

Network Access Device Profiles with Cisco Identity Services Engine

Secure Access How -To Guides Series

Table of Contents

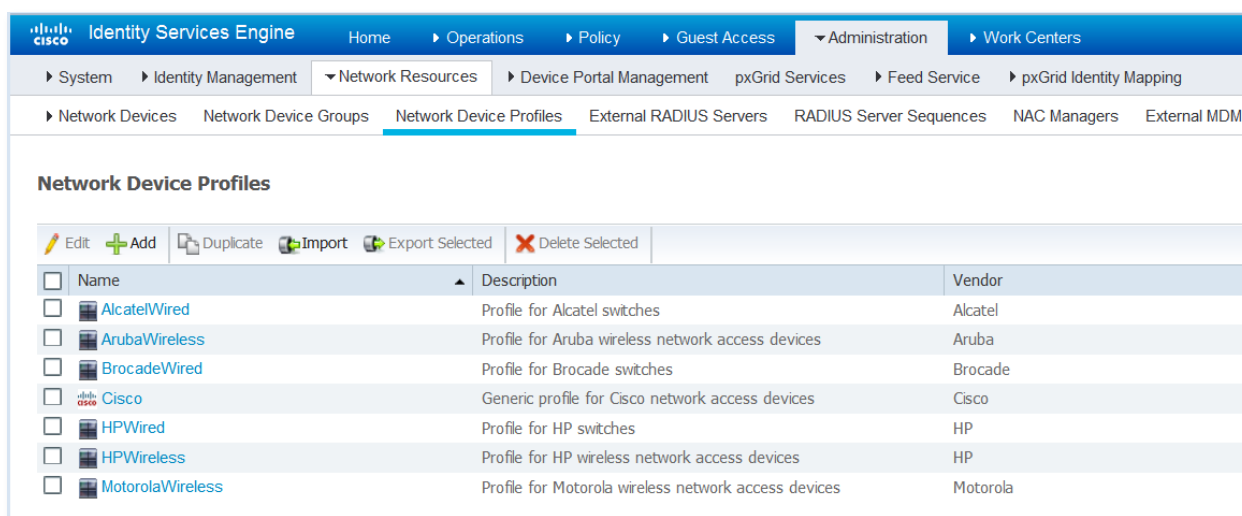
Chapter 1	Network Access Device Profiles	3
	About Network Access Device Profiles	3
	Custom Network Access Device Profiles	3
Chapter 2	Steps To Create Custom Profiles	4
	Overview	4
	Recommended Procedure	4
	Gather Information.....	4
	Device Configuration.....	4
	Profile Creation and Assignment.....	4
	Policy Configuration	4
Chapter 3	RADIUS dictionaries.....	5
	Determine if you need to import a dictionary	5
	Importing RADIUS dictionaries	5
Chapter 4	Defining The Custom Profile.....	7
	Create New Profile Entry	7
	Supported Protocols.....	8
	RADIUS Dictionaries.....	8
	Flow Type Conditions	8
	Attribute Aliasing	9
	Host Lookup.....	9
	Permissions	10
	Change of Authorization (CoA).....	11
	URL Redirect.....	12
	Generate Policy Elements.....	13
	Summary	14
Chapter 5	Using your Network Device Profile	15
	Assign the NAD Profile	15
	Authentication/Authorization Conditions	16
	Authorization Profiles	17

Chapter 1 Network Access Device Profiles

About Network Access Device Profiles

Cisco Identity Services Engine (ISE) 2.0 introduces support for some non-Cisco Network Access Devices (NADs). ISE uses *Network Access Device Profiles* to express a NAD's capabilities and requirements which ISE uses to enable flows such as MAB, Guest, BYOD and Posture.

ISE 2.0 ships with a number of built-in NAD profiles which are located under Network Resources:



Name	Description	Vendor
AlcatelWired	Profile for Alcatel switches	Alcatel
ArubaWireless	Profile for Aruba wireless network access devices	Aruba
BrocadeWired	Profile for Brocade switches	Brocade
Cisco	Generic profile for Cisco network access devices	Cisco
HPWired	Profile for HP switches	HP
HPWireless	Profile for HP wireless network access devices	HP
MotorolaWireless	Profile for Motorola wireless network access devices	Motorola

Figure 1. Built-in NAD Profiles

Custom Network Access Device Profiles

This guide describes how to create a custom NAD profile when the built-in profiles do not suffice. The number of ISE flows that will be enabled by your NAD profile depends on the NAD's capabilities.

For complex flows such as Guest, BYOD and Posture, the device needs to support RFC 5176, "Change Of Authorization" (CoA), and a URL Redirection mechanism capable of redirecting to ISE portals and passing in the client identity (MAC or IP address) as a URL parameter. If your NAD does not support these features, those flows will not work.

Chapter 2 Steps To Create Custom Profiles

Overview

Some information about your device needs to be determined before new NAD profiles can be defined. It is usually necessary to import a new RADIUS dictionary for your device before you can create a NAD profile. You may have to upgrade the device firmware to a more recent version to get CoA/URL Redirect support. It is also usually necessary to make configuration changes on the devices to configure or enable certain features, especially for URL Redirect. Once done, create the new NAD Profile in ISE and assign it to the appropriate devices. Finally, configure new authorization profile(s) and ISE policy to leverage the new profile.

Recommended Procedure

Gather Information

- Step 1** Refer to the *Administration Manual* for your NAD (often has the information we seek)
- Step 2** Determine what RADIUS dictionary, if any, is required and import it into ISE
- Step 3** Determine which attributes are used for MAB, SSID, setting VLAN, ACL – if appropriate
- Step 4** Determine if RADIUS CoA is supported and what attributes it requires in CoA requests
- Step 5** Determine if URL Redirect is supported and which attributes and URL parameters it uses

Device Configuration

- Step 6** Verify your NAD(s) firmware is at sufficient level – upgrade if necessary
- Step 7** Make any required configuration changes on the NAD (for CoA/URL Redirect)

Profile Creation and Assignment

- Step 8** Create new NAD profile using information you learned from above
- Step 9** Assign the new profile to one or more NADs

Policy Configuration

- Step 10** Create new authorization profile(s)
- Step 11** Configure ISE policy to leverage your new NAD profile
- Step 12** Verify expected behavior

These steps will be explained in more detail in subsequent chapters.

Chapter 3 RADIUS dictionaries

Determine if you need to import a dictionary

Consult the documentation for your NAD to determine what RADIUS dictionary the NAD uses. Most NADs have a vendor-specific RADIUS dictionary that provides a number of vendor-specific attributes in addition to the standard IETF RADIUS attributes. Features such as MAB, CoA, URL Redirect, ACLs, VLAN, SSID, all potentially use RADIUS attributes and sometimes they are vendor-specific (VSAs) rather than IETF.

Importing RADIUS dictionaries

If your device uses VSAs, you will usually need to install its RADIUS dictionary into ISE before you can assign it to the NAD profile. ISE has the ability to import RADIUS dictionary files in the *freeradius* format, which can be found at *Policy Elements* → *Dictionaries* → *System* → *Radius* → *RADIUS Vendors*.

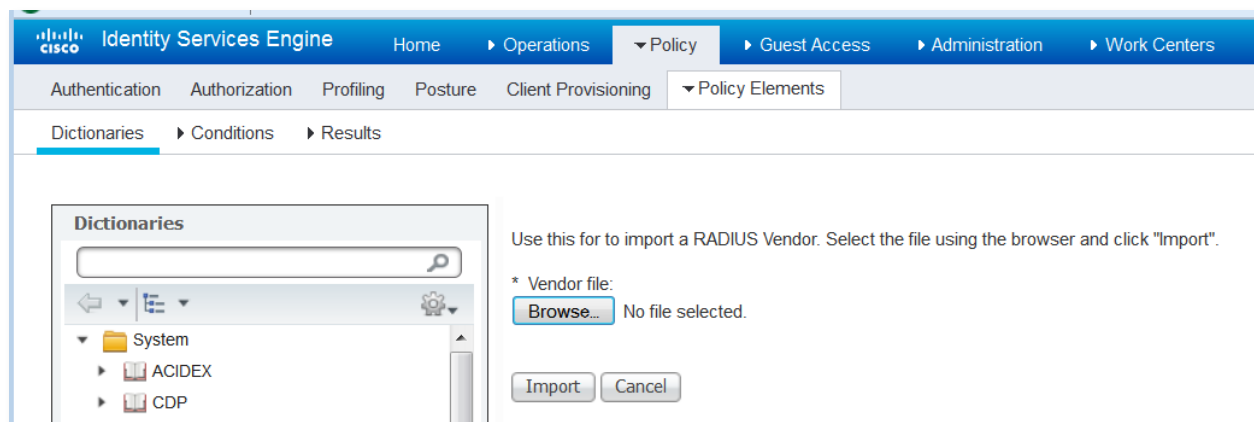
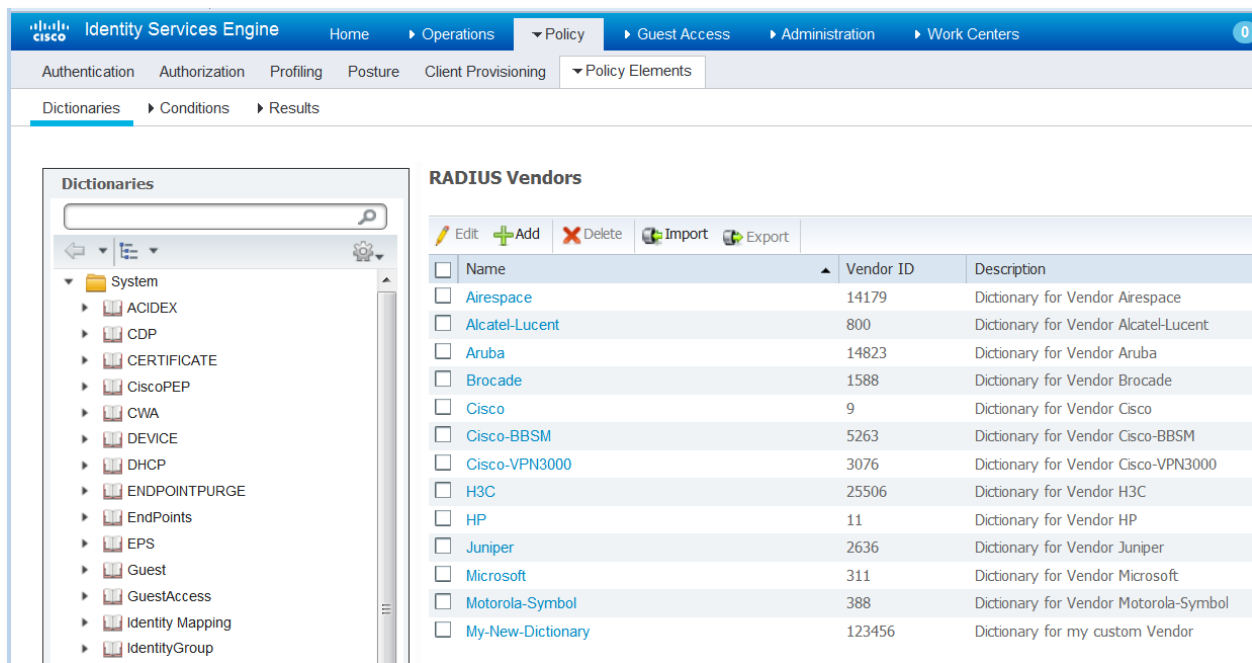


Figure 2. Import RADIUS dictionary

Once imported successfully, the new dictionary should appear in the list of RADIUS dictionary vendors:



The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Home', 'Operations', 'Policy', 'Guest Access', 'Administration', and 'Work Centers'. The 'Policy' tab is selected, and the 'Policy Elements' sub-tab is active. The 'Dictionaries' section is expanded, showing a list of dictionaries on the left and a table of RADIUS Vendors on the right.

Dictionaries

- System
 - ACIDEX
 - CDP
 - CERTIFICATE
 - CiscoPEP
 - CWA
 - DEVICE
 - DHCP
 - ENDPOINTPURGE
 - EndPoints
 - EPS
 - Guest
 - GuestAccess
 - Identity Mapping
 - IdentityGroup

RADIUS Vendors

Name	Vendor ID	Description
Airspace	14179	Dictionary for Vendor Airspace
Alcatel-Lucent	800	Dictionary for Vendor Alcatel-Lucent
Aruba	14823	Dictionary for Vendor Aruba
Brocade	1588	Dictionary for Vendor Brocade
Cisco	9	Dictionary for Vendor Cisco
Cisco-BBSM	5263	Dictionary for Vendor Cisco-BBSM
Cisco-VPN3000	3076	Dictionary for Vendor Cisco-VPN3000
H3C	25506	Dictionary for Vendor H3C
HP	11	Dictionary for Vendor HP
Juniper	2636	Dictionary for Vendor Juniper
Microsoft	311	Dictionary for Vendor Microsoft
Motorola-Symbol	388	Dictionary for Vendor Motorola-Symbol
My-New-Dictionary	123456	Dictionary for my custom Vendor

Figure 3. Newly imported dictionary

Chapter 4 Defining The Custom Profile

Create New Profile Entry



Once you have the required information and RADIUS dictionary installed, click *New Network Device Profile* to create the new NAD profile. Create a new name and description for your NAD profile. The name can be useful in policy conditions, troubleshooting and is shown in the reports. You may assign a specific icon for the new profile which will make it easier to differentiate from others.

Network Device Profile List > My_NAD_Profile

Network Device Profile

* Name

Description

Icon  

Vendor

Supported Protocols

RADIUS ☒

TACACS+ ☐

TrustSec ☐

RADIUS Dictionaries

Figure 4. New NAD Profile

For *Vendor*, if you are creating NAD profile for a device similar to one of the built-in profiles, i.e. same vendor but different model with some differences, it is best to clone the existing NAD profile and customize it. The cloned profile will have a copy of the original profile's settings so you only have to tweak it rather than define it from scratch. You may not have to define a new RADIUS dictionary either, if the current one is sufficient.

However, if your NAD vendor does not match any of the existing ones, you should set the *Vendor* field to 'Other' and enter all of its characteristics.

Supported Protocols

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.

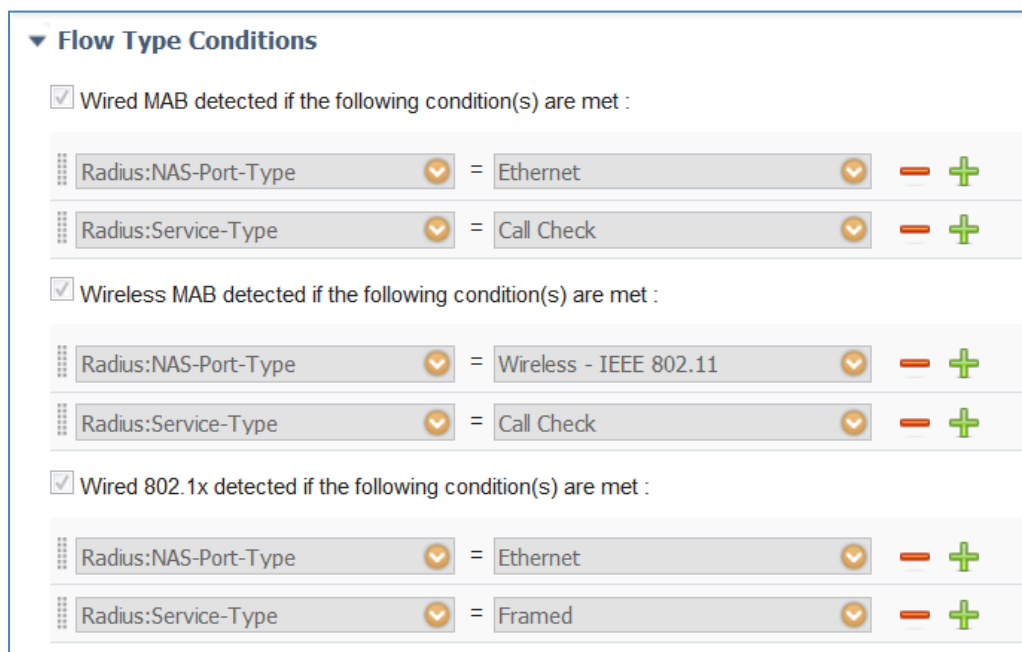
RADIUS Dictionaries

Assign the RADIUS dictionary the device supports – typically one you imported in a step beforehand.

Note: You can assign more than one dictionary as some devices do support multiple vendor dictionaries.

Flow Type Conditions

Enter the attributes and values that your device uses for the various flows like Wired MAB, 802.1x, in the Flow Type Conditions section (under Authentication/Authorization). This is necessary for ISE to detect the right 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. It may be necessary to use a sniffer trace to determine the values here if they are not documented in your device's Admin Guide.



The image shows a configuration window titled "Flow Type Conditions". It contains three sections, each with a checked checkbox and a description of conditions for detection:

- Wired MAB detected if the following condition(s) are met :**
 - Radius:NAS-Port-Type = Ethernet
 - Radius:Service-Type = Call Check
- Wireless MAB detected if the following condition(s) are met :**
 - Radius:NAS-Port-Type = Wireless - IEEE 802.11
 - Radius:Service-Type = Call Check
- Wired 802.1x detected if the following condition(s) are met :**
 - Radius:NAS-Port-Type = Ethernet
 - Radius:Service-Type = Framed

Each condition row includes a list icon on the left, a dropdown menu for the attribute, an equals sign, another dropdown menu for the value, and red minus and green plus icons on the right for editing.

Figure 5. Flow Type Conditions

Attribute Aliasing

This section allows you to map device specific attribute names to common names to simplify policy rules. Currently, only “SSID” is defined. If your device has the concept of wireless SSID then set this to the attribute it uses.

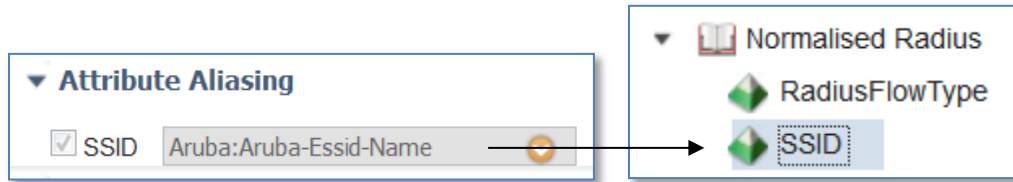


Figure 6. Attribute Aliasing (SSID)

Attribute Aliasing allows a NAD Profile to map vendor-specific attributes to a common attribute so that policy rules can use the friendly name. It simplifies attribute selection, reduces the number of authentication/authorization policy rules required for different vendor devices, and is potentially less error prone. For example, the Wireless SSID involved in a flow could be included in the Airespace-Wlan-ID, Aruba-ESSID-Name, or Called-Station-ID depending on the type of NAD involved. You can map this to the “SSID” attribute available in the “Normalised Radius” dictionary (Policy > Policy Elements > Dictionaries > Normalised Radius > SSID).

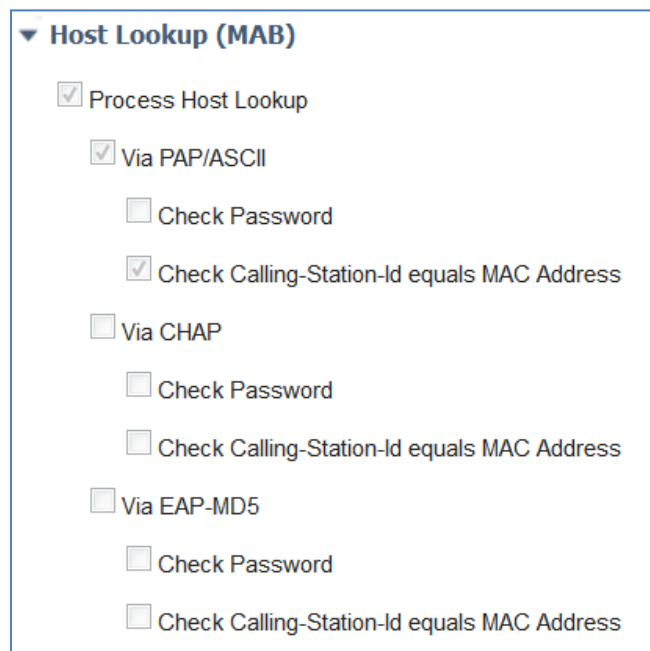
Host Lookup

This section allows you to define which attributes and protocols your device uses for MAB. Prior to 2.0, this was accomplished with various obscure combinations of checkboxes in *Allowed Protocols* page and it potentially required multiple Allowed Protocol entries. Host Lookup is now encapsulated in NAD Profiles and simplifies configuration.

When the Process Host Lookup option is enabled in the Allowed protocols page, the Host Lookup request is processed based on the NAD profile configuration (specifically the Host Lookup (MAB) settings).

Different (non-Cisco) vendors populate the RADIUS *Calling-Station-ID* and password attributes differently while doing a MAB authentication. For Cisco NADs doing MAB, enabling the Process Host Lookup option is sufficient. However, for other vendor devices, you must enable appropriate options in the Host Lookup (MAB) section, while creating the NAD profile.

As stated above, there is no standard for MAB, so the attributes and protocol it uses varies from vendor to vendor. Refer to your device Admin Guide or a sniffer trace of a MAB authentication to determine the correct settings for this section.



▼ Host Lookup (MAB)

- ☒ Process Host Lookup
 - ☒ Via PAP/ASCII
 - ☐ Check Password
 - ☒ Check Calling-Station-Id equals MAC Address
 - ☐ Via CHAP
 - ☐ Check Password
 - ☐ Check Calling-Station-Id equals MAC Address
 - ☐ Via EAP-MD5
 - ☐ Check Password
 - ☐ Check Calling-Station-Id equals MAC Address

Figure 7. Host Lookup (MAB)

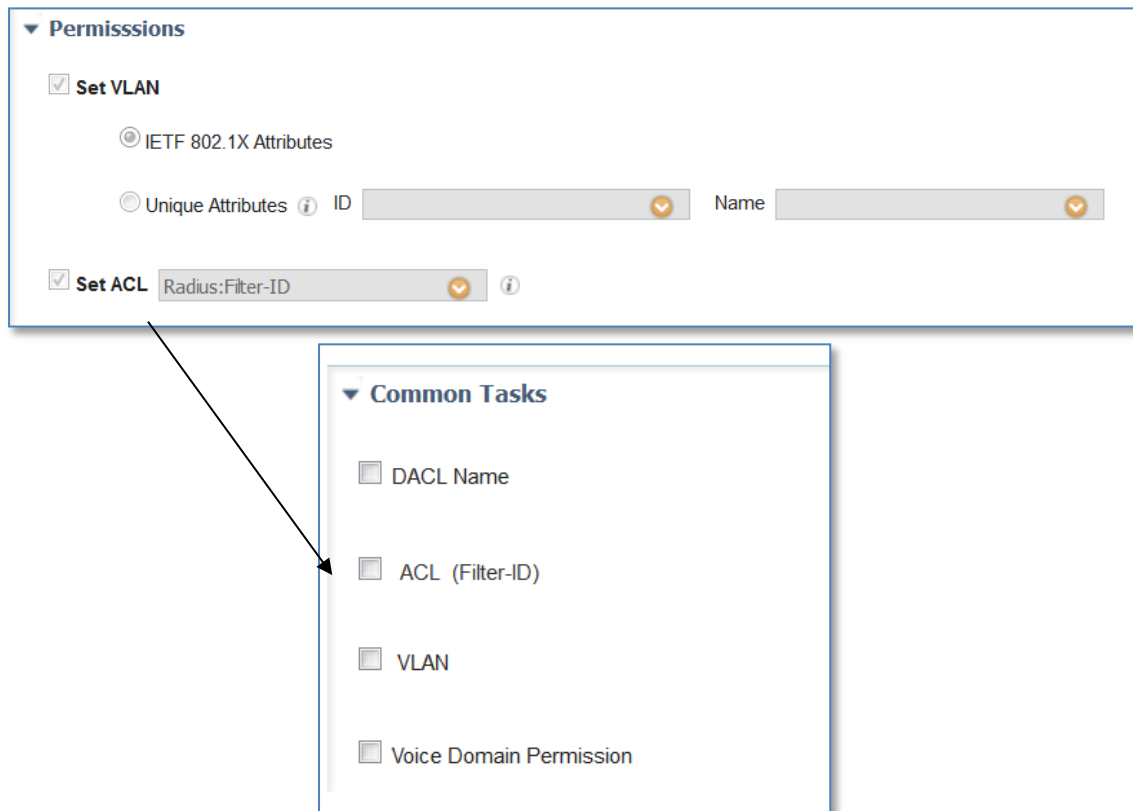
Permissions

This section defines which attributes your device uses for setting a VLAN or ACL. They may be IETF standard attributes or vendor specific. These are usually published in your device's Admin Guide.

For the VLAN permission, you can specify multiple RADIUS attribute-value pairs, or a single RADIUS attribute (e.g. Aruba-User-VLAN).

For the ACL permission, you can specify a single RADIUS attribute, to be used for setting a named ACL on NADs relevant to the current NAD profile.

Note: The options displayed in the Common Tasks section in the Authorization Profile page vary based on the attributes that you configure in the NAD Profile Permission section.



▼ Permissions

☒ **Set VLAN**

☒ IETF 802.1X Attributes

☐ Unique Attributes ⓘ ID Name

☒ **Set ACL** Radius:Filter-ID ⓘ

▼ Common Tasks

☐ DACL Name

☒ ACL (Filter-ID)

☐ VLAN

☐ Voice Domain Permission

Figure 8. Permissions and relation to Common Tasks

Change of Authorization (CoA)

This section allows you to define what CoA capabilities your device has. Refer to your device documentation for information – look for references to terms like “RFC 5176”, “Change of Authorization” or “CoA”. Most non-Cisco devices with RFC 5176 support will support “Push” and “Disconnect”, but not Re-authenticate, so if unsure try enabling the two checkboxes marked “RFC 5176”.

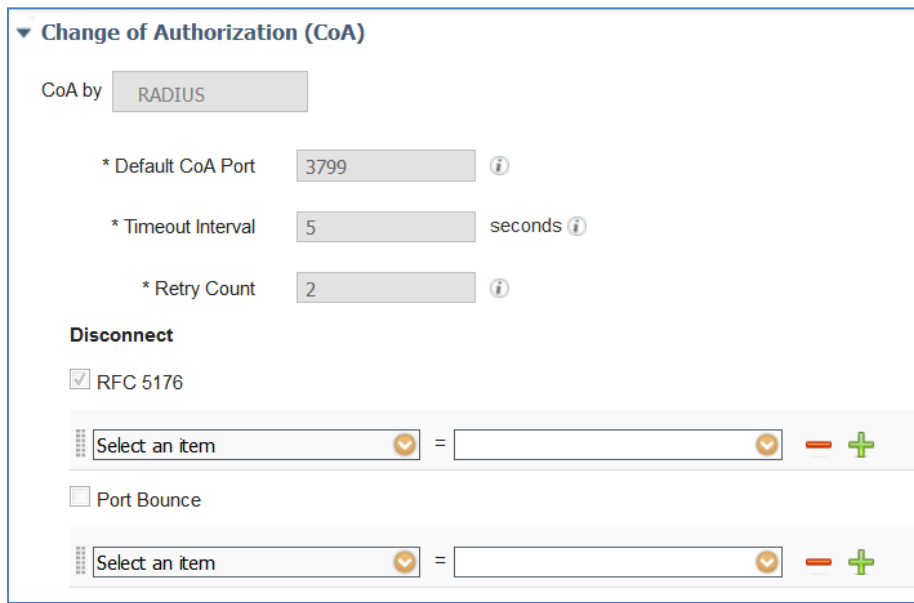


Figure 9. CoA configuration

While RFC 5176 defines the types of CoA requests, the required attributes in the requests vary from device to device. Some devices are very particular about attributes sent in the CoA request.

If your CoA requests are getting a CoA ‘NAK’ back from the device, check some of the following tips:

- Some require the RADIUS User-Name attribute from the access-request to be included in CoA requests
- Some do not accept both Calling-Station-ID and Acct-Session-ID sent in the same request (send one)
- Some do not accept other vendors VSAs in a request
- Some devices can be configured to expect (or not) Event-Timestamp and the CoA configuration above must match

While some Admin Guides do publish the attributes, some do not and it requires some trial and error to determine the right set of attributes.

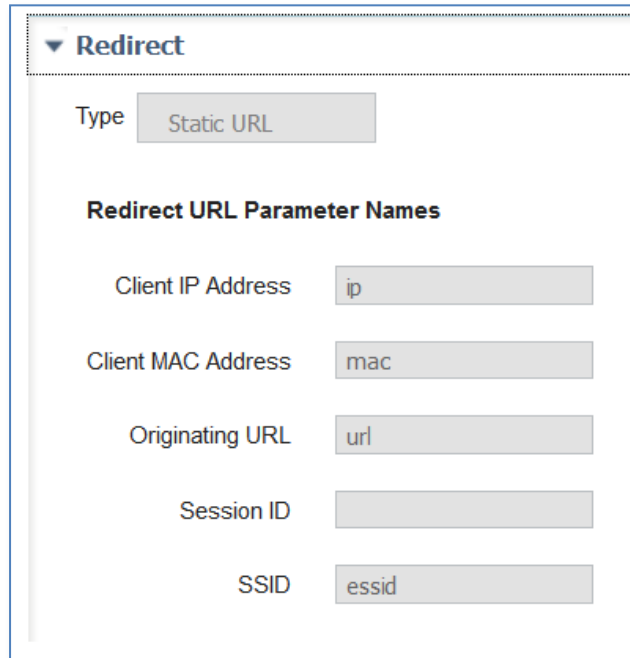
Note: Ensure that the RADIUS option is selected in the *Supported Protocols* section, before you configure the RADIUS CoA.

URL Redirect

This section defines the device’s URL Redirect capabilities. URL redirection is necessary for complex flows like Guest, BYOD and Posture. It needs to be capable of redirecting to an ISE portal, i.e. *local web auth* is not sufficient.

There are two general types of URL redirect found on devices; static and dynamic. Static means a URL has to be configured into the device (manually). It does not support being told where to redirect dynamically via a RADIUS attribute. Typically, you copy and paste the ISE portal URL into the device’s configuration.

The other type is dynamic URL – this is where ISE can use a RADIUS attribute to tell the device where to redirect to dynamically. It is not necessary to manually configure the device. If your device supports dynamic URLs, you should use it as it simplifies configuration.



▼ Redirect

Type

Redirect URL Parameter Names

Client IP Address	<input type="text" value="ip"/>
Client MAC Address	<input type="text" value="mac"/>
Originating URL	<input type="text" value="url"/>
Session ID	<input type="text"/>
SSID	<input type="text" value="essid"/>

Figure 10. URL Redirect

The Parameter Names are arguments passed by the device in the redirect URL. ISE needs to be told the names of these parameters so it can extract them correctly from the URL. It uses them to identify the client and session, as well as the original URL the client was trying to get to so that it can redirect it.

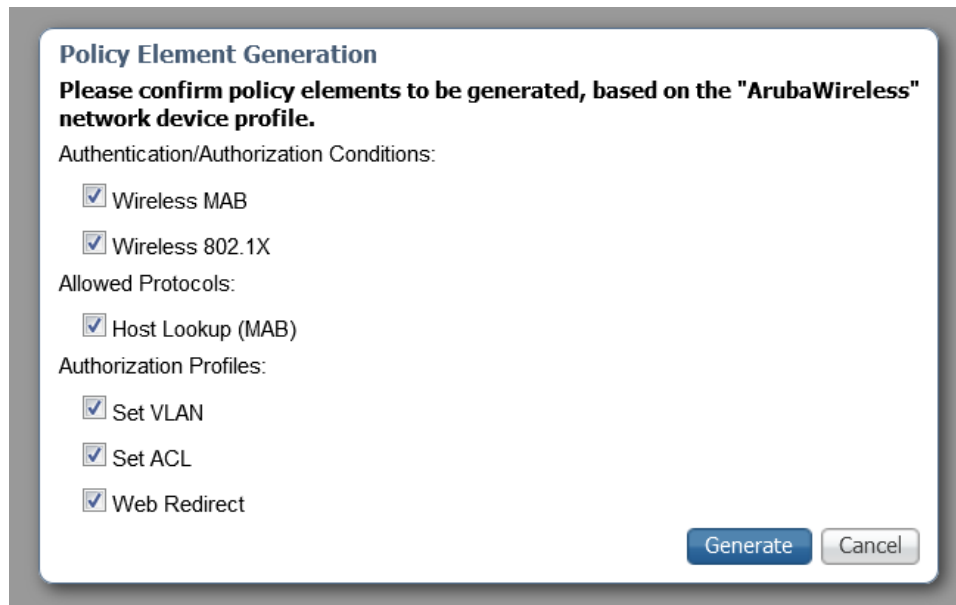
Note: Admin Guides do not usually publish these parameter names. Some do, but most do not. A few are actually programmable. What matters is the URL parameter names must match what the device sends (it may be necessary to use a browser to determine what they are if it is not published).

Note: Wired devices usually do not have a capable URL redirect.

Generate Policy Elements

Normally, it is unnecessary to create additional or modify the built-in Authentication and Authorization conditions (such as *Wired/Wireless MAB* or *Wired/Wireless 802.1X*) as these will automatically use the right NAD profile at runtime. Similarly, the built-in *Allowed Protocols* will use the correct attributes from existing NAD profiles to detect MAB.

However, should it become necessary to create a custom condition, protocol or profile, you can use the *Policy Element Generation* wizard to assist you. It can create various editable elements based on the NAD profile which you can further customize or use in policy.



Policy Element Generation

Please confirm policy elements to be generated, based on the "ArubaWireless" network device profile.

Authentication/Authorization Conditions:

- ☒ Wireless MAB
- ☒ Wireless 802.1X

Allowed Protocols:

- ☒ Host Lookup (MAB)

Authorization Profiles:

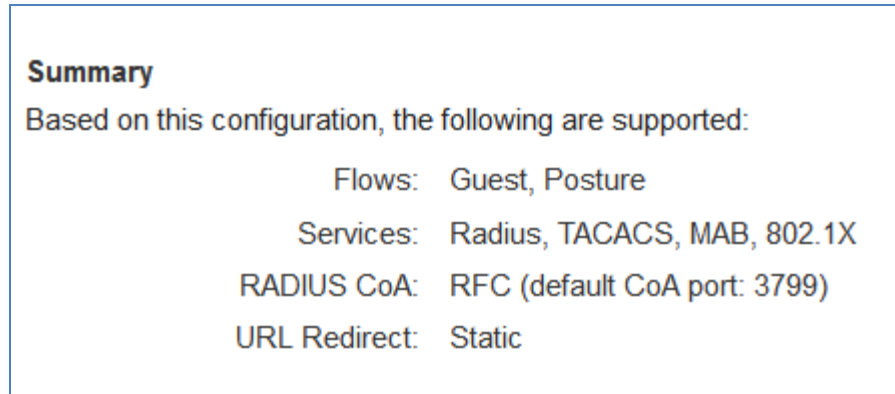
- ☒ Set VLAN
- ☒ Set ACL
- ☒ Web Redirect

Generate **Cancel**

Figure 11. Generating Policy Elements

Summary

The Summary section shows what flows and services will be enabled by your NAD profile configuration.



Summary

Based on this configuration, the following are supported:

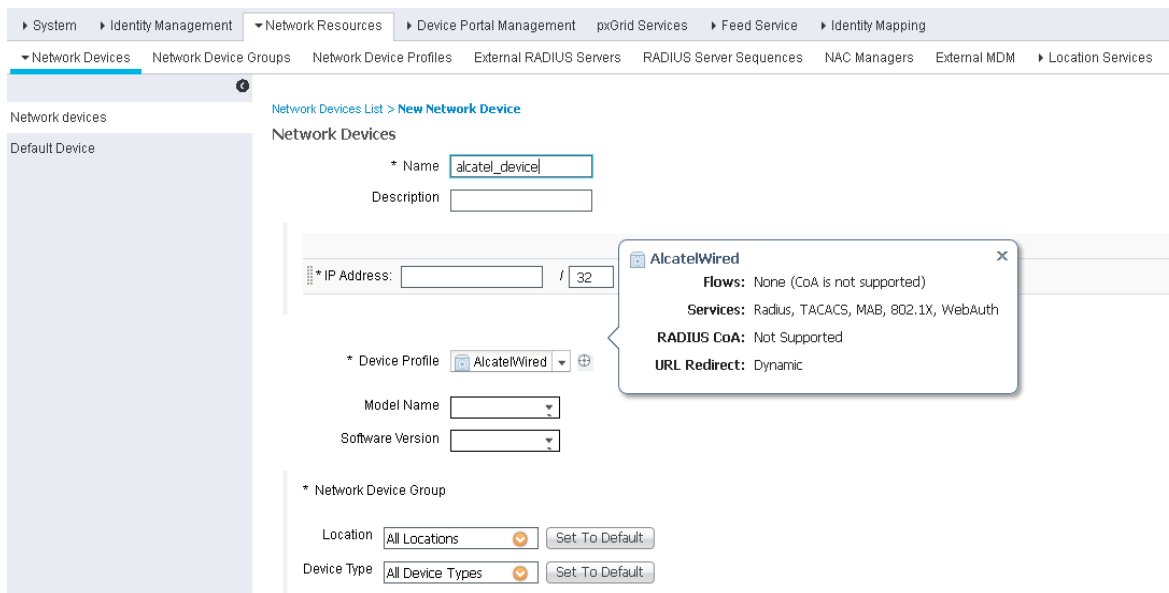
Flows:	Guest, Posture
Services:	Radius, TACACS, MAB, 802.1X
RADIUS CoA:	RFC (default CoA port: 3799)
URL Redirect:	Static

Figure 12. NAD Profile Summary

Chapter 5 Using your Network Device Profile

Assign the NAD Profile

Once your NAD profile is created, assign it to your device in Network Devices:



The screenshot displays the 'New Network Device' configuration page in the Cisco Identity Management console. The breadcrumb trail at the top indicates the path: System > Identity Management > Network Resources > Device Portal Management > pxGrid Services > Feed Service > Identity Mapping. The 'Network Devices' tab is selected, and the 'New Network Device' link is highlighted. The form contains the following fields and options:

- Name:** alcatel_device
- Description:** (empty)
- IP Address:** (empty) / 32
- Device Profile:** AlcatelWired (selected from a dropdown)
- Model Name:** (empty dropdown)
- Software Version:** (empty dropdown)
- Network Device Group:**
 - Location:** All Locations (selected) with a 'Set To Default' button.
 - Device Type:** All Device Types (selected) with a 'Set To Default' button.

A tooltip for the 'AlcatelWired' profile is displayed, providing the following details:

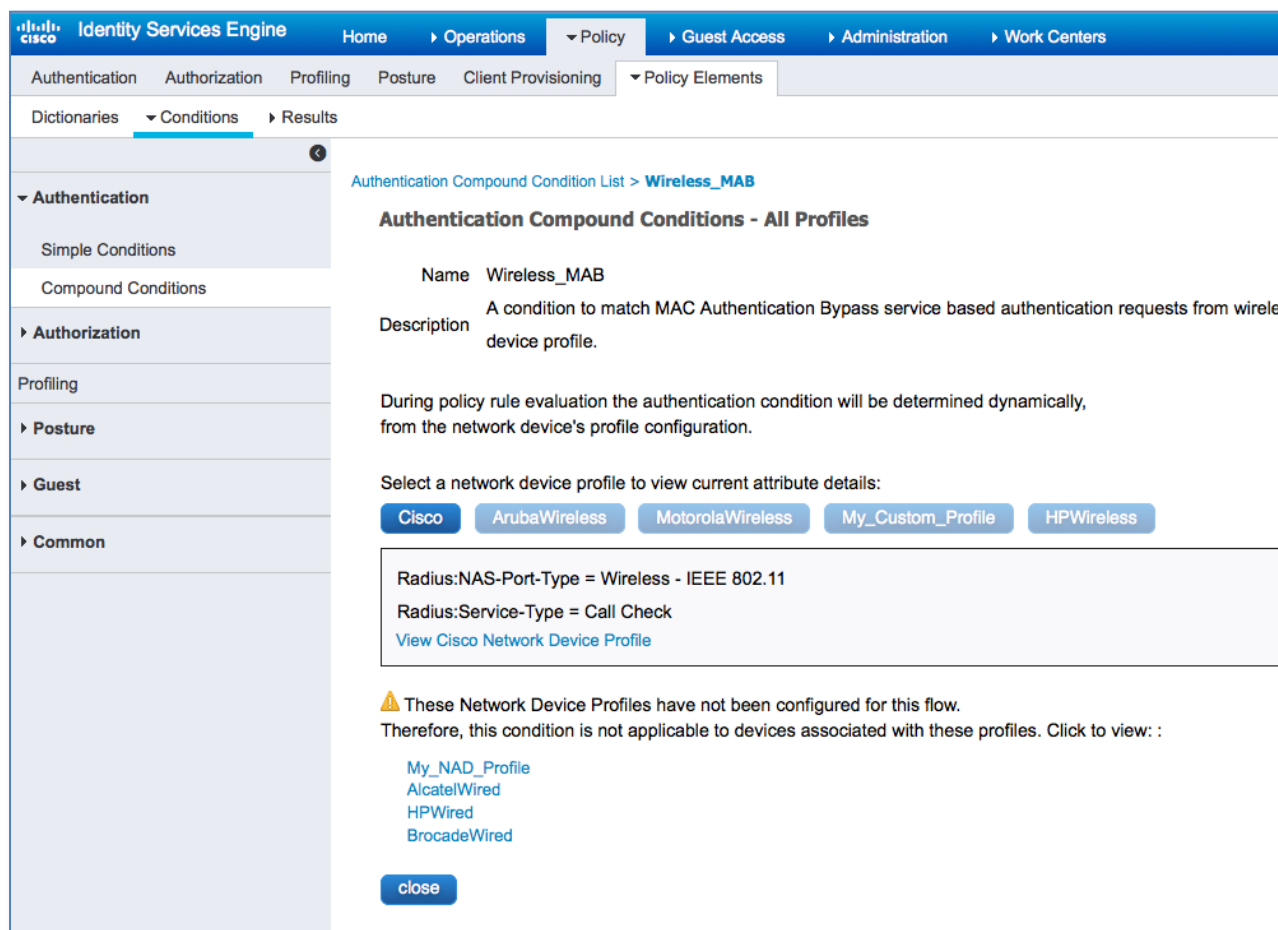
- Flows:** None (CoA is not supported)
- Services:** Radius, TACACS, MAB, 802.1X, WebAuth
- RADIUS CoA:** Not Supported
- URL Redirect:** Dynamic

Figure 13. Assigning a NAD profile

Authentication/Authorization Conditions

ISE has a number of built-in authentication and authorization conditions (Wired/Wireless MAB, 802.1x) that smartly select the right underlying conditions to evaluate. It does this by determining the NAD profile assigned to the NAD at runtime then referring to information in its NAD profile. This allows you to have significantly less authentication/authorization conditions. Often you can define a new NAD profile and it is not necessary to customize the built-in smart conditions.

If you examine one of the existing conditions you can see which NAD profiles will be taken into consideration by it and which are not:



The screenshot shows the Cisco Identity Services Engine (ISE) web interface. The top navigation bar includes 'Home', 'Operations', 'Policy', 'Guest Access', 'Administration', and 'Work Centers'. The 'Policy' tab is selected, and the 'Policy Elements' sub-tab is active. The left sidebar shows a tree view with 'Authentication' expanded, containing 'Simple Conditions' and 'Compound Conditions'. The main content area displays the 'Authentication Compound Condition List > Wireless_MAB'.

Authentication Compound Conditions - All Profiles

Name: Wireless_MAB

Description: A condition to match MAC Authentication Bypass service based authentication requests from wireless device profile.

During policy rule evaluation the authentication condition will be determined dynamically, from the network device's profile configuration.

Select a network device profile to view current attribute details:

Buttons: Cisco, ArubaWireless, MotorolaWireless, My_Custom_Profile, HPWireless

Attributes displayed:

- Radius:NAS-Port-Type = Wireless - IEEE 802.11
- Radius:Service-Type = Call Check

[View Cisco Network Device Profile](#)

Warning: These Network Device Profiles have not been configured for this flow. Therefore, this condition is not applicable to devices associated with these profiles. Click to view :

Links: [My_NAD_Profile](#), [AlcatelWired](#), [HPWired](#), [BrocadeWired](#)

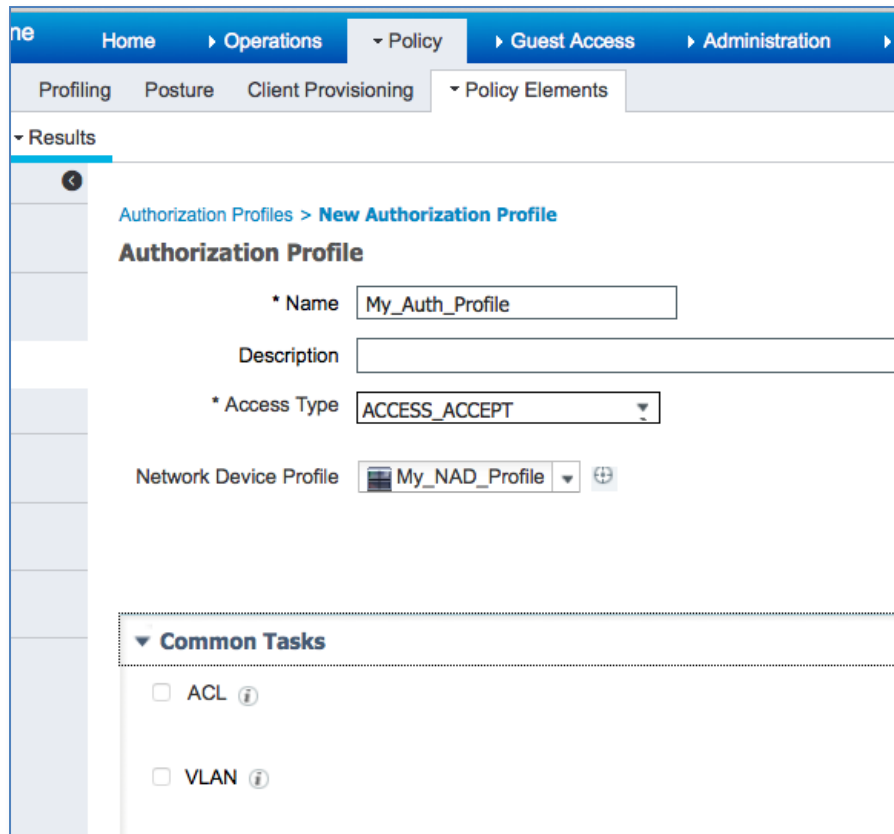
[close](#)

Figure 14. Smart Authentication Condition

Occasionally, you may wish to define a custom condition for your new device. You can use the *Generate Policy Elements* feature from the NAD profile to help you create them with the correct attribute/values in the conditions.

Authorization Profiles

You will usually need to create one or more authorization profiles for your new device. Set the *Network Device Profile* box to the name of your new NAD profile when creating the profile. This allows the ‘smart’ authorization to automatically select the right profile based on the device’s assigned NAD profile.



The screenshot displays the Cisco Secure Access configuration interface. The top navigation bar includes 'Home', 'Operations', 'Policy', 'Guest Access', and 'Administration'. The 'Policy' tab is active, and the 'Policy Elements' sub-tab is selected. The left sidebar shows a tree view with 'Results' expanded. The main content area is titled 'Authorization Profiles > New Authorization Profile'. The form includes the following fields:

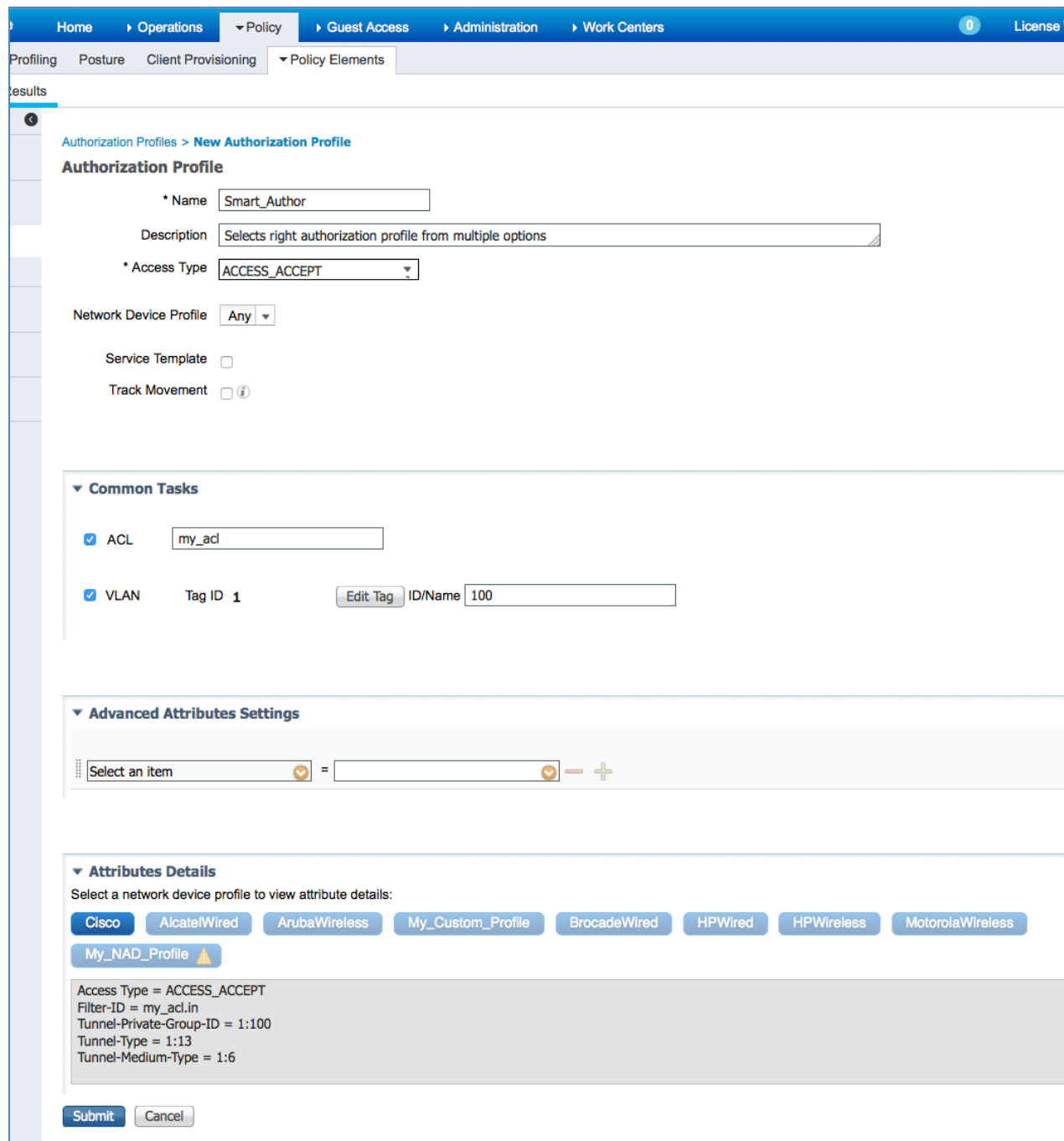
- Name:** My_Auth_Profile
- Description:** (empty text box)
- Access Type:** ACCESS_ACCEPT (dropdown menu)
- Network Device Profile:** My_NAD_Profile (dropdown menu with a plus icon)

Below the form is a section titled 'Common Tasks' with two checkboxes:

- ☐ ACL ⓘ
- ☐ VLAN ⓘ

Figure 15. New Authorization Profile

When you configure your policy rules, the authorization profile should be explicitly set to the NAD profile that you assigned to that device or “Any” if you are just using VLAN or ACL.



Home > Operations > Policy > Guest Access > Administration > Work Centers

0 License

Profiling Posture Client Provisioning Policy Elements

results

Authorization Profiles > **New Authorization Profile**

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

Service Template ☐

Track Movement ☐

Common Tasks

☒ ACL

☒ VLAN Tag ID ID/Name

Advanced Attributes Settings

Select an item =

Attributes Details

Select a network device profile to view attribute details:

Access Type = ACCESS_ACCEPT
Filter-ID = my_acl.in
Tunnel-Private-Group-ID = 1:100
Tunnel-Type = 1:13
Tunnel-Medium-Type = 1:6

Figure 16. Smart Authorization Profile

Verify Behavior

Once you have created your new NAD profile and configured ISE's policy to use it, you should verify whether the relevant flows work as expected. It is also advisable to verify devices using other NAD profiles still work as expected. The 'STEPS' detail in ISE's monitoring/reports has additional information in ISE 2.0 to help you understand which NAD profile is being used and what flow type is detected which can aid troubleshooting.