

Configure Cisco ISE 3.1 Posture with Linux

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure](#)

[Configurations on ISE](#)

[Configurations on the switch](#)

[Verify](#)

[Troubleshoot](#)

Introduction

This document describes the procedure to configure and implement a file posture policy for Linux and the Identity Services Engine (ISE).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Anyconnect
- Identity Services Engine (ISE)
- Linux

Components Used

The information in this document is based on these software and hardware versions:

- Anyconnect 4.10.05085
- ISE version 3.1 P1
- Linux Ubuntu 20.04
- Cisco Switch Catalyst 3650. Version 03.07.05.E (15.12(3)E5)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configure

Configurations on ISE

Step 1. Update posture service:

Navigate to **Work Centers > Posture > Settings > Software Updates > Posture Updates**. Select Update now and wait for the process to finish:

The screenshot shows the Cisco ISE Work Centers - Posture settings page. The left sidebar contains navigation options: Posture General Settings, Endpoint Scripts, Reassessment configurations, Acceptable Use Policy, Software Updates (expanded), Client Provisioning, Posture Updates (selected), and Proxy Settings. The main content area is titled 'Posture Updates' and includes the following configuration options:

- Web Offline
- * Update Feed URL: <https://www.cisco.com/web/secure/spa/posture-...> (Set to Default button)
- Proxy Address: _____ (info icon)
- Proxy Port: _____
- Automatically check for updates starting from initial delay: HH:MM:SS every 2 hours (info icon)

Buttons at the bottom: Save, Update Now, Reset.

Update Information

Last successful update on	2022/03/24 11:40:59
Last update status since ISE was started	Last update attempt at 2022/03/24 11:40:59 was successful
Cisco conditions version	277896.0.0.0
Cisco AV/AS support chart version for windows	261.0.0.0
Cisco AV/AS support chart version for Mac OSX	179.0.0.0
Cisco AV/AS support chart version for Linux	15.0.0.0
Cisco supported OS version	71.6.2.0

A **Cisco-provided package** is a software package that you download from the Cisco.com site, such as the AnyConnect software packages. A **customer-created package** is a profile or a configuration that you created outside the ISE user interface and want to upload to ISE for use with posture assessment. For this exercise, you can download the AnyConnect webdeploy package “anyconnect-linux64-4.10.05085-webdeploy-k9.pkg”.

Note: Due to updates and patches, the recommended version can change. Use the latest recommended version from the cisco.com site.

Step 2. Upload AnyConnect package:

From within the Posture Work center, navigate to **Client Provisioning > Resources**

Cisco ISE Work Centers - Posture

Overview Network Devices **Client Provisioning** Policy Elements Posture Policy Policy Sets Troubleshoot Reports Settings

Client Provisioning Policy
Resources
 Client Provisioning Portal

Resources

[Edit](#) [+ Add](#) [Duplicate](#) [Delete](#)

<input type="checkbox"/>	Name	Type	Version	Last Update	Description
<input type="checkbox"/>	CiscoTemporalAgentOSX 4...	CiscoTemporalAgent...	4.10.2051.0	2021/08/09 19:12:31	With CM: 4.3.1858.4353
<input type="checkbox"/>	Cisco-ISE-Chrome-NSP	Native Supplicant Pro...	Not Applic...	2016/10/06 20:01:12	Pre-configured Native S...
<input type="checkbox"/>	CiscoAgentlessOSX 4.10.02...	CiscoAgentlessOSX	4.10.2051.0	2021/08/09 19:12:36	With CM: 4.3.1858.4353
<input type="checkbox"/>	MacOsXSPWizard 2.7.0.1	MacOsXSPWizard	2.7.0.1	2021/08/09 19:12:27	Supplicant Provisioning ...
<input type="checkbox"/>	CiscoAgentlessWindows 4.1...	CiscoAgentlessWind...	4.10.2051.0	2021/08/09 19:12:33	With CM: 4.3.2227.6145
<input type="checkbox"/>	Cisco-ISE-NSP	Native Supplicant Pro...	Not Applic...	2016/10/06 20:01:12	Pre-configured Native S...
<input type="checkbox"/>	WinSPWizard 3.0.0.3	WinSPWizard	3.0.0.3	2021/08/09 19:12:27	Supplicant Provisioning ...
<input type="checkbox"/>	CiscoTemporalAgentWindo...	CiscoTemporalAgent...	4.10.2051.0	2021/08/09 19:12:28	With CM: 4.3.2227.6145

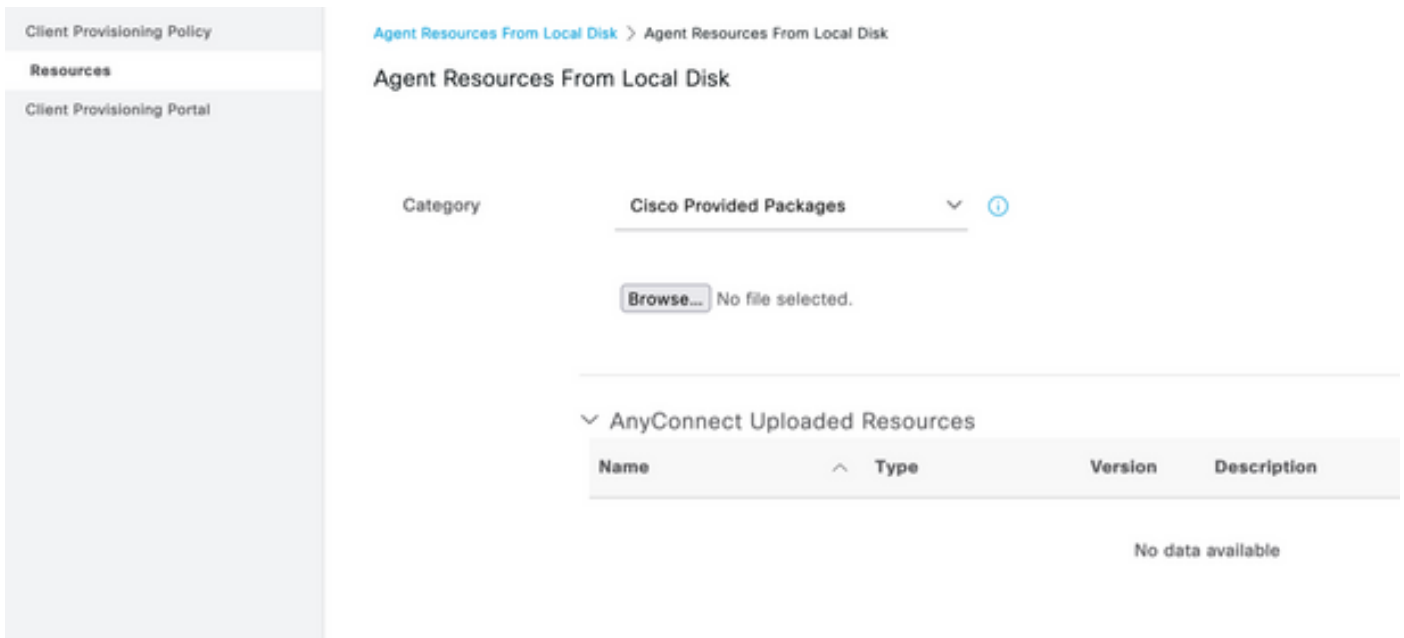
Step 3. Select Add > Agent Resources from Local Disk

Resources

[Edit](#) [+ Add](#) [^](#) [Duplicate](#) [Delete](#)

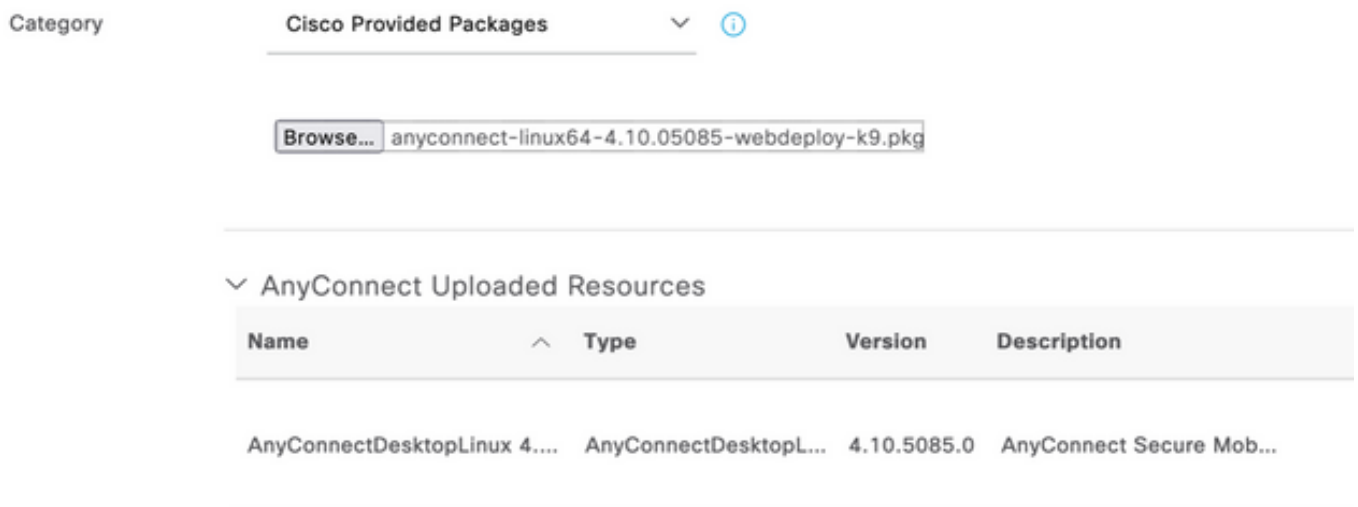
<input type="checkbox"/>	Agent resources from Cisco site
<input type="checkbox"/>	Agent resources from local disk

Step 4. Select Cisco Provided Packages from the Category dropdown.



Step 5. Click Browse.

Step 6. Choose one of the AnyConnect packages that you downloaded in the previous step. The AnyConnect image is processed, and the information about the package is displayed



Step 7. Click **Submit**. Now that AnyConnect is uploaded to ISE, you can have ISE contact and get the other client resources from Cisco.com.

Note: Agent Resources include modules used by the AnyConnect Client that provides the ability to assess an endpoint's compliance for a variety of condition checks such as Anti-Virus, Anti-Spyware, Anti-Malware, Firewall, Disk Encryption, File, and so on.

Step 8. Click **Add > Agent Resources from Cisco Site**. It takes a minute for the window to populate as ISE reaches out to Cisco.com and retrieves a manifest of all the published resources for client provisioning.

Resources

Edit + Add ^ Duplicate Delete

<input type="checkbox"/>			Version	Last Update	Description
<input type="checkbox"/>	Agent resources from Cisco site				
<input type="checkbox"/>	Agent resources from local disk	oTemporalAgent...	4.10.2051.0	2021/08/09 19:12:31	With CM: 4.3.1858.4353
<input type="checkbox"/>	Native Supplicant Profile	ve Supplicant Pro...	Not Applic...	2016/10/06 20:01:12	Pre-configured Native S...
<input type="checkbox"/>	AnyConnect Configuration	oAgentlessOSX	4.10.2051.0	2021/08/09 19:12:36	With CM: 4.3.1858.4353
<input type="checkbox"/>	AnyConnect Posture Profile	OsXSPWizard	2.7.0.1	2021/08/09 19:12:27	Supplicant Provisioning ...
<input type="checkbox"/>	AMP Enabler Profile	oAgentlessWind...	4.10.2051.0	2021/08/09 19:12:33	With CM: 4.3.2227.6145
<input type="checkbox"/>	Cisco-ISE-NSP	Native Supplicant Pro...	Not Applic...	2016/10/06 20:01:12	Pre-configured Native S...
<input type="checkbox"/>	WinSPWizard 3.0.0.3	WinSPWizard	3.0.0.3	2021/08/09 19:12:27	Supplicant Provisioning ...
<input type="checkbox"/>	CiscoTemporalAgentWindo...	CiscoTemporalAgent...	4.10.2051.0	2021/08/09 19:12:28	With CM: 4.3.2227.6145

Step 9. Select the latest AnyConnect compliance modules for Linux. In addition, you can also select the compliance module for Windows and Mac.



Download Remote Resources

<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	AnyConnectComplianceModuleLinux64 4.3.1968.0	AnyConnect Linux Compliance Module 4.3.1968.0
<input checked="" type="checkbox"/>	AnyConnectComplianceModuleLinux64 4.3.2028.0	AnyConnect Linux Compliance Module 4.3.2028.0
<input type="checkbox"/>	AnyConnectComplianceModuleOSX 3.6.11682.2	AnyConnect OS X Compliance Module 3.6.11682.2
<input type="checkbox"/>	AnyConnectComplianceModuleOSX 4.3.2277.4353	AnyConnect OSX Compliance Module 4.3.2277.4353
<input checked="" type="checkbox"/>	AnyConnectComplianceModuleOSX 4.3.2338.4353	AnyConnect OSX Compliance Module 4.3.2338.4353
<input type="checkbox"/>	AnyConnectComplianceModuleWindows 3.6.1168...	AnyConnect Windows Compliance Module 3.6.11682.2
<input type="checkbox"/>	AnyConnectComplianceModuleWindows 4.3.2617...	AnyConnect Windows Compliance Module 4.3.2617.6145
<input checked="" type="checkbox"/>	AnyConnectComplianceModuleWindows 4.3.2716...	AnyConnect Windows Compliance Module 4.3.2716.6145
<input type="checkbox"/>	CiscoAgentlessOSX 4.10.05050	With CM: 4.3.2277.4353

For AnyConnect software, please download from <http://cisco.com/go/anyconnect>. Use the "Agent resource from local disk" add option, to import into ISE

Cancel Save

Step 10. Select the latest temporal agents for Windows and Mac.

<input checked="" type="checkbox"/>	CiscoTemporalAgentOSX 4.10.06011	Cisco Temporal Agent for OSX With CM: 4.3.2338.4353
<input type="checkbox"/>	CiscoTemporalAgentWindows 4.10.05050	Cisco Temporal Agent for Windows With CM: 4.3.2617.614!
<input checked="" type="checkbox"/>	CiscoTemporalAgentWindows 4.10.06011	Cisco Temporal Agent for Windows With CM: 4.3.2716.614!

Step 11. Click Save.

Note: MAC and Windows Posture configurations are out of the scope of this configuration guide.

At this point, you have uploaded and updated all the required parts. It is now time to build the configuration and profiles required to use those components.

Step 12. Click Add > NAC Agent or AnyConnect Posture Profile.

	Version	Last Update	Description
oTemporalAgent...	4.10.2051.0	2021/08/09 19:12:31	With CM: 4.3.1858.4353
oTemporalAgent...	4.10.6011.0	2022/03/24 11:49:19	Cisco Temporal Agent fo...
ConnectComplian...	4.3.2716....	2022/03/24 11:49:39	AnyConnect Windows C...
ve Supplicant Pro...	Not Applic...	2016/10/06 20:01:12	Pre-configured Native S...
oAgentlessOSX	4.10.2051.0	2021/08/09 19:12:36	With CM: 4.3.1858.4353

ISE Posture Agent Profile Settings > New Profile

AnyConnect Posture Profile

Name *
LinuxACPosture

Description:

Parameter	Value	Description
Enable debug log	No	Enables the debug log on the agent
Operate on non-802.1X wireless	No	Enables the agent to operate on non-802.1X wireless networks.
Enable signature check ⓘ	No	Check the signature of executables before running them.
Log file size	5 MB	The maximum agent log file size
Remediation timer ⓘ	4 mins	If the user fails to remediate within this specified time, mark them as non-compliant.
Stealth Mode	Disabled	AnyConnect can act as either clientless or standard mode. When stealth mode is enabled, it runs as a service without any user interface.
Enable notifications in stealth mode	Disabled	Display user notifications even when in Stealth mode.

The parameters that need to be modified are:

- **VLAN detection interval:** This setting enables you to set the number of seconds the module waits between probing for VLAN changes. The recommendation is 5 seconds.
- **Ping or ARP:** This is the actual VLAN change detection method. The agent can ping the default gateway or monitor the ARP cache for the default gateway's entry to timeout or both. The recommended setting is ARP.
- **Remediation timer:** When an endpoint's posture is unknown, the endpoint is put through a posture assessment flow. It takes time to remediate failed posture checks; the default time is 4 minutes before marks the endpoint as noncompliant, but the values can range from 1 to 300 minutes (5 hours). The recommendation is 15 minutes; however, this can require adjustments if remediation is expected to take longer.

Note: Linux File Posture does not support automatic remediation.

For a comprehensive description of all the parameters please refer to the ISE or AnyConnect posture documentation.

Step 13. Agent Behavior select Posture probes Backup List and select **Choose**, select the PSN/Standalone FQDN and Select **Save**

Choose PSNs

Choose specific PSNs or cluster virtual IPs as the backup list to which AnyConnect sends posture state synchronization probes. You can choose a maximum of 6 entries.

List of PSNs

ise30.ciscoise.lab ×  

Cancel

Select

Step 14. Under Posture Protocols > Discovery Host define the PSN/Standalone node ip address.

Step 15. From **Discovery backup server list** and Select **choose**, select your PSN or standalone FQDN and select **Select**.

Choose PSNs

Choose specific PSNs or cluster virtual IPs as the backup list to which AnyConnect sends posture state synchronization probes. You can choose a maximum of 6 entries.

List of PSNs

ise30.ciscoise.lab ×



Cancel

Select

Step 16. Under **Server name rules** type * to contact all the servers and define the PSN/Standalone IP address under **call home list**. Alternatively, a wildcard can be used to match all potential PSNs in your network (that is *.acme.com).

Posture Protocol		
Parameter	Value	Description
PRA retransmission time	120 secs	This is the agent retry period if there is a Passive Reassessment communication failure
Retransmission Delay ⓘ	60 secs	Time (in seconds) to wait before retrying.
Retransmission Limit ⓘ	4	Number of retries allowed for a message.
Discovery host ⓘ	10.52.13.173	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 ⓘ	1 PSN(s)	By default, AnyConnect sends discovery probes to all the Cisco ISE PSNs sequentially if the PSN is unreachable. Choose specific PSNs as the backup list and restrict the nodes to which AnyConnect sends discovery probes.
Server name rules * ⓘ	*	A list of wildcarded, comma-separated names that defines the servers that the agent can connect to. E.g. *.cisco.com*
Call Home List ⓘ	10.52.13.173	A list of IP addresses, that defines the all the Policy service nodes that the agent will try to connect to if the PSN that authenticated the endpoint doesn't respond for some reason.
Back-off Timer ⓘ	30 secs	Anyconnect agent will continuously try to reach discovery targets (redirection targets and previously connected PSNs) by sending the discovery packets till this max time limit is reached

Step 17. Click **Add > AnyConnect Configuration**

Client Provisioning Policy

Resources

Client Provisioning Portal

Resources

 Edit  Add ^  Duplicate  Delete

<input type="checkbox"/>	Agent resources from Cisco site
<input type="checkbox"/>	Agent resources from local disk
<input type="checkbox"/>	Native Supplicant Profile
<input type="checkbox"/>	AnyConnect Configuration
<input type="checkbox"/>	AnyConnect Posture Profile
<input type="checkbox"/>	AMP Enabler Profile

* Select AnyConnect Package:

0.5085.0 

*

Configuration
Name:


LinuxAnyConnect Configuration

AnyConnectDesktopWindows 4.10.5085.0
AnyConnectDesktopLinux 4.10.5085.0

Description:

Description Value Notes

* Compliance
Module

3.2028.0 

AnyConnectComplianceModuleLinux64 4.3.1676.0

AnyConnectComplianceModuleLinux64 4.3.2028.0

AnyConnect

AnyConnect Module Selection

ISE Posture

VPN

ASA Posture

Network
Visibility

Diagnostic
and Reporting
Tool

Profile Selection

* ISE Posture CPosture ▾

VPN

Network
Visibility

Customer
Feedback

LinuxACPosture

▾

Scroll down and select **Submit**

Step 18. When you finished to make selections, click **Submit**.

Step 19. Select **Work Centers > Posture > Client Provisioning > Client Provisioning Portals**.

The screenshot shows the Cisco ISE configuration interface for Client Provisioning Portals. The navigation tabs at the top include Overview, Network Devices, Client Provisioning (selected), Policy Elements, Posture Policy, Policy Sets, and Troubleshoot. The left sidebar shows a tree view with Client Provisioning Policy, Resources, and Client Provisioning Portal (selected). The main content area is titled 'Client Provisioning Portals' and contains the text: 'You can edit and customize the default Client Provisioning portal and create additional ones'. Below this text are four buttons: Create, Edit, Duplicate, and Delete. A card for the 'Client Provisioning Portal (default)' is displayed, with a description: 'Default portal and user experience used to install the posture agents and verify compliance on user's devices'.

Step 20. Under the **Portal Settings** section, where you can select the interface and port, as well as the groups that are authorized to the page Select Employee, SISE_Users and Domain Users.

Configure authorized groups

User account with Super admin privilege or ERS admin privilege will have access to the portal

Available		Chosen
<input type="text"/>	<input type="button" value="➤"/>	
ALL_ACCOUNTS (default)		Employee
GROUP_ACCOUNTS (default)	<input type="button" value="➤"/>	
OWN_ACCOUNTS (default)	<input type="button" value="➤"/>	

Step 21. Under Log in Page Settings, ensure **Enable auto Log In** option is enabled

Login Page Settings

Enable Auto Login ⓘ

Maximum failed login attempts before rate limiting: 5 (1 - 999)

Time between login attempts when rate limiting: 2 (1 - 999)

Include an AUP as link ▼

- Require acceptance
- Require scrolling to end of AUP

Step 22. On the upper right corner Select **Save**

Step 23.Select **Work Centers > Posture > Client Provisioning > Client Provisioning Policy**.

Step 24. Click the down arrow next to the **IOS** rule in the **CPP** and choose **Duplicate Above**

Step 25. Name the rule **LinuxPosture**

Step 26. For Results, select the **AnyConnect Configuration** as the agent.

Note: In this case, you do not see a compliance module dropdown because it is configured as part of the AnyConnect configuration.

The screenshot displays the Cisco ISE interface for configuring a Client Provisioning Policy. The page title is "Client Provisioning Policy" and it includes a navigation menu with options like Overview, Network Devices, Client Provisioning, Policy Elements, Posture Policy, Policy Sets, Troubleshoot, Reports, and Settings. A sidebar on the left shows "Client Provisioning Policy" and "Resources". The main content area contains a table of rules. The "LinuxPosture" rule is selected, showing its configuration details.

Rule Name	Identity Groups	Operating Systems	Other Conditions	Results
LinuxPosture	If Any	and Linux All	and Condition(s)	then LinuxAnyConnect Configuration
IOS	If Any	and Apple IOS All	and Condition(s)	then Cisco-ISE-NSP
Android	If Any	and Android	and Condition(s)	then Cisco-ISE-NSP
Windows	If Any	and Windows All	and Condition(s)	then CiscoTemporalAgentWindows 4.10.02051 And WinSPWizard 3.0.0.3 And Cisco-ISE-NSP
MAC OS	If Any	and Mac OSX	and Condition(s)	then CiscoTemporalAgentOSX 4.10.02051 And MacOsXSPWizard 2.7.0.1 And Cisco-ISE-NSP

Step 27.Click **Done**.

Step 28. Click **Save**.

Posture Policy Elements

Step 29.Select **Work Centers > Posture > Policy Elements > Conditions > File**. Select **Add**.

Step 30.Define **TESTFile** as the file condition name and define the next values

File Condition

Name *	TESTFile	
Description		
* Operating System	Linux All	
Compliance Module	Any version	
* File Type	FileExistence	
* File Path	home	Testfile.csv
* File Operator	Exists	

Note: Path is based on the file location.

Step 31. Select **Save**

FileExistence. This file type of condition looks to see if a file exists in the system where it is supposed to—and that is all. With this option selected, there is no concern at all for validate the file dates, hashes, and so on

Step 32. Select Requirements and create a new policy as follows:

Name	Operating System	Compliance Module	Posture Type	Conditions	Remediations Actions
Any_AV_Installation_Win	for Windows All	using 3.x or earlier	using AnyConnect	met if ANY_av_win_inst	then Message Text Only
LinuxFile	for Linux All	using 4.x or later	using AnyConnect	met if TESTFile	then Select Remediations

Note: Linux does not support Message text only as remediation action

Requirement components

- **Operating system:** Linux All
- **Compliance module:** 4.x
- **Posture type:** AnyConnect
- **Conditions:** Compliance modules and agents (which become available after you select the OS)
- **Remediation actions:** Remediations that become available for selection after all the other conditions have been chosen.

Step 33. Select **Work Centers > Posture > Posture Policy**

Step 34. Select **Edit** on any policy and Select Insert New policy Define **LinuxPosturePolicy** as the name and ensure you add your requirement created in step 32.

Posture Policy

Define the Posture Policy by configuring rules based on operating system and/or other conditions.

Status	Policy Options	Rule Name	Identity Groups	Operating Systems	Compliance Module	Posture Type	Other Conditions	Requirements	
<input type="checkbox"/>	Policy Options	Default_AnyMalware_Policy_Ma	Any	and Mac OSX	and 4.x or later	and AnyConnect	and	than Any_AM_Installation_Ma	Edit
<input checked="" type="checkbox"/>	Policy Options	LinuxPosturePolic	Any	and Linux All	and 4.x or later	and AnyConnect	and	than LinuxFile	Edit

Step 35. Select **Done** and **Save**

Other Important Posture Settings (Posture General Settings section)

Posture General Settings (i)

Remediation Timer Minutes (i)

Network Transition Delay Seconds (i)

Default Posture Status (i)

Automatically Close Login Success Screen After Seconds (i)

Continuous Monitoring Interval Minutes (i)

Acceptable Use Policy in Stealth Mode

Posture Lease

Perform posture assessment every time a user connects to the network

Perform posture assessment every Days (i)

Cache Last Known Posture Compliant Status

Last Known Posture Compliant State

The important settings in the Posture General Settings section are as follows:

- **Remediation Timer:** This setting defines the amount of time a client has to correct a failed posture condition. There is also a remediation timer in the AnyConnect configuration; this timer is for ISE, not AnyConnect.
- **Default Posture Status:** This setting provides the posture status for devices without the posture agent or operating systems that cannot run the temporal agent, such as Linux-based operating systems.
- **Continuous Monitoring Interval:** This setting applies to the application and hardware conditions that are taking inventory of the endpoint. The setting specifies how often AnyConnect must send the monitoring data.

- **Acceptable Use Policy in Stealth Mode:** The only two choices for this setting are to block or continue. Block prevents stealth mode AnyConnect clients from proceeding if the AUP has not been acknowledged. Continue allows the stealth mode client to proceed even without acknowledging the AUP (which is often the intent when using the stealth mode setting of AnyConnect).

Reassessment Configurations

Posture reassessments are a critical component of the posture workflow. You saw how to configure the AnyConnect agent for posture reassessment in the “Posture Protocol” section. The agent periodically checks in with the PSNs defined based on the timer in that configuration.

When a request reaches the PSN, the PSN determines whether a posture reassessment is needed, based on the ISE configuration for that endpoint’s role. If the client passes the reassessment, the PSN maintains the endpoint’s posture-compliant state, and the posture lease is reset. If the endpoint fails the reassessment, the posture status changes to noncompliant, and any posture lease that existed is removed.

Step 36. Select **Policy > Policy Elements > Results > Authorization > Authorization Profile**. Select **Add**

Step 37. Define **Wired_Redirect** as the Authorization Profile and configure the next parameters

Common Tasks

Web Redirection (CWA, MDM, NSP, CPP) ⓘ

Client Provisioning (Posture) ▾ ACL ACL_REDIRECT_AV ▾ Value Client Provisioning Portal (def: ▾

Static IP/Host name/FQDN

Suppress Profiler CoA for endpoints in Logical Profile

Auto Smart Port

Step 38. Select **Save**

Step 39. Configure Authorization policies

There are three preconfigured authorization rules for posture:

1. The first is configured to match when authentication succeeds, and a device’s compliance is unknown.
2. The second rule matches successful authentications with non-compliant endpoints.

Note: Both of the first two rules have the same result, which is to use a preconfigured authorization profile that redirects the endpoint to the Client Provisioning portal.

3. The final rule matches successful authentication and posture-compliant endpoints and uses the prebuilt PermitAccess authorization profile.

Select **Policy > Policy Set** and select the right arrow for **Wired 802.1x - MAB** Created in the previous lab.

Step 40. Select **Authorization Policy** and create the next rules

	SISE_UnknownCompliance_Redirect	AND	<ul style="list-style-type: none"> Network_Access_Authentication_Passed Compliance_Unknown_Devices ISEAD ExternalGroups EQUALS ciscoise lab/Users/Domain Users 	<input type="text" value="PostureISE"/> + <input type="text" value="Select from list"/> + 9	
	SISE_NonCompliance_Redirect	AND	<ul style="list-style-type: none"> Non_Compliant_Devices Network_Access_Authentication_Passed ISEAD ExternalGroups EQUALS ciscoise lab/Users/Domain Users 	<input type="text" value="PostureISE"/> + <input type="text" value="Select from list"/> + 0	
	SISE_Compliance_Device_Access	AND	<ul style="list-style-type: none"> Compliant_Devices Network_Access_Authentication_Passed ISEAD ExternalGroups EQUALS ciscoise lab/Users/Domain Users 	<input type="text" value="NewAP"/> + <input type="text" value="Select from list"/> + 2	

Configurations on the switch

Note: The below configuration refers to IBNS 1.0. There can be differences for IBNS 2.0 capable switches. It includes Low Impact mode deployment.

```

username <admin> privilege 15 secret <password>
aaa new-model
!
aaa group server radius RAD_ISE_GRP
server name <isepsnode_1> server name ! aaa authentication dot1x default group RAD_ISE_GRP aaa
authorization network default group RAD_ISE_GRP aaa accounting update periodic 5 aaa accounting
dot1x default start-stop group RAD_ISE_GRP aaa accounting dot1x default start-stop group
RAD_ISE_GRP ! aaa server radius dynamic-author client server-key client server-key ! aaa
session-id common ! authentication critical recovery delay 1000 access-session template monitor
epm logging ! dot1x system-auth-control dot1x critical eapol ! # For Access Interfaces:
interface range GigabitEthernetx/y/z - zz
description VOICE-and-Data
switchport access vlan
switchport mode access
switchport voice vlan
ip access-group ACL_DEFAULT in
authentication control-direction in # If supported
authentication event fail action next-method
authentication host-mode multi-auth
authentication open
authentication order dot1x mab
authentication priority dot1x mab
authentication port-control auto

# Enables periodic re-auth, default = 3,600secs
authentication periodic
# Configures re-auth and inactive timers to be sent by the server
authentication timer reauthenticate server
authentication timer inactivity server
authentication violation restrict
mab
snmp trap mac-notification change added
snmp trap mac-notification change removed
dot1x pae authenticator
dot1x timeout tx-period 10
dot1x timeout server-timeout 10
dot1x max-req 3
dot1x max-reauth-req 3
auto qos trust

# BEGIN - Dead Server Actions -
authentication event server dead action authorize vlan
authentication event server dead action authorize voice
authentication event server alive action reinitialize

```

END - Dead Server Actions -

spanning-tree portfast

!

ACL_DEFAULT

! This ACL can be customized to your needs, this is the very basic access allowed prior
! to authentication/authorization. Normally ICMP, Domain Controller, DHCP and ISE
! http/https/8443 is included. Can be tailored to your needs.

!

ip access-list extended ACL_DEFAULT

permit udp any eq bootpc any eq bootps

permit udp any any eq domain

permit icmp any any

permit udp any any eq tftp

permit ip any host

permit ip any host

permit tcp any host eq www

permit tcp any host eq 443

permit tcp any host eq 8443

permit tcp any host eq www

permit tcp any host eq 443

permit tcp any host eq 8443

!

END-OF ACL_DEFAULT

!

ACL_REDIRECT

! This ACL can be customized to your needs, this ACL defines what is not redirected
! (with deny statement) to the ISE. This ACL is used for captive web portal,
! client provisioning, posture remediation, and so on.

!

ip access-list extended ACL_REDIRECT_AV

remark Configure deny ip any host to allow access to

deny udp any any eq domain

deny tcp any any eq domain

deny udp any eq bootps any

deny udp any any eq bootpc

deny udp any eq bootpc any

remark deny redirection for ISE CPP/Agent Discovery

deny tcp any host eq 8443

deny tcp any host eq 8905

deny udp any host eq 8905

deny tcp any host eq 8909

deny udp any host eq 8909

deny tcp any host eq 8443

deny tcp any host eq 8905

deny udp any host eq 8905

deny tcp any host eq 8909

deny udp any host eq 8909

remark deny redirection for remediation AV servers

deny ip any host

deny ip any host

remark deny redirection for remediation Patching servers

deny ip any host

remark redirect any http/https

permit tcp any any eq www

permit tcp any any eq 443

!

END-OF ACL-REDIRECT

!

ip radius source-interface

!

radius-server attribute 6 on-for-login-auth

radius-server attribute 6 support-multiple

```
radius-server attribute 8 include-in-access-req
radius-server attribute 55 include-in-acct-req
radius-server attribute 55 access-request include
radius-server attribute 25 access-request include
radius-server attribute 31 mac format ietf upper-case
radius-server attribute 31 send nas-port-detail
radius-server vsa send accounting
radius-server vsa send authentication
radius-server dead-criteria time 30 tries 3
!
ip http server
ip http secure-server
ip http active-session-modules none
ip http secure-active-session-modules none
!
radius server
  address ipv4 auth-port 1812 acct-port 1813
  timeout 10
  retransmit 3
  key
!
radius server
  address ipv4 auth-port 1812 acct-port 1813
  timeout 10
  retransmit 3
  key
!
aaa group server radius RAD_ISE_GRP
  server name
  server name
!
mac address-table notification change
mac address-table notification mac-move
```

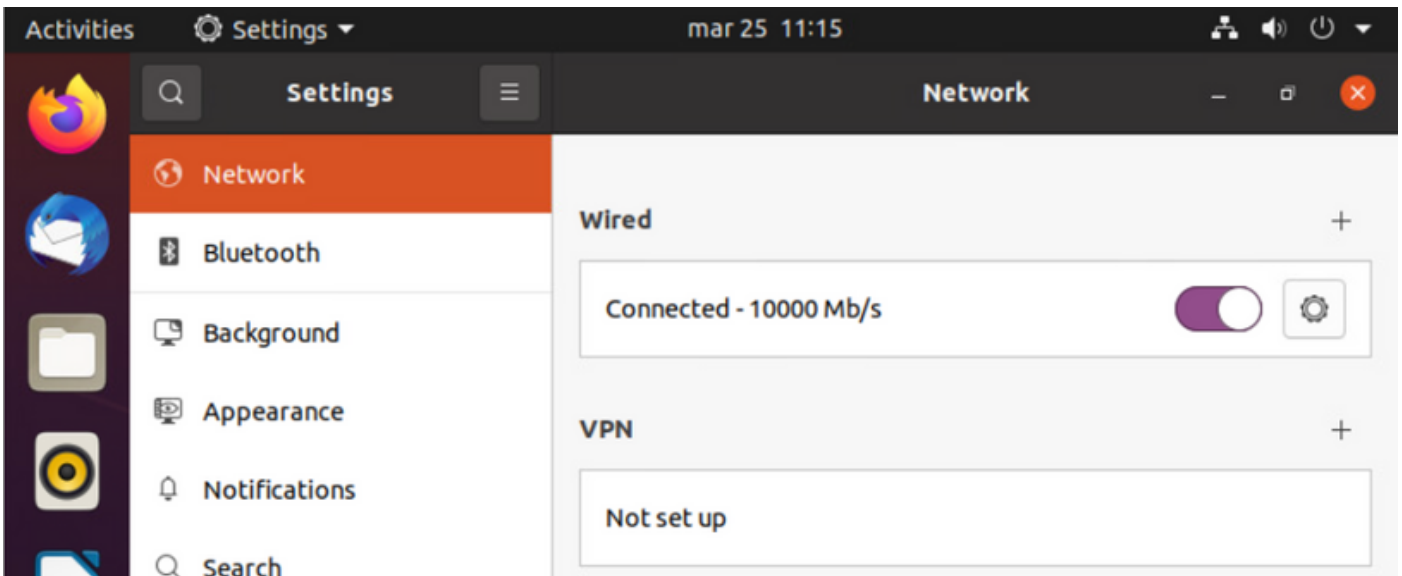
Verify

ISE Verification:

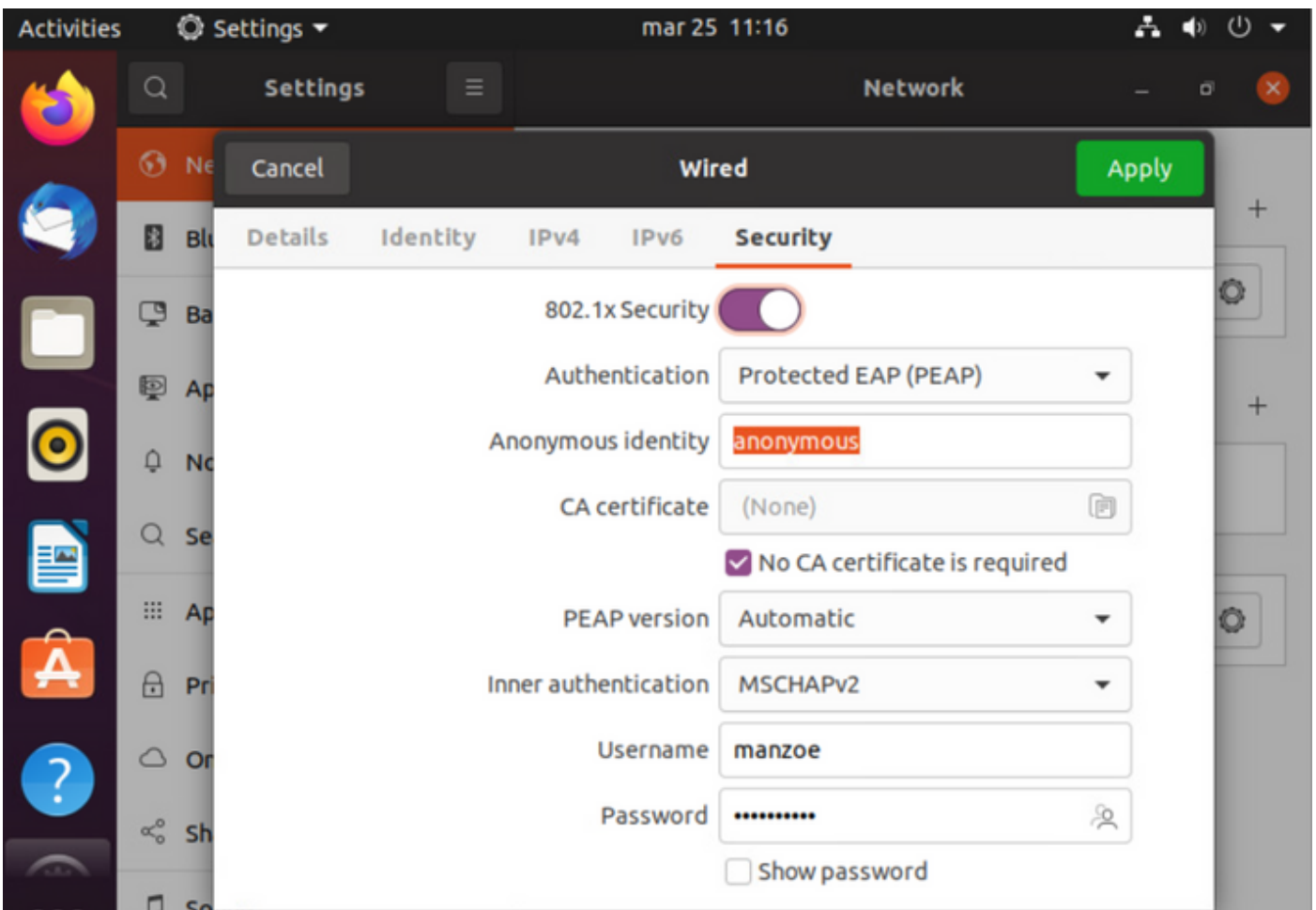
This section assumes that AnyConnect with the ISE posture module has been previously installed on the Linux System.

Authenticate PC using dot1x

Step 1. Navigate to Network Settings



Step 2. Select the Security tab and provide 802.1x configuration and user credentials



Step 3. Click “Apply”.

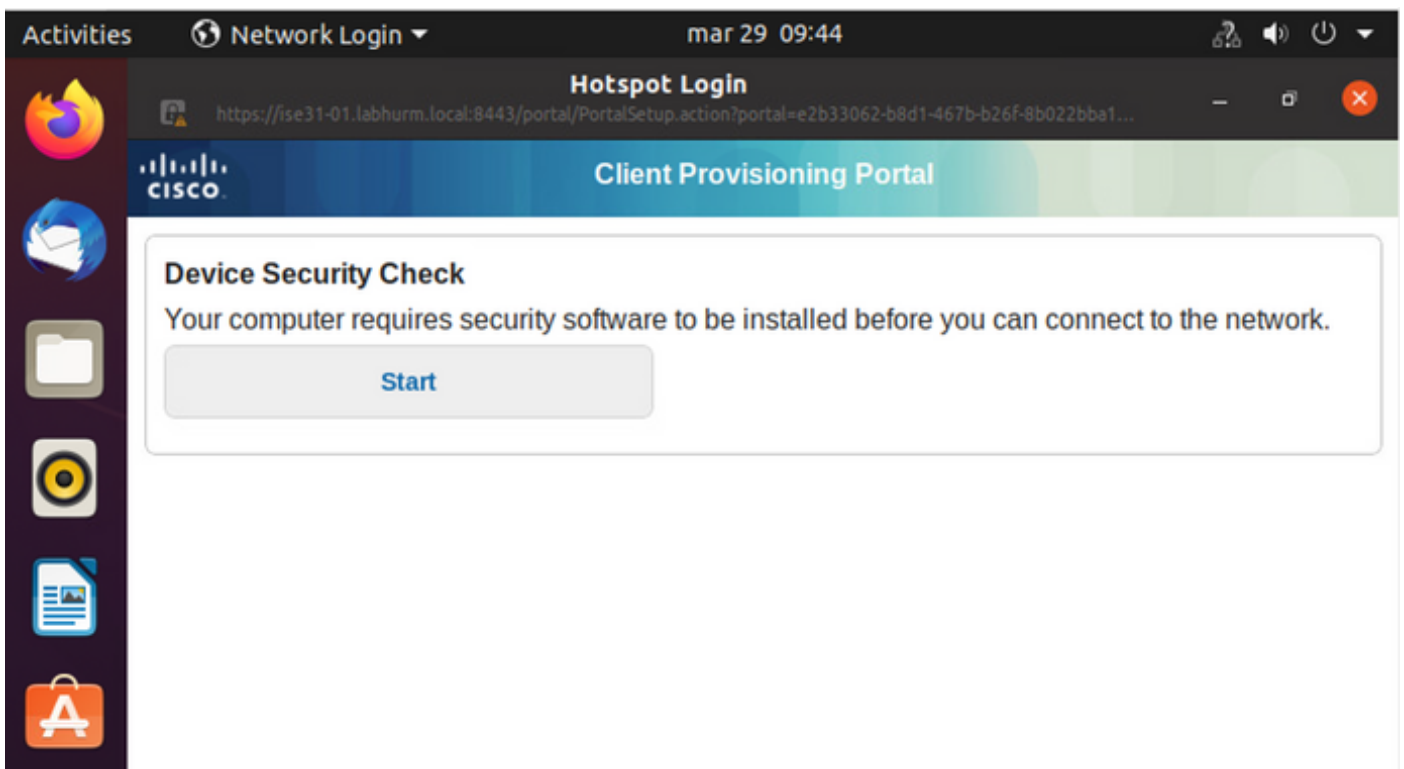
Step 4. Connect the Linux system to the 802.1x wired network and validate in the ISE live log:

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint...	Authenti...	Authoriz...	Authoriz...	IP Address	Network De...	Device Port	Identity Group	Posture
Apr 06, 2022 08:42:09.2...	●	🔒	4	manzoe	00:0C:29:45:03:8F	Ubuntu Wi...	Ubuntu Po...	Ubuntu Po...	Wired_Re...			FastEthernet1...		Pending
Apr 06, 2022 08:32:49.2...	●	🔒		manzoe	00:0C:29:45:03:8F	Ubuntu Wi...	Ubuntu Po...	Ubuntu Po...	Wired_Re...		Cart 3750	FastEthernet1...	Workstation	Pending
Apr 06, 2022 08:32:40.8...	●	🔒		manzoe	00:0C:29:45:03:8F	Ubuntu Wi...	Ubuntu Po...	Ubuntu Po...	Wired_Re...		Cart 3750	FastEthernet1...	Workstation	Pending

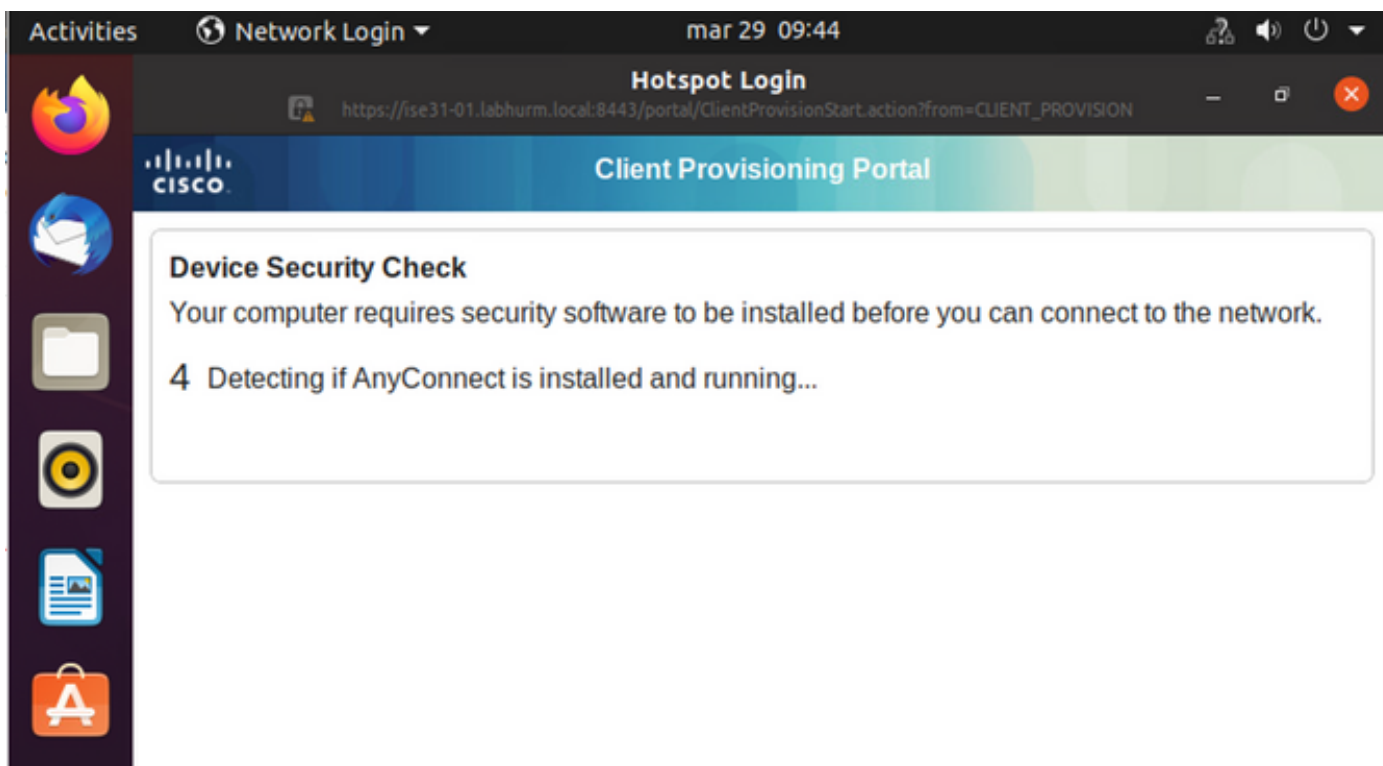
In ISE, use the horizontal scroll bar to view additional information, such as the PSN that served the flow or the posture status:

Authoriz...	Authoriz...	IP Address	Network De...	Device Port	Identity Group	Posture ...	Server
Authorizatic	Authorizatic	IP Address	Network Device	Device Port	Identity Group	Posture Sta	Server
Ubuntu Po...	Wired_Re...			FastEthernet1...		Pending	ise31-01
Ubuntu Po...	Wired_Re...		Cat-3750	FastEthernet1...	Workstation	Pending	ise31-01
Ubuntu Po...	Wired_Re...		Cat-3750	FastEthernet1...	Workstation	Pending	ise31-01

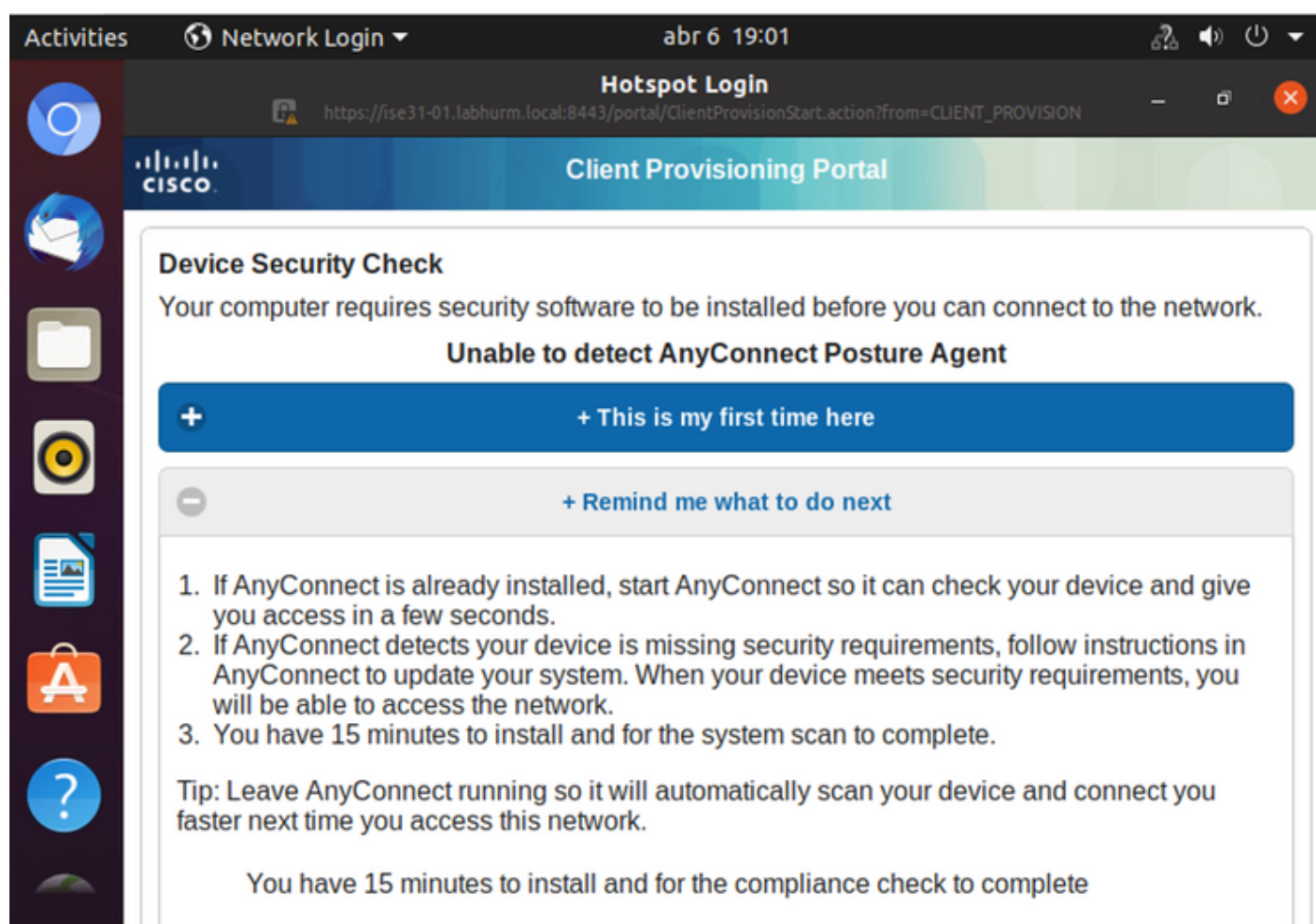
Step 5. On the Linux client, redirection must occur, and it presents the client provisioning portal indicating posture check occurs and to click **“Start”**:



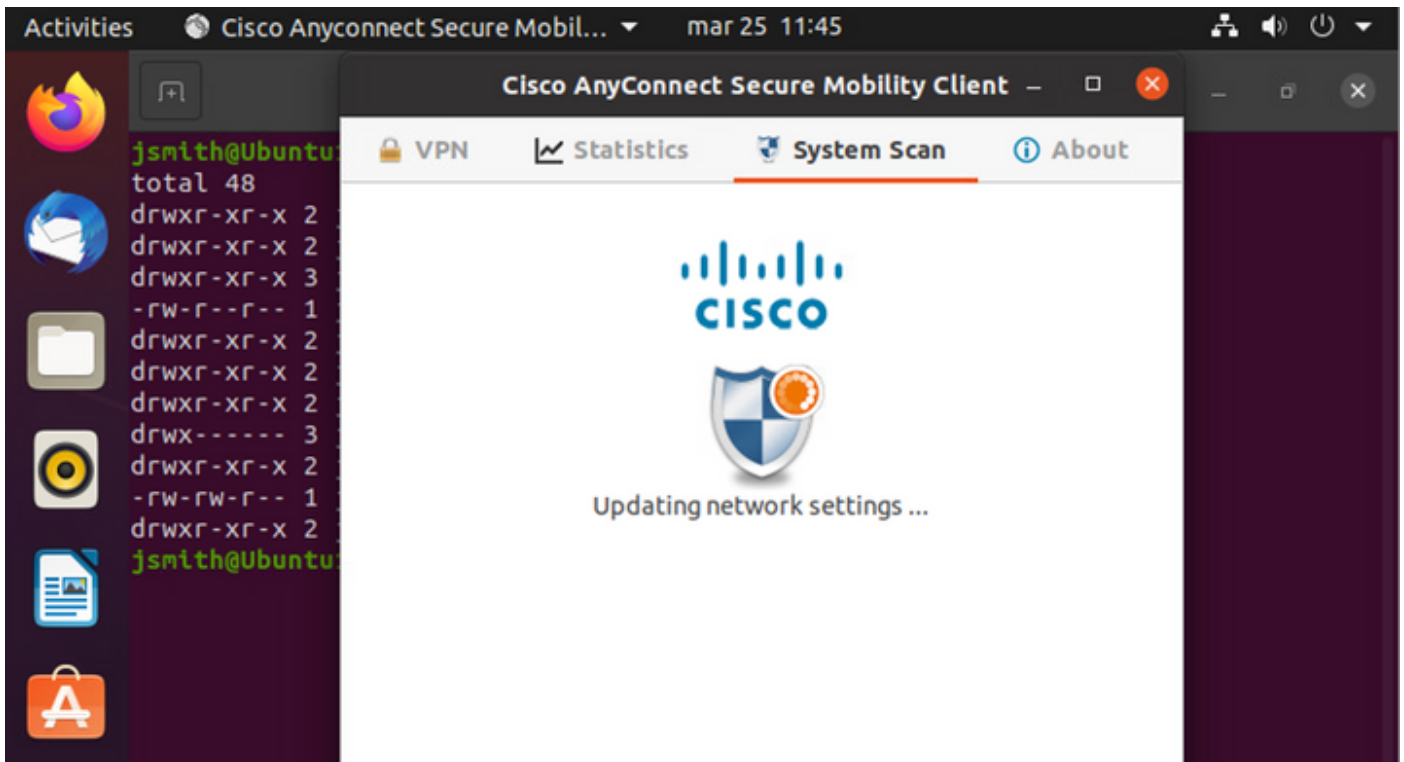
Wait a few seconds while the connector tries to detect AnyConnect:



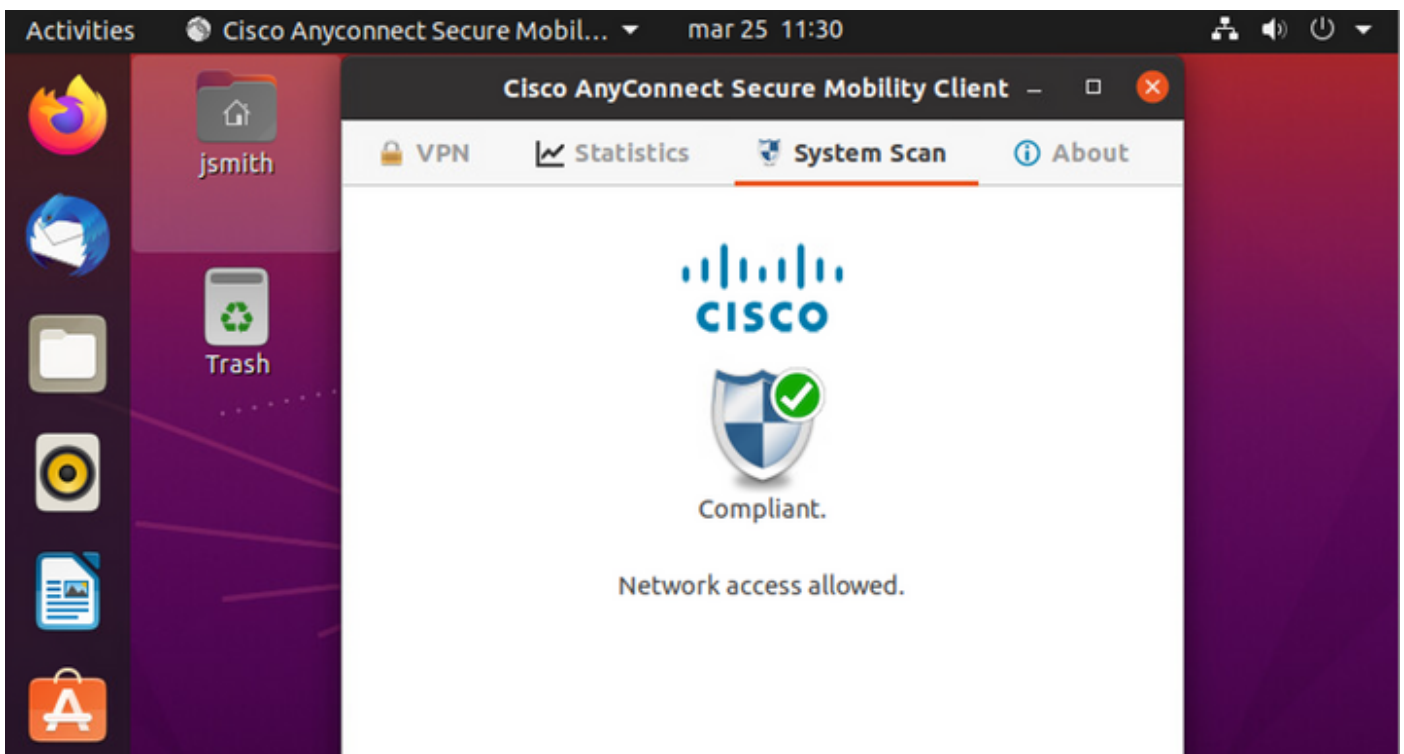
Due to a known caveat, even if AnyConnect is installed it does not detect it. Use **Alt-Tab** or the **Activities** menu to switch to the AnyConnect client.

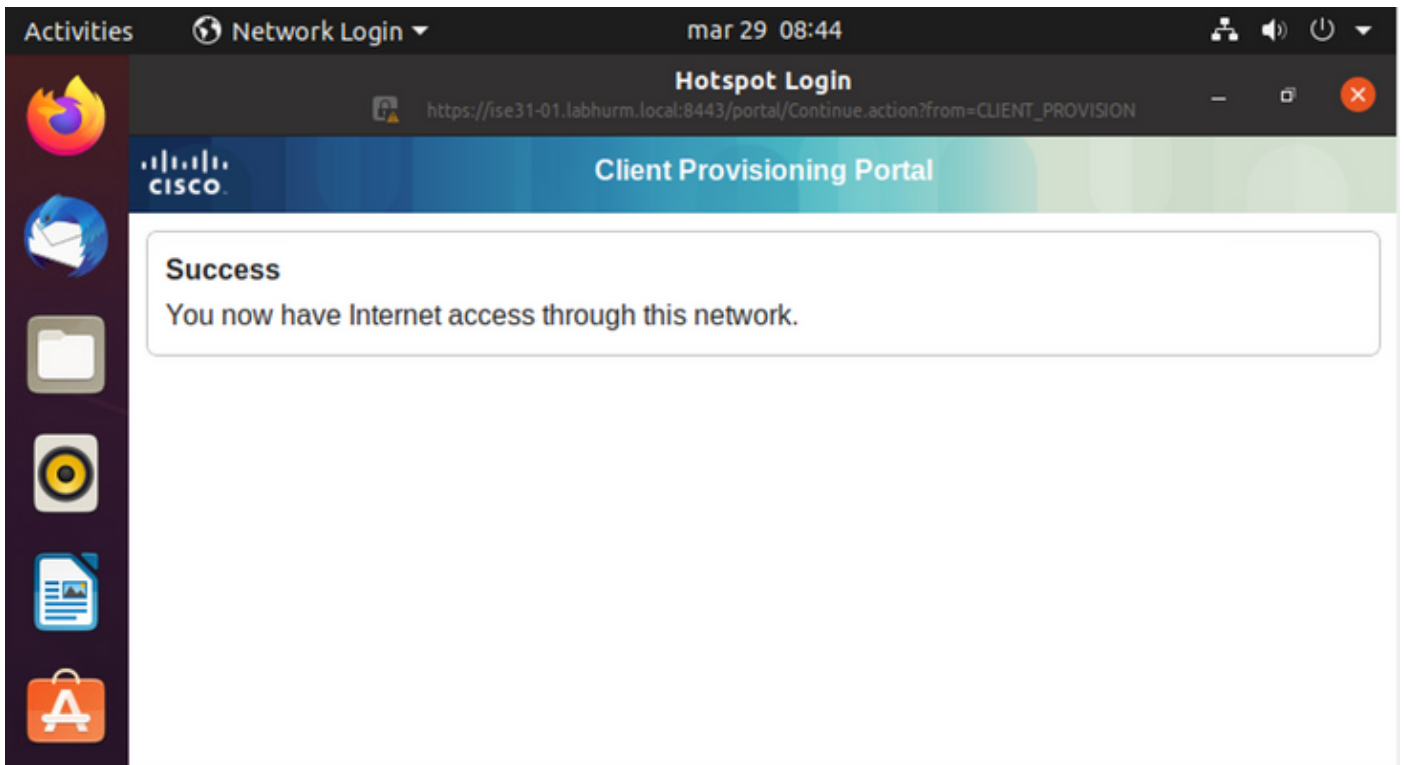


AnyConnect attempts to reach the PSN for posture policy and assess the endpoint against it.



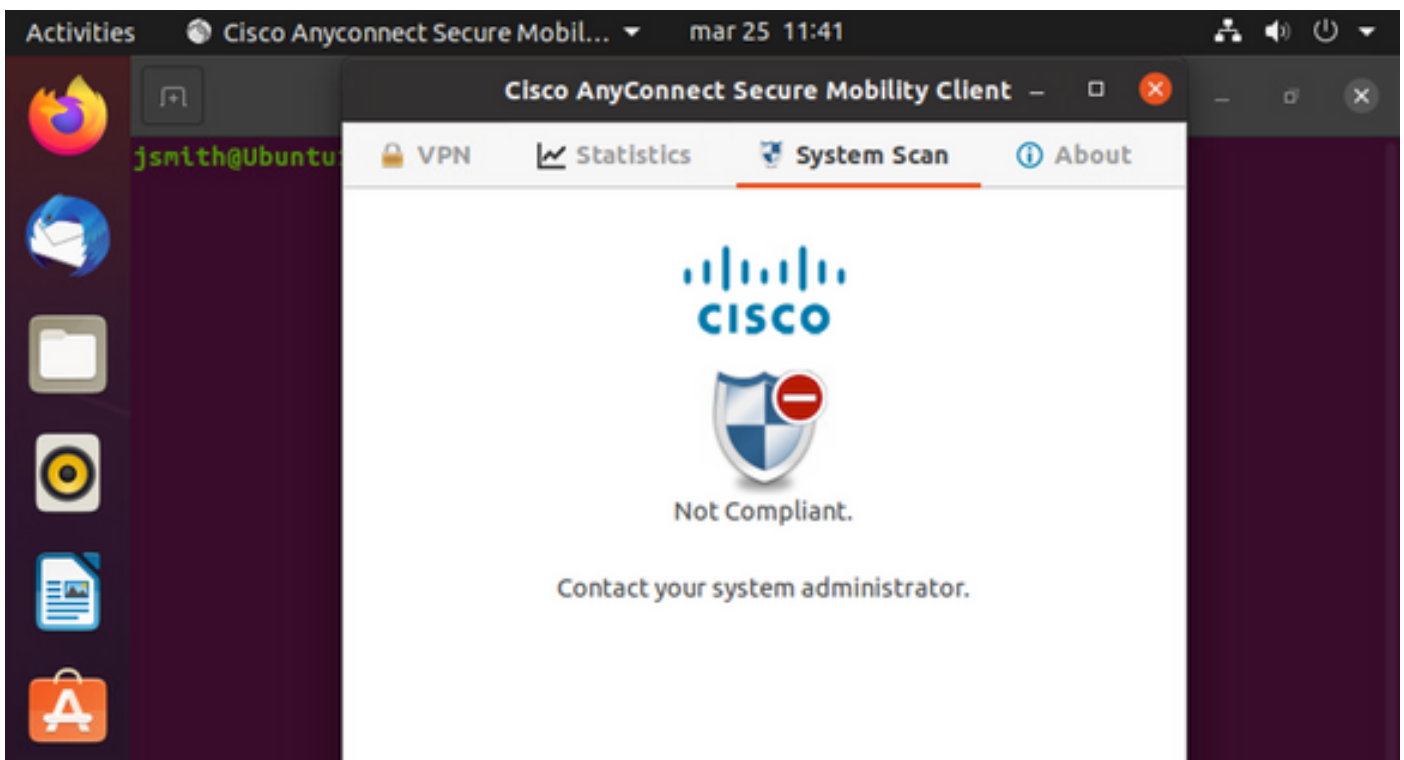
AnyConnect reports its determination of the posture policy back to ISE. In this case, compliant





Endpoint Profile	Authenti...	Authorizati...	Authorization P...	IP Address	Network De...	Device Port	Identity Group	Posture Status	Server
Endpoint Profile	Authenticat...	Authorization I...	Authorization Profile	IP Address	Network Device	Device Port	Identity Group	Posture Status	Server
Ubuntu-Workstation	Wired Merak...	Wired Merak...	PermitAccess	192.168.200.12				Compliant	ise31-01
Ubuntu-Workstation	Wired Merak...	Wired Merak...	PermitAccess		Mraki-SW		Workstation	Compliant	ise31-01
Ubuntu-Workstation	Wired Merak...	Wired Merak...	PermitAccess		Mraki-SW		Workstation	Compliant	ise31-01

On the other hand, if the file does not exist, the AnyConnect posture module reports the determination to ISE



Endpoint...	Authenti...	Authoriz...	Authoriz...	IP Address	Network De...	Device Port	Identity Group	Posture Status	Server	Mdm S
Endpoint Pr	Authenticat	Authorizatic	Authorizatic	IP Address	Network Devic	Device Port	Identity Group	Posture Status	Server	Mdm S
Ubuntu-W...	Ubuntu Po...	Ubuntu Po...	Wired_Re...	192.168.101.51		FastEthernet1...		NonCompliant	ise31-01	
Ubuntu-W...	Ubuntu Po...	Ubuntu Po...	Wired_Re...	192.168.101.51	Cat-3750	FastEthernet1...	Workstation	NonCompliant	ise31-01	

Note: ISE FQDN needs to be resolvable on Linux system through DNS or local host file.

Troubleshoot

show authentication sessions int fa1/0/35

Redirect in place:

```

LABDEMOAC01#show authentication sessions interface fastEthernet 1/0/35
  Interface: FastEthernet1/0/35
  MAC Address: 000c.2946.038f
  IP Address: 192.168.101.51
  User-Name: manzoe
  Status: Authz Success
  Domain: DATA
  Security Policy: Should Secure
  Security Status: Unsecure
  Oper host mode: multi-auth
  Oper control dir: both
  Authorized By: Authentication Server
  Vlan Group: N/A
  URL Redirect ACL: ACL_REDIRECT_AV
  URL Redirect: https://ise31-01.labhurm.local:8443/portal/gateway?sessionId=C0A8C88300000010008044A&p
33062-b8d1-467b-b26f-8b022bba10e7&action=cpp&token=05a438ecb872ce396c2912fecfe0d2aa
  Session timeout: N/A
  Idle timeout: N/A
  Common Session ID: C0A8C88300000010008044A
  Acct Session ID: 0x00000004
  Handle: 0xEB000001

Runnable methods list:
  Method  State
  dot1x   Authc Success

```

Authorization succeeded:

```

LABDEMOAC01#show authentication sessions interface fastEthernet 1/0/35
  Interface: FastEthernet1/0/35
  MAC Address: 000c.2946.038f
  IP Address: 192.168.101.51
  User-Name: manzoe
  Status: Authz Success
  Domain: DATA
  Security Policy: Should Secure
  Security Status: Unsecure
  Oper host mode: multi-auth
  Oper control dir: both
  Authorized By: Authentication Server
  Vlan Group: N/A
  ACS ACL: xACSACLx-IP-PERMIT_ALL_IPV4_TRAFFIC-57f6b0d3
  Session timeout: 28800s (server), Remaining: 28739s
  Timeout action: Reauthenticate
  Idle timeout: N/A
  Common Session ID: C0A8C88300000010008044A
  Acct Session ID: 0x00000004
  Handle: 0xEB000001

Runnable methods list:
  Method  State
  dot1x   Authc Success
  mab     Not run

```

Not Compliant, moved to quarantine VLAN and ACL:

```
LABDEMOAC01#sh auth sess int fas1/0/35
  Interface: FastEthernet1/0/35
  MAC Address: 000c.2946.038f
  IP Address: 192.168.101.51
  User-Name: manzoe
  Status: Authz Success
  Domain: DATA
  Security Policy: Should Secure
  Security Status: Unsecure
  Oper host mode: multi-auth
  Oper control dir: both
  Authorized By: Authentication Server
  Vlan Policy: 777
  ACS ACL: xACSACLx-IP-DENY_ALL_IPV4_TRAFFIC-57f6b0d3
  Session timeout: N/A
  Idle timeout: N/A
  Common Session ID: C0A86E010000000000001724F
  Acct Session ID: 0x00000003
  Handle: 0x9A000000
```

```
Runnable methods list:
  Method  State
  dot1x   Authc Success
  mab     Not run
```