Policy User Interface Reference

Authentication

This section describes the authentication policy page, which allows you to configure simple and rule-based authentication policies.

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**.

Table 1: Simple Authentication Policy Configuration Settings

Fields	Usage Guidelines
Network Access Service	Choose an allowed protocol that you have already created.
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. You can edit the default identity source that you want Cisco ISE to use in case none of the identity sources defined in this rule match the request.

Fields	Usage Guidelines
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.

Rule-Based Authentication Policy Configuration Settings

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

Table 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.
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: • **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.

Fields	Usage Guidelines
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
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

Fields	Usage Guidelines
Select Network Access	Choose from allowed protocols or RADIUS server sequence.
Arrow Button	Click to define conditions for the identity source selection.
Identity Source Sequence	You can do the following: **1** Click the action icon in the default identity source row, and click Insert new row above. **2** Enter a name for your identity source rule. **3** Click the button to define the conditions based on which you want to choose the identity source. **4** Choose the identity source sequence or the identity source and the action that you want Cisco ISE to take.

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 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.

Fields	Usage Guidelines
Permissions	Choose an authorization profile from the **Standard** category.

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 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.
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**

Fields	Usage Guidelines
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.
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

Fields	Usage Guidelines
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.

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

This section describes RADIUS vendor dictionaries used in Cisco ISE.

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 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.
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 to mark the attribute as being permitted to have a tag, as defined in RFC2868. The purpose of the tag is to allow grouping of attributes for tunnelled users. See RFC2868 for more details. The tagged attributes support ensures that all attributes pertaining to a given tunnel contain the same value in their respective tag fields, and that each set includes an appropriately-valued instance of the Tunnel-Preference attribute. This conforms to the tunnel attributes that are to be used in a multi-vendor network environment, thereby eliminating interoperability issues among Network Access Servers (NASs) manufactured by different vendors.
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 describes policy conditions used for profiling endpoints, posture clients, and to limit or extend permission to access to Cisco ISE system resources.

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 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.
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.

Posture Conditions Settings

This section describes simple and compound conditions used for posture.

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 7: File Condition Settings

Fields	Usage Guidelines
Name	Enter the name of the file condition.
Description	Enter a description for the file condition.
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. • **FileDate—**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

Fields	Usage Guidelines
Date and Time	(Available only if you select **FileDate** 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 **FileVersion** 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.

Table 8: File Condition Settings

Fields	Usage Guidelines for Windows OS	Usage Guidelines for Mac OSX
Name	Enter the name of the file condition.	Enter the name of the file condition.
Description	Enter a description for the file condition.	Enter a description for the file condition.
Operating System	Select any Windows operating system to which the file condition should be applied.	Select any Mac OSX to which the file condition should be applied.
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.	Choose one of the predefined settings: • **Root—**Checks the file in the root (/) directory. • **Home—**Checks the file in the home (~) directory.

Fields	Usage Guidelines for Windows OS	Usage Guidelines for Mac OSX
File Type	Choose one of the predefined settings: • **FileDate—**Checks whether a file with a particular file-created or file-modified date exists on the system. • **FileExistence—**Checks whether a file exists on the system. • **FileVersion—**Checks whether a particular version of a file exists on the system. • **CRC32—**Checks the data integrity of a file.	Choose one of the predefined settings: • **FileDate—**Checks whether a file with a particular file-created or file-modified date exists on the system. • **FileExistence—**Checks whether a file exists on the system. • **CRC32—**Checks the data integrity of a file.
File Date Type	(Available only if you select **FileDate** as the File Type) Choose **Creation Date** or **Modification Date**.	(Available only if you select **FileDate** as the File Type) Choose **Creation Date** or **Modification Date**.
File Operator/Operator	The File Operator options change according to the settings you select in the File Type. Choose the settings appropriately: FileDate • EarlierThan • LaterThan • EqualTo FileExistence • Exists • DoesNotExist FileVersion • EarlierThan • LaterThan • EqualTo CRC32 • File CRC Data, for example, you can enter a checksum value of 0x3c37fec3. The checksum value should start with 0x, a hexadecimal integer.	The File Operator options change according to the settings you select in the File Type. Choose the settings appropriately: FileDate • EarlierThan • LaterThan • EqualTo FileExistence • Exists • DoesNotExist CRC32 • File CRC Data, for example, you can enter a checksum value of 0x3c37fec3. The checksum value should start with 0x, a hexadecimal integer.

Fields	Usage Guidelines for Windows OS	Usage Guidelines for Mac OSX
Date and Time	(Available only if you select **FileDate** as the File Type) Enter the date and time of the client system in mm/dd/yyyy and hh:mm:ss format.	(Available only if you select **FileDate** 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 **FileVersion** as the File Type) Enter the version of the file to be checked.	NA.

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 9: 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

Fields	Usage Guidelines
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 10: 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.

Table 11: Application Condition Settings

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

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 12: 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.

Table 13: Service Conditions Settings

Fields	Usage Guidelines
Name	Enter a name for the service condition.
Description	Enter a description of the service condition.
Operating Systems	Select the operating system to which the service condition should be applied. You can select different versions of the Mac OSX or Windows OS.
Service Name	Enter the name of the service or daemon running as root. The AnyConnect agent uses the command **sudo launchctl list** to validate the service condition.
Service Operator	Choose the status that you want to check: • Windows OS—To check if a service is **Running** or **Not Running**. • Mac OSX—To check if a service is **Loaded** or **Unloaded**.

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 14: 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 15: 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.

Fields	Usage Guidelines
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.
current system 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 current system date.

Fields	Usage Guidelines
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** > **AS Compound Condition**.

Table 16: 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.

Fields	Usage Guidelines
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).
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 17: 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.

Fields	Usage Guideline
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 18: 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.
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.

Fields	Usage Guidelines
Value	Enter a value that you want to associate to the dictionary attribute, or choose a value from the drop-down list.

Patch Management Condition Settings

The following table describes the fields in the Patch Management Conditions page. The navigation path is: **Policy** > **Policy Elements** > **Conditions** > **Posture** > **Patch Management Condition**.

Table 19: Patch Management Condition

Fields	Usage Guidelines
Name	Enter the name of the patch management condition that you want to create.
Description	Enter a description for the patch management condition.
Operating System	Select an operating system to check the installation of a patch management software on the endpoint, or check the latest patch management definition file updates to which the condition is applied. You can select the Windows OS or Mac OSX. You can also select more than one version of an operating system to create the patch management condition.
Vendor Name	Choose a vendor name from the drop-down list. The patch management products of a vendor, and their supported version, check type, and minimum compliant module are retrieved and displayed in the **Products for Selected Vendor** table. The list in the table changes according to the selected operating system.
Check Type	Select any one of the following options: • **Installation—**To check if the selected product is installed on the endpoint. This check type is supported by all vendors. • **Enabled—**To check if the selected product is enabled on the endpoint. Verify if the vendor's product supports the chosen check type by referring to the **Products for Selected Vendor** list. • **Up to Date—**To check if the selected product does not have missing patches. Verify if the vendor's product supports the chosen check type by referring to the **Products for Selected Vendor** list. Click the **Products for Selected Vendor** drop-down arrow, to view the list of products that the vendor you have specified in the **Vendor Name** supports. For example, if you have selected Vendor A, that has two products, namely Product 1 and Product 2. Product 1 may support the Enabled option, whereas Product 2 might not. Or, if Product 1 does not support any of the check types, it is grayed out.

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 20: 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.
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.

Results

This section describes requirements for Cisco ISE services.

Allowed Protocols

The following table describes the fields in the Allowed Protocols 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**.

In the following table, PAC stands for Protected Access Credentials.

Table 21: Allowed Protocols

Fields	Usage Guidelines
Allowed Protocols > Authentication Bypass	
Process Host Lookup	Check this check box if you want Cisco ISE to process the Host Lookup request. The Host Lookup request is processed for PAP/CHAP protocol when the RADIUS Service-Type equals 10 (Call-Check) and the username is equal to Calling-Station-ID. The Host Lookup request is processed for EAP-MD5 protocol when the Service-Type equals 1 (Framed) and the username is equal to Calling-Station-ID. 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).
Allowed Protocols > Authentication Protocols	
Allow PAP/ASCII	This option enables PAP/ASCII. PAP uses cleartext passwords (that is, unencrypted passwords) and is the least secure authentication protocol.
Allow CHAP	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 password hashed authentication.

Fields	Usage Guidelines
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. • Allow authentication of expired certificates to allow certificate renewal in Authorization Policy—Check this check box, if you want to allow users to renew certificates. If you check this check box, ensure that you configure appropriate authorization policy rules to check if the certificate has been renewed before processing the request any further.
Allow LEAP	Check this check box to enable Lightweight Extensible Authentication Protocol (LEAP) authentication.
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 0 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 0 to 3. • Allow EAP-TLS—Check this check box to use EAP-TLS as the inner method. Check the **Allow authentication of expired certificates to allow certificate renewal in Authorization Policy** check box, if you want to allow users to renew certificates. If you check this check box, ensure that you configure appropriate authorization policy rules to check if the certificate has been renewed before processing the request any further. • 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 PEAP conversations are not dropped, check this check box.

Fields	Usage Guidelines
Allow EAP-FAST	

Fields	Usage Guidelines
	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. 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. ◦ Retry Attempts—Specifies how many times Cisco ISE requests user credentials before returning login failure. Valid values are 0-3. • Allow EAP-GTC 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 0-3. • Use PACs—Choose this option to configure Cisco ISE to provision authorization PACs 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. • Allow EAP-TLS—Check this check box to use EAP-TLS as the inner method. Check the **Allow authentication of expired certificates to allow certificate renewal in Authorization Policy** check box, if you want to allow users to renew certificates. If you check this check box, ensure that you configure appropriate authorization policy rules to check if the certificate has been renewed before processing the request any further. • Enable EAP Chaining—Check this check box to enable EAP chaining. EAP chaining allows Cisco ISE to correlate the results of user and machine authentication and apply the appropriate authorization policy using the EAPChainingResult attribute. EAP chaining requires a supplicant that supports EAP chaining on the client device. Cisco ISE supports AnyConnect 4.0. Choose the User and Machine Authentication option in the supplicant. EAP chaining is available when you choose the EAP-FAST protocol (both in PAC based and PAC less mode). For PAC-based authentication, you can use user authorization PAC or machine authorization PAC, or both to skip the inner method. For certificate-based authentication, if you enable the Accept Client Certificate for Provisioning option for the EAP-FAST protocol (in the Allowed Protocol service), and

Fields	Usage Guidelines
	if the endpoint (AnyConnect) is configured to send the user certificate inside the tunnel, then during tunnel establishment, ISE authenticates the user using the certificate (the inner method is skipped), and machine authentication is done through the inner method. If these options are not configured, EAP-TLS is used as the inner method for user authentication. After you enable EAP chaining, update your authorization policy and add a condition using the NetworkAccess:EapChainingResult attribute and assign appropriate permissions. For example: ◦ If EapChainingResult equal User and machine both succeeded - Full access ◦ If EapChainingResult equal User passed and machine failed - Restricted access ◦ If EapChainingResult equal User failed and machine passed - Restricted access ◦ If EapChainingResult equal User and machine both failed - Authentication fails. Cisco ISE does not process the authorization policy and sends a reject access message.
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, EAP-TTLS, and EAP-MD5. If you do not specify the preferred protocol, EAP-TLS is used by default.

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 22: PAC Options

Fields	Usage Guidelines
Use PAC	

Fields	Usage Guidelines
	• 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 skip 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

Fields	Usage Guidelines
	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.

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 23: 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.

Fields	Usage Guidelines
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.
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, DRW, 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.

Fields	Usage Guidelines
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.
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.

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 24: 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.
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.

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 25: 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.

Fields	Usage Guidelines
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 26: 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 27: Antivirus Remediation

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

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 28: 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.

Fields	Usage Guidelines
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 29: 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.

Fields	Usage Guidelines
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 30: 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.

Fields	Usage Guidelines
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 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 31: WSUS Remediation

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

Fields	Usage Guidelines
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.
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.

Fields	Usage Guidelines
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.

Patch Management Remediation

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

Table 32: Patch Management Remediation

Fields	Usage Guidelines
Name	Enter a name for the patch management remediation.
Description	Enter a description for the patch management remediation.
Remediation Type	Choose one of the following: • **Automatic—**Enter values for the Interval and Retry Count. The ISE server identifies non-compliant clients and selects a remediation notification method and automatically updates the latest patch on the client. • **Manual—**(Interval and Retry Count fields are disabled) Non-compliant clients should download and apply the latest patches manually.
Interval (in seconds)	(Available only when you select the Automatic remediation type) Enter the time interval in seconds after which a scheduled patch update on the client is performed.
Retry Count	(Available only when you select the Automatic remediation type) Enter the number of times that a client can attempt to update critical patches.

Fields	Usage Guidelines
Operating System	Windows OS is the only OS that is supported.
Patch Management Vendor Name	Choose a vendor name from the drop-down list. The patch management remediation products of a vendor along with their product's support for the version, enable remediation, update remediation, and show UI remediation is displayed in the **Products for Selected Vendor** table. **Note** Supported versions of Cisco ISE and AnyConnect: • Cisco ISE version 1.4 • AnyConnect version 4.1 and later
Remediation Option	Select any one of the following options: • **Enable—**Enables the patch management software, in case it is disabled on the endpoint. • **Install Missing Patches—**Updates the patch on the endpoint. • **Activate Patch Management Software GUI—**Displays the patch management software user interface. Follow the instructions on this page to change the software settings or initiate software updates. Click the **Products for Selected Vendor** drop-down arrow, to view the list of products that the vendor you have specified in the **Patch Management Vendor Name** supports. For example, if you have selected Vendor A, that has two products, namely Product 1 and Product 2. Product 1 may support the Enable remediation option, whereas Product 2 might not. Or, if Product 1 does not support the Enable and Install missing patches remediation options, then Product 1 is disabled (grayed out). The **Products for Selected Vendor** table changes according to the selected remediation option.

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 33: 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.

Fields	Usage Guidelines
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.