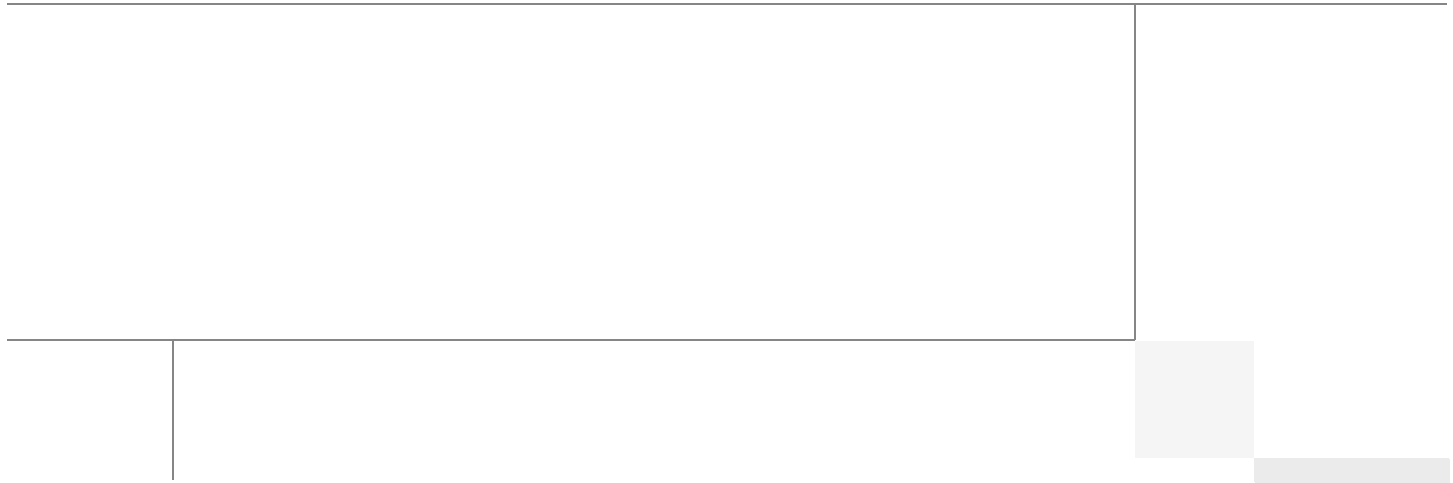




Integrating Cisco Mobile Collaboration Management Service with Cisco Identity Services Engine

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.

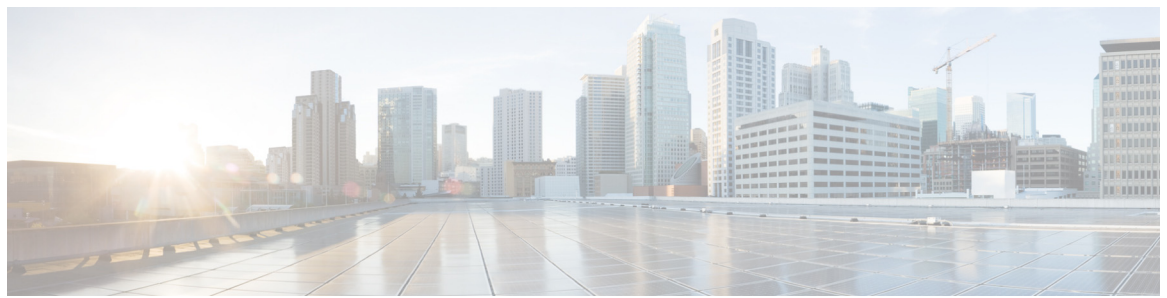
The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

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 Cisco Mobile Collaboration Management Service with Cisco Identity Services Engine

© 2013 Cisco Systems, Inc. All rights reserved.



Integrating Cisco Mobile Collaboration Management Service 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 Cisco Mobile Collaboration Management Service (MCMS) 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 AirWatch Administrator's guide.

This document is targeted at existing or new Cisco MCMS 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

Cisco Mobile Collaboration Management Service (MCMS) secures and manages personal BYOD and company-provided smartphones and tablets. This cloud-based service provides IT administrators the ability to quickly on-board and proactively secure iOS, Android, BlackBerry, and Kindle devices. Cisco MCMS also provides pre-built integrations with critical enterprise security, identity, email, and mobility infrastructure for a seamless enterprise mobility and collaboration experience on both campus WLAN and carrier networks.

MCMS Capabilities and Features

Cisco MCMS provides the life-cycle management capabilities and features highlighted in [Table 1](#).



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

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

Table 1 **Cisco MCMS—Key Capabilities**

Capability	Features
Architecture and Administration	<ul style="list-style-type: none"> • SaaS delivery model • Multi-tenant, scalable, and redundant cloud architecture • Independent SOC2 Type II cloud compliance audit conducted annually • Safe Harbor Certification for European Union Directive on Data Protection • Authority to operate (OTA) in accordance with U.S. Federal Information Security Management Act (FISMA) • Role-based admin access to Cisco MCMS Admin Portal • Custom branding capabilities • API support • Multiple mobile OS support including iOS, Android, BlackBerry, Windows, and Kindle
Device Enrollment	<ul style="list-style-type: none"> • Select device management services and configure device enrollment settings on Cisco MCMS Admin Portal • Send enrollment requests over the air using SMS, email, or a custom URL • Authenticate users against Active Directory/LDAP, one-time passcode, or SAML • Create and distribute customized acceptable use policies and End User License Agreements (EULA) • Enroll both corporate and employee owned (BYOD) devices • Initiate either individual or bulk device enrollments • Apply or modify default device policy settings
Proactive Device Security	<ul style="list-style-type: none"> • Require passcode policies with configurable quality, length, and duration • Enforce encryption and password visibility settings • Set device restrictions on features, camera, applications, iCloud, and content ratings • Detect and restrict jail broken and rooted devices • Remotely locate, lock, and wipe lost or stolen devices • Selectively wipe corporate data, leaving personal data intact • Define and implement real-time compliance rules with automated actions • Enable geo-fencing rules to enforce location related compliance
Central Policy Management	<ul style="list-style-type: none"> • Configure email, calendar, contacts, Wi-Fi, and VPN profiles over-the-air (OTA) • Approve or quarantine new mobile devices on the network • Create custom groups for granular or role-based policy management • Define role-based administrative portal access rights to Cisco MCMS Admin Portal • Decommission devices by removing corporate data and mobile device management control

Table 1 *Cisco MCMS—Key Capabilities*

Enterprise Application Catalog	<ul style="list-style-type: none"> • Manage and distribute third-party and in-house mobile apps from the Cisco MCMS Admin Portal • Develop a catalog of recommended mobile apps on iOS and Android devices • Users can view apps, install, and be alerted to updated apps on private app catalog • Manage lifecycle of app workflow: <ul style="list-style-type: none"> – Real-time software inventory reports – App distribution and installation tracking – App update publishing – Provisioning profile management • Administer mobile app security and compliance policies: <ul style="list-style-type: none"> – Blacklist and whitelist mobile apps downloaded from Apple App Store and Google Play – Enforce out-of compliance rules by sending user alerts, blocking email or VPN, and remote wiping – Limit native apps available on the device such as YouTube – Require user authentication and authorization before they download in-house apps – Detailed reporting across app compliance events and remediation actions • Host and distribute in-house mobile apps on Cisco MCMS Cloud • Support for volume purchase programs on Apple App Store: <ul style="list-style-type: none"> – Automatically upload redemption codes in Cisco MCMS Cloud – Track provisioning, manage licenses, monitor compliance, and eliminate manual VPP management
Secure Content Distribution	<ul style="list-style-type: none"> • Securely access, view, and share documents in the Doc Catalog on iPads, iPhones, and Android Devices • Add additional security with native device encryption, passcode, and remote wipe of lost or stolen devices • Support for multiple document formats including: <ul style="list-style-type: none"> – Microsoft – Google – Apple Productivity Suites – PDF, web, audio, and video files • Host documents on a corporate network or on Cisco MCMS Cloud • Block documents from being opened in file sharing or word processing applications for data loss prevention • Set policies on certain documents to restrict them from being emailed from corporate or personal accounts • Alert users on new or updated content in their Doc Catalog without the need to manually check for updates • Generate reports on documents, users, and devices to monitor status and usage for compliance

Table 1 **Cisco MCMS—Key Capabilities**

Monitoring and Reporting	<ul style="list-style-type: none">• Detailed hardware and software inventory reports• Configuration and vulnerability details• Integrated smart search capabilities across any attribute• Customizable watch lists to track and receive alerts• BYOD privacy settings block collection of personally identifiable information• Mobile expense management for real-time data usage monitoring and alerting
Enterprise Integrations	<ul style="list-style-type: none">• Instant discovery of devices accessing enterprise systems with Cisco MCMS Connector• Integrate with Microsoft Exchange, Lotus Notes, and Microsoft Office 365 including:<ul style="list-style-type: none">– Microsoft Exchange 2007 and 2010– BPOS and Office 365– Lotus Traveler 8.5.2• Integrate with existing Active Directory/LDAP and Certificate Authorities• Manage BlackBerry Enterprise Server policies on BlackBerry Enterprise Server 5.0 and higher• Connect with other operational systems through web APIs

Cisco MCMS solution has three main components:

- Portals (Administration and End User)
- MCMS Server in the Cloud that manages policies and compliance rules
- MCMS Agent software that runs on mobile devices

Beyond these, there is an additional component for enterprise integration called MCMS Cloud Extender that integrates with AD, LDAP, email servers, and PKI infrastructure. The majority of the base functionality is available through the MDM API built into the mobile device operating system. MCMS requires the client software to detect some conditions, such as jail-broken or rooted devices. Because ISE tests for these conditions, the MCMS server is configured to treat the client software as a required application and will install the software during the on-boarding process.

Deployment Models

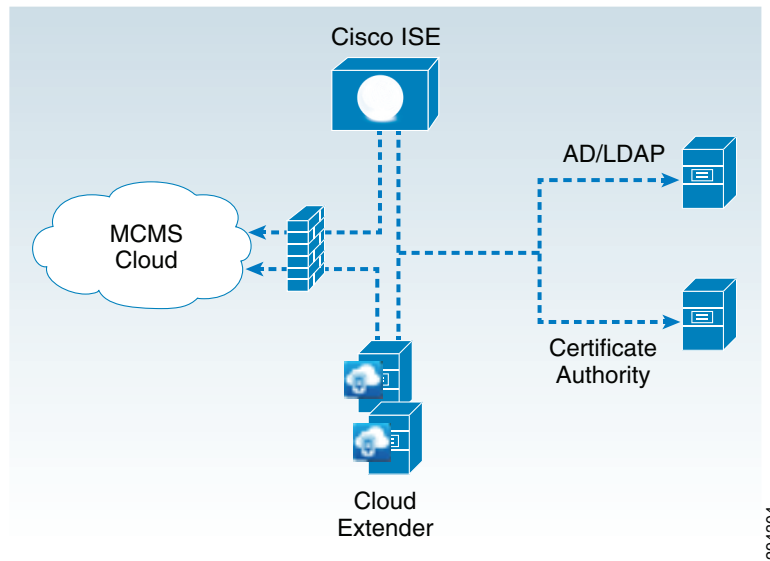
Cisco MCMS offers only a cloud-based service model. To integrate with enterprise backend systems, customers need to install a piece of software called MCMS Cloud Extender on either a physical or virtual machine within their network. MCMS Cloud Extender is a lightweight software package that establishes an outbound connection with Cisco MCMS cloud. There is no requirement to open any inbound firewall ports.

Getting MCMS Ready for ISE

The first requirement is to establish basic connectivity between the Cisco ISE server and the MCMS MDM server. MCMS supports only a cloud model. A firewall is typically located between the ISE and the MCMS cloud. The firewall should be configured to allow an HTTPS session from

the ISE located in the data center to the MCMS server located in the 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.

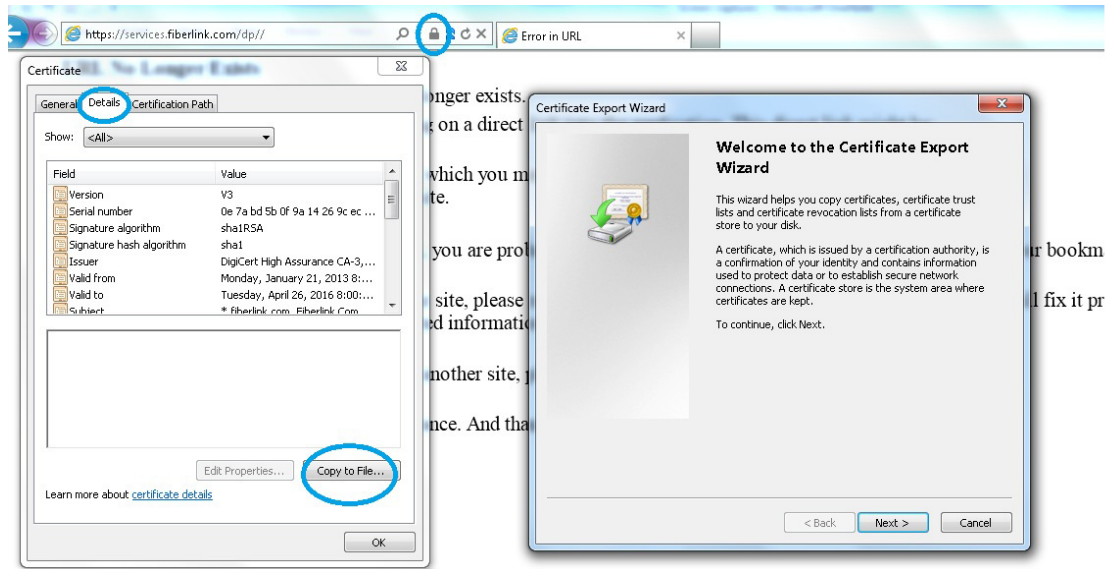
Figure 1 Firewall Traffic Flow



Import MDM Certificate to ISE

The MCMS MDM server incorporates an HTTPS portal to support the various users of the system. In the case of a 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 a local cert store in ISE. Most browsers allow this. Internet explorer is shown in [Figure 2](#) with a cloud-based MDM deployment.

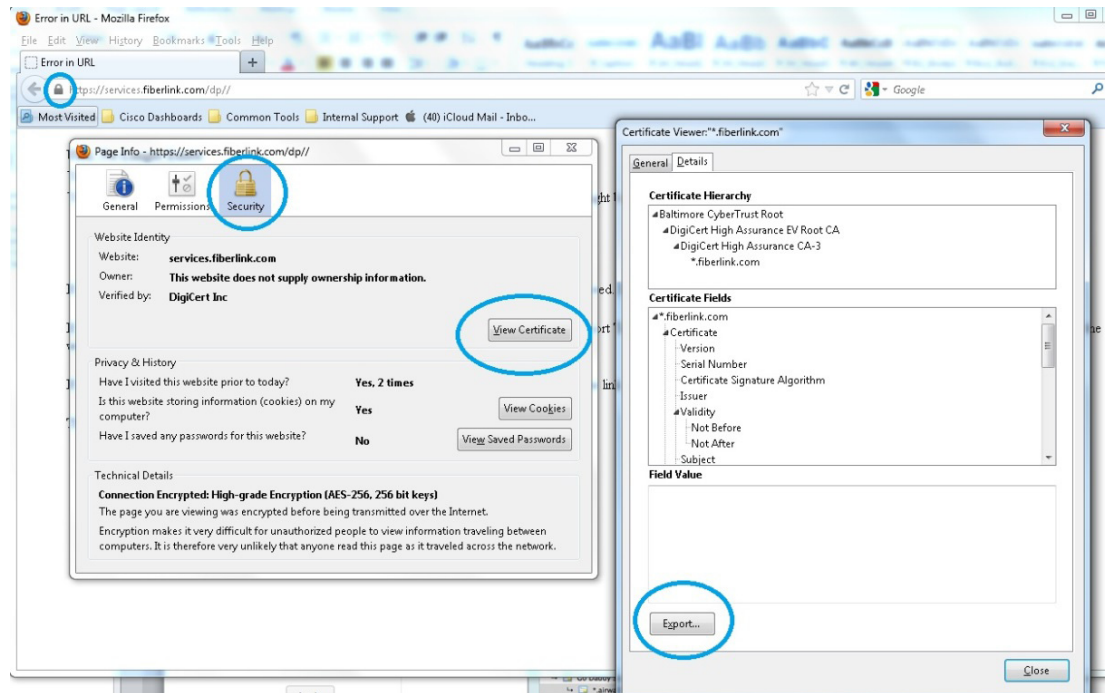
Figure 2 Exporting the MDM Site Certificate with Internet Explorer



MCMS utilizes a wildcard certificate that is valid for all portal websites belonging to the MCMS domain.

Exporting a certificate from Firefox is covered in the CVD and repeated in [Figure 3](#).

Figure 3 Exporting the MDM Site Certificate with Firefox

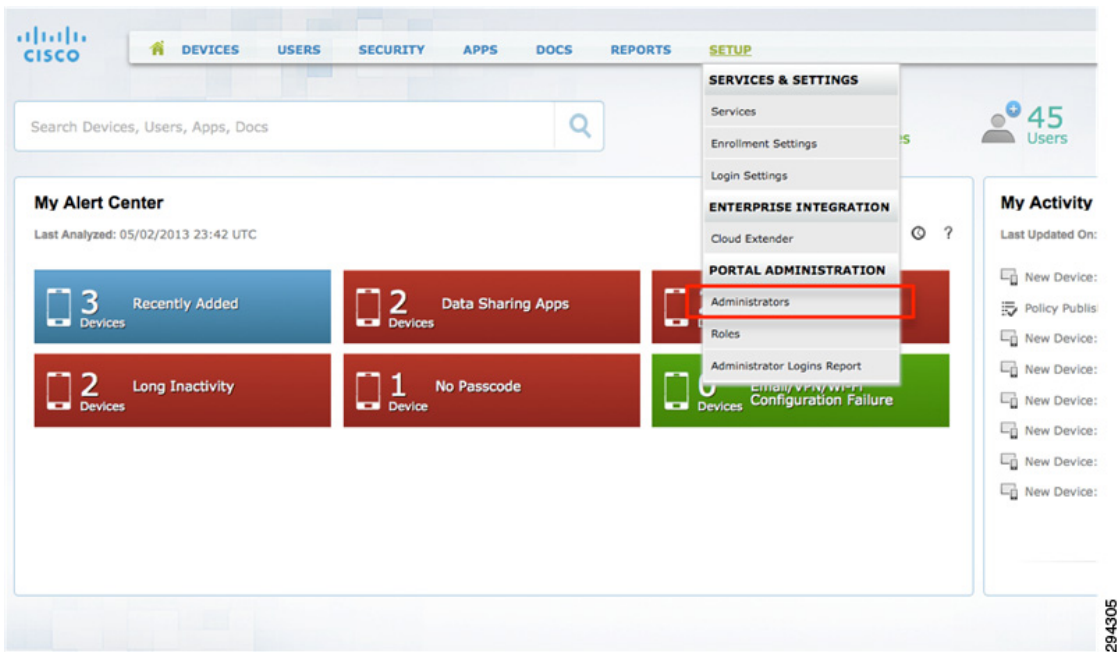


Grant ISE Access to the MCMS API

The MCMS API is protected by HTTPS and requires an administrator account that has been granted permission to the API. Ideally a specific account would be configured for ISE with a very strong password. In addition to this account, only a limited number of administrator accounts should be granted the ability to create new administrators or assign administrator roles.

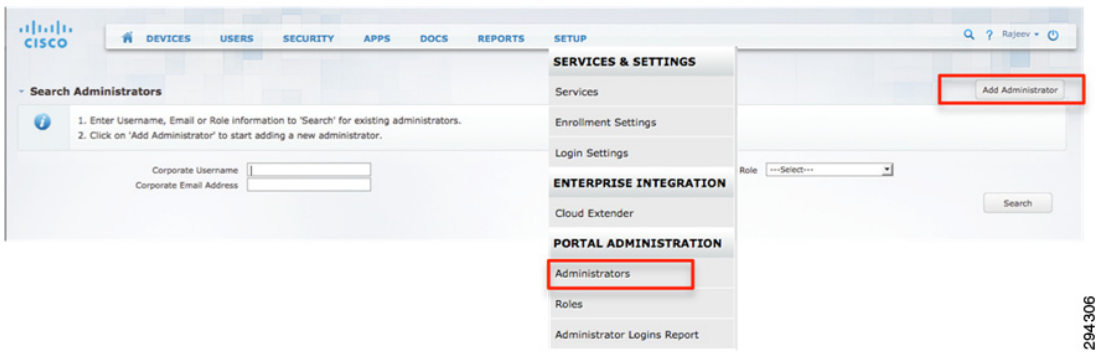
Before the user is created, an API role should be created for ISE. This role will then be tied to an administrator account assigned to ISE. Administrators can manage the system settings assigned to their role, which can be selected on a per-role basis. A local administrator account is required for the REST MDM API roles to function properly.

Figure 4 Manage Administrator Account



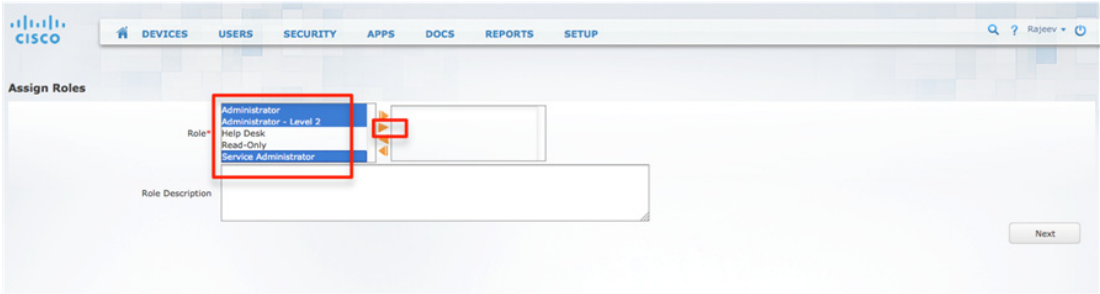
Each account type can be assigned roles entitling that user to specific features of the system. ISE uses the administrator account to make queries to MCMS.

Figure 5 Add Account



The MDM role created for ISE requires the REST API features. The list in [Figure 6](#) identifies the rights which should be selected.

Figure 6 Assign Role To the Account

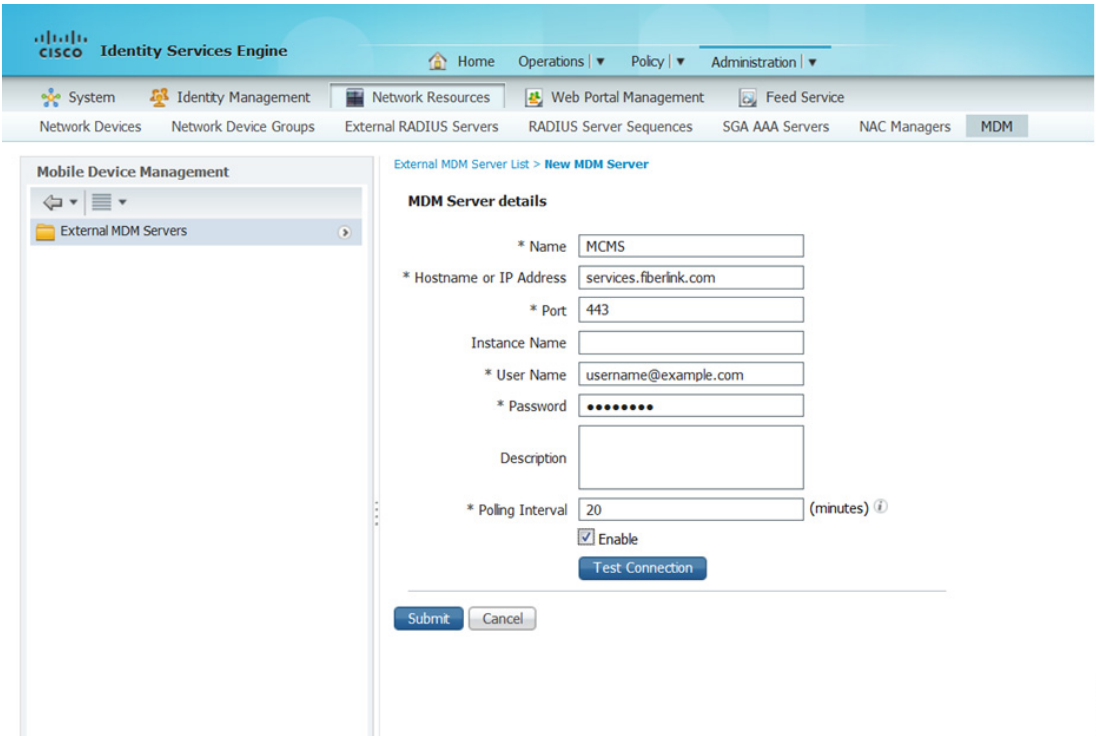


Once the role as been added, an admin account can be created for ISE.

Add MDM Server to ISE

Once the account has been defined on the MCMS MDM server with the proper roles, ISE can 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. As shown in [Figure 7](#), the URL for the MCMS server and the configuration is illustrated. This is configured under administration > Network resources > MDM.

Figure 7 Configure the MDM API on ISE



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.

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. The MDM compliance posture could include a wide range of conditions not specific to network access. For example, the device administrator may want to know when an employee on a corporate device has exceeded 80% of the data plan to avoid any overage charges. In this case, blocking network access based solely on this attribute would aggravate the MDM compliance condition and run counter the device administrator's intentions. In addition, the CoA will interrupt the user WiFi session, possibly terminating real-time applications such as VoIP calls.

The polling interval is a global setting 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 configuration is complete. 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 four hours, then ISE should be set to the same value and not less than one-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 MCMS 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 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 will not be active.

Verify Connectivity to MDM

Some problems can occur when testing the connection to the MDM server. [Table 2](#) shows some common messages generated when testing the connection between ISE and Cisco MCMS. The last message shown below confirms a successful connection.

Table 2 *Connection Messages*







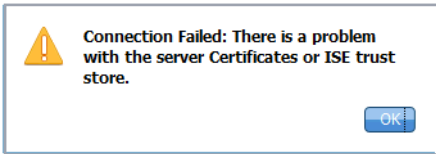
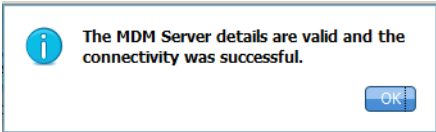
Message	Explanation
 Connection Failed: Please check the connection parameters. 	A routing or firewall problem exists between the ISE located in the data center and the MDM located in either the DMZ or Cloud. The firewall's configuration should be checked to confirm HTTPS is allowed in this direction.
 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.

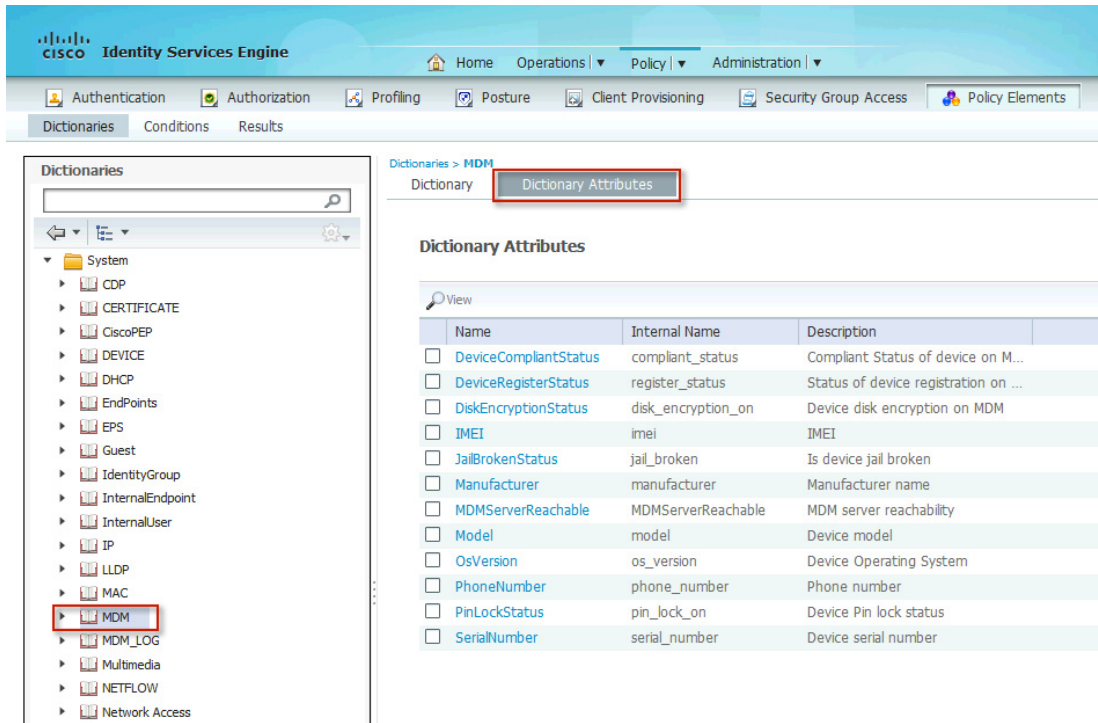
Table 2 **Connection Messages**

Message	Explanation
 <p>A dialog box with a yellow warning triangle icon. The text reads "Connection Failed 403 : Forbidden". There is an "OK" button in the bottom right corner.</p>	<p>The user account setup on the Cisco MCMS server does not have the proper roles associated to it. Validate that the account being used by ISE is assigned the REST API MDM roles as shown above.</p>
 <p>A dialog box with a yellow warning triangle icon. The text reads "Connection Failed 401 : Unauthorized". There is an "OK" button in the bottom right corner.</p>	<p>The user name or password is not correct for the account being used by ISE. Another less likely scenario is that the URL entered is a valid MDM site, but not the same site used to configure the MDM account above. Either of these could result in the Cisco MCMS server returning an HTML code 401 to ISE.</p>
 <p>A dialog box with a yellow warning triangle icon. The text reads "Connection Failed: There is a problem with the server Certificates or ISE trust store." There is an "OK" button in the bottom right corner.</p>	<p>ISE does not trust the certificate presented by the Cisco MCMS 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.</p>
 <p>A dialog box with a blue information icon. The text reads "The MDM Server details are valid and the connectivity was successful." There is an "OK" button in the bottom right corner.</p>	<p>The connection has successfully been tested. The administrator should also verify the MDM AUTHZ dictionary has been populated with attributes.</p>

Review MDM Dictionaries

When the MCMS MDM becomes active, ISE will retrieve a list of the supported dictionary attributes from the MDM. Currently MCMS supports all of the attributes that ISE can query. The dictionary attributes are shown in [Figure 8](#).

Figure 8 Dictionary Attributes



293798

Enterprise Integration

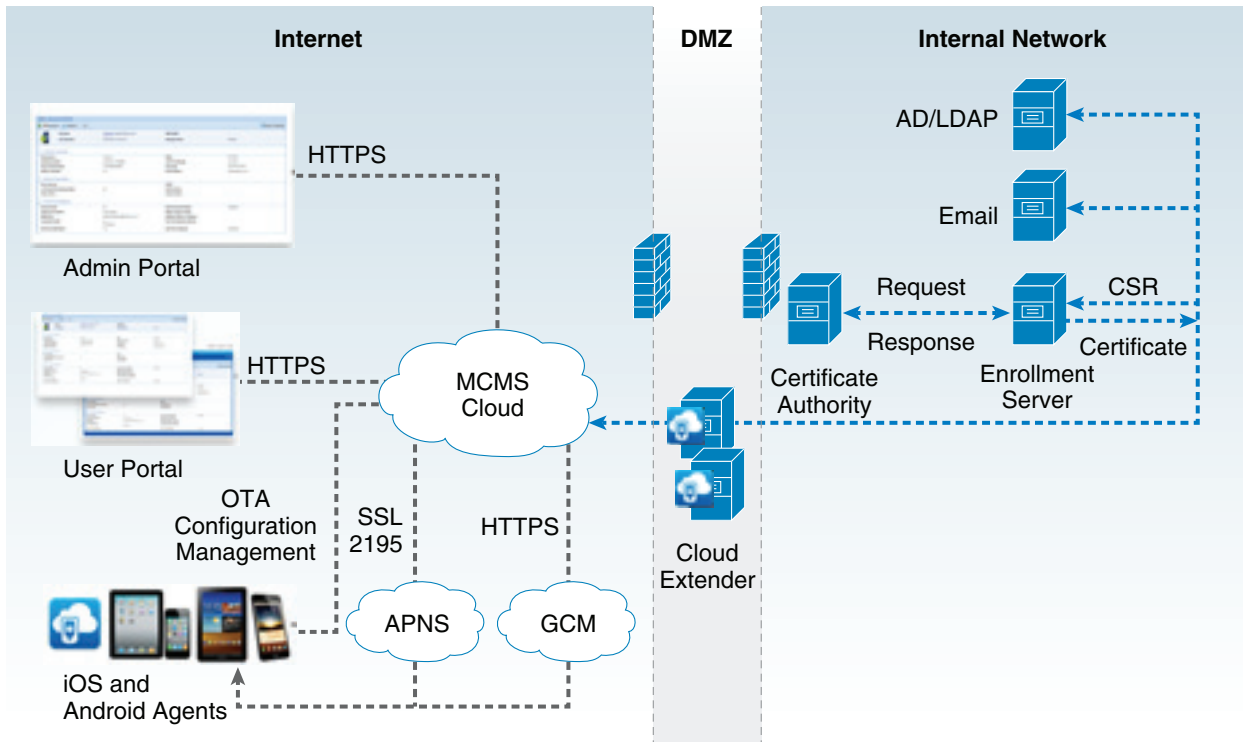
Cisco MCMS offers a solution that enables integration with existing enterprise infrastructure like AD, Exchange, and Certificate Authority. This is achieved using a component called MCMS Cloud Extender. The MCMS Cloud Extender is a small program that runs as a service on a Microsoft Windows machine in the enterprise data center. The Cloud Extender creates an outbound connection over HTTPS to the MCMS portal that is used as a bi-directional communication facility and allows the MCMS portal to integrate with an enterprise Active Directory server to perform user authentication and synchronization of users and groups using Active Directory. The MCMS Cloud Extender requires that it be configured with an account with sufficient rights to run as a service and to have read-only access to the Active Directory domain.

MCMS Cloud Extender can be installed on a Physical or Virtual Machine with following specifications:

- Windows Server 2008 R2 (64-bit)
- Dual Core, 4 GB RAM
- Access to MCMS Cloud (outbound connection, port 443)
- Read-only Administrative access to AD to read user and group information

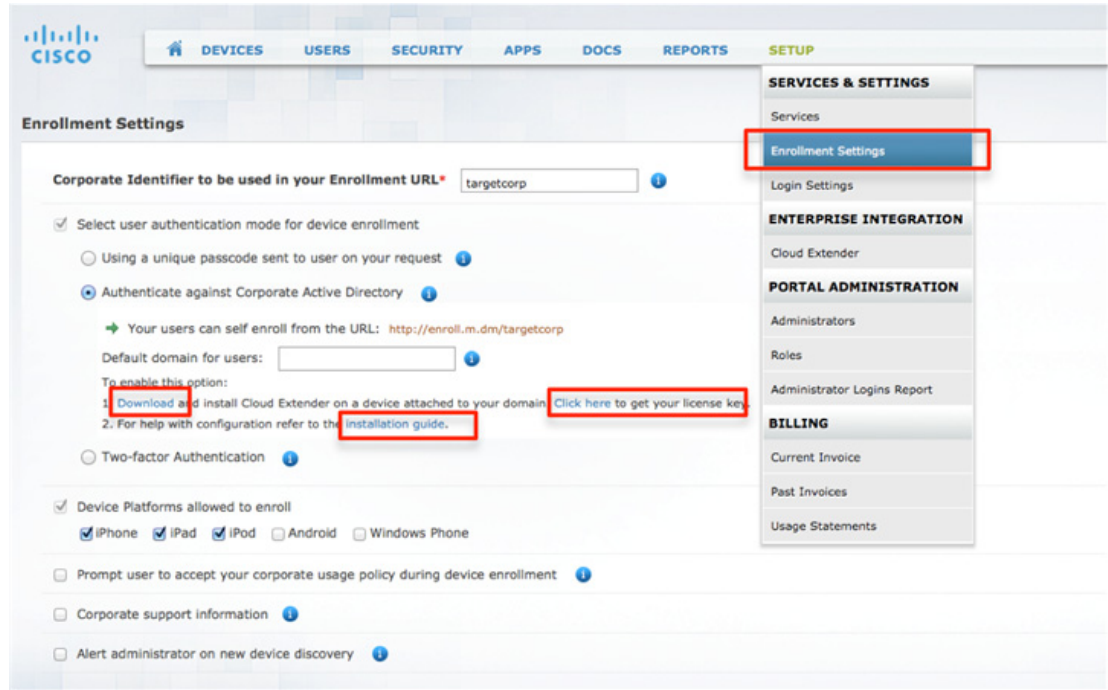
Redundancy configurations are available but are out of scope for this document. More details can be obtained at: <https://www.cisco.com/go/mcmssupport>.

Figure 9 Typical Cloud Deployment Model



The installation is straightforward and fully documented by Cisco MCMS. All the information required to install the MCMS Cloud Extender is available by logging onto MCMS and going to **SETUP > Enrollment Settings** ([Figure 10](#)).

Figure 10 *MCMS Cloud Extender Download*



When Cloud Extender is installed, an Installation Wizard prompts the administrator to configure AD for user authentication and User Visibility. User Visibility allows MCMS to import groups that are provisioned in AD. [Figure 11](#) and [Figure 12](#) show the Installation Wizard screens used to configure AD integration on MCMS.

Figure 11 *Cloud Extender Installation Wizard*

The screenshot shows the 'Cloud Extender Configuration Tool' window. The title bar says 'Cloud Extender Configuration Tool'. Below the title bar is a green header with the text 'Cloud Extender Configuration Tool' and a dropdown menu set to 'Basic'. The main content area is titled 'Select the Services to be configured:' and includes a 'Help' link. The following services are listed with checkboxes:

- ☐ Exchange ActiveSync Manager
- ☐ Lotus Traveler Manager
- ☐ BlackBerry Enterprise Server Integration
- ☒ User Authentication
- ☒ User Visibility
- ☐ Certificates Integration

For both 'User Authentication' and 'User Visibility', the following sub-options are shown in a separate box:

- ☐ Active Directory
PowerShell version 2.0 or greater must be installed on this server to continue.
- ☒ LDAP
Supported LDAPs: Active Directory, OpenLDAP, Novell eDirectory, Oracle Directory Server, IBM Domino LDAP

At the bottom of the window, there is a status bar with a green checkmark and the text 'The Cloud Extender is running'. To the right of the status bar are three buttons: '< Back', 'Next >', and 'Cancel'.

294256

Figure 12 Cloud Extender AD Configuration

The screenshot displays the 'Cloud Extender Configuration Tool' window. On the left, a 'Configure' sidebar lists 'LDAP integration' (selected), 'Cloud Extender Status', and 'Cloud Extender Auto Updates'. The main area is titled 'Configure LDAP integration:' and includes a 'Help' link. It contains several input fields: 'LDAP Server' (set to 'Active Directory'), 'Server Name' (10.5.1.10), 'Port' (389), 'Authentication Type' (Basic), 'Bind Username (Distinguished Name)' (CN=mcms,OU=UW Training Bootcamp,DC=uwtraini), 'Bind Password' (masked with asterisks), 'LDAP Search base' (OU=UW Training BootCamp,DC=uwtraining,DC=), and 'User Search Attribute' (samAccountname). A note states: 'Note: Across all specified LDAP Search bases(s), the User IDs should be unique.' At the bottom, there are 'Cancel' and 'Edit' buttons. A status bar at the very bottom shows a green checkmark and the text 'The Cloud Extender is running', along with '< Back', 'Next >', and 'Cancel' buttons. A vertical text '294257' is visible on the right edge of the window.

Active Directory/LDAP Integration





Integrating ISE and the MDM to a common directory is important for 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 base 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 13 shows the use cases presented in the CVD.

Figure 13 CVD Use Cases

Policy	AD Group	ISE	Compliant MDM	Permission	
Personal_Full Access	BYOD_Full_Access	YES	YES	Full	
Personal_Partial Access	BYOD_Partial_Access	YES	YES	Partial	
Personal_Internet Only	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 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, everyone 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 manufacture or model specific. For example, Samsung uses their SAFE API, while HTC uses its One APIs.

Profiles can be applied to devices associated to users that belong to a user group. Administrators configuring this with Cisco MCMS will take following steps:

1. Configure MCMS Cloud Extender to import groups from Corporate Directory.
2. Create profiles as desired for different AD Group Types.
3. Bind Profiles to AD groups.

Figure 14 shows the creation of a profile.

On MCMS Administration Portal, Go to Security > Policy > Add Policy to create policies.

Figure 14 Create Policies

294311

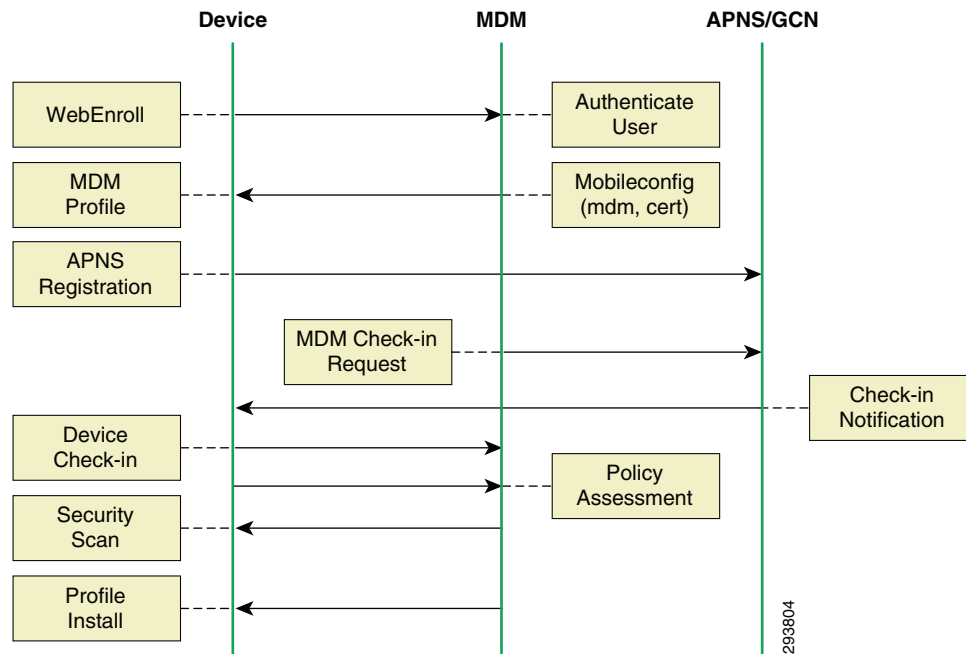
To bind policies to user groups, Go to Users > Groups and assign the appropriate policy.

Figure 15 Binding Policies to User Groups

294312

With the example configuration shown above, users that belong to BYOD_Employee_Access will get Full_Access_policy pushed to their devices. User will see two profiles installed by ISE and two or three from the MDM. The server will install the MDM payload during the on-boarding process. After that profile has been installed, the device will be issued a check-in request via APNS or GCM. When the device responds to the push notice, it will connect to the MDM where any additional profiles are installed.

Figure 16 Enrollment Network Flows



SCEP

Cisco MCMS can provision certificates onto the device via SCEP. 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](#).

MCMS Mobile Agent

The majority of MDM features are implemented directly through the operating system (iOS only) and do not require a mobile device client application. MCMS agent is always required on Android devices. The following features require that MCMS agent be installed on the device:

- Jailbreak Detection
- Location Based Services
- Application Inventory (for blacklist, mandatory apps)
- Doc Distribution
- Data Usage Tracking
- WiFi SSID Connection Tracking
- Admin to user messaging via the portal (or ISE)

Because ISE depends on these features for policy enforcement, corporate devices and personal devices with partial or full access should include a profile that specifies the MCMS Agent as a mandatory application.

During enrollment, users are automatically taken to the App Store or Google Play to install MCMS. The MCMS Agent can also be installed by the user directly from the App Store or Google Play store. In addition to supervising the device, the client application offers the end users some useful information concerning the status of their devices. Users can determine when the device last communicated with MCMS server, receive messages or alerts from administrator, track data usage, and issue an audio alert used to locate a lost device. Another 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 OS will not trigger an update to the MDM client. The client will detect the change during the next security scan interval. Only then will the server 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.

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, MCMS recommends that support staff should not be allowed 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 job. Having the ability to handle the information gathered from personal and corporate devices differently is important.

In this first release, there is not a tight integration between assets 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. Within ISE, this is the device's MAC address that is unique across the network. MCMS uses the device's UDID, which is unique over all devices.

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. MCMS allows devices to be grouped as corporate owned or personally owned only after the device enrollment. This can be done either via Web Services API or through Bulk Update feature of MCMS. Using Bulk Update, the administrator can change device ownership for the devices.

An enterprise may need to create a list of corporate MAC addresses and the associated UDIDs to provision them as corporate devices on both systems.

User Experience

For the most part, the fact that a device is under management is seamless to the user. 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 will allow Internet access, but will capture 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 the Apple App Store. When the device is captured, the user will be presented with a screen that includes two buttons. The first will redirect the client to the MDM registration page and the second issues a CoA to force a re-evaluation of the AuthZ policy after MDM enrollment completes.

Android users must load the MCMS client application on their device prior to enrolling the device with the MDM server. This can be done from either the provisioning network or the employee network, however it is not automatic. The enterprise will need to educate Android users of this requirement.

When the user lands on the Cisco MCMS registration page, they will be guided through self-explanatory steps to enroll their device. See [Figure 17](#).

Once the credentials are validated, a profile including the MDM payload and associated certificate is installed on the device and the user is notified that the on-boarding process is complete. At the end of the enrollment, the user will receive a notification from MCMS to install the MCMS Agent.

Figure 17 **MDM Enrollment**

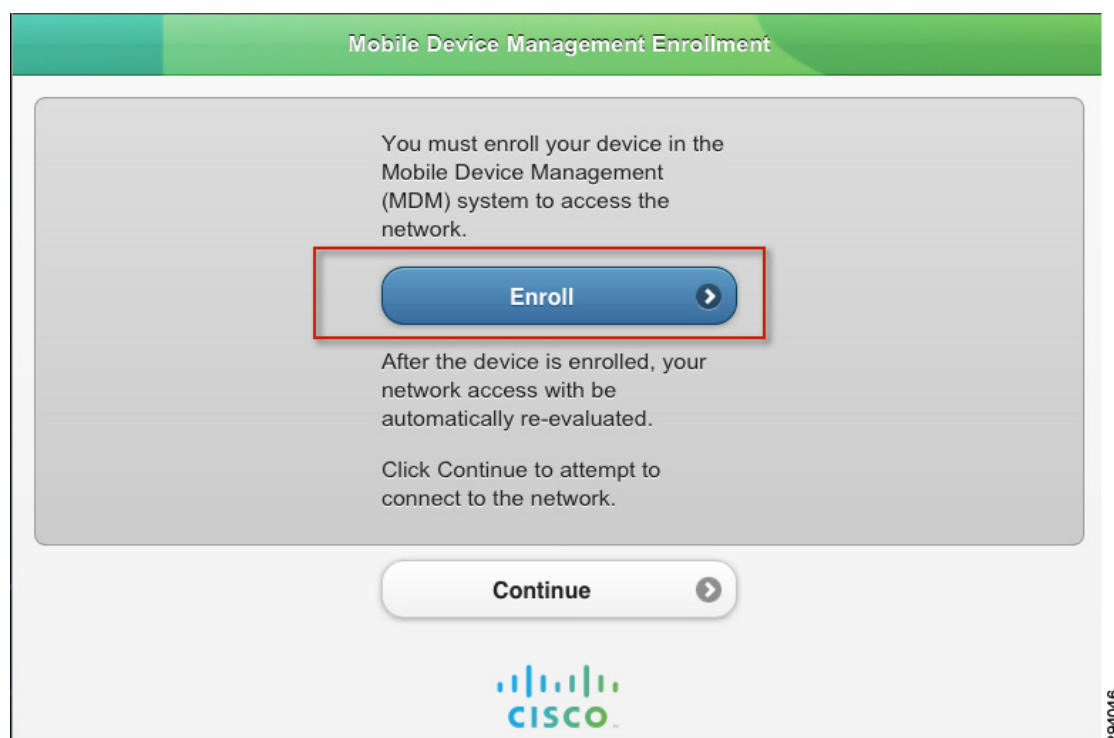


Figure 18 *MDM On-boarding—1*

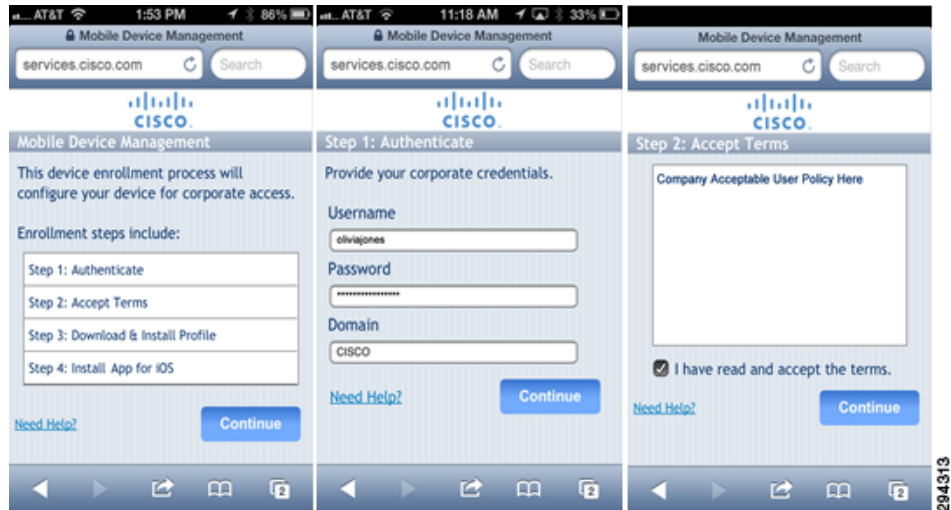
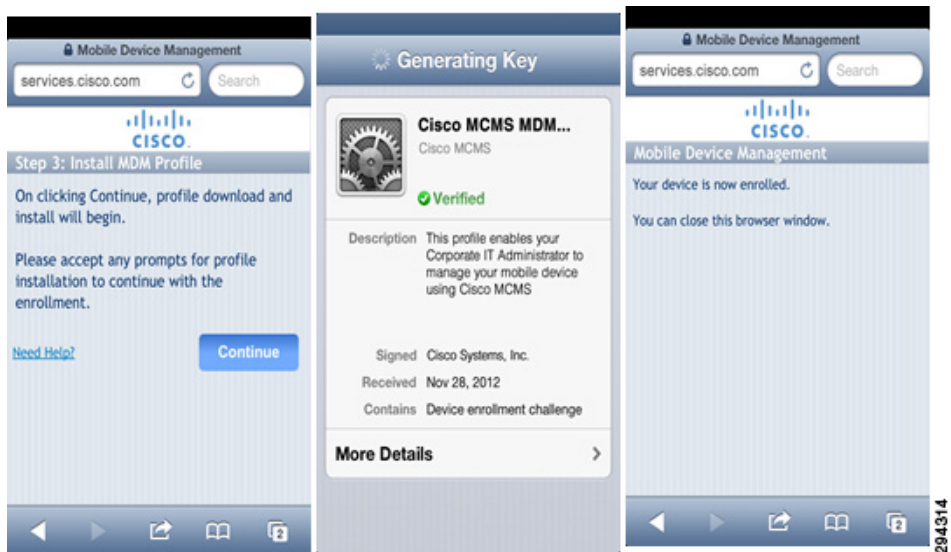


Figure 19 *MDM On-boarding—2*



After the device has enrolled, the server will request a check-in. During the 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 configuring 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 chose the minimum password length and complexity. The natural tendency is to require very strong passwords, however there may be unintended consequences. 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. 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.

Enterprise Application Store

Cisco MCMS server allows corporations to create their own App Catalog. MCMS allows the following:

- Develop a catalog of recommended mobile apps on iOS and Android devices based on roles/groups.
- Manage and distribute third-party and in-house mobile apps.
- Allow users to view, install, and be alerted to updated apps on a private catalog.
- Manage mobile app lifecycle workflow to all devices, device groups, and individual devices.
- Administer mobile app security and compliance policies.
- Host and distribute in-house developed mobile applications.
- Support for Apple App Store Volume Purchase Programs (VPPs).

Cisco MCMS supports both push and pull model for application distribution. Users can “pull” them from Enterprise Application Store on their devices or administrator can choose to “push” applications to the user's device. In case of “push”, the user is prompted to accept installation of the application.

Corporate Data

MCMS and ISE can 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 on the mobile device and data in-flight is the movement of data. This can be extended to include moving data between two storage containers on the same device.

Cisco MCMS also offers secure content distribution functionality that allows administrators to distribute documents, audio files, video files, pictures, etc. securely to mobile devices. The content is available in the MCMS agent, which provides a secure container for viewing documents. The administrator can set policies to restrict copy, paste, and emailing outside of container and password protect content.

Data at-Rest

Android and Apple handle stored data differently. Android has an open file structure that allows content to be shared between applications. Data is protected with file permissions, which creates a tight and integrated environment. Many Android devices also support external and removable storage in the form of SD Cards. iOS creates a storage environment for each application. When an application is deleted, the partition holding that application's data is also removed.

Data in-Flight

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. MCMS allows administrators to set policies to restrict data backup to cloud, enforce compliance check (Android), and enforce authentication (Android).

Certainly moving corporate data to and from the device is also a concern. The most common tool is email attachments, although cloud storage services such as Dropbox are also a concern. MCMS can blacklist these types of applications. This is most appropriate on corporate devices. ISE can deploy per-user ACL through the Wireless LAN Controller to enforce this policy at the network level for both corporate and personal devices.

Through MCMS Cloud Extender, administrators can securely integrate with all major email, calendaring, and contacts platforms including Exchange, Lotus Notes, Gmail, and Microsoft's upcoming Office 365. The Cloud Extender performs a number of functions to provide visibility and management of ActiveSync connected devices, including:

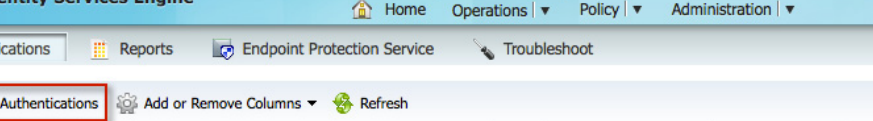
- Querying Exchange Server using Microsoft PowerShell commands and standard APIs for vital information related to the ActiveSync enabled devices on the Exchange Server. The use of PowerShell and related APIs allows for abstraction from the specifics of the Exchange Server implementation and allows the Cloud Extender to support multiple Mailbox Servers and clustered/resilient Exchange server configurations.
- Processes device and policy information and transmits it to the MCMS Portal for reporting and management functions.
- Receives ActiveSync Policies, Device Actions, and Policy Assignments actions and carries out the relevant actions on the Exchange server.

Corporate Wipe

Both ISE and MCMS can remove corporate data from personal devices. MCMS calls this Selective Wipe, while ISE refers to it as a Corporate Wipe. Other common terms used are selective wipe or partial wipe. When ISE issues this command, it is forwarded to MCMS via an API call. MCMS will then remove corporate applications using privileges granted to the MDM Profile. When these complete, the MDM profile is removed, which will remove all the associated sub-profiles. While it is also possible to leave some applications behind, all MDM profiles will be 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.

Selective wipes by themselves do not blacklist the device from either the MDM or ISE. An ISE administrator, the MDM administrator, or the user from either the ISE My Devices Portal or the MCMS may issue a selective wipe. If a selective 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 release 1.2 now supports this directly from the Operations page, as shown in [Figure 20](#). 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.



The screenshot displays the Cisco Identity Services Engine (ISE) interface. At the top, the navigation bar includes 'Home', 'Operations', 'Policy', and 'Administration'. Below this, the 'Show Live Authentications' button is highlighted with a red box. The main content area shows a table of active sessions. The table has columns for 'Initiated', 'Updated', 'Session Status', 'CoA Action', 'Endpoint ID', 'Identity', and 'IP Address'. The first session is initiated on 2013-02-24 at 20:17:08.328, updated at 20:17:14.127, and is in a 'Started' state. The second session is initiated on 2013-02-24 at 20:14:09.368, updated at 20:14:15.868, and is also in a 'Started' state. The third session is initiated on 2013-02-24 at 19:58:52.596, updated at 20:19:58:52.596, and is in an 'Authenticated' state. The fourth session is initiated on 2013-02-22 at 14:10:25.803, updated at 2013-02-22 at 14:10:30.227, and is in a 'Started' state. The fifth session is initiated on 2013-02-22 at 12:37:29.888, updated at 2013-02-22 at 12:37:34.848, and is in a 'Started' state. A red box highlights the 'Session reauthentication' option in the context menu that appears when clicking the 'CoA Action' dropdown for the first session.

	Initiated	Updated	Session Status	CoA Action	Endpoint ID	Identity	IP Address
▶	2013-02-24 20:17:08.328	2013-02-24 20:17:14.127	Started	⚙️	68:96:7B:01:2E:11	user2	10.31.1.122
▶	2013-02-24 20:14:09.368	2013-02-24 20:14:15.868	Started			user2	10.31.1.125
📄	2013-02-24 19:58:52.596	2013-02-24 19:58:52.596	Authenticated			johnjo	
▶	2013-02-22 14:10:25.803	2013-02-22 14:10:30.227	Started			D8:30:62:8E:AD:	10.31.1.130
▶	2013-02-22 12:37:29.888	2013-02-22 12:37:34.848	Started		18:E2:C2:82:43:AF	18:E2:C2:82:43:/	10.31.1.127

Cisco MCMS offers an End User portal that allows the user to manage their devices. Users can perform actions like Lock Device, Locate Device, Wipe Device, Reset Passcode, and Check-in device with MCMS service.

Cisco Mobile Collaboration Management Service

Hi rajekhur, Welcome to Cisco Mobile Collaboration Management Service User Self Service Portal

Last login time: 10/10/2012 11:12 PM

My Personal Information

User Name	rajekhur	Email Address	rajekhur@cisco.com
Domain	CISCO	Employee ID	

rajekhur-XT910

- Rajeev iPhone
- Target
- rajekhur-GT-P7310
- rajekhur-GT-I9300
- Rajeev iPhone
- Rajeev iPhone

Action Show Action History

Refresh Device Information

Lock Device rajekhur-XT910 Last Reported 04/26/2013 11:03 PM

Reset Device Passcode Android 4.0.4 (6.7.2-180_SLC-34) Custom Asset #

Wipe Device (MDM Action) motorola Model XT910

Locate Device

Current Carrier AT&T Ownership Not Specified

Security & Compliance

Hardware Encryption Partial Encryption Device Passcode Status Compliant

Wipe Supported Yes Managed Status Enrolled


Verify Device Compliance

ISE Compliance versus MDM Compliance

There are two compliance checks required of the device. The first is defined by policy configured on ISE and is specific to network access control (NAC). The other is defined on the MDM and specific to Mobile Device Policy (MDP). The use of an MDM to determine NAC is a fairly new concept, first supported in ISE 1.2. Mobile device compliance policy is an essential component of MDM and has context outside of network access, which is similar to NAC compliance prior to the integration of the MDM. Integrating the components together does not negate the need for two distinct compliance policies with meaning only within their respective context. The network administrator has to be careful not to confuse ISE compliance with MDM compliance with respect to NAC.

The attributes shown in [Table 4](#) should help clarify the difference between compliance policies.

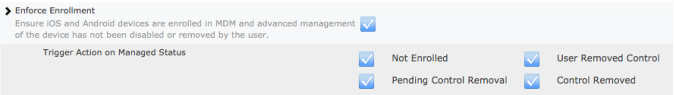
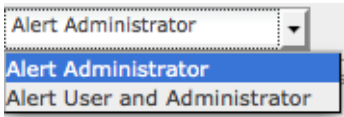
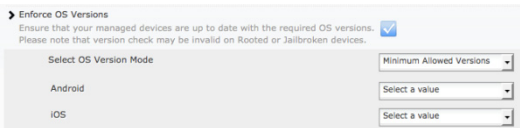
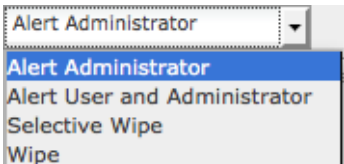
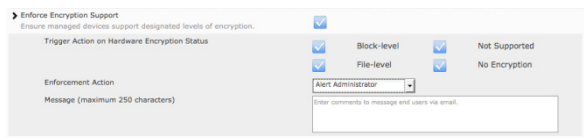
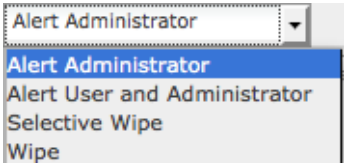
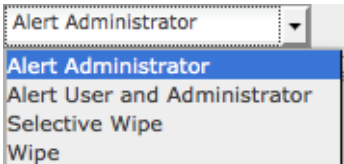
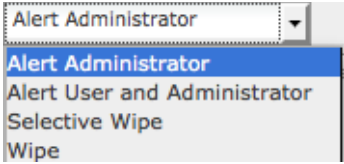
Table 4 *Compliance Attributes*

ISE Compliance Attributes	MCMS Compliance Attributes
<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>Select Enforcement Rules</div> <div><div>➤ Enforce Enrollment</div><div>Ensure iOS and Android devices are enrolled in MDM and advanced management of the device has not been disabled or removed by the user.</div><input type="checkbox"/></div> <div><div>➤ Enforce OS Versions</div><div>Ensure that your managed devices are up to date with the required OS versions. Please note that version check may be invalid on Rooted or Jailbroken devices.</div><input type="checkbox"/></div> <div><div>➤ Enforce Encryption Support</div><div>Ensure managed devices support designated levels of encryption.</div><input type="checkbox"/></div> <div><div>➤ Enforce Application Compliance</div><div>Ensure devices are in compliance with application management requirements (required, disallowed & white list policies). Application compliance is based on policy settings assigned to managed devices.</div><input type="checkbox"/></div> <div><div>➤ Restrict Jailbroken (iOS) and Rooted (Android) Devices</div><div>Ensure managed devices are not jailbroken or rooted. iOS Application is required for Jailbreak detection.</div><input type="checkbox"/></div> <div><div>➤ Restrict Corporate Resources for Blocked Devices</div><div>Ensure that devices blocked on your mail server can not access corporate resources such as Wi-Fi or VPN.</div><input type="checkbox"/></div>

Note that MCMS has ability to set thresholds for data plans. When a threshold is reached, it can send email notifications. However MCMS does not support SMS or push notifications for this.

Before using the DeviceCompliantStatus attribute provided by the MDM, especially if the ISE administrator is not the MDM administrator, great care is needed to ensure network access is not restricted due to a non-related MDM compliancy condition. The administrator must realize that MDM compliance is not specific to security concerns and that the MDM is responding to compliance conditions outside of the network domain. This point is clarified in [Table 5](#) by looking at the available MDM responses to a non-compliant condition.

Table 5 *MDM Responses*

Action Type	Options
<p>Profile Removal</p> 	
<p>OS Version Enforcement</p> 	
<p>Encryption Enforcement</p> 	
<p>Jailbreak/Rooted Device Enforcement</p>	
<p>Application Compliance</p>	

Currently the MDM does not provide a method to mark compliance checks that are not reported to ISE. ISE cannot assert that network security issue caused a device to be MDM non-compliant.

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. Non-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 different scans that run on different intervals. They also available as device queries: These 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 MCMS.
- **Apps**—A complete inventory of all the applications installed on the device.
- **Certificates**—A list of the installed certificates on the device.

Scan information is available in device details screen. When a device periodically checks in with the MDM server, it will notify the server of the current scan results.

PINLockStatus

The PINLockStatus is available to the API and can be used by ISE to set a minimum requirement for network access, as shown in the CVD. MCMS allows administrator to create a PIN lock policy and set rules to force users to set PINs with certain strength (alphanumeric, length, require special characters, etc.).

The user is provided with a grace period to set up PIN lock. If user does not set up pin code within 60 minutes, all corporate profiles pushed via MCMS will be removed from the device. During this grace period, MCMS will return status as “Out of Compliance” if queried by ISE.

As a best practice, 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 will likely end up in a quarantine state from NAC. There are two issues at play:

- First, the MDM server does not get a triggered update when a user creates a PIN lock. The user is required to enter one, but it will be some time before the server becomes aware of the PIN lock.
- Second, the MDM on-boards by installing the MDM profile and certificate first. This secures the communications between the server and device. After this profile is issued, the server will send a check-in request to the 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. Before this completes, the user will 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 work around is to open the MCMS client and click the “Refresh” button, as shown in [Figure 22](#), to update the server of the new posture. Then the user can try the continue button again or bounce their wireless to force a re-authorization.

Figure 22 *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 and 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 that the user will uninstall the MCMS agent 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 with it, 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 will check 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 MCMS 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 is on the device and that the device has responded to at least one check-in request issued through APNS or GCM. A register status does not guarantee that all the

profiles have been pushed to the device. Instead it indicates that the profile containing the MDM payload has been installed and that the device has responded to the initial check-in request. It is possible for profiles to be withheld 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 lost or stolen. Personal devices reported as stolen should undergo an enterprise wipe to remove all corporate data. Lost devices may be handled in the same manner, although the user may attempt to locate the device from the myDevices page first, but only if that service is allowed with the users role privileges and location services are enabled on the mobile device. The user or Admin can also try to issue a “find device” if the either the mobile client app or secure content locker is installed on the device. The device will emit a sound at period intervals to help the user locate the lost device. If the device remains lost after an attempt to locate it, then an enterprise wipe is prudent. The device can be restored if later 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.

Corporate devices have some more flexibility with respect to location information. If this information is available, then the administrator may have some options. They could choose to:

- Reassign the device to a secured location 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 and 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 and 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 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 MCMS App Catalog on their device. Applications can be from the public application store or developed in-house. Below is the complete list of features offered by MCMS:




- Manage and distribute third-party and in-house mobile apps from the Cisco MCMS Admin Portal.
- Develop a catalog of recommended mobile apps on iOS and Android devices.
- Users can view apps, install, and be alerted to updated apps on private app catalog.
- Manage lifecycle of app workflow:
 - Real-time software inventory reports
 - App distribution and installation tracking

- App update publishing
- Provisioning profile management
- Administer mobile app security and compliance policies:
 - Blacklist and whitelist mobile apps downloaded from Apple App Store and Google Play.
 - Enforce out-of compliance rules such sending user alerts, block email or VPN, and remote wipe.
 - Limit native apps available on the device such as YouTube.
 - Require user authentication and authorization before they download in-house apps.
 - Detailed reporting across app compliance events and remediation actions.
- Host and distribute in-house mobile apps on Cisco MCMS Cloud.
- Support for volume purchase programs on Apple App Store:
 - Automatically upload redemption codes in Cisco MCMS Cloud.
 - Track provisioning, manage licenses, monitor compliance, and eliminate manual VPP management.

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.

MCMS 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 23](#).

Figure 23 *AnyConnect Provisioning Profile*

VPN : Cisco AnyConnect Profiles

Configure for type	Cisco AnyConnect
VPN Connection Name	Cisco VPN
Host Name of the VPN Server	vpn.cisco.com
VPN User Account VPN credentials for authentication. For example, %domain%%username%, or just %username%.	%username%
Cisco VPN Group Name	
User Authentication Type	Certificate
Identity Certificate	-----Select-----
VPN On demand: Always establish for URLs Enter comma separated URLs.e.g. .com, .example.com. VPN connection will always be initiated for the domains or host names that matches these.	
VPN On demand: Never establish for URLs Enter comma separated URLs.e.g. .com, .example.com. VPN connection will not be initiated for the address that match these domains or host names.Any existing VPN connection will continue.	
VPN On demand: Establish if needed for URLs Enter comma separated URLs.e.g. .com, .example.com. VPN connection will be initiated for the address that match these domains or host names only if DNS lookup fails.	
Proxy Server Configuration Mode	None

294300

Conclusion

The integration of the network policy enforced by Cisco ISE and device policy offered by the MCMS MDM engine provides a new paradigm for BYOD deployments where security and productivity are not competing objectives.

Disclaimer

The MCMS configurations shown in this document should not be considered validated design guidance with respect to how the MCMS 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. MCMS is the only source for recommendations and best practices as it applies to their products and offerings.

