Managing Authorization Policies and Profiles

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 permissions element that maps to an authorization profile.

This chapter provides a description of authorization policies and provides example procedures for the following authorization policy-related tasks:

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”).

Related Topic

- For more information on endpoint identity groups, see Identified Endpoints Grouped in Endpoint Identity Groups, page 21-42.

Cisco ISE Authorization Profiles

Network 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 a dictionary and these are returned when the compound condition for the specific authorization policy matches. Because authorization policies can include compound conditions 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, page 20-2
- Authorization Policies and Supported Dictionaries, page 20-4
- Configuring Authorization Policies, page 20-8
- Chapter 18, “Setting Up Policy Conditions”
- Permissions for Authorization Profiles, page 20-10
- Configuring Permissions for Downloadable ACLs, page 20-13

Authorization Policy Terminology

The following is basic terminology used for Cisco ISE authorization policies and profiles:

- Authorization Profile, page 20-3
- Authorization Policy, page 20-3
- Access Control Lists, page 20-4
- Network Authorization, page 20-2
- Policy Elements, page 20-3

Network Authorization

Authorization is an important requirement to ensure which users can access the Cisco ISE network and its resources. Network authorization controls user access to the network and its resources and what each user can do on the system with those resources. The Cisco ISE network defines 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 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). Cisco ISE also uses downloadable ACL (DACLs).

Authorization Policies and Supported Dictionaries

For both simple and compound 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

See the "Dictionaries and Dictionary Attributes" section on page 10-1 for more information on Cisco ISE dictionaries.

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

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. These built-in configuration defaults contain specified values that are described in Table 20-1.

Table 20-1 Authorization Policy, Profile, and Rule Configuration Defaults

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

Table 20-1 Authorization Policy, Profile, and Rule Configuration Defaults (continued)

Name	Path in the User Interface	Description	Additional Information
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 blacklisted. All blacklisted devices are redirected to the following URL: url-redirect=https://ip:port/mydevices/blackhole.jsp	This default authorization profile is applied for all endpoints that are declared as "lost" in the My Devices Portal.
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).

Table 20-1 Authorization Policy, Profile, and Rule Configuration Defaults (continued)

Name	Path in the User Interface	Description	Additional Information
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.
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.”

Table 20-1 Authorization Policy, Profile, and Rule Configuration Defaults (continued)

Name	Path in the User Interface	Description	Additional Information
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.

Configuring 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.

Step 4 Click **Done**.

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

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”.

Related Topics

- Authorization Policy Settings, page B-5
- Simple and Compound Conditions, page 18-1
- Creating Simple Conditions, page 18-2
- Creating Compound Conditions, page 18-3

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

- Creating Time and Date Conditions, page 18-8
- Time and Date Condition Settings, page B-17

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
- Are aware of configuration default values that are described in the following topics:
  - Authorization Policies and Supported Dictionaries, page 20-4
  - Guidelines for Configuring Authorization Policies and Profiles, page 20-4
  - Default Authorization Policy, Rule, and Profile Configuration, page 20-5

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 Security Group Access 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 the Common Tasks attributes, which Cisco ISE translates to the underlying RADIUS values.

Related Topic

Configuring Permissions for New Standard Authorization Profiles, page 20-10

Configuring Permissions for New Standard Authorization Profiles

Use the Authorization profiles page to create a new standard authorization profile and configure its permissions.

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, ! # $ % & ‘ ( ) * + , - . / ; = ? @ _ {.

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

Related Topics

Authorization Profile Settings, page B-23

Downloadable ACLs

You can define DACLs for the Access-Accept message to return. Use ACLs to prevent unwanted traffic from entering the network. ACLs can filter source and destination IP addresses, transport protocols, and more by using the RADIUS protocol.

After you create DACLs as named permission objects, you can add them to authorization profiles, which you can then specify as the result of an authorization policy.

You can duplicate a DACL if you want to create a new DACL that is the same, or similar to, an existing downloadable ACL.

After duplication is complete, you access each DACL (original and duplicated) separately to edit or delete them.

Note While creating DACL, the keyword *Any* must be the source in all ACE in 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.

Related Topic

Configuring Permissions for Downloadable ACLs, page 20-13

Supported DACL Format, page 20-11

Supported DACL Format

The following is the supported format for DACL referenced by an inline posture authorization profile:

- **ACTION PROTOCOL SOURCE_SUBNET WILDCARD_MASK** [**OPERATOR**[*PORT*]] **DEST_SUBNET WILDCARD_MASK** [**OPERATOR**[*PORT*]] [*ICMP_TYPE_CODE*]

Table 20-2 describes the options in the DACL format.

Table 20-2 DACL Format - Options

Option	Description
ACTION	Specifies whether the policy element permissions should permit or deny access.
PROTOCOL	Specifies any one of the following protocols: • ICMP • UDP • TCP • IP
SOURCE_SUBNET	Specifies any one of the following source subnet formats: • any • host x.x.x.x • <subnet>
DEST_SUBNET	Specifies any one of the following destination subnet formats: • any • host x.x.x.x • <subnet>
WILDCARD_MASK	Specifies the inverse of the subnet mask. For example, 0.0.0.255.
OPERATOR	Specifies any one of the following operators: • eq • lt • gt • neq • range
PORT	Specifies the port. The valid range is from 1 to 65535.
ICMP_TYPE_CODE	Specifies any one of the following ICMP type codes: • 0—Echo reply • 8—Echo request • 3:[0-15]—Destination unreachable • 5:[0-3]—ICMP redirects

Examples of acceptable ACL Format:

permit tcp any host 192.168.1.100 eq 80—permits www traffic from anywhere to host 192.168.1.100

permit udp any eq 68 any eq 67—permits dhcp traffic

permit icmp any any 8, permit icmp any any 0—allows icmp echo-request and echo-reply

deny icmp any any 5:0—denies icmp network redirects

permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255—permits all traffic from 192.168.2.0 subnet to 192.168.1.0 subnet

permit udp any any range 16384 32767—permits voice traffic using range of udp ports

Examples of incorrect syntax:

permit ip 192.168.2.100 192.168.1.100—host/wildcard keyword missing

permit tcp host 192.168.2.100 host 192.168.1.100 eq 88 389 636 454 3268 3269 1025 1026 (You cannot club multiple ports using eq operator, and this ACL needs to be split into multiple lines one for each destination port)

Note Ensure that there are no empty spaces or hidden characters in the DACL syntax. Any unknown characters, if exists in the DACL syntax, the Inline Posture node will not accept the DACL. For more information, refer to the Inline Posture logs.

Configuring Permissions for Downloadable ACLs

Use the Downloadable ACLs page to create a new DACL and configure its permissions.

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

Step 2 Click the **action** icon and select **Create DACL** or click **Add** in the DACL Management page.

Step 3 Enter the desired values for the DACL. Supported characters for the name field are: space, ! # $ % & ‘ ( ) * + , - . / ; = ? @ _ {.

Step 4 Click **Submit**.

Related Topic

Downloadable ACLs, page 20-11

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.

Related Topics

User and Machine Authentication in Active Directory, page 14-9