



MaaS360 Mobile Device Management (MDM) Administrators Guide

Copyright © 2014 Fiberlink® Corporation. All rights reserved.

Information in this document is subject to change without notice. The software described in this document is furnished under a license agreement or nondisclosure agreement. The software may be used or copied only in accordance with the terms of those agreements. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or any means electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Fiberlink Corporation.

All brands and their products are trademarks or registered trademarks of their respective holders and should be noted as such.

Fiberlink Corporation

1787 Sentry Parkway West

Blue Bell, PA 19422

April 2014

Table of Contents

Getting Started	6
Step 1: Select Platforms	6
Step 2: Add Devices	14
Step 3: Play	14
Advanced Configuration Steps	15
Services	15
Configure the Enrollment URL, the EULA, and Support Information	16
Login Settings	18
The MaaS360 Cloud Extender	19
Enabling Auto-Quarantine	22
MaaS360 Home Page	24
Navigation and the UI	24
Search	24
Snapshots	25
My Activity Feed	25
My Alert Center	26
Creating an Alert	27
Alert Center History	28
Additional Navigation	29
Devices	31
Inventory	31
Device Views	32
Actions	33
Custom Attributes	35
Groups	37
Advanced Search	38
Defining a Group	39
Customizing Columns	39
Enrollment Requests	40
Action History	42
Exceptions (Exchange ActiveSync and Lotus Traveler Only)	42
Users	44
Directory	44
Groups	45
Security	48

Policies	48
Precedence	50
Policy Files.....	51
Compliance Rules.....	52
Compliance Log	56
Privacy.....	56
Locations.....	58
Add an Address Based Location	59
Add a Wi-Fi based Location.....	60
Applications	62
The App Catalog	62
Adding an App to the App Catalog	62
Viewing an App	69
Distributing an App.....	70
Deleting an App.....	71
Distribution Details by Devices.....	71
Apple Store: Volume Purchasing Program.....	71
Documents	74
Content Library	74
Adding Documents to the Content Library	75
Edit.....	76
Distribute	78
Delete	79
Document Settings	79
Content Sources	80
Expense Management	82
Creating a New Plan	83
Changing an Existing Plan.....	84
Deactivating and Reactivating a Plan.....	84
Viewing Audit History.....	86
Reports	87
Platform Administration.....	90
Administrators	90
Create Portal Administrator	91
Roles and Rights	93
Creating a Role	98
Managing Roles.....	100
Administrator Logins Report.....	102

Appendix A: Features List	104
Device Support	104
Activation and Enrollment	105
Device Attributes	106
Hardware Attributes	106
Network Attributes	109
Location Attributes	112
Application Inventory	113
Security and Compliance	114
Running Services	117
MaaS360 Services	118
Mobile Data Usage	119
Browser History (Visited)	120
Browser History (Blocked)	121
BES (BlackBerry) Device Features	121
Privacy Settings	123
Actions	123
Device Actions	123
Group Actions	125
Policies	125
ActiveSync Policies	125
iOS Policies	130
Android Policies	148
Windows Phone Policies	169
Mac Policies	172
Secure Browser Policies	181
Compliance/Rules Engine	185
Apps	185
Documents	187
Document Management	187
Document Policies	188
Mobile Expense Management	189
End User Portal	189
Mobility Intelligence Reports	191
Mobile Devices	191
Computers	191
Cloud Extender	192

Getting Started

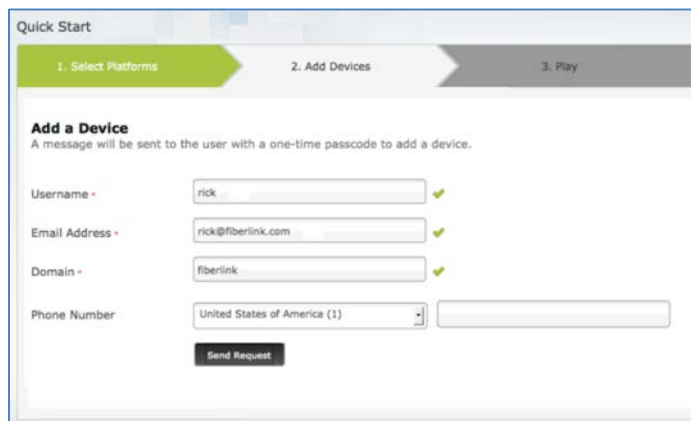
MaaS360 Mobile Device Management is a cloud-based multi-tenant platform that helps to monitor and manage your smartphones, tablets, and other mobile devices. MaaS360 is a comprehensive mobile device management solution that supports a variety of mobile device platforms including Apple iOS, Android, Windows Phones, BlackBerry and others. Ease of use, security and centralized management are some of the key features of MaaS360.

The MaaS360 system allows you to perform portal administration functions, device management, software distributions, policy self-service and device compliance functions. Monitor and manage all your mobile devices from a Web-based portal. The MaaS360 real-time reports include rich intuitive, real-time and interactive graphical reports.

You can register for a 30 day trial of the MaaS360 Mobile Device Management solution via the MaaS360 website at <http://www.maas360.com>.

After registering, a success message will appear. Click the green button to continue.

The Quick Start screens will walk you through setting up your account and enrolling devices.



Note: The account you create as part of your trial will continue into Production if you purchase MaaS360. The devices you enroll as part of your trial will not need to be enrolled again.

You will receive a welcome email containing important information about your trial. Be sure to keep this information, in case you need support later.

Step 1: Select Platforms

MaaS360 is automatically configured to support Android, Windows Phone and BlackBerry devices. If these are the only devices you will be using, click **Start without iOS** to move to the next step, **Add Devices**.

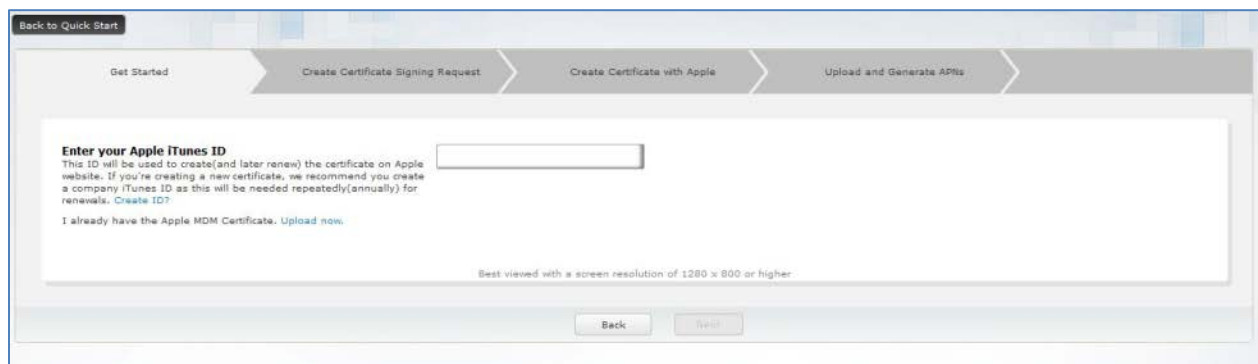


If you will be using iOS devices, Apple requires you to have an Apple Push Notification service (APNs) certificate. MaaS360 will walk you through the process of obtaining this certificate:

1. Click **Setup iOS Now**. The Safari, Chrome and Firefox web browsers are recommended for this process.
2. Enter a corporate AppleID. You must use the same AppleID every year when renewing your APNs certificate.

If you don't have an AppleID, hover over **Create ID?** and click **Apple Website**. This will take you to a page where you can create a corporate AppleID.

Enter the AppleID and click **Next**.

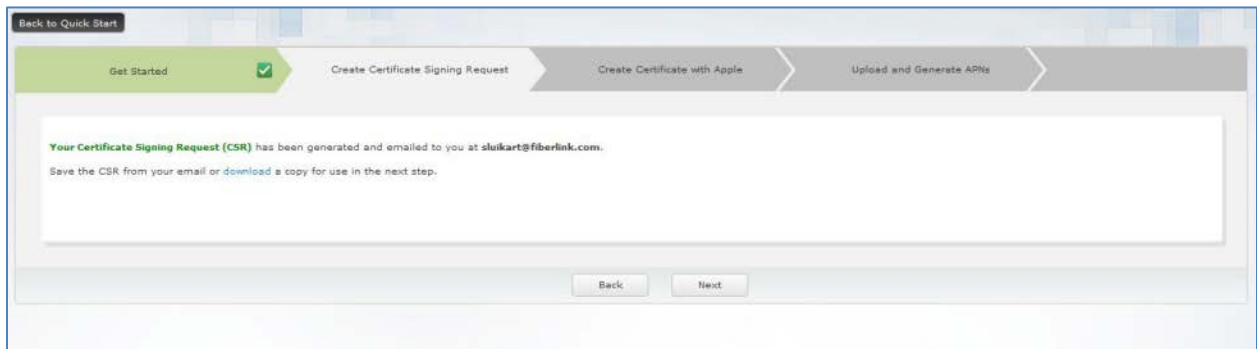


***Note:** We strongly recommend that this AppleID belong to your company and not an individual. The AppleID you use to set up your devices is the same one you will need to renew your certificate each year. If you use a personal AppleID and the person leaves your company, you will need to create a new AppleID at renewal time and re-enroll all of your iOS devices using it.*

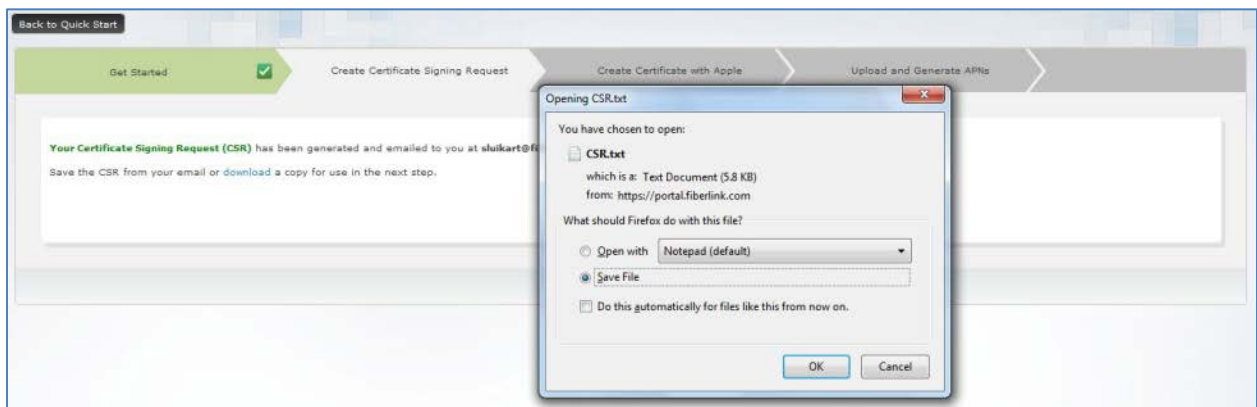
3. The Certificate Signing Request (CSR) will be generated automatically. This process can take up to 5 minutes. Please remain on this page or you will have to redo the previous steps.



4. The CSR will be emailed to the specified account. You can also click the **download** link to upload it right away.

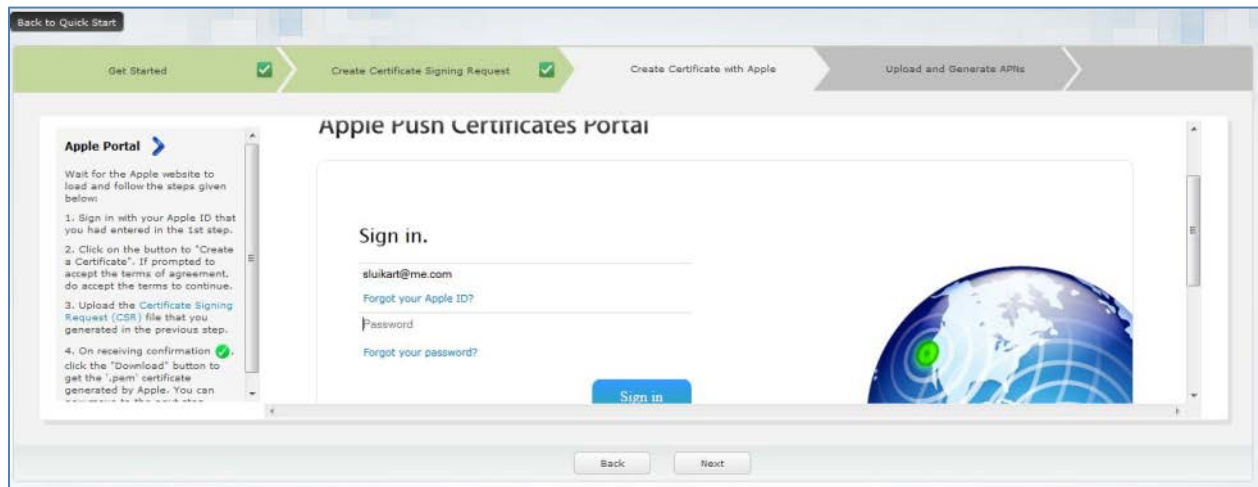


5. After clicking the **download** link, you will be able to save the file. Saving it will put it in your **Downloads** folder by default.

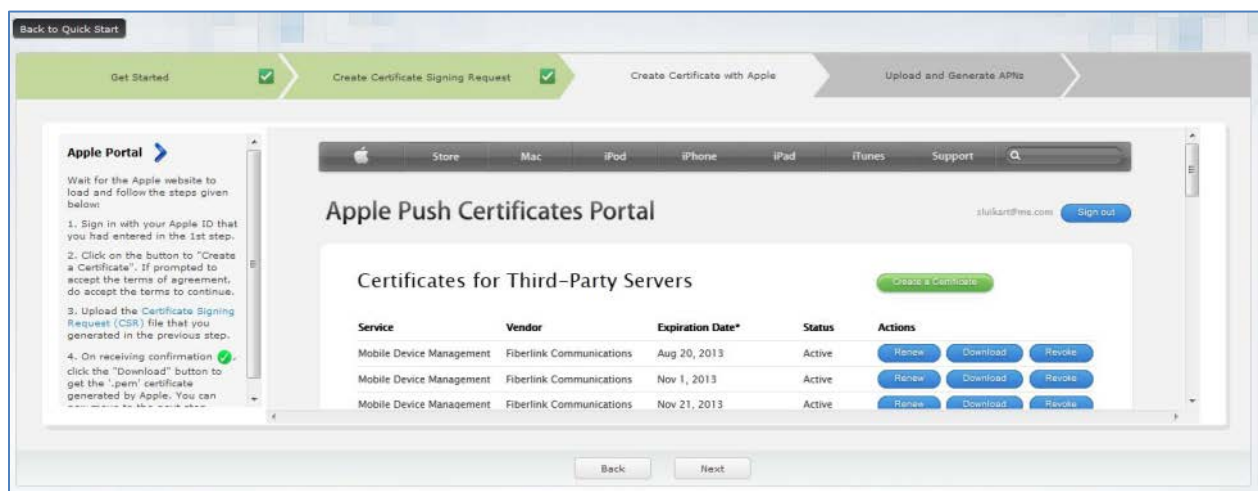


6. Enter the AppleID you used in Step 2 and the password, and then click **Sign in**.

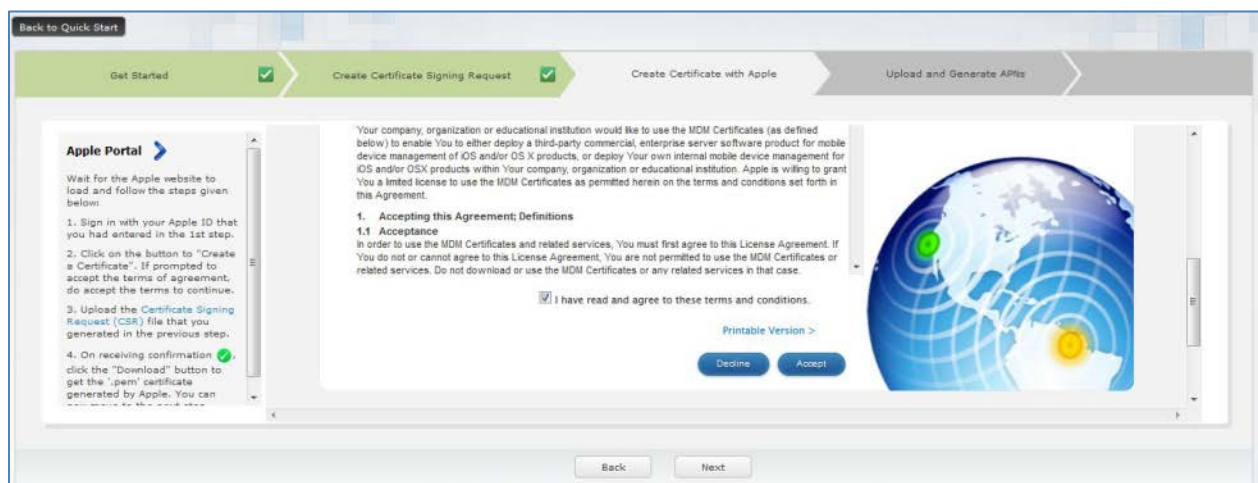
To skip the steps necessary to generate a PEM file, click **Next**. Continue with [Step #12](#).



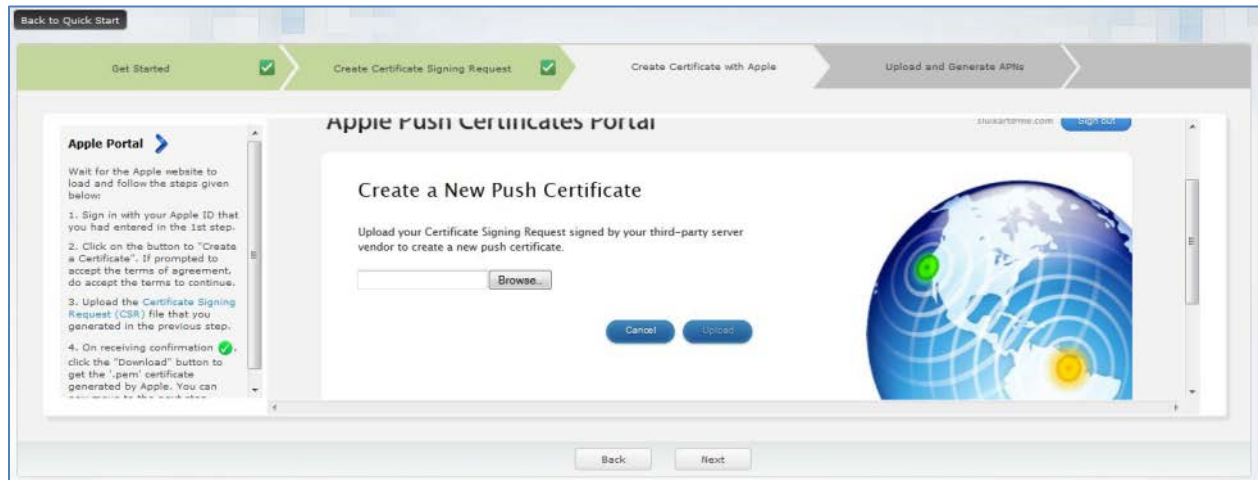
7. Click the green Create a Certificate button.



8. Check the box next to I have read and agree to these terms and conditions and click Accept.



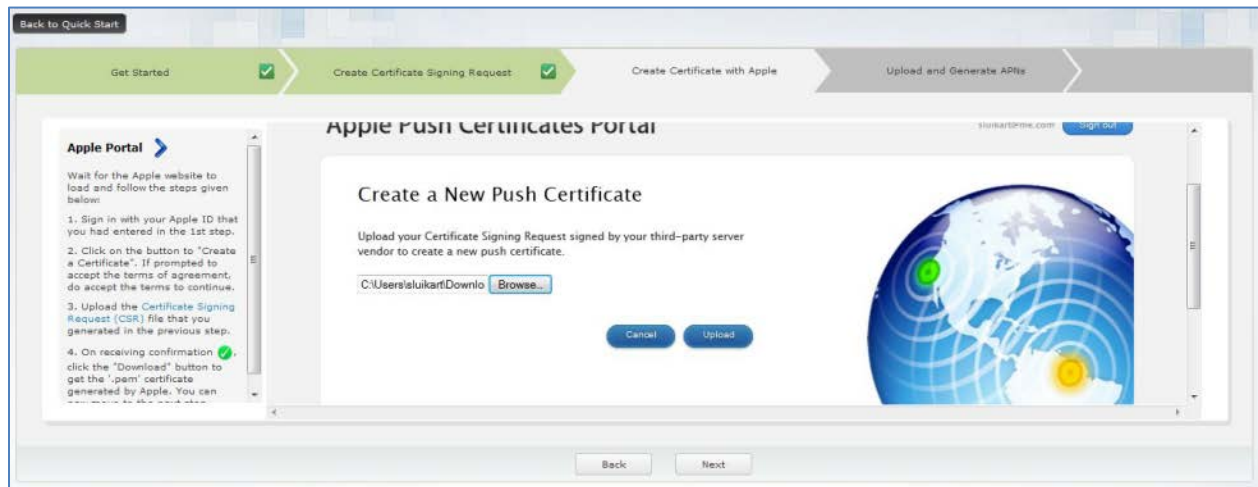
9. Now you need to find the file so you can upload it. Click **Browse**.



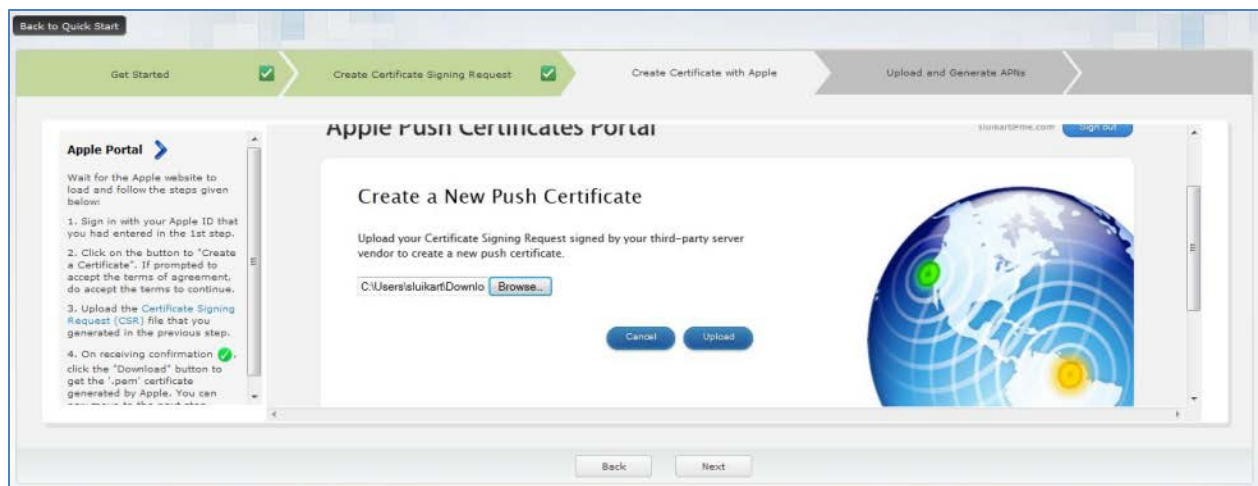
10. Find the CSR.txt file in your **Downloads** folder. Click **Open**.



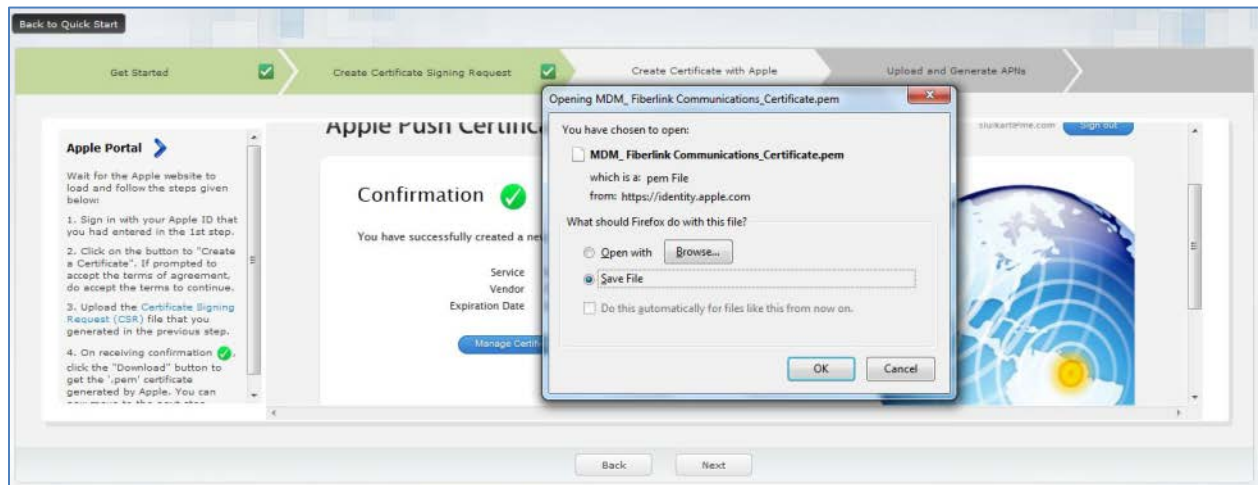
11. When the correct file is show in the field, click **Upload**.



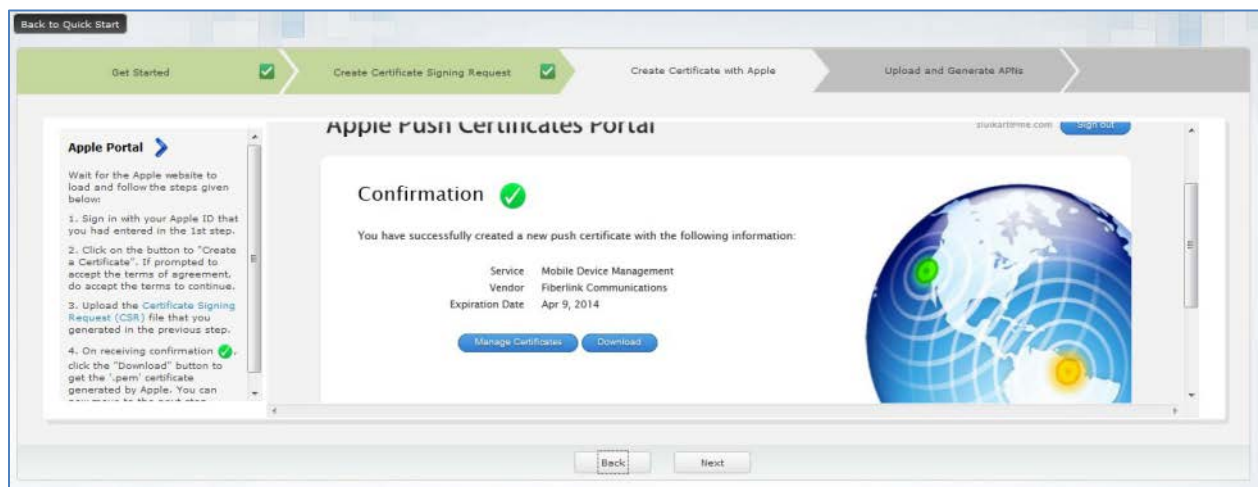
12. Click **Download** to download the PEM file. You will also receive this in email just like the CSR.txt file, but you will be using it in the very next step.



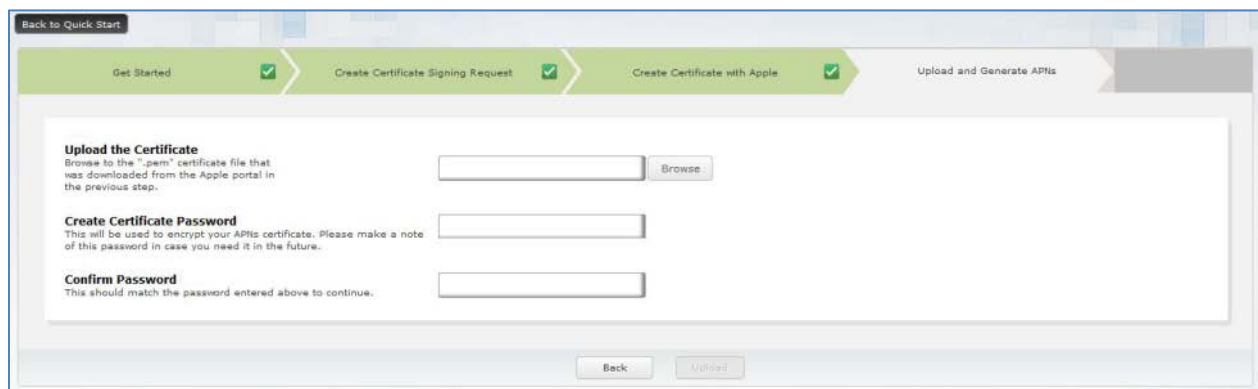
13. Click **OK** to save the PEM to your Downloads folder.



14. You will receive a confirmation message. Click Next.



15. Now you have to upload the certificate to MaaS360. Click Browse.

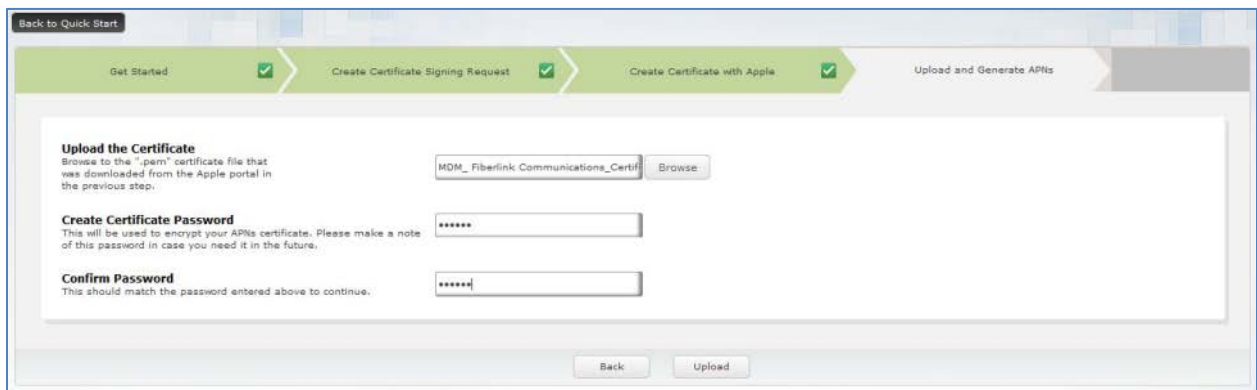


16. Find the file MDM_Fiberlink_Communications.pem in your Downloads folder. Click Open.

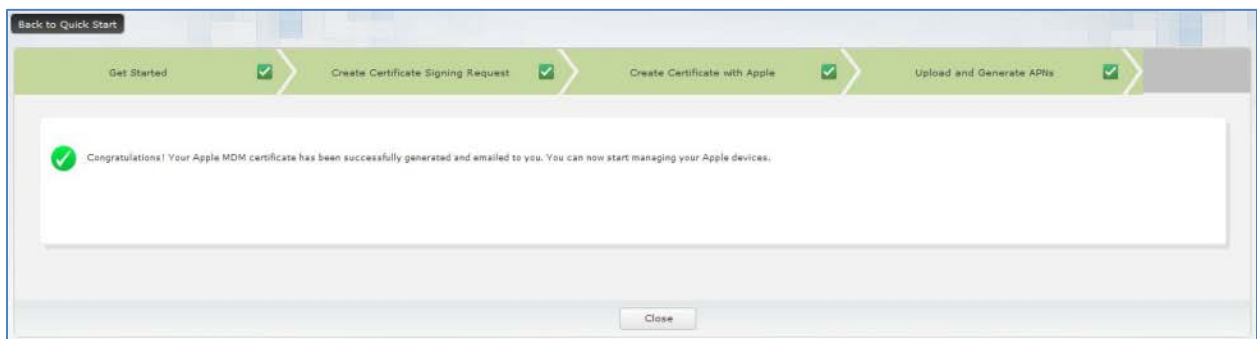


17. Enter a password. This password has no minimum security requirement. To help you remember the password, you may want to make it the same as your AppleID password.

After entering it in the Create Certificate Password and Confirm Password fields, click Upload.



18. The APNs certificate has been created. Click Close.



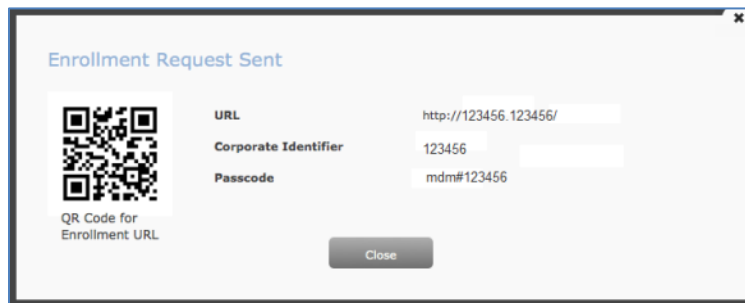
19. MaaS360 will automatically take you to the next step, adding a device.

Step 2: Add Devices

Click the second tab to begin enrolling devices in MaaS360.

1. Information from your enrollment will be automatically entered in the **Username**, **Email Address** and **Phone Number** fields, but you can override it. Review the **Domain** field; it is used for email and wireless set up, and more.
2. Click **Send Request**.

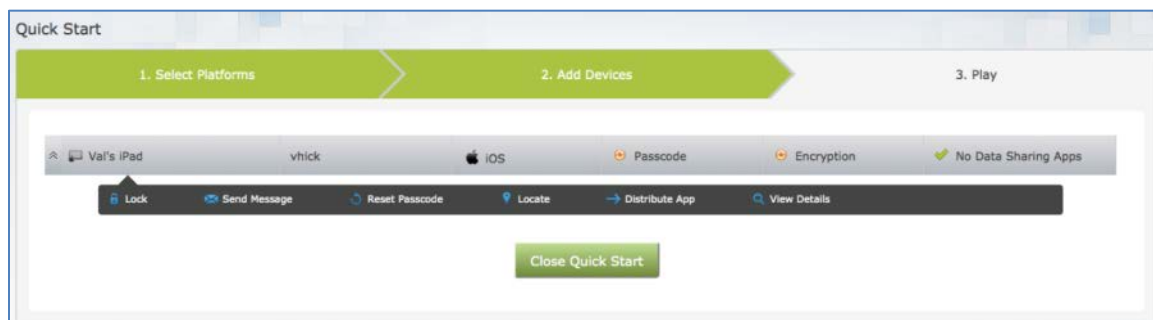
MaaS360 will send an enrollment request to the specified device.



When the end user gets the enrollment request, they will be directed to download the MaaS360 app. With just a few taps, they will install the app and the device will begin to send data to MaaS360.

Step 3: Play

Now you can review information about the enrolled device, take actions like Lock, Locate or Distribute App and more.

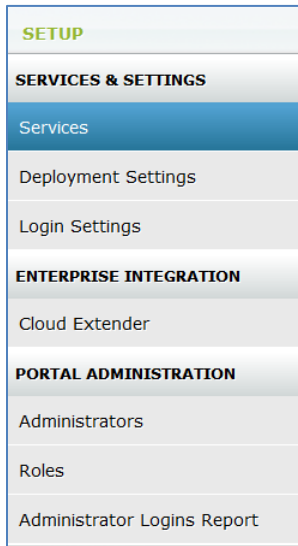


When you are finished, click **Close Quick Start** to access the MaaS360 Home page.

Advanced Configuration Steps

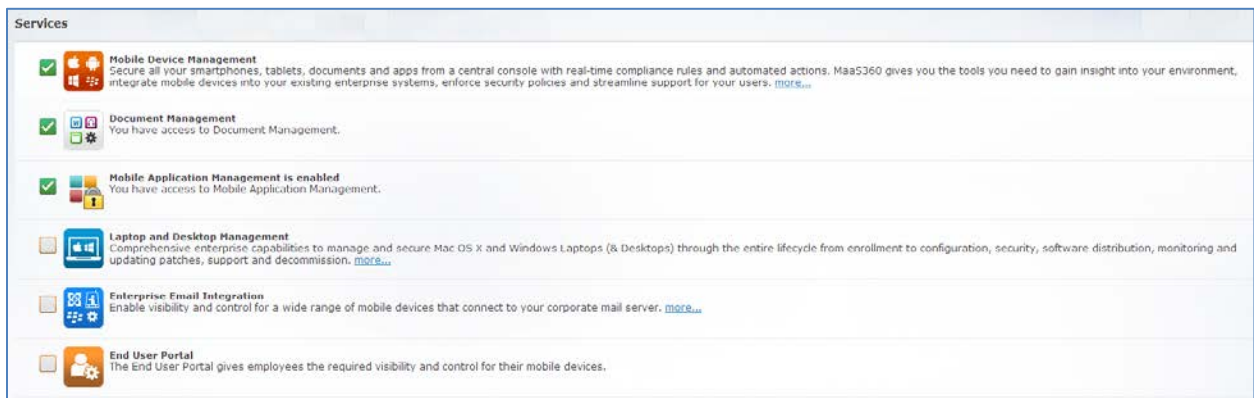
Services

To review and configure additional services, mouse over the **Setup** tab and click **Services**.




You can see the services that have already been set up and make changes.

***Note:** The items you see on this screen depend on the services you have purchased. For more information about any additional offerings, please contact your service representative.*



Mobile Device Management	If a platform has been set up for use in MaaS360, the icon will have a green checkbox in the upper left corner. You must upload an Apple MDM Certificate to manage iOS devices and a Symantec Code Signing Certificate to use the Windows Phone 8 Company Hub.
Document Management	Indicates that you can use MaaS360 Document Management.

Laptop and Desktop Management	Specifies if you are set up to use MaaS360 to manage your laptops and desktops.
ActiveSync Manager	Specifies if you are set up to use ActiveSync to manage devices that connect to your corporate Exchange Server using the ActiveSync protocol. Integration with Exchange 2007, Exchange 2010, Exchange 2013, Office 365 and Microsoft BPOS-Dedicated is supported. You will need to download and configure the MaaS360 Cloud Extender.
Lotus Traveler Manager	Specifies if you are set up to use Lotus Traveler to manage devices that connect to your corporate Domino Server using the ActiveSync protocol or Traveler client. You will need to download and configure the MaaS360 Cloud Extender.
BlackBerry Enterprise Server Manager	Specifies if you are set up to use BlackBerry Enterprise Server (BES) to manage BlackBerry devices in your enterprise. You will need to download and configure the MaaS360 Cloud Extender.
Enable End User Portal	The MaaS360 End User Portal allows your users to perform actions on their own devices. When you enable it, MaaS360 will display a log in link that you can send to your users: <div data-bbox="560 934 1425 1060" data-label="Complex-Block">  <p>End User Portal The End User Portal gives employees the required visibility and control for their mobile devices. less...</p> <p>Note: Your end users can access End User Portal using the following link: https://my.m3.maas360.com/authenticate.htm?account=30006711</p> </div>

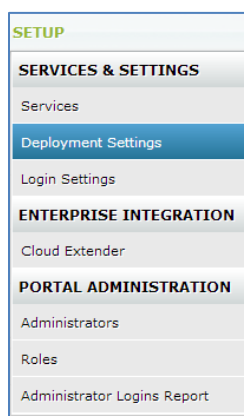
Note: The MaaS360 Cloud Extender is discussed in detail later in this document.

Before making a change, you will be prompted to enter your log in password as a security precaution.

When you are finished, click Close.

Configure the Enrollment URL, the EULA, and Support Information

Access the Deployment Settings screen, which is found on the Setup tab.



These enrollment settings are applicable to all your users. Make your changes, as needed, and click the Save button at the bottom of the page.

Deployment Settings

Corporate Identifier*

☒ Select Default User Authentication Mode

☒ Using a unique passcode sent to user on your request

[Learn more about how it works.](#)

☐ Authenticate against Corporate Active Directory

☐ Two-factor Authentication

☒ Device Platforms allowed to enroll

☒ iPhone
 ☒ iPad
 ☒ iPod
 ☒ Android
 ☒ Windows Phone

☒ Advanced Management for Corporate iOS Devices

☐ Setup Supervised Devices using Apple Configurator

 Start by downloading Enrollment profile from "Bulk Deployment" option under DEVICES > Enrollments.

☐ Select Default App Store Region for iOS devices

☐ Prompt user to accept your corporate usage policy while adding a new device

☐ Prompt for ownership

☒ Corporate Information

iOS Services Hostname

Contact Email

Phone Number

Custom Instructions

☐ Alert administrator on new device discovery

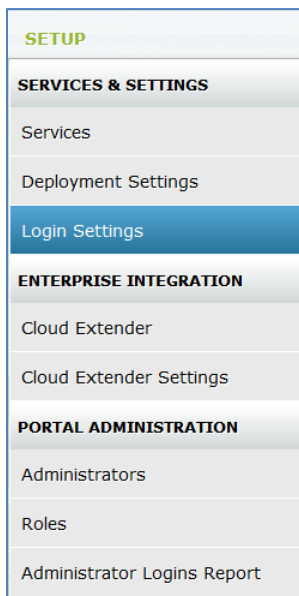
Save

Corporate Identifier to be used in your Enrollment URL	Your corporate identifier must be entered by your users when they enroll their devices.
Select Default User Authentication Mode	Specify how much authentication future device enrollments will require. You can: <ul style="list-style-type: none"> Send a passcode to the user's corporate email address, and require them to enter it during the enrollment process Require the user to enter their corporate Active Directory credentials when enrolling and authenticate against it Both of the above The MaaS360 Cloud Extender is required.
Device Platforms allowed to enroll	Specify which device types are allowed to enroll in MaaS360.
Advanced Management for Corporate iOS Devices	Specify if you want to use advanced management for corporate iOS devices.
Select Default App Store Region for iOS devices	Choose a default app store region from the pull-down menu. Users can change it in their individual app catalogs.

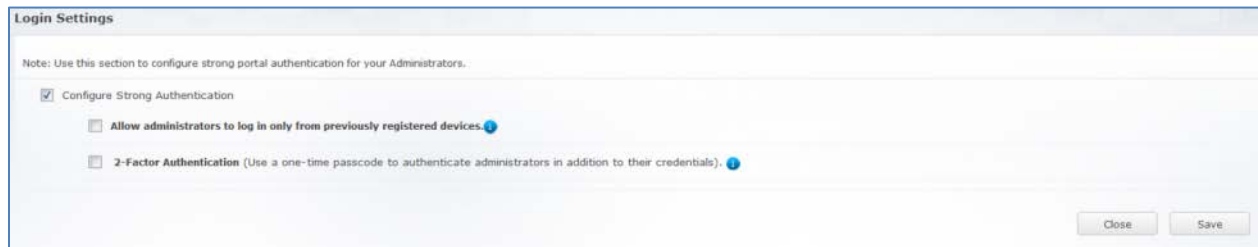
Prompt user to accept your corporate usage policy while adding a new device	<p>If checked, MaaS360 will display your usage policy to your users. They must read the policy and agree to it before downloading the MaaS360 app.</p> <p>When this box is checked, MaaS360 will allow you to browse to your usage policy and upload it.</p>
Corporate Information	<p>Any prompts for over-the-air actions scheduled for iOS 7 devices use the iOS Services Hostname.</p> <p>If you want to display a support email address and phone number in case your users need to contact you, enter the information in the respective fields. The information will appear in the MaaS360 app on the devices.</p>
Alert administrator on new device discovery	<p>Check the box if you want an email to be sent to an administrator when a new device is reported from your corporate email server or a new device.</p> <p>MaaS360 will allow you to specify which devices should trigger the alert:</p> <ul style="list-style-type: none"> • All devices • Smartphones and tablets only • Laptops and desktops only <p>It will also let you enter the email address that will be used for the notifications.</p>

Login Settings

If you want to require portal administrators to use strong authentication, select **Login Settings** from the Setup menu.



Select the login settings you want, then click **Save**.



Configure Strong Authentication	Select the checkbox to display the options.
Allow administrators to log in only from previously registered devices	MaaS360 will flag any device that has never been used to access it before, and will send the owner an email with a passcode. The person who is trying to log in must enter that passcode before accessing the portal. This only happens once—the device is automatically registered when the log in is successful.
2-Factor Authentication	Devices will be subject to the registration process and the administrators will have to enter their credentials when they log in.

The MaaS360 Cloud Extender

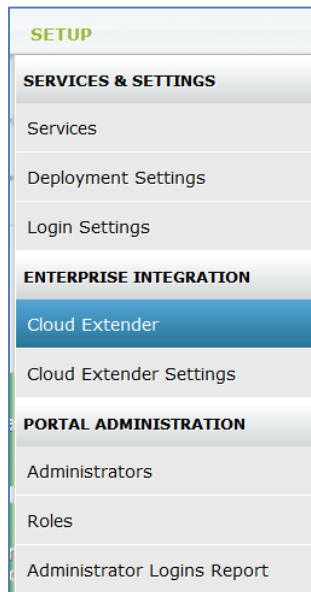
If you wish to gain visibility into your existing email platforms for Microsoft Exchange, Lotus Traveler, Office 365 or your BlackBerry Enterprise Server, you will need to install the MaaS360 Cloud Extender. Installing the Cloud Extender also allows you to use your corporate Active Directory or LDAP for self-service enrollment and visibility into your existing groups for management. The Cloud Extender can also be used to integrate with your Certificate Authority to push certs to devices to be used for email, wireless or VPN authentication.

Mouse over **Setup** and click **Cloud Extender**. Click the links to download the Cloud Extender and to request the license key.

For detailed installation instructions, refer to the *MaaS360 Cloud Extender Installation Guide*.

Enterprise Integration

You can see details about your MaaS360 Cloud Extender configuration by mousing over the **Setup** menu and clicking **Cloud Extender**.



This screen shows the steps to download the Cloud Extender, and lists your integration options.

Cloud Extender is a piece of software that runs as a service on a Microsoft Windows Server in your network to allow for integration with your corporate resources.

Integration Options

User Authentication
Integrate with your Corporate Active Directory or LDAP to allow self-service enrollment.
Note: After configuring this service on the Cloud Extender, go to [SETUP >> Deployment Settings](#) to update the User Authentication Mode.

User and Groups Import
Integrate with your Corporate Active Directory of LDAP to import existing users and user group information for management and access control.
Note: Any local user will be overwritten by your corporate data.

Mail Integration
Enable auto-discovery of devices connecting to your mail environment. Once in place use the settings to control who is allowed to connect using quarantine and block settings.
Note: This service must be enabled through [SETUP >> Services](#) prior to use.

Certificate Authority
Distribute Certificates to devices using your existing Microsoft or Symantec Certificate Authority to use for authentication of mail, wireless or vpn.

Step 1: To integrate with your Microsoft Exchange (2007+) or Traveler environment, enable the required service through [SETUP >> Services](#). For other integration, go to Step 2.

Step 2: [Click here](#) to get your License Key.

Step 3: [Click here](#) to download the Cloud Extender.

Step 4: Install the Cloud Extender software to launch the Configuration Utility.

Step 5: Follow the steps in the Cloud Extender Configuration Utility to setup the required integration.


For more information, refer to the Cloud Extender Installation Guide.

Cloud Extender Settings

Mouse over the **Setup** tab and select **Cloud Extender Settings**.

SETUP
SERVICES & SETTINGS
Services
Deployment Settings
Login Settings
ENTERPRISE INTEGRATION
Cloud Extender
Cloud Extender Settings
PORTAL ADMINISTRATION
Administrators
Roles
Administrator Logins Report

This screen shows the different settings configured for your Cloud Extender and allows you to change them.


Exchange ActiveSync

Auto-Quarantine Settings

Enable Auto-Quarantine of Devices
Disable

Note: In Exchange 2010 and Exchange 2013, setting this to "Enable" will override Auto-Quarantine setting configured directly in the Exchange server and also clear any email addresses set for notification

Data Collection Frequency

Device Data Query Frequency
Every 15 minutes

Frequency at which Exchange Server is queried to determine changes to Device data.

Device Heartbeat Query Frequency
Every hour

Frequency at which Exchange Server is queried to determine changes to Last Reported date of devices into Exchange Server.

Full Data Refresh Day
Sunday

Day of the week on which all device and policy data is uploaded from Exchange Server to ensure all data is in sync. The Refresh will start at a random time on the specified day.

Full Data Refresh Frequency
Every week

Frequency at which all device and policy data is uploaded from Exchange Server.

You can click **Edit** to change the settings, or select an action from the menu in the upper right corner.

Edit

Actions

Actions

View Audit History

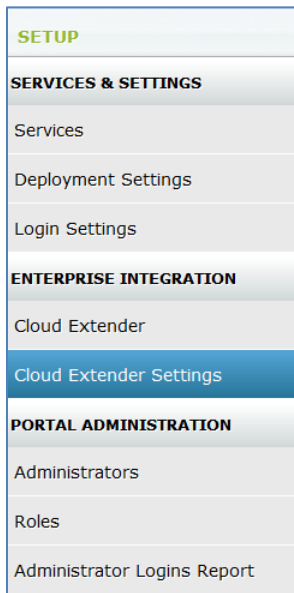
View Audit History will allow you to see the changes that have been made previously.

Enabling Auto-Quarantine

If you are using ActiveSync, MaaS360 can put all devices that attempt to access your corporate resources into quarantine automatically until an administrator approves them.

To configure Auto-Quarantine, perform the following steps:

1. Click **Setup > Cloud Extender Settings**.



2. Click **Edit**.
3. Change the **Auto-Quarantine Settings** to enable the feature, and provide an email address that will receive notifications about quarantined devices.

4. Click **Save** and **Publish** when you are finished. The policy will not go into effect until it has been published.

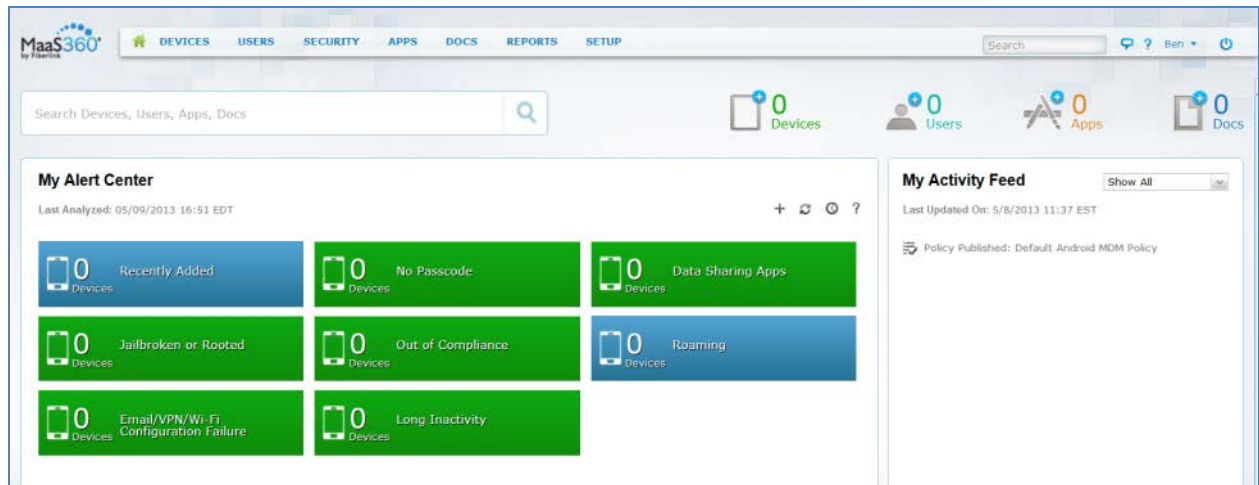
The sample configuration shown above will do the following:

- Any existing device will be grandfathered into an allowed list

- Enrolled devices will be auto-approved
- Manual Exchange configurations will be quarantined and the administrator will be notified

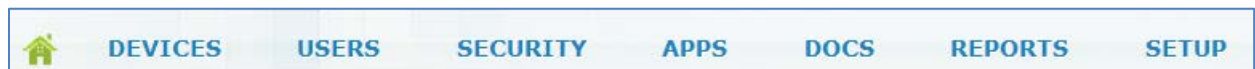
MaaS360 Home Page

MaaS360 has been designed to make it easy for you to get information and take action quickly and easily.



Navigation and the UI


The MaaS360 user interface provides an easy-to-use tab and menu navigation layout, allowing quicker access to the available applications.




Tabs correspond to a related set of applications or tasks available to the portal user.

The menus show the individual workflows, reports, etc. for the portal user. To access the menus, mouse over the tab and the menu will appear. Click once to access the item.



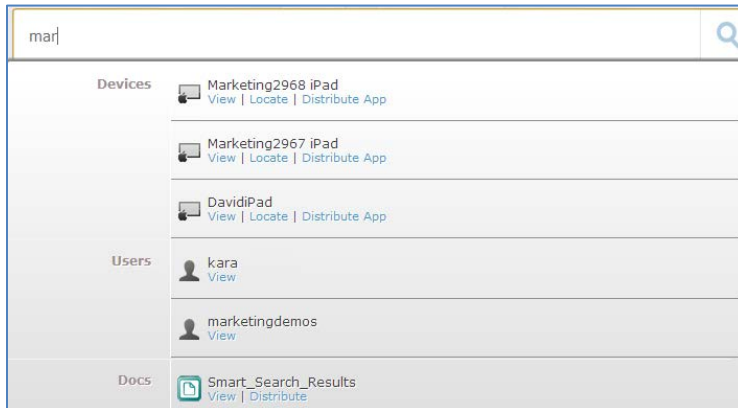
Click  to return to the Home page.

When looking at an item from a list, you can click  to return to the full list.

Click  to refresh the data.

Search

If you begin typing in the Search field, MaaS360 will give you possible matches to choose from among the devices, users, apps and documents in your environment.



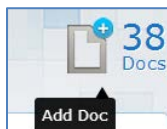
When you see the item you want, you can take action by clicking the link below it; you can view, locate, distribute an app, etc. In the example above, you can click the **Locate** link under *Marketing2968 iPad* to display a map that shows the device's location.

Snapshots

MaaS360 also gives you a snapshot of your environment at the top of the screen.



You can click one of the plus signs  to add a device, user, app or document.



The text of each snapshot is a link.



- **Devices:** Access the Device Inventory
- **Users:** Access the User Directory
- **Apps:** Access the App Catalog
- **Docs:** Access the Content Library


My Activity Feed

My Activity Feed shows you important updates, in much the same way that social networking sites do. The list of new devices, rule violations (compliance events highlighted in red), etc. is updated in real time, and you can click on them to see details about the activity.

My Activity Feed
Show All

Last Updated On: 5/9/2013 09:01 UTC

- New Document: PM_Case_Study.pdf
- New Document: DU_Case_Study.pdf
- New Document: MaaS360_Cloud_Extender_-_Office365_Confi...
- New App: Hay Day Fan Wiki HD
- New Document: import.csv
- New Document: Copy_of_RFI.xlsx
- New Document: FOODSRequirements.docx
- Policy Published: JN iOS Policy - Do Not Delete

The Home page icon shows the number of new activities that have been added to the feed. In this example, there is one new activity: 

You can use the filter to display specific types of activities.

My Activity Feed
Updates

Last Updated On: 5/9/2013 01:26 UTC

- Policy Published: JN iOS Policy - Do Not Delete
- Policy Published: JN iOS Policy - Do Not Delete
- Policy Published: JN iOS Policy - Do Not Delete
- Policy Published: JN Browser Policy - Do Not Delete
- Policy Published: Marketing - Jonathan
- Policy Published: Clint's IOS WorkPlace Policy
- Policy Published: Default Secure Browser Policy
- Policy Published: JN iOS Policy - Do Not Delete

My Alert Center

The Home page also displays My Alert Center, a dashboard of important information that you can customize to meet the needs of your organization.

My Alert Center
Last Analyzed: 05/28/2013 15:22 UTC

51 iOS Devices	51 Remote Wipe Support	28 Personal Devices
14 Data Sharing Apps	6 Samsung Devices	4 iOS Location Service Disabled
3 Passcode Not Compliant	1 Roaming Devices	1 High Data Usage
1 Quarantined: Pending ActiveSync Approval	0 Device Jailbroken	

[View less](#)

The alerts are red, green or blue. Security alerts can be red or green, depending on if the situation needs attention. Information alerts are blue.

Each administrator can customize their own alerts. They are not specific to administrators or global unless you want them to be.

- Click **+** to add an alert
- Click **↺** to refresh the data
- Click **🕒** to see Alert Center history
- Click **?** for the key to the alert color coding

Alerts are set up using the MaaS360 [Advanced Search](#) feature.

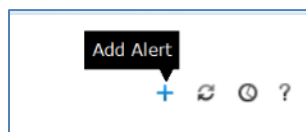
You can click on an alert to see the definition of the alert, and a list of the devices to which the alert applies:

The screenshot shows the 'Advanced Search' window. It includes sections for '1. Search for' (Active, Inactive, All Devices), '2. With Device Type(s)' (Desktops, Laptops, Smartphones, Tablets, Other), '3. Define Search Conditions' (Condition 1: Security & Compliance, Device Passcode Status, Equal To, Not Compliant), and '4. Apply' (AND, OR, Advanced criteria across the above conditions). Below the filters is a 'Search Results' table with columns: Device Name, Username, Device Type, Manufacturer, Model, Operating System, IMEI/MEID, Installed Date, Last Reported, and Mailbox Managed. Two records are shown: 'jski-9800' (BlackBerry 6.0) and 'mdm_rh' (Android 4.1.1). The bottom of the window shows pagination: 'Page 1 of 1', 'Displaying 1 - 2 of 2 records', and buttons for 'CSV' and 'Export'.

Click the [device names](#) to see even more information about them.

Creating an Alert

To create an alert, click the plus sign on the Home page.



The Add Alert screen is displayed.

Add Alert

Name & Description

Enter Name

Description, E.g. "of my devices are jailbroken"

Type

☒ Security
☐ Info

Scope

☒ Me
☐ My Organization

Condition

1. Search for

☒ Active Devices
☐ Inactive Devices
☐ All Devices

and
Last Reported in

Last 7 Days

2. With Device Type(s)

☒ Smartphones
☒ Tablets

3. Define Search Conditions

Condition 1

Select Category

Select Attribute

Select Criteria

Enter Text

Condition 2

Select Category

Select Attribute

Select Criteria

Enter Text

Condition 3

Select Category

Select Attribute

Select Criteria

Enter Text

4. Apply

☒ AND
☐ OR
☐ Advanced criteria across the above conditions

Enter the criteria here. Example: 1 AND (2 OR NOT (3))


Cancel

Save

Name & Description	Enter the name and description of the alert. The description will appear when you mouse over the alert.
Type	Specify if it is a security alert or and information alert. Security alerts will appear red or green, depending on whether the situation requires attention. Info alerts will always appear blue.
Scope	Indicate if the alert should be visible to you alone, or to you and the entire organization.
Condition	Define the alert.
Search for	Specify if the alert should apply to active devices, inactive ones or all devices. Provide the timeframe for the search; i.e., when the device last reported in to the system.
With Device Type(s)	Specify if the alert should apply to smartphones, tablets or both.
Define Search Conditions	Enter the criteria that devices must meet to be included in the alert. You can use Boolean operators if you want.

Define your alert and click **Save**.

Alert Center History

You can see the changes that have been made to the alerts by clicking  at the top of the screen.

28

To view audit history, click on the item below.

Alert Center History

Name	Scope	Status	Update Time	Administrator
(+) Employee Owned		Active		
Employee Owned	My Organization	Added	06/06/2013 11:16 EDT	1037114_bb
(+) Recently Added		Active		
(+) No Passcode		Active		
(+) Data Sharing Apps		Active		
(+) Jailbroken or Rooted		Active		
(+) Out of Compliance		Active		
(+) Roaming		Active		
(+) Email/VPN/Wi-Fi Configuration Failure		Active		
(+) Long Inactivity		Active		

Showing 1 to 9 of 9 Watch List

Click the individual alert to see details about it.

View Alert List Item

Name & Description Employee Owned Personal devices being used within the corporation

Type ☐ Security ☒ Info

Scope ☐ Me ☒ My Organization

Condition

1. Search for ☒ Active Devices ☐ Inactive Devices ☐ All Devices and Last Reported in Current & Last Month

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

3. Define Search Conditions

Condition 1 Custom Attributes Ownership Equal To Employee Owned

4. Apply ☒ AND ☐ OR ☐ Advanced criteria across the above conditions

Enter the criteria here. Example: 1 AND (2 OR NOT (3))

Close

Additional Navigation

There are a few more items at the top right-hand corner of the screen:

Search

Chat Now ? Ben

- **Search:** Begin typing a device name in this field to quickly find a device, user, app or document.
- **Chat Now:** Click the icon to chat with a MaaS360 representative.
- **Help:** Click the question mark to access help for MaaS360.
- **My Profile:** Click your name to see your profile and to change it.


You can see your account number (which you will need if you ever need to contact Customer Support), your username and your email address.

You can change your background image, your time zone and the language that the portal is displayed in. You can also sign out of MaaS360.

Account Id: 1000000

Username: [mdm_bbay](#)

Email Address: bbay@fiberlink.com

Background:  Modern ▼

Time Zone: (GMT) Coordinated Univ... ▼

Language: English ▼

[Change Password](#) [Sign Out](#)

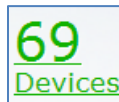
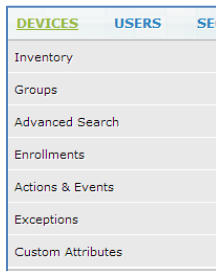
- Click the power icon  to sign out of MaaS360.

Devices

The Devices tab provides access to screens you can use to see your devices. You can also click the Devices link on the Home page.

Inventory

Select Devices > Inventory to see the Device Inventory screen, or click the Devices link on the Home page.



The Device Inventory lists your devices.

Device Name	Username	Device Type	Manufacturer	Model	Operating System	IMEI/MEID	Installed Date	Last Reported	Mailbox Managed	Managed Status
Jonathan's iPad	jdale	Tablet	Apple	iPad 2 (WiFi Only)	iOS 6		04/16/2013 15:15...	05/09/2013 21:46...	ActiveSync Manag...	Enrolled
IPad	ecarfran	Tablet	Apple	iPad 2 (CDMA)	iOS 6	A120131CA702013	04/04/2013 14:29...	05/09/2013 12:23...	ActiveSync Manag...	Enrolled
Tristan's iPad	slukale	Tablet	Apple	iPad 2 (WiFi Only)	iOS 6		08/16/2012 15:28...	04/25/2013 00:23...	ActiveSync Manag...	User Removed Co...
Jim Ski	jski	Tablet	Apple	iPad (3rd Gen, Ve...	iOS 6	201302013622013	10/11/2012 04:00...	04/24/2013 05:11...	ActiveSync Manag...	Enrolled
Jim Szaran's iPad	jszaran	Tablet	Apple	iPad (3rd Gen, Wi...	iOS 5		05/30/2012 15:51...	05/06/2013 15:26...	ActiveSync Manag...	User Removed Co...
Brian's iPad	bstini	Tablet	Apple	iPad (3rd Gen, Ve...	iOS 6	990001297566333	06/14/2012 00:28...	05/10/2013 12:24...	ActiveSync Manag...	Enrolled
IPad	jlaper	Tablet	Apple	iPad (Original)	iOS 5		10/25/2012 22:04...	04/26/2013 14:58...	ActiveSync Manag...	User Removed Co...
mamin-GT-P6210	mamin	Tablet	samsung	GT-P6210	Android 4.0.4 (IM...		08/09/2012 20:35...	04/30/2013 13:09...	ActiveSync Manag...	Enrolled
Joe Pap's iPad	jpap	Tablet	Apple	Apple-iPad3C3; iP...	Max360/2.00.16...		03/26/2013 22:08...	05/07/2013 16:13...	ActiveSync Manag...	Not Enrolled
ecarfi-Kindle Fire	ecarfi	Tablet	Amazon	Kindle Fire	Android 2.3.4 (GI...		10/24/2012 19:41...	05/10/2013 13:30...	No	Enrolled
Cist's iPad	cist	Tablet	Apple	iPad 2 (WiFi Only)	iOS 6		01/17/2013 19:46...	05/10/2013 17:44...	ActiveSync Manag...	Enrolled
Joshua's iPad	jamb	Tablet	Apple	iPad mini (CDMA...	iOS 6	201212392120124	11/29/2012 16:54...	05/09/2013 19:48...	ActiveSync Manag...	Enrolled

You can use the filter to find specific devices:

Device Type	Manufacturer	Model	MEID	Installed Date	Last Reported	Platform Name	Mailbox Managed	Managed Status
Laptop	LENOVO	ThinkPad T60	Mac	06/20/2011 17:35...	05/10/2013 18:59...	Windows	No	Not Enrolled
Laptop	LENOVO	ThinkPad T400	Other	12/22/2011 21:38...	05/10/2013 18:59...	Windows	No	Not Enrolled
Laptop	TOSHIBA	TECRA M11	Palm	04/22/2013 20:44...	05/10/2013 18:54...	Windows	No	Not Enrolled
Laptop	LENOVO	ThinkPad T400	Red Hat Enterprise Linux	05/07/2013 14:22...	05/10/2013 18:53...	Windows	No	Enrolled
Laptop	LENOVO	ThinkPad T520	Solaris	04/09/2013 15:31...	05/10/2013 18:53...	Windows	No	Enrolled
Laptop	LENOVO	ThinkPad T60	Symbian	06/20/2011 17:31...	05/10/2013 18:48...	Windows	No	Not Enrolled
Tablet	Apple	iPad mini (1st Gen...)	Windows Mobile	04/23/2013 20:03...	05/10/2013 18:48...	iOS	ActiveSync Manag...	Enrolled

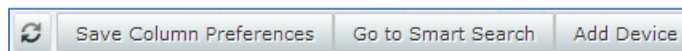
Click the Reset button to remove the filter and see the complete list again.

You can change the columns that are listed by:

1. Click on the down arrow for a column heading **Device Type**
2. Select Columns, and then check the columns you want to include.

Device Type	Manufacturer	Model	Operating System
Laptop	↓ Sort Ascending ↑ Sort Descending Columns	ThinkPad T60	Microsoft Windows...
Laptop		ThinkPad T400	Microsoft Windows...
Laptop	TOSHIBA		Microsoft Windows...
Laptop	LENOVO		Microsoft Windows...
Laptop	LENOVO		Microsoft Windows...
Laptop	LENOVO		Microsoft Windows...
Tablet	Apple		
Smartphone	samsung		
Tablet	asus		
Smartphone	HTC		
Tablet	Apple		
Smartphone	samsung		

At the top right-hand corner of the screen are additional buttons:



- Click to refresh the information.
- Click **Save Column Preferences** to preserve the changes you made to the columns.
- Click **Go to Advanced Search** to enter advanced search criteria.
- Click **Add Device** to send an enrollment request to a device.

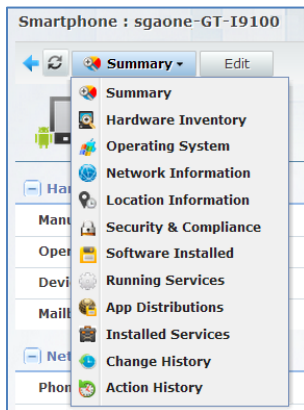
Device Views

The first device view is the **Summary** screen.

Summary • Actions • Edit			
Username	vtrick (vtrick@maas360dz.com)		IMEI/MEID
Last Reported	05/28/2013 16:01 UTC		Managed Status
			Enrolled ActiveSync Managed
[-] Hardware Inventory			
Manufacturer	Apple	Model	iPad mini (1st Gen, WiFi Only)
Operating System	iOS 6.1.3 (20F929)	Free Internal Storage	5.58 GB
Apple Serial Number	F29293902997	Ownership	
Mailbox Activated	Yes	Email Address	vtrick@maas360dz.com
[-] Network Information			
Phone Number	Not Available	ICCID	Not Available
Last Reported Roaming Status	No	Data Roaming	Not Available
Home Carrier	Not Available	Current Carrier	Not Available
[-] Security & Compliance			
Device Jailbroken	No	Device Passcode Status	Compliant
Hardware Encryption	Block-level & File-level	Mailbox Approval State	Approved
Policy	MDM: Default iOS MDM Policy(27) Browser: Default Secure Browser Policy (13)	Settings Failed to Configure	Email Settings
Compliance State	In Compliance	Out-of-Compliance Reasons	-
Rule Set Configured	iOS Compliance Rule		

Click to refresh the information.

Additional screens are available by clicking the pull-down menu. Different screens may be listed depending on the device.

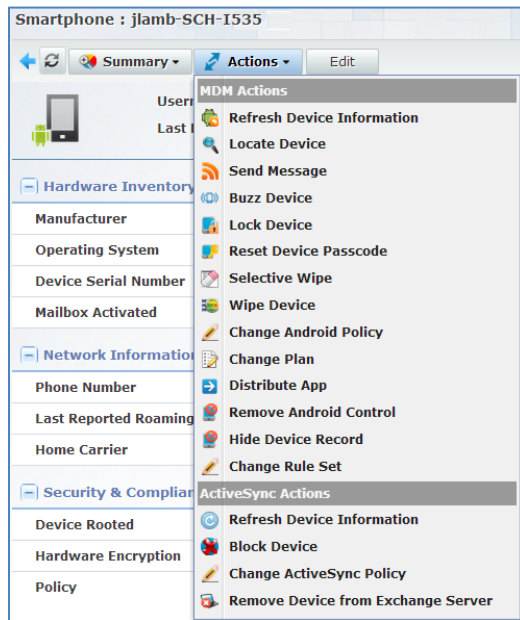


- **Summary:** Basic information about the device, including network and compliance information.
- **Hardware Inventory:** Detailed hardware and storage information about the device. Click **Edit** to update custom attribute information.
- **Operating System:** The OS, OS version, kernel version, API level and more.
- **Network Information:** Detailed information about the cellular network, Wi-Fi network and more.
- **Location Information:** A map showing the last known location of the device.
- **Security & Compliance:** Detailed information about passwords, encryption, the policy, data syncing, and more.
- **Software Installed:** The apps on the device, including the version, size and type.
- **Modules** (appears only if the Cloud Extender is installed for use with the BlackBerry Enterprise Server): The modules on the device, including the version and size.
- **Service Books** (appears only if the Cloud Extender is installed for use with the BlackBerry Enterprise Server): The service books on the device, including the service ID and content ID.
- **Running Services:** The services on the device, including the app ID, memory used, and running time.
- **App Distributions:** The apps that have been distributed to the device by MaaS360; including when they were deployed and which ones have been installed.
- **Installed Services:** Information about the MaaS360 app that is running on the device.
- **Change History:** Information about changes made to the account.
- **Action History:** Lists the actions performed on the device.

Actions

You can perform actions on the device from the Device View.

Note: The Actions that appear depend on a number of factors, including the device type and how it is being managed, and if the Cloud Extender is installed for ActiveSync options, etc. Refer to [Appendix A](#) for details.



- **Refresh Device Information:** Retrieves the most recent data from the mobile device
- **Last Known Location:** Locates the mobile device
- **Send Message:** Sends a message to it
- **Buzz Device:** Sends an alert tone to help locate it in the immediate area
- **Lock Device:** Sends a command that will lock it
- **Reset Device Passcode:** Clears the current passcode
- **Selective Wipe:** Deletes the Wi-Fi profile, Exchange ActiveSync profiles, and Web shortcuts configured on the device via MaaS360 policy. It can also remove apps and documents, if the appropriate options were selected when they were loaded into the App Catalog and Content Library, respectively
- **Wipe Device:** Erases all data on the device and resets it to the original factory settings. For Android 2.2, the Wipe Device action will reset only the phone memory. However, in Android 2.3, it will reset both the phone memory and the SD card
- **Change iOS/Android Policy:** Allows you to change the policy being enforced on the device
- **Change Plan:** Allows you to change the Mobile Expense Management plan
- **Distribute App:** Distribute an app to the device
- **Remove Control:** Allows you to unregister the device from MaaS360, and MaaS360 cannot manage it anymore. The first part of the process is a selective wipe of the device
- **Hide Device Record:** Marks a device as inactive in MaaS360 reporting, but it does not remove control on the device. This should only be performed if the device is permanently offline, destroyed, etc.
- **Change Rule Set:** Allows you to apply or update the rule set assigned to a device
- **Refresh Device Information (EAS):** Refreshes the information shown for the device from Exchange ActiveSync
- **Block Device (EAS):** Prevents the device from accessing your Exchange ActiveSync server

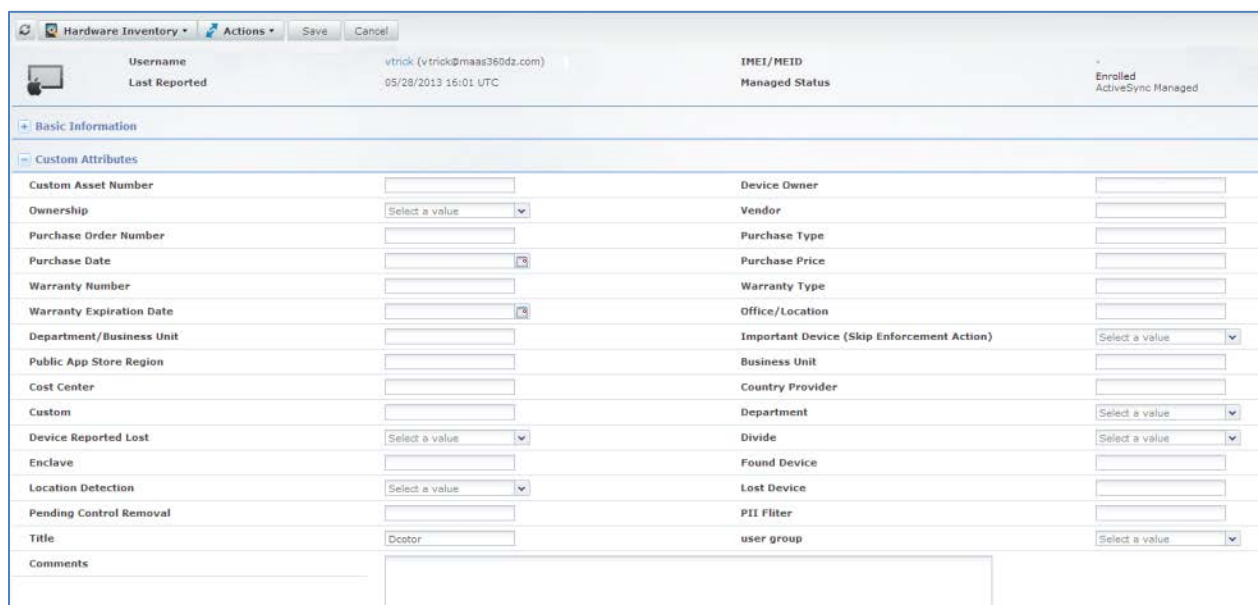
- **Change ActiveSync Policy (EAS):** Changes the policy being enforced on the device. These settings will be specific to Exchange ActiveSync
- **Remove Device from Exchange Server (EAS):** Removes the device records from your Exchange ActiveSync server
- **Reset Device Passcode (BlackBerry):** Clears the current passcode
- **Wipe Device (BlackBerry):** Allows you to wipe data and settings deployed from MaaS360
- **Change BES Policy (BlackBerry):** Changes the policy being enforced on the device
- **Remove Device from BES (BlackBerry):** Removes the device records from your BES server
- **Block Device (Lotus Traveler):** Prevents the device from accessing your Lotus Traveler server
- **Wipe Device (Lotus Traveler):** Allows you to wipe data and settings deployed from MaaS360
- **Remove Device from Traveler (Lotus Traveler):** Removes the device records from your Lotus Traveler server
- **Change Rule Set (Lotus Traveler):** Allows you to apply or update the rule set assigned to a device
- **Hide Device Record (Lotus Traveler):** Marks a device as inactive in MaaS360 reporting, but it does not remove control on the device. This should only be performed if the device is permanently offline, destroyed, etc.

Custom Attributes

Every device has a set of unique identifiers or attributes that are standard across devices. These attributes help in creating device groups that share similar attributes.

In addition to the standard attributes, you can also use custom attributes. For example, if you want to group devices based on their location, you can base your group on the contents of the **Office/Location** field.

You can add them as needed from the **Hardware Inventory** screen. Click **Edit** at the top of the screen. Click **Save** after making your changes.



The screenshot shows the 'Hardware Inventory' screen with a 'Custom Attributes' section. The top bar includes 'Username' (vtrick@maas360dz.com), 'IMEI/MEID', and 'Managed Status'. Below the 'Basic Information' tab, the 'Custom Attributes' section is expanded, displaying a grid of fields for device identification and management. Fields include Custom Asset Number, Ownership, Purchase Order Number, Purchase Date, Warranty Number, Warranty Expiration Date, Department/Business Unit, Public App Store Region, Cost Center, Custom, Device Reported Lost, Enclave, Location Detection, Pending Control Removal, Title, Device Owner, Vendor, Purchase Type, Purchase Price, Warranty Type, Office/Location, Important Device (Skip Enforcement Action), Business Unit, Country Provider, Department, Divide, Found Device, Lost Device, PII Filter, and user group. A 'Comments' field is at the bottom.

Custom Attributes	
Custom Asset Number	Device Owner
Ownership	Vendor
Purchase Order Number	Purchase Type
Purchase Date	Purchase Price
Warranty Number	Warranty Type
Warranty Expiration Date	Office/Location
Department/Business Unit	Important Device (Skip Enforcement Action)
Public App Store Region	Business Unit
Cost Center	Country Provider
Custom	Department
Device Reported Lost	Divide
Enclave	Found Device
Location Detection	Lost Device
Pending Control Removal	PII Filter
Title	user group
Comments	

One custom attribute, **Important Device (Skip Enforcement Action)**, has special properties. If it is set to **Yes**, the device will be exempt from automated enforcement actions.

Important Device (Skip Enforcement Action)	<input type="button" value="v"/>
Business Unit	No
Country Provider	Yes

You can upload a file with custom attributes so you don't have to update each record individually. Select **Devices > Custom Attributes** to see the upload screen.

Custom Attributes

[Manage Custom Attributes](#)
[Transaction Log](#)

Bulk Update File Format Requirements:

1. Must be a text file (.txt, .csv). Files in any other format will not be processed.
2. Maximum file size allowed - 2 MB.
3. First row in the file will be considered the Header row and this should contain titles of all attributes to be updated.
4. Each row in the file after the Header row should contain attributes for only 1 record. Fields must be separated by commas.
5. Each record should have Device ID as the first column and Device Name as the second column.
6. Data for date attributes must be in the format MM/dd/yyyy

Important:

1. It is recommended that you export the results using Smart Search and use this as the starting point for creating the Bulk Update File.
2. In the Header row, you should include only those attributes that need to be updated. In case an attribute is specified and its value is left blank in the records, then the value will be cleared against the record.

Available for*:

Process Request:

Available for	Select the group to be updated, or all users.
Process Request	Enter the filename with the information to be uploaded.












Click **Upload** to upload the file.


Click the **Manage Custom Attributes** button at the top of the screen to see all the existing attributes.

Manage Custom Attributes

[Back To Results](#)

Note: Custom attributes are displayed under "Custom Attributes" category.

Attribute Name	Attribute Type	Created On	Created By	Last Modified On	Last Modified By	
Business Unit	Text	01/14/2011 16:56 UTC	mdm_jd	01/14/2011 16:56 UTC	mdm_jd	
Cost Center	Text	05/04/2011 19:10 UTC	mdm_ka	05/04/2011 19:15 UTC	mdm_ka	
Country Provider	Text	04/28/2011 13:39 UTC	mdm_jball	04/28/2011 13:39 UTC	mdm_jball	
Device Reported Lost	Boolean	04/28/2012 13:57 UTC	mdm_pt	04/28/2012 13:57 UTC	mdm_pt	
Divide	Boolean	11/08/2012 22:06 UTC	mdm_cb	11/08/2012 22:06 UTC	mdm_cb	
Enclave	Text	06/22/2011 19:50 UTC	mdm_bb	06/22/2011 19:50 UTC	mdm_bb	
Found Device	Text	03/12/2012 12:50 UTC	mdm_pt	03/12/2012 12:50 UTC	mdm_pt	
Location Detection	Boolean	06/19/2012 21:06 UTC	mdm_mic	06/19/2012 21:06 UTC	mdm_mic	
Lost Device	Text	03/12/2012 12:49 UTC	mdm_pt	03/12/2012 12:49 UTC	mdm_pt	
PII Filter	Text	04/18/2012 16:16 UTC	mdm_ci	04/18/2012 16:16 UTC	mdm_ci	
Pending Control Removal	Text	01/24/2013 17:42 UTC	mdm_sp	01/24/2013 17:42 UTC	mdm_sp	

Click **Delete icon**  to delete the custom attribute, and click **Back To Results** to return to the previous screen.

You can also click the **Transaction Log** button to see the upload history.

Bulk Update Transaction Log									
No Bulk Updates are being processed.									
Upload Date/Time	Available for	Uploaded By	IP Address	Validation Status	Upload Status	Processing Time ...	Total Records	Errors	
09/10/2012 18:28 UTC	All	mdm_nalsen	188.18.118.18	Success	Success	0	13	0	
09/10/2012 18:25 UTC	All	mdm_nalsen	218.18.184.18	Failed	Failed	0	0	2	

You can see the file by clicking , and you can see any errors by clicking .

Groups

MaaS360 supports two kinds of groups: device groups and user groups. You can see the available groups by selecting **Devices > Groups**, or by selecting **Users > Groups**.

A device group can be a non-editable default device group, an editable public group, a non-editable public group or a private device group. You can search for devices matching specific search criteria and group those devices into a device group. A device group can be one of the following types:

- **Public**—the device group is visible to all administrators, and can be edited and deleted by all administrators. Actions can only be taken on public groups.
- **Private**—the device group is visible only to the administrator who created the device group, and can be edited or deleted by the person who created it.

Mouse over the **More** link associated with the group to view the available actions for it.

Groups		
Type	Name	Apps
	Corporate Owned Devices Devices Edit Delete More...	
	Devices Not Reported in Last 30 Days Devices Edit Delete More...	
	Devices with Passcode Out of Sync Devices Edit Delete More...	
	Roaming Devices Devices Edit Delete More...	
	All Devices Devices Edit Delete More...	
	Smartphones Devices Edit Delete More...	
	Tablets Devices Edit Delete More...	

Different actions are available depending on the group.

- **Create Copy of Group:** Create a duplicate group that you can modify.
- **Hide Devices:** Mark the devices in the group as Inactive in MaaS360 reporting. The **Hide Devices** action does not remove control on the devices.
- **Send Message:** Send a notification alert to all devices in the device group. This action is applicable only for iOS, Android, and Windows Phone mobile devices. The **Send Message** action for BlackBerry devices includes the additional **Message Type** option. Select the **PIN** option to send an SMS message. Otherwise, select the **Email** option to send the alert notification as Email message.
- **Change iOS MDM Policy:** Assign a specific policy to iOS devices in the group.
- **Change Android MDM Policy:** Assign a specific policy to Android devices in the group.
- **Change Plan:** Allows you to edit and assign a specific plan to devices in the group. This action is available only for devices that have enabled the Mobile Expense Manager module.

- **Change Rule Set:** Assign a compliance rule set to all devices in the device group.
- **Distribute App:** Allows you distribute applications to devices in the group.
- **Distribute Document:** Allows you distribute documents to devices in the group.
- **Edit Group:** Allows you to edit the group.
- **Delete Group:** Delete public and private device groups that you have created. It is available for private groups, but it is not available for device groups with automated actions or to public device groups created by MaaS360 or other Administrators.

Advanced Search

The Advanced Search allows you to perform basic and advanced searches for devices. Select **Devices > Advanced Search**.

1. To create a Device Group, specify the required search criteria, click Search and then click "Create Device Group".
2. To customize the columns in Search Results, click on any column and select the attributes that you want to display.
3. To save the columns for future use in Search Results, click "Save Column Preferences".

Advanced Search

1. Search for: ☐ Active Devices ☐ Inactive Devices ☐ All Devices and Last Reported in:

2. With Device Type(s): ☒ Desktops ☒ Laptops ☒ Smartphones ☒ Tablets ☒ Other

3. Define Search Conditions

Condition 1:

Condition 2:

Condition 3:

4. Apply: ☒ AND ☐ OR ☐ Advanced criteria across the above conditions

Search for	Specify if you want to search for active devices, inactive devices or all devices.
Last Reported	Specify the time period in which the devices last contacted MaaS360.
With Device Type(s)	The options listed here will vary depending on what you have purchased. Specify the device types you want to include in the search.
Define Search Conditions	Specify the category, attribute and value being searched for. For example, to see all the devices that can support remote wipe, enter the following: <div> Condition 1 <input type="text" value="Security & Compliance"/> <input type="text" value="Remote Wipe Support"/> <input type="text" value="Equal To"/> <input type="text" value="Yes"/> <input type="button" value="X"/> <input type="button" value="+"/> </div>
Apply	Specify any Boolean operators that should be used to handle multiple search conditions. Enter the additional criteria in the text box.

Click to add a row, and click to remove one.

Click **Search** to view results matching the selected criteria. The results will appear in the lower half of the screen.

Your searches can be used for different purposes:

- The alerts on the **Home** page are based on these searches
- You can use these searches to define groups
- You can customize the columns that appear in the results section

Defining a Group

To use a search to define a group, perform the following steps:

1. Click the Create Device Group button.

The screenshot shows the 'Advanced Search' window. It includes sections for '1. Search for' (Active/Inactive/All Devices), '2. With Device Type(s)' (Desktops, Laptops, Smartphones, Tablets, Other), '3. Define Search Conditions' (Condition 1: Security & Compliance, Device Passcode Status, Equal To, Not Compliant), and '4. Apply' (AND, OR, Advanced criteria). Below these is a 'Search Results' table with columns: Device Name, Username, Device Type, Manufacturer, Model, Operating System, IMEI/MEID, Installed Date, Last Reported, and Mailbox Managed. Two rows of device data are visible. The 'Create Device Group' button is highlighted in the top right of the results area.


2. Enter details about the device group in the pop-up box. Enter the name of the group, a description, and specify if it is public or private. When you are finished, click Save.

The 'Device Group Details' pop-up box contains the following information:

- Instructions:
 1. Public groups are accessible to other administrators in your organization.
 2. Automated policy assignment and App distributions can also be scheduled only for Public Groups.
- Form fields:
 - Group Name:
 - Description:
 - Group Type: ☒ Public ☐ Private
- Buttons:

The search criteria will be saved and any actions that are performed will be done for all the devices in the group at that time.

Customizing Columns

You can also change the columns that are displayed. Click the  icon on a column heading, and then select **Columns**. Check all the columns you want to see.

The screenshot shows the 'Advanced Search' interface. On the left, there are filters for 'Active Devices' (All Devices, Smartphones, Tablets), 'Compliance' (Device), and a search criteria box with the example '1 AND (2 OR NOT (3))'. The main area is a list of columns with checkboxes. The 'Columns' dropdown menu is open, showing options: 'Sort Ascending', 'Sort Descending', and 'Columns'. The 'Columns' option is selected, and a list of columns is displayed below it.

Column Name	Selected
Device Name	<input checked="" type="checkbox"/>
Device Owner	<input type="checkbox"/>
Username	<input checked="" type="checkbox"/>
Email Address	<input type="checkbox"/>
Device Type	<input checked="" type="checkbox"/>
Manufacturer	<input checked="" type="checkbox"/>
Model	<input checked="" type="checkbox"/>
Operating System	<input checked="" type="checkbox"/>
Service Pack	<input type="checkbox"/>
IMEI/MEID	<input checked="" type="checkbox"/>
Installed Date	<input checked="" type="checkbox"/>
Last Reported	<input checked="" type="checkbox"/>
MDM Device ID	<input type="checkbox"/>
Mailbox Managed	<input checked="" type="checkbox"/>
Active Module Name	<input type="checkbox"/>
Active Module Version	<input type="checkbox"/>
ActiveSync Agent	<input type="checkbox"/>
Advanced Device Management SDKs Enabled	<input type="checkbox"/>
Agent Core Version	<input type="checkbox"/>
Allow installation of Non-Market Apps	<input type="checkbox"/>
Allow Mock Locations	<input type="checkbox"/>
API Level	<input type="checkbox"/>
APNS Service Status	<input type="checkbox"/>
App Compliance State	<input type="checkbox"/>
Application Data (MB)	<input type="checkbox"/>
Application Name	<input type="checkbox"/>
Approval Comments	<input type="checkbox"/>
Auto Backup Configured	<input type="checkbox"/>
Auto-Backup Exclusions	<input type="checkbox"/>
Auto-Backup Frequency	<input type="checkbox"/>
Auto-Sync Enabled	<input type="checkbox"/>
Automatic Data Backup to Google Servers Enabled	<input type="checkbox"/>
Automatic Restore from Data Backup on Application Reinstall	<input type="checkbox"/>
Available Memory(MB)	<input type="checkbox"/>

You can save your selections by clicking Save Column Preferences.

The screenshot shows the 'Advanced Search' interface with search results. The 'Save Column Preferences' button is highlighted in the top right corner of the search results section. The search results table is displayed below.

Device Name	Username	Device Type	Manufacturer	Model	Operating System	IMEI/MEID	Installed Date	Last Reported	Mailbox Managed
jsski-9800	jsski	Smartphone	RIM	Torch (9800)	BlackBerry 6.0	133300-30 13330...	02/12/2012 15:55...	05/10/2013 17:17...	BlackBerry Manag...
mdm_rhi	mdm_rhi	Smartphone	samsung	SCH-I605	Android 4.1.1 (JR...	99933219332933	03/26/2013 18:11...	04/12/2013 18:23...	No

Enrollment Requests

You can see a list of the enrollment requests that were sent by selecting Devices > Enrollment Requests.

Enrollments (Add Device Requests)							Add Device Bulk Add Apple Configurator Streamlined Enrollment
	Status	Device...	Username	Domain	Email	Requested By	Requested Date
<input type="checkbox"/>	New Delete Renew		bcarter	fiberlink	bcarter@fiberlink.com	bcarter@fiberlink.com	05/06/2014 18:40 UTC
<input type="checkbox"/>	New Delete Renew		jvanduff	fiberlink	jvanduff@fiberlink.com	jvanduff@fiberlink.com	05/06/2014 15:16 UTC
<input type="checkbox"/>	New Delete Renew		vthotieam	fiberlink	vthotieam@fiberlink.com	vthotieam@fiberlink.com	05/06/2014 07:44 UTC
<input type="checkbox"/>	New Delete Renew		vthotieam	fiberlink	vthotieam@fiberlink.com	vthotieam@fiberlink.com	05/06/2014 04:41 UTC
<input type="checkbox"/>	New Delete Renew		cbrown	maas360dz01	cbrown@maas360dz.com	cbrown@fiberlink.com	05/05/2014 23:33 UTC
<input type="checkbox"/>	New Delete Renew		cbrown	maas360dz01	cbrown@maas360dz.com	cbrown@fiberlink.com	05/05/2014 04:47 UTC
<input type="checkbox"/>	New Delete Renew		vthotieam	fiberlink	vthotieam@fiberlink.com	vthotieam@fiberlink.com	05/05/2014 04:30 UTC
<input type="checkbox"/>	Completed	jrayment-X7 1058	jrayment	maas360dz01	jrayment@maas360dz.com	jrayment	05/05/2014 03:19 UTC

Status	Status of the request: <ul style="list-style-type: none"> • New—the request was just sent • Failed—an error prevented the request from being successful • Complete—the device was successfully enrolled • Pending—although the request was sent successfully, the device's owner has not yet enrolled the device
Device Name	The registered device name.
Platform	Device's platform.
Request Date	Date the enrollment request was created.
Domain	Domain provided in the request.
Available for	Group associated with the request.
Email Address	Email address to which the request was sent.
Policy Set	Policy that went into effect for the device when it was first enrolled.
Registration Date	When the device was successfully enrolled.
Error Information	Specifies why the enrollment request failed.
Requested By	Administrator who created the request.
Comments	Any comments about the request. They can only be seen by the administrator.
Enrollment URL	URL included in the request email. The recipient would have accessed the URL to enroll the device.
Passcode	Passcode that was included in the request email. The user would have needed to enter it to enroll the device.

At the top of the screen are three buttons:



1. **Send Enrollment Request:** sends an individual enrollment request

2. **Bulk Enroll:** allows you to upload a .csv or .txt file with user information so you can send multiple enrollment requests simultaneously
3. **Bulk Deployment:** allows you to enroll multiple devices via the Apple Configurator tool

Action History

MaaS360 can show you all the actions that have been performed on your devices. Click **Devices > Actions & Events** to see the list.

Action History									
Select Attribute	Select Criteria		Search	Clear					
Device Name	Platform	MDM Device ID	Action Date	Action	Action By	IP Address	Status	Comments	Error Description
iPad 5	(iOS)	App193193193	05/30/2013 19:17 UTC	Last Known Location	slart_mdm2	38.123.123.123	Completed	Viewed Last known loc...	
IP-A0330DF	(Cloud Extender)	725pm	05/30/2013 19:15 UTC	User Authentication	jbert	123.76.123.249	Completed		
IP-A0330DF	(Cloud Extender)	725pm	05/30/2013 18:37 UTC	User Authentication	jhen	123.76.123.249	Completed	Provided user credentials...	
Brian's iPhone	(iOS)	App193193193	05/30/2013 18:33 UTC	Last Known Location	mdm_huy	123.76.123.68	Completed	Viewed Last known loc...	
Jhan-Nexus 7	(Android)	Android193193193	05/30/2013 18:31 UTC	Remove MDM Control	mdm_jhoig	123.76.123.68	Completed		

Device Name	Name of the device.
Platform	Device the platform is on.
MDM Device ID	Device's ID.
Action Date	Date the action was taken.
Action	Action that was taken on the device.
Action By	Username of the administrator that performed the action.
IP Address	IP address of the device.
Status	Status of the action.
Comments	Any comments which were included with the action.
Error Description	Describes an error that was found while performing the action.

Exceptions (Exchange ActiveSync and Lotus Traveler Only)

Devices report into both the Exchange ActiveSync/Lotus Traveler servers and into MaaS360. To maintain data integrity, MaaS360 tries to match the mail server record with the one it receives.

iOS devices send a device serial number to the servers and to MaaS360, so there are rarely any difficulties matching these records. For other device types MaaS360 uses device-level attributes and built-in logic to match device pairs.

The mail servers and MaaS360 have the following information from the devices:

1. Email address
2. Device manufacturer


3. Device types (smartphone, tablet)

MaaS360 has a background process that compares each of them, in order.

In most cases, that is enough information to match the records.

If MaaS360 cannot make an informed decision about which devices belong together, the unmatched records will appear on the Exceptions report so an administrator can merge the records manually.

Pending Merge Devices Report									
<p>This report lists all Enrolled Android and Windows Phone devices that have been skipped by the Automated Merge Process and needs to be manually merged with a corresponding device reported from your mail server.</p> <p>Logic for Automated Merge Process: For the same email address, if there is an Enrolled device record and a Exchange (or Traveler) reported device record, both with Android or Windows Phone as Device Platform, then these records will be automatically merged.</p> <p>Automated Merge Process last executed on: -</p> <p>Scenarios where automated merge is skipped:</p> <ul style="list-style-type: none"> For the same email address, if there are multiple Enrolled device record and Exchange (or Traveler) reported device record that are yet to be merged. If device manufacturer of Enrolled device record is different from that of the Exchange (or Traveler) reported device record. If email address used in device enrollment is different from user's actual email address as reported from Exchange (or Traveler). <p>Notes: This report will be empty, in case you have not opted for Active Sync Manager or Lotus Traveler Manager service.</p>									
<div> <div>Device (MDM)</div> <div>Device (Mailbox)</div> <div>Search</div> <div>Clear</div> <div>View Merged Devices</div> </div>									
Device (MDM)	Platform	Device ID (MDM)	Email Address (MDM)	Username (MDM)	Device (Mailbox)	Installed Date (Mailbox)	Installed Date (MDM)	Last Reported (Mailbox)	Actions
						03/06/2013 15:12 EST	02/15/2012 10:31 EST	06/06/2013 15:48 EDT	Actions
						02/21/2013 17:47 EST	01/23/2013 19:40 EST	05/21/2013 14:25 EDT	Actions
						02/21/2013 17:47 EST	01/07/2013 14:48 EST	05/21/2013 14:25 EDT	Actions
<div> <div>Page 1 of 1</div> <div>Displaying 1 - 3 of 3 records</div> </div>									

The matching process runs approximately every 2 minutes, and the most recent execution time is shown on the report. Click  to refresh the data.

Click **View Merged Devices** to see a list of the devices that MaaS360 has merged automatically.

Merged Devices Report

Device (MDM)

Device (Mailbox)

Search

Clear

Device (MDM)	Platform	Device ID (MDM)	Email Address (MDM)	Username (MDM)	Last Reported...	Managed Status	Device (Mailbox)	Merged Date	Merged By	Actions
ci-GT-N7000		android20732073073	ci@maas360dz.com	ci	05/03/2013 18:...	Enrolled	ci-SCH-1535	05/29/2013 02:...	Automated Maa...	Separate

Page 1 of 1

Displaying 1 - 1 of 1 records

Click the **Separate** link to undo the merge process. If you separate a record, it will never be eligible for merging again.

Users

MaaS360 gives you a quick, easy way to see all your users and device groups. There are two choices on the Users tab:



Directory

Select **Directory** from the Users tab to see the **User Directory**.



You can also click the **Users** link on the Home page.

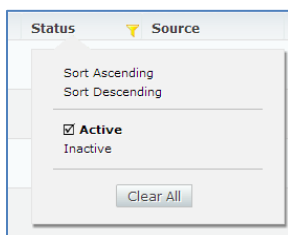


The **User Directory** shows your users.

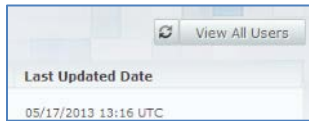
Username	Full Name	Domain	Email	Status	Source	Last Updated Date
aarontest View	Aaron Test	maas360dz01.local	aarontest@maas360dz.com	Active	User Directory	05/12/2013 20:31 UTC
abide View		maas360dz	abide@maas360dz.com	Active	Local Directory	03/05/2011 01:48 UTC
alark View		maas360dz01		Active	Local Directory	
administrator View	Administrator	maas360dz01.local		Active	User Directory	05/12/2013 20:31 UTC
aduko View		maas360dz01	aduko@fiberlink.com	Active	Local Directory	06/30/2012 14:40 UTC
aestor View	Alan	maas360dz01.local	aestor@maas360dz.com	Active	User Directory	01/20/2013 21:39 UTC
akumin View	Aaron Kumin	maas360dz01.local	AaronKumin@maas360dz.com	Active	User Directory	05/12/2013 20:31 UTC
alexa View		maas360dz01		Active	Local Directory	01/12/2012 21:38 UTC
apem View		maas360dz01		Active	Local Directory	01/12/2012 21:40 UTC
appreview View	App Review	maas360dz01.local	appreview@maas360dz.com	Active	User Directory	05/12/2013 20:31 UTC

Displaying 1 - 10 of 204 Records

You can filter the data by status (whether the person is an active or inactive user).



Click **Hide users with no Devices** to filter out users who have no devices managed by MaaS360, and **View All Users** to see the complete list again.



You can get details about a particular user by clicking the **View** link.



You can see information about the person, the groups he or she is in, and a list of the devices that they have.



Click on a device's name to see the [Device View](#).

Groups

Device groups allow you to deploy policies, apps or documents to similar categories of users.

There are several default groups:

1. **System:** groups provided by MaaS360
2. **Public:** can be used by all administrators
3. **Private:** can only be used by the administrator who created it

Note: Automated policy assignments and app distributions can only be scheduled for public groups.

Select **Groups** from the **Users** tab to see all your groups.



Groups					Show all automated actions Add User Directory Group Add Device Group
Group Type	Group Name	Applied Actions	Description	Modified On	
Public	test group	NA		02/14/2013 17:50 UTC	Actions
Public	Vans Devices	Yes		11/15/2012 20:12 UTC	Actions
Public	Tablets	NA	All active tablets that have reported in to MaaS360 in the last 7 days.	12/08/2012 14:30 UTC	Actions
Private	iOS Devices-Employee Owned	NA		02/28/2013 19:41 UTC	Actions
Private	Test Employee iOS Devices	NA		02/22/2013 16:14 UTC	Actions
Public	AD Admin Group	NA		08/28/2012 16:13 UTC	Actions
Public	All Devices	NA	This Device Group includes all active registered devices.	08/15/2011 18:52 UTC	Actions
System	BlackBerry Devices	NA	All active BlackBerry devices that have reported in the last 7 days.	02/19/2011 01:27 UTC	Actions

Note: User Groups are also displayed on this screen.

You can see any automatic actions for a device group by clicking the plus sign in the **Applied Actions** column.

Click the **Show all automated actions** to expand the automated actions.

Yes

Actions scheduled for automatic execution -
Apply iOS Policy: Default iOS - Passcode Required [Edit](#) | [Remove](#)
Apply Android Policy: Default Android Policy [Edit](#) | [Remove](#)

Click **Hide all automated actions** to collapse them. You can click **Show all automated actions** to display them again.

You can perform an action on a device group by selecting it from the pull-down menu:

11/01/2012 17:41 UTC
[Actions](#)

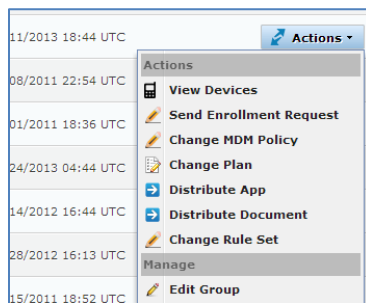
Actions
 Hide Devices
 Send Message
 Change iOS MDM Policy
 Change Android MDM Policy
 Change Plan
 Distribute Package
 Distribute App
 Distribute Document
 Change Rule Set
 Configure Patch Settings
Manage
 Refresh Group
 Edit Group
 Create Copy of Group

Note: The items you see on the pull-down menu will vary depending on the services that are enabled.

- **Hide Devices:** Mark the group as inactive in MaaS360 reporting, but does not remove MaaS360's control of the devices
- **Send Message:** Sends a text message to the devices
- **Change iOS MDM Policy:** Changes the policy being enforced on all the iOS devices in the group
- **Change Android MDM Policy:** Changes the policy being enforced on all the Android devices in the group
- **Change Plan:** This option is not visible unless you are using the Mobile Expense Management module. It changes the plan in effect for the devices in the group

- **Distribute Package:** This option is only visible if you are using the desktop/laptop module of MaaS360. It distributes a Windows package to the devices in the group
- **Distribute App:** Deploy an app that has already been uploaded to MaaS360 to all the devices in the group
- **Distribute Document:** Distribute a document that has already been uploaded to MaaS360 to all the devices in the group
- **Change Rule Set:** Change the rule set that is being enforced for the device group
- **Configure Patch Settings:** This option is only visible if you are using the desktop/laptop module of MaaS360. It lets you customize the settings for patches you push to the devices in the group
- **Refresh Group:** Update the list of devices in the group
- **Edit Group:** Change the criteria that defines the members of the group
- **Create Copy of the Group:** Copy the group, usually so it can be the basis of a new group

The available actions are slightly different for user groups.



Note: The items that appear on the menu will vary depending on the services that are enabled.

- **View Devices:** Show all the devices that belong to the users in the user group
- **Send Enrollment Request:** Send an enrollment request to the users in the group
- **Change MDM Policy:** Change the policy for the users' devices. You will be prompted to specify either iOS or Android
- **Change Plan:** This option is not visible unless you are using the Mobile Expense Management module. It changes the plan in effect for the users in the group
- **Distribute App:** Deploy an app to all the users in the group
- **Distribute Document:** Send a document to all the users that belong to the group
- **Change Rule Set:** Change the compliance rule set that is in force for the group
- **Edit Group:** Change the criteria that defines the user group

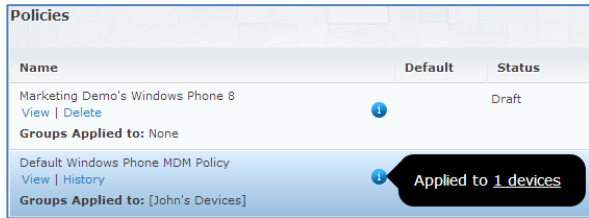
Security

MaaS360 gives you the ability to customize the security you use for your devices.

Policies

Select **Security > Policies** to access the **Policies** screen.

Policies									
Name	Default	Status	Precedence	Available for	Type	Version	Last Modified	Last Published	
Default Windows Phone MDM Policy View History			Published	2	All	3	07/23/2013 14:28 UTC	07/23/2013 14:28 UTC	
Groups Applied to: [John's Devices]									
Default Secure Browser Policy View History			Published	All		19	10/18/2013 13:45 UTC	10/18/2013 13:45 UTC	
Default OS X MDM Policy View History			Published	1	All	1	05/07/2013 14:22 UTC	05/07/2013 14:22 UTC	
Groups Applied to: None									
Default iOS MDM Policy View History			Published	1	All	33	11/05/2013 13:49 UTC	11/05/2013 13:49 UTC	
Groups Applied to: [Enterprise Admins]									
Default View History		Needs Publish		All		67	03/08/2013 20:11 UTC	09/13/2011 15:18 UTC	
BlackBerry Default View History			Published	All		2	02/20/2013 04:24 UTC	02/20/2013 04:24 UTC	
Default Android Policy View History			Published	1	All	5	04/12/2013 16:27 UTC	04/12/2013 16:27 UTC	
Groups Applied to: [VP, MULT_MDM_CORP]									

Name	Name of the policy
(Action Quick Links)	<p>Links you can use to perform common actions directly from the screen:</p> <ul style="list-style-type: none"> • View: see the policy • Set as Default: make this policy the default policy for the device type • Audit History: show the changes that have been made to the policy • Delete: delete the policy
Information icon	<p>Mouse over the icon to see the number of devices that have the policy.</p>  <p>Click the link to see a list of them.</p>
Default	If checked, this is the default policy for the specified device type. It will automatically be assigned to devices if no other policy is specified.
Status	Status of the policy. Only published policies can be given to users.
Precedence	If a device is included in multiple device or user groups, it could be subject to more than one policy. The precedence indicates which one will be applied, with the lower number having the higher priority.
Available For	Specifies the device or user group that the policy can be assigned to. <i>Note: This requires the Departmentalization feature, which is not enabled by</i>

	<i>default. Contact your account representative for details.</i>
Type	Specifies which platform the policy is designed for. Different platforms have different policy options.
Version	How many times the policy has been published.
Last Modified	The last time the policy was changed.
Last Published	<p>The last time the policy was successfully published.</p> <p>A policy will not be published successfully if there are errors. For example, if you indicate that you want the policy to require a passcode but do not specify any requirements for the passcode (length, complexity, etc.) you will receive an error and the policy will not be published.</p>

Click **View** to see the policy.



Click the **Edit** button at the top of the screen to change it.

MaaS360 provides many choices so you can make your policy as relaxed or restrictive as you need. These settings may differ, depending on the platform (iOS, Android, Windows Phone, etc.). The settings are listed in [Appendix A](#).

Click the tabs on the left side to see the different settings.

When you are finished making changes, click **Save and Publish**. Your policy cannot be assigned to any devices until it has been published.

Precedence

Note: This feature is not enabled by default. Contact your account representative for details.

In MaaS360, policies are dynamically assigned to different device groups, so the policy in force on a device can change as the circumstances change. For example, you can have a device group for a specific operating system version and assign a policy to it. When a user upgrades a device, the device would then become part of the new group and would get the associated policy automatically.

As a result, it is possible for a device to be automatically assigned to multiple groups which have conflicting policies.

Precedence allows you to prioritize policies so MaaS360 will apply the appropriate one if more than one is applicable.

Click the **Precedence** button to view the **Change Precedence** dialog box, which lists the available iOS and Android MDM policies.

Policies									
Name	Default	Status	Precedence	Available For	# of Devices	Platform	Publish V...	Last Modified	Last Successful Pub
JC SPS Test Policy View Set as Default Audit History Delete		Needs Pu...	4	All	1		5	05/20/2013 20:22 UTC	05/20/2013 18:44 UTC
Groups Applied to: None									
IL - Policy View Set as Default Audit History Delete		Published		All	2		4	06/02/2013 18:48 UTC	06/02/2013 18:48 UTC
Groups Applied to: None									
RS-Android Test View Set as Default Audit History Delete		Published	3	All	2		3	05/31/2013 20:04 UTC	05/31/2013 20:04 UTC
Groups Applied to: None									

You can change the policy precedence by dragging a policy box to the desired precedence level. Click **Save** to save changes.

Precedence

Note: Drag and drop the policies to change the precedence. Click Save to continue.
Click here to learn more about why you need to decide the precedence for your policies.

iOS MDM Policies

- Default iOS MDM Policy
- Default iOS - Passcode Required
- JN iOS Policy - Do Not Delete
- UK Demo iOS Policy - with Asavie VPN
- Block Safari and 17+

Android MDM Policies

- Default Android Policy
- ecar
- Marketing Demo's Android
- Pamid android
- kindle

Policy Files

Click the **Policy Files** button to see uploaded mobile device policy files.

Policies

Add Policy Precedence **Policy Files** Show All Search

Name	Default	Status	Precedence	Available For	# of Devices	Platform	Publish V...	Last Modified	Last Successful Pub
JC SPS Test Policy View Set as Default Audit History Delete		Needs Pu...	4	All	1		5	05/20/2013 20:22 UTC	05/20/2013 18:44 UTC
Groups Applied to: None									
JL - Policy View Set as Default Audit History Delete		Published		All	2		4	06/02/2013 18:48 UTC	06/02/2013 18:48 UTC
Groups Applied to: None									
RS-Android Test View Set as Default Audit History Delete		Published	3	All	2		3	05/31/2013 20:04 UTC	05/31/2013 20:04 UTC
Groups Applied to: None									

You can upload certificates, images and file containing mobile device settings.

Policy Files

Name	Content Type	Content Sub Type	Uploaded By	Uploaded On	Actions
MaaS360 App Store Install	Webclip Image (for iOS)	PNG	mdm_cis	06/28/2011 19:59 UTC	✗
Fiberlink	Webclip Image (for iOS)	PNG	mdm_cis	05/10/2011 19:06 UTC	✗
YouTube Demo icon	Webclip Image (for iOS)	PNG	mdm_nski	06/30/2011 00:21 UTC	✗
TestImage	Webclip Image (for iOS)	PNG	nbard@fiberlink.com	06/15/2011 15:27 UTC	✗
PF Chang's	Webclip Image (for iOS)	PNG	mdm_ppano	07/10/2012 15:02 UTC	✗
airheads-ipc-updated	Device Settings (for iOS)	mobileconfig	mdm_dalle	03/09/2013 22:21 UTC	✗
DZ Cert	Certificate (for iOS and OS X)	PKCS1	mdm_jbert	03/22/2013 04:45 UTC	✗
BlockGraphic	HTML (For Secure Browser)	HTML	mdm_trick	01/28/2013 22:50 UTC	✗
airheadsdemo-trust	Certificate (for iOS and OS X)	PKCS1	mdm_cile	03/08/2013 20:29 UTC	✗
airheadsdemo-notrust	Certificate (for iOS and OS X)	PKCS1	mdm_sdall	03/08/2013 20:30 UTC	✗

Jump [Page 1 of 2] Displaying records 1 to 10 [Total records 12] Upload Content

Click the **Upload Content** button to view the **Upload Policy Files** pop-up box.

Upload Policy Files

Content Name(max. 100 chars.):*

Type:*

Content:*

Supported: Type - PKCS1 Certificate files (*.crt, *.cer)

Upload Content

- Certificate
- iOS and OS X
- Certificate
- Webclip Image
- Device Settings
- Android
- Certificate
- Web Shortcut Image
- Wallpaper Image
- Secure Browser
- HTML

Enter relevant name in the **Content Name** field. Select the desired **Type**. The available content types that you can upload are **Certificates**, **Images** and **Device Settings**.

- **Certificates:** the Certificate type allows you to authenticate and register your mobile devices in the MaaS360 system.
- **Images:** the Image type allows you to associate an image or a picture file with your document.
- **Device Settings:** selecting the Device Settings option allows you to upload a policy file that contains the VPN, EAS and Wi-Fi policy parameters that you wish to apply to all devices that are registered using the certificate.

Click **Browse** to select the content file from your local drive, and then click **Upload Content**. The **Upload Status** box displays. Click OK, and the file will appear on the list of policy files.

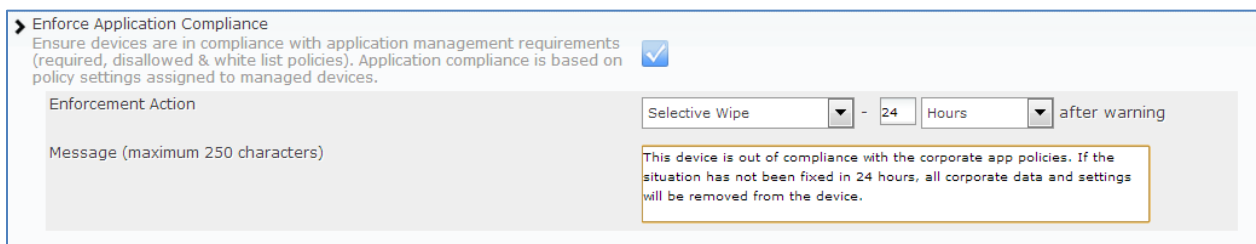
Click the delete icon  under the **Actions** column if you wish to remove an uploaded policy file.

Compliance Rules

MaaS360 allows you to apply compliance rules on mobile devices. Compliance Rule sets are conditions that are checked on devices on real-time basis. If a device is not in compliance with the defined rule sets or conditions, then appropriate enforcement actions will be taken on the device.

Most mobile device platforms allow users to ignore and override passcode policies and application restrictions. Rules such as the **Enforce MaaS360 Control** are useful, especially to track users who accidentally or willfully try to remove their organization's device management and control capabilities. It's a good idea to use Compliance Rules to enforce actions, even if you already publish policies to your devices.

Compliance rules allow you to take automated actions when a device is out of compliance. For example, the following rule will be invoked when a user installs a blacklisted app on a device:



Only devices marked as **Important** on the **View All Devices** screen will be exempt from the automated actions that will occur when a device is out of compliance. It is a [custom attribute](#).

You can choose what action to take, a timeframe for the action (where applicable), and you can send a custom message to the user.

Select **Security > Compliance Rules** to access the **Compliance Rules** screen.



The existing rules will be displayed.

Compliance Rules								
<div> Add Rule Precedence Disable All Show All Search </div>								
<p>1. Create as many Rule Sets as needed to serve the needs of different groups.</p> <p>2. Start testing any new Rule Set by applying it only to a Group.</p> <p>3. You can explicitly apply a Rule Set to a device (from device view) or a group (use actions against each Rule Set on this table or from the manage groups workflow).</p> <p>4. You can mark any of the Rule Set as a Default. This would ensure that any devices without an explicit Rule Set assignment would be evaluated based on this Rule Set.</p> <p>5. For viewing the specific Rule Set enabled for a device, look for the attribute "Rule Set" under Security & Compliance Section in Device View.</p> <p>6. Use the "Disable All Rules" button to remove Rule Set assignments and active enforcement actions from all managed devices.</p>								
Rule Set Name	Available for	Default	Status	Precedence	# of Devices	Last Updated By	Last Updated On	
JN Rule Set Edit Assign Make Default Audit Delete Groups Applied to: test	All		Active	0	2	mdm_jsen	05/09/2013 13:19 UTC	
Cecht iOS Edit Assign Make Default Audit Delete Groups Applied to: None	All		Active	0	0	mdm_cecht	06/23/2012 12:27 UTC	
Base Rule Set 3 Edit Assign Clear Default Audit Delete Groups Applied to: None	All	<input checked="" type="checkbox"/>	Active	0	2	whitehat_test	04/16/2012 15:27 UTC	
Jailbreak Notify Edit Assign Make Default Audit Delete Groups Applied to: None	All		Active	0	0	mdm_jano	03/02/2012 18:06 UTC	

Rule Set Name	Name of the compliance rule. It must be unique.
(Actions)	Click the link under the name to perform an action: <ul style="list-style-type: none"> Edit: review the rule set and change it Assign: apply it to group Make Default/Clear Default: make this rule set the default Audit: view the audit history of the rule set Delete: delete the rule set
Available for	Specifies which groups the rules set can be applied to.
Default	If checked, this rule set is the default.
Status	Specifies if the rule set is active or inactive. Click the Show All button at the top of the screen to include inactive rule sets in the list, and click Hide Inactive to only display active ones.
Precedence	You can have devices with multiple rule sets assigned to them, depending on how your groups are set up. In those cases, the rule set with the lower precedence is the one that will be enforced.
# of Devices	Specifies how many devices have been assigned this rule set. Click on the number to see a list of those devices.
Last Updated By	Username of the person who last updated the rule set.
Last Updated On	Date of the last update.

Compliance rules allow you to take automated actions under certain circumstances. For more information, refer to the [Mobile Device Management Policies Best Practices Guide](#).

To create a new one, click **Add Rule** at the top of the screen. Specify the group it is available for, the rule set's name and an existing rule to use as a starting point.

Click **Continue**. The **Basic Settings** tab appears.

Specify the platforms that the rule set will apply to, and enter the email addresses that should receive alerts for the rule set.

On the **Enforcement Rules** tab, you can have MaaS360 enforce:

- Enrollment in MDM
- Specific operating system versions
- Support for remote wipe
- Support for block- and file-level encryption, or no encryption
- Compliance with corporate app policies for blacklisted, whitelisted and required apps
- Restrictions for jailbroken and rooted devices

Note: Wipe allows you to wipe out all data on the mobile device and reset it to the original factory settings. In Android 2.2, the Wipe action will reset only the phone memory. However, in Android 2.3, the Wipe action will reset both the phone memory and the SD card.

Note: The Block and Wipe enforcement actions are only available with Cloud Extender integration. For details, refer to the [Device Actions section in Appendix A](#).

Make your changes, and then click the next tab.

Geo-Fencing Rules can be set up after you've created approved locations. You can change the policy in force on the device based on its location, or specify actions that should take place if the device is removed from one of the approved locations.

Use the **Monitoring Rules** to monitor SIM changes, when a user's device is roaming, and any operating system version changes.

Make your changes and click the next tab.

Note: *Expense Management is available for an additional cost. Please contact your account representative for more information.*

Expense Monitoring Rules apply to mobile data usage. You can monitor both roaming and in-network data usage, and take action based on the usage thresholds.

When you are finished making changes, click **Save**.

Compliance Log

The **Compliance Status Overview** report displays a list of all devices that are not in compliance with the configured compliance rules.

Device Name	Username	Active Rule Name	Rule Set Name	Action Configured	Action Status	Time of Execution
Val's iPad	vick	Enforce Enrollment	iOS Val Compliance Rule	Alert User and Adminis...	NA	05/30/2013 17:34 UTC
brecht-GT-N7000	brecht	Restrict Jailbroken (iOS) and Ro...	Base Rule Set 3	Alert User and Adminis...	NA	03/12/2013 04:14 UTC
ehitt-PG86100	ehitt	Restrict Jailbroken (iOS) and Ro...	Base Rule Set 3	Alert User and Adminis...	NA	02/28/2013 23:01 UTC
jd's iPhone	jd	Monitor In-Network Mobile Dat...	Base Rule Set 3	Alert User	NA	05/23/2013 17:01 UTC
neen-Galaxy Nexus	neen	Restrict Jailbroken (iOS) and Ro...	Base Rule Set 3	Alert User and Adminis...	NA	04/02/2013 15:09 UTC
njade-GT-I9300	njade	Restrict Jailbroken (iOS) and Ro...	Base Rule Set 3	Alert User and Adminis...	NA	04/26/2013 06:03 UTC

Page 1 of 1 | Displaying 1 - 6 of 6 records | CSV | Export

Depending on the device compliance status, the **Action Status** column will display the **Executed**, **Planned** and the **NA** (Not Available) values. **NA** is displayed only for devices that are configured to receive compliance status alerts.

When an out of compliance device is remediated and complies with the set rules, then the device name is automatically removed from the **Compliance Status Overview** list.

Privacy

Many employees are concerned about personal information from their devices ending up on corporate servers. MaaS360's privacy settings can be used to limit the collection of Personally Identifiable Information (PII) for personal devices.

Mouse over **Security** and click **Privacy**.



On the Privacy Settings screen, specify how you want to treat PII. Click Save when you are finished.

Restrict Location Information	Click to stop MaaS360 from collecting location information. This includes physical address, geographical coordinates and history, IP address and SSID.
Select Applicable Ownership Types	Specify which devices should be exempt from the collection of location information.
Select Applicable Device Group	Specify which device group should be exempt from the collection of location information.
Restrict App Inventory Information	Click to stop MaaS360 from collecting information about apps. This includes which apps the user has and data from those apps. Apps distributed from the App Catalog and apps that are included as part of the corporate security policies will be tracked.
Select Applicable Ownership Types	Specify which devices should be exempt from the collection of app information.
Select Applicable Device Group	Specify which device group should be exempt from the collection of app information.

Click View Change History to see changes that have been made over time.

Last updated by	Last updated on	IP Address	Changes
mdm_jl	08/22/2012 18:56 UTC	688.688.68.68	Restrict Location Information: Disabled Restrict App Inventory Information: Enabled - Applicable Ownership Types: Employee-owned, Unknown Employee owned - Applicable Device Group: All Devices
bc@fiberlink.com	08/13/2012 17:39 UTC	268.68.168.68	Restrict Location Information: Enabled Disabled Restrict App Inventory Information: Enabled - Applicable Ownership Types: Employee owned, Unknown - Applicable Device Group: All Devices
mnelson	08/08/2012 14:22 UTC	688.68.684.68	Restrict Location Information: Enabled - Applicable Ownership Types: Employee-owned Employee owned, Unknown - Applicable Device Group: All Devices Restrict App Inventory Information: Enabled - Applicable Ownership Types: Employee-owned Employee owned, Unknown - Applicable Device Group: All All Devices

Locations

Select **Security > Locations** to set up locations that can be used for geo-fencing rules. Locations can be based on geographical locations and Wi-Fi networks.

Locations					
<div> Add Address based Location Add Wi-Fi based Location Search </div>					
1. In order to use location based functionality, devices must be enrolled and have the respective agent or application installed. 2. Add a location by specifying a physical address or by identifying Wi-Fi network details.					
Location Name	Location Info	Policy Rules	Last Updated By	Last Updated On	Actions
London Airport	Address: heathrow Airport Range (in miles): 1.0	IOS : All Pilots : UK Demo iOS Policy - with VPN	Isen	01/23/2013 20:39 UTC	-----Select Action-----
MaaS360 - Blue Bell	Address: 1787 Sentry Park West Blue Bell PA Range (in miles): 0.5	-	mdelsen	01/26/2013 23:19 UTC	-----Select Action-----
MaaS360 - San Mateo	Address: 1510 Fashion Island Blvd., Suite 130 ... Range (in miles): 0.25	-	jriels	01/26/2013 23:20 UTC	-----Select Action-----
MaaS360 - Philadelphia	Address: 1601 Cherry Street 20th Floor Philad... Range (in miles): 0.25	-	mdm_Cherry	01/26/2013 23:20 UTC	-----Select Action-----

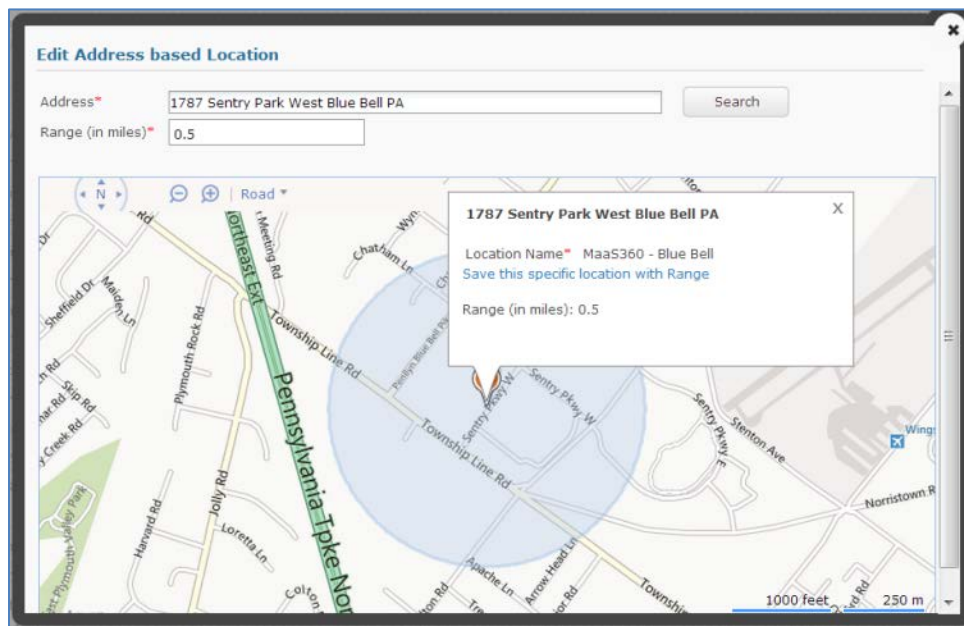
You can see the details about each location, and policies that are using it.

Click the **Actions** pull-down menu for one of the locations to perform an action on it.

Last Updated On	Actions
01/23/2013 20:39 UTC	-----Select Action-----
01/26/2013 23:19 UTC	-----Select Action----- -----Select Action----- Edit Assign Policies Delete
01/26/2013 23:20 UTC	

You can edit the location, assign a policy to it, or delete it.

Click the **Location Name** to see the address and range for the location.



Add an Address Based Location

Click Add Address based Location.

You have no Locations configured. Start with configuring Locations.

Locations Add Address based Location Add Wi-Fi based Location

1. In order to use location based functionality, devices must be enrolled and have the respective agent or application installed.
2. Add a location by specifying a physical address or by identifying Wi-Fi network details.


Location Name	Location Info	Policy Rules	Last Updated By	Last Updated On	Actions
You have no Locations configured. Start with configuring Locations.					
First Previous Next Last Showing 0 to 0 of 0 entries					

Enter the address and the range, and then click Search.

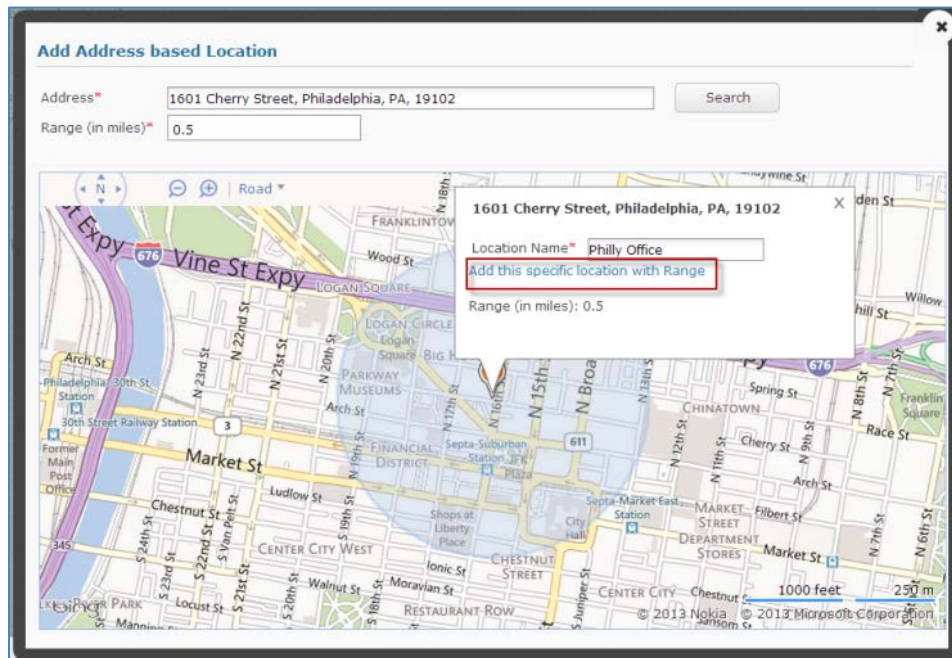
Add Address based Location

Address* Search

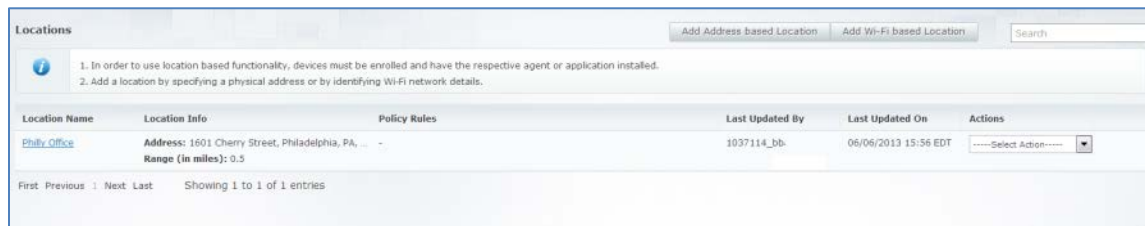
Range (in miles)*



Enter the location name and click Add this specific location with Range.

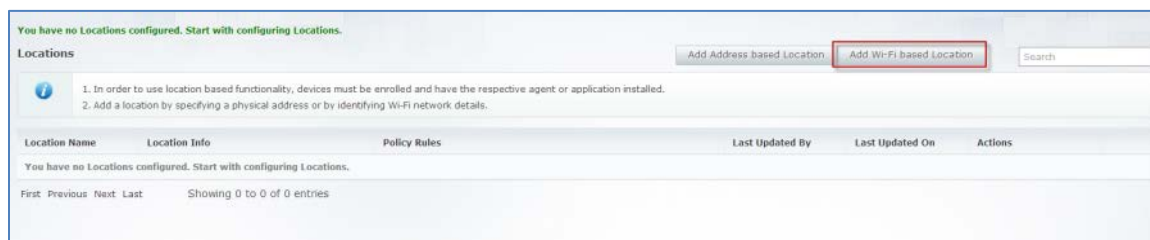


The location now appears on the **Locations** screen.



Add a Wi-Fi based Location

Click **Add a Wi-Fi based Location** from the **Locations** screen.



Enter the location name, Wi-Fi SSID and MAC address. Click **Add**.

Add Wi-Fi based Location

1. Location will be identified based on whether or not the device has connected to the specified Wi-Fi SSID.

2. Use access point MAC address for increased accuracy.

3. MAC address to be entered in the standard format of 6 groups of 1 or 2 hexadecimals each separated by a ":", for example "ae:90:30:b9:ad:dd" OR "ae:90:30:b9:d:d"

Location Name*

Wi-Fi SSID*

MAC Address

Cancel

Add

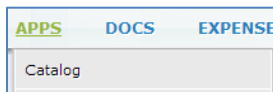
Applications

The app management features of MaaS360 are accessed from the **Apps** tab.

The App Catalog

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.

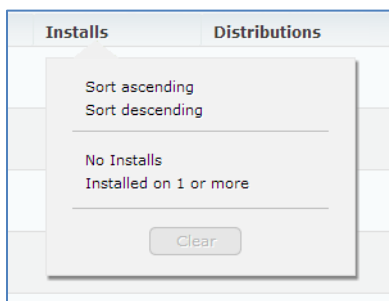
To access the App Catalog, mouse over **Apps** and click **Catalog**.



The App Catalog lists your apps and provides basic information about them.

App Catalog							
App	Name	Type	Category	VPP Codes	Last Updated	Installs	Distributio...
	Cisco WebEx Meetings View Distribute Delete More...		Business		11/27/2013 17:02 UTC	8	Yes
	Adobe Reader View Distribute Delete More...		Business		11/13/2013 07:42 UTC	0	No
	OpenTable View Distribute Delete More...		Food & Drink		11/08/2013 05:47 UTC	0	No
	MaaS360 Browser View Distribute Delete More...		Others		11/07/2013 21:01 UTC	1	Yes

You can sort and filter your apps by clicking on the column headings.



At the bottom of the screen you can see how much storage you are using, and how much is available. It also includes token information.

	MaaS360 View Distribute Delete More...		Others	11/05/2013 18:36 UTC	7	Yes
	AroundMe View Distribute Delete More...		Others	10/30/2013 18:12 UTC	0	Yes
	Mobile VPN View Distribute Delete More...		Business	10/24/2013 01:23 UTC	2	Yes

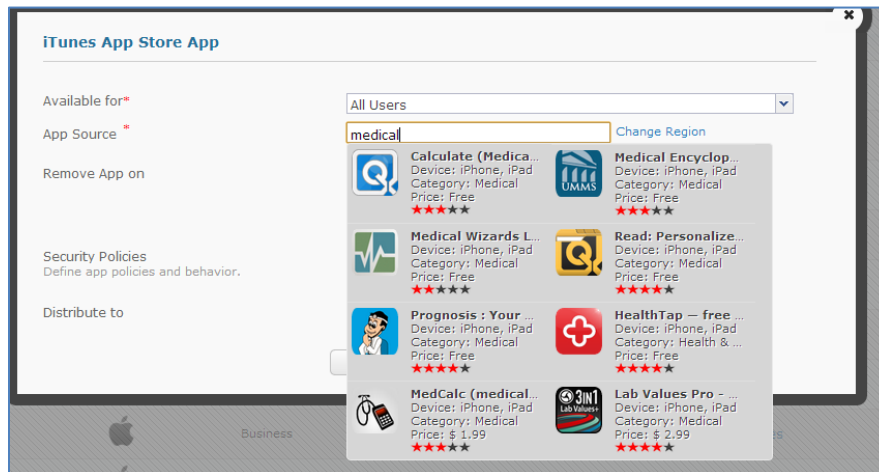
Displaying 1 - 10 of 91 Records

Total Space Available: 1 GB | Free Space Remaining: 706.53 MB | Tokens Uploaded: 1

There are links under each app you can use to take action.

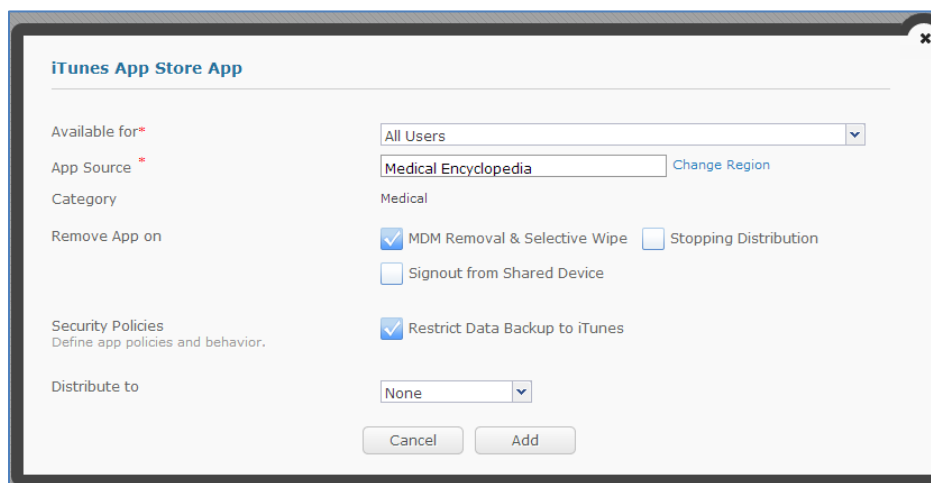
Adding an App to the App Catalog

1. Click the **Add** button to add an app.



4. Specify the app removal, security and distribution options.

Note: The security policies you used when uploading it into the catalog are in effect now.



Different options are displayed depending on the type of app:

- iTunes App Store App:
 - **App Source:** Enter the app's name. Click **Change Region** if need to change the name of the country
 - **Remove App on**
 - **MDM Removal & Selective Wipe:** The app will be removed if MaaS360's control of the device is terminated, or if a selective wipe is performed on the device
 - **Stopping Distribution:** The app will be removed if a pending distribution is ended
 - **Security Policies**
 - **Restrict Data Backup to iTunes:** App data will not be backed up to iTunes
 - **Distribute to**
 - **None:** Load the app into the App Catalog without distributing it
 - **Specific Device:** Enter the device name and specify:

- **Instant Install:** MaaS360 will prompt the recipient to download the app
 - **Send Email:** MaaS360 will send them an email telling them about the new app
- **Group:** Select the group of devices to receive the app and specify:
 - **Instant Install:** MaaS360 will prompt the recipient to download the app
 - **Send Email:** MaaS360 will send them an email telling them about the new app
- **All Devices:** All your devices will receive the app. Specify:
 - **Instant Install:** MaaS360 will prompt the recipient to download the app
 - **Send Email:** MaaS360 will send them an email telling them about the new app
- **Enterprise App for iOS:**
 - **App Source:** Enter the app's name
 - **Description:** Enter a description of the app
 - **Category:** Enter a classification for the app
 - **Screenshot:** Upload screenshots for the app
 - **Remove App on**
 - **MDM Removal & Selective Wipe:** The app will be removed if MaaS360's control of the device is terminated, or if a selective wipe is performed on the device
 - **Stopping Distribution:** The app will be removed if a pending distribution is ended
 - **Security Policies**
 - **Restrict Data Backup to iTunes:** App data will not be backed up to iTunes
 - **Distribute to**
 - **None:** Load the app into the App Catalog without distributing it
 - **Specific Device:** Enter the device name and specify:
 - **Instant Install:** MaaS360 will prompt the recipient to download the app
 - **Send Email:** MaaS360 will send them an email telling them about the new app
 - **Group:** Select the group of devices to receive the app and specify:
 - **Instant Install:** MaaS360 will prompt the recipient to download the app
 - **Send Email:** MaaS360 will send them an email telling them about the new app
 - **All Devices:** All your devices will receive the app. Specify:
 - **Instant Install:** MaaS360 will prompt the recipient to download the app
 - **Send Email:** MaaS360 will send them an email telling them about the new app

- Google Play App:
 - **App Name:** Enter the app's name. Click **Provide URL** if you need to find the app in the Google Play store
 - **Remove App on**
 - **MDM Control Removal:** The app will be removed if MaaS360's control of the device is terminated
 - **Selective Wipe:** The app will be removed if a selective wipe is performed on the device
 - **Security Policies**
 - **Enforce Authentication:** Users must enter a username and password to receive the app
 - **Enforce Compliance:** Devices must be in compliance to receive the app
 - **Distribute to**
 - **None:** Load the app into the App Catalog without distributing it
 - **Specific Device:** Enter the device name and specify:
 - **Send Email:** MaaS360 will send them an email telling them about the new app
 - **Group:** Select the group of devices to receive the app and specify:
 - **Instant Install:** MaaS360 will prompt the recipient to download the app. Instant Install is silent on Samsung SAFE devices
 - **Send Email:** MaaS360 will send them an email telling them about the new app
 - **All Devices:** All your devices will receive the app. Specify:
 - **Instant Install:** MaaS360 will prompt the recipient to download the app
 - **Send Email:** MaaS360 will send them an email telling them about the new app
- Enterprise App for Android:
 - **App Source:** Upload the file. Click **Provide URL** to use a URL instead
 - **Description:** Enter a description of the app
 - **Category:** Enter a classification for the app
 - **Screenshot:** Upload screenshots for the app
 - **Remove App on**
 - **MDM Control Removal:** The app will be removed if MaaS360's control of the device is terminated
 - **Selective Wipe:** The app will be removed if a selective wipe is performed on the device
 - **Security Policies**
 - **Restrict Data Backup to iTunes:** App data will not be backed up to iTunes
 - **Distribute to**

- None: Load the app into the App Catalog without distributing it
- Specific Device: Enter the device name and specify:
 - **Instant Install:** MaaS360 will prompt the recipient to download the app. Instant Install is silent on Samsung SAFE devices
 - **Send Email:** MaaS360 will send them an email telling them about the new app
- Group: Select the group of devices to receive the app and specify:
 - **Instant Install:** MaaS360 will prompt the recipient to download the app. Instant Install is silent on Samsung SAFE devices
 - **Send Email:** MaaS360 will send them an email telling them about the new app
- All Devices: All your devices will receive the app. Specify:
 - **Instant Install:** MaaS360 will prompt the recipient to download the app. Instant Install is silent on Samsung SAFE devices
- **Send Email:** Recipients will receive an email telling them that the app has been added to their app catalog
- Windows Phone Store App:
 - **Windows Phone Store App:** Upload the file. Click **Provide URL** to use a URL instead
 - **Distribute to**
 - None: Load the app into the App Catalog without distributing it
 - Specific Device: Enter the device name and specify:
 - **Send Email:** MaaS360 will send them an email telling them about the new app
 - Group: Select the group of devices to receive the app and specify:
 - **Send Email:** MaaS360 will send them an email telling them about the new app
 - All Devices: All your devices will receive the app. Specify:
 - **Send Email:** Recipients will receive an email telling them that the app has been added to their app catalog
- Windows Phone Private App:
 - **Windows Phone URL for App:** Specify the URL of the app
 - **Distribute to**
 - None: Load the app into the App Catalog without distributing it
 - Specific Device: Enter the device name and specify:
 - **Send Email:** MaaS360 will send them an email telling them about the new app
 - Group: Select the group of devices to receive the app and specify:
 - **Send Email:** MaaS360 will send them an email telling them about the new app

- **All Devices:** All your devices will receive the app.
- **Send Email:** Recipients will receive an email telling them that the app has been added to their app catalog
- **Enterprise Windows Phone App:**
 - **Available for:** Specify who can receive the app (all users or a specific group)
 - **App Source:** Upload the file. Click **Provide URL** to use a URL instead
 - **Description:** Enter a description of the app
 - **Category:** Enter a classification for the app
 - **Screenshot:** Upload screenshots for the app
 - **Remove App on**
 - **MDM Control Removal:** The app will be removed if MaaS360's control of the device is terminated

Note: Enterprise Windows Phone Apps are always removed if MaaS360's control of the device is terminated or if a selective wipe is performed on it.

 - **Distribute to**
 - **None:** Load the app into the App Catalog without distributing it
 - **Specific Device:** Enter the device name and specify:
 - **Instant Install:** MaaS360 will prompt the recipient to download the app
 - **Send Email:** MaaS360 will send them an email telling them about the new app
 - **Group:** Select the group of devices to receive the app and specify:
 - **Instant Install:** MaaS360 will prompt the recipient to download the app
 - **Send Email:** MaaS360 will send them an email telling them about the new app
 - **All Devices:** All your devices will receive the app. Specify:
 - **Instant Install:** MaaS360 will prompt the recipient to download the app
 - **Send Email:** MaaS360 will send them an email telling them about the new app
- **Web App for iOS:**
 - **Web App Display Name:** Enter the app's name
 - **Web App URL:** Enter the complete URL for the app
 - **Web App Icon:** Specify the icon you want to represent the app
 - **Description:** Enter a description of the app
 - **Category:** Enter a classification for the app
 - **Remove App on**
 - **Stopping Distribution:** The app will be removed if a pending distribution is ended

Note: iOS Web Apps are always removed if MaaS360's control of the device is terminated or if a selective wipe is performed on it.

- Policies
 - **Install Automatically:** App data will not be backed up to iTunes
 - **Launch in Full Screen:** Launch the app in full screen mode on the device
 - **Visual Effects on Icon:** The icon will be displayed with standard graphics
 - **Allow Users to Remove:** Allow users to remove the app from the device
- Distribute to
 - **None:** Load the app into the App Catalog without distributing it
 - **Specific Device:** Enter the device name
 - **Group:** Select the group of devices to receive the app
 - **All Devices:** All your devices will receive the app.

5. When you have finished selecting the options you want, click **Add**.

Note: The Secure Productivity Suite offers many more options for securing apps. For more information, contact your account representative.

Viewing an App

Click the View link to see detailed information about the app.

The screenshot displays the 'Jabber' app configuration page. It includes sections for App Summary, Security Policies, Details, and Update History.

Available for	All	App ID	com.cisco.jabber
Type	Google Play App	Category	Business
Supported On	Smartphone	Distributions	Device: jelsen-Galaxy Nexus Device: rseber-HTC One v
Installs	0 installed 2 distributed	App Version (Size)	NA (NA)
Update Date (Uploaded By)	04/02/2013 15:04 UTC (mdm_inelsen)		

Security Policies

Define app policies and behavior

Remove on MDM Control Removal	<input type="checkbox"/>	Remove On Selective Wipe	<input type="checkbox"/>
Enforce Compliance	<input type="checkbox"/>	Enforce Authentication	<input type="checkbox"/>

Details

Cisco Jabber for Android turns your Android device into a full-featured Cisco Unified IP Phone. The application allows you to make, receive, and manage calls using your company's telephony infrastructure and your work phone number. You can make calls using either Wi-Fi or your mobile voice network with the Dial via Office (DVO) feature. Wi-Fi provides cost savings on roaming charges and mobile minutes, and provides better in-building network coverage. The mobile voice network allows you to leverage your company's telephony infrastructure, providing additional cost savings and better voice quality when outside the corporate network. br/br/NOTE: This application requires connectivity to Cisco Unified Communications Manager (TM) and does not work without it. If you do not know if your company provides access to this service, please contact your IT department. You cannot use this application without an account on this service. br/ The Dial via Office feature requires Cisco Jabber

Update History

Action By	Action Date	Action	App Size (MB)	IP Address
mdm_inelsen	04/02/2013 15:04 UTC	Upload	-	688.68.584.68

You can see:

- The type of app
- The category
- How many devices it was distributed to
- How many have installed it
- Any security policies in effect for it
- An audit trail

If there are pending distributions, they will be marked with a red X. You can click the X to cancel the specified distribution.

Distributing an App

Click the **Distribute** link to choose the options you want for distributing the app. There are different options depending on the type of app.

Different options are displayed depending on the type of app:

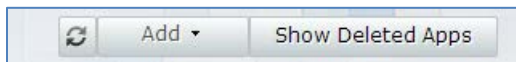
- iTunes App Store App:
 - **Available for:** Specify who can receive the app, either all users or a group
 - **Target:** Specify if it will be deployed to a device, a group or a specific device
 - **Instant Install (iOS 5+ devices):** If you are using VPP codes for paid apps, recipients will not have to pay for the app
 - **Send Email:** Recipients will receive an email telling them that the app has been added to their app catalog
- Enterprise App for iOS:
 - **Available for:** Specify who can receive the app, either all users or a group
 - **Target:** Specify if it will be deployed to a device, a group or a specific device
 - **Instant Install (iOS 5+ devices):** If you are using VPP codes for paid apps, recipients will not have to pay for the app. In addition, the users will not need to enter a password to get the enterprise app
 - **Send Email:** Recipients will receive an email telling them that the app has been added to their app catalog
- Google Play App:
 - **Available for:** Specify who can receive the app, either all users or a group
 - **Target:** Specify if it will be deployed to a device, a group or a specific device
 - **Send Email:** Recipients will receive an email telling them that the app has been added to their app catalog
- Enterprise App for Android:
 - **Available for:** Specify who can receive the app, either all users or a group
 - **Target:** Specify if it will be deployed to a device, a group or a specific device
 - **Instant Install:** Specify if the user will be prompted to install the app and the type of network:
 - All Networks
 - Wi-Fi only
 - Wi-Fi and in-network cellular
 - Note: Instant Install is silent for Samsung SAFE devices.*
 - **Send Email:** Recipients will receive an email telling them that the app has been added to their app catalog
- Windows Phone Store App:
 - **Available for:** Specify who can receive the app, either all users or a group

- **Target:** Specify if it will be deployed to a device, a group or a specific device
- **Send Email:** Recipients will receive an email telling them that the app has been added to their app catalog
- **Enterprise Windows Phone App:**
 - **Available for:** Specify who can receive the app, either all users or a group
 - **Target:** Specify if it will be deployed to a device, a group or a specific device
 - **Send Email:** Recipients will receive an email telling them that the app has been added to their app catalog
- **Windows Phone Private App:**
 - **Available for:** Specify who can receive the app, either all users or a group
 - **Target:** Specify if it will be deployed to a device, a group or a specific device
 - **Send Email:** Recipients will receive an email telling them that the app has been added to their app catalog
- **Web App for iOS:**
 - **Available for:** Specify who can receive the app, either all users or a group
 - **Target:** Specify if it will be deployed to a device, a group or a specific device

Deleting an App

Click the **Delete** link to delete the app from the App Catalog. It cannot be distributed to anyone if it has been deleted, and any existing distributions will be stopped (this may remove the app from the devices).

Click **Show Deleted Apps** to see all the apps that were deleted. You can only view them.



Distribution Details by Devices

Click the **More** link, and then click **Distribution Details by Devices** to see information about previous distributions.

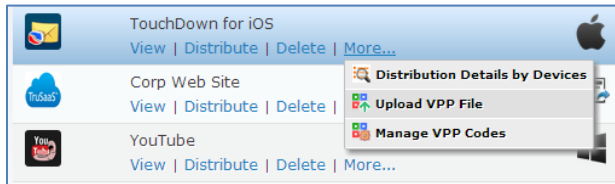
Keynote Distribution Details by Devices					
App	Installed via MDM	Device	Status	User	Paid Status
Keynote	No	Cedric's iPad	Pending Install	cedric	User Paid
Keynote	No	Jim iPhone 5	Installed	jan	User Paid
<div> 1 2 3 4 5 </div> <div>Displaying 1 - 2 of 2 Records</div> <div> <div>CSV</div> <div>Export</div> </div>					

Apple Store: Volume Purchasing Program

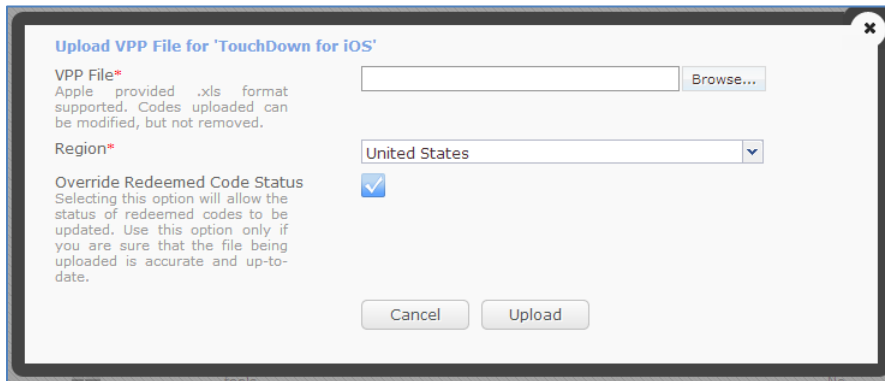
The **Apple Store Volume Purchase Program (VPP)** allows educational institutions to buy iOS apps in volume and distribute the apps to their users. The Volume Purchase Program allows developers and organizations to purchase large number of applications at special prices from the Apple Stores.

MaaS360 will allow you to load VPP codes:

1. Find the app and mouse over the **More** link. Click **Upload VPP File**.



2. Browse to the file's location and select it. Specify the region, and click **Override Redeemed Code Status** if you want to make it possible for the status of redeemed codes to be updated.



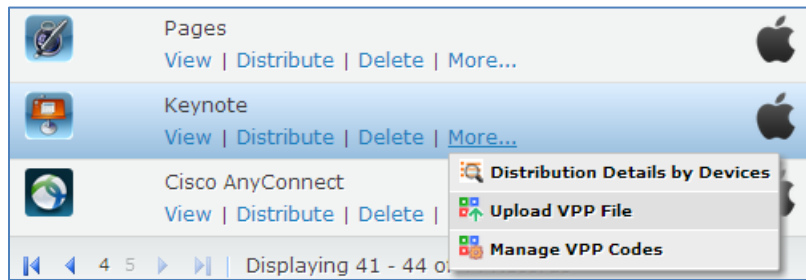
3. Click **Upload**.

You can also upload a file when viewing an app by clicking  and then entering the upload information.



You can manage or review the status of VPP codes by performing the following:

4. Find the app. Mouse over **More**, and then click **Manage VPP Codes**.



5. You can see which devices used the codes and how many codes are still available for the app.

Manage VPP Codes: 'Keynote'

Devices yet to install this app: 1 Remaining VPP Codes: 0

Upload VPP Codes Clear VPP codes

Order No	VPP code	Region	Status	Update Date	Device	Username
13YKW3YFYS Reset to NEW	3YK3YKW3Y3YK	United States	REDEEMED	05/03/2013 01:49 UTC	Drew's iPad	dline
M3YnFY5 FY5 Reset to NEW	E3YK3YKW3YK	United States	REDEEMED	03/16/2012 18:07 UTC	jdew's iPhone	jdew

Displaying 1 - 2 of 2 Records

CSV Export

6. Click the **Upload VPP Codes** button to upload another file of codes. Click **Clear VPP codes** to clear any unused codes.

Documents

The Document Management features of MaaS360 are accessed from the **Docs** tab.

Content Library

MaaS360 allows you to distribute documents and files to your users quickly and easily. Each document must be loaded into the MaaS360 Content Library before it can be distributed.

To access the Content Library, mouse over **Docs** and click **Content Library**.



The Content Library lists your files and provides basic information about them.

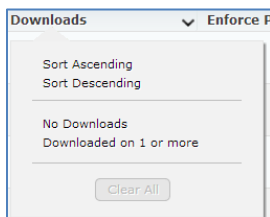
Document	Avail...	Type	Size	Tags	Downloads	Enforce Password	Restrict Export	Last Updated
ds_maas360_mdm_Secure-Productivity-Suite Edit Distribute Delete	All		1.2 MB	Others	2	No	No	09/24/2013 02:23 UTC
Test Push RS Edit Distribute Delete	All		12.79 KB	Others	0	No	Yes	09/19/2013 17:03 UTC
cloudExtender_requirementsCheatSheet Edit Distribute Delete	All		82.81 KB	Others	1	No	No	09/11/2013 04:52 UTC
BulkEnrollSampleCorp (1) Edit Distribute Delete	All		1024.0 Bytes	Others	0	Yes	Yes	09/04/2013 08:19 UTC
MJReturn Edit Distribute Delete	All		28.17 KB	Others	2	No	Yes	08/30/2013 12:48 UTC
DLP launch Edit Distribute Delete	All		1.88 MB	Others	0	No	Yes	08/30/2013 04:21 UTC
Fiberlink Sales Presentation Edit Distribute Delete	All		10.44 MB	Others	2	No	Yes	08/22/2013 21:14 UTC
Secure-Productivity-Suite Edit Distribute Delete	All		1.19 MB	Others	4	Yes	No	08/21/2013 19:04 UTC
Mutual NDA Edit Distribute Delete	All		12.63 KB	Legal	2	No	Yes	06/08/2013 16:47 UTC
iBooks File Edit Distribute Delete	All		60.37 MB	Others	0	No	No	04/15/2013 19:48 UTC

Displaying 11 - 20 of 39 Records

Total Space Available: 1 GB | Free Space Remaining: 639.09 MB

Click the highlighted number under **Downloads** to see the devices that have downloaded the file.

You can sort and filter your files by clicking on the column headings.



There are links under each document you can use to take action.

Adding Documents to the Content Library

If you wish to add a new document, mouse over **Docs** and select **Content Library**.

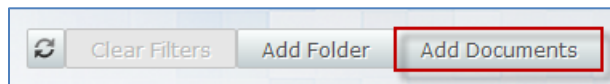
At the bottom of the page you can see how much free space is still available—you may need to delete documents before you can add the new one.

Content Library: All Docs								
Document	Avail...	Type	Size	Tags	Downloads	Enforce Password	Restrict Export	Last Updated
ds_maas360_mdm_Secure-Productivity-Suite Edit Distribute Delete	All		1.2 MB	Others	2	No	No	09/24/2013 02:23 UTC
Test Push RS Edit Distribute Delete	All		12.78 KB	Others	0	No	Yes	09/19/2013 17:03 UTC
cloudExtender_requirementsCheatSheet Edit Distribute Delete	All		82.81 KB	Others	1	No	No	09/11/2013 04:52 UTC
BulkEnrollSampleCorp (1) Edit Distribute Delete	All		1024.0 Bytes	Others	0	Yes	Yes	09/04/2013 08:19 UTC
MJReturn Edit Distribute Delete	All		28.17 KB	Others	2	No	Yes	08/30/2013 13:48 UTC
DLP launch Edit Distribute Delete	All		1.88 MB	Others	0	No	Yes	08/30/2013 04:21 UTC
Fiberlink Sales Presentation Edit Distribute Delete	All		10.44 MB	Others	2	No	Yes	08/22/2013 21:14 UTC
Secure-Productivity-Suite Edit Distribute Delete	All		1.19 MB	Others	4	Yes	No	08/21/2013 19:04 UTC
Mutual NDA Edit Distribute Delete	All		12.63 KB	Legal	2	No	Yes	06/08/2013 16:47 UTC
iBooks File Edit Distribute Delete	All		60.37 MB	Others	0	No	No	04/16/2013 19:48 UTC

Displaying 11 - 20 of 39 Records

Total Space Available: 1 GB | Free Space Remaining: 839.09 MB

Click the **Add Documents** button to upload documents that you wish to distribute to iOS and Android mobile devices.



Enter the details about the document.

Add Documents

All Docs

Available for

All

Select Files *

Multiple file selection (up to 15) supported. Selected folders will be ignored.

[Provide URL](#)

Document Names *

Tags

Security Settings

Define security settings for selected documents. Supported only on iOS App 2.2+ and Android App 4.1+(with Secure Viewer).

☐ Restrict Export
 ☐ Restrict Cut/Copy/Paste

Download Policies

Configure download policies for documents. Supported on iOS only

☐ Password Protected
 ☐ Download Automatically
 ☐ Download only on Wi-Fi
 ☐ Hide Doc Preview in App
 ☐ Restrict Delete after Download

Distribute to

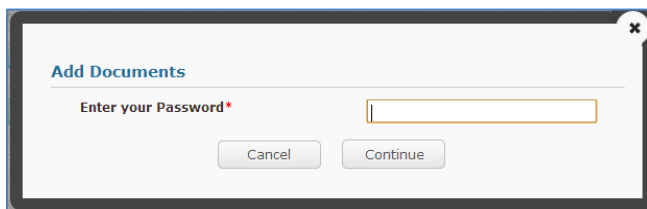
None

Available for	Specify the group that can receive the document.
---------------	--

Select Files	Browse to the file you want to add and select it. You can upload up to 15 files at a time.
Document Names	Enter the name you want your users to see.
Tags	Enter tags to help your users find the document, separated by a comma.
Security Settings	Specify the security settings that apply to this document: <ul style="list-style-type: none"> • Restrict Export: Users cannot open the document with another app. • Restrict Cut/Copy/Paste: Text in the document cannot be cut, copied or pasted into another app.
Download Policies	Specify the policies that apply to this document: <ul style="list-style-type: none"> • Password Protected: Users must enter a password to access the document • Download Automatically: The document will automatically be downloaded onto the device • Hide Doc Preview in App: A preview of the document will not be shown for file formats like iBooks where preview is not supported • Download only on Wi-Fi: To reduce costs, the document will only be downloaded on a Wi-Fi network • Restrict Delete after Download: Prevents users from removing a locally cached copy of the document
Distribute to	Specify if the document should immediately be distributed to all devices and users, a specific group, a specific device, or if it should not be distributed immediately (None). You can also enter an expiration date when the document will be removed from an individual device, a group or all users.

Click **Save**.

When prompted, enter your password and click **Continue**.



Edit

Click the **Edit** link to see detailed information about the document.

The screenshot shows the document management interface for a PDF file. The document is titled 'cloudExtender_requirementsCheatSheet.pdf' and is 82.81 KB in size. It has been updated by '1000000_jray' on 09/11/2013 04:52 UTC. The interface includes sections for Document Summary, Security Settings, Download Policies, and Version History.

Document Summary			
Name	cloudExtender_requirementsCheatSheet	Size	82.81 KB
Tags	Others	Downloads	1
Distributions	Device: iOS: Ray's iPhone ✖ Device: iOS: iPhone ✖ Device: Android: jbert-GT-N8013 ✖		

Security Settings	
Define security settings for the current document. Supported on iOS App 2.2+ and Android App 4.1+ (with Secure Viewer).	
Restrict Export Restrict opening documents using other apps.	Restrict Cut/Copy/Paste Restrict Cut/Copy/Paste to other apps (iOS only).

Download Policies	
Configure download policies for the document. Supported only on iOS.	
Download Automatically <input type="checkbox"/>	Download only on Wi-Fi <input type="checkbox"/>
Hide Doc Preview in App <input type="checkbox"/>	Restrict Delete after Download <input type="checkbox"/>
Password Protected <input type="checkbox"/>	

Version History			
File Name	Size	Updated By	Updated On
cloudExtender_requirementsCheatSheet.pdf	82.81 KB	1000000_jray	09/11/2013 04:52 UTC

You can see information about the distribution, including the size of the file and any security that has been applied to it. You can also see the version history for the file. Click the red X to delete a distribution.

For iOS devices, you can select **Restrict Share** and prevent documents from being opened with third-party apps. On Android devices it will prevent the content from going to the device.

You can also specify the download policies for iOS devices:

- **Download Automatically:** The document will automatically be downloaded onto the device
- **Hide Doc Preview in App:** A preview of the document will not be shown. This is for file formats like iBooks where preview is not supported
- **Password Protected:** Users must enter a password to access the document
- **Download only on Wi-Fi:** To reduce mobile data costs, the document will only be downloaded on a Wi-Fi network
- **Restrict Delete after Download:** Prevents users from removing a locally cached copy of the document

After making your changes, click **Save**.

You can also remove the document from the Content Library by clicking **Delete** from this screen.

Adding a Version

You may want to send different versions of a document to your users over time.

Select the document, and click the **Edit** link.

Content Library: All Docs		
Document	Available for	Type
MaaS360 - MDM Made Simple	All	
Edit Distribute Delete		

Click **Add Version**.

The screenshot shows a document management interface with a toolbar at the top containing buttons for 'Save', 'Delete', 'Distribute', and 'Add Version'. Below the toolbar, there is a table with two rows. The first row shows '7.54 MB' and the second row shows '0'.

Browse to the new version and click **Save**.

The screenshot shows a dialog box titled 'Update Document Version'. It has a text input field labeled 'New version*' containing the text 'MaaS360 - MDM Made Simple.pptx'. To the right of the input field is a 'Browse...' button. Below the input field are two buttons: 'Cancel' and 'Save'.

Enter your password and click **Continue**.

The screenshot shows a dialog box titled 'Add Document Version'. It has a text input field labeled 'Enter your Password*' with a password mask (dots). Below the input field are two buttons: 'Cancel' and 'Continue'.

The version history at the bottom of the screen will reflect the change.


The screenshot shows the document management interface for 'MaaS360 - MDM Made Simple'. It includes sections for 'Document Summary', 'Security Settings', 'Download Policies', and 'Version History'. The 'Version History' section shows a table with columns: 'File Name', 'File Size', 'Updated By', and 'Updated On'.

File Name	File Size	Updated By	Updated On
MaaS360_-_MDM_Made_Simple.pptx	7.54 MB	mdm_bb	06/04/2013 23:08 UTC
MaaS360_-_MDM_Made_Simple.pptx	7.54 MB	mdm_bb	06/04/2013 16:29 UTC

Distribute

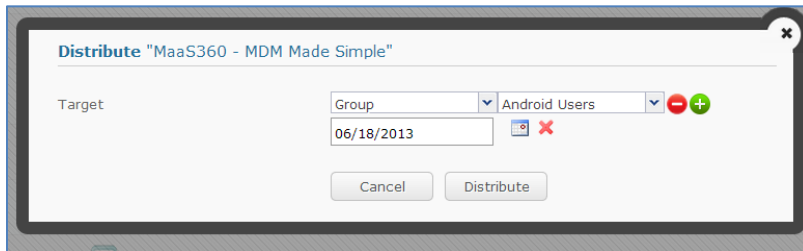
To distribute a document, click the **Distribute** link under its name.

The screenshot shows a document management interface with a table. The table has two columns: 'Document' and 'Available for'. The 'Document' column contains the text 'MaaS360 - MDM Made Simple' and a link 'Edit | Distribute | Delete'. The 'Available for' column contains the text 'All'.

Specify if an individual device, a group or all users should receive the document. If you want to distribute the document to more than one target, click .

You can also enter an expiration date when MaaS360 will remove the document from an individual device, a group or all users.

Click **Distribute**.



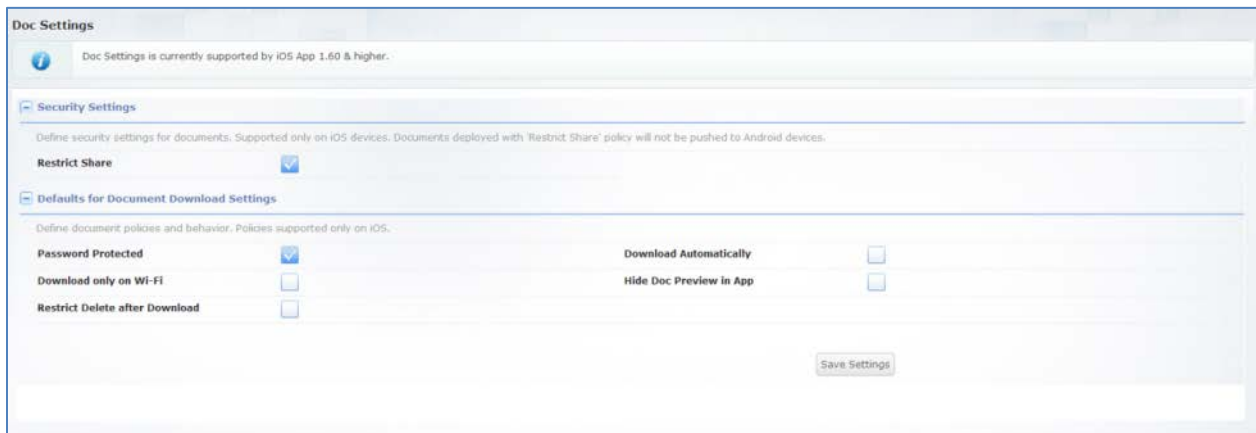
Delete

To delete a document, click the Delete link under its name.

Document	Available for
MaaS360 - MDM Made Simple	All
Edit Distribute Delete	

Document Settings

Select **Docs > Settings** to specify document policies and behavior.



Restrict Share	Users cannot open documents with third-party apps, email documents, or copy/paste the content.
Password Protected	Users must enter a passcode to access the document. The passcode will depend on the enrollment settings. For example, if the enrollment settings specify to use Active Directory credentials, the credentials entered to access document would be the user's Active Directory credentials.
Download only on Wi-Fi	To reduce costs, the document will only be downloaded on a Wi-Fi network.
Restrict Delete after Download	Prevents users from removing a locally cached copy of the document.
Download	The document will automatically be downloaded onto the device.

Automatically	
Hide Doc Preview in App	A preview of the document will not be shown for file formats like iBooks where preview is not supported.

These are the default settings for all your documents.

Content Sources

MaaS360 integrates easily with your public environments, including SharePoint, Windows File Share content and Intranet sites.

Note: If Private SharePoint is needed, you will need to install the MaaS360 Mobile Enterprise Gateway. For more information, refer to the MaaS360 Mobile Enterprise Gateway Administrators Guide.

Click Docs > SharePoint Sites to display the Manage SharePoint Settings screen.

Site Display Name	Site URL	Library/Folder	Group Access Permissions
QA Sharepoint Demo Edit Delete	http://fqa/sites/site1		Group Name: Luis Devices Permissions: Restrict Share Group Name: art hare Permissions: Restrict Share Group Name: jn hare Permissions: Restrict Share
MaaS360 SharePoint Demo Edit Delete	http://sp/sites/appreview1	Shared Documents	Group Name: CI-PII Permissions: Restrict Share Group Name: SLullen Permissions: Restrict Share

Displaying 1 - 2 of 2 Records

You can see all your sites, the site URLs, the library/folder and the group access permissions.

To add a new site, click the Add New Site button.

Add Site

Site Display Name*
This is what your end user will see.

Browser URL*
Copy this from the browser where you access a SharePoint folder.

Group Access Permissions
Select group and set permissions.

all ios View and Share

Cancel Save

Enter the Site Display Name, the Browser URL, Site URL, name of the Library or Folder that you wish to share, Group Access Permissions and sharing restrictions:

- **View and Share:** users can open documents with third-party apps, email documents, and copy/paste the content
- **Restrict Share:** users cannot open documents with third-party apps, email documents, or copy/paste the content

Click **Save**.

Click the **Edit** link under the site name to edit the settings, and **Delete** to remove the site.

MaaS360 SharePoint Demo	http://sp
Edit Delete	
⏪ ⏩ 1 ⏪ ⏩ Displaying 1 - 2 of 2 Records	

Expense Management

Note: This module may not be enabled for all users. Contact your account representative for details.

The Mobile Expense Management (MEM) module lets you enable mobile data usage tracking for specific devices.

- Plans can set up in-network and roaming data usage limits.
- Alerts can be set up to be automatically triggered when the user reaches or exceeds the specified threshold criteria. You can also specify the action to be taken by the device on exceeding the data usage limit. When devices reach the usage threshold limits, the specified alerts are automatically triggered.

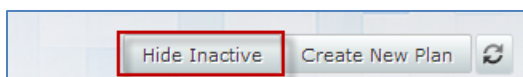
For iOS and Android devices, the MEM feature is enabled only if the selected device is associated with an MEM plan.

Note: MaaS360 allows you to perform only usage-based tracking and not cost-based tracking.

Mouse over the **Expense** tab and click **Manage Plans** to see all your company's plans.

Manage Plans							Show All Plans	Create New Plan	
Plan Name	Default	Status	Available For	First day of the Bil...	Published Version	Last Modified Date	Actions		
UK Data - High		Published	Entire Account	1	1	02/12/2013 11:31 UTC	Actions		
Carrier 1		Published	CPS			02/08/2013 15:28 UTC	Actions		
Data - High		Published	Entire Account	1	1	02/04/2013 16:13 UTC	Actions		
Carrier 2GB Data Plan		Published	Entire Account	9	1	02/03/2013 19:43 UTC	Actions		
1GB- Columbia		Published	Entire Account	15	1	01/31/2013 22:09 UTC	Actions		
Philly Office		Draft	Entire Account			01/31/2013 21:51 UTC	Actions		

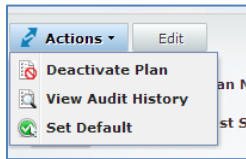
You can toggle between seeing all the plans and only seeing the active ones by clicking the appropriate button at the top of the page. The text on the button changes depending on what is being displayed.



You can click on the plan's name to see details about it.

Carrier 2GB Data Plan			
Actions	Edit		Back to Results
Plan Name *	Carrier 2GB Data Plan		
Last Successful Publish Date	02/03/2013 19:43 UTC [Version : 1]		
Description: Allotment for 2GBs of data usage			
Plan Details			
First day of the Billing cycle *	9		
In-Network Mobile Data Usage Limit (MB) *	2048		
Roaming Mobile Data Usage Limit (MB) *	100		

You can choose an **Action** from the pull-down menu or click **Edit** to update the plan.

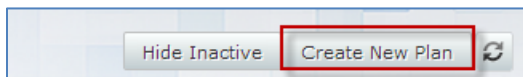


- **Deactivate Plan:** Make the plan inactive. Any devices currently assigned to the plan will not have a plan; their usage will not be tracked
- **View Audit History:** See the actions that have been taken on the plan, including when it was published
- **Set Default:** Make this plan the default plan

Creating a New Plan

To create a new plan, perform the following steps:

1. Click the Create New Plan button.



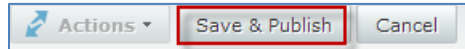
2. The Create Plan box appears.

3. Specify the group that can have the plan, the plan's name and a description. Click **Continue**.
4. Enter the plan details.

First day of the Billing cycle	Specify the day of the month on which the billing cycle begins.
In-Network Mobile Data Usage Limit (MB)	Specify the in-network data usage limit.

Roaming Mobile data Usage Limit (MB)	Specify the roaming data usage limit.
--------------------------------------	---------------------------------------

- Click **Save & Publish** when you are finished defining the plan.



The plan can now be deployed to users. It is only available to those in the group you originally specified in Step #3.

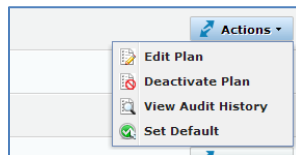
The plan will be in Draft status until it is published. It cannot be used until it is published.

Changing an Existing Plan

- Find the plan on the **Manage Plans** screen.

Manage Plans							
Plan Name	Default	Status	Available For	First day of the Bil...	Published Version	Last Modified Date	Actions
UK Data - High		Published	Entire Account	1	1	02/12/2013 11:31 UTC	Actions
Carrier 1		Published	CPS			02/08/2013 15:28 UTC	Actions
Data - High		Published	Entire Account	1	1	02/04/2013 16:13 UTC	Actions
Carrier 2GB Data Plan		Published	Entire Account	9	1	02/03/2013 19:43 UTC	Actions
IGS- Columbia		Published	Entire Account	15	1	01/31/2013 22:09 UTC	Actions
Philly Office		Draft	Entire Account			01/31/2013 21:51 UTC	Actions

- Select **Edit Plan** from the **Actions** menu:

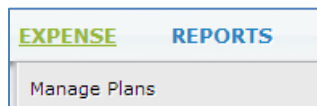


- Make your changes to the plan and click **Save & Publish** when you are finished.

Deactivating and Reactivating a Plan

To deactivate a plan, perform the following steps:

- Select **Expense > Manage Plans**.



- Find the plan you want and select the **Actions** menu for that plan.

Manage Plans							
Plan Name	Default	Status	Available For	First day of the Bil...	Published Version	Last Modified Date	Actions
May Test		Published	Entire Account	10	1	05/29/2013 18:03 UTC	Actions
3GB- LATAM		Published	Entire Account	2	1	05/23/2013 14:24 UTC	Actions
3GB LATAM		Published	Entire Account	4	1	05/17/2013 12:57 UTC	Actions

- Click Deactivate Plan on the menu. Click Continue when you see the confirmation message.

Deactivate Plan

Are you sure you want to deactivate this plan? All devices that are assigned this Plan will not have any plan assigned and hence Mobile Data Usage tracking will be stopped for these devices.

Cancel Continue

The status of the plan is now **Inactive**. MaaS360 will no longer track usage for any devices that were assigned to it.

To reactivate a plan, perform the following steps:

- On the **Manage Plans** screen, make sure all plans are visible. The **Show Active and Inactive Plans** toggle should say **Hide Inactive**.

Manage Plans							
Plan Name	Default	Status	Available For	First day of the Bil...	Published Version	Last Modified Date	Actions
May Test		Inactive	Entire Account	10	1	05/29/2013 18:03 UTC	Actions
3GB- LATAM		Published	Entire Account	2	1	05/23/2013 14:24 UTC	Actions
3GB LATAM		Published	Entire Account	4	1	05/17/2013 12:57 UTC	Actions

- Click on the **Actions** pull-down menu for that plan, and then select **Reactivate Plan**.

Actions

Actions

Reactivate Plan

View Audit History

- Specify if the plan should be the default plan, and enter a description.

Publish Plan

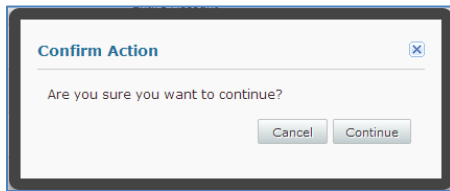
Set as default ☐

Enter a description to help with any future audits
(Maximum of 255 characters)

Add comments

Continue

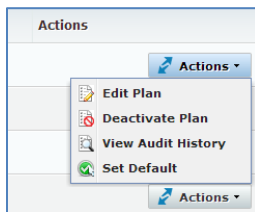
- Click **Continue**. The **Confirm Action** message appears.



- Click **Continue**. The plan has been reactivated.

Viewing Audit History

To see the changes that have been made to a plan, click **View Audit History** from the **Actions** menu for that plan.



The Audit History screen displays changes for a plan, and when they were made.

A screenshot of the 'Audit History - May Test' screen. It shows a table with columns: Published Date, Event, Published Version, Published By, and Comments. There are two rows of data. At the bottom, it says 'Page 1 of 1' and 'Displaying 1 - 2 of 2 records'.

Published Date	Event	Published Version	Published By	Comments
05/28/2013 18:45 UTC	Publish	2	mdm_bb	Reactivating a plan
05/29/2013 18:03 UTC	Publish	1	mdm_bb	Test Plan

Reports

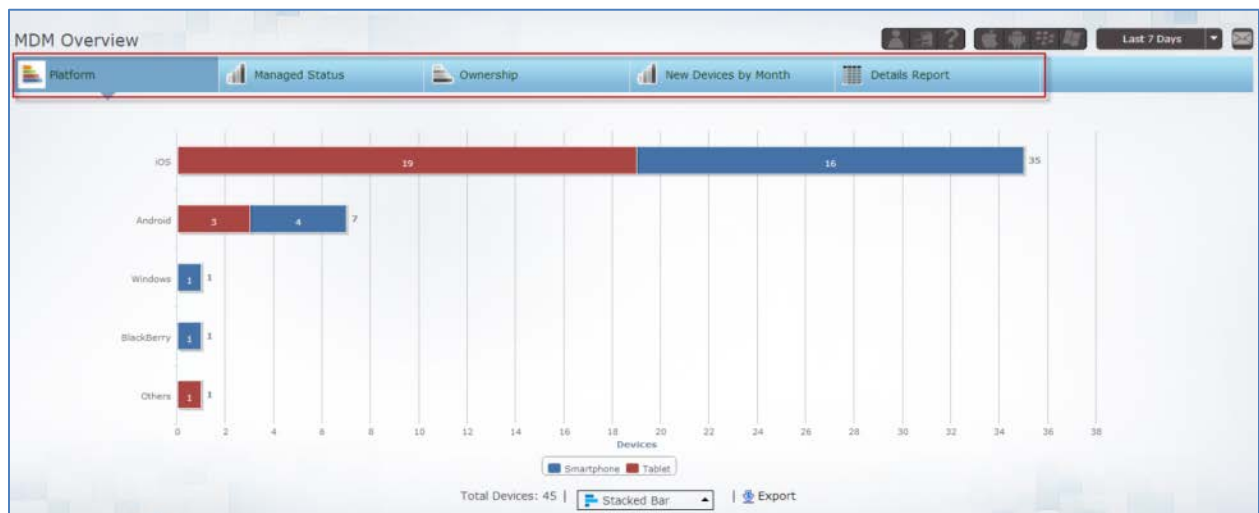
MaaS360 Mobile Intelligence™ reports allows you to use enhanced reporting functions, such as the tabular presentation of reports to group associated graphs and reports, and to provide easy navigation between the reports. It also includes filters, which help you generate a variety of real-time reports or narrow down report details based on your filter criteria.

To access the reports, mouse over the Reports tab and select the report family you want.

REPORTS SETUP Search		
MOBILE DEVICES	PC INVENTORY	PC SECURITY
MDM Overview	PC Overview	Security
Hardware Inventory	Hardware Inventory	Anti-Virus
Network	Network	Personal Firewall
BlackBerry Details	Operating System	Encryption
Deployment Overview	Software	Backup & Recovery
MOBILE APPS	Windows 7 & 8 Readiness	Patches
Apps Installed	COMMUNITY ANALYTICS	Windows App Updates
MOBILE SECURITY	Mobile Metrics	
Security Overview		
Browser Violations		
MOBILE EXPENSE MANAGEMENT		
Data Usage Overview		
Data Usage Analysis		

Note: The reports that appear on the Reports tab depend on the products you have purchased. The list you see may be different than what is shown in this document.

Separate reports in each family appear on tabs.



There are filters at the screen to help you manage your data:

- Personal

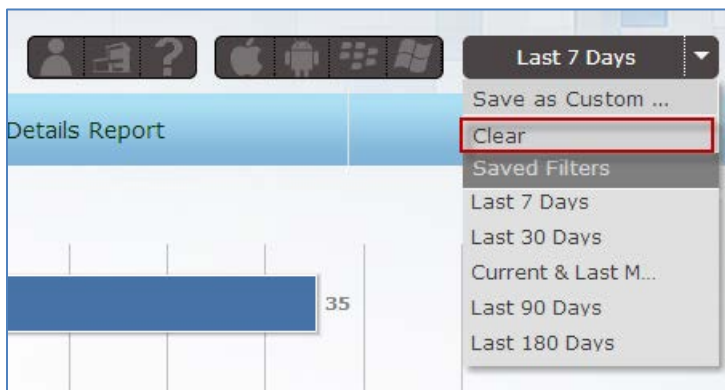
- Corporate owned
- Unspecified
- iOS
- Android
- BlackBerry
- Windows Phone
- Time period




You can save your filter so you can use it again. Click **Save as Custom**, and then enter a name and description for it.

The 'Save Filters' dialog box is shown. It has two input fields: 'Name' with a placeholder 'Max 25 characters' and 'Description' with a placeholder 'Max 255 characters'. At the bottom are 'Cancel' and 'Ok' buttons.

*Note: The filter you select for one report in a family is retained for the other reports until you clear it by clicking **Clear** on the pull-down menu.*



You can subscribe to reports by clicking .

You can specify the graphs and reports included in the subscription, the format (PDF or PPT), the email recipients, the delivery frequency and more.

You can mouse over part of a graph to see the details about it. For example, the following shows that out of the 7 Android devices, 3 are tablets:



If you click on it, MaaS360 displays the **Details Report** filtered to show information about those tablets:

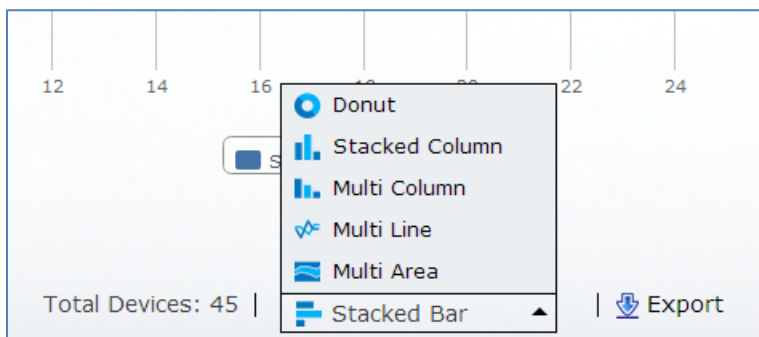
MDM Overview

Platform Managed Status Ownership New Devices by Month Details Report

Device Name	Username	Phone Number	Platform	Device Type	Ownership	Managed By	Managed Status	Install Date	Last Reported
ecarl-Kindle Fire	ecarl		Android	Tablet	Employee Owned	Agent	Enrolled	10/24/2012	05/19/2013
jhog-Nexus 7	jhog		Android	Tablet	Corporate Owned	Agent	Enrolled	04/30/2013	05/19/2013
skart-Nexus 7	skart		Android	Tablet	Corporate Owned	Agent	Enrolled	04/23/2013	05/19/2013

The active filters are highlighted (yellow) for the associated columns.

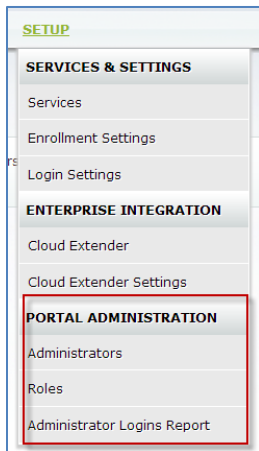
You can choose the type of chart by selecting it from the menu at the bottom of the page.



You can also download the report by clicking **Export**.

Platform Administration

Important administration tasks appear under the Portal Administration section of the **Setup** menu.



Administrators

To find or create a portal administrator, select **Setup > Administrators**.

The Search Administrators screen appears.

A screenshot of the 'Search Administrators' screen. At the top, there is a header bar with the title 'Search Administrators' and an 'Add Administrator' button. Below the header, there is a light blue box containing instructions: '1. Enter Corporate Username, Corporate Email Address or Select a Role to "Search" for existing administrators, or leave blank to Search for all.' and '2. Click the "Add Administrator" button to access the Add Administrator workflow.' Below the instructions, there are three input fields: 'Corporate Username', 'Corporate Email Address', and a 'Role' pull-down menu with a dropdown arrow. To the right of these fields is a 'Search' button.

To find an administrator, enter one or more of the following:

- Username
- Email address
- Select a role from the pull-down menu

Click **Search**.

If you do not enter any of the criteria, all administrators will be displayed.
















Search Administrators Add Administrator

1. Enter Corporate Username, Corporate Email Address or Select a Role to "Search" for existing administrators, or leave blank to Search for all.
2. Click the "Add Administrator" button to access the Add Administrator workflow.






Corporate Username:
Corporate Email Address: Role:

Search

Search Results

Email	Username	Roles	Managed User Groups	Actions
scad@fiberlink.com	1000000_sca	Software Distribution Administrator Security Manager Prospect Administrator Portal Administrator PSS Administrator IT Administrator Master Administrator Doc Mgmt DZ DZ Read Only App Management Admin-View on Groups only Helpdesk Engineer	All Groups	    
jray@fiberlink.com	1000000_jray	Master Administrator Service Administrator Helpdesk Engineer	All Groups	    
ha@fiberlink.com	1000000_ha	Master Administrator	All Groups	    

The Actions icons apply to the administrator.

	Edit the administrator's information or roles.
	Reset the administrator's password.
	Deactivate the administrator.
	Delete the administrator.
	View the change history for the administrator.


Create Portal Administrator

To create a new portal administrator:

Click **Add Administrator** at the top of the screen. The **Administrator Details** screen appears.

Administrator Details

Customer is responsible for maintaining the confidentiality of all user and administrative accounts. Authorization for any and all activities within this site are the responsibility of the customer. Customer shall provide prompt notification of any unauthorized use of this site.

Corporate Email Address*: 
Username*: ☐ same as Corporate Email Address

Next

Enter the administrator's email address and username. If the username will be the same as the email address, click the same as **Corporate Email Address** checkbox.

Click **Next**.

Assign Roles

☐ Limit portal administrator access to specified Managed User Groups

Role*

- Admin-View on Groups only
- Administrator
- Administrator - Level 2
- App Management
- Content Manager Test
- D2 Read Only
- Doc Management
- Doc Mgmt D2
- Doc Administrator
- Help Desk
- Helpdesk Engineer
- IT Administrator
- Master Administrator
- NLDH Test
- POC Customers

Role Description

This is a standard role that enables associated users with capability to view Invoices and Billing reports.

Next

Click to select one or more roles to assign to the new user. When you click to select a role, the role description appears in the **Role Description** field.

Note: A MaaS360 Portal Administrator can create Administrator accounts only with equal or lesser access rights. For example, an administrator who is assigned the Help Desk role can only create Help Desk accounts, but will be unable to create an account with more access rights (such as the Administrator).

Click the arrow buttons to move selected options or all options between the fields.

	Assign all the roles to the new administrator.
	Assign the highlighted role to the new administrator.
	Remove the highlighted role from the assignment.
	Remove all roles from the assignment.

Click **Limit portal administrator access to the specified Managed User Groups** if you do not want the user to have access to any other areas in MaaS360. **Note:** This is part of Departmentalization, a separate feature. For details, contact your account representative.

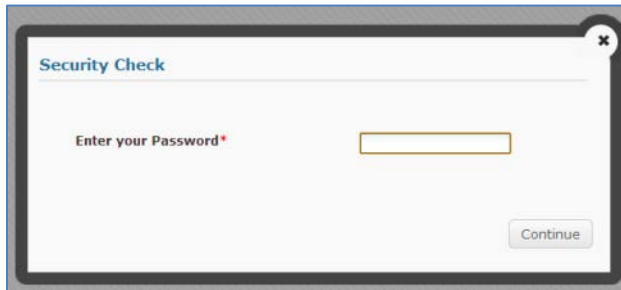
Click **Next**. The **Review Details** screen is displayed.

Review Details

Username: test12@fiberlink.com
Email Address: test12@fiberlink.com
Assigned Role(s): 1. App Management
2. Finance Manager

Save

Click **Save**. You will be asked for your password.

A screenshot of a 'Security Check' dialog box. It has a title bar with a close button (X). Inside, the text 'Enter your Password*' is followed by a password input field. At the bottom right is a 'Continue' button.

Enter your password and click **Continue**.

A screenshot of a confirmation message titled 'Administrator Created'. The text states: 'Portal Administrator Account - test12@fiberlink.com - has been successfully created. An email has been sent to the registered email address with the account details and temporary credentials to log into the portal.' At the bottom right is a button labeled 'Create Another Administrator'.

You will receive a confirmation message. You can now click **Create Another Administrator** to perform the process again.

Roles and Rights

There are a number of roles in MaaS360:

- **Read-Only:** The Read-Only role provides view-only access to all devices, policies, and applications. The Read-Only role also allows the administrator to view reports, My Alert Center, devices, policies, and the Action History report in the MaaS360 System.
- **Help Desk:** The Help Desk role provides the administrator with access rights to perform Help Desk device management actions that include locating an end-user device, sending messages or alerts to the end-user device, lock a device, or reset device passcode. The Help Desk role also allows the administrator to view My Alert Center, view policies and reports, manage device enrollments, edit device views, perform remote control and help desk actions.
- **Administrator:** In addition to the access rights of the Read-Only role, the Administrator role provides access rights to perform device management actions on end-user devices. The Administrator role allows you to view My Alert Center, view reports and policies and also manage device enrollments, edit device view, perform policy actions, perform remote control, wipe data on a mobile device, send messages to end-user devices and perform device deactivation actions.
- **Administrator Level 2:** The Administrator Level 2 role provides the Administrator with complete device management access rights that include the ability to create and manage policies and applications, The Administrator Level 2 role also allows you to view reports, and My Alert Center, manage device enrollments, perform device view bulk updates, define custom attributes, manage MaaS360 Cloud Extenders, perform group level actions, and view and publish policies in MaaS360 system.
- **MaaS360 Service Administrator:** The MaaS360 Service Administrator role provides the administrator with Master Administrator level access rights that include the ability to configure services and manage administrator accounts. The MaaS360 Service Administrator role also allows the administrator to view reports and Alert Center notifications, manage device enrollments,

perform device view bulk updates, define Custom Attributes, manage MaaS360 Cloud Extenders, perform group level actions, publish policies, and Configure Services.

<u>Role</u>	<u>Right to Access</u>	<u>Category</u>	<u>Description</u>
Administrator	Apps - Read only	App Distribution	View only access to Apps.
	Action History	Device Management	Ability to view a global action history across all devices.
	Buzz Device	Device Management	Ability to buzz a device through a Device View action.
	Change Compliance Rule Set	Device Management	Ability to change a compliance rule set through a Device View action.
	Change Device Policy	Device Management	Ability to change a device policy through a Device View action.
	Change Expense Mgmt Plan	Device Management	Ability to change a mobile expense management plan through a Device View action.
	Deactivate Device	Device Management	Ability to remove MDM control or hide devices through a Device View action.
	Device Enrollments - Read only	Device Management	View only access to device enrollment requests.
	Device View - Read only	Device Management	View only access to Device View (no actions).
	Distribute App for a device	Device Management	Ability to distribute an app through a Device View action.
	Distribute Doc for a device	Device Management	Ability to distribute a doc through a Device View action.
	Enable Alerts	Device Management	Enable Alerts for Enterprise Customers.
	Locate Device	Device Management	Ability to locate a device through a Device View action.
	Lock Device	Device Management	Ability to lock a device through a Device View action.
	Manage Device Enrollments	Device Management	Ability to manage device enrollment requests.
	Merge Duplicate Device Records	Device Management	Ability to manually merge Android or Windows Phone 7 device records if automated merge cannot identify the devices to merge.
	Refresh Device Information	Device Management	Ability to issue an on-demand refresh for all information about the device through a Device View action.
	Reset Device Passcode	Device Management	Ability to reset the device passcode through a Device View action.
	Selective Wipe	Device Management	Ability to selectively wipe (restrict) corporate data from a device and revoke the selective wipe from a device through a Device View action.
	Send Message	Device Management	Ability to send a message to a device through a Device View action.
	Set Custom Attribute Value	Device Management	Ability to set custom attribute values through a Device View action.
	User Views - Generate Password	Device Management	Ability to generate passwords for users through the View All Users workflow.
	Users - Read only	Device Management	View only access to User View.
	View Custom Attributes	Device Management	View only access to custom attributes.
	Wipe Device	Device Management	Ability to wipe the device or canceling pending wipe action through a Device View action.
	Docs - Read only	Doc Distribution	View only access to Docs.
	Manage Document Settings	Doc Distribution	Ability to modify Document settings
	Expense Mgmt Plans - Read only	Expense Management	View only access to Expense Mgmt Plans.

<u>Role</u>	<u>Right to Access</u>	<u>Category</u>	<u>Description</u>
	Mobile Metrics - View and Propose new ideas	Mobile Analytics	View only access to Mobile Metrics graphs and ability to propose new ideas.
	Manage Policies - Read only	Policy Management	View only access to Policies.
	Reports	Reports	Ability to view graphs and reports in the Reports tab
Administrator - Level 2	Manage Apps	App Distribution	Ability to add, change or delete Apps.
	Action History	Device Management	Ability to view a global action history across all devices.
	Bulk Upload Custom Attributes	Device Management	Ability to bulk upload a file to set custom attributes.
	Buzz Device	Device Management	Ability to buzz a device through a Device View action.
	Change Compliance Rule Set	Device Management	Ability to change a compliance rule set through a Device View action.
	Change Device Policy	Device Management	Ability to change a device policy through a Device View action.
	Change Expense Mgmt Plan	Device Management	Ability to change a mobile expense management plan through a Device View action.
	Deactivate Device	Device Management	Ability to remove MDM control or hide devices through a Device View action.
	Device Enrollments - Read only	Device Management	View only access to device enrollment requests.
	Device Group actions	Device Management	Ability to push actions at a group level.
	Device View - Read only	Device Management	View only access to Device View (no actions).
	Distribute App for a device	Device Management	Ability to distribute an app through a Device View action.
	Distribute Doc for a device	Device Management	Ability to distribute a doc through a Device View action.
	Enable Alerts	Device Management	Enable Alerts for Enterprise Customers.
	Locate Device	Device Management	Ability to locate a device through a Device View action.
	Lock Device	Device Management	Ability to lock a device through a Device View action.
	Manage Cloud Extenders	Device Management	Ability to manage Cloud Extenders.
	Manage Custom Attributes	Device Management	Ability to add, change or delete Custom Attributes.
	Manage Device Enrollments	Device Management	Ability to manage device enrollment requests.
	Merge Duplicate Device Records	Device Management	Ability to manually merge Android or Windows Phone 7 device records if automated merge cannot identify the devices to merge.
	Refresh Device Information	Device Management	Ability to issue an on-demand refresh for all information about the device through a Device View action.
	Remove App	Device Management	Ability to remove an app through a Device View action.
	Reset Device Passcode	Device Management	Ability to reset the device passcode through a Device View action.
	Selective Wipe	Device Management	Ability to selectively wipe (restrict) corporate data from a device and revoke the selective wipe from a device through a Device View action.
	Send Message	Device Management	Ability to send a message to a device through a Device View action.
	Set Custom Attribute Value	Device Management	Ability to set custom attribute values through a Device View action.

<u>Role</u>	<u>Right to Access</u>	<u>Category</u>	<u>Description</u>
	User Views - Generate Password	Device Management	Ability to generate passwords for users through the View All Users workflow.
	Users - Read only	Device Management	View only access to User View.
	Wipe Device	Device Management	Ability to wipe the device or canceling pending wipe action through a Device View action.
	Manage Docs	Doc Distribution	Ability to add, change or delete Docs.
	Manage Document Settings	Doc Distribution	Ability to modify Document settings
	Manage Expense Mgmt Plans	Expense Management	Ability to add, change or delete expense mgmt plans.
	Mobile Metrics - View and Propose new ideas	Mobile Analytics	View only access to Mobile Metrics graphs and ability to propose new ideas.
	Manage Policies	Policy Management	Ability to add, change, delete and publish policies.
	Reports	Reports	Ability to view graphs and reports in the Reports tab
Help Desk	Apps - Read only	App Distribution	View only access to Apps.
	Action History	Device Management	Ability to view a global action history across all devices.
	Buzz Device	Device Management	Ability to buzz a device through a Device View action.
	Device Enrollments - Read only	Device Management	View only access to device enrollment requests.
	Device View - Read only	Device Management	View only access to Device View (no actions).
	Enable Alerts	Device Management	Enable Alerts for Enterprise Customers.
	Locate Device	Device Management	Ability to locate a device through a Device View action.
	Lock Device	Device Management	Ability to lock a device through a Device View action.
	Manage Device Enrollments	Device Management	Ability to manage device enrollment requests.
	Merge Duplicate Device Records	Device Management	Ability to manually merge Android or Windows Phone 7 device records if automated merge cannot identify the devices to merge.
	Refresh Device Information	Device Management	Ability to issue an on-demand refresh for all information about the device through a Device View action.
	Reset Device Passcode	Device Management	Ability to reset the device passcode through a Device View action.
	Send Message	Device Management	Ability to send a message to a device through a Device View action.
	Set Custom Attribute Value	Device Management	Ability to set custom attribute values through a Device View action.
	User Views - Generate Password	Device Management	Ability to generate passwords for users through the View All Users workflow.
	Users - Read only	Device Management	View only access to User View.
	Docs - Read only	Doc Distribution	View only access to Docs.
	Manage Document Settings	Doc Distribution	Ability to modify Document settings
	Expense Mgmt Plans - Read only	Expense Management	View only access to Expense Mgmt Plans.
	Mobile Metrics - View and Propose new ideas	Mobile Analytics	View only access to Mobile Metrics graphs and ability to propose new ideas.
	Manage Policies - Read only	Policy Management	View only access to Policies.
	Reports	Reports	Ability to view graphs and reports in the Reports tab.

<u>Role</u>	<u>Right to Access</u>	<u>Category</u>	<u>Description</u>
Read Only	Apps - Read only	App Distribution	View only access to Apps.
	Action History	Device Management	Ability to view a global action history across all devices.
	Device Enrollments - Read only	Device Management	View only access to device enrollment requests.
	Device View - Read only	Device Management	View only access to Device View (no actions).
	Enable Alerts	Device Management	Enable Alerts for Enterprise Customers.
	Refresh Device Information	Device Management	Ability to issue an on-demand refresh for all information about the device through a Device View action.
	Users - Read only	Device Management	View only access to User View.
	Docs - Read only	Doc Distribution	View only access to Docs.
	Manage Document Settings	Doc Distribution	Ability to modify Document settings.
	Expense Mgmt Plans - Read only	Expense Management	View only access to Expense Mgmt Plans.
	Mobile Metrics - Read only	Mobile Analytics	View only access to view Mobile Metrics graphs.
	Manage Policies - Read only	Policy Management	View only access to Policies.
	Reports	Reports	Ability to view graphs and reports in the Reports tab.
Service Administrator	Manage Administrator Roles	Administrator Management	Ability to create & manage Roles. Additionally, ability to create & manage admins.
	Manage Apps	App Distribution	Ability to add, change or delete Apps.
	Bulk Upload Custom Attributes	Device Management	Ability to bulk upload a file to set custom attributes.
	Buzz Device	Device Management	Ability to buzz a device through a Device View action.
	Change Compliance Rule Set	Device Management	Ability to change a compliance rule set through a Device View action.
	Change Device Policy	Device Management	Ability to change a device policy through a Device View action.
	Change Expense Mgmt Plan	Device Management	Ability to change a mobile expense management plan through a Device View action.
	Deactivate Device	Device Management	Ability to remove MDM control or hide devices through a Device View action.
	Device Enrollments - Read only	Device Management	View only access to device enrollment requests.
	Device Group actions	Device Management	Ability to push actions at a group level.
	Device View - Read only	Device Management	View only access to Device View (no actions).
	Distribute App for a device	Device Management	Ability to distribute an app through a Device View action.
	Distribute Doc for a device	Device Management	Ability to distribute a doc through a Device View action.
	Enable Alerts	Device Management	Enable Alerts for Enterprise Customers.
	Locate Device	Device Management	Ability to locate a device through a Device View action.
	Lock Device	Device Management	Ability to lock a device through a Device View action.
	Manage Cloud Extenders	Device Management	Ability to manage Cloud Extenders.
	Manage Custom Attributes	Device Management	Ability to add, change or delete Custom Attributes.

<u>Role</u>	<u>Right to Access</u>	<u>Category</u>	<u>Description</u>
	Manage Device Enrollments	Device Management	Ability to manage device enrollment requests.
	Manage Users	Device Management	Ability to manage users.
	Merge Duplicate Device Records	Device Management	Ability to manually merge Android or Windows Phone 7 device records if automated merge cannot identify the devices to merge.
	Refresh Device Information	Device Management	Ability to issue an on-demand refresh for all information about the device through a Device View action.
	Remove App	Device Management	Ability to remove an app through a Device View action.
	Reset Device Passcode	Device Management	Ability to reset the device passcode through a Device View action.
	Selective Wipe	Device Management	Ability to selectively wipe (restrict) corporate data from a device and revoke the selective wipe from a device through a Device View action.
	Send Message	Device Management	Ability to send a message to a device through a Device View action.
	Set Custom Attribute Value	Device Management	Ability to set custom attribute values through a Device View action.
	User Views - Generate Password	Device Management	Ability to generate passwords for users through the View All Users workflow.
	Users - Read only	Device Management	View only access to User View.
	Wipe Device	Device Management	Ability to wipe the device or canceling pending wipe action through a Device View action.
	Manage Docs	Doc Distribution	Ability to add, change or delete Docs.
	Manage Document Settings	Doc Distribution	Ability to modify Document settings.
	Manage Sharepoint Settings	Doc Distribution	Ability to modify Sharepoint settings.
	Manage Policies	Policy Management	Ability to add, change, delete and publish policies.
	Reports	Reports	Ability to view graphs and reports in the Reports tab.
	Convert to Customer	Service Configuration	Restrict the visibility of account as Convert to Customer.
	Expire Account	Service Configuration	Restrict the visibility of account as Expire Account.
	Extend Trial	Service Configuration	Restrict the visibility of account as Extend Trial.
	Read-Only Account	Service Configuration	Restrict the visibility of account as Read-Only Account.
	Services Configuration	Service Configuration	Ability to enable additional services through checklist workflow.

Creating a Role

Administrators can create roles, but only with the access privileges they possess (or with fewer privileges).

To create a role, mouse over **Setup** and select **Roles**.

SETUP

SERVICES & SETTINGS

Services

Enrollment Settings

Login Settings

ENTERPRISE INTEGRATION

Cloud Extender

Cloud Extender Settings

PORTAL ADMINISTRATION

Administrators

Roles

Administrator Logins Report

Click **Add Role**.

Manage Role Add Role

Select an existing Role from the list (or Add a new Role) to continue

Role* ---Select---

Delete Change history Edit

Enter the role's name and a description. You can either create a new role or copy an existing one to use as a model.

Basic Information

1. Basic Information

Role Name*

Role Description*

2. Select Mode of Creation

Select From Existing ---Select---

Create new ---Select---

Next

Creating a Role Based on an Existing Role

If you want to use an existing one, select it from the pull-down menu and then click **Next**.

2. Select Mode of Creation

Select From Existing Administrator - Level 2

Create new ---Select---

Next

The access rights for that role are already selected. You can make your changes, and then click **Save**.

Grant Access Rights		
Right To Access	Category	Description
<input type="checkbox"/> Manage Administrator Roles	Administrator Management	Ability to create & manage Roles. Additionally, ability to create & manage admins.
<input type="checkbox"/> Manage Administrators	Administrator Management	Ability to create & manage admins.
<input type="checkbox"/> Apps - Read only	App Distribution	View only access to Apps.
<input type="checkbox"/> Distribute Apps	App Distribution	Ability to distribute Apps.
<input type="checkbox"/> Manage Apps	App Distribution	Ability to add, change or delete Apps.
<input type="checkbox"/> Action History	Device Management	Ability to view a global action history across all devices.
<input type="checkbox"/> Approve Device	Device Management	Ability to approve a blocked or quarantined device (ActiveSync/Traveler).
<input type="checkbox"/> Block Device	Device Management	Ability to block an approved or quarantined device (ActiveSync/Traveler).
<input type="checkbox"/> Bulk Upload Custom Attributes	Device Management	Ability to bulk upload a file to set custom attributes.
<input type="checkbox"/> Buzz Device	Device Management	Ability to buzz a device through a Device View action.
<input type="checkbox"/> Change Compliance Rule Set	Device Management	Ability to change a compliance rule set through a Device View action.
<input type="checkbox"/> Change Device Policy	Device Management	Ability to change a device policy through a Device View action.
<input type="checkbox"/> Change Expense Mgmt Plan	Device Management	Ability to change a mobile expense management plan through a Device View action.
<input type="checkbox"/> Deactivate Device	Device Management	Ability to remove MDM control or hide a devices through a Device View action.
<input type="checkbox"/> Device Enrollments - Read only	Device Management	View only access to device enrollment requests.
<input type="checkbox"/> Device Group actions	Device Management	Ability to push actions at a group level.
<input type="checkbox"/> Device View - Read only	Device Management	View only access to Device View (no actions).
<input type="checkbox"/> Device View-View All Devices	Device Management	Device View access restricted to View All Devices (no access to actions or smart search).
<input type="checkbox"/> Distribute App for a device	Device Management	Ability to distribute an app through a Device View action.
<input type="checkbox"/> Distribute Doc for a device	Device Management	Ability to distribute a doc through a Device View action.
<input type="checkbox"/> Enable Watchlist	Device Management	Enable Watchlist for Enterprise Customers.
<input type="checkbox"/> Locate Device	Device Management	Ability to locate a device through a Device View action.
<input type="checkbox"/> Lock Device	Device Management	Ability to lock a device through a Device View action.
<input type="checkbox"/> Manage Cloud Extenders	Device Management	Ability to manage Cloud Extenders.
<input type="checkbox"/> Manage Custom Attributes	Device Management	Ability to add, change or delete Custom Attributes.
<input type="checkbox"/> Manage Device Enrollments	Device Management	Ability to manage device enrollment requests.
<input type="checkbox"/> Manage Users	Device Management	Ability to manage users.

Creating a New Role Without Using a Model

If you choose not to use an existing role as a model, select Create new and then click Next.

2. Select Mode of Creation

Select From Existing ☐ ---Select---
Create new ☒ ---Select---

Next

On the Grant Access Rights screen none of the access rights will be selected.

Grant Access Rights		
Right To Access	Category	Description
<input type="checkbox"/> Manage Administrator Roles	Administrator Management	Ability to create & manage Roles. Additionally, ability to create & manage admins.
<input type="checkbox"/> Manage Administrators	Administrator Management	Ability to create & manage admins.
<input type="checkbox"/> Apps - Read only	App Distribution	View only access to Apps.
<input type="checkbox"/> Distribute Apps	App Distribution	Ability to distribute Apps.
<input type="checkbox"/> Manage Apps	App Distribution	Ability to add, change or delete Apps.
<input type="checkbox"/> Action History	Device Management	Ability to view a global action history across all devices.
<input type="checkbox"/> Approve Device	Device Management	Ability to approve a blocked or quarantined device (ActiveSync/Traveler).
<input type="checkbox"/> Block Device	Device Management	Ability to block an approved or quarantined device (ActiveSync/Traveler).
<input type="checkbox"/> Bulk Upload Custom Attributes	Device Management	Ability to bulk upload a file to set custom attributes.
<input type="checkbox"/> Buzz Device	Device Management	Ability to buzz a device through a Device View action.
<input type="checkbox"/> Change Compliance Rule Set	Device Management	Ability to change a compliance rule set through a Device View action.
<input type="checkbox"/> Change Device Policy	Device Management	Ability to change a device policy through a Device View action.
<input type="checkbox"/> Change Expense Mgmt Plan	Device Management	Ability to change a mobile expense management plan through a Device View action.
<input type="checkbox"/> Deactivate Device	Device Management	Ability to remove MDM control or hide a devices through a Device View action.
<input type="checkbox"/> Device Enrollments - Read only	Device Management	View only access to device enrollment requests.
<input type="checkbox"/> Device Group actions	Device Management	Ability to push actions at a group level.
<input type="checkbox"/> Device View - Read only	Device Management	View only access to Device View (no actions).
<input type="checkbox"/> Device View-View All Devices	Device Management	Device View access restricted to View All Devices (no access to actions or smart search).
<input type="checkbox"/> Distribute App for a device	Device Management	Ability to distribute an app through a Device View action.
<input type="checkbox"/> Distribute Doc for a device	Device Management	Ability to distribute a doc through a Device View action.
<input type="checkbox"/> Enable Watchlist	Device Management	Enable Watchlist for Enterprise Customers.
<input type="checkbox"/> Locate Device	Device Management	Ability to locate a device through a Device View action.
<input type="checkbox"/> Lock Device	Device Management	Ability to lock a device through a Device View action.
<input type="checkbox"/> Manage Cloud Extenders	Device Management	Ability to manage Cloud Extenders.
<input type="checkbox"/> Manage Custom Attributes	Device Management	Ability to add, change or delete Custom Attributes.
<input type="checkbox"/> Manage Device Enrollments	Device Management	Ability to manage device enrollment requests.
<input type="checkbox"/> Manage Users	Device Management	Ability to manage users.

Select the rights you want to grant to the role, and then click Save.

Managing Roles

To change, delete or view a history of changes that were made to a custom role, mouse over **Setup** and select **Roles**.

View Changes

Legend: Modified Fields New Value Original Value

Role Name	test
Role Description	test
Access Rights	Action History Approve Device Billing Reports Block Device Bulk Upload Custom Attributes Change Compliance Rule Set Change Device Policy Change Expense Mgmt Plan Deactivate Device Device Enrollments - Read only

If you want to edit a role, click the **Edit** button on the **Manage Role** screen.

Manage Role Add Role

Select an existing Role from the list (or Add a new Role) to continue

Role*

Role Description*

Delete Change History Edit

The existing rights will be selected. Make your changes and click **Save**.

Grant Access Rights

Right To Access	Category	Description
<input checked="" type="checkbox"/> Manage Administrator Roles	Administrator Management	Ability to create & manage Roles. Additionally, ability to create & manage admins.
<input checked="" type="checkbox"/> Manage Administrators	Administrator Management	Ability to create & manage admins.
<input checked="" type="checkbox"/> Apps - Read only	App Distribution	View only access to Apps.
<input checked="" type="checkbox"/> Distribute Apps	App Distribution	Ability to distribute Apps.
<input checked="" type="checkbox"/> Manage Apps	App Distribution	Ability to add, change or delete Apps.
<input checked="" type="checkbox"/> Action History	Device Management	Ability to view a global action history across all devices.
<input checked="" type="checkbox"/> Approve Device	Device Management	Ability to approve a blocked or quarantined device (ActiveSync/Traveler).
<input checked="" type="checkbox"/> Block Device	Device Management	Ability to block an approved or quarantined device (ActiveSync/Traveler).
<input checked="" type="checkbox"/> Bulk Upload Custom Attributes	Device Management	Ability to bulk upload a file to set custom attributes.
<input checked="" type="checkbox"/> Buzz Device	Device Management	Ability to buzz a device through a Device View action.
<input checked="" type="checkbox"/> Change Compliance Rule Set	Device Management	Ability to change a compliance rule set through a Device View action.
<input checked="" type="checkbox"/> Change Device Policy	Device Management	Ability to change a device policy through a Device View action.
<input checked="" type="checkbox"/> Change Expense Mgmt Plan	Device Management	Ability to change a mobile expense management plan through a Device View action.
<input checked="" type="checkbox"/> Deactivate Device	Device Management	Ability to remove MDM control or hide a devices through a Device View action.
<input checked="" type="checkbox"/> Device Enrollments - Read only	Device Management	View only access to device enrollment requests.
<input checked="" type="checkbox"/> Device Group actions	Device Management	Ability to push actions at a group level.
<input checked="" type="checkbox"/> Device View - Read only	Device Management	View only access to Device View (no actions).
<input checked="" type="checkbox"/> Device View-View All Devices	Device Management	Device View access restricted to View All Devices (no access to actions or smart search).
<input checked="" type="checkbox"/> Distribute App for a device	Device Management	Ability to distribute an app through a Device View action.
<input checked="" type="checkbox"/> Enable Watchlist	Device Management	Enable Watchlist for Enterprise Customers.
<input checked="" type="checkbox"/> Locate Device	Device Management	Ability to locate a device through a Device View action.
<input checked="" type="checkbox"/> Lock Device	Device Management	Ability to lock a device through a Device View action.
<input checked="" type="checkbox"/> Manage Cloud Extenders	Device Management	Ability to manage Cloud Extenders.
<input checked="" type="checkbox"/> Manage Custom Attributes	Device Management	Ability to add, change or delete Custom Attributes.
<input checked="" type="checkbox"/> Manage Device Enrollments	Device Management	Ability to manage device enrollment requests.
<input checked="" type="checkbox"/> Manage Users	Device Management	Ability to manage users.

Save

Administrator Logins Report

Mouse over **Setup** and click **Administrator Logins Report**.

The **Search Criteria** screen appears.

Search Criteria

Username

IP Address

Login Date

Authentication Status ---Select---

Search

Enter a username, IP address, login date range or authentication status. If you do not enter any criteria, all the logins will be listed.

Click **Search**.

Search Criteria

Username

IP Address

Login Date

Authentication Status

---Select---

Search

Search Results

Username	Login Attempt Time (GMT)	Logout Time (GMT)	Duration (Minutes)	Operating System	Browser Version	IP Address	Authentication Status
1037114_bb	06/07/2013 06:14 PM	06/07/2013 06:15 PM	.2	Windows Seven NT 6.1	Internet Explorer	013.15.013.15	Successful
1037114_bb	06/06/2013 06:34 PM	06/06/2013 09:21 PM	167	Windows Seven NT 6.1	Chrome 27.0.1453.94	013.15.013.15	Successful
1037114_bb	06/06/2013 06:00 PM	06/06/2013 06:08 PM	7.5	Windows Seven NT 6.1	Internet Explorer	013.15.013.15	Successful
1037114_bb	06/06/2013 03:00 PM	06/06/2013 03:56 PM	56	Windows Seven NT 6.1	Internet Explorer	013.15.013.15	Successful

Jump

Page 1 of 1 | Displaying records 1 to 4 | Total records 4

[CSV](#)
[XLS](#)
[XML](#)

Appendix A: Features List

Device Support

	Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Cloud Extender		
Android 2.2+	✓	✓	
Android 3.x	✓	✓	
Android 4.x	✓	✓	
BlackBerry OS 4	✓		✓
BlackBerry OS 5	✓		✓
BlackBerry OS 6	✓		✓
BlackBerry OS 7	✓		✓
BlackBerry OS 10	✓		✓
iOS 4.x (iPhone, iPad, and iPod Touch)	✓	✓	
iOS 5.x (iPhone, iPad, and iPod Touch)	✓	✓	
iOS 6.x (iPhone, iPad, and iPod Touch)	✓	✓	
iOS 7 (iPhone, iPad, and iPod Touch)	✓	✓	
iOS V3.x (iPhone, iPad, and iPod Touch)	✓		

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
	✓	✓					
	✓						
	✓	✓					
✓							
✓							
✓							
✓							Day 0 support on GA of iOS 7

	Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Cloud Extender		
Mac OS X Tiger, Lion, Mountain Lion			
QNX	✓		
Symbian (Nokia)	✓	✓	
WebOS	✓		
Windows Mobile 6.1	✓	✓	
Windows Mobile 6.5	✓	✓	
Windows Phone 7	✓		
Window Phone 7.5 (Mango)	✓		
Windows Phone 8	✓		
Windows XP, Vista, 7			
Windows 8	✓		

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
						✓	
			✓				
				✓			
					✓		
					✓		

Activation and Enrollment

	Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Cloud Extender		
AD Authenticated Enrollment			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
✓	✓	✓	✓	✓	✓	✓	

	Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Cloud Extender		
Agent based			
Bulk enrollment			✓
Certificate based			
Enrolled when Exchange Email is configured on Device	✓	✓	
Push MDM Profiles OTA			
Unattended Enrollment workflow			✓
Web Based Enrollment (no app required)			✓

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
	✓	✓	✓		✓		
✓	✓	✓	✓	✓	✓		
✓							
✓				✓		✓	
✓	✓	✓	✓	✓	✓		*AD Required
✓				✓			

Device Attributes

Hardware Attributes

	Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Cloud Extender		
Activation Date			
ActiveSync Agent	✓		
ActiveSync Device ID	✓	✓	
ActiveSync GUID	✓		
ActiveSync Identity	✓		

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
✓	✓	✓	✓	✓	✓		
				✓			

	Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Cloud Extender		
API Level			
Apple Serial Number			
Application Data			
Baseband Version			
Battery Condition			
Battery Level			✓
BES Server			✓
BIOS Date			
BIOS Serial Number			
Build Number			
CD/DVD Name			
Default Language	✓		
Device Serial Number/PIN			✓
Email Address	✓	✓	✓
File System Type			
Free External Storage			
Free Internal Storage			✓
IMEI/ESN			✓
Installed/Activation Date	✓	✓	✓
Kernel Version			
Last Reported	✓	✓	✓
Managed Status	✓	✓	✓
Manufacturer	✓	✓	✓

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
✓	✓	✓					
✓						✓	
✓	✓	✓					
	✓	✓					
	✓	✓					
✓	✓	✓					
					✓		
					✓		
✓	✓	✓					
					✓		
✓	✓	✓				✓	
✓	✓	✓	✓		✓		
					✓	✓	
	✓	✓					
✓	✓	✓		✓			
✓	✓	✓	✓		✓	✓	
	✓	✓					
✓	✓	✓	✓		✓	✓	
✓	✓	✓	✓		✓	✓	
✓	✓	✓	✓	✓	✓	✓	

	Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Cloud Extender		
Microsoft Auto-Update Status			
Model	/	/	/
Model ID			
Modem Firmware Version			/
Motherboard Serial Number			
Number of Drives			
Number of Processor Cores			
Operating System	/	/	/
Operating System Version			/
OS Architecture (32 vs. 64 bit)			
OS Edition			
OS Patches (Security and Others)			
Ownership	/	/	/
Platform Version			
Processor Name			
Processor Name			
Processor Speed			
RAM			
Screen Language			/
Screen Resolution			/
Screen Width			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
					/		
/	/	/	/	/	/	/	
/			/		/	/	
/			/	/			
					/		
					/		
	/	/					
/	/	/	/	/	/	/	
/	/	/	/	/	/	/	
					/	/	
					/	/	
/	/	/	/	/	/	/	
						/	
	/	/				/	
	/	/			/	/	
	/	/	/	/	/		
	/	/	/	/			
	/	/					

	Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Cloud Extender		
Secure Browser Policy			
Secured Boot ROM			✓
Service Pack			
Timezone			
Total External Storage			
Total Internal Storage			✓
UDID			
Username	✓	✓	✓
Volume Free Space			
Volume Label			
Volume Name			
Volume Size			
WMI Status			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
✓							
						✓	
					✓	✓	
	✓	✓			✓	✓	
	✓	✓			✓		
✓	✓	✓				✓	
✓				✓		✓	
✓	✓	✓	✓		✓	✓	
					✓	✓	
					✓	✓	
					✓	✓	
					✓		

Network Attributes

	Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Cloud Extender		
Adapter ID			
Adapter Type			
BlackBerry Internet Service			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
					✓		
					✓	✓	

	Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Cloud Extender		
(BIS) Enabled			
Bluetooth Mac Address			
Carrier (Current)			✓
Carrier (Home)			✓
Carrier Setting Version			
Country (Current)			
Country (Home)			
Device Driver Date			
Device Driver Name			
Device Driver Version			
DHCP Enabled			
Direct Connect ID			✓
DNS Servers			
Gateway			
GPS Settings Enabled			
ICCID/IMSI			✓
International Data Roaming			
IP Address			
Last Connection Date - Wi-Fi			
Network Type (Current)			✓
Phone Number			✓
Roaming			
SSID			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
✓	✓						
✓	✓		✓	✓			
✓	✓						
✓							
✓	✓						
✓	✓						
					✓		
					✓		
					✓		
					✓	✓	
					✓	✓	
					✓	✓	
	✓						
✓	✓						
✓	✓						
✓	✓	✓			✓		
✓	✓	✓					
	✓		✓		✓		
✓	✓						
✓	✓						
✓	✓	✓					

	Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Cloud Extender		
Subnet Mask			
Supported Frequencies			✓
Wi-Fi Mac Address			
Personal Hotspot			
Do Not Disturb			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
					✓	✓	
✓	✓	✓		✓	✓	✓	
✓							iOS 7 onwards
✓							iOS 7 onwards

Location Attributes

	Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Cloud Extender		
Accuracy			
Checked in Location			
Checked in status			
Latitude			
Location (Address)			
Location History			
Longitude			
Timestamp of Location Detection			
Find My Device			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
✓	✓		✓	✓		✓	
✓	✓						
✓	✓						
✓	✓		✓	✓		✓	
✓	✓		✓	✓		✓	
✓						✓	
✓	✓		✓	✓		✓	
✓	✓		✓	✓		✓	
✓							iOS 7 onwards

Application Inventory

	Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Cloud Extender		
Application Bundle Size			
Application Dynamic Size			
Application ID			
Application Install Location			
Application Name			✓
Application Source			
Application Vendor			
Application Version			✓
Installation Date			
Provisioning Profile Expiry Date			
Provisioning Profile ID			
Provisioning Profile Name			
iTunes Account Present			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
✓	✓	✓		✓			
✓	✓	✓		✓			
✓	✓	✓		✓			
	✓	✓					
✓	✓	✓		✓	✓	✓	
✓				✓	✓		
				✓	✓		
✓	✓	✓		✓	✓	✓	
				✓	✓		
✓							
✓							
✓							
✓							iOS 7 onwards

Security and Compliance

	Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Cloud Extender		
ActiveSync Policy	/		
Allow installation of Non-Market Apps			
Allow Mock Locations			
Anti-Spyware Details			
Anti-Virus Details			
App Compliance State			
Auto-Backup Configured			/
Auto-Backup Exclusions			/
Auto-Backup Frequency			/
Auto-Sync Enabled			
Automatic Data Backup to Google Servers Enabled			
Automatic Restore from Data Backup on Application Reinstall			
Background Data Sync Enabled			
Backup and Recovery			
Bluetooth Enabled			
Camera Present			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
	/	/				/	
	/						
					/		
					/	/	
/	/	/					
/							
/	/	/					
	/						
	/						
	/						
					/		
	/						
	/						

	Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Cloud Extender		
Certificates			
Configuration Profile Name			
Configurator Supervised Mode			
Data Encryption			
Data Leak Protection			
Device Passcode Status	✓	✓	✓
Device Rooted			
Device Wiped			
Failed Settings			
GPS Present			
Hardware Encryption			✓
Jailbreak Detection			
Last MDM Policy Update Date			
Last MDM Policy Update Source			
Last Policy Updated Date	✓		
Last Selective Wipe Date			
Last Successful Backup Time			✓
Last Wipe Applied Date	✓	✓	
Mailbox Approval State	✓	✓	
Master Key Vulnerability status			
Maximum Failed Password Attempts			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
✓							
✓							
✓							
					✓	✓	
					✓		
✓	✓	✓		✓			
	✓	✓					
✓	✓	✓				✓	
✓							
	✓						
✓	✓			✓			
✓							
✓	✓	✓		✓		✓	
✓	✓	✓					
✓	✓	✓				✓	
✓	✓	✓				✓	
						✓	
✓	✓	✓		✓		✓	
✓							
	✓	✓					
✓	✓	✓				✓	

	Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Cloud Extender		
Maximum Passcode Age (days)			
Maximum Time to Lock (min)			
MDM or BES Policy			✓
Minimum Passcode Length			
NFC enabled			
Number of Special Characters			
Other Device Administration Solutions			
Out-of-Compliance Reasons			
Passcode History			
Passcode Quality			
Peripheral Protection			
Personal Firewall Details			
Policy Compliance State			✓
Policy Version			
Remote Wipe Support	✓	✓	
Restrictions Applied			
Rule Compliance State			
Rule Set Configured			
Secure Browser - Last Policy Update			
Secure Browser Policy			
Selective Wipe			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
	✓	✓					
✓	✓	✓				✓	
✓	✓	✓		✓		✓	
✓	✓	✓				✓	
	✓						
✓	✓	✓				✓	
	✓	✓					
✓	✓	✓		✓			
	✓	✓					
✓	✓	✓				✓	
					✓	✓	
					✓	✓	
✓	✓	✓					
✓	✓	✓				✓	
✓						✓	
✓	✓	✓				✓	
✓	✓	✓					
✓	✓	✓					
✓	✓	✓					
✓	✓	✓					
✓	✓	✓					

	Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Cloud Extender		
Settings configured			
Settings Failed to Configure			
Visible Passwords			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
	✓	✓					
✓	✓	✓					
	✓	✓					

Running Services

	Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Cloud Extender		
App ID			
Application Name			
Memory Used			
Running Time			
Service Name			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
	✓	✓					
	✓	✓			✓		
	✓	✓					
	✓	✓					
	✓	✓			✓		

MaaS360 Services

	Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise	iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
	Cloud Extender			Requires Native App on Device							
Advanced Device Management SDKs Enabled					✓						
App ID				✓	✓	✓					
Application Name				✓	✓	✓			✓		
BlackBerry Push Notification Registration Status											
BlackBerry Push Notification Status											
Company Hub								✓			
DTM Real-time Notification									✓		
Google Real-time Notification Registered					✓						
Installed Date					✓	✓	✓	✓	✓		
Installed Services				✓							
List of Modules with versions and activation time									✓		
MaaS360 Agent Version (Current)				✓	✓	✓	✓	✓	✓	✓	
MaaS360 Agent Version (Initial)											
MaaS360 Device ID				✓	✓	✓	✓	✓			

	Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Cloud Extender		
Microsoft Device Info Collection			
Microsoft Location Services			
Microsoft Push Notifications			
Primary Google Account			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
			✓	✓			
			✓	✓			
			✓	✓			
	✓						

Mobile Data Usage

	Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Cloud Extender		
Daily Mobile Data Usage (Current Period)			
First day of the Billing cycle			
Monthly aggregate Mobile Data Usage			
Plan Name			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
✓	✓						
✓	✓						
✓	✓						
✓	✓						

Browser History (Visited)

	Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Cloud Extender		
Allowed Via Exception			
Domain			
First Visit			
Last Visit			
Number of Visits			
Policy Name			
URL Category			
Username			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
✓	✓						
✓	✓						
✓	✓						
✓	✓						
✓	✓						
✓	✓						
✓	✓						
✓	✓						

Browser History (Blocked)

	Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Cloud Extender		
Access Time			
Embedded in Page			
Policy Name			
URL			
URL Category			
Username			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
✓	✓						
✓	✓						
✓	✓						
✓	✓						
✓	✓						
✓	✓						

BES (BlackBerry) Device Features

Device Capabilities

	Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Cloud Extender		
Application Control Policies			✓
Large Attachment Upload			✓
Organizer Data Sync Encodings			✓
Wireless Application Delivery			✓
Wireless PIM Data Sync			✓

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							

Email Capabilities

	Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Cloud Extender		
Address Lookup Encodings			✓
Calendar Encodings			✓
Message Encodings			✓
PGP			✓
S/MIME Encrypted Msg			✓
Sent Items Sync			✓

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							

Messaging History

	Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Cloud Extender		
Last Contact			✓
Last Time Msg Receive			✓
Last Time Msg Sent			✓
Result of Last Transaction			✓
Uptime			✓

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							

Privacy Settings

	Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Cloud Extender		
Restrict Location Information			
Restrict App Inventory Information			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
/	/			/		/	
/	/					/	

Actions

Device Actions

	Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Cloud Extender		
Allow, Block Device for Email Access	/	/	
Approve device for Email Access	/		
Change ActiveSync Policy	/		
Change BES Policy			/
Change MDM Policy			
Change Rule Set	/	/	
Locate Device			
Buzz Device			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptop	Mac	Comments
Requires Native App on Device							
/	/	/		/		/	
/	/	/		/			
/	/		/	/		/	
/	/	/					

	Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Cloud Extender		
Lock Device			
Lock Device- Display Message and Callback no.			
Policy Assignment to AD Groups			
Policy Assignment to Device Groups			
Refresh Device Information			✓
Remote Device Wipe (Full)	✓	✓	✓
Remote Device Wipe (Selective)			
Remove Device from BES Server			✓
Remove Device from Exchange Server	✓	✓	
Remove MDM Control			
Reset Device Password			✓
Configure Patch Settings			
Send a Message			✓
Distribute App			
Change Ruleset			
Change Secure Browser Policy			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptop	Mac	Comments
Requires Native App on Device							
✓	✓	✓			✓	✓	
✓							iOS 7 onwards
✓	✓	✓		✓		✓	
✓	✓	✓		✓		✓	
✓	✓	✓	✓	✓		✓	
✓	✓	✓		✓	✓	✓	
✓	✓	✓		✓			
✓	✓	✓	✓	✓	✓	✓	
✓	✓	✓					
					✓		
✓	✓	✓	✓	✓	✓		
✓	✓	✓	✓	✓	✓	✓	
✓	✓	✓	✓	✓	✓		
✓	✓	✓					

Group Actions

	Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise	iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptop	Mac	Comments
	Cloud Extender			Requires Native App on Device							
Hide Devices				/	/	/	/	/	/	/	
Send Message				/	/	/					
Change MDM Policy				/	/	/		/			
Change Plan				/	/	/					
Distribute App				/	/	/		/	/		
Distribute Doc				/	/	/					
Change Rule Set				/	/	/		/	/		

Policies

ActiveSync Policies

		Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise	iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
	Description	Cloud Extender			Requires Native App on Device							
Allow access to Windows File Shares	The device can access Windows File Shares	/										

		Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Description	Cloud Extender		
Allow access to Windows SharePoint Services	The device has access to Windows SharePoint Services	✓		
Allow Attachments to be downloaded to the Mobile Device	Attachments can be downloaded to the device	✓		
Allow Bluetooth	The user can use Bluetooth if the device supports it	✓		
Allow Browser	The user can use the device's browser	✓		
Allow Camera	The user can use the device's camera	✓		
Allow Consumer Mail	The device can receive personal emails	✓		
Allow Desktop Synchronization	The device can be synchronized with a desktop	✓		

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							

		Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Description	Cloud Extender		
Allow HTML formatted Email	The device can receive HTML formatted emails	✓		
Allow Infrared connections	The device can make and receive infrared connections, if the device is equipped for it	✓		
Allow Internet sharing from the Mobile Device	The device can perform Internet sharing, if the device is equipped for it	✓		
Allow Non-Provisionable devices	Older devices that may not support all policy settings can still connect to the Exchange server	✓		
Allow Remote Desktop from the Mobile Device	The device can connect to a remote desktop	✓		

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							

		Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Description	Cloud Extender		
Allow Removable Storage Card	A removable storage card can be used with the device	✓		
Allow Unsigned Applications	Unsigned apps are permitted on the device	✓		
Allow Unsigned Installation Packages	Unsigned installation packages are permitted on the device	✓		
Allow Wi-Fi	The device can connect via Wi-Fi	✓		
Enable Password Recovery	The user can initiate password recovery for the device	✓		
Include past Calendar items	The device can access old calendar items	✓		
Include past Email items	The device can access old emails items	✓		

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							

		Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Description	Cloud Extender		
Limit Email size to (KB)	Specify the maximum size an email sent or received by the device can be. Longer messages will be truncated.	✓		
Maximum Attachment size (KB)	Specify the maximum size an attachment sent or received by the device can be	✓		
Mobile Device Policy Refresh interval (hours)	How often MaaS360 checks to see if a new policy has been assigned to the device	✓		
Require Encryption on Storage Card	If the device has a removable storage card, the data on it must be encrypted	✓		

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							

		Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Description	Cloud Extender		
Require Encryption on the Mobile Device	The device must be encrypted	✓		
Require Manual Synchronization while Roaming	If the device is roaming, it can only be synched manually	✓		

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							

iOS Policies

		Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Description	Cloud Extender		
Passcode Restrictions	Specify how passcodes are handled on the device			
Device Restrictions (MDM 4 API)				
- Allow Adding Game Center Friends	The device can be used to add Game Center Friends			
- Allow Automatic Synchronization While Roaming	The device can be automatically synchronized while roaming			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
✓							
✓							
✓							
✓							

		Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Description	Cloud Extender		
- Allow Explicit Music and Podcasts Purchased from iTunes	Explicit music and podcasts can be purchased from iTunes from the device and stored on it			
- Allow In-App Purchase	Purchases can be made from apps on the device			
- Allow Installing of Applications	Apps can be installed on the device			
- Allow Multiplayer Gaming	Multiplayer games can be played on the device			
- Allow Screen Capture	Screen captures can be taken with the device			
- Allow Use of iTunes for Media Download	iTunes can be used to download files			
- Allow Use of Camera	Photographs can be taken with the device's camera			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
✓							
✓							
✓							
✓							
✓							
✓							
✓							

		Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Description	Cloud Extender		
- Allow Use of Facetime	Facetime can be used			
- Allow Use of Safari	The device can use the Safari browser			
-Safari : Enable Auto-fill	When using Safari, fields in forms can be filled automatically			
-Safari : Force Fraud Warning	Safari will attempt to prevent the user from viewing websites that are fraudulent or compromised			
-Safari : Enable JavaScript on websites	JavaScript on websites will be enabled when browsing			
-Safari : Block Popups	Popups will be blocked when browsing			
-Safari : Configure Cookie settings	The user can configure cookie settings on the device			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
✓							
✓							
✓							
✓							
✓							
✓							

		Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Description	Cloud Extender		
- Allow Use of YouTube	The user can access YouTube on the device			
- Allow Voice Dialing	The user can use voice dialing on the device			
- Set Ratings for allowed Movies, TV Shows and Apps	Only movies, TV shows and apps with the specified ratings can be accessed on the device			
Device Restrictions (MDM 5 API)				
- Allow Siri	Siri can be used on the device			
- Allow Siri while Locked	Siri can be used when the device is locked and no passcode has been entered			
- Allow untrusted TLS Prompt	The device will automatically reject untrusted HTTPS certificates			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
✓							
✓							
✓							
✓							iOS 5+ Only
✓							iOS 5+ Only
✓							iOS 5+ Only
✓							iOS 5+ Only

		Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Description	Cloud Extender		
- Configure Roaming Settings (Data & Voice)	Roaming settings can be configured by the user			
- Enforce iTunes Password Entry	The iTunes password must be entered to download			
- iCloud - Allow Cloud Backup	Data on the device can be backed up to iCloud			
- iCloud - Allow Documents Sync	Documents can be synced to iCloud			
- iCloud - Allow Photo Stream Sync	Photos can be synced to iCloud			
- iCloud - Allow Shared Photo Stream	Photos can be shared via iCloud			
Open from Managed to Unmanaged apps	Files from managed apps can be opened in unmanaged apps			
Open from Unmanaged to Managed Apps	Files from unmanaged apps can be opened in unmanaged apps			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
✓							iOS 5+ Only
✓							iOS 5+ Only
✓							iOS 5+ Only
✓							iOS 5+ Only
✓							iOS 5+ Only
✓							iOS 6+ Only
✓							iOS 7+ Only
✓							iOS 7+ Only

		Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Description	Cloud Extender		
Allow Today View in Lock Screen	The Today View can be seen on the device lock screen			
Limit Ad Tracking	Ads the user sees will not be tracked			
Allow over-the-air PKI Updates	Changes to the trusted root certificates list will be allowed			
Device Restrictions (MDM 6 API)				
- Allow Passbook while Locked	Passbook notifications will not be shown on the lock screen			
- Allow submission of Diagnostic Information	Diagnostic information will be sent automatically to Apple			
- iCloud - Allow Shared Photo Stream	Photos can be shared via iCloud			
App Compliance				

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
✓							iOS 7+ Only
✓							iOS 7+ Only
✓							iOS 7+ Only
✓							iOS 6+ Only
✓							iOS 6+ Only
✓							iOS 6+ Only

		Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Description	Cloud Extender		
- Configure Restricted Applications (App Blacklist)	Specify which apps cannot be installed on the device			
- Configure Allowed Applications (App Whitelist)	Specify which apps are allowed on the device			
- Configure Required Applications	Specify which apps are required on the device			
Wi-Fi Profiles				
- Control Auto Join Behavior	Specify if the device will automatically join a Wi-Fi network			
- Proxy Settings	Specify proxy information for the device			
- Connect Priority	If multiple networks are available, the device will choose the network with the lowest priority. Zero is the default, and negative numbers are allowed			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
✓							
✓							
✓							
✓							
✓							iOS 5+ Only
✓							iOS 5+ Only
✓							iOS 7+ Only

		Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Description	Cloud Extender		
AirPrint				
- Configure AirPrint Printer List	Specify AirPrint printer settings			
AirPlay				
- Configure AirPlay destinations	Specify AirPrint printer settings			
Single Sign On				
- Configure Single Sign On via Kerberos	Specify SSO settings via Kerberos			
VPN Profiles	Specify VPN profile settings			
Email Profiles	Specify email profile settings			
Exchange ActiveSync Profiles				
- Prevent Moving Mail to other Accounts	Email cannot be moved or forwarded to other accounts			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
✓							iOS 7+ Only
✓							iOS 7+ Only
✓							iOS 7+ Only
✓							
✓							iOS 5+ Only

		Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Description	Cloud Extender		
- Prevent Third Party Apps from Sending Mail	The user cannot send emails from third-party apps on the devices			
- Prevent synchronization of Recent Contacts	Recent contacts are not synced			
LDAP	Specify LDAP settings			
CalDAV	Specify CalDAV settings			
Subscribed Calendars	Specify settings for calendar subscriptions			
CardDav	Specify CardDav settings			
Web clips	Specify web clip settings			
Certificates	Specify certificate settings			
- Use of certificates in Wi-Fi, VPN, Email	Specify if certificates will be used for Wi-Fi, VPN or email			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
✓							iOS 5+ Only
✓							iOS 6+ Only
✓							
✓							
✓							
✓							
✓							
✓							

		Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Description	Cloud Extender		
SCEP	Specify SCEP settings			
Access Point Carriers	Specify settings for access point carriers			
Import iPCU Settings	Import settings created in the iPhone Configuration Utility			
Supervised Settings	Specify the supervised settings			
- Allow Gamecenter	Gamecenter is allowed on the device			
- Allow Erotica	Erotica is allowed on the device			
- Allow iMessage	iMessage is allowed on the device			
- Enable Siri Profanity Filter	Enable the Siri Profanity Filter			
- Allow Removing Apps	The user can remove apps from the device			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
✓							
✓							
✓							
✓							iOS 6+ Only
✓							iOS 6+ Only
✓							iOS 6+ Only
✓							iOS 6+ Only
✓							iOS 6+ Only
✓							iOS 6+ Only

		Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Description	Cloud Extender		
- Allow iBookstore	iBookstore can be installed on the device			
- Allow Interactive Installation of Configuration Profiles	Allow configuration profiles to be installed interactively			
- Allow Account Modification	The user can modify the account			
- Allow Cellular Data Usage Modifications	The user can change which apps can use cellular data			
- Allow Find My Friends Modification	The user can change the Find My Friends app			
- Allow Text Define in Safari				
- Whitelist AirPlay Devices	Specify the devices that AirPlay can connect to			
Global Proxy				
- Configure Global Proxy	Select to configure the global proxy			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
✓							iOS 6+ Only
✓							iOS 6+ Only
✓							iOS 7+ Only
✓							iOS 7+ Only
✓							iOS 7+ Only
✓							iOS 7+ Only
✓							iOS 7+ Only
✓							iOS 6+ Only

		Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Description	Cloud Extender		
- Allow Bypassing Proxy to Access Captive Networks	Global proxy can be ignored to access captive networks			
- Allow Direct Connection if PAC is unreachable	If the proxy automatic configuration cannot be found, a direct connection will be allowed			
App Lock	App lock settings			
- Configure App Lock	Configure the app lock			
-Allow Touch Input	The user can touch the screen to enter data			
-Allow Device Rotation	Turning the device will rotate the display			
-Allow Volume Button Control	The user can change the device's volume			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
✓							iOS 7+ Only
✓							iOS 7+ Only
✓							iOS 6+ Only
✓							iOS 7+ Only
✓							iOS 7+ Only
✓							iOS 7+ Only

		Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Description	Cloud Extender		
-Allow Ringer Switch Control	The user can turn off the ringer			
-Allow Sleep/Wake Button Control	The user can use the sleep/wake controls			
-Allow Auto Lock	The device will automatically lock after a specified period			
-Enable Voice Over	The device can be set to provide voiceovers			
-Enable Zoom	The image in the camera can be zoomed			
-Enable Invert Colors	The colors in the display can be inverted for easier readability			
-Enable Assistive Touch	Assistive touch can be used to simulate commonly use gestures			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
✓							iOS 7+ Only
✓							iOS 7+ Only
✓							iOS 7+ Only
✓							iOS 7+ Only
✓							iOS 7+ Only
✓							iOS 7+ Only
✓							iOS 7+ Only

		Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Description	Cloud Extender		
-Enable Speaker Selection	The user can select the speaker that will be used			
-Enable Mono Audio	The device will produce mono audio			
-Allow Voice Over Adjustment	The user can change the voiceover			
-Allow Zoom Adjustment	The user can change the camera's zoom			
-Allow Invert Color Adjustment	The user can customize the colors when inverted			
-Allow Assistive Touch Adjustment	The user can customize the assistive touch feature			
Web Content Filtering				
- Limit Adult Content	Adult content cannot be viewed on the device			
- Limit Access to Specific Websites only	The user can only access the listed websites			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
✓							iOS 7+ Only
✓							iOS 7+ Only
✓							iOS 7+ Only
✓							iOS 7+ Only
✓							iOS 7+ Only
✓							iOS 7+ Only
✓							iOS 7+ Only
✓							iOS 7+ Only

		Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Description	Cloud Extender		
Configure WorkPlace Settings				
- Host name of the ActiveSync Server	The host name of the ActiveSync server			
- Use SSL	If the WorkPlace container can use SSL			
- Domain Name	The domain name of the WorkPlace container			
- Account Username	The username of the container			
- Email Address	The email address of the container			
- Restrict Email Attachment sharing in the Container	Email attachments received in the container cannot be sent outside it			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
✓							iOS 5+ only
✓							iOS 5+ only
✓							iOS 5+ only
✓							iOS 5+ only
✓							iOS 5+ only
✓							iOS 5+ only
✓							iOS 5+ only

		Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Description	Cloud Extender		
- Max days to Mail to sync	The maximum number of days before the mail in the container contacts the server			
- Max days to Calendar to sync	The maximum number of days before the calendar in the container contacts the server			
- Block use of the Container when device is Out-of-Compliance	The user cannot access the container when the device is out of compliance with security policies			
- Disable Copy-Paste outside WorkPlace	Text inside the container cannot be copied or pasted outside it			
- Restrict Contact Export	Contacts cannot be exported out of the container			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
✓							iOS 5+ only
✓							iOS 5+ only
✓							iOS 5+ only
✓							iOS 5+ only
✓							iOS 5+ only

		Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Description	Cloud Extender		
- Enable Secure Browser Integration	MaaS360 Secure Browser will be included in the WorkPlace container			
- Enforce passcode on WorkPlace	The user must enter a passcode to access the container			
- Allow Simple Passcode	The WorkPlace passcode can be simple			
- Require Alphanumeric in Passcode	The WorkPlace passcode must be alphanumeric			
- Allowed Idle Time before Auto-Lock	How long the device may be idle before it is automatically locked			
- Minimum Passcode Length	The minimum length of the container passcode			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
✓							iOS 5+ only
✓							iOS 5+ only
✓							iOS 5+ only
✓							iOS 5+ only
✓							iOS 5+ only
✓							iOS 5+ only

		Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Description	Cloud Extender		
- Number of Failed Passcode Attempts Before WorkPlace Data is Selective Wiped	How many times a passcode can be entered incorrectly before data in the container is wiped			
- Required Number of Special Characters	The number of special characters that must be in the passcode			
- Maximum Passcode Age	How old the passcode can be before it can be changed			
- Number of Unique Passcodes Required Before Reuse Allowed	The number of unique passcodes that must be used before one can be reused			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
✓							iOS 5+ only
✓							iOS 5+ only
✓							iOS 5+ only
✓							iOS 5+ only

Android Policies

		Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Description	Cloud Extender		
Device Passcode Policy	These settings apply for MaaS360, not for MaaS360 Secure Productivity Suite (SPS)			
- Passcode Quality	Specifications for the device's passcode, including Pattern , Numeric , Alphabetic , Alphanumeric , and Complex			
- Minimum Passcode Length (4-16 characters)	The minimum length of the device's passcode			
- Minimum Number of Complex Characters	The minimum number of special characters or symbols that must appear in the passcode			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
	✓	✓					
	✓	✓					
	✓	✓					
	✓						Android 3.0+ only

		Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Description	Cloud Extender		
- Maximum Passcode Age (in Days)	How old the passcode can be before it can be changed			
- Allowed Idle Time (in minutes) Before Auto-Lock	How long the device may be idle before it is automatically locked			
- Passcode history	The number of unique passcodes that must be used before one can be reused			
- Number of Failed Passcode Attempts Before All Data is Erased (4-16)	How many times a passcode can be entered incorrectly before all data is wiped			
Security Settings				

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
	✓						Android 3.0+ only
	✓	✓					
	✓						Android 3.0+ only
	✓	✓					

		Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Description	Cloud Extender		
- Enforce Device Encryption	The data on the device must be encrypted if the device supports hardware encryption. On SAFE devices, the passcode policy will automatically require a 6-digit alphanumeric passcode			
- Enforce SD Card Encryption	Any SD cards used with the device must be encrypted			
- Visible Passwords	The user can choose to make the passcode visible as it is being entered			
- Allow USB Debugging	A USB device can be used for debugging			
- Allow SD Card	SD cards are allowed			
- Allow SD Card Write	Device data can be written to an SD card			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
	✓						Android 3.0+ & Motorola
	✓						
	✓						SAFE 2.0+
	✓						SAFE 2.0+
	✓						SAFE 3.0+

		Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Description	Cloud Extender		
- Disable Keyguard Features	Prevents the user from setting Keyguard features			
- Allow Installation of Non-Google Play Apps	The user can install apps that do not come from Google Play			
- Enforce App verification before install	The app will be verified before it is installed			
- Allow Clipboard	The Clipboard can be used			
- Allow Screen Capture	Screen captures can be taken on the device			
- Backup my data	Current settings and app data will be backed up to the Google servers			
- Automatic Restore	Backed up settings and data will be restored when an app is reinstalled			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
	✓						Android 4.2+
	✓						
	✓						Android 4.2+
	✓						SAFE 2.0+
	✓						SAFE 2.0+
	✓						SAFE 2.0+
	✓						SAFE 3.0+

		Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Description	Cloud Extender		
- Allow Google Crash Report	The report will be sent			
- Allow Factory Reset	The device can be restored to factory settings			
- Allow OTA Upgrade	The device can be upgraded over the air			
Device Restrictions				
- Enable Background Data Synchronization	Devices can sync, send or receive data any time			
- Auto-Sync	The device can sync automatically			
- Camera	The device's camera can be used			
- Bluetooth	Bluetooth can be used			
- Allow USB Mass Storage	Data can be stored on a USB device			
- Allow USB Media Player (MTP, PTP)	The device can be used with a USB media player			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
	✓						SAFE 3.0+
	✓						SAFE 2.0+
	✓						SAFE 3.0+
	✓	✓					
	✓						
	✓						
	✓						
	✓						
	✓						SAFE 2.0+

		Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Description	Cloud Extender		
- Allow Microphone	The device's microphone can be used			
- Near Field Communication (NFC)	Devices can communicate via NFC			
- Use Network-provided Date & Time	The device's date and time data will come from the network			
- Use Wireless Networks / Google's Location Service for Location Detection	Wireless networks or Google's location service will be used to determine the device's location			
- Use GPS satellites for Location Detection	GPS satellites will be used to determine the device's location			
- Use sensor aiding for Location Detection	Sensors will be used to determine the device's location			
- Allow Mock Locations	Mock locations can be used.			
Network Restrictions				

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
	✓						SAFE 2.0+
	✓						
	✓						
	✓						
	✓						
	✓						SAFE 3.0+
	✓						

		Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Description	Cloud Extender		
- Allow Emergency Calls only	Only emergency calls can be made from the device			
- Allow Wi-Fi	Wi-Fi can be used on the device. There is no effect on a Wi-Fi only device			
- Whitelisted SSIDs	Network SSIDs that are allowed. Be sure you do not whitelist an invalid SSID			
- Blacklisted SSIDs	Network SSIDs that are prohibited			
- Wi-Fi Network Minimum Security Level	Specifies the minimum amount of security the network can have			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
	✓						SAFE 2.0+
	✓						SAFE 2.0+
	✓						SAFE 2.2+
	✓						SAFE 2.2+
	✓						SAFE 2.0+

		Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Description	Cloud Extender		
- Allow user to add Wi-Fi networks	The user can add Wi-Fi networks. This setting will be disabled if one or more Wi-Fi profiles are defined in the device's policies.			
- Allow Data Network	The user can add data networks			
- Mobile AP	The device can be a mobile access point hot spot. Other devices can connect to its cellular Internet connection			
- USB Tethering	The user can perform USB tethering with the device			
- Allow SMS & MMS	The device can be used to send SMS and MMS messages			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
	✓						SAFE 2.0+
	✓						
	✓						SAFE 2.2+
	✓						
	✓						SAFE 3.0+

		Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Description	Cloud Extender		
- Allow Data Roaming	The device can send and receive data while roaming			
- Allow Sync during Roaming	The device can sync with servers while roaming			
- Allow Voice Roaming	The user can make calls while roaming			
App Compliance				
- Configure Restricted Applications (App Blacklist)	Specify which apps cannot be installed on the device			
- Configure Allowed Applications (App Whitelist)	Specify which apps are allowed on the device			
- Configure Required Applications	Specify which apps are required on the device			
Native App Compliance				
- Allow Google Play	The Google Play app is allowed on the device			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
	✓						
	✓						SAFE 1.0+
	✓						SAFE 3.0+
	✓	✓					
	✓	✓					
	✓	✓					
	✓						

		Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Description	Cloud Extender		
- Allow YouTube App	The YouTube app is allowed on the device			
- Allow Email	Email can be used on the device			
- Allow Browser	The native browser can be used on the device			
- Allow Settings	The user can change the device's settings			
- Allow Gallery	The Google photo app can be installed on the device			
- Allow Gmail	Gmail can be used on the device			
- Allow Google Maps & Navigation	Google Maps and navigation can be used on the device			
- Allow Voice Dialer	The voice dialer can be used on the device			
Wi-Fi Profile	Configure your Wi-Fi profile			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
	✓						
	✓	✓					
	✓	✓					
	✓	✓					
	✓	✓					
	✓	✓					
	✓	✓					
	✓						
	✓	✓					

		Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Description	Cloud Extender		
VPN Profile	Configure your VPN profile			
Email Profile	Configure your Email profile			
ActiveSync Profile	Configure your ActiveSync profile			
- Host name of the Server	Host name of the server			
- Use SSL	If the device can use SSL			
- Account	The account ID			
- Identity Certificate	The identity certificate			
- Account Display Name	The account display name			
- Set as Default Account	This is the default account			
- Accept All Certificates	All certificates should be accepted			
- Prompt User to Install TouchDown	The user will be prompted to install the TouchDown app			
- License Key	The license key for MaaS360			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
	✓						Motorola, SAFE 2.0+
	✓						SAFE 2.0+
	✓	✓ *					"Motorola, SAFE 2.0+, TouchDown *, TouchDown
	✓	✓ *					
	✓	✓ *					
	✓	✓ *					
	✓						SAFE 1.0+
	✓						SAFE 1.0+
	✓						SAFE 1.0+
	✓	✓ *					
	✓	✓ *					

		Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Description	Cloud Extender		
Exchange Security Settings				
- Configure TouchDown Passcode	The TouchDown passcode			
- Suppress TouchDown specific Passcode policy enforced via ActiveSync	Suppress any TouchDown-specific passcode policy that is being enforced by EAS			
- Encrypt Emails	Encrypt all emails			
- Encrypt Attachments	Encrypt all attachments			
- Allow Backup of Emails and Settings	Allow emails and settings to be backed up to the EAS server			
- Disable Copy of Contacts to Phone	Do not allow contacts on the EAS server to be copied to the device			
- Disable Copy-Paste from Email	Restrict copying and pasting from emails			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
	✓	✓ *					
	✓	✓ *					
	✓	✓ *					
	✓	✓ *					
	✓	✓ *					
	✓	✓ *					
	✓	✓ *					

		Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Description	Cloud Extender		
- Device Type reported in Exchange Server	Device type that is reported in the EAS server			
- Prevent Moving Mail to other Accounts	Mail cannot be moved or forwarded to other accounts on the device			
- Allow HTML Formatted Email	Allow emails formatted in HTML on the device			
- Maximum Email Size (KB)	The maximum size for an email			
- Include Past Emails for Selected Date Range	Old emails for the date range can be loaded onto the device			
- Include Past Calendar Items for Selected Date Range	Old events for the date range can be loaded onto the device			
- Allow Attachments	The device can receive attachments			
- Maximum Attachment Size (KB)	The maximum size for an attachment			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
	✓	✓ *					
	✓						SAFE 2.1+
	✓	✓ *					
	✓	✓ *					
	✓	✓ *					
	✓	✓ *					
	✓	✓ *					
	✓	✓ *					

		Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Description	Cloud Extender		
- Sync Contacts	Contacts can be synced with the server			
- Sync Calendar	Calendar events can be synced with the server			
- Sync Tasks	Tasks can be synced with the server			
- Sync Notes	Notes can be synced with the server			
- Email Signature	Specify the signature that will appear at the bottom of all emails sent from the device			
- Allow User to change Email Signature	The user can change the email signature			
- Manual Sync when Roaming	The device must be synced manually when roaming			
- Enable TouchDown Widgets	The user can use TouchDown widgets on the device			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
	✓						SAFE 2.1+
	✓						SAFE 2.1+
	✓						SAFE 2.1+
	✓						SAFE 2.1+
	✓	✓ *					
	✓	✓ *					
	✓	✓ *					
	✓	✓ *					

		Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Description	Cloud Extender		
- Always Vibrate on New Email Notification	The device will vibrate when it receives a new email			
- Vibrate on New Email Notification if device is silent	The device will vibrate when it receives a new email and the ringer has been turned off on the device			
- Generic TouchDown Policies				
Web Clips (shortcuts)	The device can use web clips			
Wallpapers	The device can use wallpapers			
Browser Restrictions				
- Allow Pop-ups	The browser will allow pop-ups			
- Allow JavaScript	The browser will allow JavaScript			
- Accept Cookies	The browser will accept and use cookies			
- Remember Form Data for later use	Data in forms will be remembered for reuse			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
	✓						SAFE 1.0+
	✓						SAFE 1.0+
	✓	✓ *					
	✓	✓					
	✓	✓					
	✓						SAFE 2.0+
	✓						SAFE 2.0+
	✓						SAFE 2.0+
	✓						SAFE 2.0+

		Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Description	Cloud Extender		
- Show Fraud Warning Settings	If the user attempts to access a potentially fraudulent web site, warnings will be displayed			
Bluetooth Restrictions				
- Allow Device discovery via Bluetooth	The device can be discovered by Bluetooth			
- Allow Bluetooth Pairing	The device can be paired via Bluetooth			
- Allow Bluetooth Headset devices	Bluetooth headsets can be used with the device			
- Allow Bluetooth Hands-free devices	Bluetooth hands-free devices can be used			
- Allow Bluetooth A2DP (Advanced Audio Distribution Profile) devices	Bluetooth A2DP devices can be used			
- Allow Outgoing Calls	The device can be used to make outgoing calls			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
	✓						SAFE 2.0+
	✓						SAFE 2.0+
	✓						SAFE 2.0+
	✓						SAFE 2.0+
	✓						SAFE 2.0+
	✓						SAFE 2.0+

		Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Description	Cloud Extender		
- Allow Data Transfer via Bluetooth	Data can be transferred via Bluetooth			
- Allow Bluetooth Tethering	Bluetooth tethering is available on the device			
- Allow connection to Desktop or Laptop via Bluetooth	The device can connect to a desktop or laptop via Bluetooth			
Kiosk mode restrictions				
- Enable Kiosk Mode	The device is in kiosk mode. It is restricted to specific apps			
- Allowed apps in Kiosk mode	Specify the apps that are allowed on the device			
- Block Task Manager	Task Manager cannot be used			
- Hide System Bar	Hide the system bar o			
- Block Hardware Keys	The keys on the device cannot be used—only the touch screen is available			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
	✓						SAFE 2.0+
	✓						SAFE 2.0+
	✓						SAFE 2.0+
	✓						SAFE 3.0+
	✓						SAFE 3.0+
	✓						SAFE 3.0+
	✓						SAFE 3.0+
	✓						SAFE 3.0+

		Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Description	Cloud Extender		
Action on Disabling Device Management	What MaaS360 will do if the user removes the MaaS360 app			
Warning Message on Disabling Device Management	Specify the message the user will receive if the MaaS360 app is removed			
User Grace Period to Determine Device Out-of-Compliance	The grace period before a device is considered out of compliance			
Enforcement Action when the Device is Out of Compliance	The action taken by MaaS360 if the device is out of compliance			
Data Collection Timer Frequency	How often compliance data is collected from the device. Reducing this will preserve the device's battery			
WorkPlace Settings				

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
	✓	✓					
	✓	✓					
	✓	✓					
	✓	✓					
	✓	✓					
	✓						

		Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Description	Cloud Extender		
- Configure WorkPlace Settings	Select to configure WorkPlace settings			
- Host name of the ActiveSync Server	The host name of the ActiveSync server			
- Use SSL	If the WorkPlace container can use SSL			
- Domain Name	The domain name of the WorkPlace container			
- Account Username	The username of the container			
- Email Address	The email address of the container			
- Restrict Email Attachment sharing in the Container	Email attachments received in the container cannot be sent outside it			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
	✓						
	✓						
	✓						
	✓						
	✓						
	✓						
	✓						

		Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Description	Cloud Extender		
- Block use of the Container when device is Out-of-Compliance	The user cannot access the container when the device is out of compliance with security policies			
- Disable Copy-Paste outside Workplace	Text inside the container cannot be copied or pasted outside it			
- Disable Screenshots	Screen captures cannot be taken with the device			
- Enable Secure Browser Integration	MaaS360 Secure Browser will be included in the WorkPlace container			
- Use Secure Viewer	The Secure Viewer can be used			
- Enforce passcode on WorkPlace	The user must enter a passcode to access the container			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
	✓						
	✓						
	✓						
	✓						
	✓						
	✓						

		Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Description	Cloud Extender		
- Allowed Idle Time before Auto-Lock	How long the device may be idle before it is automatically locked			
- Require Alphanumeric in Passcode	The WorkPlace passcode must be alphanumeric			
- Minimum Passcode Length	The minimum length of the container passcode			
- Number of Failed Passcode Attempts Before WorkPlace Data is Selective Wiped	How many times a passcode can be entered incorrectly before data in the container is wiped			
- Required Number of Special Characters	The number of special characters that must be in the passcode			
- Maximum Passcode Age	How old the passcode can be before it can be changed			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
	✓						
	✓						
	✓						
	✓						
	✓						
	✓						

Windows Phone Policies

		Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Description	Cloud Extender		
Device Passcode Restrictions	Specify how passcodes are handled on the device			
- Allow Simple Passcode	The device's passcode can be simple			
- Passcode Quality	Specifications for the device's passcode			
- Minimum number of character sets (1-4 chars)				
- Minimum Passcode length (4-18)	The minimum length of the container passcode			
- Maximum Passcode Age(1-730 days)	How old the passcode can be before it can be changed			
- Allowed Idle Time (in minutes) Before Auto-Lock (1-999)	How long the device may be idle before it is automatically locked			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
				✓			
				✓			
				✓			
				✓			
				✓			
				✓			
				✓			

		Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Description	Cloud Extender		
- Number of Unique Passcodes Required Before Reuse Allowed (1-50)	The number of unique passcodes that must be used before one can be reused			
- Number of Failed Passcode Attempts Before All Data Is Erased (1-999)	How many times the incorrect passcode can be entered before the device is wiped			
Security Settings				
- Enforce Device Encryption	The device must be encrypted			
- Disable SD Card	An SD card cannot be used with the device			
Email Profiles				
Exchange ActiveSync Profiles				
- Account name for the ActiveSync Server	The account name for the EAS server			
- End users will see the mailbox with this name	The mailbox name displayed to the users			
- Host name for the ActiveSync Server	The host name for the EAS server			
- Use SSL	Use SSL			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
				✓			
				✓			
				✓			
				✓			
				✓			
				✓			
				✓			
				✓			
				✓			

		Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Description	Cloud Extender		
- Domain Name	The domain name			
- Account Username	The account username			
- Email Address	The email address for the account			
- Account Icon	An icon for the account			
- Sync Emails	Emails should be synced with the server			
- Sync Calendar	Calendar items should be synced with the server			
- Sync Contacts	Contacts should be synced with the server			
- Sync Tasks	Tasks should be synced with the server			
- Sync Frequency	How often data should be synced with the server			
- Download Email Period	How often emails should be downloaded from the server			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
				✓			
				✓			
				✓			
				✓			
				✓			
				✓			
				✓			
				✓			
				✓			
				✓			

Mac Policies

		Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Description	Cloud Extender		
Device Passcode Restrictions				
- Allow Simple Passcode	The device can have a simple passcode			
- Minimum Passcode Length (4-16 characters)	The minimum length of the passcode			
- Minimum Number of Complex Characters	The minimum number of complex characters in the passcode			
- Maximum Passcode Age (in Days)	How old the passcode can be before it can be changed			
- Allowed Idle Time (in minutes) Before Auto-Lock	How long the device can be idle before it is automatically locked			
- Passcode history	Previously used passcodes			
- Number of Failed Passcode Attempts Before All Data is Erased (4-16)	How many times a passcode can be entered incorrectly before all data is wiped			
Device Restrictions				

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
						/	
						/	
						/	
						/	
						/	
						/	
						/	
						/	

		Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Description	Cloud Extender		
- Restrict System Preferences	Displays system restrictions you can enable			
- Media: Restrict Network Media	Restrict access to network media			
- Media: Access Settings for AirDrop	Restrict access to AirDrop			
- Media: Restrict Hard Disk Media Access	Restrict access to hard disk media			
- Media: Allow Internal Disks	Restrict access to internal disks			
- Media: Allow Internal Disks: Enforce Authentication	Allow access to internal disks, but users must enter credentials			
- Media: Allow Internal Disks: Enforce Read Only Permissions	Allow read-only access to internal disks			
- Media: Allow External Disks	Allow the use of external disks			
- Media: Allow External Disks: Enforce Authentication	Allow access to external disks, but users must enter credentials			
- Media: Allow External Disks: Enforce Read Only Permissions	Allow read-only access to external disks			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
						✓	
						✓	
						✓	
						✓	
						✓	
						✓	
						✓	
						✓	
						✓	

		Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Description	Cloud Extender		
- Media: Allow Disk Images	Allow access to disk images			
- Media: Allow Disk Images: Enforce Authentication	Allow access to disk images, but users must enter credentials			
- Media: Allow Disk Images: Enforce Read Only Permissions	Allow read-only access to disk images			
- Media: Allow DVD-RAM	Allow the use of DVD-RAM			
- Media: Allow DVD-RAM: Enforce Authentication	Allow the use of DVD-RAM, but users must enter credentials			
- Media: Allow DVD-RAM: Enforce Read Only Permissions	Allow read-only access to DVD-RAM			
- Media: Disk Media Access	Allow the use of removable disk media			
- Media: Allow Access for CDs & CD-ROMs	Allow the use of CDs and CD-ROMs			
- Media: Require Authentication for CDs & CD-ROMs	Users must enter credentials to use CDs and CD-ROMs			
- Media: Allow DVD Access	Allow the use of DVDs			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
						✓	
						✓	
						✓	
						✓	
						✓	
						✓	
						✓	
						✓	
						✓	
						✓	

		Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Description	Cloud Extender		
- Media: Require Authentication for DVDs	Users must enter credentials to use DVDs			
- Media: Allow access for Recordable disks	Allow use of recordable disks			
- Media: Eject at Logout	All removable media will be ejected at logout			
Wi-Fi Profiles				
- Auto Join	Available networks will be joined automatically			
- Proxy Settings	Information about the proxy server			
VPN Profiles	Information about the VPN			
Certificate Credentials	Credentials needed to add certificates on the device			
Security & Privacy				
- Send diagnostic and usage data to Apple	Data will be sent to Apple daily			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
						✓	
						✓	
						✓	
						✓	
						✓	
						✓	
						✓	
						✓	

		Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Description	Cloud Extender		
- Gatekeeper	Specifies where apps on the device can come from, either the Mac App Store and specified app developers, or just the Mac App Store			
- Do not allow user to override Gatekeeper setting	Prevents the user from temporarily overriding the Gatekeeper setting by using <Ctrl>+click to install any app			
Software Update				
- Configure Software update server				
Energy Saver				
- Energy Saver Settings for Desktop				
- Energy Saver Settings for Portable Battery				
- Energy Saver Settings for Power Adapter				
- Schedule Mac Power on Timings				

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
						✓	
						✓	
						✓	
						✓	
						✓	
						✓	
						✓	

		Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Description	Cloud Extender		
- Schedule Mac Power Off/ Standby Timings				
Printing	Configures printers used by the device			
- Configure Printer Details				
- Printer Settings: Set Default				
- Printer Settings: Allow user to modify the list				
- Printer Settings: Allow printers that directly connect to computers				
- Printer Settings: Show Only Managed Printers				
- Footer Settings: Include MAC Address				
- Footer Settings: Font Name				
- Footer Settings: Font Size				
Login Window				

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
						✓	
						✓	
						✓	
						✓	
						✓	
						✓	
						✓	
						✓	
						✓	

		Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Description	Cloud Extender		
- Window: Heading	Specify the heading displayed on the login window			
- Window: Message	Specify a message to be displayed on the login window			
- Window: Style	Specify a style for the login window			
- Window: Show Shut Down Button	Display the shutdown button on the login window			
- Options: Show password hint	Display a password hint when needed and available			
- Options: Disable Automatic Login	Disable the automatic login			
- Options: Enable >console login				
- Options: Enable Fast User Switching	Different users can be changed quickly on the device			
- Options: Configure Auto logout				
- Options: Allow Computer admins to refresh or disable management	Administrators can refresh or disable management			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
						✓	
						✓	
						✓	
						✓	
						✓	
						✓	
						✓	
						✓	
						✓	

		Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Description	Cloud Extender		
- Options: Set computer name to computer record name				
- Options: Enable external accounts				
- Options: Allow Guest User				
- Options: Start screen saver				
Configure Login Items				
- Configure Items to launch and hide on login	Specify items to be launched or hidden at login			
- Configure Files and Folders to launch and hide on login	Specify folders to open at login			
- Configure network mounts on login	Specify network mounts to be used at login			
- Allow User to suppress opening of certain items by using Shift Key				
Email				
- Configure IMAP Accounts	Settings for IMAP accounts			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
						✓	
						✓	
						✓	
						✓	
						✓	
						✓	
						✓	
						✓	
						✓	

		Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Description	Cloud Extender		
- Configure POP Accounts	Settings for POP accounts			
Exchange ActiveSync				
- Prevent Moving Mail to other Accounts				
- Use only in Mail				
- Configure Internal and External Exchange Hosts				
- Enforce SSL				
- Configure no. of days to sync				

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
						✓	
						✓	
						✓	
						✓	

Secure Browser Policies

		Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Description	Cloud Extender		
URL Filtering Settings				
- Select URL Categories to Allow or Block	Specify the category and choose the action to be taken when the user tries to access a site in that category			
- Enter Domain Name Category Exceptions	Specify any domains within a restricted category that should be allowed			
- Enter Email Address for Notifications	Specify the notification recipient			
- Enable Text Notification	Provide the text that will appear when a user tries to access a blocked site, up to 255 characters. Basic HTML formatting is supported			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
✓	✓	✓					
✓	✓	✓					
✓	✓	✓					
✓	✓	✓					
✓	✓	✓					

		Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Description	Cloud Extender		
- Enable HTML Notification	Provide custom HTML content that will appear when a user tries to access a blocked site. You can upload HTML files by clicking the Policy Files button on the Policies screen.			
- Enable URL Redirect	Provide the URL that the user will be sent to when attempting to access a blocked URL			
- Send Notification on Block Events	Specify if the administrator should be notified when a user attempts to access a blocked URL			
- Notification Threshold Events (occurrences)	Specify how many times a user can visit a blocked site before the administrator receives a notification			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
✓	✓	✓					
✓	✓	✓					
✓	✓	✓					
✓	✓	✓					

		Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Description	Cloud Extender		
- Notification Threshold Time (in hours)	Specify the time between multiple attempts to access blocked sites before a notification is triggered			
- Data Collection Frequency (in minutes)	Specify how often data about the device is collected			
- Visited Site Upload Frequency (in minutes)	Specify how often the sites visited by the user are uploaded to MaaS360			
- Data Group Frequency (in minutes)	Specify when the visited URL domain information will be rolled up into MaaS360			
- Heartbeat Frequency (in minutes)	Specify how long before MaaS360 checks for policy changes and new assignments			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
✓	✓	✓					
✓	✓	✓					
✓	✓	✓					
✓	✓	✓					
✓	✓	✓					

		Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Description	Cloud Extender		
- Configure as default browser on Android	Specify if the Secure Browser will be the default for Android devices			
- Accept Cookies	Specify if the device can accept cookies			
- Disable Print	Prevent the user from printing from the device			
- Disable Copy/Paste	Prevent the user from copying and pasting text			
- Enable File Downloads	Allow files to be downloaded onto the device			
Mobile Enterprise Gateway for Intranet access	Use the MaaS360 Mobile Enterprise Gateway for Internet access			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
	✓	✓					
	✓	✓					
	✓	✓					
	✓	✓					
	✓	✓					
✓	✓	✓					

Compliance/Rules Engine

	Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Cloud Extender		
Enforce Application Compliance			
Enforce Encryption Support			
Enforce Enrollment	✓	✓	
Enforce OS Versions (Minimum or Specific versions)	✓	✓	
Enforce Remote Wipe Support	✓		
Monitor OS Version Changes			
Monitor Roaming Changes			
Monitor SIM Changes			
Restrict Corp Resources for Blocked Devices			
Restrict Jailbroken (iOS) or Rooted (Android) Devices			
Enable Geofencing			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
✓	✓	✓					
✓	✓	✓		✓			
✓	✓	✓		✓			
✓	✓	✓		✓			
✓	✓	✓		✓			
✓	✓	✓	✓	✓			
✓	✓						
✓	✓						
✓	✓	✓					
✓	✓	✓					
✓	✓						

Apps

	Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Cloud Extender		
MaaS360 Application Catalog (Public Apps)			
- Specify Region for all download			
- Remove app on MDM profile removal			
- Remove app on Selective Wipe			
- Remove app on Stopping Distribution			
- Remove app on Signout from Shared Device			
- Restrict backup to iTunes for app data			
MaaS360 Application Catalog (Private Apps)			
- Remove app on MDM profile removal			
- Remove app on Selective Wipe			
- Remove app on Stopping Distribution			
- Remove app on Signout from Shared Device			
- Restrict backup to iTunes for app data			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
✓	✓	✓	✓	✓			
✓							
✓	✓			✓			SAFE 2.0+
✓	✓						SAFE 2.0+
✓							
✓							
✓							
✓	✓	✓	✓	✓	✓		
✓	✓			✓			SAFE 2.0+
✓							SAFE 2.0+
✓							
✓							
✓							

	Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Cloud Extender		
- Enforce Authentication			
- Restrict Cut/Copy/Paste			
- Enforce Compliance			
- Update iOS Provisioning Profile			
- Upgrade App			
Restricted Applications (App Blacklist)			
Allowed Applications (App Whitelist)			
Required Applications			
Apple Volume Purchase Program (VPP)			
Manage Provisioning Profiles			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
✓							
✓							
✓							
✓							
✓				✓			
✓	✓	✓					
✓	✓	✓					
✓	✓	✓					
✓	-	-	-				Support for both old (till iOS 6.x) and new (iOS 7+) VPP Programs
✓	-	-	-				

Documents

Document Management

	Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Cloud Extender		
Admin driven Document Distribution			
MaaS360 hosted documents			
Custom URL support			
SharePoint integration			
Windows File Share integration			
Folder Support			
Inbuilt Secure Viewer			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
✓	✓	✓					
✓	✓	✓					
✓	✓	✓					
✓	✓	✓					
✓							
✓							
✓	✓						

Document Policies

	Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Cloud Extender		
Restrict Access on Jailbroken devices			
Restrict Export			
Restrict Cut/Copy/Paste			
Password Protected			
Download Automatically			
Download only on Wi-Fi			
Hide Doc Preview in App			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
✓							
✓	✓						
✓							
✓							
✓							
✓							
✓							

	Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Cloud Extender		
Restrict Delete after Download			
Allow Whitelisted Apps			
Restrict Secure Mail			
Override Persona Policies			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
✓							
✓							
✓							
✓							

Mobile Expense Management

	Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Cloud Extender		
Monitor In-Network Mobile Data Usage			
Monitor Roaming Mobile Data Usage			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
✓	✓						
✓	✓						

End User Portal

	Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Cloud Extender		

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							

	Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Cloud Extender		
Device Visibility	✓	✓	✓
Last Known Location			
Locate Device			
Lock Device			
Refresh Device Information			
Remote Device Wipe (Full)	✓	✓	✓
Reset Device Passcode			✓

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
✓	✓	✓	✓	✓	✓	✓	
✓			✓				
	✓						
✓	✓	✓					
✓	✓	✓	✓				
✓	✓	✓					
✓	✓	✓					

Mobility Intelligence Reports

Mobile Devices

	Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Cloud Extender		
Mobile Devices			
MDM Overview	✓	✓	✓
Hardware Inventory	✓	✓	✓
Network			✓
BlackBerry Details			✓
Apps Installed			✓
Security Overview			✓
Browser Violations			
Mobile Data Usage Overview			
Mobile Data Usage Analysis			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
✓	✓	✓	✓	✓			
✓	✓	✓	✓	✓			
✓	✓	✓	✓	✓			
✓	✓	✓					
✓	✓	✓		✓			
✓	✓	✓					
✓	✓						
✓	✓						

Computers

	Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
--	------------------------	----------------	--------------------------

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
-----	---------	----------------	---------------------	-------------------	--------------------	-----	----------

	Cloud Extender		
PC Overview			
Hardware Inventory			
Network			
Operating System			
Software			
Windows 7 & 8 Readiness			
PC Security			
Anti-Virus			
Personal Firewall			
Encryption			
Backup & Recovery			
Patches			

Requires Native App on Device						
					✓	
					✓	
					✓	
					✓	
					✓	
					✓	
					✓	
					✓	
					✓	
					✓	
					✓	

Cloud Extender

	Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Cloud Extender		
Cloud Extender for Active Directory Authentication (for unattended enrollment only)			
Cloud Extender for BES			✓
Cloud Extender for Exchange/ActiveSync	✓		

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
✓	✓	✓	✓	✓	✓	✓	

	Exchange ActiveSync	Lotus Notes	BlackBerry Enterprise
	Cloud Extender		
Cloud Extender for Lotus Traveler		✓	
Cloud Extender for Certificate Authority integration			

iOS	Android	Kindle Fire	Win Phone 7.5	Win Phone 8	Windows Laptops	Mac	Comments
Requires Native App on Device							
✓	✓						