Manage Network Devices

Network Devices Definitions in Cisco ISE

A network device such as a switch or a router is an authentication, authorization, and accounting (AAA) client through which AAA service requests are sent to Cisco ISE. You must define network devices for Cisco ISE to interact with the network devices. You can configure network devices for RADIUS AAA, Simple Network Management Protocol (SNMP) for the Profiling service to collect Cisco Discovery Protocol and Link Layer Discovery Protocol attributes for profiling endpoints, and Trustsec attributes for Trustsec devices. A network device that is not defined in Cisco ISE cannot receive AAA services from Cisco ISE.

In the network device definition:

- You can configure the RADIUS protocol for RADIUS authentications. When Cisco ISE receives a RADIUS request from a network device, it looks for the corresponding device definition to retrieve the shared secret that is configured. If it finds the device definition, it obtains the shared secret that is configured on the device and matches it against the shared secret in the request to authenticate access. If the shared secrets match, the RADIUS server will process the request further based upon the policy and configuration. If they do not match, a reject response is sent to the network device. A failed authentication report is generated, which provides the failure reason.

-
- You can configure the Simple Network Management Protocol (SNMP) in the network device definition for the Profiling service to communicate with the network devices and profile endpoints that are connected to the network devices.
- You must define Trustsec-enabled devices in Cisco ISE to process requests from Trustsec-enabled devices that can be part of the Cisco Trustsec solution. Any switch that supports the Trustsec solution is an Trustsec-enabled device.

  Trustsec devices do not use the IP address. Instead, you must define other settings so that Trustsec devices can communicate with Cisco ISE.

  Trustsec-enabled devices use the Trustsec attributes to communicate with Cisco ISE. Trustsec-enabled devices, such as the Nexus 7000 series switches, Catalyst 6000 series switches, Catalyst 4000 series switches, and Catalyst 3000 series switches are authenticated using the Trustsec attributes that you define while adding Trustsec devices.

Default Network Device Definition in Cisco ISE

Cisco ISE supports the default device definition for RADIUS authentications. You can define a default network device that Cisco ISE can use if it does not find a device definition for a particular IP address. This feature enables you to define a default RADIUS shared secret and the level of access for newly provisioned devices.

Note We recommend that you add the default device definition only for basic RADIUS authentications. For advanced flows, you must add separate device definition for each network device.

Cisco ISE looks for the corresponding device definition to retrieve the shared secret that is configured in the network device definition when it receives a RADIUS request from a network device.

Cisco ISE performs the following procedure when a RADIUS request is received:

1. Looks for a specific IP address that matches the one in the request.
2. Looks up the ranges to see if the IP address in the request falls within the range that is specified.
3. If both step 1 and 2 fail, it uses the default device definition (if defined) to process the request.

Cisco ISE obtains the shared secret that is configured in the device definition for that device and matches it against the shared secret in the RADIUS request to authenticate access. If no device definitions are found, Cisco ISE obtains the shared secret from the default network device definition and processes the RADIUS request.

Create a Network Device Definition in Cisco ISE

You can create a network device definition in Cisco ISE and use the default network device definition when there is no network device definition in Cisco ISE.

Step 1 Choose **Administration** > **Network Resources** > **Network Devices**.

Step 2 Click **Add**.

Step 3 Enter the required information in the **Network Devices** section.

Step 4 Check the **Authentication Settings** check box to configure RADIUS protocol for authentication.

Step 5 (Optional) Check the **SNMP Settings** check box to configure the Simple Network Management Protocol for the Profiling service to collect device information.

Step 6 (Optional) Check the **Advanced Trustsec Settings** check box to configure a Trustsec-enabled device.

Step 7 Click **Submit**.

Related Topics

Network Devices Definitions in Cisco ISE, on page 1

Import Network Devices into Cisco ISE

You can import a list of device definitions into a Cisco ISE node using a comma-separated value (CSV) file. You must first update the imported template before you can import network devices into Cisco ISE. You cannot run an import of the same resource type at the same time. For example, you cannot concurrently import network devices from two different import files.

You can download the CSV template from the Admin portal, enter your device definition details in the template, and save it as a CSV file, which you can then import this back in to Cisco ISE.

While importing devices, you can create new records or update existing records. Cisco ISE displays the summary of the number of devices that are imported and also reports any errors that were found during the import process. When you import devices, you can also define whether you want Cisco ISE to overwrite the existing device definitions with the new definitions or stop the import process when Cisco ISE encounters the first error.

You cannot import network devices that are exported in previous releases of Cisco ISE, as the import template for these releases are different.

Step 1 Choose **Administration** > **Network Resources** > **Network Devices**.

Step 2 Click **Import**.

Step 3 Click **Browse** to choose the CSV file from the system that is running the client browser.

Step 4 Check the **Overwrite Existing Data with New Data** check box.

Step 5 Check the **Stop Import on First Error** check box.

Step 6 Click **Import**.

Related Topics

Export Network Devices from Cisco ISE, on page 4

Network Devices Import Template Format, on page 7

Export Network Devices from Cisco ISE

You can export network devices configured in Cisco ISE in the form of a CSV file that you can use to import these network devices into another Cisco ISE node.

Step 1 Choose **Administration** > **Network Resources** > **Network Devices**.

Step 2 Click **Export**.

Step 3 To export network devices, you can do one of the following:

- Check the check boxes next to the devices that you want to export, and choose **Export** > **Export Selected**.
- Choose **Export** > **Export All** to export all the network devices that are defined.

Step 4 Save the export.csv file to your local hard disk.

Related Topics

Import Network Devices into Cisco ISE, on page 3

Network Device Groups

Cisco ISE allows you to create hierarchical Network Device Groups (NDGs) that contain network devices. NDGs logically group network devices based on various criteria such as geographic location, device type, and the relative place in the network (like “Access Layer” or “Data Center,” for example).

For example, to organize your network devices by geographic location, you can group them by continent, region, and country:

- Africa -> Southern -> Namibia
- Africa -> Southern -> South Africa
- Africa -> Southern -> Botswana

You can also group network devices by device type:

- Africa -> Southern -> Botswana -> Firewalls
- Africa -> Southern -> Botswana -> Routers
- Africa -> Southern -> Botswana -> Switches

Network devices can be assigned to one or more hierarchical NDGs. Thus, when Cisco ISE passes through the ordered list of configured NDGs to determine the appropriate group to assign to a particular device, it may find that the same device profile applies to multiple Device Groups, and will apply the first Device Group matched.

Root Network Device Groups

Cisco ISE includes two predefined root NDGs: All Device Types and All Locations. You cannot edit, duplicate, or delete these predefined NDGs, but you can add new device groups under them.

You can also create a root Network Device Group (NDG), and then create child NDGs under the root group in the Network Device Groups page. When you create a new root NDG, you must provide the name and type of the NDG. This information is not required when you create a child under the root NDG.

Network Device Attributes Used By Cisco ISE in Policy Evaluation

When you create a new network device group, a new network device attribute is added to the Device dictionary defined in the system, which you can use in policy definitions. Cisco ISE allows you to configure authentication and authorization policies based on Device dictionary attributes, such as device type, location, model name, and software version that is running on the network device.

Import Network Device Groups in to Cisco ISE

You can import network device groups in to a Cisco ISE node using a comma-separated value (CSV) file. You cannot run import of the same resource type at the same time. For example, you cannot concurrently import network device groups from two different import files.

You can download the CSV template from the Admin portal, enter your device group details in the template, and save the template as a CSV file, which you can then import back into Cisco ISE.

While importing device groups, you can create new records or update existing records. When you import device groups, you can also define whether you want Cisco ISE to overwrite the existing device groups with the new groups or stop the import process when Cisco ISE encounters the first error.

Step 1 Choose **Administration** > **Network Resources** > **Network Device Groups** > **Groups**.

Step 2 Click **Import**.

Step 3 Click **Browse** to choose the CSV file from the system that is running the client browser.

Step 4 Check the **Overwrite Existing Data with New Data** check box.

Step 5 Check the **Stop Import on First Error** check box.

Step 6 Click **Import or** click the **Network Device Groups List** link to return to the Network Device Groups list page.

Export Network Device Groups from Cisco ISE

You can export network device groups configured in Cisco ISE in the form of a CSV file that you can use to import these network device groups into another Cisco ISE node.

Step 1 Choose **Administration** > **Network Resources** > **Network Device Groups** > **Groups**.

Step 2 To export the network device groups, you can do one of the following:

- Check the check boxes next to the device groups that you want to export, and choose m**Export** > **Export Selected**.
- Choose **Export** > **Export All** to export all the network device groups that are defined.

Step 3 Save the export.csv file to your local hard disk.

Related Topics

Import Network Device Groups into Cisco ISE

Import Templates in Cisco ISE

Cisco ISE allows you to import a large number of network devices and network device groups using comma-separated value (CSV) files. The template contains a header row that defines the format of the fields. The header row should not be edited, and should be used as is.

By default, you can use the Generate a Template link to download a CSV file in the Microsoft Office Excel application and save the file format locally on your system. When you click the Generate a Template link, the Cisco ISE server displays the Opening template.csv dialog. This dialog allows you to open the template.csv file and save the template.csv file locally on your system with an appropriate name for network devices and network device groups. If you choose to open the template.csv file from the dialog, the file opens in the Microsoft Office Excel application by default.

Related Topics

- Import Network Devices into Cisco ISE, on page 3
- Export Network Devices from Cisco ISE, on page 4
- Import Network Device Groups into Cisco ISE
- Export Network Device Groups from Cisco ISE, on page 6
- Network Devices Import Template Format, on page 7
- Network Device Groups Import Template Format, on page 10

Network Devices Import Template Format

The following table lists the fields in the template header and provides a description of the fields in the Network Device CSV file.

Table 1: CSV Template Fields and Description for Network Devices

Field	Description
Name:String(32):	(Required) This field is the network device name. It is an alphanumeric string, with a maximum of 32 characters in length.
Description:String(256)	This field is an optional description for the network device. A string, with a maximum of 256 characters in length.
IP Address:Subnets(a.b.c.d/m|...)	(Required) This field is the IP address and subnet mask of the network device. (It can take on more than one value separated by a pipe "|" symbol).
Model Name:String(32):	(Required) This field is the network device model name. It is a string, with a maximum of 32 characters in length.
Software Version:String(32):	(Required) This field is the network device software version. It is a string, with a maximum of 32 characters in length.
Network Device Groups:String(100):	(Required) This field should be an existing network device group. It can be a subgroup, but must include both the parent and subgroup separated by a space. It is a string, with a maximum of 100 characters, for example, Location#All Location#US
Authentication:Protocol:String(6)	This is an optional field. It is the protocol that you want to use for authentication. The only valid value is RADIUS (not case sensitive).
Authentication:Shared Secret:String(128)	(Required, if you enter a value for the Authentication Protocol field) This field is a string, with a maximum of 128 characters in length.

Field	Description
EnableKeyWrap:Boolean(true|false)	This is an optional field. It is enabled only when it is supported on the network device. Valid value is true or false.
EncryptionKey:String(ascii:16|hexa:32)	(Required, if you enable KeyWrap) Indicates the encryption key that is used for session encryption. ASCII—16 characters (bytes) long Hexadecimal—32 characters (bytes) long.
AuthenticationKey:String(ascii:20|hexa:40)	(Required, if you enable KeyWrap). Indicates the keyed Hashed Message Authentication Code (HMAC) calculation over RADIUS messages. ASCII—20 characters (bytes) long Hexadecimal—40 characters (bytes) long.
InputFormat:String(32)	Indicates encryption and authentication keys input format. Valid value is ASCII or Hexadecimal.
SNMP:Version:Enumeration (|2c|3)	This is an optional field, used by the Profiler service. It is the version of the SNMP protocol. Valid value is 1, 2c, or 3.
SNMP:RO Community:String(32)	(Required, if you enter a value for the SNMP Version field) SNMP Read Only community. It is a string, with a maximum of 32 characters in length.
SNMP:RW Community:String(32)	(Required, if you enter a value for the SNMP Version field) SNMP Read Write community. It is a string, with a maximum of 32 characters in length.
SNMP:Username:String(32)	This is an optional field. It is a string, with a maximum of 32 characters in length.
SNMP:Security Level:Enumeration(Auth|No Auth|Priv)	(Required if you choose SNMP version 3) Valid value is Auth, No Auth, or Priv.
SNMP:Authentication Protocol:Enumeration(MD5|SHA)	(Required if you have entered Auth or Priv for the SNMP security level) Valid value is MD5 or SHA.
SNMP:Authentication Password:String(32)	(Required if you have entered Auth for the SNMP security level) It is a string, with a maximum of 32 characters in length.
SNMP:Privacy Protocol:Enumeration(DES|AES128|AES192|AES256|3DES)	(Required if you have entered Priv for the SNMP security level) Valid value is DES, AES128, AES192, AES256, or 3DES.

Field	Description
SNMP:Privacy Password:String(32)	(Required if you have entered Priv for the SNMP security level) It is a string, with a maximum of 32 characters in length.
SNMP:Polling Interval:Integer:600-86400 seconds	This is an optional field to set the SNMP polling interval. Valid value is an integer between 600 and 86400.
SNMP:Is Link Trap Query:Boolean(true|false)	This is an optional field to enable or disable the SNMP link trap. Valid value is true or false.
SNMP:Is MAC Trap Query:Boolean(true|false)	This is an optional field to enable or disable the SNMP MAC trap. Valid value is true or false.
SNMP:Originating Policy Services Node:String(32)	This is an optional field. Indicates which ISE server to be used to poll for SNMP data. By default, it is automatic, but you can overwrite the setting by assigning different values.
Trustsec:Device Id:String(32)	This is an optional field. It is the Trustsec device ID, and is a string, with a maximum of 32 characters in length.
Trustsec:Device Password:String(256)	(Required if you have entered Trustsec device ID) This is the Trustsec device password and is a string, with a maximum of 256 characters in length.
Trustsec:Environment Data Download Interval:Integer:1-2147040000 seconds	This is an optional field. It is the Trustsec environment data download interval. Valid value is an integer between 1 and 24850.
Trustsec:Peer Authorization Policy Download Interval:Integer:1-2147040000 seconds	This is an optional field. It is the Trustsec peer authorization policy download interval. Valid value is an integer between 1 and 24850.
Trustsec:Reauthentication Interval:Integer:1-2147040000 seconds	This is an optional field. It is the Trustsec reauthentication interval. Valid value is an integer between 1 and 24850.
Trustsec:SGACL List Download Interval:Integer:1-2147040000 seconds	This is an optional field. It is the Trustsec SGACL list download interval. Valid value is an integer between 1 and 24850.
Trustsec:Is Other Trustsec Devices Trusted:Boolean(true|false)	This is an optional field. Indicates whether Trustsec is trusted. Valid value is true or false.
Trustsec:Notify this device about Trustsec configuration changes:String(ENABLE_ALL|DISABLE_ALL)	This is an optional field. Notifies Trustsec configuration changes to the Trustsec device. Valid value is ENABLE_ALL or DISABLE_ALL

Field	Description
Trustsec:Include this device when deploying Security Group Tag Mapping Updates:Boolean(true|false)	This is an optional field. It is the Trustsec device included on SGT. Valid value is true or false.
Deployment:Execution Mode Username:String(32)	This is an optional field. It is the username that has privileges to edit the device configuration. It is a string, with a maximum of 32 characters in length.
Deployment:Execution Mode Password:String(32)	This is an optional field. It is the device password and is a string, with a maximum of 32 characters in length.
Deployment:Enable Mode Password:String(32)	This is an optional field. It is the enable password of the device that would allow you to edit its configuration and is a string, with a maximum of 32 characters in length.
Trustsec:PAC issue date:Date	This is the field that displays the issuing date of the last Trustsec PAC that has been generated by Cisco ISE for the Trustsec device.
Trustsec:PAC expiration date:Date	This is the field that displays the expiration date of the last Trustsec PAC that has been generated by Cisco ISE for the Trustsec device.
Trustsec:PAC issued by:String	This is a field that displays the name of the issuer (a Trustsec administrator) of the last Trustsec PAC that has been generated by Cisco ISE for the Trustsec device. It is a string.

Network Device Groups Import Template Format

The following table lists the fields in the template header and provides a description of the fields in the Network Device Group CSV file.

Table 2: CSV Template Fields and Description for Network Device Groups

Field	Description
Name:String(100):	(Required) This field is the network device group name. It is a string with a maximum of 100 characters in length. The full name of an NDG can have a maximum of 100 characters in length. For example, if you are creating a subgroup India under the parent groups Global > Asia, then the full name of the NDG that you are creating would be Global#Asia#India and this full name cannot exceed 100 characters in length. If the full name of the NDG exceeds 100 characters in length, the NDG creation fails.

Field	Description
Description:String(1024)	This is an optional network device group description. It is a string, with a maximum of 1024 characters in length.
Type:String(64):	(Required) This field is the network device group type. It is a string, with a maximum of 64 characters in length.
Is Root:Boolean(true|false):	(Required) This is a field that determines if the specific network device group is a root group. Valid value is true or false.

Mobile Device Manager Interoperability with Cisco ISE

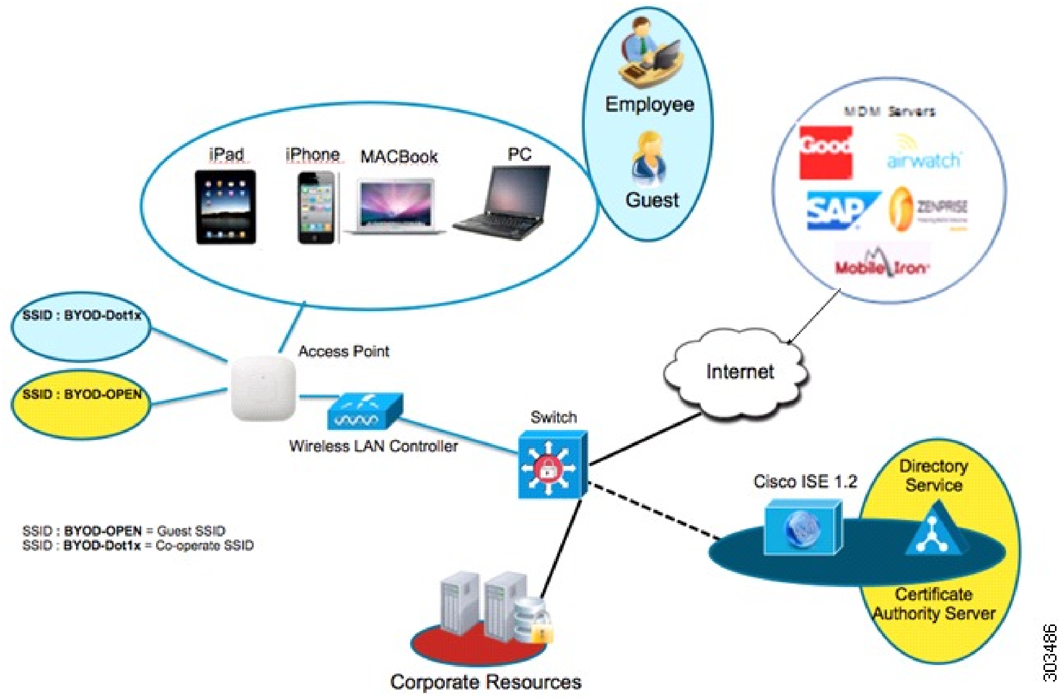
Mobile Device Management (MDM) servers secure, monitor, manage, and support mobile devices deployed across mobile operators, service providers, and enterprises. MDM servers act as a policy server that controls the use of some applications on a mobile device (for example, an e-mail application) in the deployed environment. However, the network is the only entity that can provide granular access to endpoints based on ACLs. Cisco ISE queries the MDM servers for the necessary device attributes to create ACLs that provide network access control for those devices.

You can run multiple active MDM servers on your network, including ones 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 Cisco's MDM API version 2 to allow devices access the network over VPN via AnyConnect 4.1 and Cisco ASA 9.3.2 or later.

In this 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



The following table lists the components that are used in the MDM setup.

Table 3: Components Used in the MDM Setup

Component	Specification
Cisco Identity Services Engine, Release 1.3 Cisco Identity Services Engine, Release 1.4	Any of the following: ISE 3315, 3355, 3395, 3415, 3495, or VMware
MDM Server	—
(*Optional*) Certificate Authority Server	As per Microsoft specification (Windows 2008 R2 Enterprise SP2, Windows 2012 R2)
Wireless LAN Controller (WLC)	• Hardware: 5500 Series, 2500 Series, WLSM-2 • Software: Unified Wireless Network Software, Release 7.2, WLC 8.1
Mobile Devices	Devices supported by the MDM vendor. For example, Apple iOS 5.0 and higher, Google Android 3.x and higher.

You can configure Cisco ISE to interoperate with an external Mobile Device Manager (MDM) server. By setting up this type of third-party connection, you can leverage the detailed information available in the MDM database. Cisco ISE uses REST API calls over HTTPS to pull the various pieces of information from the external MDM server. Cisco ISE applies appropriate access control policies to switches, access routers, wireless access points, and other network access points to achieve greater control of remote device access to your Cisco ISE network.

You can configure Cisco ISE to interoperate with one or more external Mobile Device Manager (MDM) servers. By setting up this type of third-party connection, you can leverage 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 appropriate access control policies to switches, access routers, wireless access points, and other network access points to achieve greater control of remote device access to your Cisco ISE network.

The supported MDM vendors are listed here: Supported MDM Servers, on page 14.

Supported MDM Use Cases

The functions Cisco ISE performs in conjunction with the external MDM server are as follows:

- Facilitating device registration—Unregistered endpoints accessing the network are redirected to a registration page hosted on the MDM server for registration based on user role, device type, and so on.
- Handling device remediation—Endpoints are granted only restricted access.
- Augmenting endpoint data—Update the endpoint database with information from the MDM server that you cannot gather using the Cisco ISE Profiler. Cisco ISE uses six device attributes you can view using the **Administration** > **Identity Management** > **Identities** > **Endpoints** page if an endpoint is a MDM monitored device. For example:
    - MDMImei: 99 000100 160803 3
    - MDMManufacturer: Apple
    - MDMModel: iPhone
    - MDMOSVersion: iOS 6.0.0
    - MDMPhoneNumber: 9783148806
    - MDMSerialNumber: DNPGQZGUDTF9
- Cisco ISE polls the MDM server once every four hours for device compliance data. This is configurable by the administrator.
- Issuing device instructions through the MDM server—Issues remote actions for users' devices through the MDM server. Administrators initiate remote actions from the ISE console.

Cisco ISE allows you to configure MDM policy based on the following attributes:

- DeviceRegisterStatus
- DeviceCompliantStatus
- DiskEncryptionStatus
- PinLockStatus

- JailBrokenStatus
- Manufacturer
- IMEI
- SerialNumber
- OsVersion
- PhoneNumber
- MDMServerName
- MDMServerReachable
- MEID
- Model
- UDID

Supported MDM Servers

Supported MDM servers include products from the following vendors:

- Airwatch, Inc.
- Good Technology
- MobileIron, Inc.
- Zenprise, Inc.
- SAP Afaria
- Fiberlink MaaS
- Meraki

Ports Used by the MDM Server

The following table lists the ports that must be open between the Cisco ISE and the MDM server to enable them to communicate with each other. Refer to the MDM Server Documentation for a list of ports that must be open on the MDM agent and server.

Table 4: Ports Used by the MDM Server

MDM Server	Ports
Mobile Iron	443
Zenprise	443
Good	19005

MDM Server	Ports
Airwatch	443
Afaria	443
Fiberlink MaaS	443
Meraki	443
Microsoft Intune	80 and 443
Microsoft SCCM	80 and 443

MDM Dictionary Attributes

After you add the MDM server definition in Cisco ISE, the MDM dictionary attributes are available in Cisco ISE that you can use in authorization policies. You can view the dictionary attributes that are available for use in authorization policies.

When you are using these MDM dictionary attributes in policies, you cannot delete the MDM server configuration from Cisco ISE. To remove the MDM server configuration, you must first remove the MDM dictionary attributes from policies, and then remove the MDM server from Cisco ISE.

MDM Integration Process Flow

This section describes the MDM integration process:

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

Note The input parameter is the MAC address of the endpoint device. For off-premise Apple iOS devices, this is the UDID.

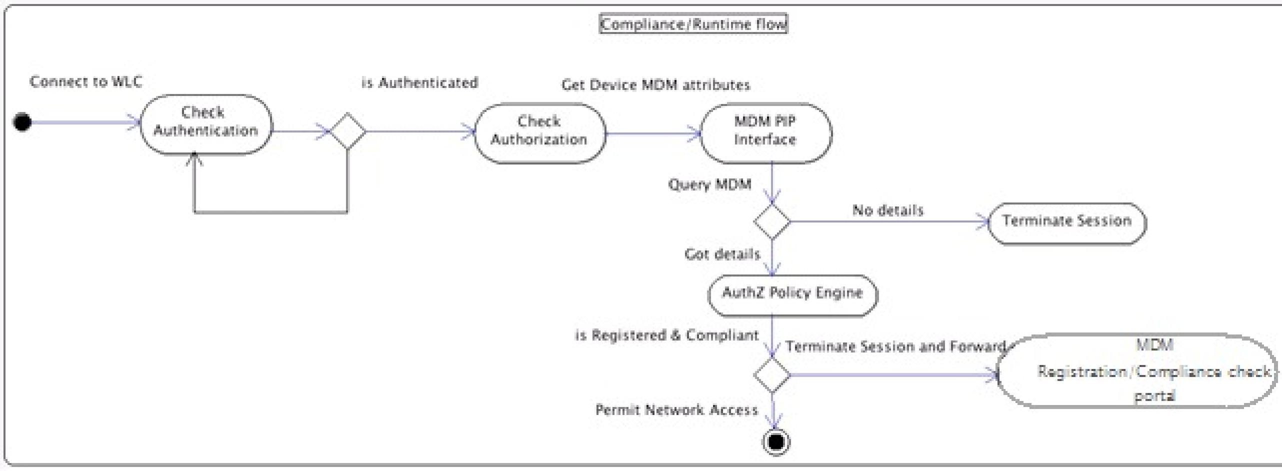
4. If the user's device is not in this list, it means the device is not registered. Cisco ISE sends an authorization request to the NAD to redirect to Cisco ISE. The user is presented the MDM server page.

Note A device that was enrolled on the MDM server outside of a Cisco ISE network will be automatically registered with Cisco ISE if it is compliant with the posture policies.

5. Cisco ISE uses MDM to provision the device and presents an appropriate page 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 to the posture (compliance) policies configured on the MDM server, the user is notified that the device is out of compliance and must be compliant.
9. After the user’s device becomes compliant, the MDM server updates the device 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 once every four hours to get compliance information and issues Change of Authorization (CoA) appropriately. This can be configured by the administrator. Cisco ISE also checks the MDM server every 5 minutes to make sure that it is available.

The following figure illustrates the MDM process flow.



Note A device can only be enrolled to 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 Settings > General >Device management, and click remove management. Or the user can go to the MyDevices portal in ISE, and click corporate wipe.

Set Up MDM Servers With Cisco ISE

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

Step 1 Import MDM server certificate into Cisco ISE.

Step 2 Create mobile device manager definitions.

Step 3 Configure ACLs on the Wireless LAN Controllers.

Step 4 Configure authorization profile for redirecting non-registered devices.

Step 5 If there are more than one MDM server on the network, configure separate authorization profiles for each vendor.

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

Import MDM 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 Certificate Store. If your MDM server has a CA-signed certificate, you must import the root CA into the Cisco ISE Certificate Store.

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 Click **Browse** to select the MDM server certificate that you obtained from the MDM server.

Step 4 Add a friendly name.

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

Step 6 Click **Submit**.

Step 7 Verify that the Certificate Store list page lists the MDM server certificate.

Set Permissions When AD User in the Domain Admin Group

For Windows 2008 R2,Windows 2012, and Windows 2012 R2, the Domain Admin group does not have full control on certain registry keys in the Windows operating system by default. The Active Directory admin must give the 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}**

No registry changes are required for the following Active Directory versions:

- Windows 2003

- Windows 2003R2
- Windows 2008

To grant full control, the Active Directory admin must first take ownership of the key, as shown below.

Step 1 Go to the Owner tab by right clicking the key.

Step 2 Click **Permissions**.

Step 3 Click **Advanced**.

Required Permissions When AD User Not in Domain Admin Group

For Windows 2012 R2, give the 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 permissions also are required when an Active Directory user is not in the Domain Admin group, but is in the Domain Users group:

- Add Registry Keys to Allow ISE to Connect to the Domain Controller (see below)
- Permissions to Use DCOM on the Domain Controller
- Set Permissions for Access to WMI Root/CIMv2 Name Space
- Grant Access to the Security Event Log on the AD Domain Controller

These permissions are only required for the following Active Directory versions:

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

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

You must manually add some registry keys to the domain controller to allow ISE to connect as a Domain User, and retrieve login authentication events. An agent is not required on the domain controllers or on any machine 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 key **DllSurrogate**.

Keep the empty lines as shown in the script above, including an empty line at the end of the file.

Permissions to Use DCOM on the Domain Controller

The Active Directory user used for ISE ID Mapping must have permissions to use DCOM (remote COM) on the Domain Controller. You can configure permissions with the **dcomcnfg** command line tool.

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

Step 2 Expand Component Services.

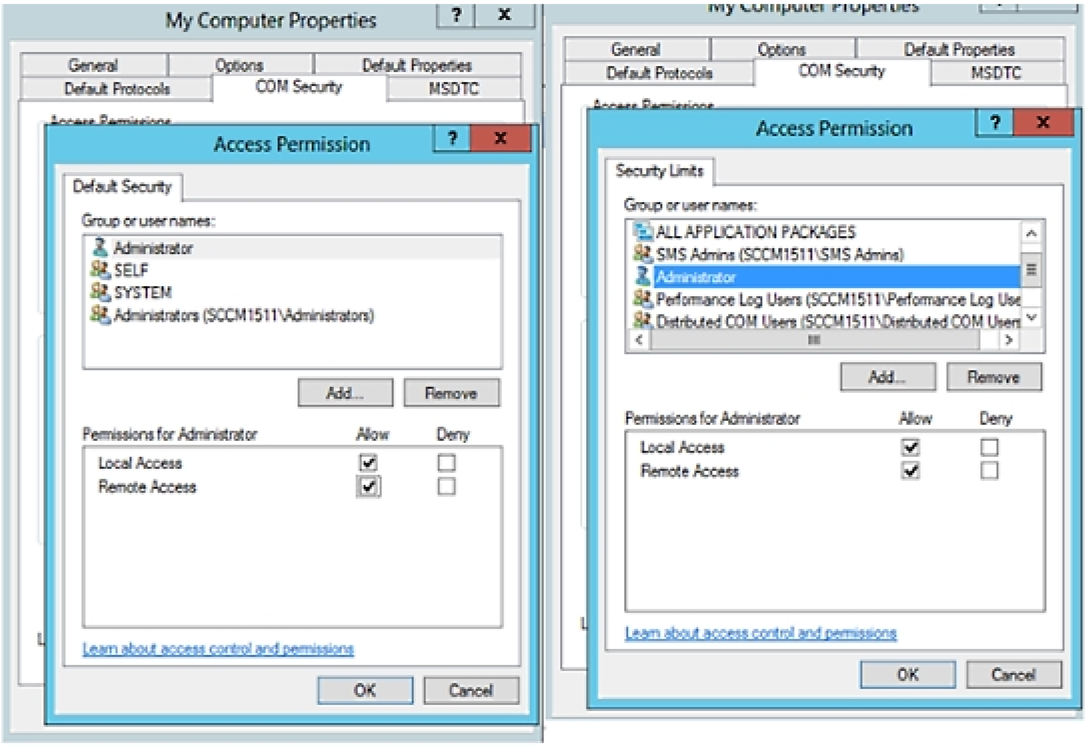
Step 3 Expand **Computers** > **My Computer**.

Step 4 Select Action from the menu bar, click **properties**, and click **COM Security**.

Step 5 Make sure that the account that ISE will use for both Access and Launch has Allow permissions. That Active Directory user should be added 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 access for both Access Permissions and Launch and Activation Permissions.

Figure 2: Local and Remote Access for Access Permissions



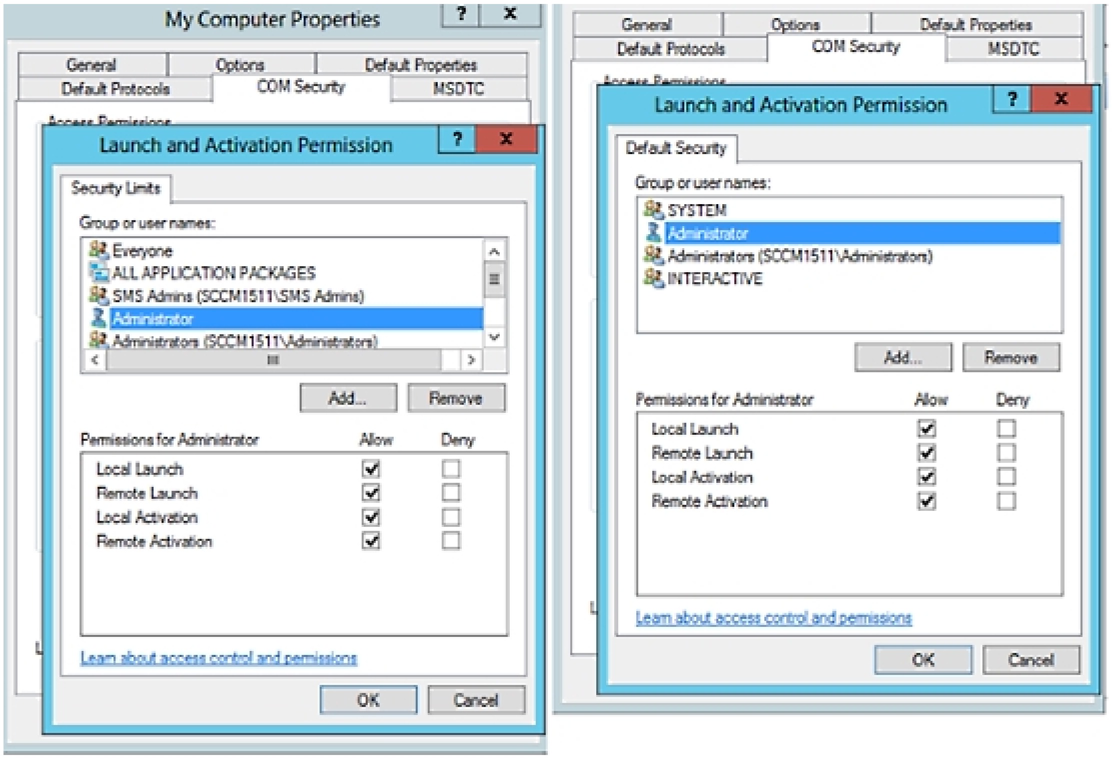
Default Security — Permissions for Administrator:

	Allow	Deny
Local Access	☑	□
Remote Access	☑	□

Security Limits — Permissions for Administrator:

	Allow	Deny
Local Access	☑	□
Remote Access	☑	□

Figure 3: Local and Remote Access for Launch and Activation Permissions



Group or user names:

- Everyone
- ALL APPLICATION PACKAGES
- SMS Admins (SCCM1511\SMS Admins)
- Administrator
- Administrators (SCCM1511\Administrators)

Permissions for Administrator	Allow	Deny
Local Launch	☑	☐
Remote Launch	☑	☐
Local Activation	☑	☐
Remote Activation	☑	☐

Group or user names:

- SYSTEM
- Administrator
- Administrators (SCCM1511\Administrators)
- INTERACTIVE

Permissions for Administrator	Allow	Deny
Local Launch	☑	☐
Remote Launch	☑	☐
Local Activation	☑	☐
Remote Activation	☑	☐

Set Permissions for Access to WMI Root/CIMv2 Name Space

By default, 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 Click Start > Run and type `wmimgmt.msc`.

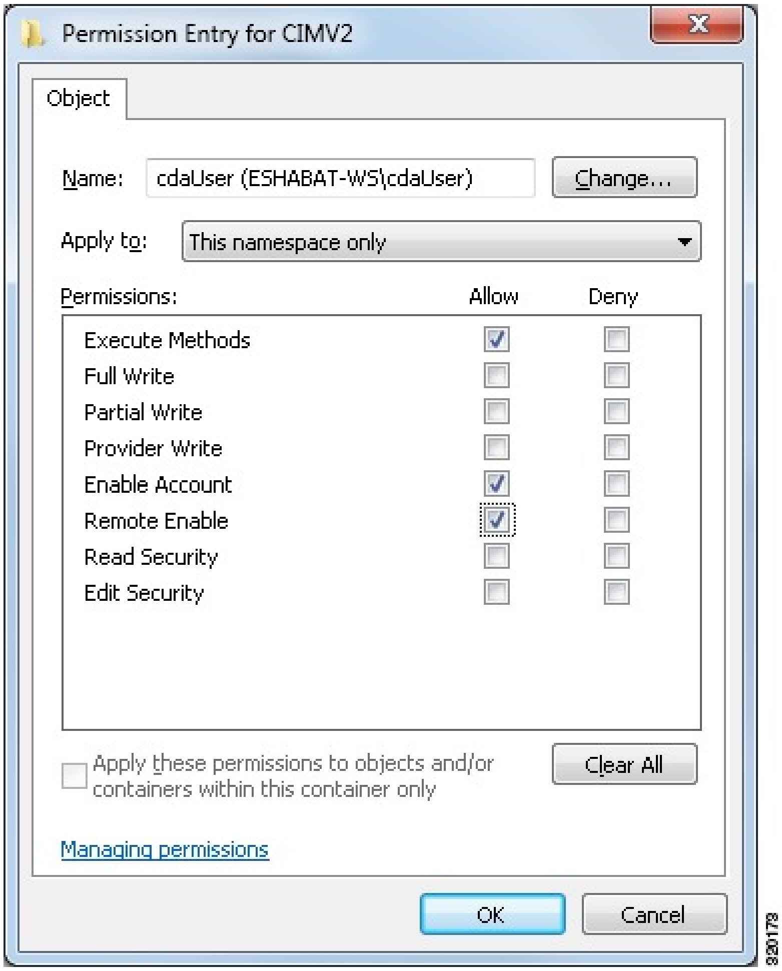
Step 2 Right-click WMI Control and click **Properties**.

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

Step 4 Click **Security**.

Step 5 Add the Active Directory user, and configure the required permissions as shown below.

Figure 4: Required Permissions for WMI Root\CIMv2 Name Space



Permission Entry for CIMV2

Object

Name: cdaUser (ESHABAT-WS\cdaUser)

Apply to: This namespace only

Permissions:	Allow	Deny
Execute Methods	☑	□
Full Write	□	□
Partial Write	□	□
Provider Write	□	□
Enable Account	☑	□
Remote Enable	☑	□
Read Security	□	□
Edit Security	□	□

□ Apply these permissions to objects and/or containers within this container only

Open Firewall Ports for WMI Access

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

- TCP 135: General RPC Port. When doing 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: SMB

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 specific IP (ISE IP).

Configure an Authorization Profile for Redirecting Nonregistered Devices

You must configure an authorization profile in Cisco ISE to redirect 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 ISE with the MDM server does the MDM dictionary gets populated and you can create authorization policy using the MDM dictionary attributes.
- Configure ACLs on the Wireless LAN Controller for redirecting unregistered devices.
- If you are using a proxy for the internet connection and MDM server is part of internal network then you have to put the MDM server name or its IP address in the Proxy-Bypass list. Choose **Administration** > **Settings** > **Proxy Settings** 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.

Step 4 Choose ACCESS_ACCEPT as the Access Type.

Step 5 Check the **Web Redirection** check box and choose MDM Redirect from the drop-down list.

Step 6 Enter the name of the ACL that you configured on the wireless LAN controller in the ACL field.

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

Step 8 Select the MDM server you want to use from the drop-down list.

Step 9 Click **Submit**.

What to Do Next

Configure Authorization Policy Rules for the MDM Use Cases.

Related Topics

Configure Authorization Policy Rules for the MDM Use Cases, on page 24

Configure Authorization Policy Rules for the MDM Use Cases

You must 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 ISE with the MDM server, the MDM dictionary gets populated and you can create authorization policy using the MDM dictionary attributes.
- Configure ACLs on the Wireless LAN Controller for redirecting unregistered or noncompliant devices.

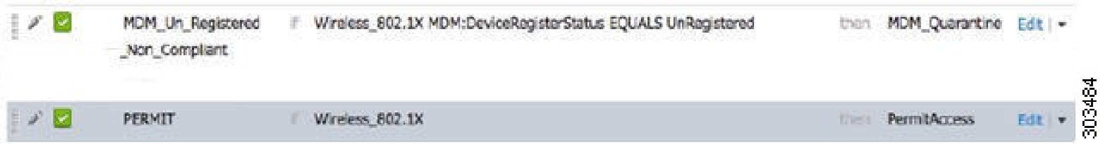
Step 1 Choose **Policy** > **Authorization** > **Insert New Rule Below**.

Step 2 Add the following rules:

- MDM_Un_Registered_Non_Compliant—For devices that are not yet registered with an MDM server or compliant with MDM policies. Once a request matches this rule, the ISE MDM page appears with information on registering the device with MDM.
- PERMIT—If the device is registered with Cisco ISE, registered with MDM, and is compliant with Cisco ISE and MDM policies, it will be 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 5: Authorization Policy Rules for the MDM Use Cases



☑	MDM_Un_Registered_Non_Compliant	if	Wireless_802.1X MDM:DeviceRegisterStatus EQUALS UnRegistered	then	MDM_Quarantine	Edit ▾
☑	PERMIT	if	Wireless_802.1X	then	PermitAccess	Edit ▾

Step 3 Click **Save**.

Related Topics

Import MDM Server Certificate into Cisco ISE, on page 17

Wipe or Lock a Device

Cisco ISE allows you to wipe or turn on pin lock for a device that is lost. You can do this from the Endpoints page.

Step 1 Choose **Administration** > **Identity Management** > **Identities** > **Endpoints** .

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

Step 3 From the MDM Access drop-down list, choose any 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—Removes applications that you have configured in the MDM server policies
- PIN Lock—Locks the device

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

View Mobile Device Manager Reports

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

Choose **Operations** > **Reports** > **Change Configuration Audit** > **MDM**, and specify the period of time to display in the resulting report.

Related Topics

Mobile Device Manager Interoperability with Cisco ISE, on page 11
Supported MDM Use Cases, on page 13
View Mobile Device Manager Logs, on page 25
Supported MDM Servers, on page 14

View Mobile Device Manager Logs

You can use the Message Catalog page to view Mobile Device Manager log messages. Choose **Administration** > **System** > **Logging** > **Message Catalog**. The default reporting level for MDM log entries is "INFO." You can change the reporting level to "DEBUB" or "TRACE."

Related Topics

Mobile Device Manager Interoperability with Cisco ISE, on page 11
Supported MDM Use Cases, on page 13
View Mobile Device Manager Reports, on page 25

Supported MDM Servers, on page 14