Set Up Policy Conditions

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.

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.

Policy Evaluation

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.

In Cisco ISE, the **Policy** > **Policy Sets** table provides a list of all policy sets currently configured in the system. The order of the enabled policy sets determines the order by which the system searches for the relevant policy set every time an endpoint requests access. The last row in the **Policy** page is the default policy that will be applied if none of the rules match the request in any of the other configured policy sets. You can edit the allowed protocols and identity source selection in default policy set, but you cannot delete it.

Create 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.

If you specify any Identity Group in simple conditions, ensure that you represented them in FQDN form, like the following:
`(InternalUser:IdentityGroup) : Equal : (UserIdentityGroups: 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.

Related Topics

Policy Evaluation, on page 2
Simple and Compound Conditions, on page 1

Create 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.

Related Topics

Policy Evaluation, on page 2
Simple and Compound Conditions, on page 1

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.

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 window. 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** window.

Although, the recommended upper limit for the number of profiling policies is 1000, you can stretch up to 2000 profiling policies.

Create 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 Endpoint Profiling Policies Settings.

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

Step 4 Repeat this procedure to create more conditions.

Related Topics

Profiler Conditions, on page 4

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. 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.

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 or process is running or not running on the client.

Note If a process is installed and running, user is compliant. However, the Application condition works in reverse logic; If an application is not installed and not running, the end user is complaint. If an application is installed and running, the end user is non-complaint.

- 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.
- USB Conditions: A condition that checks for the presence of USB mass storage device.

Related Topics

File Condition Settings
Registry Condition Settings
Application Condition Settings
Service Condition Settings
Dictionary Simple Condition Settings
USB Condition Settings

Create 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**.

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
- Antimalware Conditions: Contains one or more AM conditions.

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 window. 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.

Preconfigured Antivirus and Antispyware Conditions

Cisco ISE loads preconfigured antivirus and antispyware compound conditions in the AV and AS Compound Condition windows, 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 agents receive a new antivirus and antispyware library. It helps the Agents to support newer additions. Once the 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 agents for validating their existence, and the status of particular antivirus and antispyware products on the clients during posture validation.

For more information on the antivirus and anti-malware products supported by the ISE posture agent, see the Cisco AnyConnect ISE Posture Support Charts: Cisco ISE Compatibility Guide.

You can verify the minimum compliance module version while creating an anti-malware posture condition. After the posture feed is updated, choose **Work Centers > Posture > Policy Elements > Anti-Malware Condition** and then choose the **Operating System** and **Vendor** to view the support chart.

Note Some of the Anti-Malware endpoint security solutions (such as FireEye, Cisco AMP, Sophos, and so on) require network access to their respective centralized service for functioning. For such products, AnyConnect ISE posture module (or OESIS library) expects the endpoints to have internet connectivity. It is recommended that internet access is allowed for such endpoints during pre-posture for these online agents (if offline detection is not enabled). Signature Definition condition might not be applicable in such cases.

Compliance Module

The compliance module contains a list of fields, such as vendor name, product version, product name, and attributes provided by OPSWAT that supports Cisco ISE posture conditions.

Vendors frequently update the product version and date in the definition files, therefore, you must look for the latest version and date in the definition files for each vendor product by frequently polling the compliance module for updates. Each time the compliance module is updated to reflect the support for new vendors, products, and their releases, the AnyConnect agent receives a new library. It helps the AnyConnect agent to support newer additions. The AnyConnect agent retrieves this support information and checks 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 library for a particular antivirus, antispyware, antimalware, disk encryption, or patch management product, the appropriate requirements will be sent to the AnyConnect agent for validating their existence, and the status of the particular products on the clients during posture validation.

The compliance module is available on Cisco.com.

Table given below lists the OPSWAT API versions that support and do not support the ISE posture policy. There are different policy rules for agents that support versions 3 and 4.

Table 1: OPSWAT API Versions

Posture Condition	Compliance Module Version
OPSWAT	
Antivirus	3.x or earlier
Antispyware	3.x or earlier
Antimalware	4.x or later
Disk Encryption	3.x or earlier and 4.x or later
Patch Management	3.x or earlier and 4.x or later
USB	4.x or later
Non-OPSWAT	
File	Any version
Application	Any version
Compound	Any version
Registry	Any version
Service	Any version

Note

- Be sure to create separate posture policies for version 3.x or earlier and version 4.x or later, in anticipation of clients that may have installed any one of the above versions.
- OESIS version 4 support is provided for compliance module 4.x and Cisco AnyConnect 4.3 and higher. However, AnyConnect 4.3 supports both OESIS version 3 and version 4 policies.
- Version 4 compliance module is supported by ISE 2.1 and higher.

Create 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

Posture Conditions, on page 5
Simple Posture Conditions, on page 5
Compound Posture Conditions, on page 6
Predefined Condition for Enabling Automatic Updates in Windows Clients, on page 6
Preconfigured Antivirus and Antispyware Conditions, on page 6

Create Patch Management Conditions

You can create a policy to check the status of a selected vendor's patch management product.

For example, you can create a condition to check if Microsoft System Center Configuration Manager (SCCM), Client Version 4.x software product is installed at an endpoint.

Note Supported versions of Cisco ISE and AnyConnect:

- Cisco ISE version 1.4 and later
- AnyConnect version 4.1 and later

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** > **Patch Management Condition**.
Step 2 Click **Add**.
Step 3 Enter the condition name and description in the **Name** and **Description** fields.
Step 4 Choose the appropriate operating system from the **Operating System** drop-down field.
Step 5 Choose the **Compliance Module** from the drop-down list.
Step 6 Choose the **Vendor Name** from the drop-down list.
Step 7 Choose the **Check Type.**
Step 8 Choose the appropriate patch from the **Check patches installed** drop-down list.
Step 9 Click **Submit**.

Related Topics

Patch Management Condition Settings
Add a Patch Management Remediation

Create Disk Encryption Conditions

You can create a policy to check if an end point is compliant with the specified data encryption software.

For example, you can create a condition to check if the C: drive is encrypted in an end point. If the C: drive is not encrypted then the end point receives a non-compliance notification and ISE logs a message.

Before you begin

To perform the following task, you must be a Super Admin or Policy Admin. You can associate a Disk Encryption condition with a posture requirement only when you use the AnyConnect ISE posture agent.

Step 1 Choose **Policy** > **Policy Elements** > **Conditions** > **Posture** > **Disk Encryption Condition**.

Step 2 Click **Add**.

Step 3 In the **Disk Encryption Condition** window, enter the appropriate values in the fields.

Step 4 Click **Submit**.

Network Conditions

A policy is a set of conditions and a result. A policy condition consists of an operand (attribute), an operator (equal to, not equal to, greater than, and so on), and a value. Compound conditions are made up of one or more simple conditions that are connected by the AND or OR operator. At runtime, Cisco ISE evaluates a policy condition and then applies the result that you have defined based on whether the policy evaluation returns a true or a false value.

Each network condition defines a list of objects that can be included in policy conditions, resulting in a set of definitions that are matched against those presented in the request.

You can use the operator, `EQUALS true`, to check if the network condition evaluates to true (whether the value presented in the request matches at least one entry within the network condition) or `EQUALS false` to test whether the network condition evaluates to false (does not match any entry in the network condition).

After you create a network condition with a name, you can reuse this condition multiple times across various rules and policies by selecting the network condition from the Network Conditions dictionary, for example:

```
Network Conditions.MyNetworkCondition EQUALS true
```

You can create the following network conditions to restrict access to the network:

- Endstation Network Conditions—Based on endstations that initiate and terminate the connection.

  Cisco ISE evaluates the remote address TO field (which is obtained based on whether it is a TACACS+ or RADIUS request) to identity whether it is the IP address, MAC address, calling line identification (CLI), or dialed number identification service (DNIS) of the endpoint.

  In a RADIUS request, this identifier is available in Attribute 31 (Calling-Station-Id).

  In a TACACS+ request, if the remote address includes a slash (/), the part before the slash is taken as the FROM value and the part after the slash is taken as the TO value. For example, if a request has

CLI/DNIS, CLI is taken as the FROM value and DNIS is taken as the TO value. If a slash is not included, the entire remote address is taken as the FROM value (whether IP address, MAC address, or CLI).

- Device Network Conditions—Based on the AAA client that processes the request.

  A network device can be identified by its IP address, device name that is defined in the network device repository, or Network Device Group.

  In a RADIUS request, if Attribute 4 (NAS-IP-Address) is present, Cisco ISE obtains the IP address from this attribute. If Attribute 32 (NAS-Identifier) is present, Cisco ISE obtains the IP address from Attribute 32. If these attributes are not found, it obtains the IP address from the packet that it receives.

  The device dictionary (NDG dictionary) contains network device group attributes such as Location, Device Type, or other dynamically created attributes that represent NDGs. These attributes contain the groups that the current device is related to.

- Device Port Network Conditions—Based on the device's IP address, name, NDG, and port (physical port of the device that the endstation is connected to).

  In a RADIUS request, if Attribute 5 (NAS-Port) is present in the request, Cisco ISE obtains the value from this attribute. If Attribute 87 (NAS-Port-Id) is present in the request, Cisco ISE obtains the request from Attribute 87.

  In a TACACS+ request, Cisco ISE obtains this identifier from the port field of the start request (of every phase).

Configure Endstation Network Conditions

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

Step 2 Click **Add**.

Step 3 Enter a name and description for the network condition.

Step 4 Enter the following details:

- IP Addresses—You can add a list of IP addresses or subnets, one per line. The IP address/subnet can be in IPv4 or IPv6 format.
- MAC Addresses—You can enter a list of Endstation MAC addresses and Destination MAC addresses, separated by a comma. Each MAC address must include 12 hexadecimal digits and must be in one of the following formats: nn:nn:nn:nn:nn:nn, nn-nn-nn-nn-nn-nn, nnnn.nnnn.nnnn, or nnnnnnnnnnnn.

  If the Endstation MAC or the Destination MAC is not required, use the token "-ANY-" instead.

- CLI/DNIS—You can add a list of Caller IDs (CLI) and Called IDs (DNIS), separated by a comma. If the Caller ID (CLI) or the Called ID (DNIS) is not required, use the token "-ANY-" instead.

Step 5 Click **Submit**.

Configure Device Network Conditions

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

Step 2 Click **Add**.

Step 3 Enter a name and description for the network condition.

Step 4 Enter the following details:

- IP Addresses—You can add a list of IP addresses or subnets, one per line. The IP address/subnet can be in IPv4 or IPv6 format.
- Device Name—You can add a list of device names, one per line. You must enter the same device name that is configured in the Network Device object.
- Device Groups—You can add a list of tuples in the following order: Root NDG, comma, and an NDG (that it under the root NDG). There must be one tuple per line.

Step 5 Click **Submit**.

Configure Device Port Network Condition

Step 1 Choose **Policy > Policy Elements > Conditions > Network Conditions > Device Port Network Conditions**.

Step 2 Click **Add**.

Step 3 Enter a name and description for the network condition.

Step 4 Enter the following details:

- IP Addresses—Enter the details in the following order: IP address or subnet, comma, and a port (that is used by the device). There must be one tuple per line.
- Devices— Enter the details in the following order: device name, comma, and a port. There must be one tuple per line. You must enter the same device name that is configured in the Network Device object.
- Device Groups— Enter the details in the following order: Root NDG, comma, NDG (that it under the root), and a port. There must be one tuple per line.

Step 5 Click **Submit**.

Create 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.

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**.