CHAPTER 19

Setting Up Policy Conditions

Cisco ISE is a policy-based, network-access-control solution, which offers the following services: network-access, guest, posture, client provisioning, and profiler services. While configuring Cisco ISE, you create authentication, authorization, guest, posture, and profiler policies. Policy conditions are basic building blocks of policies. There are two types of policy conditions, simple and compound.

This chapter describes the policy conditions and how you can create them for the various services that Cisco ISE offers.

This chapter contains the following sections:

Simple and Compound Conditions

Cisco ISE uses rule-based policies to provide network access, profiler, posture, and guest services. These rule-based policies consist of rules that are made up of conditions. Cisco ISE allows you to create conditions as individual, reusable policy elements that can be referred from other rule-based policies. There are two types of conditions:

- Simple condition—A simple condition consists of an operand (attribute), an operator (equal to, not equal to, greater than, and so on), and a value. You can save simple conditions and use them in other rule-based policies.

  Simple condition takes the form: A operand B, where A can be any attribute from the Cisco ISE dictionary and B can be one of the values that the attribute A can take. The Device Type is used as an attribute for all network devices that can include all device types as its value, which means that A Equals B in the following form:

  DEVICE:Device Type Equals All Device Types

- Compound condition—A compound condition is made up of one or more simple conditions that are connected by the AND or OR operator. Compound conditions are built on top of simple conditions. You can save and reuse compound conditions in other rule-based policies.

Compound condition can take any one of the following forms:

- (X operand Y) AND (A operand B) AND (X operand Z) AND so on
- (X operand Y) OR (A operand B) OR (X operand Z) OR so on

  where X and A are attributes from the Cisco ISE dictionary such as the username and device type.

This is an example of a compound condition:

DEVICE:Model Name Matches Catalyst6K AND Network Access:Use Case Equals Host Lookup.

You cannot delete conditions that are used in a policy or are part of a compound condition.

Related Topics

- Creating Simple Conditions, page 19-2
- Creating Compound Conditions, page 19-3

Policy Evaluation

Typically, policies consist of rules, where each rule consists of conditions to be satisfied that allow actions to be performed such as access to network resources. Rule-based conditions form the basis of policies, the sets of rules used when evaluating requests.

At run-time, Cisco ISE evaluates the policy conditions and then applies the result that you define based on whether the policy evaluation returns a true or a false value.

During policy-condition evaluation, Cisco ISE compares an attribute with a value. It is possible that where the attribute specified in the policy condition may not have a value assigned in the request. In such cases, if the operator that is used for comparison is “not equal to,” then the condition will evaluate to true. In all other cases, the condition will evaluate to false.

For example, in the condition Radius.Calling_Station_ID Not Equal to 1.1.1.1, if the Calling Station ID is not present in the RADIUS request, then this condition will evaluate to true. This evaluation is not unique to the RADIUS dictionary and occurs because of the usage of the “Not Equal to” operator.

Creating Simple Conditions

You can create simple conditions and reuse them when you define authentication, authorization, or guest policies.

Before You Begin

To perform the following task, you must be a Super Admin or Policy Admin.

Step 1 Choose **Policy > Policy Elements > Conditions**.

Step 2 Click the arrow next to **Authentication** or **Authorization** or **Guest,** and then click **Simple Conditions**.

Step 3 Click **Add**.

Step 4 Enter appropriate values for the Name, Description, Attribute, Operator, and Value fields.

Note If you specify any Identity Group in simple conditions, ensure that you represented them in FQDN form, like the following:

```
(InternalUser:IdentityGroup) : Equal : (User Identity Groups:Identity Group Name)
```

Cisco ISE will not accurately resolve Identity Group entries in the following form:

```
(InternalUser:IdentityGroup) : Equal :  (Identity Group Name).
```

Step 5 Click **Submit** to save the condition.

What to Do Next

- See the "Creating a Rule-Based Authentication Policy" section on page 16-27 for information on how to define a rule-based authentication policies using simple conditions.
- See the "Configuring Authorization Policies" section on page 17-8 for information on how to create authorization policies using simple conditions.
- See the "Creating a Sponsor Group Policy" section on page 17-6 for information on how to define sponsor group policies using simple conditions.

Creating Compound Conditions

You can create compound conditions and reuse them when you define authentication policies.

Before You Begin

- Cisco ISE includes predefined compound conditions for some of the most common use cases. You can edit these predefined conditions to suit your requirements.
- To perform the following task, you must be a Super Admin or Policy Admin.

Step 1 Choose **Policy > Policy Elements > Conditions**.

Step 2 Click the arrow next to **Authentication** or **Authorization** or **Guest** and then click **Compound Conditions**.

Step 3 Click **Add.**

Step 4 Enter a name for the compound condition. You can enter an optional description.

Step 5 Click **Select Existing Condition from Library** to choose an existing simple condition or click **Create New Condition** to choose an attribute, operator, and value from the expression builder.

Step 6 Click the action icon at the end of this row to add more conditions.

Step 7 Click **Add Attribute/Value** to create a new condition or click **Add Condition from Library** to add an existing simple condition.

Step 8 Select operand from the drop-down list. You can choose AND or OR and the same operand will be used between all the conditions in this compound condition.

Step 9 Click **Submit** to create the compound condition.

What to Do Next

- See the "Creating a Rule-Based Authentication Policy" section on page 16-27 for information on how to define a rule-based authentication policies using compound conditions
- See the "Configuring Authorization Policies" section on page 17-8 for information on how to create authorization policies using compound conditions.
- See the "Creating a Sponsor Group Policy" section on page 17-6 for information on how to define sponsor group policies using compound conditions.

Profiler Conditions

Profiling conditions are policy elements and are similar to other conditions. However unlike authentication, authorization, and guest conditions, the profiling conditions can be based on a limited number of attributes. The Profiler Conditions page lists the attributes that are available in Cisco ISE and their description. The upper limit for the number of profiling policies is 500.

Profiler conditions can be one of the following:

- Cisco Provided—Cisco ISE includes predefined profiling conditions when deployed and they are identified as Cisco Provided in the Profiler Conditions page. You cannot delete Cisco Provided profiling conditions.

  You can also find Cisco Provided conditions in the System profiler dictionaries in the following location: Policy > Policy Elements > Dictionaries > System.

  For example, MAC dictionary. For some products, the OUI (Organizationally Unique Identifier) is an unique attribute that you can use it first for identifying the manufacturing organization of devices. It is a component of the device MAC address. The MAC dictionary contains the MACAddress and OUI attributes.
- Administrator Created—Profiler conditions that you create as an administrator of Cisco ISE or predefined profiling conditions that are duplicated are identified as Administrator Created. You can create a profiler condition of DHCP, MAC, SNMP, IP, RADIUS, NetFlow, CDP, LLDP, and NMAP types using the profiler dictionaries in the Profiler Conditions page.

Creating a Profiler Condition

Endpoint profiling policies in Cisco ISE allow you to categorize discovered endpoints on your network, and assign them to specific endpoint identity groups. These endpoint profiling policies are made up of profiling conditions that Cisco ISE evaluates to categorize and group endpoints.

Before You Begin

To perform the following task, you must be a Super Admin or Policy Admin.

Step 1 Choose **Policy > Policy Elements > Conditions > Profiling > Add**.

Step 2 Enter values for the fields as described in the Profiler Condition Settings, page C-9.

Step 3 Click **Submit** to save the profiler condition.

Step 4 Repeat this procedure to create more conditions.

Related Topics

- Simple and Compound Conditions, page 19-1
- Policy Evaluation, page 19-2
- Profiler Condition Settings, page C-9

Posture Conditions

A posture condition can be any one of the following simple conditions: a file, a registry, an application, a service, or a dictionary condition. One or more conditions from these simple conditions form a compound condition, which can be associated to a posture requirement.

When you deploy Cisco ISE on your network for the first time, you can download posture updates from the web for the first time. This process is called the initial posture update.

After an initial posture update, Cisco ISE also creates Cisco defined simple and compound conditions. Cisco defined simple conditions have pc_ as their prefixes and compound conditions have pr_ as their prefixes.

You can also configure Cisco ISE to download the Cisco-defined conditions periodically as a result of dynamic posture updates through the web. You cannot delete or edit Cisco defined posture conditions.

A user defined condition or a Cisco defined condition includes both simple conditions and compound conditions.

Related Topics

- Downloading Posture Updates, page 24-9
- Simple and Compound Conditions, page 19-1
- Policy Evaluation, page 19-2
- Posture Conditions Settings, page C-10

Simple Posture Conditions

You can use the Posture navigation pane to manage the following simple conditions:

- File Conditions—A condition that checks the existence of a file, the date of a file, and the versions of a file on the client.
- Registry Conditions—A condition that checks for the existence of a registry key or the value of the registry key on the client.
- Application Conditions—A condition that checks if an application (process) is running or not running on the client.
- Service Conditions—A condition that checks if a service is running or not running on the client.
- Dictionary Conditions—A condition that checks a dictionary attribute with a value.

Related Topics

- Simple and Compound Conditions, page 19-1
- Policy Evaluation, page 19-2
- Posture Conditions Settings, page C-10

Creating Simple Posture Conditions

You can create file, registry, application, service, and dictionary simple conditions that can be used in posture policies or in other compound conditions.

Before You Begin

To perform the following task, you must be a Super Admin or Policy Admin.

Step 1 Choose **Policy > Policy Elements > Conditions > Posture**.

Step 2 Choose any one of the following: File, Registry, Application, Service, or Dictionary Simple Condition.

Step 3 Click **Add**.

Step 4 Enter the appropriate values in the fields.

Step 5 Click **Submit**.

Related Topics

- Simple and Compound Conditions, page 19-1
- Policy Evaluation, page 19-2
- File Condition Settings, page C-10
- Registry Condition Settings, page C-11
- Application Condition Settings, page C-12
- Service Conditions Settings, page C-13
- Dictionary Simple Conditions Settings, page C-16

padramak--will add the concept topic link as well.

hkearns--so would have xrefs to each table and also to the concept topic

Compound Posture Conditions

Compound conditions are made up of one or more simple conditions, or compound conditions. You can make use of the following compound conditions while defining a Posture policy.

- Compound Conditions—Contains one or more simple conditions, or compound conditions of the type File, Registry, Application, or Service condition
- Antivirus Compound Conditions—Contains one or more AV conditions, or AV compound conditions
- Antispyware Compound Conditions—Contains one or more AS conditions, or AS compound conditions
- Dictionary Compound Conditions—Contains one or more dictionary simple conditions or dictionary compound conditions

Related Topics

- Simple and Compound Conditions, page 19-1
- Policy Evaluation, page 19-2

- Posture Compound Condition Settings, page C-13
- Antivirus Compound Condition Settings, page C-13
- Antispyware Compound Condition Settings, page C-15
- Dictionary Compound Condition Settings, page C-16
- Antivirus and Antispyware Support Chart, page 19-7

Cisco-Predefined Condition for Enabling Automatic Updates in Windows Clients

The pr_AutoUpdateCheck_Rule is a Cisco predefined condition, which is downloaded to the Compound Conditions page. This condition allows you to check whether the automatic updates feature is enabled on Windows clients. If a Windows client fails to meet this requirement, then the Network Access Control (NAC) Agents enforce the Windows client to enable (remediate) the automatic updates feature. After this remediation is done, the Windows client becomes posture compliant. The Windows update remediation that you associate in the posture policy overrides the Windows administrator setting, if the automatic updates feature is not enabled on the Windows client.

Cisco-Preconfigured Antivirus and Antispyware Conditions

Cisco ISE loads preconfigured antivirus and antispyware compound conditions in the AV and AS Compound Condition pages, which are defined in the antivirus and antispyware support charts for Windows and Macintosh operating systems. These compound conditions can check if the specified antivirus and antispyware products exist on all the clients. You can also create new antivirus and antispyware compound conditions in Cisco ISE.

Antivirus and Antispyware Support Chart

Cisco ISE uses an antivirus and antispyware support chart, which provides the latest version and date in the definition files for each vendor product. Users must frequently poll antivirus and antispyware support charts for updates. The antivirus and antispyware vendors frequently update antivirus and antispyware definition files, look for the latest version and date in the definition files for each vendor product.

Each time the antivirus and antispyware support chart is updated to reflect support for new antivirus and antispyware vendors, products, and their releases, the NAC Agents receive a new antivirus and antispyware library. It helps NAC Agents to support newer additions. Once the NAC Agents retrieve this support information, they check the latest definition information from the periodically updated se-checks.xml file (which is published along with the se-rules.xml file in the se-templates.tar.gz archive), and determine whether clients are compliant with the posture policies. Depending upon what is supported by the antivirus and antispyware library for a particular antivirus, or antispyware product, the appropriate requirements will be sent to the NAC Agents for validating their existence, and the status of particular antivirus and antispyware products on the clients during posture validation.

The antivirus and antispyware support chart is available on Cisco.com at:

http://www.cisco.com/en/US/docs/security/ise/1.1/release_notes/win-avas-3-4-27-1.pdf

Creating Compound Posture Conditions

You can create compound conditions that can be used in posture policies for posture assessment and validation.

Before You Begin

To perform the following task, you must be a Super Admin or Policy Admin.

Step 1 Choose **Policy > Policy Elements > Conditions > Posture > Compound Conditions > Add**.

Step 2 Enter appropriate values for the fields.

Step 3 Click **Validate Expression** to validate the condition.

Step 4 Click **Submit**.

Related Topics

- Simple and Compound Conditions, page 19-1
- Policy Evaluation, page 19-2
- Posture Compound Condition Settings, page C-13
- Antivirus Compound Condition Settings, page C-13
- Antispyware Compound Condition Settings, page C-15
- Dictionary Compound Condition Settings, page C-16

Creating Time and Date Conditions

Time and date conditions allow you to limit or extend permission to access to Cisco ISE system resources.

Before You Begin

To perform the following task, you must be a Super Admin or Policy Admin.

Step 1 Choose **Policy > Policy Elements > Conditions > Time and Date > Add**.

Step 2 Enter appropriate values in the fields.

- In the Standard Settings area, specify the time and date to provide access.
- In the Exceptions area, specify the time and date range to limit access.

Step 3 Click **Submit**.

Related Topics

- Simple and Compound Conditions, page 19-1
- Policy Evaluation, page 19-2