Define Network Devices 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 or TACACS 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 select the vendor profile that fits the network device. The profile includes pre-defined configurations for the device, such as settings for URL direct and change of authorization.

- 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 TACACS+ protocol for TACACS+ authentications. When Cisco ISE receives a TACACS+ 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 TACACS+ 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.

Note
When you configure a network device on Cisco ISE, we recommend that you do not include a backslash (\) in the shared secret. This is because when you upgrade Cisco ISE the backslash will not appear in the shared secret. Note, however, that if you reimage Cisco ISE instead of upgrading it, the backslash appears in the shared secret.

Support for Session Aware Networking (SAnet)

Cisco ISE provides limited support for Session Aware Networking (SAnet). SAnet is a session management framework that runs on many Cisco switches. SAnet manages access sessions, including visibility, authentication, and authorization. SAnet uses a service template, which contains RADIUS authorization attributes. Cisco ISE includes a service template inside an authorization profile. Cisco ISE identifies service templates in an authorization profile using a flag that identifies the profile as “Service Template” compatible.

Cisco ISE authorization profiles contain RADIUS authorization attributes that are transformed into a list of attributes. SAnet service templates also contain of RADIUS authorization attributes, but those attributes are not transformed into a list.

For SAnet devices, Cisco ISE sends the name of the service template. The device downloads the content of the service template, unless it already has that content in a cache or statically defined configuration. Cisco ISE sends a CoA notification to the device when a service template changes RADIUS attributes.
Define a Default Network Device in Cisco ISE

Cisco ISE supports the default device definition for RADIUS and TACACS 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 or TACACS 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 and TACACS 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 or TACACS request from a network device.

Cisco ISE performs the following procedure when a RADIUS or TACACS 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 or TACACS 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 or TACACS request.

Add a Network Device in Cisco ISE

You can add a network device in Cisco ISE or use the default network device.

You can also add the network device in the Work Centers > Device Administration > Network Resources > Network Devices page.

Before you begin
Make sure that the AAA function is enabled on the network devices. To know more, refer Command to Enable AAA Functions

Step 1 Choose Administration > Network Resources > Network Devices.
Step 2 Click Add.
Step 3 Enter the Name of the network device.
Step 4 Enter the IP address.
Step 5 (Optional) Check the RADIUS Authentication Settings check box to configure the RADIUS protocol for authentication.
Step 6 (Optional) Check the TACACS Authentication Settings check box to configure the TACACS protocol for authentication.
Step 7 (Optional) Check the SNMP Settings check box to configure the Simple Network Management Protocol for the Profiling service to collect device information.
Step 8 (Optional) Check the Advanced Trustsec Settings check box to configure a Trustsec-enabled device.
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.

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 9 Click Submit.

---

### 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.

### 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.

---
Third-Party Network Device Support in Cisco ISE

Cisco ISE supports third-party network access devices (NADs) through the use of network device profiles. NAD profiles define the capabilities of the third-party device with simplified policy configuration, regardless of the vendor-side implementation. A network device profile contains the following:

- The protocols the network device support, such as RADIUS, TACACS+, and TrustSec. You can import any vendor-specific RADIUS dictionaries that exist for the device into Cisco ISE.

- The attributes and values that the device uses for the various flows such as Wired MAB and 802.1x. This allows Cisco ISE to detect the right flow type for your device according to the attributes it uses.

- The Change of Authorization (CoA) capabilities the device has. While RFC 5176 defines the types of CoA requests, the required attributes in the requests vary depending on the device. Most non-Cisco devices with RFC 5176 support will also support the "Push" and "Disconnect" functions. For devices that do not support the RADIUS CoA type, ISE also supports SNMP CoA. CoA types are described in further detail below.

- The attributes and protocols the device uses for MAB. Network devices from different vendors perform MAB authentication differently.

- The VLAN and ACL permissions used by the device. After the profile is saved, Cisco ISE automatically generates authorization profiles for each configured permission.

- URL redirection is necessary for advanced flows like BYOD, Guest, and Posture. There are two types of URL redirection found on a device: static and dynamic. For static URL redirection, you can copy and paste the ISE portal URL into the configuration. For dynamic URL redirection, ISE uses a RADIUS attribute to tell the network device where to redirect to. In addition, if the device supports neither dynamic nor static URL redirect, ISE provides an Auth VLAN by which it simulates URL redirect. Auth VLAN is based on a DHCP/DNS service running on the ISE box. To create the Auth VLAN, define the DHCP/DNS service settings. For more information, see the DHCP and DNS Services section in see DHCP and DNS services. The URL redirect flow is described in further detail below.

Once you have defined your devices in ISE, configure these device profiles or used the preconfigured device profiles offered by ISE in order to define the capabilities that Cisco ISE uses to enable basic flows, as well as advanced flows such as Profiler, Guest, BYOD, MAB, and Posture.

URL Redirect Mechanism and Auth VLAN

When a third-party device is used in the network and the device does not support dynamic or static URL redirect, ISE simulates the URL redirect flow. The URL redirect simulation flow for such devices is operated by running a DHCP/DNS service on the ISE box (For more information, see the DHCP and DNS Services section in see DHCP and DNS services), and the Auth VLAN flow is as follows:

1. A guest endpoint connects to the NAD.
2. The device sends the RADIUS/MAB request to ISE.
3. ISE runs the authentication/authorization policy and stores the user accounting information.
4. ISE sends the RADIUS access/accept message, containing the Auth VLAN ID.
5. The guest endpoint receives network access.
6. The endpoint broadcasts a DHCP request and obtains a client IP address and the ISE sinkhole DNS IP address from the ISE DHCP service.

7. The guest endpoint opens a browser. The browser sends a DNS query and receives the ISE IP address.

8. The endpoint HTTP or HTTPS request is directed to the ISE box.

9. ISE responds with HTTP 301/Moved, providing the guest portal URL. The endpoint browser redirects to the Guest portal page.

10. The guest endpoint user logs in for authentication.

11. Once compliance is validated, ISE responds to the NAD, sending the CoA, authorizing the endpoint and bypassing the sinkhole.

12. Appropriate access is provided to the user based on the CoA, the endpoint receives an IP address from an enterprise DHCP and the user can now use the network.

The Auth VLAN should be separated from the corporate network in order to prevent unauthorized network access by the guest endpoint before the endpoint passes authentication. Configure the Auth VLAN IP helper to point to the ISE machine, or connect one of the ISE network interfaces to the Auth VLAN. For more information about VLAN (DHCP/DNS server) settings, see the DHCP and DNS Services section in see DHCP and DNS Services. Multiple VLANs may be connected to one network interface card by configuring a VLAN IP-helper from the NAD configuration. For more information about configuring an IP helper, refer to the administration guide for the device for instructions. In addition, for Guest flows, define a guest portal and select that portal in an Authorization profile that is bound to MAB authorization, similar to regular Guest flows. For more information about guest portals, see the Cisco ISE Guest Services section in see Cisco ISE Guest Services.

The following diagram displays the basic network setup when an Auth VLAN is defined (the Auth VLAN is connected directly to the Cisco ISE node):

**Figure 1: Auth VLAN connect to Cisco ISE Node**

The following diagram displays the network with Auth VLAN and an IP helper:
CoA Types

ISE supports both RADIUS and SNMP CoA types. RADIUS or SNMP CoA type support is required in order for the NAD to work in complex flows, while it is not mandatory for basic flows. Define the RADIUS and SNMP settings supported by the device when configuring the NAD from ISE, and indicate the CoA type to be used for a specific flow when configuring the NAD profile. For more information about defining protocols for your NADs, see the Network Devices section in see Network Devices. Check with your third party supplier to verify which type your NAD supports prior to creating the device and NAD profile in ISE.

Network Device Profiles

Cisco ISE supports some third-party network access devices (NADs) through the use of network device profiles. These profiles define the capabilities that Cisco ISE uses to enable basic flows, and advanced flows such as Guest, BYOD, MAB, and Posture.

Cisco ISE includes predefined profiles for network devices from several vendors. Cisco ISE 2.1 has been tested with the vendor devices listed in the following table:

Table 1: Vendor Devices Tested With Cisco ISE 2.1

<table>
<thead>
<tr>
<th>Device Type</th>
<th>Vendor</th>
<th>CoA Type</th>
<th>URL Redirect Type</th>
<th>Supported/Validated Use Cases</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>802.1X/MAB</td>
<td>Profiler without CoA</td>
</tr>
</tbody>
</table>

Figure 2: Auth VLAN with IP Helper
<table>
<thead>
<tr>
<th>Wireless</th>
<th>Vendor</th>
<th>Authentication Method</th>
<th>URL Type</th>
<th>Requires CoA support</th>
<th>Requires URL redirect</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aruba 7000, InstantAP</td>
<td>RADIUS</td>
<td>Static URL</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Motorola RFS 4000</td>
<td>RADIUS</td>
<td>Dynamic URL</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>HP 830</td>
<td>RADIUS</td>
<td>Static URL</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Ruckus ZD 1200</td>
<td>RADIUS</td>
<td>—</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Wired</th>
<th>Vendor</th>
<th>Authentication Method</th>
<th>URL Type</th>
<th>Requires CoA support</th>
<th>Requires URL redirect</th>
</tr>
</thead>
<tbody>
<tr>
<td>HP A5500</td>
<td>RADIUS</td>
<td>Auth VLAN provided by ISE</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>HP 3800 and 2920 (ProCurve)</td>
<td>RADIUS</td>
<td>Auth VLAN provided by ISE</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Alcatel 6850</td>
<td>SNMP</td>
<td>Dynamic URL</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Brocade ICX 6610</td>
<td>RADIUS</td>
<td>Auth VLAN provided by ISE</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Juniper EX3300-24p</td>
<td>RADIUS</td>
<td>Auth VLAN provided by ISE</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

For additional third-party NADs, you must identify the device properties and capabilities and create custom NAD profiles in Cisco ISE.

You can create custom NAD profiles for additional third-party network devices that do not have a predefined profile. For advanced flows such as Guest, BYOD, and Posture, the device needs to support RFC 5176, "Change of Authorization" (CoA) Support for these flows depends on the NAD's capabilities. You may need to refer to the device's administration guide for information on many of the attributes required for a network device profile.
If you have deployed non-Cisco NADs prior to Release 2.0 and created policy rules/RADIUS dictionaries to use them, after upgrade these will continue to work as usual.

ISE Community Resource
For information about third-party NAD profiles, see ISE Third-Party NAD Profiles and Configs.

Configure Third-Party Network Device in Cisco ISE

Cisco ISE supports third-party network access devices (NADs) through the use of network device profiles. These profiles define the capabilities that Cisco ISE uses to enable flows such as Guest, BYOD, MAB, and Posture.

Before you begin

Read the definition for Network Device Profiles, on page 7 in the Cisco Identity Services Engine Administration Guide.

Step 1
Ensure your device is configured in ISE. If you are configuring Guest, BYOD, or Posture workflows, ensure Change of Authorization (CoA) is defined and the NAD’s URL redirect mechanism is configured to point at the relevant ISE Portal. For the URL redirect, you can copy the ISE portal URL from the portal’s landing page. For more information about configuring CoA types and URL redirect for the NAD in ISE, see the Network Devices section in see Network Devices. In addition, refer to the third party device’s administration guide for instructions.

Step 2
Ensure an appropriate NAD profile for your device is available in ISE. To view existing profiles, choose Administration > Network Resources > Network Device Profiles. If an appropriate profile does not already exist in ISE, create a custom profile. See Create a Network Device Profile, on page 9 for information on how to create custom profiles.

Step 3
Assign a NAD profile to the NAD that you want to configure. Choose Administration > Network Resources > Network Devices. Open the device to which you would like to assign a profile and from Device Profile, select the correct profile from the dropdown list.

Step 4
When you configure your policy rules, the authorization profile should be explicitly set to the NAD profile in step 1, or “Any” if you are just using VLAN or ACL or if you have different devices from different vendors in your network. To set the NAD profile for the authorization profile, choose Policy > Policy Elements > Results > Authorization > Authorization Profiles. Open the relevant authorization profile and from Network Device Profile, select the relevant NAD profile from the dropdown list. When using Auth VLAN for Guest flows, you should also define a guest portal and select that portal in an Authorization profile that is bound to MAB authorization, similar to regular Guest flows. For more information about guest portals, see the Cisco ISE Guest Services section in see Cisco ISE Guest Services.

Create a Network Device Profile

Before you begin

• For more information about creating a custom profile, read the Network Access Device Profiles with Cisco Identity Services Engine document.

• Most NADs have a vendor-specific RADIUS dictionary that provides a number of vendor-specific attributes in addition to the standard IETF RADIUS attributes. If the network device has a vendor-specific RADIUS dictionary, import it into Cisco ISE. Refer to the third party device’s administration guide for
instructions on which RADIUS dictionary is required. From ISE, choose Policy Elements > Dictionaries > System > Radius > RADIUS Vendors. For more information about importing RADIUS dictionaries, see the Create RADIUS-Vendor Dictionaries section in see Create RADIUS-Vendor Dictionaries.

- For complex flows such as Guest and Posture, the device needs to support RFC 5176, Change of Authorization (CoA)
- For more information about the fields and possible values for creating a network device profile, see the Network Device Profiles Settings section in see Network Device Profile Settings.

### Step 1
Choose Administration > Network Resources > Network Device Profiles.

### Step 2
Click Add.

### Step 3
Enter a name and description for the network device.

### Step 4
Select the vendor of the network device.

### Step 5
Check the check boxes for the protocols that the device supports. Check each box if your device supports RADIUS, TACACS+ and/or TrustSec. It is only necessary to check the protocols you want to actually use. If the device supports RADIUS, select the RADIUS dictionary to use with the network device from the dynamic dropdown list in the RADIUS Dictionaries field.

### Step 6
From the Templates section, enter relevant details as follows:

a) From Authentication/Authorization configure the device's default settings for flow types, attribute aliasing, and host lookup: From Flow Type Conditions, enter the attributes and values that your device uses for the various flows such as Wired MAB, or 802.1x. This enables ISE to detect the correct flow type for your device according to the attributes it uses. There is no IETF standard for MAB and different vendors use different values for Service-Type. Refer to the device's user guide or use a sniffer trace of a MAB authentication to determine the correct settings. From Attribute Aliasing, map device specific attribute names to common names to simplify policy rules. Currently, only SSID is defined. If you device has the concept of wireless SSID and then to set this to the attribute it uses. ISE maps this to an attribute called SSID in the Normalised Radius dictionary. This simplifies policy rule configuration as you can refer to SSID in one rule and it will work for multiple devices even if the underlying attributes are different. From Host Lookup, enable the Process Host Lookup option and select the relevant MAB protocols and attributes for your device, based on the third-party instructions.

b) From Permissions configure the network device's default settings for VLAN and ACL. These are automatically mapped based on the authorization profiles you created in ISE.

c) From Change of Authorization (CoA) configure the device's CoA capabilities.

d) Expand the Redirect section to configure the device's URL redirect capabilities. URL redirection is necessary for Guest, BYOD, and Posture.

### Step 7
Click Submit.

---

### Export Network Device Profiles from Cisco ISE

Export single or multiple network device profiles configured in Cisco ISE in the form of an XML file in order to edit the XML file and then import the file as new network profiles.

**Before you begin**

Read the Network Access Device Profiles with Cisco Identity Services Engine document.
Step 1 Choose Administration > Network Resources > Network Device Profiles.
Step 2 Click Export.
Step 3 Check the check boxes next to the devices that you want to export, and choose Export > Export Selected
Step 4 The DeviceProfiles.xml file downloads to your local hard disk.

Import Network Device Profiles into Cisco ISE

You can import a single or multiple network device profiles into ISE using a single XML file with the Cisco ISE XML structure. You cannot concurrently import network device profiles from multiple import files.

Typically, you would first export an existing profile from the Admin portal to use as a template. Enter your device profile details as necessary in the file and save it as an XML file, and then import the edited file back in to Cisco ISE. In order to work with multiple profiles, you can export multiple profiles structured together as a single XML file, edit the file and then import them together, creating multiple files in ISE.

While importing device profiles, you can only create new records. You cannot overwrite an existing profile. In order to edit an existing profile and then overwrite it, export the existing profile, delete the profile from ISE and then import that profile once you have edited it accordingly.

Before you begin
Read the Network Access Device Profiles with Cisco Identity Services Engine document.

Step 1 Choose Administration > Network Resources > Network Device Profiles.
Step 2 Click Import.
Step 3 Click Browse to choose the XML file from the system that is running the client browser.
Step 4 Click Import.

Network Device Groups

Cisco ISE allows you to create hierarchical Network Device Groups (NDGs). NDGs can be used to logically group network devices based on various criteria, such as geographic location, device type, or the relative place in the network (Access Layer, Data Center, and so on). For example, to organize your network devices based on geographic location, you can group them by continent, region, or country:

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

You can also group the network devices based on the device type:

- Africa -> Southern -> Botswana -> Firewalls
- Africa -> Southern -> Botswana -> Routers
Network devices can be assigned to one or more hierarchical NDGs. Thus, when Cisco ISE processes 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.

There is no limit on the maximum number of NDGs that can be created. There is also no restriction on the maximum number of hierarchy levels.

You can view the device group hierarchy in Tree view or Flat Table view. In the Tree view, the root node appears at the top of the tree followed by the child groups in hierarchical order. Click Expand All to view all the device groups under each root group. Click Collapse All to list only the root groups.

In the Flat Table view, you can view the hierarchy of each device group in the Group Hierarchy column.

You can also view the number of network devices that are assigned to each child group. Click the number link to launch the Network Devices window, which lists all the network devices that are assigned to that device group. You can add additional devices to a device group or move the existing devices to another device group.

While adding a device group, you can specify whether the new group must be added as a root group or select an already existing group as the parent group.

Note

You cannot delete a device group if any devices are assigned to that device group. Before deleting a device group you must move all the existing devices to another device group.

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 create a root Network Device Group (NDG), and then create child NDGs under the root group in the Network Device Groups page.

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 into 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 mExport > 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.

---

**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.

**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>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name:String(32):</td>
<td>(Required) This field is the network device name. It is an alphanumeric string, with a maximum of 32 characters in length.</td>
</tr>
<tr>
<td>Description:String(256)</td>
<td>This field is an optional description for the network device. A string, with a maximum of 256 characters in length.</td>
</tr>
<tr>
<td>IP Address:Subnets(a.b.c.d/m</td>
<td>...)</td>
</tr>
<tr>
<td>Model Name:String(32):</td>
<td>(Required) This field is the network device model name. It is a string, with a maximum of 32 characters in length.</td>
</tr>
<tr>
<td>Software Version:String(32):</td>
<td>(Required) This field is the network device software version. It is a string, with a maximum of 32 characters in length.</td>
</tr>
<tr>
<td>Network Device Groups:String(100):</td>
<td>(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</td>
</tr>
<tr>
<td>Authentication:Protocol:String(6)</td>
<td>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).</td>
</tr>
<tr>
<td>Authentication:Shared Secret:String(128)</td>
<td>(Required, if you enter a value for the Authentication Protocol field) This field is a string, with a maximum of 128 characters in length.</td>
</tr>
<tr>
<td>EnableKeyWrap:Boolean(true</td>
<td>false)</td>
</tr>
<tr>
<td>EncryptionKey:String(ascii:16</td>
<td>hexa:32)</td>
</tr>
</tbody>
</table>

Manage Network Devices
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AuthenticationKey:String(ascii:20</td>
<td>hexa:40)</td>
</tr>
<tr>
<td>InputFormat:String(32)</td>
<td>Indicates encryption and authentication keys input format. Valid value is ASCII or Hexadecimal.</td>
</tr>
<tr>
<td>SNMP:Version:Enumeration ([2c</td>
<td>3)</td>
</tr>
<tr>
<td>SNMP:RO Community:String(32)</td>
<td>(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.</td>
</tr>
<tr>
<td>SNMP:RW Community:String(32)</td>
<td>(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.</td>
</tr>
<tr>
<td>SNMP:Username:String(32)</td>
<td>This is an optional field. It is a string, with a maximum of 32 characters in length.</td>
</tr>
<tr>
<td>SNMP:Security Level:Enumeration(Auth</td>
<td>No Auth</td>
</tr>
<tr>
<td>SNMP:Authentication Protocol:Enumeration(MD5</td>
<td>SHA)</td>
</tr>
<tr>
<td>SNMP:Authentication Password:String(32)</td>
<td>(Required if you have entered Auth for the SNMP security level) It is a string, with a maximum of 32 characters in length.</td>
</tr>
<tr>
<td>SNMP:Privacy Protocol:Enumeration(DES</td>
<td>AES128</td>
</tr>
<tr>
<td>SNMP:Privacy Password:String(32)</td>
<td>(Required if you have entered Priv for the SNMP security level) It is a string, with a maximum of 32 characters in length.</td>
</tr>
<tr>
<td>SNMP:Polling Interval:Integer:600-86400 seconds</td>
<td>This is an optional field to set the SNMP polling interval. Valid value is an integer between 600 and 86400.</td>
</tr>
<tr>
<td>SNMP:Is Link Trap Query:Boolean(true</td>
<td>false)</td>
</tr>
<tr>
<td>SNMP:Is MAC Trap Query:Boolean(true</td>
<td>false)</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>SNMP:Originating Policy Services Node:String(32)</td>
<td>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.</td>
</tr>
<tr>
<td>Trustsec:Device Id:String(32)</td>
<td>This is an optional field. It is the Trustsec device ID, and is a string, with a maximum of 32 characters in length.</td>
</tr>
<tr>
<td>Trustsec:Device Password:String(256)</td>
<td>(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.</td>
</tr>
<tr>
<td>Trustsec:Environment Data Download Interval:Integer:1-2147040000 seconds</td>
<td>This is an optional field. It is the Trustsec environment data download interval. Valid value is an integer between 1 and 24850.</td>
</tr>
<tr>
<td>Trustsec:Peer Authorization Policy Download Interval:Integer:1-2147040000 seconds</td>
<td>This is an optional field. It is the Trustsec peer authorization policy download interval. Valid value is an integer between 1 and 24850.</td>
</tr>
<tr>
<td>Trustsec:Reauthentication Interval:Integer:1-2147040000 seconds</td>
<td>This is an optional field. It is the Trustsec reauthentication interval. Valid value is an integer between 1 and 24850.</td>
</tr>
<tr>
<td>Trustsec:SGACL List Download Interval:Integer:1-2147040000 seconds</td>
<td>This is an optional field. It is the Trustsec SGACL list download interval. Valid value is an integer between 1 and 24850.</td>
</tr>
<tr>
<td>Trustsec:Is Other Trustsec Devices Trusted:Boolean(true</td>
<td>false)</td>
</tr>
<tr>
<td>Trustsec:Notify this device about Trustsec configuration changes:String(ENABLE_ALL</td>
<td>DISABLE_ALL)</td>
</tr>
<tr>
<td>Trustsec:Include this device when deploying Security Group Tag Mapping Updates:Boolean(true</td>
<td>false)</td>
</tr>
<tr>
<td>Deployment:Execution Mode Username:String(32)</td>
<td>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.</td>
</tr>
<tr>
<td>Deployment:Execution Mode Password:String(32)</td>
<td>This is an optional field. It is the device password and is a string, with a maximum of 32 characters in length.</td>
</tr>
<tr>
<td>Deployment:Enable Mode Password:String(32)</td>
<td>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.</td>
</tr>
</tbody>
</table>
### 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 3: CSV Template Fields and Description for Network Device Groups**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name: String(100):</td>
<td><em>(Required)</em> 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 &gt; 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.</td>
</tr>
<tr>
<td>Description: String(1024)</td>
<td>This is an optional network device group description. It is a string, with a maximum of 1024 characters in length.</td>
</tr>
<tr>
<td>Type: String(64):</td>
<td><em>(Required)</em> This field is the network device group type. It is a string, with a maximum of 64 characters in length.</td>
</tr>
<tr>
<td>Is Root: Boolean(true/false):</td>
<td><em>(Required)</em> This is a field that determines if the specific network device group is a root group. Valid value is true or false.</td>
</tr>
</tbody>
</table>
IPsec Security to Secure Cisco ISE-NAD Communication

Internet Protocol security (IPsec) is a set of protocols that provides security to Internet Protocol. The AAA protocols, RADIUS and TACACS+, use the MD5 hashing algorithm. For greater security, Cisco ISE offers the IPsec feature. IPsec provides secure communication by authenticating the sender, discovering any changes in data during transmission, and encrypting the data that is sent.

Cisco ISE supports IPsec in Tunnel and Transport modes. When you enable IPsec on a Cisco ISE interface and configure the peers, an IPsec tunnel is created between Cisco ISE and the NAD to secure the communication.

You can define a pre-shared key or use X.509 certificates for IPsec authentication. IPsec can be enabled on Gigabit Ethernet 1 through Gigabit Ethernet 5 interfaces. You can configure IPsec on only one Cisco ISE interface per PSN.

IPSec cannot be enabled on Gigabit Ethernet 2 as the smart license is enabled (e0/2—> eth2) by default. However, if you are required to enable IPsec, you have to choose a different interface for smart licensing.

**Note**

Gigabit Ethernet 0 and Bond 0 (when Gigabit Ethernet 0 and Gigabit Ethernet 1 interfaces are bonded) are management interfaces in the Cisco ISE CLI; IPsec is not supported on Gigabit Ethernet 0 and Bond 0.

Required components include:

- Cisco ISE, Release 2.2 and later
- Cisco IOS Software, C5921 ESR (Embedded Services Router) Software (C5921_I86-UNIVERSALK9-M)—The ESR 5921 configuration, by default, supports IPsec in Tunnel and Transport modes. Diffie-Hellman Group 14 and Group 16 are supported.

**Note**

The C5921 ESR software is bundled with Cisco ISE, Releases 2.2 and later. You need an ESR license to enable it. See Cisco 5921 Embedded Services Router Integration Guide for ESR licensing information.

Configure RADIUS IPsec on Cisco ISE

To configure RADIUS IPsec on Cisco ISE, you must:

**Step 1**
Configure IP address on the interface from the Cisco ISE CLI.

Gigabit Ethernet 1 through Gigabit Ethernet 5 interfaces (Bond 1 and Bond 2) support IPsec. However, IPsec can be configured on only one interface in a Cisco ISE node.

**Step 2**
Add a directly-connected network device to the IPsec network device group.

**Note**

RADIUS IPsec requires the static route gateway to be directly connected through an interface of the device.

a) Choose Administration > Network Resources > Network Devices.
b) In the Network Devices page, click Add.
c) Enter the name and IP address and subnet of the network device that you want to add.
d) From the IPSEC drop-down list, choose Yes.
e) Check the RADIUS Authentication Settings checkbox.
f) In the Shared Secret field, enter the shared secret key that you have configured on the network device.
g) Click Submit.

**Step 3** (Optional; required only for Smart Licensing) Add a separate management interface to interact with the Cisco Smart Software Manager (CSSM). You can also use Smart Software Manager satellite for ESR. To do this, from the Cisco ISE CLI, run the following command to select the corresponding management interface (Gigabit Ethernet 1-5 (or Bond 1 or 2)):

`ise/admin# license esr smart {interface}`

This interface must be able to reach Cisco.com to access the Cisco online licensing server.

**Step 4** Add a network device to a directly-connected gateway from the Cisco ISE CLI.

`ip route [destination network] [network mask] gateway [next-hop address]`

**Step 5** Activate Cisco ISE nodes for IPSec.

a) Choose Administration > System > Settings > Protocols > IPSec.

All the Cisco ISE nodes in the deployment are listed in this page.

b) Check the check box next to the Cisco ISE node on which you want to activate IPsec, and then click the Enable radio button.

c) Select the interface that you want to use for IPsec communication.

d) Choose an authentication type for the selected ISE node from the following options:

- **Pre-shared Key**—If you choose this option, you must enter the pre-shared key and configure the same key on the network device. Use alphanumeric characters for the pre-shared key. Special characters are not supported. For instructions on how to configure the pre-shared key on the network device, see the network device documentation. For an example of the pre-shared key configuration output, see Example: Output of PreShared Key Configuration on Cisco Catalyst 3850, on page 27.

- **X.509 Certificates**—If you choose this option, from the Cisco ISE CLI, go to the ESR shell and configure and install X.509 Certificates for ESR 5921. Then, configure the network device for IPsec. For instructions, see Configure and Install X.509 Certificates on ESR-5921, on page 21.

e) Click Save.

**Note** You cannot modify IPsec configuration directly. If you want to modify the tunnel or authentication when IPsec is enabled, disable the current IPsec tunnel, modify the IPsec configuration and then re-enable the IPsec tunnel with a different configuration.

**Note** If enabled, IPsec removes the IP address from the Cisco ISE interface and shuts down the interface. When the user logs in from Cisco ISE CLI, the interface is displayed with no IP address and in shutdown state. This IP address will be configured on the ESR-5921 interface.

**Step 6** Type esr to enter into the ESR shell.

`ise/admin# esr`

% Enter ESR 5921 shell

% Cisco IOS Software, C5921 Software (C5921_I86-UNIVERSALK9-M), Version 15.5(2)T2, RELEASE SOFTWARE (fc3)`
For FIPS compliance, you must configure a secret password of at least 8 characters in length. Enter the **Enable secret level 1** command to specify the password:

```
ise-esr5921(config)#enable secret level 1 ?
0 Specifies an UNENCRYPTED password will follow
5 Specifies a MD5 HASHED secret will follow
8 Specifies a PBKDF2 HASHED secret will follow
9 Specifies a SCRYPT HASHED secret will follow
LINE The UNENCRYPTED (cleartext) 'enable' secret
```

**Note** If you configure customized RADIUS ports from the GUI (other than 1645, 1646, 1812, and 1813), you must enter the following CLI command in the ESR shell to accept the RADIUS port(s) that are configured:

```
ip nat inside source static udp 10.1.1.2 [port_number] interface Ethernet0/0 [port_number]
```

**Step 7** (Optional; required only if you have not enabled Smart Licensing in Step 3) Add a Classic license or an Evaluation license (that is valid for 90 days) to Cisco ISE appliances.

- Run the following command from the Cisco ISE CLI to download the license file:

  ```
  ise/admin# license esr classic import esr.lic repository esrrepo
  ```

  For more information on Classic licensing, see the section: Licensing the Software with Classic Licensing in Cisco 5921 Embedded Services Router Integration Guide.

**Step 8** Verify IPsec tunnel and RADIUS authentication over IPsec tunnel.

a) Add a user in Cisco ISE and assign to the user group (Administration > Identity Management > Identities > Users).

b) Verify if the IPsec tunnel is established between Cisco ISE and the NAD. To do this:

1. Use the **ping** command to test if the connection between Cisco ISE and the NAD is established.

2. Run the following command from the ESR shell or the NAD CLI to verify if the connection is in Active state:

   ```
   show crypto isakmp sa
   ```

   ```
   IPv4 Crypto ISAKMP SA
dst src state conn-id status
   192.168.30.1 192.168.30.3 QM_IDLE 1001 ACTIVE
   ```

3. Run the following command from the ESR shell or the NAD CLI to verify if the tunnel is established: **show crypto ipsec sa**

   ```
   interface: Ethernet0/0
   Crypto map tag: radius, local addr 192.168.30.1
   protected vrf: (none)
   local ident (addr/mask/prot/port): (192.168.30.1/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (192.168.30.2/255.255.255.255/0/0)
   current_peer 192.168.30.2 port 500
   PERMIT, flags=()
   #pkts encaps: 52, #pkts encrypt: 52, #pkts digest: 52
   ```
c) Verify the RADIUS authentication using one of the following methods:

- Log in to the network device using the credentials of the user that you created in Step 8 (a). The RADIUS authentication request is sent to the Cisco ISE node. View the details in the Live Authentications page.

- Connect the end host with the network device and configure 802.1X authentication. Log in to the end host using the credentials of the user that you created in Step 8 (a). The RADIUS authentication request is sent to the Cisco ISE node. View the details in the Live Authentications page.

---

**Configure and Install X.509 Certificates on ESR-5921**

To configure and install X.509 Certificates on ESR-5921:

**Step 1**  
Type `esr` to enter into the ESR shell.

```
ise/admin# esr
% Entering ESR 5921 shell
```
For FIPS compliance, you must configure a secret password of at least 8 characters in length. Enter the `enable secret level 1` command to specify the password:

```
ise-esr5921(config)#enable secret level 1
```

0 Specifies an UNENCRYPTED password will follow
5 Specifies a MD5 HASHED secret will follow
8 Specifies a PBKDF2 HASHED secret will follow
9 Specifies a SCRYPT HASHED secret will follow
 LINE The UNENCRYPTED (cleartext) 'enable' secret

**Note** If you configure customized RADIUS ports from the GUI (other than 1645, 1646, 1812, and 1813), you must enter the following CLI command in the ESR shell to accept the RADIUS port(s) that are configured:

```
ip nat inside source static udp 10.1.1.2 [port_number] interface Ethernet0/0 [port_number]
```

**Step 2** Generate an RSA key pair using the following command:

**Example:**
```
crypto key generate rsa label rsa2048 exportable modulus 2048
```

**Step 3** Create a trust point using the following command:

**Example:**
```
crypto pki trustpoint trustpoint-name

enrollment terminal
serial-number none
fqdn none
ip-address none
subject-name cn=networkdevicename.cisco.com
revocation-check none
rsakeypair rsa2048
```

**Step 4** Generate a CSR using the following command:

**Example:**
```
crypto pki enroll rsaca-mytrustpoint

Display Certificate Request to terminal? [yes/no]: yes
```

**Step 5** Copy the output of the CSR to a text file, submit it to an external CA for signing, and obtain the signed certificate and the CA certificate.

**Step 6** Import the CA using the following command:

**Example:**
```
crypto pki authenticate rsaca-mytrustpoint

Copy and paste the contents of the CA certificate, including the “—BEGIN—” and “—End—” lines.
```

**Step 7** Import the signed certificate using the following command:
Example:

crypto pki import rsaca-mytrustpoint

Copy and paste the contents of the signed certificate, including the “—BEGIN—” and “—End—” lines.

Following is an example output when you configure and install X.509 Certificates on Cisco 5921 ESR:

ise-esr5921#show running-config
!
hostname ise-esr5921
!
boot-start-marker
boot host unix:default-config
boot-end-marker
!
no aaa new-model
bsd-client server url https://cloudsso.cisco.com/as/token.oauth2
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi amnp-timeout 180
call-home
! If contact email address in call-home is configured as sch-smart-licensing@cisco.com
! the email address configured in Cisco Smart License Portal will be used as contact email address
! to send SCH notifications.
contact-email-addr sch-smart-licensing@cisco.com
profile "CiscoTAC-1"
    active
destination transport-method http
    no destination transport-method email
!
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
crypto pki trustpoint SLA-TrustPoint
enrollment pkcs12
revocation-check crl
!
crypto pki trustpoint rsaca-mytrustpoint
enrollment terminal
serial-number none
fqdn none
ip-address none
subject-name cn=ise-5921.cisco.com
revocation-check none
rsakeypair rsa2048
!
crypto pki certificate chain SLA-TrustPoint
certificate ca 01
  30820321 30820209 A0030201 02020101 300D0609 2A864886 F70D0101 0B050030
  32310E30 0C060355 040A1305 43697361 6F312030 1E060355 04031317 43697361
  6F204C69 6D6573696E6720 526F6F74 20434130 82012230 0D06092A 864886F7
  0D010101 05000382 010F0030 82010201 02012300 0D06092A 864886F7 0D010101
  05000382 010F0030 82010201 02012300 0D06092A 864886F7 0D010101 05000382
  010F0030 82010201 02012300 0D06092A 864886F7 0D010101 05000382 010F0030
  82010201 02012300 0D06092A 864886F7 0D010101 05000382 010F0030

1C394D78 462EF239 C659F715 B98C04A9 5B8B5CB6 0CFEEBA3 700A8BF7 D8F256EE
4AA4E530 DB6F12D9 6B1F068E FF69C096 6F6A8957 A2617DE7 104FDC5F
73903ABE 2B5435AD C847A2B5 DAB5357E 69A9A352 58E9F3E3 C0BD23CF 58BD7188
686E9A5F 20320E7 948E711D E3BCC84 F1067B20 4BC4E08F 539BA42B 42C6A9B7
C7479096 B4CB2B62 EA2F505D C7B062A4 6811D95B E8250FC4 5D5D5FB9 8F27D191
Raw text not provided.
A196DA5A 1B525175 C26B3581 EA4B0203 010001A3 5D305B30 1D060355 1D0E0416 0414966A 0C21AF96 423599CC EE8087A1 2909301F 0603551D 23041830 16801496 6A0C21AF 963E8276 90423599 CCEE8087 A1290930 0C060355 1D130405 00692B01 0100032A 5B0E5D3 4D299825 67A07754 73EC52E3 05B7D05F 926CC563 2269F34B 861C56B2 EF7C3485 47D4DE0F 73895879 CAE088BB 183B7CFA A20C4354 86C6D9DF D445DACE C52C608 236F6673 F3F3C329 474B22E8 660BF91E 4105FBBD 43B80E44 AE69C61E 2C9F41A2 8284FS77 21FFAB8E A6771A5E DD34EB4A A0DC2EAD 95702010 02964566 478DA90F SE134643 81A5F5EA 362D0394 189F23D1 DE050B07 12938299 1AF11A36 82DAFC6A 164B2F66 8B0AB7CC 9A723B8C 50E740B 0A927E03 60E24D2 7F10DA1F F6735144 AE93BF86 3D5A0502 6811DB2D 6E694693 28DE84C5 3747C5A0 D2B86C9 EBEBA0A D1137CF8 E31CBF6B 43782DD D74A4A9F 3557B3D9 D5BD035F 65A8

quit
license udi pid CISCO5921-K9 an 9XG4481W768
username lab password 0 lab
! redundancy
!
crypto keyring MVPN-spokes
rsa-pubkey address 0.0.0.0
   address 0.0.0.0
   key-string
quit
!
crypto isakmp policy 10
encl aes
hash sha256
!”
crypto isakmp policy 20
encr aes
hash sha256
group 16
!”
crypto isakmp profile MVPN-profile
   description LAN-to-LAN for spoke router(a) connection
   keyring MVPN-spokes
   match identity address 0.0.0.0
!
crypto ipsec transform-set radius esp-aes esp-sha256-hmac
   mode tunnel
   crypto ipsec transform-set radius-2 esp-aes esp-sha256-hmac
   mode transport
!
crypto dynamic-map MVPN-dynmap 10
   set transform-set radius radius-2
!
crypto map radius 10 ipsec-isakmp dynamic MVPN-dynmap
!
interface Ethernet0/0
description e0/0->connection to external NAD
ip address 192.168.20.1 255.255.255.0
ip nat outside
ip virtual-reassembly in
no ip route-cache
crypto map radius
!
interface Ethernet0/1
description e0/1->tap0 internal connection to ISE
ip address 10.1.1.1 255.255.255.252
ip nat inside
ip virtual-reassembly in
no ip route-cache
!
interface Ethernet0/2
no ip address
shutdown
!
interface Ethernet0/3
no ip address
shutdown
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
ip nat inside source list 1 interface Ethernet0/0 overload
ip nat inside source static udp 10.1.1.2 1645 interface Ethernet0/0 1645
ip nat inside source static udp 10.1.1.2 1646 interface Ethernet0/0 1646
ip nat inside source static udp 10.1.1.2 1812 interface Ethernet0/0 1812
ip nat inside source static udp 10.1.1.2 1813 interface Ethernet0/0 1813
!
access-list 1 permit 10.1.1.0 0.0.0.3
!
control-plane
!
line con 0
logging synchronous
line aux 0
line vty 0 4
login
transport input none
!
end

Following is an example output when you configure and install X.509 Certificates on Cisco Catalyst 3850:

```
cat3850#show running-config

enable password lab
!
username lab password 0 lab
aaa new-model
!

aaa group server radius ise
server name ise-vm
deadtime 60
!
aaa authentication login default group radius local

aaa authentication enable default group radius enable
!
crypto isakmp policy 10
enr aes

hash sha256
authentication rsa-sig
group 16
!
crypto ipsec security-association lifetime seconds 86400
!
crypto ipsec transform-set radius esp-aes esp-sha256-hmac
mode tunnel
```
crypto ipsec profile radius-profile
!
crypto map radius 10 ipsec-isakmp
set peer 192.168.20.1
set transform-set radius
match address 100
!
interface GigabitEthernet1/0/1
no switchport
ip address 192.168.20.2 255.255.255.0
crypto map radius
!
access-list 100 permit ip host 192.168.20.2 host 192.168.20.1
!
snmp-server community public RO
snmp-server community private RW
!
radius server rad-ise
address ipv4 192.168.20.1 auth-port 1645 acct-port 1646
key secret

Example: Output of PreShared Key Configuration on Cisco Catalyst 3850

Following is an example of the output when you configure the pre-shared key on Cisco Catalyst 3850:

cat3850#show running-config
enable password lab
!
username lab password 0 lab
aaa new-model
!
aaa group server radius ise
server name ise-vm
deadtime 60
!
aaa authentication login default group radius local

aaa authentication enable default group radius enable
!
crypto isakmp policy 10
enr aes
hash sha256
authentication pre-share
group 16
crypto isakmp key 123456789 address 0.0.0.0
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.
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 30.

**Supported MDM Use Cases**

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

- Managing device registration—Unregistered endpoints accessing the network are redirected to a registration page, which is hosted on the MDM server. Device registration includes user role, device type, and so on.

- Handling device remediation—Endpoints are granted only restricted access during remediation.

- 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 **Work Centers > Network Access > Identities > Endpoints** page if an endpoint is an 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 4 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.

**Vendor MDM Attributes**

When you configure an MDM server in ISE, that vendor's attributes are added to a new entry in the ISE system dictionary, named `mdm`. The following attributes are used for registration status, and are commonly supported by MDM vendors.

• DeviceRegisterStatus
• DeviceCompliantStatus
• DiskEncryptionStatus
• PinLockStatus
• JailBrokenStatus
• Manufacturer
• IMEI
• SerialNumber
• OsVersion
• PhoneNumber
• MDMServerName
• MDMServerReachable
• MEID
• Model
• UDID

Vendor's unique attributes are not supported, but you may be able to use ERS APIs to exchange vendor-specific attributes, if the vendor supports that.

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

**Supported MDM Servers**

Supported MDM servers include products from the following vendors:

• Absolute
• AirWatch
Some versions of MobileIron do not work with ISE. MobileIron is aware of this problem, and have a fix. Please contact MobileIron for more information.

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

<table>
<thead>
<tr>
<th>MDM Server</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>MobileIron</td>
<td>443</td>
</tr>
<tr>
<td>Zenprise</td>
<td>443</td>
</tr>
<tr>
<td>Good</td>
<td>19005</td>
</tr>
<tr>
<td>Airwatch</td>
<td>443</td>
</tr>
<tr>
<td>Afaria</td>
<td>443</td>
</tr>
<tr>
<td>Fiberlink MaaS</td>
<td>443</td>
</tr>
</tbody>
</table>
### 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**

You must register a device that is enrolled on the MDM server outside of a Cisco ISE network via the MDM portal. This is applicable for Cisco ISE, Release 1.4 and later. Earlier ISE versions allow devices enrolled outside of a Cisco ISE network to be automatically enrolled if they are 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.
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, except for Intune, where you import the PAN's certificate into Azure.
- **Step 2** Create mobile device manager definitions.
- **Step 3** Configure ACLs on the Wireless LAN Controllers.
- **Step 4** Configure an authorization profile that redirects non-registered devices to the MDM server.
- **Step 5** If there is 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.

**Note**

For Microsoft Azure, you import the ISE certificate into Azure. For more information, see Configuring Microsoft Intune as an MDM Server, on page 37.
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.

What to do next

Define Mobile Device Management Servers in ISE, on page 34

Define Mobile Device Management Servers in ISE

You can create one or more Mobile Device Management (MDM) and Desktop Device Manager (SCCM) definitions for external MDM servers.

1. Choose Administration > Network Resources > External MDM.
2. Click Add.
3. Enter the name and description of the MDM server that you want to add.
4. Choose the Server Type, Mobile Device Manager, or Desktop Device Manager. Your choice determines which fields you see next. If you chose Desktop Device Manager, go to Desktop Device Management, on page 35. If you chose Mobile Device Manager, then continue this list of steps.
5. Choose Authentication Type, Basic, or OAuth - Client Credentials. If you chose OAuth - Client credentials to configure a Microsoft Intune server, go to Mobile Device Management - OAuth - Client Credentials, on page 35. If you chose Basic, then continue this list of steps.
6. All screens ask for a name and describe this MDM server definition. The following section describes the additional fields and steps, which are based on server and authentication type.

Mobile Device Management - Basic

- **Host Name / IP Address**—Enter the hostname or IP address of the MDM server.
- **Port**—Enter the port to use 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.
- **Polling Interval**—Enter the polling interval in minutes for Cisco ISE to poll the MDM server for compliance check information. Set this value to match the polling interval on your MDM server. The valid range is from 15 to 240 minutes. The default value is 240 minutes. We recommend that you set the polling interval below 60 minutes only for testing a few active clients on your network. If you set this
value below 60 minutes for a production environment with many active clients, the system’s load increases significantly and may negatively affect performance.

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

- **Time Interval For Compliance Device ReAuth Query**—When the endpoint is authenticated or re-authenticated, ISE uses a cache to get the MDM variables for that endpoint. If the age of cached value is older than the value of Time Interval For Compliance Device ReAuth Query, then ISE makes a device query to the MDM server to get new values. If the compliance status changed, then ISE triggers a CoA.

  The valid range is from 1 to 1440 minutes. The default value is 1 minute.

**Mobile Device Management - OAuth - Client Credentials**

Using OAuth requires configuration of the OAuth server, which is described in Configuring Microsoft Intune as an MDM Server, on page 37

- **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 Azure AD directory using the Graph API. The URL is of the form: https://<hostname>/<tenant id>, for example, https://graph.ppe.windows.net/47f09275-5bc0-4807-8aee-f35cb0341329. An expanded version of this URL is also in the property file, which is of the form: https://<Graph_API_Endpoint>/<TenantId_Or_Domain>/servicePrincipalsByAppId/<Microsoft Intune AppId>/serviceEndpoints?api-version=1.6&client-request-id=<Guid.NewGuid()>.

- **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* from the previous step. This is the endpoint at which your app can obtain an access token using OAuth2.0. After your app is authenticated, Microsoft Azure AD issues your app (ISE) an access token, which allows your app to call the Graph API/Intune API.

- **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.

- **Polling Interval**—Enter the polling interval in minutes for Cisco ISE to poll the MDM server for compliance check information. Set this value to match the polling interval on your MDM server. The valid range is from 15 to 240 minutes. The default value is 240 minutes. We recommend that you set the polling interval below 60 minutes only for testing a few active clients on your network. If you set this value below 60 minutes for a production environment with many active clients, the system’s load increases significantly and may negatively affect performance.

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

**Desktop Device Management**

The following settings require you to configure WMI on the SCCM server, so it can communicate with ISE. See Configure the Microsoft SCCM Server for ISE, on page 40 for more information.

- **Host Name / IP Address**—Enter the hostname or IP address of the MDM server.

- **Site or Instance Name**—Enter the site name, or if the MDM server has several instances, the instance name.
ISE MDM Support for Microsoft Intune and SCCM

• **Microsoft Intune** - MDM-ISE supports Microsoft’s Intune device management as a partner MDM server managing mobile devices.

  You configure ISE as an OAuth 2.0 client application on the Intune server managing mobile devices. ISE gets a token from Azure to establish a session with that ISE Intune application.


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

**SCCM Workflow**

ISE is able to retrieve information from the SCCM server about whether a device is registered, and if it is registered, is it compliant. The following diagram shows the workflow for devices managed by SCCM.

*Figure 4: SCCM Workflow*

![SCCM Workflow Diagram](image)

When a device connects and a SCCM policy is matched, ISE queries the SCCM server specified in the authorization policy to retrieve compliance and last logon (check-in) time. With this information, ISE updates the compliance status and lastCheckinTimeStamp of the device in the Endpoint list.

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

**Microsoft SCCM Server Connection Monitoring**

Polling is not configurable for SCCM.

ISE runs an MDM HeartBeat job that verifies connection to the SCCM server, and raises alarms if ISE loses the connection to the SCCM server. The HeartBeat job interval is not configurable.
Configuring Microsoft Intune as an MDM Server

Configuring Microsoft Intune as an MDM server for ISE is slightly differently from configuring other MDM servers. Use the following steps to configure ISE's connection to Azure and Azure's connection to ISE.

1. Get the public certificate from the Intune/Azure Active Directory tenant, and import it into ISE to support SSL handshake.
   a. Log on to the Intune Admin Console or Azure Admin console, whichever site has your tenant.
   b. Use the browser to get the certificate details. For example, with Internet Explorer:
      1. Click on the lock symbol in the browser's toolbar, then click View Certificates.
      2. In the Certificate window, select the tab Certification Path.
      3. Find Baltimore Cyber Trust root, and export the root cert.
   c. In ISE, choose Administration > System > Certificates > Trusted Certificates, and import the root certificate that you just saved. Give the certificate a meaningful name, such as Azure MDM.

2. Export the ISE self-signed certificate, and prepare it for InTune/Azure.
   a. On the PAN, navigate to Administration > System > Certificates > System Certificates, select the Default self-signed server certificate, and click Export.
   b. Select Export Certificate Only (default), and select a place to save it.
   c. Run the following PowerShell script on the exported certificate file:

   ```powershell
   $cer.Import("mycer.cer")
   $bin = $cer.GetRawCertData()
   $base64Value = [System.Convert]::ToBase64String($bin)
   $bin = $cer.GetCertHash()
   $base64Thumbprint = [System.Convert]::ToBase64String($bin)
   $keyid = [System.Guid]::NewGuid().ToString()
   ``
   Keep the values for $base64Thumbprint, $base64Value and $keyid, which will be used in the next step.

3. Create an ISE application in Intune.
   a. Sign in to your customer domain on the Microsoft Azure management portal, navigate to Directory > Applications > Add an Application, and choose Add an application my organization is developing.
   b. Configure the ISE application in Azure with the following parameters:
      1. Application Name—enter ISE.
      2. Select WEB APPLICATION AND/OR WEB APP.
      3. SIGN-ON URL and APP ID URL—Add any valid URL, these values are not used by ISE.

4. Get the manifest file from Azure, add the ISE certificate information, and upload the updated manifest into Azure.
a. On the Microsoft Azure management portal (https://manage.windowsazure.com), open the AAD snap-in, and navigate to the ISE application.

Download the application manifest file from the Manage Manifest menu.

5. Update the keyCredentials field in Manifest json file as shown in the following example, replacing Base64 Encoded String of ISE PAN cert with the exported, edited, certificate file from ISE, which is the $base64Value from the PowerShell script:

```
"keyCredentials": [
    {
        "customKeyIdentifier": "$base64Thumbprint_from_above",
        "keyId": "$keyid_from_above",
        "type": "AsymmetricX509Cert",
        "usage": "Verify",
        "value": "Base64 Encoded String of ISE PAN cert"
    }
]
```

Do not change the name of the manifest file.


6. Upload the updated manifest file to Azure.

7. On the Microsoft Azure management portal, navigate to the list of App Endpoints. You will use the values of following endpoint attributes to configure ISE:

   • MICROSOFT AZURE AD GRAPH API ENDPOINT
   • OAUTH 2.0 TOKEN ENDPOINT

8. In ISE, configure the Intune server in ISE. For more information about configuring and external MDM server, see Define Mobile Device Management Servers in ISE, on page 34. The fields that are important for Intune are described below:

   • 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 Azure AD directory using the Graph API. The URL is of the form:
     https://<hostname>/<tenant id>, for example, https://graph.ppe.windows.net/47f09275-5bc0-4807-8aae-f35cb0341329. An expanded version of this URL is also in the property file, which is of the form:
     https://<Graph_API_Endpoint>/<TenantId_Or_Domain>/servicePrincipalsByAppId/<Microsoft Intune AppId>/serviceEndpoints?api-version=1.6&client-request-id=<Guid.NewGuid()>.

   • 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 Oauth2.0 Authorization Endpoint from the previous step. This is the endpoint at which your app can obtain an access token using OAuth2.0. After your app is authenticated, Microsoft Azure AD issues your app (ISE) an access token, which allows your app to call the Graph API/ Intune API.
• **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.

For more information about Intune applications, see the following links:


### Policy Set Example for Microsoft SCCM

The following new dictionary entries can be used in policies to support SCCM.

- **MDM.DaysSinceLastCheckin** - Number of days since a user last checked in or synched a device with SCCM, from 1 to 365 days.

- **MDM.UserNotified** - Values are Y or N. Indicates whether the user was notified that they are not registered. You can then allow limited access and redirect to registration portal, or deny access.

- **MDM.ServerType** - Values are MDM for Mobile Device Manager or DM for Desktop Device Manager.

The following example Policy Set shows a set of policies to support SCCM:

<table>
<thead>
<tr>
<th>Policy Name</th>
<th>If</th>
<th>Then</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCCM_Comp</td>
<td>Wireless_802.1X AND MDM:MDMServerName EQUALS SccmServer1 AND MDM:DeviceRegisterStatus EQUALS Registered</td>
<td>PermitAccess</td>
</tr>
<tr>
<td>SCCM_NonComp_Notify</td>
<td>Wireless_802.1X AND MDM:MDMServerName EQUALS SccmServer1 AND MDM:DeviceCompliantStatus EQUALS NonCompliant AND MDM:UserNotified EQUALS 28</td>
<td>PermitAccess</td>
</tr>
</tbody>
</table>
### Configure the Microsoft SCCM Server for ISE

ISE communicates with the SCCM server using WMI. WMI must be configured on the Windows server running SCCM.

**Note**

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

- Be a member of SMS Admins user group.
- Have the same permissions as the SMS object under the WMI namespace `root\sms\site_<sitecode>`

where `<sitecode>` is the SCCM site.

### 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}`

<table>
<thead>
<tr>
<th>Policy Name</th>
<th>If</th>
<th>Then</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCCM_NonComp_Days</td>
<td>Wireless_802.1X AND MDM:MDMServerName EQUALS SccmServer1 AND MDM:MDMDeviceCompliantStatus EQUALS NonCompliant AND MDM:DeviceRegisterStatus EQUALS Registered</td>
<td>SCCMRedirect</td>
</tr>
<tr>
<td>SCCM_NonComp</td>
<td>Wireless_802.1X AND MDM:MDMServerName EQUALS SccmServer1 AND MDM:DeviceCompliantStatus EQUALS NonCompliant AND MDM:DeviceRegisterStatus EQUALS Registered</td>
<td>SCCMRedirect</td>
</tr>
<tr>
<td>SCCM_UnReg_Notify</td>
<td>Wireless_802.1X AND MDM:DeviceRegisterStatus EQUALS Registered AND MDM:UserNotified EQUALS Yes</td>
<td>PermitAccess</td>
</tr>
</tbody>
</table>
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, on page 42
- Set Permissions for Access to WMI Root/CIMv2 Name Space, on page 44

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
- Windows 2016

### 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 Passive Identity services 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 5: Local and Remote Access for Access Permissions
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 wmiimgmt.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.
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

Note: Cisco ISE 1.3 and above support 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 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 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.

**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  Choose Policy > Policy Sets, and expand the policy set to view the authorization policy rules.
Step 3  Add the following rules:

- MDM_UnRegistered_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 8: Authorization Policy Rules for the MDM Use Cases*

Step 4  Click Save.

---

### 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 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 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.

**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 "DEBUG" or "TRACE."