ISE Posture Prescriptive Deployment Guide

Timothy Abbott **Cisco Employee**

on 09-06-2018 08:38 AM - edited on 11-20-2023 09:57 AM by thomas

ISE Posture Prescriptive Deployment Guide

Version 1.0

Tim Abbott

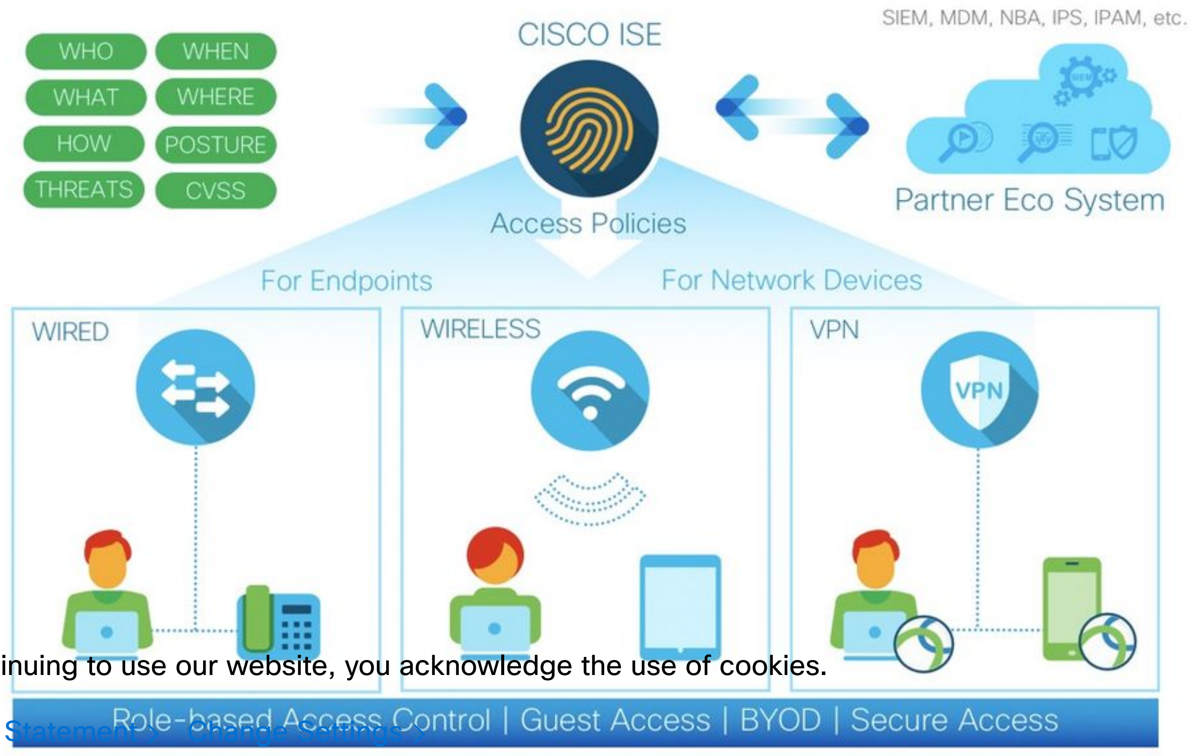
Technical Marketing Engineer, Cisco Systems, Inc.

Cisco ISE Posture Configuration Video Series on YouTube

Table of Contents

Introduction

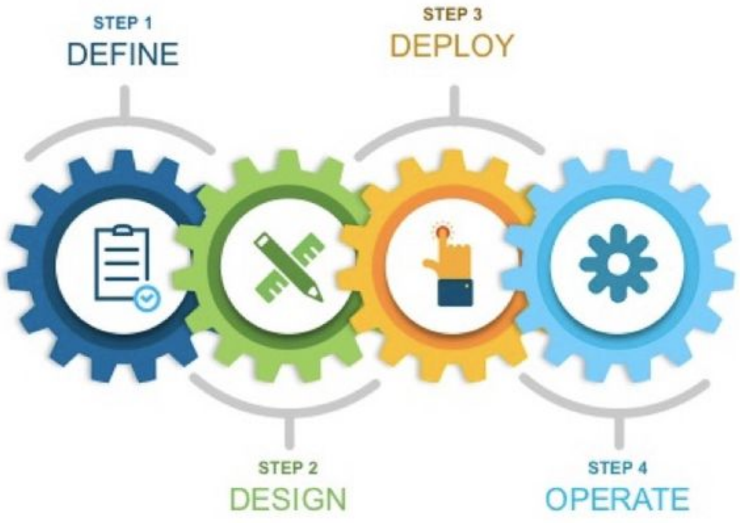
About Cisco Identity Services Engine (ISE)



Cisco ISE is a leading, identity-based network access control and policy enforcement system. It is a common policy engine for controlling, endpoint access and network device administration for enterprises. ISE allows an administrator to centrally control access policies for wired, wireless, and VPN endpoints in a network. ISE builds context about the endpoints that include users and groups (Who), device type (What), access time (When), access location (Where), access type (Wired/Wireless/VPN) (How), threats, and vulnerabilities. By sharing vital contextual data with technology partner integrations and the implementation of the Cisco TrustSec® policy for software-defined segmentation, ISE transforms a network from a conduit for data into a security enforcer that accelerates the time-to-detection and time-to-resolution of network threats.

About This Guide

This guide is intended to provide technical guidance to design, deploy and operate Cisco Identity Services Engine (ISE) for posture assessment. The first half of the document focuses on the planning and design activities, the other half covers specifics of configurations and operations. There are four major sections in this document. The initial, **define** part talks about defining the problem area, planning for deployment, and other considerations. Next, in the **design** section, you will see how to design for posture assessment. Third, in the **deploy** part, the various configuration and best practice guidance will be provided. Lastly, in the **operate** section, you will learn how to manage a posture deployment with Cisco ISE. Before you begin, be sure you have the correct licensing required for posture assessment by reviewing the ISE Ordering Guide. You will also want to ensure you have any required external resource such as Active Directory configured and operating properly.

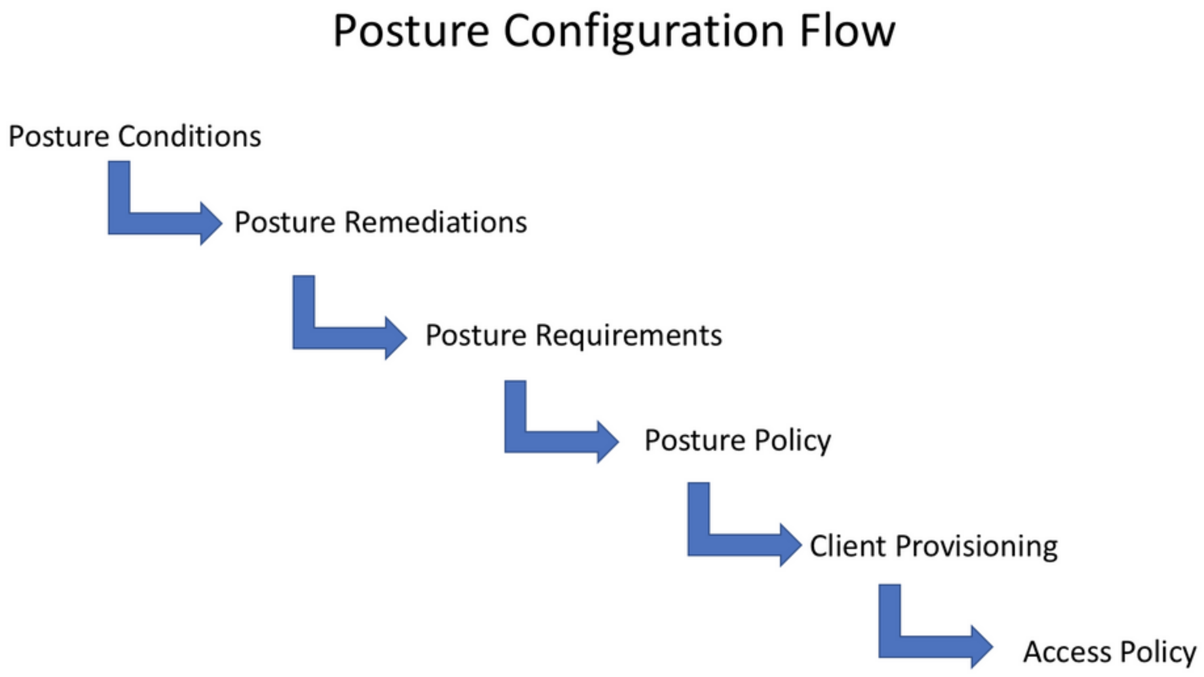


Define

Posture Configuration Flow

Configuring posture assessment in ISE requires several components to be taken into consideration: Conditions, Remediations, Requirements, Posture Policy, Client Provisioning and Access Policy. Following the below posture configuration flow will ensure that each required section to configuring ISE for posture assessment will be addressed. Posture conditions are the set of rules in our security policy that define a compliant endpoint. Some of the these items include the installation of a firewall, anti-virus software, anti-malware, hotfixes, disk encryption and more. Once posture conditions are defined, posture remediations (if required) can be configured. Posture remediations are the methods AnyConnect will handle endpoints that are out of compliance. Some remediations can be automatically resolved through AnyConnect while other might be resolved manually by the end user. Posture requirements are the immediate actions steps taken by AnyConnect when an endpoint is out of compliance. An endpoint is deemed compliant if it satisfies all the posture conditions. Once configured, posture requirements can then be reference by posture policy for compliance enforcement. Client provisioning is the policy used to determine the version of AnyConnect used as well as the compliance module that will be installed on the endpoint during the provisioning process. The compliance module is a library that the posture agent uses to determine if the endpoint is in compliance with defined posture conditions.

Lastly, access policy will enable our posture policy and define what form of policy the endpoint will be subjected to if it is compliant, non-compliant or requires provisioning of AnyConnect.



Security Policy Example

Now that we understand the configuration flow, we need to review our deployment options. Most critical is defining security policy. Without a predefined security policy, we will not be able to configure ISE posture to protect our endpoints and network. While ISE contains a number options for checking endpoint compliance, this guide will use the following security policy example for Windows 10 endpoints:

- Ensure Windows firewall is enabled
- Check for USB attached devices
- Anti-malware installation
- Critical patch installation
- Application installation

To enforce our example security policy, we will use the following components:

- Identity Services Engine 2.4
- AnyConnect 4.5

- AnyConnect Compliance Module 4.2.1134.0

Design

Agent Considerations

Depending on your security policy, you will want to select the correct agent for your deployment. Since this guide will use ISE 2.4, there are a few options to consider. Mainly, there are three types of agent that can be used. Each one has its advantages and disadvantages in term of posture options.

Temporal Agent

The temporal agent is relatively new to ISE and is designed to be dissolvable. That means no permanent software will be installed on the endpoint. The ability to not force software installation on the endpoints is a clear advantage for the temporal agent. Ideally, you can use the temporal agent on guest or contractor endpoints. The disadvantage of using the temporal agent is that it is limited in the number of posture conditions it currently supports. The temporal agent only requires an ISE Apex license since it does not require AnyConnect. Use it for only the most basic of posture checks.

Stealth AnyConnect

The Stealth AnyConnect posture agent is also relatively new and is design to be a permanent installation on the endpoint but in a "headless" configuration. The advantages of the Stealth AnyConnect posture agent is that it supports basically all the posture conditions as the AnyConnect agent however it will run as a background process to the end-user. There is no UI for the Stealth AnyConnect posture. However, if you include other modules such as AMP Enabler or VPN, you will see the UI. The Stealth AnyConnect posture agent requires an AnyConnect Apex license in addition to an ISE Apex license.

AnyConnect

The AnyConnect posture agent is the replacement for the NAC agent as well as OS X agent. It has the most support for posture conditions as well as automatic remediation support and passive reassessment. Where as the NAC agent could automatically be downloaded from Cisco, AnyConnect cannot. Since AnyConnect is a separate product from ISE, It requires entitlement to be downloaded from Cisco. Lastly, it also requires an AnyConnect Apex license in addition to the ISE Apex license requirement whether it is configured for stealth use or not.

Windows Posture Assessment Options

	Temporal Agent	Stealth AnyConnect	AnyConnect
Posture Conditions	Supported Conditions: • AM Installation • Firewall Installation • Application Inventory • Hardware Inventory • USB Check • AV Installation • AV version / date • AS Installation • AS version / date • Application / File Check • Service packs / Hotfixes • Process / Registry Check	Supported Conditions: • AM Installation • Firewall Installation • Application Inventory • Hardware Inventory • USB Check • AV Installation • AV version / date • AS Installation • AS version / date • Application / File Check • Service packs / Hotfixes • Process / Registry Check • Patch Management • Disk Encryption • Service Condition • Registry Condition • Dictionary Condition	Supported Conditions: • AM Installation • Firewall Installation • Application Inventory • Hardware Inventory • USB Check • AV Installation • AV version / date • AS Installation • AS version / date • Application / File Check • Service packs / Hotfixes • Process / Registry Check • Patch Management • Disk Encryption • Service Condition • Registry Condition • Dictionary Condition
Remediation Actions	Manual Remediations	Partial Automatic Remediation: File, Link, WSUS Show UI, PM activate UI, Message Text. Manual remediation not supported.	Both Automatic and Manual Remediation supported

Passive Reassessment	None	Supported	Supported

macOS Posture Assessment Options

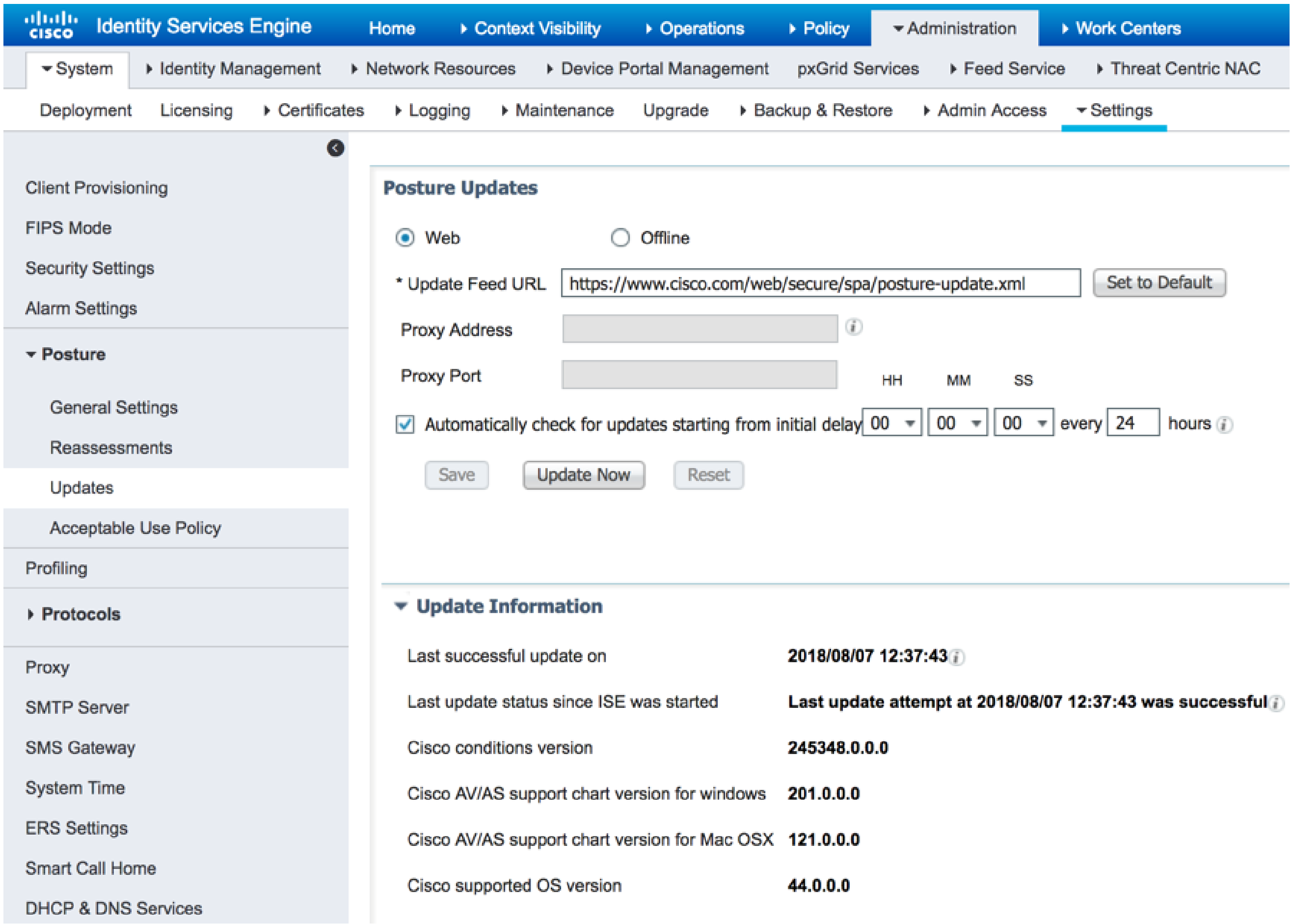
	Temporal Agent	Stealth AnyConnect	AnyConnect
Posture Conditions	Unsupported Conditions: • Service Condition-macOS –System Daemon check • Service Condition-macOS –Daemon or User Agent check • PM–Up to Date check • PM–Enabled check • DE–Encryption Location based check	Supported Conditions: • AM Installation • Firewall Enabled • Application Inventory • Hardware Inventory • AV Installation • AV version / date • AS Installation • AS version / date • Application Check • Plist Check • File Check • Patch Management • Service packs / Hotfixes • Disk Encryption • Service Condition • Dictionary Condition	Supported Conditions: • AM Installation • Firewall Enabled • Application Inventory • Hardware Inventory • AV Installation • AV version / date • AS Installation • AS version / date • Application Check • Plist Check • File Check • Patch Management • Service packs / Hotfixes • Disk Encryption • Service Condition • Dictionary Condition
Remediation Actions	Not Supported	Unsupported: Manual, Launch program, File condition, Patch management, USB	Unsupported: Manual, Launch program, File condition, Patch management, USB
Passive Reassessment	Not Supported	Not Supported	Not Supported

Deploy

Posture Updates

Posture updates include a set of predefined checks, rules, and support charts for antivirus and anti-spyware for both Windows and Macintosh 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. Lastly, ISE posture updates can be configured for offline updates for those deployments that do not have internet access. Simply download the zip file from Cisco and upload them manually into the system as required.

Step 1	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 on the Posture Updates page.
Step 5	Click Update Now to download updates from Cisco.
Step 6	Click OK to continue with other tasks on Cisco ISE. Once updated, the Posture Updates page displays the current Cisco updates version information as a verification of an update under Update Information section in the Posture Updates page.



Posture Updates

● Web ○ Offline

* Update Feed URL https://www.cisco.com/web/secure/spa/posture-update.xml

Proxy Address

Proxy Port

☑ Automatically check for updates starting from initial delay 00 HH 00 MM 00 SS every 24 hours

Update Information

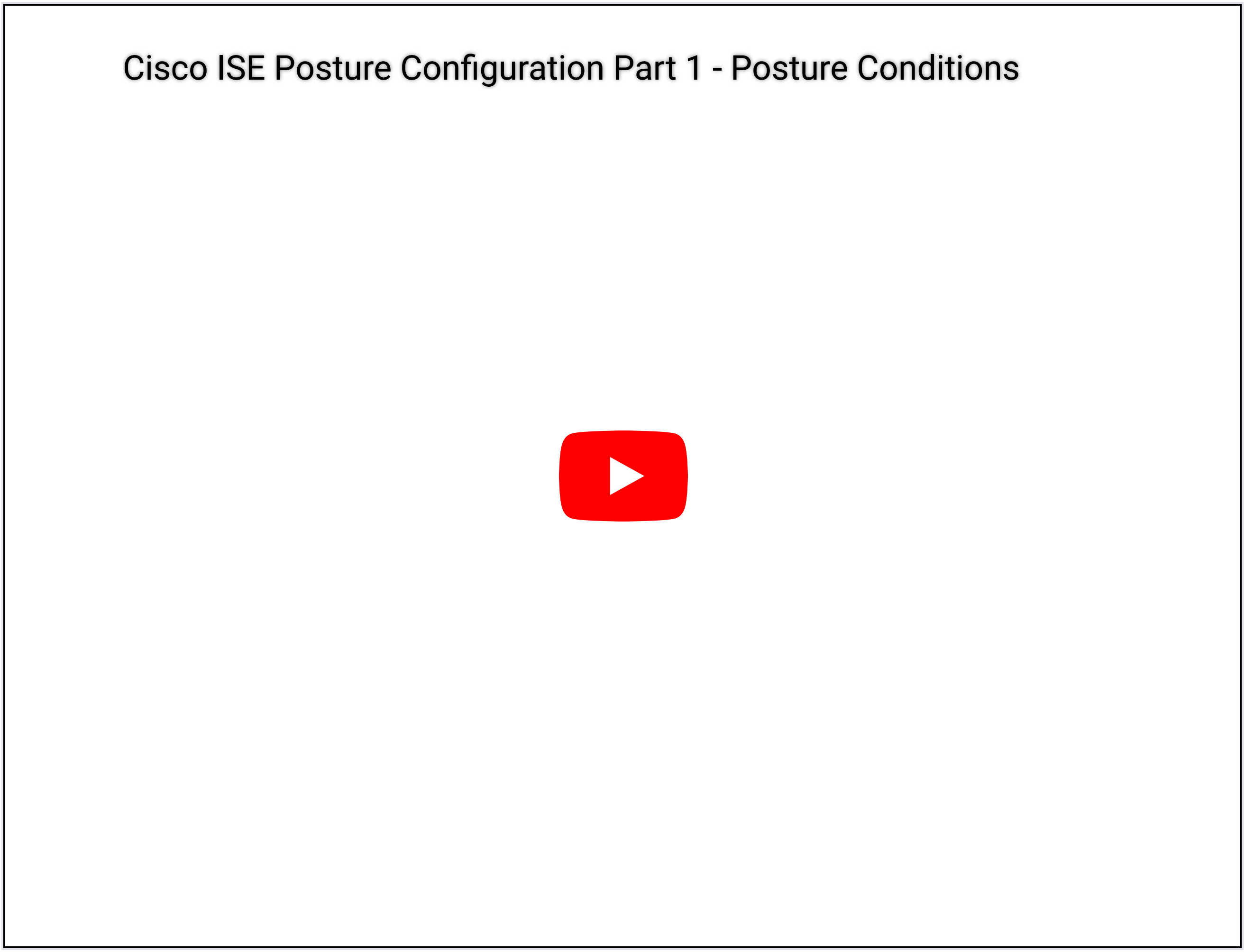
Last successful update on	2018/08/07 12:37:43
Last update status since ISE was started	Last update attempt at 2018/08/07 12:37:43 was successful
Cisco conditions version	245348.0.0.0
Cisco AV/AS support chart version for windows	201.0.0.0
Cisco AV/AS support chart version for Mac OSX	121.0.0.0
Cisco supported OS version	44.0.0.0

Periodic Reassessments

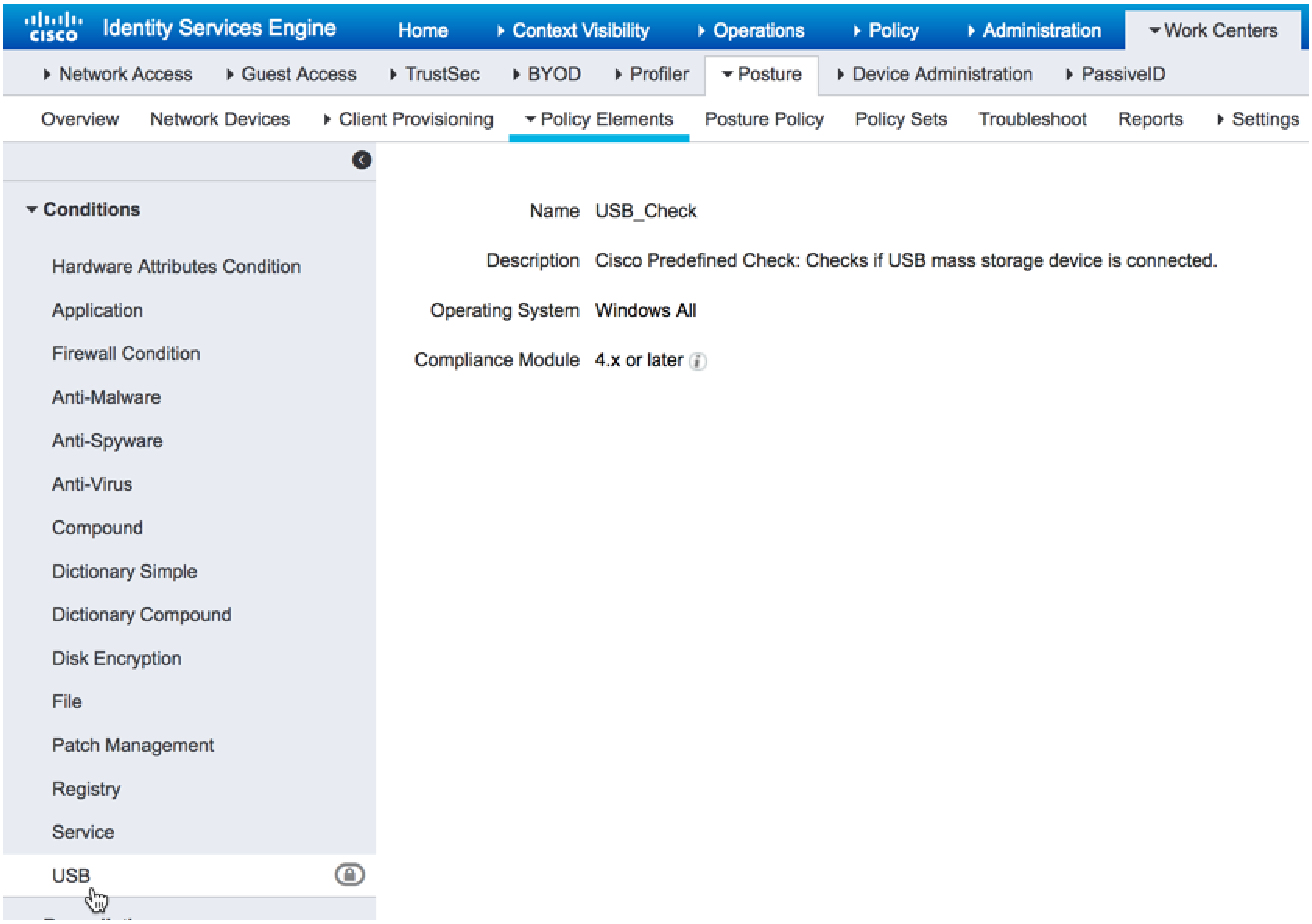
Periodic reassessment (PRA) can be done only for clients that are already successfully postured for compliance. PRA cannot occur if clients are not compliant on your network. A PRA is valid and applicable only if the endpoints are in a compliant state. The policy service node checks the relevant policies, 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. For a more detailed explanation of the configuration parameters for PRAs, reference the ISE administration guide.

Posture Conditions

As previously stated, posture conditions form are the check we want to to perform against the endpoint to ensure our security policy is being met. In our example security policy, the first check is to determine whether or not a USB device is being used on the endpoint. Since ISE 2.4 is being used in our example, there will be a pre-configured USB check in our posture condition. However, we will still verify our condition is configured. Navigate to Work Centers > Posture > Policy Elements > Conditions > USB to view the pre-configured USB check provided by ISE.



USB Condition



Name USB_Check

Description Cisco Predefined Check: Checks if USB mass storage device is connected.

Operating System Windows All

Compliance Module 4.x or later

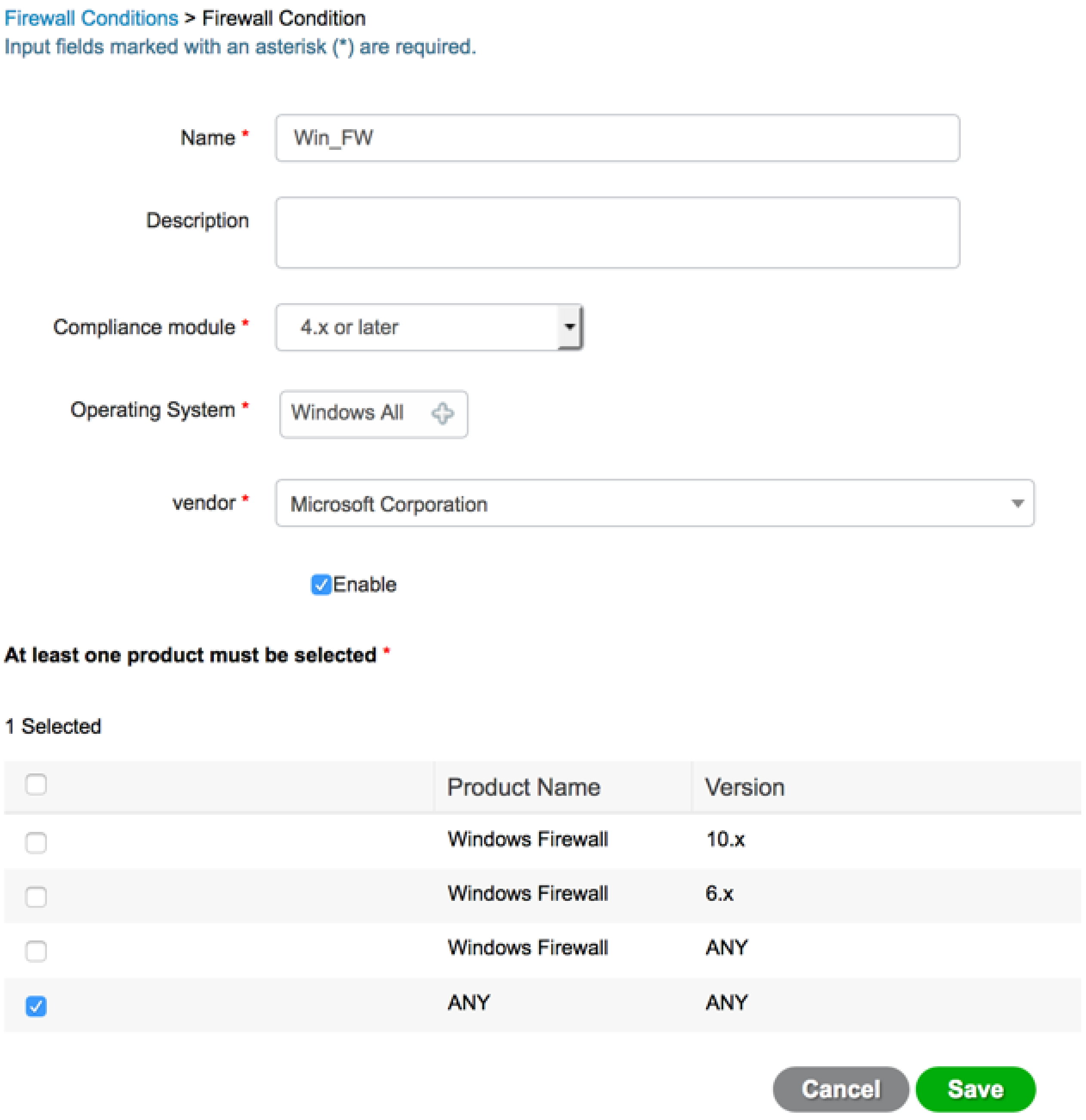
Note: The USB condition check only checks to see if a USB device is connected. It currently does not differentiate between device types. Lastly, the USB check is a real time check and not a periodic one.

Firewall Condition

The Firewall condition checks if a specific Firewall product is enabled 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 however we are going to configure the firewall condition from scratch. Navigate to Work Centers > Posture > Policy Elements > Conditions > Firewall Condition.

Step 1	Navigate to Work Centers > Posture > Policy Elements > Conditions > Firewall Condition
Step 2	Click the "+ Add" icon to configure a new Firewall Condition
Step 3	Give the new condition a name
Step 4	Select "4.x or later" for the Compliance module drop down
Step 5	Select "Windows All" for the operating system
Step 6	Select "Microsoft Corporation" from the vendor drop down

Step 7	Click the "Enable" check box
Step 8	Select "ANY / ANY" for the firewall name and version
Step 9	Click save



Firewall Conditions > Firewall Condition

Input fields marked with an asterisk (*) are required.

Name * Win_FW

Description

Compliance module * 4.x or later

Operating System * Windows All

vendor * Microsoft Corporation

☑ Enable

At least one product must be selected *

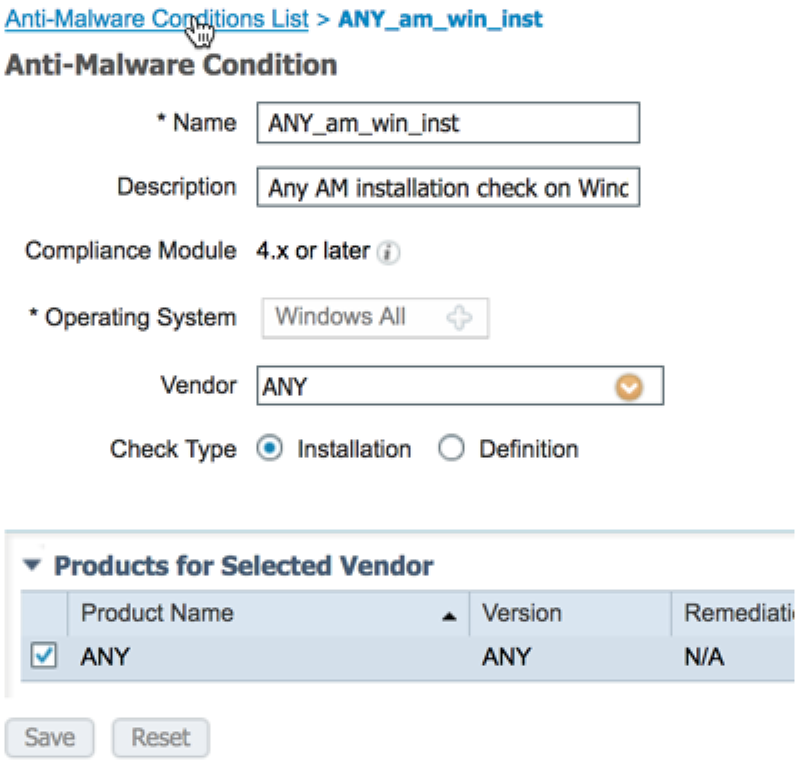
1 Selected

□	Product Name	Version
□	Windows Firewall	10.x
□	Windows Firewall	6.x
□	Windows Firewall	ANY
☑	ANY	ANY

Anti-malware Condition

The anti-malware condition is a combination of the anti-spyware and antivirus conditions and is supported by OESIS version 4.x or later compliance module. The intelligent defaults in ISE have pre-configured anti-malware conditions for ease of use. Follow the steps below to review the pre-configured anti-malware condition.

Step 1	Work Centers > Posture > Posture Elements > Conditions > Antimalware
Step 2	Select "ANY_am_win_inst"
Step 3	Click edit
Step 4	Review the configuration for the condition



Anti-Malware Conditions List > **ANY_am_win_inst**

Anti-Malware Condition

* Name: ANY_am_win_inst

Description: Any AM installation check on Winc

Compliance Module: 4.x or later

* Operating System: Windows All

Vendor: ANY

Check Type: ● Installation ○ Definition

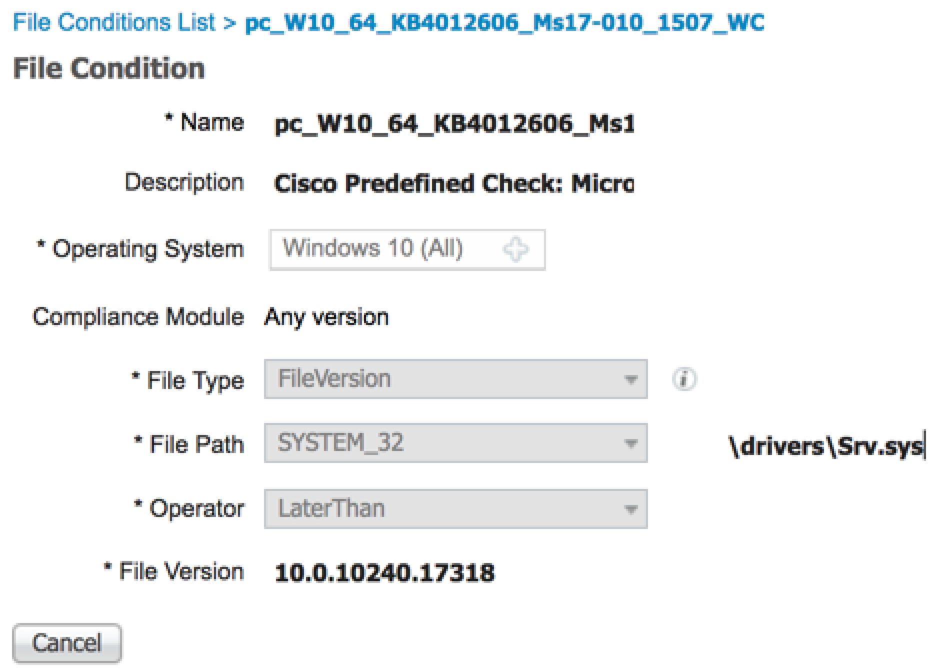
Products for Selected Vendor

	Product Name	Version	Remediati
☑	ANY	ANY	N/A

Critical Patch Condition

The next item in our security policy concerns the installation of a critical patch. In this example, we are going to use the predefined file check to ensure that our Windows 10 clients have the critical security patch installed to prevent the Wanna Cry malware. To review the predefined file check follow the steps below.

Step 1	Work Centers > Posture > Posture Elements > Conditions > File
Step 2	Click the hopper icon on the far right to expose the search menu
Step 3	In the name field, enter: pc_W10_64_KB4012606_Ms17-010_1507_WC
Step 4	Check the box and click the view button at the top


File Conditions List > **pc_W10_64_KB4012606_Ms17-010_1507_WC**

File Condition

* Name: **pc_W10_64_KB4012606_Ms1**

Description: **Cisco Predefined Check: Micro**

* Operating System: Windows 10 (All)

Compliance Module: Any version

* File Type: FileVersion

* File Path: SYSTEM_32 **\drivers\Srv.sys**

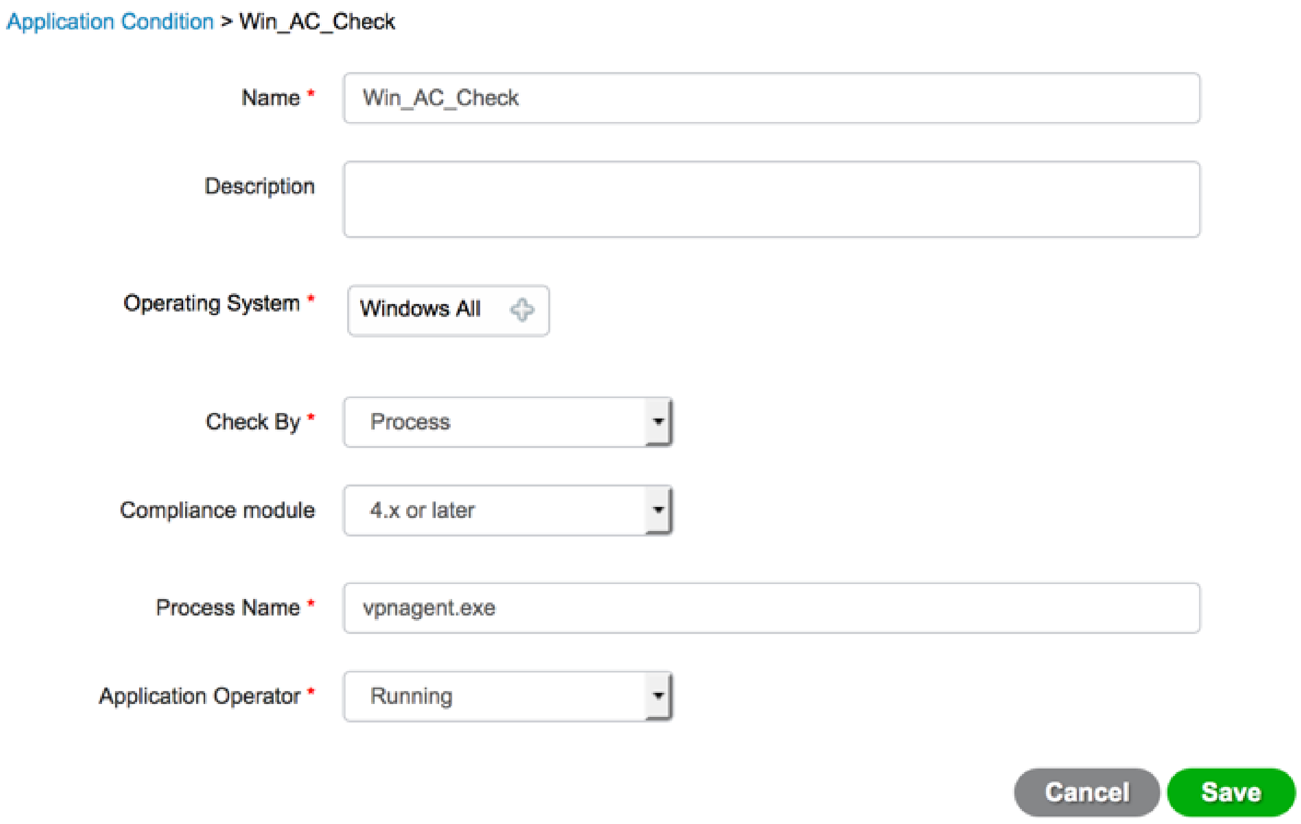
* Operator: LaterThan

* File Version: **10.0.10240.17318**

Application Condition

The last condition required in our example security policy is to check for the installation of a specific application. There are two forms of application checks when doing ISE posture. one to check is application is installed and other to check if application is running. Scenarios to ensure a necessary application is installed and scenarios where any mischievous applications are not installed can both be configured. In both scenarios the installation check however remains the same. For the case of an unwanted application the required remediation action needs to be tied to the condition to take actions to terminate/uninstall the unwanted application. This example security policy will check for the required installation of a VPN client. We will cover the steps necessary to create application compliance for an application that should not be installed on the endpoint later in this guide. To configure a condition for an appliance installation, follow the steps below

Step 1	Navigate to Work Centers > Posture > Policy Elements > Conditions > Application
Step 2	Click the "+ Add" icon to configure a new application condition
Step 3	Give the new condition a name
Step 4	Select "Windows All" as the operating system
Step 5	Select "Process" from the check by drop down
Step 6	Enter the process name in the process name field
Step 7	Select "Running" for the application operator drop down
Step 8	Select "ANY / ANY" for the firewall name and version
Step 9	Select "Cisco System, Inc" from the vendor drop down
Step 11	Click save


Application Condition > Win_AC_Check

Name * Win_AC_Check

Description

Operating System * Windows All

Check By * Process

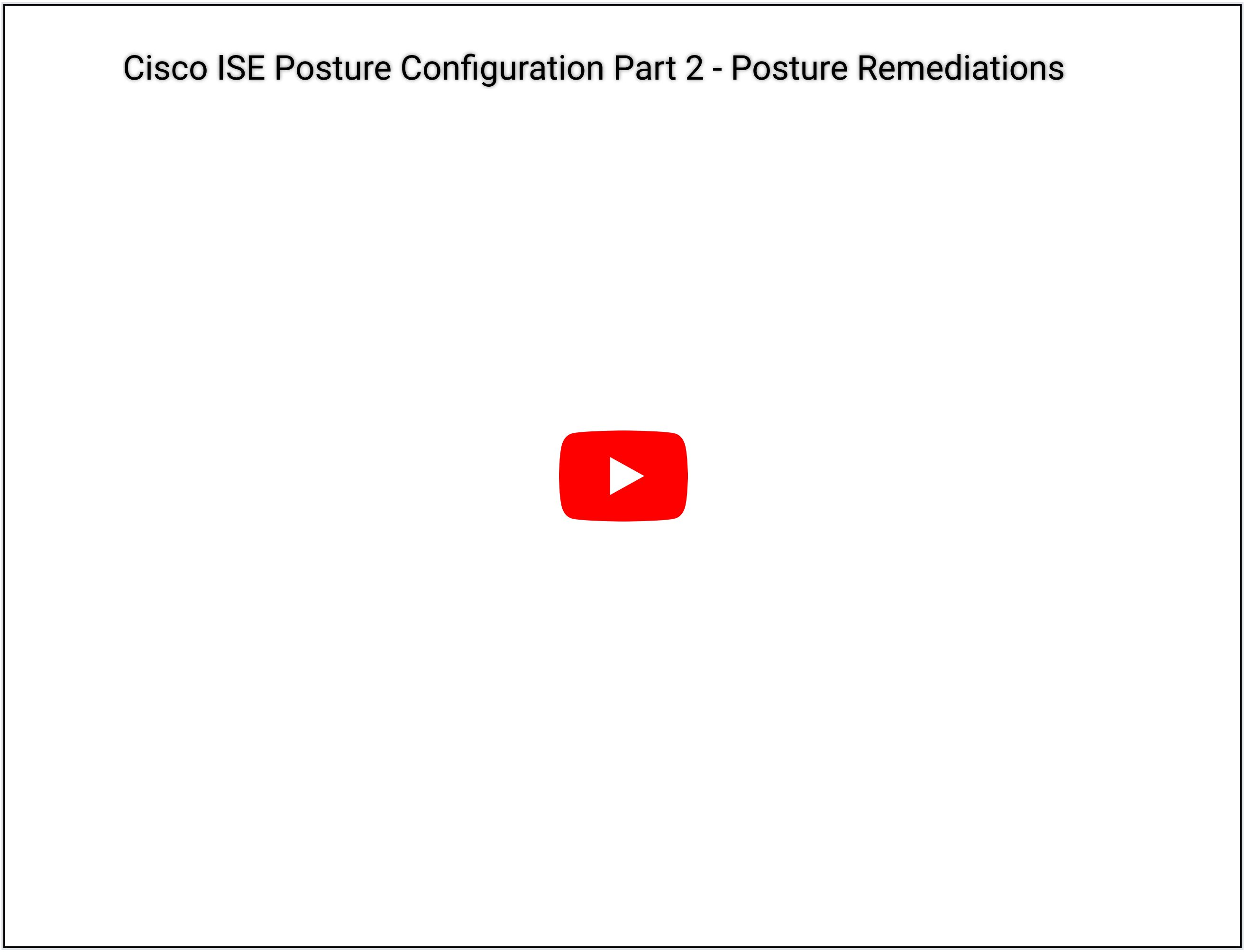
Compliance module 4.x or later

Process Name * vpnagent.exe

Application Operator * Running

Posture Remediations

Posture remediations are the actions AnyConnect will take if it determines that the endpoint is out of compliance. There are two main types of remediation AnyConnect: automatic and manual. Automatic remediation is performed by AnyConnect without intervention by the end user of the endpoint. Manual remediation requires the end user of the endpoint to resolve the compliance issue before the endpoint is allowed network access. To understand which conditions are supported for automatic remediation or manual remediation, please review "Windows Posture Assessment Options" and "macOS Posture Assessment Options" sections of this guide.

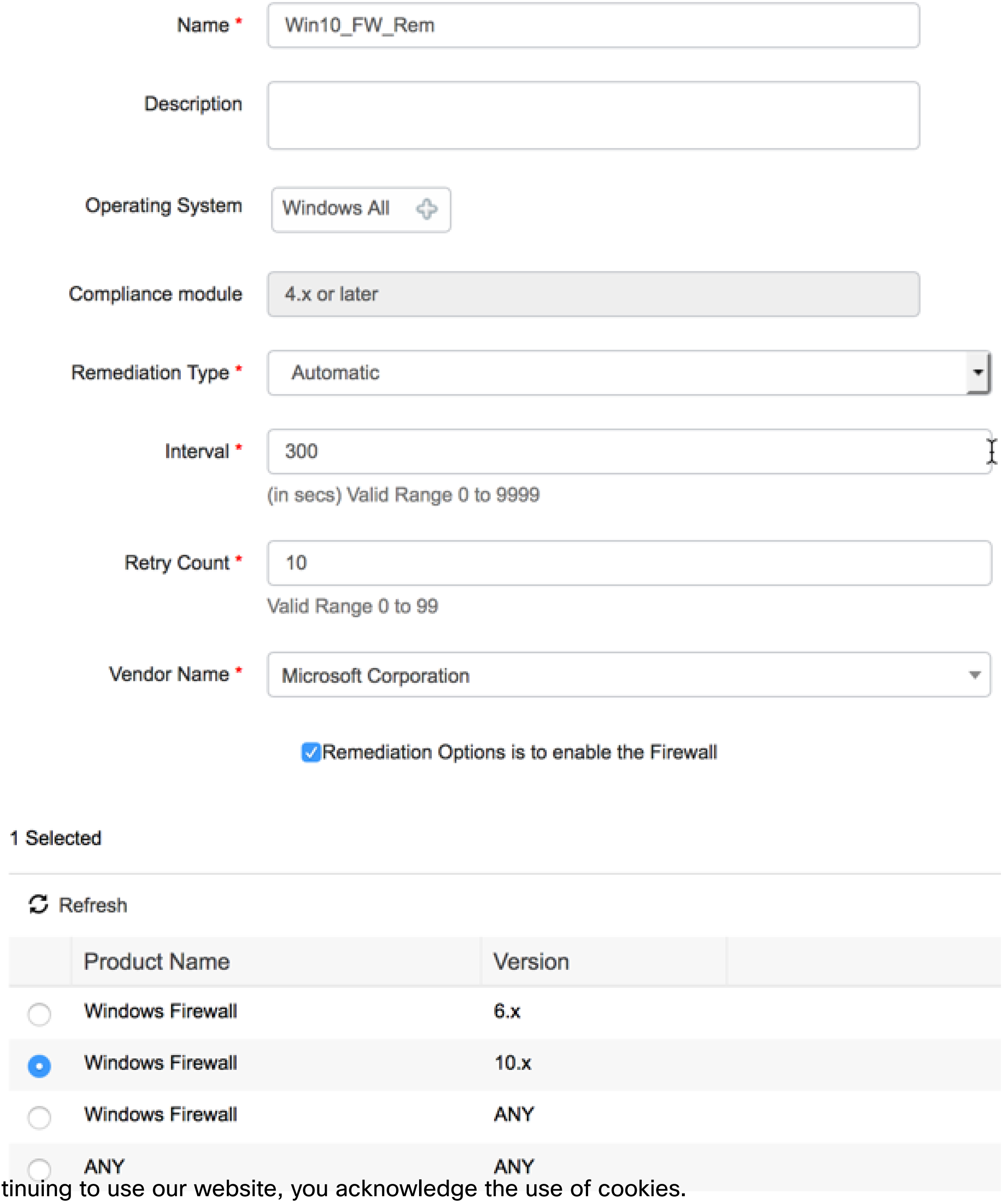

Cisco ISE Posture Configuration Part 2 - Posture Remediations

Firewall Remediation

Our example security policy requires that Windows firewall be enabled for endpoint accessing the network. To configure a firewall remediation, follow the steps below.

Step 1	Navigate to Work Centers > Posture > Policy Elements > Remediations > Firewall
Step 2	Click the "+Add" icon to configure a new application condition
Step 3	Give the new condition a name
Step 4	Select "Windows All" as the operating system

Step 5	Select "Automatic" from the remediation type by drop down
Step 6	Enter values (in seconds) for interval and retry count field
Step 7	Select "Microsoft Corporation" from the vendor drop down
Step 8	Ensure "Remediation Options is to enable the Firewall" is checked
Step 9	Select "Windows Firewall 10.x"
Step 10	Click save



Name * Win10_FW_Rem

Description

Operating System: Windows All

Compliance module: 4.x or later

Remediation Type * Automatic

Interval * 300

(in secs) Valid Range 0 to 9999

Retry Count * 10

Valid Range 0 to 99

Vendor Name * Microsoft Corporation

☑ Remediation Options is to enable the Firewall

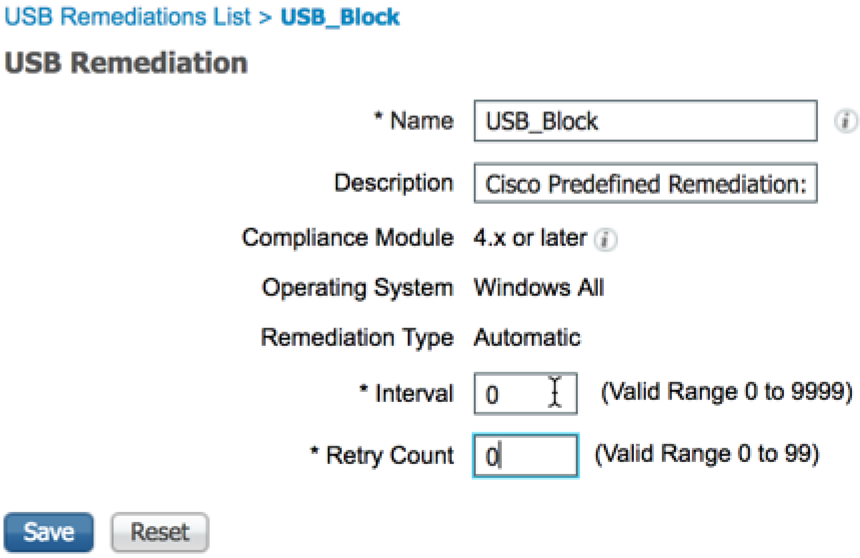
1 Selected

	Product Name	Version
○	Windows Firewall	6.x
●	Windows Firewall	10.x
○	Windows Firewall	ANY
○	ANY	ANY

USB Remediation

In addition to a preconfigured condition for USB, Cisco ISE also has a preconfigured remediation for USB as well. To review the USB remediation, follow the steps below.

Step 1	Navigate to Work Centers > Posture > Policy Elements > Remediations > USB
Step 2	Click the "USB_Block" icon then click "Edit"
Step 3	If required, you can modify the interval and retry count values
Step 4	Click save


USB Remediations List > **USB_Block**

USB Remediation

* Name: USB_Block

Description: Cisco Predefined Remediation:

Compliance Module: 4.x or later

Operating System: Windows All

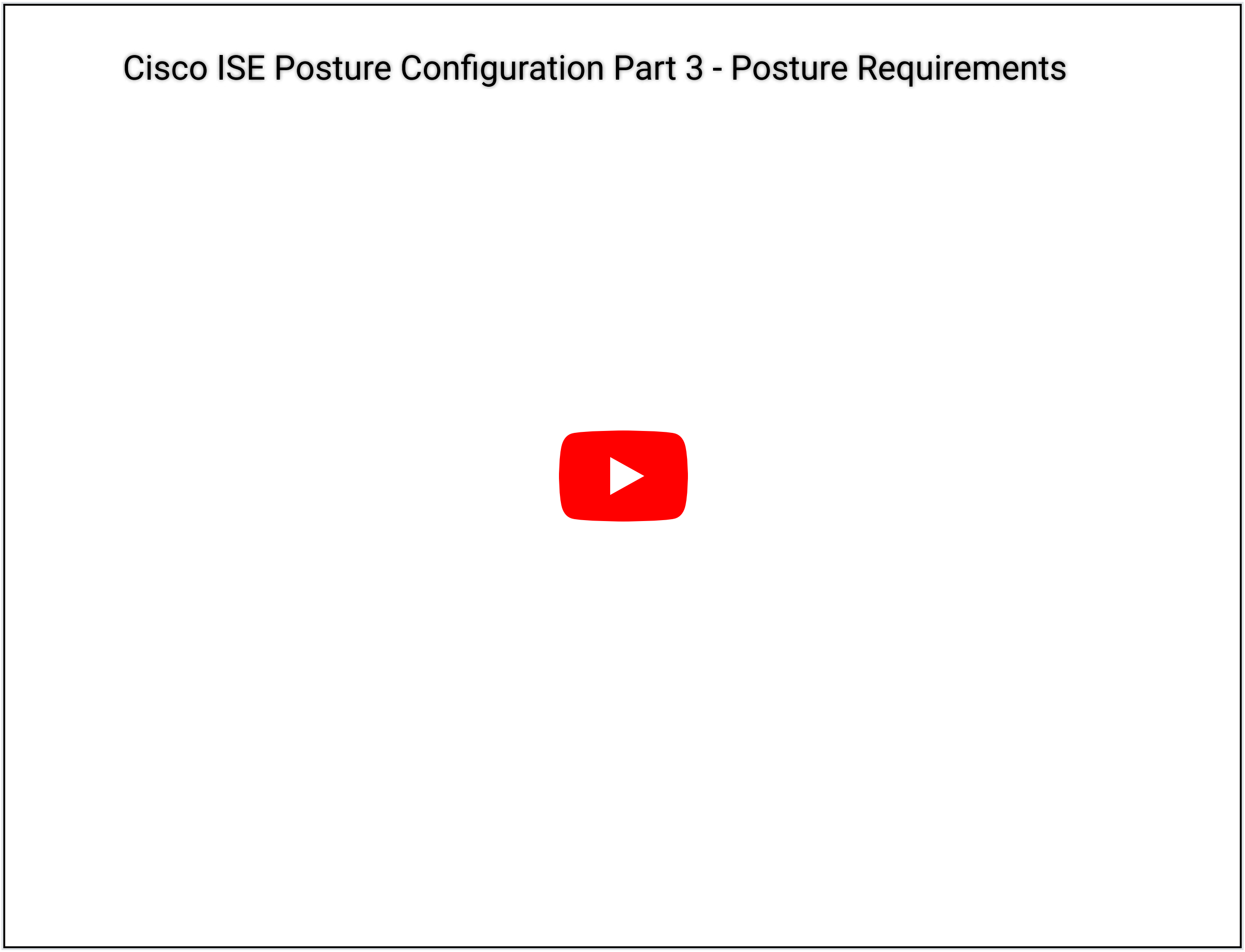
Remediation Type: Automatic

* Interval: 0 (Valid Range 0 to 9999)

* Retry Count: 0 (Valid Range 0 to 99)

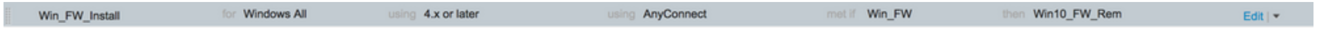
Posture Requirements

Now that we have our posture conditions and remediations defined to reflect our example security policy, it is time to tie them together using posture requirements. Similar to access policy, posture requirements are a set of rules that outline the posture condition, operating system, compliance module, agent type and remediation action. Just like posture conditions, ISE has preconfigured posture requirement that allows you to quickly enable posture requirements. However, this guide will outline the steps necessary to build them from scratch (with the exception of the USB requirement and anti malware requirement as they are already configured by default in ISE 2.4). Follow the steps below to configure posture requirements.


Cisco ISE Posture Configuration Part 3 - Posture Requirements

Firewall Requirement

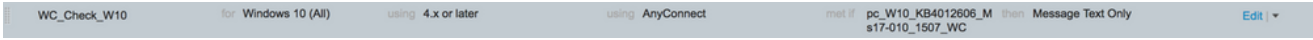
Step 1	Navigate to Work Centers > Posture > Policy Elements > Requirements
Step 2	Click the "down arrow" icon to the right of the "Edit" hyperlink
Step 3	Select "Insert new requirement"
Step 4	Give the requirement a name
Step 5	Select "Windows All" as the operating system
Step 6	Select "4.x or later" for the compliance module
Step 7	Select "AnyConnect" as the posture type
Step 8	Select the name of the firewall condition configured earlier
Step 9	Select the name of the firewall remediation configured earlier
Step10	Click done
Step 11	Click save at the bottom of the page


Win_FW_Install for Windows All using 4.x or later using AnyConnect met if Win_FW then Win10_FW_Rem Edit | ▾

Critical Patch Requirement

Note: *Since the file check is specific to Windows 10, be sure you select Windows 10 as the operating system when configuring the rule. Otherwise, it will not show up as an option in the drop down box.*

Step 1	Navigate to Work Centers > Posture > Policy Elements > Requirements
Step 2	Click the "down arrow" icon to the right of the "Edit" hyperlink
Step 3	Select "Insert new requirement"
Step 4	Give the requirement a name
Step 5	Select "Windows 10 All" as the operating system
Step 6	Select "4.x or later" for the compliance module
Step 7	Select "AnyConnect" as the posture type
Step 8	Select "pc_W10_KB4012606_Ms17-010_1507_WC"
Step 9	Select "Message Text" as the remediation
Step 10	Enter a message for the end user
Step 11	Click done
Step 12	Click save at the bottom of the page

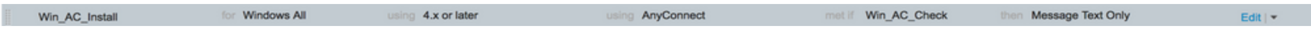


WC_Check_W10 for Windows 10 (All) using 4.x or later using AnyConnect met if pc_W10_KB4012606_Ms17-010_1507_WC then Message Text Only

Application Requirement

Step 1	Navigate to Work Centers > Posture > Policy Elements > Requirements
Step 2	Click the "down arrow" icon to the right of the "Edit" hyperlink
Step 3	Select "Insert new requirement"
Step 4	Give the requirement a name
Step 5	Select "Windows All" as the operating system
Step 6	Select "4.x or later" for the compliance module
Step 7	Select "AnyConnect" as the posture type
Step 8	Select the name of the application condition configured earlier
Step 9	Select "Message Text" as the remediation
Step 10	Enter a message for the end user
Step 11	Click done

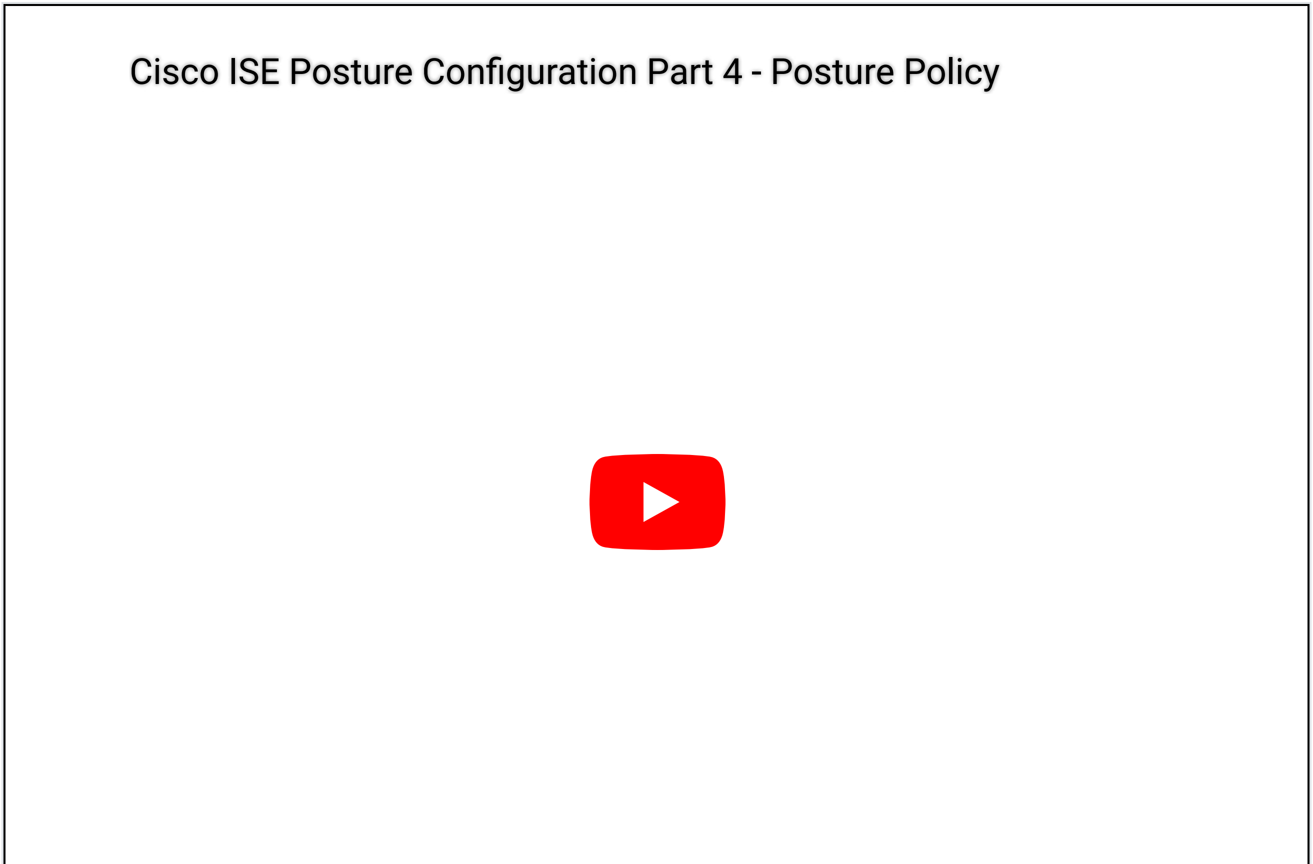
Step 12	Click save at the bottom of the page



Win_AC_Install for Windows All using 4.x or later using AnyConnect met if Win_AC_Check then Message Text Only

Posture Policy

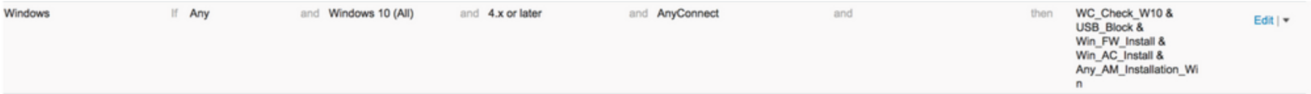
A posture policy is a collection of posture requirements, which are associated with one or more identity groups, and operating systems. The Dictionary Attributes are optional conditions in conjunction with the identity groups and the operating systems that allow you to define different policies for the clients. Cisco ISE provides an option to configure a grace period for devices that become noncompliant. ISE caches the results of posture assessment for a configurable amount of time. If a device is found to be noncompliant, Cisco ISE looks for the previously known good state in its cache and provides grace for the device, during which the device is granted access to the network. You can configure the grace period in minutes, hours, or days (up to a maximum of 30 days). An endpoint is eligible to utilize this grace period only if it has previously been in a good/compliant state.



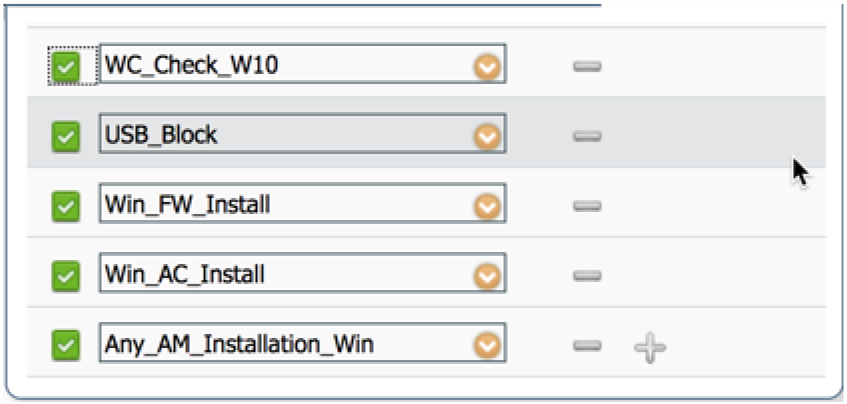
Cisco ISE Posture Configuration Part 4 - Posture Policy

To configure posture policy, follow the steps below.

Step 1	Navigate to Work Centers > Posture > Posture Policy
Step 2	Click the "down arrow" icon to the right of the "Edit" hyperlink
Step 3	Select "Insert new policy"
Step 4	Give the rule a name
Step 5	Select "Windows 10 All" as the operating system
Step 6	Select "4.x or later" for the compliance module
Step 7	Select "AnyConnect" as the posture type
Step 8	In the requirements field, select all 5 requirement by using the "+" sign
Step 9	Click done
Step 10	Click Save



Windows	If	Any	and	Windows 10 (All)	and	4.x or later	and	AnyConnect	and	then	WC_Check_W10 & USB_Block & Win_FW_Install & Win_AC_Install & Any_AM_Installation_Win	Edit | ▾



☑ WC_Check_W10

☑ USB_Block

☑ Win_FW_Install

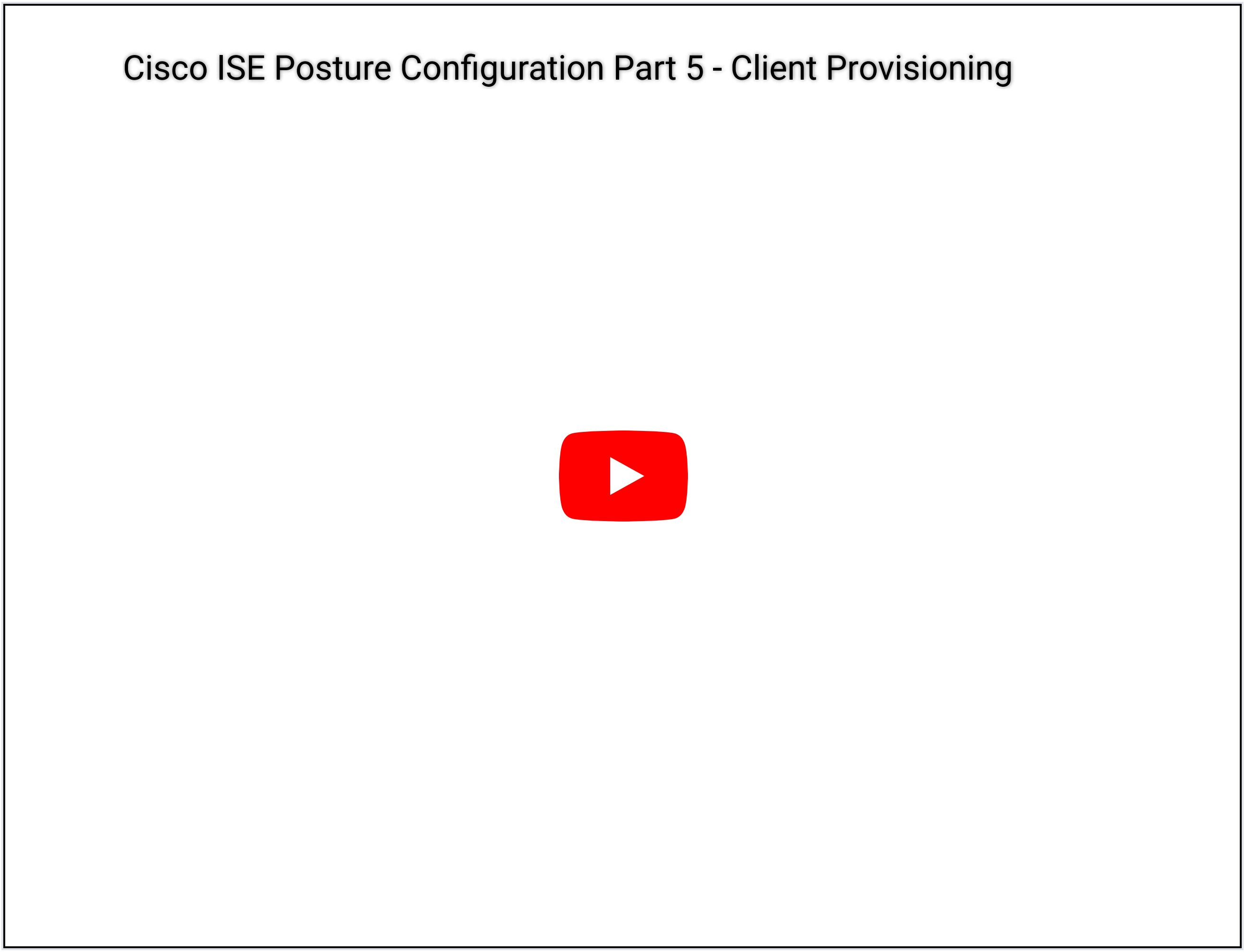
☑ Win_AC_Install

☑ Any_AM_Installation_Win

Client Provisioning

For clients, the client provisioning resource policies determine which users receive which version (or versions) of resources (agents, agent compliance modules, and/or agent customization packages/profiles) from Cisco ISE upon login and user session initiation. For AnyConnect, resources can be selected from the client provisioning resources page to create an AnyConnect configuration that you can use in the client provisioning policy page. AnyConnect configuration is the AnyConnect software and its association with different configuration files that includes AnyConnect binary package for Windows and macOS X clients, compliance module. module profiles, customization and language packages for AnyConnect.

There are two method for provisioning client with ISE alone. While enterprise software product can allow for wide distribution of software, ISE can provision client in a couple of ways: URL-Redirection and download or a provisioning URL. Before you begin, you will need to download the AnyConnect software from cisco.com as it cannot be automatically downloaded through provisioning resources such as the compliance module. The agent configuration in client provisioning policy requires three components at minimum: an AnyConnect profile, an AnyConnect configuration and a compliant module. Begin by creating an AnyConnect profile.


Cisco ISE Posture Configuration Part 5 - Client Provisioning

Step 1	Navigate to Work Centers > Posture > Client Provisioning > Resources
Step 2	Click the "Add" button and select AnyConnect Posture profile
Step 3	Enter the configuration parameters for how AnyConnect will operate
Step 4	Click Save

Note: *For a detailed explanation of the posture profile configuration parameters, please reference the ISE Administration guide or by "launching page level help" from the menu*

Now that that a posture profile has been configured, you can upload AnyConnect to ISE:

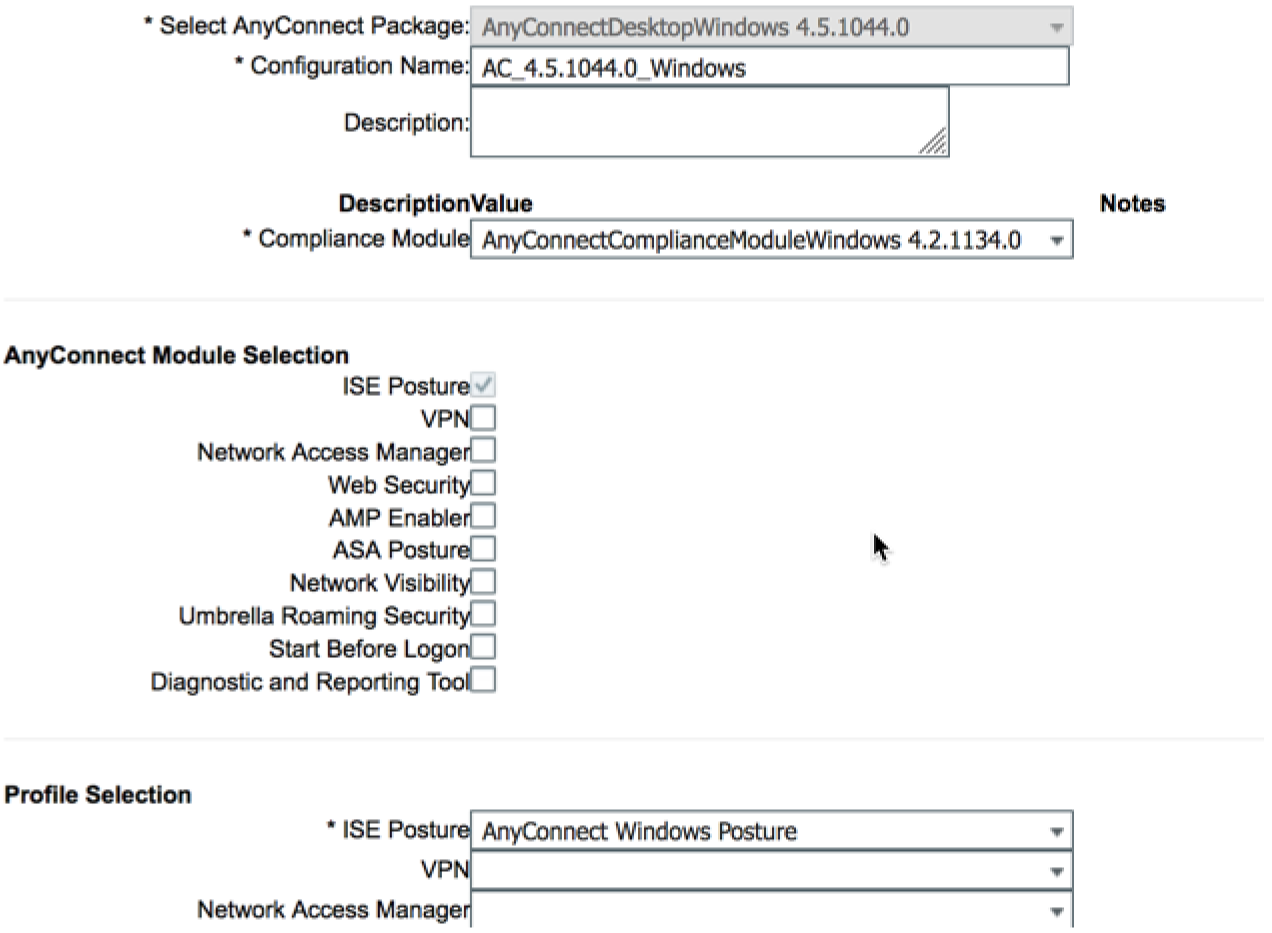
Step 1	Navigate to Work Centers > Posture > Client Provisioning > Resources
Step 2	Click the "Add" button
Step 3	Select "Agent resources from local disk"
Step 4	Select "Cisco provided packages" from the Category drop down
Step 5	Select the AnyConnect software from the local disk by using the "browse" button
Step 6	Click Submit

Once AnyConnect is uploaded to ISE, we now need to download a compliance module:

Step 1	Navigate to Work Centers > Posture > Client Provisioning > Resources
Step 2	Click the "Add" button
Step 3	Select "Agent resources from Cisco site"
Step 4	Select the desired compliance module from the list
Step 5	Click Save

Finally, we can create the required AnyConnect configuration for use in client provisioning policy:

Step 1	Navigate to Work Centers > Posture > Client Provisioning > Resources
Step 2	Click the "Add" button
Step 3	Select "AnyConnect Configuration"
Step 4	Select the AnyConnect version uploaded from cisco.com
Step 5	Give the configuration a name
Step 6	Select the compliance module downloaded from cisco.com
Step 7	Select the posture profile previously created
Step 8	Click Save



* Select AnyConnect Package: AnyConnectDesktopWindows 4.5.1044.0

* Configuration Name: AC_4.5.1044.0_Windows

Description:

Description	Value	Notes
* Compliance Module	AnyConnectComplianceModuleWindows 4.2.1134.0	

AnyConnect Module Selection

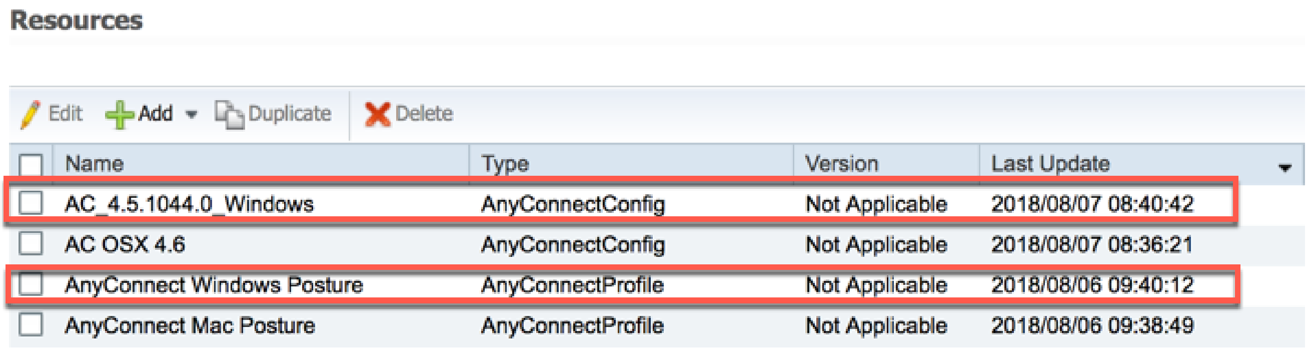
- ISE Posture ☑
- VPN □
- Network Access Manager □
- Web Security □
- AMP Enabler □
- ASA Posture □
- Network Visibility □
- Umbrella Roaming Security □
- Start Before Logon □
- Diagnostic and Reporting Tool □

Profile Selection

* ISE Posture: AnyConnect Windows Posture

VPN:

Network Access Manager:



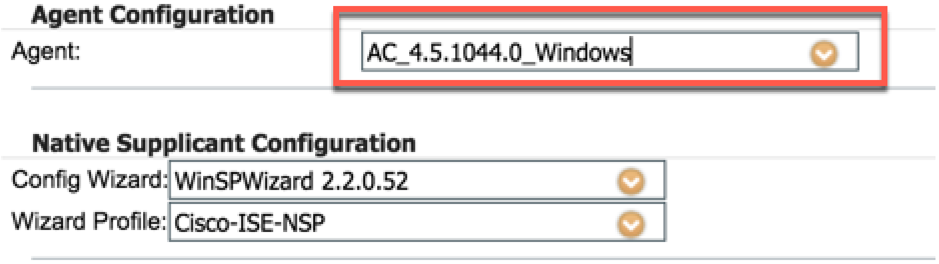
Resources

Name	Type	Version	Last Update
AC_4.5.1044.0_Windows	AnyConnectConfig	Not Applicable	2018/08/07 08:40:42
AC OSX 4.6	AnyConnectConfig	Not Applicable	2018/08/07 08:36:21
AnyConnect Windows Posture	AnyConnectProfile	Not Applicable	2018/08/06 09:40:12
AnyConnect Mac Posture	AnyConnectProfile	Not Applicable	2018/08/06 09:38:49

Lastly, create client provisioning policy using the newly created AnyConnect configuration:

Step 1	Navigate to Work Centers > Posture > Client Provisioning
Step 2	Click the "Edit" hyperlink for the preconfigured Windows rule
Step 3	Click the "+" icon [illegible]
Step 4	Select the AnyConnect Configuration from the Agent drop down
Step 5	Click down

Step 6	Click save



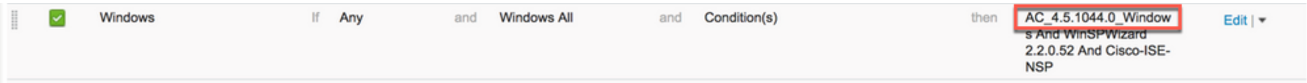
Agent Configuration

Agent: AC_4.5.1044.0_Windows

Native Supplicant Configuration

Config Wizard: WinSPWizard 2.2.0.52

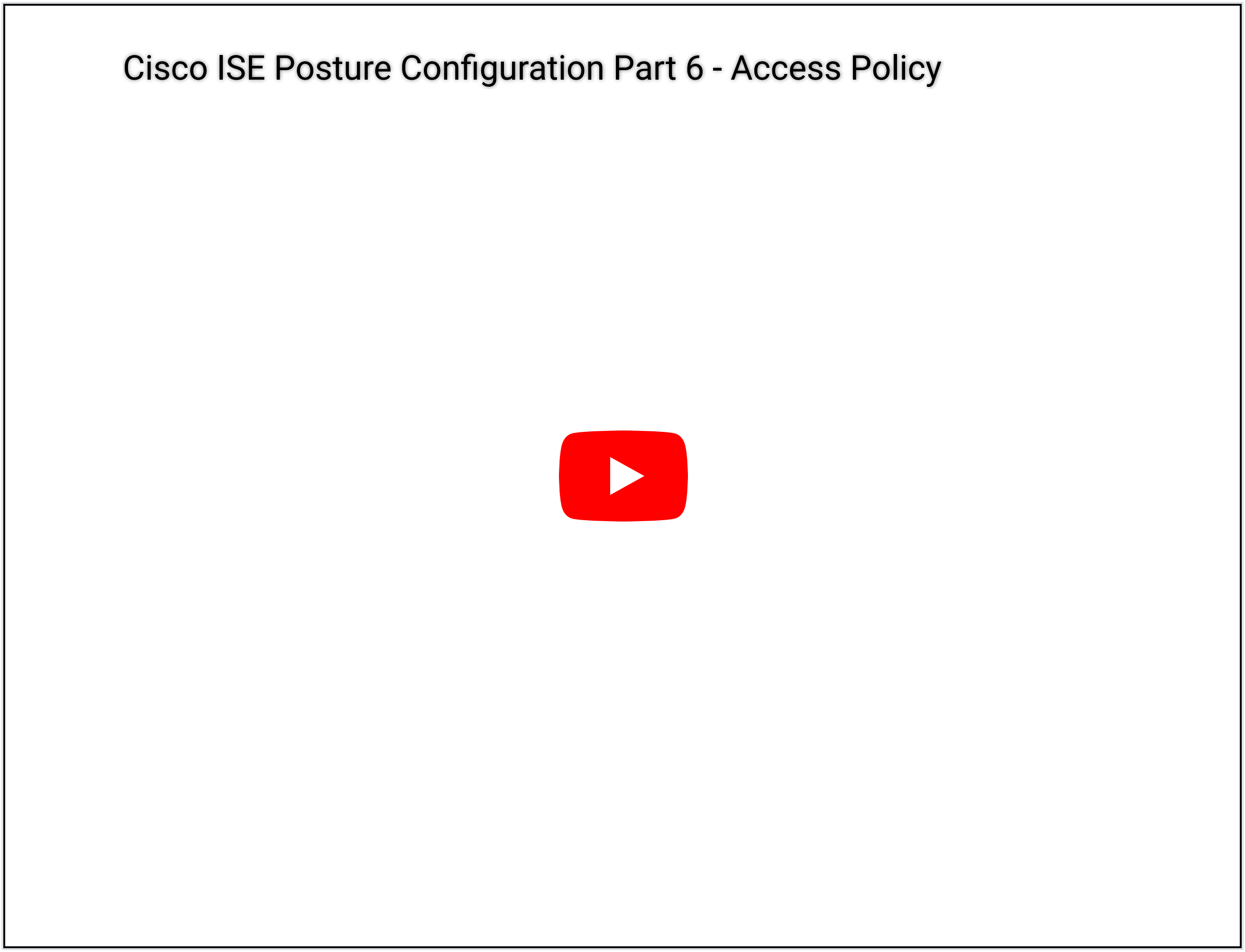
Wizard Profile: Cisco-ISE-NSP



Windows If Any and Windows All and Condition(s) then AC_4.5.1044.0_Windows And WinSPWizard 2.2.0.52 And Cisco-ISE-NSP

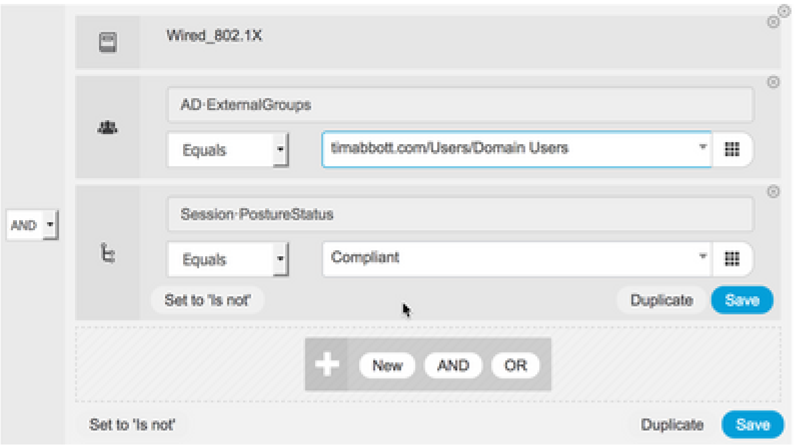
Access Policy

The final section in our deploy section is the configuration of access policy. Cisco ISE is a policy-based, network-access-control solution, which offers network access policy sets, allowing you to manage several different network access use cases such as wireless, wired, guest, and client provisioning. Policy sets (both network access and device administration sets) enable you to logically group authentication and authorization policies within the same set. You can have several policy sets based on an area, such as policy sets based on location, access type and similar parameters. When you install ISE, there is always one policy set defined, which is the default policy set, and the default policy set contains within it, predefined and default authentication, authorization and exception policy rules. This guide will use a preconfigured policy set to enforce the addition of the example security policy.

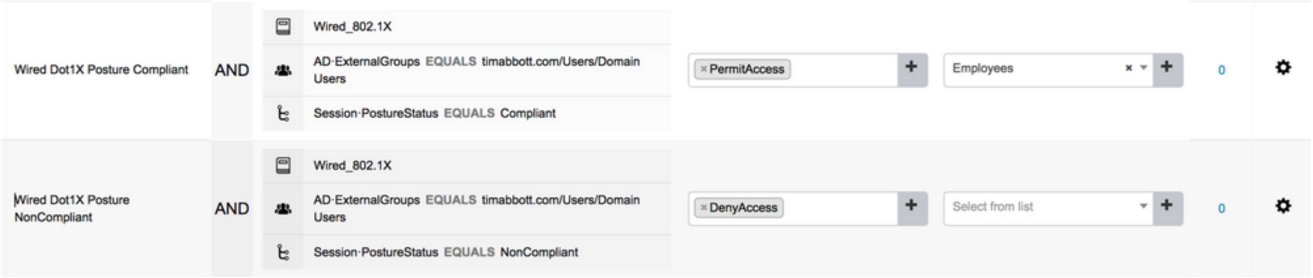


Cisco ISE Posture Configuration Part 6 - Access Policy

Step 1	Navigate to Policy > Policy Sets
Step 2	Select the Policy Set that will contain the enforcement conditions for the posture policy
Step 3	Select "Authorization Policy"
Step 4	Select the authorization rule that requires the compliant condition
Step 5	Click the condition field to open the condition studio
Step 6	Click the "New" button
Step 7	Click to add a new attribute and select "session" from the Dictionaries drop down
Step 8	Select the "PostureStatus" attribute

Step 9	Click "Choose from the list" and select "compliant"  Wired_802.1X AD-ExternalGroups Equals timabbott.com/Users/Domain Users Session-PostureStatus Equals Compliant
Step 10	Click "Use"
Step 11	Click the gear icon of the newly modified rule and select "duplicate below"
Step 12	Repeat steps 5 through 9 but select "noncompliant" instead of "compliant"
Step 13	Click "Use"
Step 14	Change the "Results Profiles" to deny access and rename the authorization rule
Step 15	Save the authorization policy

The new policy should resemble the below:



Wired Dot1X Posture Compliant	AND	Wired_802.1X AD-ExternalGroups EQUALS timabbott.com/Users/Domain Users Session-PostureStatus EQUALS Compliant	PermitAccess	Employees	0	⚙
Wired Dot1X Posture NonCompliant	AND	Wired_802.1X AD-ExternalGroups EQUALS timabbott.com/Users/Domain Users Session-PostureStatus EQUALS NonCompliant	DenyAccess	Select from list	0	⚙

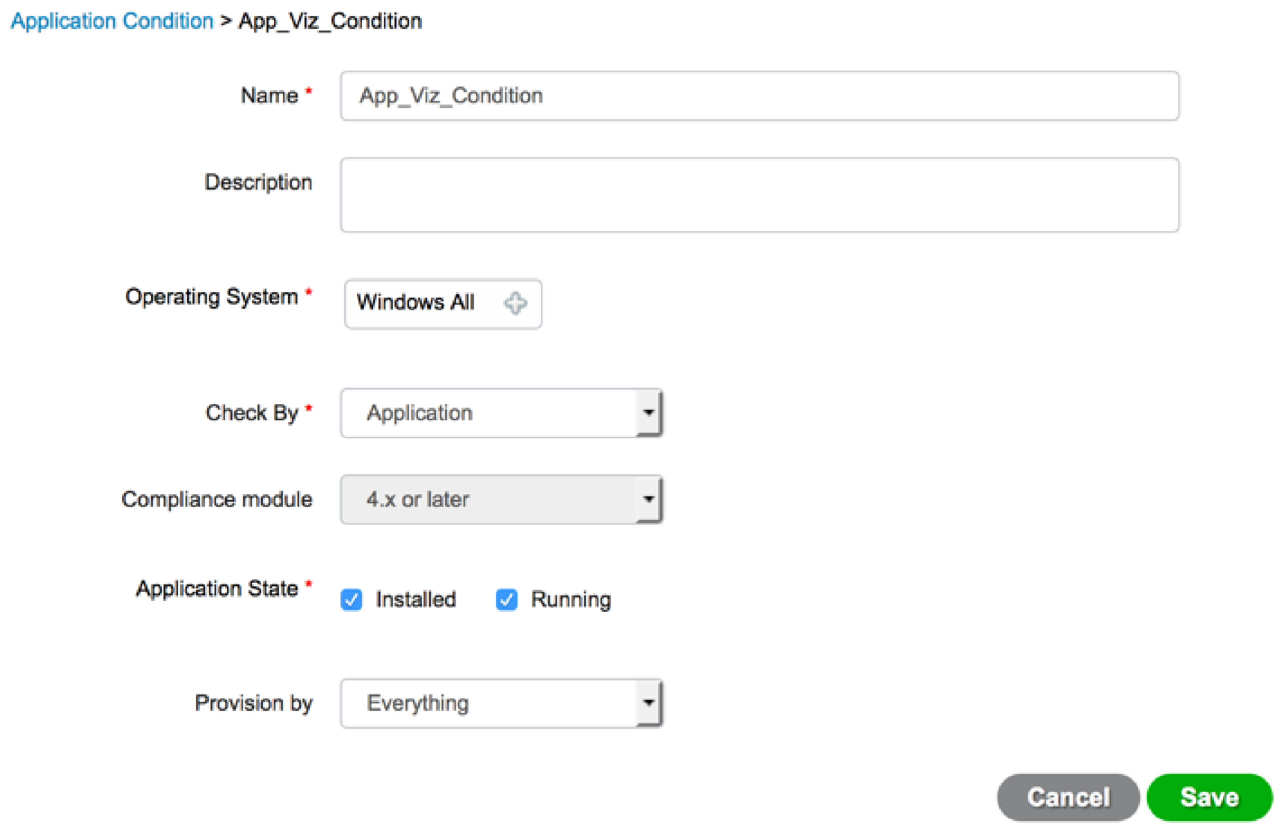
Operate

Context Visibility

Context Visibility give an ISE administrator the ability to review various details about an ISE deployment. From authenticated endpoint to posture compliance, Context Visibility provides a vast amount of information. As of ISE 2.4, Context Visibility has four main sections: Endpoints, Users, Network Devices and Application. As stated either in this guide, there are two way to enforce application compliance with ISE posture: ensuring an application is installed on an endpoint and ensuring an application is not installed on an endpoint. In this section, we will cover the steps necessary to ensure an application that was discovered during application inventory is not installed on an endpoint.

Application Condition

Step 1	Navigate to Work Centers > Posture > Policy Elements > Conditions > Application
Step 2	Click the "Add" button
Step 3	Give the condition a name
Step 4	Select "Windows All" as the operating system
Step 5	Select "Application" for the check by drop down
Step 6	Select "Installed" and "running" for the application state
Step 7	Select "Everything" from the provision by drop down
Step 8	Click Save



Application Condition > App_Viz_Condition

Name * App_Viz_Condition

Description

Operating System * Windows All

Check By * Application

Compliance module 4.x or later

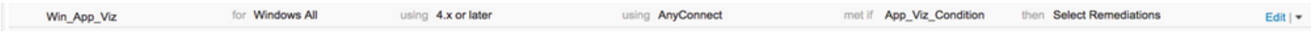
Application State * ☑ Installed ☑ Running

Provision by Everything

Application Requirement

Step 1	Navigate to Work Centers > Posture > Policy Elements > Requirements
Step 2	Select the down arrow on the far left of one of the rules and select "Insert new requirement"
Step 3	Select "AnyConnect Configuration"
Step 4	Give the rule a name
Step 5	Select "Windows All" as the operating system
Step 6	Select "4.x or later" for the compliance module

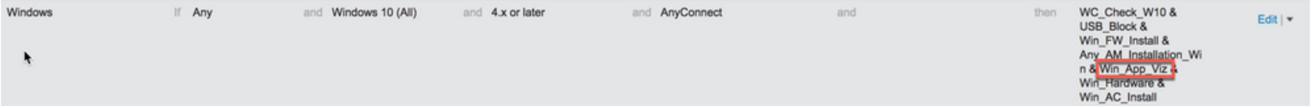
Step 7	Select "AnyConnect" for the posture type
Step 8	Select the application condition name used in the previous section
Step 9	Click "done" on the far left
Step 10	Click Save



Win_App_Viz for Windows All using 4.x or later using AnyConnect met if App_Viz_Condition then Select Remediations

Posture Policy

Step 1	Navigate to Work Centers > Posture > Policy
Step 2	Click the "Edit" hyperlink for the windows posture rule
Step 3	Select "AnyConnect Configuration"
Step 4	Add the posture requirement created in the last section to the list of requirements
Step 5	Click done
Step 6	Click save

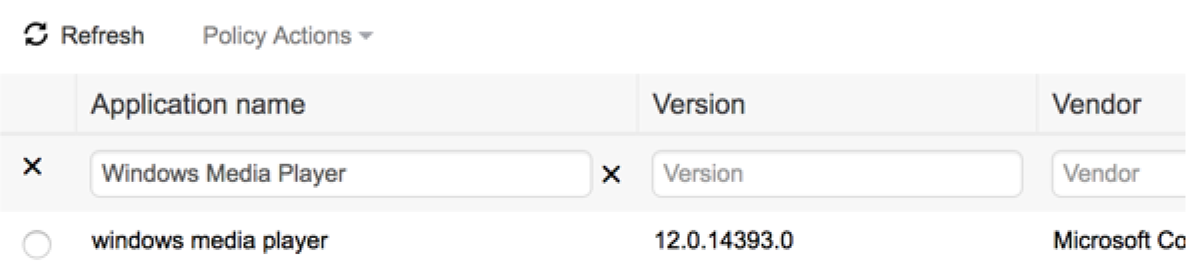
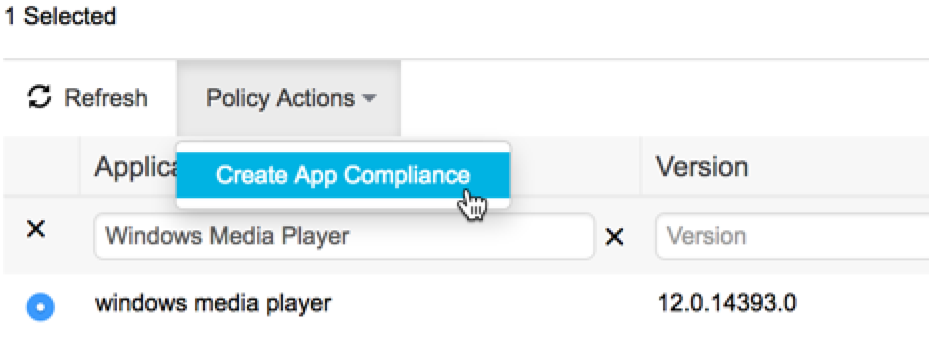
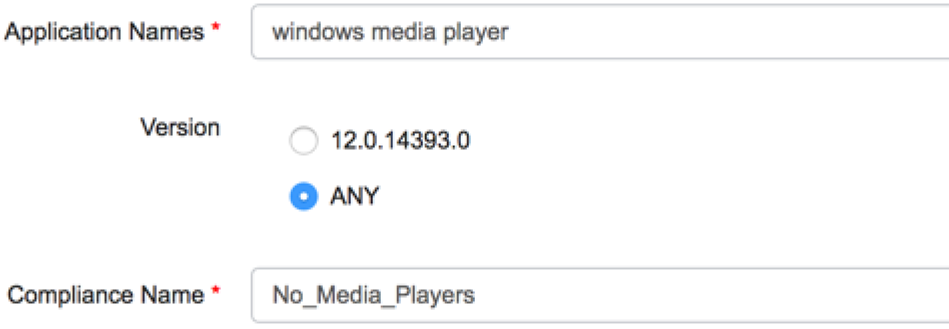


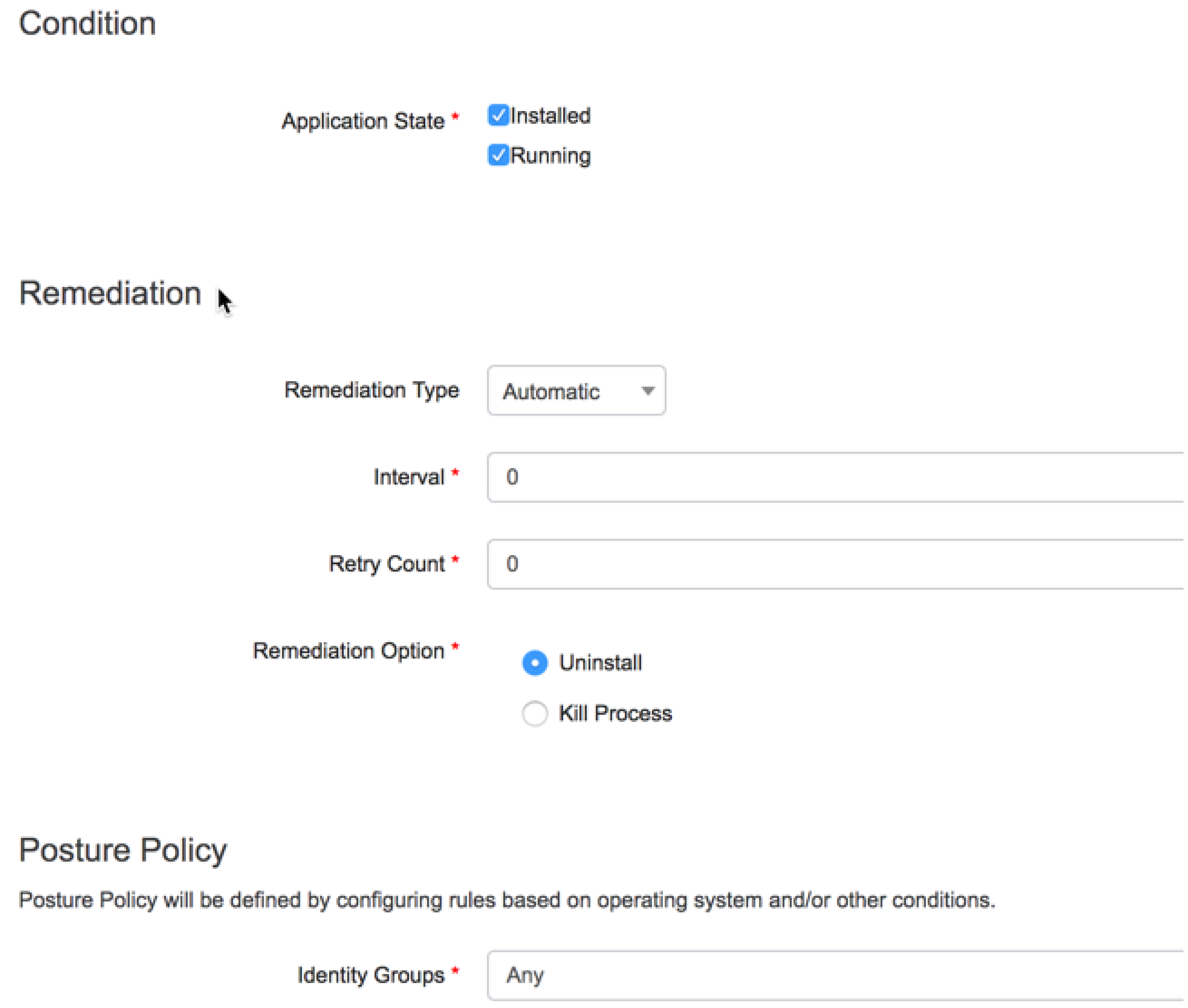
Windows If Any and Windows 10 (All) and 4.x or later and AnyConnect and then WC_Check_W10 & USB_Block & Win_FW_Install & Any_AM_Installation_Win & Win_App_Viz & Win_Hardware & Win_AC_Install

Context Visibility Application Compliance Creation

Once AnyConnect sends ISE an application inventory for each postured endpoint, the list of applications will be visible in Context Visibility under the Application section. Here is where the ISE administrator will be able to view the list of installed applications for each endpoint and create application compliance if so desired. To create application compliance, follow the steps below

Step 1	Navigate to Context Visibility > Application

Step 2	Under the search field for Application name, enter the name of the application  Refresh Policy Actions Application name: Windows Media Player Version: Version Vendor: Vendor ○ windows media player 12.0.14393.0 Microsoft Co
Step 3	Select the radio button beside the application
Step 4	Under "Policy Actions," select create app compliance  1 Selected Refresh Policy Actions Create App Compliance Applic… : Windows Media Player Version: Version ● windows media player 12.0.14393.0
Step 5	Select the version of the software for the compliance rule
Step 6	Give the compliance rule a name  Application Names * windows media player Version ○ 12.0.14393.0 ● ANY Compliance Name * No_Media_Players
Step 7	Select "Installed" and / or "Running" for the application state
Step 8	Select the remediation type
Step 9	Select either "Uninstall" or "Kill process" as the remediation option
Step 10	Select the required identity group if required
Step 11	Click save policy



Condition

Application State * ☑ Installed ☑ Running

Remediation

Remediation Type: Automatic

Interval * 0

Retry Count * 0

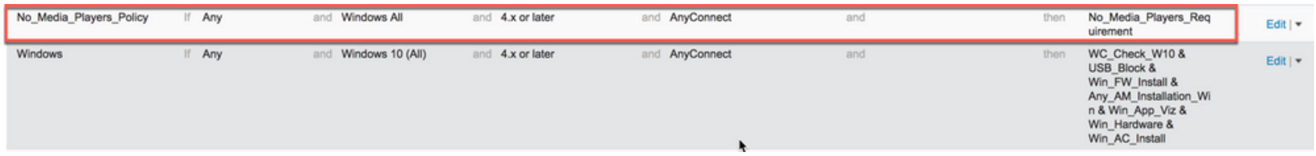
Remediation Option * ● Uninstall ○ Kill Process

Posture Policy

Posture Policy will be defined by configuring rules based on operating system and/or other conditions.

Identity Groups * Any

At this point, ISE as automatically created the application condition, application remediation and application requirement. It has also create a separate posture policy rule for windows endpoints with the new posture requirement:



No_Media_Players_Policy	If	Any	and	Windows All	and	4.x or later	and	AnyConnect	and	then	No_Media_Players_Requirement
Windows	If	Any	and	Windows 10 (All)	and	4.x or later	and	AnyConnect	and	then	WC_Check_W10 & USB_Block & Win_FW_Install & Any_AM_Installation_Win & Win_App_Viz & Win_Hardware & Win_AC_Install

Reporting

ISE posture has two reports available to the administrator: Posture Assessment by Condition and Posture Assessment by Endpoint. To run either of these reports, navigate to Operations > Reports > Endpoints and Users. The Posture Assessment by Condition report will show the over all compliance status of the endpoint and which conditions passed or failed. The Posture Assessment by Endpoint report shows which endpoints have been subject to posture assessment and also gives the administrator the ability to view the details of each endpoint's posture assessment report.

Identity Services Engine (ISE)

anyconnect compliance conditions deployment design file guide identity services engine ise macos patch policy posture prescriptive registry Remediation usb windows

71 Helpful

Getting Started

Find answers to your questions by entering keywords or phrases in the Search bar above. New here? Use these resources to familiarize yourself with the community:

How to use Community >

New Community Member Guide >

RECOMMENDED

You may like these Guided Resources

Use Guided Resources to complete tasks and track your progress as you realize the value of your technology.

Data Center Guided Resources >

Networking Guided Resources >

Security Guided Resources >

See more >

Quick Links

Discussions >

Guided Resources >

Cisco Cybersecurity Viewpoints >

Related community topics

ISE Wired PoC Prescriptive Guide

GQ

08-12-2019 03:17 PM

✓ Prescriptive guide for ISE VPN

Madura Malwatte

04-05-2019 09:51 PM

✔ **Cisco ISE Device Administration Prescriptive Deployment Guide**

gvanbon
04-26-2019 12:42 AM

✔ **Cisco Anyconnect ISE Posture with intune**

ipagliani
07-21-2023 05:49 AM

2. Introducing Cisco ISE Deployment - 2.1 & 2.2

Kai Shin
08-10-2023 12:59 AM

Customers Also Viewed These Support Documents

Compare ISE Posture Redirection Flow to ISE Posture Redirectionless Flow

Cisco Identity Services Engine Administrator Guide, Release 2.2 --- Configure Client Posture Policies

Cisco Identity Services Engine Administrator Guide, Release 3.2 --- Compliance

ISE Posture Deployment Best Practices and Considerations

Cisco Identity Services Engine Administrator Guide, Release 3.1 --- Compliance

Top
Privacy Statement › Change Settings ›

Quick Links −

Contacts

Resources and Legal −

Community Feedback

Help

Terms & Conditions

Privacy Statement

Cookie Policy

Trademarks

Site Map