ForeScout MDM

ForeScout MDM helps IT administrators streamline the process to provision, manage and secure today's expanding suite of smartphones and tablets, all from a single portal. ForeScout MDM for mobile devices is an easy to use platform that includes all of the essential functionality for end-to-end management of iOS, Android, BlackBerry, and Windows Phone devices.

ForeScout MDM is powered by MaaS360, a powerful cloud-based technology used by over 1200 companies around the world, and named the "Clear Choice Test" winner by Network World.

Total Endpoint Policy Management

With the explosion of handheld mobile devices, we are all hurtling toward a "post PC" world in which employees will be carrying various mobile devices, some owned by them, some owned by the company. This new paradigm of computing is challenging our existing paradigms of network security, data security, and device security.

Wouldn't it be nice if, instead of implementing new security silos that are limited to mobile devices, you could extend your PC and network security systems to encompass mobile devices? With a single unified security management and reporting system, you would be confident that your network is secure regardless of what type of device a user may be carrying – a PC, a Mac, a smartphone or tablet. You would minimize costs and administrative overhead.

That future is today.

ForeScout MDM

ForeScout MDM, powered by MaaS360, is an easy-to-use platform that includes all of the essential functionality that you need for end-to-end management of iOS, Android, Blackberry, and Windows Phone devices. And what's better is that it integrates with ForeScout CounterACT, our flagship network security and policy automation system, to give you unified visibility and control over everything on your network.

ForeScout MDM is a cloud-based solution, so deployment is quick and easy. In just a few clicks, IT can start enrolling devices and managing the entire mobile device lifecycle, from enrollment to security, monitoring, application management and support. Together with ForeScout CounterACT, ForeScout MDM provides a whole new level of centralized visibility and control for actionable insights into your entire computing landscape.

» **Secure all Mobile Devices -** ForeScout MDM supports all major smartphone and tablet platforms including iOS, Android, Windows Phone, and BlackBerry - in both Exchange and Lotus Notes environments.

» **Embrace BYOD -** ForeScout MDM provides workflows to discover, enroll, manage and report on personally owned devices as part of your mobile device operations.

» **Experience simple device enrollment and approval** - ForeScout MDM provides auto-quarantine for Exchange, and alerts IT personnel to approve all new devices. Additionally provides for easy user self-enrollment, via web, email or SMS.

ForeScout MDM is powered by MaaS360, a powerful cloud-based technology that is used to manage and secure more than one million endpoints for more than 1200 companies around the world. The MaaS360 platform was honored with the 2012 Global Mobile Award for "Best Enterprise Mobile Service" at Mobile World Congress.

ForeScout
Access ability.

iOS Visibility

- » Model and serial number
- » Operating system
- » Home network/current network
- » Amount of free storage
- » Applications, versions and size
- » Device ID (phone number, IMEI, email address)
- » Device configuration
  - Encryption level
  - Jailbreak detection
  - Passcode status
  - Device restrictions
  - Installed profiles
  - Security policies

iOS Actions

- » Refresh device details in real-time
- » Perform help desk operations like lock device, or reset passcode
- » Full or selective data wipe
- » Change iOS policy

Set and Distribute Policies

- » Enforce passcode requirements
- » Configure device restrictions
  - Enforce encrypted backups
  - Restrict the use of the camera, FaceTime, and screen capture
  - Restrict application installation
  - Restrict the use of YouTube, Safari, and voice dialing
  - Distribute Wi-Fi, VPN, and email profiles, such as Exchange ActiveSync settings
  - And much more…

Application Storefront

- » Suggest iTunes applications for employees
- » Distribute "home grown" applications
- » Publish updates to applications
- » Distribute documents to devices

How ForeScout MDM Works

With an intuitive interface and easy to use workflows, ForeScout MDM enables you to support the entire mobility lifecycle -- from enrollment to configuration management, compliance, security, app and document management, along with help desk support.

Provision

ForeScout MDM streamlines the configuration and device enrollment process using SMS, email or URL to make life simple for IT and mobile employees. Device enrollment takes just minutes instead of hours. ForeScout MDM discovers new users and devices, and allows IT to launch a simple end-user self-service over-the-air enrollment process.

Integrate

With ForeScout MDM Cloud Extender, you can securely integrate with all major email, calendar and contacts platforms including Exchange, Lotus Notes, and Microsoft's Office 365, plus Active Directory and any required Certificate Authorities.

Manage

OTA configuration management provides simple delivery and maintenance of corporate device profiles, including WiFi and VPN settings. Through device quarantine and approval, IT is automatically notified of any new devices on the network and can block or approve them, ensuring compliance with corporate policies.

Secure

ForeScout MDM provides dynamic, end-to-end security and compliance management. Enforcement of passcode policies and strong encryption keys protects sensitive business and personal data on mobile devices. Through real-time compliance management, ForeScout MDM can detect when users opt out of your MDM program, install prohibited applications, or initiate SIM changes. Based on this information, you can take automated actions such as messaging the user, blocking email, or wiping corporate data from the device. Through integration with ForeScout CounterACT, you can quarantine the device or remove it from the network.
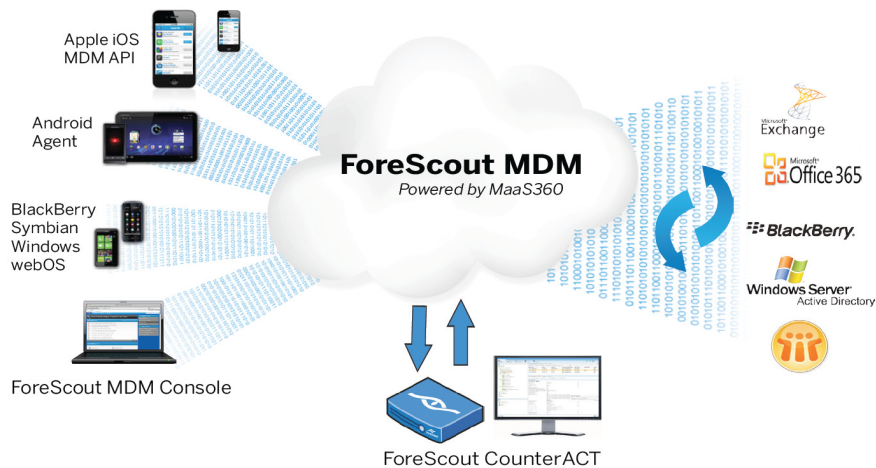
Monitor

Dashboards deliver an interactive, graphical summary of your mobile device operations and compliance. ForeScout MDM provides integrated reporting and analytics to provide a high level view into your mobile device landscape across your enterprise with detailed hardware and software inventory reports, plus configuration and vulnerability details.

Support

ForeScout MDM provides robust help desk capabilities for support procedures such as locating a device with GPS, resetting a user's passcode, and sending a direct message to a device. ForeScout MDM also provides an end-user support portal that allows users to do basic self-management of their device, such as wiping or resetting the password on a lost device.

Optional App Management

ForeScout MDM allows enterprises to have their own App Catalog of approved or recommended public applications and in-house developed applications. Within the catalog users can instantly view apps available to them, install apps, and be alerted to update apps. Additionally, our SDKs allow enterprises to more easily develop in-house apps for key functions such as authentication, updates, and usage reporting.

Apple iOS
MDM API

Android
Agent

BlackBerry
Symbian
Windows
webOS

ForeScout MDM Console

ForeScout MDM
Powered by MaaS360

Exchange

Office 365

BlackBerry.

Windows Server
Active Directory

ForeScout CounterACT

The Benefits of Integration

Mobile Device Management (MDM) can help IT security managers secure mobile devices and the sensitive corporate data that is frequently stored on such devices. But by itself, MDM is not a complete security solution for the following reasons:

1. MDM systems can only see and manage devices that have already been enrolled in the MDM system. MDM has no control over unmanaged devices on the network.

2. MDM systems typically do not control access to the network. Thus, MDM does not prevent unauthorized access to the network, nor does MDM prevent infecteddevices from attacking the network.

3. MDM systems typically do not manage personally-owned Windows and MacOS computers. Thus, MDM is not a comprehensive solution for BYOD.

4. MDM systems are often operated as another management silo, with another set of reports.

Through a simple plug-in module, ForeScout MDM can integrate within the broader context of unified security control that ForeScout CounterACT provides. Once integrated, you will obtain many valuable synergies:

» **Automated real-time detection of** mobile devices the moment they try to connect to your network, including unmanaged and unknown devices.

» **Improved security** by blocking unauthorized users and devices from the network.

» **Unified compliance reporting** for all endpoint devices PCs, smartphones, and tablets.

» **Automated installation of MDM agents** by directing unmanaged devices to an installation web page.

» **Unified network access control** policy enforcement options

• **Allow** compliant and managed devices onto the network.

• **Limit** network access based on device type, ownership, time of day, and compliance.

• **Block** non-compliant, or certain types of devices, from your network completely.

» **Guest registration** for personal mobile devices that are not owned by employees, Once a guest has registered and been approved, ForeScout CounterACT can restrict the user's access to just the Internet.

» **Continuous protection**. If malware on a mobile device tries to propagate or interrogate your network, ForeScout CounterACT will block the threat, and remove the device from your network.

Android Visibility

» Device ID (phone number, IMEI, email address)

» Serial number

» Processor and RAM

» Amount of free storage

» Battery level and condition

» Operating system

» Home network/current network

» Applications, versions and size

» Device restrictions

» Security policies

• Encryption level
• Rooted detection
• Passcode status

» Running services

Android Actions

» Refresh device details in real-time

» Perform help desk operations like send message, lock device, reset passcode

» Full or selective data wipe

» Locate lost devices

» Change Android policy

Set and Distribute Policies

» Enforce passcode requirements

» Configure device restrictions

• Application blacklisting

• Data roaming, Bluetooth, tethering

• Non-market application installation

• Distribute email, Wi-Fi, VPN profiles to supported devices

Application Storefront:

» Suggest Android applications for employees

» Distribute "home grown" applications

» Publish updates to applications

» Distribute documents to devices

	NAC Alone	MDM Alone	NAC+MDM
Visibility	Basic OS info on all devices	Full info on managed only	Complete
Network Access Control	Complete	No	Complete
Mobile device compliance	Very limited	Complete	Complete
Agent deployment	Network based	Pre-registration	Both

The ForeScout Difference

Choices are good. Unlike other security vendors, ForeScout lets you choose your level of investment in mobile security, which may be different for different classes of users. This lets you "right size" your security program.

If you are looking for a strong foundation of basic mobile security, then our flagship product ForeScout CounterACT is right for you. It works with PCs and handheld devices. It gives you immediate, real-time visibility of every device on your network, without the need for agents or enrollment. It ties into directory services and provides role-based network access control. Different users and devices can get different access. The price is low, and the impact to your users is trivial because it's transparent.

If you need stronger mobile security, we offer ForeScout CounterACT with our optional ForeScout Mobile Security Module. With ForeScout Mobile Security Module, you gain deep inspection of Android and iOS devices, so you can determine the security posture of the device. This lets you enforce more sophisticated network access control policies. In addition, you can manage the security configuration of Apple iOS devices.

For the strongest security, combine ForeScout MDM with ForeScout CounterACT. ForeScout MDM provides the most extensive feature set and wide support of mobile platforms. As described previously, when you link ForeScout MDM to ForeScout CounterACT, you gain significant benefits in terms of stronger security and improved operational efficiency.

Or, choose all three solutions. By using a tiered security approach—deploying the MDM solution for only your most critical users—you can save money compared with using MDM on every device.

Device Support

- » iOS version 4.0 and higher
- » Android version 2.2 and higher
- » BlackBerry Enterprise Server (BES) version 5.0 and higher
- » Windows Phone—all operating systems when integrated with Exchange ActiveSync and Lotus Traveler
- » Symbian—all operating systems when integrated with Exchange ActiveSync and Lotus Traveler

About ForeScout

ForeScout Technologies is a leading provider of automated security control solutions for Fortune 1000 enterprises and government organizations. With ForeScout, organizations can accelerate productivity and connectivity by enabling people to access corporate network resources where, how and when needed without compromising security.

ForeScout's automated solutions for network access control, mobile security, endpoint compliance and threat prevention empower organizations to gain access agility while preempting risks and eliminating remediation costs. ForeScout CounterACT has been chosen by over 1300 of the world's most secure enterprises and military installations for global deployments spanning 37 countries. The company delivers its solutions through its network of authorized partners worldwide. http://www.forescout.com