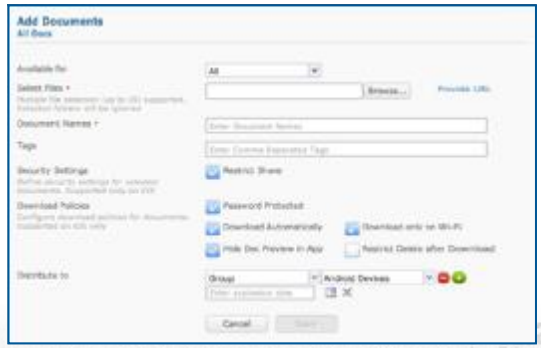
Secure Document Sharing

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

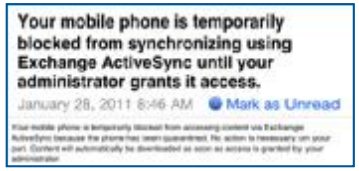
Auto Quarantine

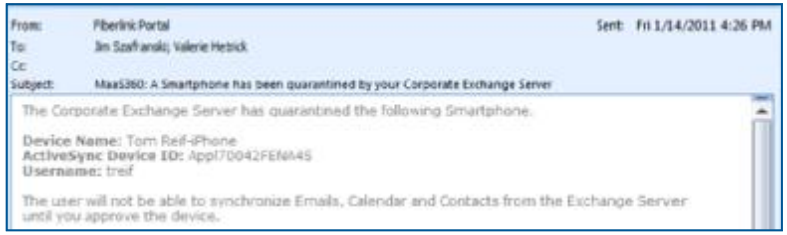
With ActiveSync enabled, you can still require approval

End user receives an alert (from Exchange or Notes)

Admin receives an alert (from MaaS360)

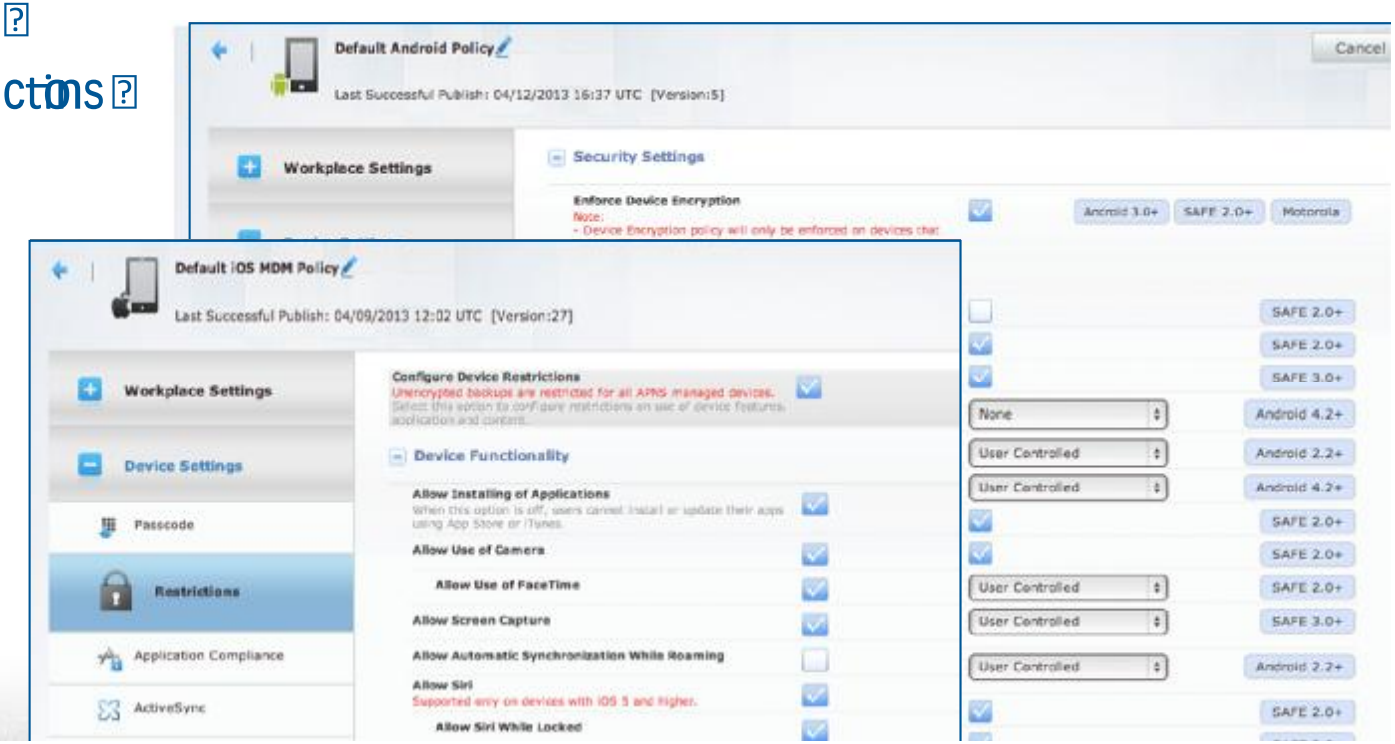
Admin can view details, set policy, and approve the device





OTA Configuration Management

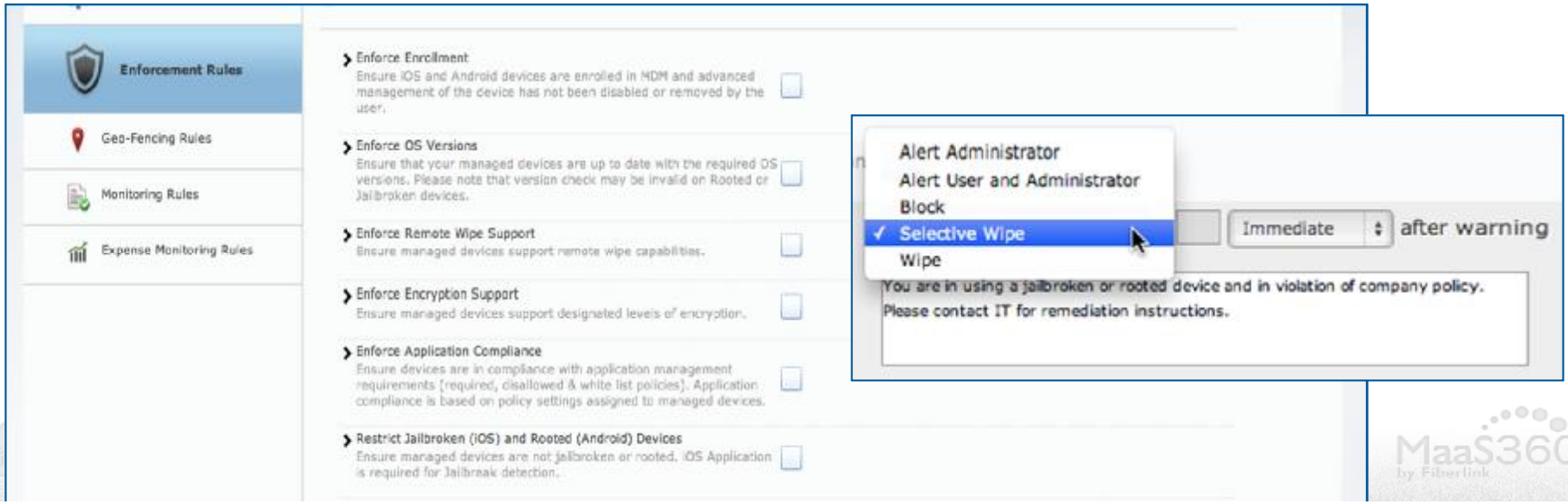
- Passcode settings
- Corporate email, calendar and contacts
- Wi-Fi and VPN profiles
- Device features restrictions
  - Camera
  - FaceTime
  - Siri
  - iCloud
  - Screen Captures
  - ...and many more
- App compliance
- Roaming settings
- Device groupings



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



Contextual Event Management

Location-Based Policies

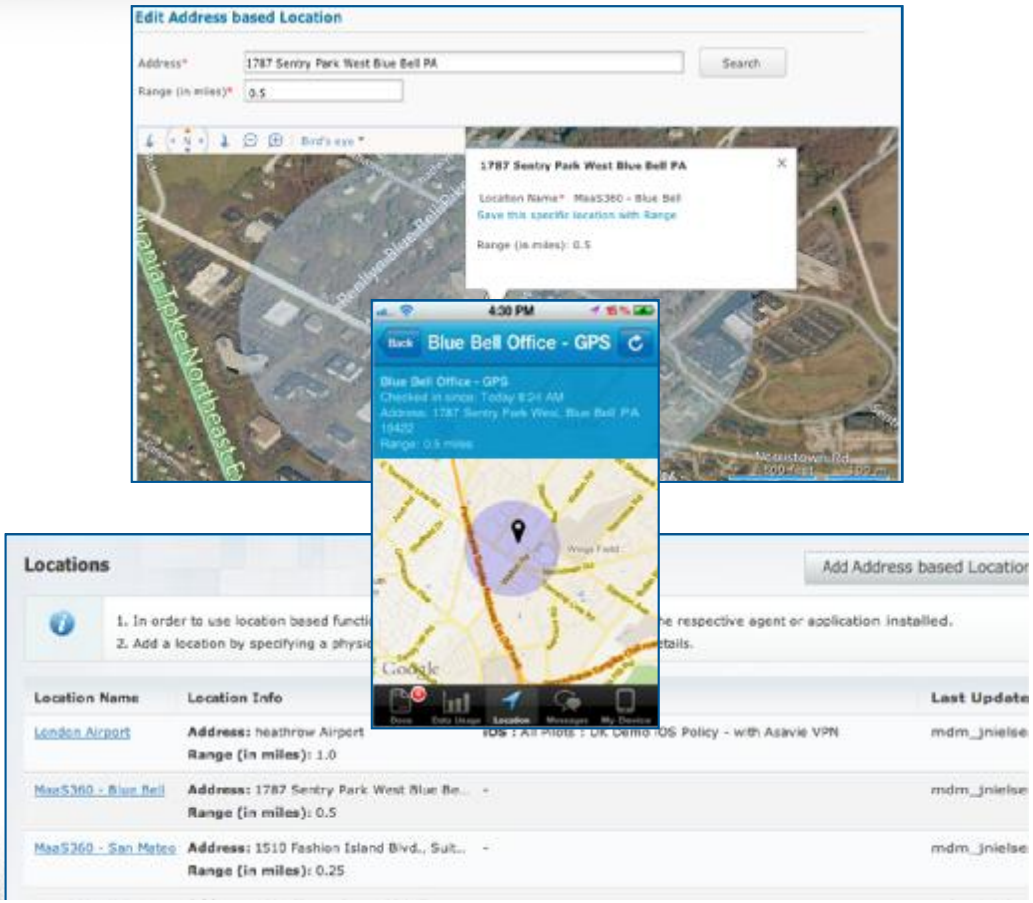
- Physical location (e.g. Address)
- Network connection (e.g. SSID)

Dynamic Policy Assignment

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

Geo-Fencing Rules

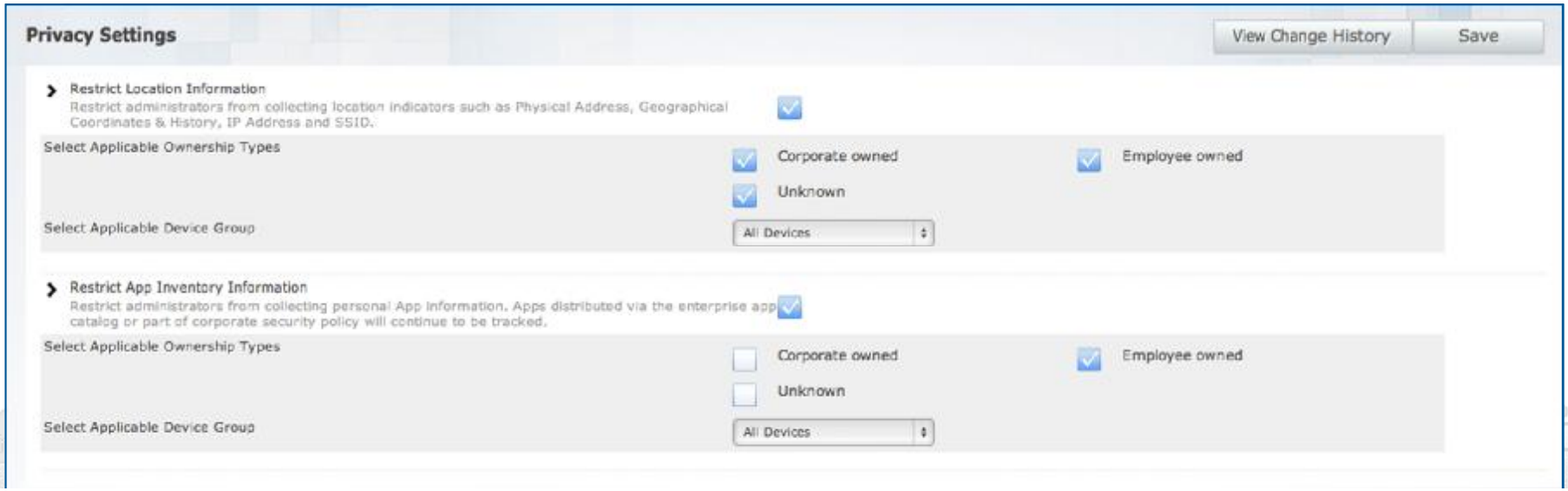
- Take action on:
  - Device leaving specified location
  - Device entering specified location



BYOD Privacy Settings

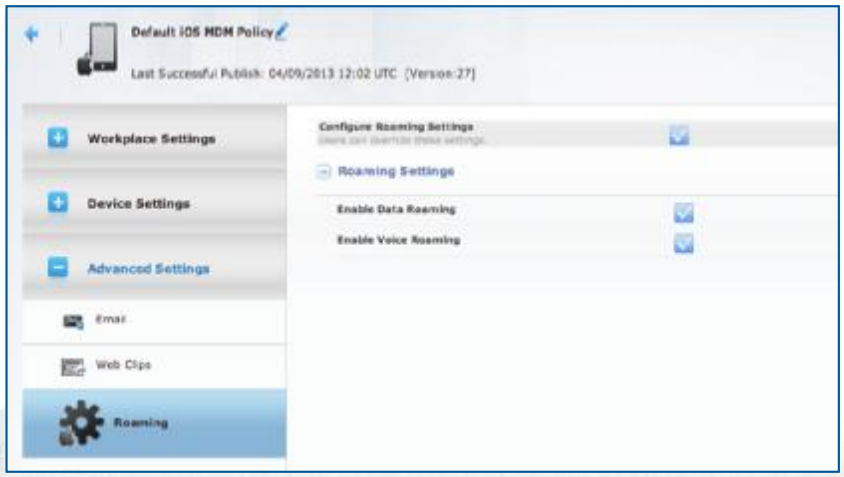
Disable collection of personal information on a single device, all devices, or a device group

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



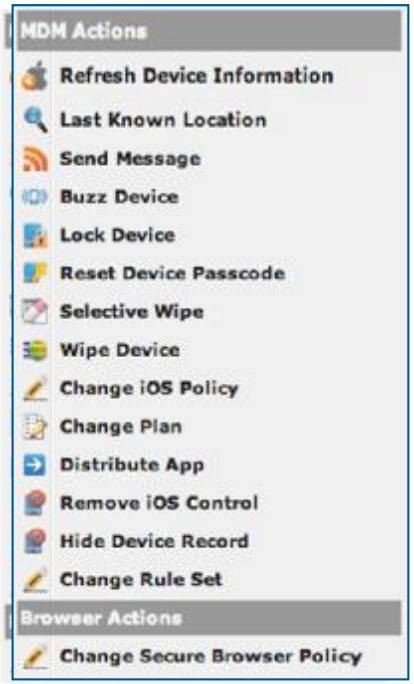
Mobile Expense Management

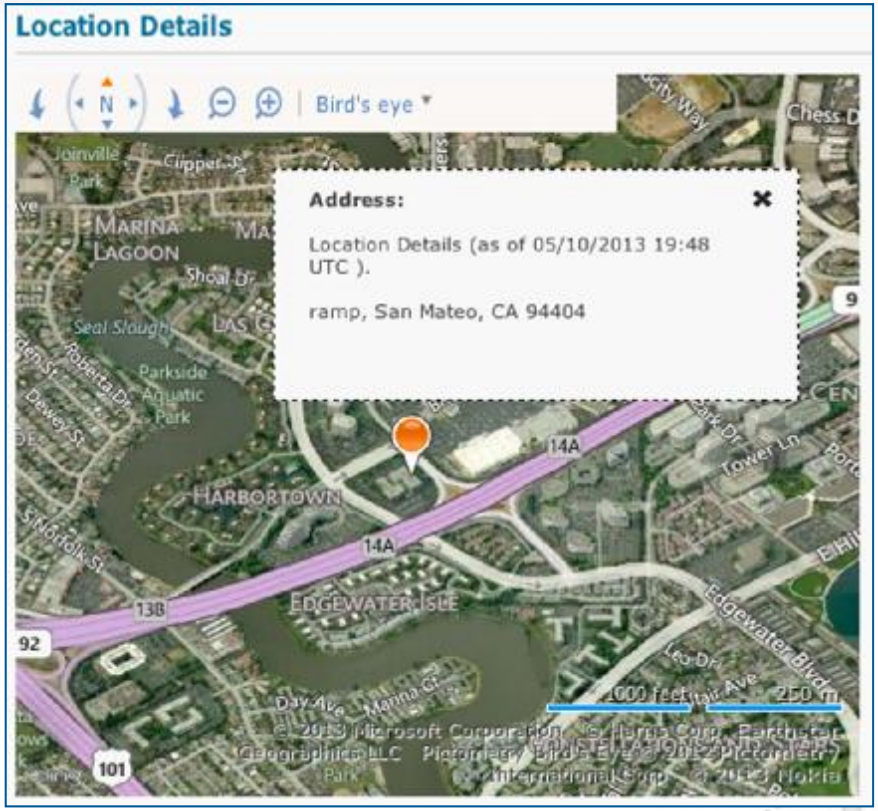
- Real-time usage monitoring and alerting
- Policies based on specific groups
- Policies restricting or limiting roaming
- Integrated reporting and analytics
- On-device app to monitor usage



Remote Help Desk Support

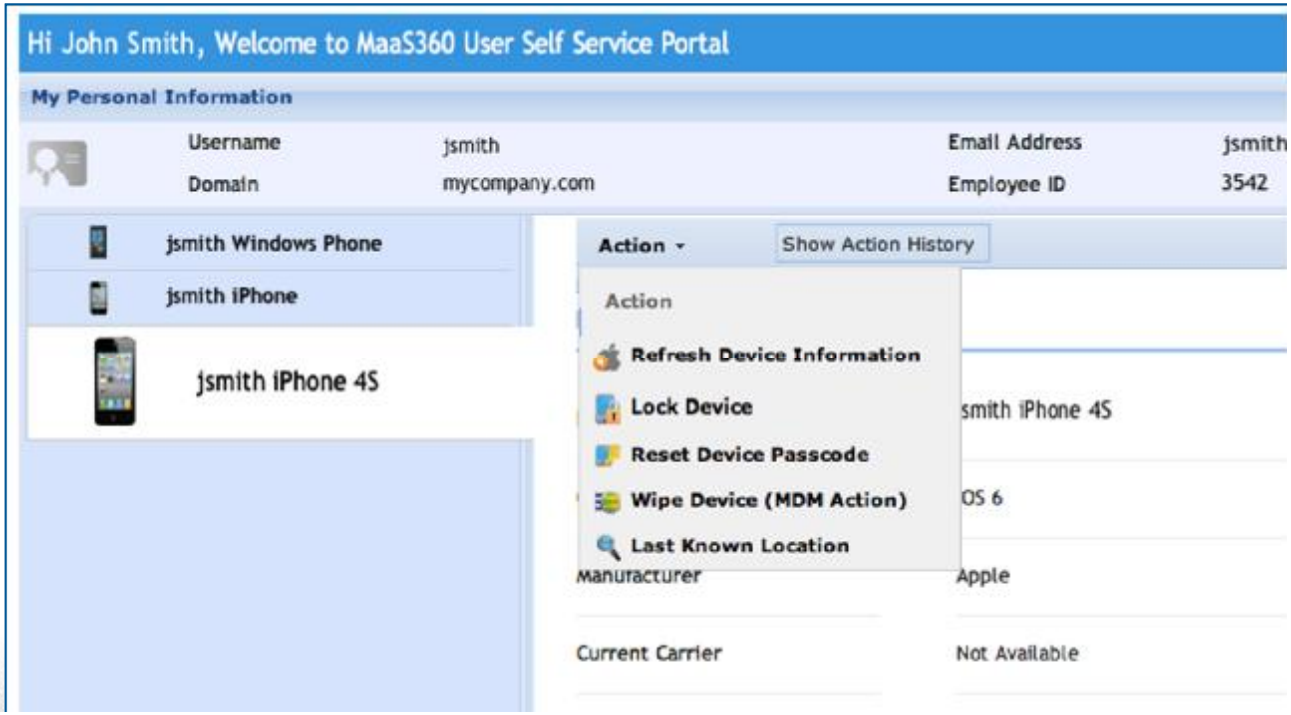
- Reset forgotten device passcode
- Locate lost device
- Buzz lost device
- Selective wipe
- Full device wipe
- Send message
- Change policy
- Remove control





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

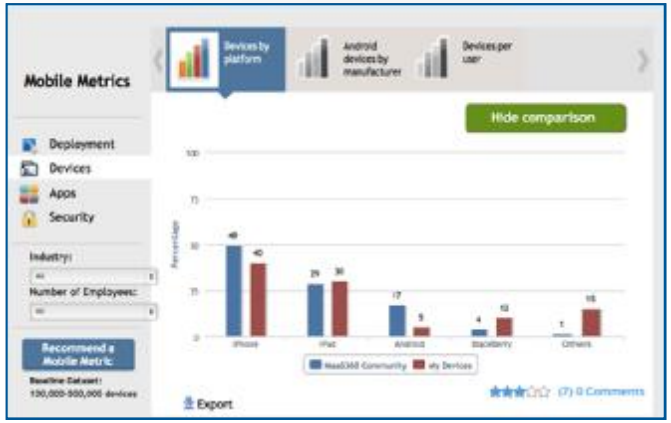


Mobility Intelligence™

Dashboards deliver a real-time, interactive, graphical summary of your mobile IT 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

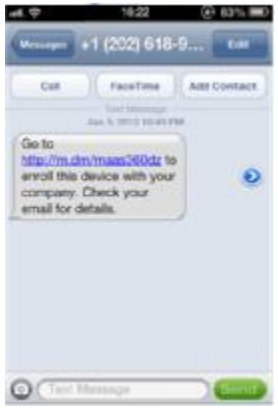
MaaS360 for Mac OS X

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
  - Anti-Virus
  - Personal Firewall
- Data protection
- Custom attributes

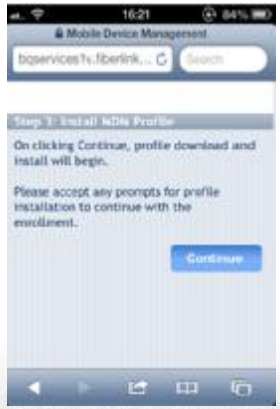
Simple Enrollment



SMS text message

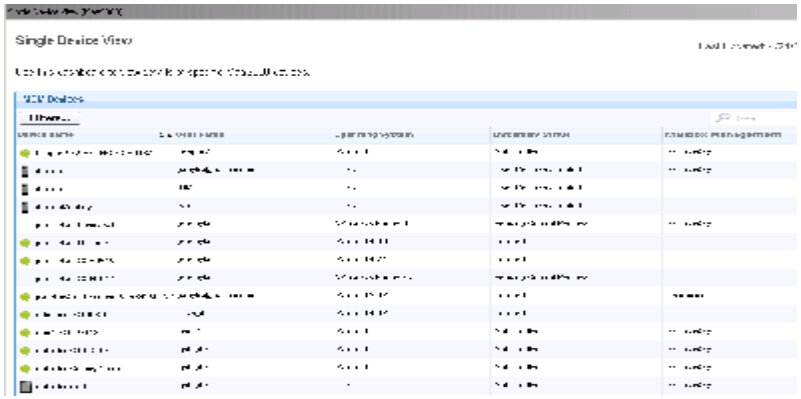
and/or

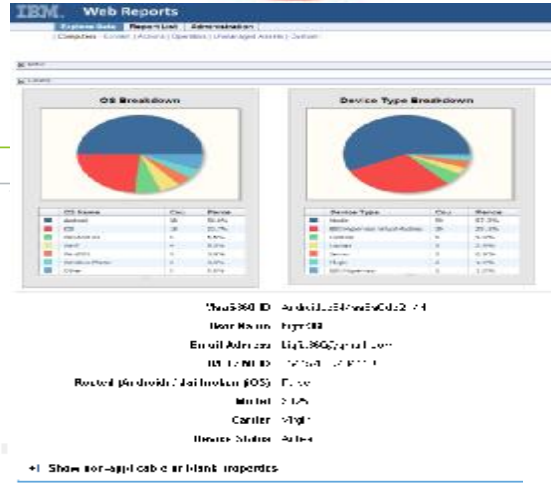
Email with one-time passcode + custom URL + QR code



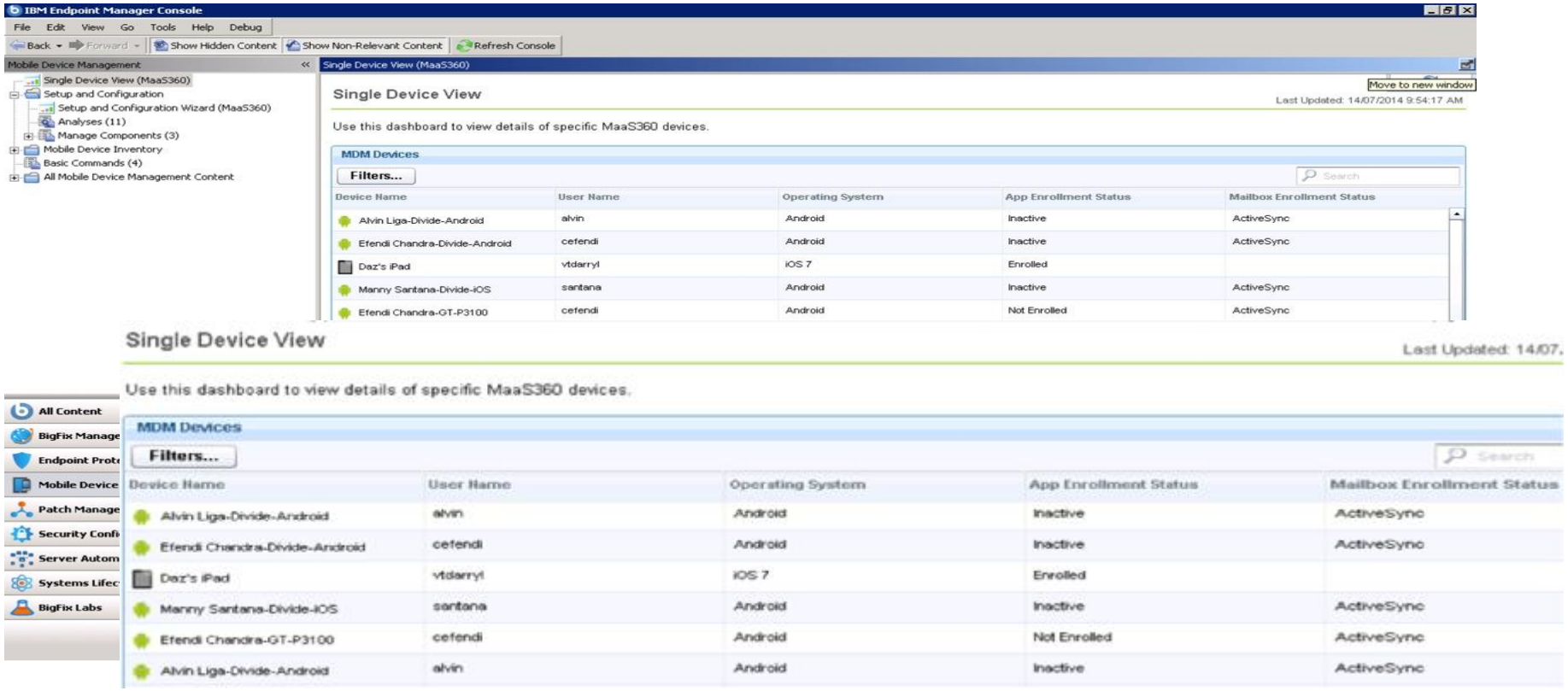
Unified Device Management with IBM Endpoint Manager and IBM MaaS360

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

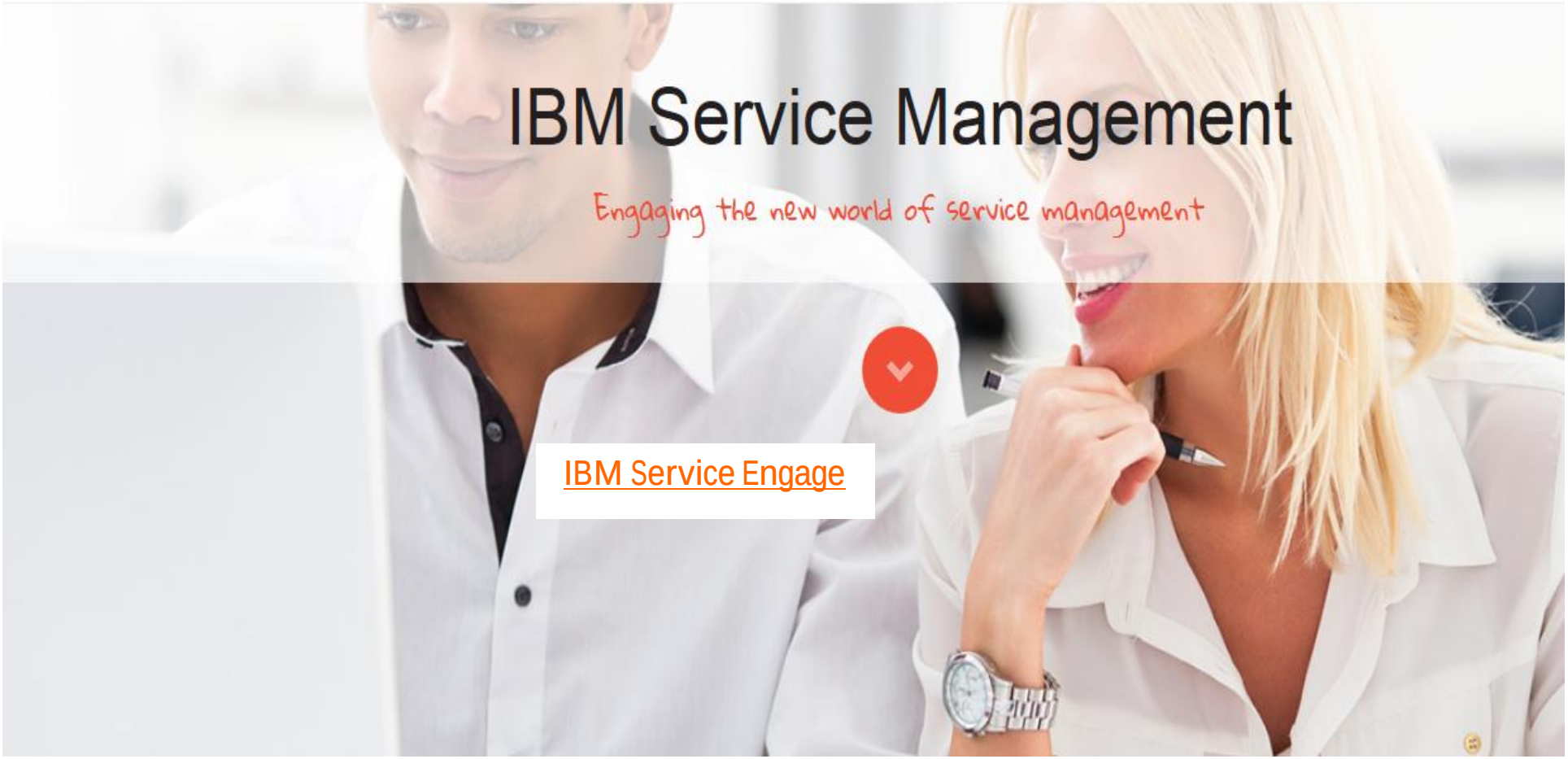




Within the IEM console, a list of MaaS360 registered devices are shown in the view:



IBM Service Engage



Service Engage Offerings Timeline

- SaaS – SmartCloud Analytics
  - SaaS – SmartCloud Log Analysis
  - SaaS - SmartCloud Predictive Insights
- **SaaS** – SmartCloud Orchestrator **
- **SaaS** – Netcool Operations Insight **

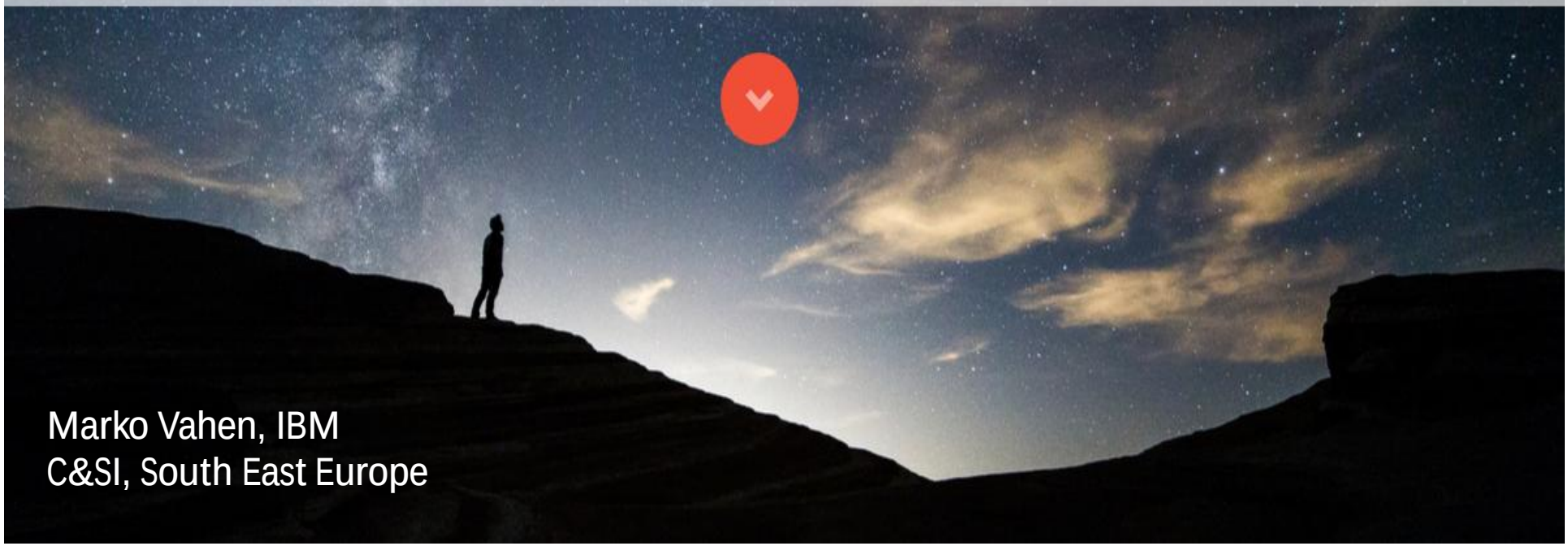
- **SaaS** - Mobile Device Mgmt (MaaS360)
- **SaaS** - Application Performance Mgmt

- ***SaaS** - Performance Mgmt for Applications & Infrastructure
  - IBM Monitoring
  - IBM Application Diagnostics
- ***SaaS** - SmartCloud Control Desk
- ***SaaS** - Workload Automation
- ***SaaS** - Maximo Asset Mgmt
- **SaaS** - Maximo Inventory Insights

IBM Unified Endpoint Management

Manage your devices across the world

Start your jurney TODAY!



Marko Vahen, IBM
C&SI, South East Europe

Thank you