Mobile Device Manager Interoperability with Cisco ISE

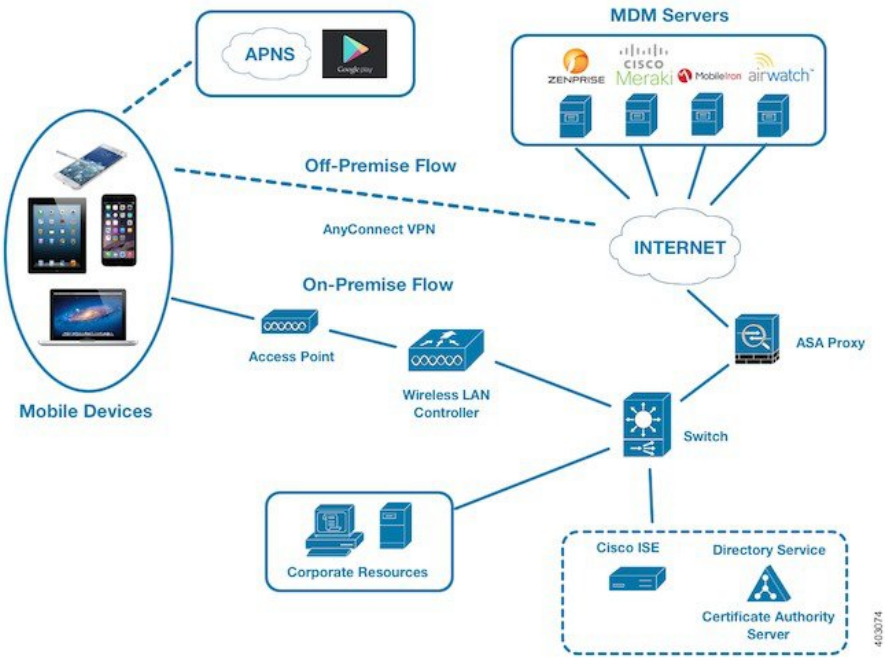
Mobile Device Management (MDM) servers secure, monitor, manage, and support mobile devices that are deployed across mobile operators, service providers, and enterprises. Traditionally, MDM servers have only supported mobile devices. Some MDM servers now manage all types of devices in a network (mobile phones, tablets, laptops, and desktops) and are called Unified Endpoint Management (UEM) servers. MDM servers act as a policy server that controls the use of some applications on a mobile device (for example, an email application) in the deployed environment. Cisco ISE queries a connected MDM server for information about various attributes that you can use to create network authorization policies.

You can run multiple active MDM servers on your network, from different vendors. This allows you to route different endpoints to different MDM servers based on device factors such as location or device type.

Cisco ISE also integrates with MDM servers using the Cisco MDM Server Info APIs, Version 2 and later versions, to allow devices to access the network over VPN via Cisco AnyConnect 4.1 and Cisco Adaptive Security Appliances 9.3.2 or later.

In the following illustration, Cisco ISE is the enforcement point and the MDM policy server is the policy information point. Cisco ISE obtains data from the MDM server to provide a complete solution.

Figure 1: MDM Interoperability with Cisco ISE



Configure Cisco ISE to interoperate with one or more external MDM servers. By setting up this type of third-party connection, you can use the detailed information available in the MDM database. Cisco ISE uses REST API calls to retrieve information from the external MDM server. Cisco ISE applies the appropriate access control policies to switches, access routers, wireless access points, and other network access points. The policies give you greater control of the remote devices that are accessing the Cisco ISE-enabled network.

For a list of the MDM vendors supported by Cisco ISE, see Supported Unified Endpoint Management and Mobile Device Management Servers, on page 5.

Supported Mobile Device Management Use Cases

Cisco ISE performs the following functions with external MDM servers:

- Manages device registration: Unregistered endpoints that access the network are redirected to a registration page that is hosted on the MDM server. Device registration includes the user role, device type, and so on.
- Handles device remediation: Endpoints are granted restricted access during remediation.
- Augments endpoint data: The endpoint database is updated with information from the MDM server that you cannot gather using the Cisco ISE profiling services. Cisco ISE uses multiple device attributes that you can view in the **Endpoints** page. Choose **Work Centers** > **Network Access** > **Identities** > **Endpoints**.

The following are examples of the device attributes available.

- MDMImei: xx xxxxxx xxxxxx x
- MDMManufacturer: Apple
- MDMModel: iPhone
- MDMOSVersion: iOS 6.0.0
- MDMPhoneNumber: 5550100
- MDMSerialNumber: DNPGQZGUDTFx

- Polls the MDM server every four hours for device compliance data. Configure the polling interval in the **External MDM Servers** page. (To view this page, choose **Work Centers** > **Network Access** > **Network Resources** > **External MDM Servers**.
- Issues device instructions through the MDM server: Cisco ISE issues remote actions for user devices through the MDM server. Initiate remote actions from the Cisco ISE administration portal through the **Endpoints** page. To view this page, choose **Context Visibility** > **Endpoints**. Check the check box next to the MDM server and click **MDM Actions**. Choose the required action from the drop-down list displayed.

Vendor MDM Attributes

When you configure an MDM server in Cisco ISE, Cisco ISE queries the MDM server for device attribute information and adds the information to the MDM system dictionary. The following attributes are used for registration status, and are commonly supported by MDM vendors.

Cisco ISE uses APIs to query MDM servers for the required device attributes. Cisco ISE Release 3.1 and later releases support MDM APIs Version 3. The Version 3 APIs include APIs that allow Cisco ISE to send queries to MDM servers for device attributes that help Cisco ISE identify endpoints that use MAC address randomization. Cisco ISE queries the MDM server for the following attributes:

- GUID: A unique device identifier that replaces the use of MAC address to identify a device.
- MAC addresses: The list of MAC addresses that a UEM or MDM server has recorded for a particular device. A maximum of five MAC addresses are shared for a device.

If an MDM server does not provide values for the required attributes, Cisco ISE fills the attributes fields with the default values that are mentioned in the following table.

Table 1: MDM Attributes and Values

Attribute Name	Attribute Dictionary	Default Value	Data That is Expected From UEM or MDM Servers	Data That is Expected From Microsoft SCCM Servers
DaysSinceLastCheckin Supported from MDM API Version 3	MDM	None	The number of days since a user has last checked in or synchronized a device with the UEM or MDM server. The valid range is 1–365 days.	The number of days since a user has last checked in or synchronized a device with the SCCM server. The valid range is 1–365 days.
DeviceCompliantStatus	MDM	NonCompliant	**Compliant** or **NonCompliant**.	**Compliant** or **NonCompliant**.
DeviceRegisterStatus	MDM	UnRegistered	**Registered** or **UnRegistered**.	**Registered** or **UnRegistered**.
DiskEncryptionStatus	MDM	Off	**On** or **Off**.	**On** or **Off**.
IMEI	MDM	None	The IMEI number of the device.	Not applicable.
JailBrokenStatus	MDM	Unbroken	**Reachable** or **UnReachable**.	**Reachable** or **UnReachable**.
MDMFailureReason	MDM	None	The device failure reason.	The device failure reason.
MDMServerName	MDM	None	The name of the server.	The name of the server.
MDMServerReachable	MDM	Reachable	**Reachable** or **UnReachable**.	**Reachable** or **UnReachable**.
MEID	MDM	None	The MEID value of the device.	Not applicable.
Manufacturer	MDM	None	The name of the device manufacturer.	Not applicable.
Model	MDM	None	The name of the device model.	Not applicable.
OsVersion	MDM	None	The operating system version of the device.	Not applicable.

Attribute Name	Attribute Dictionary	Default Value	Data That is Expected From UEM or MDM Servers	Data That is Expected From Microsoft SCCM Servers
PhoneNumber	MDM	None	The phone number of the device.	Not applicable.
PinLockStatus	MDM	Off	**On** or **Off**.	Not applicable.
SerialNumber	MDM	None	The serial number of the device.	Not applicable.
ServerType	MDM	None	**MDM** for a Mobile Device Manager server. **DM** for Desktop Device Manager server.	**DM** for Desktop Device Manager server.
UDID	MDM	None	The UDID number of the device.	Not applicable.
UserNotified	MDM	No	**Yes** or **No**	Not applicable.

If a vendor's unique attributes are not supported, you may be able to use ERS APIs to exchange vendor-specific attributes. Check the vendor's documentation for information on the ERS APIs that are supported.

The new MDM dictionary attributes are available for use in authorization policies.

Supported Unified Endpoint Management and Mobile Device Management Servers

Supported MDM servers include products from the following vendors:

- Absolute
- Blackberry - BES
- Blackberry - Good Secure EMM
- Cisco Meraki Systems Manager
- Citrix XenMobile 10.x (On-prem)
- Globo
- IBM MaaS360
- Ivanti (previously MobileIron UEM), core and cloud UEM services

Note Some versions of MobileIron do not work with Cisco ISE. MobileIron is aware of this problem, and have a fix. Contact MobileIron for more information.

- JAMF Casper Suite
- Microsoft Endpoint Configuration Manager
- Microsoft Endpoint Manager Intune
- Mosyle
- SAP Afaria
- Sophos
- SOTI MobiControl
- Symantec
- Tangoe
- VMware Workspace ONE (earlier known as AirWatch)
- 42Gears

For the configurations that you must perform in your endpoint management servers to integrate the servers with Cisco ISE, see Integrate UEM and MDM Servers With Cisco ISE.

ISE Community Resource

How To: Meraki EMM / MDM Integration with ISE

Ports Used by the Mobile Device Management Server

The following table lists the ports that must be open between Cisco ISE and an MDM server to enable them to communicate with each other. See the documentation from the MDM vendor for a list of ports that must be open on the MDM agent and server.

Table 2: Ports Used by the MDM Server

MDM Server	Ports
MobileIron	443
Citrix XenMobile 10.x (On-prem)	443
Blackberry - Good Secure EMM	19005

MDM Server	Ports
VMware Workspace ONE (earlier known as AirWatch)	443
SAP Afaria	443
IBM MaaS360	443
Cisco Meraki	443
Microsoft Intune	80 and 443
Microsoft SCCM	80 and 443

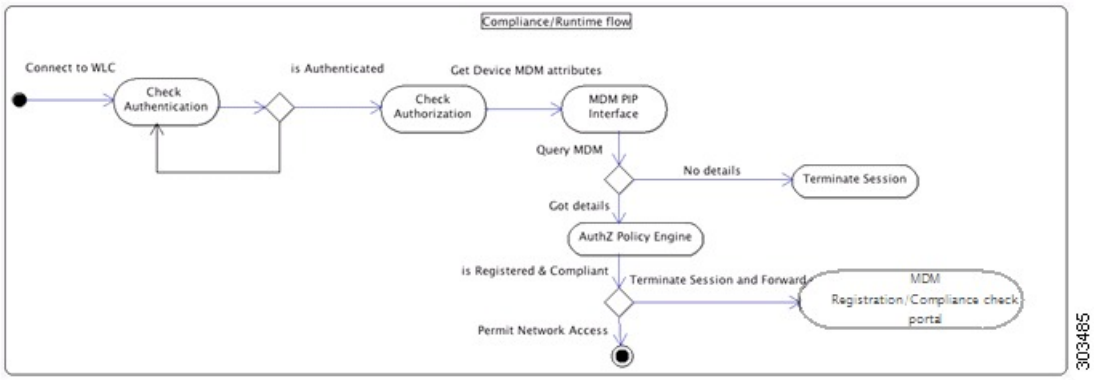
Mobile Device Management Integration Process Flow

1. The user associates a device with an SSID.
2. Cisco ISE makes an API call to the MDM server.
3. This API call returns a list of devices for the user and the posture statuses for the devices.

Note The input parameter is the MAC address of the endpoint device. For off-premise Apple iOS devices (any device that connects to Cisco ISE through a VPN), the input parameter is the UDID.

4. If the user's device is not on this list, it means that the device is not registered. Cisco ISE sends an authorization request to the NAD to redirect to Cisco ISE. The user is presented with the MDM server page.
5. Cisco ISE uses MDM to provision the device and presents the appropriate window for the user to register the device.
6. The user registers the device in the MDM server, and the MDM server redirects the request to Cisco ISE through automatic redirection or manual browser refresh.
7. Cisco ISE queries the MDM server again for the posture status.
8. If the user's device is not compliant with the posture (compliance) policies that are configured on the MDM server, the user is notified that the device is out of compliance. The user must take the necessary action to ensure that the device is compliant.
9. When the user's device is compliant, the MDM server updates the device's state in its internal tables.
10. If the user refreshes the browser now, the control is transferred back to Cisco ISE.
11. Cisco ISE polls the MDM server every four hours to get compliance information and issues the appropriate Change of Authorization (CoA). You can configure the polling interval. Cisco ISE also checks the MDM server every five minutes to make sure that it is available.

Figure 2: The MDM Process Flow in Cisco ISE



Note A device can only be enrolled in a single MDM server at a time. If you want to enroll the same device to an MDM service from another vendor, the previous vendor's profiles must be removed from the device. The MDM service usually offers a "corporate wipe", which only deletes the vendor's configuration from the device (not the whole device). The user can also remove the files. For example, on an iOS device, the user can go to the **Settings** > **General** > **Device management** window, and click **Remove Management**. Or the user can go to the MyDevices portal in Cisco ISE and click **Corporate Wipe**.

Set Up Mobile Device Management Servers with Cisco ISE

To set up MDM servers with Cisco ISE, you must perform the following high-level tasks:

Step 1 Import the MDM server certificate into Cisco ISE, except for Intune, where you import the Policy Administration node's (PAN) certificate into Azure.

Step 2 Create mobile device manager definitions.

Step 3 Configure ACLs on the Cisco WLCs.

Step 4 Configure an authorization profile that redirects nonregistered devices to the MDM server.

Step 5 If there are multiple MDM servers on the network, configure separate authorization profiles for each vendor.

Step 6 Configure authorization policy rules for the MDM use cases.

Import Mobile Device Management Server Certificate into Cisco ISE

For Cisco ISE to connect with the MDM server, you must import the MDM server certificate into the Cisco ISE Trusted Certificates store. If your MDM server has a CA-signed certificate, you must import the root certificate into the Cisco ISE Trusted Certificates store.

Note For Microsoft Azure, import the Cisco ISE certificate into Azure. See Connect Microsoft Intune to Cisco ISE as a Mobile Device Management Server.

Step 1 Export the MDM server certificate from your MDM server and save it on your local machine.

Step 2 Choose **Administration** > **System** > **Certificates** > **Trusted Certificate** > **Import**.

Step 3 In the **Import a new Certificate into the Certificate Store** window, click **Choose File** to select the MDM server certificate that you obtained from the MDM server.

Step 4 Add a name for the certificate in the **Friendly Name** field.

Step 5 Check the **Trust for authentication within ISE** check box.

Step 6 Click **Submit**.

Step 7 Verify that the **Trust Certificates** window lists the newly added MDM server certificate.

Define Device Management Servers in Cisco ISE

Define mobile and desktop device management servers in Cisco ISE to allow Cisco ISE to communicate with the required servers. You can configure the authentication type that is used to communicate with the servers, the frequency at which Cisco ISE requests device information from a device management server, and so on.

To define a mobile management server, see Configure Mobile Device Management Servers in Cisco ISE, on page 9.

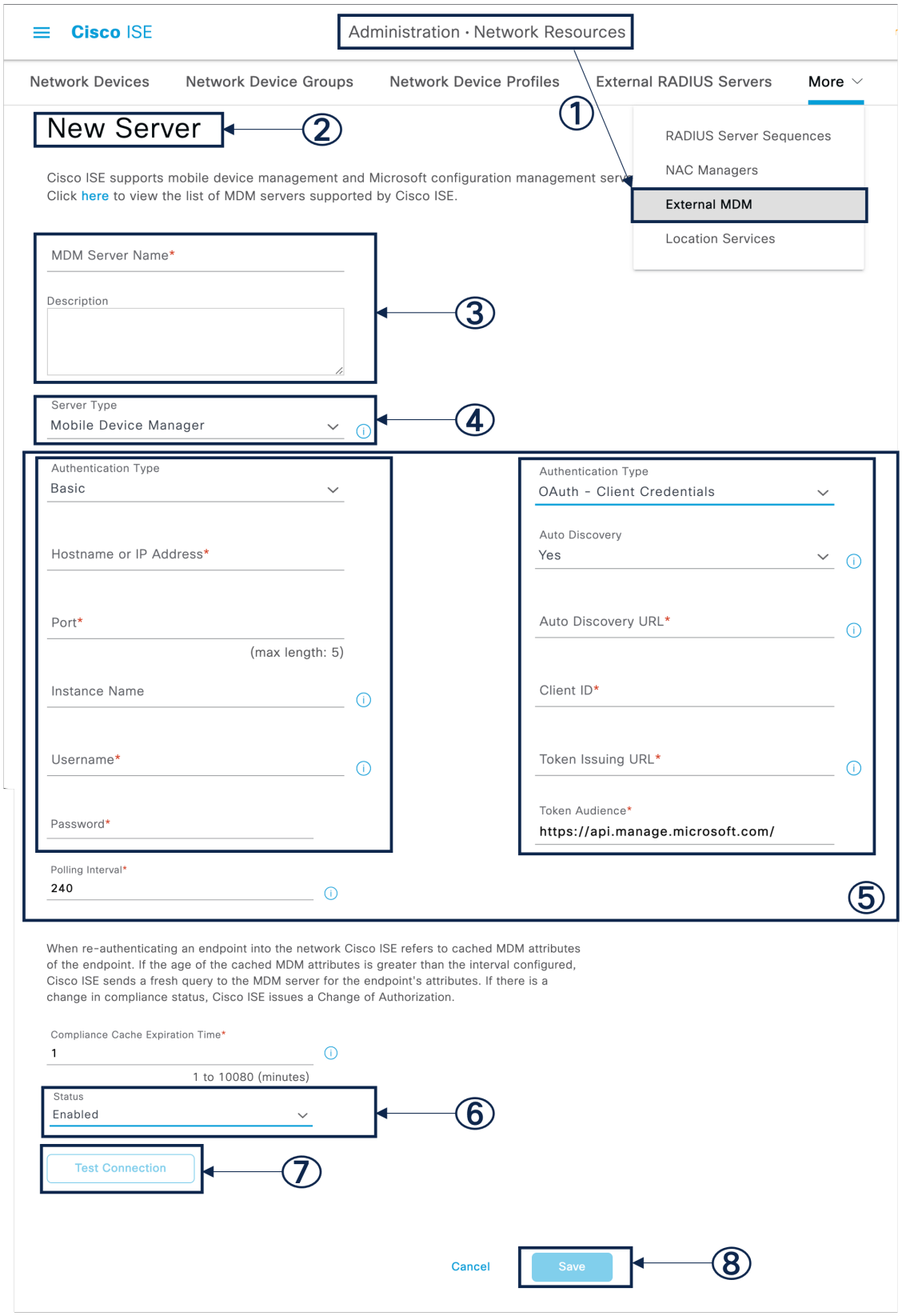
To define a Microsoft System Center Configuration Manager (SCCM) server, see Define Microsoft System Center Configuration Manager Servers in Cisco ISE, on page 13.

Configure Mobile Device Management Servers in Cisco ISE

The first MDM server that provides an endpoint's information to Cisco ISE is displayed in the endpoint information in the **Context Visibility** > **Endpoints** window. The MDM server information is not automatically updated when an endpoint connects with a different MDM server. You must delete the endpoint from the **Context Visibility** window, and then the endpoint must reconnect with an MDM server, for the **Context Visibility** window to display the updated information.

The following image displays the Cisco ISE GUI fields that you must work with during this task. The numbers in the image correspond to the step numbers in the following task.

Figure 3: Add an MDM Server in Cisco ISE


Cisco ISE
Administration · Network Resources
Network Devices
Network Device Groups
Network Device Profiles
External RADIUS Servers
More
1
RADIUS Server Sequences
NAC Managers
External MDM
Location Services
New Server
2
Cisco ISE supports mobile device management and Microsoft configuration management serv
Click here to view the list of MDM servers supported by Cisco ISE.
MDM Server Name*
Description
3
Server Type
Mobile Device Manager
4
Authentication Type
Basic
Hostname or IP Address*
Port*
(max length: 5)
Instance Name
Username*
Password*
Authentication Type
OAuth - Client Credentials
Auto Discovery
Yes
Auto Discovery URL*
Client ID*
Token Issuing URL*
Token Audience*
https://api.manage.microsoft.com/
Polling Interval*
240
5
When re-authenticating an endpoint into the network Cisco ISE refers to cached MDM attributes of the endpoint. If the age of the cached MDM attributes is greater than the interval configured, Cisco ISE sends a fresh query to the MDM server for the endpoint's attributes. If there is a change in compliance status, Cisco ISE issues a Change of Authorization.
Compliance Cache Expiration Time*
1
1 to 10080 (minutes)
Status
Enabled
6
Test Connection
7
Cancel
Save
8

Step 1 Choose **Administration** > **Network Resources** > **External MDM**.

Step 2 In the **MDM Servers** window, click **Add**.

Step 3 Enter the name and description of the MDM server that you want to add in the corresponding fields.

Step 4 From the **Server Type** drop-down list, choose **Mobile Device Manager**.

Step 5 From the **Authentication Type** drop-down list, choose either **Basic** or **OAuth - Client Credentials**.

If you choose the **Basic** authentication type, the following fields are displayed:

- **Host Name / IP Address**: Enter the hostname or IP address of the MDM server.
- **Port**: Specify the port to be used when connecting to the MDM server, which is usually 443.
- **Instance Name**: If this MDM server has several instances, enter the instance that you want to connect to.
- **Username**: Enter the username that must be used to connect to the MDM server.
- **Password**: Enter the password that must be used to connect to the MDM server.

If you choose the **OAuth - Client Credentials** authentication type, the following fields are displayed:

- From the **Auto Discovery** drop-down list, choose **Yes** or **No**.
- **Auto Discovery URL**: Enter the value of Microsoft Azure AD Graph API Endpoint from the Microsoft Azure management portal. This URL is the endpoint at which an application can access directory data in your Microsoft Entra ID using the Graph API. For more information, see Integrate MDM and UEM Servers with Cisco ISE.
- **Client ID**: The unique identifier for your application. Use this attribute if your application accesses data in another application, such as the Microsoft Azure AD Graph API, Microsoft Intune API, and so on.
- **Token Issuing URL**: Enter the value of the Oauth2.0 Authorization Endpoint. This is the endpoint from which Cisco ISE obtains an access token using OAuth2.0.
- **Token Audience**: The recipient resource that the token is intended for, which is a public, well-known **APP ID URL** to the Microsoft Intune API.

Time Interval For Compliance Device ReAuth Query: When an endpoint is authenticated or reauthenticated, Cisco ISE uses a cache to get the MDM variables for that endpoint. If the age of the cached value is greater than the value configured in this field, Cisco ISE sends a new device query to the MDM server to get new values. If the compliance status has changed, then Cisco ISE triggers the appropriate CoA. The valid range is from 1 to 1440 minutes. The default value is one minute.

Polling Interval: Enter the polling interval, in minutes, for Cisco ISE to poll the MDM server for noncompliant endpoints. Set this value to match the polling interval on your MDM server. The valid range is from 15 to 1440 minutes. The default value is 240 minutes. We recommend that you set the polling interval more than 60 minutes in production environments to minimize any performance impact that might occur due to large numbers of noncompliant endpoints.

If you set the polling interval to 0, Cisco ISE disables polling with the MDM server.

Note If the external MDM server receives requests from more than 20000 noncompliant endpoints, the external MDM server polling interval is automatically set to 0. You also receive the following alarm on Cisco ISE:

```
MDM Compliance Polling Disabled: Reason is Periodic Compliance Polling received huge
non-compliance device information.
```

Step 6 From the **Status** drop-down list, choose **Enabled**.

Step 7 To verify whether the MDM server is connected to Cisco ISE, click **Test Connection**. Note that **Test Connection** is not intended to check permissions for all the use cases (get baselines, get device information, and so on). These are validated when the server is added to Cisco ISE.

Step 8 Click **Save**.

Define Microsoft System Center Configuration Manager Servers in Cisco ISE

Step 1 Choose **Administration** > **Network Resources** > **External MDM** > **MDM Servers**.

Step 2 In the **MDM Servers** window, click **Add**.

Step 3 Choose **Desktop Device Manager** from the **Server Type** drop-down list.

Step 4 In the **Host Name / IP Address** field, enter the hostname or IP address of the Microsoft SCCM server.

Step 5 In the **Instance Name** field, if the Microsoft SCCM server has several instances, enter the instance that you want to connect to.

Step 6 In the **Username** field, enter the username that must be used to connect to the Microsoft SCCM server.

Step 7 In the **Password** field, enter the password that must be used to connect to the Microsoft SCCM server.

Step 8 In the **Time Interval For Compliance Device ReAuth Query** field, enter a value from 1 to 1440 minutes. The default value is one minute. When an endpoint is authenticated or reauthenticated, Cisco ISE uses a cache to get the MDM variables for that endpoint. If the age of the cached value is higher than the value configured in this field, Cisco ISE sends a new device query to the MDM server to get new values. If the compliance status has changed, then Cisco ISE triggers the appropriate CoA.

Step 9 Choose **Enabled** from the **Status** drop-down list.

Step 10 Click **Test Connection** to check if Cisco ISE can connect to the defined Microsoft SCCM server.

Step 11 Click **Save**.

Cisco ISE MDM Support for Microsoft Intune and Microsoft SCCM

- **Microsoft Intune**: Cisco ISE supports Microsoft Intune device management as a partner MDM server to manage mobile devices.

  Configure Cisco ISE as an OAuth 2.0 client application with the Microsoft Intune server managing mobile devices. Cisco ISE gets a token from Azure to establish a session with the Cisco ISE Intune application.

  For information about how Microsoft Intune communicates with a client application, see https://msdn.microsoft.com/en-us/library/azure/dn645543.aspx.

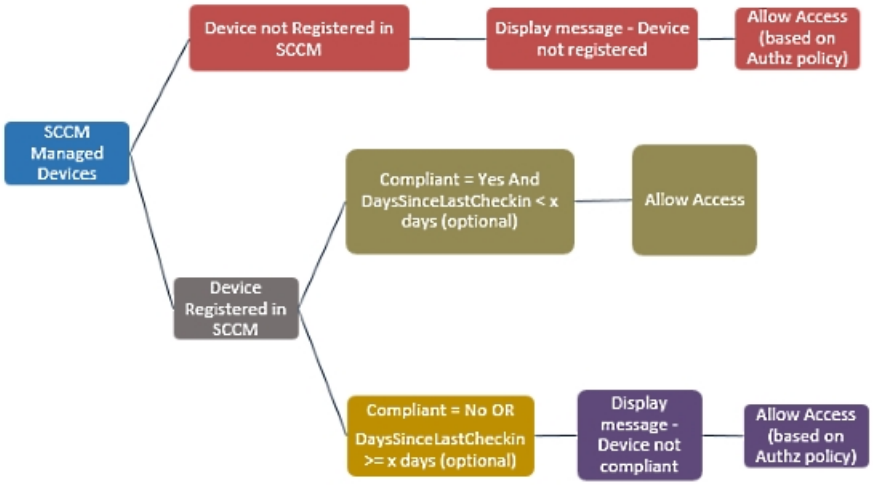
- **Desktop Device Manager (Microsoft SCCM)**: Cisco ISE supports the Microsoft System Center Configuration Manager (SCCM) as a partner MDM server for managing Windows computers. Cisco ISE retrieves compliance information from the Microsoft SCCM server using WMI, and uses that information to grant or deny network access to a user's Windows device.

  For performance and scalability information for Microsoft SCCM integrations, see Size and Scale Numbers for Configuration Manager. Microsoft uses Windows Management Instrumentation (WMI) interfaces based on the Component Object Model (COM), which results in scalability limitations.

Microsoft SCCM Workflow

Cisco ISE retrieves information from the Microsoft SCCM server about whether a device is registered. If the endpoint is registered, Cisco ISE checks for its compliance status. The following diagram shows the workflow for devices that Microsoft SCCM manages.

Figure 4: SCCM Workflow



When a device connects to the network and a Microsoft SCCM policy matches, Cisco ISE queries the relevant SCCM server to retrieve compliance and last login (check-in) time. With this information, Cisco ISE updates the compliance status and the lastCheckinTimeStamp of the device in the **Endpoint** list.

If the device is not compliant or not registered with the Microsoft SCCM server, and the authorization policy uses a redirect profile, a message is displayed to the user that the device is not compliant, or is not registered with the Microsoft SCCM. After the user acknowledges the message, Cisco ISE can issue a CoA to the Microsoft SCCM registration site. Users are granted access based on the authorization policy and profile.

Microsoft SCCM Server Connection Monitoring

You cannot configure polling intervals for Microsoft SCCM.

Cisco ISE runs an MDM HeartBeat job that verifies connection with the Microsoft SCCM server, and raises alarms if Cisco ISE loses the connection to the Microsoft SCCM server. The HeartBeat job interval cannot be configured.

Policy Set Example for Microsoft System Center Configuration Manager

The following new dictionary entries are used in policies to support Microsoft SCCM.

- **MDM.DaysSinceLastCheckin**: The number of days since a user last checked in or synchronized a device with Microsoft SCCM. The value may range from 1 to 365 days.
- **MDM.UserNotified**: The valid values are **Y** or **N**. The value indicates whether the user was notified that their device is not registered. You can then allow the user limited access to the network and then redirect them to the registration portal, or deny them access to the network.
- **MDM.ServerType**: The valid value is **MDM** for MDM servers and **DM** for desktop device management.

The following is an example of a policy set that supports Microsoft SCCM.

Policy Name	If	Then
SCCM_Comp	Wireless_802.1X AND MDM:MDMServerName EQUALS SccmServer1 AND MDM:DeviceRegisterStatus EQUALS Registered	PermitAccess
SCCM_NonComp_Notify	Wireless_802.1X AND MDM:MDMServerName EQUALS SccmServer1 AND MDM:DeviceCompliantStatus EQUALS NonCompliant AND MDM:UserNotified EQUALS 28	PermitAccess
SCCM_NonComp_Days	Wireless_802.1X AND MDM:MDMServerName EQUALS SccmServer1 AND MDM:MDMDeviceCompliantStatus EQUALS Registered AND MDM:DaysSinceLastCheckin EQUALS 28	SCCMRedirect
SCCM_NonComp	Wireless_802.1X AND MDM:MDMServerName EQUALS SccmServer1 AND MDM:DeviceCompliantStatus EQUALS NonCompliant AND MDM:DeviceRegisterStatus EQUALS Registered	SCCMRedirect
SCCM_UnReg_Notify	Wireless_802.1X AND MDM:DeviceRegisterStatus EQUALS Registered AND MDM:UserNotified EQUALS Yes	PermitAccess

Configure the Microsoft System Center Configuration Manager Server for Cisco ISE

Cisco ISE communicates with the Microsoft SCCM server using Windows Management Instrumentation (WMI). Configure WMI on the Windows server running Microsoft SCCM.

Note The user account that you use for Cisco ISE integration must either:

- Be a member of the SMS Admins user group.
- Have the same permissions as the SMS object under the WMI namespace:

  `root\sms\site_<sitecode>`

  where *sitecode* is the Microsoft SCCM site.

Set Permissions when Microsoft Active Directory Users are in Domain Admin Group

For Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2, the Domain Admin group does not have full control of certain registry keys in the Windows operating system by default. The Microsoft Active Directory administrator must give the Microsoft Active Directory user full control permissions on the following registry keys:

- **HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}**
- **HKLM\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}**

The following Microsoft Active Directory versions require no registry changes:

- Windows 2003
- Windows 2003R2
- Windows 2008

To grant full control, the Microsoft Active Directory admin must first take ownership of the key:

Step 1 Right-click the key icon and choose the **Owner** tab.

Step 2 Click **Permissions**.

Step 3 Click **Advanced**.

Permissions for Microsoft Active Directory Users Not in Domain Admin Group

For Windows Server 2012 R2, give the Microsoft AD user full control permissions on the following registry keys:

- `HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}`
- `HKLM\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}`

Use the following commands in Windows PowerShell to check if full permission is given to the registry keys:

- `get-acl -path "Microsoft.PowerShell.Core\Registry::HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}" | format-list`
- `get-acl -path "hklm:\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}" | format-list`

The following permissions are required when a Microsoft AD user is not in the Domain Admin group, but is in the Domain Users group:

- Add registry keys to allow Cisco ISE to connect to the domain controller.
- Permissions to Use DCOM on the Domain Controller
- Set Permissions for Access to WMI Root and CIMv2 Namespace, on page 20

These permissions are only required for the following Microsoft AD versions:

- Windows 2003
- Windows 2003R2
- Windows 2008
- Windows 2008 R2
- Windows 2012
- Windows 2012 R2
- Windows 2016

Add Registry Keys to Allow Cisco ISE to Connect to the Domain Controller

You must manually add some registry keys to the domain controller to allow Cisco ISE to connect as a domain user, and retrieve login authentication events. An agent is not required on the domain controllers or on any machines in the domain.

The following registry script shows the keys to add. You can copy and paste this into a text file, save the file with a .reg extension, and double click the file to make the registry changes. To add registry keys, the user must be an owner of the root key.

```
Windows Registry Editor Version 5.00

[HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"AppID"="{76A64158-CB41-11D1-8B02-00600806D9B6}"

[HKEY_CLASSES_ROOT\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"DllSurrogate"="  "

[HKEY_CLASSES_ROOT\Wow6432Node\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"DllSurrogate"="  "
```

Make sure that you include two spaces in the value of the DllSurrogate key. If the registry is manually updated, you must include only the two spaces and do not include the quotes. While updating the registry manually, ensure that quotes are not included for AppID, DllSurrogate, and its values.

Retain the empty lines as shown in the preceding script, including the empty line at the end of the file.

Use the following commands in the Windows command prompt to confirm if the registry keys are created and have the correct values:

- `reg query "HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}" /f "{76A64158-CB41-11D1-8B02-00600806D9B6}" /e`
- `reg query HKEY_CLASSES_ROOT\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6} /f "  " /e`
- `reg query HKEY_CLASSES_ROOT\Wow6432Node\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6} /f "  " /e`

Permissions to Use DCOM on the Domain Controller

The Microsoft Active Directory user who is used for Cisco ISE Passive Identity service must have the permissions to use DCOM on the domain controller server. Configure permissions with the **dcomcnfg** command line tool.

Step 1 Run the **dcomcnfg** tool from the command line.

Step 2 Expand **`Component Services`**.

Step 3 Expand **Computers** > **My Computer**.

Step 4 Choose **Action** from the menu bar, click **Properties**, and click **COM Security**.

Step 5 The account that Cisco ISE uses for both access and launch must have Allow permissions. Add the Microsoft Active Directory user to all the four options, **Edit Limits** and **Edit Default** for both **Access Permissions** and **Launch and Activation Permissions**.

Step 6 Allow all local and remote accesses for both **Access Permissions** and **Launch and Activation Permissions**.

Figure 5: Local and Remote Accesses for Access Permissions

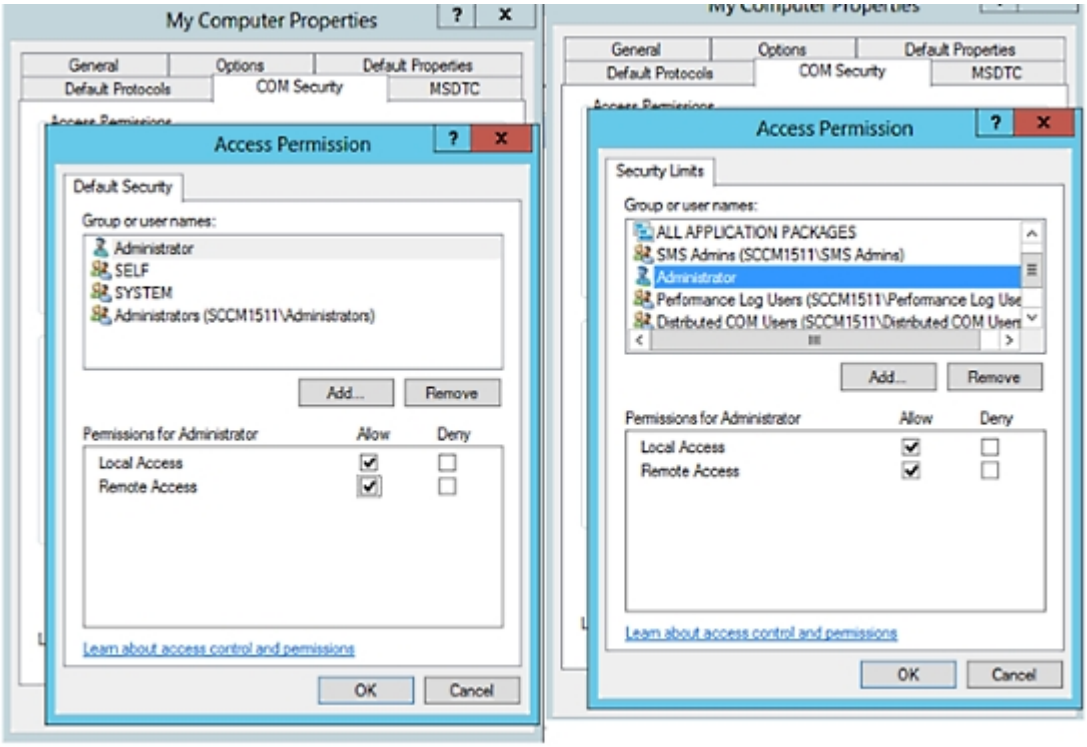
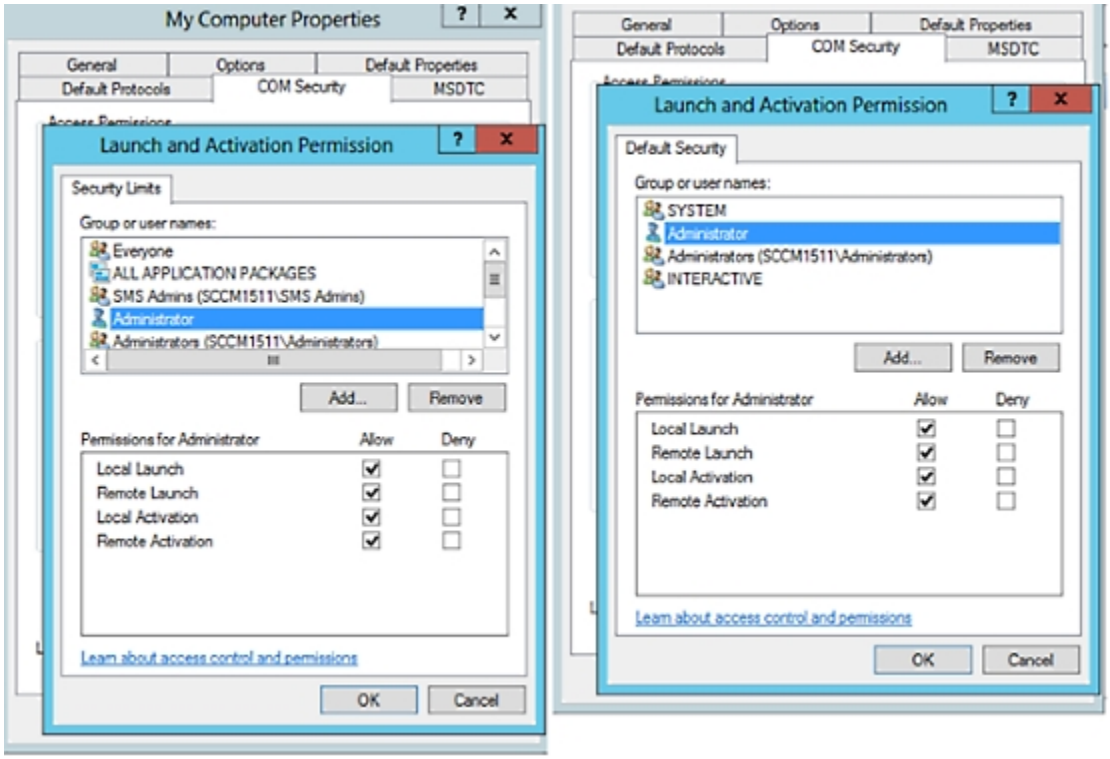


Figure 6: Local and Remote Accesses for Launch and Activation Permissions



Set Permissions for Access to WMI Root and CIMv2 Namespace

By default, Microsoft Active Directory users do not have permissions for the Execute Methods and Remote Enable. You can grant access using the wmimgmt.msc MMC console.

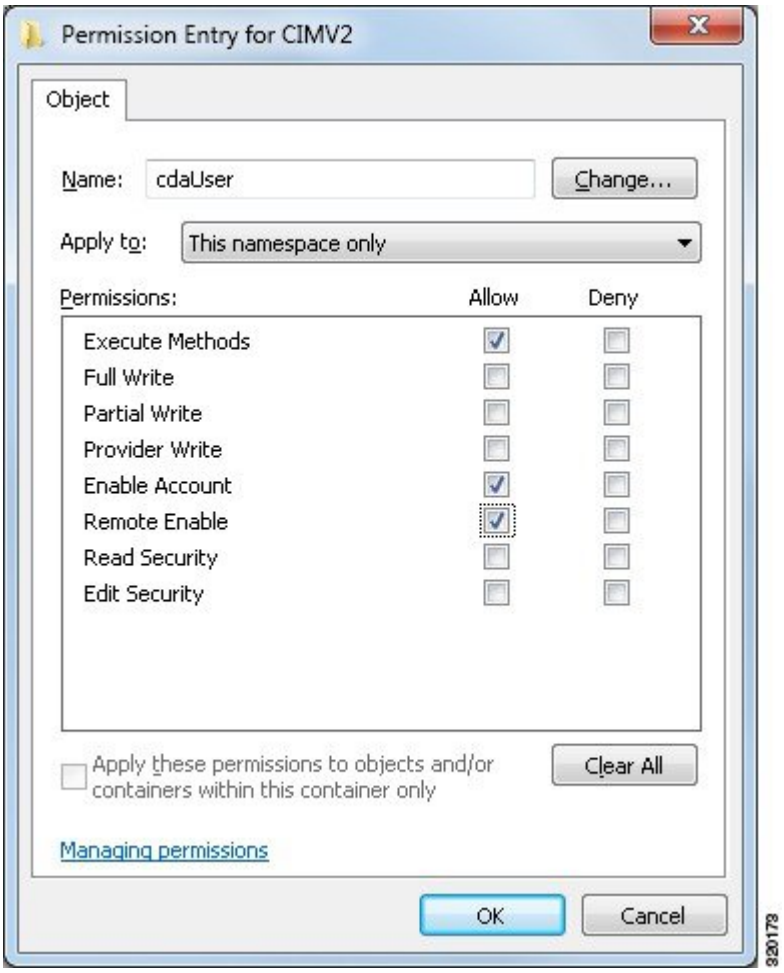
Step 1 Choose **Start** > **Run** and enter `wmimgmt.msc`.

Step 2 Right-click **WMI Control** and click **Properties**.

Step 3 Under the **Security** tab, expand **Root** and choose **CIMV2**.

Step 4 Click **Security**.

Step 5 Add the Microsoft Active Directory user, and configure the required permissions as shown in the following image.



Open Firewall Ports for WMI Access

The firewall software on the Microsoft Active Directory domain controller may block access to WMI. You can either turn off the firewall, or allow access on a specific IP address (Cisco ISE IP address) to the following ports:

- TCP 135: General RPC Port. When performing asynchronous RPC calls, the service listening on this port tells the client which port the component servicing this request is using.
- UDP 138: NetBIOS Datagram Service
- TCP 139: NetBIOS Session Service
- TCP 445: Server Message Block (SMB)

Note Cisco ISE supports SMB 2.0.

Higher ports are assigned dynamically, or you can configure them manually. We recommend that you add *%SystemRoot%\System32\dllhost.exe* as a target. This program manages ports dynamically.

All firewall rules can be assigned to a specific IP address (Cisco ISE IP).

Configure an Authorization Profile for Redirecting Nonregistered Devices

You must configure an authorization profile in Cisco ISE to redirect nonregistered devices for each external MDM server.

Before you begin

- Ensure that you have created an MDM server definition in Cisco ISE. Only after you successfully integrate Cisco ISE with the MDM server is the MDM dictionary populated. You can then create an authorization policy using the MDM dictionary attributes.
- Configure ACLs on the Cisco WLC for redirecting unregistered devices.
- If you are using a proxy for Internet connection and the MDM server is part of the internal network, then you have to put the MDM server name or its IP address in the Proxy-Bypass list. Choose **Administration** > **System** > **Settings** > **Proxy** to perform this action.

Step 1 Choose **Policy** > **Policy Elements** > **Results** > **Authorization** > **Authorization Profiles** > **Add**.

Step 2 Create an authorization profile for redirecting nonregistered devices that are not compliant or registered.

Step 3 Enter a name for the authorization profile that matches the MDM server name, in the **Name** field.

Step 4 Choose **ACCESS_ACCEPT** from the **Access Type** drop-down list.

Step 5 In the **Common Tasks** section, check the **Web Redirection** check box and choose **MDM Redirect** from the drop-down list.

Step 6 Choose the name of the ACL that you configured on the wireless LAN controller from the **ACL** drop-down list.

Step 7 Choose the MDM portal from the **Value** drop-down list.

Step 8 Choose the MDM server that you want to use from the **MDM Server** drop-down list.

Step 9 Click **Submit**.

What to do next

Configure Authorization Policy Rules for the MDM Use Cases.

Configure Authorization Policy Rules for the MDM Use Cases

Configure authorization policy rules in Cisco ISE to complete the MDM configuration.

Before you begin

- Add the MDM server certificate to the Cisco ISE certificate store.

- Ensure that you have created the MDM server definition in Cisco ISE. Only after you successfully integrate Cisco ISE with the MDM server does the MDM dictionary get populated, and you can create an authorization policy using the MDM dictionary attributes.
- Configure ACLs on the Cisco WLC for redirecting unregistered or noncompliant devices.

Step 1 Choose **Policy** > **Policy Sets**, and expand the policy set to view the authorization policy rules.

Step 2 Add the following rules:

- **MDM_Un_Registered_Non_Compliant**: For devices that are not yet registered with an MDM server or noncompliant with MDM policies. When a request matches this rule, the Cisco ISE MDM window is displayed to a user, with information on registering the device with the MDM server.

  Note Do not use the **MDM.MDMServerName** condition in this policy. When this condition is used, an endpoint matches the policy only if the endpoint is registered with the MDM server.

- **PERMIT**: If the device is registered with Cisco ISE, registered with MDM, and is compliant with Cisco ISE and MDM policies, it is granted access to the network based on the access control policies configured in Cisco ISE.

  The following illustration shows an example of this configuration.

Figure 7: Authorization Policy Rules for the MDM Use Cases

Step 3 Click **Save**.

Configure ACLs on Wireless Controllers for MDM Interoperability

Configure ACLs on the Wireless Controller for use in an authorization policy to redirect nonregistered devices and certificate provisioning. Your ACLs must be in the following sequence.

Step 1 Allow all outbound traffic from the server to the client.

Step 2 (Optional) Allow ICMP inbound traffic from the client to the server for troubleshooting.

Step 3 Allow access to the MDM server for unregistered and noncompliant devices to download the MDM agent and proceed with compliance checks.

Step 4 Allow all inbound traffic from the client to the server to Cisco ISE for the web portal and supplicant, and certificate provisioning flows.

Step 5 Allow inbound Domain Name System (DNS) traffic from the client to the server for name resolution.

Step 6 Allow inbound DHCP traffic from the client to the server for IP addresses.

Step 7 Deny all inbound traffic from the client to the server to corporate resources for redirection to Cisco ISE (as per your company policy).

Step 8 (Optional) Permit the rest of the traffic.

Example

The following example shows the ACLs for redirecting a nonregistered device to the BYOD flow. In this example, the Cisco ISE IP address is 10.35.50.165, the internal corporate network IP addresses are 192.168.0.0 and 172.16.0.0 (to redirect), and the MDM server subnet is 204.8.168.0.

Figure 8: ACLs for Redirecting Nonregistered Device

General

Access List Name: NSP-ACL

Deny Counters: 0

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Outbound	150720
2	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	ICMP	Any	Any	Any	Inbound	7227
3	Permit	0.0.0.0 / 0.0.0.0	204.8.168.0 / 255.255.255.0	Any	Any	Any	Any	Any	17626
4	Permit	0.0.0.0 / 0.0.0.0	10.35.50.165 / 255.255.255.255	Any	Any	Any	Any	Inbound	7505
5	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Inbound	2864
6	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DHCP Server	Any	Inbound	0
7	Deny	0.0.0.0 / 0.0.0.0	192.168.0.0 / 255.255.0.0	Any	Any	Any	Any	Inbound	0
8	Deny	0.0.0.0 / 0.0.0.0	172.16.0.0 / 255.240.0.0	Any	Any	Any	Any	Inbound	4
9	Deny	0.0.0.0 / 0.0.0.0	10.0.0.0 / 255.0.0.0	Any	Any	Any	Any	Inbound	457
10	Deny	0.0.0.0 / 0.0.0.0	173.194.0.0 / 255.255.0.0	Any	Any	Any	Any	Inbound	1256
11	Deny	0.0.0.0 / 0.0.0.0	171.68.0.0 / 255.252.0.0	Any	Any	Any	Any	Inbound	11310
12	Deny	0.0.0.0 / 0.0.0.0	171.71.181.0 / 255.255.255.0	Any	Any	Any	Any	Any	0
13	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	71819

Wipe or Lock a Device

Cisco ISE allows you to wipe or enable a pin lock for a lost device. You can configure this from the **Endpoints** window.

Step 1 Choose **Work Centers** > **Network Access** > **Identities** > **Endpoints**.

Step 2 Check the check box next to the device that you want to wipe or lock.

Step 3 From the **MDM Actions** drop-down list, choose one of the following options:

- **Full Wipe**: Depending on the MDM vendor, this option either removes the corporate apps or resets the device to the factory settings.

- **Corporate Wipe**: This option removes applications that you have configured in the MDM server policies.
- **PIN Lock**: This option locks the device.

Step 4 Click **Yes** to wipe or lock the device.

View Mobile Device Management Reports

Cisco ISE records all additions, updates, and deletions of MDM server definitions. You can view these events in the **Change Configuration Audit** report, which displays all the configuration changes from any system administrator for a selected time period.

Choose **Operations** > **Reports** > **Reports** > **Audit** > **Change Configuration Audit**. Check the entries in the **Object Type** and **Object Name** columns for the MDM server that you want to review, and click the corresponding **Event** value to view the details of the configuration event.

View Mobile Device Management Logs

You can use the **Debug Log Configuration** window to view Mobile Device Management log messages. Choose **Administration** > **System** > **Logging** > **Debug Log Configuration**. Click the radio button next to a Cisco ISE node and click **Edit**. In the new window displayed, click the radio button next to the component name **external-mdm**, and click **Edit**. The default log level for this component is **INFO**. Choose **DEBUG** or **TRACE** from the corresponding **Log Level** drop-down list, and click **Save**.