IBM MaaS360 with Watson

Evaluator’s Guide

Version 2.2

Introduction

IBM MaaS360 | With Watson

Welcome to the IBM MaaS360 with Watson Evaluator's Guide. This document provides you with a self-guided, hands-on review of our leading cognitive Unified Endpoint Management (UEM) solution. The content is intended to show how easily you can trial MaaS360 to evaluate the management of iOS, Android, Windows and macOS devices.

The guide is divided into the following sections:

1. **MaaS360 Components**
2. **Trial**
3. **Setup**
4. **Evaluation Tasks**

This document assumes you have knowledge of networking concepts and the use of iOS, Android, Windows and macOS.

After you start a free 30 day trial, this document guides you through some typical device management scenarios. This guide is not intended to substitute for product documentation. For detailed information, please refer to the knowledge center, online documentation and how to videos.

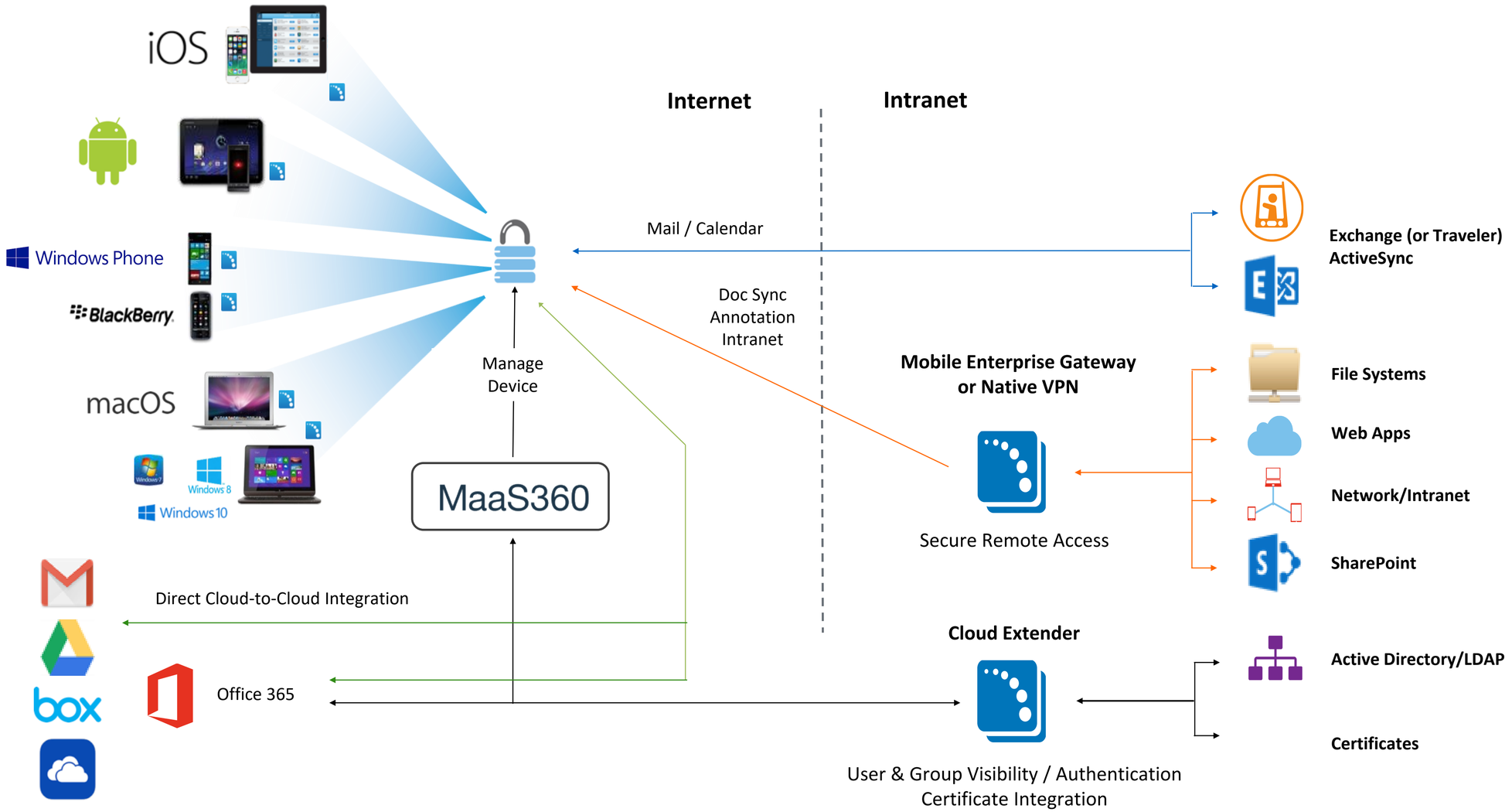
Need help? Please visit our support page for more information.

Thank you for evaluating MaaS360!

1 MaaS360 Components

Components: MaaS360 Architecture

The following diagram provides an architecture overview of MaaS360. This be will explained further in the following pages.



Components: (Optional) Cloud Extender

IBM MaaS360 with Watson Unified Enterprise Management is a cloud-based multi-tenant platform that helps to monitor and manage your smartphones, tablets, PC and macOS.

As part of your evaluation you're not required to install any on-premises components. You can enroll your devices via a one time passcode into your MaaS360 account.

Cloud Extender (CE)

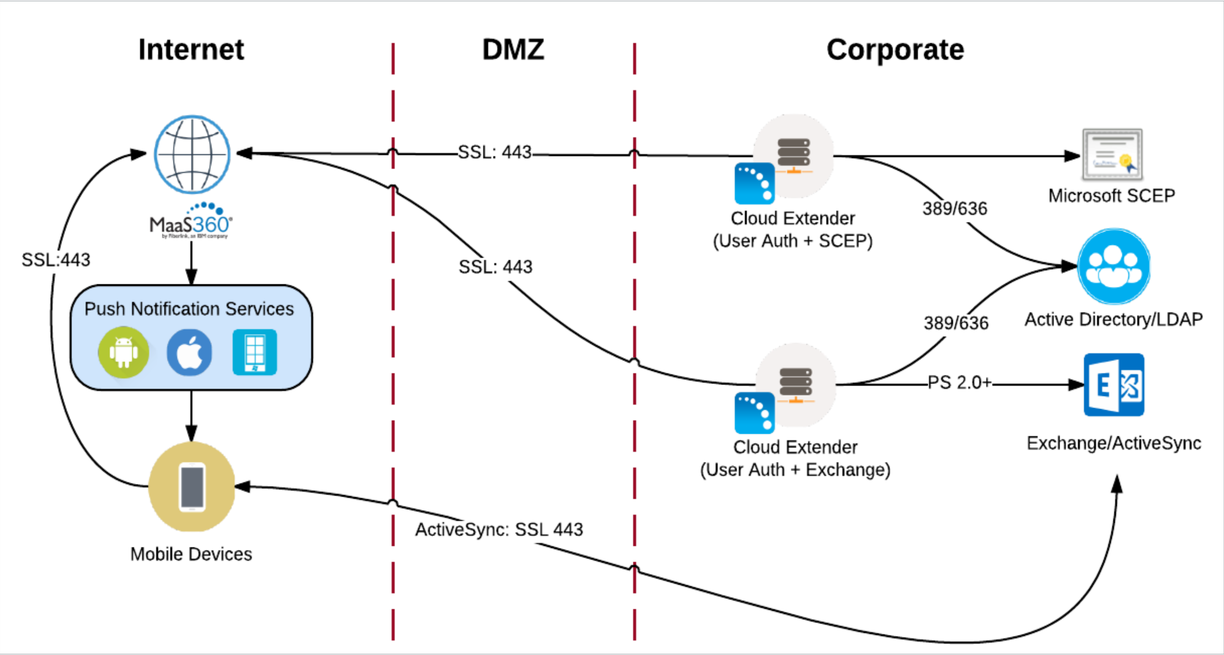
The MaaS360 Cloud Extender is a small program that runs as a service on a Microsoft Windows machine in your network. The Cloud Extender creates an outbound connection over HTTPS (443) to the MaaS360 portal that is used as a bi-directional communication facility and allows the MaaS360 portal to integrate with your Active Directory, Exchange, Traveler or Certificate Authority.

The primary role of the CE is to make device enrollment a completely self service user activity. i.e. Users enroll their device by going to *m.dm/companyname*. The URL is specific to your organization.

Components: Cloud Extender (CE) Architecture

The MaaS360 Cloud Extender is a lightweight agent that enhances device management capabilities by integrating with on-premises systems within your environment, such as email, corporate directories, certificate authorities, and application and content servers.

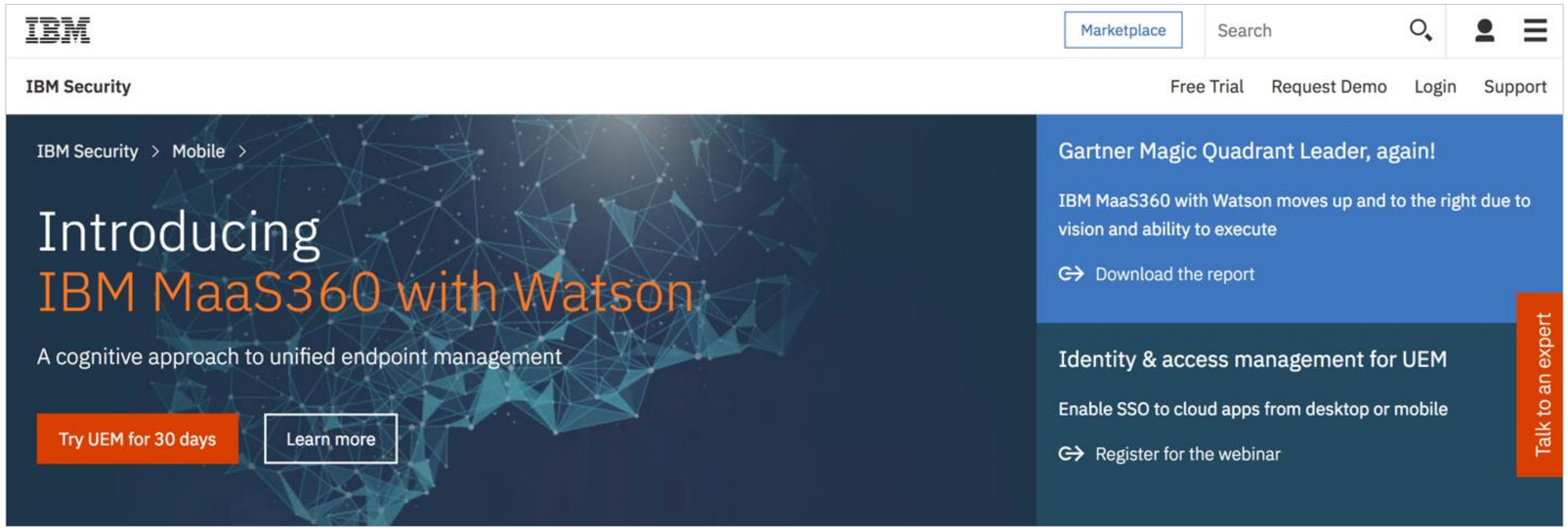
The Cloud Extender is primarily recommended for automated enrollment and simpler group management. Clients also leverage the CE for certificate delivery, visibility into your exchange/traveler environment for unmanaged rogue devices.



2 Trial

Trial: Start a free 30-day trial

Go to www.ibm.com/maas360 and select **Free Trial** to start your free 30 day trial of MaaS360.



Enter your Login details including your email address, a password for your account, company name and contact details. The **Quick Start** screens will walk you through setting up your account and enrolling devices.

Note: The account that you create as part of your trial continues into Production if you purchase MaaS360. You will receive a Welcome email that contains important information about your trial. Make sure that you save this email in case you need to contact IBM Support.

Trial: Select Platforms and Apple APNS certificate

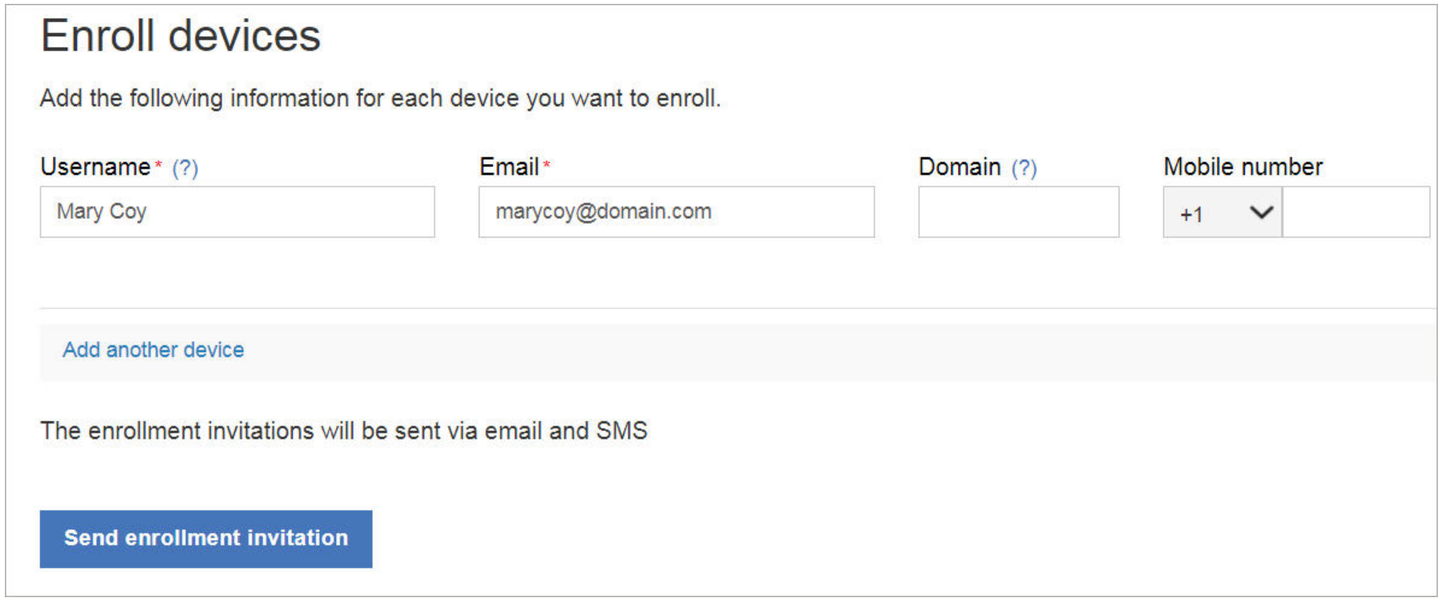
MaaS360 is automatically configured to support Android devices. To manage iOS and macOS devices, Apple requires you to have an Apple Push Notification service (APNs) certificate. MaaS360 will walk you through the process of obtaining this certificate.

- Safari, Chrome and Firefox web browsers are recommended for this straightforward process, which usually takes less than 5 minutes to complete.
- Detailed step by instructions are available here.
- We strongly recommend that an Apple ID is registered to your company and not an individual. If you use a personal Apple ID and the person leaves your company, you will need to create a new Apple ID at renewal time and re-enroll all of your iOS devices again. The Apple ID you use needs to be renewed anually.

The setup and annual renewal of an APNs certificate is an Apple requirement, which you perform via the MaaS360 console. It’s not a task the users must perform on their iOS device.

Trial: Enrolling your first device

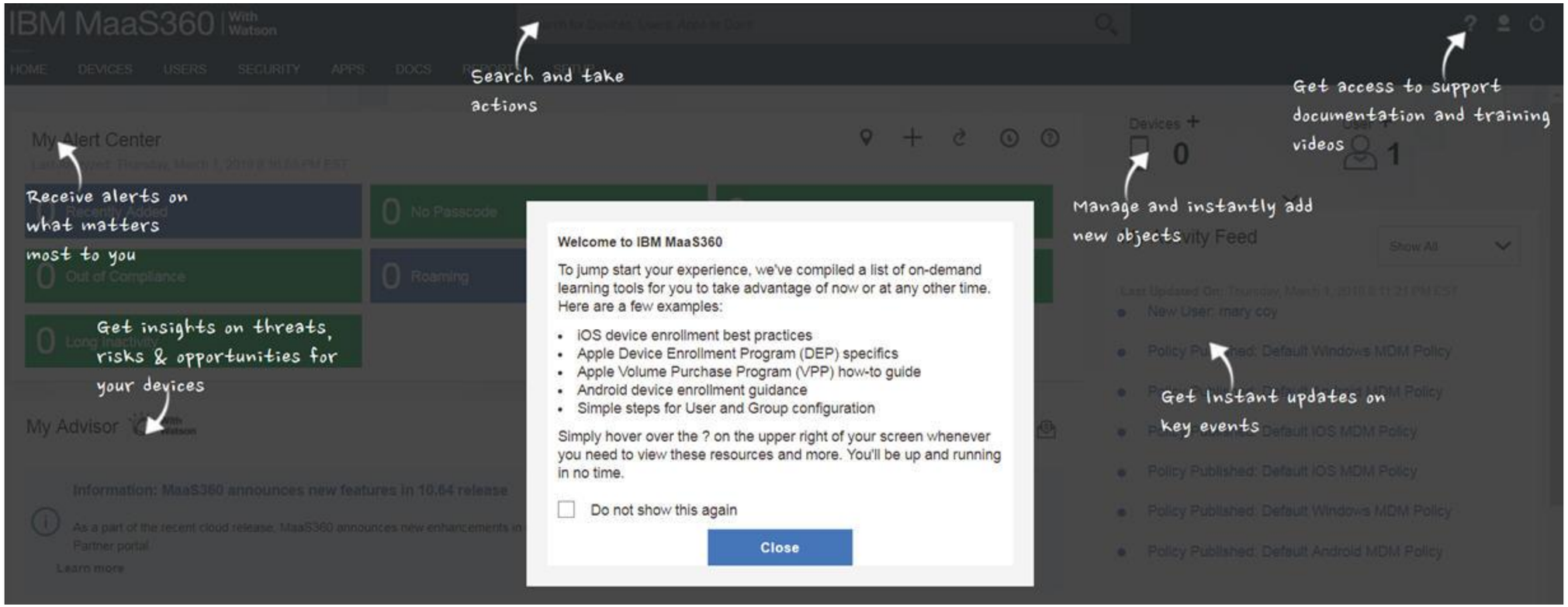
Click on Enroll devices to begin enrolling devices in MaaS360. Enter your **Username**, **Email Address** and optionally **Domain** and **Phone Number** fields. Then select **Send enrollment invitation** which will send information via email or text message to enroll your first device.



MaaS360 will send an enrollment request to the specified device. You can enter the enrollment URL into your device's web browser or via the email or text message link if applicable.

Trial: Tips

Now you can review information about the enrolled device, take actions like Lock, Locate or Distribute Apps and more. If you click **Close Quick Start**, you'll be presented with a tips page showing you key items of interest with the MaaS360 console.

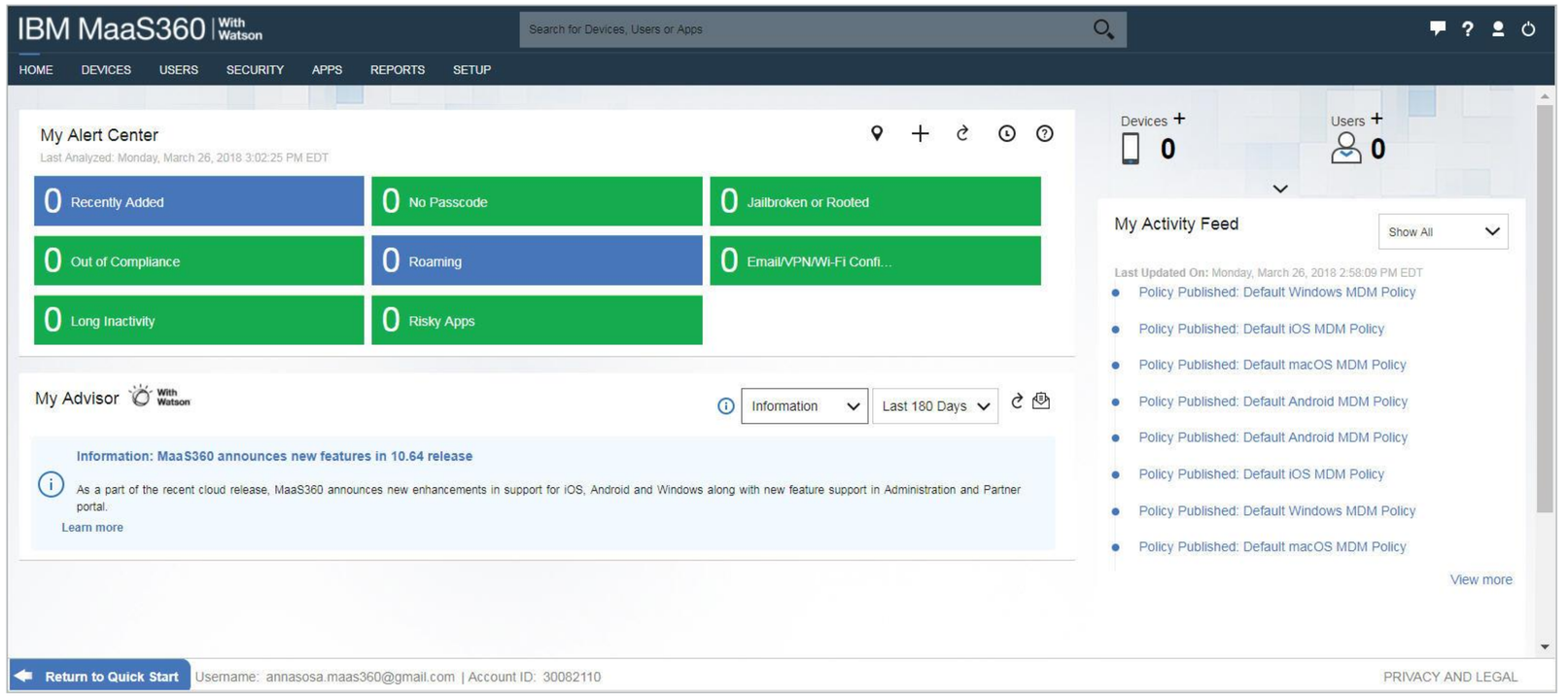


3 Setup

Setup: Navigating the MaaS360 Portal

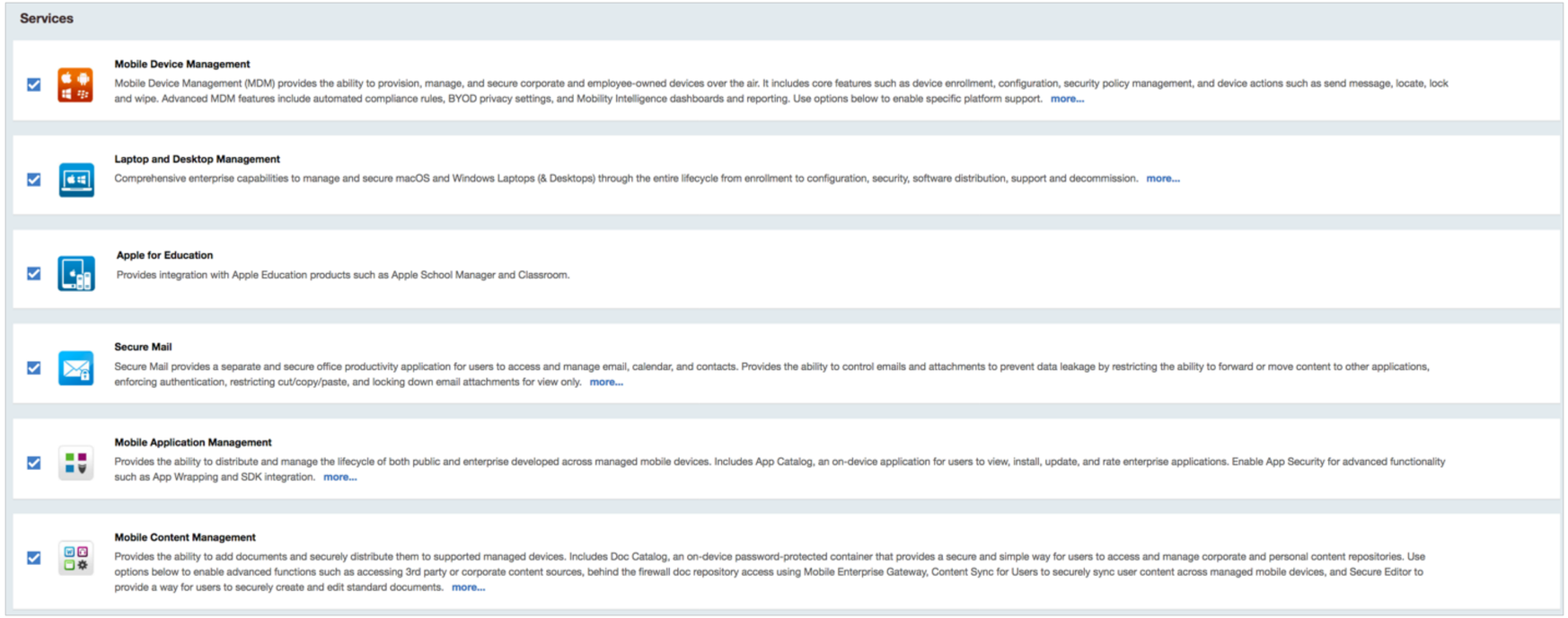
MaaS360 has been designed to make it easy for you to get information and take action quickly and easily. The MaaS360 user interface provides an easy-to-use tab and menu navigation layout, allowing quicker access to the available workflows.

Please watch the **Getting Started with MaaS360** video here.



Setup: Enable Services

To review and configure additional services, mouse over the Setup tab and click **Services**. To enable a new service, click on the box next to the service, then enter your portal password.



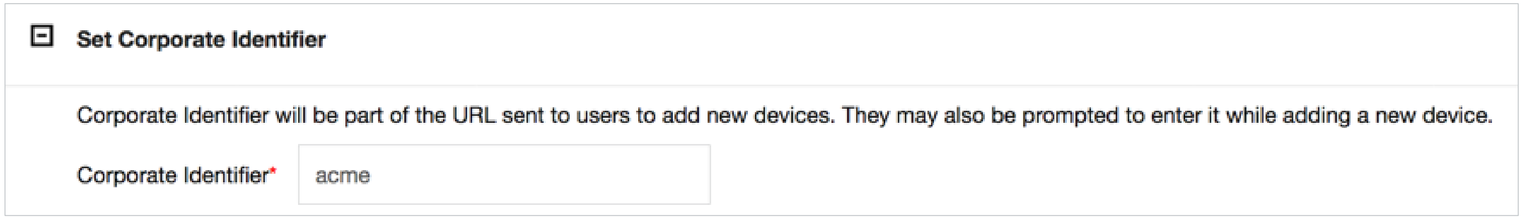
Please contact your MaaS360 representative to enable additional services as part of your trial. Alternatively send a request by email to support@maas360.ibm.com

Video

Setup: Device Enrollment Settings

Next we'll review and configure deployment settings. Mouse over the **Setup** tab and click **Settings** then **Device Enrollment Settings** and **Basic**. You'll see a corporate identifier which is your 8 digit Account ID (which you'll use when contacting support via chat, email or phone).

To make the user device enrollment easier (particularly if you setup the Cloud Extender), replace the existing number with your company name or abbreviation. For example, **acme** or **acmemdm**.



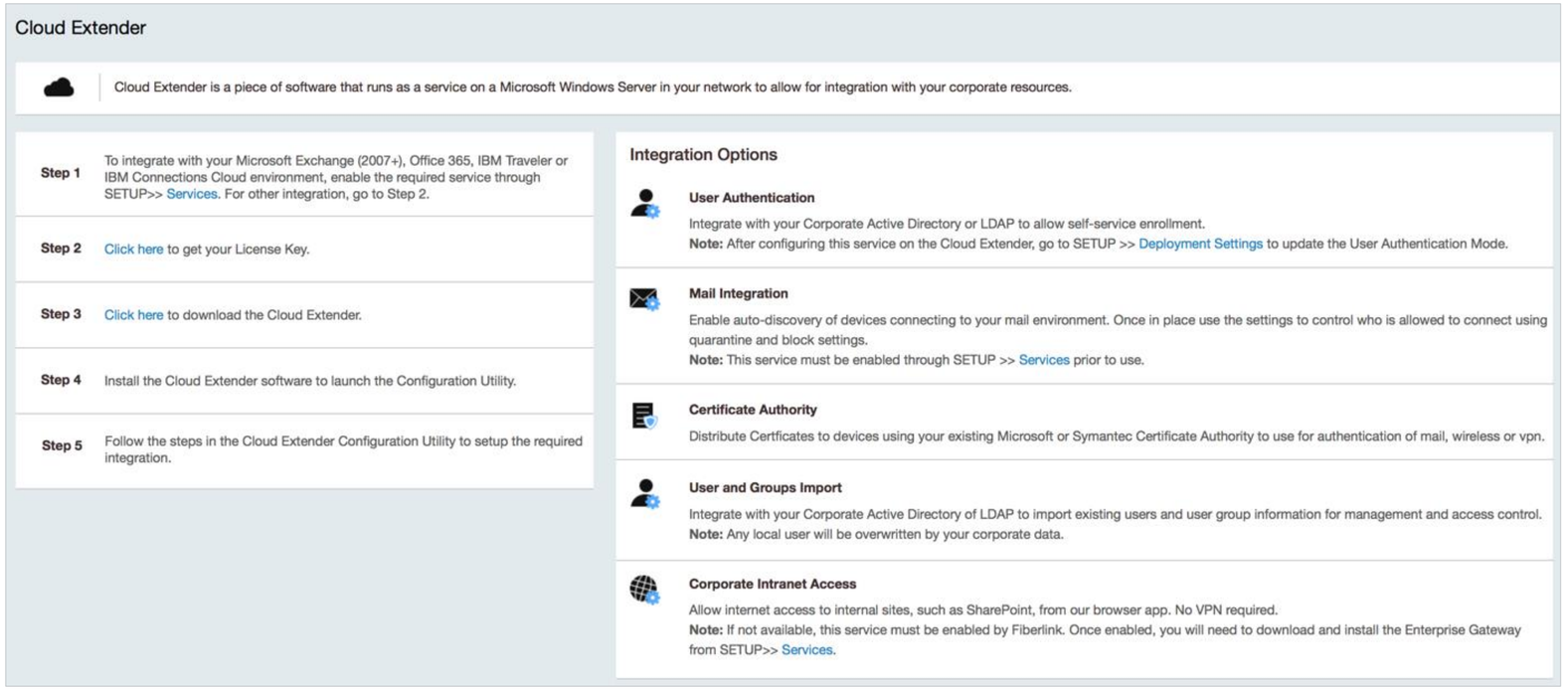
Review any other features such as the default such as the default **AppStore region**, **Corporate Information** and **End User License Agreement** etc. When completed, select **Save**.

Video

Setup: Install the Cloud Extender

The MaaS360 Cloud Extender (CE) is a lightweight agent that enhances device management capabilities by integrating with on-premises systems within your environment, such as email, corporate directories, certificate authorities, and application and content servers. The Cloud Extender requires minimum resources, easily traverses proxy environments, and provides secure messaging and data transfer between the MaaS360 platform and your on-premises systems.

Select **Setup** – **Cloud Extender** to be shown the following screen. Follow the five steps to download and install/configure the CE. The following videos can also assist you with guidance on the install and configuration.



Cloud Extender Requirements

The following table outlines the system requirements for the Cloud Extender:

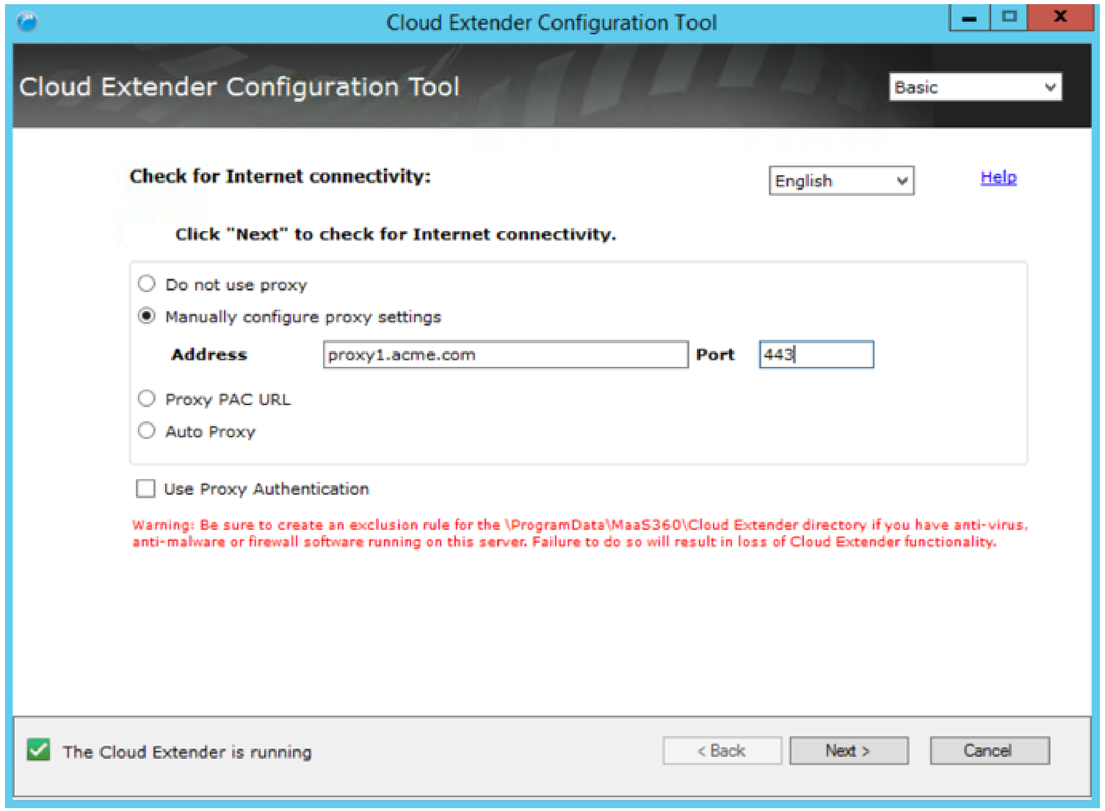
Component	Minimum Requirement
Operating System	Windows Server 2016, 2012 R2, 2012, 2008 R2, or 2008
Other software	.NET Framework 3.5
Domain Membership	Member Server
Minimum RAM / CPU	8 GB / Dual Core 2.8 GHz
Minimum Disk Free	10 GB
Service Account	Read only access to the Active Directory Local Administrator
Network Connection	Outbound Port 443 (SSL) – Direct or via a Proxy

Note: These requirements are for evaluations of the MaaS360 platform (< 1000 devices). Use the Cloud Extender Sizing Tool in the portal to assist with sizing your CE servers.

Setup: Setup the Cloud Extender with a Proxy

The MaaS360 Cloud Extender can communicate to the SaaS service via a proxy as outlined below. If the connectivity check “Internet access available” is not displayed, check if you need to include authentication information.

Specific IP addresses that must be permitted are detailed here



Setup: Cloud Extender Options

For the purposes of an initial Cloud Extender setup, select **User Authentication** and **User Visibility**. The complete list of options are detailed here.

User Authentication
The User Authentication module integrates with your Active Directory (AD) or LDAP environment to authenticate users by using various workflows within MaaS360®. With this module, your users can reuse corporate credentials without having to generate and manage a new set of credentials.

User Visibility
The User Visibility module manages mobile devices based on corporate directory structure. With this module, administrators can manage user devices that belong to specific groups, and target apps, policies, and content to user devices that are members of a specific directory group.

Other options such as MaaS360 VPN, Exchange Integration, Traveler Integration, Certificate Integration can be tested as part of your trial. Seek assistance from IBM on the appropriate setup documentation as you test these modules.

Note: Most clients select the LDAP option, as it provides the ability to select what components of your Active Directory you wish to synchronize. If you select the **Active Directory** option with **User Visibility**, it will synchronise ALL users and groups into the MaaS360 portal.

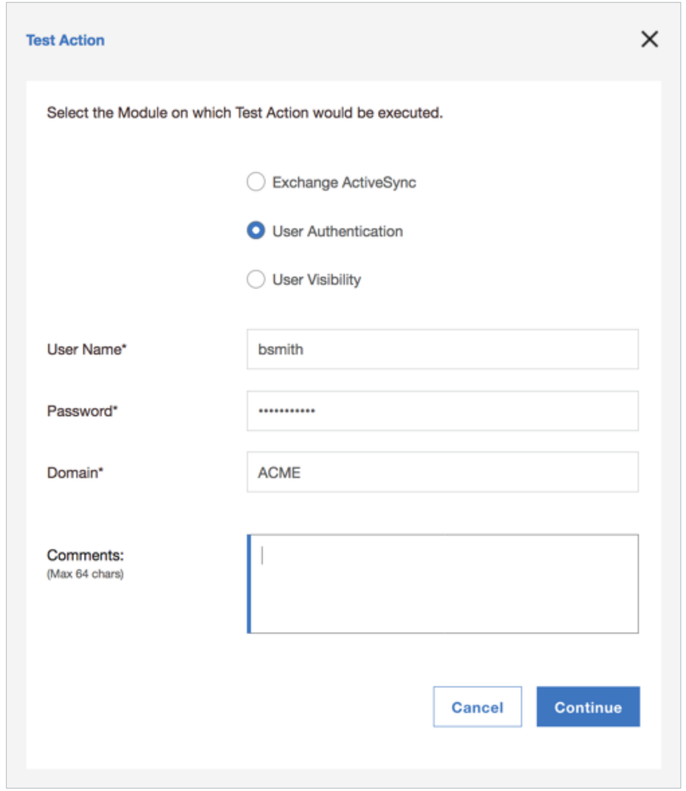
Setup: Test the Cloud Extender

When the Cloud Extender is installed, after a few minutes the Cloud Extender collects data and uploads that data to the MaaS360 Portal.

You can check this process by logging in to the MaaS360 Portal with your portal URL and selecting **Setup > Cloud Extender**. The Cloud Extender in the MaaS360 Portal shows connection status and the configured services. However, depending on the speed of your installation and the number and the size of enabled modules, you might see a slight delay with updated status information.

Select **Actions** - **Test Action**

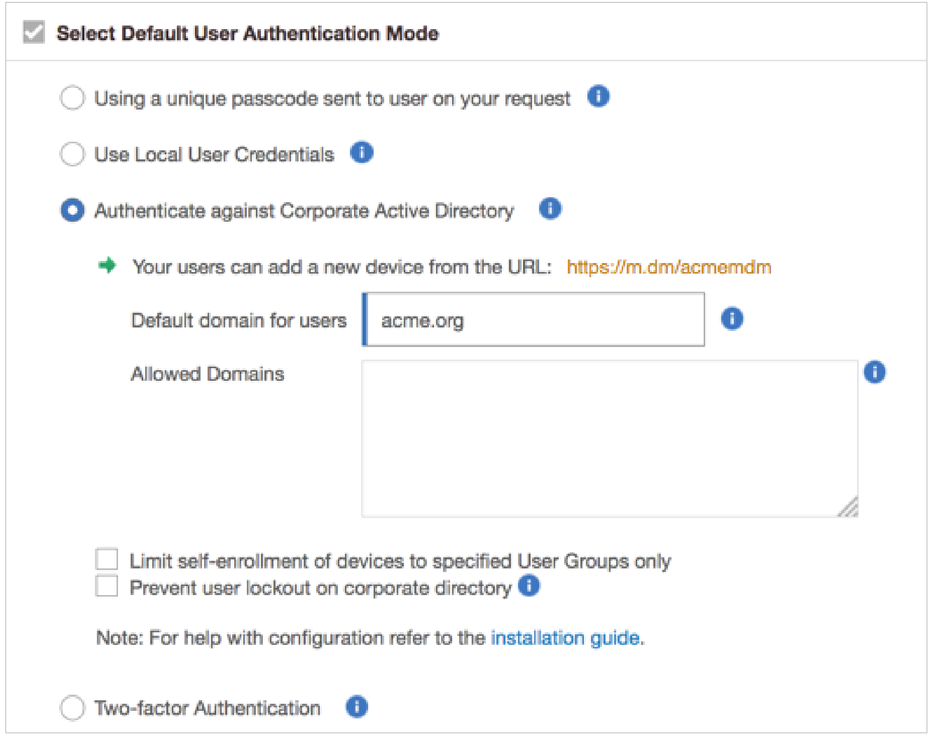
You can then test **User Authentication** and **User Visibility**.



Setup: Authenticate using your Corporate Directory

With the CE up and running, access the **Deployment Settings** screen, which is found on the **Setup** tab.

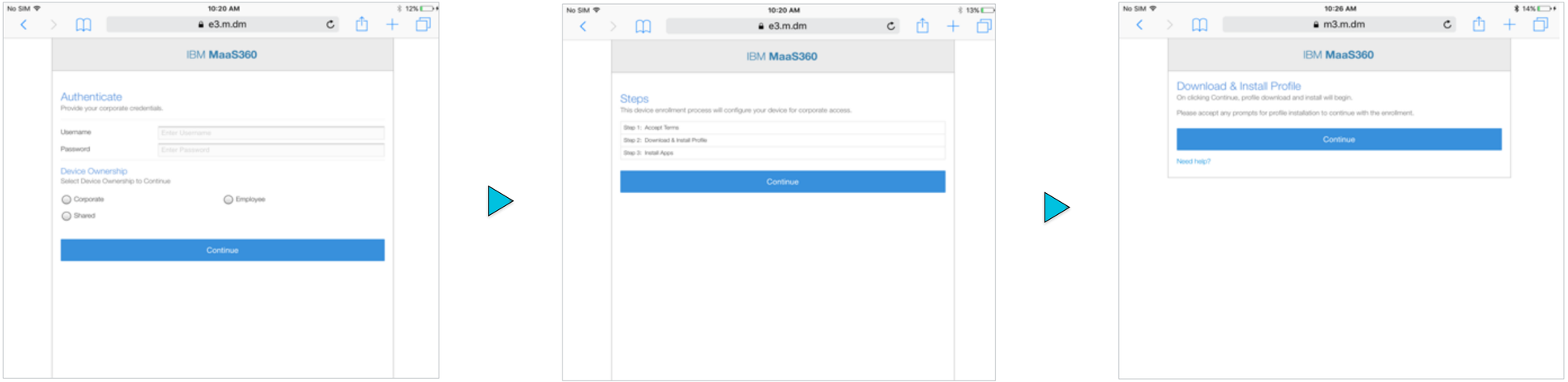
Change **Select Default User Authentication Mode** to **Authenticate against Corporate Active Directory**.



When completed, select **Save.**

Setup: Enrolling your device using your corporate directory

Users can now enroll their device by going to m.dm/*companyname* (using the devices mobile browser). **The URL is specific to your organization**. This is a completely self service process for the user.



Otherwise the administrator can perform a passcode enrollment. This is performed under **Devices** > **Inventory** and then selecting **Add Device.** This sends a specific enrollment URL and passcode to the device.

The following article shows you the iOS enrollment with a corporate directory. This video shows a iOS passcode enrollment.

4 Evaluation Tasks

The remainder of the guide outlines key tasks you may wish to test with your iOS, Android, Windows and macOS devices. These include links to detailed online documentation and short training videos.

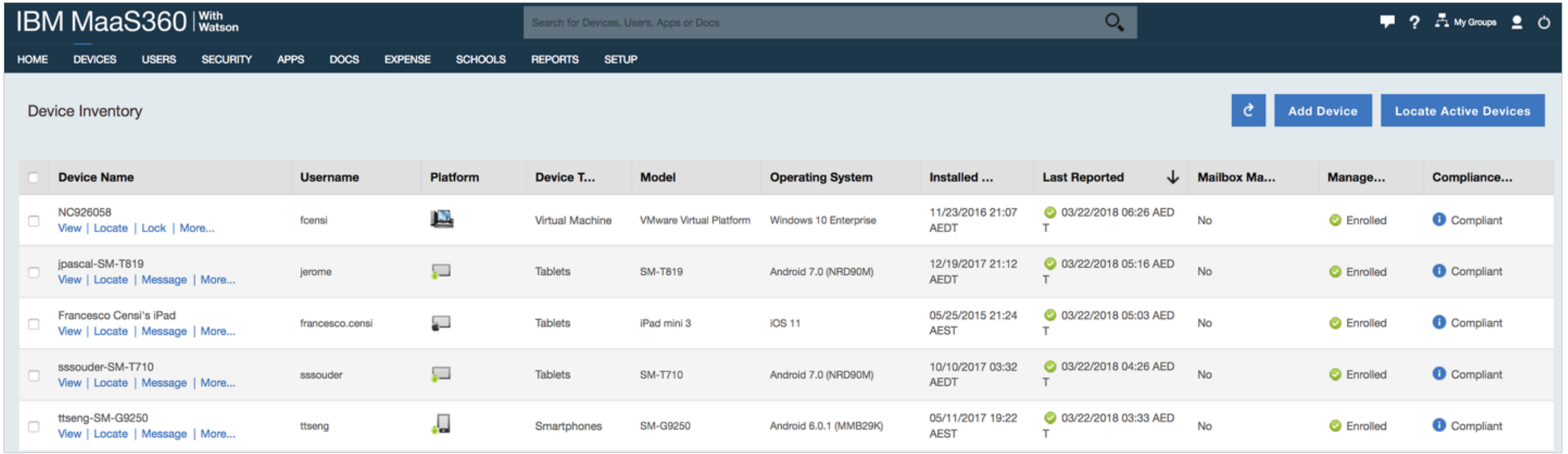
- Device Inventory
- Device Management Policies
- Adding an Active Directory Group
- iOS Management Policies
- Android Management Policies
- Typical Device Actions
- iOS and Android App Catalog
- Windows and macOS App Catalog
- Android Enterprise (Android for Work)
- Compliance Rules
- Single Sign-on (SSO)
- Threat Prevention
- Remote Support
- Windows and macOS Patch Management
- iOS and macOS Apple Device Enrollment Program (DEP)
- iOS and macOS Volume Purchase Program (VPP)
- MaaS360 VPN
- Samsung Knox Mobile Enrollment (KME)
- Android Kiosk
- Apple School Manager (ASM)
- iOS Update Controls
- MaaS360 Advisor: Cognitive Insights and Contextual Analytics

Tasks: Device Inventory

Administrators can manage all the devices in the environment by selecting **Devices** > **Inventory**.

Perform the following tasks to become familiar with the list of enrolled devices:

1. Find devices by Device Name, Username, Email Address
2. Filter devices by Install Date, OS Name, Last Reported, Managed Status
3. Sort devices, view devices, carry out actions on devices

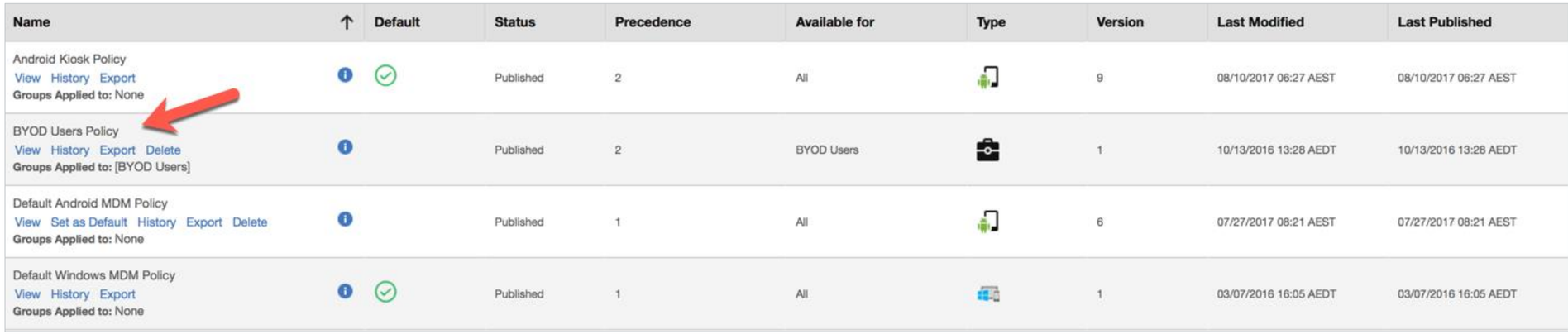


Video

Tasks: Device Management Policies

Policies and compliance rules work together to ensure that mobile users in your enterprise are adhering to corporate policy. Administrators enter policies in the MaaS360 portal that align with industry best practices and company standards. These policies can then be assigned to mobile devices, PCs and Mac OS X.

You are provided a number of template policies for a range of different device types. You can change these default policies, or create a new policy called **BYOD Users Policy** (as an example) then link it to an Active Directory Group which you'll assign shortly.



Name	Default	Status	Precedence	Available for	Type	Version	Last Modified	Last Published
Android Kiosk Policy View History Export **Groups Applied to:** None		Published	2	All		9	08/10/2017 06:27 AEST	08/10/2017 06:27 AEST
BYOD Users Policy View History Export Delete **Groups Applied to:** [BYOD Users]		Published	2	BYOD Users		1	10/13/2016 13:28 AEDT	10/13/2016 13:28 AEDT
Default Android MDM Policy View Set as Default History Export Delete **Groups Applied to:** None		Published	1	All		6	07/27/2017 08:21 AEST	07/27/2017 08:21 AEST
Default Windows MDM Policy View History Export **Groups Applied to:** None		Published	1	All		1	03/07/2016 16:05 AEDT	03/07/2016 16:05 AEDT

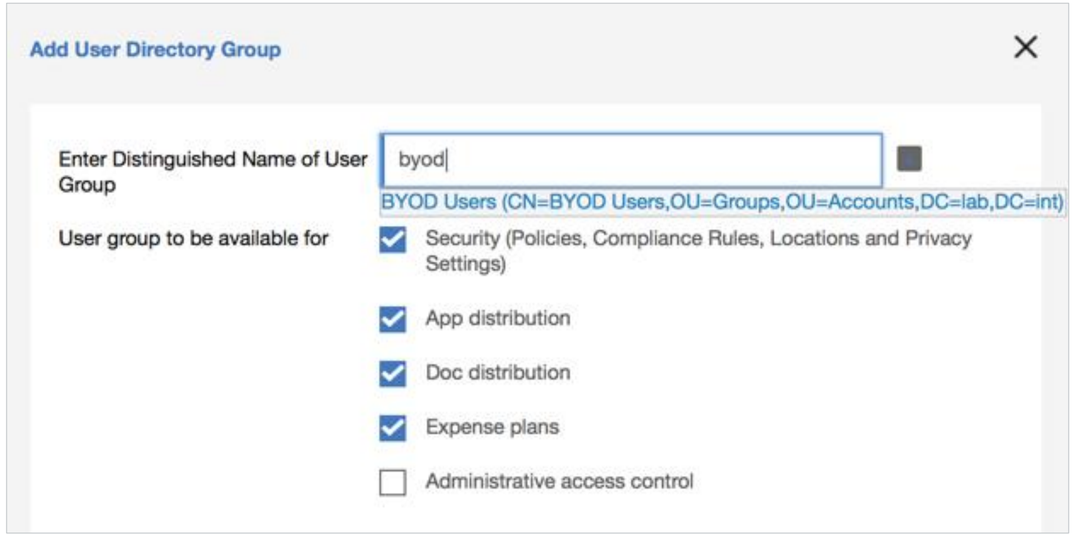
After you've updated an existing or new policy, in the upper right of the policy page, click **Save and Publish**. Each policy starts at Version 1 and increments with each policy change. The applied policy is also displayed within the MaaS360 application on the mobile device

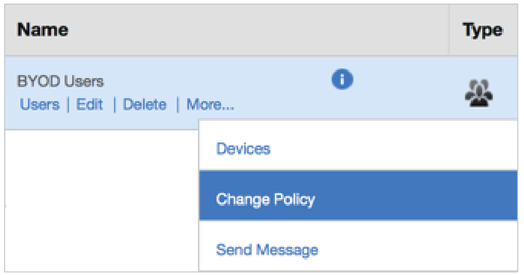
Video

Tasks: Adding an Active Directory Group

With the Cloud Extender (CE) up and running, you can now add those groups from Active Directory into the MaaS360 portal. This allows you to apply policies or distributed apps to users devices in those groups.

1. Select **Users – Groups**
2. Select **Add User Directory Group**
3. Enter the name of the group. The example shown on this page is an Active Directory group called **BYOD Users** (The group must contain one or more users).
4. Select **Save** and note that users may take up to 5 minutes to be displayed in the portal.
5. Select the user group and select **More…** then Change Policy. You may then select the test policy you created previously (**BYOD Users Policy**).

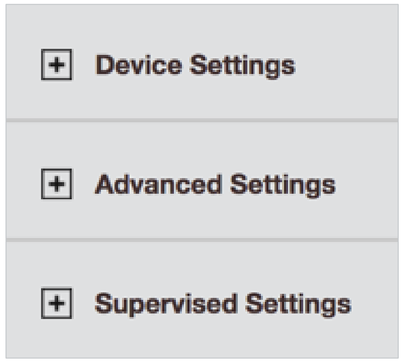




Video

Tasks: iOS Management Policies

iOS policies are grouped into the following categories:



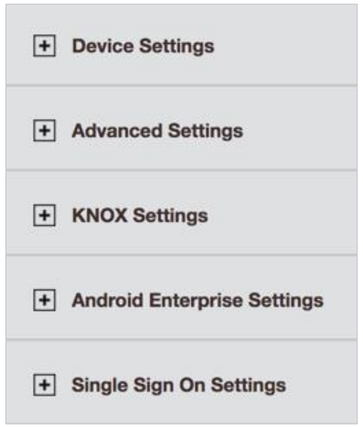
- **Device Settings**: Configure options for *Passcode, Restrictions, Application Compliance, ActiveSync, Threat Management (when enabled), Wi-Fi, VPN, AirPrint* etc.
- **Advanced Settings**: Configure *Email, Web Clips, Web Domains, Cellular, Fonts, LDAP, SSO* etc.
- **Supervised Settings**: Further advanced options for Supervised / Apple DEP devices such as *App Lock, Home Screen, Web Content and Shared Device*.

The following guide and video details how to deliver certificates to iOS (and macOS) devices for WiFi, ActiveSync and VPN and how this is configured in the iOS policy.

Video

Tasks: Android Management Policies

Android policies are grouped into the following categories:



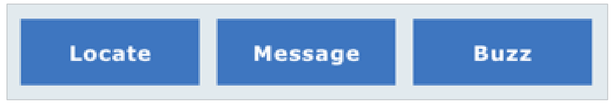
- **Device Settings**: Configure options for *Passcode, Restrictions, Application Compliance, ActiveSync, Threat Management (when enabled), Wi-Fi, VPN, Device Management* etc.
- **Advanced Settings**: Configure *Email, Wallpapers, Lock Screen, Certificates, APN, Kiosk Mode* etc.
- **KNOX Settings**: (When enabled) Further advanced options for Knox such as *Knox Setup, Passcode, Restrictions, App Compliance Accounts, SSO and Networking* etc.
- **Android for Work Settings**: (When enabled) For devices enrolled as Android Enterprise (previously Android for Work) these policies apply instead of Device or Advanced Settings. See the separate section on this feature.
- **Single Sign On Settings:** Enabling Single Sign On Conditional Access using IBM Cloud Identity

Video

Tasks: Typical Device Actions

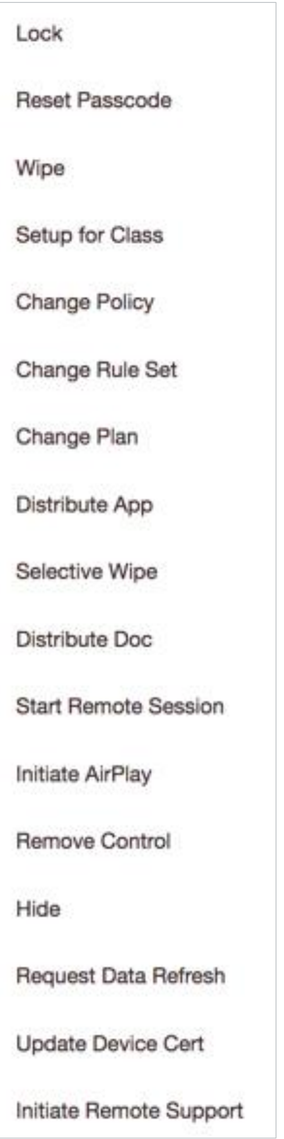
An administrator can select a specific device to view and manage, from **Devices** > **Inventory**. The administrator can also get to this view by selecting the devices that are highlighted in the **My Alert Center**. This provides a quick method to review and take action on devices that meet the alert criteria.

After the device information is displayed, the administrator selects the **More** menu to display the list of actions. The Actions that appear depend on a number of factors, including the device type and how it is being managed.



Try some of the following actions:

1. **Locate**: Locates the mobile device.
2. **Message**: Send a message to a device
3. **Buzz**: Sends an alert tone to help the user find the device in the immediate area
4. **Lock**: Sends a command that locks the device
5. **Selective Wipe**: Removes Apps, Content and Credentials from the device that was provisioned by MaaS360.
6. **Change Policy**: Changes the policy enforced on the device.

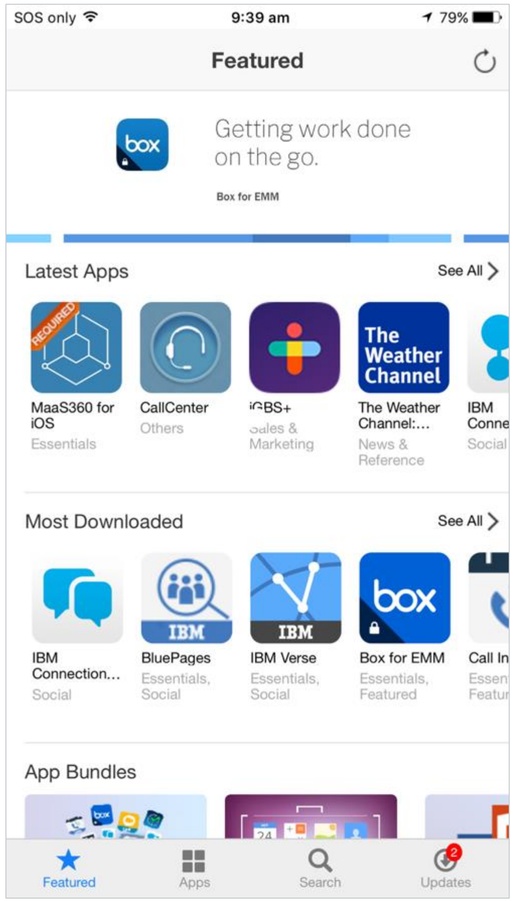


Tasks: iOS and Android App Catalog

The app management features of MaaS360 are accessed from the **Apps** tab. MaaS360 allows you to deploy apps to your users quickly and easily. Each app must be loaded into the MaaS360 App Catalog before it can be distributed.

To distribute an app, perform the following steps:

1. From the **Apps** – **Catalog** menu click the **Add** button
2. For iOS select **iOS** - **iTunes App Store App**.
3. In the App box, type in the name of the application. For example enter the word **Adobe**
4. Select **Adobe Acrobat Reader**
5. Select the **Policies and Distribution** tab
6. Select **Distribute to** and change to a Specific Device or group.
7. Click **Add** and enter your portal password.
8. The Adobe Reader application will shortly be displayed on the users mobile device under App Catalog



Video

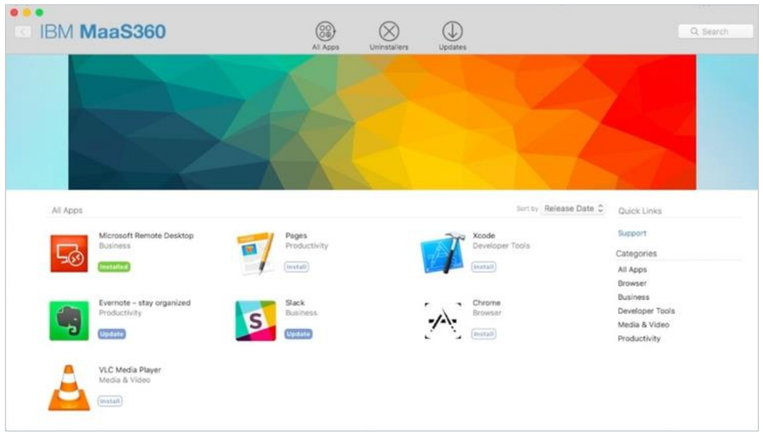
Tasks: Windows and macOS App Catalog

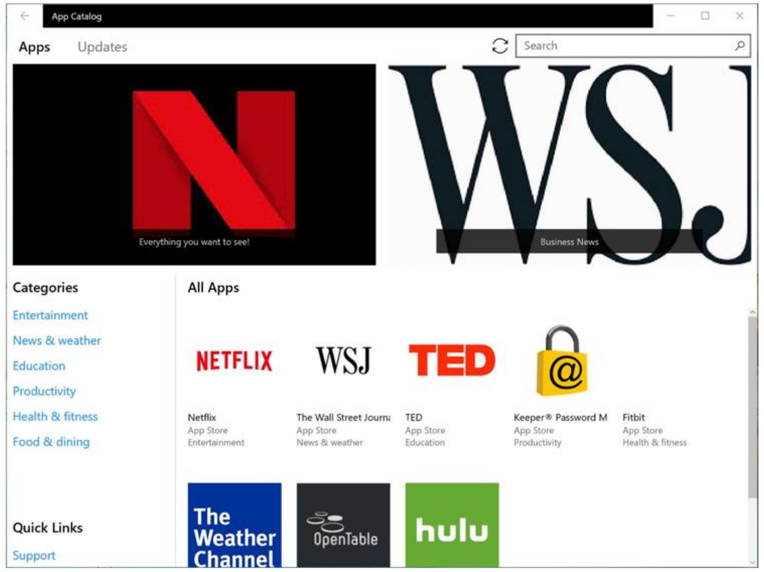
The app management features of MaaS360 are accessed from the **Apps** tab. MaaS360 allows you to deploy apps to your users quickly and easily. Each app must be loaded into the MaaS360 App Catalog before it can be distributed.

You can publish applications from the App Store to the Macs. This will be displayed in the MaaS360 App Catalog as shown on this example screen capture.

To distribute an Enterprise App for macOS (not from the macOS App Store) you will also need a macOS developer account to create a self signed cert. This is required for the uploaded apps, or the cert itself from the developer (Apple requirement).

Further information on the Windows App Catalog is available in this article, for macOS please see in this article.



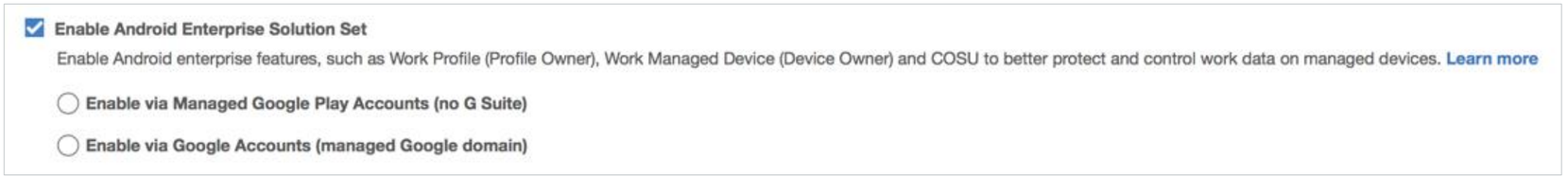


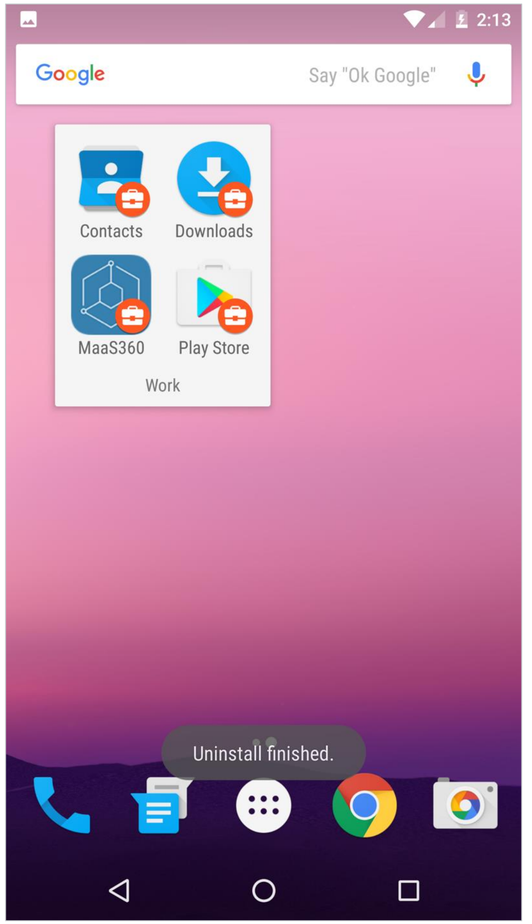
Video

Tasks: Android Enterprise (previously Android for Work)

MaaS360 seamlessly integrates with Google's Android Enterprise (previously Android for Work or AfW) to provide advanced Android management features. Note: Some items are still labelled as AfW.

Contact support@maas360.ibm.com to have Android for Work enabled as a new Service in your MaaS360 account. It will then be listed as follows:





Please see this detailed step by step guide on how to setup Android Enterprise.
Please see the following three videos for further information:

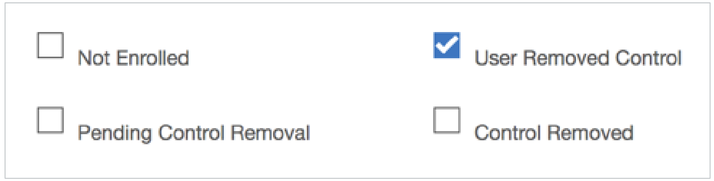
- Android Enterprise Integration – video
- Application management - video
- Android for Work Device Owner Mode - video

Video

Tasks: Compliance Rules

With MaaS360, you can apply compliance rules on your managed mobile devices. Compliance rules sets are conditions that are checked on devices on a real-time basis. If a device is not in compliance with the defined rule sets or conditions, appropriate enforcement actions are taken on the device.

1. Place your cursor over Security in the MaaS360 portal and select Compliance Rules.
2. Click **Add Rule Set**, enter **Test Rule 1** (as an example). Click **Continue**.
3. On the left side of the page, click **Enforcement Rules**.
4. Select the check box beside **Enrollment**
5. In the **Trigger Action on Managed Status** settings, clear the following check boxes as an example:



6. Verify that the Enforcement Action is set to **Alert** and clear the Email check box in the Notify User settings. Click **Save**. You are prompted for your portal password.
7. Click the blue arrow in the upper left to return to the Compliance Rules page.
8. Under the **Test Rule 1** compliance rule set, click the **Assign** link. The Assign Rule Set window opens.
9. Select an appropriate group from the **Group** drop-down list

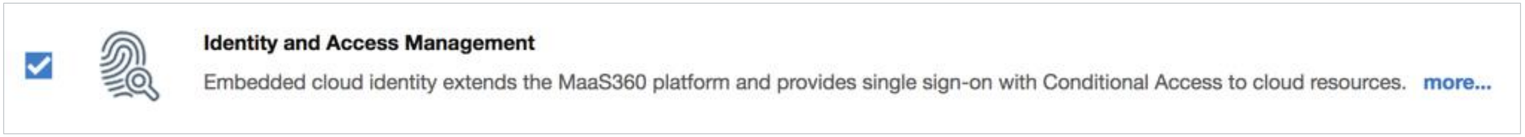
Video

Tasks: Single Sign-on (SSO)

IBM Cloud Identity (ICI) is an Identity as a Service (IDaaS) included with your MaaS360 license. ICI provides a number of services for iOS:

- Log in with Single Sign-On
- Conditional Access Management: Enforces only entitled users and devices to access SaaS apps
- Easy Identity Federation: Leverage pre-integrated connectors in ICI to easily integrate with SaaS apps - ie. Box, Workday, Salesforce, Concur

Contact support@maas360.ibm.com to have ICI enabled as a new Service in your MaaS360 account. It will then be listed as follows:



Create an ICI tenant using your IBMID. Next use the following article to add an application from one of the many app-connectors and publish this in MaaS360 with SSO enabled.

ICI documentation is available here.

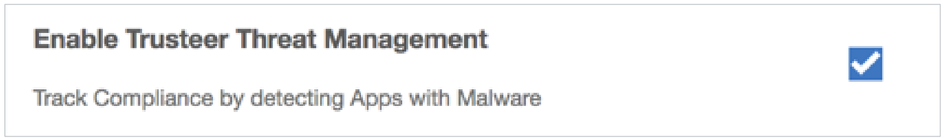
Tasks: Threat Prevention

Starting from iOS 9, enterprise applications can be restricted from installation unless they are installed by MaaS360. This can be configured for supervised devices via **Restrictions & Network - Allow Trust of Enterprise Apps.**

IBM MaaS360 Mobile Threat Management delivers a state-of-the-art system to further protect the user by alerting/blocking access to malicious web sites and apps, detecting insecure Wi-Fi hotspots and supplemental jailbreak discovery for iOS and Android.

Contact support@maas360.ibm.com to have Threat Prevention enabled in your MaaS360 account

1. To enable Threat Prevention, open the applicable iOS and Android policy.
2. Select **Trusteer Threat Management**
3. Select the option as shown:



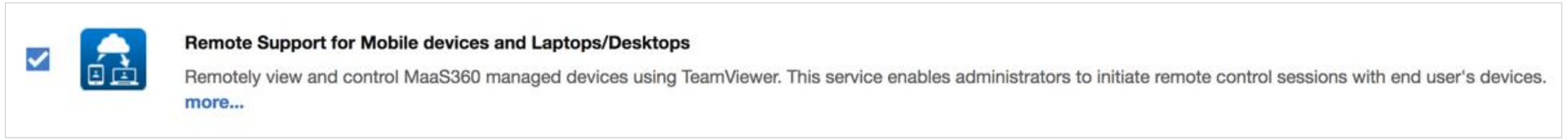
4. Select **Save and Publish**.

Video

Tasks: Remote Support

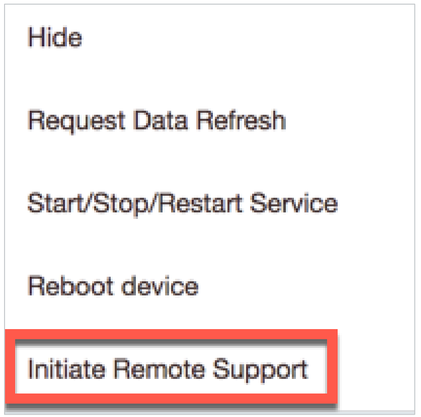
TeamViewer Remote Support for MaaS360 provides administrators remote view capabilities of iOS and remote control of macOS devices (when authorised by the remote user).

Contact support@maas360.ibm.com to trial this capability in your MaaS360 account. It will then be listed as follows:



Detailed setup documentation is available here.

1. Setup your TeamViewer trial
2. Distribute the **TeamViewer QuickSupport** application to all iOS devices
3. Select an iOS device and choose Initiate Remote Support (View for iOS)
4. Via the TeamViewer applications initate a remote view session
5. On the remote iOS device press the Power and Home button to send the devices current screen to the administrator

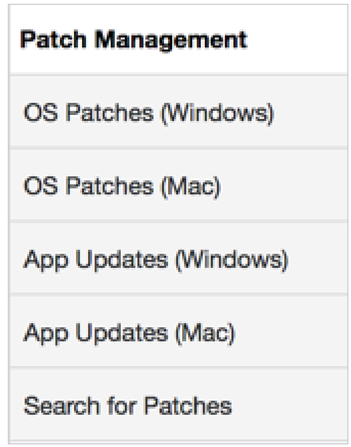


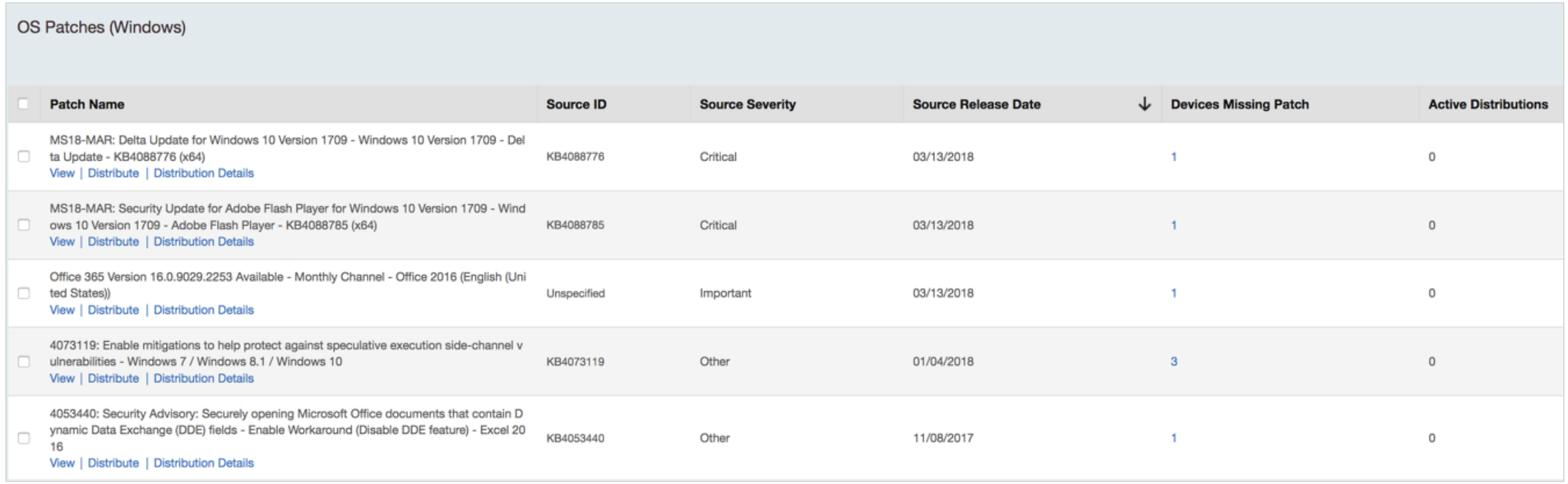
Video

Tasks: Windows and macOS Patch Management

MaaS360 provides patch management of Windows and macOS and 3rd party applications such as iTunes, Adobe and Java. Patches which need to be applied for all enrolled Macs is shown via **Security – Missing OS Patches**.

Contact support@maas360.ibm.com if you need to have this feature enabled on your account.





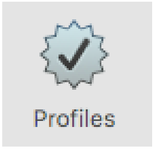
Tasks: iOS and macOS Apple Device Enrollment Program (DEP)

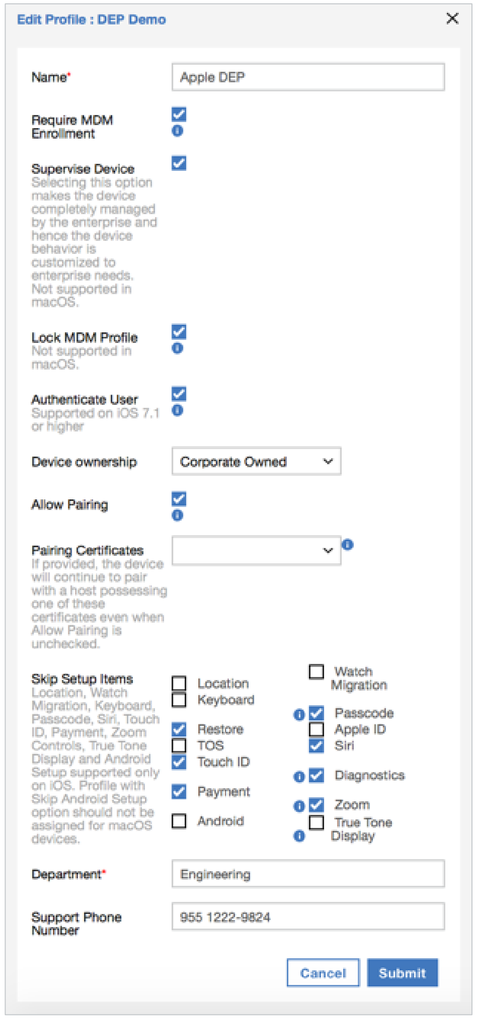
Apple DEP provides a fast, streamlined way to deploy your corporate-owned iOS and macOS devices, whether purchased directly from Apple or through participating Apple Authorized Resellers.

You can enable DEP via the **Services** menu within your MaaS360 portal.

A key benefit of DEP is that you're provided an enhanced list of policy controls plus your devices can be locked into MaaS360 too.

- The following article details how to setup DEP with MaaS360 along with an associated step by step video
- This article details the iOS DEP enrollment
- This article details the macOS DEP enrollment. A managed Mac will have the **Profiles** icon shown within System Preferences

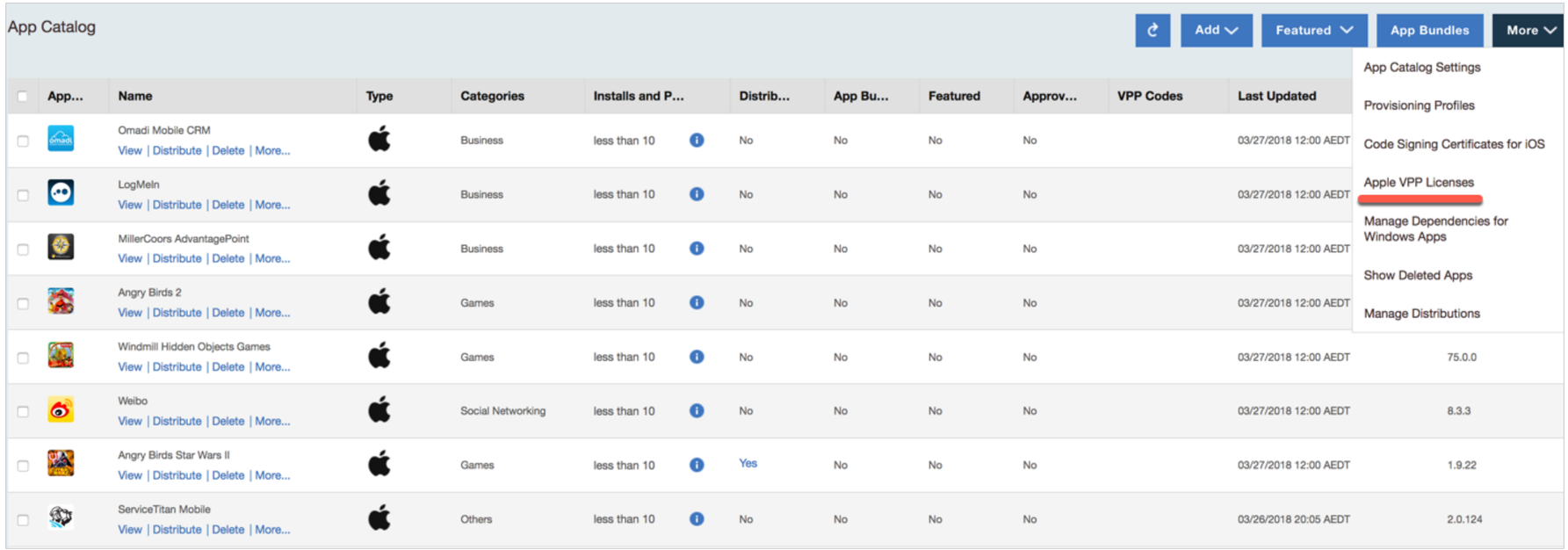




Tasks: iOS and macOS Volume Purchase Program (VPP)

Apple VPP enables the distribution of prepaid and free applications to users through MaaS360. With an Apple VPP license association, you always retain ownership of the application. At any time, you can remove the application from users' devices and reclaim the license for use on other devices.

- The following article details how to setup VPP with MaaS360 along with an associated step by step video
- Frequently asked questions (FAQs) about managed license integration VPP is available here
- The annual VPP token renew process is detailed here



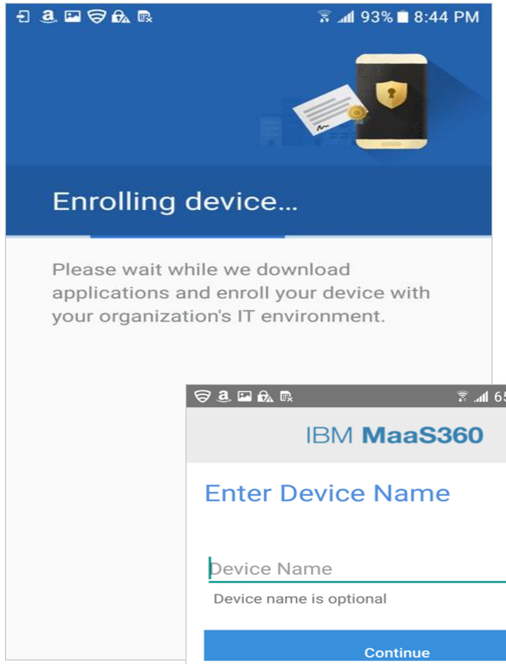
Tasks: Samsung Knox Mobile Enrollment (KME)

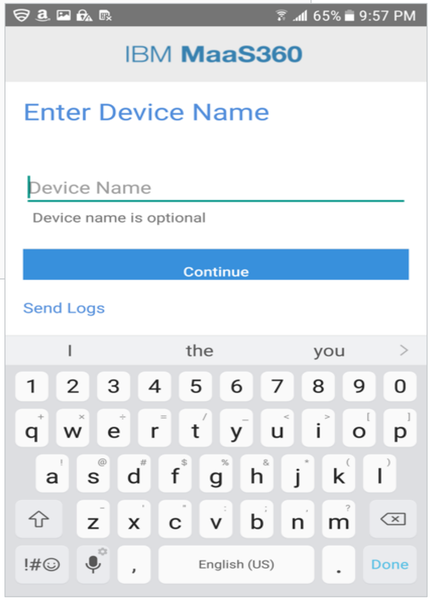
Samsung KME provides a streamlined way to deploy Samsung Android devices purchased via participating Samsung resellers.

To setup KME, select **Devices** - **Enrollments** - **More** - **Knox Mobile Enrollments**.

There are a number of enrollment options to choose from. Please see the following article for more information and further details on how to setup KME with MaaS360.

Note: The KME Shared Device Mode should be enabled on the account prior to enrolling devices. Contact support@maas360.ibm.com to enable this feature.





Tasks: Android Kiosk

Android Kiosk is an advanced security feature that allows an organization to restrict users to selective applications. This capability will locking down the device to display a single App or a specific set of Apps.

Android devices can operate as a Kiosk with MaaS360, although Samsung devices have additional capabilities. Android Kiosk is also available with Android Enterprise (called Corporate-Owned, Single-Use or COSU).

Kiosk settings are available under the **Android policy - Advanced Settings**. Or if you're using *Android for Work*, these are listed under **Android Policy – Android for Work - COSU (Kiosk Mode)**

- The following article provides further information on enabling Android Kiosk

- You can use an application such as Apk Extractor to identify the apk for the kiosk mode.

Tasks: Apple School Manager (ASM)

MaaS360 introduces support for **Apple School Manager** - an Apple program that allows easy deployment of iPads in Classroom environments by providing a platform to manage people, devices and content.

ASM allows creation of managed Apple ID's for students that can be used on iPads to login to access content and services like iTunes and iCloud. Click here to learn more about this program.

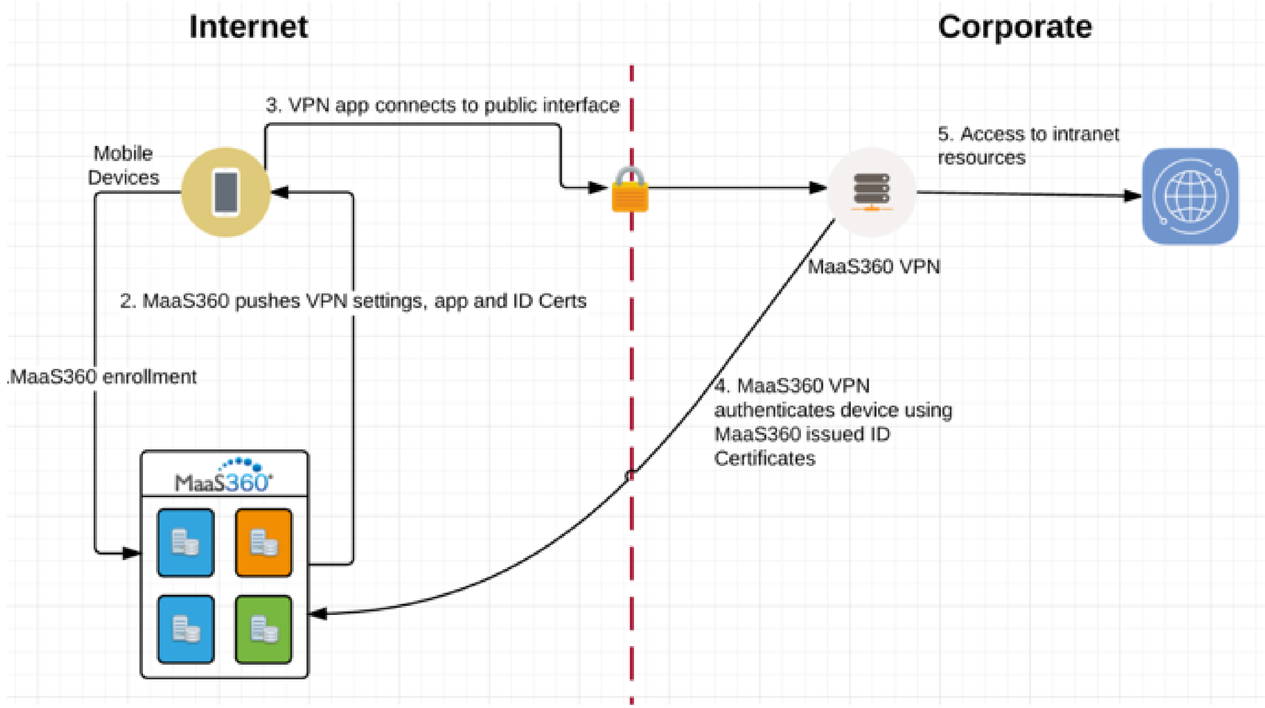
Contact support@maas360.ibm.com if you need to have this feature enabled on your account.

- The following article details how to setup ASM
- This article details ASM Shared Device support

Tasks: MaaS360 VPN

The MaaS360® VPN module is a VPN solution that allows users to access their corporate network from an iOS or an Android device (using the device's native VPN feature).

The MaaS360 VPN requires the Cloud Extender operates on at least a Windows Server 2012 R2 server.

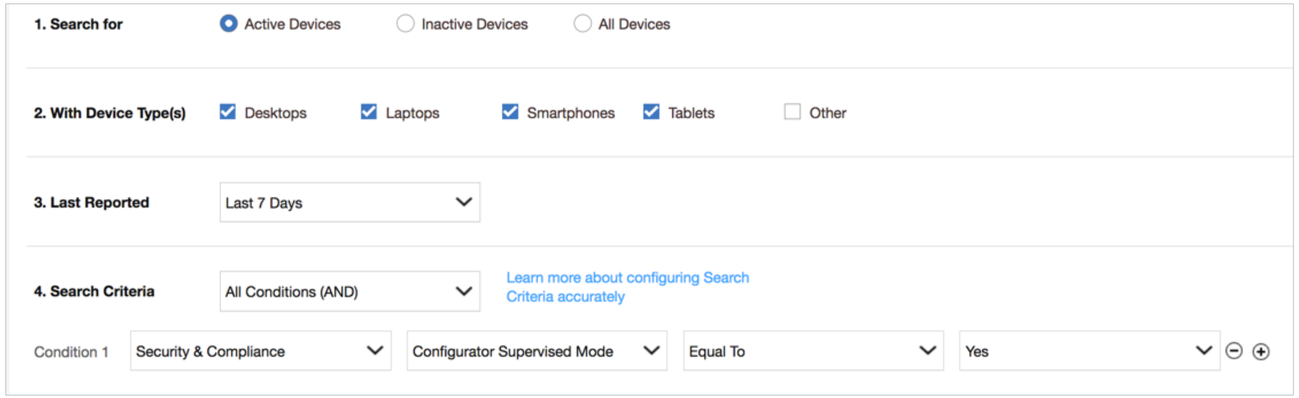


- The following article provides step by step instructions to install the MaaS360 VPN on the Cloud Extender.
- This article provides a VPN Setup Checklist and FAQ

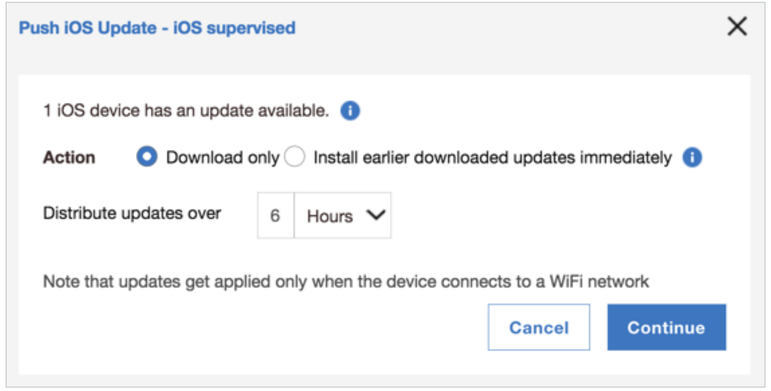
Video

Tasks: iOS Update Controls

For iOS Supervised devices, Apple provide additional iOS update controls. These are supported in MaaS360 by creating a device group for Supervised devices as shown:



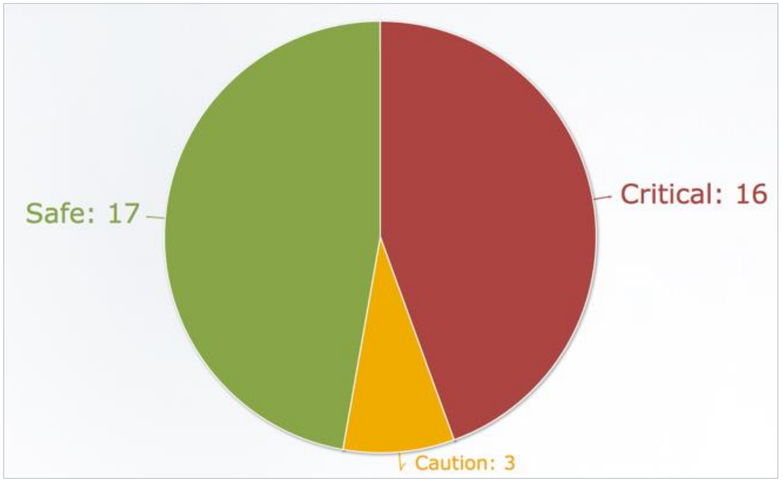
New iOS controls such as **Push iOS Update**, **Restart iOS Devices** and **Shutdown iOS Devices** can then be initiated to all devices in the group. Note: Devices with a passcode will need to enter it during an update.



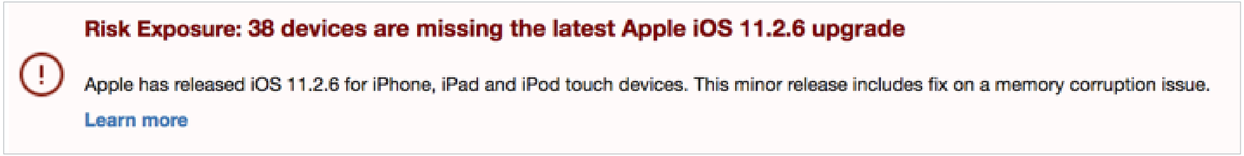
Tasks: MaaS360 Advisor: Cognitive Insights and Contextual Analytics

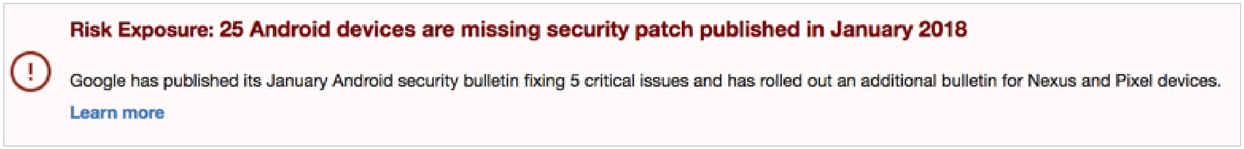
MaaS360 has several reports that are available in the Reports workflow in the portal. There are several categories to choose from based on the services that are enabled in your portal. The available report categories are Mobile Devices, Mobile Apps, Mobile Security, Mobile Expense Management, PC Inventory, and PC Security.

Report information is refreshed every 24 hours.



MaaS360 Advisor delivers cognitive insights, contextual analytics, and cloud-sourced benchmarking capabilities. These insights provide you with alerts tailored to your enrolled devices as shown below. Here is a video showing this capability.

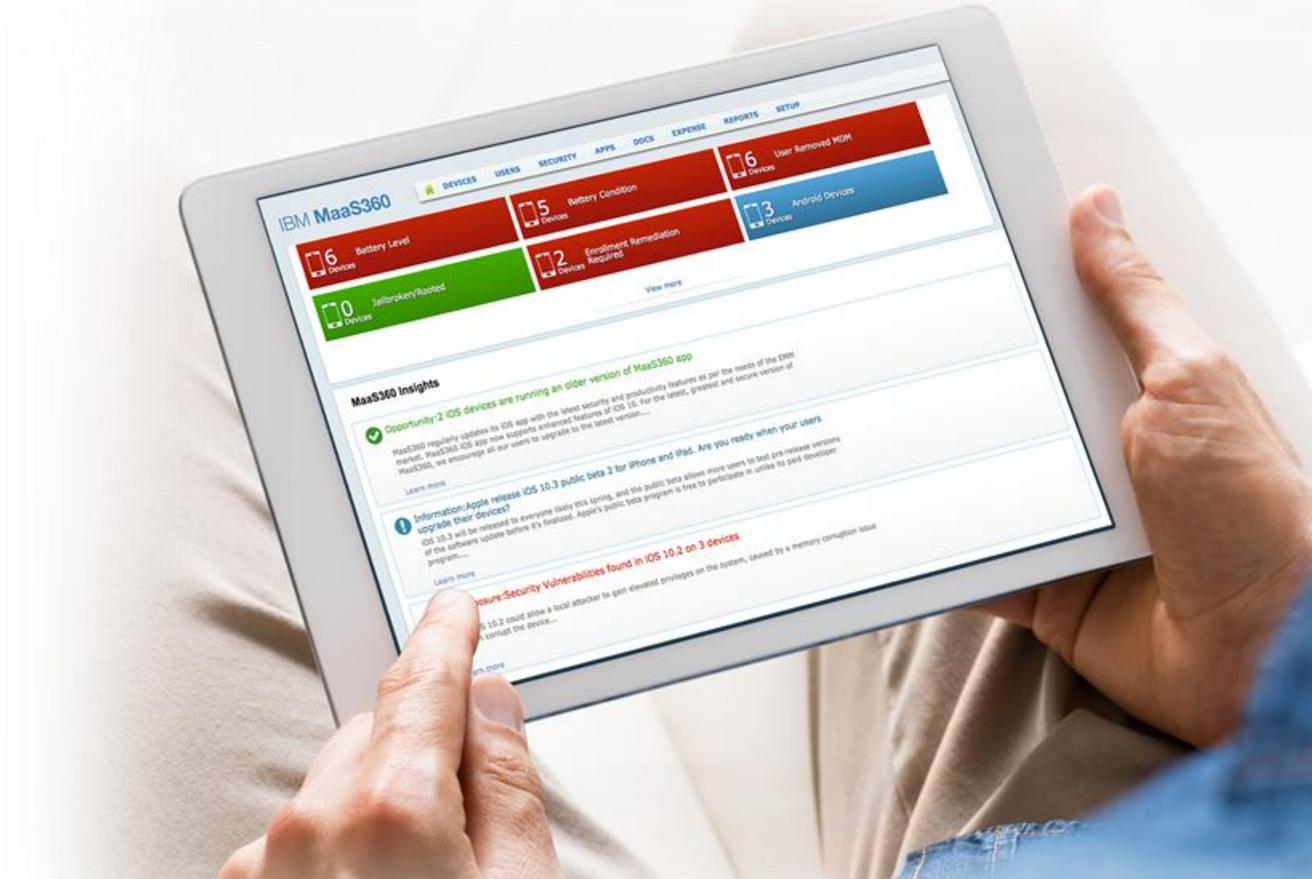




Resources

IBM MaaS360 | With Watson

- MaaS360 Information Sources - here
- Getting Started with MaaS360 video - here
- MaaS360 Release Announcement Wiki - here
- MaaS360 MDM SaaS Documentation Knowledge Center - here
- MaaS360 MaaSters Center Community on Developerworks - here
- MaaS360 Video Channel - here



FOLLOW US ON:

- www.ibm.com/maas360
- ibm.com/security
- securityintelligence.com
- xforce.ibmcloud.com
- @ibmsecurity
- youtube/user/ibmsecuritysolutions

MaaS360 with Watson Evaluator's Guide. Created by Darryl Miles, IBM Australia. September 2017. v2.2 (April 2018)

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective.

IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.