

Configurazione della postura di Cisco ISE 3.1 con Linux

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Configurazioni su ISE](#)

[Configurazioni sullo switch](#)

[Verifica](#)

[Risoluzione dei problemi](#)

Introduzione

Questo documento descrive la procedura per configurare e implementare un criterio di postura dei file per Linux e Identity Services Engine (ISE).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- AnyConnect
- Identity Services Engine (ISE)
- Linux

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Configurazioni su ISE

Passaggio 1. Aggiornare il servizio di postura:

Passare a **Centri di lavoro > Postura > Impostazioni > Aggiornamenti software > Aggiornamenti postura**. Selezionare **Aggiorna** e attendere il completamento del processo:

The screenshot shows the Cisco ISE Work Centers - Posture configuration page. The left sidebar contains a navigation menu with the following items: 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 features a radio button selection for "Web" (selected) and "Offline". Below this, there is a field for "Update Feed URL" with the value "https://www.cisco.com/web/secure/spa/posture-..." and a "Set to Default" button. There are also fields for "Proxy Address" and "Proxy Port". A checkbox labeled "Automatically check for updates starting from initial delay" is present, followed by a time selection interface with dropdowns for HH (11), MM (32), and SS (21), and a frequency of "every 2 hours". At the bottom of the configuration section are three buttons: "Save", "Update Now", and "Reset". Below the configuration section is an "Update Information" section with a table of update details.

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

Un **pacchetto fornito da Cisco** è un pacchetto software che viene scaricato dal sito Cisco.com, ad esempio i pacchetti software AnyConnect. Un **pacchetto creato dal cliente** è un profilo o una configurazione creata al di fuori dell'interfaccia utente ISE e che si desidera caricare nell'ISE per una valutazione della postura. Per questo esercizio, è possibile scaricare il pacchetto AnyConnect webdeploy "anyconnect-linux64-4.10.05085-webdeploy-k9.pkg".

Nota: A causa di aggiornamenti e patch, la versione consigliata può cambiare. Utilizzare la versione più recente consigliata dal sito cisco.com.

Passaggio 2. Caricare il pacchetto AnyConnect:

Dal centro di lavoro di postura, passare a **Provisioning client > Risorse**

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

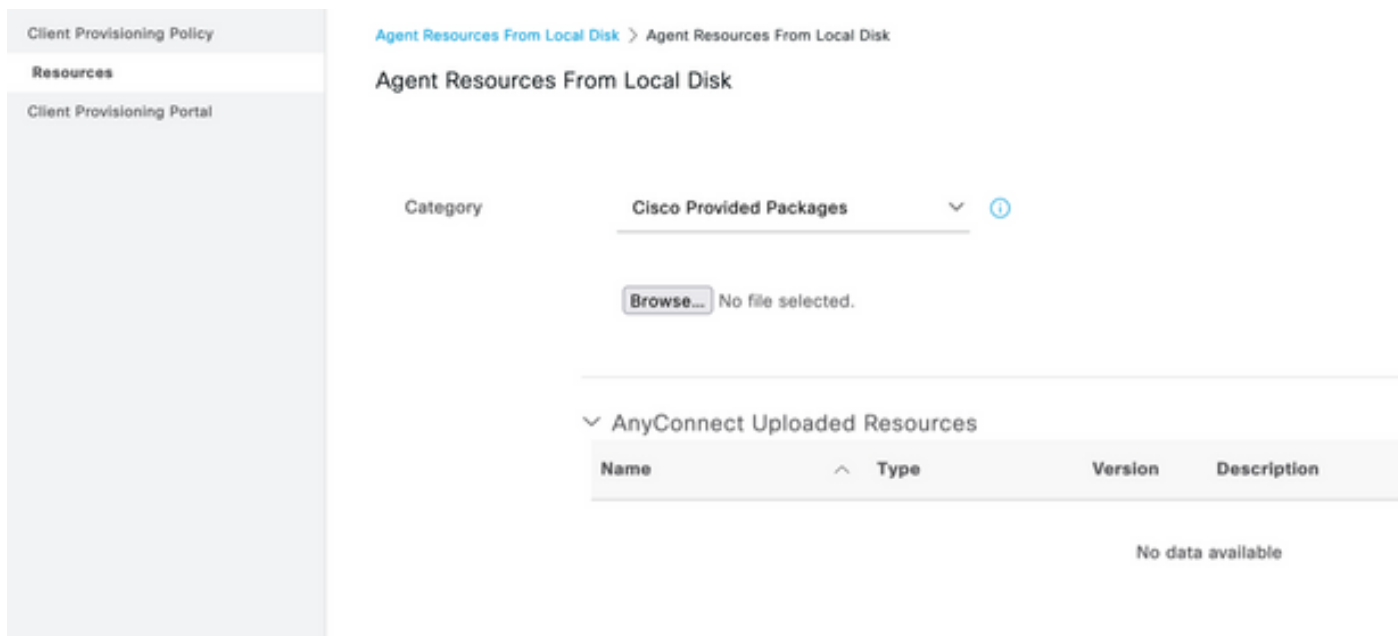
Passaggio 3. Selezionare **Aggiungi > Risorse agente da disco locale**

Resources

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

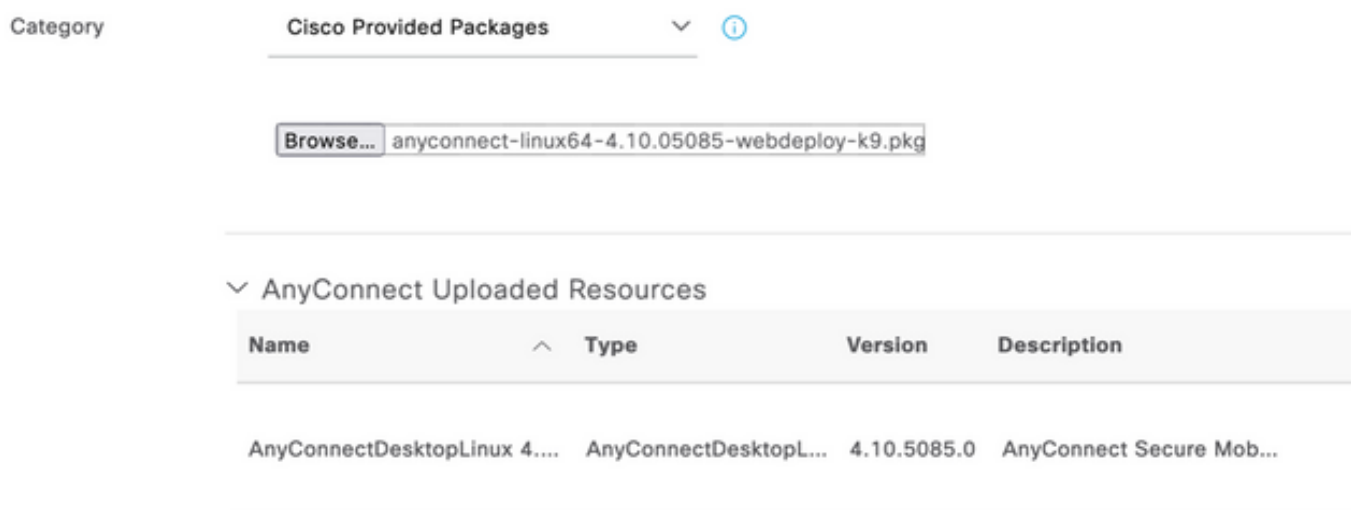
<input type="checkbox"/>	Agent resources from Cisco site
<input type="checkbox"/>	Agent resources from local disk

Passaggio 4. Selezionare **Pacchetti forniti da Cisco** dall'elenco a discesa Categoria.



Passaggio 5. Fare clic su Sfoglia.

Passaggio 6. Scegliere uno dei pacchetti AnyConnect scaricati nel passaggio precedente. L'immagine AnyConnect viene elaborata e vengono visualizzate le informazioni sul pacchetto



Passaggio 7. Fare clic su **Sottometti**. Ora che AnyConnect è stato caricato su ISE, è possibile contattare ISE e ottenere le altre risorse client da Cisco.com.

Nota: Le risorse agente includono moduli utilizzati dal client AnyConnect che consentono di valutare la conformità di un endpoint per una serie di controlli delle condizioni, ad esempio antivirus, antispyware, antimalware, firewall, crittografia del disco, file e così via.

Passaggio 8. Fare clic su **Aggiungi > Risorse agente dal sito Cisco**. Il completamento della finestra richiede un minuto quando ISE raggiunge Cisco.com e recupera un manifesto di tutte le risorse pubblicate per il provisioning del client.

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

Passaggio 9. Selezionare i moduli di conformità AnyConnect più recenti per Linux. Inoltre, puoi anche selezionare il modulo di conformità per Windows e 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

Passaggio 10. Selezionare gli ultimi agenti temporali per Windows e 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!

Passaggio 11. Fare clic su **Salva**.

Nota: Le configurazioni di postura di Windows e MAC non rientrano nell'ambito di questa guida alla configurazione.

A questo punto, sono state caricate e aggiornate tutte le parti necessarie. È giunto il momento di creare la configurazione e i profili necessari per utilizzare tali componenti.

Passaggio 12. Fare clic su **Add > NAC Agent o AnyConnect Posture Profile**.

The screenshot shows the Cisco ISE configuration interface. At the top, there are action buttons: Edit, Add, Duplicate, and Delete. Below these is a table of installed agents with columns for checkboxes, agent names, versions, last update times, and descriptions. A dropdown menu is open over the table, listing options: 'Agent resources from Cisco site', 'Agent resources from local disk', 'Native Supplicant Profile', 'AnyConnect Configuration', 'AnyConnect Posture Profile' (which is highlighted), and 'AMP Enabler Profile'. Below the table, the configuration page for 'AnyConnect Posture Profile' is visible. It includes a breadcrumb 'ISE Posture Agent Profile Settings > New Profile', the title 'AnyConnect Posture Profile', a 'Name' field containing 'LinuxACPosture', and a 'Description' field. The 'Agent Behavior' section contains a table of parameters:

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.

I parametri da modificare sono:

- **Intervallo di rilevamento VLAN:** Questa impostazione consente di impostare il numero di secondi di attesa del modulo tra il rilevamento delle modifiche alla VLAN. Si consiglia 5 secondi.
- **Ping o ARP:** Questo è il metodo di rilevamento delle modifiche alla VLAN. L'agente può eseguire il ping del gateway predefinito o monitorare la cache ARP per verificare che la voce del gateway predefinito abbia un timeout o entrambi. L'impostazione consigliata è ARP.
- **Timer di monitoraggio e aggiornamento:** Quando la postura di un endpoint è sconosciuta, l'endpoint viene sottoposto a un flusso di valutazione della postura. Occorre del tempo per porre rimedio ai controlli di postura falliti; il tempo predefinito è 4 minuti prima che l'endpoint venga contrassegnato come non conforme, ma i valori possono variare da 1 a 300 minuti (5 ore). La raccomandazione è di 15 minuti; tuttavia, ciò potrebbe richiedere degli aggiustamenti se ci si aspetta che le misure correttive richiedano più tempo.

Nota: Linux File Posture non supporta il monitoraggio e l'aggiornamento automatici.

Per una descrizione completa di tutti i parametri, consultare la documentazione sulla postura di ISE o AnyConnect.

Passaggio 13. Comportamento dell'agente: selezionare Elenco di backup richieste postura e scegliere **Scegli**, selezionare il nome di dominio completo (FQDN) PSN/Standalone e Seleziona salvataggio

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 x



Cancel

Select

Passaggio 14. In Protocolli di postura > Host di individuazione definire l'indirizzo IP del nodo PSN/Standalone.

Passaggio 15. Dall'elenco dei server di backup di individuazione e selezionare **scegli**, selezionare il PSN o il FQDN autonomo e selezionare **Seleziona**.

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

Passaggio 16. In **Regole nome server** digitare ***** per contattare tutti i server e definire l'indirizzo IP PSN/Standalone in **call home list**. In alternativa, è possibile utilizzare un carattere jolly per identificare tutti i potenziali PSN nella rete (ovvero *.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

Passaggio 17. Fare clic su **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

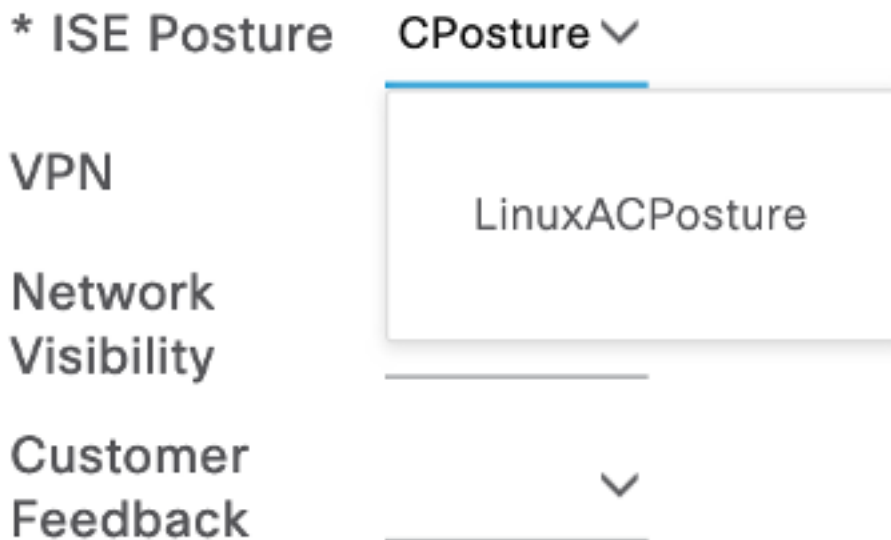
VPN

ASA Posture

Network
Visibility

Diagnostic
and Reporting
Tool

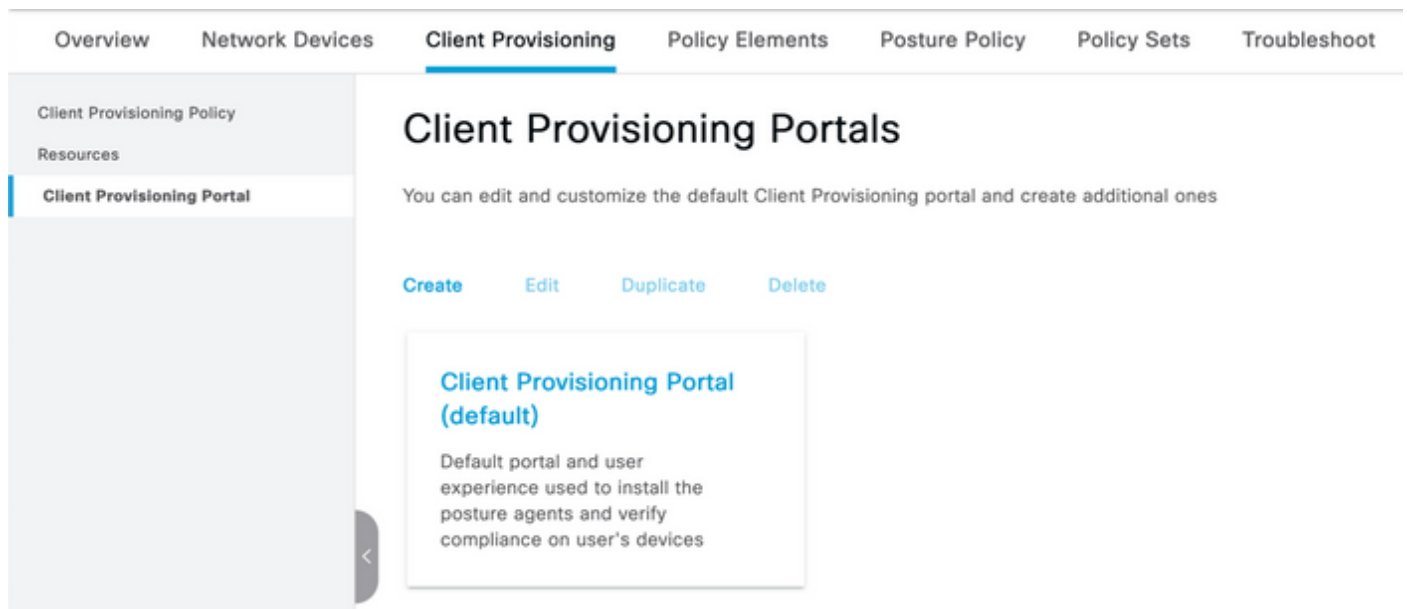
Profile Selection



Scorrere verso il basso e selezionare Invia

Passaggio 18. Dopo aver effettuato le selezioni, fare clic su **Sottometti**.

Passaggio 19. Selezionare **Workcenter > Postura > Client Provisioning > Client Provisioning Portals**.



Passaggio 20. Nella sezione **Impostazioni portale**, in cui è possibile selezionare l'interfaccia e la porta, nonché i gruppi autorizzati alla pagina Selezionare Dipendente, SISE_Users e Utenti dominio.

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)		
GROUP_ACCOUNTS (default)		
OWN_ACCOUNTS (default)	<input type="button" value="➤"/>	Employee
	<input type="button" value="➤"/>	
<input type="button" value="Choose all"/>		<input type="button" value="Clear all"/>

Passaggio 21. In Log in Page Settings, verificare che l'opzione **Enable auto Log In** sia abilitata

✓ 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

Passaggio 2. Nell'angolo superiore destro selezionare **Save (Salva)**

Passaggio 23. Selezionare **Centri di lavoro > Postura > Provisioning client > Criteri di provisioning client.**

Passaggio 24. Fare clic sulla freccia in giù accanto alla **regola IOS** nel **CPP** e scegliere **Duplica sopra**

Passaggio 25. Assegnare un nome alla regola **LinuxPosture**

Passaggio 26. Per i risultati, selezionare **AnyConnect Configuration** come agente.

Nota: In questo caso, non viene visualizzato l'elenco a discesa del modulo conformità perché è configurato come parte della configurazione AnyConnect.

The screenshot shows the Cisco ISE interface for configuring a Client Provisioning Policy. The page title is "Client Provisioning Policy" and it includes a description: "Define the Client Provisioning Policy to determine what users will receive upon login and user session initiation: For Agent Configuration: version of agent, agent profile, agent compliance module, and/or agent customization package. For Native Supplciant Configuration: wizard profile and/or wizard. Drag and drop rules to change the order." Below this is a table of rules:

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

Passaggio 27. Fare clic su **Fine**.

Passaggio 28. Fare clic su **Salva**.

Elementi criteri di postura

Passaggio 29. Selezionare **Centri di lavoro > Postura > Elementi criteri > Condizioni > File.** Selezionare **Aggiungi**.

Passaggio 30. Definire **TESTFile** come nome della condizione del file e definire i valori successivi

File Condition

Name *	TESTFile	
Description		
* Operating System	Linux All	▼
Compliance Module	Any version	
* File Type	FileExistence	▼ ⓘ
* File Path	home	▼
		<u>Testfile.csv</u> ⓘ
* File Operator	Exists	▼

Nota: Il percorso è basato sul percorso del file.

Passaggio 31. Selezionare Salva

FileExistence. Questo tipo di condizione di file cerca di verificare se un file è presente nel sistema in cui si suppone che esista. Se questa opzione è selezionata, non vi è alcun problema per la convalida delle date dei file, degli hash e così via

Passaggio 32. Selezionare Requisiti e creare un nuovo criterio come indicato di seguito:

Requirements

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 Edit ▼
LinuxFile	for Linux All	using 4.x or later	using AnyConnect	met if TESTFile	then Select Remediations Edit ▼

Nota: Linux non supporta solo il testo del messaggio come azione di correzione

Componenti dei requisiti

- **Sistema operativo:** Linux All
- **Modulo sulla conformità:** 4,x
- **Tipo di postura:** AnyConnect
- **Condizioni:** Moduli e agenti di conformità (disponibili dopo la selezione del sistema operativo)
- **Azioni correttive:** Correzioni che diventano disponibili per la selezione dopo aver scelto tutte le altre condizioni.

Passaggio 3. Selezionare Centri di lavoro > Postura > Criteri di postura

Passaggio 34. Selezionare **Edit** on any policy e Selezionare **Insert New policy Define LinuxPosturePolicy Policy Policy** as the name (Inserisci nuovo criterio) e assicurarsi di aggiungere il requisito creato nel passaggio 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_AntMalware_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	LinuxPostureP001	Any	and Linux All	and 4.x or later	and AnyConnect	and	than LinuxP01	Edit

Passaggio 35. Selezionare **Fine e Salva**

Altre impostazioni di postura importanti (sezione Impostazioni generali della postura)

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

Le impostazioni importanti nella sezione Impostazioni generali della postura sono le seguenti:

- **Timer monitoraggio e aggiornamento:** Questa impostazione definisce il tempo necessario a un client per correggere una condizione di postura non riuscita. La configurazione AnyConnect prevede anche un timer di monitoraggio e aggiornamento; questo timer è per ISE, non per AnyConnect.
- **Stato postura predefinito:** Questa impostazione fornisce lo stato della postura per i dispositivi senza l'agente di postura o i sistemi operativi che non possono eseguire l'agente temporale, ad esempio i sistemi operativi basati su Linux.
- **Intervallo di monitoraggio continuo:** Questa impostazione si applica alle condizioni

dell'applicazione e dell'hardware che eseguono l'inventario dell'endpoint. L'impostazione specifica la frequenza con cui AnyConnect deve inviare i dati di monitoraggio.

- **Criterio d'uso accettabile in modalità celata:** Le uniche due opzioni disponibili per questa impostazione sono il blocco o la continuazione. Il blocco impedisce ai client AnyConnect in modalità stealth di procedere se l'AUP non è stata riconosciuta. Continue consente al client in modalità stealth di procedere anche senza riconoscere l'AUP (che è spesso l'intento quando si utilizza l'impostazione della modalità stealth di AnyConnect).

Configurazioni di rivalutazione

Le rivalutazioni della postura sono un componente critico del flusso di lavoro della postura. Nella sezione "Protocollo postura" è stato spiegato come configurare l'agente AnyConnect per la rivalutazione della postura. L'agente esegue periodicamente il Check-In con i PSN definiti in base al timer nella configurazione.

Quando una richiesta raggiunge il PSN, il PSN determina se è necessaria una rivalutazione della postura, in base alla configurazione ISE per il ruolo dell'endpoint. Se il client supera la rivalutazione, il PSN mantiene lo stato di conformità alla postura dell'endpoint e il lease della postura viene reimpostato. Se l'endpoint non supera la rivalutazione, lo stato della postura diventa non conforme e qualsiasi lease di postura esistente viene rimosso.

Passaggio 36. Selezionare **Criterio > Elementi criteri > Risultati > Autorizzazione > Profilo autorizzazione**. Selezionare **Aggiungi**

Passaggio 37. Definire **Wired_Redirect** come profilo di autorizzazione e configurare i parametri successivi

▼ 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

Passaggio 38. Selezionare **Salva**

Passaggio 39. Configurazione dei criteri di autorizzazione

Esistono tre regole di autorizzazione preconfigurate per la postura:

1. La prima è configurata per corrispondere quando l'autenticazione ha esito positivo e la conformità di un dispositivo è sconosciuta.
2. La seconda regola associa le autenticazioni riuscite agli endpoint non conformi.

Nota: Entrambe le prime due regole restituiscono lo stesso risultato, ovvero utilizzano un profilo di autorizzazione preconfigurato che reindirizza l'endpoint al portale di provisioning client.

3. La regola finale corrisponde all'autenticazione riuscita e agli endpoint conformi alla postura e utilizza il profilo di autorizzazione PermitAccess predefinito.

Selezionare **Policy > Policy Set** (Criteri impostati) e fare clic sulla freccia destra per **Wired 802.1x - MAB** Creato nel laboratorio precedente.

Passaggio 40. Selezionare **Criteri di autorizzazione** e creare le regole successive



Configurazioni sullo switch

Nota: La configurazione riportata di seguito fa riferimento a IBNS 1.0. Possono esistere differenze per gli switch compatibili con IBNS 2.0. Include l'installazione in modalità a basso impatto.

```
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 redireciton 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
```

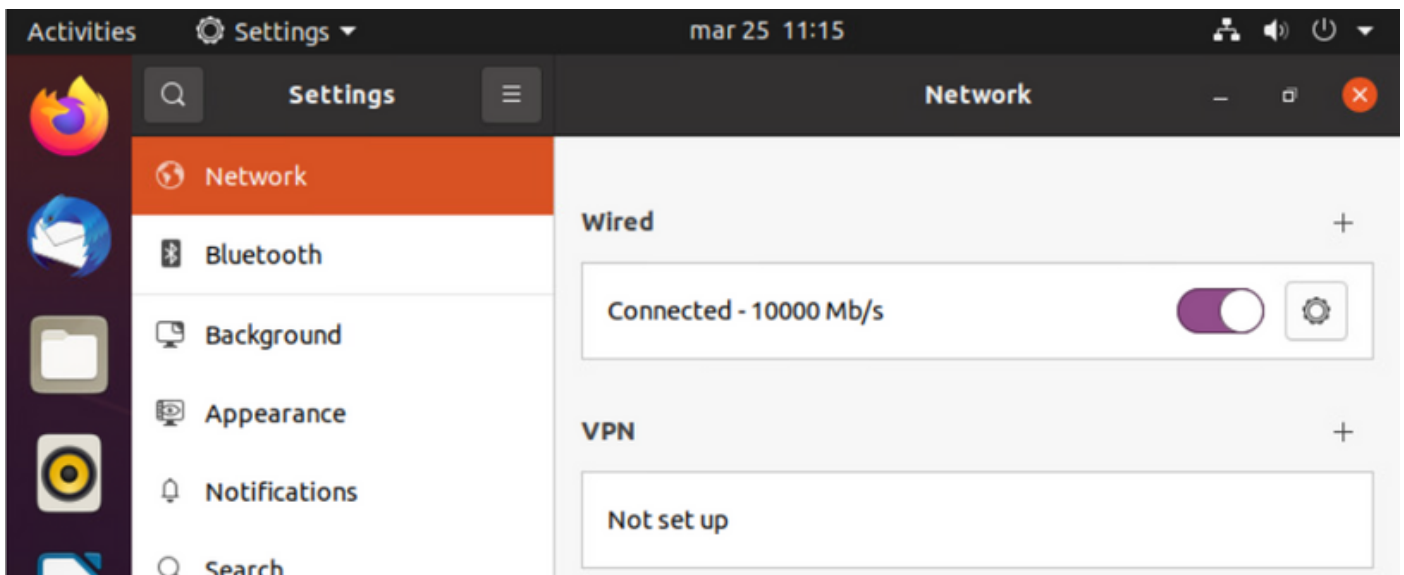
Verifica

Verifica ISE:

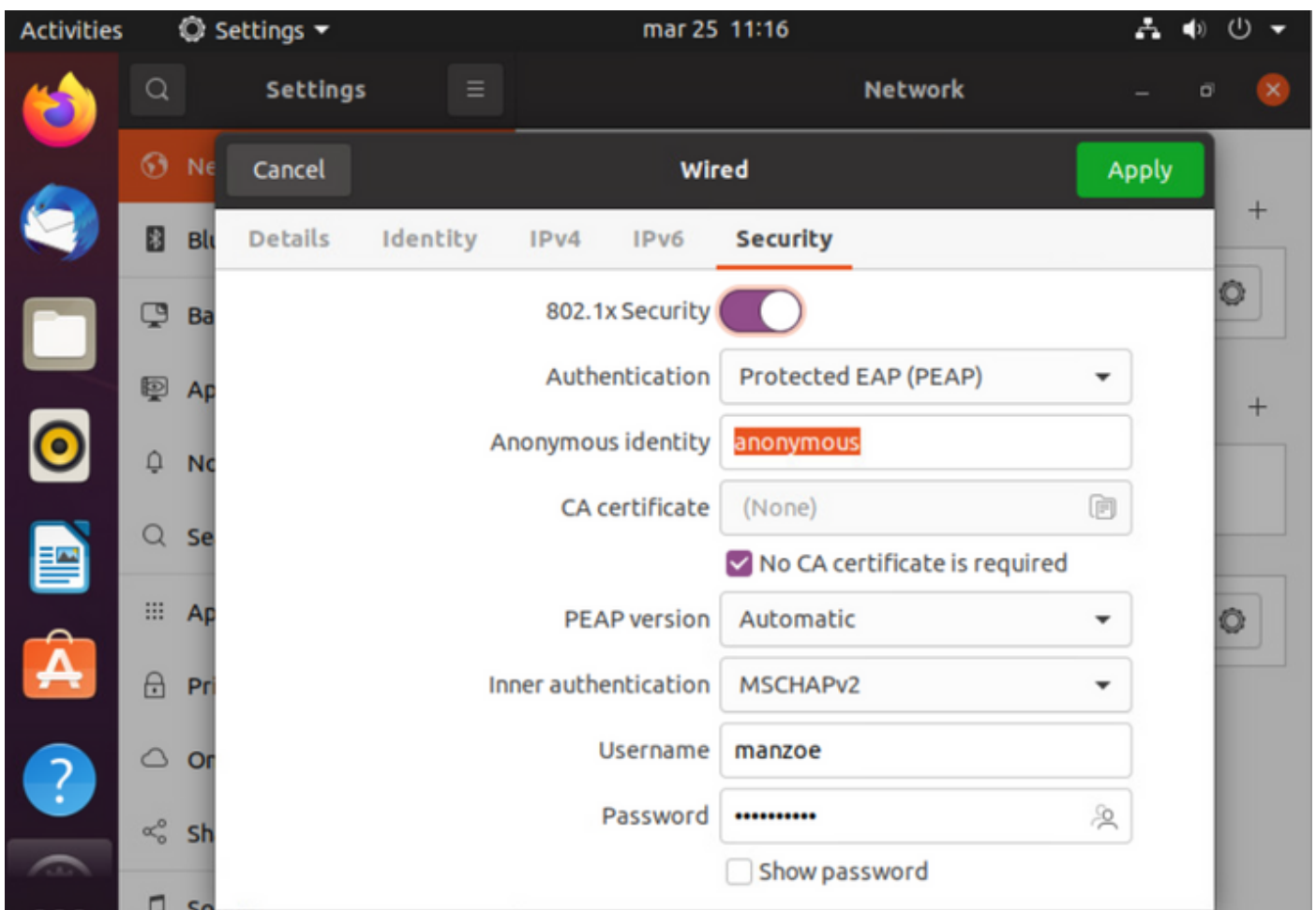
In questa sezione si presume che AnyConnect con il modulo di postura ISE sia stato precedentemente installato sul sistema Linux.

Autentica PC tramite dot1x

Passaggio 1. Passare a Impostazioni di rete



Passaggio 2. Selezionare la scheda Protezione e fornire la configurazione 802.1x e le credenziali utente



3. Fare clic su "Apply" (Applica).

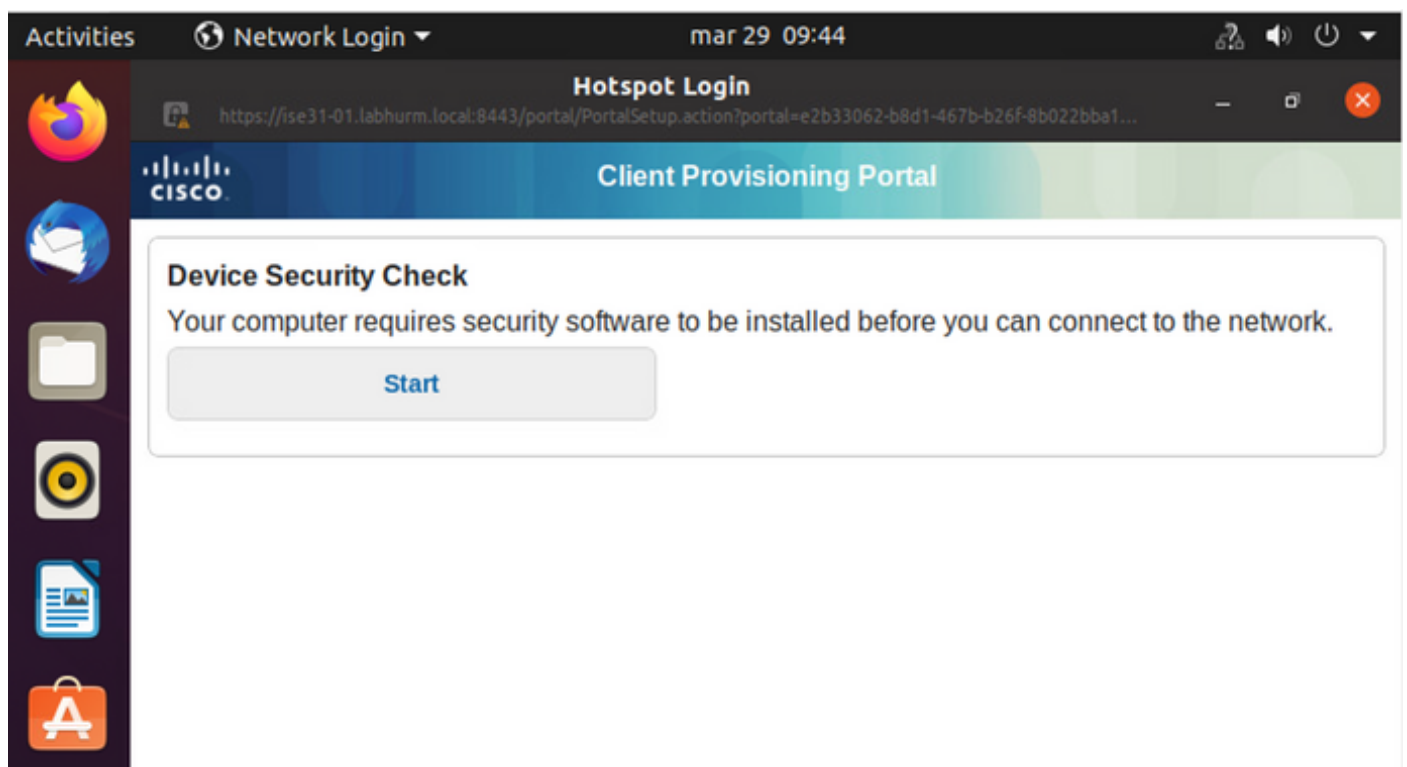
Passaggio 4. Collegare il sistema Linux alla rete cablata 802.1x e convalidare nel registro ISE live:

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint...	Authenti...	Authoriz...	Authoriz...	IP Address	Network De...	Device Port	Identity Group	Posture
Apr 06, 2022 08:42:08.2...	●		5	marzio	00:0C:29:44:03:8F	Ubuntu W...	Ubuntu Po...	Ubuntu Po...	Wired_Re...			FastEthernet1...		Pending
Apr 06, 2022 08:32:48.2...	●			marzio	00:0C:29:44:03:8F	Ubuntu W...	Ubuntu Po...	Ubuntu Po...	Wired_Re...		Cat-3750	FastEthernet1...	Workstation	Pending
Apr 06, 2022 08:32:40.8...	●			marzio	00:0C:29:44:03:8F	Ubuntu W...	Ubuntu Po...	Ubuntu Po...	Wired_Re...		Cat-3750	FastEthernet1...	Workstation	Pending

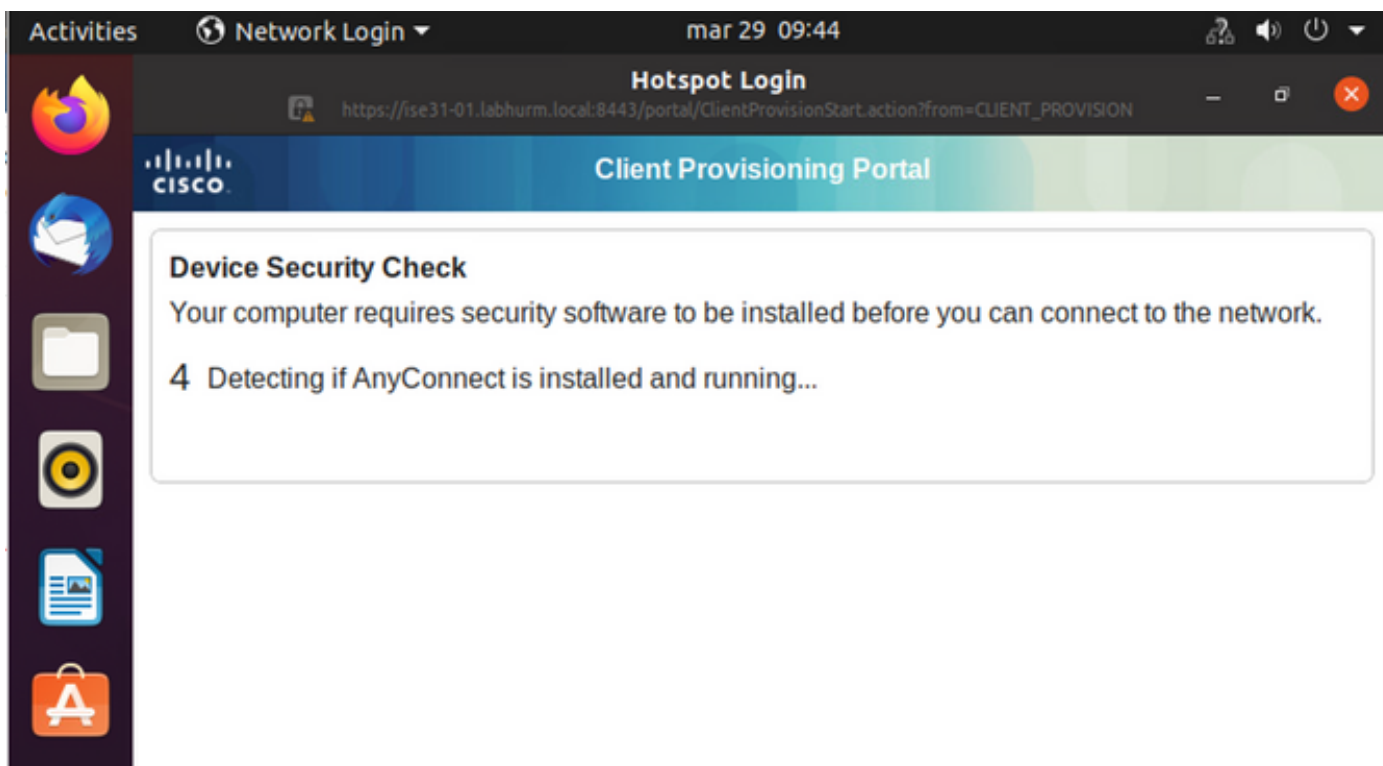
In ISE, usare la barra di scorrimento orizzontale per visualizzare ulteriori informazioni, come il PSN che ha servito il flusso o lo stato della postura:

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

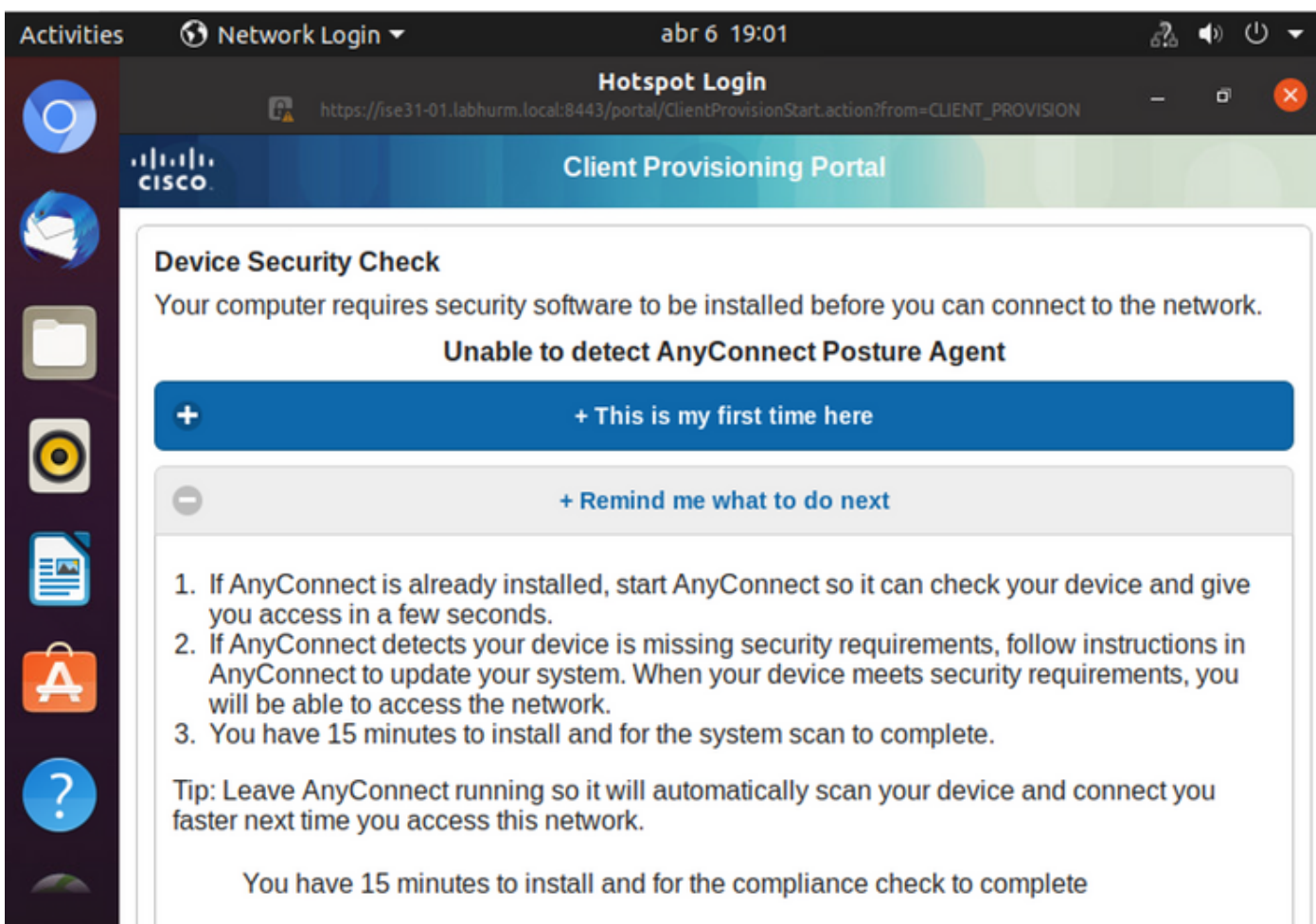
Passaggio 5. Sul client Linux, il reindirizzamento deve essere eseguito e viene visualizzato il portale di provisioning del client che indica che si è verificato il controllo della postura e fare clic su "Avvia":



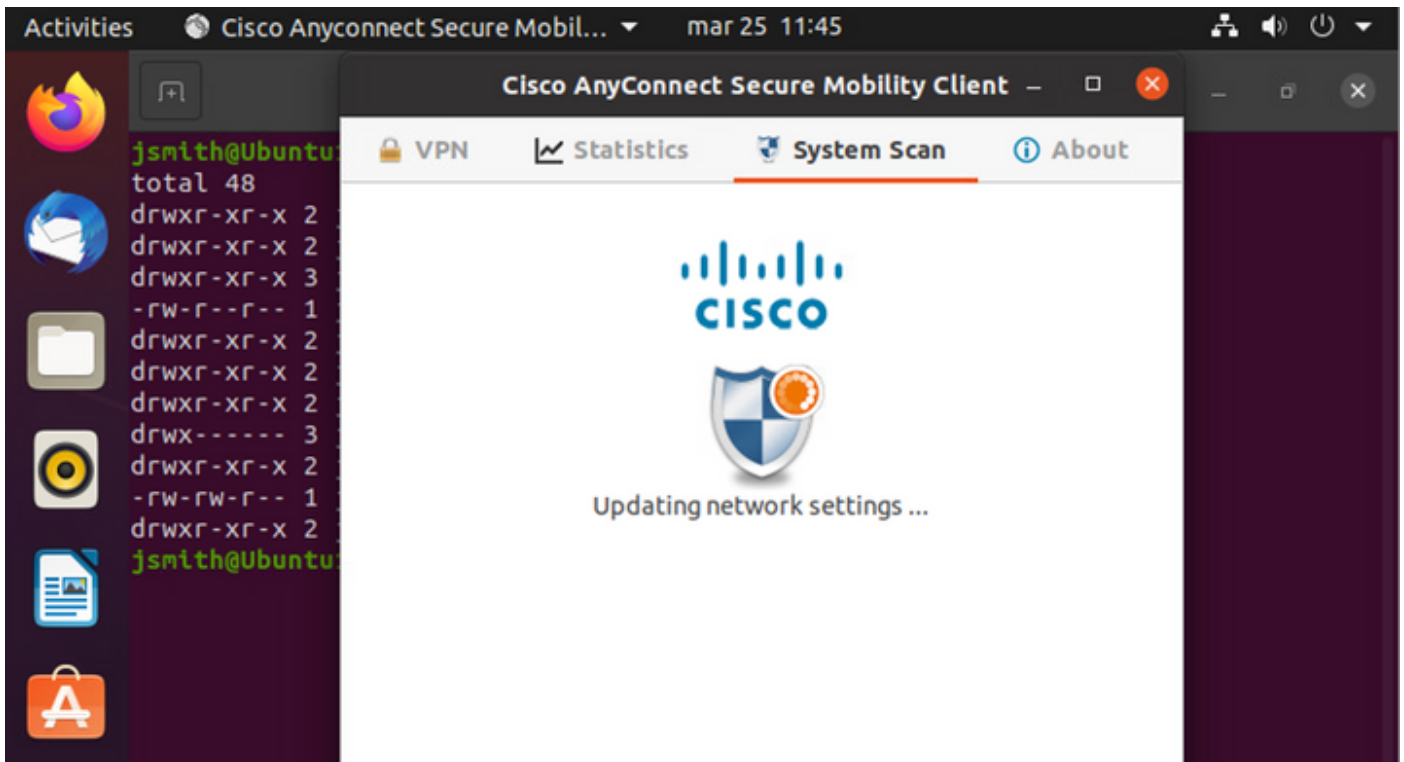
Attendere qualche secondo quando il connettore tenta di rilevare AnyConnect:



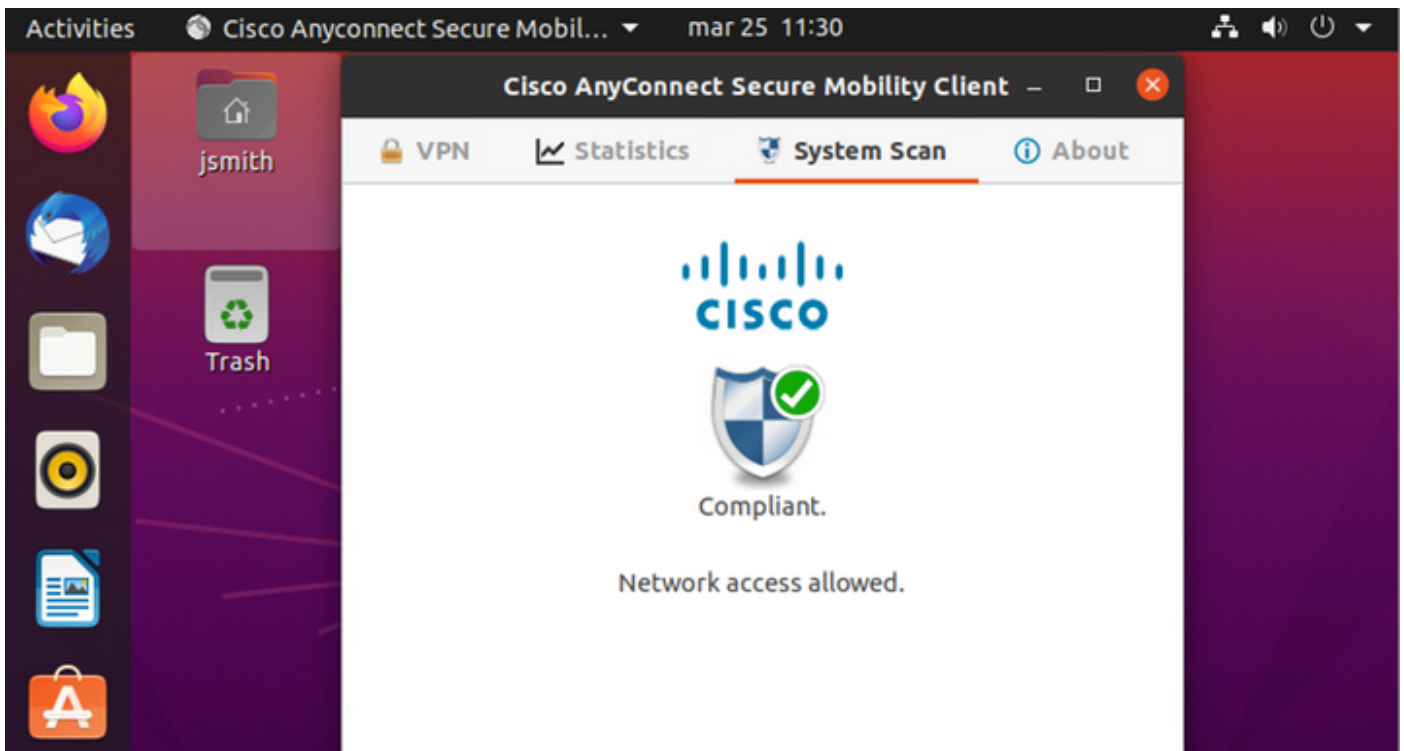
A causa di un problema noto, anche se AnyConnect è installato, non viene rilevato. Per passare al client AnyConnect, usare **Alt-Tab** o il menu **Attività**.

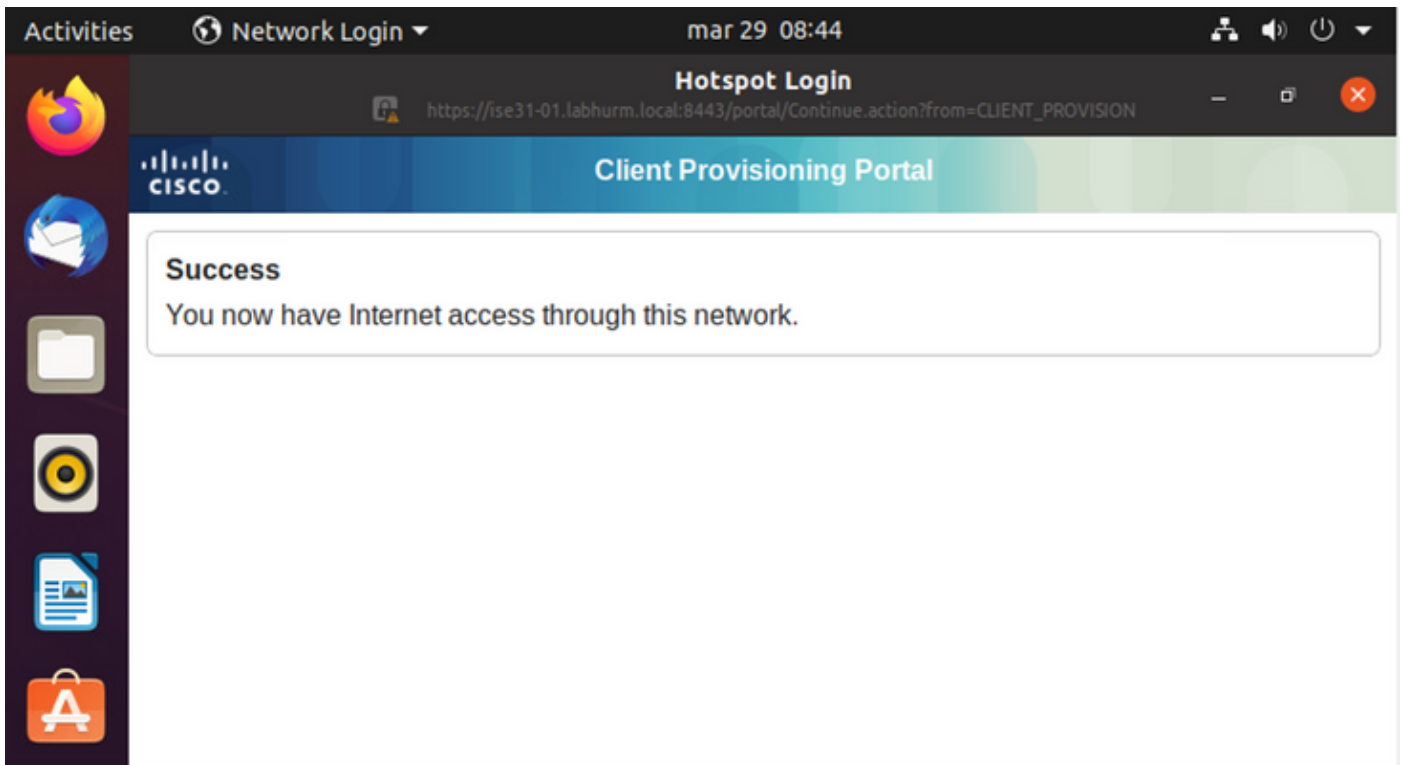


AnyConnect cerca di raggiungere il PSN per il criterio di postura e di valutare l'endpoint in base a esso.



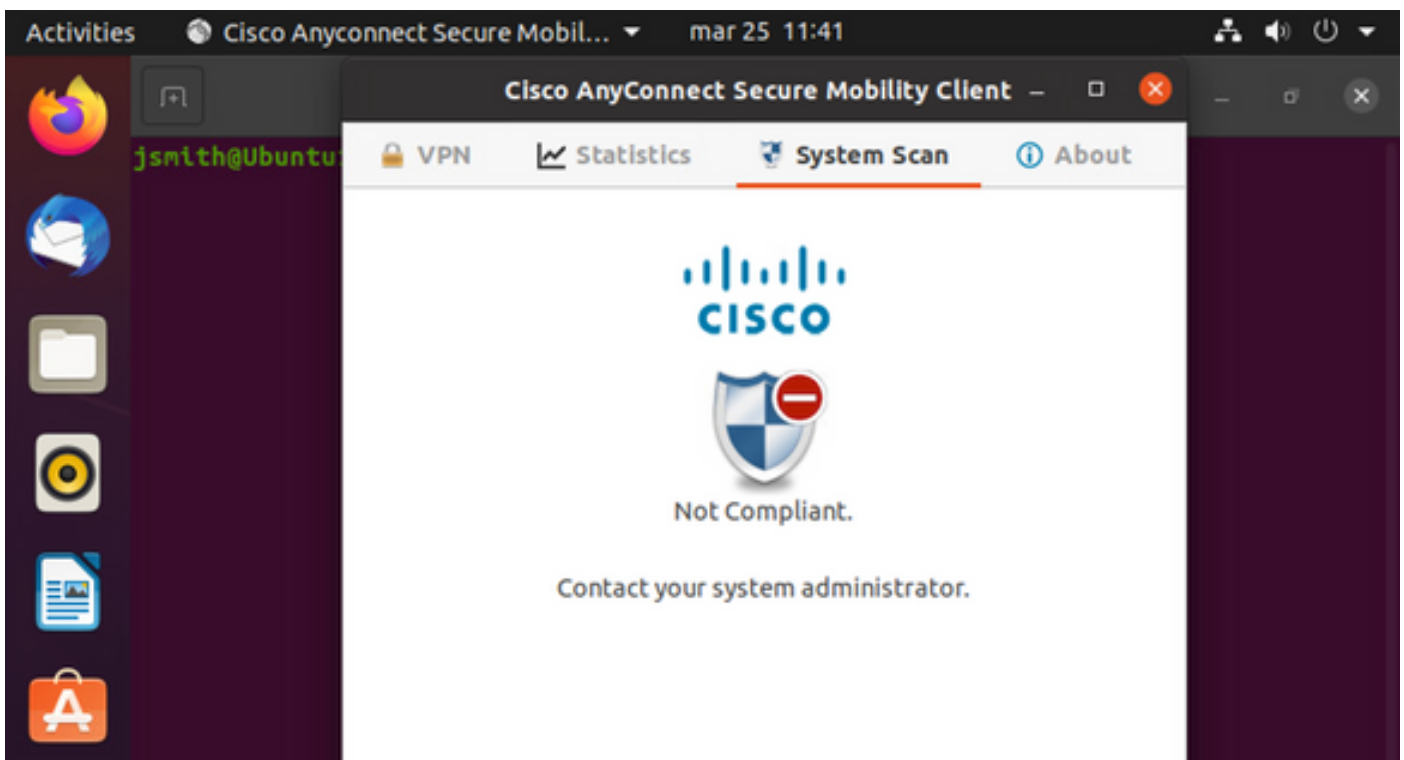
AnyConnect segnala all'ISE la sua determinazione della policy di postura. In questo caso,





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 Mer...	Wired Merak...	PermitAccess	192.168.200.12				Compliant	ise31-01
Ubuntu-Workstation	Wired Mer...	Wired Merak...	PermitAccess		Mraki-SW		Workstation	Compliant	ise31-01
Ubuntu-Workstation	Wired Mer...	Wired Merak...	PermitAccess		Mraki-SW		Workstation	Compliant	ise31-01

D'altra parte, se il file non esiste, il modulo di postura di AnyConnect segnala la determinazione all'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	

Nota: L'FQDN ISE deve essere risolvibile sul sistema Linux tramite file DNS o host locale.

Risoluzione dei problemi

```
show authentication sessions int fa1/0/35
```

Reindirizzamento sul posto:

```
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&p33062-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
```

Autorizzazione completata:

```
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
```

Non conforme, spostato sulla VLAN di quarantena e sull'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
```