

LinuxでのCisco ISE 3.1ポスチャの設定

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[ISEでの設定](#)

[スイッチの設定](#)

[確認](#)

[トラブルシューティング](#)

概要

このドキュメントでは、LinuxおよびIdentity Services Engine(ISE)のファイルポスチャポリシーを設定および実装する手順について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- AnyConnect
- Identity Services Engine (ISE)
- Linux

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Anyconnect 4.10.05085
- ISEバージョン3.1 P1
- Linux Ubuntu 20.04
- CiscoスイッチCatalyst 3650。バージョン03.07.05.E(15.12(3)E5)

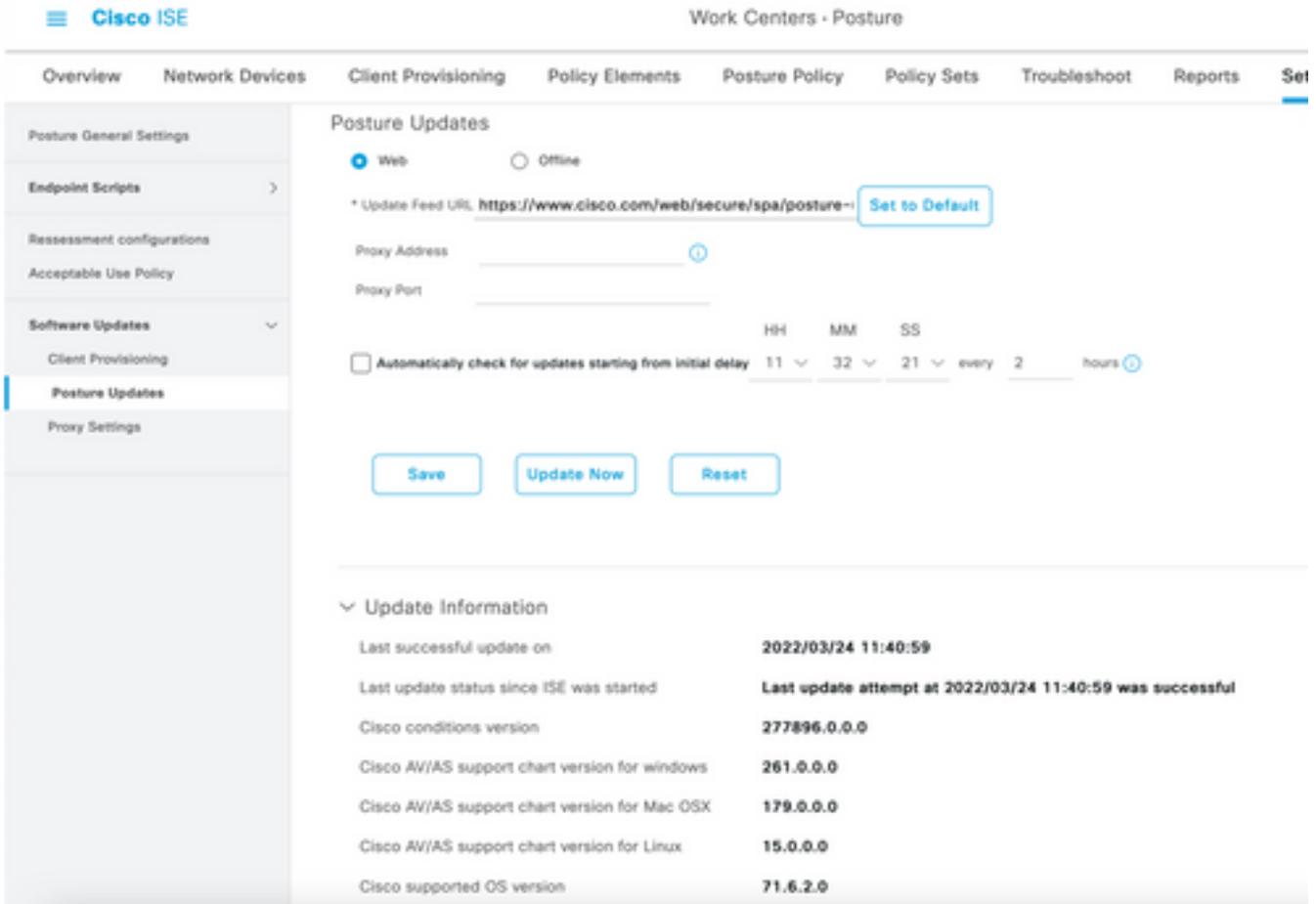
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

ISEでの設定

ステップ1: ポスチャサービスを更新します。

[Work Centers] > [Posture] > [Settings] > [Software Updates] > [Posture Updates]に移動します。
[今すぐ更新(Update now)]を選択し、プロセスが終了するまで待ちます。



The screenshot displays the Cisco ISE configuration interface for 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 configuration options:

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

Buttons: Save, Update Now, Reset

Update Information:

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

シスコが提供するパッケージは、Cisco.comサイトからダウンロードするソフトウェアパッケージ (AnyConnectソフトウェアパッケージなど) です。customer-created packageは、ISEユーザーインターフェイスの外部で作成し、ポスチャアセスメントで使用するためにISEにアップロードするプロファイルまたは設定です。この演習では、AnyConnect webdeployパッケージ「 anyconnect-linux64-4.10.05085-webdeploy-k9.pkg」をダウンロードできます。

注: アップデートやパッチにより、推奨バージョンが変更される可能性があります。
cisco.comサイトにある最新の推奨バージョンを使用します。

ステップ2: AnyConnectパッケージをアップロードします。

ポスチャワークセンターから、[Client Provisioning] > [Resources] に移動します。

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 |

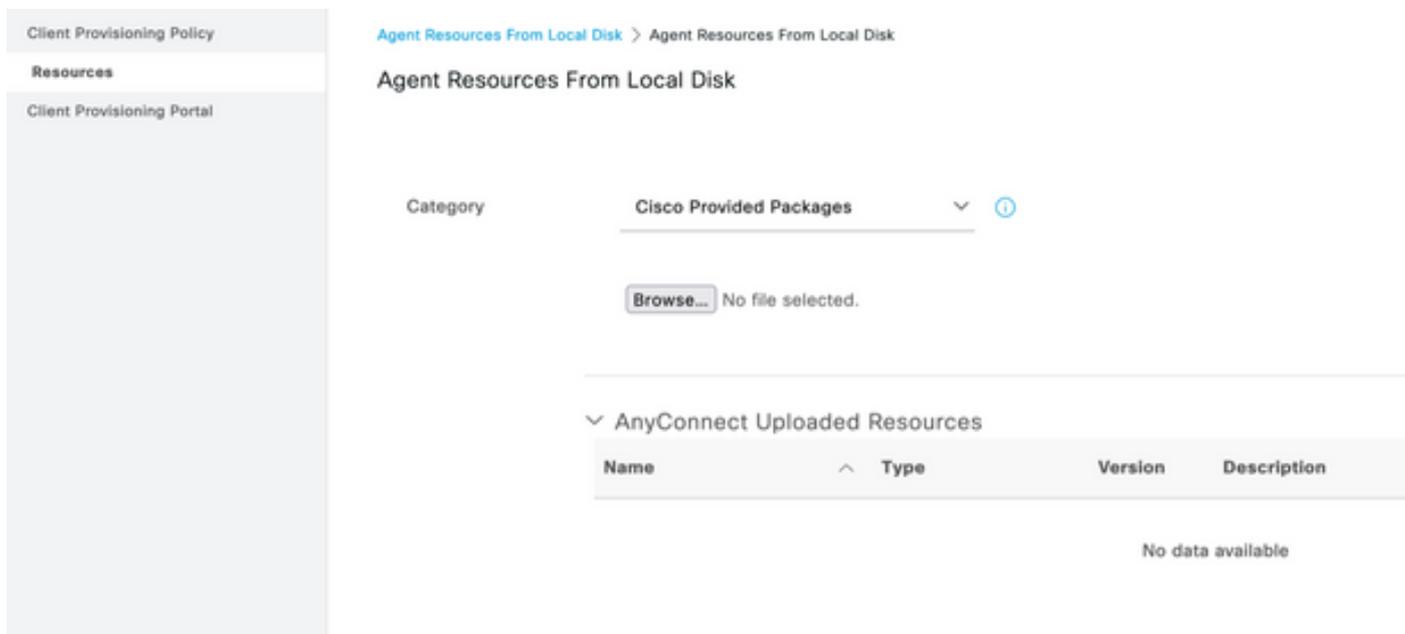
ステップ3:[Add] > [Agent Resources from Local Disk]を選択します。

Resources

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

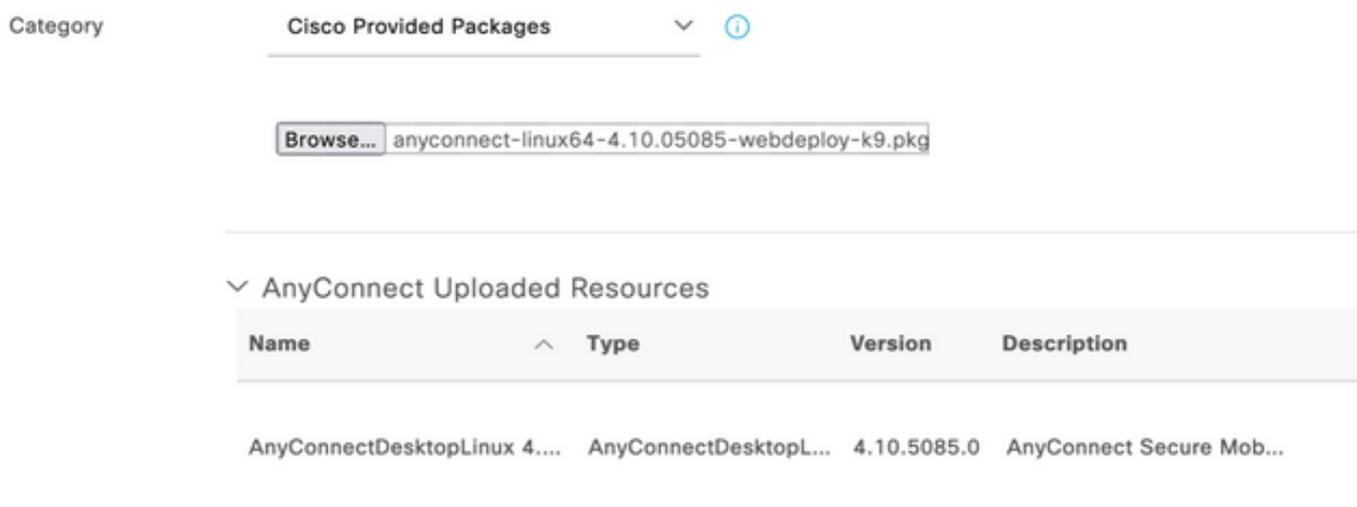
| | |
|--------------------------|---------------------------------|
| <input type="checkbox"/> | Agent resources from Cisco site |
| <input type="checkbox"/> | Agent resources from local disk |

ステップ4:[Category]ドロップダウンから[Cisco Provided Packages]を選択します。



ステップ 5 : [Browse] をクリックします。

ステップ6:前のステップでダウンロードしたAnyConnectパッケージのいずれかを選択します。AnyConnectイメージが処理され、パッケージに関する情報が表示されます



ステップ 7 : [Submit] をクリックします。AnyConnectがISEにアップロードされたので、ISEに連絡してCisco.comから他のクライアントリソースを取得できます。

注：エージェントリソースには、アンチウイルス、アンチスパイウェア、アンチマルウェア、ファイアウォール、ディスク暗号化、ファイルなどのさまざまな条件チェックについてエンドポイントのコンプライアンスを評価する機能を提供するAnyConnectクライアントで使用されるモジュールが含まれます。

ステップ8:[Add] > [Agent Resources from Cisco Site] をクリックします。ISEがCisco.comに到達し、クライアントプロビジョニング用に公開されたすべてのリソースのマニフェストを取得するため、ウィンドウにデータが入力されるまで1分かかります。

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 |

ステップ9:Linux用の最新のAnyConnectコンプライアンスモジュールを選択します。また、WindowsとMacのコンプライアンスモジュールを選択することもできます。

✕

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

ステップ10:WindowsおよびMac用の最新のテンポラルエージェントを選択します。

| | | |
|-------------------------------------|--------------------------------------|---|
| <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! |

ステップ11:[Save] をクリックします。

注：MACおよびWindowsポスチャの設定は、この設定ガイドの範囲外です。

この時点で、必要な部品をすべてアップロードして更新しています。次に、これらのコンポーネントを使用するために必要な設定とプロファイルを作成します。

ステップ12:[Add] > [NAC Agent]または[AnyConnect Posture Profile]をクリックします。

ISE Posture Agent Profile Settings > New Profile

AnyConnect Posture Profile

Name *
LinuxACPosture

Description:

Agent Behavior

| 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. |

変更する必要があるパラメータは次のとおりです。

- **VLAN検出間隔**:この設定では、VLANの変更をプローブする間にモジュールが待機する秒数を設定できます。推奨値は5秒です。
- **PingまたはARP**:これは実際のVLAN変更検出方法です。エージェントは、デフォルトゲートウェイにpingを実行するか、デフォルトゲートウェイのエントリのARPキャッシュを監視してタイムアウトまたは両方にすることができます。推奨される設定はARPです。
- **修復タイマー** : エンドポイントのポスチャが不明な場合、エンドポイントはポスチャアクセスメントフローを通過します。失敗したポスチャチェックの修復には時間がかかります。デフォルトでは、エンドポイントが非準拠としてマークされるまでの時間は4分ですが、値の範囲は1 ~ 300分 (5時間) です。推奨は15分です。ただし、修復に時間がかかる場合は、調整が必要になることがあります。

注 : Linuxファイルポスチャは自動修復をサポートしていません。

すべてのパラメータの包括的な説明については、ISEまたはAnyConnectポスチャドキュメントを参照してください。

ステップ13:[Agent Behavior] [Posture probes] [Backup List]を選択し、[Choose] を選択して [PSN/Standalone FQDN]を選択し、[Save] を選択します

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

ステップ14:[Posture Protocols] > [Discovery Host]で、PSN/スタンドアロンノードのIPアドレスを定義します。

ステップ15:[Discovery backup server] リストから[Select] を選択し、PSNまたはスタンドアロンFQDNを選択して[Select] を選択します。

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

ステップ16:[Server name rules] で*と入力してすべてのサーバに接続し、call homeリストでPSN/スタンドアロンIPアドレスを定義します。または、ネットワーク内のすべての潜在的なPSNを照合するためにワイルドカードを使用できます(*.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 |

ステップ17:[Add] > [AnyConnect Configuration] をクリックします。

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

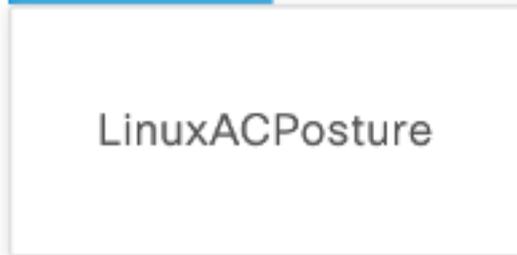
Profile Selection

* ISE Posture CPosture ▾

VPN

Network
Visibility

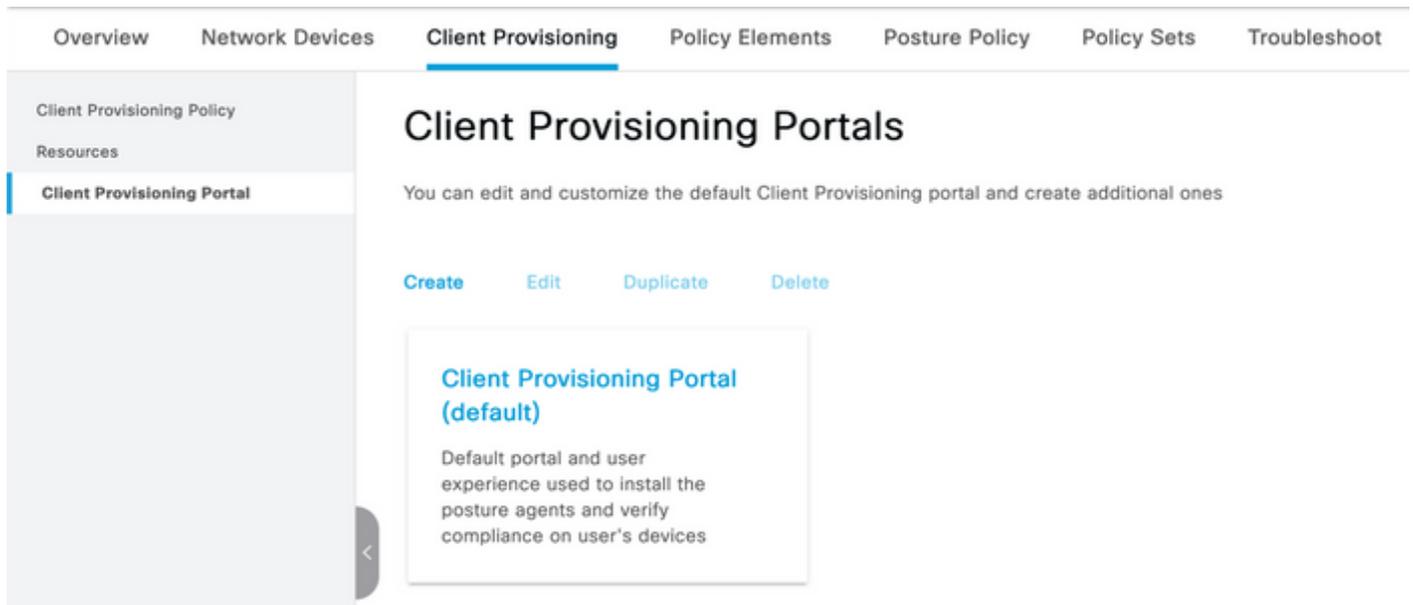
Customer
Feedback



下にスクロールして[Submit]を選択します

ステップ18:選択を終了したら、[Submit] をクリックします。

ステップ19:[Work Centers] > [Posture] > [Client Provisioning] > [Client Provisioning Portals] を選択します。



ステップ20:[Portal Settings] セクションで、インターフェイスとポートを選択し、ページ[Select Employee]、[SISE_Users]、および[Domain Users]に対して権限のあるグループを選択します。

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) | | |

ステップ21:[Log in Page Settings] で、[Enable auto Log In]オプションが有効になっていることを確認します

Login Page Settings

Enable Auto Login (i)

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

ステップ22:右上隅の[Save]を選択します

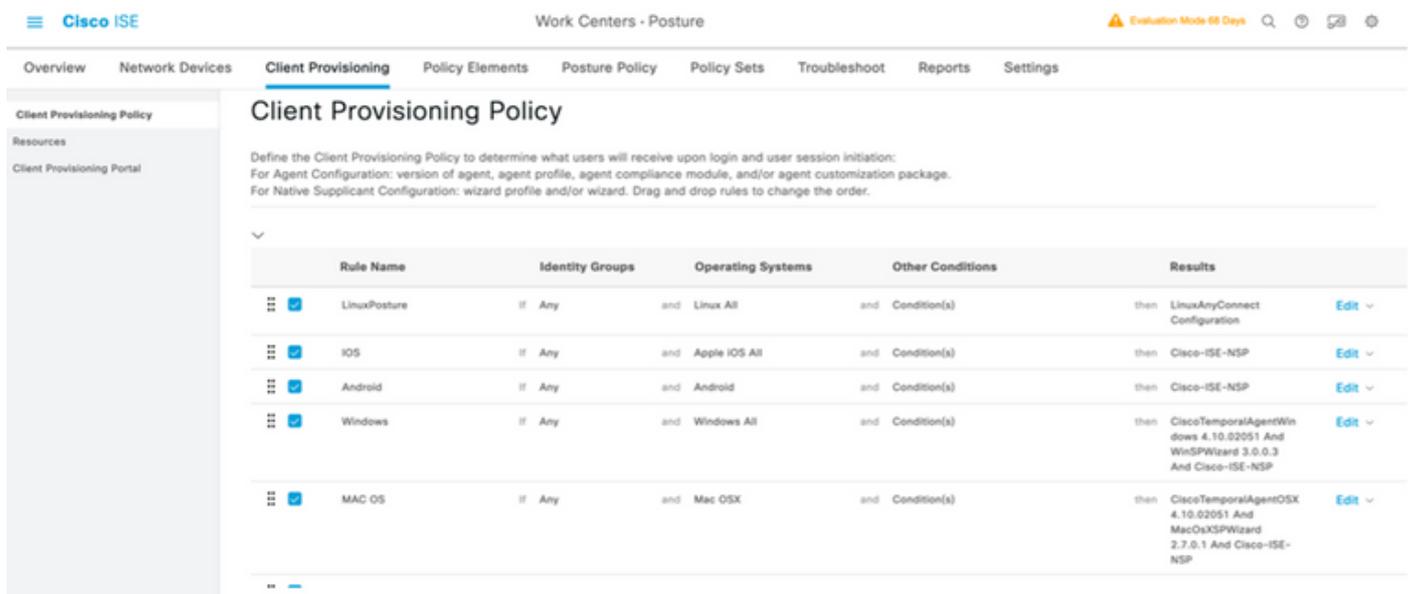
ステップ23:[Work Centers] > [Posture] > [Client Provisioning] > [Client Provisioning Policy] を選択します。

ステップ24:[CPP] のIOSルールのある下向き矢印をクリックし、[Duplicate Above] を選択します。

ステップ25:ルールにLinuxPostureという名前を付けます

ステップ26:[Results] で、エージェントとして[AnyConnect Configuration] を選択します。

注：この場合、AnyConnect設定の一部として設定されているため、コンプライアンスモジュールのドロップダウンは表示されません。



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 |

ステップ27:[Done] をクリックします。

ステップ28:[Save] をクリックします。

ポスチャ ポリシー要素

ステップ29:[Work Centers] > [Posture] > [Policy Elements] > [Conditions] > [File] を選択します。
[Add] を選択します。

ステップ30:ファイル条件名としてTESTFileを定義し、次の値を定義します

File Condition

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

注：パスはファイルの場所に基づきます。

ステップ31:[Save] を選択します。

FileExistence。このファイルタイプの条件は、想定されるシステムにファイルが存在するかどうかを確認します。これだけです。このオプションを選択すると、ファイルの日付やハッシュなどを検証する必要がなくなります

ステップ32:[Requirements] を選択し、次のように新しいポリシーを作成します。

| 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 |

注：Linuxでは、修復アクションとしてメッセージテキストのみをサポートしていません

要件コンポーネント

- ・オペレーティング システム：Linuxすべて
- ・コンプライアンス モジュール：4.(x)
- ・ポスタチャタイプ：AnyConnect
- ・条件：コンプライアンスモジュールとエージェント（OSを選択すると使用可能）
- ・修復アクション:他のすべての条件を選択した後に選択可能になる是正。

ステップ33:[Work Centers] > [Posture] > [Posture Policy] を選択します。

ステップ34：任意のポリシーで[Edit] を選択し、[Insert New policy]を選択します。名前として

LinuxPosturePolicy Policyを定義し、ステップ32で作成した要件を追加します。

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 LinuxFile | Edit |

ステップ35:[Done] を選択し、[Save] を選択します。

その他の重要なポスチャ設定([ポスチャ一般設定(Posture General Settings)]セクション)

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]セクションの重要な設定は次のとおりです。

- **修復タイマー**：この設定は、クライアントが失敗したポスチャ状態を修正する必要がある時間を定義します。AnyConnect設定には修復タイマーもあります。このタイマーはAnyConnectではなくISE用です。
- **デフォルトのポスチャステータス**：この設定は、ポスチャエージェントがないデバイス、またはLinuxベースのオペレーティングシステムなどのテンポラルエージェントを実行できないオペレーティングシステムのポスチャステータスを提供します。
- **継続的な監視の間隔**：この設定は、エンドポイントのインベントリを取得するアプリケーションとハードウェアの条件に適用されます。この設定は、AnyConnectがモニタリングデータを送信する頻度を指定します。
- **ステルスモードでのアクセプタブルユースポリシー**：この設定の選択肢は、ブロックまたは続

行の2つだけです。ブロックは、AUPが確認応答されない場合に、ステルスモードのAnyConnectクライアントが処理を続行するのを防ぎます。Continueを使用すると、AUPの確認応答がなくてもステルスモードクライアントを続行できます（これは、AnyConnectのステルスモード設定を使用する場合に意図されていることがよくあります）。

再評価の設定

ポスチャ再評価は、ポスチャワークフローの重要なコンポーネントです。「ポスチャプロトコル」セクションで、ポスチャ再評価のためのAnyConnectエージェントの設定方法を説明しました。エージェントは、その設定のタイマーに基づいて定義されたPSNで定期的にチェックインします。

要求がPSNに到達すると、PSNはそのエンドポイントのロールのISE設定に基づいて、ポスチャ再評価が必要かどうかを判断します。クライアントが再評価に合格すると、PSNはエンドポイントのポスチャ準拠状態を維持し、ポスチャリースがリセットされます。エンドポイントが再評価に失敗すると、ポスチャステータスは非準拠に変わり、存在していたポスチャリースが削除されます。

ステップ36:[Policy] > [Policy Elements] > [Results] > [Authorization] > [Authorization Profile] を選択します。[Add] を選択します

ステップ37:認可プロファイルとしてWired_Redirectを定義し、次のパラメータを設定します

▼ 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

ステップ38:[Save]を選択します

ステップ 39 : 認証ポリシーの設定

ポスチャには、事前設定された3つの認可ルールがあります。

1. 1つ目は、認証が成功したときに一致するように設定され、デバイスのコンプライアンスは不明です。
2. 2番目のルールは、非準拠のエンドポイントとの正常な認証に一致します。

注：最初の2つのルールは両方とも同じ結果になります。つまり、エンドポイントをクライアントプロビジョニングポータルにリダイレクトする事前設定された認可プロファイルを使用します。

3. 最後のルールは、正常な認証とポスチャ準拠のエンドポイントに一致し、事前に作成されたPermitAccess認可プロファイルを使用します。

Policy > Policy Setの順に選択し、前のラボで作成したWired 802.1x - MABの右矢印を選択します。

ステップ40:[Authorization Policy] を選択し、次のルールを作成します

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

スイッチの設定

注：次の設定はIBNS 1.0を示しています。IBNS 2.0対応スイッチには違いがある場合があります。これには、影響の少ないモードの導入が含まれます。

```

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
```

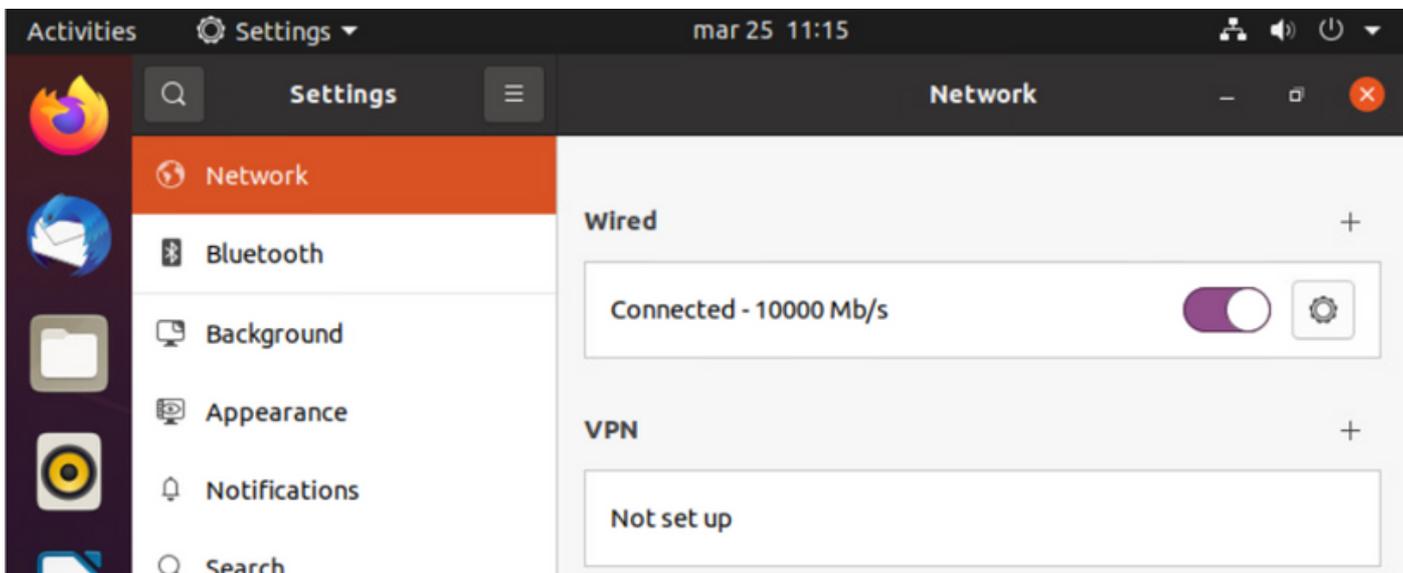
確認

ISEの検証：

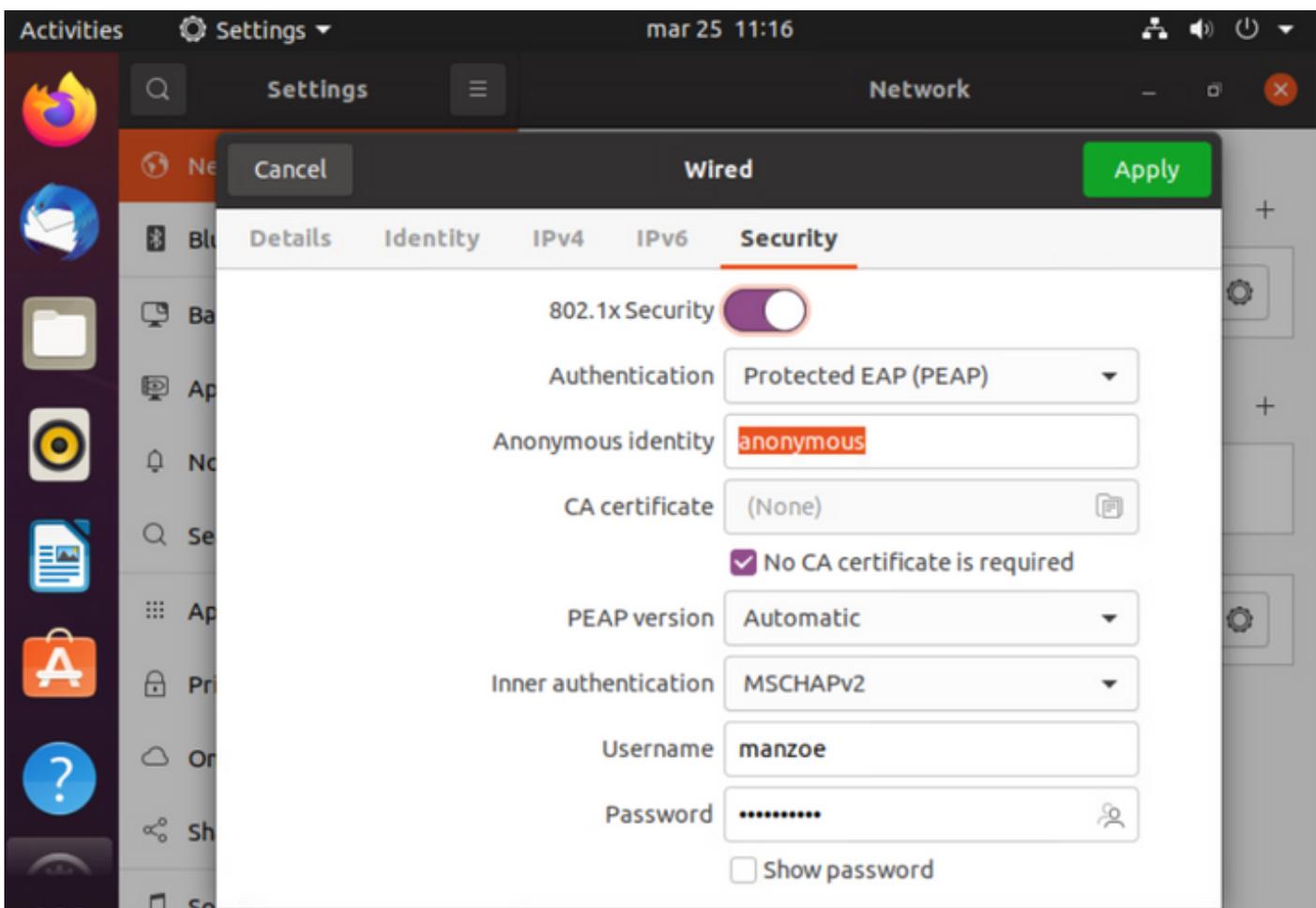
このセクションでは、ISEポスチャモジュールを使用するAnyConnectがLinuxシステムにすでにインストールされていることを前提としています。

dot1xを使用したPCの認証

ステップ1:[Network Settings]に移動します。



ステップ2:[Security]タブを選択し、802.1x設定とユーザクレデンシャルを入力します



ステップ3:[Apply]をクリックします。

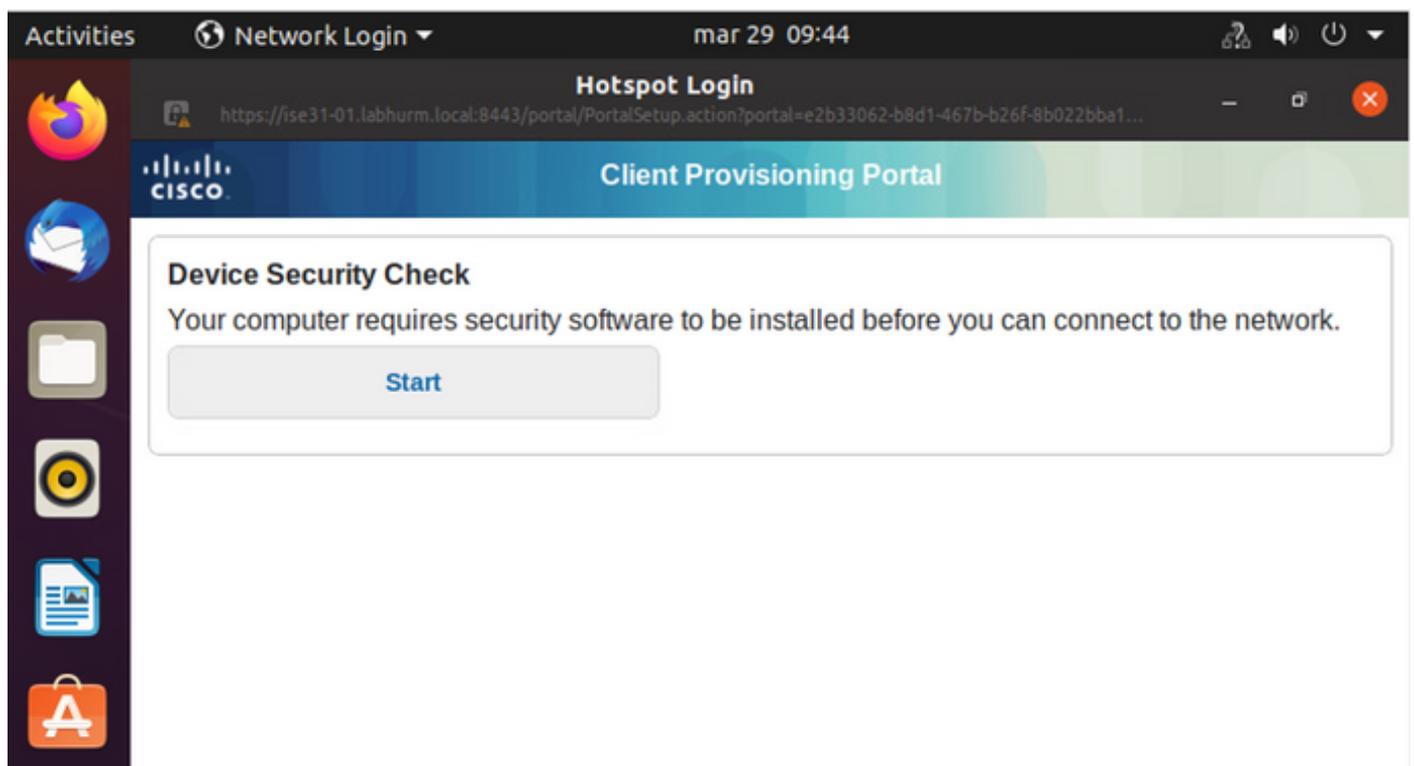
ステップ4:Linuxシステムを802.1x有線ネットワークに接続し、ISEライブログで検証します。

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

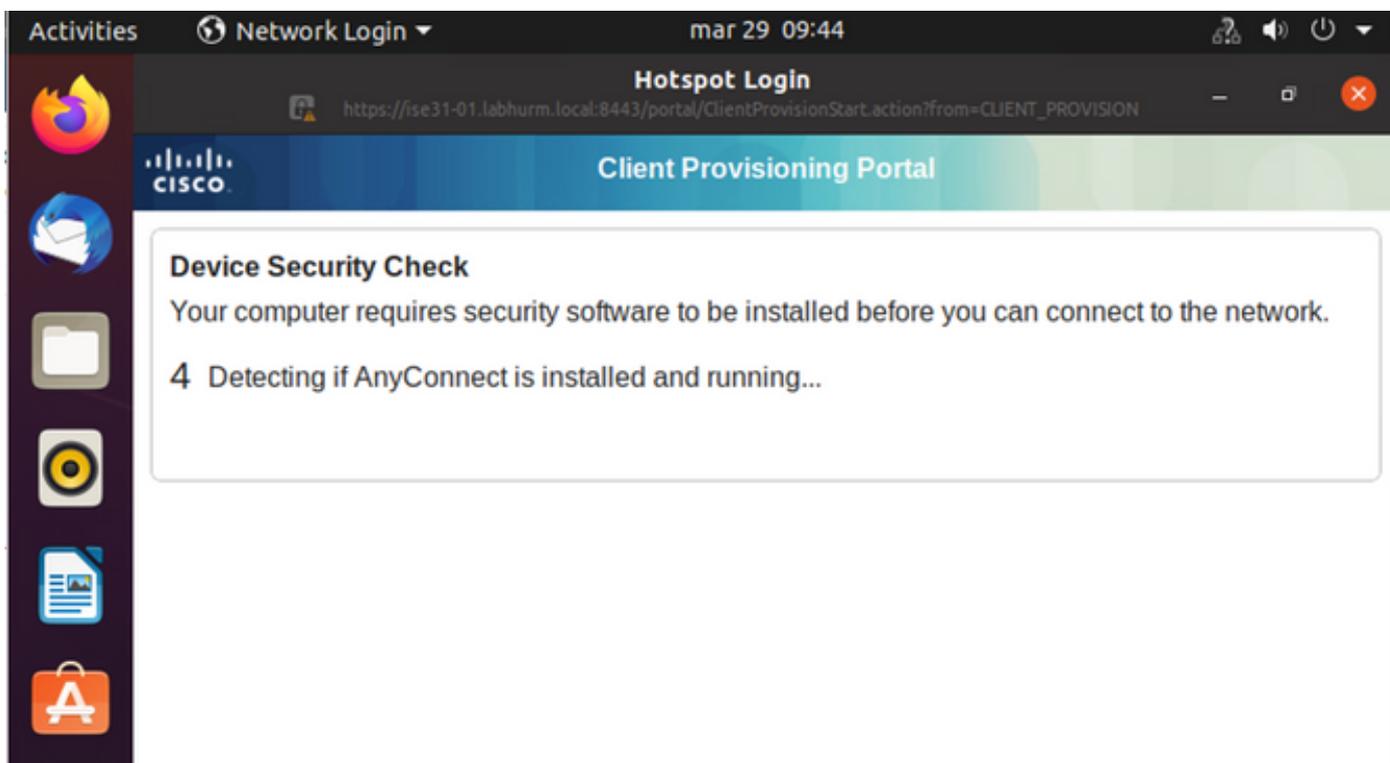
ISEでは、水平スクロールバーを使用して、フローを処理したPSNやポスチャステータスなどの追加情報を表示します。

| Authoriz... | Authoriz... | IP Address | Network De... | Device Port | Identity Group | Posture ... | Server |
|--------------|--------------|------------|---------------|------------------|----------------|-------------|----------|
| Authorizatic | Authorizatic | IP Address | Network Devi | 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 |

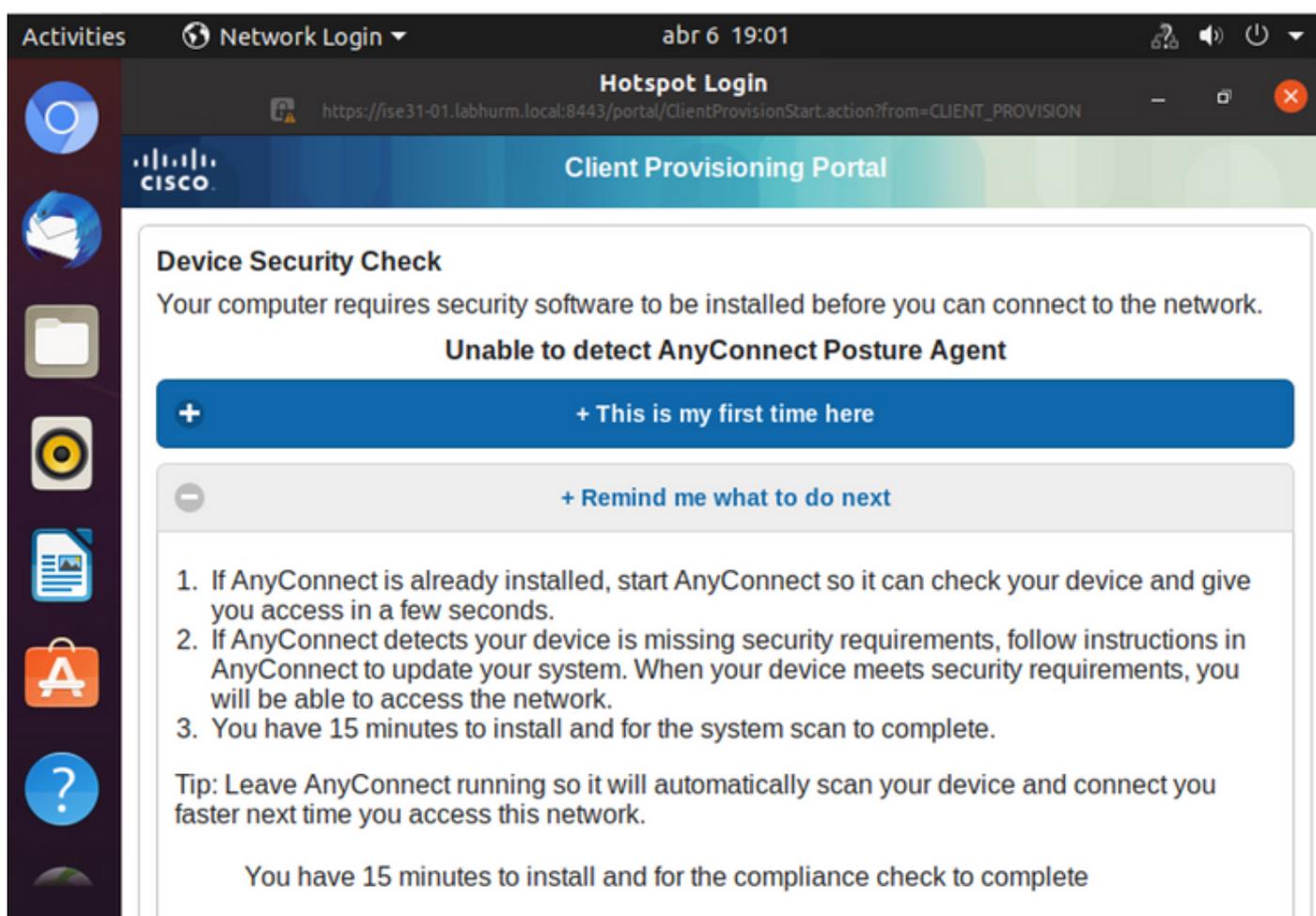
ステップ5:Linuxクライアントでリダイレクションを実行する必要があり、ポスチャチェックが発生したことを示すクライアントプロビジョニングポータルが表示され、[Start]をクリックします。



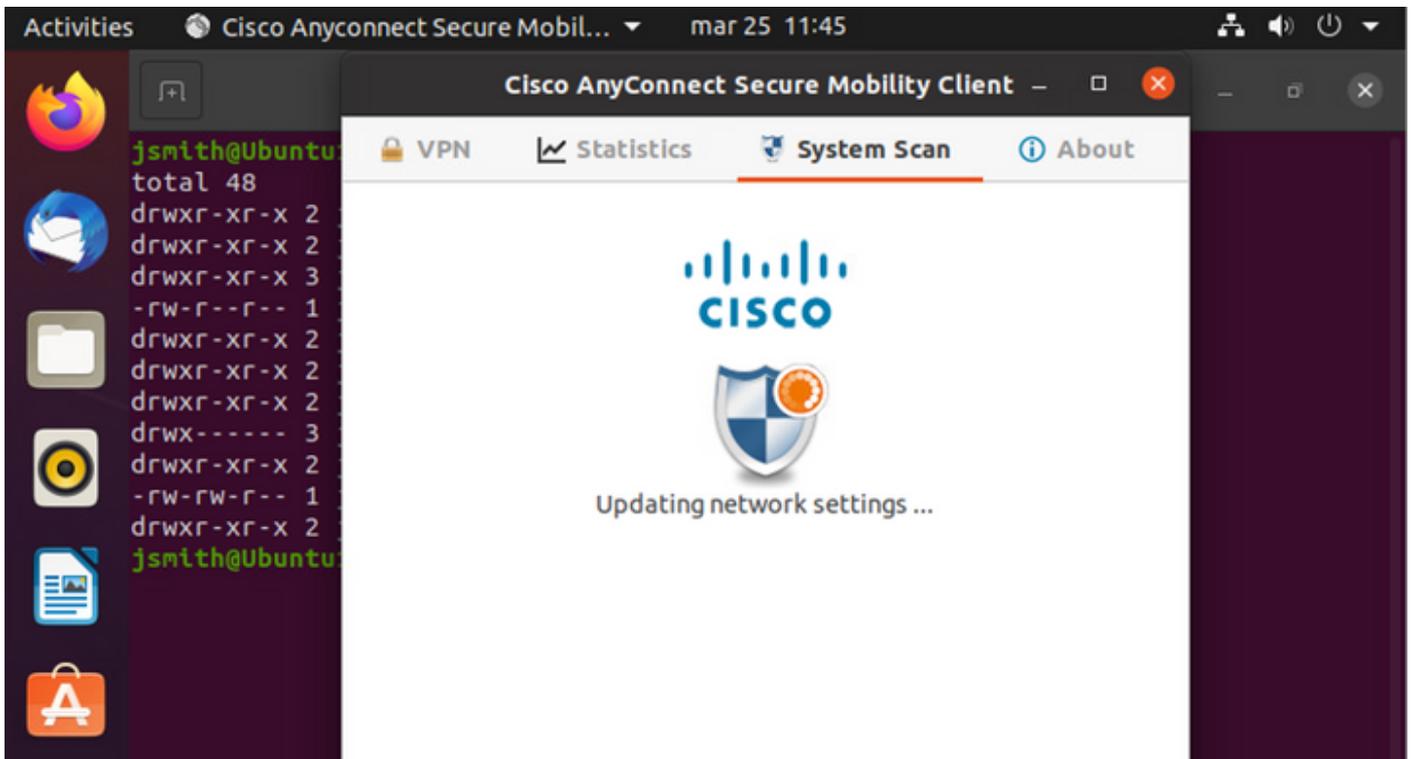
コネクタがAnyConnectの検出を試行する間、数秒待ちます。



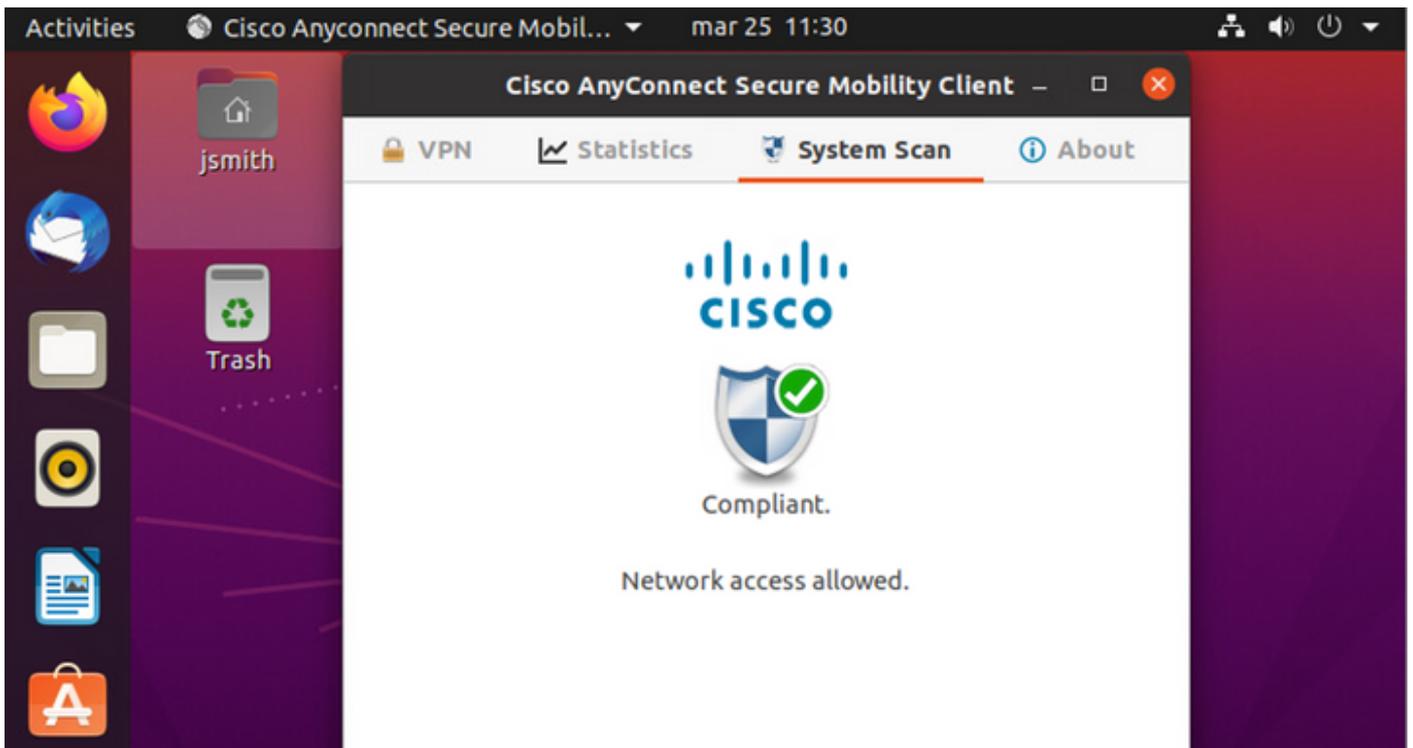
既知の警告により、AnyConnectがインストールされていても検出されません。AnyConnectクライアントに切り替えるには、Alt-Tabキーまたは[Activities]メニューを使用します。

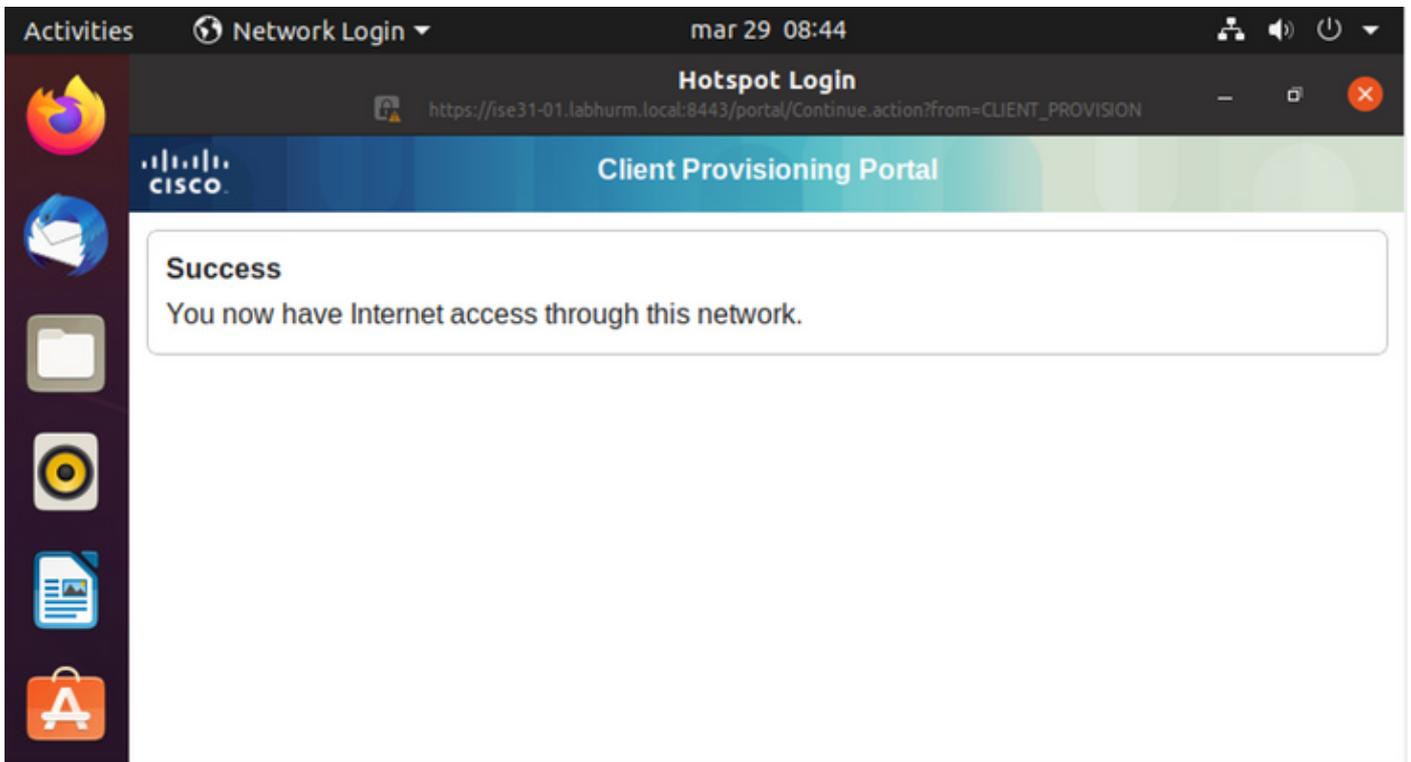


AnyConnectは、ポスチャポリシーのためにPSNに到達し、それに対してエンドポイントを評価しようとしています。



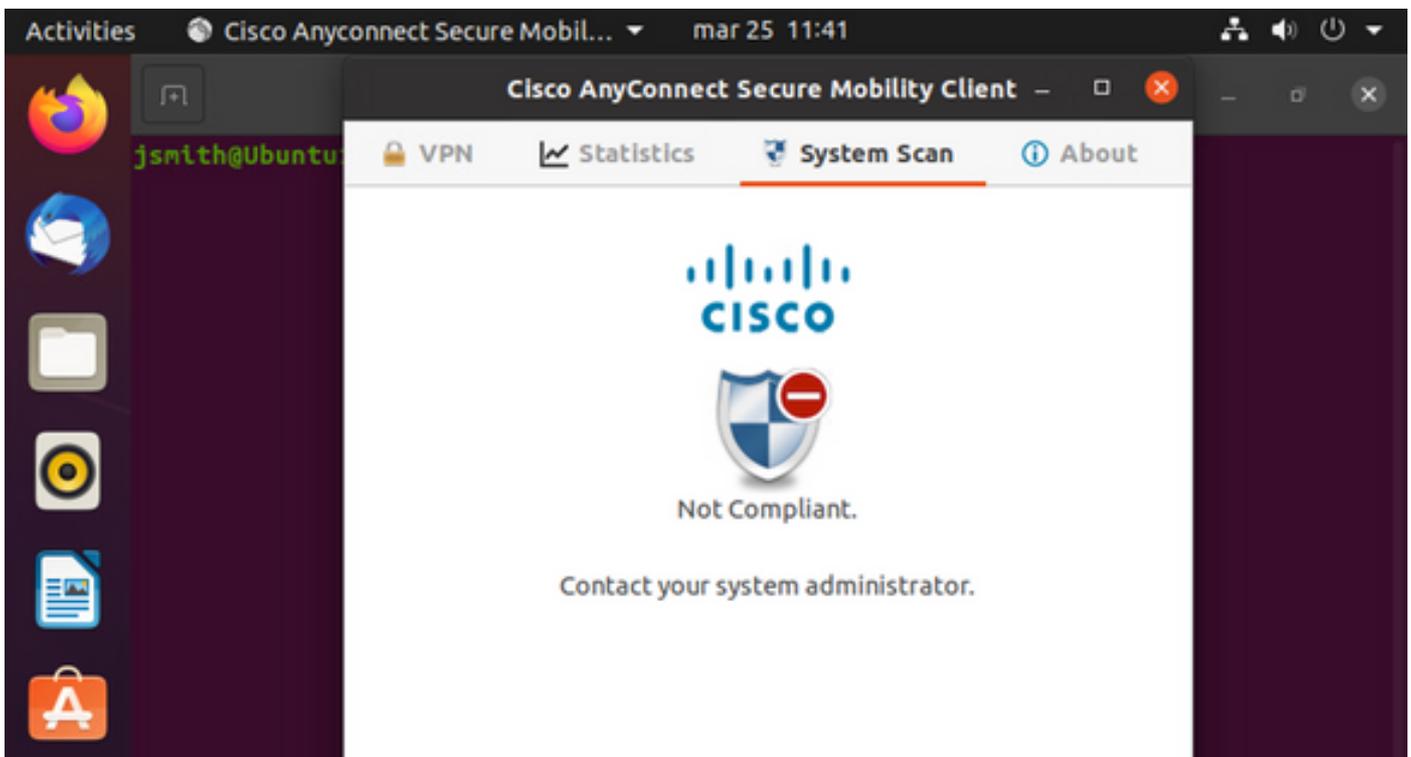
AnyConnectは、ポスチャポリシーの決定をISEに報告します。この場合、準拠





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

一方、ファイルが存在しない場合、AnyConnectポスチャモジュールは決定をISEに報告します



| 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 Devicr | 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 | |

注：ISE FQDNは、LinuxシステムでDNSまたはローカルホストファイルを介して解決できる必要があります。

トラブルシュート

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

リダイレクトする場所：

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

Runnable methods list:
  Method  State
  dot1x   Authc Success
```

Authorization succeeded:

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

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

非準拠、隔離VLANおよびACLに移動：

```
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
```