MobileIron

White Paper

Real-World Scale for Mobile IT: Nine Core Performance Requirements

Mobile IT Scale

As the leader in Mobile IT, MobileIron has worked with hundreds of Global 2000 companies to scale their mobile deployments.

This experience has identified nine core performance requirements for real-world scale in large mobile enterprises:

- Simultaneous registrations
- Complex configurations
- High-volume app delivery
- High-volume certificate management
- High-volume email delivery
- Operational longevity
- Scalability with iOS and Android
- Network integration
- Operational efficiency

Contact

MobileIron
415 East Middlefield Road
Mountain View, CA 94043 USA
Tel. +1.650.919.8100
Fax +1.650.919.8006
info@mobileiron.com
www.mobileiron.com

Introduction

Mobile enterprise computing is a relatively new phenomenon, and the IT community is still learning about the factors that affect scalability. Mobile IT is quite different from traditional corporate computing environments, which are based on laptops and desktops. Organizations can be taken by surprise unless they gain expertise on the real-world scalability issues inherent in mobile and how to address them. Many mobile device management (MDM) and mobile application management (MAM) vendors will claim scale without being able to define, substantiate, or even test actual performance.

This paper is intended for large enterprises planning smartphone and tablet deployments greater than 20,000 devices. It describes the key performance requirements for deploying a scalable mobile infrastructure, the importance of these requirements, and how MobileIron's Mobile IT platform is uniquely architected to meet these requirements for the security and management of mobile apps, content, and devices.

What Makes Mobile Scale Different?

The unique scalability requirements for mobile computing arise from the following important differences between mobile and desktop environments. Note that, for the purposes of this document, "desktop" represents the traditional desktop and laptop, and "mobile" represents the new generation of smartphones and tablets.

- **Configuration**: Device models and operating system (OS) versions change much more frequently on mobile than on desktop. Even more importantly, mobile OS upgrades are controlled by the user, not by IT, so the variability of configurations is much greater and keeping track of them is harder.
- **Compliance**: Mobile devices fall out of compliance more frequently than desktops because IT cannot image or lock them down as tightly. The end user is given more freedom because user experience is paramount for mobile adoption, and the mobile device is often owned by the employee, not the company.
- **Number of devices**: The total number of mobile devices in an enterprise will dramatically exceed the number of desktops because many employees will have two or more smartphones and tablets. Even employees without a desktop, such as field workers, carry mobile devices.
- **Number of apps**: The total number of mobile apps is higher, and the pace of introduction is faster than for desktop apps. Mobile apps are smaller in scope,

task-specific, and in high demand by the business. Large enterprises will support hundreds of mobile apps running on thousands of devices.

- **Wireless infrastructure**: Mobile apps are updated more frequently than desktop apps. Mobile app installation files are large because mobile is an immersive experience, and apps often rely on rich media. Many MobileIron customers have apps with a download size greater than 100MB. Because of the sheer number of mobile apps and devices, the corporate wireless network can get hit with massive load during initial app installations and ongoing app upgrades. Unlike the desktop, the mobile app download is almost always user-initiated and wireless, so the load is unpredictable.
- **Identity**: Mobile IT is increasingly using certificates to manage identity, an approach that is much less common on desktops. Certificates authenticate users and devices without forcing the user to continually re-enter credentials, thereby establishing identity and improving the user experience.
- **Access control**: Access control is at the core of mobile security. Since mobile endpoints can fall out of compliance frequently, the ability to block access to corporate email and apps or to quarantine the device based on the security state (“posture”) of the device is very important. Access control for mobile fulfills the promise of traditional network access control (NAC) solutions for desktops. Those solutions were not designed for mobile devices and the more complex rules governing their access.
- **New platforms**: Finally, unlike corporate desktop environments, which are primarily Windows-based, mobile environments are multi-OS. The scaling architectures of Android, BlackBerry, iOS, Windows Mobile, and Windows Phone are all very different from each other.

Nine Core Performance Requirements for Real-World Scale

These unique characteristics of mobile computing drive nine core performance requirements that must be addressed to achieve real-world scale for Mobile IT. MDM and MAM vendors will often claim their solutions scale without considering what scale actually means for mobile computing or being able to demonstrate real-world scale in an on-premise deployment. This section provides a guide to the real-world performance requirements of Mobile IT and a set of questions to test whether a vendor can truly support a large mobile deployment.

1. **Simultaneous registrations**
   Because users are constantly changing mobile devices and new users are constantly being given mobile access, the Mobile IT infrastructure must make it easy to register multiple devices at the same time. In a large enterprise rollout of thousands of devices, there will be many new devices brought online simultaneously.
   Ask: Can more than 50 devices register simultaneously without error?
2. **Complex configurations**
   Even basic mobile device management solutions can support deployments of 1,000+ devices if they do not have email access and are minimally configured. However, real-world deployments require email, apps, Wi-Fi, VPN, and certificates. These configurations must be monitored regularly, along with the security posture of the device, to ensure compliance. The frequency of monitoring is called the check-in interval. Many vendors claim scalability, but can only support light configurations with no email or apps. These vendors can also do this only by setting very long, and therefore not secure, check-in intervals for monitoring compliance.
   Ask: Does the vendor have multiple 10,000+ device deployments with real-world configurations (email, apps, Wi-Fi, VPN, certificates) and secure check-in intervals of four hours or less?

3. **High-volume app delivery**
   Consider an organization that supports 20,000 mobile devices, each running four mobile apps with an average size of 100 MB. An upgrade to new versions of all apps would generate eight terabytes of network traffic over a short period of time. This is enough to crush the app download server as well as corporate networks which are not built for such significant spikes.
   Ask: Can the vendor securely off-load large-scale app downloads from the corporate network?
4. **High-volume certificate management**
   Certificates are a scalable way to establish user identity while enhancing user experience. Certificates streamline authentication to key enterprise resources, such as email, Wi-Fi, and VPN. From a scalability perspective, certificates are small in size, so the challenge is not how to deliver them over the network, but how to manage them efficiently. The Mobile IT platform must provide tools for certificate delivery and management. If not, IT staff will spend many hours just trying to stay on top of certificate locations, expiration times, and methods for distributing new certificates to avoid service outages for users. One device will likely have many certificates, so a 20,000 device deployment could have more than 100,000 certificates.
   Ask: Has the vendor deployed more than 100,000 certificates in a single installation?
5. **High-volume email delivery**
   Email is the first app for most mobile deployments. To secure ActiveSync-based email systems, email should flow through an intelligent gateway before reaching the device so that access can be allowed or blocked based on device and user compliance. This intelligent gateway is a proxy that must scale to allow tens of thousands of devices to each send and receive hundreds of emails daily. This gateway also needs to prevent rogue Wi-Fi access to the email stream and enforce data loss prevention for email attachments.
   Ask: Does the vendor have multiple 10,000+ device deployments securing ActiveSync email?
6. **Operational longevity**
   The Mobile IT platform must be able to provide high service levels when heavy loads are sustained over an extended period of time. Every enterprise's mobile deployments will only become larger and more complicated over time. However, testing reliability and longevity under stress is very difficult and, due to the relative infancy of mobile computing, there is no packaged test automation framework available in the market.
   Ask: Can the vendor accurately simulate 100,000 configured devices in their QA lab?
7. **Scalability with iOS and Android**
   A platform that has demonstrated scalability with legacy Windows Mobile or BlackBerry devices will not necessarily scale well with newer operating systems such as iOS and Android. Windows Mobile employs a direct client conduit from device to server that is fully controlled by the management platform. As a result, only a very small amount of data needs to be exchanged. Both iOS and Android devices require a greater volume of information to be exchanged during check-ins to ensure security compliance. Also, because Windows Mobile devices tend to have locked-down configurations, compliance issues are rare. Support for iOS and Android, especially in a BYOD environment, requires the Mobile IT platform to communicate frequently with devices to ensure they remain in compliance. The mobile scaling architecture for Windows 8 will be more like iOS and Android than Windows Mobile.
   Ask: Does the vendor have multiple 10,000+ device deployments running iOS with real-world configurations and secure check-in intervals of four hours or less?

8. **Network integration**

   A Mobile IT platform must be tightly connected to existing enterprise back-end infrastructure for authentication and security. It must be able to connect to and pull information from large-scale LDAP environments and do so across diverse domains. This is especially important for companies that, usually after a merger or acquisition, have a distributed LDAP infrastructure (federated domains) that needs to be crawled in a timely fashion. The platform must also integrate and scale with network firewalls, load balancers, proxy servers, certificate authorities, NAC, and other networking services.
   Ask: Has the vendor integrated with federated domains at multiple customers?

9. **Operational efficiency**

   One path to scale is brute force: more servers, more infrastructure, and more IT staff to manage. This approach is expensive and limiting. The other path is to architect for scale: build the underlying Mobile IT platform to meet the requirements listed above efficiently and without the need for large additional investments in infrastructure and staff.
   Ask: Can one IT administrator manage 10,000 to 20,000 devices, including system upgrades?

MobileIron is the Only Mobile IT Platform Architected for Real-World Scale

MobileIron products are architected for real-world scale. Design, development, and testing focus on the rigorous standards and complex needs of global deployments. MobileIron customers include the largest companies with the most complex iOS and Android deployments in the world. MobileIron approaches scale very differently than other Mobile IT vendors:

- *Multiple deployment options*: Both on-premise and cloud options provide real-world scale.
- *Appliance model*: Virtual or physical appliance minimizes customer's ongoing operational costs – no additional Windows server or database licensing, patching, or maintenance, plus easy server upgrades without the need for professional services.
- *Vertical scale*: One appliance scales to 100,000 devices with MobileIron's Fall 2012 release.
- *Horizontal scale*: Multiple appliances are managed centrally through the MobileIron Atlas central console.
- *Automation*: Security and compliance workflow is event-driven and automated.
- *Low total cost of ownership*: A staff of one can manage over 10,000 devices.

The following sections describe how the MobileIron platform addresses each of the nine core performance requirements for real-world scale.

1. **Simultaneous registrations – MobileIron approach**

   MobileIron powered the fastest iPad deployment in the world. 7,000 iPads were deployed in four weeks to high school students and faculty at a top school district in the United States. That experience was formative in defining the performance requirements for scaling registration capabilities in the MobileIron platform. Another common use case among MobileIron customers is deploying large numbers of mobile devices at a worldwide sales conference, where device enrollment and configuration must happen in a very short timeframe with little, if any, margin for error.

   MobileIron's testing criteria for real-world scale of device registration is *50 simultaneous registrations, but actual performance is even higher at 200 simultaneous registrations.* This scale is achieved through efficient threading of registration tasks within MobileIron.

MobileIron bulk device registration is one of the many additional MobileIron capabilities that help streamline registration and automate administration tasks. Bulk registration enables administrators to import new device configuration information from external files, such as a directory, so that many devices can be assigned a common security profile with registrations kicked off in parallel.

2. **Complex configurations – MobileIron approach**

   The MobileIron platform covers the full mobile enterprise lifecycle and supports the broadest range of configuration capabilities, from email and apps access, to Wi-Fi and VPN connectivity, to device and OS controls.

   A common use case is delivering email, VPN, and Wi-Fi configurations to a global workforce dynamically during registration based on the user's identity and group membership in LDAP.

   MobileIron's testing criteria for real-world scale of configuration and compliance is that each device should be fully configured and check-in with the MobileIron server at least *once every four hours* so that configurations can be maintained and compliance confirmed. Otherwise the deployment will not be secure because devices will fall out of compliance without any notification or automated remediation triggered.

3. **High-volume app delivery – MobileIron approach**

   The MobileIron App Delivery Network (AppDN) allows Mobile IT administrators to provision apps of any size to any number of users — quickly, securely, and reliably — without putting load on the corporate network. This dramatically improves the speed of app downloads for the user and saves the corporate network from massive, spiky loads that it cannot handle. AppDN utilizes a secure content delivery network with global points of presence (POPs) and server clusters that include built-in redundancy and automatic failover. Existing app privileges and permissions are maintained, and the user download experience is functionally unchanged, but faster. All connections, including from the MobileIron server to AppDN, are protected using certificates, HTTPS, and SSLv3.

   A common use case is found in the retail industry: An updated point-of-sales app must be downloaded by the entire device population to match a server-side application upgrade. Devices that fail to upgrade are no longer available for sales use, significantly reducing revenue opportunities for the company.

   MobileIron's testing criteria for real-world scale of app delivery is the ability to support *multiple terabytes of app downloads per customer* without introducing extra load on the corporate network or noticeable latency for the end user.

4. **High-volume certificate management – MobileIron approach**

   MobileIron supports the world's largest mobile enterprise certificate deployment, with more than 150,000 certificates delivered. The MobileIron platform makes certificate-based security easy by automating much of the process for deploying and managing certificates on mobile devices, and by providing the broadest set of architectural choices for certificate implementation. For organizations without any certificate infrastructure in place, MobileIron offers an embedded certificate authority that greatly simplifies deployment. MobileIron also provides direct integration with existing enterprise certificate authorities including Microsoft, Entrust, and Symantec.

Companies planning to implement certificate-based authentication for Wi-Fi present a common use case. Getting those certificates distributed to devices quickly is essential to maintaining network access during the switchover.

MobileIron administration tools simplify certificate management. Certificates can be automatically renewed before they expire. They can be delivered on a per-user or per-device basis. Certificates can also be automatically removed from a device if the device fails to meet organizational security requirements, if the device is lost or stolen, or if the user leaves the organization.

All of these features make it easy for administrators to handle the extremely high volume of certificates that are often required for a secure enterprise-class mobile deployment.

MobileIron's testing criteria for real-world scale in certificate management is the ability to actively manage and maintain *100,000+ certificates per customer*.

5. **High-volume email delivery – MobileIron approach**

   Email is the single biggest source of corporate activity and data on a mobile device. MobileIron Sentry is a scalable intelligent gateway that controls all corporate ActiveSync-based email traffic to and from mobile devices. Sentry blocks email to unauthorized or non-compliant devices; creates secure, certificate-based email sessions that cannot be intercepted by third parties; and prevents data leakage of email attachments while preserving the native email experience of the device.

   High availability and scale are essential for Sentry because it is on the critical path for the delivery of mobile email. Sentry was the first intelligent gateway for ActiveSync email and has been used by MobileIron customers since 2009. It is a broadly deployed and very well tested technology.

   A common use case is planning for a datacenter failover scenario where a regional datacenter fails and all email must now be routed through the disaster recovery location. The intelligent gateway must be ready to handle this.

   MobileIron's testing criteria for real-world scale of email delivery is that every device under management, no matter how big the deployment, should be able to *send and receive email reliably with a great end-user experience*. For large deployments, multiple Sentry intelligent gateways connect to the organization's email servers, and a load balancer then routes traffic in either a round-robin or priority fashion based on IT policy.

6. **Operational longevity – MobileIron approach**

   In mid-2011, MobileIron saw its customer deployments growing rapidly as large enterprises committed to mobility as a core computing platform. Global 2000 customers were adopting iOS quickly and planning deployments that would grow to 50,000 devices and beyond. However, there was no way in the industry to test real-world mobile scale other than waiting for large customer deployments to encounter scalability issues.

   MobileIron built a Test Automation Framework (TAF) to accurately simulate large numbers of mobile devices and apps under management. This testing environment is the first of its kind in the industry, and MobileIron has become the only Mobile IT vendor with the ability to test reliability under high stress and massive scale.

A typical customer operational profile of multiple months (or years) is compressed into a time period of 120 hours to stress test the environment:

- 50,000 to 100,000 new devices are registered on a single MobileIron server to verify that simultaneous registrations can work in volume.
- Each device is configured.
- Email profiles are created for each device.
- Required apps are installed on each device
- Appropriate security, privacy, and access control policies are applied.
- All devices check-in at least once every four hours to confirm that compliance monitoring is scaling.

After two hours, TAF repeats the entire process again, starting from the initial configuration of devices. In other words, every two hours the entire deployment is redeployed, which tests system reliability under stress over time.

MobileIron's testing criteria for real-world scale of ongoing operations is that for the *entire* 120 test hours of constant load:

- No more than 0.1% of registrations may fail.
- The check-in interval must remain less than four hours for every device.
- All pages must display in less than five seconds.
- No more than 0.1% of MDM commands may fail.
- No more than 0.1% of app downloads may fail.

These scalability tests enable MobileIron to identify and fix performance bottlenecks before they appear in customer implementations. This includes changes to the threading capabilities in the MobileIron server to take greater advantage of additional CPU power and database optimizations to minimize bottlenecks and reduce latency for queries.

As a result of this optimization work, MobileIron’s Fall 2012 release can support 100,000 devices per server and scale horizontally beyond that, meeting all the performance requirements described in this document. This is a 5x improvement in vertical scale from the prior version and 20x the real-world scale of any other Mobile IT vendor’s appliance.

Total cost of ownership is an enormous advantage of the appliance model. A MobileIron deployment of 100,000 devices will require only a fraction of the hardware, licensing, and personnel cost of an unbundled software installation.

MobileIron customers can also continue to combine multiple servers to scale horizontally for even larger deployments. Many Global 2000 companies operate in this distributed fashion, using the central console, MobileIron Atlas, for managing deployments and delegating administration across MobileIron servers.

7. **Scalability with iOS and Android – MobileIron approach**

MobileIron scalability testing with TAF is always done using iOS and Android, which are harder to scale than legacy Windows Mobile.

MobileIron’s testing criteria for real-world scale of mobile platforms is that *all scale requirements should be met on iOS and Android.* Windows Phone will be added to the testing criteria soon.

8. **Network integration – MobileIron approach**

   Many large MobileIron customers have very complex LDAP and networking infrastructures. A common use case is deploying mobile consistently across business units with federated domains that have to be crawled quickly and reliably.

   MobileIron's testing criteria for real-world scale of network integration is that once the system is operational, the back-end integration should be *transparent* to the MobileIron administrator and the end user from a management and performance perspective.

9. **Operational efficiency – MobileIron approach**

   The MobileIron on-premise and cloud models of deployment are focused on scaling without sacrificing operational efficiency. The combination of automation (for both models) and appliance (for on-premise) allows large companies to deploy quickly without having to incur large ongoing operational expenses. As a result, MobileIron's total cost of ownership is much lower than that of other vendors that require the customer to manage new Windows server and database licensing, deployment, and maintenance in order to add scale.

   MobileIron's testing criteria for real-world scale of operations is that one IT staff member should be able to manage *10,000+ devices for ongoing operations and not require professional services assistance for system upgrades.*

Conclusion

Mobile IT is evolving rapidly. It has unique characteristics that must be well understood in order to build a scalable infrastructure that will stand the test of time.

The largest companies in the world use MobileIron as their underlying platform for global mobility initiatives because **MobileIron is the only Mobile IT platform architected for real-world scale**.

MobileIron invests continually in building product capabilities and testing infrastructure that can hit the real-world scale performance requirements of global organizations. The company's experience with sophisticated Global 2000 deployments has led to a superior platform design and the ability to address scalability issues that other vendors have not yet even realized they will need to confront.

For more information about Mobile IT solutions from MobileIron for the security and management of mobile apps, content, and devices, visit http://www.mobileiron.com/.