

# Forescout eyeExtend for MobileIron® UEM

## Automate mobile device enrollment, improve security management and enforce continuous compliance

Whether on the road or in the office, enterprise employees increasingly access corporate resources and data via their laptops, tablets and smartphones. These same mobile devices can also be found monitoring, managing and controlling Internet of Things (IoT) devices in operational technology (OT) networks, potentially allowing threats to jump from one part of the network to the other. Enterprises implement unified endpoint management (UEM) platforms such as MobileIron UEM to help manage and secure mobile devices and applications accessing the network. However, effective security and management in the face of today's sophisticated, fast-changing threats remains a challenge, particularly for bring your own device (BYOD), guest and other nontraditional devices that are not always visible, compliant or enrolled in an UEM platform.

Forescout eyeExtend for MobileIron fills in the security and mobile device gaps left by MobileIron UEM alone. This enables robust, enterprise-wide mobile device management, security, compliance and access control to help IT and security administrators streamline the process of managing and securing an increasingly diverse and expanding mobile device environment.

### Challenges

- Discovering, classifying, assessing and monitoring all IP-connected corporate and BYOD mobile devices accessing corporate resources in real time
- Ensuring all mobile devices are enrolled in MobileIron UEM for unified management
- Reducing IT and security staffs' manual workload of managing device hygiene and compliance
- Reducing lengthy response times and automating manual processes to address security threats posed by noncompliant and compromised mobile devices

### The Solution

Forescout eyeExtend for MobileIron UEM orchestrates information sharing and workflows between the Forescout platform and MobileIron UEM to help organizations improve security, compliance and control of all mobile devices accessing corporate data.

eyeExtend for MobileIron UEM powered by the Forescout platform helps organizations streamline and automate enrollment of unregistered mobile devices in MobileIron UEM. It works with MobileIron UEM to reduce any manual workload that your IT staff has for enrolling devices not listed in MobileIron UEM as they come onto your network. In addition to helping with mobile device enrollment, the Forescout platform helps ensure that, as devices connect to the network, they have the right security posture and are compliant throughout the time they remain connected to the



eyeExtend

### Benefits

- <> Gain complete visibility across all IP-connected devices, including mobile devices accessing corporate networks
- <> Increase operational efficiency through real-time assessment and enrollment of mobile devices in MobileIron UEM
- <> Reduce security risk by continuously enforcing proper device configuration and security policies
- <> Automate remediation and response for noncompliant or compromised mobile devices

### Highlights

- <> Real-time discovery of diverse mobile devices without requiring agents
- <> Seamless enrollment of non-registered devices to MobileIron UEM
- <> Policy-driven device wipe, forced check-in and other enforcement actions for jailbroken or noncompliant devices
- <> Network access control that dynamically quarantines or blocks deviant devices from accessing the corporate network

network and continuously monitors all mobile devices against MobileIron UEM security policies. If a device falls out of compliance or gets compromised as identified by the Forescout platform or MobileIron UEM, Forescout eyeExtend can help orchestrate the remediation process automatically with MobileIron UEM to help increase security operations efficiency while reducing business risk in real time.

In summary, eyeExtend for MobileIron UEM helps you with unified security management for all mobile devices on the network, regardless of type (PC, tablet, smartphone), connection (wired wireless, VPN), location (on-premises and off-premises), or ownership (corporate or personal).

## Use Cases

### Automate MobileIron UEM Device Enrollment

The Forescout platform helps drive MobileIron UEM device enrollment by continuously discovering and relaying enrollment and compliance state information to MobileIron UEM for diverse PCs, Macs, Linux, smartphones and tablets the moment they connect to the network. It automates device onboarding by directing new devices to self-register with MobileIron UEM in real time.

### Enforce Device Compliance

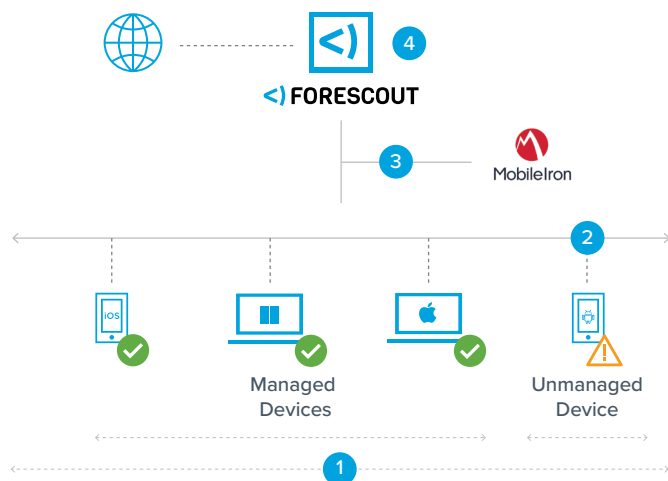
If devices deviate from security policies, the Forescout platform restricts their access to the network and notifies security and IT administrators. It can automatically take policy-driven actions such as a full wipe of jailbroken devices or forced device check-in to connect to the MobileIron Core for other noncompliance issues—either natively or through MobileIron UEM.

### Apply custom access controls

The Forescout platform enables enterprises to control access to resources based on user profile (guest, employee, contractor) and device classification by operating systems. You can apply differentiated access for guest and BYOD mobile devices by limiting their access to the guest wireless network.

### Accelerate response actions and remediation

When a device is identified as either noncompliant or compromised, the Forescout platform can dynamically quarantine or block the device from accessing the network and can initiate remediation workflows until the device is deemed compliant and healthy. It can also proactively target remediation actions such as installing required security software, updating agents or applying security patches.



- 1 Forescout discovers, classifies and assesses all devices connecting to the network.
- 2 Forescout verifies with MobileIron UEM if the device is enrolled with it
- 3 If not enrolled, Forescout restricts the device's network access and redirects it for self-enrollment in MobileIron UEM.
- 4 Forescout moves device back to appropriate network access once MobileIron UEM confirms endpoint is managed and policy compliant



Forescout Technologies, Inc.  
190 W Tasman Dr.  
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771  
Tel (Intl) +1-408-213-3191  
Support +1-708-237-6591

Learn more at [Forescout.com](https://www.forescout.com)

© 2020 Forescout Technologies, Inc. All rights reserved. Forescout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents can be found at [www.forescout.com/company/legal/intellectual-property-patents-trademarks](https://www.forescout.com/company/legal/intellectual-property-patents-trademarks). Other brands, products, or service names may be trademarks or service marks of their respective owners. Version 12\_19