Mobile Device Managers for BYOD

Revised: August 7, 2013

Mobile Device Managers (MDMs) secure, monitor, and manage mobile devices, including both corporate-owned devices as well as employee-owned BYOD devices. MDM functionality typically includes Over-the-Air (OTA) distribution of policies and profiles, digital certificates, applications, data and configuration settings for all types of devices. MDM-supported and managed devices include not only handheld devices, such as smartphones and tablets, but increasingly laptop and desktop computing devices as well.

Critical MDM functions include-but are not limited to:

- PIN enforcement—Enforcing a PIN lock is the first and most effective step in preventing unauthorized access to a device; furthermore, strong password policies can also be enforced by an MDM, reducing the likelihood of brute-force attacks.
- Jailbreak/Root Detection—Jailbreaking (on Apple iOS devices) and rooting (on Android devices) are means to bypass the management of a device and remove SP control. MDMs can detect such bypasses and immediately restrict a device's access to the network or other corporate assets.
- Data Encryption—Most devices have built-in encryption capabilities-both at the device and file level. MDMs can ensure that only devices that support data encryption and have it enabled can access the network and corporate content.
- Data Wipe—Lost or stolen devices can be remotely full- or partial-wiped, either by the user or by an administrator via the MDM.
- Data Loss Prevention (DLP)—While data protection functions (like PIN locking, data encryption and remote data wiping) prevent unauthorized users from accessing data, DLP prevents authorized users from doing careless or malicious things with critical data.
- Application Tunnels—Secure connections to corporate networks are often a mandatory requirement for mobile devices.

Cisco ISE 1.2 with MDM API Integration

While Cisco ISE provides critical policy functionality to enable the BYOD solution, it has limited awareness of device posture. For example, ISE has no awareness of whether a device has a PIN lock enforced or whether the device has been jailbroken or whether a device is encrypting data, etc. On the other hand, MDMs have such device posture awareness, but are quite limited as to network policy enforcement capacity.

Therefore, to complement the strengths of both ISE and MDMs, ISE 1.2 includes support of an MDM integration API which allows it to both:

- Pull various informational elements from MDM servers in order to make granular network access policy decisions that include device-details and/or device-posture.
- Push administrative actions to the managed devices (such as remote-wiping) via the MDM.

As of the publication date of this CVD, ISE 1.2 supports an API for MDM integration with the following third-party MDM vendors:

- AirWatch
- MobileIron
- Good Technologies
- XenMobile
- SAP Afaria
- FiberLink Maas360

The following MDM API pull/push capabilities are supported in ISE 1.2 for all third-party MDM systems:

- PIN lock Check
- Jailbroken Check
- Data Encryption Check
- Device Augmentation Information Check
- Registration Status Check
- Compliance Status Check
- Periodic Compliance Status Check
- MDM Reachability Check
- (Full/Partial) Remote Wipe
- Remote PIN lock

MDM Deployment Options and Considerations

With MDM solutions, there are two main deployment models:

- On-Premise—In this model, MDM software is installed on servers in the corporate DMZ or data center, which are supported and maintained by the enterprise IT staff.
- Cloud-based—In this model-also known as a MDM Software-as-a-Service (SaaS) model-MDM software is hosted, supported and maintained by a provider at a remote Network Operation Center (NOC); customers subscribe on a monthly or yearly basis and are granted access to all MDM hardware/software via the Internet.

Before deploying a MDM, businesses must make the pivotal decision of whether their MDM solutions should be on premise (on-prem) or cloud-based. Several business and technical factors are involved in this decision, including:

- Cost—Cloud-based MDM solutions often are more cost-effective than on-prem; this is because these eliminate the need for incremental and ongoing hardware, operating system, database and networking costs associated with a dedicated MDM server. Also avoided is any additional training

that may be required by IT staff to support these servers. From a cloud-provider's perspective: since these fixed infrastructure costs have already been invested, there are very little marginal cost to provisioning custom-tailored virtual-instances to enterprise subscribers, and as such, these can be priced attractively.

- Control—On-prem models offer enterprises the greatest degree of control, of not only the MDM solution, but also the enterprise systems that these integrate with (such as the corporate directory, certificate authority, email infrastructure, content repositories and management systems-all of which will be discussed in additional detail below). This is because an on-prem model requires no transmission or storage of corporate data offsite. Conversely, a cloud-based service requires giving up a level of control over the overall solution, as confidential information, data and documents will be required to be transmitted to the provider, and (depending on the details of the service) may also be stored offsite. Cloud providers may also update the software on the servers without following the enterprise change control protocol.
- Security—On-prem MDM models are often perceived as being more secure than cloud-based models; however, this perceived difference in security-levels may be lessening, especially when considering that over $14B of business was securely conducted via SaaS in 2012 alone. Ultimately, the security of a system will principally depend, not only on the technologies deployed, but also on the processes in place to keep the hardware and software updated and managed properly.
- Intellectual Property—Most MDMs support secure isolation of corporate data on the devices they manage; however, these systems typically require corporate data to be passed through the MDM in order to be transmitted OTA to the device's secure and encrypted compartment. This process may represent an additional security concern in a cloud-based model, as now the enterprise is called on to trust the MDM SaaS provider with not only device management, but also with intellectual property and confidential data.
- Regulatory Compliance—Regulatory compliance can dictate where and how financial, healthcare and government (and other) organizations can store their data. Such regulations include PCI, HIPAA, HITECH, Sarbanes-Oxley, and even the US Patriot Act. Such regulations may preclude storing sensitive information in the cloud, forcing the choice of an on-prem MDM model.
- Scalability—Cloud-based models offer better scalability than on-prem models, as these can accommodate either small or large deployments (and anything in-between) without any increased infrastructure costs to the subscriber. Conversely, on-prem models may have difficulty in cost-effectively accommodating small deployments. For example, consider the cost of deploying an MDM server that can support 100,000 devices being deployed to support only 100. Additionally, on-prem models will incrementally require more hardware and infrastructure as the number of devices increases.
- Speed of Deployment—Cloud-based solutions are typically faster to deploy (and can often be enabled the same-day as these are ordered), whereas on-prem solutions often take a couple of weeks (or more) to plan out, install and deploy.
- Flexibility—Cloud-based MDM solutions typically have day-one support for new releases of device hardware and software; alternatively, on-prem solutions will require an upgrade to the MDM software for each new device/software supported.
- Ease of Management—With on-prem models, the IT department must ensure the MDM has all the latest updates; in a cloud-based system, this responsibility rests with the provider.

Note Cisco is not advocating the use of one MDM deployment model over another, nor does Cisco recommend any specific third-party MDM solution. These business and technical considerations are included simply to help draw attention to the many factors that an IT architect may find helpful in reviewing when evaluating which MDM solution works best to meet their specific business needs.

On-Premise

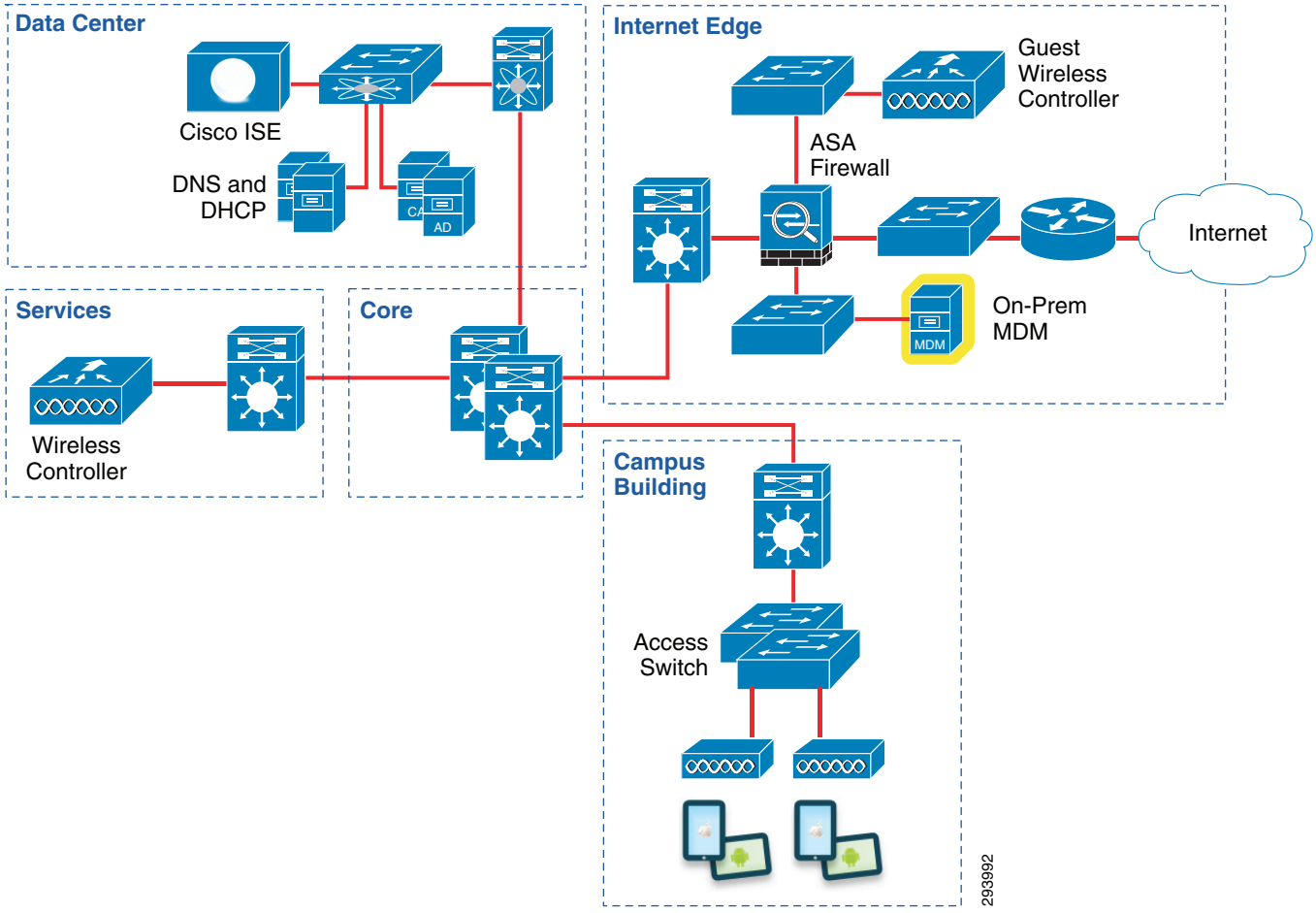
In the on-premise MDM deployment model, the MDM software resides on premises on a dedicated server (or servers), typically within the Internet Edge or DMZ.

This model is generally better suited to IT staff that have a higher-level of technical expertise (such that they can configure, periodically-update and manage such a server) or to enterprises that may have stricter security/confidentiality requirements (which may preclude the management of their devices by a cloud-based service).

The on-premise model may also present moderate performance benefits to some operational flows (due to its relative proximity to the devices, as opposed to a cloud-based service). For example, if a network access policy included the "MDM Reachability" check, this test would likely be much more responsive in an on-premise MDM deployment model versus a cloud-based model.

The network topology for a campus BYOD network utilizing an On-Prem MDM deployment model is illustrated in Figure 6-1.

Figure 6-1 Campus BYOD Network with On-Prem MDM (at the Internet Edge)



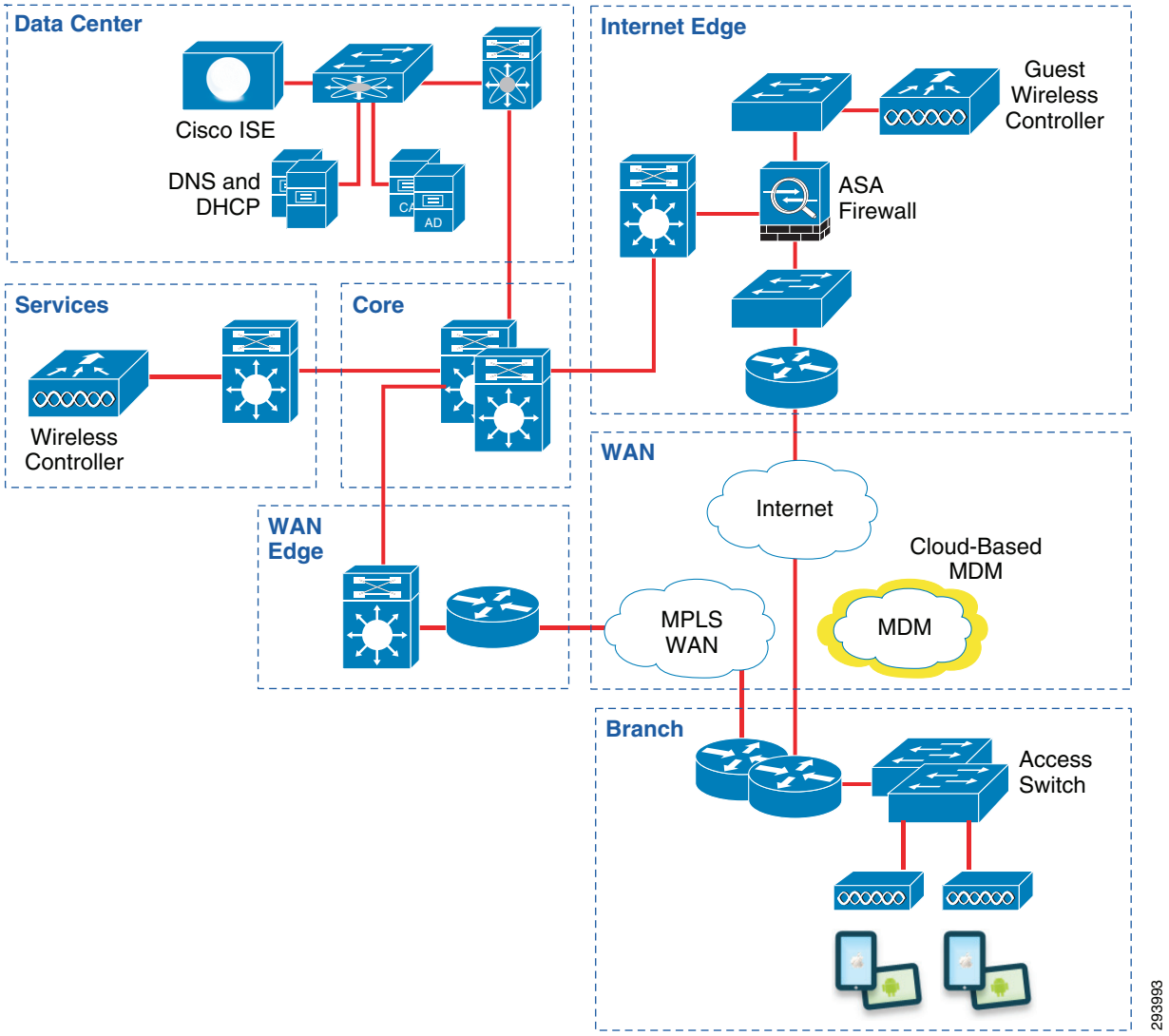
Cloud-Based

In the Cloud-Based MDM deployment model, MDM functionality is delivered to customers in a SaaS manner: the software resides wholly within the MDM vendor's cloud, with a custom-tailored virtual instance provided for each customer.

From a customer's perspective, this model is greatly simplified (as now they do not have to configure, update, maintain and manage the MDM software); however, as a trade-off, they relinquish a degree of control over all their devices (and also some of the data on these devices) to the third-party MDM SaaS provider, which may pose security concerns. As such, this model may be better suited to small- or medium-sized businesses that have moderate IT technical expertise and unexceptional security requirements.

The network topology for a branch BYOD network utilizing a cloud-based MDM deployment model is illustrated in Figure 6-2.

Figure 6-2 Branch BYOD Network with Cloud-Based MDM



Enterprise Integration Considerations

In addition to the integrating the corporate network with the MDM—which is discussed in great detail in this document—other enterprise services and resources are also important to integrate with the MDM system, including:

- Corporate Directory Services
- Certificate Authority (CA) and Public Key Infrastructure (PKI)
- Email Infrastructure
- Content Repositories
- Management Systems

Corporate Directory Services Integration

Corporate directory services (such as LDAP-based directory, Active Directory, etc.) can be leveraged by MDMs to efficiently organize and manage user access. Administrators can assign device profiles, apps, and content to users based on their directory-group memberships. Additionally, some MDMs can detect directory changes and automatically update device-policies. For example, if a user is deactivated in a directory system, then the MDM can remove device-based corporate network access and selectively wipe the device.

Corporate Certificates Authority and Public Key Infrastructure Integration

Certificate Authorities (such as Microsoft CA) or SCEP certificate services providers (such as MSCEP and VeriSign) can be leveraged by MDMs to assign and verify certificates for advanced user authentication and to secure access to corporate systems. CA integration ensures message integrity, authenticity and confidentiality. Additionally CA integration enables client authentication, encryption and message signatures.

Furthermore, MDMs can also integrate with Public Key Infrastructure (PKI) or third-party providers to configure certificates and distribute these to devices without user interaction.

Email Integration

The corporate email infrastructure can be integrated with the MDM solution to provide security, visibility and control in managing mobile email. This enables employees to access corporate email on their mobile devices without sacrificing security. Additionally such integration facilitates the management of mobile email (such as configuring email settings over-the-air, blocking unmanaged devices from receiving email, enforcing device encryption, etc.) The MDMs approach to email management varies among MDM providers and is feature differentiator. Email policy information is not available to ISE via the API.

Content Repository Integration

Integrating MDM systems with content repositories enables administrators to deliver secure mobile access to corporate documents while managing document distribution and access permissions (including the ability to view, view-offline, email, or print on a document). This ensures the right content gets to

the right employees without sacrificing the security of the documents themselves, which are distributed to mobile devices over encrypted connections. Furthermore, files and documents can be synchronized with corporate file systems and share points, so that the latest version of a document is automatically updated on employee mobile devices. To ensure security, users can be authenticated with a username, password, and certificate before they can access corporate content. Additionally, document metadata (including author, keywords, version, and dates created or modified) can be restricted on a per-user basis.

Management Integration

MDM systems can be integrated with enterprise management systems for enhanced logging, recording and reporting of device and console events. Event logging settings can be configured based on severity levels, with the ability to send specific levels to external systems via Syslog integration. Events can include login events, failed login attempts, changes to system settings and configurations, changes to profiles, apps and content, etc. Such management systems integration ensures security and compliance with regulations and corporate policies.

Integration Servers

The integration of these enterprise systems with MDMs in on-premise deployment models is relatively straightforward, as it is largely a matter of ensuring the proper protocols are configured correctly and the necessary ports are opened in any firewalls within the paths. However, in cloud-based deployment models, such integration requires secure transport protocols (such as over HTTPS) from the customer to the MDM service provider and/or a specialized MDM integration servers (or similar proxy-servers) located within the client's DMZ.