Manage Authorization Policies and Profiles

Cisco ISE Authorization Policies

Authorization policies are a component of the Cisco ISE network authorization service. This service allows you to define authorization policies and configure authorization profiles for specific users and groups that access your network resources.

Authorization policies can contain conditional requirements that combine one or more identity groups using a compound condition that includes authorization checks that can return one or more authorization profiles. In addition, conditional requirements can exist apart from the use of a specific identity group (such as in using the default “Any”).

Authorization policies are used when creating authorization profiles in Cisco Identity Services Engine (Cisco ISE). An authorization policy is composed of authorization rules. Authorization rules have three elements: name, attributes, and permissions. The permission element is that maps to an authorization profile.

Cisco ISE Authorization Profiles

Authorization policies associate rules with specific user and group identities to create the corresponding profiles. Whenever these rules match the configured attributes, the corresponding authorization profile that grants permission is returned by the policy and network access is authorized accordingly.

For example, authorization profiles can include a range of permissions that are contained in the following types:

- Standard profiles
- Exception profiles
- Device-based profiles

Profiles consist of attributes chosen from a set of resources, which are stored in any of the available vendor dictionaries, and these are returned when the compound condition for the specific authorization policy matches. Because authorization policies can include compound condition mapping to a single network service rule, these can also include a list of authorization checks.

For simple scenarios, all authorization checks are made using the AND Boolean operator within the rule. For advanced scenarios, any type of authorization verification expression can be used, but all these authorization verifications must comply with the authorization profiles to be returned. Authorization verifications typically comprise one or more conditions, including a user-defined name that can be added to a library, which can then be reused by other authorization policies.

Related Topics

Authorization Policy Terminology, on page 2
Authorization Policies and Supported Dictionaries, on page 4
Configure Authorization Policies, on page 9
Permissions for Authorization Profiles, on page 13
Configure Permissions for Downloadable ACLs, on page 14

Authorization Policy Terminology

You can define authorization profiles and policies for network authorization of users to access Cisco ISE network and its resources. Cisco ISE also uses downloadable ACLs (DACLs), which are configured and implemented through authorization profiles. For more information about authorization profiles, see Authorization Profile, on page 3. For more information about DACLs, see Downloadable ACLs, on page 14.

Network Authorization

Network authorization controls user access to the network and its resources and what each user can do on the system with those resources. Activate network authorization from Cisco ISE by defining sets of permissions that authorize read, write, and execute privileges. Cisco ISE lets you create a number of different authorization policies to suit your network needs. This release supports only RADIUS access to the Cisco ISE network and its resources.

Policy Elements

Policy elements are components that define an authorization policy and are as follows:

- Rule name
- Identity groups
- Conditions
- Permissions

These policy elements are referenced when you create policy rules and your choice of conditions and attributes can create specific types of authorization profiles.

Authorization Profile

An authorization profile acts as a container where a number of specific permissions allow access to a set of network services. The authorization profile is where you define a set of permissions to be granted for a network access request and can include:

- A profile name
- A profile description
- An associated ACL (Filter-ID)
- An associated DACL
- An associated VLAN
- An associated SGACL
- Any number of other dictionary-based attributes

Authorization Policy

An authorization policy can consist of a single rule or a set of rules that are user-defined. These rules act to create a specific policy. For example, a standard policy can include the rule name using an If-Then convention that links a value entered for identity groups with specific conditions or attributes to produce a specific set of permissions that create a unique authorization profile. There are two authorization policy options you can set:

- First Matched Rules Apply
- Multiple Matched Rule Applies

These two options direct Cisco ISE to use either the first matched or the multiple matched rule type listed in the standard policy table when it matches the user's set of permissions. These are the two types of authorization policies that you can configure:

- Standard—Standard policies are policies created to remain in effect for long periods of time, to apply to a larger group of users, devices, or groups, and to allow access to specific or all network endpoints. Standard policies are intended to be stable and apply to a large groups of users, devices, and groups that share a common set of privileges.

  Standard policies can be used as templates that you modify to serve the needs of a specific identity group, using specific conditions or permissions, to create another type of standard policy to meet the needs of new divisions, or user groups, devices, or network groups.

- Exception—By contrast, exception policies are appropriately named because this type of policy acts as an exception to the standard policies. Exception polices are intended for authorizing limited access that is based on a variety of factors, such as short-term policy duration, specific types of network devices, network endpoints or groups, or the need to meet special conditions or permissions or an immediate requirement.

  Exception policies are created to meet an immediate or short-term need, such as authorizing a limited number of users, devices, or groups to access network resources. An exception policy lets you create a specific set of customized values for an identity group, condition, or permission that are tailored for one user or a subset of users. This allows you to create different or customized policies to meet your corporate, group, or network needs.

Access Control Lists

An Access Control List (ACL) in the Cisco ISE system is a list of permissions attached to a specific object or network resource. An ACL specifies which users or groups are granted access to an object, as well as what operations are allowed on a given object or network resource. Each entry in a typical ACL specifies a subject and an operation or provides the state (such as, Permit or Deny).

Authorization Policies and Supported Dictionaries

For authorization policy types, the verification must comply with the authorization profiles to be returned.

Verifications typically include one or more conditions that include a user-defined name that can then be added to a library and reused by other policies. You define conditions using the attributes from the Cisco ISE dictionary, which supports the following dictionaries:

- System-defined dictionary:
  - RADIUS
- RADIUS-vendor dictionaries
  - Airespace
  - Cisco
  - Cisco-BBSM
  - Cisco-VPN3000
  - Microsoft

Guidelines for Configuring Authorization Policies and Profiles

Observe the following guidelines when managing or administering authorization polices and profiles:

- Rule names you create must use only the following supported characters:
  - Symbols: plus (+), hyphen (-), underscore (_), period (.), and a space ( ).
  - Alphabetic characters: A-Z and a-z.
  - Numeric characters: 0-9.
- Identity groups default to “Any” (you can use this global default to apply to all users).
- Conditions allow you to set one or more policy values. However, conditions are optional and are not required to create an authorization policy. These are the two methods for creating conditions:
  - Choose an existing condition or attribute from a corresponding dictionary of choices.
  - Create a custom condition that allows you to select a suggested value or use a text box to enter a custom value.
- Condition names you create must use only the following supported characters:
  - Symbols: hyphen (-), underscore (_), and period (.).

  - Alphabetic characters: A-Z and a-z.
  - Numeric characters: 0-9.

- Permissions are important when choosing an authorization profile to use for a policy. A permission can grant access to specific resources or allow you to perform specific tasks. For example, if a user belongs to a specific identity group (such as Device Admins), and the user meets the defined conditions (such as a site in Boston), then this user is granted the permissions associated with that group (such as access to a specific set of network resources or permission to perform a specific operation on a device).
- When you use the **radius** attribute **Tunnel-Private-Group-ID** in an authorization condition, you must mention both the tag and the value in the condition when the **EQUALS** operator is being used, for example:

  ```
  Tunnel-Private-Group-ID EQUALS (tag=0) 77
  ```

- Make sure that you click Save to save the new or modified policy or profile in the Cisco ISE database.

Note As of Cisco ISE 1.4, ANC replaces Endpoint Protection Services (EPS). ANC provides additional classifications, and performance improvements. While using ERS attributes in a policy might still work for some ANC actions some of the time, you should use ANC attributes. For example, **Session:EPSStatus=Quarantine** may fail. Use **Session:ANCPolicy** as a condition in a policy.

Default Authorization Policy, Rule, and Profile Configuration

The Cisco ISE software comes installed with a number of preinstalled default conditions, rules, and profiles that provide common settings that make it easier for you to create the rules and policies required in Cisco ISE authorization policies and profiles.

The table describes built-in configuration defaults that contain specified values in Cisco ISE.

Table 1: Authorization Policy, Profile, and Rule Configuration Defaults

Name	Path in the User Interface	Description	Additional Information
Authorization Policy Configuration Defaults			

Name	Path in the User Interface	Description	Additional Information
Default Compound Conditions for Authorization Policies	Policy > Policy Elements > Conditions > Authorization	These are preinstalled configuration defaults for conditions, rules, and profiles to be used in authorization policies.	You can use the related attributes for creating authorization policies: • Wired 802.1x • Wired MAB • Wireless 802.1x • Catalyst Switch Local Web authentication • WLC Web authentication
Wired MAB Compound Condition	Policy > Policy Elements > Conditions > Authorization > Compound Conditions	This compound condition checks for the following attributes and values: • RADIUS:Service-Type = Call-Check • RADIUS:NAS-Port-Type = Ethernet	This compound condition is used in the Wired MAB authorization policy. Any request that matches the criteria specified in this policy would be evaluated based on the Wired MAB authorization policy.
Wireless 802.1X Compound Condition	Policy > Policy Elements > Conditions > Authorization > Compound Conditions	This compound condition checks for the following attributes and values: • RADIUS:Service-Type = Framed • RADIUS:NAS-Port-Type = Wireless-IEEE802.11	This compound condition is used in the Wireless 802.1X authorization policy. Any request that matches the criteria specified in this policy would be evaluated based on the Wireless 802.1X authorization policy.
Authorization Profile Configuration Defaults			
Blacklist_Access	Policy > Policy Elements > Results > Authorization Profiles > Blacklist_Access	This authorization profile rejects access to devices that are block listed. All block listed devices are redirected to the following URL: https://portal.ise.pot/gateway?portalId=PortalID	This default authorization profile is applied for all endpoints that are declared as “lost” in the My Devices Portal.

Name	Path in the User Interface	Description	Additional Information
Cisco_IP_Phones	Policy > Policy Elements > Results > Authorization Profiles > Cisco_IP_Phones	This authorization profiles uses a configuration default profile with the following values: • Name: Cisco IP Phones • DACL: PERMIT_ALL_TRAFFIC • VSA: cisco-av-pair=device-traffic-class=voice This profile will evaluate requests that match the criteria specified in this profile.	This default authorization profile uses the DACL and vendor-specific attribute (VSA) to authorize all "voice" traffic (PERMIT_ALL_TRAFFIC).
Authorization Policy Configuration Defaults			
Wired 802.1X Compound Condition	Policy > Policy Elements > Conditions > Authorization > Compound Conditions	This compound condition checks for the following attributes and values: • RADIUS:Service-Type = Framed • RADIUS:NAS-Port-Type = Ethernet	This compound condition is used in the Wired 802.1X authorization policy. Any request that matches the criteria specified in this policy would be evaluated based on the Wired 802.1X authorization policy.
Catalyst Switch Local Web Authentication Compound Condition	Policy > Policy Elements > Conditions > Authorization > Compound Conditions	This compound condition checks for the following attributes and values: • RADIUS:Service-Type = Outbound • RADIUS:NAS-Port-Type = Ethernet	To use this compound condition, you must create an authorization policy that would check for this condition.
Wireless Lan Controller (WLC) Local Web Authentication Compound Condition	Policy > Policy Elements > Conditions > Authorization > Compound Conditions	This compound condition checks for the following attributes and values: • RADIUS:Service-Type = Outbound • RADIUS:NAS-Port-Type = Wireless-IEEE802.11	To use this compound condition, you must create an authorization policy that would check for this condition.

Name	Path in the User Interface	Description	Additional Information
Black List Default Authorization Rule	Policy > Authorization Policy	This authorization policy uses a configuration default rule with the following values: • Rule Name: Black List Default • Endpoint Identity Group: Blacklist • Conditions: Any • Permissions/Authorization Profile: Blacklist_Access	This default rule is designed to appropriately provision “lost” user devices until they are either removed from the system or “reinstated.”
Profiled Cisco IP Phones Authorization Rule	Policy > Authorization Policy	This authorization policy uses a configuration default rule with the following values: • Rule Name: Profiled Cisco IP Phones • Endpoint Identity Group: Cisco-IP-Phones • Conditions: Any • Permissions/Authorization Profile: Cisco_IP_Phones	This default rule uses Cisco IP Phones as its default endpoint identity group and the values listed in this table.
Authorization Rule Configuration Defaults			
Default Authorization Rule	Policy > Authorization Policy	This authorization policy uses a configuration default rule with the following values: • Rule Name: Default • Endpoint Identity Group: Any • Conditions: Any • Authorization Profile: PermitAccess	This default rule uses “any” as its default endpoint identity group and the values listed in this table.

Default Authorization Rules

The Cisco ISE software comes with a number of pre-configured authorization rules that make it easier for you to create the authorization policies and profiles. These rules are disabled by default. You can enable these rules based on your requirements.

Table 2: **Pre-configured Authorization Rules**

Rule Name	Description	Conditions	Permissions
Basic_Authenticated_Access	To enable access to authenticated users.	Network_Access_Authentication_Passed	PermitAccess
Wi-Fi_Redirect_to_Guest_Login	To redirect users to the CWA Portal.	Wireless_MAB	Cisco_WebAuth
Wi-Fi_Guest_Access	To permit Guest access, after a Guest user is authenticated from the WebAuth.	(GuestType_Daily (default) OR GuestType_Weekly (default) OR GuestType_Contractor (default)) AND (Wireless_MAB AND Guest_Flow)	Guest AND PermitAccess
Compliant_Devices_Access	To enable access for compliant devices.	Compliant_Devices	PermitAccess
Employee_Onboarding	Any wireless 802.1X authentication that uses MSCHAPv2 would be redirected to the Native Supplicant Provisioning process.	(Wireless_802.1X AND EAP-MSCHAPv2)	NSP_Onboard AND BYOD

Note The pre-configured authorization rules are available only on new installations. These rules are not available if you are upgrading from earlier versions of Cisco ISE.

Configure Authorization Policies

The Authorization Policy page lets you display, create, duplicate, modify, or delete authorization policies. The following authorization policy profile sections reference example actions directed at a standard authorization policy. You can follow the same process for managing an exception authorization policy.

Before you begin

Before you begin this procedure, you should have a basic understanding of simple and rule-based conditions, the basic building blocks of identity groups, conditions, and permissions, and how they are used in the Admin portal.

Step 1 Choose **Policy** > **Authorization** > **Standard**.

Step 2 Click the down arrow on the far-right and select either **Insert New Rule Above** or **Insert New Rule Below**.

Step 3 Enter the rule name and select identity group, condition, attribute and permission for the authorization policy.

Not all attributes you select will include the "Equals," "Not Equals," "Matches," "Starts With," or "Not Starts With" operator options.

The "Matches" operator supports and uses regular expressions (REGEX) not wildcards.

Note You must use the "equals" operator for straight forward comparison. "Contains" operator can be used for multi-value attributes. "Matches" operator should be used for regular expression comparison. When "Matches" operator is used, regular expression will be interpreted for both static and dynamic values.

Step 4 Click **Done**.

Step 5 Click **Save** to save your changes to the Cisco ISE system database and create this new authorization policy.

Related Topics

Create Simple Conditions
Create Compound Conditions
Simple and Compound Conditions
Authorization Policy Settings

Authorization Policy Attributes and Conditions

To reuse a valid attribute when creating authorization policy conditions, select it from a dictionary that contains the supported attributes. For example, Cisco ISE provides an attribute named AuthenticationIdentityStore, which is located in the NetworkAccess dictionary. This attribute identifies the last identity source that was accessed during the authentication of a user:

- When a single identity source is used during authentication, this attribute includes the name of the identity store in which the authentication succeeded.
- When an identity source sequence is used during authentication, this attribute includes the name of the last identity source accessed.

You can use the AuthenticationStatus attribute in combination with the AuthenticationIdentityStore attribute to define a condition that identifies the identity source to which a user has successfully been authenticated. For example, to check for a condition where a user authenticated using an LDAP directory (LDAP13) in the authorization policy, you can define the following reusable condition:

```
If NetworkAccess.AuthenticationStatus EQUALS AuthenticationPassed AND
NetworkAccess.AuthenticationIdentityStore EQUALS LDAP13
```

Note The AuthenticationIdentityStore represents a text field that allows you to enter data for the condition. Ensure that you enter or copy the name correctly into this field. If the name of the identity source changes, you must ensure to modify this condition to match the change to the identity source.

To define authorization conditions that are based on an endpoint identity group that has been previously authenticated, Cisco ISE supports authorization that was defined during endpoint identity group 802.1X authentication status. When Cisco ISE performs 802.1X authentication, it extracts the MAC address from the "Calling-Station-ID" field in the RADIUS request and uses this value to look up and populate the session cache for the device's endpoint identity group (defined as an endpointIDgroup attribute).

This process makes the endpointIDgroup attribute available for use in creating authorization policy conditions, and allows you to define an authorization policy based on endpoint identity group information using this attribute, in addition to user information.

The condition for the endpoint identity group can be defined in the ID Groups column of the authorization policy configuration page. Conditions that are based on user-related information need to be defined in the "Other Conditions" section of the authorization policy. If user information is based on internal user attributes, then use the ID Group attribute in the internal user dictionary. For example, you can enter the full value path in the identity group using a value like "User Identity Group:Employee:US".

ISE Community Resource

For an example of how to configure authorization policies in Cisco ISE based on SSIDs, see ISE Policies Based on SSID Configuration Example.

Time and Date Conditions

Use the Policy Elements Conditions page to display, create, modify, delete, duplicate, and search time and date policy element conditions. Policy elements are shared objects that define a condition that is based on specific time and date attribute settings that you configure.

Time and date conditions let you set or limit permission to access Cisco ISE system resources to specific times and days as directed by the attribute settings you make.

Related Topics

Time and Date Condition Settings
Create Time and Date Conditions

Use IPv6 Condition Attributes in Authorization Policies

Cisco ISE can detect, manage, and secure IPv6 traffic from endpoints.

When an IPv6-enabled endpoint connects to the Cisco ISE network, it communicates with the Network Access Device (NAD) over an IPv6 network. The NAD conveys the accounting and profiling information from the endpoint (including IPv6 values) to Cisco ISE over an IPv4 network. You can configure authorization profiles and policies in Cisco ISE using the IPv6 attributes in your rule conditions to process such requests from IPv6-enabled endpoints and ensure that the endpoint is compliant.

You can use wildcard characters in IPv6 prefix and IPv6 interface values. For example: 2001:db8:1234::/48.

Supported IPv6 address formats include:

- Full notation: Eight groups of four hexadecimal digits separated by colons. For example, 2001:0db8:85a3:0000:0000:8a2e:0370:7334
- Shortened notation: Exclude leading zeros in a group; replace groups of zeros with two consecutive colons. For example: 2001:db8:85a3::8a2e:370:7334
- Dotted-quad notation (IPv4-mapped and IPv4 compatible-IPv6 addresses): For example, ::ffff:192.0.2.128

Supported IPv6 attributes include:

- NAS-IPv6-Address
- Framed-Interface-Id
- Framed-IPv6-Prefix
- Login-IPv6-Host
- Framed-IPv6-Route
- Framed-IPv6-Pool
- Delegated-IPv6-Prefix
- Framed-IPv6-Address
- DNS-Server-IPv6-Address
- Route-IPv6-Information
- Delegated-IPv6-Prefix-Pool
- Stateful-IPv6-Address-Pool

The following table lists Supported Cisco Attribute-Value pairs and their equivalent IETF attributes:

Cisco Attribute-Value Pairs	IETF Attributes
ipv6:addrv6=<ipv6 address>	Framed-ipv6-Address
ipv6:stateful-ipv6-address-pool=<name>	Stateful-IPv6-Address-Pool
ipv6:delegated-ipv6-pool=<name>	Delegated-IPv6-Prefix-Pool
ipv6:ipv6-dns-servers-addr=<ipv6 address>	DNS-Server-IPv6-Address

The RADIUS Live Logs page, RADIUS Authentication report, RADIUS Accounting report, Current Active Session report, RADIUS Error report, Misconfigured NAS report, EPS Audit report, and Misconfigured Supplicant report support IPv6 addresses. You can view the details about these sessions from the RADIUS Live Logs page or from any of these reports. You can filter the records by IPv4, IPv6, or MAC addresses.

Note If you connect an Android device to an IPv6 enabled DHCPv6 network, it receives only the link-local IPv6 address from the DHCP server. Hence, global IPv6 address is not displayed in the Live Logs and in the Endpoints page (**Work Centers** > **Network Access** > **Identities** > **Endpoints**).

The following procedure describes how to configure IPv6 attributes in authorization policies.

Before you begin

Ensure that the NADs in your deployment support AAA with IPv6. See **AAA Support for IPv6** for information on how to enable AAA support for IPv6 on your NADs.

Step 1 Choose **Policy** > **Authorization** > **Standard**.

Step 2 Click the down arrow on the far right and select either **Insert New Rule Above** or **Insert New Rule Below**.

Step 3 Enter the rule name and specify the condition.

From the RADIUS dictionary, choose the RADIUS IPv6 attribute, the operator, and the value.

Step 4 Click **Done**.

Permissions for Authorization Profiles

Before you start configuring permissions for authorization profiles, make sure you:

- Understand the relationship between authorization policies and profiles.
- Are familiar with the **Authorization Profile** page.
- Know the basic guidelines to follow when configuring policies and profiles.
- Understand what comprises permissions in an authorization profile.

To work with authorization profiles, choose **Policy** > **Policy Elements** > **Results**. From the menu on the left, choose **Authorization** > **Authorization Profiles**.

Use the **Results** navigation pane as your starting point in the process for displaying, creating, modifying, deleting, duplicating, or searching policy element permissions for the different types of authorization profiles on your network. The **Results** pane initially displays Authentication, Authorization, Profiling, Posture, Client Provisioning, and Trustsec options.

Authorization profiles let you choose the attributes to be returned when a RADIUS request is accepted. Cisco ISE provides a mechanism where you can configure **Common Tasks Settings** to support commonly used attributes. You must enter the value for **Common Tasks Attributes**, which Cisco ISE translates to the underlying RADIUS values.

ISE Community Resource

For an example of how to configure Media Access Control Security (MACsec) encryption between an 802.1x supplicant (Cisco AnyConnect Mobile Security) and an authenticator (switch), see MACsec Switch-host Encryption with Cisco AnyConnect and ISE Configuration Example.

Related Topics

Authorization Policies and Supported Dictionaries, on page 4
Guidelines for Configuring Authorization Policies and Profiles, on page 4
Configure Permissions for New Standard Authorization Profiles, on page 14
Default Authorization Policy, Rule, and Profile Configuration, on page 5
Default Authorization Rules, on page 9

Configure Permissions for New Standard Authorization Profiles

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

Step 2 Click **Add.**

Step 3 Enter values as required to configure a new authorization profile. Supported characters for the name field are: space, ! # $ % & ‘ ( ) * + , - . / ; = ? @ _ {. Once you configure the profile, you can double-check the RADIUS syntax from the **Attributes Details** that dynamically appear at the bottom of the screen.

Step 4 Click **Submit** to save your changes to the Cisco ISE system database to create an authorization profile.

Related Topics

Authorization Profile Settings

Downloadable ACLs

Access control lists (ACLs) are lists of access control entries (ACEs), which may be applied by a Policy Enforcement Point (for example, a switch) to a resource. Each ACE identifies the permissions allowed per user for that object, such as read, write, execute and more. For example, an ACL may be configured for use the Sales area of the network, with an ACE allowing Write permissions for the Sales group and a separate ACE allowing Read permissions for all other employees of the organization. With RADIUS protocol, ACLs grant authorization by filtering source and destination IP addresses, transport protocols, and additional parameters. Static ACLs reside on and are directly configured from the switch and can be applied in your authorization policies from the ISE GUI; downloadable ACLs (DACLs) can be configured, managed and applied in your authorization policies from the ISE GUI.

To implement DACLs in your network authorization policy in ISE:

1. Configure a new or existing DACL from **Policy** > **Policy Elements** > **Results** > **Downloadable ACLs**. For more information see Configure Permissions for Downloadable ACLs, on page 14.
2. Configure a new or existing authorization profile from **Policy** > **Policy Elements** > **Results** > **Authorization Profiles**, using any of the DACLs you already configured.

Related Topics

Configure Permissions for Downloadable ACLs, on page 14

Configure Permissions for Downloadable ACLs

With ISE, downloadable ACLs (DACLs) can be configured and implemented in your authorization policies for control of how the network is accessed by different users and groups of users. Default authorization DACLs are available with installation of ISE, including the following default profiles:

- DENY_ALL_TRAFFIC
- PERMIT_ALL_TRAFFIC

When working with DACLs, these defaults cannot be changed, but you can duplicate them in order to create additional, similar, DACLs.

Step 1 Choose **Policy** > **Policy Elements** > **Results** > **Authorization** > **Downloadable ACLs**.

Step 2 Click **Add** from the top of the **Downloadable ACLs** table or alternatively, choose any of the existing DACLs and click **Duplicate** from the top of the table.

Step 3 Enter or edit the desired values for the DACL, keeping in mind the following rules:

- Supported characters for the name field are: alphanumeric, hyphen(-), dot(.) and underscore(_)
- The keyword **Any** must be the source in all ACEs in the DACL. Once the DACL is pushed, the **Any** in the source is replaced with the IP address of the client that is connecting to the switch.

Note The **IP Version** field is noneditable when DACL is mapped to any authorization profile. In this case, remove the DACL reference from **Authorization Profiles**, edit the IP version and remap the DACL in **Authorization Profiles**.

Step 4 Optionally, when you finish creating the complete list of ACEs, click **Check DACL Syntax** to validate the list. If there are validation errors, the check returns specific instructions identifying the invalid syntax in the window that opens automatically.

Step 5 Click **Submit**.

Related Topics

Configure Permissions for Downloadable ACLs, on page 14

Machine Access Restriction for Active Directory User Authorization

Cisco ISE contains a Machine Access Restriction (MAR) component that provides an additional means of controlling authorization for Microsoft Active Directory-authentication users. This form of authorization is based on the machine authentication of the computer used to access the Cisco ISE network. For every successful machine authentication, Cisco ISE caches the value that was received in the RADIUS Calling-Station-ID attribute (attribute 31) as evidence of a successful machine authentication.

Cisco ISE retains each Calling-Station-ID attribute value in cache until the number of hours that was configured in the “Time to Live” parameter in the Active Directory Settings page expires. Once the parameter has expired, Cisco ISE deletes it from its cache.

When a user authenticates from an end-user client, Cisco ISE searches the cache for a Calling-Station-ID value from successful machine authentications for the Calling-Station-ID value that was received in the user authentication request. If Cisco ISE finds a matching user-authentication Calling-Station-ID value in the cache, this affects how Cisco ISE assigns permissions for the user that requests authentication in the following ways:

- If the Calling-Station-ID value matches one found in the Cisco ISE cache, then the authorization profile for a successful authorization is assigned.
- If the Calling-Station-ID value is not found to match one in the Cisco ISE cache, then the authorization profile for a successful user authentication without machine authentication is assigned.