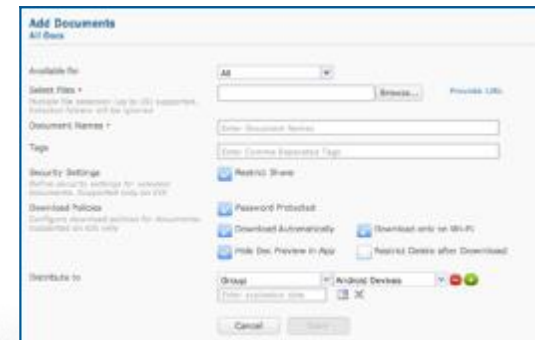


# Secure Document Sharing

A fully secure document container with expanded user support

- Securely distribute documents directly to the container
- Enforce user authentication
- Allow users to edit and share attachments
- Add, sync, and remove documents
- Protect sensitive documents with DLP controls
- Integrates with SharePoint and other file stores
- Works with Secure Mail for easy attachment viewing and security



# Secure Browser

A fully-functional web browser to enforce compliance and control access to content



- Define URL filters and security policies based on categories
- Block known malicious websites
- Enforce whitelist exceptions to specific websites
- Allow access to corporate intranet sites
- Restrict cookies, downloads, copy, paste, and print features to prevent data leaks
- Disable native and 3rd party web browsers
- Customizable event alerting and reporting

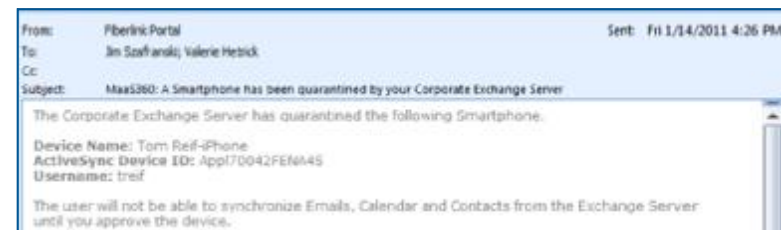
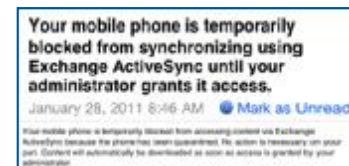
# Auto Quarantine?

With ActiveSync enabled, you can still require approval

End user receives an alert  
(from Exchange or Notes)

Admin receives an alert  
(from MaaS360)

Admin can view details, set policy,  
and approve the device



# OTA Configuration Management

## Passcode settings

## Corporate email, calendar and contacts

## Wi-Fi and VPN profiles

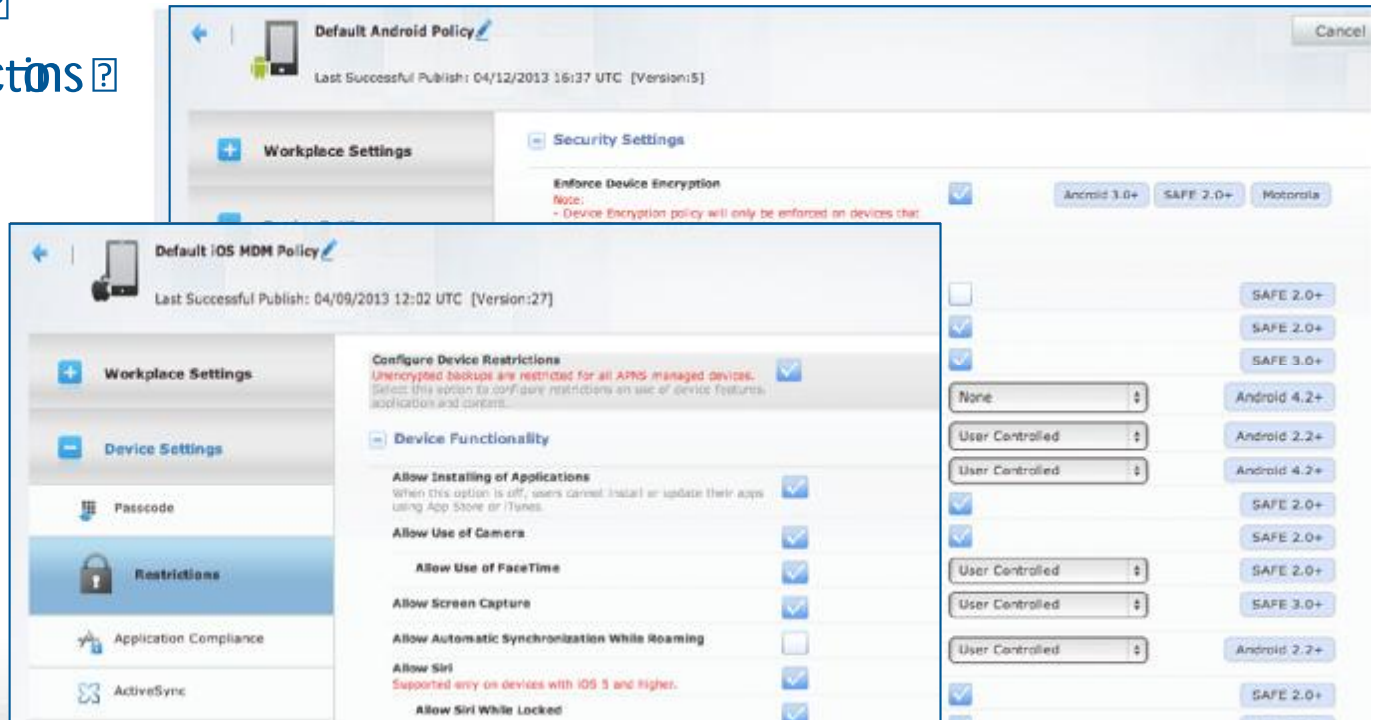
## Device features restrictions

- Camera
- FaceTime
- Siri
- iCloud
- Screen Captures
- ...and many more

## App compliance

## Roaming settings

## Device groupings



# Policy Enforcement

## Automated action on non-compliant events?

- Enforce MDM management
- Minimum OS version
- Remote wipe support
- SIM change
- Encryption support?
- Application compliance?
- Jailbreak / Root detection?
- Roaming state change

The screenshot displays the MaaS360 Policy Enforcement interface. On the left, a sidebar lists categories: Enforcement Rules, Geo-Fencing Rules, Monitoring Rules, and Expense Monitoring Rules. The main area shows a list of enforcement rules, each with a description and a checkbox. The 'Restrict Jailbroken (iOS) and Rooted (Android) Devices' rule is selected, and a configuration dialog is open over it. The dialog shows a dropdown menu with options: Alert Administrator, Alert User and Administrator, Block, Selective Wipe (highlighted with a checkmark), and Wipe. To the right of the dropdown, there is a button labeled 'Immediate' and a text field containing 'after warning'. Below these, a text box displays a warning message: 'You are in using a jailbroken or rooted device and in violation of company policy. Please contact IT for remediation instructions.'

**Enforcement Rules**

- Geo-Fencing Rules
- Monitoring Rules
- Expense Monitoring Rules

**Enforcement Rules List:**

- Enforce Enrollment: Ensure iOS and Android devices are enrolled in MDM and advanced management of the device has not been disabled or removed by the user.
- Enforce OS Versions: Ensure that your managed devices are up to date with the required OS versions. Please note that version check may be invalid on Rooted or Jailbroken devices.
- Enforce Remote Wipe Support: Ensure managed devices support remote wipe capabilities.
- Enforce Encryption Support: Ensure managed devices support designated levels of encryption.
- Enforce Application Compliance: Ensure devices are in compliance with application management requirements [required, disallowed & white list policies]. Application compliance is based on policy settings assigned to managed devices.
- Restrict Jailbroken (iOS) and Rooted (Android) Devices: Ensure managed devices are not jailbroken or rooted. iOS Application is required for Jailbreak detection.

**Configuration Dialog for 'Restrict Jailbroken (iOS) and Rooted (Android) Devices':**

- Alert Administrator
- Alert User and Administrator
- Block
- ✓ Selective Wipe
- Wipe
- Immediate after warning
- You are in using a jailbroken or rooted device and in violation of company policy. Please contact IT for remediation instructions.

**MaaS360 by Fiberlink**



# Contextual Event Management

## Location-Based Policies

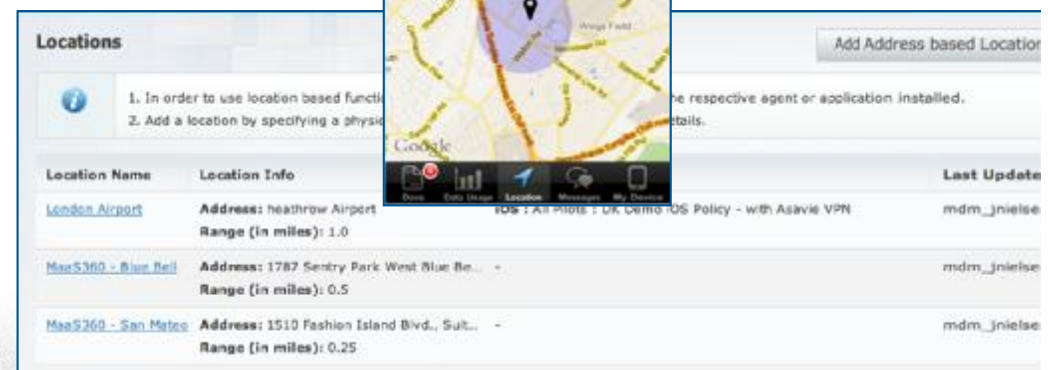
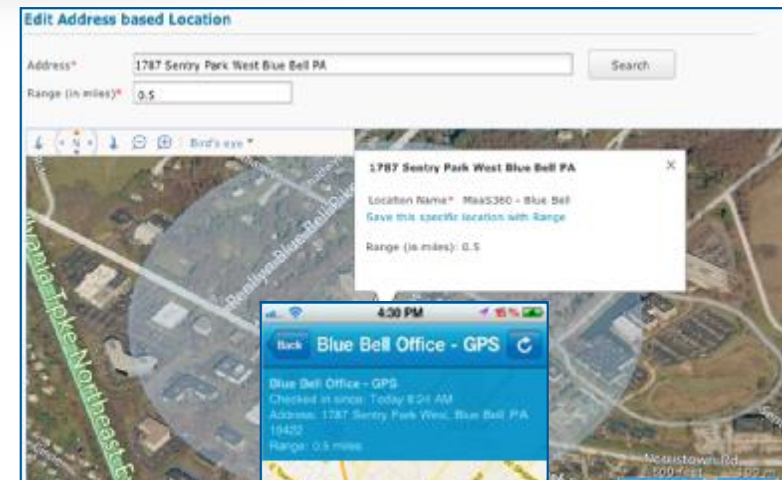
- Physical location (e.g. Address)
- Network connection (e.g. SSID)

## Dynamic Policy Assignment

- Change policy on:
  - Automated location Check in
  - Automated location Check out

## Geo-Fencing Rules

- Take action on:
  - Device leaving specified location
  - Device entering specified location



# BYOD Privacy Settings ? ?

Disable collection of personal information on a single device, all devices, ? ?  
or a device group

- App inventory information ?
- Location information ? ?
- IP address and SSID

The screenshot displays the 'Privacy Settings' configuration page. At the top right, there are buttons for 'View Change History' and 'Save'. The page is divided into two main sections: 'Restrict Location Information' and 'Restrict App Inventory Information'. Each section includes a descriptive text, a checkbox to enable the restriction, and a configuration area for ownership types and device groups.

**Privacy Settings** [View Change History] [Save]

**> Restrict Location Information**  
Restrict administrators from collecting location indicators such as Physical Address, Geographical Coordinates & History, IP Address and SSID. ☒

Select Applicable Ownership Types

<input checked="" type="checkbox"/> Corporate owned	<input checked="" type="checkbox"/> Employee owned
<input checked="" type="checkbox"/> Unknown	

Select Applicable Device Group: All Devices

**> Restrict App Inventory Information**  
Restrict administrators from collecting personal App Information. Apps distributed via the enterprise app catalog or part of corporate security policy will continue to be tracked. ☒

Select Applicable Ownership Types

<input type="checkbox"/> Corporate owned	<input checked="" type="checkbox"/> Employee owned
<input type="checkbox"/> Unknown	

Select Applicable Device Group: All Devices

# Mobile Expense Management

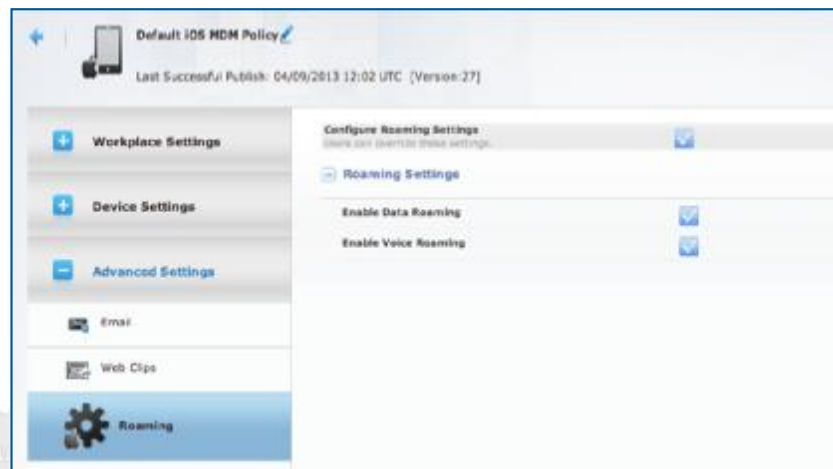
Real-time usage monitoring and alerting ? ?

Policies based on specific groups ?

Policies restricting or limiting roaming ? ?

Integrated reporting and analytics ? ?

On-device app to monitor usage





# Remote Help Desk Support

Reset forgotten device passcode?

Locate lost device

Buzz lost device

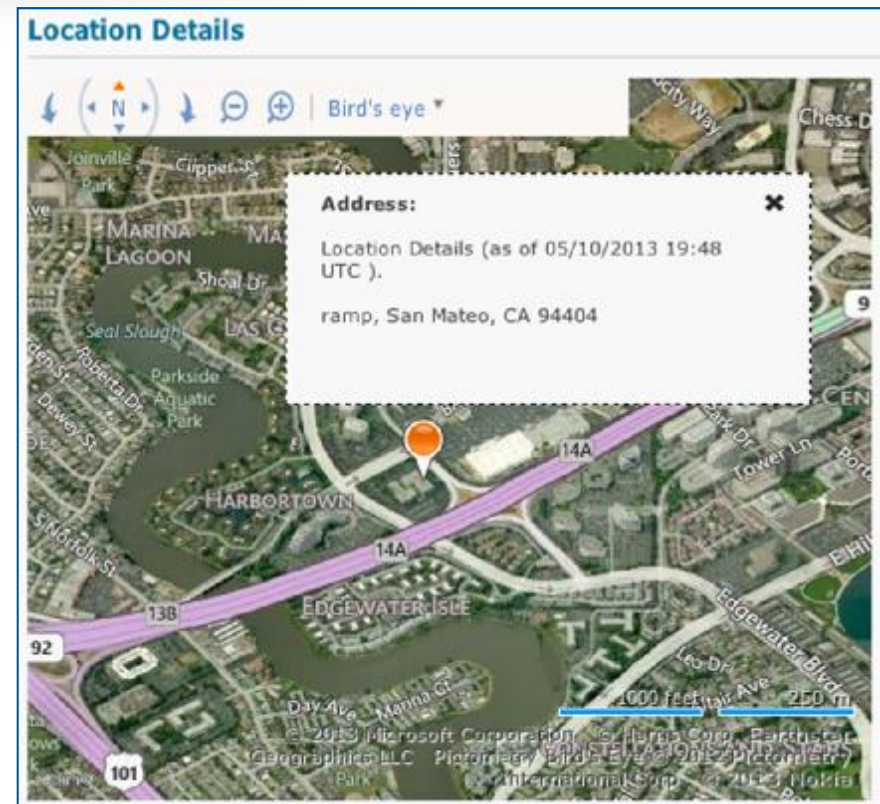
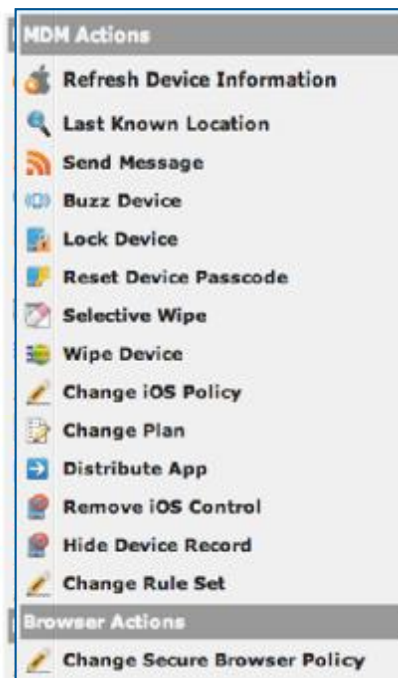
Selective wipe?

Full device wipe

Send message

Change policy

Remove control



# User Self Service Portal

Dedicated end user portal URL

Authenticated via AD or Local MaaS360

Take action on devices

- Lock device
- Reset device passcode
- Locate device
- Wipe device
- View action history

View personal & corporate devices

- View hardware & network information
- View security & compliance state

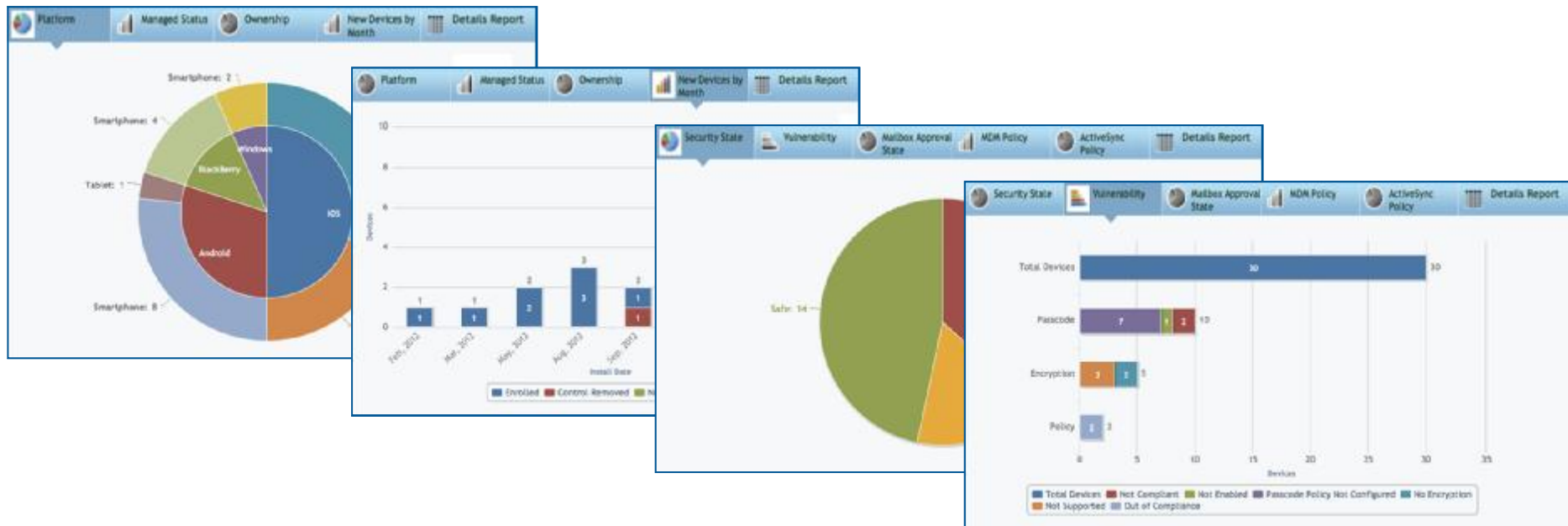
The screenshot displays the MaaS360 User Self Service Portal for user John Smith. The interface includes a welcome message, a 'My Personal Information' section with fields for Username (jsmith), Domain (mycompany.com), Email Address (jsmith), and Employee ID (3542). Below this, there is a list of devices: 'jsmith Windows Phone', 'jsmith iPhone', and 'jsmith iPhone 4S'. The 'jsmith iPhone 4S' device is selected, showing a dropdown menu with actions: 'Refresh Device Information', 'Lock Device', 'Reset Device Passcode', 'Wipe Device (MDM Action)', and 'Last Known Location'. The 'Wipe Device (MDM Action)' option is highlighted. The device details for the iPhone 4S are also visible, including the OS version (OS 6), Manufacturer (Apple), and Current Carrier (Not Available).

Hi John Smith, Welcome to MaaS360 User Self Service Portal			
My Personal Information			
Username	jsmith	Email Address	jsmith
Domain	mycompany.com	Employee ID	3542
<b>Devices</b>			
jsmith Windows Phone			
jsmith iPhone			
jsmith iPhone 4S			
<b>Actions for jsmith iPhone 4S</b>			
Action ▾ Show Action History			
Refresh Device Information			
Lock Device			
Reset Device Passcode			
Wipe Device (MDM Action)			
Last Known Location			
Manufacturer		Apple	
Current Carrier		Not Available	



# Mobility Intelligence™

Dashboards deliver a real-time, interactive graphical summary of your mobile environment and security overviews



# Mobile Metrics

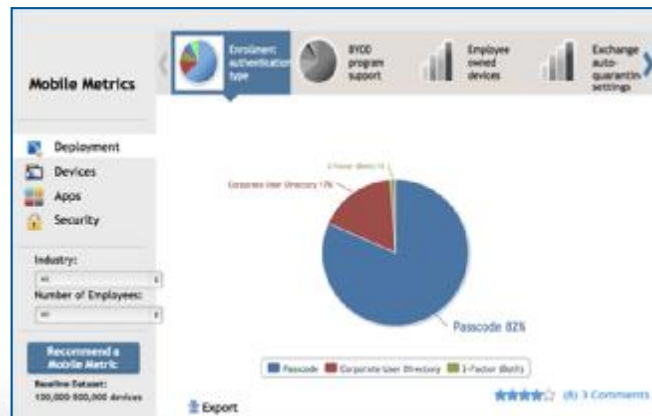
Benchmark key metrics

Compare against other MaaS360 customers

Learn what others are doing with mobility

Gain valuable insights and opportunities?

Make a stronger business case





# MaaS360 Device Management for Windows

Just as simple as managing mobile devices, all from a single portal  
Supports XP SP3, Vista, Windows 7, 8 (including Pro), and 32-bit and 64-bit where applicable

## Gain Instant Insight

- Hardware inventory
- Software inventory
- Security & compliance
- Custom attributes

## Take Immediate Action

- Enroll over-the-air
- Deploy Windows OS patches
- Distribute software via self-service
- Send message
- Lock device
- Erase the hard drive



# MaaS360 Managed Service for Windows

Delivered as a Managed Service

Supports XP SP3 and higher, Vista, Windows 7, 8 (Including Pro) and 32-bit and 64-bit where applicable

Standard Windows installation process

Gain Instant Insight

- Hardware inventory
- Software inventory
- Security & compliance
- Custom attributes

Managed Service Actions

- Send message
- Erase the hard drive
- Patch management
- Software distribution





# MaaS360 for Mac OS X

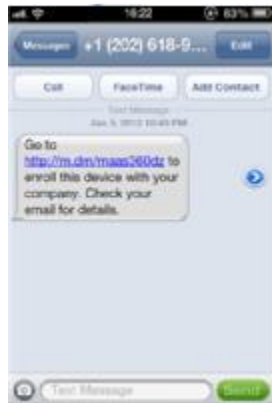
Easy enrollment process as simple as MDM

Gain Instant Insight

- Hardware inventory
- Software inventory
- Network information
- Software installed
- Operating system
- Missing OS patches
- Security & compliance
  - AntiVirus
  - Personal Firewall
- Data protection
- Custom attributes



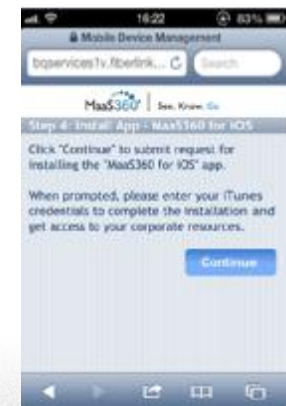
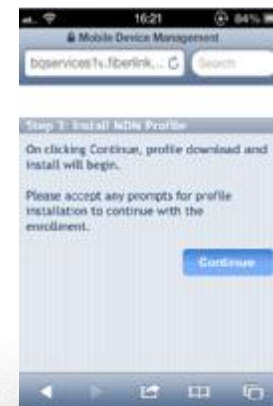
# Simple Enrollment



SMS text message

and/or

Email with one-time passcode + custom URL + QR code



## Unified Device Management With IBM Endpoint Manager and IBM MaaS360

## Consolidated view of managed endpoints (Laptops, Desktops, Servers, Mobile Devices)

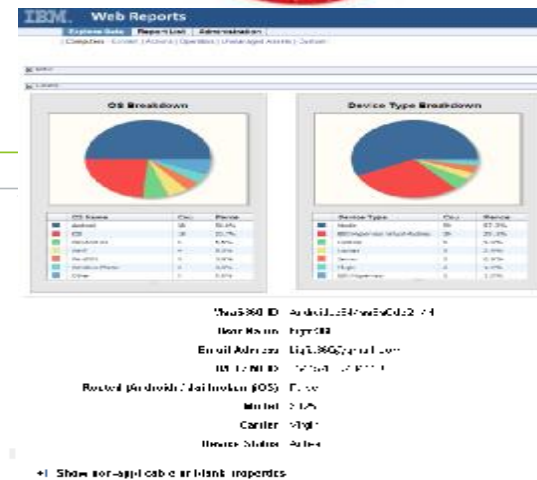
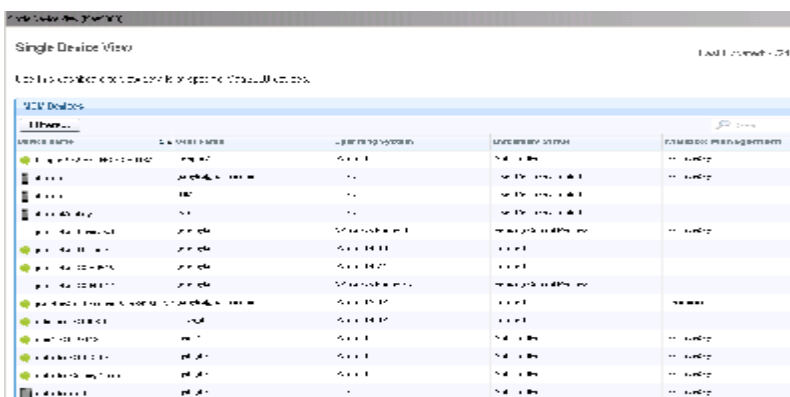
## ð Detailed mobile device views

### Ability to drive simple actions on mobile devices

(Lock, Wipe, Locate, etc)

## Consolidated asset reporting

Launch in context to IBM MaaS360 portal from IBM Endpoint Management for more complex workflow.



Within the IEM console, a list of MaaS360 registered devices are shown in the view:

**Single Device View**

Use this dashboard to view details of specific MaaS360 devices.

MDM Devices

Filters...

Device Name	User Name	Operating System	App Enrollment Status	Mailbox Enrollment Status
Alvin Liga-Divide-Android	alvin	Android	Inactive	ActiveSync
Efendi Chandra-Divide-Android	cefendi	Android	Inactive	ActiveSync
Daz's iPad	vtidarryl	iOS 7	Enrolled	
Manny Santana-Divide-iOS	santana	Android	Inactive	ActiveSync
Efendi Chandra-GT-P3100	cefendi	Android	Not Enrolled	ActiveSync

Last Updated: 14/07/2014 9:54:17 AM

**Single Device View**

Use this dashboard to view details of specific MaaS360 devices.

MDM Devices

Filters...

Device Name	User Name	Operating System	App Enrollment Status	Mailbox Enrollment Status
Alvin Liga-Divide-Android	alvin	Android	Inactive	ActiveSync
Efendi Chandra-Divide-Android	cefendi	Android	Inactive	ActiveSync
Daz's iPad	vtidarryl	iOS 7	Enrolled	
Manny Santana-Divide-iOS	santana	Android	Inactive	ActiveSync
Efendi Chandra-GT-P3100	cefendi	Android	Not Enrolled	ActiveSync
Alvin Liga-Divide-Android	alvin	Android	Inactive	ActiveSync

Last Updated: 14/07/2014 9:54:17 AM

IBM Service Engage

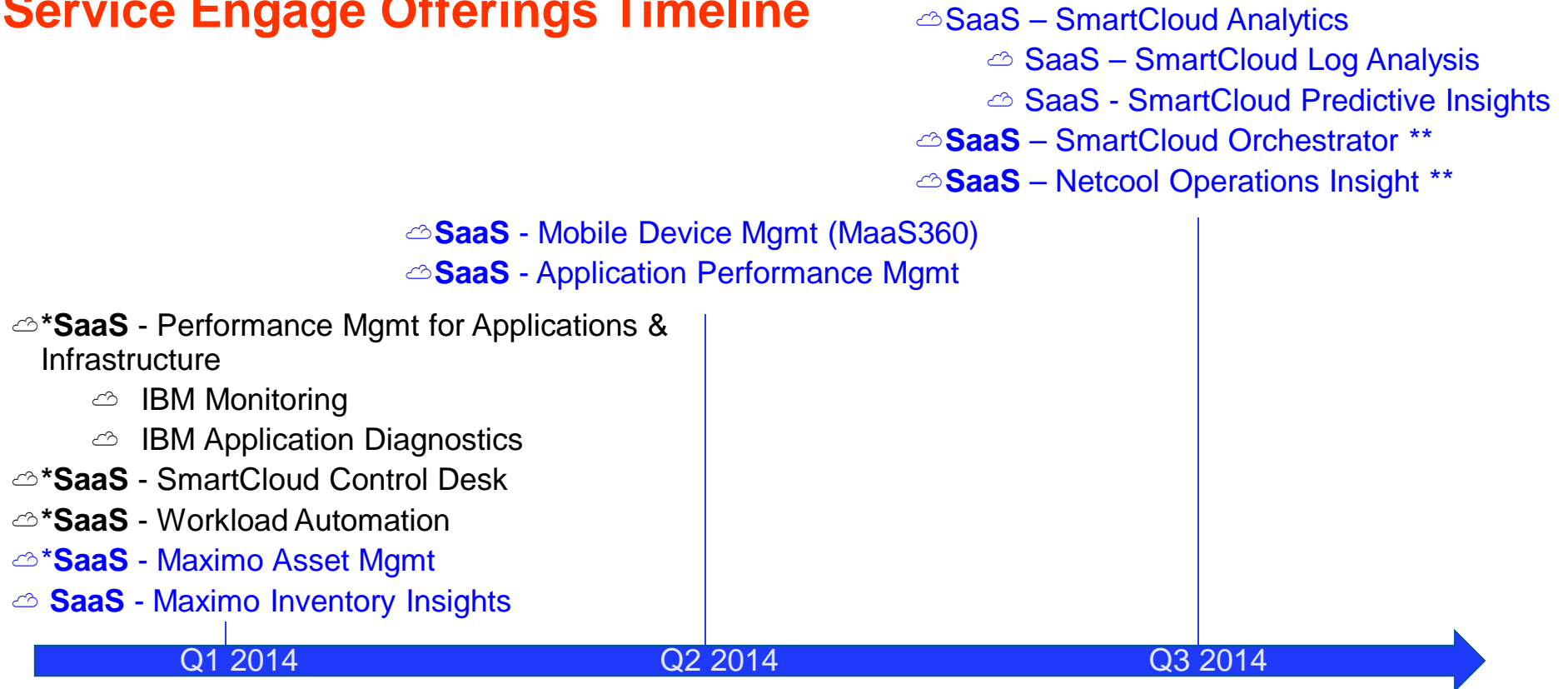
# IBM Service Management

*Engaging the new world of service management*



[IBM Service Engage](#)

## Service Engage Offerings Timeline





# IBM Unified Endpoint Management

*Manage your devices across the world*

Start your journey TODAY!



Marko Vahen, IBM  
C&SI, South East Europe

**Thank you**

