



Integrating Citrix XenMobile with Cisco Identity Services Engine

Revised: August 6, 2013



ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

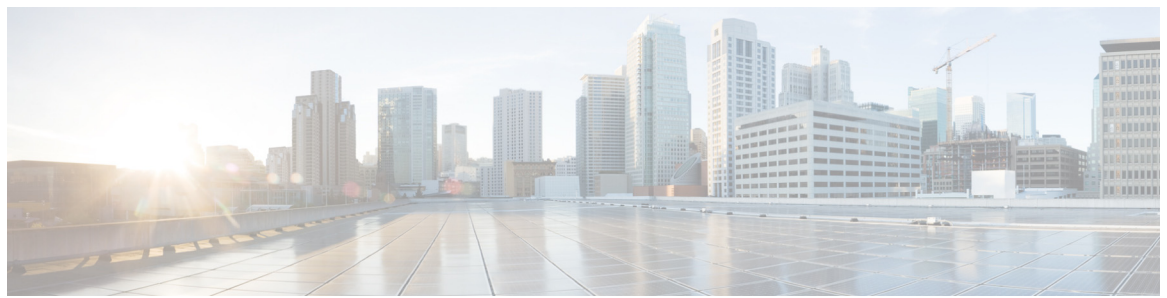
The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at <http://www.cisco.com/go/trademarks>. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Integrating Citrix XenMobile with Cisco Identity Services Engine

© 2013 Cisco Systems, Inc. All rights reserved.



Integrating Citrix XenMobile with Cisco Identity Services Engine

This document supplements the Cisco Bring Your Own Device (BYOD) CVD (http://www.cisco.com/en/US/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/BYOD_Design_Guide.html) and provides mobile device management (MDM) partner-specific information as needed to integrate with Cisco ISE. In an effort to maintain readability, some of the information presented in the CVD is repeated here. However this document is not intended to provide standalone BYOD guidance. Furthermore, only a subset of the Citrix XenMobile functionality is discussed. Features not required to extend ISE's capabilities may be mentioned, but not in the detail required for a comprehensive understanding. The reader should be familiar with the XenMobile Administrator's guide.

This document is targeted at existing Citrix XenMobile customers. Information necessary to select an MDM partner is not offered in this document. The features discussed are considered to be core functionality present in all MDM software and are required to be compatible with the ISE API.

Overview

Citrix XenMobile is a comprehensive solution to manage mobile applications, data, and devices. Users have single-click access to all of their apps from a unified corporate app store and IT can easily configure, secure, and support mobile devices. With XenMobile, IT can meet their compliance and control needs while giving users the freedom to experience work and life their way.

With XenMobile, Citrix is a leading provider of enterprise mobility management (EMM) software used to establish and enforce device policy on hand-held endpoints. This could include corporate- or employee-owned phones and tablets. Devices manufactured by all the major equipment providers are supported at some level. Apple and Android devices are the primary focus, but XenMobile also supports Blackberry and Windows 8 mobile devices.

Enterprise mobility management is a relatively new phenomenon and is in a constant state of expansion. Features can be thought of in several categories:

- **Device Restrictions**—There are two common types of restrictions. Either some feature of the device is disabled, such as the camera, or there are additional requirements for basic usage, such as a PIN lock or storage encryption. When a restriction is in place, the user is not offered the choice of non-compliance. Restrictions are used to reduce security risks to the enterprise.



Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Copyright © 2013 Cisco Systems, Inc. All rights reserved.

- **Device Compliance**—This may also be referred to as posture enforcement. The MDM will check the attributes of the device against a list of acceptable operational conditions. Compliance checks can be enforced based on their severity. For example, an email could be sent to the user if they are running a software version known to contain a vulnerability or XenMobile can automatically issue a corporate wipe if the device has been compromised. A compliance check is different from a restriction because the user can become out of compliance. XenMobile uses Automatic Actions to respond to non-compliant devices. Compliance can be used to increase security and reduce operational costs.
- **Notifications**—Administrators can send a message to a large population of devices. This could be a push message to the XenMobile Worx Home application or SMS and SMTP messages if properly configured. For example, “The fire drill is complete, you may return to the building” could be sent to all devices on a particular campus. Notifications are used to increase productivity.
- **Content Distribution**—Bookmarks, Web Clips, and other content can be pushed to devices in the background without user intervention or made available on demand. Content distribution is used to increase productivity. XenMobile can push content to Android devices natively. Both Apple and Android can leverage Citrix’s ShareFile to distribute SharePoint content. Web Clips are HTML bookmarks that are displayed as application icons on an Apple mobile device.
- **Application Distribution**—The MDM can offer a company catalog of available software or install required software. The software can come from public repositories or can be corporate-developed applications. Application distribution has both security and productivity gains. Security is enhanced because any software distributed by the MDM, including local storage associated to the software, can be removed as part of a corporate wipe. This is not true if the user installs the same software from Apple’s App Store or Google Play. The Device Manager can also inventory devices for installed software.

The MDM capabilities in Citrix XenMobile have three main components as deployed in the CVD

- Device manager
- Mobile device OS API
- Worx Home client software

Beyond these, there are additional components for enterprise integration, email, secure Web, and data loss prevention. The majority of the base MDM functionality is available through the MDM API built into the mobile device operating system. XenMobile requires the client software to detect some conditions, such as jail-broken¹ or rooted devices, as well as enforce location-based policy. XenMobile uses an In-App enrollment process when integrating with ISE. The Worx Enroll and Worx Home mobile applications are installed on iOS devices during the ISE onboarding work flow. Android devices enroll directly from the Worx Home application and do not require the Worx Enroll application.



Note

The MDM capabilities in XenMobile are the result of the acquisition of Zenprise in January 2013. Citrix has rapidly integrated Zenprise into its mobile ecosystem. XenMobile version 8.0.1 is the initial release. Some components of the product still retain Zenprise branding, for example the cloud service. Full integration is expected during Q1 of 2014.

1. Apple prefers the term Compromised OS when referring to devices where the user has gained elevated privileges to the operating system.

Deployment Models

The XenMobile MDM Edition is available in both an on-premise model and cloud service model. The two models are functionally equivalent. The CVD explores the advantages and disadvantages of each of the models. An obvious difference is the topology. An on-premise model is defined when the MDM server is located in the enterprise DMZ and managed directly by the enterprise. A cloud model places the MDM server in the cloud and is offered as a software subscription. Both models support integration with corporate services such as corporate directories, Microsoft Exchange, or a Blackberry Enterprise Server. The cloud model provides this functionality with the XenMobile Enterprise Connection. The discussion below, including the illustrations, is based on an on-premise deployment model.



Note

This document may refer to the XenMobile Device Manager as the MDM Server when speaking in generic terms.



Note

Citrix offers XenMobile as an MDM Edition, an App Edition, or an Enterprise Edition. The Enterprise edition includes both the MDM and MAM features and is a true EMM solution.

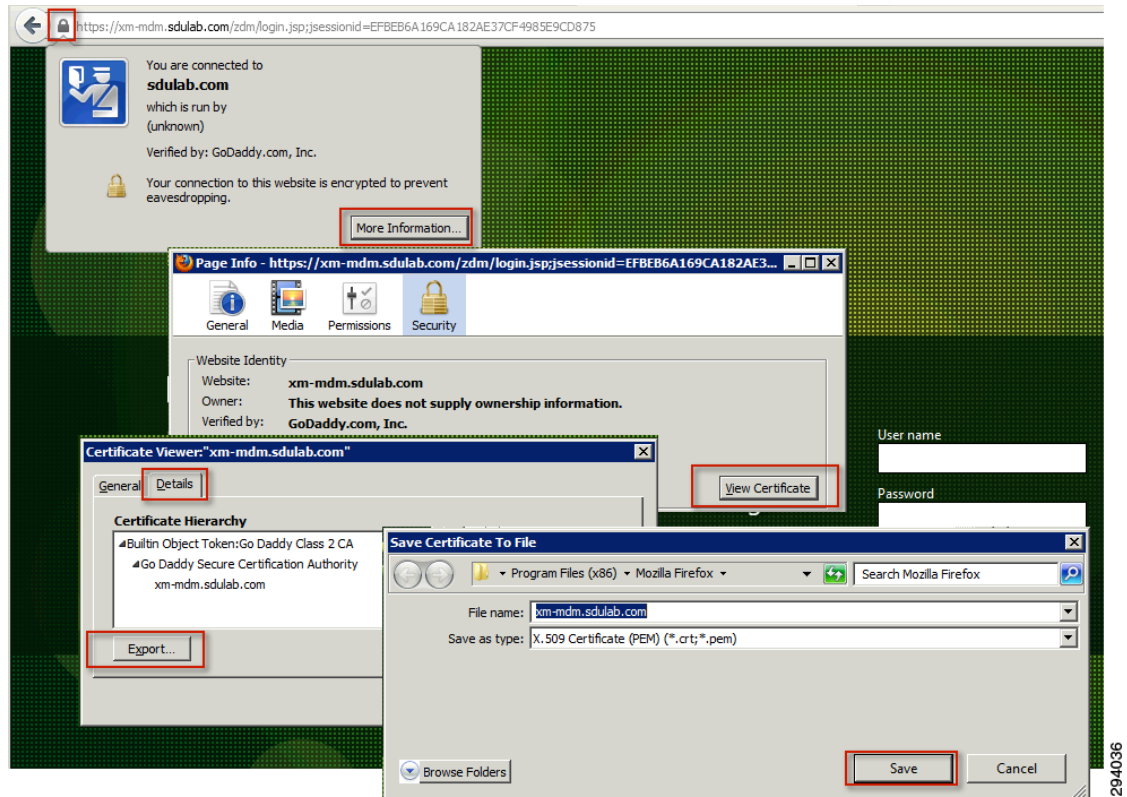
Getting XenMobile Ready for ISE

The first requirement is to establish basic connectivity between the Cisco ISE server and the XenMobile Device Manager. In both the on-premise and the cloud model, a firewall is typically located between these two components. The firewall should be configured to allow an HTTPS session from the ISE located in the data center to the MDM server located in either the corporate DMZ or public Internet. The session is established outbound from ISE towards the MDM where ISE takes the client role. This is a common direction for Web traffic over corporate firewalls.

Import API Portal Certificate to ISE

The XenMobile Device Manager incorporates an HTTPS portal to support the various users of the system. In the case of cloud service, this website will be provided to the enterprise. ISE must establish trust with this website. Even though the cloud website is authenticated with a publicly signed certificate, ISE does not maintain a list of trusted root CAs. Therefore the administrator must establish the trust relationship. The simplest approach is to export the MDM site certificate, then import the certificate into local cert store in ISE. Most browsers allow this. Firefox is shown in [Figure 1](#) with an on-premise MDM deployment.

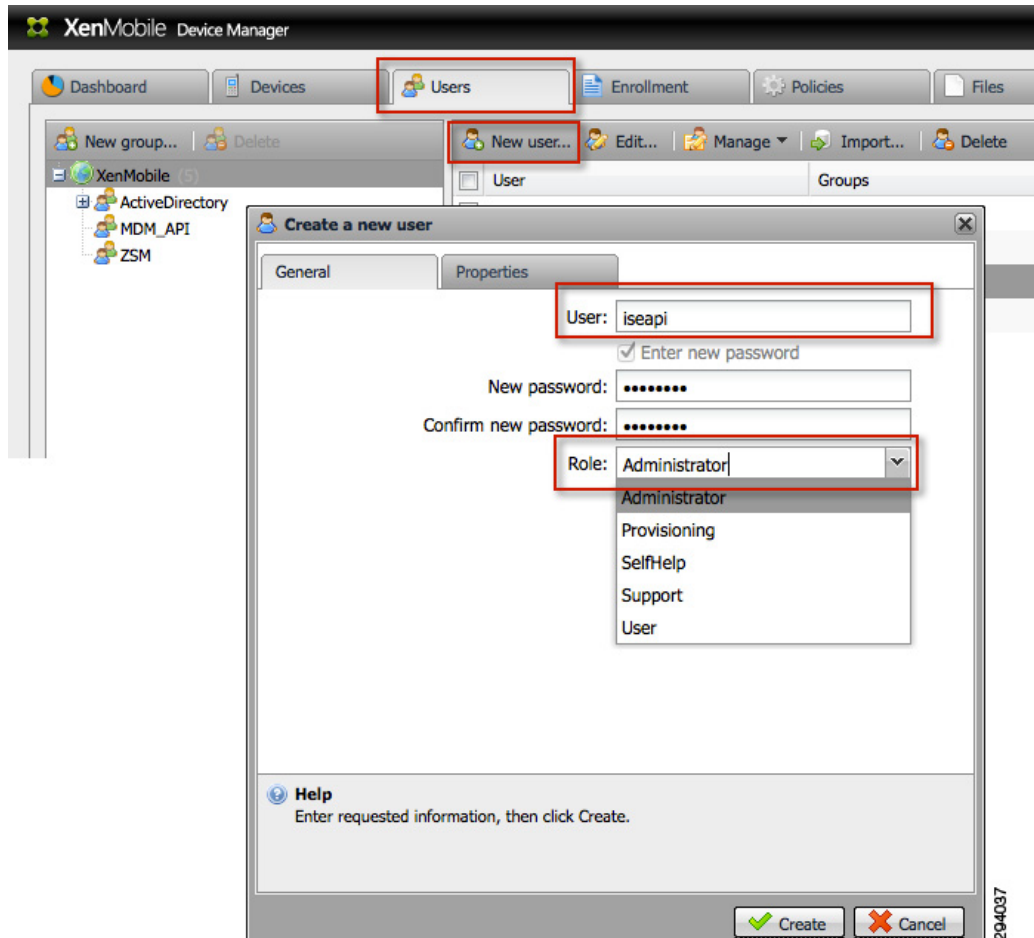
Figure 1 *Exporting the MDM Site Certificate with Firefox*



Grant ISE Access to the XenMobile API

The XenMobile API is protected by HTTPS and requires credentials. Ideally a specific account would be configured for ISE with a very strong password. A locally defined user account with the Administrator role is required to access the MDM API functionality.

Figure 2 *Select Administrator Account*



Add MDM Server to ISE

Once the ISE API administrator account has been defined on the XenMobile Device Manager, ISE must be configured to use this account when querying the MDM for device information. ISE will contact the MDM to gather posture information about devices or to issue device commands, such as corporate wipe or lock. The session is initiated from ISE towards the MDM server on TCP port 443.

As shown in [Figure 3](#), the URL for the XenMobile server is the same as the admin page and used earlier to export the certificate. The Instance Name field is used to specify the path. With an on-premise deployment, the default Instance Name is zdm. Citrix may provide a different value to be used with the XenMobile service. The port should be configured for HTTPS (TCP port 443). The MDM cannot be configured to listen on a dedicated port for API messages. Any change to the Device Manager's Web settings will also impact the user portal pages.

Figure 3 *Configure the MDM API on ISE*

The screenshot shows the Cisco Identity Services Engine (ISE) Administration interface. The top navigation bar includes 'Home', 'Operations', 'Policy', and 'Administration'. The 'Administration' menu is expanded, showing 'Network Resources', 'Web Portal Management', 'Feed Service', 'SGA AAA Servers', 'NAC Managers', and 'MDM'. The 'MDM' option is selected. The left sidebar shows 'Mobile Device Management' with 'External MDM Servers' selected. The main content area displays the 'MDM Server details' for 'XenMobile'. The configuration fields are as follows:

Field	Value
* Name	XenMobile
* Server host	xm-mdm.sdulab.com
* Port	443
Instance Name	zdm
* User Name	iseapi
* Password	*****
Description	
* Polling Interval	0 (minutes)
Enable	<input checked="" type="checkbox"/>
Test Connection	Test Connection
Save	Save
Reset	Reset

The polling interval specifies how often ISE will query the MDM for changes to device posture. Polling can be disabled by setting the value to 0 minutes. Polling can be used to periodically check the MDM compliance posture of an end station. If the device is found to be out of MDM compliance and the device is associated to the network, then ISE will issue a Change of Authorization (CoA), forcing the device to re-authenticate. Likely the device will need to remediate with the MDM, although this will depend on how the ISE policy is configured. Note that MDM compliance requirements are configured on the MDM and are independent of the policy configured on ISE. It is possible, although not practical, to set the polling interval even if the ISE policy does not consider the MDM_Compliant dictionary attribute.



Note

ISE requests a list of non-compliant devices from the MDM Server. XenMobile Device Manager can be configured to limit the maximum number of stations returned in the list. See the XenMobile REST API documentation for further information.

The advantage of polling is that if a user takes the device out of MDM compliance, they will be forced to reauthorize that device. The shorter the window, the quicker ISE will discover the condition. There are some considerations to be aware of before setting this value. XenMobile defines eleven conditions that can result in a device being marked as non-compliant. ISE cannot distinguish which condition caused the non-compliance event and will treat all in the same manner. In all cases, ISE will instruct the WLC to issue a CoA that will interrupt the user's WiFi session, possibly terminating real-time applications such as VoIP calls. The user is not redirected to the remediation portal until they attempt to connect to a website that results in a redirect.













The polling interval is a global configuration and cannot be set for specific users or asset classes. The recommendation is to leave the polling interval at 0 until a full understanding of the MDM's configuration is attained. If the polling interval is set, then it should match the device check-in period defined on the MDM. For example, if the MDM is configured such that devices will report their status every 360 minutes, then ISE should be set to the same value and no less than half this value. Oversampling the device posture will create unnecessary loads on the MDM server and reduced battery life on the mobile devices. There are other considerations with respect to scan intervals. Changing MDM timers should be done only after consulting with XenMobile's best practices.

The Test Connection button will attempt to log in to the API and is required prior to saving the settings with the MDM check box set to Enable. If the test does not complete successfully, the settings can still be saved, but the Enable box will be deselected and the MDM connection will not be active.

Verify Connectivity to MDM

Some problems can occur when testing the connection to the MDM server. [Table 1](#) shows some common messages generated when testing the connection between ISE and XenMobile. The last message shown below confirms a successful connection.

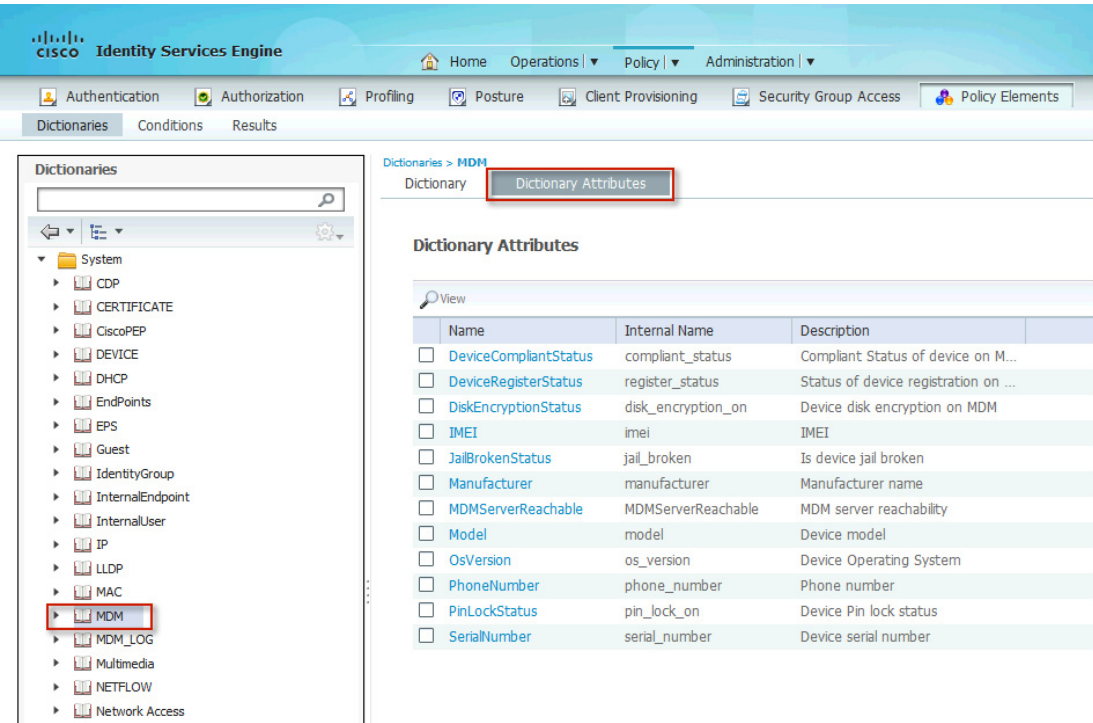
Table 1 **Connection Messages**

Message	Explanation
 Connection Failed: Please check the connection parameters. 	A routing or firewall problem exists between the ISE located in the data center and the MDM located in either the DMZ or Cloud. The firewall's configuration should be checked to confirm HTTPS is allowed in this direction.
 Connection Failed 404 : Not Found 	The most likely cause of an HTML 404 error code is that an instance was configured when it was not required or that the wrong instance has been configured.
 Connection Failed 403 : Forbidden 	The account setup on the XenMobile server does not have administrator privileges. Validate that the account being used by ISE is assigned the administrator role as shown above.
 Connection Failed 401 : Unauthorized 	The user name or password is not correct for the account being used by ISE when trying to login to the XenMobile Device Manager.
 Connection Failed: There is a problem with the server Certificates or ISE trust store. 	ISE does not trust the certificate presented by the XenMobile website. This indicates the certificate was not imported to the ISE certificate store as described above or the certificate has expired since it was imported.
 The MDM Server details are valid and the connectivity was successful. 	The connection has successfully been tested. The administrator should also verify the MDM dictionary has been populated with attributes.

Review MDM Dictionaries

When the XenMobile MDM becomes active, ISE will retrieve a list of the supported dictionary attributes from the MDM. Currently XenMobile supports all of the attributes that ISE can query. The dictionary attributes are shown in [Figure 4](#).

Figure 4 Dictionary Attributes



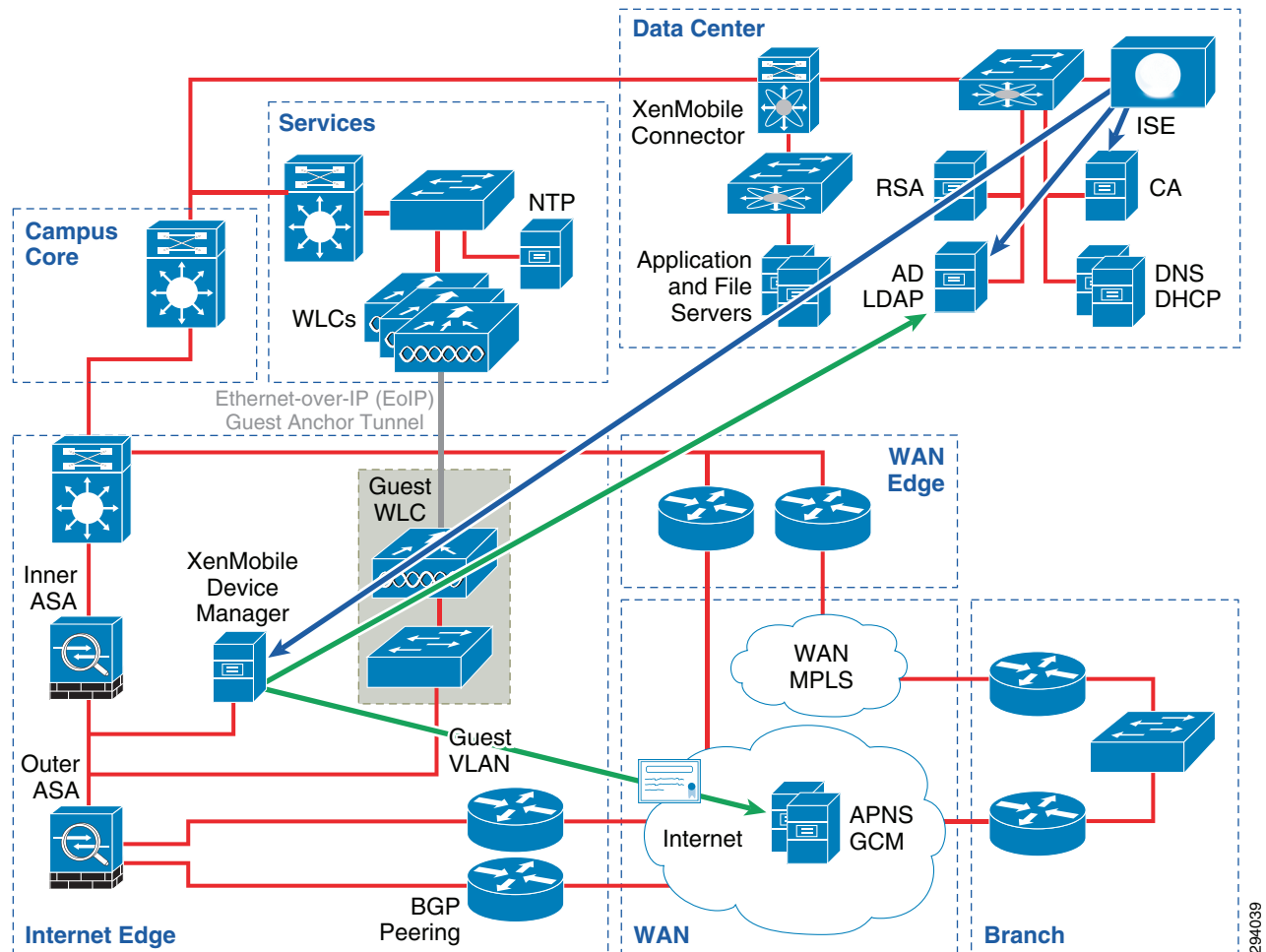
Enterprise Integration

Both ISE and MDM should be integrated into a common enterprise environment. At the basic level, this involves sharing the same directory structure. A common directory simplifies the operational aspects of the overall system, but also allows a consistent policy structure around AD group membership. For example, if a user is a member of the FULL_ACCESS group, that membership should result in a policy from both ISE and MDM that is consistent with the group and cognizant of the other component. If the MDM installs an application on a device, then ISE should allow the application on the network for members of that AD group.

XenMobile as a cloud service offers an Enterprise Connection between the cloud and the enterprise to enable directory resources to be available. The connection is based on an encrypted VPN tunnel between the cloud service and an ASA in the enterprise DMZ. In addition to directory services, the VPN tunnel allows the XenMobile service to integrate with an on-premise CA server, Microsoft ActiveSync service, or Blackberry's Mobile Service Provider (MSP) component. Furthermore, XenMobile Enterprise Connector can be used to provide Mobile Application Tunnels (MAT) to applications running the mobile device. Additional details, including installation and deployment, are available from Citrix.

For the remainder of this section, an on-premise model is assumed where the administrator has allowed the XenMobile Device Manager LDAP access to the corporate directory structure, either directly or via a third-party reverse proxy. The Device manager will also need to establish a connection with the Apple Push Notification Service (APNS). Finally, mobile devices must be able to establish connections to the device manager from both the campus and Internet to allow device check-ins. There are additional components typically found in an on-premise model that are not discussed here, including ZSM-Lite, SharePoint server, Zenprise Secure Mobile Gateway (SMG), and the BES server.

Figure 5 *Typical On-Premise Deployment Model*



Socket Requirements

There are several flows that need to be allowed between the various components. The full list is available from Citrix. [Table 2](#) summarizes the required sessions.

Table 2 **Common Socket Requirements**

Source	Destination	TCP Port	Purpose	Comment
ISE	Device Manager	443	MDM API	Cert Required
Device Manager	APNS	2195	Apple Push Notification	Cert Required
Device Manager	APNS	2196	Apple Push Feedback Service	APNs Message Status
Device Manager	LDAP (sLDAP)	389 (636)	Directory	
Mobile Device	ISE	8443	Captive Portal	On-Boarding, Remediation
Mobile Device	Device Manager	8443	OTA	Enrollment
Mobile iOS Device	APNS	5223	Apple Push Notification	

Active Directory/LDAP Integration

With either an on-premise or cloud model, integrating ISE and the MDM to a common directory is important for the overall operations. One benefit is the ability to set a requirement that a user periodically change their directory password. If the MDM were using a local directory, it would be nearly impossible to keep the accounts in synchronization. But with a centralized directory structure, password management can be simplified. The main advantage is the ability to establish complementary network and device policy based on group membership. The CVD provides examples of how groups can be used to establish a user's entitlement to network resources. Likewise, the same group membership can be used to differentiate access to device resources and mobile applications.

AD Group Memberships

Three possible AD groups are presented in the CVD to illustrate their usage—Domain Users, BYOD_Partial_Access, and BYOD_Full_Access. ISE establishes the device's network access based on the associated user's membership.

Figure 6 shows the policies presented in the CVD.

Figure 6 **CVD Use Policies**

Policy	AD Group	Compliant		Permission	
		ISE	MDM		
Personal_FullAccess	BYOD_Full_Access	YES	YES	Full	✓
Personal_PartialAccess	BYOD_Partial_Access	YES	YES	Partial	⚠
Personal_InternetOnly	Domain Users	YES	YES	Internet Only	🌐
Corporate Devices		YES	YES	Full	✓

These groups can be extended to the MDM such that members are issued profiles that complement their level of network access. As an example, Table 3 shows some arbitrary policies that can be established and enforced based on the CVD use cases.

Table 3 *Policies Based on CVD Cases*

Ownership	User Group	Restrictions
Employee-Owned Device	Domain Users	Internet Only, personal devices are not required to on-board with the MDM.
	BYOD_Partial_Access	Fairly restrictive policy that isolates corporate data into containers. Restrictions prevent users from disabling the policy.
	BYOD_Full_Access	Trusted users are offered a slightly less restrictive policy. Corporate data is still isolated in containers.
Corporate-Owned Device	All Users classes	Very restrictive device policy disabling non-essential business functions such as the game center.

Domain Users is the default AD group. By definition, every user defined in the directory is a domain user. While it is possible to create the reciprocal group on the MDM, it is not needed. The CVD treats non-domain members as temporary guests. These guests are unlikely to need MDM management. More important, if a user is not a domain member, then the MDM administrator will need to define a local user account. This is likely a very small set of users that are handled as an exception, such as distinguished guests. Domain Users are essentially everyone with an account on the MDM, including members of BYOD_Partial_Access and BYOD_Full_Access.

MDM profiles and ISE Authorization rules are fundamentally different with respect to AD Groups. ISE policy may include the AD group match as a condition for establishing a specific and single policy. MDM profiles are not a singular result. Most devices will be provisioned with multiple policy profiles based on various attributes. Members of the BYOD_Full_Access and Domain Users groups can each be configured for a specific profile. But if a user happens to have membership in both BYOD_Partial_Access and BYOD_Full_Access, then that user's device is provisioned with both profiles. In addition, every device will be provisioned with basic security restrictions. ISE will check the device to ensure these restrictions are met before granting network access. These restrictions establish ISE compliance and are defined here as required PIN lock, encrypted storage, and non-jail broken or rooted devices.

Device Policy

Apple and Android differ in how device management is implemented. Each offers APIs natively in the operating system that the MDM is able to leverage.

Device Profiles

Apple defines profiles that are an important concept of mobile device management. They are a foundational component of Apple's mobile device management protocol that is implemented by the operating system (iOS). This concept can be extended to application profiles, but as discussed here, they are found under the settings of the device. Each profile can contain one or more payloads. A payload has all the attributes needed to provision some aspect of built-in system functions, such as PIN lock. One special payload is the MDM payload that defines the MDM server as the device administrator. There can only be one MDM payload installed on any iOS device. In iOS 5 and earlier, the profile containing the

MDM payload cannot be locked and the user is free to delete it at any time. When this occurs, all other profiles installed by the MDM are also removed, essentially resulting in a corporate wipe. The MDM may lock any sub-profile that it installed to prevent the user from removing them individually. The MDM is allowed to inspect other profiles, such as the WiFi profile installed by ISE, but is not allowed to remove any profile that it did not install, including the WiFi profile as detailed in the BYOD CVD. Because multiple profiles can be installed on a device and profiles have payloads, it is possible to have a payload collision. Devices with multiple security payloads will install all the payloads by aggregating the most secure settings from each as a logical OR function. In most other cases the first payload is installed and subsequent payloads are ignored or multiple payloads are accepted. For example, the device can have multiple VPNs provisioned, but only one can be named XYZ.



Note

Starting in iOS6, Apple does allow the MDM payload to be locked if the user has not set a PIN lock. As presented in the CVD, a PIN lock is required to gain network access.

Android devices generally implement device management functions through a specific set of APIs, most of which are manufacturer or model specific. For example, Samsung uses their SAFE API while HTC uses its One APIs.

XenMobile uses policies to create and define device profiles. These policies can then be deployed to the device through the use of packages. XenMobile defines a rich set of conditions that can be placed on the deployment of these packages, including membership to an AD group. For example, a policy can be created for all employee-owned devices called BYOD_Employee.

Figure 7 *Configure Employee Device Policy*

The figure consists of two screenshots of a 'Password policy configuration creation' dialog box.

Top Screenshot (General Tab):

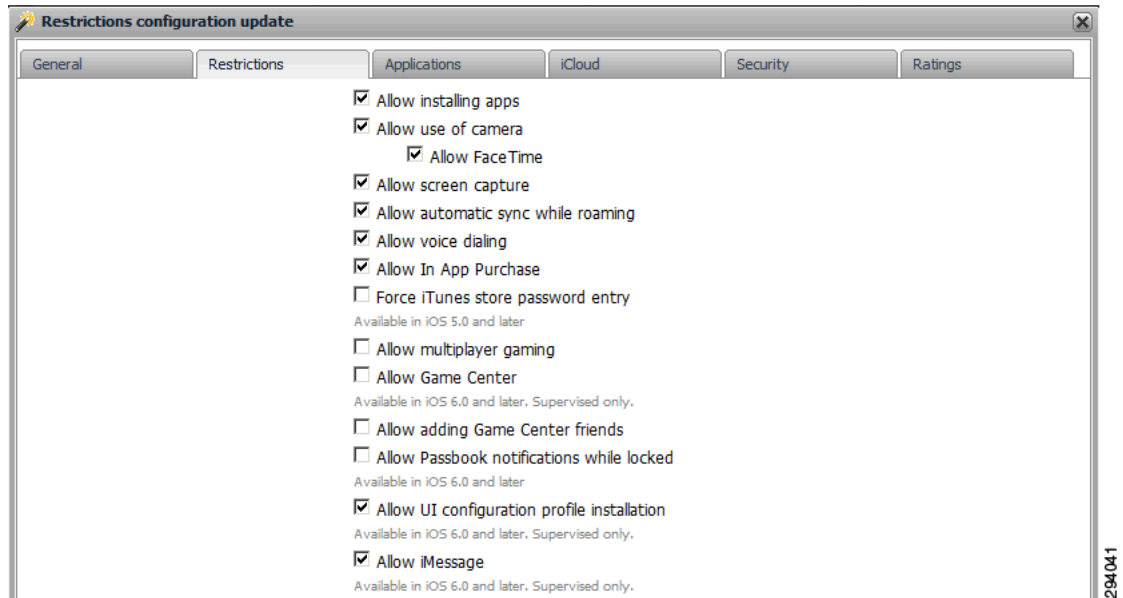
- Identifier:** BYOD_Employee
- Display name:** BYOD_Employee
- Organization:** SDU Lab
- Description:** Policy Applied to all Employee owned devices
- Allow profile removal operation:** Never

Bottom Screenshot (Policy Tab):

- ☒ **Require a code on the device**
Require a code to use the device
- ☒ **Allow simple values**
Allow the use of repetitive, bottom-up and top-down character sequences
- ☐ **Require alphanumeric values**
Require at least one letter
- Minimum length codes:** --
- Allowed minimum non-alphanumeric characters:** --
- Maximum passcode age(1-730 days, or none):** 0
- Auto lock (1-5, 10 or 15 minutes or none):** --
- Codes History (1 to 50 codes or none):** 0
- Grace period before device lock:** --
- Maximum failed attempts:** --

The policy can include password policy or restrictions specific to employee devices. Additional policies can be created for users who belong to either the BYOD_Full_Access or BYOD_Partial_Access Active Directory group. [Figure 8](#) shows a hypothetical example of restrictions that will be applied to BYOD_Full_Access members.

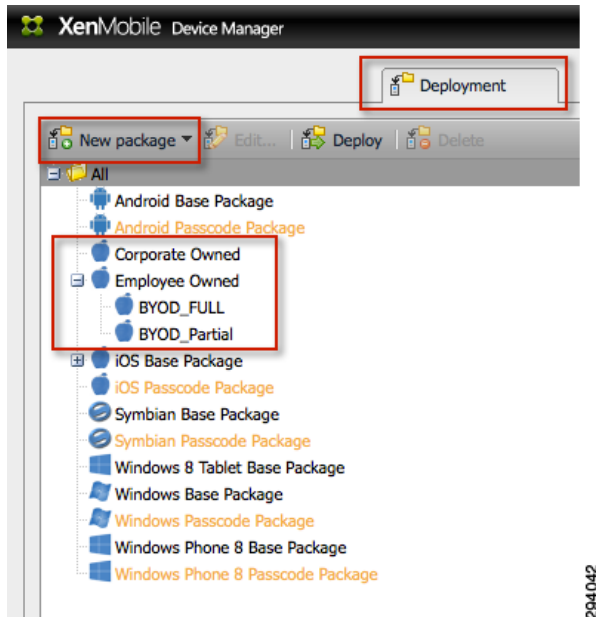
Figure 8 *Setting Device Restrictions*



Deploying Policy to the Device

After creating these policies, deployment packages are used to determine how policies will be applied. Deployment packages and the logic used to deploy them provide structure to XenMobile's policy management. There are two components to this structure, inheritance and compound logic. First, deployment packages have inheritance. For example, a package may be created for employee devices. It will deploy policy that should be applied to all employee devices. From this package, two child packages may be created, one specific to members of AD group BYOD_Partial_Access and the other for members of BYOD_Full_Access. These child packages will contain policy specific to users of the matching AD group and do not need to replicate the policy applied from the Employee package. The resulting profiles installed on the device will depend both on the device ownership and the user's AD group membership.

Figure 9 Hierarchal Deployment Packages



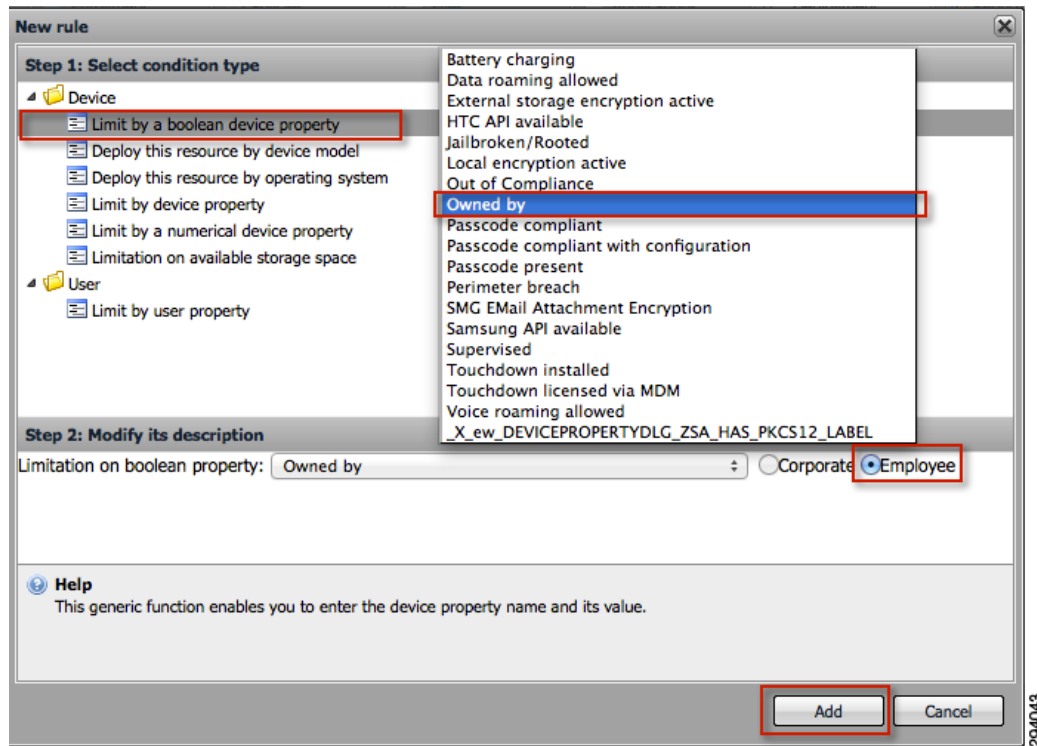
XenMobile comes preinstalled with two default packages for each of the various supported devices: Base Package and Passcode Package. These can be used to accelerate the initial deployment. However administrators should carefully review the policy each implements to ensure it is appropriate. In many cases, it may be advisable to use the preinstalled packages as templates to create new policy profile, leaving the XenMobile policies unmodified. The example deployment packages shown in [Figure 9](#) are used to extend the use cases presented in the CVD and are intentionally simplistic. It is usually a good idea to create specific policies and deployment packages that align with the enterprise organization so that changes can be applied to a targeted group of devices. For example, a change may be required for outside sales employees that would not benefit inside sales employees. This change may be difficult if devices used by all sales employees were initially setup with the same deployment package set.

A deployment package has several common components:

- A unique and descriptive package name.
- Groups of users that the package will be deployed to. User groups can be either from Active Directory or locally defined user groups.
- A resource or list of resources. Resources are the objects that will be deployed by the deployment package. They can include applications, policy configurations, SharePoint, Application Tunnels, etc.
- A deployment schedule that determines when the deployment will occur. This is not the same as time based restrictions. Generally packages should be tested on a small set of devices before global deployment.
- Deployment rules that determine to which devices the package will be deployed. Deployment rules can be configured with a simple or advanced dialog. Rules can consider a comprehensive list of device attributes that can be combined in any logical combination. Rules can also consider specific user attributes not related to the user group. For example, if a user belongs to several groups, a user attribute can be used to match the user's primary AD group. In order to extend the use cases presented in the CVD, only the device Boolean "Owned by" is needed, as show in [Figure 10](#).

Deployment rules can be used as another method to provide a logical hierarchal structure. In this case, the deployment rules of multiple packages will include a check for “employee owned”. When using this approach, it is a good idea to code the structure into the name of the package since the natural tree structure will not be readily apparent.

Figure 10 **Deployment Based on Device Ownership**



The complete logic is summarized in [Figure 11](#).

Figure 11 *Deployment Package Summary*

Edit package

Step 6/6

- Package name
- Groups of users
- Resources
- Schedule
- Deployment rules
- Summary**

Package summary
Review the settings and click "Finish" to create this package

Package name: Employee Owned
Default deployment: No

Groups of users: ActiveDirectory.SDULAB.COM
Deploy to anonymous users: No

Resources to be deployed: BYOD_Employee

Deployment schedule: Each time the device is connected
Always deployed

Deployment rules: Limitation on boolean property: Owned by Employee

< Previous Next > Finish Cancel

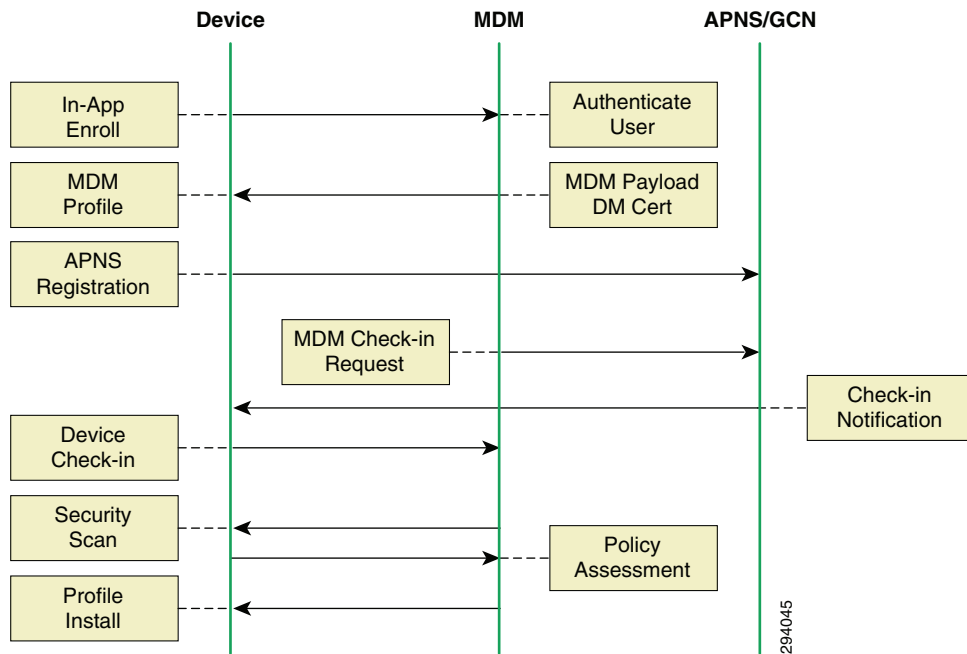
With the example configuration shown above, all Active Directory users with a personal device will have the BYOD_Employee resource installed. This will establish a password policy on the device. Only devices that match this deployment package will be considered for the two child packages, BYOD_Full_Access and BYOD_Partial_Access, that are used to place additional policy on the device based solely on Active Directory user groups. The end device will see two profiles, one because the device is employee owned, the other based on their membership to an AD group.

Policy Deployment During Enrollment

When an iOS device initially enrolls with the XenMobile Device Manager, it gets two profiles. One has certificates that ensure the device will trust the XenMobile Device Manager. The other is the MDM payload that allows the device to receive secure messaging from the push service. The Device Manager will request a device check-in via the push service. The device will then contact the XenMobile Device Manager to complete the check-in request. At this time, the additional deployment packages are installed securely on the device. When integrating with ISE, there are some timing issues that need to be considered and are discussed in [PINLockStatus](#).

[Figure 12](#) shows the steps required of a device to enroll with the MDM.

Figure 12 Enrollment Network Flows



SCEP

The XenMobile MDM can provision certificates onto the device. This allows profiles to contain a payload that provisions a service that requires authentication via a certificate and another payload contains the associated certificate. One such example is VPN payload for either AnyConnect or Cisco IPsec. This is discussed in more detail in [Application Distribution](#). Cisco ISE also uses SCEP to install user certificates for the WiFi profile.

Device Ownership

One of the key components of BYOD is the mix of personal devices and corporate devices on the network and the ability to establish policy based on this attribute. Both the ISE and the MDM have the concept of asset classes. This allows corporate devices to be distinguished from all other devices in the system. Ownership is an important aspect of BYOD. For example, an administrator may not want to issue a full wipe of personal devices or track the location of a personal device. However, corporate devices may get full wipes as a matter of normal operation and may be used to track location, especially if travel is a key component of the employee's job. Having the ability to handle the information gathered from personal and corporate devices differently is important.

In this first release of the MDM dictionary, there is not a tight integration between asset classes defined on ISE and those defined on the MDM. The API does not support such a device attribute. Complicating matters somewhat is the key index used to identify a device. ISE uses the device's MAC address, which is unique across the network, whereas XenMobile uses the device's serial number.

ISE determines corporate devices through an identity group referred to as the Whitelist, which contains the MAC addresses of corporate assets. Discovering the MAC address of Android and Apple devices is typically a manual process. Apple lists the MAC on the Settings > General > About page. XenMobile does allow devices to be bulk-imported into the system using the device serial number for iOS or

Android devices and either the device serial number or IMEI for Android devices. An enterprise may need to create a list of corporate owned device by MAC addresses and the associated serial numbers to pre-provision them on both systems. Apart from bulk imports, another option used to automatically mark ownership is device tagging with a script. This is covered in the XenMobile Administrator's guide. Users can declare device ownership when enrolling a device through the Self-Help portal page.

Device Restrictions

A device may be provisioned with multiple profiles that contain a restrictions payload. For example, a member of BYOD_Partial will get a restrictions payload that prevents devices from synchronizing documents with the iCloud. They will also receive a restrictions payload from the parent group Employee Owned that will set the ISE compliance restrictions, e.g., PIN lock, device encryption, and not compromised. When multiple restriction payloads are installed on a device, the device will aggregate the settings by keeping the more restrictive attributes. Since the enterprise-wide policy is for a PIN lock, the child organization groups are not required to repeat the PIN lock requirement and can focus on what makes that profile unique for that particular set of devices.

Table 4 *Device Policies at the BYOD Subgroup Level for Personal Devices*

Profile	PIN lock	Encryption	No iCloud Sync	Restriction A	Restriction B	Restriction C
Employee Owned	X	X		X		
BYOD_Partial			X	X		X
Result	X	X	X	X		X

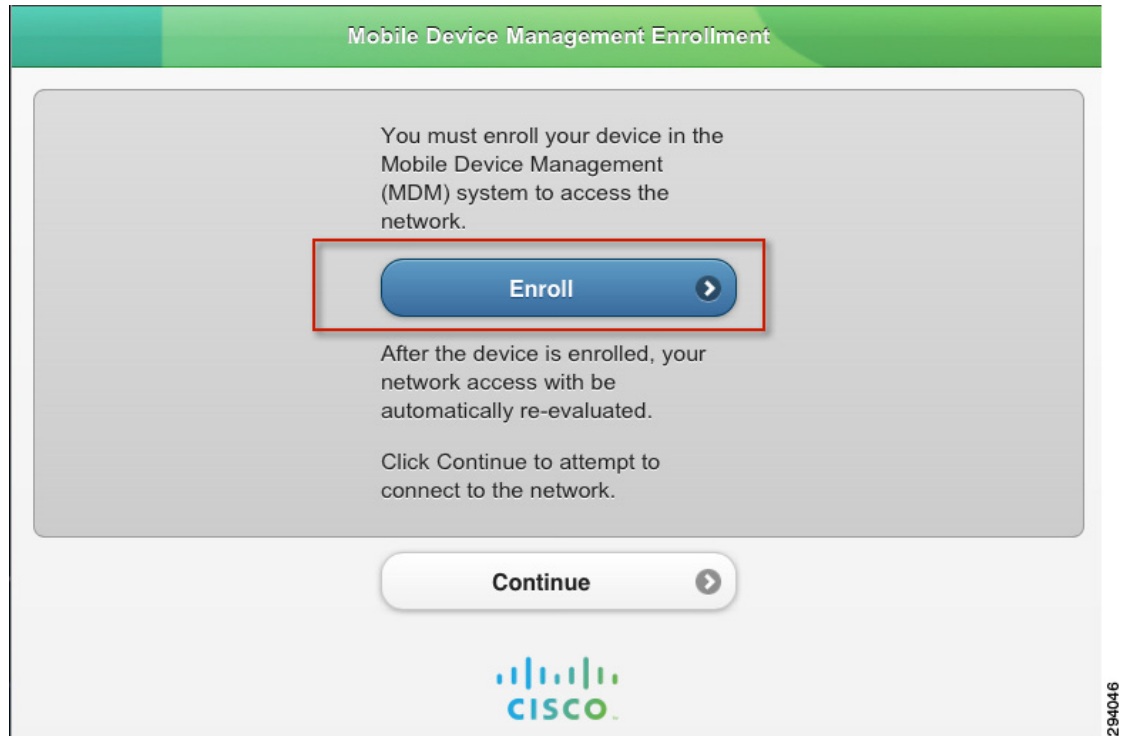
User Experience

For the most part, the fact that a device is under management is seamless to the user with the exception of the enrollment process. If they are running the mobile client application, as recommended for ISE compliance checks, then the user will have some additional information about their device that will be useful for troubleshooting with ISE. Users will also be required to complete the on-boarding procedure.

MDM On-boarding

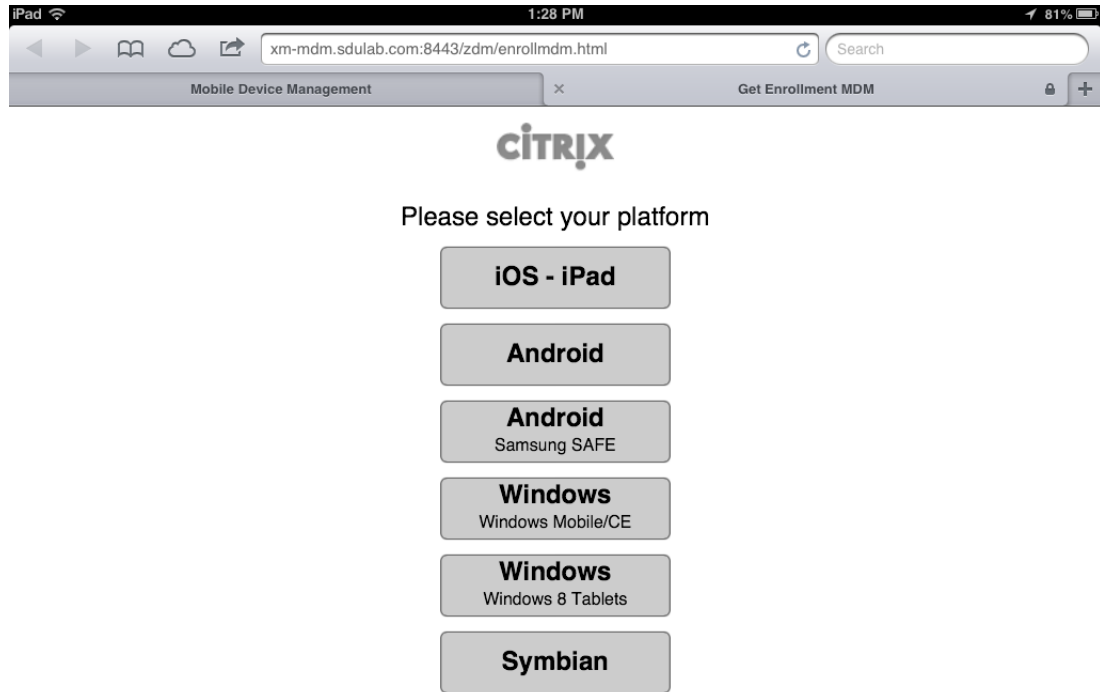
The workflow that users must complete to on-board their device is set by the ISE policy. As presented in the CVD, the user will first on-board with ISE. When the user first joins the BYOD_Employee SSID, ISE will check the device's MDM Registration status through the MDM API. If the device is not registered, then a captive ACL is activated. This ACL allows Internet access, but captures any attempts to access corporate resources. A full explanation is provided in the CVD. The device requires Internet access to complete the MDM on-boarding process, including downloading the client application from either Google Play or Apple's App Store. When the device is captured the user is presented with a screen that includes two buttons, as shown in [Figure 13](#). The first redirects the client to the MDM registration page. The second button issues a CoA to force a re-evaluation of the AuthZ policy after MDM enrollment completes.

Figure 13 **MDM Redirect for Enrollment**



When the user lands on the XenMobile registration page, they are asked to choose their platform type. This allows the system to direct the client to the proper location to download the client applications. XenMobile version 8.0.1 will direct the user to download both the Worx Home application and the Enroll application. [Figure 14](#) shows the platform options available to the user. Note that in the current version of the CVD, only Apple iOS and Android devices are supported.

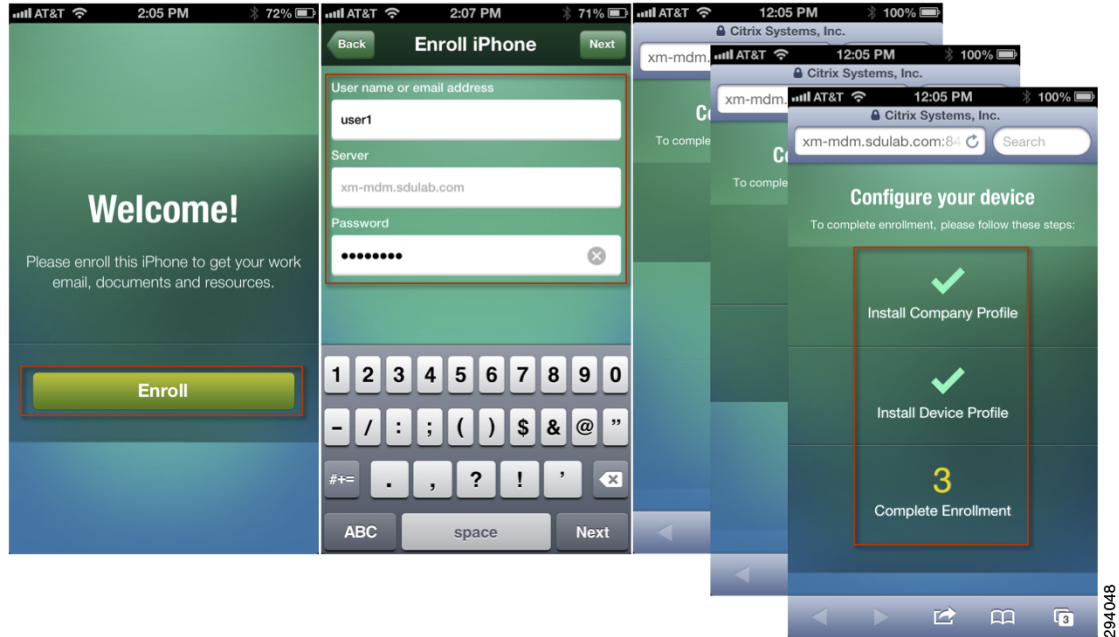
Figure 14 **XenMobile Platform Selector**



294047

After the user launches the Enroll mobile application, they will be asked for their credentials and the server they wish to connect to, as shown in [Figure 15](#). Server information should be provided to the user prior to starting the enrollment process. If the user successfully authenticates, a profile including the MDM payload and associated certificate is installed on the device. The user will be led step-by-step through the enrollment process. The final step verifies that the mobile device can establish a secure session with the XenMobile Device Manager.

Figure 15 *XenMobile Enroll Mobile Application*



After enrollment, the user returns to the page shown in [Figure 13](#) and chooses the “continue” button. This button notifies ISE that the user has completed the MDM enrollment process. ISE responds by issuing a CoA to the device, causing the device to re-authorize. This time, the MDM should respond that the device’s status is now “enrolled”.

While this is occurring, the XenMobile Device Manager will push a check-in request to the iOS device through APNS. During this initial check-in, additional profiles, applications, or Web Clips will be provisioned on the device. Web Clips are HTML bookmarks that are displayed as application icons on an Apple mobile device. Android devices simply call these bookmarks.

Pass Code Complexity

The user may be required to configure a PIN lock on their device during the on-boarding process if the device is not already configured with one. When this occurs, the user will need to launch the client app and send data. This is explained in more detail in [Device Compliance/Restrictions](#). The MDM administrator can choose the minimum password length and complexity. The natural tendency is to require very strong passwords. However there may be unintended consequences, especially with employee-owned devices. The PIN lock will need to be entered any time the employee wants to use their phone. While texting and driving is illegal in many locations, the PIN lock is also required to make phone calls. If the user is required to navigate through several keyboards to enter the PIN lock, the administrator may be creating an environment of risk taking. There may be legal implications outside the scope of this document that should be considered. The more likely scenario is that the user will opt-out of the BYOD network for their personal devices. Devices not managed could have no PIN lock at all and yet still contain corporate data that the employee improperly put on the device such as SMS logs. A practical approach is to require a simple four digit PIN on personal mobile phones. Corporate tablets can still be profiled with complex passcodes including special characters. This provides a balanced approach and will not discourage participation. Four digit PINs or the last four digits of a SSN are used fairly often to provide some level of security. Android and Apple devices can limit the ability to attempt to guess the code by implementing timed retries or, in some cases, wiping the device completely.

**Note**

Apple iOS7 is expected to change the behavior of full wipes on previously-owned devices. If the device was previously registered to an iTunes account, the device will continue to require owner credentials even after a full wipe has been executed.

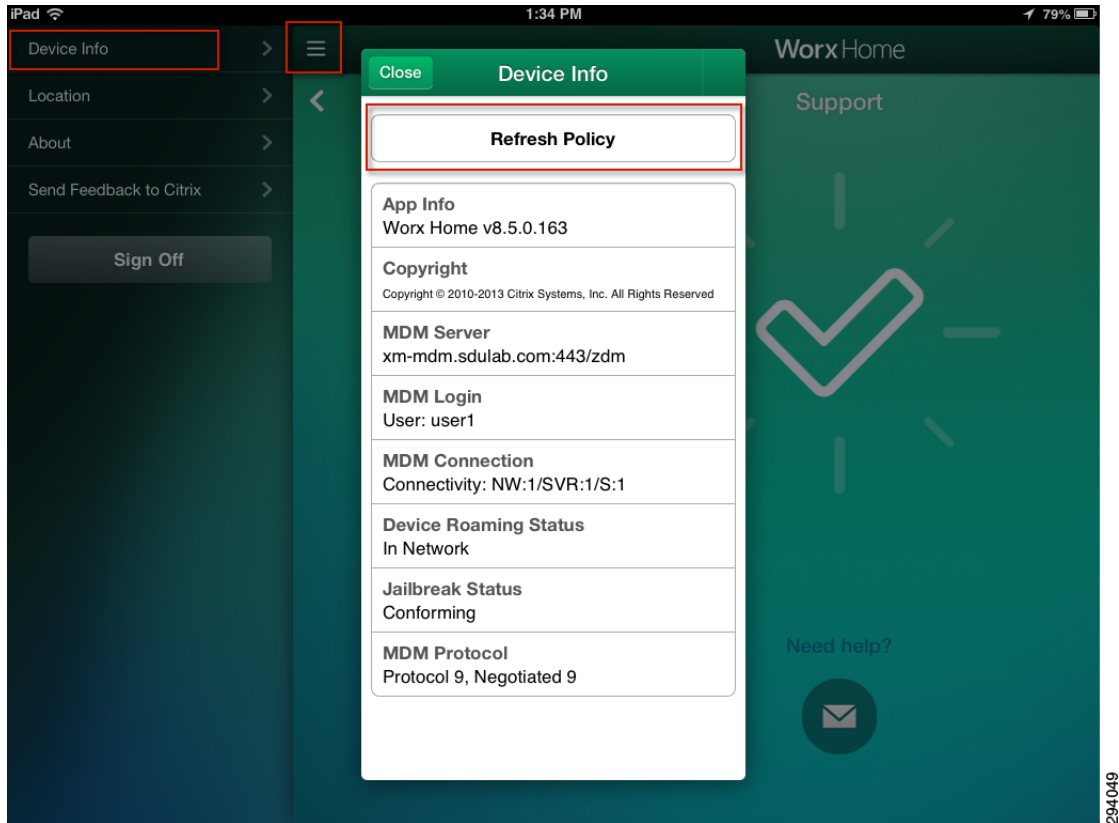
Mobile Client Application

With Apple devices, the majority of MDM features are implemented directly through the operating system and do not require a mobile device client application. However some of the advanced functionality does require a client running on the endpoint. In particular, jailbreak and rooted detection requires the XenMobile Worx Home client, as does location-based policy. The Worx Home client application is installed on Android devices during the enrollment process. It is recommended to mark Worx Home as a required application on all devices because the XenMobile Device Manager depends on Worx Home to perform jailbreak and root detection, which are attributes ISE considers when making policy decisions and because some users may enroll with the MDM outside of the ISE on-boarding workflow.

In addition to providing specific device information, the client application offers the end users some useful troubleshooting information, including application logs that users can use to monitor the client's interaction with the server. Users can also use the Worx Home application to determine their geographical location. If location services are enabled, this will also be the location provided to the server. The XenMobile Device Manager can use location to establish geo-fencing and location-based policy.

One useful feature of the client application is the ability to manually refresh the device's posture to the server. The need arises when the device has been placed in MDM quarantine due to a compliance violation. For example, the device may not have a PIN lock when one is required. When the user configures the device with a PIN lock, the phone's OS will not trigger an update to the MDM agent. The agent will detect the change during the next security scan interval. The server will only discover this the next time the device is polled. This could result in ISE continuing to place the device in quarantine, even after the user has corrected the issue. Rather than waiting for the MDM to poll the device for an update, the user could use the mobile application to send the current data to the server. [Figure 16](#) shows the refresh button on the mobile client.

Figure 16 **Manually Refresh Server Data**



In addition to the mobile device client application, Citrix offers a range of other solutions to enhance the user experience by seamlessly distributing content securely to those users entitled to access it. Products such as ShareFile can be deployed on the device via the XenMobile Device Manager. In addition, the MDM can also integrate with a SharePoint server.

Application Stores

The XenMobile Device Manager can install applications from the XenMobile Self-Serve app store or the public stores, such as Apple's App Store and Google Play, once they have been loaded into the Device Manager. Public applications can be part of a Volume Purchasing Program (VPP) where the enterprise can purchase licenses in bulk. Enterprise-developed applications can also be made available to users via the Self-Serve store. The Self-Serve store allows users to browse through recommended applications. For mandatory applications, a policy can be created to push the application to the device. The user has the option to decline the install, which could trigger an MDM event if configured to do so. Some applications such as Cisco AnyConnect can be provisioned directly as shown in [Cisco Applications \(Jabber, etc.\)](#).

Corporate Data

XenMobile, Citrix ShareFile, and ISE work closely together to create a fairly comprehensive approach to managing corporate data. This is generally known as data loss prevention (DLP). Data comes in two forms, at-rest and in-flight. Data at-rest is stored directly the mobile device and data in-flight is the movement of data to and from the device. This can be extended to include moving data between two storage containers on the same device.

Data at-Rest

Android and Apple handle stored data differently. Android has an open file structure that allows content to be shared between applications. Files are protected with various levels of file permissions. This creates a tight and integrated environment. Many Android devices also support external and removable storage in the form of SD Cards. Apple iOS creates a storage environment for each application. When an application is deleted, the partition holding that application's data is also removed. XenMobile can load files directly on an Android device from the device manager. It also supports SharePoint provisioning. Citrix also offers their ShareFile product specifically to allow users to collaborate with secure corporate data. ShareFile has its own administrator console separate from the XenMobile Device Manager. The ShareFile service can interface with Microsoft Active Directory to allow the same group membership used by both ISE and XenMobile to be used for content distribution policy. XenMobile also offers email attachment policies that are available when integrating with Microsoft Exchange. This can be used to restrict the user's ability to print, forward, copy/paste, etc. email attachments. In the case of Android devices, the Device Manager can administer policy to the TouchDown email application.

Data in-Flight

XenMobile supports application tunnels. These tunnels protect corporate data moving to and from the device by encrypting application data. Each application is assigned to a unique tunnel that terminates on the Device Manager. The XenMobile Administrator's guide has more information on using application tunnels.

Sharing data between applications is fairly common. Built-in system applications like Contacts can share their information. With Apple devices, the data is passed through owning application. Apple iOS now provides privacy settings to control access to system data stores. The common thread with both Android and Apple is tight application integration. This functionality presents challenges when trying to contain data.

Users may be tempted to install third-party cloud storage applications. Common examples include Dropbox, SkyDrive, Google Drive, and iCloud. This is obviously a concern because data is moved off the enterprise network and stored on servers not under enterprise control. XenMobile can blacklist these applications. This is most appropriate on corporate devices, but could also be applicable on personal devices when specified in the user agreement. Note that restrictions on personal devices are in effect continuously unless the policy enforcing the restriction is tied to time or location information. Citrix can also reduce the temptation to use third-party storage services by offering ShareFile, which is better integrated with corporate content and provides a more effective method to collaborate.

Email attachments, SMS messaging, and many other messaging clients and their chat logs are also a concern when enforcing data loss prevention. XenMobile has several approaches to email management. The most comprehensive is securing and encrypting email attachments that route through corporate exchange servers. Policy can be set to prevent attachments from being forwarded, printed, or pasted into another application. Additional components include AppTunnels to a SharePoint server. Email

attachments can be placed on the SharePoint. XenMobile also offers a Secure Mobile Gateway (SMG). These capabilities are detailed in the XenMobile configuration guides. In each case, network policy can be established with ISE to reinforce the device's application policy.

Corporate Wipe

Both ISE and XenMobile Device Manager can remove corporate data from personal devices. XenMobile calls this a selective wipe, while ISE refers to it as a Corporate Wipe. Other common terms used are enterprise wipe or partial wipe. When ISE issues this command, it is forwarded to XenMobile via an API call. The MDM in turn removes corporate applications using privileges granted to the MDM Profile (iOS) or the device administrator (Android). When these complete, the MDM profile is removed, which also removes all the associated sub-profiles. While it is also possible to leave some applications behind, all MDM installed profiles are removed. Profiles not installed by the MDM are not deleted. This includes two profiles that were installed by ISE, one containing the CA certificate and the other containing the WiFi profile and user certificate. When an application is deleted, the associated data is also removed. This is especially effective when ShareFile has been deployed because it is a centralized location that holds sensitive corporate data. If a built-in application was disabled by the XenMobile Device Manager, it will be restored.

The relationship between the MDM profile, sub-profiles, and applications is important to understand. [Figure 17](#) shows this relationship. The top two profiles were installed by ISE and will remain on the device after a corporate wipe has been issued. The Citrix installed CA profile named Citrix (01) NOAM Partners will also remain on the device. The remaining four profiles will be removed. The profile labeled MDM Configuration contains the MDM payload and the certificate used to sign the sub-profiles. This profile is used to remove applications and sub-profiles. Removing any application, such as the Citrix ShareFile, also removes the data associated with the application. The MDM_Configuration is not associated to any specific policy and is required to place the device under management. The profiles BYOD_Full is a sub policy of BYOD_Employee. The ISE_MyDevices profile contains the Web Clip and is independent of the other policies installed on the device.

Figure 17 *XenMobile Enterprise Wipe*



The mobile client application can be removed. However, typically it is left on the device to facilitate an authenticated user to re-enroll the device. Corporate wipes by themselves do not blacklist the device from either the XenMobile Device Manager or ISE. An ISE administrator, the MDM administrator, or the user from either the ISE My Devices Portal or the XenMobile Self-Serve page may issue a selective wipe. If a wipe is being issued as a result of an employee's termination, then additional steps must be undertaken, such as blacklisting the device with ISE and removing the user AD group memberships. This will prevent the user from re-enrolling the device. Optionally, the user certificate can be revoked on the CA server.

The final action is to force the user to re-authorize against ISE by disassociating them from the network. ISE supports this directly from the Operations page, as shown in [Figure 18](#). The device may immediately try to re-associate, but will match the blacklist thereby denying the device network access. The user will not be able to self-enroll this particular device until IT has removed the MAC address from the blacklist.

Figure 18 *Forced CoA from ISE*

</

Self-Serve Portal

XenMobile offers a Self-Serve portal that allows the user to manage their devices, as shown in Figure 19. This site can be configured to give users access to various Device Manager functions across all of their enrolled devices via user roles. An employee can lock, wipe, or locate their device. Users can also view information about the device properties, software, profiles, and MDM status.

Figure 19 *XenMobile Self-Help Portal for Users*

XenMobile Device Manager Welcome, user1@sdulab.com | Log Out

iPhone iPad **Enroll Device**

Refresh Locking Wiping Locating

Device information

- General
- Properties
- Software
- iOS Profiles
- MDM status

General

Identifiers of device

Serial number: F4KJP1V9F19F

IMEI/MEID: 01 335900 809819 1

ActiveSync Id: ApplF4KJP1V9F19F

Wifi Mac Address: E4:8B:7F:70:7E:B8

Bluetooth Mac address: E4:8B:7F:70:7E:B9

Security

Strong ID: HCUSSATB

Device lock: No device lock

Device unlock: No device unlock

Device full wipe: No device full wipe

Selective wipe: The last device selective wipe was completed on 5/21/13 2:39:39 PM.

ISE also provides a My Devices Portal as detailed in the CVD. Currently the two sites are distinct and not cross-linked. Some of the functionality does overlap, such as the MDM actions. But users will likely want a Web Clip to both locations.

Verify Device Compliance


ISE Compliance versus MDM Compliance

There are two compliance checks required of the device as configured in the CVD. The first is defined by policy configured on ISE. This is specific to corporate network access control (NAC). XenMobile also offers attributes that result in the ISE dictionary attribute DeviceCompliantStatus to be marked NotCompliant. These may overlap the posture attributes ISE has been configured to use. The ISE administrator and MDM administrator should work together to ensure the DeviceCompliantStatus is being used as intended. Some attributes such as PIN lock could be considered twice. The more restrictive results should occur earlier in the ISE Authorization policy stack as is shown in the CVD. One difference is that the MDM NAC Compliance attributes are a system-wide setting. All devices will use the same parameters to establish the compliance policy and will have the same result. ISE can be configured to apply different compliance results by combining the compliance attribute with other ISE dictionary elements, such as AD user groups. While not shown in the CVD, it is possible to configure two distinct ISE compliance policies, one corporate and a different one for personal devices.

XenMobile is able to distinguish NAC compliance from MDM compliance that might result in an automated action. Integrating MDM compliance with NAC compliance is a relatively new concept. Again some coordination is required so that an automated response is not blocked by an ISE policy resulting in Quarantine.

The attributes shown in Table 5 shows the attributes that ISE can use and the attributes the MDM can consider when setting DeviceCommpliantStatus that is reported to ISE via the MDM API.

Table 5 Compliance Attributes

ISE Compliance Attributes	XM NAC Compliance Attributes
<div><div><input type="checkbox"/> DeviceCompliantStatus </div><div><input type="checkbox"/> DeviceRegisterStatus</div><div><input type="checkbox"/> DiskEncryptionStatus</div><div><input type="checkbox"/> IMEI</div><div><input type="checkbox"/> JailBrokenStatus</div><div><input type="checkbox"/> Manufacturer</div><div><input type="checkbox"/> Model</div><div><input type="checkbox"/> OsVersion</div><div><input type="checkbox"/> PhoneNumber</div><div><input type="checkbox"/> PinLockStatus</div><div><input type="checkbox"/> SerialNumber</div></div>	<div><div>Forbidden Apps</div><div>Non Suggested Apps</div><div>Missing Required Apps</div><div>Rooted Android / Jailbroken iOS Devices</div><div>Revoked Status</div><div>Unmanaged Devices</div><div>Inactive Devices</div><div>Noncompliant Password</div><div>Anonymous Devices</div><div>Out of Compliance Devices</div><div>Non Encrypted Devices</div></div>

Forbidden Apps

Non Suggested Apps

Missing Required Apps

Rooted Android / Jailbroken iOS Devices

Revoked Status

Unmanaged Devices

Inactive Devices

Noncompliant Password

Anonymous Devices

Out of Compliance Devices

Non Encrypted Devices

XenMobile can also trigger automatic responses to address a specific condition. Each automated action consists of a trigger, condition, action, and options. There are four triggers available: Event, Device Property, User Property, and Application. Each trigger includes specific properties that can be checked.

Figure 20 shows about half the available device properties. The available actions are selective wipe, wipe, revoke, set as out of compliance, and notify. The set as out of compliance is tied to the out of compliant devices NAC condition resulting in an ISE policy response.

Figure 20 **Automated Actions**

Device Compliance/Restrictions

Restrictions and compliance are distinct but related concepts. A user is not offered the option of not adhering to a restriction. If a PIN lock is required, the device will be locked until the user selects a PIN that meets the established complexity. If the camera has been disabled, the icon is removed and the user has no way to launch the camera application. Restrictions are policy elements that are enforced without exception. Compliance is when a device is operating outside of the established policy. Non-restrictive items that could cause compliance events are things such as the minimum OS version. The key point is that it is not possible to be non-compliant with a restriction. The exception is restrictions that include a grace period.

Device Scanning Intervals

The MDM client application can periodically scan the device. There are several scans that run on different intervals, also available as device queries. The scans are:

- **Device Information**—General information about the device includes serial numbers, UDID, phone number, operating system, model, battery status, etc.
- **Security**—Includes encryption status, device compromised, data roaming, SIM card status, and the number of profiles installed but not active.
- **Profiles**—The installed profiles on the device, including those not installed by XenMobile.

- Apps—A complete inventory of all the applications installed on the device.
- Certificates—A list of the installed certificates on the device.

When a device periodically checks in with the MDM server, it notifies the server of the current scan results allowing the Device Manager to determine if any parameters are out of policy. XenMobile allows Android schedules to be configured as part of policy.

PINLockStatus

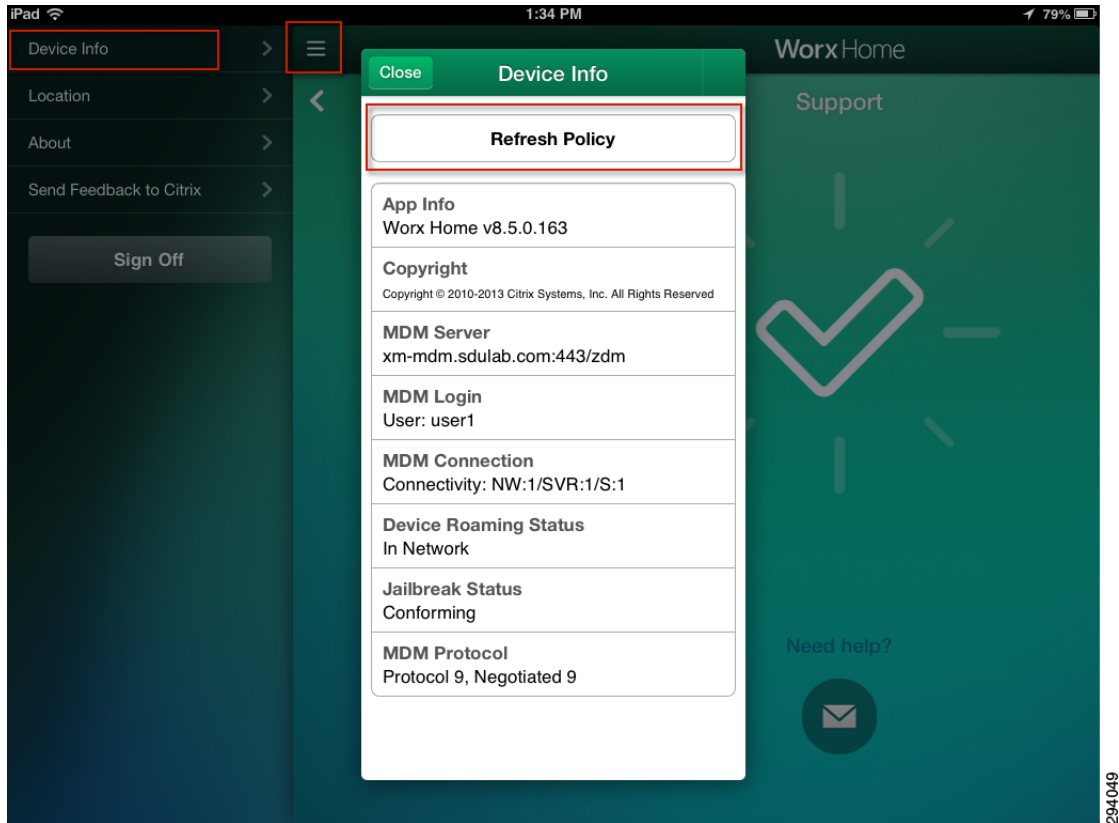
The PINLockStatus is available to the API and can be used by ISE to set a minimum requirement for network access, as is shown in the CVD. Typically PIN lock is set as a restriction. But there are some cases where the MDM can set compliance check against a restriction specific to PIN lock. It is possible to set a PIN lock with a grace period. During this time, the MDM can poll the device for the PIN lock status. When set, the triggered action could be the installation of additional profiles. By doing this, the device could be on-boarded with the MDM but not granted full access until the user sets the password or the grace period expires.

There are some caveats to be aware of with respect to ISE creating a PIN lock requirement for network access. These are not specific to XenMobile, however the workaround is. When users are issued instructions explaining the on-boarding process, they should be asked to set a PIN lock on their device prior to starting the on-boarding process, rather than waiting for the forced PIN lock mid-way through the procedure. If the user does not follow this, they could end up in a quarantine state. There are two issues at play:

- First, the MDM server does not get a triggered update when a user creates a PIN lock. Because it is set as a restriction, the user is required to enter one, but it will be some time before the server will become aware of the PIN lock. If the authorization policy is applied to the device, the MDM will report that the device is enrolled but is not configured with a PIN lock, resulting in the device being placed in quarantine.
- Second, the MDM on-boards by installing the MDM profile and certificate first. This secures the communications between the server and device. Because the MDM payload is required to respond to check-in messages, this confirms the device is fully under management. On the initial check-in, the device is loaded with the remaining profiles, including the one containing the PIN lock restriction. Before this completes, the user may have clicked the continue button on the MDM redirect page, resulting in a CoA. This will re-authorize the device before the user has been prompted to enter a PIN lock and the user will end up being quarantined.

The workaround for both conditions is to open the Worx Home client and update the device's posture information with the server. In addition to the scenarios described above, this should be done any time the device has been quarantined by ISE. Once the client believes the device is compliant, the user should choose the "Refresh" button as shown in [Figure 21](#) to update the server. The user can then try the continue button again or bounce their wireless to force a re-authorization.

Figure 21 **Manually Updating the MDM Server**



Jailbroken or Rooted devices

These are devices where the user has gained direct access to the operating system, bypassing the control imposed on the device by the service provider. Devices in this state are generally considered compromised. There has been some recent legislative action to prohibit users defeating locks imposed on the device by the providers. The BYOD CVD offers a policy that does not allow jailbroken or rooted devices on the network. This is based on the MDM API. The MDM server will require a mobile client app installed on the device to determine the root status of the device. There are a few limitations to be aware of. Usually the process of rooting a device requires the user to reinstall the operating system. There is a good chance the user will uninstall the XenMobile mobile client at the same time. Without the software, the server cannot with certainty say the device is rooted, only that it has been compromised and is no longer under management. If the user also removes the MDM profile, then all of the child profiles are also removed, effectively resulting in a selective wipe. As a reminder, the MDM profile may not be locked. At this point, the user may attempt to on-board the device in a rooted or jailbroken state. The server will not be able to assess this condition until the mobile client is reinstalled on the device and has had a chance to complete a scan. There is a time delay between when a device is first compromised and when the MDM server will be first aware of a problem. There is no requirement in the MDM protocol that a device should contact the MDM when the MDM payload is removed. The server is left to poll for the condition periodically. This delay can carry forth into ISE policy because ISE can only respond to the attributes are they are returned by the MDM.

RegisterStatus

When a device is being on-boarded, ISE checks the RegisterStatus attribute of the device via an API call to the MDM. If the device is not registered, the user is redirected to the XenMobile enrollment page. Obtaining a status of registered with the MDM means that the device is known to the MDM and that an MDM payload and the associated certificate are on the device and that the device has responded to at least one check-in request issued through APNS. A register status does not guarantee that all the profiles have been pushed to the device. It is possible for profiles to be withheld by the MDM until a posture assessment has been completed and reported back to the server. This could result in a registered device that is not equipped with the full set of intended restrictions.

Manage Lost/Stolen Devices

Corporate and personal devices require specific responses when reported as lost or stolen. Personal devices reported as stolen should undergo an enterprise wipe to remove all corporate data. Employee-owned devices reported as lost may be located by the MDM if the Worx Home client has been allowed access to location information. A corporate wipe may also be issued to lost employee owned devices, however if the Worx Home application is removed during a corporate wipe, the MDM will no longer be able to locate the device. If the device remains lost after an attempt to locate it, then an enterprise wipe is prudent. The device can be re-enrolled later if found by the user. The admin may also choose to blacklist the device on the network depending on the situation, forcing the user to call support to regain access.

Unlike employee-owned devices, corporate devices have some flexibility with respect to providing location information. If this information is available, then the administrator may have some options. They could choose to:

- Reassign the device to a secured organization group. This group effectively removes all corporate applications and data, provisions lock-down profiles, effectively rendering the device useless, and leaves the device under management such that forensic data is available in the event the enterprise would pursue legal options.
- Blacklist the device in ISE to prevent corporate access. Also issue an Enterprise Wipe command to the device to remove all corporate data. This also removes the MDM profile. The device will become unmanaged, lifting all operational restrictions on the device including the ability to locate the device.
- Blacklist the device in ISE to prevent corporate access. Also issue a Full Wipe to the device to remove all information and return it to the factory default configuration. The carrier will need to be involved to prevent the now factory fresh device from having a resale value.

The exact response an enterprise would take in the event of a stolen device should not be public knowledge, especially where a Full Wipe is issued since the response could be an incentive to some criminals.

Application Distribution




Applications can be marked as required or optional. Required applications are usually automatically pushed to the device. Users can browse optional applications using the XenMobile Self-Serve App Store via a Web Clip or bookmark provisioned on their device. Applications can be from the public application store or developed in-house. Apple and Google both offer a volume purchasing program if paid

applications are distributed. Application management will be explored in future releases of this document. Readers are encouraged to view XenMobile's Device Manager configuration guide for additional information.

Cisco Applications (Jabber, etc.)

Cisco offers a wide range of mobile business applications for both increased productive and security. [Table 6](#) shows some popular applications.

Table 6 **Popular Cisco Mobile Applications**

	AnyConnect—AnyConnect is a security application for improved VPN access, including on-demand domain-based split tunneling.
	WebEx—WebEx is a productive application to allow mobile users to connect to online meetings. The application allows content sharing, video sharing, and VoIP or cellular audio.
	Jabber—Jabber is a productivity application that integrates IP telephony, chat, and video conferencing using Cisco Call managers.

XenMobile allows users to pre-provision the AnyConnect application using an application profile. Users can be prompted to enter their username and password or the profile can include a certificate payload that can be used to authenticate the users. The provisioning is found as part of a VPN profile, as shown in [Figure 22](#).

Figure 22 **AnyConnect Provisioning Profile**

VPN configuration creation

General **VPN** Proxy

Connection name displayed on the device: Cisco VPN

Connection type: Cisco AnyConnect

Hostname or IP address for server: ignore.sdulab.com

User account:

Group: SDU_TEaM

Authentication type for the connection: Credential

Identity credential: AnyConnect Cert

☒ Enable VPN on demand

+ New domain... Edit... Delete

Domain or host name	On demand action
sdulab.com	Always establish

294054

Conclusion

The integration of the network policy enforced by Cisco ISE and device policy offered by Citrix's XenMobile Device Manager provides a new paradigm for BYOD deployments where security and productivity are not competing objectives.

Disclaimer

The XenMobile configurations shown in this document should not be considered validated design guidance with respect to how the XenMobile MDM should be configured and deployed. They are provided as a working example that details how the case studies explored in the CVD can be carried forward to the MDM in an effort to provide a fully integrated and complementary policy across both platforms. This in turn will result in a comprehensive solution where the network and mobile devices are in pursuit of a common business objective. XenMobile is the only source for recommendations and best practices as it applies to their products and offerings.