Compliance

Posture Types

The following posture agents monitor and enforce Cisco ISE posture policies:

- **Agent**: Deploys the agent to monitor and enforce Cisco ISE posture policies that require interaction with the client. The agent stays on the client. For more information about using agent in Cisco ISE, see Cisco Secure Client, on page 104.
- **Agent Stealth**: Runs posture as a service, with no user interface. The agent stays on the client.

  When you choose the Agent Stealth posture type in the posture requirement, some of the conditions, remediations, or attributes in a condition are disabled (grayed out). For example, when you enable Agent Stealth requirement, the Manual Remediation Type is disabled (grayed out) because this action requires client-side interaction.

  When you map the posture profile to the agent configuration, and then map the agent configuration to the Client Provisioning window for Agent Stealth mode deployment:

  - Agent can read the posture profile and set it to the intended mode.
  - Agent can send information related to the selected mode to Cisco ISE during the initial posture request.
  - Cisco ISE can match the right policy, based on the mode and other factors, such as identity group, OS, and compliance module.

Note Agent Stealth mode requires AnyConnect version 4.4 and later.

For more information about configuring Agent Stealth in Cisco ISE, see Configure Agent Stealth Mode Workflow, on page 74.

- **Temporal Agent**: When a client attempts to access the trusted network, Cisco ISE opens the Client Provisioning portal. The portal instructs the user to download and install the agent, and run the agent. The temporal agent checks the compliance status, and sends the status to Cisco ISE. Cisco ISE acts based on the results. The temporal agent removes itself from the client after compliance processing completes. The temporal agent does not support custom remediation. The default remediation supports only message text.

  The Temporal Agent does not support the following conditions:

  - Service Condition MAC—System Daemon check
  - Service Condition-MAC—Daemon or User Agent check
  - PM—Up To Date check
  - PM—Enabled check
  - DE—Encryption check

  - Configure posture policies using the **Posture Types Temporal Agent** and **Compliance Module 4.x or later**. Do not configure the compliance module as **3.x or earlier** or **Any Version**.
  - For the Temporal Agent, you can only view Patch Management conditions containing the **Installation** check type in the **Requirements** window.
  - Cisco ISE does not support VLAN-controlled posture with the Temporal Agent for macOS. When you change the network access from an existing VLAN to a new VLAN, the user's IP address is released before the VLAN change. The client gets a new IP address by DHCP when the user connects to the new VLAN. Recognizing the new IP address requires root privileges, but the Temporal Agent runs as a user process.
  - Cisco ISE supports ACL-controlled posture environment, which does not require the refreshing of endpoint IP addresses.
  - For more information about configuring the Temporal agent in Cisco ISE, see Configure Cisco Temporal Agent Workflow, on page 79.

- **AMP Enabler**—The AMP Enabler pushes the AMP for Endpoints software to a subset of endpoints from a server hosted locally within the enterprise, and installs AMP services to its existing user base.
- **Agentless Posture**—Agentless posture provides posture information from clients, and completely removes itself when finished. No action is required from the end user. Unlike the Temporal agent, Agentless Posture connects to the client as an administrative user. For more information about using Agentless Posture in Cisco ISE, see Agentless Posture, on page 4.

You can select the posture type in the **Client Provisioning** window (**Policy > Policy Elements > Results > Client Provisioning > Resources**) and the **Posture Requirements** window (**Policy > Policy Elements > Results > Posture > Requirements**). The best practice is to provision the posture profile in the Client Provisioning window.

Related Topics

Configure Agent Stealth Mode Workflow, on page 74
Configure Cisco Temporal Agent Workflow, on page 79

Agentless Posture

Agentless posture provides posture information from clients, and completely removes itself when finished, until invoked by Cisco ISE again. No action is required from the end user.

The agentless posture package is available as part of the default Cisco ISE client provisioning resources. You can select this package while creating an agent configuration to be used for the client provisioning policy.

Prerequisites:

- The client must be reachable through its IPv4 address, and that IP address must be available in RADIUS accounting. IPv6 is not supported.
- Windows and Mac clients are currently supported:
  - For Windows clients, port 5985 to access powershell on the client must be open. Powershell must be v5.1 or later. The client must have cURL v7.34 or later.
  - For MacOS clients, port 22 to access SSH must be open to access the client. The client must have cURL v7.34 or later.
- Client credentials for shell login must have local admin privileges.
- Run the posture feed update to get the latest clients, as described in the configuration steps.
- Ensure that the following entry is updated in the sudoers file to avoid certificate installation failure on the endpoints:

```
<macadminusername> ALL = (ALL) NOPASSWD: /usr/bin/security, /usr/bin/osascript
```

- For MacOS, the user account that is configured must be an administrator's account. Agentless posture for MacOS does not work with any other account type, even if you grant more privileges. To view this window, click the **Menu** icon (☰) and choose **Administration** > **System** > **Settings** > **Endpoint Scripts** > **Login Configuration** > **MAC Local User**.
- In case of changes in port-related activities in Windows clients due to updates from Microsoft, you might have to reconfigure the agentless posture configuration workflow for Windows clients.

Supported Posture Conditions

- File conditions, except the conditions that use the USER_DESKTOP and USER_PROFILE file paths
- Service conditions, except System Daemon and Daemon or User Agent checks on macOS
- Application conditions
- External Data Source conditions
- Compound conditions
- Anti-malware conditions
- Patch management condition, except the **Enabled** and **Up To Date** condition checks
- Firewall conditions
- Disk encryption conditions, except the encryption location-based condition check
- Registry conditions, except the conditions that use HCSK as root key

Note If dual stack protocol is used for authentication in the agentless posture flow, the NADs must also use the same protocol.

Unsupported Posture Conditions

- Remediation
- Grace period
- Periodic Reassessment
- Acceptable Use-policy

Supported Client Operating Systems

- Microsoft Windows versions: 10, 11
- macOS versions: 10.13, 10.14, 10.15, 13.x, and 14

Agentless Posture Process Flow

1. The client connects to the network.
2. Cisco ISE detects if agentless posture is enabled in the authorization profile used by client.
3. If so, Cisco ISE sends an agentless posture job request to the Cisco ISE Messaging queue.
4. Cisco ISE gets the job from the messaging queue, and starts the agentless posture flow.
5. Cisco ISE connects to the client via power shell or SSH.
6. Cisco ISE pushes the certificate, if it’s not already in the client's trust certificate authority store.
7. Cisco ISE runs the client provisioning policy.
8. Cisco ISE pushes the agentless plug-in to the client and launches the plug-in.
9. Posture evaluation runs on the client, and sends the status to Cisco ISE.
10. Cisco ISE removes the agentless plug-in from the client. Logs of the posture flow remain on the client for 24 hours, or until the client deletes them.

Agentless Posture Configuration

1. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy > Policy Elements > Results > Posture > Requirements**, and create one or more Posture Requirements that use Agentless posture to identify the requirement.
2. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers > Posture > Posture Policy**, and create one or more supported Posture Policy rules that use Agentless posture for that Posture Requirement. You can duplicate the rules you plan to use, and change the Posture type to Agentless.
3. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy > Policy Elements > Results > Authoriation > Authorization Profiles** and create an Authorization Profile that evaluates the results from Agentless Posture.

- Enable Agentless posture in the authorization profile.
- Use this profile only for Agentless posture. Do not also use this for other posture types.
- CWA and Redirect ACL is not required for Agentless posture. You can use VLANs, DACLs, or ACLs as part of your segmentation rules.

4. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy > Client Provisioning** and add a Client Provisioning policy. For the Cisco Agent Configuration, choose the Agentless plug-in for the Operating System that you configured. For Windows, the plug-in is CiscoAgentlessWindows 4.9.01095. For MacOS, the plug-in is CiscoAgentlessOSX 4.9.01095. Select the posture condition this rule checks for. Note, if you're using Active Directory, you can use Active Directory groups in your policy.

Note Agentless posture configuration for MACOSX 10.14 and 10.15 versions aren't available until you update the posture feed. Before you can run the posture feed, update the posture feed URL. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Posture** > **Settings** > **Software Updates** > **Posture Updates**. In the **Posture Updates** window, enter the url (https://www.cisco.com/web/secure/spa/posture-update.xml) in the **Update Feed URL** field and click **Update Now**.

5. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy > Policy Sets** and expand Authorization Policy. Enable and configure the following three Authorization policies:
   - **Unknown_Compliance_Redirect**: Configure conditions Network_Access_Authentication_Passed AND Compliance_Unknown_Devices with result Agentless Posture.
   - **NonCompliant_Devices_Redirect**: Configure conditions Network_Access_Authentication_Passed and Non_Compliant_Devices with result DenyAccess.
   - **Compliant_Devices_Access**: Configure conditions Network_Access_Authentication_Passed and Compliant_Devices with result PermitAccess.
6. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration > Settings > Endpoint Scripts > Endpoint Login Configuration** , and configure the client credentials to log onto clients. These same credentials are used by the Endpoint Scripts.
7. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration > Settings > Endpoint Scripts > Settings**, and configure **Max retry attempts for OS identification** and **Delay between retries for OS identification**. These settings determine how quickly connectivity issues can be confirmed. For example, an error that the PowerShell port is not open displays in logs only after all retries are not exhausted.
8. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration > System > Settings > Posture > General Settings**, and configure the Agentless Posture settings.
9. As clients connect with Agentless posture, you can see them in the Live Logs.

Debugging and Troubleshooting

Enable debug log level for:

- Infrastructure
- Client Provisioning

- Posture

The debug log is in *ise-psc.log*

Agentless Posture Troubleshooting is available under:

- In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations** > **Live Logs**—The three dots under the Posture Status column opens Agentless Posture Troubleshooting.
- In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations** > **Troubleshoot** > **Diagnostics** > **General Tools**

Agentless Posture Troubleshooting

The Agentless Posture report is the main troubleshooting tool to use when agentless posture isn't working as expected. This report shows the stages of agentless flow, including events such as script upload completed, script upload failed, script execution completed, and so on, along with any known failure reasons, if any.

Note The agentless posture script cannot verify itself, but the script verifies the data received from Cisco ISE after it is executed.

You can access Agentless Posture Troubleshooting from two locations:

- In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations** > **Live Logs**, and click the vertical three dots in the **Posture Status** column adjacent to the client you want to troubleshoot.
- In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations** > **Troubleshoot** > **Diagnostics** > **General Tools** > **Agentless Posture Troubleshooting**.

The Agentless Posture Troubleshooting tool collects Agentless Posture activity for a specified client. **Agentless Posture Flow** initiates posture and displays all the interactions between a currently active client and Cisco ISE. **Only Download Client Logs** creates logs with up to 24 hours of posture flows from the client. The client can delete the logs at any time. After collection is completed, you can export a ZIP file of the logs.

Reports

In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations** > **Reports** > **Reports** > **Endpoints and Users** > **Agentless Posture** to view all the endpoints that ran Agentless posture.

Posture Administration Settings

You can globally configure the Admin portal for posture services. You can download updates automatically to the Cisco ISE server through the web from Cisco. You can also update Cisco ISE manually offline later. In addition, having an agent like Cisco Secure Client or the Web Agent installed on the clients provides posture assessment and remediation services to clients. The client agent periodically updates the compliance status of clients to Cisco ISE. After login and successful requirement assessment for posture, the client agent displays a dialog with a link that requires end users to comply with terms and conditions of network usage. You can

use this link to define network usage information for your enterprise network that end users accept before they can gain access to your network.

Client Posture Requirements

To create a posture requirement:

1. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > **Posture** > **Requirements**.
2. From the **Edit** drop-down list at the end of any requirement row, choose **Insert New Requirement**.
3. Enter the required details and click **Done**.

The following table describes the fields in the **Client Posture Requirements** window.

Table 1: Posture Requirement

Field Name	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.
Compliance Module	From the **Compliance Module** drop-down list, choose the required compliance module: • 4.x or Later: Supports antimalware, disk encryption, patch management, and USB conditions. • 3.x or Earlier: Supports antivirus, antispyware, disk encryption, and patch management conditions. • Any Version: Supports file, service, registry, application, and compound conditions. For more information about compliance module, see Compliance Module, on page 23.
Posture Type	From the **Posture Type** drop-down list, choose the required posture type. • Agent: Deploys the agent to monitor and enforce Cisco ISE policies that require client interaction. • Agent Stealth: Deploys the agent to monitor and enforce Cisco ISE posture policies without any client interaction. • Temporal Agent: A temporary executable file that is run on the client to check the compliance status.

Field Name	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 agent 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 agent does not trigger any remediation action.

Related Topics

Configure Acceptable Use Policies for Posture Assessment, on page 19
Create Client Posture Requirements, on page 70

Timer Settings for Clients

You can set up timers for users to remediate, to transition from one state to another, and to control the login success screen.

We recommend configuring agent profiles with remediation timers and network transition delay timers and the timer used to control the login success screen on client machines so that these settings are policy based. You can configure all these timers for agents in client provisioning resources in the **Agent Posture Profile** window (**Policy** > **Policy Elements** > **Results** > **Client Provisioning** > **Resources** > **Add** > **Agent Posture Profile**).

However, when there are no agent profiles configured to match the client provisioning policies, you can use the settings in the **General Settings** configuration window (**Administration** > **System** > **Settings** > **Posture** > **General Settings**).

Set Remediation Timer for Clients to Remediate Within Specified Time

You can configure the timer for client remediation within a specified time. When clients fail to satisfy configured posture policies during an initial assessment, the agent waits for the clients to remediate within the time configured in the remediation timer. If the client fails to remediate within this specified time, then the client

agent sends a report to the posture run-time services after which the clients are moved to the noncompliance state.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Settings** > **Posture** > **General Settings**.

Step 2 In the **Remediation Timer** field, enter a time value in minutes.

The default value is 4 minutes. The valid range is 1–300 minutes.

Step 3 Click **Save**.

Set Network Transition Delay Timer for Clients to Transition

You can configure the timer for clients to transition from one state to the other state within a specified time using the network transition delay timer, which is required for Change of Authorization (CoA) to complete. It may require a longer delay time when clients need time to get a new VLAN IP address during success and failure of posture. When successfully postured, Cisco ISE allows clients to transition from unknown to compliant mode within the time specified in the network transition delay timer. Upon failure of posture, Cisco ISE allows clients to transition from unknown to noncompliant mode within the time specified in the timer.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Settings** > **Posture** > **General Settings**.

Step 2 Enter a time value in seconds, in the **Network Transition Delay** field.

The default value is 3 seconds. The valid range is 2 to 30 seconds.

Step 3 Click **Save**.

Set Login Success Window to Close Automatically

After successful posture assessment, the client agent displays a temporary network access screen. The user needs to click the **OK** button in the login window to close it. You can set up a timer to close this login screen automatically after specified time.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Settings** > **Posture** > **General Settings**.

Step 2 Check the **Automatically Close Login Success Screen After** check box.

Step 3 Enter a time value in seconds, in the field next to **Automatically Close Login Success Screen After** check box.

The valid range is 0 to 300 seconds. If the time is set to zero, then agent does not display the login success screen.

Step 4 Click **Save**.

Set Posture Status for Nonagent Devices

You can configure the posture status of endpoints that run on non-agent devices. When Android devices and Apple devices such as an iPod, iPhone, or iPad connect to a Cisco ISE enabled network, these devices assume the Default Posture Status settings.

These settings can also be applied to endpoints that run on Windows and MacOS operating systems when a matching client provisioning policy is not found during posture runtime while redirecting the endpoints to the client provisioning portal.

Before you begin

In order to enforce policy on an endpoint, you must configure a corresponding Client Provisioning policy (Agent installation package). Otherwise, the posture status of the endpoint automatically reflects the default setting.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Settings** > **Posture** > **General Settings**.

Step 2 From the **Default Posture Status** drop-down list, choose the option as **Compliant** or **Noncompliant**.

Step 3 Click **Save**.

Posture Lease

You can configure Cisco ISE to perform posture assessment every time a user logs into your network or perform posture assessment in specified intervals. The valid range is from 1 to 365 days.

This configuration applies only for those who use agent for posture assessment.

When the posture lease is active, Cisco ISE will use the last known posture state and will not reach out to the endpoint to check for compliance. But when the posture lease expires, Cisco ISE does not automatically trigger a re-authentication or a posture reassessment for the endpoint. The endpoint will stay in the same compliance state since the same session is being used. When the endpoint re-authenticates, posture will be run and the posture lease time will be reset.

Example Use Case Scenario:

- The user logs on to the endpoint and gets it posture compliant with the posture lease set to one day.
- Four hours later the user logs off from the endpoint (the posture lease now has 20 hours left).
- One hour later the user logs on again. Now the posture lease has 19 hours left. The last know posture state was compliant. Hence the user is provided access without posture being run on the endpoint.
- Four hours later the user logs off (the posture lease now has 15 hours left).
- 14 hours later, the user logs on. The posture lease has one hour left. The last known posture state was compliant. The user is provided access without posture being run on the endpoint.
- One hour later, the posture lease expires. The user is still connected to the network as the same user session is being used.

- One hour later, user logs off (the session is tied to the user but not to the machine, so the machine can stay on the network).
- One hour later the user logs on. Since the posture lease has expired and a new user session is launched, the machine performs a posture assessment, the results are sent to the Cisco ISE and the posture lease timer is reset to one day in case of this use case.

Periodic Reassessments

Periodic reassessment (PRA) can be done only for clients that are already successfully postured for compliance. PRA cannot occur if clients are not compliant on your network.

A PRA is valid and applicable only if the endpoints are in a compliant state. The policy service node checks the relevant policies, and compiles the requirements depending on the client role that is defined in the configuration to enforce a PRA. If a PRA configuration match is found, the policy service node responds to the client agent with the PRA attributes that are defined in the PRA configuration for the client before issuing a CoA request. The client agent periodically sends the PRA requests based on the interval specified in the configuration. The client remains in the compliant state if the PRA succeeds, or the action configured in the PRA configuration is to continue. If the client fails to meet PRA, then the client is moved from the compliant state to the noncompliant state.

The PostureStatus attribute shows the current posture status as compliant in a PRA request instead of unknown even though it is a posture reassessment request. The PostureStatus is updated in the Monitoring reports as well.

When the posture lease has not expired, an endpoint becomes compliant based on the Access Control List (ACL), and PRA is initiated. If PRA fails, the endpoint is deemed noncompliant and the posture lease is reset.

Note PRA is not supported during PSN failover. After PSN failover, you must either enable rescan on the client or enable posture lease.

Configure Periodic Reassessments

You can configure periodic reassessments only for clients that are already successfully postured for compliance. You can configure each PRA to a user identity group that is defined in the system.

Before you begin

- Ensure that each Periodic reassessment (PRA) configuration has a unique group or a unique combination of user identity groups assigned to the configuration.
- You can assign a role_test_1 and a role_test_2, which are the two unique roles to a PRA configuration. You can combine these two roles with a logical operator and assign the PRA configuration as a unique combination of two roles. For example, role_test_1 OR role_test_2.
- Ensure that two PRA configurations do not have a user identity group in common.
- If a PRA configuration already exists with a user identity group *Any*, you cannot create other PRA configurations unless you perform one of the following:
  - Update the existing PRA configuration with the Any user identity group to reflect a user identity group other than *Any*.

• Delete the existing PRA configuration with a user identity group "*Any*".

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Settings** > **Posture** > **Reassessments**.

Step 2 Click **Add**.

Step 3 Modify the values in the **New Reassessment Configuration** window to create a new PRA.

Step 4 Click **Submit** to create a PRA configuration.

Posture Troubleshooting Settings

The following table describes the fields on the Posture troubleshooting window, which you use to find and resolve posture problems on the network. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations** > **Troubleshoot** > **Diagnostic Tools** > **General Tools** > **Posture Troubleshooting**.

Table 2: Posture Troubleshooting Settings

Field Name	Usage Guidelines
Search and Select a Posture event for troubleshooting	
Username	Enter the username to filter on.
MAC Address	Enter the MAC address to filter on, using format: xx-xx-xx-xx-xx-xx
Posture Status	Select the authentication status to filter on:
Failure Reason	Enter the failure reason or click **Select** to choose a failure reason from a list. Click **Clear** to clear the failure reason.
Time Range	Select a time range. The RADIUS authentication records that are created during this time range are used.
Start Date-Time:	(Available only when you choose Custom Time Range) Enter the start date and time, or click the calendar icon to select the start date and time. The date should be in the *mm/dd/yyyy* format and time in the *hh:mm* format.
End Date-Time:	(Available only when you choose Custom Time Range) Enter the end date and time, or click the calendar icon to select the start date and time. The date should be in the *mm/dd/yyyy* format and time in the *hh:mm* format.
Fetch Number of Records	Select the number of records to display: 10, 20, 50, 100, 200, 500
Search Result	
Time	Time of the event
Status	Posture status

Field Name	Usage Guidelines
Username	User name associated with the event
MAC Address	MAC address of the system
Failure Reason	Failure reason for the event

Related Topics

Posture Troubleshooting Tool, on page 81

Posture General Settings

The following table describes the fields on the Posture General Settings window, which you can use to configure general posture settings such as remediation time and posture status. To view this window, click the **Menu** icon (☰) and choose **Administration** > **System** > **Settings** > **Posture** > **General Settings**.

These settings are the default settings for posture, which can be overridden by a posture profile.

General Posture Settings

- **Remediation Timer**: Enter the time to wait before starting remediation. The default value is 4 minutes. The valid range is 1–300 minutes.
- **Network Transition Delay**: Enter a time value in seconds. The default value is 3 seconds. The valid range is from 2 to 30 seconds.
- **Default Posture Status**: Choose **Compliant** or **Noncompliant**. Non-agent devices assume this status while connecting to the network.
- **Automatically Close Login Success Screen After**: Check the check box to close the login success screen automatically after the specified time. You can configure the timer to close the login screen automatically. The valid range is from 0 to 300 seconds. If the time is set to zero, then the agents on the client do not display the login success screen.
- **Continuous Monitoring Interval**: Specify the time interval after which the agent should start sending monitoring data. For application and hardware conditions, for Cisco ISE 3.2 and above, the default value is 15 minutes.

Note To avoid performance impact on Cisco ISE, we recommend that you set the continuous monitoring interval to no less than 1 minute, for each 3,000 endpoints in the network being postured. For example, in an environment with 30,000 endpoints being postured, set the interval to no less than 10 minutes.

- **Agentless posture client timeout**: Specify how long to wait before a posture check is considered as failed.
- **Remove Agentless Plugin after each run**: Enabling this setting removes the agent from the client after running Agentless posture. We strongly recommend that you leave this disabled, so that the downloaded plugin can be reused, until newer versions are available. Leaving this disabled helps to reduce network traffic.

- **Acceptable Use Policy in Stealth Mode**: Choose **Block** in stealth mode to move a client to noncompliant posture status, if your company's network-usage terms and conditions are not met.

Posture Lease

- **Perform posture assessment every time a user connects to the network**: Select this option to initiate posture assessment every time the user connects to network
- **Perform posture assessment every n days**: Select this option to initiate posture assessment after the specified number of days, even if the client is already postured Compliant.
- **Cache Last Known Posture Compliant Status**: Check this check box for Cisco ISE to cache the result of posture assessment. By default, this field is disabled.
- **Last Known Posture Compliant Status**: This setting only applies if you have checked **Cache Last Known Posture Compliant Status**. Cisco ISE caches the result of posture assessment for the amount of time specified in this field. Valid values are from 1 to 30 days, or from 1 to 720 hours, or from 1 to 43200 minutes.

Related Topics

Posture Administration Settings, on page 7
Posture Lease, on page 11
Set Remediation Timer for Clients to Remediate Within Specified Time, on page 9
Set Network Transition Delay Timer for Clients to Transition, on page 10
Set Login Success Window to Close Automatically, on page 10
Set Posture Status for Nonagent Devices, on page 11

Download Posture Updates to Cisco ISE

Posture updates include a set of predefined checks, rules, and support charts for antivirus and antispyware for both Windows and MacOS operating systems, and operating systems information that are supported by Cisco. You can also update Cisco ISE offline from a file on your local system, which contains the latest archives of updates.

When you deploy Cisco ISE on your network for the first time, you can download posture updates from the web. This process usually takes approximately 20 minutes. After the initial download, you can configure Cisco ISE to verify and download incremental updates to occur automatically.

Cisco ISE creates default posture policies, requirements, and remediations only once during an initial posture updates. If you delete them, Cisco ISE does not create them again during subsequent manual or scheduled updates.

Before you begin

To ensure that you are able to access the appropriate remote location from which you can download posture resources to Cisco ISE, you may be required to verify that you have the correct proxy settings configured for your network as described in Specifying Proxy Settings in Cisco ISE.

You can use the Posture Update window to download updates dynamically from the web.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Settings** > **Posture** > **Updates**.

Step 2 Choose the **Web** option to download updates dynamically.

Step 3 Click **Set to Default** to set the Cisco default value for the **Update Feed URL** field.

If your network restricts URL-redirection functions (via a proxy server, for example) and you are experiencing difficulty accessing the above URL, try also pointing your Cisco ISE to the alternative URL in the related topics.

Step 4 Modify the values in the **Posture Updates** window.

Step 5 Click **Update Now** to download updates from Cisco.

After being updated, the Posture Updates window displays the current Cisco updates version information as a verification of an update under Update Information section in the Posture Updates window.

Step 6 Click **Yes** to continue.

Cisco ISE Offline Updates

This offline update option allows you to download client provisioning and posture updates, when direct internet access to Cisco.com from a device using Cisco ISE is not available or is not permitted by a security policy.

To download offline client provisioning resources:

Step 1 Go to: https://software.cisco.com/download/home/283801620/type/283802505/release/3.0.0.

Step 2 Provide your login credentials.

Step 3 Navigate to the Cisco Identity Services Engine download window, and select the release.

The following Offline Installation Packages are available for download:

- **win_spw-**<*version*>**-isebundle.zip**—Offline SPW Installation Package for Windows
- **mac-spw-**<*version*>.**zip**—Offline SPW Installation Package for Mac OS X
- **compliancemodule-**<*version*>**-isebundle.zip**—Offline Compliance Module Installation Package
- **macagent-**<*version*>**-isebundle.zip**—Offline Mac Agent Installation Package
- **webagent-**<*version*>**-isebundle.zip**—Offline Web Agent Installation Package

Step 4 Click either **Download** or **Add to Cart**.

For more information on adding the downloaded installation packages to Cisco ISE, see the "Add Client Provisioning Resources from a Local Machine" section in the Cisco Identity Services Engine Administrator Guide.

You can update the checks, operating system information, and antivirus and antispyware support charts for Windows and Mac operating systems offline from an archive in your local system, using posture updates.

For offline updates, ensure that the versions of the archive files match the versions in the configuration file. Use offline posture updates after you configure Cisco ISE and want to enable dynamic updates for the posture policy service.

To download offline posture updates:

Step 1 Go to https://www.cisco.com/web/secure/spa/posture-offline.html.

Step 2 Save the **posture-offline.zip** file to your local system. This file is used to update the operating system information, checks, rules, and antivirus and antispyware support charts for Windows and Mac operating systems.

Step 3 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration > System > Settings > Posture**.

Step 4 Click the arrow to view the settings for posture.

Step 5 Click **Updates**.
The **Posture Updates** window is displayed.

Step 6 Click the **Offline** option.

Step 7 Click **Browse** to locate the archive file (posture-offline.zip) from the local folder in your system.

Note The **File to Update** field is a mandatory field. You can select only one archive file (.zip) containing the appropriate files. Archive files other than .zip, such as .tar, and .gz are not supported.

Step 8 Click **Update Now**.

Download Posture Updates Automatically

After an initial update, you can configure Cisco ISE to check for the updates and download them automatically.

Before you begin

- You should have initially downloaded the posture updates to configure Cisco ISE to check for the updates and download them automatically.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Settings** > **Posture** > **Updates**.

Step 2 In the **Posture Updates** window, check the **Automatically check for updates starting from initial delay** check box.

Step 3 Enter the initial delay time in hh:mm:ss format.

Cisco ISE starts checking for updates after the initial delay time is over.

Step 4 Enter the time interval in hours.

Cisco ISE downloads the updates to your deployment at specified intervals from the initial delay time.

Step 5 Click **Save**.

Posture Acceptable Use Policy Configuration Settings

The following table describes the fields in the Posture Acceptable Use Policy Configurations window, which you can use to configure an acceptable use policy for posture. To view this window, click the **Menu** icon (☰) and choose **Administration** > **System** > **Settings** > **Posture** > **Acceptable Use Policy**.

Table 3: Posture AUP Configurations Settings

Field Name	Usage Guidelines
Configuration Name	Enter the name of the AUP configuration that you want to create.
Configuration Description	Enter the description of the AUP configuration that you want to create.
Show AUP to Agent users (for Windows only)	When selected, the link to network usage terms and conditions for your network is displayed to users upon successful authentication and posture assessment.
Use URL for AUP message	When selected, you must enter the URL to the AUP message in the AUP URL field.
Use file for AUP message	When selected, you must browse to the location and upload a file in a zipped format. The file must contain the index.html at the top level. The .zip file can include other files and subdirectories in addition to the index.html file. These files can reference each other using HTML tags.
AUP URL	Enter the URL to the AUP, which users must access upon successful authentication and posture assessment.
AUP File	Browse to the file and upload it to the Cisco ISE server. It should be a zipped file and should contain the index.html file at the top level.
Select User Identity Groups	Choose a unique user identity group or a unique combination of user identity groups for your AUP configuration. Note the following while creating an AUP configuration: • Posture AUP is not applicable for a guest flow • No two configurations have any user identity group in common • If you want to create a AUP configuration with a user identity group “Any”, then delete all other AUP configurations first • If you create a AUP configuration with a user identity group “Any”, then you cannot create other AUP configurations with a unique user identity group or user identity groups. To create an AUP configuration with a user identity group other than Any, either delete an existing AUP configuration with a user identity group “Any” first, or update an existing AUP configuration with a user identity group “Any” with a unique user identity group or user identity groups.

Field Name	Usage Guidelines
Acceptable use policy configurations—Configurations list	Lists existing AUP configurations and end user identity groups associated with AUP configurations.

Related Topics

Configure Acceptable Use Policies for Posture Assessment, on page 19

Configure Acceptable Use Policies for Posture Assessment

After login and successful posture assessment of clients, the client agent displays a temporary network access screen. This screen contains a link to an acceptable use policy (AUP). When the user clicks the link, they are redirected to a page that displays the network-usage terms and conditions, which they must read and accept.

Each Acceptable Use Policy configuration must have a unique user identity group, or a unique combination of user identity groups. Cisco ISE finds the AUP for the first matched user identity group, and then it communicates to the client agent that displays the AUP.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Settings** > **Posture** > **Acceptable Use Policy**.

Step 2 Click **Add**.

Step 3 Modify the values in the **New Acceptable Use Policy Configuration** window.

Step 4 Click **Submit**.

Posture Conditions

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

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

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

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

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

Simple Posture Conditions

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

- File Conditions: A condition that checks the existence of a file, the date of a file, and the versions of a file on the client.
- Registry Conditions: A condition that checks for the existence of a registry key or the value of the registry key on the client.
- Application Conditions: A condition that checks if an application or process is running or not running on the client.

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

- Service Conditions: A condition that checks if a service is running or not running on the client.
- Dictionary Conditions: A condition that checks a dictionary attribute with a value.
- USB Conditions: A condition that checks for the presence of USB mass storage device.

Create Simple Posture Conditions

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

Before you begin

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

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Conditions** > **Posture**.

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

Step 3 Click **Add**.

Step 4 Enter the appropriate values in the fields.

Step 5 Click **Submit**.

Compound Posture Conditions

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

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

- Dictionary Compound Conditions: Contains one or more dictionary simple conditions or dictionary compound conditions
- Antimalware Conditions: Contains one or more AM conditions.

Create Compound Posture Conditions

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

Before you begin

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

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Conditions** > **Posture** > **Compound Conditions** > **Add**.

Step 2 Enter appropriate values for the fields.

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

Step 4 Click **Submit**.

Dictionary Compound Condition Settings

Table 4: Dictionary Compound Condition Settings

Field Name	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.

Field Name	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 Cisco ISE will process each OR condition in a compound condition sequentially. For example, if a compound condition checks for A OR B, Cisco ISE first checks A and then B. If either condition A or B is passed, the overall result is marked as passed. If condition A fails and condition B succeeds, then the overall result is marked as passed. In this case, condition A is marked as failed and condition B as passed in the posture reports. If condition A succeeds, Cisco ISE skips condition B and marks the overall result as passed. In the posture reports, condition A is marked as passed, condition B as skipped, and the overall result as passed.
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

Compound Posture Conditions, on page 20
Create Compound Posture Conditions, on page 21

Predefined Condition for Enabling Automatic Updates in Windows Clients

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

Preconfigured Antivirus and Antispyware Conditions

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

Antivirus and Antispyware Support Chart

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

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

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

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

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

Compliance Module

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

The compliance module is available on Cisco.com.

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

Table 5: OPSWAT API Versions

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

Note

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

Check Posture Compliance

Step 1 Log in to Cisco ISE and access the dashboard.

Step 2 In the **Posture Compliance** dashlet, hover your cursor over a stack bar or sparkline.

A tooltip provides detailed information.

Step 3 Expand the data categories for more information.

Step 4 Expand the **Posture Compliance** dashlet.

A detailed real-time report is displayed.

Note You can view the posture compliance report in the **Context Visibility** window. Navigate **Context Visibility > Endpoints > Compliance**. This window displays different charts based on **Compliance Status**, **Location**, **Endpoints**, and **Applications by Categories**.

You might see the posture status for endpoints that do not have any active sessions. For example, if the last known posture status for an endpoint is **Compliant**, the status remains **Compliant** in the **Context Visibility** window until the next update is received for the endpoint, even if the endpoint session is terminated. The posture status is retained in the **Context Visibility** window until that endpoint is deleted or purged.

Create Patch Management Conditions

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

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

Before you begin

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

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Conditions** > **Posture** > **Patch Management Condition**.

Step 2 Click **Add**.

Step 3 Enter the condition name and description in the **Name** and **Description** fields.

Step 4 Choose the appropriate operating system from the **Operating System** drop-down field.

Step 5 Choose the **Compliance Module** from the drop-down list.

Step 6 Choose the **Vendor Name** from the drop-down list.

Step 7 Choose the **Check Type.**

Step 8 Choose the appropriate patch from the **Check patches installed** drop-down list.

Step 9 Click **Submit**.

Related Topics

Patch Management Condition Settings, on page 45
Add a Patch Management Remediation, on page 67

Create Disk Encryption Conditions

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

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

Before you begin

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

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Conditions** > **Posture** > **Disk Encryption Condition**.

Step 2 Click **Add**.

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

Step 4 Click **Submit**.

Posture Condition Settings

This section describes simple and compound conditions used for posture.

File Condition Settings

The following table describes the fields in the **File Conditions** window. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Conditions** > **Posture** > **File Condition**.

Table 6: File Condition Settings

Field Name	Usage Guidelines for Windows OS	Usage Guidelines for macOS	Usage Guidelines for Linux OS
Name	Enter the name of the file condition.	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.	Enter a description for the file condition.

Field Name	Usage Guidelines for Windows OS	Usage Guidelines for macOS	Usage Guidelines for Linux OS

Operating System	Choose any Windows operating system to which the file condition should be applied.	Choose any macOS to which the file condition should be applied.	Choose any Linux OS to which the file condition should be applied. The following options are available:
			• **Ubuntu**
			  • **18.04**
			  • **20.04**
			• **Red Hat**
			  • **7.5**
			  • **7.9**
			  • **8.1**
			  • **8.2**
			  • **8.3**
			• **SUSE**
			  • **12.3**
			  • **12.4**
			  • **12.5**
			  • **15.0**
			  • **15.1**
			  • **15.2**

Field Name	Usage Guidelines for Windows OS	Usage Guidelines for macOS	Usage Guidelines for Linux OS
File Type	Choose one of the following options: • **FileDate**: Checks whether a file with a particular file-created or file-modified date exists in the system. • **FileExistence**: Checks whether a file exists in the system. • **FileVersion**: Checks whether a particular version of a file exists in the system. • **CRC32**: Checks the data integrity of a file using the checksum function. • **SHA-256**: Checks the data integrity of a file using the hash function.	Choose one of the following options: • **FileDate**: Checks whether a file with a particular file-created or file-modified date exists in the system. • **FileExistence**: Checks whether a file exists in the system. • **CRC32**: Checks the data integrity of a file using the checksum function. • **SHA-256**: Checks the data integrity of a file using the hash function. • **PropertyList**: Checks the property value in a plist file, such as loginwindow.plist.	Choose one of the following options: • **FileDate**: Checks whether a file with a particular file-created or file-modified date exists in the system. • **FileExistence**: Checks whether a file exists in the system. • **CRC32**: Checks the data integrity of a file using the checksum function. • **SHA-256**: Checks the data integrity of a file using the hash function.

Field Name	Usage Guidelines for Windows OS	Usage Guidelines for macOS	Usage Guidelines for Linux OS
Data Type and Operator	NA	(Available only if you select **PropertyList** as the File Type) Choose the data type or value of the key to be searched in the plist files. Each data type contains a set of operators. • **Unspecified**: Checks the existence of the specified key. Enter an Operator (Exists, DoesNotExist). • **Number**: Checks for the specified key of number data type. Enter an Operator (equals, does not equal, greater than, less than, greater than or equal to, less than or equal to) and a Value. • **String**: Checks for the specified key of string data type. Enter an Operator (equals, does not equal, equals (ignore case), starts with, does not start with, contains, does not contain, ends with, does not end with) and a Value. • **Version**: Checks for the value of the specified key as a version string. Enter an Operator (earlier than, later than, same as) and a Value.	NA

Field Name	Usage Guidelines for Windows OS	Usage Guidelines for macOS	Usage Guidelines for Linux OS
Property Name	NA	(Available only if you select **PropertyList** as the File Type) Enter the name of the key, for example, BuildVersionStampAsNumber	NA

Field Name	Usage Guidelines for Windows OS	Usage Guidelines for macOS	Usage Guidelines for Linux OS
File Path	Choose one of the following options: • **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. • **USER_DESKTOP**: Checks if the specified file is present on the Windows user's desktop. Enter the file name. • **USER_PROFILE**: Checks if the file is present in the Windows user's local profile directory. Enter the file path.	Choose one of the following options: • **Root**: Checks the file in the root (/) directory. Enter the file path. • **Home**: Checks the file in the home (~) directory. Enter the file path.	Choose one of the following options: • **Root**: Checks the file in the root (/) directory. Enter the file path. • **Home**: Checks the file in the home (~) directory. Enter the file path.

Field Name	Usage Guidelines for Windows OS	Usage Guidelines for macOS	Usage Guidelines for Linux OS
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**.	(Available only if you select **FileDate** as the File Type) Choose **Creation Date** or **Modification Date**.
File Operator	The **File Operator** options change according to the settings you select in the **File Type**. Choose the settings appropriately: **FileDate** • **EarlierThan** • **LaterThan** • **EqualTo** • **Within**: The last *n* number of days. Valid range is from 1 to 300. **FileExistence** • **Exists** • **DoesNotExist** **FileVersion** • **EarlierThan** • **LaterThan** • **EqualTo**	The **File Operator** options change according to the settings you select in the **File Type**. Choose the settings appropriately: **FileDate** • **EarlierThan** • **LaterThan** • **EqualTo** • **Within**: The last *n* number of days. Valid range is from 1 to 300. **FileExistence** • **Exists** • **DoesNotExist**	The **File Operator** options change according to the settings you select in the **File Type**. Choose the settings appropriately: **FileDate** • **EarlierThan** • **LaterThan** • **EqualTo** • **Within**: The last *n* number of days. Valid range is from 1 to 300. **FileExistence** • **Exists** • **DoesNotExist**
File CRC Data	(Available only if you select **CRC32** as the **File Type**) You can enter a checksum value, for example, 0x3c37fec3 to check file integrity. The checksum value should start with 0x, a hexadecimal integer.	(Available only if you select **CRC32** as the **File Type**) You can enter a checksum value, for example, 0x3c37fec3 to check file integrity. The checksum value should start with 0x, a hexadecimal integer.	(Available only if you select **CRC32** as the **File Type**) You can enter a checksum value, for example, 0x3c37fec3 to check file integrity. The checksum value should start with 0x, a hexadecimal integer.

Field Name	Usage Guidelines for Windows OS	Usage Guidelines for macOS	Usage Guidelines for Linux OS
File SHA-256 Data	(Available only if you select **SHA-256** as the **File Type**) You can enter a 64-byte hexadecimal hash value to check file integrity.	(Available only if you select **SHA-256** as the **File Type**) You can enter a 64-byte hexadecimal hash value to check file integrity.	(Available only if you select **SHA-256** as the **File Type**) You can enter a 64-byte hexadecimal hash value to check file integrity.
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.	(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.

Related Topics

Simple Posture Conditions, on page 19
Compound Posture Conditions, on page 20
Create a Posture Condition, on page 77

Firewall Condition Settings

The Firewall condition checks if a specific Firewall product is running on an endpoint. The list of supported Firewall products is based on the OPSWAT support charts. You can enforce policies during initial posture and Periodic Reassessment (PRA).

Cisco ISE provides default Firewall conditions for Windows and macOS. These conditions are disabled by default.

Field Name	Usage Guidelines
Name	Enter the name of the Firewall condition.
Description	Enter a description for the Firewall condition.
Compliance Module	Choose the required compliance module. • 4.x or later • 3.x or later • Any Version
Operating System	Checks If the required Firewall product is installed on an endpoint. You can select the Windows OS or macOS.
Vendor	Choose a vendor name from the drop-down list. The Firewall products of a vendor and their check type are retrieved and displayed in the **Products for Selected Vendor** table. The list in the table changes according to the selected operating system.

Field Name	Usage Guidelines
Check Type	Enabled: To check if a specific Firewall is running on an endpoint. Verify if the vendor's product supports the chosen check type by referring to the **Products for Selected Vendor** list.

Registry Condition Settings

The following table describes the fields in the Registry Conditions window. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Conditions** > **Posture** > **Registry Condition**.

Table 7: Registry Condition Settings

Field Name	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.

Related Topics

Simple Posture Conditions, on page 19
Compound Posture Conditions, on page 20

Continuous Endpoint Attribute Monitoring

You can use the agent to continuously monitor different endpoint attributes to ensure that dynamic changes are observed during posture assessment. This improves the overall visibility of an endpoint and helps you create posture policies based on their behavior. The agent monitors applications that are installed and running on an endpoint. You can turn on and off the feature and configure how often the data should be monitored. By default, data is collected every 5 minutes and is stored in the database. During initial posture, the agent reports a complete list of running and installed applications. After initial posture, the agent scans the applications every X minute and sends the differences from the last scan to the server. The server displays the complete list of running and installed applications.

Application Condition Settings

The application condition queries for applications that are installed on an endpoint. This helps you to get an aggregate visibility of the software distributed on your endpoints.

The following table describes the fields in the **Application Conditions** window. To view this window, click the **Menu** icon (☰) and choose **Work Centers** > **Posture** > **Policy Elements** > **Application Condition** > **Add**.

Field Name	Usage Guidelines
Name	Enter the name of the application condition.
Description	Enter the description for the application condition.
Operating System	Select the operating system to which the application condition should be applied. options are available: • **Windows** • **Mac OSX** • **Linux**
Compliance Module	Choose one of the following options: • **4.x or later** • **3.x or earlier** • **Any Version**
Check By	Choose one of the following options: • **Process**: Choose this option to check if a process is running on an endpoint • **Application**: Choose this option to check if an application is running on an **Note** Only the **Process** option is displayed for Linux OS.

Field Name	Usage Guidelines
Process Name	(Available only when you select **Process** as the **Check By** option) Enter the required name.
Application Operator	(Available only when you select **Process** as the **Check By** option) Choose one of the options: • **Running**: Choose this option to check if an application is running on an endpo • **Not Running**: Choose this option to check whether an application is not runnir endpoint.
Application State	(Available only when you select **Application** as the **Check By** option) Choose one o following options: • **Installed**: Choose this option to check whether the clients have malicious appli installed. If a malicious application is found, the remediation action is triggered • **Running**: Choose this option to check if an application is running on an endpo
Provision By	(Available only when you select **Application** as the **Check By** option) Choose one o following options: • **Everything**: You can select all listed categories such as Browser, Patch Manage so on. • **Name**: You should select at least one category. For example, if you choose the category, it displays the corresponding vendors in the **Vendor** drop-down list. • **Category**: You can check one or more categories such as Anti-Malware, Backup or Data Storage. **Note** Categories are dynamically updated from the OPSWAT library.

You can view the number of installed and running applications for each endpoint in the **Context Visibility** > **Endpoints** > **Compliance** window.

The **Home** > **Summary** > **Compliance** window displays the percentage of endpoints that are subject to posture assessment and are compliant.

Service Condition Settings

The following table describes the fields in the **Service Conditions** window. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Conditions** > **Posture** > **Service Condition**.

Table 8: Service Conditions Settings

Field Name	Usage Guidelines
Name	Enter a name for the service condition.
Description	Enter a description of the service condition.

Field Name	Usage Guidelines
Operating Systems	Select the operating system to which the service condition should be applied. You can select different versions of the Windows OS or macOS.
Service Name	Enter the name of the Daemon or User Agent service, for example, com.apple.geod, running as root. The agent uses the command **sudo launchctl list** to validate the service condition.
Service Type	Choose the type of service that agent should check for to ensure client compliance: • **Daemon**: Checks if a specified service, such as scanning a client device for malware, is present in the specified list of Daemon services in the client. • **User Agent**: Checks if a specified service, such as a service that runs when malware is detected, is present in the specified list of User services in the client. • **Daemon or User Agent**: Checks if the specified services are present either in the Daemon or User Agent services list.
Service Operator	Choose the service status that you want to check in the client: • **Windows OS**: To check if a service is **Running** or **Not Running**. • **Mac OSX**: To check if a service is **Loaded**, **Not Loaded**, **Loaded and Running**, **Loaded with Exit Code**, and **Loaded and running or with Exit code**.

Related Topics

Simple Posture Conditions, on page 19
Compound Posture Conditions, on page 20

Posture Compound Condition Settings

The following table describes the fields in the **Compound Conditions** window. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Conditions** > **Posture** > **Compound Condition**.

Table 9: Posture Compound Condition Settings

Field Name	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 allows 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**.

Field Name	Usage Guidelines
(|): 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.

Related Topics

Posture Conditions, on page 19
Create Compound Posture Conditions, on page 21

AntiVirus Condition Settings

In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Conditions** > **Posture** > **Anti-Virus Condition**.

Field Name	Usage Guidelines
Name	Enter the name of the antivirus condition that you want to create.
Description	Enter the description of the antivirus condition that you want to create.
Operating System	Select an operating system to check the installation of an antivirus program 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.

Products for Selected Vendor

Choose an antivirus product from the table. Based on the vendor that you select in the New Anti-virus 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.

Note Only one condition can be configured for each antivirus product from either **Baseline Condition** or **Advance Condition**.

Baseline Condition

Field Name	Guideline
Minimum Version	(Available only when you update the Operating System and Vendor) Choose minimum version of the antivirus from the drop down list. The check will enforce the network policy on all the endpoints on your network to comply with the mimimum version of antivirus.
Maximum Version	The maximum version for antivirus is revised automatically when you update the posture feed.
Minimum Compliance Module Version	The minimum compliance module version is updated from the agent.

Advance Condition

Field Name	Guidelines
Check against latest AV definition file version, if available	(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.

Field Name	Guidelines
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.

Related Topics

Compound Posture Conditions, on page 20
Preconfigured Antivirus and Antispyware Conditions, on page 23
Antivirus and Antispyware Support Chart, on page 23

Antispyware Compound Condition Settings

The following table describes the fields in the **AS Compound Conditions** window. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Conditions** > **AS Compound Condition**.

Table 10: Antispyware Compound Condition Settings

Field Name	Usage Guidelines
Name	Enter the name of the antispyware compound condition that you want to create.

Field Name	Usage Guidelines
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 program 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).
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.

Related Topics

Compound Posture Conditions, on page 20
Preconfigured Antivirus and Antispyware Conditions, on page 23
Antivirus and Antispyware Support Chart, on page 23

Antimalware Condition Settings

The antimalware condition is a combination of the antispyware and antivirus conditions and is supported by OESIS version 4.x or later compliance module.

To view this window, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Conditions** > **Posture** > **Antimalware Condition**.

Note It is recommended that you manually update the installed Antimalware products to have the latest definitions at least once. Otherwise, the posture checks using agent for Antimalware definitions might fail.

Field Name	Usage Guidelines
Name	Enter a name for the antimalware condition.
Description	Enter a description for the antimalware condition.
Operating System	Choose an operating system to check the installation of antimalware programs on your client, or check the latest antimalware definition file updates to which the condition is applied. It supports Windows, macOS, and Linux operating systems.
Vendor	Choose a vendor from the drop-down list. The selected vendor's antimalware products, versions, latest definition dates, latest definition versions, and minimum compliance module versions are displayed in the **Products for Selected Vendor** table.
Check Type	Choose one of the following options: • **Installation**: Choose this option to check only the installation of an antimalware program on the client. • **Definition**: Choose this option to check only the latest definition file update of an antimalware product on the client.
Check Against Latest AV Definition File Version, if Available	(Available only when you choose **Definition** check type) Choose this option to check the antimalware definition file version on the client against the latest antimalware 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. This check will only work if there is a value listed in Cisco ISE for the **Latest Definition Date** or **Latest Definition Version** field for the selected product. Otherwise, the **Current System Date** field must be used.
Allow Virus Definition File to be	(Available only when you choose **Definition** check type) Choose this option to check the antimalware definition file version and the latest antimalware definition file date on the client. The latest definition file date cannot be older than that you define in the **Days Older Than** field. If unchecked, Cisco ISE allows you to check only the version of the antimalware definition file using the **Check against latest AV definition file version** option.

Field Name	Usage Guidelines
Days Older Than	Define the number of days that the latest antimalware definition file date on the client can be older than the latest antimalware definition file date of the product or the current system date. The default value is zero.
Latest File Date	Choose this option to define the number of days that the latest antimalware definition file date on the client can be older than the latest antimalware definition file date of the product. If you set the number of days to the default value, then the antimalware definition file date on the client should not be older than the latest antimalware definition file date of the product. This check works only if there is a value listed in Cisco ISE for the **Latest Definition Date** field for the selected product. Otherwise, the **Current System Date** field must be used.
Current System Date	Choose this option to define the number of days that the latest antimalware definition file date on the client can be older than the current system date. If you set the number of days to the default value, then the antimalware definition file date on the client should not be older than the current system date.

For an antimalware condition for Carbon Black Cloud 3.x on Mac OS to be successful, the condition must meet the following requirements:

- The compliance module must be greater than 4.3.2741.
- The condition must be associated with the vendor VMware, Inc.

When you upgrade from one Cisco ISE release to another with a preconfigured Carbon Black Cloud 3.x condition, after a posture feed update, two Carbon Black Cloud 3.x conditions are listed in the **Advanced Conditions** area of the **Anti-Malware Condition** windows.

You must delete the Carbon Black Cloud 3.x condition associated with the vendor Carbon Black, Inc. You must reconfigure any existing antimalware conditions that use the Carbon Black Cloud 3.x from Carbon Black, Inc. to use the condition from the vendor VMware, Inc.

Related Topics

Compound Posture Conditions, on page 20

Dictionary Simple Condition Settings

The following table describes the fields in the **Dictionary Simple Conditions** window. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Conditions** > **Posture** > **Dictionary Simple Condition**.

Table 11: Dictionary Simple Condition Settings

Field Name	Usage Guidelines
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.

Field Name	Usage Guidelines
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.

Related Topics

Simple Posture Conditions, on page 19
Create Simple Posture Conditions, on page 20

Dictionary Compound Condition Settings

Table 12: Dictionary Compound Condition Settings

Field Name	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.

Field Name	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 Cisco ISE will process each OR condition in a compound condition sequentially. For example, if a compound condition checks for A OR B, Cisco ISE first checks A and then B. If either condition A or B is passed, the overall result is marked as passed. If condition A fails and condition B succeeds, then the overall result is marked as passed. In this case, condition A is marked as failed and condition B as passed in the posture reports. If condition A succeeds, Cisco ISE skips condition B and marks the overall result as passed. In the posture reports, condition A is marked as passed, condition B as skipped, and the overall result as passed.
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

Compound Posture Conditions, on page 20
Create Compound Posture Conditions, on page 21

Patch Management Condition Settings

The following table describes the fields in the **Patch Management Conditions** window. To view this window, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Conditions** > **Posture** > **Patch Management Condition**.

Table 13: Patch Management Condition

Field Name	Usage Guidelines
Name	Enter the name of the patch management condition.

Field Name	Usage Guidelines
Description	Enter a description for the patch management condition.
Operating System	Choose 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 Windows, macOS, or Linux OS. You can also select more than one version of an operating system to create the patch management condition.
Vendor Name	Choose a vendor from the **Vendor Name** drop-down list. Based on your selection, the patch management products and their supported versions, check type, and minimum compliant module support details are displayed in the **Products for Selected Vendor** table. The list in the table changes according to the selected operating system.
Check Type	Choose 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. **Note** For the Cisco Temporal Agent, you can only view the Patch Management conditions containing the **Installation** check type in the **Requirements** window. • **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 list to view the list of products that the vendor you have specified in the **Vendor Name** field 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.
Check Patches Installed	(Available only when you select the **Up To Date** check type) You can configure severity levels for missing patches, which are then deployed based on the severity. Choose one of the following options: • **Critical Only**: To check if critical software patches are installed on the endpoints in your deployment. • **Important and Critical**: To check if important and critical software patches are installed on the endpoints in your deployment. • **Moderate, Important, and Critical**: To check if moderate, important, and critical software patches are installed on the endpoints in your deployment. • **Low To Critical**: To check if low, moderate, important, and critical software patches are installed on the endpoints in your deployment. • **All**: To install the missing patches for all severity levels.

Related Topics

Create Patch Management Conditions, on page 25

Disk Encryption Condition Settings

The following table describes the fields in the **Disk Encryption Condition** window. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Conditions** > **Posture** > **Disk Encryption Condition**.

Table 14: Disk Encryption Condition Settings

Field Name	Usage Guidelines
Name	Enter the name of the disk encryption condition that you want to create.
Description	Enter a description for the disk encryption condition.
Operating System	Select an operating system of the end point, whose disk is to be checked for encryption. You can select the Windows OS or macOS. You can also select more than one version of an operating system to create the disk encryption condition.
Vendor Name	Choose a vendor name from the drop-down list. The data encryption products of a vendor, and their supported version, the encryption state check, and the minimum compliant module support are retrieved and displayed in the **Products for Selected Vendor** table. The list in the table changes according to the selected operating system.

Location	Enabled only when an option is checked in the **Products for Selected Vendor** section. Select any one of the following options:
	• **Specific Location**: To check if the specified disk drive is encrypted in the end point, (for example, C: for Windows OS) or a specified volume label is encrypted, (for example, Mackintosh HD for macOS).
	• **System Location**: To check if the default Windows OS system drive or macOS hard drive is encrypted in the end point.
	• **All Internal Drives**: To check the internal drives. Includes all hard disks that are mounted and encrypted, and all internal partitions. Excludes read only drives, system recovery disk/partition, boot partition, network partitions, and the different physical disk drives that are external to the endpoint (including but not limited to disk drives connected via USB and Thunderbolt). Encryption software products that are validated include:
	  • Bit-locker-6.*x*/10.*x*
	  • Checkpoint 80.*x* on Windows 7

Field Name	Usage Guidelines
Encryption State	The Encryption State checkbox is disabled when the selected product does not support encryption state check. The repeater is displayed only when the checkbox is checked. You can select the Fully Encrypted option to check if the client's disk drive is wholly encrypted. If you create a condition, for example for TrendMicro, and select two vendors—one with the Encryption State "Yes" and another with the Encryption State "No", then the Encryption State will be disabled because one of the Vendor Encryption States is "No". **Note** You can click the repeater to add more Locations and the relationship between each location is the logical AND operator.

Related Topics

Create Disk Encryption Conditions, on page 25

USB Condition Settings

The following table describes the fields in the **USB Condition** window. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Posture** > **Policy Elements** > **USB**. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Conditions** > **Posture** > **USB Condition**

The USB check is a predefined condition and supports only Windows OS.

Table 15: USB Condition Settings

Field Name	Usage Guidelines
Name	USB_Check
Description	Cisco predefined check
Operating System	Windows
Compliance Module	A display-only field for ISE posture compliance module support for version 4.x (and later).

Related Topics

Simple Posture Conditions, on page 19

Hardware Attributes Condition Settings

In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Hardware Attributes Condition** to access the **Hardware Attributes Condition** window. The following table describes the fields in the **Hardware Attributes Condition** window.

Field Name	Usage Guidelines
Name	Hardware_Attributes_Check: The default name assigned to the condition.
Description	Cisco predefined check that collects hardware attributes from clients.

Field Name	Usage Guidelines
Operating System	Windows All or Mac OS
Compliance Module	4.x or later

Posture External DataSource Condition

You can configure conditions to match an endpoints UDID with an external datasource. Currently, only Active Directory is supported. The scripts required on the posture agent to send UDID to Active Directory are not included with ISE.

Add a Script Condition

You can create and upload a posture condition script to check the compliance status of an endpoint. Here is a sample Linux script that checks whether a file exists or not:

```
#!/bin/bash
TESTFILE=/tmp/sample.log
if [ -f $TESTFILE ]
then
    echo "Success: File $TESTFILE exist."
    exit 0
else
    echo "Failed: File $TESTFILE does not exist."
    exit 1
fi
```

The following platforms and script types are supported:

Platform	Supported Script Type
Windows	PowerShell script (.ps1)
macOS	Shell script (.sh)
Linux	Shell script (.sh)

Before you begin

- Establish trust to execute the scripts on endpoints. For more information, see Establish Trust to Execute Script Condition, on page 50.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy > Policy Elements > Conditions > Posture > Script**.

Step 2 Click **Add**.

Step 3 Enter the name and description of the script.

Step 4 From the **Operating System** drop-down list, choose the required operating system.

If you choose the Windows operating system, the **Script Type** and **Windows PowerShell Execution Policy** fields are displayed.

Choose one of the following options for **Script Type**:

- **PowerShell**
- **PowerShell Core**

Note The **Script Type** is set as **Shell Script** for macOS and Linux operating systems by default.

Choose one of the following options for **Windows PowerShell Execution Policy**:

- **Bypass**: The script doesn't require any digital signatures to execute, even if the other policies that are configured on the endpoint mandate digital signatures or signed PowerShell scripts.
- **AllSigned**: The script must be digitally signed to execute, even if the other policies configured on the endpoint do not mandate digital signatures.
- **None**: The script is executed according to the existing script execution policies in the endpoint. Cisco ISE doesn't define the execution policy of the script.

If you choose the **AllSigned** option to run a signed Powershell script, ensure that the root certificate is placed in the Trusted Root Certificate Authorities store of the endpoint. The certificate used to sign the script must be placed under the Trusted Publisher store, and the intermediate certificates must be placed in the Intermediate Certificate Authorities store. **AllSigned** requires your script to be signed by a trusted publisher. Having *only* the root certificate in the Trusted Root Certificate Authorities store is not enough.

Step 5 Click **Choose File** and select the script that you want to upload from your local system.

Step 6 In the **Timeout** field, enter the timeout duration, in seconds, for the script.

The valid range is from 1 to 60 seconds.

If the script run time exceeds the configured timeout duration, the agent stops the script and marks the condition based on the option selected in the **Script Condition Execution Failure or Timeout** field.

Step 7 Under **Script Condition Execution Failure or Timeout**, specify what happens to a condition if the script does not exit before the configured timeout, or if the script execution fails.

- If you choose **Pass**, the condition is marked as met.
- If you choose **Fail**, the condition is marked as not met.

Step 8 To run the script as an administrator, click the **Administrator/Root** radio button. To run the script as a logged-in user, click the **Logged-in User** radio button.

Note Agentless posture workflows use Administrator privilege, and temporal agents use Logged-in user privilege, regardless of the user privilege that you choose for the script.

Step 9 Click **Submit**.

Establish Trust to Execute Script Condition

You must establish trust to be able to execute the scripts on endpoints and make sure that the Cisco ISE server is not compromised. A Cisco ISE environment can have one or more PSNs configured. Every PSN has a valid

certificate chain. The certificate chain starts with any certificate, followed by an intermediate certificate or a root CA certificate. You can use any certificate in the certificate chain for fingerprint verification.

You can configure the SHA-256 fingerprint of any certificate in the certificate chain in the AnyConnectLocalPolicy's profile editor. For example, the following command generates the SHA-256 fingerprint of a certificate with the name input.cer:

```
openssl x509 -inform DER -in <input.cer> -out <output.crt>
openssl x509 -in <output.crt> -fingerprint -noout -sha256
```

The following is an example of the output:

```
openssl x509 -in 535-pos.crt -fingerprint -noout -sha256
SHA256
Fingerprint=B9:42:7F:85:09:18:30:40:06:0B:DB:9C:48:36:F0:60:90:75:AB:D3:E9:83:AB:1A:BF:01:8F:6E:F0:11:9A:B5
```

The following example shows the new tag in AnyConnectLocalPolicy.xml:

```
<TrustedISECertFingerprints>
<fingerprint>
<algorithm>SHA-256</algorithm>
<hash>B9:42:7F:85:09:18:30:40:06:0B:DB:9C:48:36:F0:60:90:75:AB:D3:E9:83:AB:1A:BF:01:8F:6E:F0:11:9A:B5</hash>
</fingerprint>
</TrustedISECertFingerprints>
```

Note An SHA-256 fingerprint can be added with or without a colon. You can add the fingerprint in either of the following formats: `B9:42:7F:85:09:18:30:40:06:0B:DB:9C:48:36:F0:60:90:75:AB:D3:E9:83:AB:1A:BF:01:8F:6E:F0:11:9A:B5` or `B9427F8509183040060BDB9C4836F0609075ABD3E983AB1ABF018F6EF0119AB5`. Fingerprints are not case-sensitive.

The agent matches the Cisco ISE certificate fingerprint with the trusted certificate fingerprint (present in AnyConnectLocalPolicy.xml) while fetching the script. If an endpoint does not have a valid certificate fingerprint, the script is not executed on the endpoint.

Note If fingerprints are configured in AnyConnectLocalPolicy.xml, they are used to validate Cisco ISE trust for all flows. If the certificate is not trusted or if there is a fingerprint mismatch, no error messages are displayed. However, the following error message is included in the **Posture Script Condition** report (**Operations > Reports > Endpoints and Users**):

```
Condition Script certificate verification failed. Client could not verify the server
certificate presented by Cisco ISE.
```

Script Exit Code

The script should have explicit exit codes to determine whether a condition passed or failed. If the script exits with zero, the condition is marked as passed. If the exit code is greater than zero, the condition is marked as failed.

If there are any failures before script execution (such as failure to download the script or hash verification error), the condition is marked as failed.

If the script fails to exit within the configured timeout, the script is terminated and the exit code is set appropriately.

In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations > Reports > Endpoints and Users > Posture Script Condition** to check the status of script execution.

One of the following statuses is displayed:

- 0 – Condition script execution was successful.
- > 0 – Condition script was executed and the script exited with failure code.
- -1 – Condition script was not attempted.
- -2 – Condition script was not executed. The policy failed an integrity check.
- -3 – Condition script was not executed. Client failed to download the script.
- -4 – Condition script was not executed. The script failed an integrity check.
- -5 – Condition script failed. The script was executed but did not exit in time (timeout).
- -6 – Condition script failed. A generic internal system failure occurred.
- -7 – Condition script was not executed. The script type is not supported.
- -8 – Condition script failed. Failed to launch the script.
- -9 – Condition script certificate verification failed. Client could not verify the server certificate presented by Cisco ISE.

Script Download

The posture agent downloads the script from the HTTPS URL included in the posture policy. The script is downloaded only if the following conditions are met:

- Trusted certificate fingerprint must be present in AnyConnectLocalPolicy.xml.
- The fingerprint presented by the HTTPS URL should match the trusted certificate fingerprint present in AnyConnectLocalPolicy.xml.

Note

- Fingerprint verification is not done for temporal agent and agentless posture flows.
- Policy integrity check is bypassed for temporal agent and agentless posture flows.

Configure Posture Policies

A posture policy is a collection of posture requirements that are associated with one or more identity groups and operating systems. The Dictionary Attributes are optional conditions that can be used along with the identity groups and the operating systems to define different policies for the devices.

Cisco ISE provides an option to configure the grace time for the devices that are noncompliant. If a device is found to be noncompliant, Cisco ISE looks for the previously known good state in the posture assessment result cache and provides grace time for the device accordingly. The device is granted access to the network during the grace period. You can configure the grace time period in minutes, hours, or days (up to a maximum of 30 days).

See the section "Posture Policy" in ISE Posture Prescriptive Deployment Guide for more information.

Note Profiler policy evaluation will not work if both 'Endpoint policies' and 'Logical Profiles' are configured under Other Conditions in **Policy** > **Posture**.

Note

- When the grace period is extended or reduced, if the device goes through the posture flow again (for example, if the **Delayed Notification** option is enabled, **Re-Scan** option is selected, device disconnects or reconnects to a network), the new grace period and delayed notification will be applied.
- Grace period is not applicable for the temporal agent.
- Grace period is not supported for Linux agent.
- When a device matches multiple posture policies, with each policy having a different grace period, the device gets the maximum grace period configured among the different policies.
- The Acceptable Use Policy (AUP) is not displayed when the device is in the grace period.

Before you begin

- You must understand the Acceptable Use Policy (AUP).
- You must understand periodic reassessments (PRA).

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Posture** or **Work Centers** > **Posture** > **Posture Policy**.

Step 2 Use the drop-down arrow to add a new policy.

Step 3 To edit the profile, either double-click a policy or click Edit at the end of the row.

Step 4 From the **Rule Status** drop-down list, choose **Enabled** or **Disabled**.

Step 5 Choose the drop-down under **Policy Options**, and specify the **Grace Period Settings** in minutes, hours, or days.

The valid values are:

- 1 to 90 days
- 1 to 2,160 hours
- 1 to 129,600 minutes

By default, this setting is disabled.

Note Even if the posture assessment result is noncompliant, if the device is found to be previously compliant and the cache is not yet expired, the device is granted access for the amount of time specified in the **Grace Period Settings**.

Step 6 (Optional) Drag the slider named **Delayed Notification** to delay the grace period prompt from being displayed to the user until a specific percentage of grace period has elapsed. For example, if the notification delay period is set to 50% and the configured grace period is 10 minutes, Cisco ISE checks the posture status after 5 minutes and displays the grace period notification if the endpoint is found to be noncompliant. Grace period notification is not displayed if the endpoint status is compliant. If the notification delay period is set to 0%, the user is prompted immediately at the beginning of the grace period to remediate the problem. However, the endpoint is granted access until the grace period expires. The default value for this field is 0%. The valid range is from 0 to 95%.

Step 7 In the **Rule Name** field, enter the name of the policy.

Note It is a best practice to configure a posture policy with each requirement as a separate rule in order to avoid unexpected results.

Step 8 From the **Identity Groups** column, select the desired identity group.

You can create posture policies based on user or end-point identity groups.

Step 9 From the **Operating Systems** column, select the operating system.

Step 10 From the **Compliance Module** column, select the required compliance module:

- **4.x or Later**: Supports antimalware, disk encryption, patch management, and USB conditions.
- **3.x or Earlier**: Supports antivirus, antispyware, disk encryption, and patch management conditions
- **Any Version**—: upports file, service, registry, application, and compound conditions.

Step 11 From the **Posture Type** column, select the Posture Type.

- **Agent**—Deploys the agent to monitor and enforce Cisco ISE policies that require client interaction.
- **Agent Stealth**—Deploys the agent to monitor and enforce Cisco ISE posture policies without any client interaction.
- **Temporal Agent**—A temporary executable file that is run on the client to check the compliance status.

Step 12 In **Other Conditions**, you can add one or more dictionary attributes and save them as simple or compound conditions to a dictionary.

Note The dictionary simple conditions and compound conditions that you create in the **Posture Policy** window are not displayed while configuring an authorization policy.

Step 13 Specify the requirements in the **Requirements** field.

Step 14 Click **Save**.

Configure Agent Workflow

To configure the agent, perform the following steps in Cisco ISE:

Before you begin

In the following Cisco ISE releases, the bug CSCvs39880 results in garbage collection processes that impacted memory space and file replication from a primary PSN to secondary PSNs. Because of this bug, in the following Cisco ISE releases, uploading an agent package in a large Cisco ISE deployment can take about 7 hours and about 40 minutes in a small deployment.

The following are the affected Cisco ISE releases:

3.2 FCS release

3.1 Patch 4 and earlier

3.0 Patch 6 and earlier

2.7 Patch 7 and earlier

In the later Cisco ISE releases, this bug has been fixed resulting in an agent package upload time of about 5 minutes.

Step 1 Create an agent profile.

Step 2 Create agent configuration for agent packages.

Step 3 Create a client provisioning policy.

Step 4 (Optional) Create custom posture condition.

Step 5 (Optional) Create custom remediation action.

Step 6 (Optional) Create custom posture requirements.

Step 7 Create a posture policy.

Step 8 Configure the client provisioning policy.

Step 9 Create an authorization profile.

Step 10 Configure the authorization policies.

Step 11 Download and launch agent.

a) Connect to the SSID.
b) Launch a Browser and you will be redirected to the Client Provisioning Portal.
c) Click **Start**. This checks if the agent is installed and running.
d) Click **This Is My First Time Here**.
e) Choose **Click Here to Download and Launch Agent**.
f) Save the agent .exe or .dmg file for Windows or macOS respectively. For Windows, run the .exe file and for macOS, double-click the .dmg file and run the app.

Note Note the following points if you are using ARM64 version of agent:

- If ARM64 agent package is pre-deployed on ARM64 endpoint:
  - Posture flow works.
  - Agent auto upgrade will not work. This is because ISE does not support uploading ARM64 package and does not support Client Provisioning policy for provisioning ARM64 package.

    If you configure a higher agent version (x86) in the Client Provisioning policy, ARM64 endpoint will try to upgrade to that version and the subsequent posture flow will fail.
- You cannot provision ARM64 package from ISE because ISE does not support uploading ARM64 package and does not support Client Provisioning policy for provisioning ARM64 package.

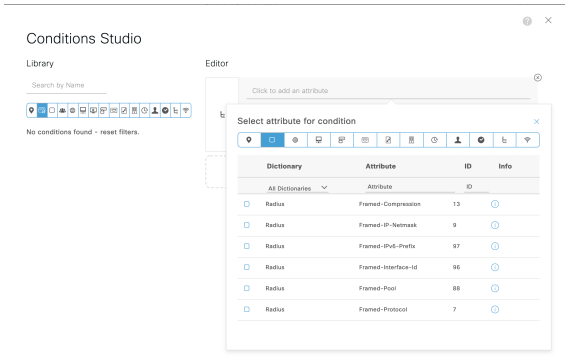
Prerequisite for Certificate-Based Conditions

Client Provisioning and Posture Policy rules may include conditions based on certificate attributes. A prerequisite for certificate-based conditions in either the Client Provisioning or Posture Policy is to ensure that there is s a matching Authorization Policy rule based on the same certificate attribute.

For example, you should use the same attribute as shown in the figures, the Issuer – Common Name attribute is used in both Client Provisioning or posture and authorization policies.

Figure 1: Cisco Provisioning Policy

Figure 2: Conditions Studio



Note ISE server certificate must be trusted in the System Certificate store for AnyConnect 4.6 MR2 and above. Any posture check or remediation that requires elevated privileges will not work if the server is untrusted.

- Windows OS: The server certificate must be added to the System Certificate store.
- MAC OS: The server certificate must be added to the System Keychain. It is recommended that you use the command-line utility to trust the certificate. Adding the certificate to the System Keychain using the Keychain Access app might not work if it is already present in the Login Keychain.

Default Posture Policies

The Cisco ISE software comes with a number of pre-configured posture policies that make it easier for you to create the posture policies and profiles. These policies are disabled by default. You can enable these policies based on your requirements. Following are some of the default posture policies.

Rule Name	Description	Requirements
Default_Antimalware_Policy_Mac	Checks if endpoints have any of the supported vendor's antimalware software (that is recognized by agent) installed and running in their devices.	Any_AM_Installation
Default_Antimalware_Policy_Win	Checks if endpoints have any of the supported vendor's antimalware software (that is recognized by agent) installed and running in their devices.	Any_AM_Installation_Win
Default_AppVis_Policy_Mac	Gathers information and reports all the applications that are installed on a given endpoint.	Default_AppVis_Requirement_Mac

Rule Name	Description	Requirements
Default_AppVis_Policy_Win	Gathers information and reports all the applications that are installed on a given endpoint.	Default_AppVis_Requirement_Win
Default_Firewall_Policy_Mac	Checks if endpoints have any of the supported vendor's Firewall program (that is recognized by agent) installed.	Default_Firewall_Requirement_Mac
Default_Firewall_Policy_Win	Checks if endpoints have any of the supported vendor's Firewall program (that is recognized by agent) installed.	Default_Firewall_Requirement_Win
Default_USB_Block_Win	Ensures that the endpoint device does not have any USB storage devices connected.	USB_Block

Client Posture Assessment

To ensure that the imposed network security measures remain relevant and effective, Cisco ISE enables you to validate and maintain security capabilities on any client machine that accesses the protected network. By employing posture policies that are designed to ensure that up-to-date security settings or applications are available on client machines, the Cisco ISE administrator can ensure that any client machine that accesses the network meets, and continues to meet, the defined security standards for enterprise network access. Posture compliance reports provide Cisco ISE with a snapshot of the compliance level of the client machine at the time of user login, as well as any time a periodic reassessment occurs.

Posture Assessment Options

The following table provides a list of posture assessment (posture conditions) options that are supported by the Cisco ISE Posture Agents for Windows and MacOS, and the Web Agent for Windows.

Table 16: Posture Assessment Options

ISE Posture Agent for Windows	Cisco Temporal Agent for Windows	ISE Posture Agent for MacOS	Cisco Temporal Agent for MacOS
Operating System/Service Packs/Hotfixes	—	—	—
Service Check	Service Check (Temporal agent 4.5)	Service Check	Daemon checks are not supported
Registry Check	Registry Check (Temporal agent 4.5)	—	—

ISE Posture Agent for Windows	Cisco Temporal Agent for Windows	ISE Posture Agent for MacOS	Cisco Temporal Agent for MacOS
File Check	File Check (Temporal agent 4.5)	File Check	File Check (Temporal agent 4.5)
Application Check	Application Check (Temporal agent 4.5)	Application Check	Application Check (Temporal agent 4.5)
Antivirus Installation	Antimalware Installation	Antivirus Installation	Antimalware Installation
Antivirus Version/ Antivirus Definition Date	OPSWAT version 4 is used, hence no Antivirus/Antispyware support; only Antimalware is supported	Antivirus Version/ Antivirus Definition Date	OPSWAT version 4 is used, hence no Antivirus/Antispyware support; only Antimalware is supported
Antispyware Installation	OPSWAT version 4 is used, hence no Antivirus/Antispyware support; only Antimalware is supported	Antispyware Installation	OPSWAT version 4 is used, hence no Antivirus/Antispyware support; only Antimalware is supported
Antispyware Version/ Antispyware Definition Date	OPSWAT version 4 is used, hence no Antivirus/Antispyware support; only Antimalware is supported	Antispyware Version/ Antispyware Definition Date	OPSWAT version 4 is used, hence no Antivirus/Antispyware support; only Antimalware is supported
Patch Management Check	Only Patch Management installation check	Patch Management Check	—
Windows Update Running	—	—	—
Windows Update Configuration	—	—	—
WSUS Compliance Settings	—	—	—

Posture Remediation Options

The following table provides a list of posture remediation options that are supported by the Cisco ISE Posture Agents for Windows and MacOS, and the Web Agent for Windows.

Table 17: Posture Remediation Options

ISE Posture Agent for Windows	ISE Posture Agent for MacOS
Message Text (Local Check)	Message Text (Local Check)

ISE Posture Agent for Windows	ISE Posture Agent for MacOS
URL Link (Link Distribution)	URL Link (Link Distribution)
File Distribution	—
Launch Program	—
Antivirus Definition Update	Antivirus Live Update
Antispyware Definition Update	Antispyware Live Update
Patch Management Remediation	—
Windows Update	—
WSUS	—

ISE Community Resource

Cisco ISE and SCCM Integration Workflow

Custom Conditions for Posture

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

After an initial posture update, Cisco ISE also creates Cisco-defined simple and compound conditions. Cisco-defined simple conditions use the pc_ as and compound conditions use pr_ as.

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

Posture service makes use of internal checks based on antivirus and antispyware (AV/AS) compound conditions. Hence, posture reports do not reflect the exact AV/AS compound-condition names that you have created. The reports display only the internal check names of AV/AS compound conditions.

For example, if you have created an AV compound condition named "MyCondition_AV_Check" to check any Vendor and any Product, the posture reports will display the internal check, that is “av_def_ANY”, as the condition name, instead of "MyCondition_AV_Check".

Posture Endpoint Custom Attributes

You can use the posture endpoint custom attributes to create client provisioning and posture policies. You can create a maximum of 100 endpoint custom attributes. The following types of endpoint custom attributes are supported: Int, String, Long, Boolean, Float, IP, and Date.

Endpoint custom attributes can be used to allow or block devices based on certain attributes or to assign certain privileges based on the posture or client provisioning policies.

Create Posture Policy Using Endpoint Custom Attributes

To create a posture policy using endpoint custom attributes:

Step 1 Create the endpoint custom attributes.

a) In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Identity Management** > **Settings** > **Endpoint Custom Attributes**.

b) Enter the **Attribute Name** (for example, deviceType) and Data Type (for example, String) in the **Endpoint Custom Attributes** area.

c) Click **Save**.

Step 2 Assign values to the custom attributes.

a) In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Context Visibility** > **Endpoints**.

b) Assign the custom attribute values.

- Check the required MAC address check box, and then click **Edit**.
- Or, click the required MAC address, and then click **Edit** in the **Endpoints** page.

c) Ensure that the custom attribute that you created is displayed in the **Custom Attributes** area in the **Edit Endpoint** dialog box.

d) Click **Edit** and enter the required attribute value (for example, deviceType = Apple-iPhone).

e) Click **Save**.

Step 3 Create a posture policy using the custom attributes and values.

a) In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Posture** > **Posture Policy**.

b) Create the required policy. Choose the custom attributes by clicking **Other Conditions** and select the required dictionary (for example, choose Endpoints > deviceType, the custom attribute that you created in Step 1). For more information, see the Configure Cisco Temporal Agent Workflow, on page 79 .

c) Click **Save**.

To create a client provisioning policy using endpoint custom attributes:

1. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Posture** > **Client Provisioning** > **Client Provisioning Policy**.
2. Create the required policy.
   - Create the required rule (for example, Rule Name=WindowsAll, if Identity Groups=Any and Operating Systems=Windows All and Other Conditions=Conditions, then Results=AC_Win_44117).
   - Choose the custom attributes by clicking **Other Conditions** and selecting the required dictionary.

Custom Posture Remediation Actions

A custom posture remediation action is a file, a link, an antivirus or antispyware definition updates, launching programs, Windows updates, or Windows Server Update Services (WSUS) remediation types.

Add an Antispyware Remediation

You can create an antispyware remediation, which updates clients with up-to-date file definitions for compliance after remediation.

The AS Remediations window displays all the antivirus remediations along with their name and description and their modes of remediation.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > **Posture**.
Step 2 Click **Remediation Actions**.
Step 3 Click **AS Remediation**.
Step 4 Click **Add**.
Step 5 Modify the values in the **New AS Remediations** window.
Step 6 Click **Submit**.

Add an Antivirus Remediation

You can create an antivirus remediation, which updates clients with up-to-date file definitions for compliance after remediation.

The AV Remediations window displays all the antivirus remediations along with their name and description and their modes of remediation.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > **Posture**.
Step 2 Click **Remediation Actions**.
Step 3 Click **AV Remediation**.
Step 4 Click **Add**.
Step 5 Modify the values in the **New AV Remediation** window.
Step 6 Click **Submit**.

Add a File Remediation

A file remediation allows clients to download the required file version for compliance. The client agent remediates an endpoint with a file that is required by the client for compliance.

You can filter, view, add, or delete file remediations in the File Remediations window, but you cannot edit file remediations. The File Remediations window displays all the file remediations along with their name and description and the files that are required for remediation.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > **Posture**.

Step 2 Click **Remediation Actions**.

Step 3 Click **File Remediation**.

Step 4 Click **Add**.

Step 5 Enter the name and description of the file remediation in the **Name** and **Description** fields.

Step 6 Modify the values in the **New File Remediation** window.

Step 7 Click **Submit**.

Add a Script Remediation

You can create and upload posture remediation scripts into Cisco ISE to solve non-compliance issues in endpoints.

Before you begin

- Establish trust to fetch posture policies. For more information, see Establish Trust to Execute Script Condition, on page 50
- Download the script. For more information, see Script Download, on page 66

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > **Posture**.

Step 2 Click **Remediation Actions**.

Step 3 Click **Script Remediations**.

Step 4 Click **Add**.

Step 5 Enter the **Name** and **Description** of the script.

Step 6 Choose the **Operating System** and **Remediation Type** from the corresponding drop-down lists.

If you choose the **Windows** operating system, the **Script Type** and **Windows PowerShell Execution policy** fields are displayed. Choose the required script type and execution policy by clicking the corresponding radio buttons.

Step 7 From the **Remediation Type** drop-down list, choose **Automatic** or **Manual**.

Note
- Only automatic remediation is supported for Linux agent. Manual remediation is not supported.
- Only shell scripts are supported for Linux agent.

Step 8 Enter the **Interval** and **Retry Count**. The valid range is 0 to 999.

Step 9 Click **Choose File**, next to **File To Upload** and select the script that you want to upload from your local system.

Step 10 To run the script as an administrator, click the **Administrator/ Root** radio button. To run the script as a logged-in user, click the **Logged-in User** radio button.

Step 11 Click **Submit**.

Step 12 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations** > **Reports** > **Endpoints and Users** > **Posture Script Remediation** to check the status of the remediation script execution.

One of the following statuses is displayed: :

- Remediation script execution was successful.
- Remediation was attempted, and the script exited with failure.
- Remediation was not attempted (default).
- Remediation attempt failed. The script failed an integrity check as the policy included might have been tampered with.
- Remediation attempt failed. Client failed to download the script.
- Remediation attempt failed. The script failed an integrity test as the script might be corrupt or has been tampered with.
- Remediation attempt failed. The script was executed but did not exit in time (timeout).
- Remediation attempt failed. A generic internal system failure occurred.
- Remediation attempt failed. The script type is not supported.
- Remediation attempt failed. Failure with launching the script.
- Certificate verification failure. Client could not verify the server certificate presented by Cisco ISE.

Establish Trust to Execute Script Condition

You must establish trust to be able to execute the scripts on endpoints and make sure that the Cisco ISE server is not compromised. A Cisco ISE environment can have one or more PSNs configured. Every PSN has a valid certificate chain. The certificate chain starts with any certificate, followed by an intermediate certificate or a root CA certificate. You can use any certificate in the certificate chain for fingerprint verification.

You can configure the SHA-256 fingerprint of any certificate in the certificate chain in the AnyConnectLocalPolicy's profile editor. For example, the following command generates the SHA-256 fingerprint of a certificate with the name input.cer:

```
openssl x509 -inform DER -in <input.cer> -out <output.crt>
openssl x509 -in <output.crt> -fingerprint -noout -sha256
```

The following is an example of the output:

```
openssl x509 -in 535-pos.crt -fingerprint -noout -sha256
SHA256
Fingerprint=B9:42:7F:85:09:18:30:40:06:0B:DB:9C:48:36:F0:60:90:75:AB:D3:E9:83:AB:1A:BF:01:8F:6E:F0:11:9A:B5
```

The following example shows the new tag in AnyConnectLocalPolicy.xml:

```
<TrustedISECertFingerprints>
<fingerprint>
<algorithm>SHA-256</algorithm>
<hash>B9:42:7F:85:09:18:30:40:06:0B:DB:9C:48:36:F0:60:90:75:AB:D3:E9:83:AB:1A:BF:01:8F:6E:F0:11:9A:B5</hash>
</fingerprint>
</TrustedISECertFingerprints>
```

Note An SHA-256 fingerprint can be added with or without a colon. You can add the fingerprint in either of the following formats: `B9:42:7F:85:09:18:30:40:06:0B:DB:9C:48:36:F0:60:90:75:AB:D3:E9:83:AB:1A:BF:01:8F:6E:F0:11:9A:B5` or `B9427F8509183040060BDB9C4836F0609075ABD3E983AB1ABF018F6EF0119AB5`. Fingerprints are not case-sensitive.

The agent matches the Cisco ISE certificate fingerprint with the trusted certificate fingerprint (present in AnyConnectLocalPolicy.xml) while fetching the script. If an endpoint does not have a valid certificate fingerprint, the script is not executed on the endpoint.

Note If fingerprints are configured in AnyConnectLocalPolicy.xml, they are used to validate Cisco ISE trust for all flows. If the certificate is not trusted or if there is a fingerprint mismatch, no error messages are displayed. However, the following error message is included in the **Posture Script Condition** report (**Operations > Reports > Endpoints and Users**):

```
Condition Script certificate verification failed. Client could not verify the server
certificate presented by Cisco ISE.
```

Script Download

When a posture check fails and when the relevant remediation action is triggered, the agent downloads the script from the HTTPS URL configured in the posture policy. The following conditions must be met for the script to get downloaded:

- Trusted fingerprints should exist in AnyConnectLocalPolicy.xml.
- The fingerprint presented by the HTTPS URL should match the trusted certificate fingerprint present in AnyConnectLocalPolicy.xml .

Add a Launch Program Remediation

You can create a launch program remediation, where the client agent remediates clients by launching one or more applications for compliance.

The Launch Program Remediations page displays all the launch program remediations along with their name and description and their modes of remediation.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > **Posture**.

Step 2 Click **Remediation Actions**.

Step 3 Click **Launch Program Remediation**.

Step 4 Click **Add**.

Step 5 Modify the values in the **New Launch Program Remediation** page.

Step 6 Click **Submit**.

Troubleshoot Launch Program Remediation

Problem

When an application is launched as a remediation using Launch Program Remediation, the application is successfully launched (observed in the Windows Task Manager), however, the application UI is not visible.

Solution

The Launch program UI application runs with system privileges, and is visible in the Interactive Service Detection (ISD) window. To view the Launch program UI application, ISD should be enabled for the following OS:

- Windows Vista: ISD is in stop state by default. Enable ISD by starting ISD service in services.msc.
- Windows 7: ISD service is enabled by default.
- Windows 8/8.1: Enable ISD by changing "NoInteractiveServices" from 1 to 0 in the registry: \HKEY_LOCAL_MACHINE \ SYSTEM \ CurrentControlSet \ Control \ Windows.

Add a Link Remediation

A link remediation allows clients to click a URL to access a remediation window or resource. The client agent opens a browser with the link and allow the clients to remediate themselves for compliance.

The Link Remediation window displays all the link remediations along with their name and description and their modes of remediation.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > **Posture**.
Step 2 Click **Remediation Actions.**
Step 3 Click **Link Remediation**.
Step 4 Click **Add**.
Step 5 Modify the values in the **New Link Remediation** window.
Step 6 Click **Submit**.

Add a Patch Management Remediation

You can create a patch management remediation, which updates clients with up-to-date file definitions for compliance after remediation.

The Patch Management Remediation window displays the remediation type, patch management vendor names, and various remediation options.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > **Posture**.
Step 2 Click **Remediation Actions**.
Step 3 Click **Patch Mangement Remediation**.

Step 4 Click **Add**.

Step 5 Modify the values in the **Patch Management Remediation** window.

Step 6 Click **Submit** to add the remediation action to the **Patch Management Remediations** window.

Add a Windows Server Update Services Remediation

You can configure Windows clients to receive the latest WSUS updates from a locally administered or a Microsoft-managed WSUS server for compliance. A Windows Server Update Services (WSUS) remediation installs latest Windows service packs, hotfixes, and patches from a locally managed WSUS server or a Microsoft-managed WSUS server.

You can create a WSUS remediation where the client agent integrates with the local WSUS Agent to check whether the endpoint is up-to-date for WSUS updates.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > **Posture**.

Step 2 Click **Remediation Actions**.

Step 3 Click **Windows Server Update Services Remediation**.

Step 4 Click **Add**.

Step 5 Modify the values in the **New Windows Server Update Services Remediation** window.

Step 6 Click **Submit**.

Add a Windows Update Remediation

The Windows Update Remediations page displays all the Windows update remediations along with their name and description and their modes of remediation.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > > **Posture.**.

Step 2 Click **Remediation Actions.**

Step 3 Click **Windows Update Remediation**.

Step 4 Click **Add**.

Step 5 Modify the values in the **New Windows Update Remediation** window.

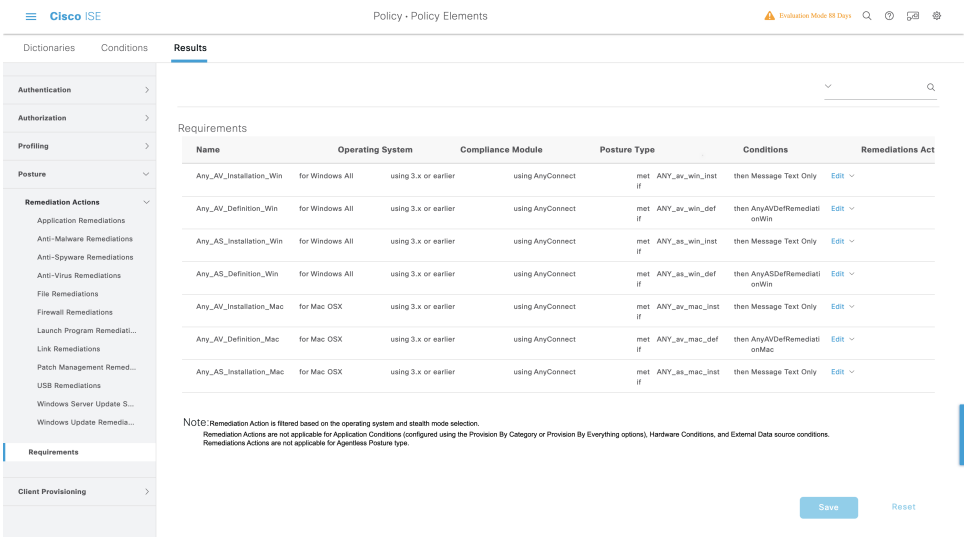
Step 6 Click **Submit**.

Posture Assessment Requirements

A posture requirement is a set of compound conditions with an associated remediation action that can be linked with a role and an operating system. All the clients connecting to your network must meet mandatory requirements during posture evaluation to become compliant on the network.

Posture-policy requirements can be set to mandatory, optional, or audit types in posture policies. If requirements are optional and clients fail these requirements, then the clients have an option to continue during posture evaluation of endpoints.

Figure 3: Posture Policy Requirement Types



Mandatory Requirements

During policy evaluation, the agent provides remediation options to clients who fail to meet the mandatory requirements defined in the posture policy. End users must remediate to meet the requirements within the time specified in the remediation timer settings.

For example, you have specified a mandatory requirement with a user-defined condition to check the existence of C:\temp\text.file in the absolute path. If the file does not exist, the mandatory requirement fails and the user will be moved to Non-Compliant state.

Optional Requirements

During policy evaluation, the agent provides an option to clients to continue, when they fail to meet the optional requirements specified in the posture policy. End users are allowed to skip the specified optional requirements.

For example, you have specified an optional requirement with a user-defined condition to check for an application running on the client machine, such as Calc.exe. Although, the client fails to meet the condition, the agent prompts an option to continue further so that the optional requirement is skipped and the end user is moved to Compliant state.

Audit Requirements

Audit requirements are specified for internal purposes and the agent does not prompt any message or input from end users, regardless of the pass or fail status during policy evaluation.

For example, you are in the process of creating a mandatory policy condition to check if end users have the latest version of the antivirus program. If you want to find out the non-compliant end users before actually enforcing it as a policy condition, you can specify it as an audit requirement.

Visibility Requirements

During policy evaluation, the agent reports compliance data for visibility requirements, every five to ten minutes.

Client System Stuck in Noncompliant State

If a client machine is unable to remediate a mandatory requirement, the posture status changes to "noncompliant" and the agent session is quarantined. To get the client machine past this "noncompliant" state, you need to restart the posture session so that the agent starts posture assessment on the client machine again. You can restart the posture session as follows:

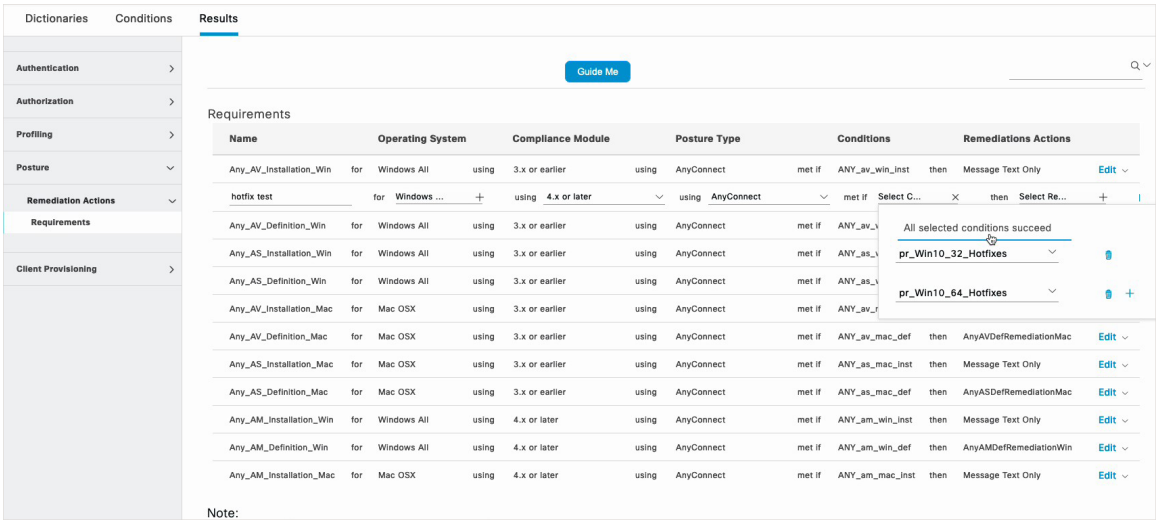
- In wired and wireless Change of Authorization (CoA) in an 802.1X environment:
  - You can configure the Reauthentication timer for a specific authorization policy when you create a new authorization profile in the New Authorization Profiles window.
  - Wired users can get out of the quarantine state once they disconnect and reconnect to the network. In a wireless environment, the user must disconnect from the wireless lan controller (WLC) and wait until the user idle timeout period has expired before attempting to reconnect to the network.
- In a VPN environment—Disconnect and reconnect the VPN tunnel.

Create Client Posture Requirements

You can create a requirement in the Requirements window where you can associate user-defined conditions and Cisco defined conditions, and remediation actions. Once created and saved in the Requirements window, user-defined conditions and remediation actions can be viewed from their respective list windows.

Note To create a Posture Requirement to validate all Windows 10 hotfixes in the environment, you must configure the Conditions area of your Requirement to include both pr_Win10_32_Hotfixes and pr_Win10_64_Hotfixes. At the top of the conditions, ensure **All selected conditions succeed** is selected. If the configuration is successful, **pr_Win10_32_Hotfixes & pr_Win10_64_Hotfixes** will be displayed. To view the details of the validated conditions for an endpoint, from the main menu, choose **Operations** > **Reports** > **Reports** > **Endpoints and Users** > **Posture Assessment by Endpoints**. Click the endpoint to view the corresponding posture details.

Figure 4: Validating Posture Requirements in Windows 10



Before you begin

- You must have an understanding of acceptable use policies (AUPs) for a posture.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > **Posture** > **Requirements**.

Step 2 Enter the values in the **Requirements** window.

Step 3 Click **Done** to save the posture requirement in read-only mode.

Step 4 Click **Save**.

Posture Reassessment Configuration Settings

The following table describes the fields in the Posture Reassessment Configurations window, which you can use to configure posture reassessment. To view this window, click the **Menu** icon (☰) and choose **Administration** > **System** > **Settings** > **Posture** > **Reassessments**.

Table 18: Posture Reassessment Configuration Settings

Field Name	Usage Guidelines
Configuration Name	Enter the name of PRA configuration.
Configuration Description	Enter a description for PRA configuration.
Use Reassessment Enforcement?	Check the check box to apply the PRA configurations for the user identity groups.
Enforcement Type	Choose the action to be enforced: • **Continue**: The user continues to have the privileged access without any user intervention to remediate the client irrespective of the posture requirement. • **Logoff**: If the client is not compliant, the user is forced to logoff from the network. When the client logs in again, the compliance status is unknown. • **Remediate**: If the client is not compliant, the agent waits for a specified time for the remediation to happen. Once the client has remediated, the agent sends the PRA report to the policy service node. If the remediation is ignored on the client, then the agent sends a logoff request to the policy service node to force the client to logoff from the network. If the posture requirement is set to mandatory, then the RADIUS session will be cleared as a result of the PRA failure action and a new RADIUS session has to start for the client to be postured again. If the posture requirement is set to optional, then the agent on the client allows the user to click the continue option from the agent. The user can continue to stay in the current network without any restriction.
Interval	Enter a time interval in minutes to initiate PRA on the clients after the first successful login. The default value is 240 minutes. Minimum value is 60 minutes and maximum is 1440 minutes.
Grace time	Enter a time interval in minutes to allow the client to complete remediation. The grace time cannot be zero, and should be greater than the PRA interval. It can range between the default minimum interval (5 minutes) and the minimum PRA interval. The minimum value is 5 minutes and the maximum value is 60 minutes. **Note** The grace time is enabled only when the enforcement type is set to remediate action after the client fails the posture reassessment.
Select User Identity Groups	Choose a unique group or a unique combination of groups for your PRA configuration.
PRA configurations	Displays existing PRA configurations and user identity groups associated to PRA configurations.

Related Topics

Posture Lease, on page 11
Periodic Reassessments, on page 12
Posture Assessment Options, on page 59
Posture Remediation Options, on page 60
Custom Conditions for Posture, on page 61
Custom Posture Remediation Actions, on page 63
Configure Periodic Reassessments, on page 12

Custom Permissions for Posture

A custom permission is a standard authorization profile that you define in Cisco ISE. Standard authorization profiles set access privileges based on the matching compliance status of the endpoints. The posture service broadly classifies the posture into unknown, compliant, and noncompliant profiles. The posture policies and the posture requirements determine the compliance status of the endpoint.

You must create three different authorization profiles for an unknown, compliant, and noncompliant posture status of endpoints that can have different set of VLANs, DACLs, and other attribute value pairs. These profiles can be associated with three different authorization policies. To differentiate these authorization policies, you can use the Session:PostureStatus attribute along with other conditions.

Unknown Profile

If no matching posture policy is defined for an endpoint, then the posture compliance status of the endpoint may be set to unknown. A posture compliance status of unknown can also apply to an endpoint where a matching posture policy is enabled but posture assessment has not yet occurred for that endpoint and, therefore no compliance report has been provided by the client agent.

Note We recommend you to use posture with redirection for all Cisco network access devices.

Compliant Profile

If a matching posture policy is defined for an endpoint, then the posture compliance status of the endpoint is set to compliant. When the posture assessment occurs, the endpoint meets all the mandatory requirements that are defined in the matching posture policy. For an endpoint that is postured compliant, it can be granted privileged network access on your network.

Noncompliant Profile

The posture compliance status of an endpoint is set to noncompliant when a matching posture policy is defined for that endpoint but it fails to meet all the mandatory requirements during posture assessment. An endpoint that is postured noncompliant matches a posture requirement with a remediation action, and it should be granted limited network access to remediation resources in order to remediate itself.

Configure Standard Authorization Policies

You can define two types of authorization policies on the Authorization Policy window, standard exceptions authorization policies. The standard authorization policies that are specific to posture are used to make policy decisions based on the compliance status of endpoints.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Sets**.

Step 2 In the **View** column, click the arrow icon adjacent the corresponding Default Policy.

Step 3 In the **Actions** column, click the cog icon, and then from the dropdown list, choose a new authorization policy. A new row appears in the **Policy Sets** table.

Step 4 Enter a rule name.

Step 5 From the **Conditions** column, click the (+) symbol.

Step 6 Create the required conditions on the **Conditions Studio Page**. In the **Editor** section, click the **Click To Add an Attribute** text box, and select the required Dictionary and Attribute.

You can drag and drop a Library condition to the **Click To Add An Attribute** text box.

Step 7 Click **Use** to create a new standard authorization policy in read-only mode.

Step 8 Click **Save**.

Best Practices for Network Drive Mapping with Posture

During posture assessment of a Windows endpoint, the endpoint user may encounter a delay in accessing the desktop. This may be due to Windows trying to restore the file server drive letter mappings before providing the user access to the desktop. The best practices to avoid the delay during posture are:

- Endpoints should be able to reach the Active Directory server because the file server drive letter cannot be mapped without reaching the AD. When posture (with ISE posture agent) triggers, it blocks access to AD, causing delay in login. Use Posture Remediation ACLs to provide access to AD servers before posture is completed.
- You should set a delay for the login script until posture completes and then you have to set the Persistence attribute to NO. Windows tries to reconnect all the network drives during login and this cannot be done until ISE posture agent gains full network access.

Configure Agent Stealth Mode Workflow

The process of configuring agent in the stealth mode involves a series of steps. You should perform the following steps in Cisco ISE.

Step 1 Create an agent profile, see Create an Agent Profile.

Step 2 Create an agent configuration for agent packages, see Create an Agent Configuration for Agent Packages.

Step 3 Upload a Open DNS Profile in Cisco ISE, see Upload an Open DNS Profile in Cisco ISE.

Step 4 Create a Client Provisioning Policy, see Create a Client Provisioning Policy.

Step 5 Create a Posture Condition, see Create a Posture Condition.

Step 6 Create Posture Remediation, see Create Posture Remediation

Step 7 Create Posture Requirement in Clientless Mode, see Create Posture Requirement in Stealth Mode.

Step 8 Create Posture Policy, see Create Posture Policy.

Step 9 Configure authorization profile.

a) In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > **Authorization** > **Authorization Profiles**.

b) Click **Add** and enter the **Name** of the profile.

c) In Common Tasks, enable **Web Redirection (CWA, MDM, NSP, CPP)** and choose **Client provisioning (Posture)** from the drop-down list, enter the redirect **ACL** name and choose the Client Provisioning Portal **Value**. You can edit or create a new Client Provisioning Portal in **Work Centers** > **Posture** > **Client Provisioning** > **Client Provisioning Portal**.

Step 10 Configure authorization policies.

a) In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Sets**

b) Click > and choose **Authorization Policy** and click on + icon to create a new authorization rule that features **Session:Posture Status EQUALS Unknown** condition and the authorization profiled configured previously.

c) Above the previous rule, create a new authorization rule that features **Session:Posture Status EQUALS NonCompliant** condition and another one that features **Session:Posture Status EQUALS Compliant** condition.

Create an Agent Profile

Before you begin

You must upload the agent packages for MAC and Windows OS and the compliance modules.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > **Client Provisioning** > **Resources**.

Step 2 From the **Add** drop-down list, choose **Agent Posture Profile**.

Step 3 From the **Posture Agent Profile Settings** drop-down list, choose **Agent**.

Step 4 In the **Name** field, type the required name (for example, AC_Agent_Profile).

Step 5 In the **Agent Behavior** section, select the **Stealth Mode** parameter as **Enabled** .

Step 6 Click **Save**.

What to do next

You should create the agent configuration for the agent packages.

Create an Agent Configuration for Agent Packages

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > **Client Provisioning** > **Resources**.

Step 2 From the **Add** drop-down list, choose **Agent Configuration**.

Step 3 From the **Select Agent Package** drop-down list, choose the required agent package.

Step 4 In the **Configuration Name** text box, type the required Name.

Step 5 In the **Compliance Module** drop-down list, choose the required compliance module.

Step 6 In the **Agent Module Selection** section, check the **ISE Posture** and **Network Access Manager** check boxes.

Step 7 In the **Profile Selection** section, from the **ISE Posture** drop-down list, choose the agent profile.

Step 8 From the **Network Access Manager** drop-down list, choose the required agent profile.

What to do next

You should upload the Open DNS profile to be pushed to the client.

Upload an Open DNS Profile in Cisco ISE

The Open DNS profile is pushed to the client.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > **Client Provisioning** > **Resources**.

Step 2 From the **Add** drop-down list, choose **Agent Resources From Local Disk**.

Step 3 From the **Category** drop-down list, choose **Customer Created Packages**.

Step 4 From the **Type** drop-down list, choose **Agent Profile**.

Step 5 In the **Name** text box, type the required name (for example, OpenDNS).

Step 6 Click **Browse** and locate the JSON file from the local disk.

Step 7 Click **Submit**.

What to do next

You should create the client provisioning policy.

Create a Client Provisioning Policy

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Client Provisioning**.

Step 2 Create the required rule (for example, Rule Name=WindowsAll, if Identity Groups=Any and Operating Systems=Windows All and Other Conditions=Conditions, then Results=AC_Win_44117).

What to do next

You should create the posture condition.

Create a Posture Condition

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Conditions** > **Posture** > **File Condition**.

Step 2 Enter the required name (for example, filechk).

Step 3 From the **Operating Systems** drop-down list, choose Windows 7 (All).

Step 4 From the **File Type** drop-down list, choose FileExistence.

Step 5 From the **File Path** drop-down list, choose ABSOLUTE_PATH C:\test.txt.

Step 6 From the **File Operator** drop-down list, choose DoesNotExist.

What to do next

You should create the posture remediation.

Create Posture Remediation

The file condition checks if test.txt file exists on the endpoint. If it does not exist, the remediation is to block the USB port and prevent the installation of the file using a USB device.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > **Remediation Actions** > **USB Remediations**.

Step 2 Enter the required name (for example, clientless_mode_block).

Step 3 Click **Submit**.

What to do next

You should create the posture requirement.

Create Posture Requirement in Stealth Mode

When you create a Remediation action from the Requirements page, only the remediations that are applicable to stealth mode are displayed: Anti-Malware, Launch Program, Patch Management, USB, Windows Server Update Services, and Windows Update.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > **Client Provisioning** > **Resources**.

Step 2 Create the required posture requirement (for example, Name=win7Req for Operating Systems=Windows7(All) using Compliance Module=4.x or later using Posture Type=Agent Stealth met if Condition=filechk then Remediation Actions=clientless_mode_block).

What to do next

You should create the posture policy.

Create Posture Policy

Before you begin

Ensure that the posture policy requirement and the policy are created in the clientless mode.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Posture**

Step 2 Create the required rule. For example, if Identity Groups=Any and Operating Systems=Windows 7(All) and Compliance Module=4.x or later and Posture Type=Agent Stealth then Requirements=win7Req.

Note For Client Provisioning without URL redirection, configuring the conditions with attributes specific to Network Access or Radius will not work and matching of the client provisioning policy might fail due to the non-availability of session information for the specific user in the Cisco ISE server. However, Cisco ISE allows configuring conditions for the externally added identity groups.

Enable Agent Stealth Mode Notifications

Cisco ISE provides several new failure notifications for agent stealth mode deployments. Enabling failure notifications in stealth mode helps you to identify issues with wired, wireless, or VPN connections. To enable notifications in stealth mode:

Note AnyConnect version 4.5.0.3040 and higher supports stealth mode notifications.

Before you begin

Configure agent in stealth mode.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose Choose **Policy** > **Policy Elements** > **Results** > **Client Provisioning** > **Resources**.

Step 2 Choose **Add** > **Agent Posture Profile**.

Step 3 From the **Select a Category** drop-down list, choose **Agent**.

Step 4 From the **Agent Behavior** section, choose **Enabled** for the **Enable notifications in stealth mode** option.

Configure Cisco Temporal Agent Workflow

The process of configuring the Cisco temporal agent involves a series of steps. You should perform the following steps in Cisco ISE.

Step 1 Create Posture Condition

Step 2 Create Posture Requirements

Step 3 Create the Posture Policy

Step 4 Configure the Client Provisioning Policy

Step 5 Configure authorization profile.

a) In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > **Authorization** > **Authorization Profiles**.

b) Click **Add** and enter the **Name** of the profile.

c) In Common Tasks, enable **Web Redirection (CWA, MDM, NSP, CPP)** and choose **Client provisioning (Posture)** from the drop-down list, enter the redirect **ACL** name and choose the Client Provisioning Portal **Value**. You can edit or create a new Client Provisioning Portal in **Work Centers** > **Posture** > **Client Provisioning** > **Client Provisioning Portal**.

Step 6 Configure authorization policies.

a) In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Sets**.

b) Click > and choose **Authorization Policy** and click on + icon to create a new authorization rule that features **Session:Posture Status EQUALS Unknown** condition and the authorization profiled configured previously.

c) Above the previous rule, create a new authorization rule that features **Session:Posture Status EQUALS NonCompliant** condition and another one that features **Session:Posture Status EQUALS Compliant** condition.

Step 7 Download and Launch Cisco Temporal Agent

Create Posture Condition

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Conditions** > **Posture** > **File Condition**.

Step 2 Enter the required name (for example, filecondwin).

Step 3 From the **Operating Systems** drop-down list, choose Windows 7 (All).

Step 4 From the **File Type** drop-down list, choose FileExistence.

Step 5 From the **File Path** drop-down list, choose ABSOLUTE_PATH C:\test.txt.

Step 6 From the **File Operator** drop-down list, choose DoesNotExist.

Create Posture Requirements

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > **Posture** > **Requirements**.

Step 2 From the **Edit** drop-down list, choose **Insert New Requirement**.

Step 3 Enter the **Name**, **Operating Systems**, and **Compliance Module** (for example, Name filereqwin, Operating Systems Windows All, Compliance Module 4.x or later).

Step 4 In the **Posture Type** drop-down, choose **Temporal Agent**.

Step 5 Select the required condition (for example, filecondwin).

Note For the Cisco Termporal Agent, you can only view Patch Management conditions containing the **Installation** check type in the **Requirements** page.

Step 6 Select the **Message Text Only** remediation action.

Note The temporal agent is supported by AnyConnect 4.x or later.

Create the Posture Policy

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Posture**.

Step 2 Create the required rule (for example, Name=filepolicywin, Identity Groups=Any, Operating Systems=Windows All, Compliance Module=4.x or later, Posture Type=Temporal Agent, and Requirements=filereqwin).

Configure the Client Provisioning Policy

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Client Provisioning**.

Step 2 Create the required rule (for example, Rule Name=Win, Identity Groups=Any, Operating Systems=Windows All, Other Conditions=Conditions, Results=CiscoTemporalAgentWindows4.5).

Download and Launch Cisco Temporal Agent

Step 1 Connect to the SSID.

Step 2 Launch a Browser and you will be redirected to the Client Provisioning Portal.

Step 3 Click **Start**. This checks if the Cisco Temporal agent is installed and running.

Step 4 Click **This Is My First Time Here**.

Step 5 Choose **Click Here to Download and Launch Cisco Temporal Agent**.

Step 6 Save the Cisco Temporal Agent .exe or .dmg file for Windows or macOS respectively. For Windows, run the .exe file and for macOS, double-click the .dmg file and run the acisetempagent app.
The Cisco Temporal Agent scans the client and displays the results, such as Red cross marks for non-compliant checks.

Posture Troubleshooting Tool

The Posture Troubleshooting tool helps you find the cause of a posture-check failure to identify the following:

- Which endpoints were successful in posture and which were not.
- If an endpoint failed in posture, what steps failed in the posture process.
- Which mandatory and optional checks passed and failed.

You determine this information by filtering requests based on parameters, such as username, MAC address, and posture status.

Configure Endpoint Login Credentials

The **Endpoint Login Configuration** window is where you configure login credentials so Cisco ISE can log in to clients. The login credentials that are configured in this window are used by the following Cisco ISE features:

In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Settings** > **Endpoint Scripts** > **Settings**.

The following tabs are displayed:

- **Windows Domain User**: Configure the domain credentials that Cisco ISE must use to log in to a client via SSH. Click the **Plus** icon and enter as many Windows logins as you need. For each domain, enter the required values in the **Domain**, **Username**, and **Password** fields. If you configure domain credentials, the local user credentials that are configured in the **Windows Local User** tab are ignored.
- **Windows Local User**: Configure the local account that Cisco ISE uses to access the client via SSH. The local account must be able to run Powershell and Powershell remote.
- **MAC Local User**: Configure the local account that Cisco ISE uses to access the client via SSH. The local account must be able to run Powershell and Powershell remote. In the **Username** field, enter the Account Name of the local account. To view a Mac OS Account Name, run the following command in the Terminal:

  ```
  whoami
  ```

Endpoint Scripts Settings

This page configures options for Endpoint Scripts and Agentless Posture.

- **Upload endpoint script execution logs to ISE**: Enabled by default, you can upload endpoint scripts to Cisco ISE. Disabling this disables endpoint scripts, you cannot upload or run endpoint scripts.

- **Endpoint script execution verbose logging**: Enable verbose logging for debugging.
- **Endpoints processor batch size**: You can adjust this accommodate network loads and system performance.
- **Endpoints processing concurrency for MAC**
- **Endpoints processing concurrency for Windows**
- **Maximum retry attempts for OS identification**
- **Delay between retries for OS identification (msec)**
- **Endpoint pagination batch size**
- **Log retention period on Endpoints (Days)**
- **Connection Time out (sec)**
- **Max-retry attempts for Connection**
- **Port Number for Powershell**: Change this to use a nonstandard port number.
- **Port Number for SSH Connection**: Change this to use a nonstandard port number.

Configure Client Provisioning in Cisco ISE

Enable client provisioning to allow users to download client provisioning resources and configure agent profiles. You can configure agent profiles for Windows, Mac OS X, and Linux clients, and native supplicant profiles for personal devices. If you disable client provisioning, users attempting to access the network will receive a warning message indicating that they are not able to download client provisioning resources.

Before you begin

If you are using a proxy and hosting client provisioning resources on a remote system, verify that the proxy allows clients to access that remote location.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Settings** > **Client Provisioning** or **Work Centers** > **Posture** > **Settings** > **Software Updates** > **Client Provisioning**.

Step 2 From the **Enable Provisioning** drop-down list, choose **Enable** or **Disable**.

Step 3 From the **Enable Automatic Download** drop-down list, choose **Enable**.

Feed downloads include all the available client provisioning resources. Some of these resources may not be pertinent to your deployment. Cisco recommends manually downloading resources whenever possible instead of setting this option.

Step 4 Specify the URL where Cisco ISE searches for system updates in the **Update Feed URL** text box. For example, the default URL for downloading client-provisioning resources is https://www.cisco.com/web/secure/spa/provisioning-update.xml.

Step 5 When there is no client provisioning resource for a device, choose one of the following options:

- **Allow Network Access**: Users are allowed to register their device on the network without having to install and launch the native supplicant wizard.

- **Apply Defined Authorization Policy**: Users must try to access the Cisco ISE network via standard authentication and authorization policy application (outside of the native supplicant provisioning process). If you enable this option, the user device goes through standard registration according to any client-provisioning policy applied to the user's ID. If the user's device requires a certificate to access the Cisco ISE network, you must also provide detailed instructions to the user describing how to obtain and apply a valid certificate using the customizable user-facing text fields.

Step 6 Click **Save**.

Note If the ISE certificates are cached in the HTTP Strict Transport Security (HSTS) store of the endpoint, client provisioning portal redirection might fail and you might see the following error message:

```
You cannot visit hostname.domain.com right now because the website uses HSTS. Network errors
and attacks are temporary, so this page will probably work later.
```

To resolve this issue, delete the browser cache on the endpoint or navigate to chrome://net-internals/#hsts and delete the self-signed ISE certificates.

What to do next

Configure client provisioning resource policies.

Client Provisioning Resources

Client provisioning resources are downloaded to endpoints after the endpoint connects to the network. Client provisioning resources consist of compliance and posture agents for desktops, and native supplicant profiles for phones and tablets. Client provisioning policies assign these provisioning resources to endpoints to start a network session.

In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy Elements** > **Results** > **Client Provisioning** > **Resources**. The following resource types can be added to the list by clicking the **Add** button:

- **Agent resources from Cisco Site**: Select the agent and supplicant provisioning wizards you want to make available for client provisioning policies. Cisco periodically updates this list of resources, adding new ones and updating existing ones. You can also set up ISE to download all the Cisco resources and resource updates automatically, see Configure Client Provisioning in Cisco ISE, on page 82 for more information.
- **Agent resources from local disk**: Select resources on your PC that you want to upload to ISE, see Add Cisco Provided Client Provisioning Resources from a Local Machine, on page 85.
- **Agent Configuration**: Select the agent clients that you want to make available for client provisioning. See Create Agent Configuration for more information.
- **Native Supplicant Profile**: Configure a supplicant profile for phones and tablets that contain settings for your network. For more information, see Create Native Supplicant Profiles.
- **Agent Posture Profile**: Configure the Agent ISE Posture here when you don't want to create and distribute agent XML profiles. .

After creating client provisioning resources, create client provisioning policies that apply the client provisioning resources to the endpoints. See Configure Client Provisioning Resource Policies, on page 111.

Related Topics

Configure Client Provisioning in Cisco ISE, on page 82
Add Client Provisioning Resources from Cisco, on page 84
Add Cisco Provided Client Provisioning Resources from a Local Machine, on page 85
Add Customer Created Resources for Agent from a Local Machine, on page 86

Add Client Provisioning Resources from Cisco

You can add client provisioning resources from Cisco.com for Cisco Web agent, Agent Windows, MacOS, and Linux clients. Depending on the resources that you select and available network bandwidth, Cisco ISE can take a few minutes to download client provisioning resources to Cisco ISE.

Before you begin

- Ensure that you have configured the correct proxy settings in Cisco ISE.
- Enable client provisioning in Cisco ISE.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > **Client Provisioning** > **Resources**.

Step 2 Choose **Add** > **Agent resources from Cisco site**.

Step 3 Select one or more required client provisioning resources from the list available in the **Download Remote Resources** dialog box.

Step 4 Click **Save**.

Note the following while installing the Linux agent:

- If you are using self-signed certificates:
  - You must enable the SSH agent to copy the ISE certificate to the Linux agent.
    - For RHEL:
      1. Export the certificate from Cisco ISE GUI.

Attention For Red Hat Linux, you must add the IP address to the SAN field of the self-signed certificate.

      2. Copy <certificate>.pem to /etc/pki/ca-trust/source/anchors/ and rename the file to <certificate>.crt.
      3. Run the following command: **sudo update-ca-trust extract**
      4. Go to /etc/pki/tls/certs/
      5. Run the following command: **openssl x509 -in ca-bundle.crt -text -noout**

- For Ubuntu:
  1. Export the certificate from Cisco ISE GUI.
  2. Copy <certificate>.pem to /usr/local/share/ca-certificates/ and rename it to <certificate>.crt.
  3. Run the following command: **sudo update-ca-certificates**

     To verify whether the CA certificate is installed properly, go to /etc/ssl/certs/ca-certificates.crt and check the certificate present in this file.

Note Certificate import is not required, if the ISE certificate is issued by a trusted CA.

- Initiate dot1x redirect or non-redirect flow.
- If you are using RHEL, ensure that yum is updated with subscription manager. Update apt-get if you are using Ubuntu.

  For more information about the system requirements for Linux agent, see the Release Notes for Cisco AnyConnect Secure Mobility Client, Release 4.9.

What to do next

After you have successfully added client provisioning resources to Cisco ISE, you can begin to configure client provisioning resource policies.

Add Cisco Provided Client Provisioning Resources from a Local Machine

You can add client provisioning resources from the local disk, which you previously downloaded from Cisco.

Before you begin

Be sure to upload only current, supported resources to Cisco ISE. Older, unsupported resources are likely to cause serious issues for client access.

If you are downloading the resource files manually from the Cisco.com, see the Section “Cisco ISE Offline Updates” in the Cisco ISE Release Notes.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > **Client Provisioning** > **Resources**

Step 2 Choose **Add** > **Agent resources from local disk**.

Step 3 Choose **Cisco Provided Packages** from the **Category** drop-down list.

Step 4 Click **Browse** to the directory on your local machine where the resource file that you want to download to Cisco ISE resides.

You can add agent or Cisco Web Agent resources that you previously downloaded from Cisco to your local machine.

Step 5 Click **Submit**.

What to do next

After you have successfully added client provisioning resources to Cisco ISE, you can configure client provisioning resource policies.

Add Customer Created Resources for Agent from a Local Machine

Add customer created resources like agent customization and localization packages and agent profiles from the local machine to Cisco ISE.

Before you begin

Ensure that customer created resources for agent are zipped files and available in your local disk.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > **Client provisioning** > **Resources**.

Step 2 Choose **Add** > **Agent Resources from local disk**.

Step 3 Choose **Customer Created Packages** from the **Category** drop-down list.

Step 4 Enter the name and description for agent resources.

Step 5 Click **Browse** to the directory on your local machine where the resource file that you want to download to Cisco ISE resides.

Step 6 Choose the following agent resources to upload to Cisco ISE:

- Agent customization bundle
- Agent localization bundle
- Agent profile
- Advanced Malware Protection (AMP) Enabler Profile

Step 7 Click **Submit**.
The Uploaded Agent Resources table displays Agent resources that you add to Cisco ISE.

What to do next

Create agent configuration.

Create Native Supplicant Profiles

You can create native supplicant profiles to enable users to bring their own devices into the Cisco ISE network. When the user signs in, Cisco ISE uses the profile that you associated with that user's authorization requirements to choose the necessary supplicant provisioning wizard. The wizard runs and sets up the user's personal device to access the network.

Note The provisioning wizard only configures interfaces which are active. Because of this, users with Wired and Wireless connections will not be provisioned for both interfaces, unless they are both active.

Before you begin

- Open up TCP port 8905 to enable the installation of Cisco Agent, Cisco Web Agent, and supplicant provisioning wizard. For more information about port usage, see the "Cisco ISE Appliance Ports Reference" appendix in the *Cisco Identity Services Engine Hardware Installation Guide*.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > **Client Provisioning** > **Resources**.

Step 2 Choose **Add** > **Native Supplicant Profile**.

Step 3 Create a profile, using the procedure described in Native Supplicant Profile Settings, on page 87 .

What to do next

Enable self-provisioning capabilities that allow employees to directly connect their personal devices to the network, as described in the Support for multiple Guest Portals section.

Native Supplicant Profile Settings

In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > **Client Provisioning** > **Resources** > **Add** > **Native Supplicant Profile**. The following settings are displayed.

- **Name**: Enter the name of the native supplicant profile that you are creating.
- **Operating System**: Choose which operating system(s) this profile should apply to from the drop-down list.

Each profile defines the settings for a network connection that Cisco ISE will apply to the client's native supplicant.

Wireless Profile

Configure a wireless profile, one for each SSID that you want to make available to the client:

- **SSID Name**: Enter the name of the SSID that the client will connect to.
- **Proxy Auto-Config File URL**: If the client will connect to a proxy to get the network configuration for its supplicant, enter the URL of that proxy server.
- **Proxy Host/IP**: If the client will connect to a proxy to get the network configuration for its supplicant, enter the Host/IP of that proxy server.
- **Proxy Port**: If the client will connect to a proxy to get the network configuration for its supplicant, enter the port of that proxy server.
- **Security**: Choose either **WPA** or **WPA2**.
- **Allowed Procotol**: Choose either **PEAP** or **EAP-TLS**.
- **Certificate Template**: For TLS, choose one of the certificate templates. The certificate templates are defined in **Administration** > **System Certificates** > **Certificate Authority** > **Certificate Templates**.

Optional Settings

If you expand **Optional**, the following fields are displayed.

Windows Setings

- **Authentication Mode**: Choose **User**, **Machine** or **both** as credentials for authorization.
- **Do not prompt user to authorize new servers or trusted certification authorities**: If this option is enabled, the user is not prompted to authorize. User certificates are automatically accepted.
- **Use a different user name for the connection**: This is applicable only for wireless profiles. Use a different user name for the connection.
- **Connect even if the network is not broadcasting its name (SSID)**: This is applicable only for wireless profiles. Connect to a network even when its SSID is not being broadcasted.

iOS Settings

- **Enable if target network is hidden**: Check this check box if the target network is hidden.

Android Settings

- **Certificate Enrollment Protocol:** : Click either of these radio buttons to choose the Certificate Enrollment Protocol: **Enrollment over Secure Transport (EST)** or **Simple Certificate Enrollment Protocol (SCEP)**. If you choose the EST protocol, Cisco ISE will ask for additional password inputs from Android users when issuing certificates.

Wired Profile

- **Allowed Protocol**: Choose either **PEAP** or **EAP-TLS**.
- **Certificate Template**: For TLS, choose one of the certificate templates. The certificate templates are defined in **Administration** > **System Certificates** > **Certificate Authority** > **Certificate Templates**.

Optional Settings

If you expand **Optional**, the following fields are also available for Windows clients.

- **Authentication Mode**: Choose **User**, **Machine** or **both** as credentials for authorization.
- **Automatically use logon name and password (and domain if any)**: If you selected **User** for **Authentication Mode**, use the logon and password to without prompting the user, if that information is available.
- **Enable Fast Reconnect**: Allow a PEAP session to resume without checking user credentials when the session resume feature is enabled in the PEAP protocol options, which is configured on **Administration** > **System** > **Settings** > **Protocols** > **PEAP**.
- **Enable Quarantine Checks**: Check if the client has been quarantined.
- **Disconnect if server does not present cryptobinding TLV**: Disconnect if cryptobinding TLV is not supported for the network connection.
- **Do not prompt user to authorize new servers or trusted certification authorities**: Automatically accept user certificates; do not prompt the user.

Client Provisioning Without URL Redirection for Different Networks

Client provisioning without URL redirection is required when the third party NAC does not support CoA. You can perform client provisioning with and without URL redirection.

Note For client provisioning with URL redirection, if the client machine has proxy settings configured, ensure that you add Cisco ISE to the list of exceptions in the browser settings. This setting is applicable for all flows, BYOD, MDM, Guest, and Posture that use URL redirection. For example, on Windows machines, do the following:

1. From Control Panel, click **Internet Properties**.
2. Select the **Connections** tab.
3. Click **LAN settings**.
4. Click **Advanced** from the Proxy server area.
5. Enter the IP addresses of the Cisco ISE nodes in the **Exceptions** box.
6. Click **OK**.

Given below are the steps you perform to provision an endpoint without redirection for different networks.

Dot1X EAP-TLS

1. Connect the Cisco ISE network with provisioned certification.
2. Open a browser window and type in the provisioning URL: provisioning.cisco.com.
3. Log into the CP portal via internal user, AD, LDAP, or SAML.

   Agent performs posture. The endpoint moves to the right network based on posture compliance.

Dot1X PEAP

1. Connect the Cisco ISE network with User Name and Password through NSP
2. Open a browser window and type in the provisioning URL: provisioning.cisco.com.
3. Log into the CP portal via internal user, AD, LDAP, or SAML

   Agent performs posture. The endpoint moves to the right network based on posture compliance.

MAB (Wired Networks)

1. Connect the Cisco ISE network.
2. Open a browser window and type in the provisioning URL: provisioning.cisco.com.
3. Log into the CP portal via internal user, AD, LDAP, or SAML.

   Agent performs posture. The endpoint moves to the right network based on posture compliance.

MAB (Wireless Networks)

1. Connect the Cisco ISE network
2. Open a browser window and type in the provisioning URL: provisioning.cisco.com.
3. Log into the CP portal via internal user, AD, LDAP, or SAML.

   Agent performs posture. Posture starts for wireless 802.1X only.

AMP Enabler Profile Settings

The following table describes the fields in the Advanced Malware Protection (AMP) Enabler Profile window. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > **Client Provisioning** > **Resources**.

Click the **Add** drop-down arrow and select the **AMP Enabler Profile**.

Table 19: AMP Enabler Profile Page

Field Names	Usage Guidelines
Name	Enter the name of the AMP enabler profile that you want to create.
Description	Enter a description for the AMP enabler profile.
Install AMP Enabler	• **Windows Installer**: Specify the URL of the local server that hosts the AMP for Windows OS software. The agent module uses this URL to download the .exe file to the endpoint. The file size is approximately 25 MB. • **Mac Installer**: Specify the URL of the local server that hosts the AMP for macOS software. The agent module uses this URL to download the .pkg file to the endpoint. The file size is approximately 6 MB. The **Check** button communicates with the server to verify if the URL is valid. If the URL is valid, a "File found" message is displayed or else an error message is displayed.
Uninstall AMP Enabler	Uninstalls the AMP for endpoint software from the endpoint.
Add to Start Menu	Adds a shortcut for the AMP for endpoint software in the Start menu of the endpoint, after the AMP for endpoint software is installed on the endpoint.
Add to Desktop	Adds an icon for the AMP for endpoint software on the desktop of the endpoint, after the AMP for endpoint software is installed on the endpoint.
Add to Context Menu	Adds the Scan Now option in the right-click context menu of the endpoint, after the AMP for endpoint software is installed on the endpoint.

Create an AMP Enabler Profile Using the Embedded Profile Editor

Note AMP Enabler is applicable only for clients with AnyConnect. Cisco Secure Client includes Secure Endpoint instead. For information on how to use Secure Endpoint with Cisco Secure Client, see the *Cisco Secure Client Administrator Guide*.

You can create the AMP enabler profile using the Cisco ISE embedded profile editor or the standalone editor.

To create the AMP enable profile using the Cisco ISE embedded profile editor:

Before you begin

- Download the AMP for Endpoint software from the SOURCEfire portal and host it on a local server.
- Import the certificate of the server that hosts the AMP for endpoint software to the ISE certificate store. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Certificates** > **Trusted Certificates**.
- Ensure that the **AMP Enabler** options are selected in the **Agent Module Selection** and **Profile Selection** sections in the **Agent Configuration** window (**Policy** > **Policy Elements** > **Results** > **Client provisioning** > **Resources** > **Add** > **Agent Configuration** > **Select Agent Package**).
- You must log in to the SOURCEfire portal, create policies for endpoint groups, and download the AMP for endpoint software. The software comes preconfigured with the policies that you have chosen. You must download two images, namely, the redistributable version of the AMP for endpoint software for Windows OS and AMP for endpoint software for macOS. The downloaded software is hosted on a server that is accessible from the enterprise network.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > **Client Provision** > **Resources**.

Step 2 Click the **Add** drop-down.

Step 3 Choose **AMP Enabler Profile** to create a new AMP enabler profile.

Step 4 Enter the appropriate values in the fields.

Create an AMP Enabler Profile Using the Standalone Editor

To create an AMP enabler profile using the agent standalone editor.

Before you begin

You can create an AMP enabler profile by uploading the XML format of the profile using the AnyConnect 4.1 standalone editor.

- Download the agent standalone profile editor for Windows and Mac OS from Cisco.com.
- Launch the standalone profile editor and enter the fields as specified in the AMP Enabler Profile Settings.
- Save the profile as an XML file in your local disk.

- Ensure that the **AMP Enabler** options are selected in the **Agent Module Selection** and **Profile Selection** sections in the **Agent Configuration** window (**Policy** > **Policy Elements** > **Results** > **Client provisioning** > **Resources** > **Add** > **Agent Configuration** > **Select Agent Package**).

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > **Client provisioning** > **Resources**

Step 2 Click **Add**.

Step 3 Choose **Agent resources from local disk**.

Step 4 Choose **Customer Created Packages** from the **Category** drop-down.

Step 5 Choose **AMP Enabler Profile** from the **Type** drop-down.

Step 6 Enter a **Name** and **Description**.

Step 7 Click **Browse** and select the saved profile (XML file) from the local disk. The following example shows a customized install file.

```
<?xml version="1.0" encoding="UTF-8"?>
<FAProfile xsi:noNamespaceSchemaLocation="FAProfile.xsd"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
 <FAConfiguration>
 <Install>
 <WindowsConnectorLocation>
https://fa_webserver/ACFA_Mac_FireAMPSetup.exe
</WindowsConnectorLocation>
 <MacConnectorLocation>
https://fa_webserver/ACFA_Mac_FireAMPSetup.exe
</MacConnectorLocation>
 <StartMenu>true</StartMenu>
 <DesktopIcon>false</DesktopIcon>
 <ContextIcon>true</ContextIcon>
 </Install>
 </FAConfiguration>
</FAProfile>
```

The following example shows a customized uninstall file.

```
<?xml version="1.0" encoding="UTF-8"?>
<FAProfile xsi:noNamespaceSchemaLocation="FAProfile.xsd"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
 <FAConfiguration>
 <Uninstall>
 </Uninstall>
 </FAConfiguration>
</FAProfile>
```

Step 8 Click **Submit**.
The newly created AMP Enabler profile is displayed in the **Resources** page.

Troubleshoot Common AMP Enabler Installation Errors

When you enter the SOURCEfire URL in the Windows or MAC Installer text box and click **Check**, you might encounter any of the following errors:

- Error Message: The certificate for the server containing the Mac/Windows installer file is not trusted by ISE. Add a trust certificate to **Administration** > **Certificates** > **Trusted Certificates**.

This error message appears if you have not imported the SOURCEfire trusted certificate in to the Cisco ISE certificate store. Obtain a SOURCEfire trusted certificate and import it in to the Cisco ISE trusted certificate store (Administration > Certificates > Trusted Certificates).

- Error Message: The installer file is not found at this location, this may be due to a connection issue. Enter a valid path in the Installer text box or check your connection.

  This error message appears when the server hosting the AMP for Endpoint software is down or if there is a typographic error in the Windows Installer or MAC Installer text box.

- Error Message: The Windows/Mac installer text box does not contain a valid URL.

  This error message appears when you enter a syntactically incorrect URL format.

Cisco ISE Support for Onboarding Chromebook Devices

Chromebook devices are managed devices (managed by the Google domain), unlike other devices (Apple, Windows, Android) and have limited onboarding support. Cisco ISE supports the onboarding of Chromebook devices on a network. Onboarding refers to the process of delivering the required settings and files to an endpoint such that it is able to connect securely to a network after authenticating with Cisco ISE. This process includes certificate provisioning and/or native supplicant provisioning. However, in Chromebook devices, you can only perform certificate provisioning. Native supplicant provisioning is done via the Google Admin Console.

Unmanaged Chromebook devices cannot be onboarded to a secure network.

The entities involved in the Chromebook onboarding process are the:

- Google Administrator
- ISE Administrator
- Chromebook User/Device
- Google Admin Console (Managed by the Google Administrator)

The Google administrator:

- Secures the following licenses:

  1. Google Apps Administrator license for the Google Admin Console configuration—URL: https://admin.google.com. The Google Admin Console enables an administrator to manage Google services for people in an organization.
  2. Chromebook device management license—URL: https://support.google.com/chrome/a/answer/2717664?hl=en. A Chromebook device management license is used to configure settings and enforce policies for a specific Chromebook device. It gives the Google Administrator access to device settings to control user access, customize features, configure network access, and more.

- Facilitates provisioning and enrolling of Chromebook devices with a Google device license.
- Manages Chromebook devices through the Google Admin Console.
- Sets up and manages the Wi-Fi network configuration for each Chromebook user.

- Manages the Chromebook devices by configuring applications and forced extensions to be installed on the Chromebook device. Onboarding the Chromebook device requires the Cisco Network Setup Assistant extensions to be installed in the Chromebook device. This allows the Chromebook device to connect to Cisco ISE and install the ISE certificate. The extension is forcibly installed because the action of certificate installation is allowed only for managed devices.
- Ensures that the Cisco ISE certificates are installed in the Google Admin Console to provide server validation and secure connection. The Google administrator decides whether a certificate should be generated for a device or a user. Cisco ISE provides options to:
  - Generate the certificate for a single user who does not share the Chromebook device.
  - Generate a certificate for a Chromebook device that is shared by multiple users. Refer to Step 5 in the Configure the Network and Force Extensions in the Google Admin Console section for the required additional configuration.

  The Google Administrator installs the ISE server certificate so that ISE is trusted to perform the certificate provisioning on the Chromebook device and also to allow EAP-TLS certificate-based authentication. Google Chrome version 37 and higher supports certificate-based authentication for Chromebook devices. The google administrator needs to load the ISE provisioning application in the Google Admin Console and make it available to the Chromebook devices to get the certificate from ISE.
- Ensures that the recommended Google host names are allowed in the ACL definition list configured in the WLC for SSL secure connections. Refer to the recommended and allowed host names in the Google Support page.

The ISE Administrator:

- Defines the native supplicant profile for the Chromebook OS that includes the certificate template structure.
- Creates the necessary authorization rules and client provisioning policies in Cisco ISE for Chromebook users.

The Chromebook User:

- Wipes out the Chromebook device and enrolls it to the Google domain to secure the enforced policy that was defined by the Google administrator.
- Receives the Chromebook device polices and the Cisco Network Setup Assistant forced extension installed by the Google Admin Console.
- Connects to the provisioned SSID, as defined by the Google administrator, opens the browser, displays the BYOD pages, and starts the onboarding process.
- The Cisco Network Setup Assistant installs a client certificate in the Chromebook device, which allows the device to perform EAP-TLS certificate-based authentication.

The Google Admin Console:

The Google Admin Console supports Chromebook device management and allows configuring a secure network and pushing Cisco Network Setup Assistant certificate management extensions to the Chromebook. The extension sends an SCEP request to Cisco ISE and installs the client certificate to allow secure connection and access to the network.

Best Practices for Using Chromebook Device in a Shared Environment

When a Chromebook device is used in a shared environment, such as schools and libraries, the Chromebook device is shared by different users. Some of the best practices that Cisco recommends include:

- When onboarding a Chromebook device with a specific user (student or professor) name, the user's name will be populated in the Common Name (CN) in the Subject field of the certificate. Also, the shared Chromebook is listed in the My Devices portal under that specific user. Therefore, it is recommended for shared devices to use a shared credential when onboarding, so that devices show up only under the specific user's My Devices portal listing. The shared account can be administered by the administrator or professor as a separate account to control shared devices.
- The Cisco ISE administrator can create a custom certificate template for shared Chromebook devices and use it in the policy. For example, instead of using the standard certificate template that matches the Subject-Common Name (CN) value, you can specify a Name (for example, chrome-shared-grp1) in the certificate and the same name can be assigned to the Chromebook device. A policy can be designed to match the name to allow or deny access to a Chromebook device.
- The Cisco ISE administrator can create an endpoint group with all the Chromebook devices' MAC addresses that needs to go through Chromebook onboarding (devices for which access need to be restricted). The authorization rule should call this out along with device type Chromebook—this would allow access to be redirected to the NSP.

Chromebook Onboarding Process

The Chromebook onboarding process involves a series of steps:

Step 1 Configure the Network and Force Extensions in the Google Admin Console .

Step 2 Configure Cisco ISE for Chromebook Onboarding.

Step 3 Wipe a Chromebook Device.

Step 4 Enroll Chromebook to the Google Admin Console.

Step 5 Connect Chromebook to the Cisco ISE Network for BYOD On Boarding.

Configure the Network and Force Extensions in the Google Admin Console

The Google administrator performs the following steps.

Step 1 Log in to the Google Admin Console.

a) Enter the following URL: https://admin.google.com in the browser.
b) Enter the required username and password.
c) In the **Welcome to Admin Console** window, click **Device Management**.
d) On the **Device Management** window, click **Network**.

Step 2 Set up the Wi-Fi network for managed devices.

a) In the **Networks** window, click **Wi-Fi**.

b) Click **Add Wi-Fi** to add the required SSIDs. See Google Admin Console - Wi-Fi Network Settings for more information.

For MAB flows, create two SSIDs, one for the open network, and the other for certificate authentication. When you connect to the open network, Cisco ISE ACLs redirect you to the credentialed guest portal for authentication. After successful authentication, ACLs redirect you to the BYOD portal.

If the ISE certificate is issued by an intermediate CA, then you must map the intermediate certificate to the "Server certificate authority", instead of to the Root CA.

c) Click **Add**.

Step 3 Create the forced extensions.

a) In the **Device Management** window, under the **Device Settings** , click **Chrome Management**.
b) Click **User Settings**.
c) Scroll down, and in the **Apps and Extensions** section, in the **Force-Installed Apps and Extensions** option, click **Manage Force-Installed Apps**.

Step 4 Install the forced extensions.

a) In the **Force-Installed Apps and Extensions** window, click **Chrome Web Store**.
b) In the **Search** text box, type "Cisco Network Setup Assistant" to locate the extension.

The forced Cisco Network Setup Assistant extension of the Chromebook device requests the certificate from Cisco ISE, and installs the ISE certificate on the Chromebook device. The extension must be configured as force-installed because certificate installation is only allowed for managed devices. If the extension was not installed during the enrollment process, the Cisco ISE certificate cannot be installed.

c) Click **Add** to force install apps.
d) Click **Save**.

Step 5 (Optional) Define the configuration file to install a certificate in a Chromebook device which is shared by multiple users.

a) Copy and paste the following code in a Notepad file and save it to your local disk.

```
{
  "certType": {
    "Value": "system"
  }
}
```

b) Choose **Device Management** > **Chromebook Management** > **App Management**.
c) Click the **Cisco Network Setup Assistant** extension.
d) Click **User Settings** and choose your domain.
e) Click **Upload Configuration File** and choose the .txt file that you saved in your local disk.

Note In order for the Cisco Network Setup Assistant to create a certificate for a device that is shared by multiple users, you must add the Notepad file in the Google Admin Console. Otherwise, the Cisco NSA creates a certificate for a single user.

f) Click **Save**.

Step 6 (Optional) Install a certificate for a single user who does not share the Chromebook.

a) Choose **Device Management** > **Network** > **Certificates**.
b) In the **Certificates** window, click **Add Certificate** and upload the Cisco ISE certificate file.

What to do next

Configure Cisco ISE for Chromebook on board.

Configure Cisco ISE for Chromebook Onboarding

Before you begin

The Cisco ISE administrator must create the required policy. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Sets** window.

Given below is an example of an authorization policy:

Rule Name: Full_Access_After_Onboarding, Conditions: If RegisteredDevices AND Wireless_802.1x AND Endpoints:BYODRegistration EQUALS Yes AND Certificate: Subject Alternative Name Equals RadiusCalling-Station-ID AND Network Access: EAP-Authentication EQUALS EAP-TLS Then CompliantNetworkAccess.

The CompliantNetworkAccess is an authorization result that is configured. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > **Authorization** > **Authorization Profiles** window.

Step 1 Configure the Native Supplicant Profile (NSP) on Cisco ISE.

a) In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > **Client Provisioning** > **Resources**.

The Chromebook device is displayed in the Client Provisioning page for a fresh Cisco ISE installation. However, for upgrade, you should download posture updates. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration > System > Settings > Posture > Updates** window.

b) Click **Add** > **Native Supplicant Profile**.
c) Enter the **Name** and **Description**.
d) In the **Operating System** field, choose **Chrome OS All**.
e) In the **Certificate Template** field, select the required certificate template.
f) Click **Submit**. Observe that the SSID is provisioned via the Google Admin Console and not through the native supplicant provisioning flow.

Step 2 Map the NSP in the Client Provisioning page.

a) In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Client Provisioning**.
b) Define the result.

- Choose the in-built Native Supplicant configuration (Cisco-ISE-Chrome-NSP) in the **Results** of the client provisioning policy.
- Or, create a new rule and ensure to choose the **Result** created for the Chromebook device.

Wipe a Chromebook Device

The Chromebook device must be wiped after the Google Admin Console is configured by the Google Administrator. The Chromebook user must wipe the device, which is a one-time process, to force extensions and configure the network settings. You can refer to the following URL: https://support.google.com/chrome/a/answer/1360642 for further information.

The Chromebook user performs the following steps:

Step 1 Press **Esc-Refresh-Power** key combination. The screen displays a yellow exclamation point (!).

Step 2 Press **Ctrl -D** key combination to begin dev mode, then press **Enter** key. The screen displays a red exclamation point.

Step 3 Press **Ctrl -D** key combination. The Chromebook deletes its local data, returning to its initial state. The deletion takes approximately 15 minutes.

Step 4 When the transition completes, press the **Spacebar** key, then press the **Enter** key to return to verified mode.

Step 5 Enroll the Chromebook before signing in.

What to do next

Enroll Chromebook to the Google Admin Console.

Enroll Chromebook to the Google Admin Console

In order to provision a Chromebook device, the Chromebook user must first enroll in the Google Admin Console page and receive device policies and forced extensions.

Step 1 Turn on the Chromebook device and follow the onscreen instructions until you see the sign on screen. Do not sign in yet.

Step 2 Before signing in to the Chromebook device, press **Ctrl-Alt-E** key combination. The **Enterprise Enrolment** screen appears.

Step 3 Enter your email address and click **Next**.
You will receive the following message: Your device has successfully been enrolled for enterprise management.

Step 4 Click **Done**.

Step 5 Enter the username and password from your Google admin welcome letter, or the username and password for an existing Google Apps user on your account that has eligibility to enroll.

Step 6 Click **Enroll Device**. You will receive a confirmation message that the device has been successfully enrolled.

Note that the Chromebook enrollment is a one-time process.

Connect Chromebook to the Cisco ISE Network for BYOD On Boarding

The procedure is for Dual SSID—To connect to a 802.x network using the EAP-TLS protocol, the Chromebook user performs the following steps:

Note If you are using Dual SSID—When connecting from 802.x PEAP to an EAP-TLS network, connect to the network by entering your credentials in the network supplicant, not the web browser.

Step 1 In the Chromebook, click **Settings**.

Step 2 In the **Internet Connection** section, click **Provisioning Wi-Fi Network**, and then click your network.

Step 3 The credentialed guest portal opens.

a. On the Sign On page, enter the **Username** and **Password**.

b. Click **Sign-on**.

Step 4 In the BYOD Welcome page, click **Start**.

Step 5 In the **Device Information** field, enter a name and a description for your device. For example, "Personal Devices: Jane's Chromebook Used for School or Shared Devices: Library Chromebook #1 or Classroom 1 Chromebook #1".

Step 6 Click **Continue**.

Step 7 Click **Yes** in the **Cisco Network Setup Assistant** dialog box to install the certificate to access the secure network.

If the Google Administrator configured secure Wi-Fi, the network connection should happen automatically. If it does not, choose the secure SSID from the list of available networks.

Chromebook users who have already enrolled in the domain, and have the Cisco Network Setup Assistant extension, can update the extension without waiting for the auto update. Manually update the extension by performing the following steps.

a. In your Chromebook, open the browser and enter the following **URL: chrome://Extensions**.

b. Check the **Developer Mode** check box.

c. Click **Update Extensions Now**.

d. Verify that the Cisco Network Setup Assistant extension version is 2.1.0.35 and higher.

Google Admin Console - Wi-Fi Network Settings

The Wi-Fi network configuration is used to configure an SSID in a customer network or to match the certificate using certificate attributes (for EAP-TLS). When the certificate is installed in the Chromebook, it is synchronized with the Google admin settings. Connection is established only when one of the defined certificate attributes matches the SSID configuration.

Listed below are the mandatory fields, specific to EAP-TLS, PEAP, and Open network flows, which the Google administrator configures to set up the Wi-Fi network in the Google Admin Console page (**Device Management > Network > Wi-Fi > Add Wi-Fi**) for each Chromebook user.

Field	EAP-TLS	PEAP	Open
Name	Enter the name of the network connection.	Enter the name of the network connection.	Enter the name of the network connection.

Field	EAP-TLS	PEAP	Open
Service Set Identifier (SSID)	Enter the SSID (for example, tls_ssid).	Enter the SSID (for example, tls_ssid).	Enter the SSID (for example, tls_ssid).
This SSID Is Not Broadcast	Select the option.	Select the option.	Select the option.
Automatically Connect	Select the option.	Select the option.	Select the option.
Security Type	WPA/WPA2 Enterprise (802.1x)	WPA/WPA2 Enterprise (802.1x)	Open
Extensible Authentication Protocol	EAP-TLS	PEAP	—
Inner Protocol	—	• Automatic • MSCHAP v2 (Select the option) • MD5 • PAP • MSCHAP • GTC	—
Outer Identity	—	—	—
Username	Optional, either set a fixed value or use variables from the user login: ${LOGIN_ ID} or ${LOGIN_EMAIL}.	Enter the PEAP credentials to authenticate against ISE (internal ISE user/AD/other ISE identities) and the Password field.	—
Server Certificate Authority	Select the ISE certificate (imported from Device Management > Network > Certificates).	Select the ISE certificate (imported from Device Management > Network > Certificates).	—
Restrict Access to this Wi-Fi Network by Platform	• Select Mobile Devices. • Select Chromebooks.	• Select Mobile Devices. • Select Chromebooks.	—

Field	EAP-TLS	PEAP	Open
Client Enrollment URL	Enter a URL to which the Chromebook device browser is redirected for users who are not enrolled. Configure ACLs on the Wireless LAN Controller for redirecting unenrolled users.	—	—
Issuer Pattern	An attribute in the certificate. Select at least one attribute from either the Issuer Pattern or Subject Pattern that should match installed certificate attributes. Specify certificate attributes that will be matched with the Chromebook device to accept the certificate. • Common Name: Refers to the Subject field of the certificate or the wildcard domain in the Subject field of the certificate, which must match the FQDN of the node. • Locality: Refers to the test locality (City) that is associated with the certificate subject. • Organization: Refers to the organization name that is associated with the certificate subject. • Organizational Unit: Refers to the organizational unit name that is associated with the certificate subject.	—	—

Field	EAP-TLS	PEAP	Open
Subject Pattern	An attribute in the certificate. Select at least one attribute from either the Issuer Pattern or Subject Pattern that should match installed certificate attributes. Specify certificate attributes that will be matched with the Chromebook device to accept the certificate. • Common Name: Refers to the Subject field of the certificate or the wildcard domain in the Subject field of the certificate, which must match the FQDN of the node. • Locality: Refers to the test locality (City) that is associated with the certificate subject. • Organization: Refers to the organization name that is associated with the certificate subject. • Organizational Unit: Refers to the organizational unit name that is associated with the certificate subject.	—	—
Proxy Settings	• Direct Internet Connection (Selected) • Manual Proxy Configuration • Automatic Proxy Configuration	• Direct Internet Connection (Selected) • Manual Proxy Configuration • Automatic Proxy Configuration	—

Field	EAP-TLS	PEAP	Open
Apply Network	By User	By User	—

Monitor Chromebook Device Activities in Cisco ISE

Cisco ISE provides various reports and logs to view information related to the authentication and authorization of Chromebook devices. You can run these reports either on demand or on regular basis. You can view the authentication method (for example, 802.1x) and authentication protocol (for example, EAP-TLS). In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations** > **RADIUS** > **Live Logs** window. You can also identify the number of end points that are classified as Chromebook devices. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Work Centers** > **Network Access** > **Identities** > **Endpoints** window.

Troubleshoot Chromebook Device Onboarding

This section describes problems that you may encounter while onboarding your Chromebook device.

- Error: Unable to install the extension from the webstore—You cannot install the extension from the webstore. It will be automatically installed on your Chromebook device by the network administrator.
- Error: Completed the installation of the certificate, however, unable to connect to the secure network—Verify on the Admin Console that the installed certificate matches defined Issuer/Subject attribute pattern. You can get information about installed certificate from: chrome://settings/certificates
- Error: Displays an error message "Obtain Network Certificate", when trying to manually connect to the secure network on the Chromebook—Click Get New Certificate, the browser opens and redirects you to the ISE BYOD flow to install the certificate. However, if you are unable to connect to the secure network, verify on the Admin Console that the installed certificate matches the defined Issuer/Subject attribute pattern.
- Error: Clicked Get New Certificate but is forwarded to the www.cisco.com site—User needs to be connected to the provisioning SSID, in order to be redirected to ISE and commence the certificate installation process. Be sure that the correct access list is defined for this network.
- Error: Displays an error message "Only managed devices can use this extension. Contact helpdesk or network administrator"—Chromebook is a managed device and the extension must be configured as a forced install to gain access to the Chrome OS APIs to install the certificate on the device. Although, the extension can be installed manually by downloading it from the Google web store, an unenrolled Chromebook user cannot install the certificate.

  An unenrolled Chromebook device can secure a certificate if the user belongs to the Domain Users group. The extension tracks the domain user on any device. However, the domain user can produce user-based authentication keys for an unenrolled device.
- Error: Unclear of the order in which SSIDs are connected in the Google Admin Console—
  - If several SSIDs (PEAP and EAP-TLS) are configured on the Google Admin Console, after the certificate is installed and the attributes are matched, the Chrome OS automatically connects to the SSID with certificate-based authentication regardless of the order in which the SSIDs are configured.
  - If two EAP-TLS SSIDs match the same attribute, the connection depends on other factors such as signal strength and other network level signals, which cannot be controlled by the user or admin.

- If multiple EAP-TLS certificates are installed on the Chromebook device and all of them match the certificate pattern configured on the Admin Console, the newest certificate will be used for the connection.

Cisco Secure Client

Cisco ISE uses an integrated module in Cisco Secure Client for Cisco ISE posture requirements.

Note Cisco ISE 2.7 Patch 8 and above, Cisco ISE 3.0 Patch 7 and above, Cisco ISE 3.1 Patch 5 and above, Cisco ISE 3.2 Patch 1 and above, and Cisco ISE 3.3 and above releases support both AnyConnect and Cisco Secure Client for Windows, macOS, and Linux operating systems. The following Cisco Secure Client versions are supported for these operating systems:

- Windows: Cisco Secure Client version 5.00529 and later
- macOS: Cisco Secure Client version 5.00556 and later
- Linux: Cisco Secure Client version 5.00556 and later

You can configure both AnyConnect and Cisco Secure Client for your endpoints on these operating systems but only one policy will be considered at run time for an endpoint. In either case, if the endpoint does not connect to a Cisco ISE managed network device, it should block HTTP probing from the endpoint to all Cisco ISE PSNs for TCP port 8905 and Client Provisioning Portal port. The default Client Provisioning Portal port is TCP port 8443.

When you integrate Cisco ISE with the agent, Cisco ISE:

- Serves as a staging server to deploy Cisco Secure Client
- Interacts with the agent posture component for Cisco ISE posture requirements
- Supports deployment of agent profiles, customization and language packages, and OPSWAT library updates

Note When switching network mediums, you must change the default gateway so the posture module can detect the changed network and reassess the client.

Create Agent Configuration

Agent configuration includes agent software and its associated configuration files. This configuration can be used in the client provisioning policy that allows users to download and install agent resources on the clients. If you use both ISE and an ASA to deploy agent, then the configurations must match on both headends.

To push the ISE posture module when connected to a VPN, Cisco recommends that you install the agent through Cisco Adaptive Security Appliance (ASA), which uses the Cisco's Adaptive Security Device Manager (ASDM) GUI tool. ASA does the installation using the VPN downloader. With the download, the ISE posture profile is pushed via ASA, and the discovery host needed for later provisioning the profile is available before

the ISE posture module contacts ISE. Whereas with ISE, the ISE posture module will get the profile only after ISE is discovered, which could result in errors. Therefore, ASA is recommended to push the ISE posture module when connected to a VPN.

Note When Cisco ISE is integrated with ASA, ensure that the Accounting mode is set to **Single** in ASA. Accounting data is sent to only one accounting server in Single mode.

Before you begin

Before configuring an agent configuration object, you must:

1. Download the Agent Headend Deployment package and compliance module from Cisco Software download page.
2. Upload these resources to Cisco ISE (see Add Cisco Provided Client Provisioning Resources from a Local Machine, on page 85).
3. (Optional) Add the customization and localization bundles (see Add Customer Created Resources for Agent from a Local Machine, on page 86).
4. Configure an posture agent profile (see Create a Posture Agent Profile, on page 106).

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > **Client Provision** > **Resources**.

Step 2 Click **Add** to create an agent configuration.

Step 3 Choose **Agent Configuration**.

Step 4 Choose an Agent Package, which you previously uploaded. For example, cisco-secure-client-win-x.x.xxxxx-webdeploy-k9.pkg.

Step 5 Enter the name for the current Agent Configuration. For example, AC Config xxx.x.xxxxx.x.

Step 6 Choose the compliance module, which you previously uploaded. For example, cisco-secure-client-win-x.x.xxxxx-isecompliance-predeploy-k9.msi.

Step 7 Check one or more Agent module check boxes. For example, choose one or more modules from the following: ISE Posture, VPN, Network Access Manager, Web Security, AMP Enabler, ASA Posture, Start Before Log on (only for Windows OS), and Diagnostic and Reporting Tool.

Note Un-checking the VPN module under Agent Module Selection does not disable the VPN tile in the provisioned client. You must configure VPNDisable_ServiceProfile.xml to disable the VPN tile on agent GUI. In a system where agent is installed at the default location, you can find this file under C:\Program Files\Cisco. If agent is installed at a different location, then the file will be available under <Agent Installed path>\Cisco.

Step 8 Choose agent profiles for selected agent modules. For example, ISE Posture, VPN, NAM, and Web Security.

Step 9 Choose agent customization and localization bundles.

Step 10 Click **Submit**.

Create a Posture Agent Profile

Use this procedure to create posture agent profile, where you can specify parameters that define the agent behavior for the posture protocol.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > **Client Provisioning** > **Resources**.

Step 2 Click **Add**.

Step 3 Choose **Agent Posture Profile**.

Step 4 Enter **Name** of the profile.

Step 5 Configure parameters for the following:

- Cisco ISE posture agent behavior
- Client IP Address Changes
- Cisco ISE posture protocol

Step 6 Click **Submit**.

Client IP Address Refresh Configuration

The following table describes the fields in the Agent Posture Profile window, which allows you to configure parameters for the client to renew or refresh its IP address after VLAN change. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Resilts** > **Client Provisioning** > **Resources** > **Add** > **Agent Posture Profile**.

Field Name	Default Value	Usage Guidelines
VLAN detection interval	0, 5	This setting is the interval at which the agent check for the VLAN change. For the Mac OS X agent, the default value is 5. By default, the access to authentication VLAN change feature is enabled with VlanDetectInteval as 5 seconds for Mac OS X. The valid range is 5 to 900 seconds. 0 —Access to Authentication VLAN change feature is disabled. 1 to 5—Agent sends an Internet Control Message Protocol (ICMP) or Address Resolution Protocol (ARP) query every 5 seconds. 6 to 900—An ICMP or ARP query is sent every x seconds.

Field Name	Default Value	Usage Guidelines
Enable VLAN detection without UI (Not applicable for a Mac OS X client)	No	This setting enables or disables VLAN detection even when the user is not logged in. No—VLAN detect feature is disabled. Yes—VLAN detect feature is enabled.
Retry detection count	3	If the Internet Control Message Protocol (ICMP) or Address Resolution Protocol (ARP) polling fails, this setting configures the agent to retry x times before refreshing the client IP address.
Ping or ARP	0 The valid range is 0 to 2.	This setting specifies the method used for detecting the client IP address change. 0—Poll using ICMP 1—Poll using ARP 2—Poll using ICMP first, then (if ICMP fails) ARP
Maximum timeout for ping	1 The valid range is 1 to 10 seconds.	Poll using ICMP, and if there is no response within the specified time, then declare an ICMP polling failure.
Enable agent IP refresh	Yes (Default)	This setting specifies whether or not the client machine to renew or refresh its IP address after the switch (or WLC) changes the VLAN for the login session of the client on the respective switch port.
DHCP renew delay	0 The valid range is 0 to 60 seconds.	This setting specifies that the client machine waits before attempting to request for a new IP address from the network DHCP server.
DHCP release delay	0 The valid range is 0 to 60 seconds.	The setting specifies that the client machine waits before releasing its current IP address.

Note Merge parameter values with existing agent profile settings or overwrite them to appropriately configure clients on Windows and Mac OS X clients for refreshing IP addresses.

Posture Protocol Settings

The following table describes the fields in the Agent Posture Profile window, which allows you to configure posture protocol settings for agent. For more information, see the Cisco AnyConnect Secure Mobility Client Administrator Guide for your version of agent.

Field Name	Default Value	Usage Guidelines
PRA Retransmission Time	120 seconds	This is the agent retry period if there is a Passive Reassessment communication failure.
Retransmission Delay	60 seconds	Time (in seconds) to wait before retrying.
Retransmission Limit	4	Number of retries allowed for a message.
Discovery Host	—	Enter any IP address or FQDN that is routed through a NAD. The NAD detects and redirects that HTTP traffic to the Client Provisioning portal.
Discovery Backup Server List	—	Choose the PSNs from the drop-down list. Agent probes this server list to find the PSN node on which posture must be performed. If you don't select any PSN, all the PSNs in the node group or cluster are sent to agent as the backup server list.
Server Name Rules	—	A list of wildcarded, comma-separated names that defines the servers that the agent can connect to.
Call Home List	—	Enter a comma-separated list of IP addresses and ports with colon in between the IP address and the port.
Back-off Timer	30 sec	This setting enables the agent to continuously to reach the discovery targets (redirection targets and previously connected PSNs) by sending the discovery packets till this maximum time limit is reached. The valid range is from 10 to 600 seconds.

Continuous Endpoint Attribute Monitoring

You can use the agent to continuously monitor different endpoint attributes to ensure that dynamic changes are observed during posture assessment. This improves the overall visibility of an endpoint and helps you create posture policies based on their behavior. The agent monitors applications that are installed and running on an endpoint. You can turn on and off the feature and configure how often the data should be monitored. By default, data is collected every 5 minutes and is stored in the database. During initial posture, the agent reports a complete list of running and installed applications. After initial posture, the agent scans the applications

every X minute and sends the differences from the last scan to the server. The server displays the complete list of running and installed applications.

Posture State Synchronization

Sometimes, Cisco ISE might move a client or an endpoint to Pending state because of a change in network configuration. However, the agent cannot detect this change, and retains the client or endpoint in Compliant state. Thus, there is a mismatch in posture status and ideally, Cisco ISE must be probed in this scenario to obtain the correct posture status. You can do this by configuring the agent to probe Cisco ISE at specified intervals so that when the posture status of a client or endpoint is pending, this probing will prevent the client or endpoint from being stuck in Pending state in Cisco ISE.

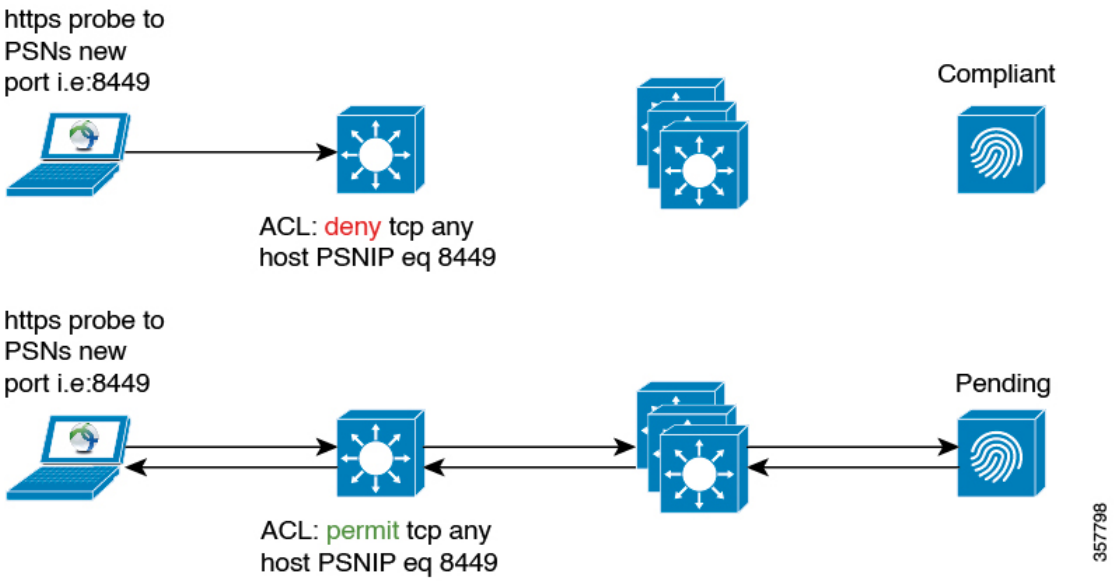
The posture state synchronization is supported for Windows, Linux, and MacOS clients.

The posture state synchronization includes the following steps:

1. The client tries to connect to the network.
2. The PSN performs the posture flow. The endpoint is moved to Compliant state if the client is compliant with the posture policies.
3. The agent receives Posture Probing Backup List and Posture State Synchronization Interval configuration details from Cisco ISE.
4. The agent starts probing Cisco ISE, at specified intervals.

   For example, Cisco ISE shows the posture status as pending and the agent shows the posture status as Compliant. When the agent probes Cisco ISE and learns the new state, a reassesment could be triggered.

Figure 5: Posture State Synchronization



Note If the status of a client has moved to **Pending** for whatever reason, the agent will receive a probing request from the client. It will probe and receive the correct client state from Cisco ISE and then move the client to the correct state.

Configure Posture State Synchronization

Step 1 Configure **Posture Probing Backup List** and **Posture State Synchronization Interval** in the **Agent Posture Profile**. To do this:

a) In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy > Policy Elements > Results > Client Provisioning > Resources**.

b) From the **Add** drop-down list, choose **Agent Posture Profile**.

c) In the **Agent Behavior** area, configure the following settings:

- **Posture Probing Backup List**: From this drop-down list, choose the PSNs that agent must probe for endpoint posture compliance status. You can choose up to six PSNs.

  Agent sends probes to these PSNs to check whether the posture compliance status for an endpoint is still valid. If you don't choose any PSN, the connected PSN and any two backup servers are used as backups for posture state synchronization.

- **Posture State Synchronization Interval**: Define the frequency at which the agent synchronizes the posture status with Cisco ISE. The valid range is from 0 to 300. If you enter 0, posture state synchronization probing is disabled. The posture state synchronization port must be blocked for compliant authorization profiles when this value is greater than 0.

Step 2 Configure port 8449 for bidirectional communication. To do this:

a) In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration > Device Portal Management > Client Provisioning Portals > Portal Behavior and Flow Settings**.

b) Click **Portal Settings**.

c) In the **Bidirectional Port** field, ensure that port 8449 is set for bidirectional communication.

By default, port 8449 is used for bidirectional communication.

Step 3 Configure an ACL to block posture state synchronization probe from reaching Cisco ISE when the client posture status is compliant. To do this:

a) In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy > Policy Elements > Results > Authorization > Downloadable ACLs**.

b) Configure the ACL.

Ensure that only the clients in Pending state are allowed to reach the configured PSNs over the bidirectional port. This will avoid unwanted traffic from clients that are in Compliant state. The following is an example of ACL:

```
deny tcp any host <ip address> eq 8449
deny tcp any host <ip address> eq 8449
deny tcp any host <ip address> eq 8449
permit ip any any
```

If ACL is not configured, the Posture Configuration Detection alarm is triggered on the Cisco ISE dashboard. ACL should only be configured on policy sets that are complaint. The main purpose of this alarm is to prevent heavy traffic to Cisco ISE.

Note Ensure that the firewall does not block the communication on the corresponding port when a client is in Pending state.

Cisco Web Agent

The Cisco Web Agent provides temporal posture assessment for client machines.

Users can launch the Cisco Web Agent executable, which installs the Web Agent files in a temporary directory on the client machine via ActiveX control or Java applet.

After users log in to the Cisco Web Agent, the Web Agent gets the requirements that are configured for the user role and the operating system from the Cisco ISE server, checks the host registry, processes, applications, and services for required packages and sends a report back to the Cisco ISE server. If requirements are met on the client machine, the user is allowed network access. If requirements are not met, the Web Agent presents a dialog to the user for each requirement that is not satisfied. The dialog provides the user with instructions and the action to take for the client machine to meet the requirement. Alternatively, if the specified requirements are not met, users can choose to accept the restricted network access while they try to remediate the client system so that it meets requirements for the user login role.

Note ActiveX is supported only on the 32-bit versions of Internet Explorer. You cannot install ActiveX on a Firefox web browser or on a 64-bit version of Internet Explorer.

Configure Client Provisioning Resource Policies

For clients, the client provisioning resource policies determine which users receive which version of resources (agents, agent compliance modules, and agent customization packages or profiles) from Cisco ISE upon login and user session initiation.

For agent, resources can be selected from the **Client Provisioning Resources** window to create an agent configuration that you can use in the **Client Provisioning Policy** window. Agent configuration specifies the agent software and its association with different configuration files that includes agent binary package for Windows, macOS, and Linux clients, compliance module, module profiles, customization, and language packages.

Before you begin

- Before you can create effective client-provisioning resource policies, ensure that you have added resources to Cisco ISE. When you download the agent compliance module, it always overwrites the existing one, if any, available in the system.

- Check the native supplicant profile that is used in the client provisioning policy and ensure that the wireless SSID is correct. For iOS devices, if the network that you are trying to connect is hidden, check the **Enable if target network is hidden** check box in the **iOS Settings** area.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Client Provisioning**.

Step 2 From the **Behavior** drop-down list, choose one of the following options:

- **Enable**: Ensures Cisco ISE uses this policy to help fulfill client-provisioning functions when users log in to the network and conform to the client-provisioning policy guidelines.
- **Disable**: Cisco ISE does not use the specified resource policy to fulfill client-provisioning functions.
- **Monitor**: Disables the policy and "watches" the client-provisioning session requests to see how many times Cisco ISE tries to invoke based on the "Monitored" policy.

Step 3 Enter a name for the new resource policy in the **Rule Name** text box.

Step 4 Specify one or more Identity Groups to which a user who logs into Cisco ISE might belong.

You can choose to specify the **Any** identity group type, or choose one or more groups from a list of existing Identity Groups that you have configured.

Step 5 Use the **Operating Systems** field to specify one or more operating systems that might be running on the client machine or device through which the user is logging into Cisco ISE.

Note Though the option to select macOS 10.6, 10.7, and 10.8 is available in the **Client Provisioning** window in Cisco ISE GUI, these versions are not supported by the agent.

Step 6 In the **Other Conditions** field, specify a new expression that you want to create for this particular resource policy.

Step 7 For client machines, use the **Agent Configuration** option to specify which agent type, compliance module, agent customization package, and profile to make available and provision on the client machine.

It is mandatory to include the client provisioning URL in authorization policy to enable the agent to popup in the client machines. This prevents request from any random clients and ensures that only clients with proper redirect URL can request for posture assessment.

Step 8 Click **Save**.

What to do next

After you have successfully configured one or more client provisioning resource policies, you can start to configure Cisco ISE to perform posture assessment on client machines during login.

Configure Cisco ISE Posture Agent in the Client Provisioning Policy

For client machines, configure the agent type, compliance module, agent customization package, and/or profile to make available and provision for users to download and install on the client machine.

Before you begin

You must add client provisioning resources for agent in Cisco ISE.

Step 1 Choose an available agent from the **Agent** drop-down list and specify whether the agent upgrade (download) defined here is mandatory for the client machine by enabling or disabling the **Is Upgrade Mandatory** option, as appropriate.

The **Is Upgrade Mandatory** setting only applies to agent downloads. Agent profile, compliance module, and agent customization package updates are always mandatory.

Step 2 Choose an existing agent profile from the **Profile** drop-down list.

Step 3 Choose an available compliance module to download to the client machine using the **Compliance Module** drop-down list.

Step 4 Choose an available agent customization package for the client machine from the **Agent Customization Package** drop-down list.

Configure Native Supplicants for Personal Devices

Employees can connect their personal devices to the network directly using native supplicants, which are available for Windows, Mac OS, iOS, and Android devices. For personal devices, specify which Native Supplicant configuration to make available and provision on the registered personal device.

Before you begin

Create native supplicant profiles so that when user log in, based on the profile that you associate with that users authorization requirements, Cisco ISE provides the necessary supplicant provisioning wizard to set up the users personal devices to access the network.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose Choose **Policy** > **Client Provisioning**.

Step 2 Choose **Enable**, **Disable**, or **Monitor** from the behavior drop-down list.

Step 3 Enter a name for the new resource policy in the Rule Name text box.

Step 4 Specify the following:

- Use the **Identity Groups** field to specify one or more Identity Groups to which a user who logs into Cisco ISE might belong.
- Use the **Operating System** field to specify one or more operating systems that might be running on the personal device through which the user is logging into Cisco ISE.
- Use the **Other Conditions** field to specify a new expression that you want to create for this particular resource policy.

Step 5 For personal devices, use **Native Supplicant Configuration** to choose the specific **Configuration Wizard** to distribute to these personal devices.

Step 6 Specify the applicable **Wizard Profile** for the given personal device type.

Step 7 Click **Save**.

Client Provisioning Reports

You can access the Cisco ISE monitoring and troubleshooting functions to check on overall trends for successful or unsuccessful user login sessions, gather statistics about the number and types of client machines logging into the network during a specified time period, or check on any recent configuration changes in client provisioning resources.

Client Provisioning Requests

The **Operations** > **Reports** > **ISE Reports** > **Endpoints and Users** > **Client Provisioning** report displays statistics about successful and unsuccessful client provisioning requests. When you choose **Run** and specify one of the preset time periods, Cisco ISE combs the database and displays the resulting client provisioning data.

Supplicant Provisioning Requests

The **Operations** > **Reports** > **ISE Reports** > **Endpoints and Users** > **Supplicant Provisioning** window displays information about recent successful and unsuccessful user device registration and supplicant provisioning requests. When you choose **Run** and specify one of the preset time periods, Cisco ISE combs the database and displays the resulting supplicant provisioning data.

The Supplicant Provisioning report provides information about a list of endpoints that are registered through the device registration portal for a specific period of time, including data like the Logged at Date and Time, Identity (user ID), IP Address, MAC Address (endpoint ID), Server, profile, Endpoint Operating System, SPW Version, Failure Reason (if any), and the Status of the registration.

Client Provisioning Event Logs

You can search event log entries to help diagnose a possible problem with client login behavior. For example, you may need to determine the source of an issue where client machines on your network are not able to get client provisioning resource updates upon login. You can use logging entries for Posture and Client Provisioning Audit and Posture and Client Provisioning Diagnostics.

Portal Settings for Client Provisioning Portals

To view this window, click the **Menu** icon (☰) and choose **Administration** > **Device Portal Management** > **Client Provisioning Portals** > **Create, Edit, Duplicate, or Delete** > **Portal Behavior and Flow Settings**.

Portal Settings

- **HTTPS Port**: Enter a port value between 8000 to 8999; the default value is 8443 for all the default portals, except the **Blocked List** Portal, which is 8444. If you upgraded with port values outside this range, they are honored until you make any change to this page. If you make any change to this page, you must update the port setting to comply with this restriction.
- **Allowed Interfaces**: Select the PSN interfaces which can run a portal. Only a PSN with an available allowed interface on a PSN can create a portal. You can configure any combination of physical and

bonded interfaces. This is a PSN-wide configuration; all portals can only run on these interfaces, this interface configuration is pushed to all the PSNs.

- You must configure the Ethernet interfaces using IP addresses on different subnets.
- The interfaces you enable here must be available on all your PSNs, including VM-based ones when Policy Services turned on. This is required because any of these PSNs can be used for a redirect at the start of the guest session.
- The portal certificate Subject Name/Alternate Subject Name must resolve to the interface IP.
- Configure ip host x.x.x.x yyy.domain.com in ISE CLI to map secondary interface IP to FQDN, which will be used to match Certificate Subject Name/Alternate Subject Name.
- If only the bonded NIC is selected, when the PSN attempts to configure the portal it first attempts to configure the Bond interface. If that is not successful, perhaps because there was no bond set upon that PSN, then the PSN logs an error and exits. It will NOT attempt to start the portal on the physical interface.
- **NIC Teaming** or bonding is an O/S configuration option that allows you to configure two individual NICs for high availability (fault tolerance). If one of the NICs fails, the other NIC that is part of the bonded connection continues the connection. A NIC is selected for a portal based on the portal settings configuration:
  - If both physical NICs and the corresponding bonded NIC are configured - When the PSN attempts to configure the portal, it first attempts to connect to the Bond interface. If that is not successful, perhaps because there was no bond setup on that PSN, then the PSN attempts to start the portal on the physical interface.

- **Certificate Group Tag**: Select the group tag of the certificate group to use for the portal's HTTPS traffic.
- **Authentication Method**: Choose which identity source sequence (ISS) or Identity Provider (IdP) to use for user authentication. The ISS is a list of Identity Stores that are searched in sequence to verify user credentials. Some examples include: Internal Guest Users, Internal Users, Active Directory, and LDAP.

  Cisco ISE includes a default client provisioning Identity Source Sequence for Client Provisioning Portals, Certificate_Request_Sequence.
- **Fully Qualified Domain Name (FQDN)**: Enter at least one unique FQDN and/or hostname for your Client Provisioning portal. For example, you can enter provisionportal.yourcompany.com, so that when the user enters either of those into a browser, they will reach the Client Provisioning Portal.
  - Update DNS to ensure that the FQDN of the new URL resolves to a valid Policy Services Node (PSN) IP address. Optionally, this address could point to a load balancer virtual IP address that serves a pool of PSNs.
  - To avoid certificate warning messages due to name mismatches, include the FQDN of the customized URL, or a wildcard, in the subject alternative name (SAN) attribute of the local server certificate of the Cisco ISE PSN.

Note For Client Provisioning without URL redirection, the portal name that is entered in the Fully Qualified Domain Name (FQDN) field must be configured in the DNS configuration. This URL must be communicated to the users to enable Client Provisioning without URL redirection.

- **Idle Timeout**: Enter the time in minutes that you want Cisco ISE to wait before it logs out the user if there is no activity in the portal. The valid range is from 1 to 30 minutes..

Note In the Client Provisioning Portal, you can define the port number and the certificate so that the host allows you to download the same certificate for Client Provisioning and Posture. If the portal certificate is signed by the officials certificate authority, you will not receive any security warning. If the certificate is self-signed, you will receive one security warning for both the portals and Cisco Agent Posture component.

Login Page Settings

- Enable Login: Select this check box to enable the login step in the Client Provisioning Portal
- Maximum failed login attempts before rate limiting: Specify the number of failed login attempts from a single browser session before Cisco ISE starts to artificially slow down the rate at which login attempts can be made, preventing additional login attempts. The time between attempts after this number of failed logins is reached is specified in **Time between login attempts when rate limiting**.
- Time between login attempts when rate limiting: Set the length of time in minutes that a user must wait before attempting to log in again, after failing to log in the number of times defined in **Maximum failed login attempts before rate limiting**.
- Include an AUP (on page/as link): Display your company's network-usage terms and conditions, either as text on the page currently being displayed for the user or as a link that opens a new tab or window with AUP text.
- Require acceptance: Require users to accept an AUP before they can access the portal. The **Login** button is not enabled unless the user accepts the AUP. If users do not accept the AUP, they will not be able to access the portal.
- Require scrolling to end of AUP: This option displays only if **Include an AUP on page** is enabled. Ensure that the user has read the AUP completely. The **Accept** button activates only after the user has scrolled to the end of the AUP.

Acceptable Use Policy (AUP) Page Settings

- Include an AUP: Display your company's network-usage terms and conditions on a separate page to the user.
- Require scrolling to end of AUP: Ensure that the user has read the AUP completely. The Accept button activates only after the user has scrolled to the end of the AUP.
- On first login only: Display an AUP when the user logs into the network or portal for the first time only.
- On every login: Display an AUP each time the user logs into the network or portal.

- Every _____ days (starting at first login): Display an AUP periodically after the user first logs into the network or portal.

Post-Login Banner Page Settings

Include a Post-Login Banner page: Display additional information after the users successfully log in and before they are granted network access.

Change Password Settings

Allow internal users to change their own passwords: Allow employees to change their passwords after they log in to the Client Provisioning Portal. This only applies to employees whose accounts are stored in the Cisco ISE database and not to those stored in external databases, such as Active Directory or LDAP.

HTML Support for Client Provisioning Portal Language Files

To view this window, click the **Menu** icon (☰) and choose **Administration** > **Device Portal Management** > **Client Provisioning Portals** > **Edit** > **Portal Page Customization** > **Pages**. You can use the **View HTML Source** icon in the mini-editor and add HTML code in your content.

These dictionary keys in the portal's language properties files support HTML in their text.

Note This is not a complete list of the dictionary keys in the files.

- key.guest.ui_client_provision_agent_installed_instructions_without_java_message
- key.guest.ui_contact_instruction_message
- key.guest.ui_success_message
- key.guest.ui_client_provision_unable_to_detect_message
- key.guest.ui_client_provision_instruction_message
- key.guest.ui_client_provision_agent_installation_message
- key.guest.ui_client_provision_posture_agent_check_message
- key.guest.ui_vlan_instruction_message
- key.guest.ui_client_provision_agent_installation_instructions_with_no_java_message
- key.guest.ui_success_instruction_message
- key.guest.ui_vlan_optional_content_1
- key.guest.ui_vlan_optional_content_2
- key.guest.ui_contact_optional_content_2
- key.guest.ui_contact_optional_content_1
- key.guest.ui_contact_optional_content_1

- key.guest.ui_client_provision_posture_check_compliant_message
- key.guest.ui_client_provision_optional_content_2
- key.guest.ui_client_provision_optional_content_1
- key.guest.ui_error_optional_content_2
- key.guest.ui_error_optional_content_1
- key.guest.ui_client_provision_posture_check_non_compliant_message
- key.guest.ui_vlan_install_message
- key.guest.ui_success_optional_content_1
- key.guest.ui_success_optional_content_2
- key.guest.ui_client_provision_posture_agent_scan_message