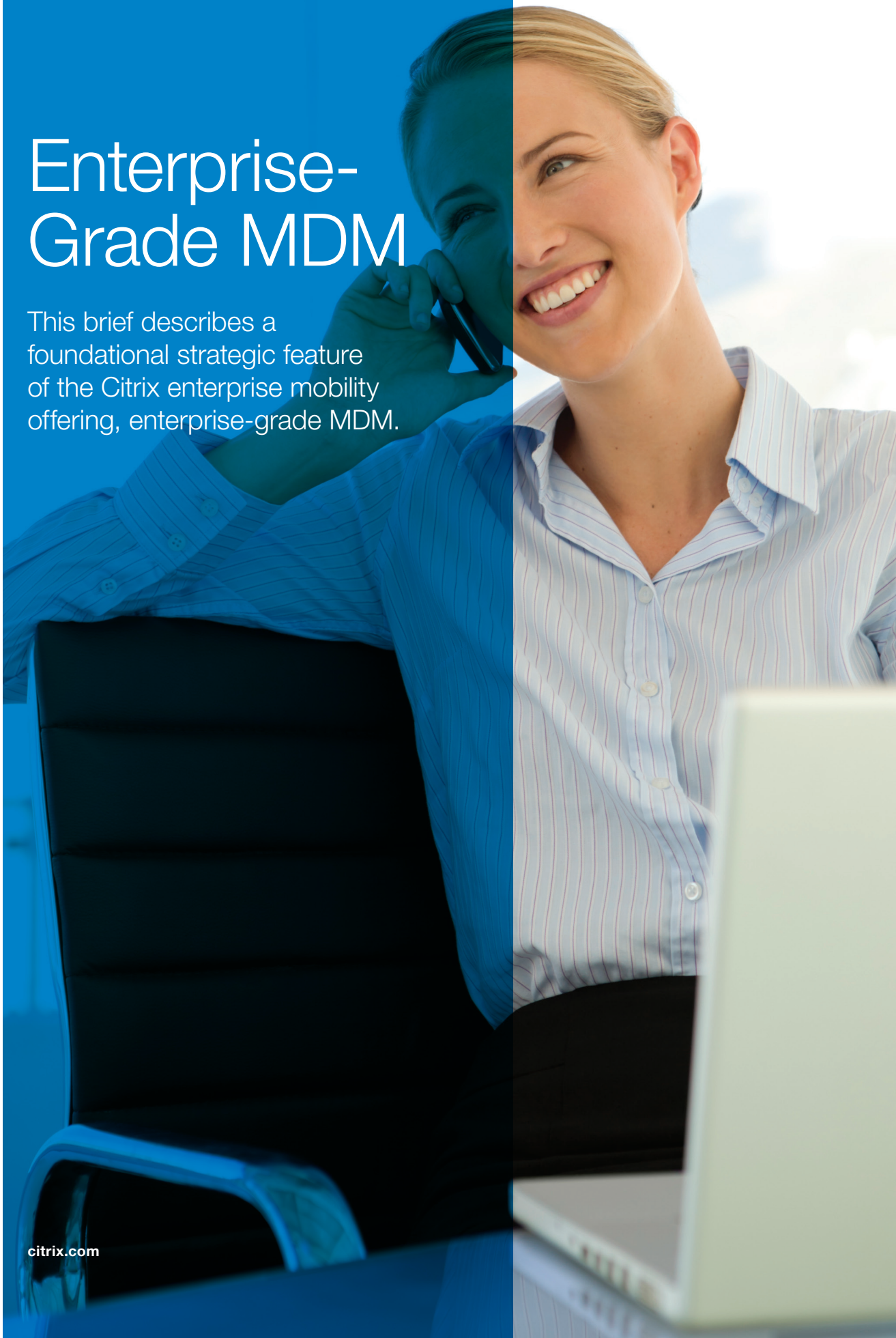
Enterprise-Grade MDM

This brief describes a foundational strategic feature of the Citrix enterprise mobility offering, enterprise-grade MDM.



CITRIX®

citrix.com

While the transition of mobile phones into computers has been a long time coming, the sea change in the past few years is dramatic: Consumer smartphones and tablets have become so compelling to business users that enterprise executives and IT are willing to upend the 'way we do things around here' to let users have them at work. According to research performed by the Center for Telecom Environment Management Standards, 78 percent of organizations allow employee-owned mobile devices in the business environment.[1] And lines of business are getting in on the action: A Citrix survey found that more than three-quarters of organizations will deploy mobile apps for line-of-business use this year, and over half of those will be mission critical.

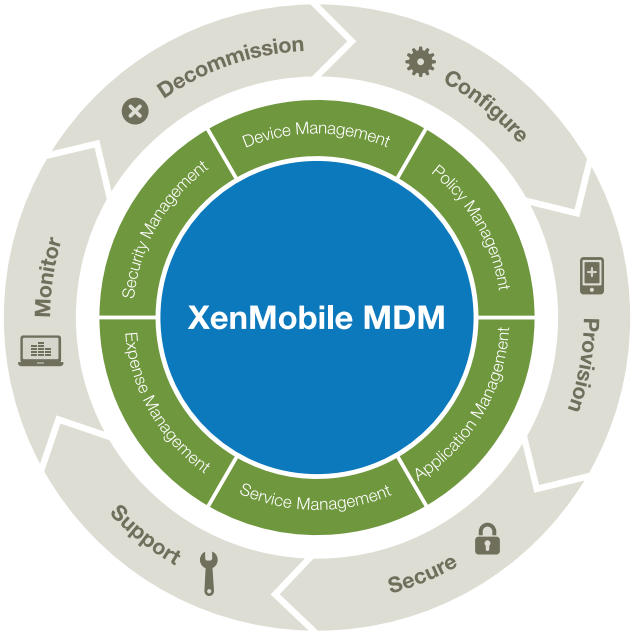
MDM – A Foundational Element

What has become a powerful medium for learning, transacting, sharing, presenting —even transforming business—also brings tremendous management complexity and potential enterprise risk. A foundational element of many enterprises' mobility agendas is Mobile Device Management (MDM). MDM provides management and security of mobile devices through their lifecycle.

Citrix XenMobile MDM Edition

Citrix® features enterprise-grade MDM in its full-stack enterprise mobility offering. XenMobile™ MDM Edition provides role-based management, configuration and security of corporate and user-owned devices, all running on a secure, enterprise-grade architecture. Among other things, IT can enroll and manage any device, blacklist or whitelist apps, detect jailbroken devices and do a full or selective wipe of a device that is out of compliance. This solution gives users device choice while ensuring compliance of corporate assets and the security of corporate content on the device. A good way to organize the key features of MDM is to consider the steps of the mobile device lifecycle, including:

1. Configure
2. Provision
3. Secure
4. Support
5. Monitor and report
6. Decommission



Configure

XenMobile MDM Edition lets administrators configure both corporate and bring-your-own (BYO) device settings and integrate with IT resources in a centralized, role-based way that's integrated with enterprise directories like Microsoft Active Directory. This includes:

- Configure all devices from an intuitive, wizard-based interface
- Specify which OSs and patch levels can enroll and receive policy profiles
- Designate device ownership (user or corporate), including tag import from an asset or configuration management database
- Configure platform- or OS-specific settings, such as block iTunes or iCloud in iOS or OTA updates, background data, or power off in Samsung SAFE devices
- Configure enterprise integration and access such as Wi-Fi, VPN, public key infrastructure, and corporate email, including deployment of certificates for authentication and user single sign-on
- Set device security such as passcodes and encryption
- Create app blacklists/whitelists, push and remove apps, restrict apps and device resources (such as YouTube, camera, and Bluetooth), and prevent apps from launching
- Lock and prevent a user from removing a device profile

Benefit: Taken together, these features allow administrators to rapidly configure large numbers of devices in way that complies with enterprise policy.

Provision

XenMobile MDM Edition lets users self-service enroll, select apps from an app catalog, and perform some self-help functions, and lets administrators provision policies and apps automatically over-the-air to users. This includes:

- Allow users to self-service enroll
- Specify the right level of enrollment authentication for the organization's risk profile, with one-, two- or three-factor authentication
- Automatically conduct a device pre-enrollment compliance check
- Rapidly provision policies to groups of devices over-the-air
- Distribute apps by pushing them or making them available via an enterprise app catalog
- Remove apps automatically, including silently for some device types
- Support Apple's volume purchase program

Benefit: Taken together, these features make user self-service drop-dead simple and over-the-air provisioning automated and straightforward for administrators with minimal opportunity for error.

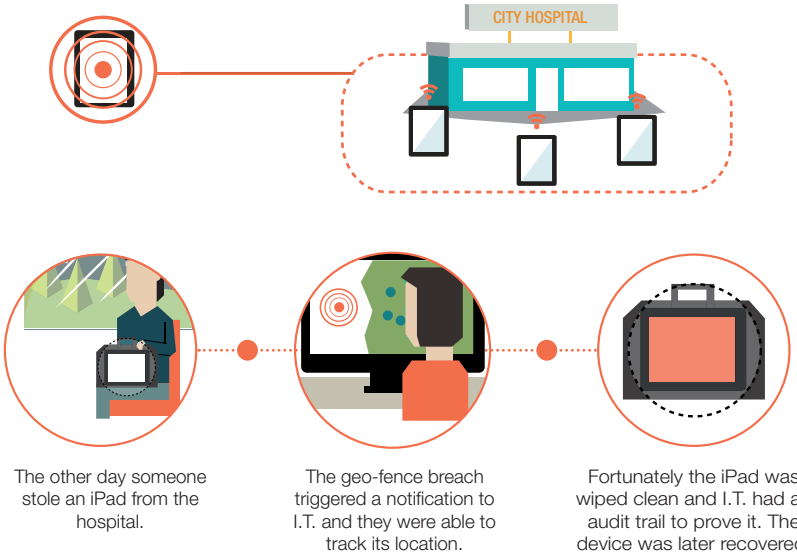
Secure

Besides configuring device and app security settings during configuration, XenMobile MDM Edition lets administrators take further security action in the event of loss, theft, or user departure. The solution keeps an audit trail of administrator actions and integrates with enterprise security systems for threat correlation and analysis. This includes:

- Locate, track, and geo-fence devices
- Lock devices or set an auto-lock policy after a defined period of time
- Create automated compliance actions such as wipe devices after a defined number of failed login attempts or if devices leave a defined geo-fence
- Integrate with security information tools for threat detection and reporting

Benefit: Taken together, these features allow administrators to take automated or manual security actions and bring mobile in-line with the organization's security and compliance status.

Geo-Fencing allows City Hospital to create an electronic fence around its facility. If an Apple® iPad® gets too far away, it's wiped clean of its data.



Support

XenMobile MDM Edition lets administrators provide help desk functions, remote support, and troubleshooting for mobile users. This includes:

- Respond to system alerts with one-click from dashboard
- Drill down to and easily remedy device issues individually or by group
- Offer remote support via VOIP and chat for some devices

Beyond the administrator's ability to support users, Citrix provides its customers global, 24x7x365, follow-the-sun support, as well as a host of local and web-based training options, backed by a whole-company commitment to customer success evidenced by top customer satisfaction and net promoter scores.

Benefit: Taken together, these features allow administrators to manage a large mobile deployment without breaking its IT support organization.

Monitor and Report

XenMobile MDM Edition lets administrators monitor and report on device and app inventory, device status, and security and compliance status. This includes:

- View MDM deployment status, compliance, and alerts via drill-down, actionable dashboard
- Monitor device and app inventory, status, and statistics
- See usage details such as roaming, location, and inactivity
- See and take action on system notifications and alerts
- Report by device ownership (BYO or corporate)
- Unmanaged device reporting
- Mobile security intelligence and integration with SIEM tools

Benefit: Taken together, these features allow IT to easily sort through data and quickly identify mobile issues, as well as automatically report on security and compliance status.

Decommission

XenMobile MDM Edition lets administrators decommission devices when they are lost, stolen, replaced, or upon user departure in a secure, auditable way that's appropriate to the scenario. This includes:

- Identify inactive devices
- Fully wipe corporate devices
- Selectively wipe BYO devices
- Disable fully device wipe to prevent administrators from executing a full device wipe
- Fully audit and report on device decommissioning activities

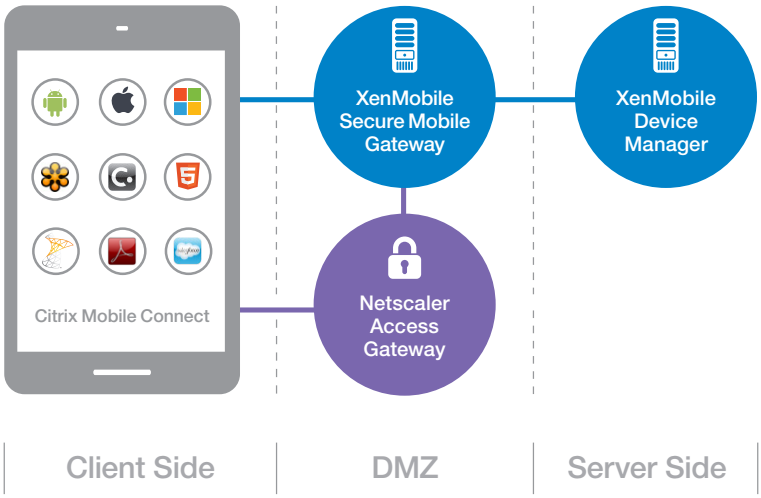
Benefit: Taken together, these features enable IT to easily revoke access and wipe data from devices for security purposes and report on those actions for compliance purposes.

Enterprise-Grade Architecture

XenMobile MDM Edition features a secure, scalable, and highly available architecture. This includes:

- Policy server, database, and enterprise directory that reside in the datacenter, where data won't be exposed to the internet
- Scale-out architecture front-ended by industry-leading load balancing technology
- Industry-standard high availability with clustering, no points of failure, and automated failover and failback processes

Benefit: This architecture gives customers comfort that they are compliant with their organization's data security policies, lets them support large mobile deployments without increasing management complexity or performance, and gives them the assurance that they can maintain uptime even in the event of technology failure.



Conclusion

The tremendous opportunity created by enterprise adoption of consumer mobile devices certainly brings risk and complexity. With enterprise-grade MDM provided by Citrix XenMobile MDM Edition, IT can take its enterprise to the next level in mobility in a simple, straightforward, and secure manner.

1. "AOTMP: CTEMS Research Finds 78% of Enterprises Allow Bring Your Own Device", TMCnet, August 1, 2012

Corporate Headquarters
Fort Lauderdale, FL, USA

Silicon Valley Headquarters
Santa Clara, CA, USA

EMEA Headquarters
Schaffhausen, Switzerland

India Development Center
Bangalore, India

Online Division Headquarters
Santa Barbara, CA, USA

Pacific Headquarters
Hong Kong, China

Latin America Headquarters
Coral Gables, FL, USA

UK Development Center
Chalfont, United Kingdom

About Citrix
Citrix (NASDAQ:CTXS) is the company transforming how people, businesses and IT work and collaborate in the cloud era. With market-leading cloud, collaboration, networking and virtualization technologies, Citrix powers mobile workstyles and cloud services, making complex enterprise IT simpler and more accessible for 260,000 enterprises. Citrix touches 75 percent of Internet users each day and partners with more than 10,000 companies in 100 countries. Annual revenue in 2011 was $2.21 billion. Learn more at www.citrix.com.