

Linux에서 Cisco ISE 3.1 상태 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[구성](#)

[ISE의 컨피그레이션](#)

[스위치의 컨피그레이션](#)

[다음을 확인합니다.](#)

[문제 해결](#)

소개

이 문서에서는 Linux 및 ISE(Identity Services Engine)에 대한 파일 상태 정책을 구성하고 구현하는 절차에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- AnyConnect
- Identity Services Engine(ISE)
- Linux

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

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

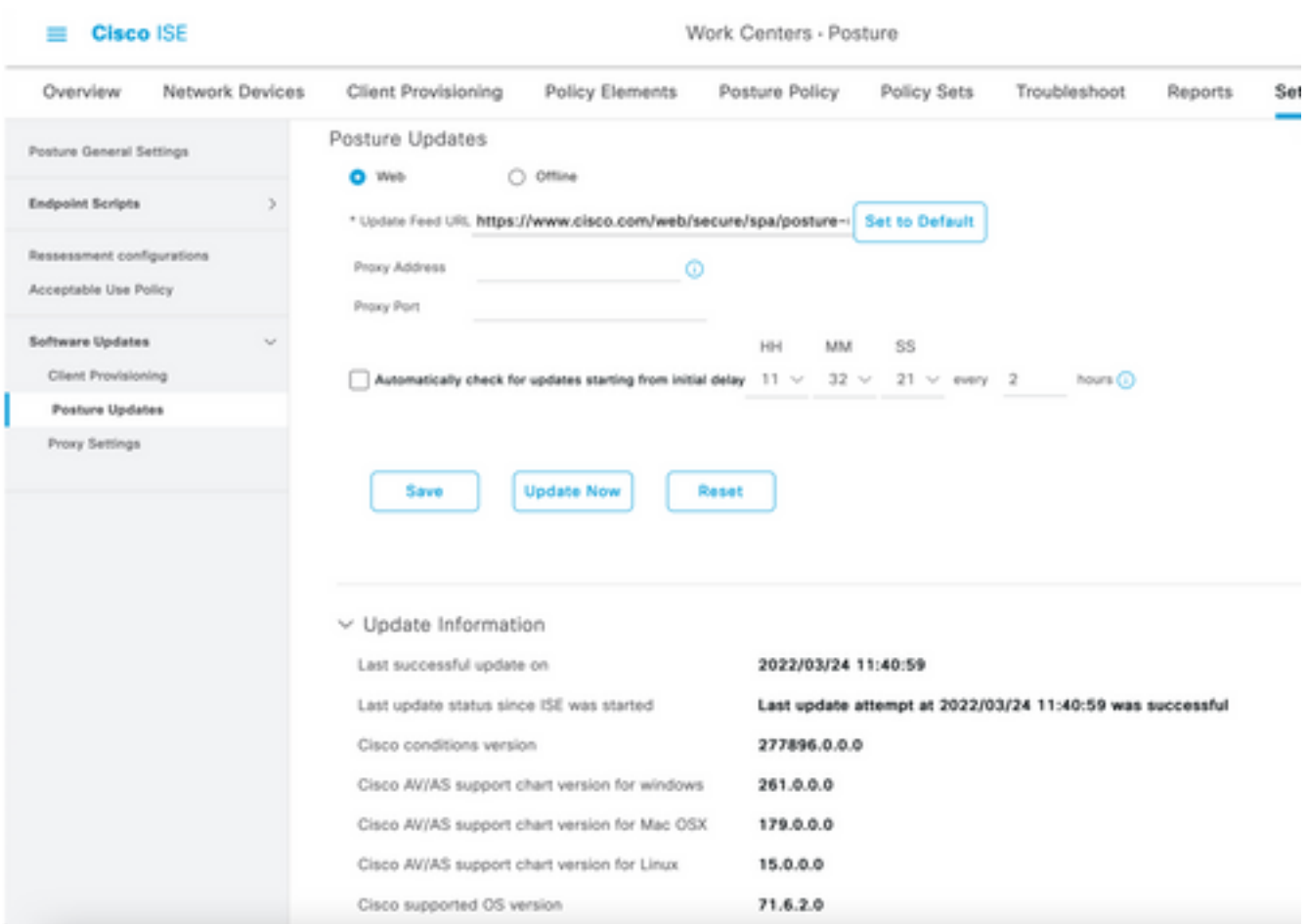
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

ISE의 컨피그레이션

1단계. 상태 서비스 업데이트:

Work Centers(작업 센터) > Posture(포스처) > Settings(설정) > Software Updates(소프트웨어 업데이트) > Posture Updates(포스처 업데이트)로 이동합니다. 지금 업데이트를 선택하고 프로세스가 완료될 때까지 기다립니다.



Cisco 제공 패키지는 AnyConnect 소프트웨어 패키지와 같이 Cisco.com 사이트에서 다운로드하는 소프트웨어 패키지입니다. 고객이 생성한 패키지는 ISE 사용자 인터페이스 외부에서 생성한 프로파일 또는 컨피그레이션으로, 상태 평가에 사용할 수 있도록 ISE에 업로드하려고 합니다. 이 연습에서는 AnyConnect webdeploy 패키지 "anyconnect-linux64-4.10.05085-webdeploy-k9.pkg"를 다운로드할 수 있습니다.

참고: 업데이트 및 패치 때문에 권장 버전이 변경될 수 있습니다. cisco.com 사이트의 최신 권장 버전을 사용하십시오.

2단계.AnyConnect 패키지 업로드:

Posture Work(포스처 작업) 센터 내에서 Client Provisioning(클라이언트 프로비저닝) > Resources(리소스)로 이동합니다

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

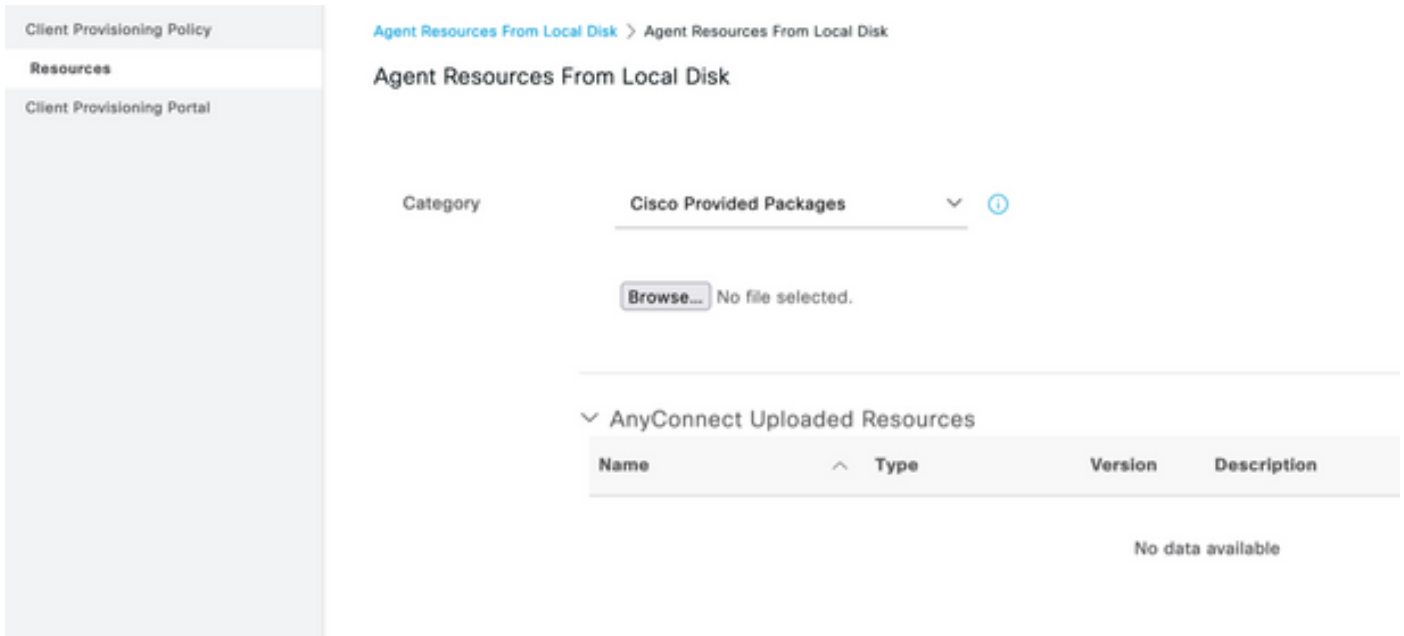
3단계. Add(추가) > Agent Resources from Local Disk(로컬 디스크의 에이전트 리소스)를 선택합니다

Resources

Edit + Add Duplicate Delete

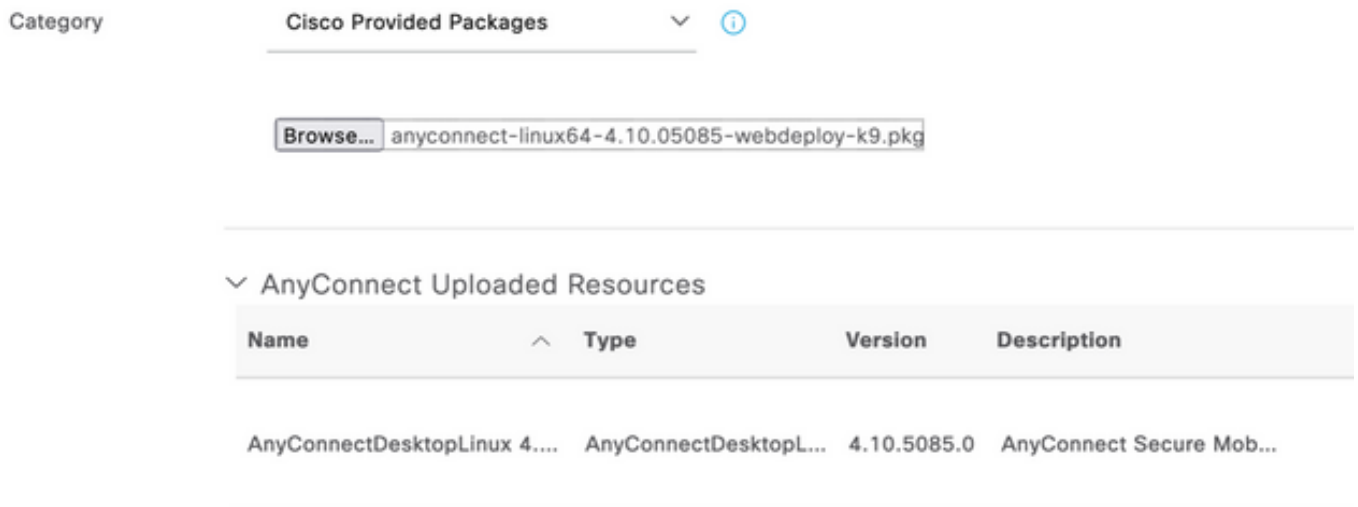
<input type="checkbox"/>	Agent resources from Cisco site
<input type="checkbox"/>	Agent resources from local disk

4단계. Category(카테고리) 드롭다운에서 Cisco Provided Packages(Cisco 제공 패키지)를 선택합니다.



5단계. **Browse(찾아보기)**를 클릭합니다.

6단계. 이전 단계에서 다운로드한 AnyConnect 패키지 중 하나를 선택합니다. AnyConnect 이미지가 처리되고 패키지에 대한 정보가 표시됩니다



7단계. **Submit**을 클릭합니다. 이제 AnyConnect가 ISE에 업로드되었으므로 ISE 담당자를 확보하고 Cisco.com에서 다른 클라이언트 리소스를 가져올 수 있습니다.

참고: 에이전트 리소스에는 안티바이러스, 안티스파이웨어, 안티멀웨어, 방화벽, 디스크 암호화, 파일 등과 같은 다양한 조건 검사에 대한 엔드포인트의 규정 준수를 평가하는 기능을 제공하는 AnyConnect 클라이언트에서 사용하는 모듈이 포함됩니다.

8단계. **Add(추가) > Agent Resources from Cisco Site(Cisco 사이트에서 에이전트 리소스)**를 클릭합니다. ISE가 Cisco.com에 접속하여 클라이언트 프로비저닝을 위해 게시된 모든 리소스의 매니페스트를 검색할 때 창이 채워지는 데 1분 정도 걸립니다.

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

9단계. Linux용 최신 AnyConnect 규정 준수 모듈을 선택합니다. 또한 Windows 및 Mac용 규정 준수 모듈을 선택할 수도 있습니다.



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

10단계. Windows 및 Mac용 최신 임시 에이전트를 선택합니다.

<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!

11단계. 저장을 클릭합니다.

참고: MAC 및 Windows Posture 컨피그레이션은 이 컨피그레이션 가이드의 범위에 속하지 않습니다.

이 시점에서 모든 필수 부품을 업로드하고 업데이트했습니다. 이제 이러한 구성 요소를 사용하는데 필요한 컨피그레이션 및 프로필을 작성할 때입니다.

12단계. Add(추가) > NAC Agent 또는 AnyConnect Posture Profile(NAC 에이전트 또는 AnyConnect 포스처 프로파일)을 클릭합니다.

The screenshot shows the ISE Posture Agent Profile Settings interface. At the top, there are action buttons: Edit, Add, Duplicate, and Delete. Below these is a table of existing profiles:

	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	oTemporalAgent...	4.10.6011.0 2022/03/24 11:49:19	Cisco Temporal Agent fo...
<input type="checkbox"/> AnyConnect Configuration	ConnectComplian...	4.3.2716.... 2022/03/24 11:49:39	AnyConnect Windows C...
<input type="checkbox"/> AnyConnect Posture Profile	ve Supplicant Pro...	Not Applic... 2016/10/06 20:01:12	Pre-configured Native S...
<input type="checkbox"/> AMP Enabler Profile	oAgentlessOSX	4.10.2051.0 2021/08/09 19:12:36	With CM: 4.3.1858.4353

Below the table, the 'AnyConnect Posture Profile' configuration form is shown. The 'Name' field is set to 'LinuxACPosture'. The 'Description' field is empty. The 'Agent Behavior' section contains the following 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.

수정해야 하는 매개변수는 다음과 같습니다.

- **VLAN 탐지 간격:** 이 설정을 사용하면 VLAN 변경 사항을 프로빙하는 동안 모듈에서 대기하는 시간(초)을 설정할 수 있습니다. 권장 사항은 5초입니다.
- **Ping 또는 ARP:** 이것이 실제 VLAN 변경 감지 방법입니다. 에이전트는 기본 게이트웨이를 ping하거나 기본 게이트웨이의 항목이 시간 초과되거나 둘 다 초과될 수 있도록 ARP 캐시를 모니터링할 수 있습니다. 권장 설정은 ARP입니다.
- **교정 타이머:** 엔드포인트의 상태를 알 수 없는 경우 엔드포인트는 상태 평가 플로우를 거칩니다. 실패한 상태 검사를 해결하는 데 시간이 걸립니다. 기본 시간은 엔드포인트를 비호환 상태로 표시하기 전 4분이지만, 값의 범위는 1~300분(5시간)입니다. 권장 시간은 15분입니다. 그러나 교정이 더 오래 걸릴 것으로 예상되는 경우 이를 조정해야 할 수 있습니다.

참고: Linux 파일 상태는 자동 교정을 지원하지 않습니다.

모든 매개변수에 대한 포괄적인 설명은 ISE 또는 AnyConnect 상태 설명서를 참조하십시오.

13단계. 에이전트 동작에서는 Posture Probes Backup List(포스처 프로브 백업 목록)를 선택하고 **Choose(선택)**, PSN/Standalone FQDN(PSN/독립형 FQDN) 선택 및 **Select Save(저장 선택)**를 선택합니다.

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

14단계. Posture Protocols(포스처 프로토콜) > Discovery Host(검색 호스트)에서 PSN/독립형 노드 ip 주소를 정의합니다.

15단계. Discovery Backup Server 목록과 **Select Choose**에서 PSN 또는 독립형 FQDN을 선택하고 **Select**를 선택합니다.

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

16단계. Server name rules(서버 이름 규칙)에서*를 입력하여 모든 서버에 연결하고 Call Home(콜 홈) 목록에서 PSN/Standalone IP 주소를 정의합니다. 또는 와일드카드를 사용하여 네트워크의 모든 잠재적 PSN을 일치시킬 수 있습니다(예: *.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

17단계. Add(추가) > AnyConnect Configuration(AnyConnect 컨피그레이션)을 클릭합니다

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

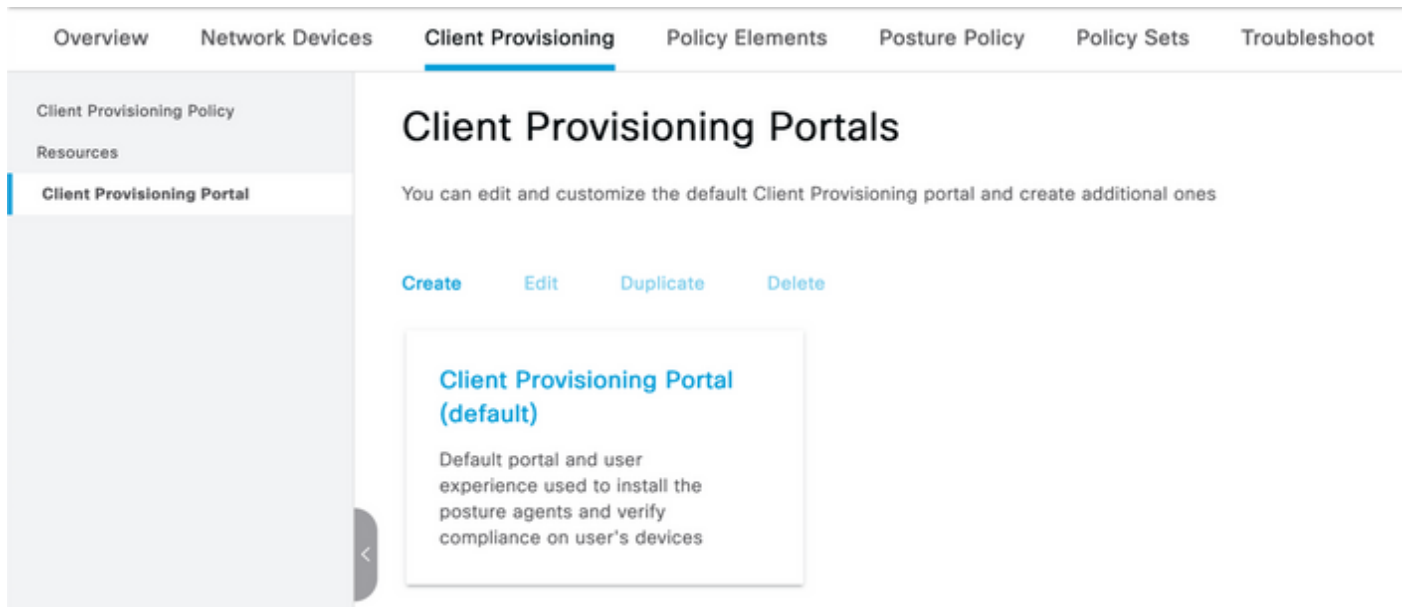
Customer
Feedback ▾

LinuxACPosture

아래로 스크롤하여 Submit(제출)을 선택합니다.

18단계. 선택을 마쳤으면 실행을 누릅니다.

19단계. Work Centers(작업 센터) > Posture(포스처) > Client Provisioning(클라이언트 프로비저닝) > Client Provisioning Portals(클라이언트 프로비저닝 포털)를 선택합니다.



20단계. Portal Settings(포털 설정) 섹션 아래에서 인터페이스 및 포트를 선택하고 페이지에 대한 권한이 부여된 그룹을 선택할 수 있습니다. Select Employee, SISE_Users and Domain Users(직원, SISE_사용자 및 도메인 사용자 선택)

Configure authorized groups

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

Available

SEARCH

ALL_ACCOUNTS (default)

GROUP_ACCOUNTS (default)

OWN_ACCOUNTS (default)

>

<

Chosen

Employee

Choose all

Clear all

21단계. Log in Page Settings(로그인 페이지 설정) 아래에서 **Enable auto Log In(자동 로그인 활성화)** 옵션이 활성화되었는지 확인합니다

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

22단계. 오른쪽 상단에서 Save(저장)를 선택합니다

23단계. Work Centers(작업 센터) > Posture(포스처) > Client Provisioning(클라이언트 프로비저닝) > Client Provisioning Policy(클라이언트 프로비저닝 정책)를 선택합니다.

24단계. CPP에서 IOS 규칙 옆에 있는 아래쪽 화살표를 클릭하고 Duplicate Above(위 복제)를 선택합니다

25단계. 규칙의 이름을 LinuxPosture로 지정합니다.

26단계. 결과에서 AnyConnect 컨피그레이션을 에이전트로 선택합니다.

참고: 이 경우 규정 준수 모듈 드롭다운은 AnyConnect 컨피그레이션의 일부로 구성되므로 표시되지 않습니다.

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 Supplicant 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

27단계. 완료를 클릭합니다.

28단계. 저장을 클릭합니다.

상태 정책 요소

29단계. Work Centers(작업 센터) > Posture(상태) > Policy Elements(정책 요소) > Conditions(조건) > File(파일)을 선택합니다. Add를 선택합니다.

30단계. TESTFile을 파일 조건 이름으로 정의하고 다음 값을 정의합니다

File Condition

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

참고: 경로는 파일 위치를 기반으로 합니다.

31단계. 저장을 선택합니다

FileExistence. 이 파일 유형의 조건은 파일이 있어야 할 시스템에 있는지, 그리고 그것이 전부인지 확인합니다. 이 옵션을 선택하면 파일 날짜, 해시 등의 유효성을 검사할 필요가 없습니다

32단계. Requirements를 선택하고 다음과 같이 새 정책을 생성합니다.

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

참고: Linux에서는 메시지 텍스트를 교정 작업으로만 지원하지 않습니다

요구 사항 구성 요소

- 운영 체제: Linux 모두
- 규정 준수 모듈: 4.x
- 상태 유형: AnyConnect
- 조건: 규정 준수 모듈 및 에이전트(OS를 선택한 후 사용 가능)
- 교정 작업: 다른 모든 조건을 선택한 후 선택할 수 있게 되는 교정.

33단계. Work Centers(작업 센터) > Posture(포스처) > Posture Policy(포스처 정책)를 선택합니다

34단계. Edit on any policy(정책에 대한 편집)를 선택하고 Insert New policy Define LinuxPosturePolicy Policy(새 정책에 LinuxPosturePolicy 정책 정의)를 이름으로 선택하고 32단계

에서 생성한 요구 사항을 추가합니다.

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	LinuxPosturePOlic	Any	and Linux All	and 4.x or later	and AnyConnect	and	than LinuxFile	Edit

35단계. 완료를 선택하고 저장을 선택합니다

기타 중요한 상태 설정 (상태 일반 설정 섹션)

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

Posture General Settings(포스처 일반 설정) 섹션의 중요한 설정은 다음과 같습니다.

- **교정 타이머:** 이 설정은 클라이언트가 실패한 상태 조건을 수정해야 하는 시간을 정의합니다. AnyConnect 컨피그레이션에도 교정 타이머가 있습니다. 이 타이머는 AnyConnect가 아니라 ISE용입니다.
- **기본 상태 상태:** 이 설정은 Linux 기반 운영 체제와 같이 임시 에이전트를 실행할 수 없는 운영 체제 또는 포스처 에이전트가 없는 디바이스에 대한 포스처 상태를 제공합니다.
- **연속 모니터링 간격:** 이 설정은 엔드포인트의 인벤토리를 수행하는 애플리케이션 및 하드웨어 조건에 적용됩니다. 이 설정은 AnyConnect에서 모니터링 데이터를 전송해야 하는 빈도를 지정합니다.
- **스텔스 모드의 수락 가능한 사용 정책:** 이 설정에 대한 두 가지 선택 사항은 차단 또는 계속입니다. Block은 AUP가 승인되지 않은 경우 스텔스 모드 AnyConnect 클라이언트가 진행되지 않

도록 합니다. Continue(계속)를 사용하면 AUP(AnyConnect의 스텔스 모드 설정 사용 시 종종 의도)를 승인하지 않아도 스텔스 모드 클라이언트가 계속 진행할 수 있습니다.

구성 재평가

상태 재평가는 상태 워크플로의 중요한 구성 요소입니다. "Posture Protocol(포스처 프로토콜)" 섹션에서 포스처 재평가를 위해 AnyConnect 에이전트를 구성하는 방법을 확인했습니다. 에이전트는 해당 컨피그레이션의 타이머에 따라 정의된 PSN을 주기적으로 확인합니다.

요청이 PSN에 도달하면 PSN은 해당 엔드포인트 역할에 대한 ISE 컨피그레이션을 기반으로 포스처 재평가가 필요한지 여부를 결정합니다. 클라이언트가 재평가를 통과하면 PSN은 엔드포인트의 포스처 호환 상태를 유지하고 포스처 리스가 재설정됩니다. 엔드포인트가 재평가에 실패하면 포스처 상태가 비호환으로 변경되고 존재하던 포스처 리스가 제거됩니다.

36단계. Policy(정책) > Policy Elements(정책 요소) > Results(결과) > Authorization(권한 부여) > Authorization Profile(권한 부여 프로파일)을 선택합니다. 추가 선택

37단계. Wired_Redirect를 권한 부여 프로파일로 정의하고 다음 매개변수를 구성합니다

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

38단계. 저장을 선택합니다

39단계. 권한 부여 정책 구성

Posture에는 세 가지 사전 구성된 권한 부여 규칙이 있습니다.

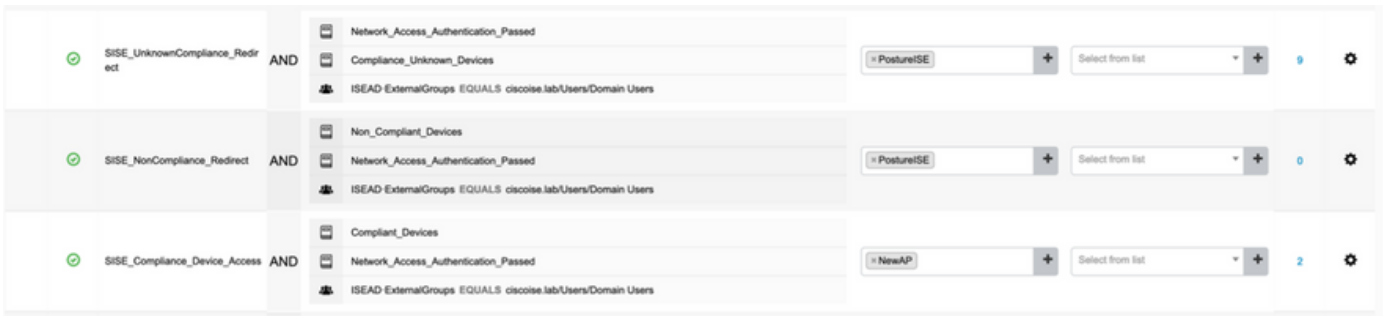
1. 첫 번째는 인증이 성공하고 디바이스의 규정 준수를 알 수 없는 경우에 일치하도록 구성됩니다.
2. 두 번째 규칙은 규정을 준수하지 않는 엔드포인트와 성공한 인증을 매칭합니다.

참고: 처음 두 규칙 모두 동일한 결과를 갖습니다. 즉, 엔드포인트를 클라이언트 프로비저닝 포털로 리디렉션하는 사전 구성된 권한 부여 프로파일을 사용합니다.

3. 최종 규칙은 성공적인 인증 및 포스처 호환 엔드포인트와 일치하며 사전 구축된 PermitAccess 권한 부여 프로파일을 사용합니다.

Policy(정책) > Policy Set(정책 세트)를 선택하고 **Wired 802.1x - MAB Created in the previous lab**(이전 실습에서 생성된 MAB)에 대한 오른쪽 화살표를 선택합니다.

40단계. Authorization Policy(권한 부여 정책)를 선택하고 다음 규칙을 생성합니다



스위치의 컨피그레이션

참고: 아래 구성은 IBNS 1.0을 나타냅니다. IBNS 2.0 지원 스위치에는 차이가 있을 수 있습니다. 여기에는 로우 임팩트 모드 구축이 포함됩니다.

```

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 preiodic 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
```

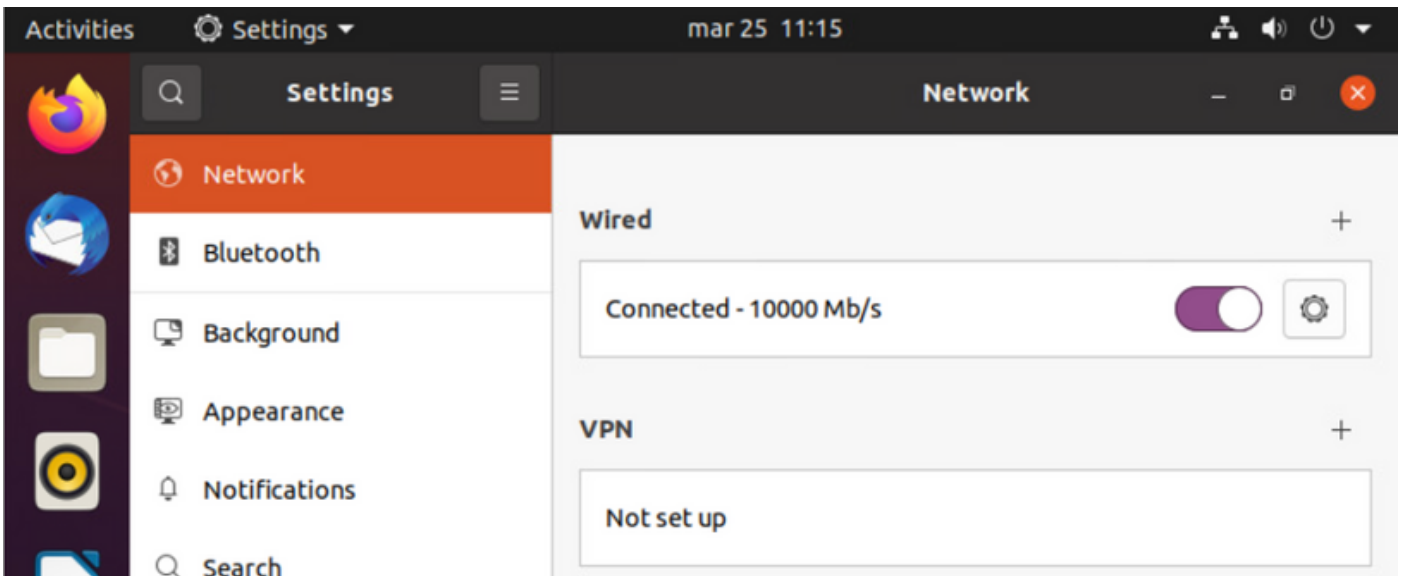
다음을 확인합니다.

ISE 확인:

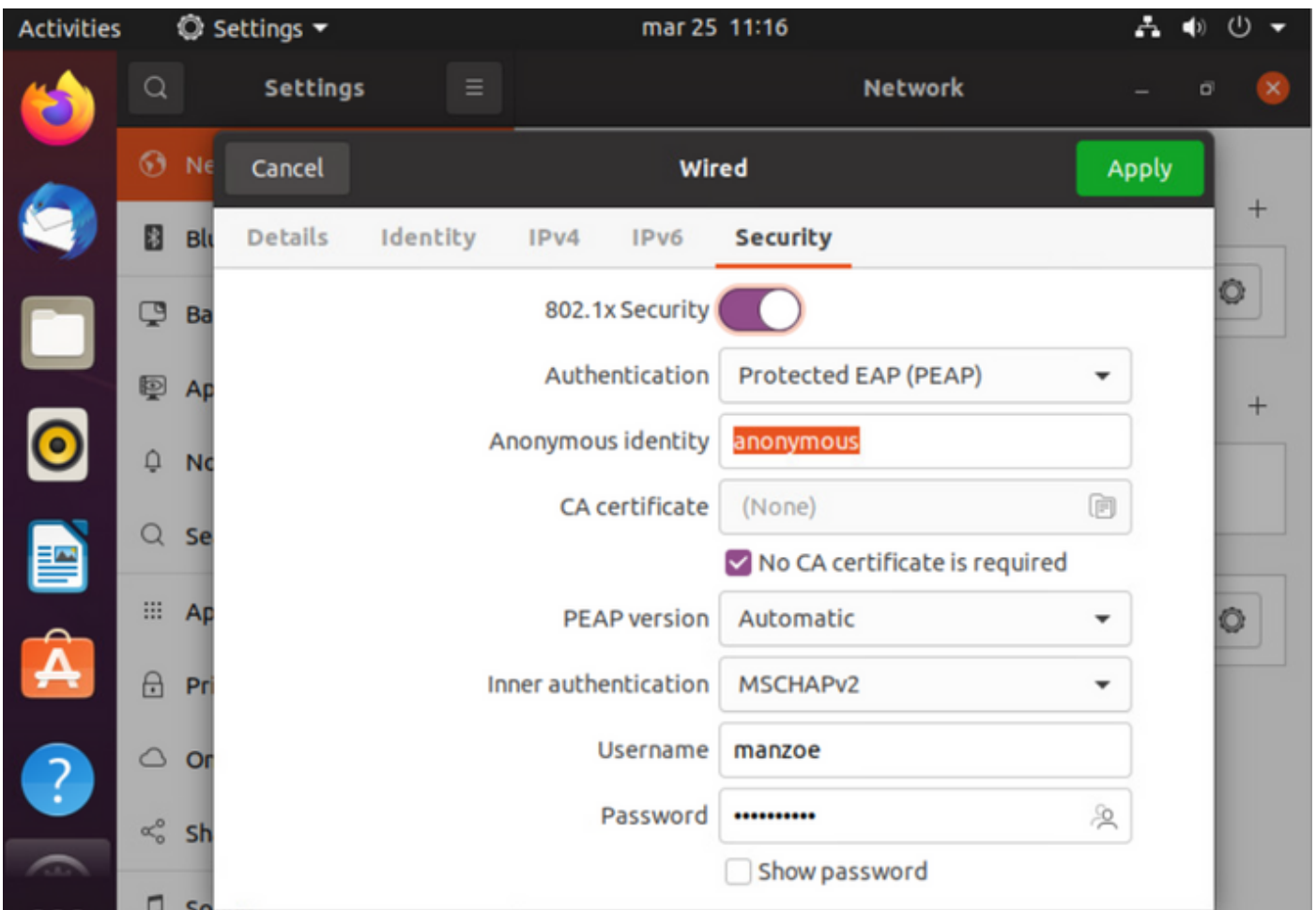
이 섹션에서는 ISE Posture 모듈이 포함된 AnyConnect가 이전에 Linux 시스템에 설치된 것으로 가정합니다.

dot1x를 사용하여 PC 인증

1단계. 네트워크 설정으로 이동합니다.



2단계. Security(보안) 탭을 선택하고 802.1x 컨피그레이션 및 사용자 자격 증명을 제공합니다



3단계. "Apply(적용)"를 클릭합니다.

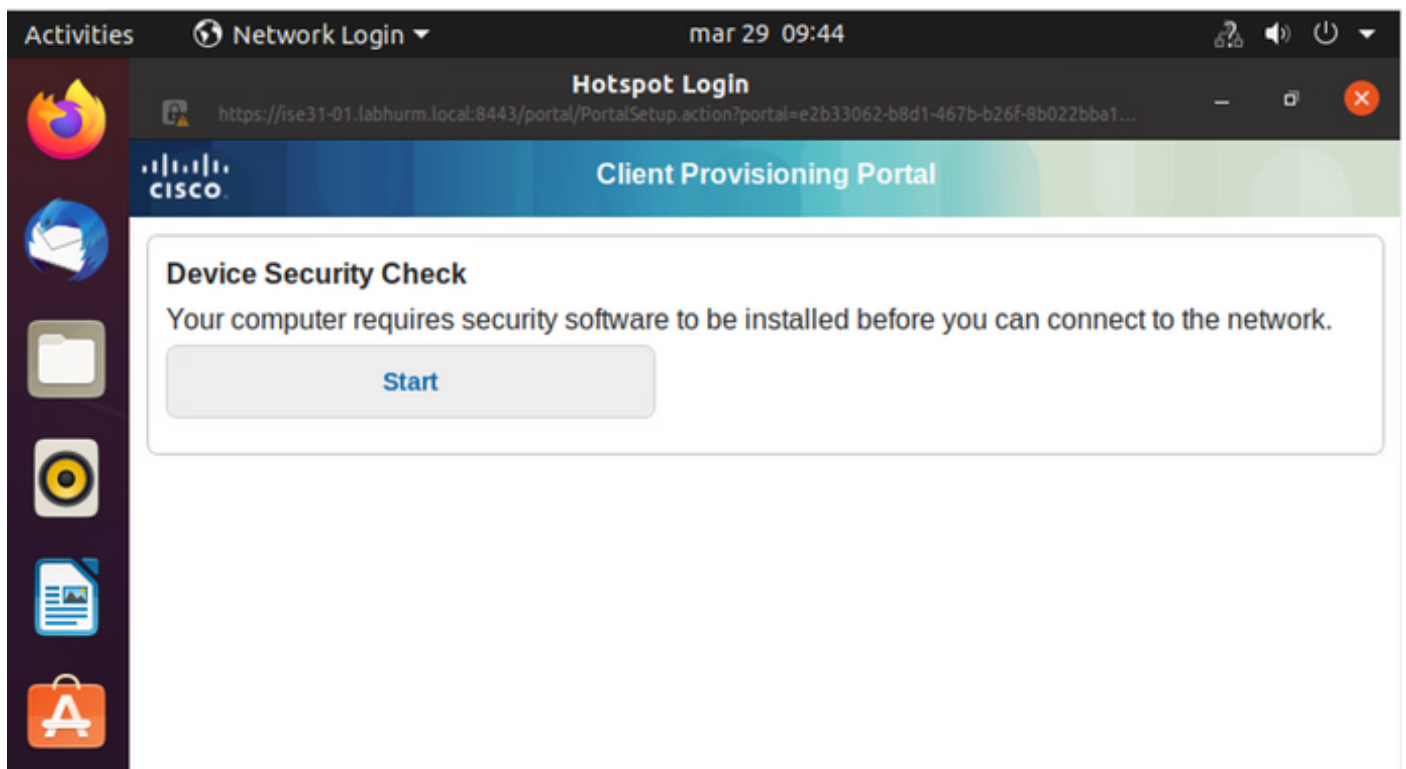
4단계. Linux 시스템을 802.1x 유선 네트워크에 연결하고 ISE 라이브 로그에서 확인합니다.

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint...	Authenti...	Authoria...	AuthORIZ...	IP Address	Network De...	Device Port	Identity Group	Posture
Apr 06, 2022 08:42:08.2...	●		5	manzoe	00:0C:29:44:03:8F	Ubuntu W...	Ubuntu Po...	Ubuntu Po...	Wired_Re...			FastEthernet1...		Pending
Apr 06, 2022 08:32:49.2...	●			manzoe	00:0C:29:44:03:8F	Ubuntu W...	Ubuntu Po...	Ubuntu Po...	Wired_Re...		Can 1750	FastEthernet1...	Workstation	Pending
Apr 06, 2022 08:32:40.8...	●			manzoe	00:0C:29:44:03:8F	Ubuntu W...	Ubuntu Po...	Ubuntu Po...	Wired_Re...		Can 1750	FastEthernet1...	Workstation	Pending

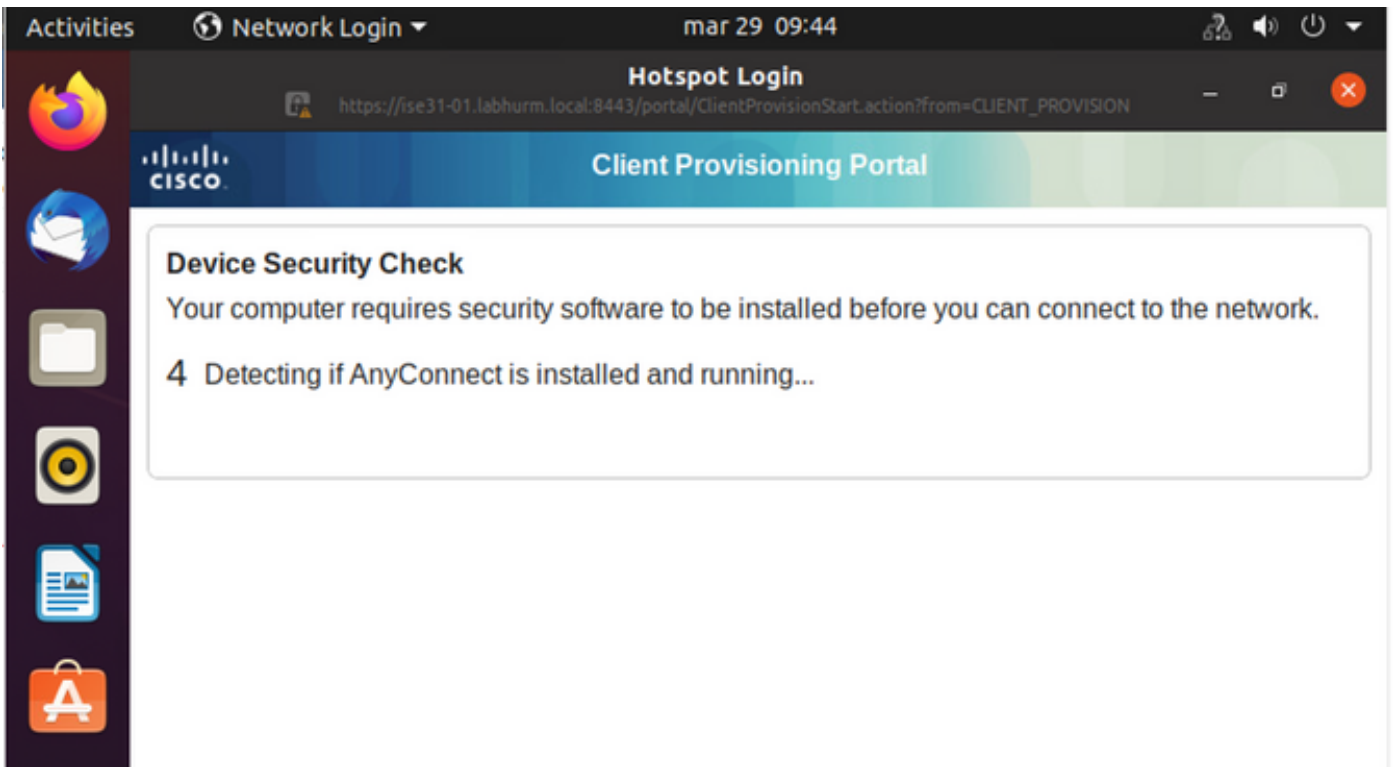
ISE에서 가로 스크롤 막대를 사용하여 플로우나 포스터 상태를 제공하는 PSN과 같은 추가 정보를 봅니다.

Authoriz...	Authoriz...	IP Address	Network De...	Device Port	Identity Group	Posture ...	Server
Authorizatic	Authorizatic	IP Address	Network Devicr	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

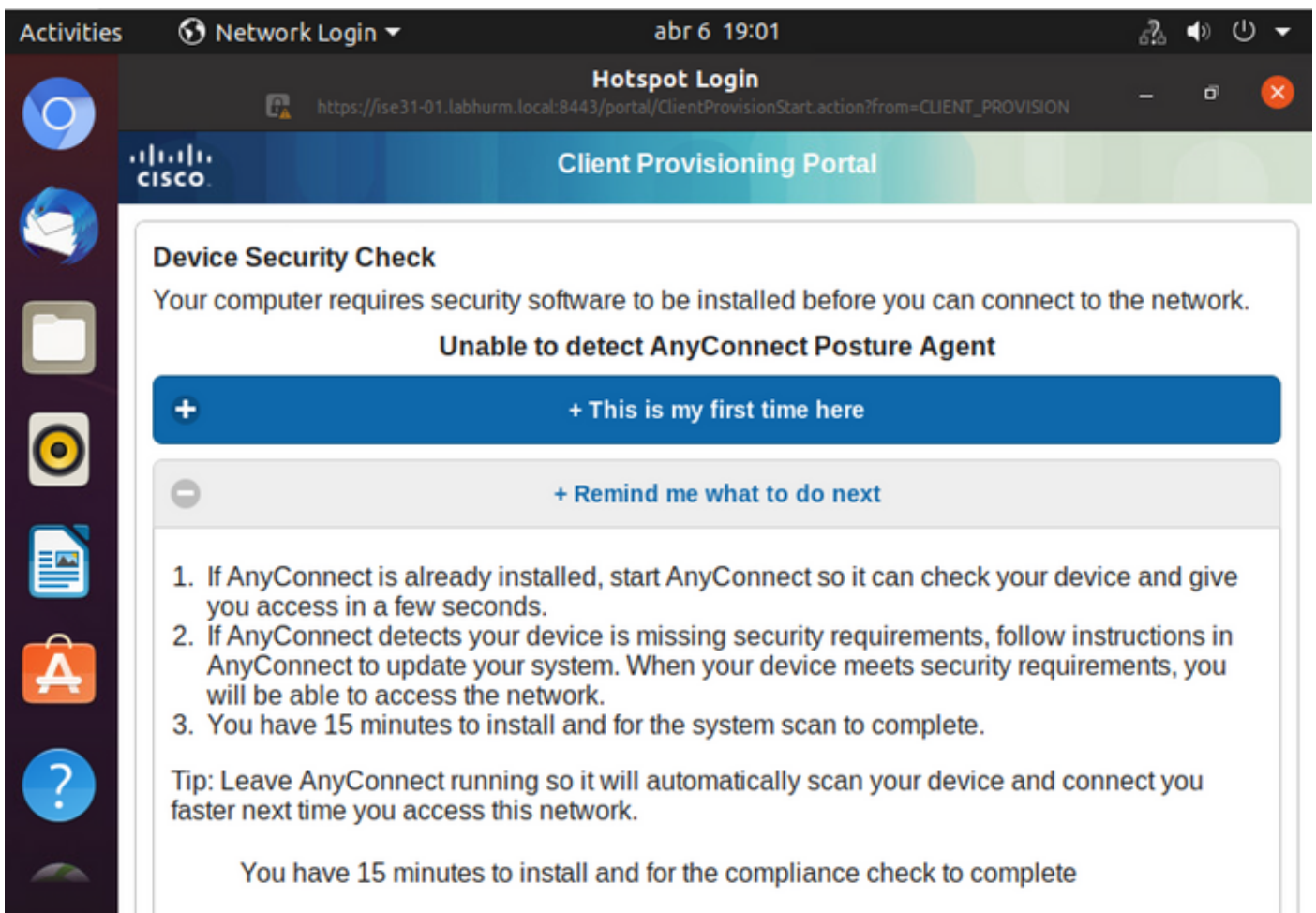
5단계. Linux 클라이언트에서 리디렉션이 발생해야 하며, 상태 검사가 발생했음을 나타내는 클라이언트 프로비저닝 포털을 표시하고 "시작"을 클릭합니다.



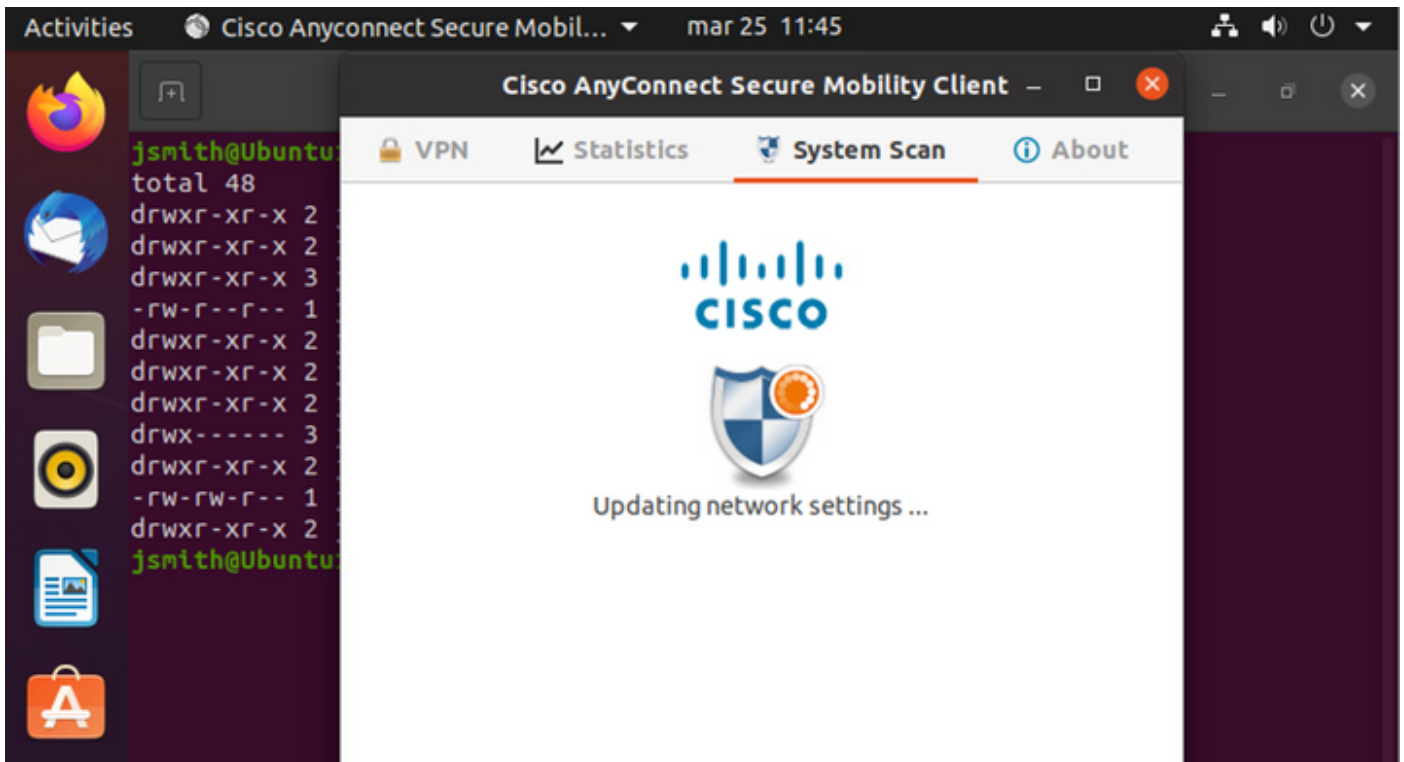
커넥터가 AnyConnect 탐지를 시도하는 동안 잠시 기다려 주십시오.



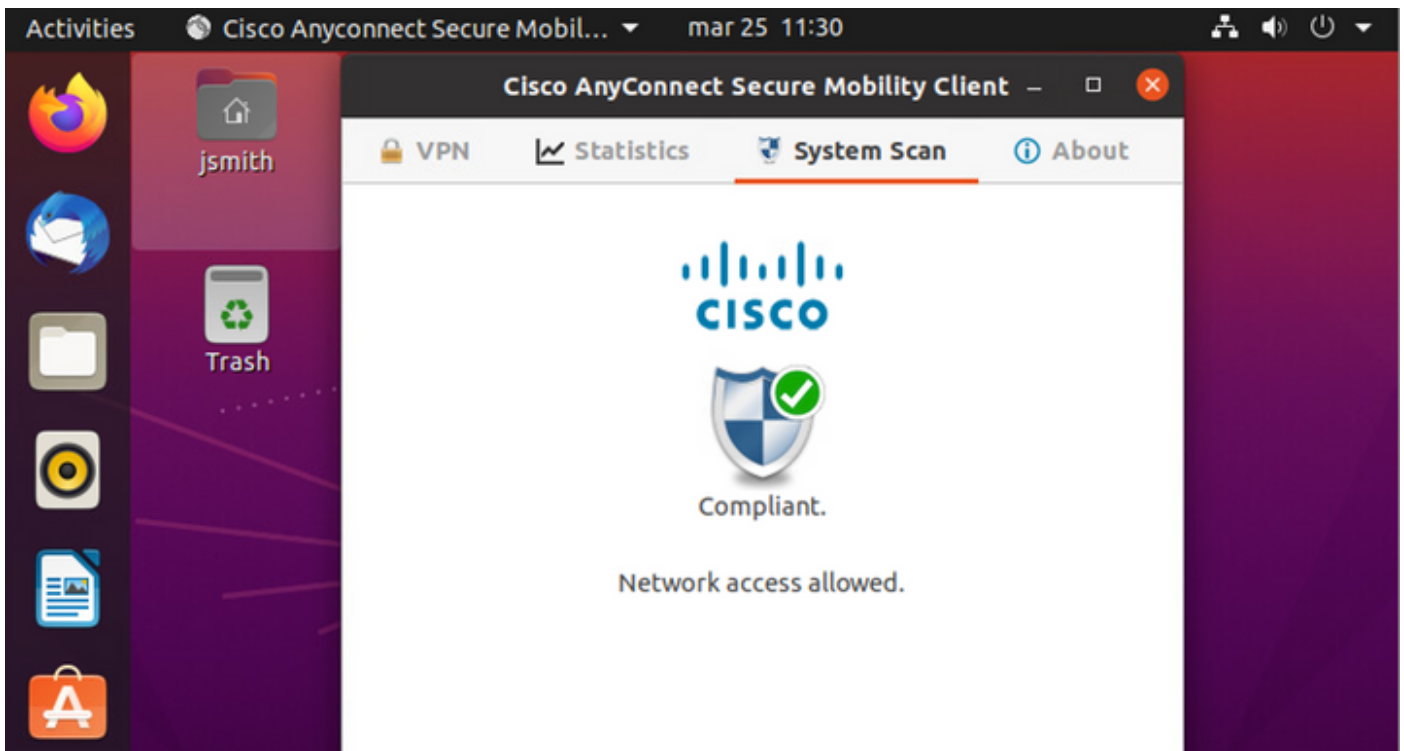
알려진 주의 사항으로 인해 AnyConnect가 설치되어 있더라도 이를 탐지하지 못합니다. AnyConnect 클라이언트로 전환하려면 Alt-Tab 또는 Activities 메뉴를 사용합니다.

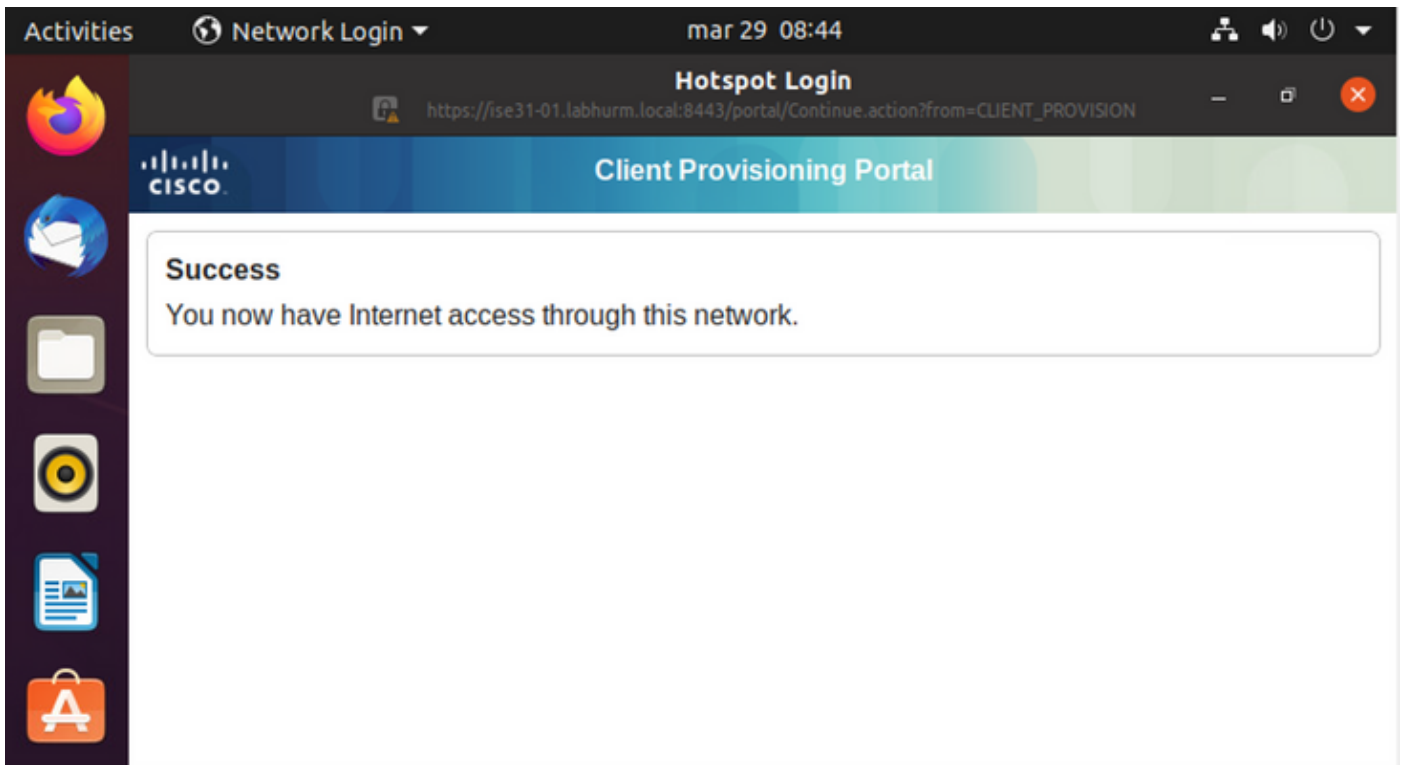


AnyConnect는 포스처 정책을 위해 PSN에 연결하고 엔드포인트를 평가합니다.



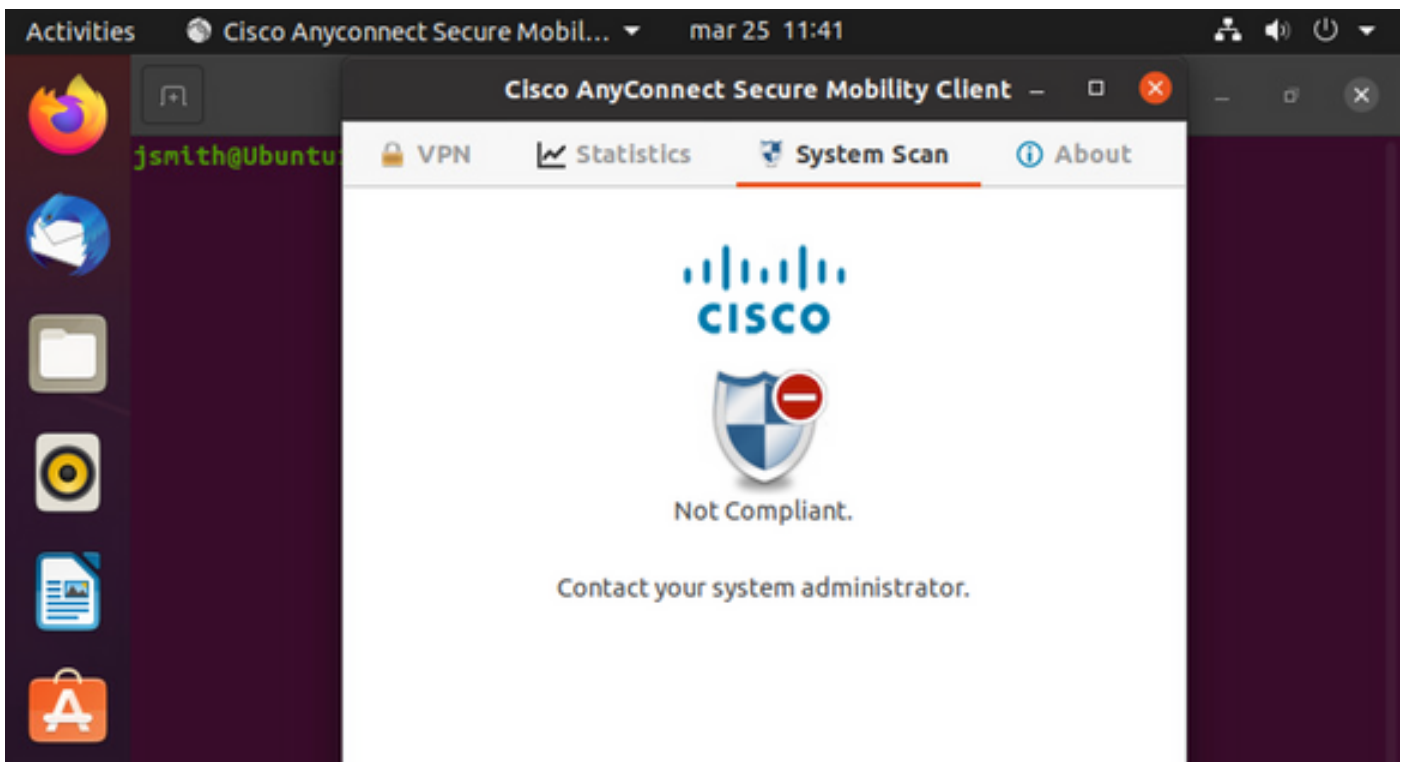
AnyConnect는 상태 정책 결정을 다시 ISE에 보고합니다. 이 경우 규정 준수





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

반면, 파일이 없으면 AnyConnect Posture 모듈은 ISE에 결정을 보고합니다



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	

참고: ISE FQDN은 DNS 또는 로컬 호스트 파일을 통해 Linux 시스템에서 확인할 수 있어야 합니다.

문제 해결

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

이동 위치:

```
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
```

권한 부여 성공:

```
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
```

규정 미준수, 격리 VLAN 및 ACL로 이동:

```
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
```