.

For example, if you have an Lookout MES tenant for your test environment and one for production, add the `.apk` for your test environment first and only deploy that app to test devices. When you deploy in production, repeat these steps on your production instance of MaaS360 for the `.apk` that matches your production Lookout MES tenant.

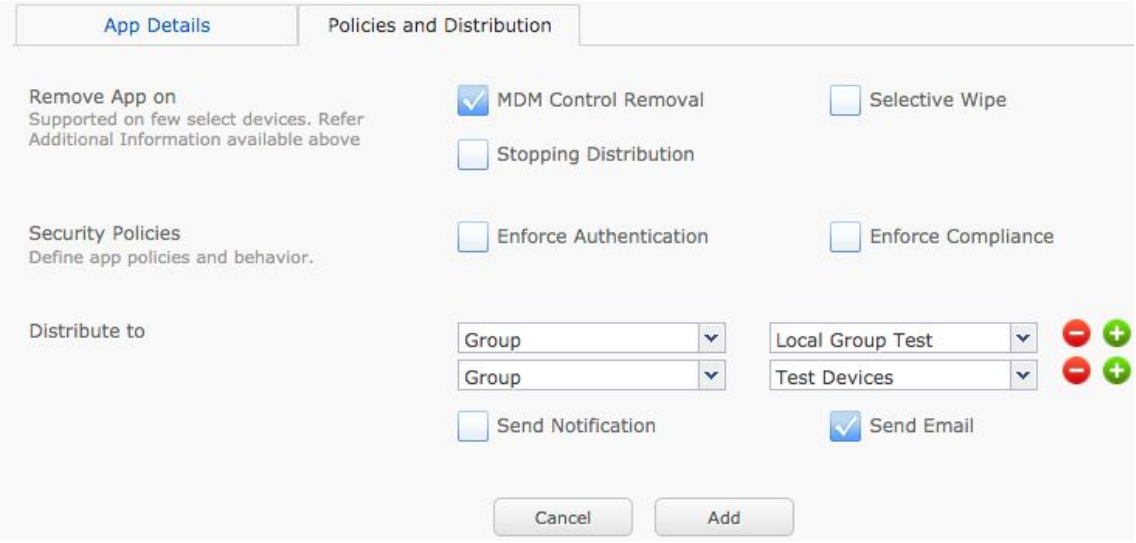
1. In the MaaS360 Admin Portal, navigate to **APPS > Catalog** and click **Add > Android > Enterprise App for Android:**

2. From the App Details tab, click **Browse** to upload the Lookout for Work `.apk` file provided by the Enterprise Support team:



IMPORTANT: The embedded Global Enrollment Code is tenant specific. Be sure to upload the `.apk` for the desired tenant, and deploy the app to the devices that you want to associate with that specific tenant.

3. In the **Description** field, enter the Lookout MES tenant for the app.
4. Click the **Policies and Distribution** tab, then set the following:



Setting	Value
Remove App on	MDM Control Removal
Security Policies	Configure based on your company requirements.
Distribute to	Set to **Group** and select your test user group. Add additional groups or individual devices if necessary.
Send Email	Enabled

5. Click **Add**, then enter your password and click **Continue**.
MaaS360 adds the app.

Monitoring Enrollment and Activation

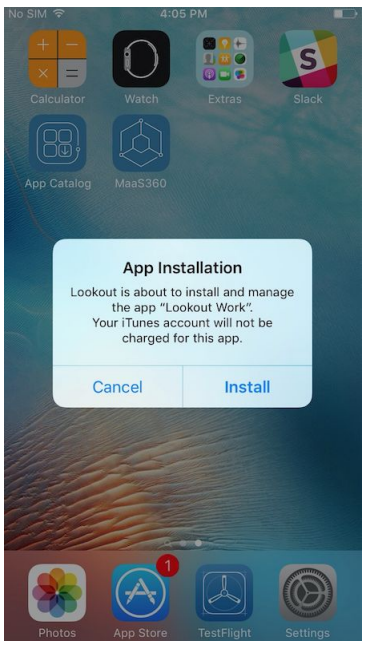
You can review the enrolled devices in a group from the MaaS360 Admin Portal. Navigate to **DEVICES > Groups** and click the group's **Devices** link (for Device groups) or **Users** link (for Local User or User Directory groups).

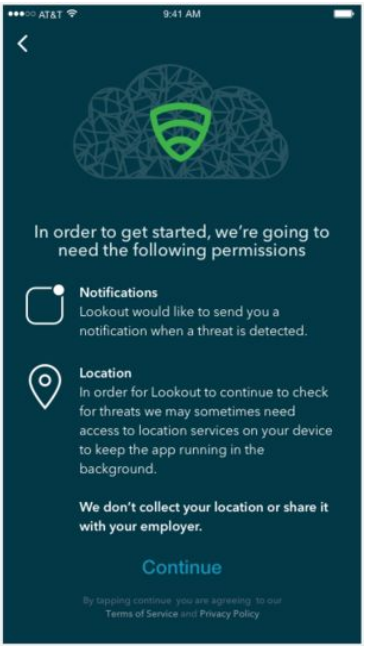
As users activate Lookout for Work, their devices appear on the Devices page of the Lookout MES Console with a value of "MaaS360" in the MDM column:

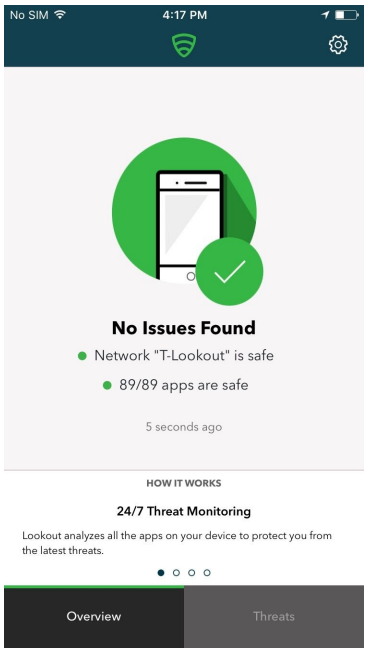
STATUS	DEVICE TYPE	MDM	CONNECTION
High Risk	iPhone 7 Plus iOS 11.2.2	MaaS360	Connected 21 hours ago
High Risk	Nexus 5 Android 5.0.1	MaaS360	Connected 7 days ago
Medium Risk	STUDIO M HD Android 5.1	MaaS360	Connected 2 days ago
Secured	iPhone 5s iOS 10.1.1	MaaS360	Connected 6 days ago

End User Device Activation

MaaS360 automatically pushes Lookout for Work to all of the devices you select in the Policies and Distribution tab when you create the app (as documented in Adding Lookout for Work to MaaS360). The device user must install the app, and then open it. On opening Lookout for Work, the user must click **Activate** if running a version of the app prior to 4.11 on iOS or 4.13 on Android. On later versions, the app activates automatically when opened and prompts for the required permissions:







NOTE: If the user declines permissions or closes the app, their device is still activated and secured in Lookout and in your MDM. Lookout cannot alert the user of issues without having device permissions, but it continues to report issues to the Lookout MES Console.

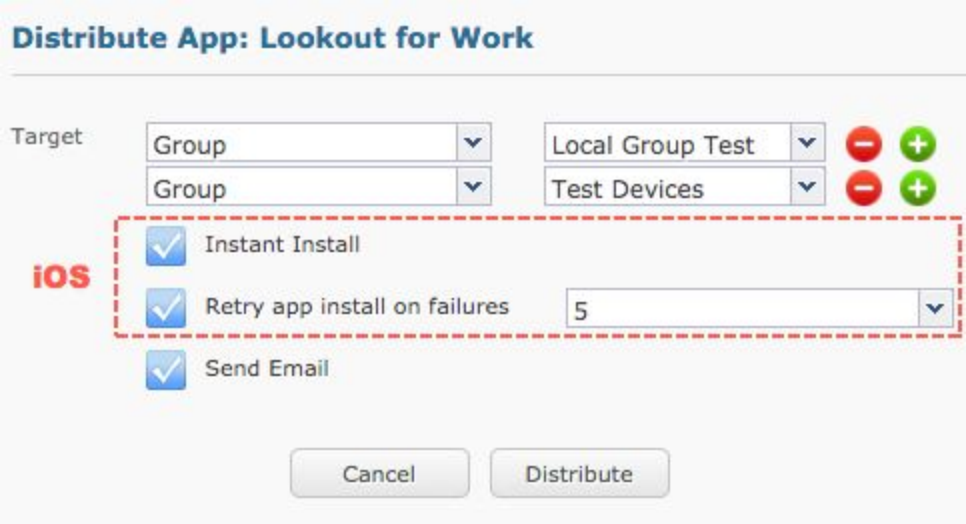
Deploying Lookout for Work to Additional Users

MaaS360 automatically pushes the app to any new devices registered for the configured Groups. For example, if you have Lookout for Work configured to distribute to devices in a “Lookout Enrollment” Group, then any new users or devices added to that group automatically receive the app.

To extend enrollment to additional groups or specific devices:

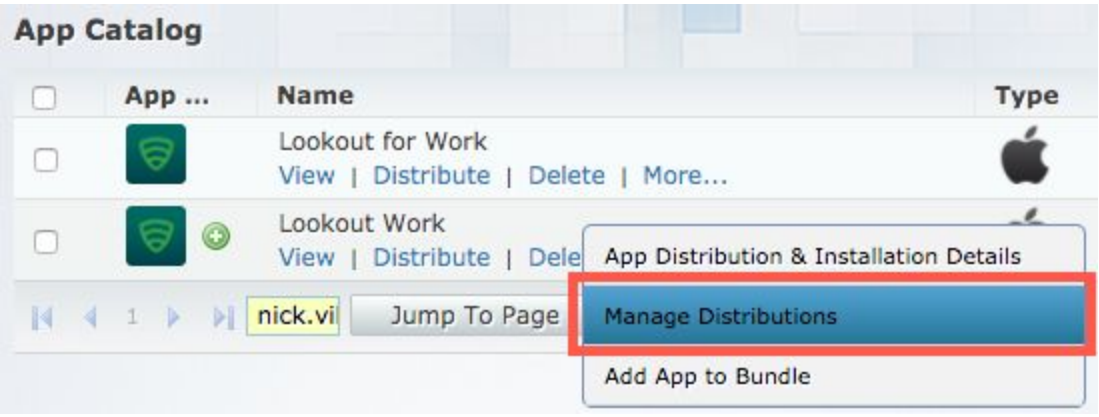
1. In the MaaS360 Admin Portal, navigate to **APPS > Catalog** and select the edition of Lookout for Work you want to distribute.
2. Click **Distribute**:

3. Set the following:



Setting	Value
Target	Set to **Group** and select your test user group. Add additional groups or individual devices if necessary.
(iOS app only) Instant Install	Enabled
(iOS app only) Retry app install on failures	Enabled, **5** (maximum)
Send Email	Enabled

4. Click **Distribute**.
5. Repeat Steps 2-4 if you are distributing both the iOS and Android versions of the app.
6. After distributing the app, you can review distributions by selecting it in the App Catalog and clicking **Manage Distributions**:



Configuring and Enforcing Security Policies

When Lookout detects a security issue on a protected device, it reports the device state in the `lookout_threat_level` custom attribute based on the risk levels you set during Configuring Threat Classification in Lookout Mobile Endpoint Security.

To take policy actions in MaaS360 based on risk levels reported by Lookout:

1. Optionally, create policies to enforce at each risk level.
   You may wish to only create policies for medium or high risk devices, and restrict actions for low risk devices to alerts and other low-impact measures.
2. Create a Device Group for each risk level.
3. For each risk level, create a Compliance Rule Set and set it to a Group Based Rule that applies to the corresponding Device Group.

Devices with the reported `lookout_threat_level` value are automatically moved into the corresponding group, and the Compliance Rule Set takes effect for those devices. When all active threats are remediated or removed, Lookout sets the `lookout_threat_level` to `none` and the device is returned to the previous (normal) Groups and associated policies in MaaS360.

Creating Security Policies

You can create Security Policies for each Lookout risk level. By starting each policy where the previous one leaves off, you can configure only the new actions for each severity level. For example, your “Lookout iOS High Risk Policy” should have the “Start From” value set to “Lookout iOS Medium Risk Policy”

1. In the MaaS360 Admin Portal, navigate to **SECURITY > Policies** and click **Add Policy**.
2. Set the following:

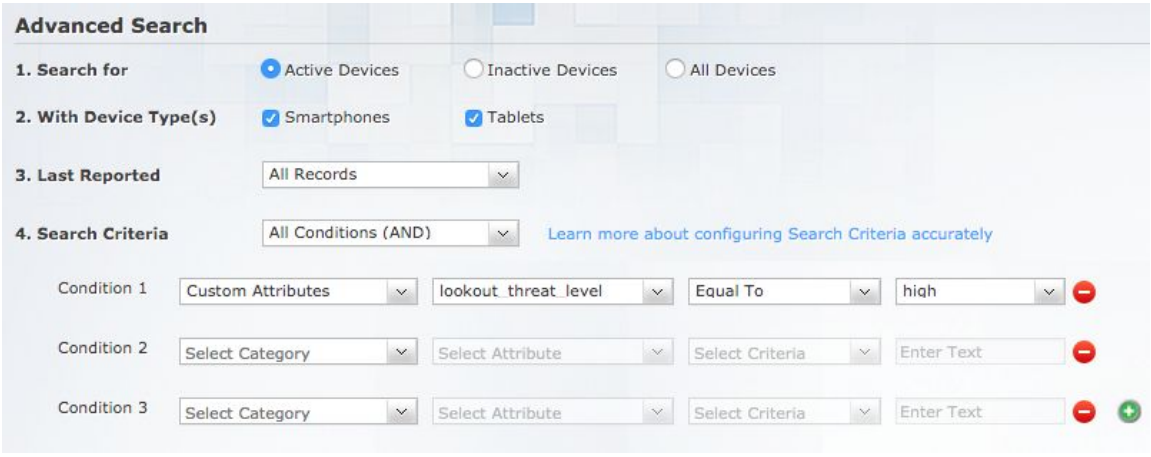
Setting	Value
Name	`Lookout <iOS / Android> <Low/Medium/High> Risk Policy`
Type	**iOS MDM** or **Android MDM**
Start From	• **For Low Risk:** Select your default device policy. • **For Medium Risk:** Select your Low Risk policy. • **For High Risk:** Select your Medium Risk policy.

3. Click **Continue**.
   MaaS360 creates the policy.
4. Configure the policy as desired.
5. Click **Save** to save the policy as a draft, or **Save and Publish** to publish.
6. Repeat the Steps above until you have the desired set of policies for both iOS and Android devices.

For more information about creating device policies, see the IBM documentation here: https://www.ibm.com/support/knowledgecenter/en/SS8H2S/com.ibm.mc.doc/pag_source/tasks/pag_sec_policies_managing.htm

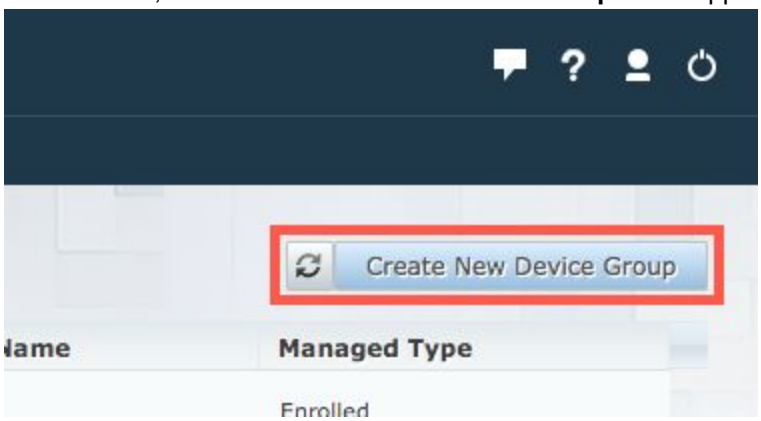
Creating Device Groups for Policy Actions

7. In the MaaS360 Admin Portal, navigate to **DEVICES > Groups** and click **Add > Device Group**.
8. Set the following:



Setting	Value
1. Search for	**Active Devices**
2. With Device Type(s)	**Smartphones, Tablets**
3. Last Reported	**All Records**
4. Search Criteria	**All Conditions (AND)**
Condition 1	**Custom Attributes, lookout_threat_level, Equal To, high**

9. Click **Search**, then click **Create New Device Group** in the upper-right corner:



10. In the **Group Name** field, enter `Lookout <Low/Medium/High> Risk Devices` and click **Save**.
11. Repeat Steps 1-4 above for **lookout_threat_level** values of **medium** and **low**.

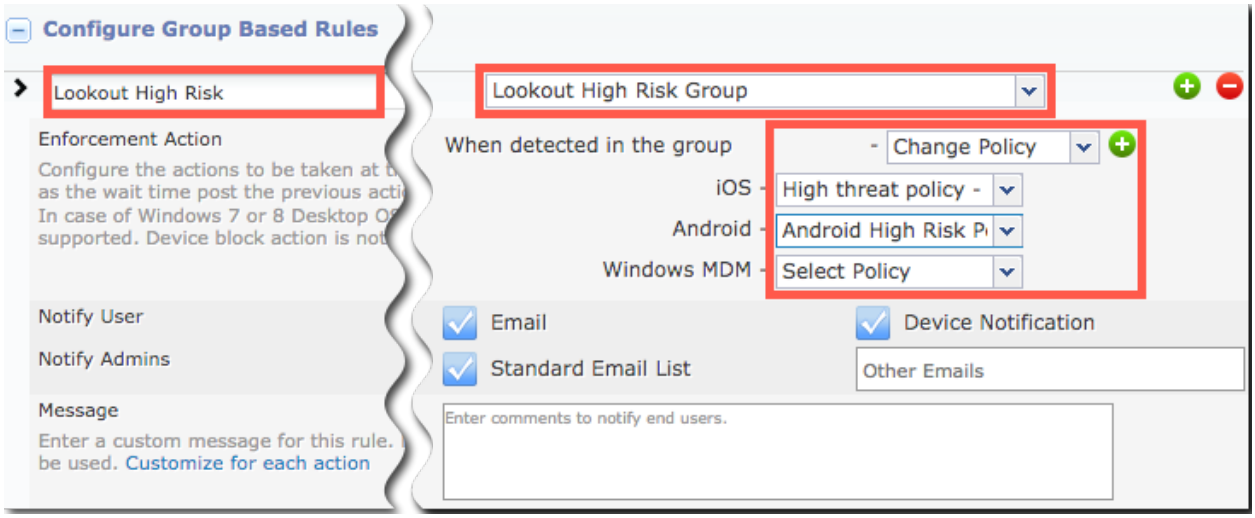
Using Lookout Risk Levels to Drive Compliance Rules

MaaS360 supports Compliance Rules which contain Group Based Rules. By mapping these Group Based Rules to the Device Groups you created for the different `lookout_threat_level` values, you can take policy actions on risky devices based on the severity of the risk.

1. In the MaaS360 Admin Portal, navigate to **SECURITY > Compliance Rules** and click **Add Rule Set**.
2. In the **Rule Set Name** field, enter `Lookout Risk Rules` and click **Continue**.
3. Click the **Group Based Rules** tab and click **Add New Rule**.
4. Set the following:

Setting	Value
Enter Rule Name	`Lookout Low Risk`
No Group Selected	**Lookout Low Risk Devices**

5. Set the **Enforcement Action**, notification settings, and custom **Message** based on your organization's requirements. For example, the rule below applies the **High threat policy** against iOS devices in the group, and the **Android High Risk Policy** against Android devices:



You can click the **+** icon beside the Enforcement Action to add more actions as time passes after the original event.

6. Click the **+** icon on the right side of the rule to add a new rule.
7. Repeat Steps 4-6 until you have created rules for low, medium, and high risk devices, then click **Save**.