CHAPTER 13

Mobile Device Manager Integration for BYOD

Revised: August 7, 2013

The Cisco ISE can be configured to integrate with third-party Mobile Device Manager (MDM) products through an XML-based API. This allows network policy decisions based on mobile device posture that can include PIN lock, storage encryption, or registration status. In this release, both Apple and Android devices are supported. Configuring the infrastructure to support this functionality involves setting up ISE to send API requests to the MDM and configuring the MDM to accept these requests. Chapter 6, "Mobile Device Managers for BYOD" includes a discussion of the communications between the various components. Some MDM configurations, including device compliance policy, are discussed in general terms in this section. Detailed partner specific information can be found in supporting documentation at: http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns743/ns1050/own_device.html.

An overview of the topology common with the MDM architecture is presented below. The two basic models that are detailed in this section are an On-Premise model and a Cloud-based SaaS model. The components are similar except that the cloud model can also include an on-premise component to facilitate the integration with the enterprise.

Establishing IP Connectivity for an On-Premise MDM

Typically the on-premise MDM resides in the DMZ or some location where mobile devices can establish inbound connections. This allows the MDM to monitor the device's posture while the device is on the outside of the firewall. Without this access, the device would need to be placed on the network and interrogated prior to establishing the posture compliance of the device. The device does not automatically update the server whenever it joins a new network, therefore this interrogation would need to be manually initiated by the enterprise. If the MDM is located in the data center, some provision is required to allow inbound TCP sockets from the Internet. The specific ports vary based on the MDM partner and are detailed in the supporting documentation on Design Zone.

In addition to inbound sessions from the devices, the MDM needs to establish outbound connections to the push servers. The MDM uses the push service to locate and notify the device of changes to the MDM policy. Apple refers their service as the Apple Push Notification Service (APNS) and requires an Apple signed certificate to authenticate the MDM. Google refers to their service as Google Cloud Messaging for Android (GCM). This service replaces the older Cloud to Device Messaging Framework (C2DM). Both Apple and Android incorporate the push service into the device's operating system (OS) to allow the MDM server to communicate with the MDM client application. Apple devices also allow the MDM to communicate with the OS MDM API with the appropriate credentials. Both require the end user to establish an account with either Google or Apple respectively. This account effectively binds a device list to a user.

The MDM will also host a user-centric My Devices Portal to allow users to log into the MDM and manage some aspects of their device. This is similar but distinct from the My Devices Portal offered by ISE and serves a different purpose. Users may attach from either the mobile device or their standard desktop. The MDM web server can be configured with ACLs to restrict access to the My Devices Portal page from specific source address. For example, it is possible to block Internet access to the portal. The same is true for the administrator website.

The MDM will also receive inbound HTTPS session on port 443 by default to support the API used by ISE. In contrast to the MDM placement, ISE should be located in the data center. Firewall policy should be set to allow TCP 443 sessions that are initiated from ISE towards the MDM server. The MDM will have a default route pointing towards an outbound firewall and a more specific route to ISE pointing towards an inbound firewall. The majority of MDM partners support on-premise deployments on VM servers that may support multiple interfaces. It is possible that the route to ISE may be over a dedicated link. The topology of the DMZ should match the established corporate policy for servers. Typically the MDM will also allow the administrator to protect the API with an ACL. In this case, the ACL could be configured to permit ISE but deny any other connections.

ISE supports the use of a proxy for external connections. Currently the proxy configuration is globally configured. If ISE is required to use a proxy for the feed service, then it will also direct MDM requests to the proxy. This could cause connectivity issues between ISE and an on-premise MDM. In this scenario, the proxy configuration will require careful review to ensure that the ISE can connect to the MDM via the proxy.

Establishing IP Connectivity for a Cloud-Based MDM

Subscribing to an online MDM service simplifies many of the connectivity issues, especially between the mobile devices and the device manager. Because personal mobile devices spend the majority of time connected to the public Internet, choosing this model offers some advantages over a traditional on-premise model. The Apple APNS or Google GCM are also simplified when a cloud model is in use. The enterprise will still need to generate a certificate-signing request and present that to Apple prior to using the APNS service. This is explained in the partner-specific supporting documentation. However with the advantages realized with a cloud deployment, there are also challenges with respect to enterprise integration, specifically the corporate directory structure. Without any integration, a separate and dedicated user database would need to be established and maintained on the MDM servers. Typically in the cloud model, the enterprise will establish a small integration server that resides in the DMZ and serves as a proxy to a secure LDAP binding. This is explained in the partner-specific supporting documentation. With the exception of this additional server, all of the other components found in the on-premise model are present in a cloud model.

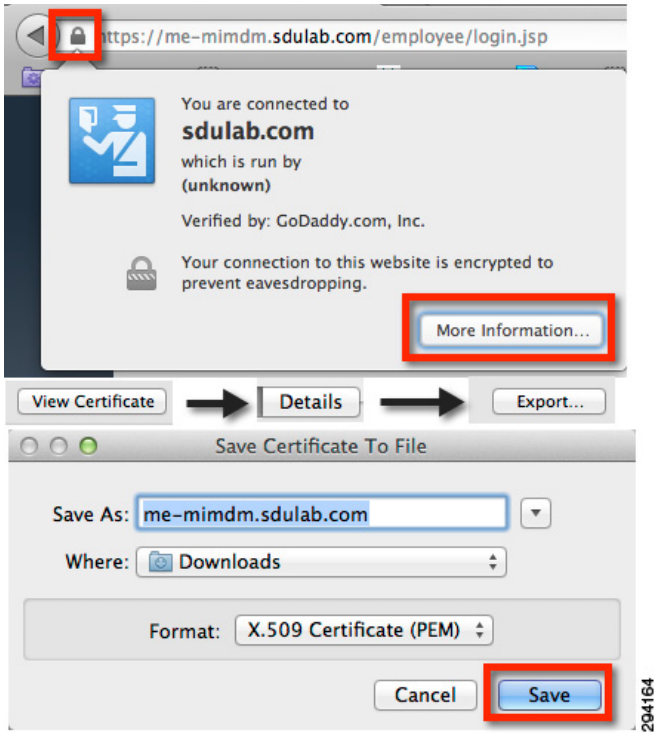
The primary concern is the HTTPS connection between ISE and the cloud-based MDM server, which is outbound from ISE. Corporate firewalls need to allow the ISE server siting in the data center to establish outbound HTTPS servers to the MDM server. The MDM partner may be able to provide a range of destination subnets if outbound sessions are restricted from data center servers such as ISE. Before ISE will trust the MDM server, the MDM server's certificate should be imported into the local ISE certificate store (this is explained below). The MDM service will provide the URL of the API. It is this certificate on this site that should be imported. In addition, users will need to be able to establish outbound HTTPS connections to the My Devices Portal page on the cloud-based MDM server. This would only be a concern in environments where users are not allowed access to Internet websites. If WCS or ScanSafe is in use, then the enterprise should confirm that the MDM site has a reputation score that exceeds the threshold needed for access or the site should be manually added to the permitted whitelist. Routing is straightforward. ISE and the user devices will follow the default route towards the Internet. The session may flow over NAT boundaries without requiring a NAT fix-up.

Connectivity must also be provided to mobile clients that have been quarantined to the MDM and to either the Apple Push Service or Google Cloud Messaging Servers. This allows the MDM to communicate with the device as needed to update the device's posture information on the server. In some situations, the mobile client may also need access to Google Play and the Apple AppStore to download required applications such as the MDM mobile client.

Configure ISE to Authenticate the MDM API

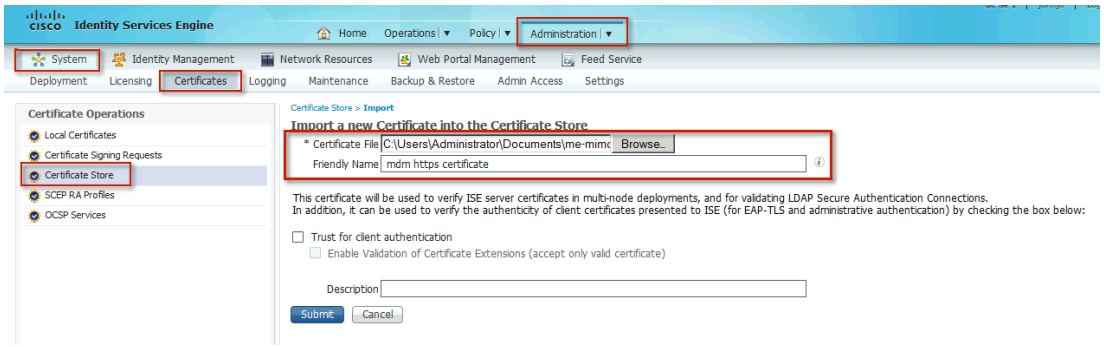
Prior to configuring the MDM, ISE must trust the HTTPS certificate presented by the MDM website. In either the cloud or on-premise deployment model, this can be accomplished by installing the MDM's HTTPS certificate in the ISE certificate store. The easiest method is to browse to the MDM server, export the HTTPS certificate, and then import it into ISE. Figure 13-1 shows this in Firefox, however the procedure may be different for other browsers.

Figure 13-1 Exporting MDM Certificate



Once the certificate has been saved to the local disk, the user will import it into the local certificate store on ISE. By default, the browser will save the certificate file with a name based on identity contained in the certificate, which is typically the FQDN of the site. The file extension could be .com, which is a well-known MS-DOS extension, making the cert more difficult to locate. While this does not affect importing the certificate, it could make browsing for the file on the hard drive less obvious. Importing the certificate into ISE is shown in Figure 13-2.

Figure 13-2 Importing Certificate into ISE



If ISE and the MDM are using the same CA, then importing the MDM SSL certificate may not be required. ISE does not maintain a system list of well-known public root certificates, therefore all trust relationships must be established by the administrator. Installing the MDM SSL certificate is the simplest approach and is shown here to ensure success.

Creating the MDM API User Account

In addition to the certificate, ISE will need a user account on the MDM that will allow access to the API. The previously installed certificate allows ISE to attach to the MDM via HTTPS, which will encrypt all data exchanges between ISE and the MDM, including the API credentials. All of the MDM partners support a local user account that can be granted API privileges. Some vendors may allow the account to be defined in an external data store such as Active Directory. This could be useful if ISE is using the same account to access AD or other resources and centralized machine account management is in use. In all cases, the API user account should be protected by strong passwords. For specific guidance on setting up this account, refer to the partner-specific supporting documentation or the partner MDM Administrator guide.

There are two account issues that may prevent the API from functioning properly:

- Incorrect username or password combination
- Defined user has not been granted API access

Setting Up the MDM Connection

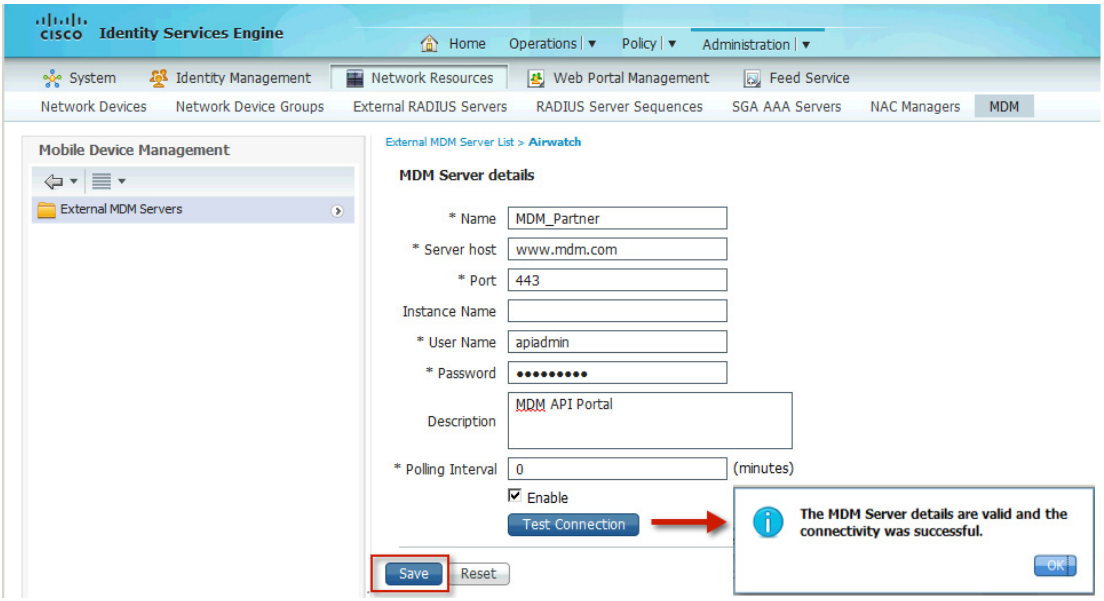
ISE will contact the MDM to gather posture information about devices or to issue device commands such as corporate wipe or lock. The session is initiated from ISE towards the MDM server. The URL for the MDM server is typically the same as the admin page and will be the same website used to export the certificate. The directory path is handled automatically by the system and is not specified as part of the configuration. The instance is used in multi-tenant deployments more commonly found when subscribing to a cloud service. The field should be left blank unless the cloud provider has instructed otherwise. The port will typically be TCP 443 for HTTPS. Typically the MDM cannot be configured to listen on a specific port for API users. Any change will also impact both the admin and user portal pages.

The polling interval specifies how often ISE will query the MDM for changes to device posture. By default, this is set to 0 minutes, effectively disabling polling. Polling can be enabled to periodically check the MDM compliance posture of an endpoint. If the device is found to be out of compliance and the device is associated to the network, then ISE will issue a CoA forcing the device to re-authenticate. Likely the device will need to remediate with the MDM, although this will depend on how the 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 this 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 to an aggressively low 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 had exceeded 80% of the data plan to avoid 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 intentions. In addition, the CoA will interrupt the user WiFi session, possibly terminating real-time applications such as VoIP calls. The recommendation is to leave the polling interval at 0 until a full understanding of the MDM's 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 half of this value. Over sampling the device posture will create unnecessary loads on the MDM server and reduced battery life on the mobile devices.

Finally, the enable check box will be set to active on one MDM server. It is possible to save multiple configurations, but only one can be active at a time. Figure 13-3 shows a typical configuration.

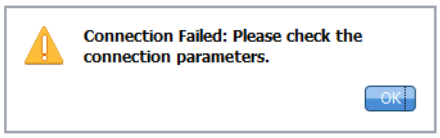
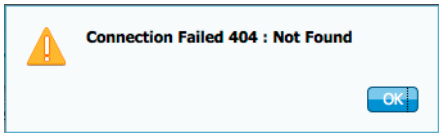
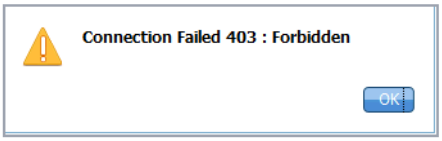
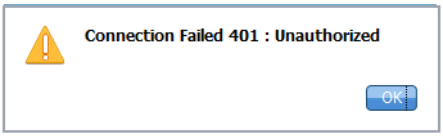
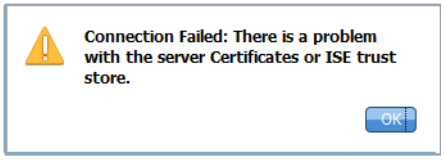
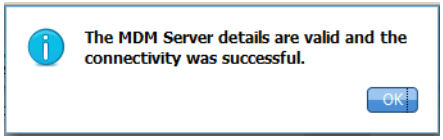
Figure 13-3 MDM Server Details



Verifying the MDM Connection

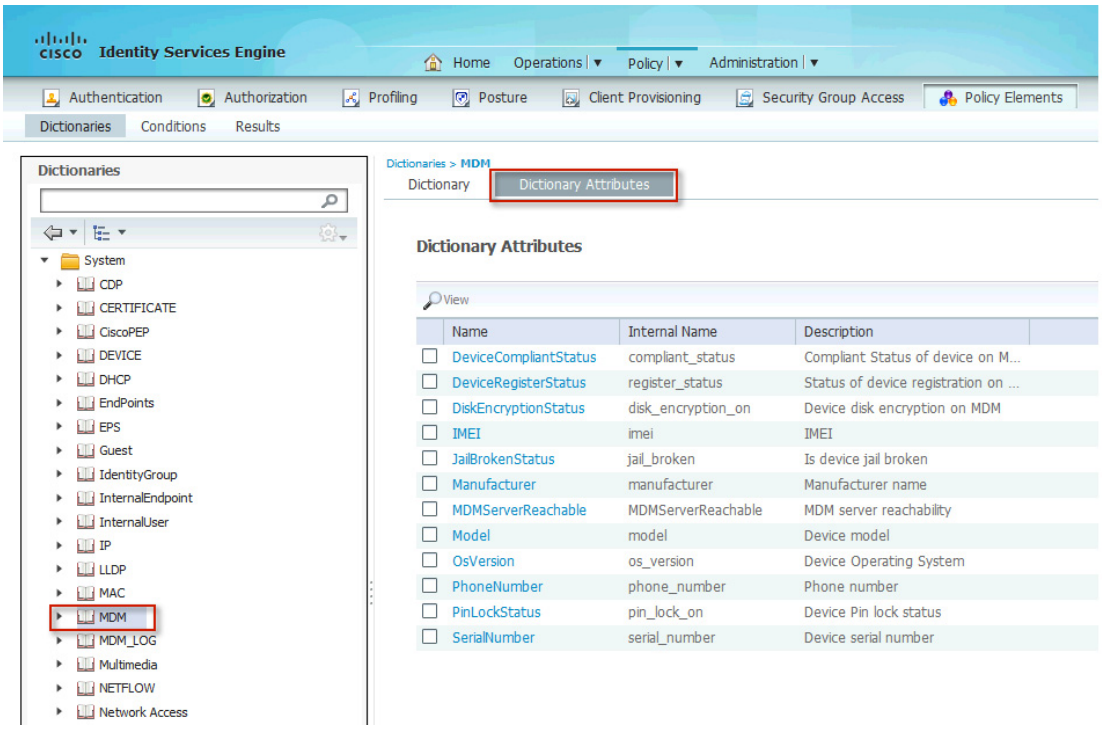
The test button will establish a connection to the MDM and attempt to authenticate using the configured credentials. This should be complete prior to saving the settings. If not, then the save button will validate the settings. If any errors are encountered, the MDM Enable button will be deselected prior to saving. If any error messages are presented, the administrator can refer to Table 13-1 for guidance in correcting the setup. In order to re-run the test on a previously validated server, the user should deselect the Enable checkbox, save, and then re-enable the checkbox.

Table 13-1 Common MDM Connection Error Codes

	A routing or firewall problem exists between 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.
	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.
	The user account setup on the MDM 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.
	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 MDM server returning an HTML code 401 to ISE.
	ISE does not trust the certificate presented by the MDM 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 connection has successfully been tested. The administrator should also verify the MDM dictionary has been populated with attributes.

After successfully configuring the MDM, the ISE policy dictionary will contain the attributes needed to create policy. The user can verify the dictionary by clicking **Policy > Dictionaries > System > MDM**, as shown in Figure 13-4.

Figure 13-4 Dictionary Attributes



Configuring the MDM

In addition to the API user account needed for ISE, there are several other administrative tasks that need to be accomplished on the MDM, such as signing and installing the APNS certificates before ISE can issue device actions through the API. The partner-specific supporting documentation has additional details on the minimum requirements. The MDM can also be configured to integrate with the corporate directory structure through LDAP. The administrator should review the MDM installation and administration guides to bring the MDM system into a fully functional state.