Policy User Interface Reference

This chapter is a reference for the Cisco Identity Services Engine (ISE) Admin Portal elements, and contains the following Policy related sections:

Authentication

This section contains the following topics:

Simple Authentication Policy Configuration Settings

The following table describes the fields in the simple authentication policy page, which allows you to configure simple authentication policies. The navigation path for this page is: Policy > Authentication > Simple.

Table B-1 Simple Authentication Policy Configuration Settings

Fields	Usage Guidelines
Network Access Service	Choose an allowed protocol that you have already created.

Table B-1 Simple Authentication Policy Configuration Settings (continued)

Fields	Usage Guidelines
Identity Source	Choose the identity source that you want to use for authentication. You can also choose an identity source sequence if you have configured it. See the "Creating Identity Source Sequences" section on page 14-38 for information on how to configure identity source sequences.
Options	Define a further course of action for authentication failure, user not found, or process failure events. You can choose one of the following options: • Reject—A reject response is sent. • Drop—No response is sent. • Continue—Cisco ISE proceeds with the authorization policy.

Related Topics

- Configuring a Simple Authentication Policy, page 19-21
- See the "Creating Identity Source Sequences" section on page 14-38 for information on how to configure identity source sequences.

Rule-Based Authentication Policy Configuration Settings

The following table describes the fields in the rule-based authentication policy page, which allows you to configure rule-based authentication policies. The navigation path for this page is: Policy > Authentication > Rule-Based.

Table B-2 Rule-Based Authentication Policy Configuration Settings

Fields	Usage Guidelines
Status	Choose the status of this policy. It can be one of the following: • Enabled—This policy condition is active. • Disabled—This policy condition is inactive and will not be evaluated. • Monitor Only—This policy condition will be evaluated, but the result will not be enforced. You can view the results of this policy condition in the Live Log authentication page. In this, see the detailed report which will have the monitored step and attribute. For example, you may want to add a new policy condition, but are not sure if the condition would provide you with the correct results. In this situation, you can create the policy condition in monitored mode to view the results and then enable it if you are satisfied with the results.
Standard Rule	Enter a name for this policy and select condition and allowed protocol.

Table B-2 Rule-Based Authentication Policy Configuration Settings (continued)

Fields	Usage Guidelines
Conditions	Click the plus [+] sign to expand the Conditions anchored overlay, and click the minus [-] sign, or click outside the anchored overlay to close it. Click **Select Existing Condition from Library** or **Create New Condition (Advanced Option)** **Select Existing Condition from Library—**You can define an expression by selecting Cisco predefined conditions from the policy elements library. **Create New Condition (Advanced Option)—**You can define an expression by selecting attributes from various system or user-defined dictionaries.
Select Existing Condition from Library	You can do the following: 1. You can choose the predefined conditions that you would have defined for authentication in the policy elements, and then use an AND or OR operator to add multiple conditions. You cannot select certain predefined conditions that contain the following dictionaries or attributes: • Dictionary “Certificate”, with any attribute • Dictionary “Network Access”, with the following attributes: – Device IP Address – ISE Host Name – NetworkDeviceName – Protocol – UseCase In case such conditions are available, the first entry in the select box will be “Only relevant conditions are selectable”. 2. Click the **Action** icon to do the following in the subsequent steps: • Add Attribute/Value—You can add ad-hoc attribute/value pairs • Add Condition from Library—You can add Cisco predefined conditions • Duplicate—Create a copy of the selected condition • Add Condition to Library— You can save ad-hoc attribute/value pairs that you create to the policy elements library • Delete—Delete the selected condition.

Table B-2 Rule-Based Authentication Policy Configuration Settings (continued)

Fields	Usage Guidelines
Create New Condition (Advance Option)	You can do the following: 1. You can add ad-hoc attribute/value pairs to your expression, and then use an AND or OR operator to add multiple conditions. 2. Click the **Action** icon to do the following in the subsequent steps: – Add Attribute/Value—You can add ad-hoc attribute/value pairs – Add Condition from Library—You can add Cisco predefined conditions – Duplicate—Create a copy of the selected condition – Add Condition to Library— You can save ad-hoc attribute/value pairs that you create to the policy elements library – Delete—Delete the selected condition.Here, you can use the AND or OR operator
Select Network Access	Choose from allowed protocols or RADIUS server sequence.
	Click to define conditions for the identity source selection.
Identity Source Sequence	
Action Icon	Click the action icon in the default identity source row, and click **Insert new row above**.
Enter a store rule name 1	Enter a name for your identity source rule.
	Click the button to define the conditions based on which you want to choose the identity source.
Internal Users	Choose the identity source sequence or the identity source and the action that you want Cisco ISE to take.

Related Topics

Configuring a Rule-Based Authentication Policy, page 19-22

Authorization Policy Settings

The following table describes the fields in the authorization policy page, which allows you to configure authorization policies. The navigation path for this page is: Policy > Authorization.

Table B-3 Authorization Policy Settings

Fields	Usage Guidelines
Status	Choose one of the following to enforce the policies: • Enabled—This policy condition is active. • Disabled—This policy condition is inactive and will not be evaluated. • Monitor Only—This policy condition will be evaluated, but the result will not be enforced. You can view the results of this policy condition in the Live Log authentication page. In this, see the detailed report which will have the monitored step and attribute. For example, you may want to add a new policy condition, but are not sure if the condition would provide you with the correct results. In this situation, you can create the policy condition in monitored mode to view the results and then enable it if you are satisfied with the results.
Rule Name	Enter a name for the Rule Name.
Conditions (identity groups and other conditions)	Choose an identity group from the first drop-down. Choose a condition from the second drop-down. You can either select from the existing conditions or create a new condition.
Permissions	Choose an authorization profile from the **Standard** category.

Related Topics

Configuring Authorization Policies, page 20-8

Endpoint Profiling Policies Settings

The following table describes the fields in the Endpoint Policies page. The navigation path for this page is: Policy > Profiling > Profiling Policies.

Table B-4 Endpoint Profiling Policies Settings

Fields	Usage Guidelines
Name	Enter the name of the endpoint profiling policy that you want to create.
Description	Enter the description of the endpoint profiling policy that you want to create.
Policy Enabled	By default, the **Policy Enabled** check box is checked to associate a matching profiling policy when you profile an endpoint. When unchecked, the endpoint profiling policy is excluded when you profile an endpoint.
Minimum Certainty Factor	Enter the minimum value that you want to associate with the profiling policy. The default value is 10.

Table B-4 Endpoint Profiling Policies Settings (continued)

Fields	Usage Guidelines
Exception Action	Choose an exception action, which you want to associate with the conditions when defining a rule in the profiling policy. The default is NONE. The exception actions are defined in the following location: Policy > Policy Elements > Results > Profiling > Exception Actions.
Network Scan (NMAP) Action	Choose a network scan action from the list, which you want to associate with the conditions when defining a rule in the profiling policy, if required. The default is NONE. The exception actions are defined in the following location: Policy > Policy Elements > Results > Profiling > Network Scan (NMAP) Actions.
Create an Identity Group for the policy	Check one of the following options to create an endpoint identity group: • **Yes, create matching Identity Group** • **No, use existing Identity Group hierarchy**
Yes, create matching Identity Group	Choose this option to use an existing profiling policy. This option creates a matching identity group for those endpoints and the identity group will be the child of the Profiled endpoint identity group when an endpoint profile matches an existing profiling policy. For example, the Xerox-Device endpoint identity group is created in the Endpoints Identity Groups page when endpoints discovered on your network match the Xerox-Device profile.
No, use existing Identity Group hierarchy	Check this check box to assign endpoints to the matching parent endpoint identity group using hierarchical construction of profiling policies and identity groups. This option allows you to make use of the endpoint profiling policies hierarchy to assign endpoints to one of the matching parent endpoint identity groups, as well as to the associated endpoint identity groups to the parent identity group. For example, endpoints that match an existing profile are grouped under the appropriate parent endpoint identity group. Here, endpoints that match the Unknown profile are grouped under Unknown, and endpoints that match an existing profile are grouped under the Profiled endpoint identity group. For example, • If endpoints match the Cisco-IP-Phone profile, then they are grouped under the Cisco-IP-Phone endpoint identity group. • If endpoints match the Workstation profile, then they are grouped under the Workstation endpoint identity group. The Cisco-IP-Phone and Workstation endpoint identity groups are associated to the Profiled endpoint identity group in the system.
Parent Policy	Choose a parent profiling policy that are defined in the system to which you want to associate the new endpoint profiling policy. You can choose a parent profiling policy from which you can inherit rules and conditions to its child.

Table B-4 Endpoint Profiling Policies Settings (continued)

Fields	Usage Guidelines
Associated CoA Type	Choose one of the following CoA types that you want to associate with the endpoint profiling policy: • No CoA • Port Bounce • Reauth • Global Settings that is applied from the profiler configuration set in Administration > System > Settings > Profiling
Rules	One or more rules that are defined in endpoint profiling policies determine the matching profiling policy for endpoints, which allows you to group endpoints according to their profiles. One or more profiling conditions from the policy elements library are used in rules for validating endpoint attributes and their values for the overall classification.
Conditions	Click the plus [+] sign to expand the Conditions anchored overlay, and click the minus [-] sign, or click outside the anchored overlay to close it. Click **Select Existing Condition from Library** or **Create New Condition (Advanced Option)** **Select Existing Condition from Library—**You can define an expression by selecting Cisco predefined conditions from the policy elements library. **Create New Condition (Advanced Option)—**You can define an expression by selecting attributes from various system or user-defined dictionaries. You can associate one of the following with the profiling conditions: • An integer value for the certainty factor for each condition • Either an exception action or a network scan action for that condition Choose one of the following predefined settings to associate with the profiling condition: • Certainty Factor Increases—Enter the certainty value for each rule, which can be added for all the matching rules with respect to the overall classification. • Take Exception Action—Triggers an exception action that is configured in the Exception Action field for this endpoint profiling policy. • Take Network Scan Action—Triggers a network scan action that is configured in the Network Scan (NMAP) Action field for this endpoint profiling policy.

Table B-4 Endpoint Profiling Policies Settings (continued)

Fields	Usage Guidelines
Select Existing Condition from Library	You can do the following: • You can choose Cisco predefined conditions that are available in the policy elements library, and then use an AND or OR operator to add multiple conditions. • Click the **Action** icon to do the following in the subsequent steps: – Add Attribute/Value—You can add ad-hoc attribute/value pairs – Add Condition from Library—You can add Cisco predefined conditions – Duplicate—Create a copy of the selected condition – Add Condition to Library— You can save ad-hoc attribute/value pairs that you create to the policy elements library – Delete—Delete the selected condition.
Create New Condition (Advance Option)	You can do the following: • You can add ad-hoc attribute/value pairs to your expression, and then use an AND or OR operator to add multiple conditions. • Click the **Action** icon to do the following in the subsequent steps: – Add Attribute/Value—You can add ad-hoc attribute/value pairs – Add Condition from Library—You can add Cisco predefined conditions – Duplicate—Create a copy of the selected condition – Add Condition to Library— You can save ad-hoc attribute/value pairs that you create to the policy elements library – Delete—Delete the selected condition.Here, you can use the AND or OR operator

Dictionaries

RADIUS Vendor Dictionary Attribute Settings

The following table describes the fields in the Dictionary page for RADIUS vendors, which allows you to configure dictionary attributes for the RADIUS vendors. The navigation path for this page is: Policy > Policy Elements > Dictionaries > System > RADIUS > RADIUS Vendors.

Table B-5 RADIUS Vendor Dictionary Attribute Settings

Fields	Usage Guidelines
Attribute Name	Enter the vendor specific attribute name for the selected RADIUS vendor.
Description	Enter an optional description for the vendor specific attribute.
Internal Name	Enter the name for the vendor specific attribute that refers to it internally in the database.

Table B-5 RADIUS Vendor Dictionary Attribute Settings (continued)

Fields	Usage Guidelines
Data Type	Choose one of the following data types for the vendor specific attribute: • STRING • OCTET_STRING • UNIT32 • UNIT64 • IPV4
Enable MAC option	Check this check box to enable the comparison of RADIUS attribute as MAC address. By default, for the RADIUS attribute calling-station-id this option is marked as enabled and you cannot disable it. For other dictionary attributes (of string types) within the RADIUS vendor dictionary, you can enable or disable this option. Once you enable this option, while setting the authentication and authorization conditions, you can define whether the comparison is clear string by selecting the Text option or whether it is MAC address by selecting the MAC address option.
Direction	Choose one of the options that applies to RADIUS messages:
ID	Enter the vendor attribute ID. The valid range is 0 to 255.
Allow Tagging	Check this check box.
Allow multiple instances of this attribute in a profile	Check this check box when you want multiple instances of this RADIUS vendor specific attribute in profiles.

Conditions

This section includes the following field setting tables:

- Profiler Condition Settings, page B-9
- Posture Conditions Settings, page B-10
- Time and Date Condition Settings, page B-17

Profiler Condition Settings

The following table describes the fields in the Profiler Condition page. The navigation path for this page is: Policy > Policy Elements > Conditions > Profiling.

Table B-6 Profiler Condition Settings

Fields	Usage Guidelines
Name	Name of the profiler condition.
Description	Description of the profiler condition.
Type	Choose any one of the predefined types.
Attribute Name	Choose an attribute on which to base the profiler condition.
Operator	Choose an operator.

Table B-6 Profiler Condition Settings (continued)

Fields	Usage Guidelines
Attribute Value	Enter the value for the attribute that you have chosen. For Attribute Names that contain pre-defined Attribute Values, this option displays a drop-down list with the pre-defined values, and you can choose a value.
System Type	Profiling conditions can be any one of the following types: • Cisco Provided—Profiling conditions that are provided by Cisco ISE when deployed are identified as Cisco Provided. You cannot edit or delete them from the system. • Administrator Created—Profiling conditions that you create as an administrator of Cisco ISE are identified as Administrator Created.

Related Topics

Profiler Conditions, page 18-4

Posture Conditions Settings

This section contains the following field setting tables:

File Condition Settings

The following table describes the fields in the File Conditions page. The navigation path for this page is: Policy > Policy Elements > Conditions > Posture > File Condition.

Table B-7 File Condition Settings

Fields	Usage Guidelines
Name	Enter the name of the file condition.
Description	Enter a description for the file condition.

Table B-7 File Condition Settings (continued)

Fields	Usage Guidelines
File Path	Choose one of the predefined settings: • **ABSOLUTE_PATH**—Checks the file in the fully qualified path of the file. For example, C:\<directory>\file name. For other settings, enter only the file name. • **SYSTEM_32**—Checks the file in the C:\WINDOWS\system32 directory. Enter the file name. • **SYSTEM_DRIVE**—Checks the file in the C:\ drive. Enter the file name. • **SYSTEM_PROGRAMS**—Checks the file in the C:\Program Files. Enter the file name. • **SYSTEM_ROOT**—Checks the file in the root path for Windows system. Enter the file name.
File Type	Choose one of the predefined settings: • **FileExistence**—Checks whether a file exists on the system. • **FileDat**e—Checks whether a file with a particular file-created or file-modified date exists on the system. • **FileVersion**—Checks whether a particular version of a file exists on the system.
File Date Type	(Available only if you select **FileDate** as the File Type) Choose a file data type.
File Operator/Operator	The File Operator options change according to the settings you select in the File Type. Choose the settings appropriately: **FileExistence** • Exists • DoesNotExist **FileDate** • EarlierThan • LaterThan • EqualTo **FileVersion** • EarlierThan • LaterThan • EqualTo
Date and Time	(Available only if you select **File Date** as the File Type) Enter the date and time of the client system in mm/dd/yyyy and hh:mm:ss format.
File Version	(Available only if you have selected **File Version** as the File Type) Enter the version of the file to be checked.
Operating System	Select the operating system to which the file condition should be applied.

Registry Condition Settings

The following table describes the fields in the Registry Conditions page. The navigation path for this page is: Policy > Policy Elements > Conditions > Posture > Registry Condition.

Table B-8 Registry Condition Settings

Fields	Usage Guidelines
Name	Enter the name of the registry condition.
Description	Enter a description for the registry condition.
Registry Type	Choose one of the predefined settings as the registry type.
Registry Root Key	Choose one of the predefined settings as the registry root key.
Sub Key	Enter the sub key without the backslash ("\") to check the registry key in the path specified in the Registry Root Key. For example, SOFTWARE\Symantec\Norton AntiVirus\version will check the key in the following path: HKLM\SOFTWARE\Symantec\NortonAntiVirus\version
Value Name	(Available only if you select **RegistryValue** or **RegistryValueDefault** as the Registry Type) Enter the name of the registry key value to be checked for **RegistryValue.** This is the default field for **RegistryValueDefault**.
Value Data Type	(Available only if you select **RegistryValue** or **RegistryValueDefault** as the Registry Type) Choose one of the following settings: • **Unspecified**—Checks whether the registry key value exists or not. This option is available only for **RegistryValue**. • **Number**—Checks the specified number in the registry key value • **String**—Checks the string in the registry key value • **Version**—Checks the version in the registry key value
Value Operator	Choose the settings appropriately.
Value Data	(Available only if you select **RegistryValue** or **RegistryValueDefault** as the Registry Type) Enter the value of the registry key according to the data type you have selected in **Value Data Type**.
Operating System	Select the operating system to which the registry condition should be applied.

Application Condition Settings

The following table describes the fields in the Application Conditions page. The navigation path for this page is: Policy > Policy Elements > Conditions > Posture > Application Condition.

Table B-9 Application Condition Settings

Fields	Usage Guidelines
Name	Enter the name of the application condition.
Description	Enter a description of the application condition.
Process Name	Enter the name of the application to be checked.
Application Operator	Choose the status to be checked.
Operating System	Select the operating system to which the application condition should be applied.

Service Conditions Settings

The following table describes the fields in the Service Conditions page. The navigation path for this page is: Policy > Policy Elements > Conditions > Posture > Service Condition.

Table B-10 Service Conditions Settings

Fields	Usage Guidelines
Name	Enter a name for the service condition.
Description	Enter a description of the service condition.
Service Name	Enter the name of the service to be checked.
Service Operator	Choose the status to be checked.
Operating System	Select the operating system to which the service condition should be applied.

Posture Compound Condition Settings

The following table describes the fields in the Compound Conditions page. The navigation path for this page is: Policy > Policy Elements > Conditions > Posture > Compound Condition.

Table B-11 Posture Compound Condition Settings

Fields	Usage Guidelines
Name	Enter the name of the compound condition that you want to create.
Description	Enter the description of the compound condition that you want to create.
Operating System	Select one or more Windows operating systems. This allow you to associate Windows operating systems to which the condition is applied.
Parentheses ( )	Click the parentheses to combine two simple conditions from the following simple condition types: file, registry, application, and service conditions.
(&)—AND operator (use "&" for an AND operator, without the quotes)	You can use the AND operator (ampersand [&]) in a compound condition. For example, enter **Condition1 & Condition2**.
(|)—OR operator (use "|" for an OR operator, without the quotes)	You can use the OR operator (horizontal bar [|]) in a compound condition. For example, enter **Condition1 | Condition2**.
(!)—NOT operator (use "!" for a NOT operator, without the quotes)	You can use the NOT operator (exclamation point [!]) in a compound conditions. For example, enter **Condition1 & (!Condition2)**.
Simple Conditions	Choose from a list of simple conditions of the following types: file, registry, application, and service conditions. You can also create simple conditions of file, registry, application and service conditions from the object selector. Click the quick picker (down arrow) on the **Action** button to create simple conditions of file, registry, application, and service conditions.

Antivirus Compound Condition Settings

The following table describes the fields in the AV Compound Conditions page. The navigation path for this page is: Policy > Policy Elements > Conditions > Posture > AV Compound Condition.

Table B-12 Antivirus Compound Condition Settings

Fields	Usage Guidelines
Name	Enter the name of the antivirus compound condition that you want to create.
Description	Enter the description of the antivirus compound condition that you want to create.
Operating System	Select an operating system to check the installation of an antivirus programs on your client, or check the latest antivirus definition file updates to which the condition is applied.
Vendor	Choose a vendor from the drop-down list. The selection of Vendor retrieves their antivirus products and versions, which are displayed in the Products for Selected Vendor table.
Check Type	Choose whether to check an installation or check the latest definition file update on the client.
Installation	Choose to check only the installation of an antivirus program on the client.
Definition	Choose to check only the latest definition file update of an antivirus product on the client.
Check against latest AV definition file version, if available. (Otherwise check against latest definition file date).	(Available only when you choose Definition check type) Choose to check the antivirus definition file version on the client against the latest antivirus definition file version, if available as a result of posture updates in Cisco ISE. Otherwise, this option allows you to check the definition file date on the client against the latest definition file date in Cisco ISE.
Allow virus definition file to be (Enabled)	(Available only when you choose Definition check type) Choose to check the antivirus definition file version and the latest antivirus definition file date on the client. The latest definition file date cannot be older than that you define in the next field (days older than field) from the latest antivirus definition file date of the product or the current system date. If unchecked, Cisco ISE allows you to check only the version of the antivirus definition file using the Check against latest AV definition file version, if available option.
days older than	Define the number of days that the latest antivirus definition file date on the client can be older from the latest antivirus definition file date of the product or the current system date. The default value is zero (0).
latest file date	Choose to check the antivirus definition file date on the client, which can be older by the number of days that you define in the days older than field. If you set the number of days to the default value (0), then the antivirus definition file date on the client should not be older than the latest antivirus definition file date of the product.

Table B-12 Antivirus Compound Condition Settings (continued)

Fields	Usage Guidelines
current system date	Choose to checks the antivirus definition file date on the client, which can be older by the number of days that you define in the days older than field. If you set the number of days to the default value (0), then the antivirus definition file date on the client should not be older than the current system date.
Products for Selected Vendor	Choose an antivirus product from the table. Based on the vendor that you select in the New Anti-virus Compound Condition page, the table retrieves information on their antivirus products and their version, remediation support that they provide, latest definition file date and its version. The selection of a product from the table allows you to check for the installation of an antivirus program, or check for the latest antivirus definition file date, and its latest version.

Antispyware Compound Condition Settings

The following table describes the fields in the AS Compound Conditions page. The navigation path for this page is: Policy > Policy Elements > Conditions > Posture > AS Compound Condition.

Table B-13 Antispyware Compound Condition Settings

Fields	Usage Guidelines
Name	Enter the name of the antispyware compound condition that you want to create.
Description	Enter the description of the antispyware compound condition that you want to create.
Operating System	Selecting an operating system allows you to check the installation of an antispyware programs on your client, or check the latest antispyware definition file updates to which the condition is applied.
Vendor	Choose a vendor from the drop-down list. The selection of Vendor retrieves their antispyware products and versions, which are displayed in the Products for Selected Vendor table.
Check Type	Choose if you want to choose a type whether to check an installation, or check the latest definition file update on the client.
Installation	Choose if you want to check only the installation of an antispyware program on the client.
Definition	Choose if you want to check only the latest definition file update of an antispyware product on the client.
Allow virus definition file to be (Enabled)	Check this check box when you are creating antispyware definition check types, and disabled when creating antispyware installation check types. If checked, the selection allows you to check antispyware definition file version and the latest antispyware definition file date on the client. The latest definition file date cannot be older than that you define in the days older than field from the current system date. If unchecked, the selection allows you to check only the version of the antispyware definition file as the Allow virus definition file to be check box is not checked.
days older than	Define the number of days that the latest antispyware definition file date on the client can be older from the current system date. The default value is zero (0).

Table B-13 Antispyware Compound Condition Settings (continued)

Fields	Usage Guidelines
The current system date	Choose to check the antispyware definition file date on the client, which can be older by the number of days that you define in the days older than field. If you set the number of days to the default value (0), then the antispyware definition file date on the client should not be older than the current system date.
Products for Selected Vendor	Choose an antispyware product from the table. Based on the vendor that you select in the New Anti-spyware Compound Condition page, the table retrieves information on their antispyware products and their version, remediation support that they provide, latest definition file date and its version. The selection of a product from the table allows you to check for the installation of an antispyware program, or check for the latest antispyware definition file date, and its latest version.

Dictionary Simple Conditions Settings

The following table describes the fields in the Dictionary Simple Conditions page. The navigation path for this page is: Policy > Policy Elements > Conditions > Posture > Dictionary Simple Condition.

Table B-14 Dictionary Simple Condition Settings

Fields	Usage Guideline
Name	Enter the name of the dictionary simple condition that you want to create.
Description	Enter the description of the dictionary simple condition that you want to create.
Attribute	Choose an attribute from the dictionary.
Operator	Choose an operator to associate a value to the attribute that you have selected.
Value	Enter a value that you want to associate to the dictionary attribute, or choose a predefined value from the drop-down list.

Dictionary Compound Condition Settings

The following table describes the fields in the Dictionary Compound Conditions page. The navigation path for this page is: Policy > Policy Elements > Conditions > Posture > Dictionary Compound Condition.

Table B-15 Dictionary Compound Condition Settings

Fields	Usage Guidelines
Name	Enter the name of the dictionary compound condition that you want to create.
Description	Enter the description of the dictionary compound condition that you want to create.
Select Existing Condition from Library	Define an expression by selecting pre-defined conditions from the policy elements library or add ad-hoc attribute/value pairs to your expression in the subsequent steps.
Condition Name	Choose dictionary simple conditions that you have already created from the policy elements library.
Expression	The Expression is updated based on your selection from the Condition Name drop-down list.

Table B-15 Dictionary Compound Condition Settings (continued)

Fields	Usage Guidelines
AND or OR operator	Choose an AND, or an OR operator to logically combine dictionary simple conditions, which can be added from the library. Click the **Action** icon to do the following: • Add Attribute/Value • Add Condition from Library • Delete
Create New Condition (Advance Option)	Select attributes from various system or user-defined dictionaries. You can also add predefined conditions from the policy elements library in the subsequent steps.
Condition Name	Choose a dictionary simple condition that you have already created.
Expression	From the Expression drop-down list, you can create a dictionary simple condition.
Operator	Choose an operator to associate a value to an attribute.
Value	Enter a value that you want to associate to the dictionary attribute, or choose a value from the drop-down list.

Related Topics

Creating Endpoint Profiling Policies, page 21-22

Time and Date Condition Settings

The following table describes the fields in the Time and Date Conditions page. The navigation path for this page is: Policy > Policy Elements > Conditions > Common > Time and Date.

Table B-16 Time and Date Condition Settings

Fields	Usage Guidelines
Condition Name	Enter the name of the time and date condition.
Description	Enter a description of the time and date condition.
Standard Settings	
All Day	(Default) Set for the entire day.
Specific Hours	Configure hours, minutes, and AM/PM to set a to-and-from time range.
Every Day	(Default) Set for every day.
Specific Days	Configure one or more specific days of the week.
No Start and End Dates	(Default) Set with no start or end date.
Specific Date Range	Configure the month, day, and year to set a to-and-from date range.
Specific Date	Configure a specific month, day, and year.
Exceptions	
Time Range	Configure the hours, minutes, and AM/PM to set a to-and-from time range.

Table B-16 Time and Date Condition Settings (continued)

Fields	Usage Guidelines
Week Days	Configure one or more specific days of the week.
Date Range	Choose on the following two options: • Specific Date Range—Provides drop-down lists you can use to configure a specific to-and-from date range by month, day, and year. • Specific Date—Provides drop-down lists you can use to configure a specific month, day, and year.

Related Topics

Creating Time and Date Conditions, page 18-8

Results

This section contains the following topics:

Allowed Protocols Services Settings

The following table describes the fields in the Allowed Protocols Services page, which allows you to configure the protocols to be used during authentication. The navigation path for this page is: Policy > Policy Elements > Results >Authentication > Allowed Protocols.

Table B-17 Allowed Protocols Services Settings

Fields	Usage Guidelines
Allowed Protocols	
Process Host Lookup	Check this check box to configure Cisco ISE to process the Host Lookup field (for example, when the RADIUS Service-Type equals 10) and use the System UserName attribute from the RADIUS Calling-Station-ID attribute. Uncheck this check box if you want Cisco ISE to ignore the Host Lookup request and use the original value of the system UserName attribute for authentication. When unchecked, message processing is done according to the protocol (for example, PAP).
Authentication Protocols	
Allow PAP/ASCII	Check this check box to check the Detect PAP as Host Lookup check box to configure Cisco ISE to detect this type of request as a Host Lookup (instead of PAP) request. This option enables PAP/ASCII. PAP uses cleartext passwords (that is, unencrypted passwords) and is the least secure authentication protocol.
Allow CHAP	Check this check box to check the Detect CHAP as Host Lookup check box to configure Cisco ISE to detect this type of request as a Host Lookup request. If you enable this option, ISE will allow MAB on non-Cisco devices. This option enables CHAP authentication. CHAP uses a challenge-response mechanism with password encryption. CHAP does not work with Microsoft Active Directory.
Allow MS-CHAPv1	Check this check box to enable MS-CHAPv1.
Allow MS-CHAPv2	Check this check box to enable MS-CHAPv2.
Allow EAP-MD5	Check this check box to enable EAP-based MD5 hashed authentication. When you check the Allow EAP-MD5 check box, you can check the Detect EAP-MD5 as Host Lookup check box to configure Cisco ISE to detect this type of request as a Host Lookup (instead of EAP-MD5) request.
Allow EAP-TLS	Check this check box to enable EAP-TLS Authentication protocol and configures EAP-TLS settings. You can specify how Cisco ISE will verify the user identity as presented in the EAP identity response from the end-user client. User identity is verified against information in the certificate that the end-user client presents. This comparison occurs after an EAP-TLS tunnel is established between Cisco ISE and the end-user client. **Note** EAP-TLS is a certificate-based authentication protocol. EAP-TLS authentication can occur only after you have completed the required steps to configure certificates. Refer to Chapter 8, "Managing Certificates" for more information on certificates.
Allow LEAP	Check this check box to enable Lightweight Extensible Authentication Protocol (LEAP) authentication.

Table B-17 Allowed Protocols Services Settings (continued)

Fields	Usage Guidelines
Allow PEAP	Check this check box to enable PEAP authentication protocol and PEAP settings. The default inner method is MS-CHAPv2. When you check the Allow PEAP check box, you can configure the following PEAP inner methods: • Allow EAP-MS-CHAPv2—Check this check box to use EAP-MS-CHAPv2 as the inner method. – Allow Password Change—Check this check box for Cisco ISE to support password changes. – Retry Attempts—Specifies how many times Cisco ISE requests user credentials before returning login failure. Valid values are 1 to 3. • Allow EAP-GTC—Check this check box to use EAP-GTC as the inner method. – Allow Password Change—Check this check box for Cisco ISE to support password changes. – Retry Attempts—Specifies how many times Cisco ISE requests user credentials before returning login failure. Valid values are 1 to 3. • Allow EAP-TLS—Check this check box to use EAP-TLS as the inner method. • Allow PEAPv0 only for legacy clients—Check this check box to allow PEAP supplicants to negotiate using PEAPv0. Some legacy clients do not conform to the PEAPv1 protocol standards. To ensure that such EAP conversations are not dropped, check this check box.
Allow EAP-FAST	Check this check box to enable EAP-FAST authentication protocol and EAP-FAST settings. The EAP-FAST protocol can support multiple internal protocols on the same server. The default inner method is MS-CHAPv2. See PAC Options, page B-22 for using protected access credentials with EAP-FAST. Refer to Guidelines for Using EAP-FAST as Authentication Protocol, page 19-11 for information on EAP chaining. When you check the Allow EAP-FAST check box, you can configure EAP-FAST as the inner method: • Allow EAP-MS-CHAPv2 – Allow Password Change—Check this check box for Cisco ISE to support password changes in phase zero and phase two of EAP-FAST. – Retry Attempts—Specifies how many times Cisco ISE requests user credentials before returning login failure. Valid values are 1-3. • Allow EAP-GTC – Allow Password Change—Check this check box for Cisco ISE to support password changes in phase zero and phase two of EAP-FAST. – Retry Attempts—Specifies how many times Cisco ISE requests user credentials before returning login failure. Valid values are 1-3. • Use PACs—Choose this option to configure Cisco ISE to provision authorization PACs[1] for EAP-FAST clients. Additional PAC options appear. • Don't use PACs—Choose this option to configure Cisco ISE to use EAP-FAST without issuing or accepting any tunnel or machine PACs. All requests for PACs are ignored and Cisco ISE responds with a Success-TLV without a PAC. When you choose this option, you can configure Cisco ISE to perform machine authentication.

1. PACs = Protected Access Credentials.

Related Topics

Defining Allowed Protocols for Network Access, page 19-14

PAC Options

The following table describes the fields after you select Use PACs in the Allowed Protocols Services List page. The navigation path for this page is: Policy > Policy Elements > Results >Authentication > Allowed Protocols.

Table B-18 PAC Options

Fields	Usage Guidelines
Use PAC	• Tunnel PAC Time To Live—The Time to Live (TTL) value restricts the lifetime of the PAC. Specify the lifetime value and units. The default is 90 days. The range is between 1 and 1825 days. • Proactive PAC Update When: <n%> of PAC TTL is Left—The Update value ensures that the client has a valid PAC. Cisco ISE initiates an update after the first successful authentication but before the expiration time that is set by the TTL. The update value is a percentage of the remaining time in the TTL. The default is 90%. • Allow Anonymous In-band PAC Provisioning—Check this check box for Cisco ISE to establish a secure anonymous TLS handshake with the client and provision it with a PAC by using phase zero of EAP-FAST with EAP-MSCHAPv2. To enable anonymous PAC provisioning, you must choose both of the inner methods, EAP-MSCHAPv2 and EAP-GTC. • Allow Authenticated In-band PAC Provisioning—Cisco ISE uses SSL server-side authentication to provision the client with a PAC during phase zero of EAP-FAST. This option is more secure than anonymous provisioning but requires that a server certificate and a trusted root CA be installed on Cisco ISE. When you check this option, you can configure Cisco ISE to return an Access-Accept message to the client after successful authenticated PAC provisioning. – Server Returns Access Accept After Authenticated Provisioning—Check this check box if you want Cisco ISE to return an access-accept package after authenticated PAC provisioning. • Allow Machine Authentication—Check this check box for Cisco ISE to provision an end-user client with a machine PAC and perform machine authentication (for end-user clients who do not have the machine credentials). The machine PAC can be provisioned to the client by request (in-band) or by the administrator (out-of-band). When Cisco ISE receives a valid machine PAC from the end-user client, the machine identity details are extracted from the PAC and verified in the Cisco ISE external identity source. Cisco ISE only supports Active Directory as an external identity source for machine authentication. After these details are correctly verified, no further authentication is performed. When you check this option, you can enter a value for the amount of time that a machine PAC is acceptable for use. When Cisco ISE receives an expired machine PAC, it automatically reprovisions the end-user client with a new machine PAC (without waiting for a new machine PAC request from the end-user client). • Enable Stateless Session Resume—Check this check box for Cisco ISE to provision authorization PACs for EAP-FAST clients and always perform phase two of EAP-FAST (default = enabled). Uncheck this check box in the following cases: – If you do not want Cisco ISE to provision authorization PACs for EAP-FAST clients – To always perform phase two of EAP-FAST When you check this option, you can enter the authorization period of the user authorization PAC. After this period, the PAC expires. When Cisco ISE receives an expired authorization PAC, it performs phase two EAP-FAST authentication. • Preferred EAP Protocol—Check this check box to choose your preferred EAP protocols from any of the following options: EAP-FAST, PEAP, LEAP, EAP-TLS, and EAP-MD5. By default, LEAP is the preferred protocol to use if you do not enable this field.

Related Topics

Defining Allowed Protocols for Network Access, page 19-14

Authorization Profile Settings

The following table describes the fields in the Standard Authorization Profiles page. The navigation path for this page is: Policy > Policy Elements > Results > Authorization > Authorization Profiles.

Table B-19 Authorization Profile settings

Fields	Usage Guidelines
Name	Enter a name that identifies the new authorization profile.
Description	Enter a description of the authorization profile.
Access Type	Choose the access type options (**ACCESS_ACCEPT** or **ACCESS_REJECT**).
Service Template	Check the check box to enable Cisco ISE to support sessions connecting from SAnet capable devices. ISE implements service templates as authorization profiles that contain a special flag that marks them as "Service Template" compatible. This way, the service template, which is also an authorization profile, can be used in a single policy to support connection with SAnet as well as non-SAnet devices.
Common Tasks	
DACL Name	Check the check box and choose existing downloadable ACL options available (for example, Cisco ISE provides two default values in the drop-down list: **PERMIT_ALL_TRAFFIC** or **DENY_ALL_TRAFFIC**). The list will include all current DACLs in the local database.
VLAN	Check the check box and enter an attribute value that identifies a virtual LAN (VLAN) ID that you want associated with the new authorization profile you are creating (both integer and string values are supported for the VLAN ID). The format for this entry would be *Tunnel-Private-Group-ID:VLANnumber*. **Note** If you do not select a VLAN ID, Cisco ISE uses a default value of VLAN ID = 1. For example, if you only entered 123 as your VLAN number, the Attributes Details pane reflects the following value: Tunnel-Private-Group-ID = 1:123.
Voice Domain Permission	Check the check box to enable the vendor-specific attribute (VSA) of "cisco-av-pair" to be associated with a value of "device-traffic-class=voice". In a multi-domain authorization mode, if the network switch receives this VSA, the endpoint is placed on to a voice domain after authorization.
Posture Discovery	Check the check box to enable a redirection process used for Posture discovery in Cisco ISE, and enter an ACL on the device that you want to associate with this authorization profile. For example, if the value you entered is acl119, this is reflected in the Attributes Details pane as: cisco-av-pair = url-redirect-acl = acl119. The Attributes Details pane also displays: cisco-av-pair = url-redirect=https://ip:8443/guestportal/gateway?sessionid=SessionValueIdValue&action=cpp.

Table B-19 Authorization Profile settings (continued)

Fields	Usage Guidelines
Centralized Web Authentication	Check the check box to enable a redirection process that is similar to Posture discovery, but it redirects guest user access requests to the Guest server in Cisco ISE. Enter an ACL on the device that you want to associate with this authorization profile, and select **Default** or **Manual** as the redirect option. For example, if the value you entered is acl-999, this is reflected in the Attributes Details pane as: cisco-av-pair = url-redirect-acl = acl-99. The Attributes Details pane also displays: cisco-av-pair = url-redirect=https://ip:8443/guestportal/gateway?sessionid=SessionValueIdValue&action=cwa. Check the **Static IP/Host Name** check box to specify an exact IP address or hostname to which you want the user to be redirected to. If this check box is not checked, the user will be redirected to the FQDN of the policy service node that received this request.
Web Redirection (CWA, RWA, MDM, NSP, CPP)	
Auto SmartPort	Check the check box to enable Auto SmartPort functionality and enter a corresponding event name value in the text box. This enables the VSA cisco-av-pair with a value for this option as "auto-smart-port=event_name". Your choice is reflected in the Attributes Details pane.
Filter-ID	Check the check box to enable a RADIUS filter attribute that sends the ACL name that you define in the text box (which is automatically appended with ".in"). Your choice is reflected in the Attributes Details pane.
Reauthentication	Check the check box and enter a value in seconds for maintaining connectivity during reauthentication. You can also choose attribute values from the Timer drop-down list. You choose to maintain connectivity during reauthentication by choosing to use either the default (a value of 0) or **RADIUS-Request** (a value of 1). Setting this to the RADIUS-Request value maintains connectivity during the reauthentication process.
MACSec Policy	Check the check box to enable the MACSec encryption policy whenever a MACSec-enabled client connects to Cisco ISE, and choose one of the following three options: **must-secure**, **should-secure**, or **must-not-secure**. For example, your choice is reflected in the Attributes Details pane as: cisco-av-pair = linksec-policy=must-secure.
NEAT	Check the check box to enable Network Edge Access Topology (NEAT), a feature that extends identity recognition between networks. Checking this check box displays the following value in the Attributes Details pane: cisco-av-pair = device-traffic-class=switch.
Web Authentication (Local Web Auth)	Check the check box to enable local web authentication for this authorization profile. This value lets the switch recognize authorization for web authentication by Cisco ISE sending a VSA along with a DACL. The VSA is cisco-av-pair = priv-lvl=15 and this is reflected in the Attributes Details pane.
Wireless LAN Controller (WLC)	Check the check box and enter an ACL name in the text field. This value is used in a required Airespace VSA to authorize the addition of a locally defined ACL to a connection on the WLC. For example, if you entered rsa-1188, this would be reflected in the Attributes Details pane as: Airespace-ACL-Name = rsa-1188.
ASA VPN	Check the check box to enable an Adaptive Security Appliances (ASA) VPN group policy. From the Attribute list, choose a value to configure this setting.
Advanced Attributes Settings	
Dictionaries	Click the down-arrow icon to display the available options in the Dictionaries window. Click to select the desired dictionary and attribute to configure in the first field.

Table B-19 Authorization Profile settings (continued)

Fields	Usage Guidelines
Attribute Values	Click the down-arrow icon to display the available options in the Attribute Values window. Click to select the desired attribute group and attribute value for the second field. This value matches the one selected in the first field. Any Advanced Attributes setting(s) that you configure will be displayed in the Attribute Details panel. **Note** To modify or delete any of the read-only values that are displayed in the Attributes Details pane, you must modify or delete these values in the corresponding Common Tasks field or in the attribute that you selected in the Attribute Values text box in the Advanced Attributes Settings pane.
Attributes Details	This pane displays any of the configured attribute values that you set for the Common Tasks and Advanced Attributes. **Note** The values displayed in the Attributes Details pane are read-only and cannot be edited or deleted in this pane.

Related Topics

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

Profiling Exception Action Settings

The following table describes the fields in the New Profiler Exception Action page. The navigation path for this page is: Policy > Policy Elements > Results > Profiling > Exception Actions.

Table B-20 Creating an Exception Action

Fields	Usage Guidelines
Name	Enter the name of the exception action that you want to create.
Description	Enter the description of the exception action that you want to create.
CoA Action to enforce CoA	Check the **CoA Action** check box to enforce CoA. When you associate an exception action in the endpoint profiling policy and enforce a CoA, you must configure CoA globally in Cisco ISE that can be done in the following location: Administration > System > Settings > Profiling. For information, see Setting up COA, SNMP RO Community and Endpoint Attribute Filter, page 21-15.
Policy Assignment	Click the **Policy Assignment** drop-down list that displays endpoint profiling policies that are configured in Cisco ISE, and choose the profiling policy against which the endpoint will be profiled when the exception action is triggered, regardless of its matched value.
System Type	Exception Actions can be any one of the following types: • Cisco Provided—Includes AuthorizationChange, EndpointDelete, and FirstTimeProfile • Administrator Created—Includes that are created by you as an administrator of Cisco ISE.

Related Topics

Creating Exception Actions, page 21-30

File Remediation

The following table describes the fields in the File Remediation page. The navigation path is: Policy > Policy Elements > Results > Posture > Remediation Actions > File Remediation.

Table B-21 File Remediation

Fields	Usage Guidelines
File Remediation Name	Enter a name for the file remediation. Once created and saved, you cannot edit the name of the file remediation.
File Remediation Description	Enter a description for the file remediation.
Version	Enter the file version.
File to upload	Click **Browse** to locate the name of the file to be uploaded to the Cisco ISE server. This is the file that will be downloaded to the client when the file remediation action is triggered.

Link Remediation

The following table describes the fields in the Link Remediation page. The navigation path is: Policy > Policy Elements > Results > Posture > Remediation Actions > Link Remediation.

Table B-22 Link Remediation

Fields	Usage Guidelines
Link Remediation Name	Enter a name for link remediation.
Link Remediation Description	Enter a description for the link remediation.
Remediation Type	Choose one of the following: • **Automatic**—When selected, you should enter values for the Interval and Retry Count. • **Manual**—When selected, Retry Count and Interval fields are not editable.
Retry Count	Enter the number of attempts that clients can try to remediate from the link.
Interval (in seconds)	Enter the time interval in seconds that clients can try to remediate from the link after previous attempts.
URL	Enter a valid URL that leads to a remediation page or resource.

Antivirus Remediation

The following table describes the fields in the AV Remediation page. The navigation path is Policy > Policy Elements > Results > Posture > Remediation Actions > AV Remediation.

Table B-23 Antivirus Remediation

Fields	Usage Guidelines
Name	Enter a name for the antivirus remediation.
Description	Enter a description for the antivirus remediation.

Table B-23 Antivirus Remediation (continued)

Fields	Usage Guidelines
Remediation Type	Choose one of the following: • **Automatic**—When selected, you should enter values for the Interval and Retry Count. • **Manual**—When selected, Retry Count and Interval fields are not editable.
Interval (in seconds)	Enter the time interval in seconds that clients can try to remediate after previous attempts.
Retry Count	Enter the number of attempts that clients can try to update an antivirus definition.
Operating System	Choose one of the following: • **Windows** • **Macintosh**—when selected Remediation Type, Interval, and Retry Count fields are not editable
AV Vendor Name	Choose the antivirus vendor.

Antispyware Remediation

The following table describes the fields in the AS Remediation page. The navigation path is Policy > Policy Elements > Results > Posture > Remediation Actions > AS Remediation.

Table B-24 Antispyware Remediation

Fields	Usage Guidelines
Name	Enter a name for the antispyware remediation.
Description	Enter a description for the antispyware remediation.
Remediation Type	Choose one of the following: • **Automatic**—When selected, you should enter values for the Interval and Retry Count. • **Manual**—When selected, Retry Count and Interval fields are not editable.
Interval (in seconds)	Enter the time interval in seconds that clients can try to remediate after previous attempts.
Retry Count	Enter the number of attempts that clients can try to update an antispyware definition.
Operating System	Choose one of the following: • **Windows** • **Macintosh**—when selected, Remediation Type, Interval, and Retry Count fields are not editable
AS Vendor Name	Choose the antispyware vendor.

Launch Program Remediation

The following table describes the fields in the Launch Program Remediation page. The navigation path is: Policy > Policy Elements > Results > Posture > Remediation Actions > Launch Program Remediation.

Table B-25 Launch Program Remediation

Fields	Usage Guidelines
Name	Enter a name for the launch program remediation.
Description	Enter a description for the launch program remediation that you want to create.
Remediation Type	Choose one of the following: • **Automatic**—When selected, you should enter the Retry Count and Interval options. • **Manual**—When selected, Interval and Retry Count fields are not editable.
Interval (in seconds)	Enter the time interval in seconds that clients can try to remediate after previous attempts.
Retry Count	Enter the number of attempts that clients can try to launch required programs.
Program Installation Path	From the drop-down list, choose the path where the remediation program has to be installed. • **ABSOLUTE_PATH**—remediation program is installed in the fully qualified path of the file. For example, C:\<directory>\ • **SYSTEM_32**—remediation program is installed in the C:\WINDOWS\system32 directory • **SYSTEM_DRIVE**—remediation program is installed in the C:\ drive • **SYSTEM_PROGRAMS**—remediation program is installed in the C:\Program Files • **SYSTEM_ROOT**—remediation program is installed in the root path of Windows system
Program Executable	Enter the name of the remediation program executable, or an installation file.
Program Parameters	Enter required parameters for the remediation programs.
Existing Programs	Existing Programs table displays the installation paths, name of the remediation programs, and parameters if any. • Click **Add** to add remediation programs to the Existing Programs list. • Click the delete icon to remove the remediation programs from the list.

Windows Update Remediation

The following table describes the fields in the Windows Update Remediation page. The navigation path is: Policy > Policy Elements > Results > Posture > Remediation Actions > Windows Update Remediation.

Table B-26 Windows Update Remediation

Fields	Usage Guidelines
Name	Enter a name for the Windows update remediation.
Description	Enter a description for the Windows update remediation.
Remediation Type	Choose one of the following: • **Automatic**—When selected, you should enter the Retry Count and Interval options. • **Manual**—When selected, Interval and Retry Count fields are not editable.
Interval (in seconds)	Enter the time interval in seconds that clients can try to remediate after previous attempts.

Table B-26 Windows Update Remediation (continued)

Fields	Usage Guidelines
Retry Count	Enter the number of attempts that Windows clients can try for Windows updates.
Windows Update Setting	Choose from the following: • Do not change setting—The Windows Automatic Updates client configuration does not change during or after Windows update remediation. • Notify to download and install—Windows only notifies clients, but does not automatically download, or install them. • Automatically download and notify to install—Windows downloads updates for clients, and notifies clients to install Windows updates. • Automatically download and install—Windows automatically downloads, and installs Windows updates. This is the highly recommended setting for Windows clients.
Override User's Windows Update setting with administrator's	Check this check box to enforce the administrator-specified setting for Windows Automatic Updates on all the clients during, and after Windows update remediation. If unchecked, the setting enforces the following: • The administrator-specified setting only when Automatic Updates are disabled on Windows clients. • The Windows clients-specified setting only when Windows Automatic Updates are enabled on the client.

Windows Server Update Services Remediation

The following table describes the fields in the Windows Update Remediation page. The navigation path is: Policy > Policy Elements > Results > Posture > Remediation Actions > Windows Update Remediation.

Table B-27 WSUS Remediation

Fields	Usage Guidelines
Name	Enter a name for the WSUS remediation.
Description	Enter a description for the WSUS remediation.
Remediation Type	Choose from the following: • **Automatic**—The NAC Agents automatically updates Windows clients with the latest WSUS updates. • **Manual**—If selected, the Interval and Retry Count fields are nor editable. The user manually updates the Windows client with the latest WSUS updates from a Microsoft-managed WSUS server, or from the locally administered WSUS server for compliance.
Interval (in seconds)	Enter the interval in seconds (the default interval is 0) to delay WSUS updates before the NAC Agents and Web Agents attempt to retry after the previous attempt.
Retry Count	Enter the number of attempts that the NAC Agents and web Agents retry to update Windows clients with WSUS updates.

Table B-27 WSUS Remediation (continued)

Fields	Usage Guidelines
Validate Windows updates using	Choose from the following: • **Cisco Rules**—If you choose this option, you can select custom or preconfigured rules as conditions in the posture requirement • **Severity Level**—If you choose this option, you can select custom or preconfigured rules as conditions in the posture requirement, but they are not used. The pr_WSUSRule can be used as a placeholder condition (a dummy condition) in the posture requirement that specifies a WSUS remediation.
Windows Updates Severity Level	Choose the severity level: • **Critical**—Installs only critical Windows updates • **Express**—Installs important and critical Windows updates • **Medium**—Installs all critical, important, and moderate Windows updates • **All**—Installs all critical, important, moderate, and low Windows updates **Note** When you associate a WSUS remediation action to a posture requirement to validate Windows updates by using the severity level option, you must choose the pr_WSUSRule (a dummy compound condition) compound condition in the posture requirement. When the posture requirement fails, the NAC Agent enforces the remediation action (Windows updates) based on the severity level that you define in the WSUS remediation.
Update to latest OS Service Pack	Check this check box to allow WSUS remediation install the latest service pack available for the client's operating system automatically. **Note** The operating system service packs are updated automatically irrespective of the Medium and All severity level options selected in WSUS remediation.
Windows Updates Installation Source	Specifies the source from where you install WSUS updates on Windows clients: • **Microsoft server**—Microsoft-managed WSUS server • **Managed server**—Locally administered WSUS server
Installation Wizard Interface Setting	Allows you to display the installation wizard on the client during WSUS updates: • **Show UI**—Displays the Windows Update Installation Wizard progress on Windows clients. Users must have Administrator privileges on clients to view the installation wizard during WSUS updates. • **No UI**—Hides the Windows Update Installation Wizard progress on Windows clients.

Client Posture Requirements

The following table describes the fields in the Posture Requirements page. The navigation path is: Policy > Policy Elements > Results > Posture > Requirements.

Table B-28 Posture Requirement

Fields	Usage Guidelines
Name	Enter a name for the requirement.
Operating Systems	Choose an operating system. Click plus [+] to associate more than one operating system to the policy. Click minus [-] to remove the operating system from the policy.
Conditions	Choose a Condition from the list. You can also create any user defined condition by clicking the Action Icon and associate it with the requirement. You cannot edit the associated parent operating system while creating user defined conditions. The pr_WSUSRule is a dummy compound condition, which is used in a posture requirement with an associated Windows Server Update Services (WSUS) remediation. The associated WSUS remediation action must be configured to validate Windows updates by using the severity level option. When this requirement fails, the NAC Agent that is installed on the Windows client enforces the WSUS remediation action based on the severity level that you define in the WSUS remediation. The pr_WSUSRule cannot be viewed in the Compound conditions list page. You can only select the pr_WSUSRule from the Conditions widget.
Remediation Actions	Choose a Remediation from the list. You can also create a remediation action and associate it with the requirement. You have a text box for all the remediation types that can be used to communicate to the Agent users. In addition to remediation actions, you can communicate to Agent users about the non compliance of clients with messages. The **Message Text Only** option informs Agent users about the noncompliance. It also provides optional instructions to the user to contact the Help desk for more information, or to remediate the client manually. In this scenario, the NAC Agent does not trigger any remediation action.