

Lookout® Mobile Endpoint Security

# Lookout® Mobile Endpoint Security Console

## Administrator's Guide

March 2018

# Copyright and disclaimer

Copyright © 2018, Lookout, Inc. and/or its affiliates. All rights reserved.

Lookout, Inc., Lookout, the Shield Logo, and Everything is OK are registered trademarks of Lookout, Inc. Android is a trademark of Google Inc. Apple, the Apple logo, and iPhone are trademarks of Apple Inc., registered in the U.S. and other countries. App Store is a service mark of Apple Inc. UNIX is a registered trademark of The Open Group.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing at [enterprisesupport@lookout.com](mailto:enterprisesupport@lookout.com).

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

**U.S. GOVERNMENT END USERS:** Lookout, Inc. programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Lookout, Inc. and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

This software or hardware and documentation may provide access to or information on content, products and services from third parties. Lookout, Inc. and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Lookout, Inc. and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

# Table of contents

[Copyright and disclaimer](#)

[Table of contents](#)

[Preface](#)

[About this guide](#)

[Audience](#)

[Typographic conventions](#)

[Introduction to the Lookout Mobile Endpoint Security Console](#)

[Logging in to the MES Console](#)

[Switching the Active Console](#)

[MES Console Overview](#)

[Searching and Filtering Lists](#)

[Exporting Filtered Data](#)

[Configuring Notification and Summary Emails](#)

[Lookout Mobile Endpoint Security Console UI Reference](#)

[The Dashboard Module](#)

[Device Deployment](#)

[App Analysis \(MES Comprehensive\)](#)

[Issue Trends](#)

[Issue Detections Breakdown](#)

[The Issues Module](#)

[Filtering the Issue List](#)

[Issue Details](#)

[The Devices Module](#)

[Device Details](#)

[The Apps Module \(MES Comprehensive\)](#)

[App Details](#)

[Analyzing an App](#)

[Blacklisting and Un-Blacklisting Apps](#)

[The Policies Module](#)

[Whitelisting Non-App Store Signers and Sideloaded Apps](#)

[Defining Custom Policies for Apps \(MES Comprehensive\)](#)

[The Account Module](#)

[The Manage Admins Module](#)

[The Enrollment Settings Module](#)

[Creating a Custom Invitation or Reminder Email](#)

[The Send Invites Module](#)

[The Manage Invites Module](#)

[Managing Invites](#)

[The iOS Configuration Module](#)

[The Connectors Module](#)

[The Application Keys Module](#)

# Preface

Lookout Mobile Endpoint Security (MES) provides comprehensive risk management across iOS and Android devices to secure against app, device, and network-based threats and vulnerabilities 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 serves as an overview of the Lookout MES Console and outlines the administrative tasks involved in managing users and devices, and responding to issues.

## Audience

This guide is for administrators, business users, and mobile security engineers who administer and support a Lookout deployment.

## Typographic conventions

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

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

# Introduction to the Lookout Mobile Endpoint Security Console

The Lookout MES (Mobile Endpoint Security) Console is the main interface for analyzing and responding to threats and vulnerabilities affecting your company's mobile devices. It monitors mobile devices from threats by malicious applications, or potential risks from benign apps that may be installed on a device. The MES Console provides a comprehensive view of applications installed on any device enrolled in Lookout's Mobile Endpoint Security product.

The Lookout for Work mobile application is the device-side agent, detecting threats on mobile devices and reporting the information to the end user and also to the console. Lookout for Work is available for iOS as an enterprise signed .ipa file or from the App Store. It is available for Android as an .apk file or from the Google Play Store.

This section serves as a guide for your initial login to the Lookout MES Console, so that you can find the information you need and set up your notification email preferences.

**NOTE:** If you are deploying Lookout for the first time, follow the steps in the Deployment Guide for your environment to integrate your MDM with Lookout:

- [Deploying Lookout with Microsoft Azure Active Directory and Intune](#)
- [Deploying Lookout with MobileIron](#)
- [Deploying Lookout with VMware AirWatch](#)
- [Deploying Lookout with IBM MaaS360](#)
- [Deploying Lookout with BlackBerry UEM](#)

## Logging in to the MES Console

You log in to the Lookout MES Console at <https://app.lookout.com>, or <https://aad.lookout.com> for Azure Active Directory integrations.

Lookout creates MES Console Administrators for the users your company requests during initial setup. New Administrators receive a welcome email that directs them to the console and prompts them to set a password.

**IMPORTANT:** Deployments with Microsoft Azure Active Directory and Intune require an AAD Global Administrator to accept initial consent before users can log in to MES. For more information, see [Deploying Lookout with Microsoft Azure Active Directory and Intune](#).

## Switching the Active Console

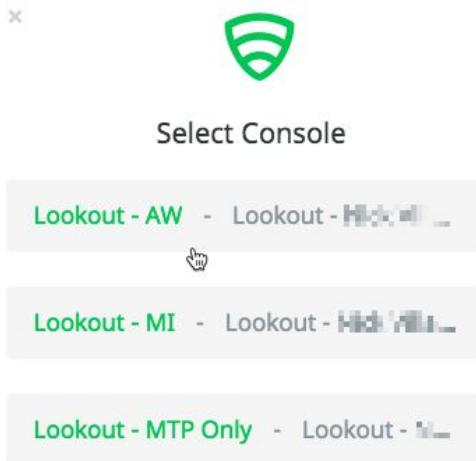
If you have access to the MES Console for multiple tenants, such as test and production environments, Lookout prompts you to select one on login. Once you are logged in, you can switch between tenants using the Switch Console option in your user menu:

1. Click on your username at the bottom of the Navigation Bar and click **Switch Console**:



A dialog appears that lists your available consoles.

2. Select the console you wish to access:



## MES Console Overview

The Navigation Bar on the left side of the MES Console lists the available modules. Click any of the links in the left column to read about a module in detail:

Module	Description
<a href="#">Dashboard</a>	The landing module for the MES Console. The Dashboard provides an overview of Devices, Risks, and Active Issues. It also features App Analysis information if you have purchased Lookout MES Comprehensive.
<a href="#">Issues</a>	Lists both Active and Resolved Issues, as well as the affected device and the detection date.  You can click an issue for additional information. You can also filter the list as described in <a href="#">Filtering Search Results</a> .
<a href="#">Devices</a>	Lists Active, Inactive, and Disconnected devices.

	You can click a device for more information. You can also filter the list as described in <a href="#">Filtering Search Results</a> .
<a href="#">Apps</a>	<p><b>(MES Comprehensive customers)</b> Lists apps detected on enrolled devices, including the app version, operating system, number and percentage of devices running the app, detection date, and detected security violations.</p> <p>You can click an app for more information. You can also filter the list as described in <a href="#">Filtering Search Results</a>.</p>
<a href="#">Policies</a>	<p>Review and set the policies for different issue classifications, including assigning a severity level (Low, Medium, or High) and setting a Response (Alert or Don't Alert the user on the affected device).</p> <p>Compliance actions, such as restricting an affected device from your network, are typically handled by an MDM based on the severity level information sent by Lookout.</p>
<a href="#">System</a>	Replaces the Navigation Bar with the System bar. See below.
<a href="#">Support</a>	Opens the Lookout Enterprise Support Portal in a new browser tab. Use your Lookout MES Console login credentials to log in. From here, you can access product documentation or file a ticket with the Support team.

## System Modules

The System bar includes the modules below:

Page	Description
<a href="#">Account</a>	Displays your company account information including organization, license usage, and the global enrollment code for manually adding devices to your Lookout MES tenant.
<a href="#">Manage Admins</a>	<p>Lists all MES Console Administrators. You can add new Administrators from here, or search the list by name or email.</p> <p><b>NOTE:</b> For Azure Active Directory integrations, you do not modify Admin users from this module. Instead, add new administrators directly to the AAD Groups specified in the Intune Connector.</p>
<a href="#">Enrollment Settings</a>	<p><b>(Non-MDM deployments)</b> If you are not using a Mobile Device Management (MDM) solution, you can enroll devices directly from the MES Console. If you are running Lookout alongside an MDM, you should send invitations from the MDM, as documented in the corresponding Deployment Guide.</p> <p>Review and set the maximum number of devices to enroll from a single Lookout for Work invitation email, as well as the expiration period before the invitation becomes invalid. You can also set the disconnection period before</p>

	a device is considered unenrolled.
<a href="#"><u>Send Invites</u></a>	<b>(Non-MDM deployments)</b> Send Lookout for Work invitation emails by uploading a <code>.csv</code> file or by manually entering a list of email addresses.
<a href="#"><u>Manage Invites</u></a>	<b>(Non-MDM deployments)</b> Lists email invite information, including date sent, recipient email address, status, device quota, reminders sent, expiration date, and enrollment token.  You can archive invites to remove them from the list. You can also filter the list as described in <a href="#">Filtering Search Results</a> .
<a href="#"><u>iOS Configuration</u></a>	Review and set the deployment method and other options for the iOS Lookout for Work app.  Depending on your tenant configuration, this module may contain options for uploading the Enterprise Signed Lookout for Work <code>.ipa</code> file, or it may require a link to the App Store edition of Lookout for Work.
<a href="#"><u>Connectors</u></a>	Review and configure MDM connectors.
<a href="#"><u>Application Keys</u></a>	Review and generate application keys for communicating with Lookout from your SIEM application.

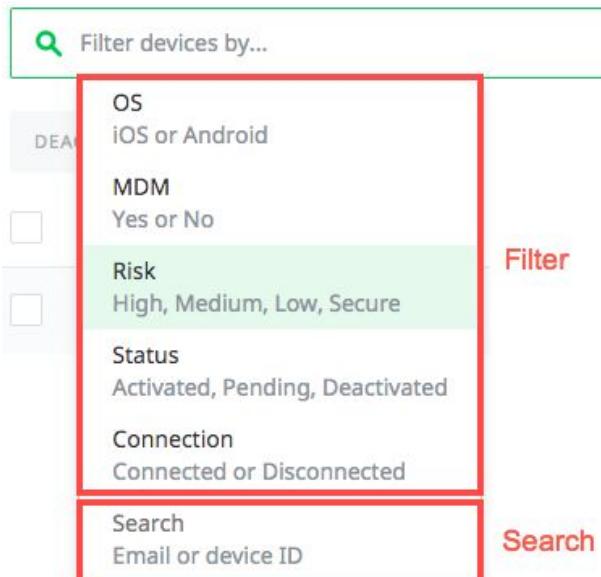
## Searching and Filtering Lists

Most of the modules in the Lookout MES Console support text search, as well as filtering based on the available columns. You can also sort many of the columns in Ascending or Descending order.

To search or filter a list on a module:

1. Click the Search field.

A list displays with the available filters, as well as the searchable fields at the bottom:



Filter devices by...

DEA

OS  
iOS or Android

MDM  
Yes or No

Risk  
High, Medium, Low, Secure

Status  
Activated, Pending, Deactivated

Connection  
Connected or Disconnected

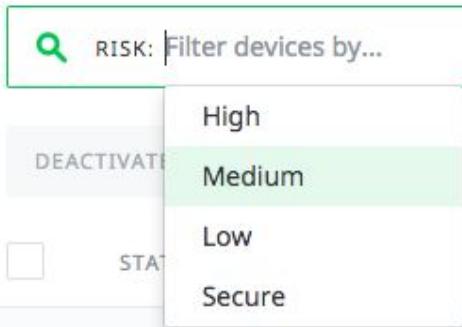
Search  
Email or device ID

Filter

Search

2. To search, enter your query text. To filter, click a filter.

The filter list is replaced with a list of available values:



3. Click a value.

The list is filtered based on the value, and the search bar is updated to indicate the active filter:



4. To apply multiple filters, repeat Steps 1-3 as many times as desired.

You can also add multiple values for the same filter:



For multiple values, such as Risk: Medium and Risk: Low, the results display items matching any of the values. A filter for **OS: Android, Risk: Medium, Risk: Low** returns Android devices that are Risk: Medium and Android devices that are Risk: Low.

5. To remove a filter, click its **X** icon.

You can filter the modules below for the listed fields:

- **Issues:** Discovered In last x days, Risk, Status, OS, Issue Type, Classification
- **Devices:** OS, MDM, Risk, Status, Connection
- **Apps:** Data Access, Cloud Service, Malware, Data Transfer, Source, OS, Blacklisted, Custom Policies

## Exporting Filtered Data

Several modules have an **Export Data** button in the top-right. This operation exports information to a **.csv** file. It respects any active filters, so if you are viewing the Issues page and have it filtered to Risk: High, then the MES Console exports a list of only High Risk issues.

## Configuring Notification and Summary Emails

By default, new MES Console Administrators receive notification emails for any Medium or High severity issues, plus weekly summary emails. You can modify these settings from your **My Preferences** module.

1. Click on your username at the bottom of the Navigation Bar and click **My Preferences**:



2. Toggle the notification and summary emails you want to receive:

My Preferences SAVE

Personal Info

Name

Email Notifications

High Risk Issue Notifications  ON

Medium Risk Issue Notifications  ON

Low Risk Issue Notifications  ON

Daily Summary  OFF

Weekly Summary  OFF

Monthly Summary  OFF

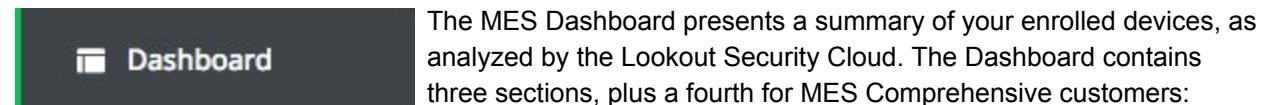
Quarterly Summary  OFF

3. Click **Save**.

# Lookout Mobile Endpoint Security Console UI Reference

This reference provides detailed information about the modules in the MES Console.

## The Dashboard Module



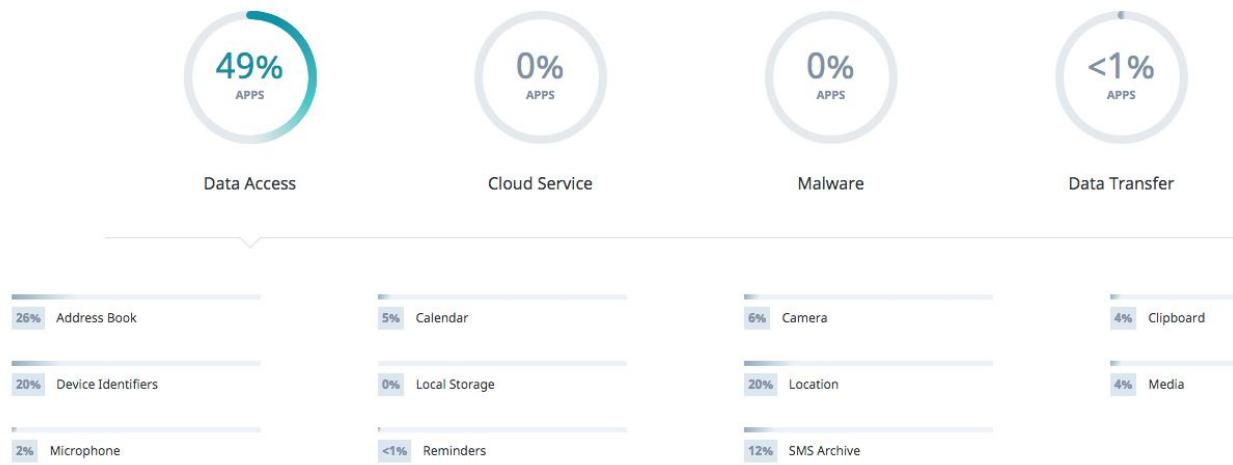
### Device Deployment

Device Deployment	Deployment Risk	Active Issues																												
<span>1 Activated Device</span> <span>1 Disconnected Device</span>	<span>0 High Risk Devices</span>	<table><thead><tr><th></th><th>High</th><th>Med</th><th>Low</th></tr></thead><tbody><tr><td>Total</td><td>0</td><td>0</td><td>0</td></tr><tr><td>App</td><td>0</td><td>0</td><td>0</td></tr><tr><td>Config</td><td>0</td><td>0</td><td>0</td></tr><tr><td>File</td><td>0</td><td>0</td><td>0</td></tr><tr><td>Network</td><td>0</td><td>0</td><td>0</td></tr><tr><td>OS</td><td>0</td><td>0</td><td>0</td></tr></tbody></table>		High	Med	Low	Total	0	0	0	App	0	0	0	Config	0	0	0	File	0	0	0	Network	0	0	0	OS	0	0	0
	High	Med	Low																											
Total	0	0	0																											
App	0	0	0																											
Config	0	0	0																											
File	0	0	0																											
Network	0	0	0																											
OS	0	0	0																											
<span>0 Pending Devices</span>	<span>0 Medium Risk Devices</span>																													
<span>0 Deactivated Devices</span>	<span>0 Low Risk Devices</span>																													

Device Deployment reflects a summary of the devices enrolled in the MES application, the risk to each device, and active issues across devices. This summary can be used as a “quick view” to understand what you should address in order to mitigate threats to the organization.

## App Analysis (MES Comprehensive)

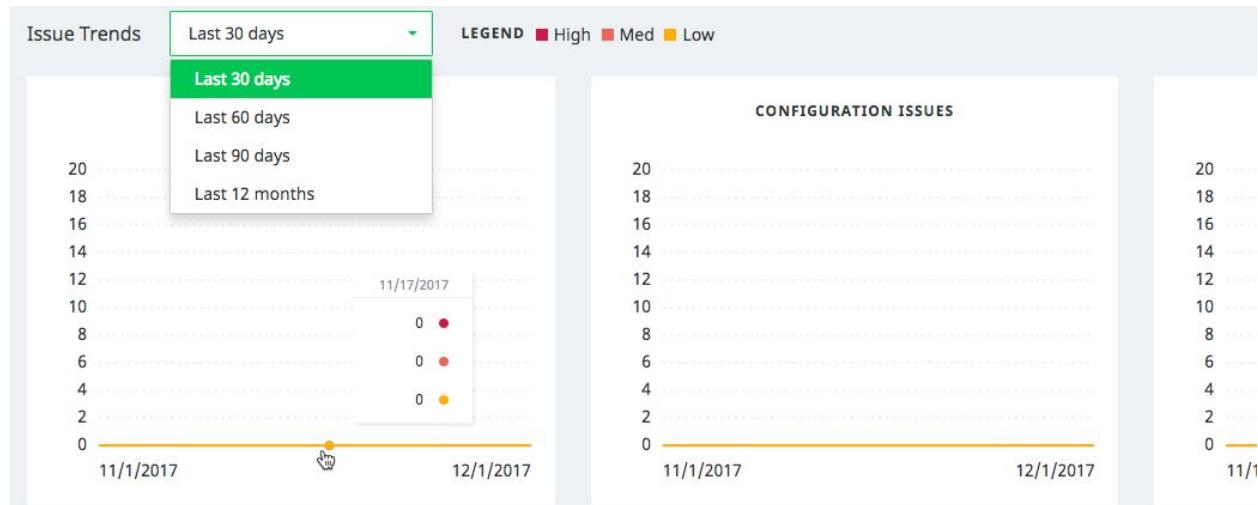
App Analysis (138 Apps Analyzed)



MES Comprehensive customers can review the App Analysis section to see the major vulnerability categories for apps on enrolled devices, as well as details on specific vulnerabilities. The four major categories are Data Access, Cloud Service, Malware, and Data Transfer. The center of each graph shows the percentage of enrolled devices with installed apps in that category. Clicking any category shows the issue types for that category.

Click an issue type in the lower list to immediately navigate to the **Apps** module, with filters applied to show only Apps with issues of that type.

## Issue Trends



Issue Trends displays trends in the issues affecting your enrolled devices. Trends are displayed across the following categories:

- Application Issues

- Configuration Issues
- File Issues
- Network Issues
- Operating System Issues

You can change the displayed time period using the dropdown at the top of the section, or mouseover the X-axis to display the number and severity of issues for a given date.

**IMPORTANT:** Modifying the displayed time period also affects the Issue Detections Breakdown below.

## Issue Detections Breakdown

Issue Detections Breakdown

CLASSIFICATION	DETECTION TRENDS Last 60 days	DETECTIONS BY RISK			TOTAL DETECTED / RESOLVED		AVG. RESOLUTION TIME
		High	Med	Low	Detected	Resolved	
Adware		0	0	0	0	0	-
App Dropper		0	0	0	0	0	-
Backdoor		0	0	0	0	0	-
Blacklisted App		0	0	0	0	0	-
Bot		0	0	0	0	0	-
Chargeware		0	0	0	0	0	-
Malware		0	0	0	0	0	-

The Issue Detections Breakdown shows issue information by classification. The information uses the same time period that you set in the Issue Trends dropdown. The columns are:

- Issue classification.
- Miniature trend graph for the time period.
- Detections over the time period, sorted into High, Medium, and Low risk categories.
- Number of detected and resolved issues over the time period, along with the percentage of resolved issues.
- Average resolution time.

Click a row in the table to immediately navigate to the **Issues** module, with filters applied to show only that class of issues.

## The Issues Module

### Issues

The Issues module displays a list of all issues against enrolled devices so that you can review attacks or vulnerabilities across issue types, operating systems, and other categories.

DISCOVERED IN: LAST 30 DAYS Filter issues by...

IGNORE REOPEN 1-20 of 20

<input type="checkbox"/>	STATUS	ISSUE	DEVICE	DETECTED
<input type="checkbox"/>	● Active Medium Risk	Android (Compromised) Root / Jailbreak	     	Feb 20, 2018 3:51 PM
<input type="checkbox"/>	✓ Resolved High Risk	test-rogue-mojito-00 Rogue WiFi	     	Feb 16, 2018 4:06 PM
<input type="checkbox"/>	✓ Resolved Low Risk	AV Test App Virus	     	Feb 16, 2018 2:52 PM
<input type="checkbox"/>	✓ Resolved Medium Risk	Android (Compromised) Root / Jailbreak	     	Feb 16, 2018 2:10 PM

- **Status:** Active or Resolved, and the Risk Level as determined by your Policies settings.
- **Issue:** A summary of the issue or the cause (such as the network name for a Rogue Wi-Fi detection), with the Issue Classification listed below.
- **Device:** The end user email associated with the compromised device. If you have Privacy Controls enabled, this column is present, but left blank.
- **Detected:** The date and time that the issue was detected.

You can select one or more issues and click the **Ignore** button at the top of the list to mark them as ignored issues. In the MES Console, ignored issues are treated as if they are not present. This means:

- They do not modify the device's Risk Level. If all issues on a device are set to Ignored, then the device is marked as Secured.
- They do not generate alerts in the MES Console.
  - For iOS devices, Ignoring an issue removes the notification from the end user device.
  - For Android devices, Ignoring an issue does not affect the issue count and notification on the end user device.
- They are not included in summary emails.

You can review ignored issues by filtering the list on **Status > Ignored**.

You can Reopen a Resolved issue by selecting it and clicking the **Reopen** button at the top of the list.

You can export issue information to a CSV file by clicking the **Export List** link in the upper-right.

## Filtering the Issue List

The filtering options are:

- **Discovered In Last [30 days/60 days/90 days/12 months]:** View recent issues only. The "Last 30 days" filter is applied by default.
- **Risk:** View High, Medium, or Low severity issues, based on the assigned levels from the Policies module.
- **Status:** View Active, Resolved, or Ignored issues to see current issues, remediated issues, and issues that are active but have been ignored by an MES Console Administrator.
- **OS:** View only iOS or Android issues to get a better idea of operating system vulnerability across your enrolled users.

- **Issue Type:** View one or more types of issues.
  - **Application:** Installed apps that pose a risk.
  - **Configuration:** Device settings that leave the device exposed to attack.
  - **File:** Issues on the file system, such as downloaded third party apps (.ipa or .apk).
  - **Network:** Issues that allow a malicious actor to intercept data sent between two parties.
  - **OS:** Compromised operating systems, such as those on jailbroken or rooted devices.
- **Classification:** View specific classes of issues, such as Spyware or Trojans.  
For a description of each classification, see the Policies module in the MES Console.

## Issue Details

Click any issue to see the Issue Details page. It includes the following:

- **Issue Status:** Active, Resolved, or Ignored.  
For “Active” issues, an MES Console Administrator can change the status to “Ignored”
- **Risk:** High, Medium, or Low.
- **Issue Type:** The high level category, such as Application, Configuration, File, Network, or OS.
- **User:** Typically the email address for the user associated with the device.
- **Dwell time:** The time between detection and resolution.
- **Classification:** The specific category, such as Spyware or Trojan.
- **Family Name:** Issues are often grouped into families based on their authorship, shared code, and common purpose or motivation
- **Classification Description:** A definition of the issue classification that describes the general capabilities and behaviors.
- **About <Family Name>:** Provides greater detail around the detected issue and its potential impact.
- **Application Details (MES Comprehensive only):** Lists the app package and includes a link that to the app analysis results.
- **Device Details:** Lists the device owner and includes a link to Device Details page.  
For more information, see [Device Details](#).
- **Issue History:** Lists the actions involving the issue, which may be **Security event detected** or **Issue status changed/resolved/ignored**.  
Each action has an associated actor, who may be the MES Console Administrator or the device end user. For App or File issues that are resolved by the endpoint, the actor is listed as the LES Client.

## The Devices Module



The Devices module lists all devices that are currently enrolled in Lookout, or were previously enrolled.

STATUS	DEVICE TYPE	USER	MDM
Pending	Nexus 6P Android 8.0		MobileIron-86716 ad6d0663-20fe-4ddc-947c- <a href="#">full user ID</a>
Pending	SM-N950U1 Android 7.1		MobileIron-86716 78ca214e-539c-4406-a65d- <a href="#">full user ID</a>
Secured	XT1058 Android 5.1		MobileIron-39218 4c255e28-1614-494c-8ae8- <a href="#">full user ID</a>

- **Status:** Activated, Pending (for devices where an enrollment email has been sent but the user has not yet enrolled), and Deactivated.
- **Device Type:** The device model and operating system.
- **User:** Typically the email address for the user associated with the device.
- **MDM:** The MDM managing the device, if any. For deployments with multiple MDM Connectors, this also includes the connector ID to determine which instance of an MDM a device is associated with.
- **Connection:** Whether the device is Connected to Lookout or Disconnected. Typically, you should expect a mobile device that is operating normally to connect to Lookout at least once every 3 days.

You can export this information to a CSV file by clicking the **Export List** link in the upper-right.

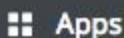
You can also **Deactivate** or **Delete** a device by checking it and clicking the corresponding button at the top of the list, or by selecting the device and clicking the button on the Device Details page.

## Device Details

Click any device to see the Device Details page. It includes the following:

- **Status, User, Device Type, MDM, and Connection** as in the Devices table.
- **Issues:** The issue history of the device.
- **Configuration:** Whether the device has a lock screen or device encryption, and if it has Developer Mode, USB debugging, or apps from unknown sources enabled.
- **Software:** The device OS including the current version, latest available version, and number of unpatched known CVEs.
- **Lookout for Work App:** The device ID, app package, and app version.
- **Specs:** General device data.

## The Apps Module (MES Comprehensive)



The Apps module is available to MES Comprehensive customers. The Apps Explorer shows all apps present across your enrolled devices as analyzed by Lookout Mobile Endpoint Security. The list is sorted in descending order of the percent of devices with an app installed.

APP NAME	VERSION	OS	DEVICES ▾	FIRST DETECTED ▾	VIOLATIONS ▾
 News com.apple.news	3.0		8 62%	Dec 27, 2017 3:38 PM	0
 Yelp com.yelp.yelpiphone	4 VERSIONS		6 46%	Jun 19, 2017 8:40 PM	4
 Outlook com.microsoft.Office.Outlook	3 VERSIONS		6 46%	Jun 19, 2017 8:40 PM	2
 -	2.4.7	-	3 23%	Dec 27, 2017 3:38 PM	-
 -	2.6.2	-	2 15%	Jan 2, 2018 4:33 PM	-

- **App Name:** The app name and app package.
- **Version:** The version(s) present. You can click the row to expand if multiple versions are present.
- **OS:** Android or iOS.
- **Devices:** The number of devices running the app, and the percentage of total enrolled devices that represents.
- **First Detected:** The date and time the app was first detected on any of your enrolled devices.
- **Violations:** The number of known CVEs in the app.

## App Details

Click any app in the Apps Explorer to see the App Details page. For apps with multiple versions, clicking the row expands the table to show all versions. You must select a specific version if you wish to review the details. The page includes the following:

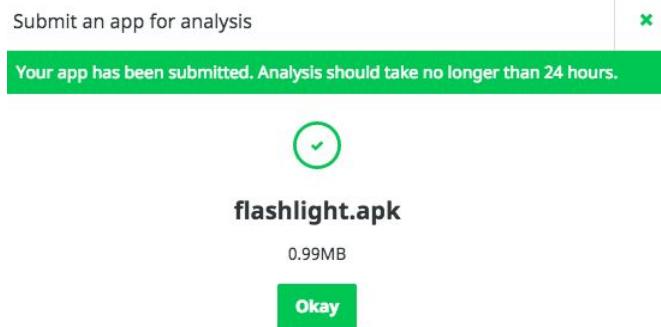
- **OS, Version, Prevalence in Fleet, First Detected** as in the Apps Explorer.
- **Developer:** The app developer.
- **File Size:** The size of the .ipa or .apk file.
- **Identification:** ID information such as the Bundle ID, Signing ID, Object ID, and App Store ID.
- **Description:** The app description as taken from the App Store or Google Play Store.
- **Violations:** A list of detected security violations.
- **Data Handling Security:** Whether the app transports and stores data securely.
- **Data Access and Transfer:** Whether the app accesses user data and/or transfers it.
- **Network Traffic:** A list of hosts the app communicates with.
- **Cloud Services in Use:** A list of Cloud services the app communicates with.
- **Components:** A list of components that have the potential for malevolent use.

## Analyzing an App

You can upload an .ipa or .apk file to analyze an app even if it isn't present in your fleet. Note that after you upload the file, analysis can take up to 24 hours.

1. In the upper-right corner, click **ADD APP**.  
The Submit an app for analysis window appears.
2. Click and drag your .ipa or .apk file into the window, or click **choose a file** to browse to it.  
A progress ring displays while Lookout analyzes the app.

- Upon success, the console displays the following confirmation screen:



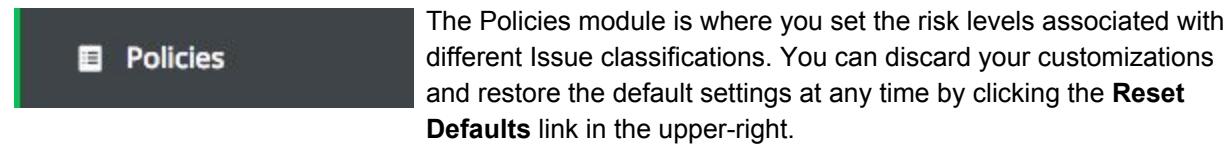
## Blacklisting and Un-Blacklisting Apps

Blacklisting an App works together with defining a custom policy, as documented in [Defining Custom Policies for Apps \(MES Comprehensive\)](#).

1. Navigate to the App Details page for the app.
2. To blacklist an app, in the upper-right corner, click **BLACKLIST**.
3. To remove an app from the blacklist, click **UNBLACKLIST**.

**NOTE:** Adding or removing an app from the Blacklist affects all versions of that app.

## The Policies Module



Each issue classification includes the following information:

CLASSIFICATION	OS	DESCRIPTION	RISK LEVEL	RESPONSE
Backdoor	Android iOS	Opens up protected components to an attacker	High	Alert device
Bot	Android iOS	Enables remote access	High	Alert device

- **Classification:** The name of the issue classification.
- **OS:** Whether the issue affects Android devices, Apple devices, or both.
- **Description:** A brief summary of the classification. You can mouse over the ? icon for more details
- **Risk Level:** The risk level represents the severity of that issue classification. Lookout includes a set of default risk levels, but you should use the dropdown to set the risk levels appropriate to your organization.
- **Response:** For each classification, you can either alert the end user of the device or choose not to alert them.

By default, Lookout alerts the device user for all issue classifications except for non-App Store or sideloaded apps, since organizations often distribute their own signed apps for internal use.

## Whitelisting Non-App Store Signers and Sideloaded Apps

For iOS, Lookout reports the presence of apps that don't originate from the App Store. On iOS 8, 9, and 10 these issues are classified as sideloaded apps. On iOS 11, they are classified as non-App Store signers. For either classification, you can whitelist approved apps or signers in order to resolve any existing issues and prevent future issues and alerts:

**NOTE:** If you have existing issues against a sideloaded app or non-App Store signer, you can go to the Issues module and click the issue in order to whitelist the app or signer without having to input the information manually.

To whitelist apps or signers from the Policies module:

1. Click the gear icon next to the issue classification:



The **Configure Sideloaded App Policy** or **Configure Non-App Store Signer Policy** dialog appears.

2. Click **Add an Entry**.
3. For sideloaded apps, input the **Team ID**, **Bundle ID**, and an optional **Custom Label** to distinguish the app:

TEAM ID <small>?</small>	BUNDLE ID <small>?</small>	CUSTOM LABEL <small>?</small>
<input type="text" value="REQUIRED"/>	<input type="text" value="i.e. com.inc.app"/>	<input checked="" type="checkbox"/> Any <input type="text" value="Custom label"/>

Please check and correct the team id field. It must be alphanumeric with a length of ten.

4. For non-App Store signers, input the exact Developer Name and an optional **Custom Label** to distinguish the signer:

DEVELOPER NAME	CUSTOM LABEL <small>?</small>
<input type="text" value="required"/>	<input type="text" value="Custom label"/>

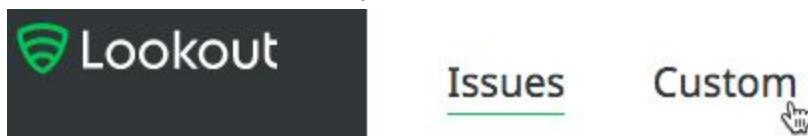
Please check and correct the developer name field. It is required.

5. Click **Done**, then click **Save Changes**.

## Defining Custom Policies for Apps (MES Comprehensive)

If you have Lookout MES Comprehensive, you can add your own policies for apps that fit specific criteria.

1. Click the **Custom** tab at the top of the screen:



2. Click **Add Policy**.
3. Enter a name for the policy.
4. Use the Search and Filter field to add app filters.

For example, to add a policy for submitted apps that access either the user's Address Book or their Location, select **Source > Submissions** then **Data Access > Address Book** then **Data Access > Location**:

Submitted Apps with Address Book and Location access

Filter apps by...

- Data Access
  - Address Book, Calendar, Camera, Clipboard...
- Cloud Service
  - Amazon Cloud Services, Amazon S3, Box, Dropbox...
- Malware
  - Adware, App Dropper, Backdoor, Bot, Chargeware...
- Data Transfer
  - Address Book, Calendar, Camera, Clipboard...
- Source**
  - Public apps or Submissions
- OS
  - iOS or Android

Submitted Apps with Address Book and Location access

SOURCE: SUBMISSIONS X DATA ACCESS: ADDRESS BOOK X DATA ACCESS: Filter apps by...

Apps that access address book should be marked as policy violations.

Add policy

- Calendar
- Camera
- Clipboard
- Device Identifiers
- Local Storage
- Location**
- Media
- Microphone
- Reminders
- SMS Archive

5. Click **Add policy**.

Creating the policy causes the App Explorer module to flag all apps that violate the policy. Once

you have reviewed a questionable app in App Explorer, you can choose to blacklist it by clicking the **Blacklist** button. For more information, see [Blacklisting Apps](#).

6. To configure a risk level, return to the **Policies** module **Issues** tab and set the policy for the **Blacklisted App** classification.

This classification only applies to apps that you explicitly blacklist. It does not automatically apply to apps in violation of a custom policy.

You can delete an existing custom policy by highlighting the row and clicking the trashcan icon:



## The Account Module

The Account module displays by default when you click open the System navigation bar. It displays your organization name and license status. This includes the number of purchased licenses, the license type, and the number of active users and devices. Contact your Lookout Sales representative if the license information is not what you expect.

It also displays your Global Enrollment Code, which you can use if users aren't able to successfully activate via email. If you have previously distributed the enrollment code to help users activate Lookout, you should use either the **Disable Global Code** or **Reset Global Code** buttons when you no longer want the previous code to be active.

## The Manage Admins Module

Unless you are running a Microsoft Intune integration, the Manage admins module displays a list of all MES Console Administrators. You can add new Administrators from here by clicking **ADD ADMIN**, or search the list by name or email.

For Microsoft Intune, the Manage Admins module displays a notification indicating that MES Console Administrators are set based on Azure Active Directory (AAD) Groups. These are the groups configured for Full Access / Restricted Access / Read-Only Access in your Intune Connector settings under **System > Connectors**. To modify access, either change the groups directly in AAD or change the Intune Connector settings to map to different groups.

Available access levels are:

- **Full Access:** No restrictions.
- **Restricted access:** The Admin can manage devices and issues, export content, or edit personal preferences. They can't edit security policies, enroll devices, or edit system preferences. Cannot edit security policy, enroll devices, or edit system preferences.
- **Read-Only access:** The Admin can only export content or edit personal preferences.

## The Enrollment Settings Module

If you are not using a Mobile Device Management (MDM) solution, you can enroll devices directly from MES.

- **Email Templates:** Create or Edit default or custom email invitations and reminders.

- **Device Allotment:** The number of devices that a user can enroll using one activation email.
- **Invite Expiration:** How long an email invite remains usable, from 1 day to 5 weeks.
- **Disconnected Status:** How long a device can go without connecting to Lookout before it is considered Disconnected, from 1 to 90 days.
- **Language:** See the [Lookout Supported Platforms](#) document for supported languages.

## Creating a Custom Invitation or Reminder Email

Lookout has default email invites and reminders configured by default. To create a custom invite or reminder:

1. Verify that the **Custom** radio button appears:

Invite:	<input checked="" type="radio"/> Default	<input type="radio"/> Custom	<a href="#">Create</a>	<a href="#">Test email</a>
Reminder:	<input type="radio"/> Default	<input checked="" type="radio"/> Custom	<a href="#">Edit</a>	<a href="#">Test email</a>

If it is not present, contact [Lookout Enterprise Support](#) to enable this feature for your tenant.

2. Click the **Custom** radio button.  
The Custom email or reminder template window opens.
3. Enter the following:

Field	Value
Logo URL	A link to your hosted logo image. This appears at the top of the email.
Subject	The email subject line.
Email Content	The email body.
Include Enrollment Link	Enabled by default.

4. Click **Save**
5. When you return to the Enrollment Settings module, click **Save** again.
6. To test the email, click the **Test email** link and input your email address, then click **Send**.

For example, these settings:

## Custom email template

### Logo URL

`https://www.lookout.com//images/logos/lookout-logo-1280x720.png`

### Subject

Test enrollment email

### Email content

You can include `html` `tags` in your email.

You can also add `&lt;encoded&gt;` characters.

If you're feeling fancy, throw in an `span style="color:blue;">inline`  
`style`

Include enrollment link

Result in this email:

Logo

Lookout

Protect yourself from mobile threats

You can include `html` tags in your email.

Please click the button below to download the Lookout app on your tablet or phone.

Install Lookout for Work

Enrollment Link

You can also add `<encoded>` characters.

M D

If you're feeling fancy, throw in an [inline style](#)

Powered by

Lookout

Add [no-reply@lookout.com](mailto:no-reply@lookout.com) to your address book to ensure delivery of our emails to your inbox.

This message was sent to [REDACTED] on behalf of [REDACTED]

[Privacy Policy](#)

The recipient's email address and the Lookout MES Console tenant name are included at the bottom of the email.

## The Send Invites Module

Once you've configured enrollment and reminder emails, you can send invites by uploading a `.csv` file or by entering a comma or semicolon delimited list of email addresses.

1. Click **Import Emails From a .CSV** and upload the file or input the names in the provided field and click **Add Addresses**.

Lookout displays a summary showing which emails are valid, which are invalid, and which already have either pending invites or activated devices:

The screenshot shows a user interface for managing email invites. At the top, there are two input fields: 'Import Emails From a .CSV' and 'Enter emails separated by commas, or semicolons.' Below these is a note: 'You can upload or paste in more email addresses. They'll get added to your list.' A 'Add Addresses' button is also present. The main area displays a list of invite status categories:

- 4 valid email addresses.
- 0 addresses already have pending invites. (With a checkbox to 'Send them invites anyway.')
- 0 addresses already have active devices. (With a checkbox to 'Send them invites anyway.')
- 1 invalid address. (Note: These will not receive invites.)

At the bottom of the list are two buttons: 'Send 4 Invite Emails' (highlighted in green) and 'Generate Enrollment Tokens'.

2. Click one of the following:
  - **Send <number> Invite Emails:** Send invites using the settings from [The Enrollment Settings Module](#).
  - **Generate Enrollment Tokens:** This generates an enrollment token and adds the email addresses to the Manage Invites list, but lets you stop short of sending the actual email. To continue sending an invitation, navigate to the Manage Invites module, select the invitation(s), and click **Send New Invites**.

## The Manage Invites Module

The Manage Invites module lists all invites from the Send Invites module and their status:

The screenshot shows the 'Manage Invites' module interface. At the top, there is a search bar labeled 'Filter invites by...' and a dropdown menu with the following options:

- Status: Unused, Valid, Quota Reached, Expired
- Search
- Email

The main table lists invites with the following columns:

Date	Email Address	Status
Feb 20, 2018 4:26 PM	gmail.com	Unused, Valid
Feb 20, 2018 4:25 PM	@gmail.com	Unused, Valid
Feb 20, 2018 2:56 PM	mail.com	Unused, Valid

- **Initial Invite Sent:** The date and time of the original invitation email.
- **Email Address:** The recipient's email address.
- **Status:** Unused, Valid, Quota Reached, or Expired.
- **Devices Used:** The number of devices used out of the total number available for that invite.
- **Reminders Sent:** The number of reminders sent.
- **Expiration:** The invitation expiration date.
- **Token:** The enrollment token associated with the invite.

You can export this information to a CSV file by clicking the **Export List** link in the upper-right.

## Managing Invites

You can perform the following actions using the buttons at the top of the invites list:

- **Send Reminders:** Check one or more invitations and click this button to send a reminder email using the settings from [The Enrollment Settings Module](#). Alternately, click the drop-down arrow to send reminders to **All Unused Invites** or **All Active Invites**.
- **Send New Invites:** Check one or more invitations and click this button to send new invitations using the settings from [The Enrollment Settings Module](#). Alternately, click the drop-down arrow to send new invitations to **All Unused Invites**, **All Expired Invites**, or **All Expired & Unused Invites**.
- **Archive Invites:** Archive the invite, preventing the end user from using it to activate a device. Alternately, click the drop-down arrow to archive **All Expired Invites**, **All Invites That Have Reached Quota**, **All Unused Invites**, **All Invites Used At Least Once**, or **All Invites**.

## The iOS Configuration Module

The iOS Configuration Module is where you review and set the deployment method and other options for the iOS Lookout for Work app. Depending on your tenant configuration, this module may contain options for uploading the Enterprise Signed Lookout for Work .ipa file, or it may require a link to the App Store edition of Lookout for Work.

Initially, the MES Console shows that the iOS app is not configured:

### Configuration Status

- ⓘ iOS support is not configured.
- ⓘ No hosted .ipa file
- ⓘ No enterprise certificate
- ⓘ No VoIP Services certificate

To distribute the In-House edition of the Lookout for Work iOS app, follow the steps in the [iOS App Re-Signing Process](#) article. This process is outlined in detail in the deployment guide for your MDM.

**NOTE:** If you have uploaded a resigned Lookout for Work .ipa file, you cannot upload a prior version. For example, uploading the resigned .ipa for version 4.9 prevents you from reverting to the resigned .ipa for version 4.8, despite the upload process appearing to work.

## The Connectors Module

The Connectors module lists any active MDM connectors. If you have no active connectors or if you are using an MDM that supports multiple connectors, then you can add a new connector by clicking **Add Connector**.

For detailed information on the connector settings for your MDM, refer to the Deployment Guide for your environment:

- [Deploying Lookout with Microsoft Azure Active Directory and Intune](#)
- [Deploying Lookout with MobileIron](#)
- [Deploying Lookout with VMware AirWatch](#)
- [Deploying Lookout with IBM MaaS360](#)
- [Deploying Lookout with BlackBerry UEM](#)

## The Application Keys Module

If you are running an integration that communicates with Lookout's Mobile Risk API for logging purposes, you can review and generate application keys from the Application Keys module. For more information, refer to the [SIEM Connector Guide](#).