

# Konfigurieren des Cisco ISE 3.1-Status mit Linux

## Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Konfigurationen auf der ISE](#)

[Konfigurationen auf dem Switch](#)

[Überprüfung](#)

[Fehlerbehebung](#)

## Einleitung

Dieses Dokument beschreibt das Verfahren zum Konfigurieren und Implementieren einer Dateistatusrichtlinie für Linux und die Identity Services Engine (ISE).

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- AnyConnect
- Identity Services Engine (ISE)
- Linux

### Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- 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)

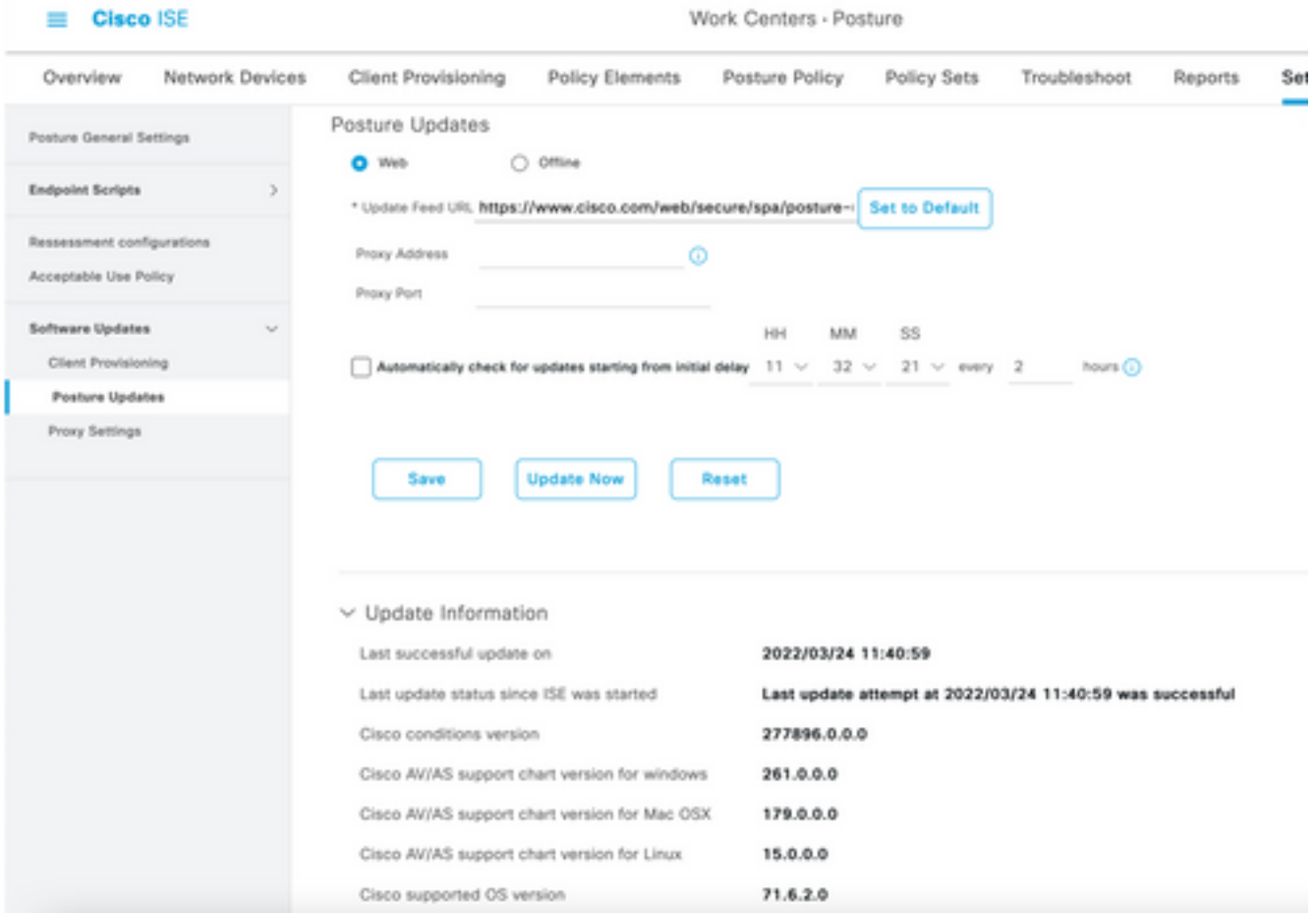
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

## Konfigurieren

### Konfigurationen auf der ISE

## Schritt 1: Status-Service aktualisieren:

Navigieren Sie zu **Work Center > Status > Settings > Software Updates > Posture Updates**. Wählen Sie **Jetzt aktualisieren** aus, und warten Sie, bis der Vorgang abgeschlossen ist:



The screenshot displays the Cisco ISE interface for configuring Posture Updates. The left sidebar shows the navigation menu with 'Posture Updates' selected. The main content area is titled 'Posture Updates' and includes the following elements:

- Radio buttons for 'Web' (selected) and 'Offline'.
- 'Update Feed URL' field with a 'Set to Default' button.
- 'Proxy Address' and 'Proxy Port' input fields.
- 'Automatically check for updates starting from initial delay' section with dropdowns for HH (11), MM (32), SS (21), and 'every 2 hours'.
- 'Save', 'Update Now', and 'Reset' buttons.
- 'Update Information' section with the following data:

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

Ein **von Cisco bereitgestelltes Paket** ist ein Softwarepaket, das Sie von der Cisco.com-Website herunterladen, z. B. die AnyConnect-Softwarepakete. Ein **vom Kunden erstelltes Paket** ist ein Profil oder eine Konfiguration, das bzw. die Sie außerhalb der ISE-Benutzeroberfläche erstellt haben und zur Statusüberprüfung in die ISE hochladen möchten. Für diese Übung können Sie das AnyConnect-Webdeploy-Paket "anyconnect-linux64-4.10.05085-webdeploy-k9.pkg" herunterladen.

**Anmerkung:** Aufgrund von Updates und Patches kann sich die empfohlene Version ändern. Verwenden Sie die neueste empfohlene Version von der Website cisco.com.

## Schritt 2. AnyConnect-Paket hochladen:

Navigieren Sie im Posture Work Center zu **Client Provisioning > Resources (Client-Bereitstellung > Ressourcen)**.

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

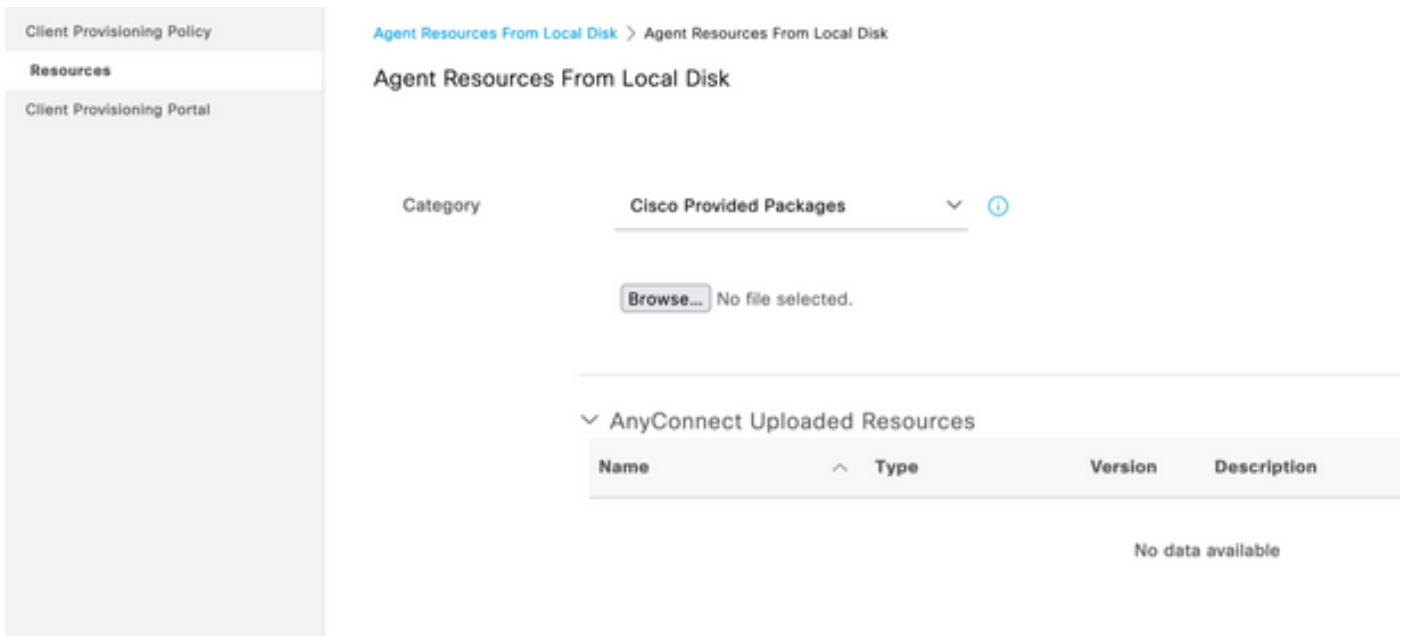
Schritt 3: Wählen Sie Add > Agent Resources von Local Disk aus.

# Resources

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

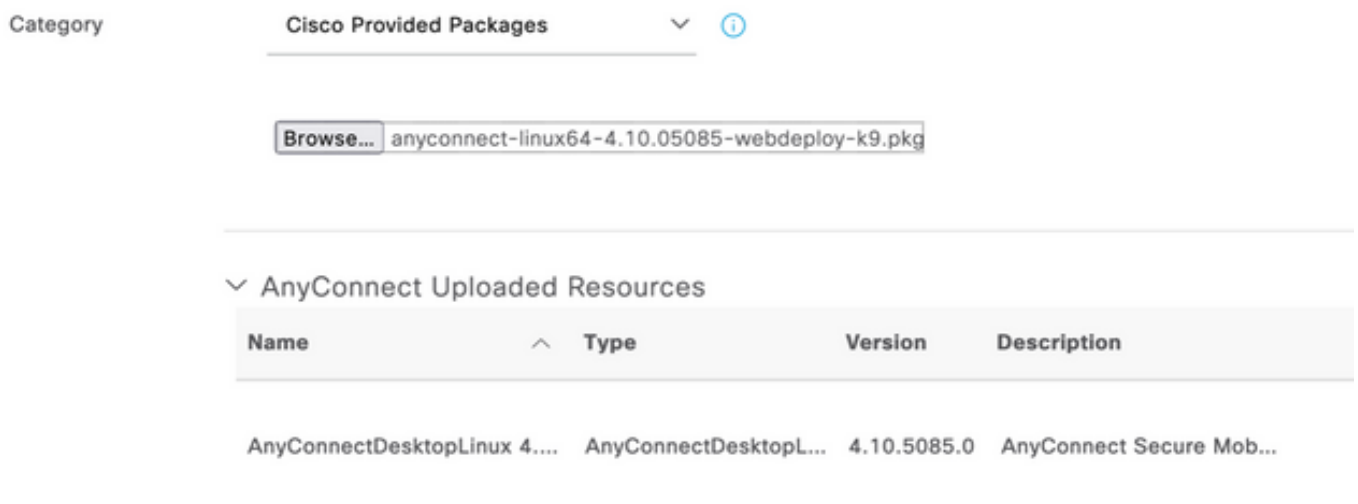
<input type="checkbox"/>	Agent resources from Cisco site
<input type="checkbox"/>	Agent resources from local disk

Schritt 4: Wählen Sie Cisco Provided Packages aus dem Dropdown-Menü Kategorie aus.



**Schritt 5:** Klicken Sie auf Durchsuchen.

**Schritt 6:** Wählen Sie eines der AnyConnect-Pakete aus, die Sie im vorherigen Schritt heruntergeladen haben. Das AnyConnect-Image wird verarbeitet, und die Informationen zum Paket werden angezeigt



**Schritt 7.** Klicken Sie auf **Senden**. Nachdem AnyConnect auf die ISE hochgeladen wurde, können Sie einen ISE-Kontakt haben und die anderen Client-Ressourcen von Cisco.com beziehen.

**Anmerkung:** Zu den Agenten-Ressourcen gehören Module, die vom AnyConnect Client verwendet werden und die die Möglichkeit bieten, die Konformität eines Endpunkts für eine Reihe von Zustandsüberprüfungen wie Anti-Virus, Anti-Spyware, Anti-Malware, Firewall, Festplattenverschlüsselung, Datei usw. zu bewerten.

**Schritt 8:** Klicken Sie auf **Hinzufügen > Agent Resources von Cisco Site**. Das Ausfüllen des Fensters dauert eine Minute, wenn die ISE Cisco.com erreicht und ein Manifest aller veröffentlichten Ressourcen für die Client-Bereitstellung abrufen.

# 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

**Schritt 9.** Wählen Sie die neuesten AnyConnect Compliance-Module für Linux aus. Darüber hinaus können Sie auch das Compliance-Modul für Windows und Mac auswählen.



## 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

**Schritt 10.** Wählen Sie die neuesten temporalen Agenten für Windows und Mac aus.

<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!

**Schritt 11.** Klicken Sie auf **Speichern**.

**Anmerkung:** MAC- und Windows-Statuskonfigurationen sind nicht Bestandteil dieses Konfigurationsleitfadens.

Jetzt haben Sie alle erforderlichen Teile hochgeladen und aktualisiert. Jetzt ist es an der Zeit, die Konfigurationen und Profile zu erstellen, die für die Verwendung dieser Komponenten erforderlich sind.

**Schritt 12:** Klicken Sie auf Hinzufügen > NAC Agent oder AnyConnect Posture Profile.

[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			
<input type="checkbox"/>	Native Supplicant Profile			
<input type="checkbox"/>	AnyConnect Configuration			
<input type="checkbox"/>	AnyConnect Posture Profile			
<input type="checkbox"/>	AMP Enabler Profile			
<input type="checkbox"/>	oTemporalAgent...	4.10.2051.0	2021/08/09 19:12:31	With CM: 4.3.1858.4353
<input type="checkbox"/>	oTemporalAgent...	4.10.6011.0	2022/03/24 11:49:19	Cisco Temporal Agent fo...
<input type="checkbox"/>	ConnectComplian...	4.3.2716....	2022/03/24 11:49:39	AnyConnect Windows C...
<input type="checkbox"/>	ve Supplicant Pro...	Not Applic...	2016/10/06 20:01:12	Pre-configured Native S...
<input type="checkbox"/>	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:

#### Agent Behavior

Parameter	Value	Description
Enable debug log	No <input type="button" value="v"/>	Enables the debug log on the agent
Operate on non-802.1X wireless	No <input type="button" value="v"/>	Enables the agent to operate on non-802.1X wireless networks.
Enable signature check <span style="color:blue;">?</span>	No <input type="button" value="v"/>	Check the signature of executables before running them.
Log file size	5 MB	The maximum agent log file size
Remediation timer <span style="color:blue;">?</span>	4 mins	If the user fails to remediate within this specified time, mark them as non-compliant.
Stealth Mode	Disabled <input type="button" value="v"/>	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 <input type="button" value="v"/>	Display user notifications even when in Stealth mode.

Folgende Parameter müssen geändert werden:

- **VLAN-Erkennungsintervall:** Mit dieser Einstellung können Sie die Anzahl der Sekunden festlegen, die das Modul zwischen der Suche nach VLAN-Änderungen wartet. Die Empfehlung lautet 5 Sekunden.
- **Ping oder ARP:** Dies ist die tatsächliche Methode zur Erkennung von VLAN-Änderungen. Der Agent kann einen Ping an das Standard-Gateway senden oder den ARP-Cache überwachen, um das Timeout oder beide einzugeben. Die empfohlene Einstellung ist ARP.
- **Behebungs-Timer:** Wenn der Status eines Endpunkts unbekannt ist, wird der Endpunkt in einem Statusüberprüfungsablauf platziert. Es braucht Zeit, um ausgefallene Statusprüfungen zu beheben. Die Standardzeit beträgt 4 Minuten, bevor der Endpunkt als nicht konform gekennzeichnet wird. Die Werte können jedoch zwischen 1 und 300 Minuten (5 Stunden) liegen. Die Empfehlung beträgt 15 Minuten. Dies kann jedoch Anpassungen erfordern, wenn die Behebung voraussichtlich länger dauern wird.

**Anmerkung:** Der Linux-Dateistatus unterstützt keine automatische Problembeseitigung.

Eine umfassende Beschreibung aller Parameter finden Sie in der ISE- oder AnyConnect-Statusdokumentation.

**Schritt 13:** Agent Behavior wählt Status Probes Backup List (Sicherungsliste für Status) aus und wählt **Wählen Sie**, wählen Sie PSN/Standalone FQDN aus, und wählen Sie **Save (Speichern) aus**.

## 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

**Schritt 14:** Definieren Sie unter Statusprotokolle > Discovery Host die IP-Adresse des PSN/Standalone-Knotens.

**Schritt 15:** Wählen Sie aus der **Liste der Discovery-Backup-Server** und Select (Auswählen) Ihren PSN oder Standalone FQDN aus, und wählen Sie **Select (Auswählen) aus**.



# 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

**Schritt 16:** Geben Sie unter **Servernamen-Regeln** \*ein, um alle Server zu kontaktieren und die PSN-/Standalone-IP-Adresse unter **Call Home List** zu definieren. Alternativ kann ein Platzhalter verwendet werden, um alle potenziellen PSNs in Ihrem Netzwerk abzugleichen (das ist \*.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

**Schritt 17:** Klicken Sie auf **Hinzufügen > AnyConnect-Konfiguration**



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"/>	<b>AnyConnect Configuration</b>
<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
<b>AnyConnectDesktopLinux 4.10.5085.0</b>

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

---

Blättern Sie nach unten, und wählen Sie Senden aus

**Schritt 18:** Wenn Sie die Auswahl abgeschlossen haben, klicken Sie auf **Senden**.

**Schritt 19:** Wählen Sie **Work Centers > Status > Client Provisioning > Client Provisioning Portals (Portale für Client-Bereitstellung)** aus.

The screenshot shows the Cisco ISE GUI for Client Provisioning. The navigation tabs at the top are: Overview, Network Devices, Client Provisioning (selected), Policy Elements, Posture Policy, Policy Sets, and Troubleshoot. On the left sidebar, the menu items are: Client Provisioning Policy, Resources, and Client Provisioning Portal (selected). The main content area is titled "Client Provisioning Portals" and includes 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 the description: "Default portal and user experience used to install the posture agents and verify compliance on user's devices".

**Schritt 20:** Im Bereich "**Portal Settings**" können Sie die Schnittstelle und den Port sowie die Gruppen auswählen, die zur Seite Select Employee, SISE\_Users and Domain Users autorisiert sind.

### 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="➤"/>	

**Schritt 21:** Stellen Sie sicher, dass unter Seiteneinstellungen für die Anmeldung die Option **Automatische Anmeldung aktivieren** aktiviert ist.

✓ 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

**Schritt 22:** Klicken Sie in der rechten oberen Ecke auf **Speichern**.

**Schritt 23.**Wählen Sie **Work Centers > Status > Client Provisioning > Client Provisioning Policy** aus.

**Schritt 24:** Klicken Sie auf den Abwärtspfeil neben der **IOS-Regel** im **CPP**, und wählen Sie **Oben** duplizieren aus.

**Schritt 25:** Benennen Sie die Regel **LinuxPosture**

**Schritt 26:** Wählen Sie als Ergebnisse die **AnyConnect-Konfiguration** als Agent aus.

**Anmerkung:** In diesem Fall wird kein Compliance-Modul Dropdown-Menü angezeigt, da es als Teil der AnyConnect-Konfiguration konfiguriert ist.

The screenshot shows 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:

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

**Schritt 27.**Klicken Sie auf **Fertig**.

**Schritt 28:** Klicken Sie auf **Speichern**.

## Richtlinienelemente für den Status

**Schritt 29.**Wählen Sie **Work Center > Status > Policy Elements > Conditions > File** aus. Wählen Sie **Hinzufügen** aus.

**Schritt 30.**Definieren Sie **TESTFile** als Dateinamenbedingung, und definieren Sie die nächsten Werte.

## File Condition

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

**Anmerkung:** Der Pfad basiert auf dem Dateispeicherort.

### Schritt 31: Wählen Sie **Speichern**

**FileExistence.** Dieser Dateityp überprüft, ob eine Datei im System vorhanden ist, in dem sie enthalten sein soll - und das ist alles. Wenn diese Option ausgewählt ist, gibt es keinerlei Bedenken hinsichtlich der Validierung von Dateidaten, Hashes usw.

**Schritt 32:** Wählen Sie Anforderungen aus, und erstellen Sie eine neue Richtlinie wie folgt:

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				

**Anmerkung:** Linux unterstützt den Nachrichtentext nicht nur als Behebungsmaßnahme.

### Anforderungskomponenten

- **Betriebssystem:** Linux Alle
- **Compliance-Modul:** 4,x
- **Status:** AnyConnect
- **Bedingungen:** Compliance-Module und -Agenten (die verfügbar werden, nachdem Sie das Betriebssystem ausgewählt haben)
- **Sanierungsmaßnahmen:** Sanierungen, die nach Auswahl aller anderen Bedingungen zur Auswahl stehen.

**Schritt 33:** Wählen Sie **Work Center > Status > Status Policy (Statusrichtlinie)** aus.

**Schritt 34:** Wählen Sie **Bearbeiten** für eine Richtlinie aus, und wählen Sie **Neue Richtlinie einfügen** **LinuxPosturePolicy** als Namen **definieren** aus, und stellen Sie sicher, dass Sie Ihre Anforderung, die in Schritt 32 erstellt wurde, hinzufügen.

## 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_AntiMalware_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	LinuxPosturePoli	Any	and Linux All	and 4.x or later	and AnyConnect	and	than LinuxPoli	Edit

**Schritt 35:** Wählen Sie **Fertig** und **Speichern** aus

Weitere wichtige Stauseinstellungen (Abschnitt "Allgemeine Stauseinstellungen")

### 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

Die wichtigsten Einstellungen im Abschnitt Allgemeine Stauseinstellungen sind:

- **Behebungs-Timer:** Diese Einstellung legt fest, wie lange ein Client eine fehlerhafte Statusbedingung korrigieren muss. In der AnyConnect-Konfiguration gibt es auch einen Behebungs-Timer. Dieser Timer gilt für die ISE, nicht für AnyConnect.
- **Standardstatus für den Status:** Diese Einstellung stellt den Statusstatus für Geräte ohne den Statusagent oder Betriebssysteme bereit, auf denen der temporale Agent nicht ausgeführt werden kann, z. B. Linux-basierte Betriebssysteme.
- **Unterbrechungsfreie Überwachung:** Diese Einstellung gilt für die Anwendungs- und Hardwarebedingungen, die das Endgerät inventarisieren. Die Einstellung legt fest, wie oft



AnyConnect die Überwachungsdaten senden muss.

- **Richtlinien zur akzeptablen Nutzung im Stealth-Modus:** Die einzigen beiden Optionen für diese Einstellung sind Blockieren oder Fortfahren. Blockierung verhindert, dass AnyConnect-Clients im Stealth-Modus fortfahren, wenn die AUP nicht bestätigt wurde. Continue ermöglicht dem Stealth-Mode-Client, auch ohne Bestätigung der AUP fortzufahren (dies ist bei Verwendung der Stealth-Modus-Einstellung von AnyConnect oft die Absicht).

## Konfigurationen für Neubewertungen

Statusneubewertungen sind eine wichtige Komponente des Statusworkflows. Im Abschnitt "Posture Protocol" (Status-Protokoll) haben Sie gesehen, wie Sie den AnyConnect-Agent für Statusüberprüfungen konfigurieren. Der Agent überprüft regelmäßig die PSNs, die basierend auf dem Timer in dieser Konfiguration definiert wurden.

Wenn eine Anforderung das PSN erreicht, bestimmt das PSN, ob eine Statusüberprüfung auf Basis der ISE-Konfiguration für die Rolle dieses Endpunkts erforderlich ist. Wenn der Client die Neubewertung besteht, behält das PSN den Status-konform des Endpunkts bei, und der Status-Lease wird zurückgesetzt. Wenn der Endpunkt die Neubewertung nicht bestanden hat, ändert sich der Status in "Nicht konform", und alle vorhandenen Statusleasen werden entfernt.

**Schritt 36:** Wählen Sie **Richtlinien > Richtlinienelemente > Ergebnisse > Autorisierung > Autorisierungsprofil aus. Hinzufügen** auswählen

**Schritt 37:** Definieren Sie **Wired\_Redirect** als Autorisierungsprofil, und konfigurieren Sie die nächsten Parameter.

### 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

**Schritt 38:** Wählen Sie **Speichern**

**Schritt 39:** Autorisierungsrichtlinien konfigurieren

Es gibt drei vorkonfigurierte Autorisierungsregeln für den Status:

1. Die erste wird so konfiguriert, dass sie bei erfolgreicher Authentifizierung übereinstimmt. Die Compliance eines Geräts ist unbekannt.
2. Die zweite Regel vergleicht erfolgreiche Authentifizierungen mit nicht konformen Endpunkten.

**Anmerkung:** Beide ersten beiden Regeln haben dasselbe Ergebnis, d. h. die Verwendung eines vorkonfigurierten Autorisierungsprofils, das den Endpunkt zum Client Provisioning-Portal umleitet.

3. Die letzte Regel stimmt mit erfolgreichen authentifizierungs- und statuskonformen Endpunkten überein und verwendet das vordefinierte PermitAccess-Autorisierungsprofil.

Wählen Sie **Policy > Policy Set (Richtlinie > Richtlinienansatz)** aus, und klicken Sie auf den Pfeil nach rechts für **Wired 802.1x - MAB Created in the previous lab**.

**Schritt 40:** Wählen Sie **Autorisierungsrichtlinie** aus, und erstellen Sie die nächsten Regeln.



## Konfigurationen auf dem Switch

**Anmerkung:** Die nachfolgende Konfiguration bezieht sich auf IBNS 1.0. Für IBNS 2.0-fähige Switches können Unterschiede bestehen. Sie umfasst die Bereitstellung im Low Impact-Modus.

```
username <admin> privilege 15 secret <password>
aaa new-model
!
aaa group server radius RAD_ISE_GRP
server name <isepsnnode_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
```

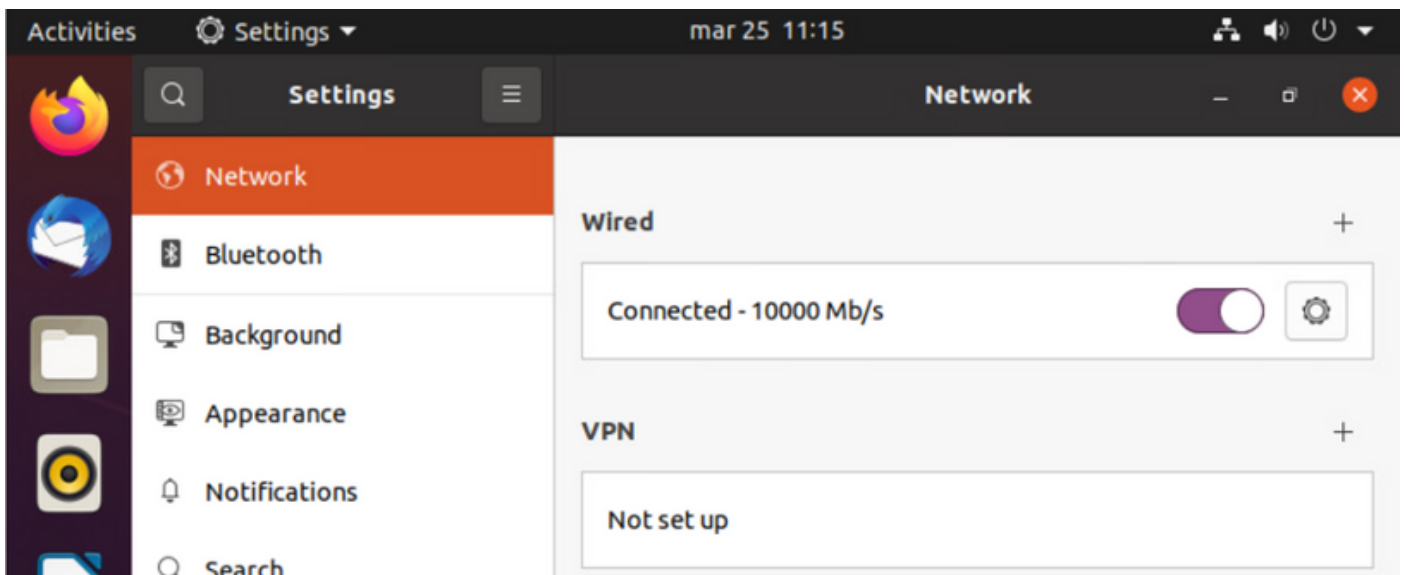
## Überprüfung

### ISE-Verifizierung:

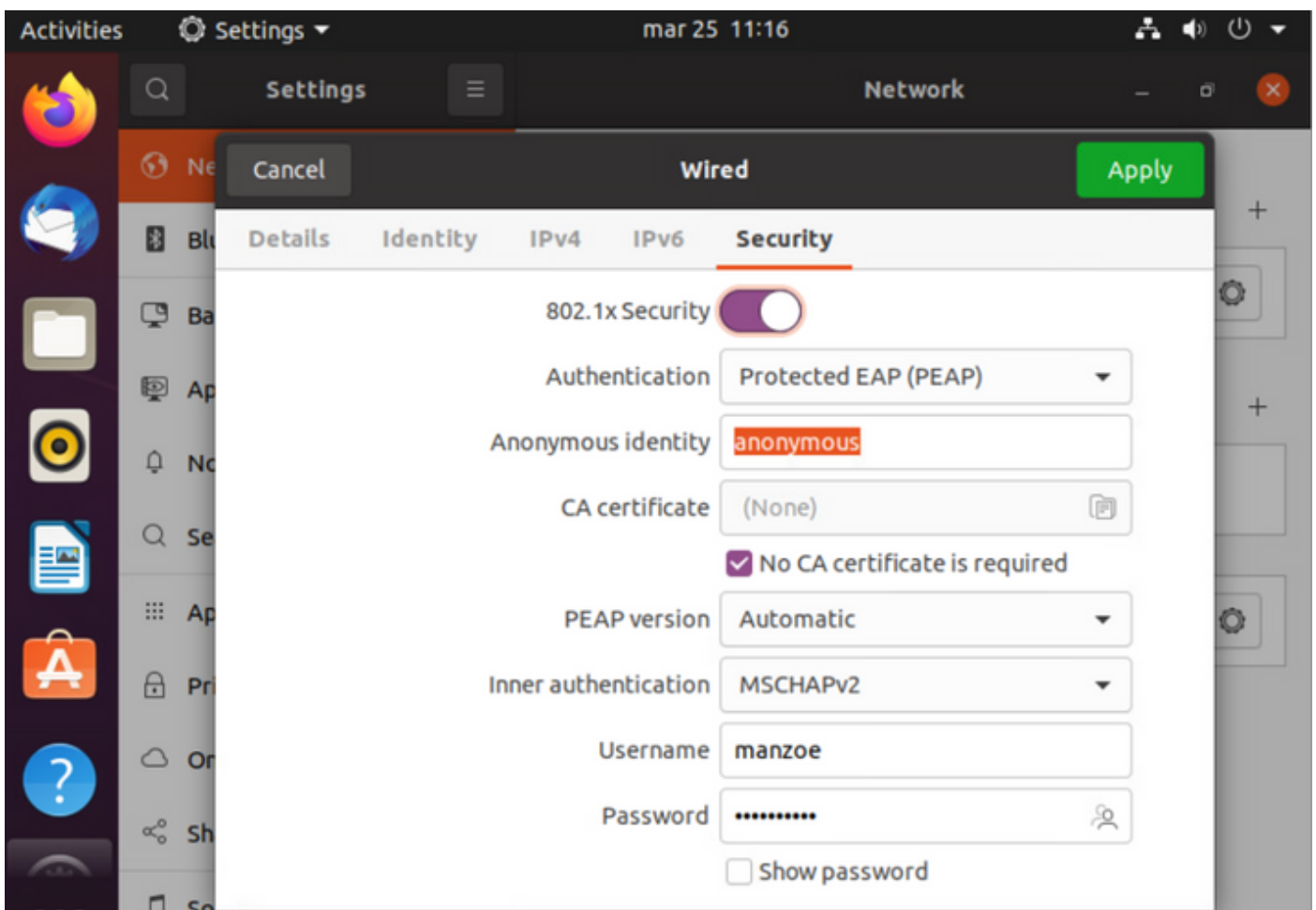
In diesem Abschnitt wird davon ausgegangen, dass AnyConnect mit dem ISE-Statusmodul bereits auf dem Linux-System installiert wurde.

### PC mit dot1x authentifizieren

**Schritt 1:** Navigieren Sie zu Netzwerkeinstellungen.



**Schritt 2:** Wählen Sie die Registerkarte Sicherheit aus, und stellen Sie 802.1x-Konfigurationen und Benutzeranmeldeinformationen bereit.



**Schritt 3.** Klicken Sie auf "Übernehmen".

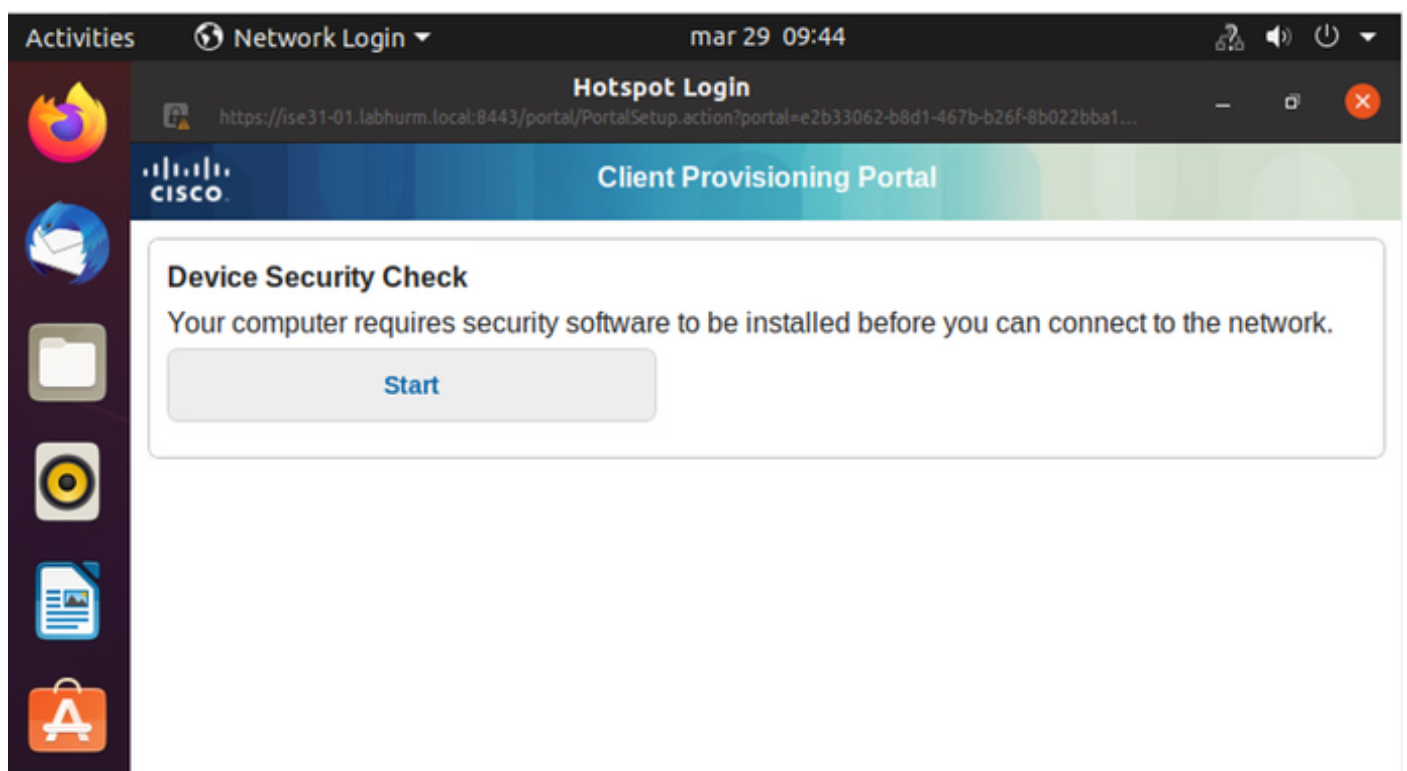
**Schritt 4:** Verbinden Sie das Linux-System mit dem 802.1x-kabelgebundenen Netzwerk, und validieren Sie es im ISE-Live-Protokoll:

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...	<span style="color: blue;">●</span>		4	marcoe	00:0C:29:44:03:8F	Ubuntu W...	Ubuntu Po...	Ubuntu Po...	Wired_Re...			FastEthernet1...		Pending
Apr 06, 2022 08:32:48.2...	<span style="color: green;">●</span>			marcoe	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...	<span style="color: green;">●</span>			marcoe	00:0C:29:44:03:8F	Ubuntu W...	Ubuntu Po...	Ubuntu Po...	Wired_Re...		Cat-3750	FastEthernet1...	Workstation	Pending

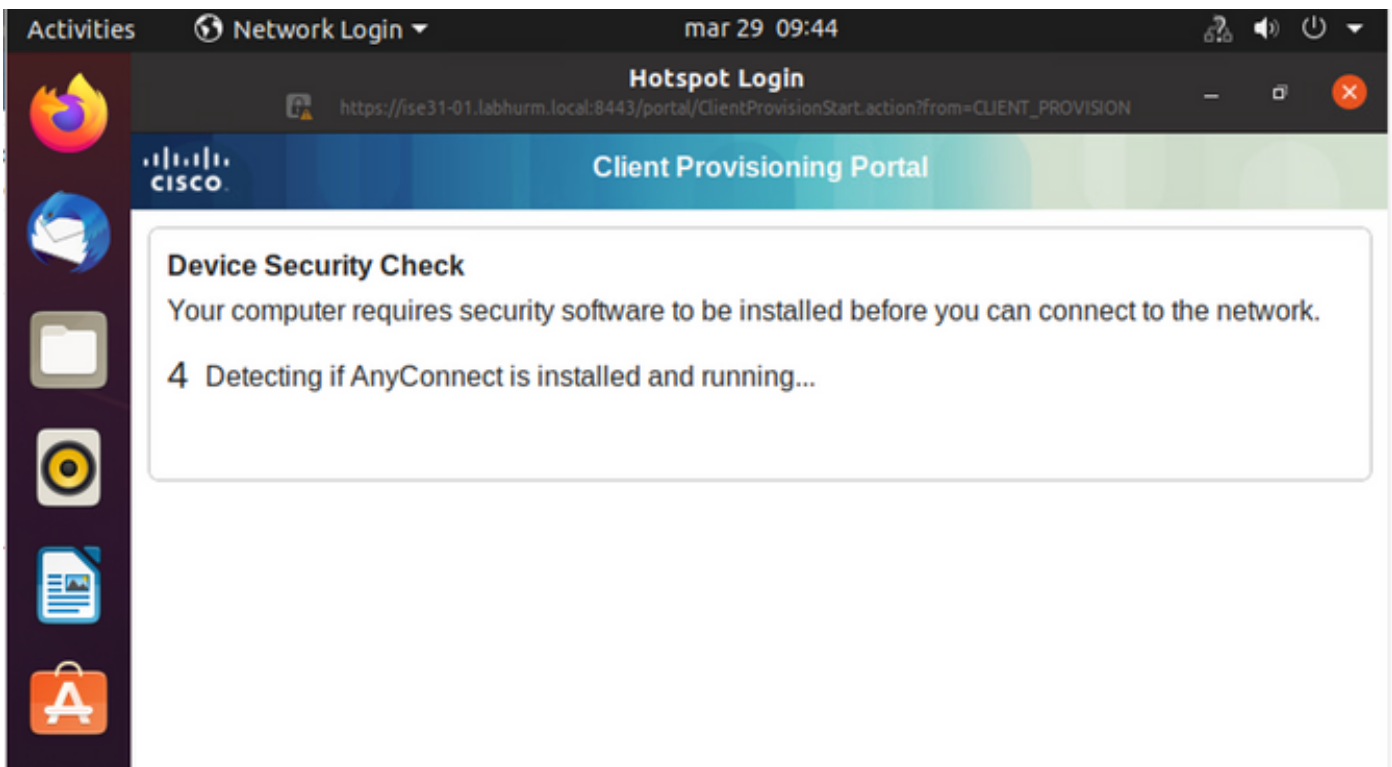
Verwenden Sie in ISE die horizontale Bildlaufleiste, um zusätzliche Informationen anzuzeigen, z. B. das PSN, das den Fluss bereitgestellt hat, oder den Status:

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

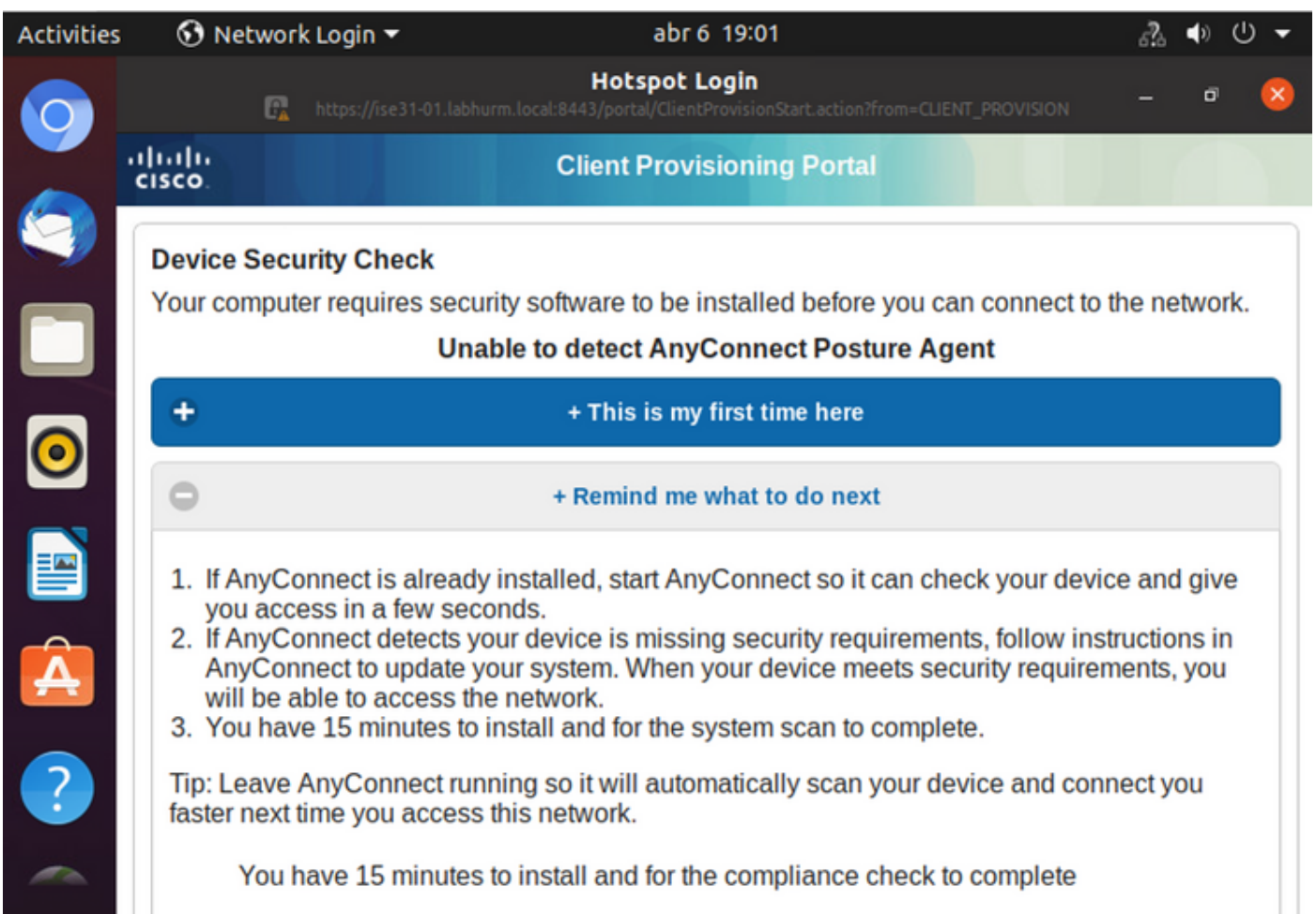
**Schritt 5:** Auf dem Linux-Client muss eine Umleitung erfolgen, und es wird das Client-Bereitstellungsportal angezeigt, das eine Statusüberprüfung anzeigt, und auf **"Start"** klicken:



Warten Sie einige Sekunden, während der Connector versucht, AnyConnect zu erkennen:

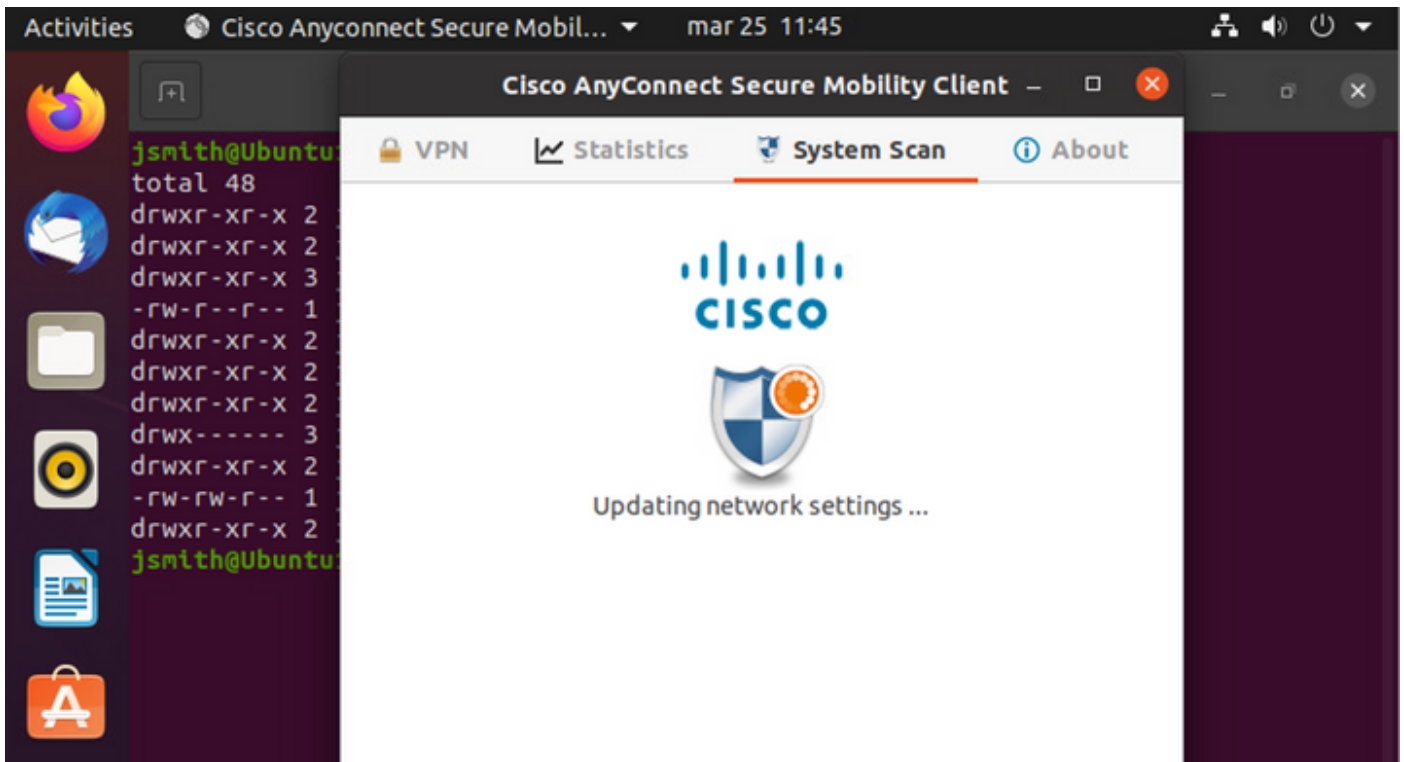


Aufgrund eines bekannten Vorbehalts erkennt AnyConnect selbst dann nicht, wenn AnyConnect installiert ist. Wechseln Sie mit **Alt-Tab** oder dem **Aktivitäts-Menü** zum AnyConnect-Client.

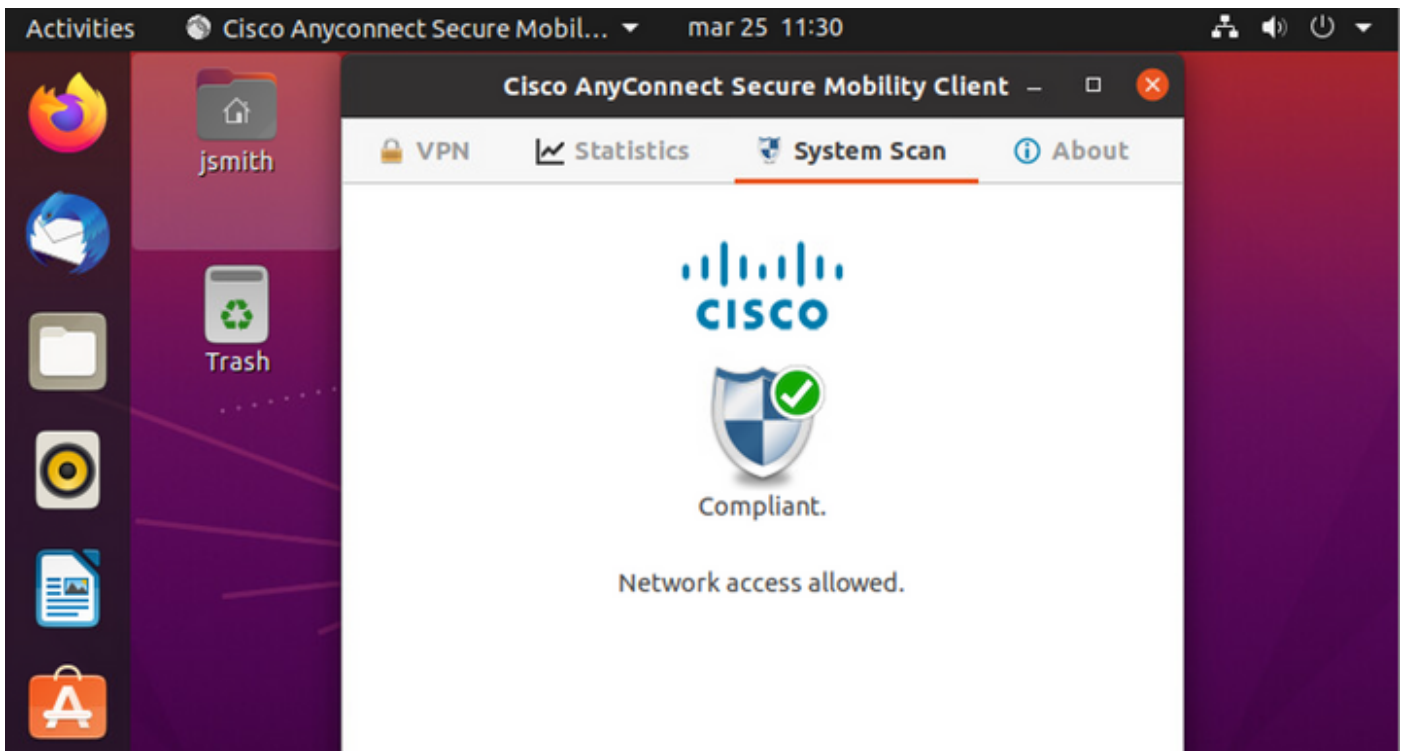


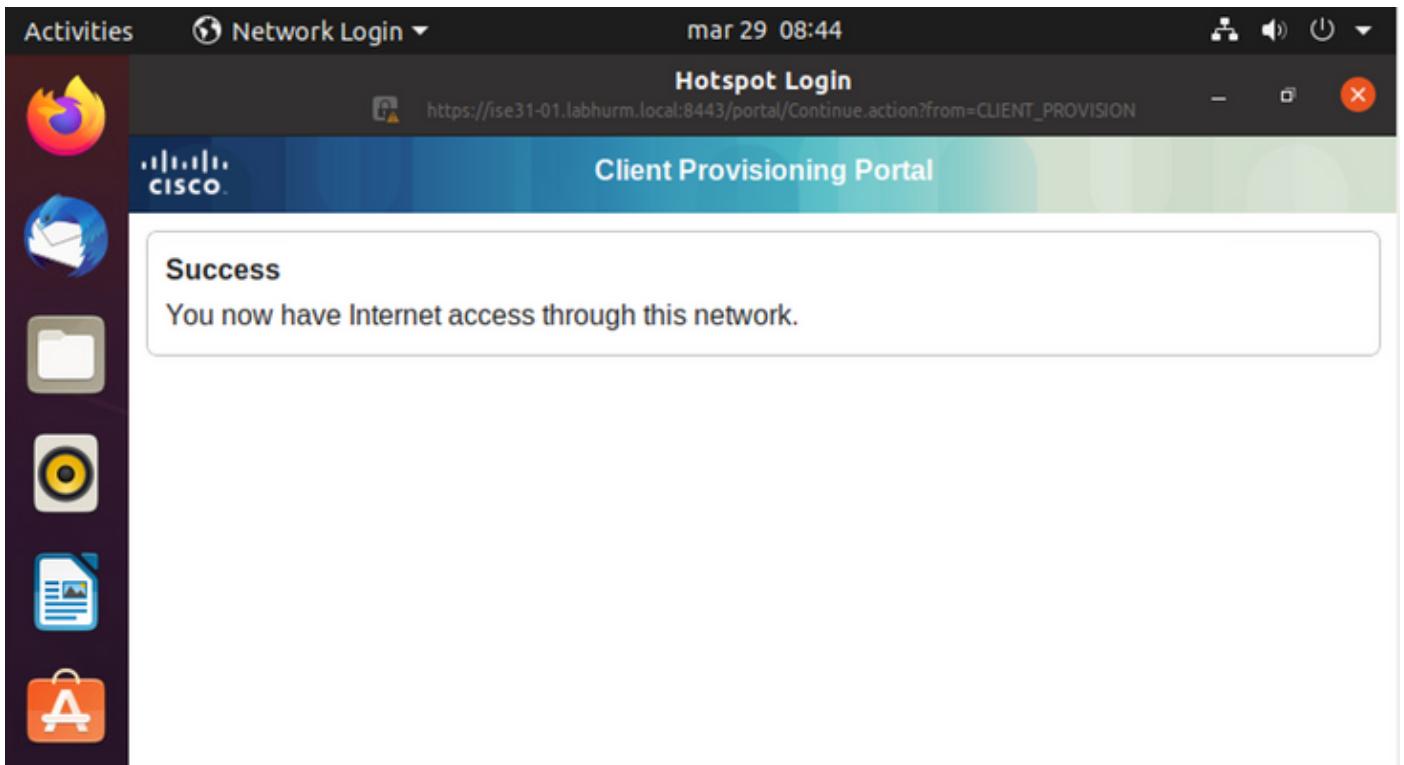
AnyConnect versucht, das PSN für Statusrichtlinien zu erreichen und den Endpunkt dagegen zu bewerten.





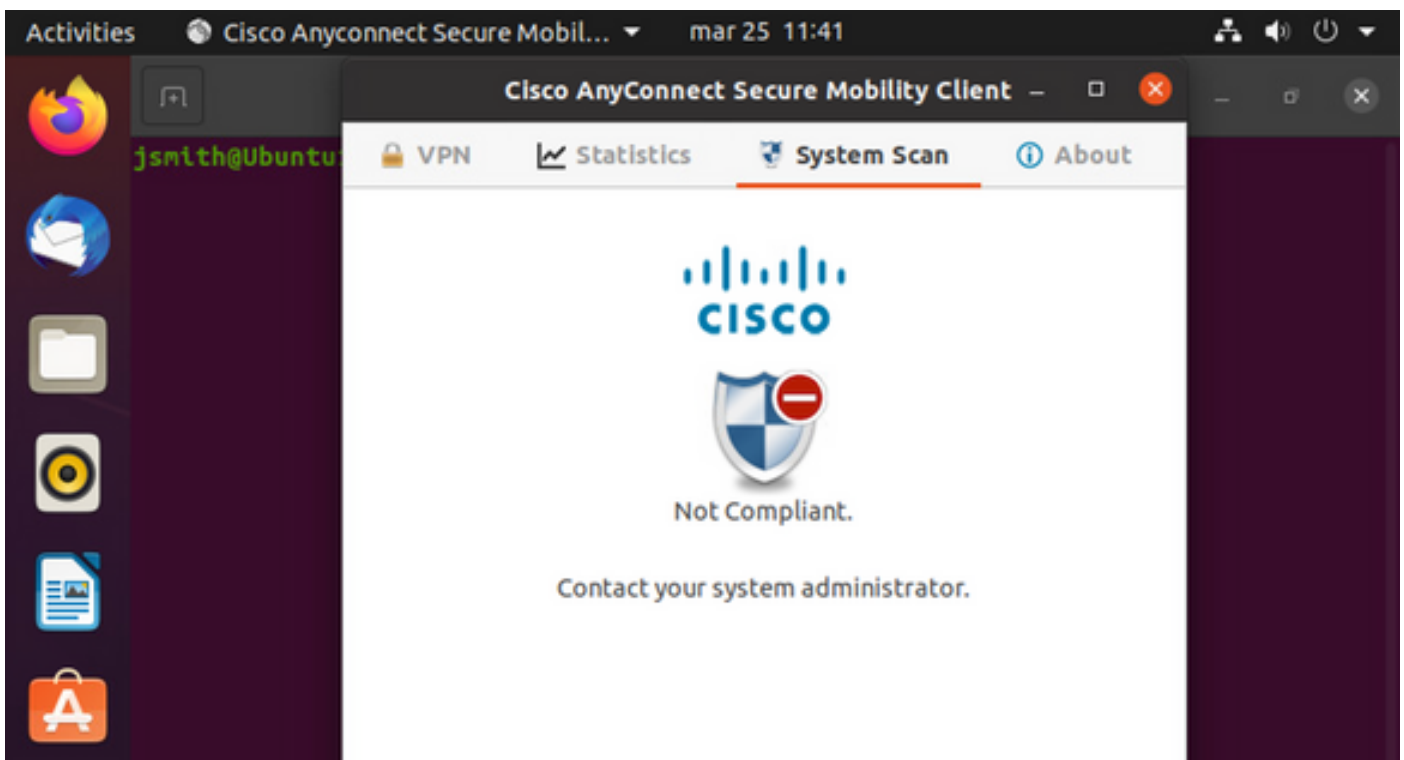
AnyConnect meldet die Festlegung der Statusrichtlinie an die ISE zurück. In diesem Fall konform





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

Wenn die Datei jedoch nicht vorhanden ist, meldet das AnyConnect-Statusmodul die Entschlossenheit an die 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 Device	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

**Anmerkung:** ISE FQDN muss unter Linux über DNS oder eine lokale Host-Datei auflösbar sein.

## Fehlerbehebung

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

**Nächste Schritte:**

```
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&
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
```

**Autorisierung erfolgreich:**

```
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
```

Nicht konform, in Quarantäne für VLAN und ACL verschoben:

```
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
```