

使用Linux配置Cisco ISE 3.1终端安全评估

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[ISE上的配置](#)

[交换机上的配置](#)

[验证](#)

[故障排除](#)

简介

本文档介绍为Linux和身份服务引擎(ISE)配置和实施文件状态策略的过程。

先决条件

要求

Cisco 建议您了解以下主题：

- Anyconnect
- 身份服务引擎 (ISE)
- Linux

使用的组件

本文档中的信息基于以下软件和硬件版本：

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

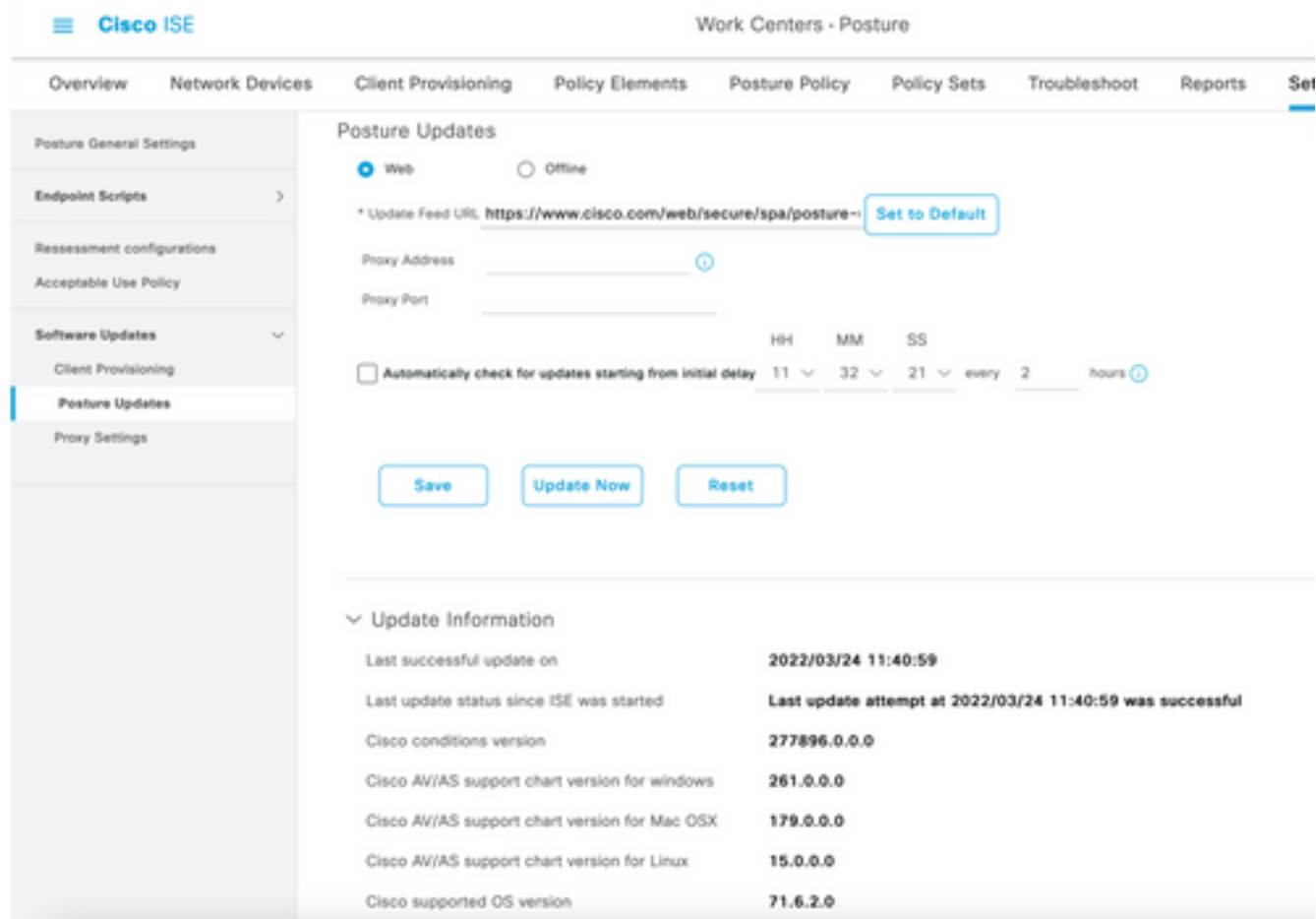
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

ISE上的配置

步骤1.更新状况服务：

导航至Work Centers > Posture > Settings > Software Updates > Posture Updates。选择Update now (立即更新) 并等待流程完成：



Cisco提供的软件包是您从Cisco.com站点下载的软件包，例如AnyConnect软件包。**客户创建的包**是您在ISE用户界面外创建的配置文件或配置，并且希望上传到ISE以便与状况评估配合使用。在本练习中，您可以下载AnyConnect webdeploy软件包“anyconnect-linux64-4.10.05085-webdeploy-k9.pkg”。

注意：由于有更新和补丁，建议的版本可能会更改。使用来自cisco.com站点的最新推荐版本。

步骤2.上传AnyConnect软件包：

在Posture Work中心内，导航至**Client Provisioning > Resources**

Cisco ISE Work Centers - Posture

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

Client Provisioning Policy
Resources
 Client Provisioning Portal

Resources

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

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

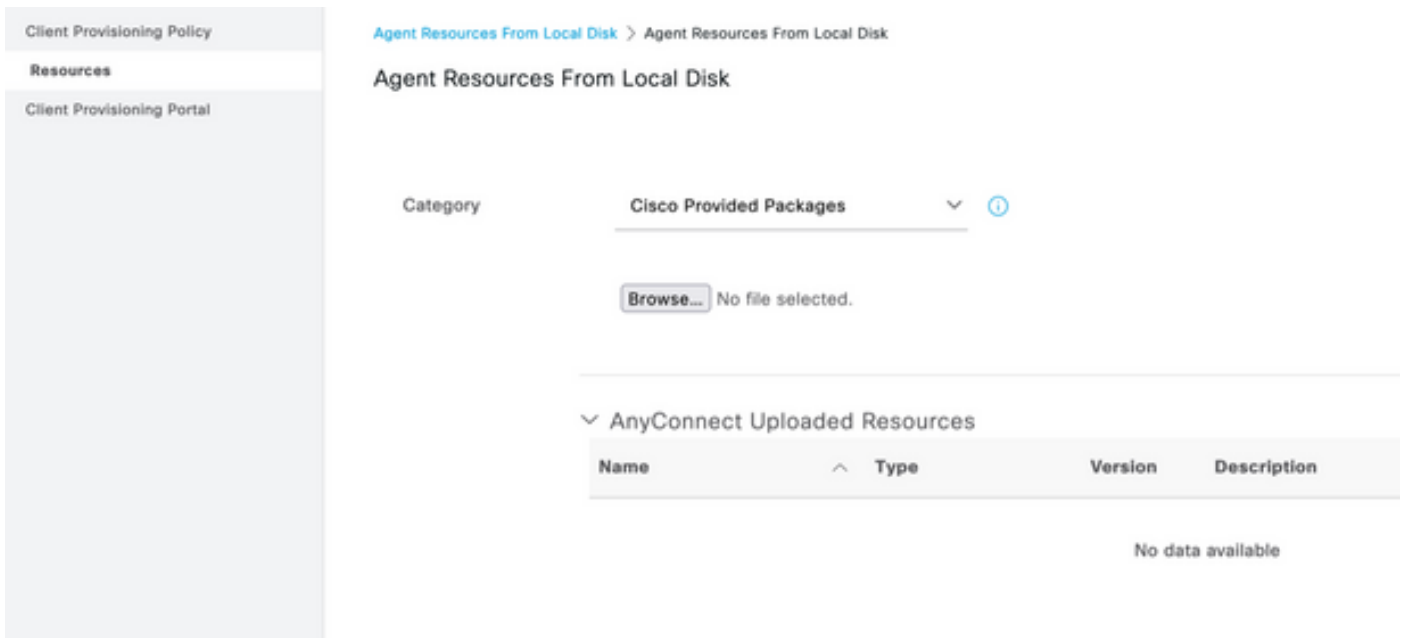
步骤3.选择Add > Agent Resources from Local Disk

Resources

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

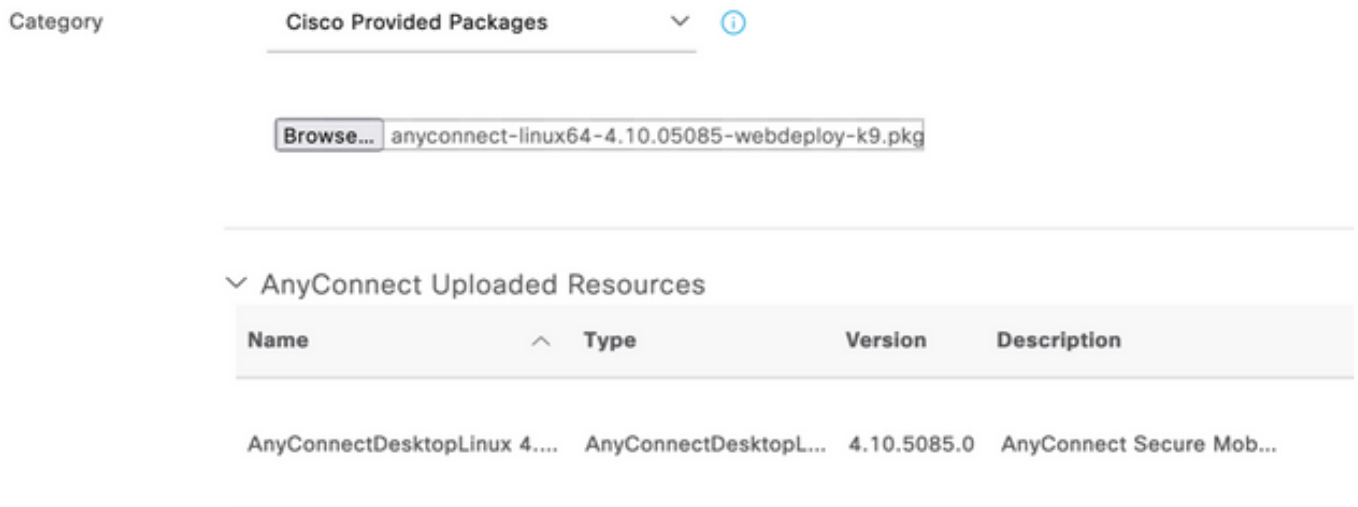
<input type="checkbox"/>	Agent resources from Cisco site
<input type="checkbox"/>	Agent resources from local disk

步骤4.从Category下拉列表中选择Cisco Provided Packages。



步骤5.单击浏览。

步骤6.选择您在上一步中下载的一个AnyConnect软件包。系统会处理AnyConnect映像，并显示有关软件包的信息



步骤7.单击提交。现在，AnyConnect已上传到ISE，您可以与ISE联系并从Cisco.com获取其他客户端资源。

注意：代理资源包括AnyConnect客户端使用的模块，该模块能够评估终端对各种状况检查（例如防病毒、防间谍软件、防恶意软件、防火墙、磁盘加密、文件等）的合规性。

步骤8.单击Add > Agent Resources from Cisco Site。当ISE访问Cisco.com并检索所有已发布资源的清单进行客户端调配时，该窗口需要一分钟时间进行填充。

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

步骤9.选择适用于Linux的最新AnyConnect合规性模块。此外，您还可以选择Windows和Mac的合规性模块。

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

步骤10.选择Windows和Mac的最新临时代理。

<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!

步骤11.单击保存。

注意：MAC和Windows终端安全评估配置不属于本配置指南的范围。

此时，您已上传并更新所有必需部件。现在应构建使用这些组件所需的配置和配置文件。

第12步： 点击添加> NAC代理或AnyConnect状态配置文件。

The screenshot shows the ISE Posture Agent Profile Settings interface. At the top, there are action buttons: Edit, Add, Duplicate, and Delete. Below is a table of profiles with columns for checkboxes, names, versions, last update times, and descriptions. The 'AnyConnect Posture Profile' is highlighted in the table. Below the table, the configuration for the 'AnyConnect Posture Profile' is shown, including a name field (LinuxACPosture), a description field, and a table of agent behavior parameters.

	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"/> CiscoTemporalAgent...	4.10.2051.0	2021/08/09 19:12:31	With CM: 4.3.1858.4353
<input type="checkbox"/> CiscoTemporalAgent...	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"/> CiscoAgentlessOSX	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	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.

需要修改的参数包括：

- **VLAN检测间隔:**通过此设置，可以设置模块在探测VLAN更改之间等待的秒数。建议时间为5秒

。

- **Ping或ARP**:这是实际的VLAN更改检测方法。代理可以ping默认网关或监控ARP缓存，使默认网关条目超时或同时超时。推荐的设置为ARP。

- **补救计时器**:当终端的状况未知时，终端将通过状况评估流程。修复失败的状况检查需要时间；默认时间是4分钟，之后才会将终端标记为不合规，但值的范围可以是1到300分钟（5小时）。建议为15分钟；但是，如果预计补救需要更长时间，则需要进行调整。

注意：Linux文件状态不支持自动补救。

有关所有参数的全面说明，请参阅ISE或AnyConnect终端安全评估文档。

第13步：Agent Behavior选择Posture probes Backup List并选择**Choose**，选择PSN/独立FQDN并选择**Save**

Choose PSNs

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

List of PSNs

ise30.ciscoise.lab ×



Cancel

Select

步骤14.在Posture Protocols > Discovery Host下定义PSN/独立节点ip地址。

步骤15.从Discovery备份服务器列表和选择中选择PSN或独立FQDN，然后选择**选择**。

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

步骤16.在Server name rules下，键入*联系所有服务器，并在call home list下定义PSN/Standalone IP address。或者，可以使用通配符匹配网络中的所有潜在PSN(即*.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

步骤17.点击Add > AnyConnect Configuration

Client Provisioning Policy

Resources

Client Provisioning Portal

Resources

 Edit  Add ^  Duplicate  Delete

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

* Select AnyConnect Package:

0.5085.0 ▾

*

Configuration
Name:


LinuxAnyConnect Configuration

AnyConnectDesktopWindows 4.10.5085.0
AnyConnectDesktopLinux 4.10.5085.0

Description:

Description Value Notes

* Compliance
Module

3.2028.0 

AnyConnectComplianceModuleLinux64 4.3.1676.0

AnyConnectComplianceModuleLinux64 4.3.2028.0

AnyConnect

AnyConnect Module Selection

ISE Posture

VPN

ASA Posture

Network
Visibility

Diagnostic
and Reporting
Tool

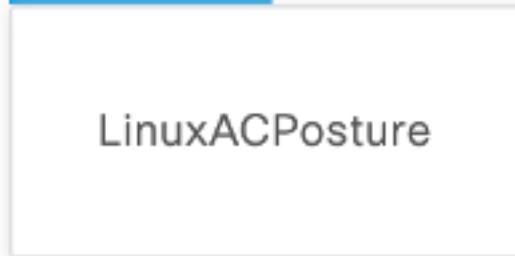
Profile Selection

* ISE Posture CPosture ▾

VPN

Network
Visibility

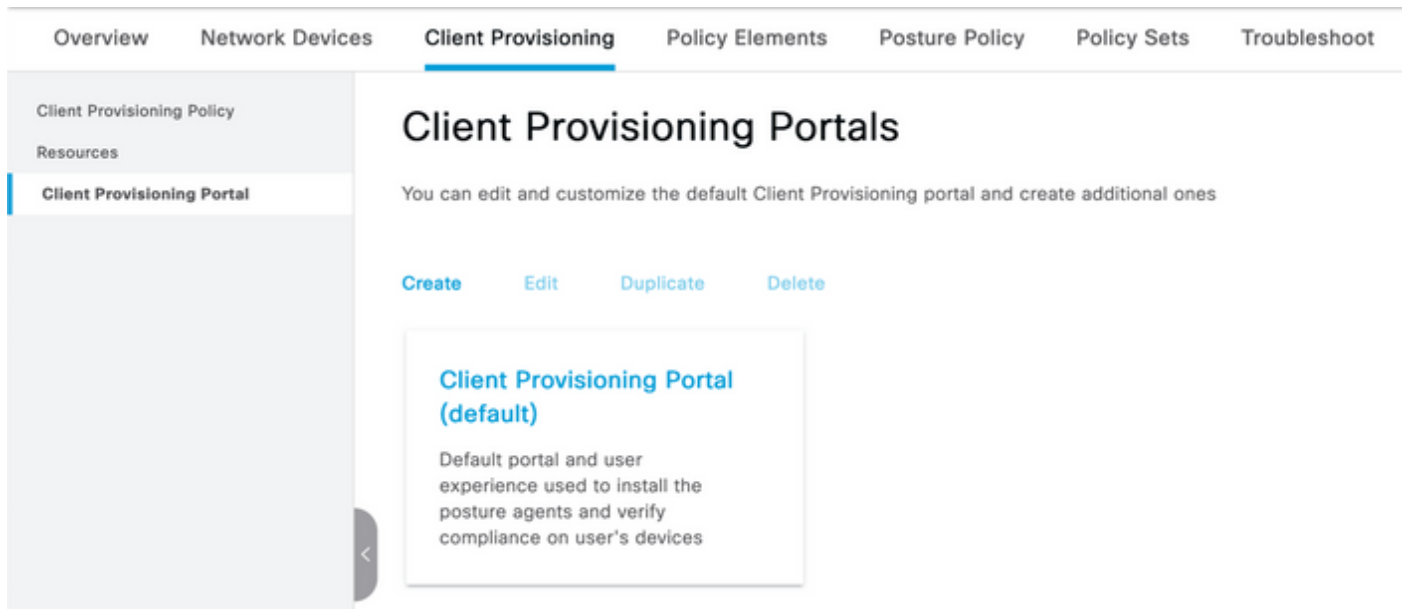
Customer
Feedback



向下滚动并选择“提交”

步骤18.完成选择后，点击提交。

步骤19.选择Work Centers > Posture > Client Provisioning > Client Provisioning Portals。



步骤20.在Portal Settings部分下，您可以在其中选择接口和端口，以及授权到Select Employee、SISE_Users和Domain Users页面的组。

Configure authorized groups

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

Available

Chosen

ALL_ACCOUNTS (default)

GROUP_ACCOUNTS (default)

OWN_ACCOUNTS (default)

Employee

Choose all

Clear all

步骤21.在Log in Page Settings下，确保启用Enable auto Log In选项

Login Page Settings

Enable Auto Login

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

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

Include an AUP as link

Require acceptance

Require scrolling to end of AUP

步骤22.在右上角选择Save

第23步：选择Work Centers > Posture > Client Provisioning > Client Provisioning Policy。

步骤24.单击CPP中IOS规则旁边的向下箭头，然后选择Duplicate Above

步骤25.将规则命名为LinuxPosture

步骤26.对于结果，选择AnyConnect Configuration作为代理。

注意：在这种情况下，您不会看到合规性模块下拉列表，因为它配置为AnyConnect配置的一部分。

The screenshot displays 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

步骤27.点击完成。

步骤28.单击保存。

状态策略元素

第29步：选择Work Centers > Posture > Policy Elements > Conditions > File。选择添加。

步骤30.将TESTFile定义为文件条件名称并定义下一个值

File Condition

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

Testfile.csv

注意：路径基于文件位置。

步骤31.选择保存

FileExistence。此文件类型的条件查看文件是否存在于其应该存在的系统中，仅此而已。选中此选项后，完全不需要验证文件日期、散列值等

步骤32.选择需求并创建新策略，如下所示：

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				

注意：Linux不支持仅作为补救操作的消息文本

需求组件

- 操作系统：Linux全部
- 合规性模块：4.x
- 状态类型：AnyConnect
- 条件:合规性模块和代理（在选择操作系统后可用）
- 补救措施：选择所有其他条件后可供选择的补救。

第33步：选择Work Centers > Posture > Posture Policy

第34步选择Edit on any policy，然后选择Insert New policy Define LinuxPosturePolicy Policy作为名称，并确保添加在步骤32中创建的需求。

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

步骤35.选择完成并保存

其他重要的终端安全评估设置（终端安全评估常规设置部分）

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部分的重要设置如下：

- **补救计时器**:此设置定义客户端更正故障状态条件的时间量。AnyConnect配置中还有补救计时器；此计时器用于ISE，而不是AnyConnect。
- **默认安全评估状态**：此设置提供没有状态代理的设备或无法运行临时代理的操作系统（例如基于Linux的操作系统）的状态状态。
- **连续监控间隔**:此设置适用于清点终端的应用和硬件条件。该设置指定AnyConnect必须发送监控数据的频率。
- **隐藏模式中的可接受使用策略**:此设置的唯一两个选项是阻止或继续。如果未确认AUP，则阻止隐藏模式AnyConnect客户端继续进行。“继续”允许即使不确认AUP（使用AnyConnect的隐身模式设置时，AUP通常是此意图）也能继续隐身模式客户端。

重新评估配置

状况重新评估是状况工作流程的关键组成部分。您在“Posture Protocol”部分看到如何配置

AnyConnect代理进行状态重新评估。代理定期签入基于该配置中的计时器定义的PSN。

当请求到达PSN时，PSN会根据该终端角色的ISE配置确定是否需要状态重新评估。如果客户端通过重新评估，PSN将保持终端的安全状态合规状态，并且安全状态租期将重置。如果终端未通过重新评估，安全评估状态将更改为不合规状态，并且已存在的任何安全评估租期将被删除。

第36步选择Policy > Policy Elements > Results > Authorization > Authorization Profile。选择**添加**

步骤37.将Wired_Redirect定义为授权配置文件并配置下一个参数

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

步骤38.选择保存

步骤39.配置授权策略

安全评估有三个预配置的授权规则：

1. 第一个配置为在身份验证成功时匹配，设备的合规性未知。
2. 第二条 规则将成功的身份验证与不合规的终端相匹配。

注意：前两个规则的结果相同，即使用预配置的授权配置文件，将终端重定向到客户端调配门户。

3. 最终规则匹配成功的身份验证和状态兼容终端，并使用预构建的PermitAccess授权配置文件。选择Policy > Policy Set，并为前一实验中的Wired 802.1x - MAB选择右箭头。

步骤40.选择Authorization Policy并创建下一个规则

<input checked="" type="checkbox"/> SISE_UnknownCompliance_Redirect	AND	<input type="checkbox"/> Network_Access_Authentication_Passed <input type="checkbox"/> Compliance_Unknown_Devices <input type="checkbox"/> ISEAD ExternalGroups EQUALS ciscoise.lab/Users/Domain Users	<input type="text" value="PostureISE"/> +	Select from list ▼ +	9	⚙
<input checked="" type="checkbox"/> SISE_NonCompliance_Redirect	AND	<input type="checkbox"/> Non_Compliant_Devices <input type="checkbox"/> Network_Access_Authentication_Passed <input type="checkbox"/> ISEAD ExternalGroups EQUALS ciscoise.lab/Users/Domain Users	<input type="text" value="PostureISE"/> +	Select from list ▼ +	0	⚙
<input checked="" type="checkbox"/> SISE_Compliance_Device_Access	AND	<input type="checkbox"/> Compliant_Devices <input type="checkbox"/> Network_Access_Authentication_Passed <input type="checkbox"/> ISEAD ExternalGroups EQUALS ciscoise.lab/Users/Domain Users	<input type="text" value="NewAP"/> +	Select from list ▼ +	2	⚙

交换机上的配置

注意：以下配置是指IBNS 1.0。支持IBNS 2.0的交换机可能存在差异。它包括低影响模式部署。

```
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
```

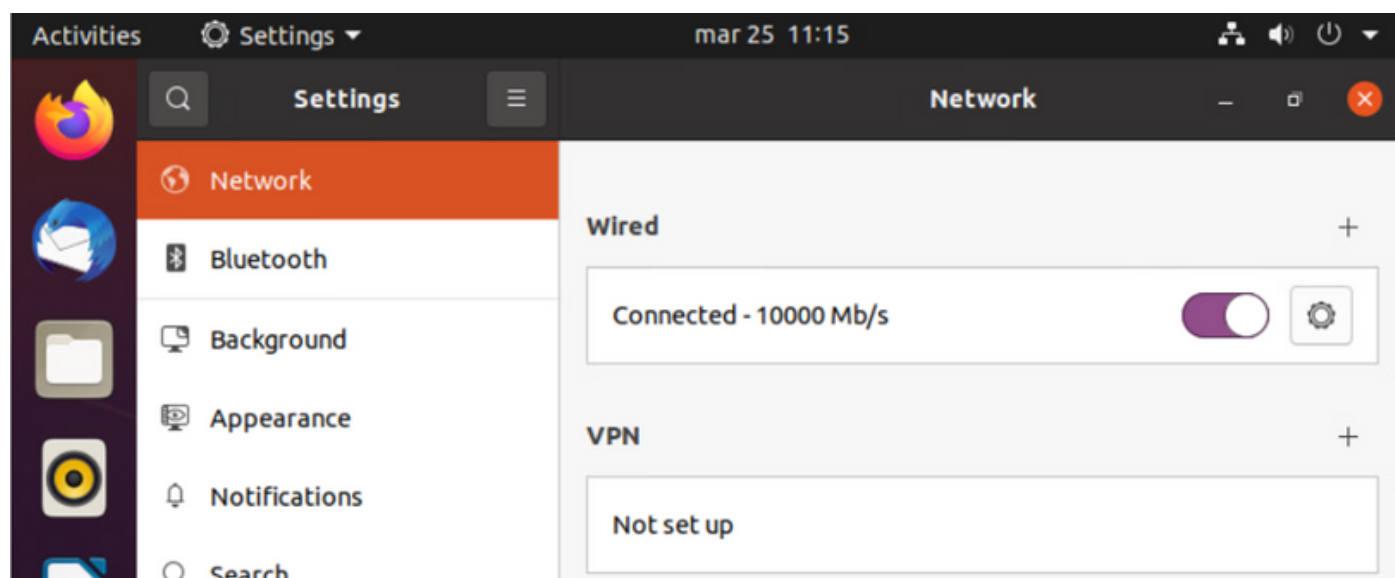
验证

ISE验证：

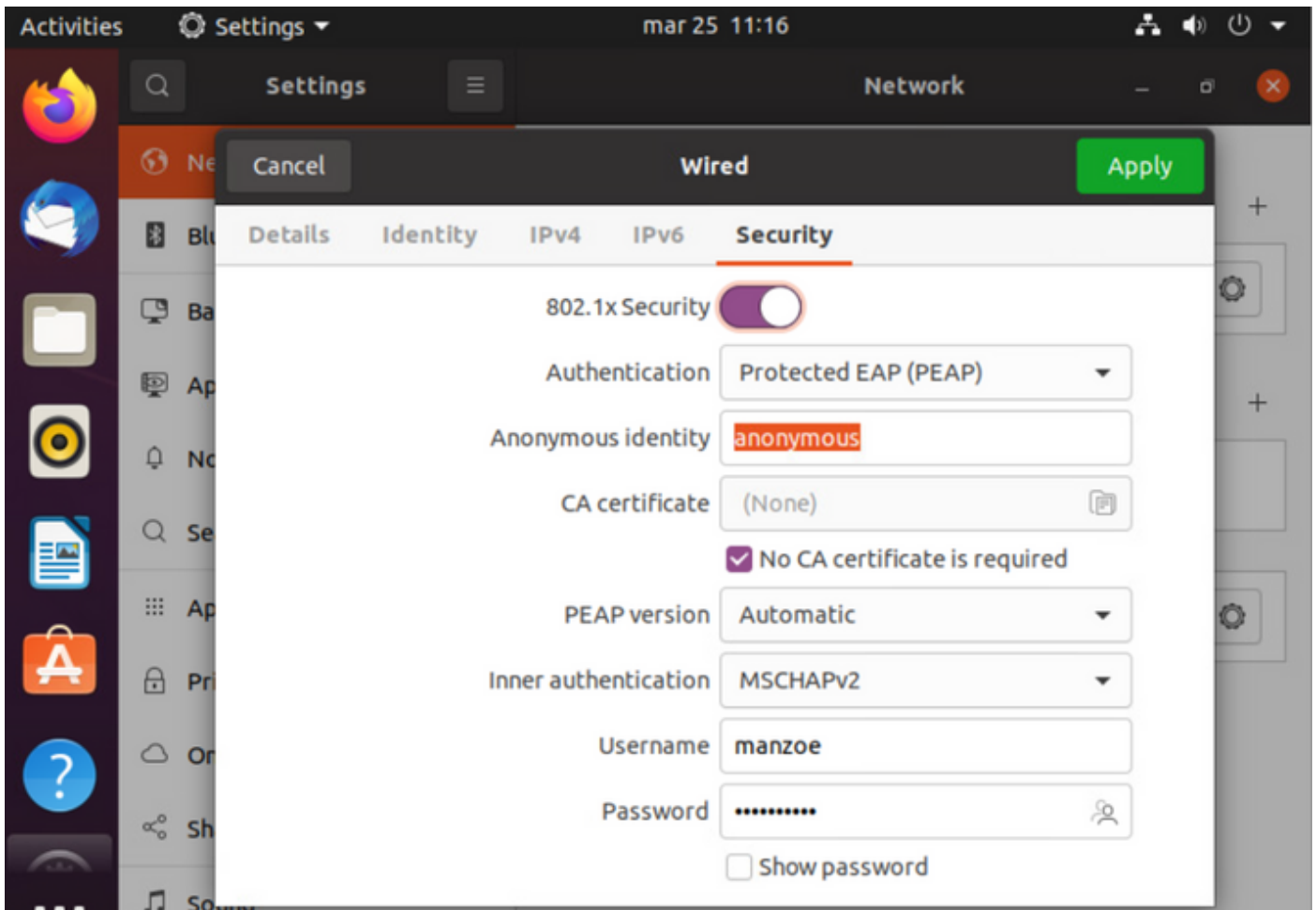
本节假设之前已在Linux系统上安装了带有ISE终端安全评估模块的AnyConnect。

使用dot1x验证PC

步骤1.导航到网络设置



步骤2.选择Security选项卡并提供802.1x配置和用户凭证



步骤3.单击“应用”。

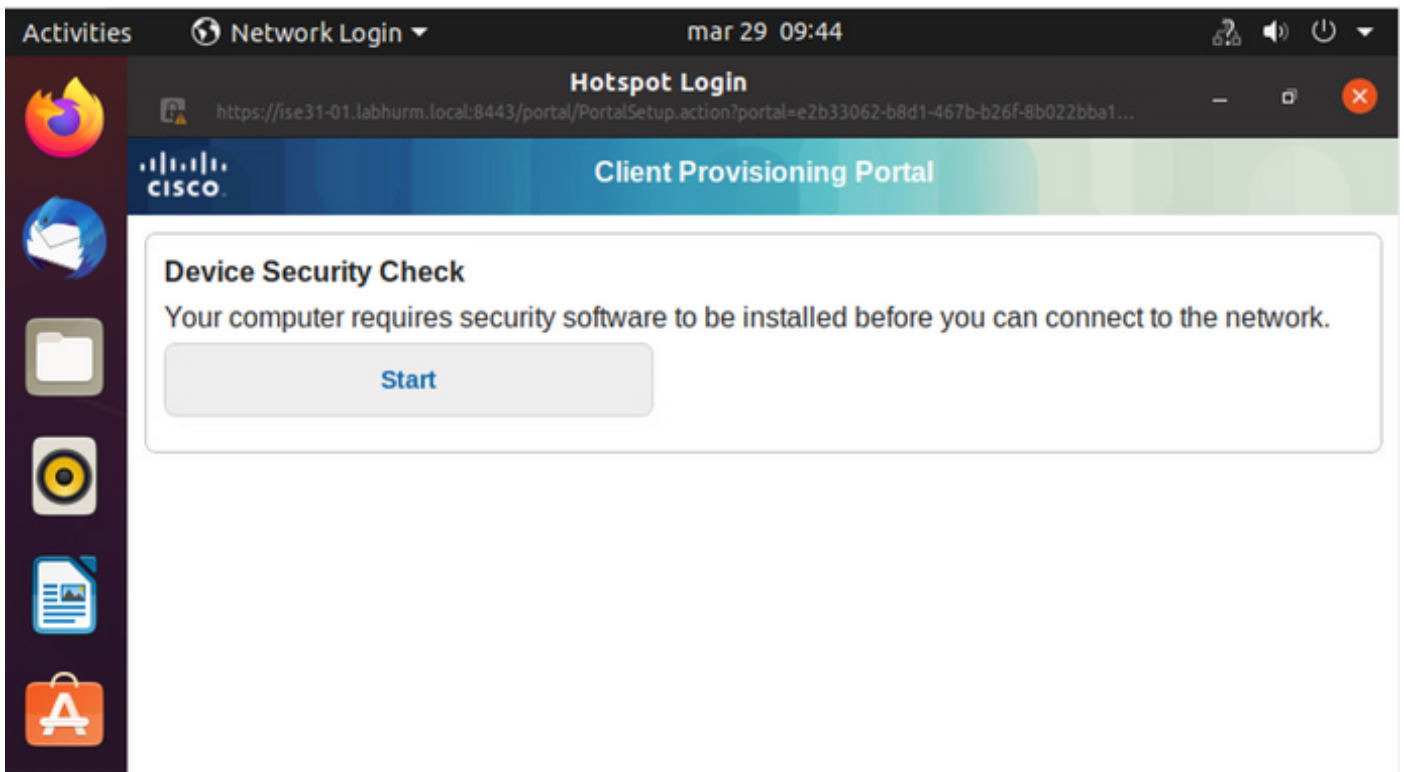
第4步：将Linux系统连接到802.1x有线网络，并在ISE实时日志中验证：

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...	●	🔒	0	manzoe	00:0C:29:45:03:8F	Ubuntu-W...	Ubuntu Po...	Ubuntu Po...	Wired_Re...			FastEthernet1...		Pending
Apr 06, 2022 08:32:48.2...	●	🔒		manzoe	00:0C:29:45:03:8F	Ubuntu-W...	Ubuntu Po...	Ubuntu Po...	Wired_Re...		Cat-3750	FastEthernet1...	Workstation	Pending
Apr 06, 2022 08:32:40.8...	●	🔒		manzoe	00:0C:29:45:03:8F	Ubuntu-W...	Ubuntu Po...	Ubuntu Po...	Wired_Re...		Cat-3750	FastEthernet1...	Workstation	Pending

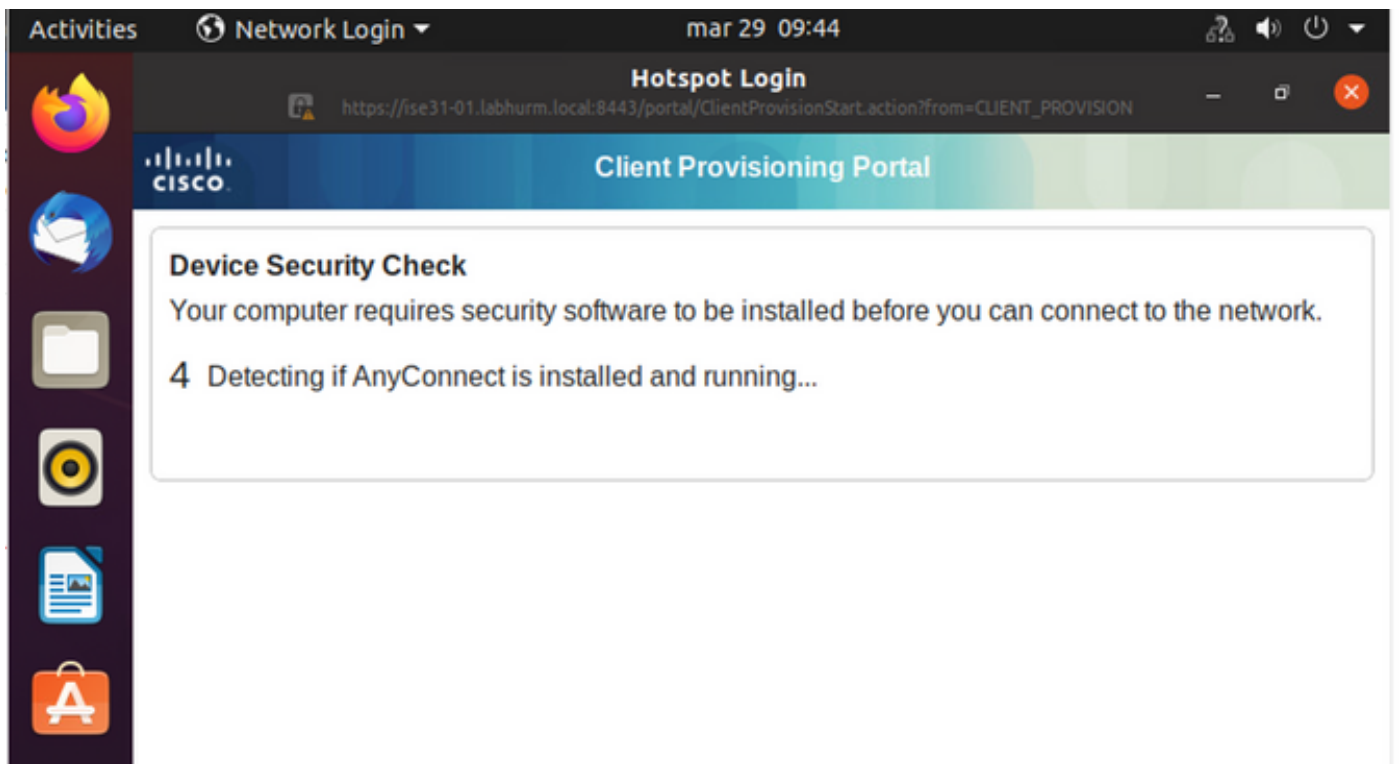
在ISE中，使用水平滚动条查看其他信息，例如服务流的PSN或终端安全评估状态：

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

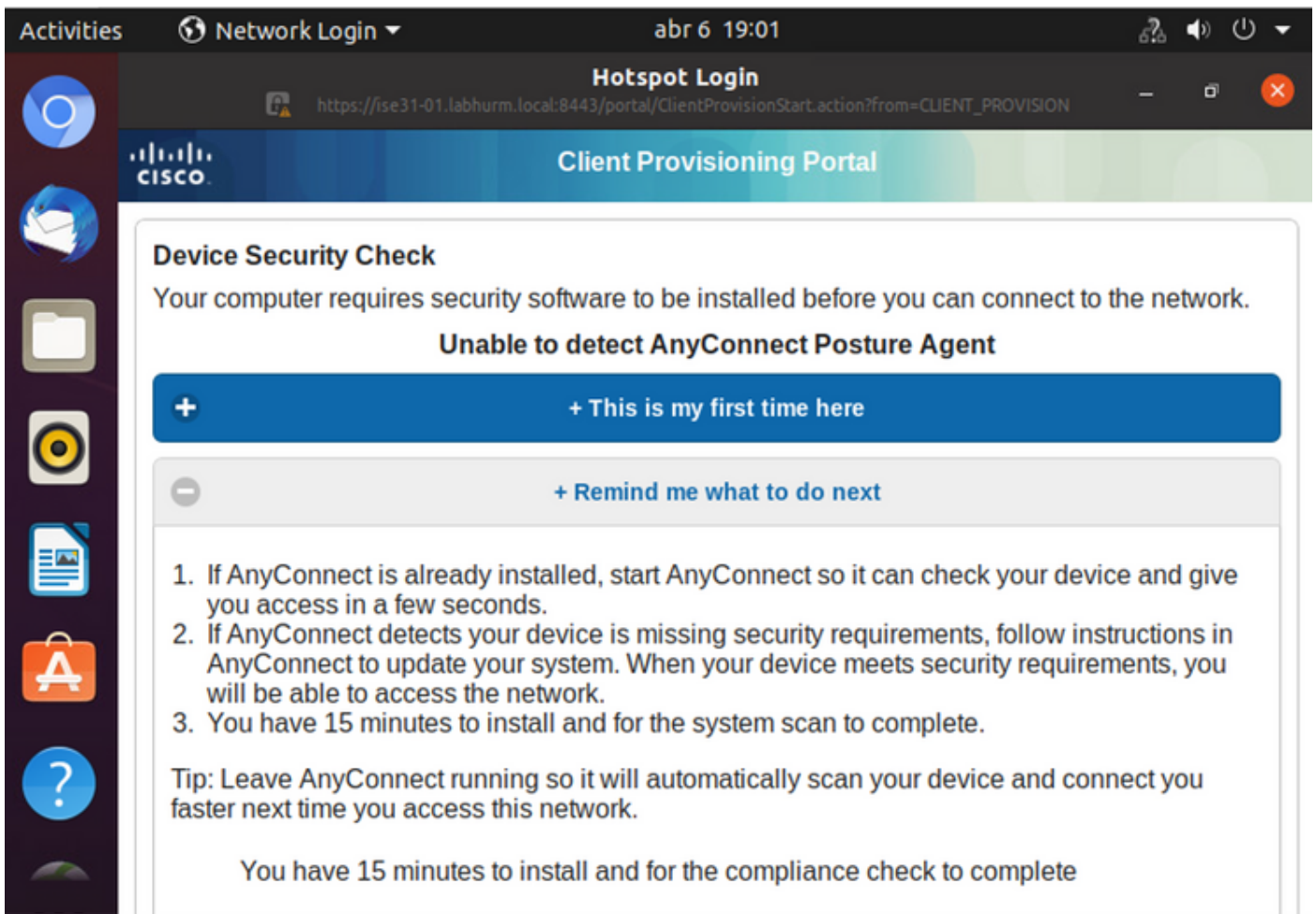
第5步：在Linux客户端上，必须发生重定向，并且它显示客户端调配门户，指示进行状态检查并点击“开始”：



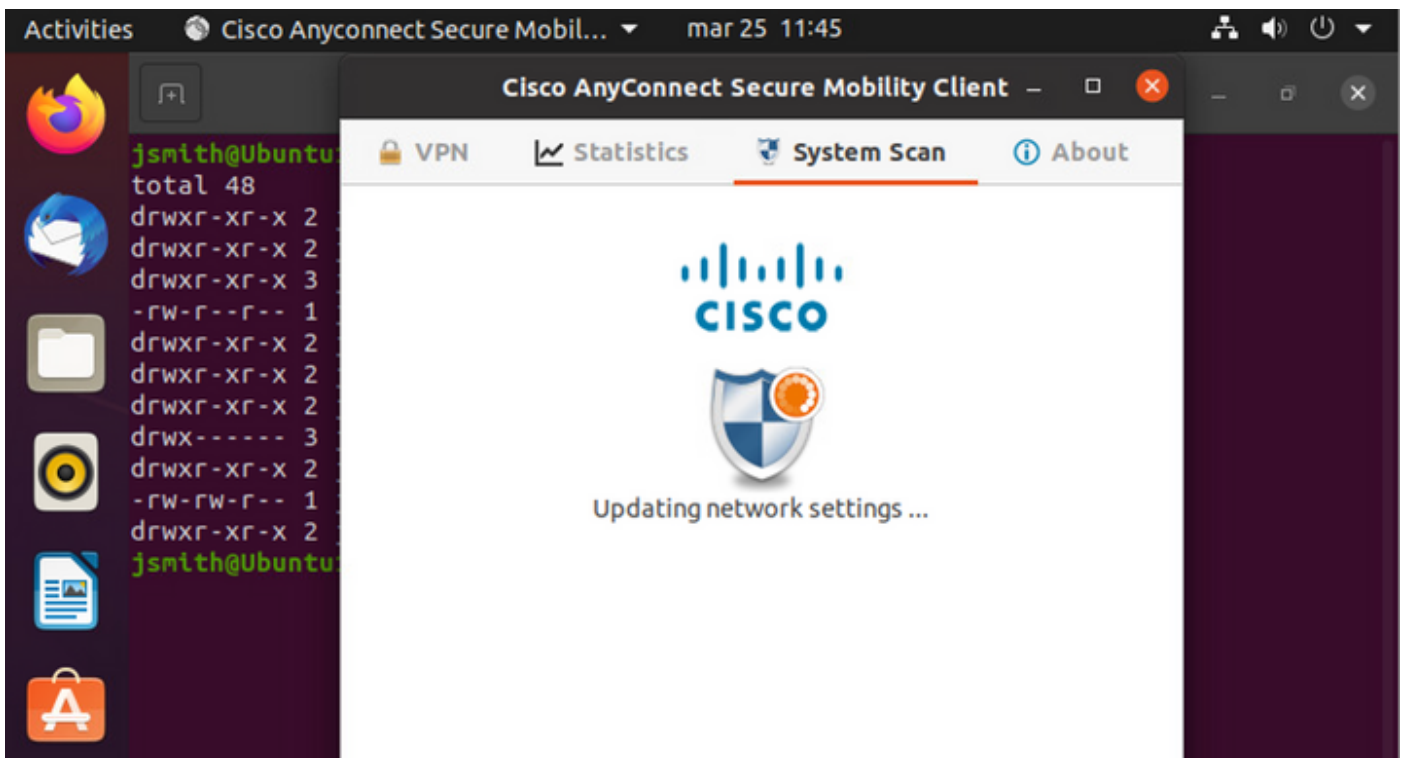
等待几秒钟，等待连接器尝试检测AnyConnect:



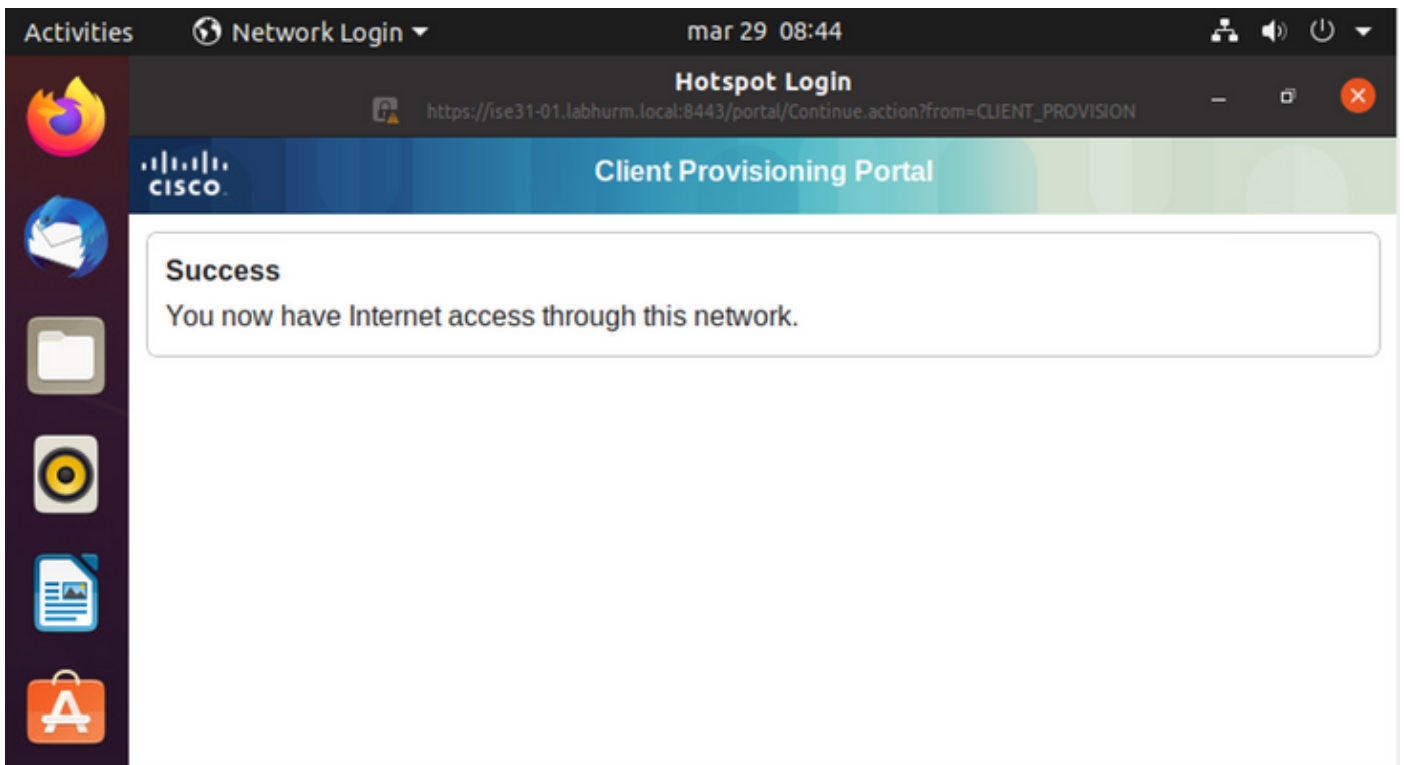
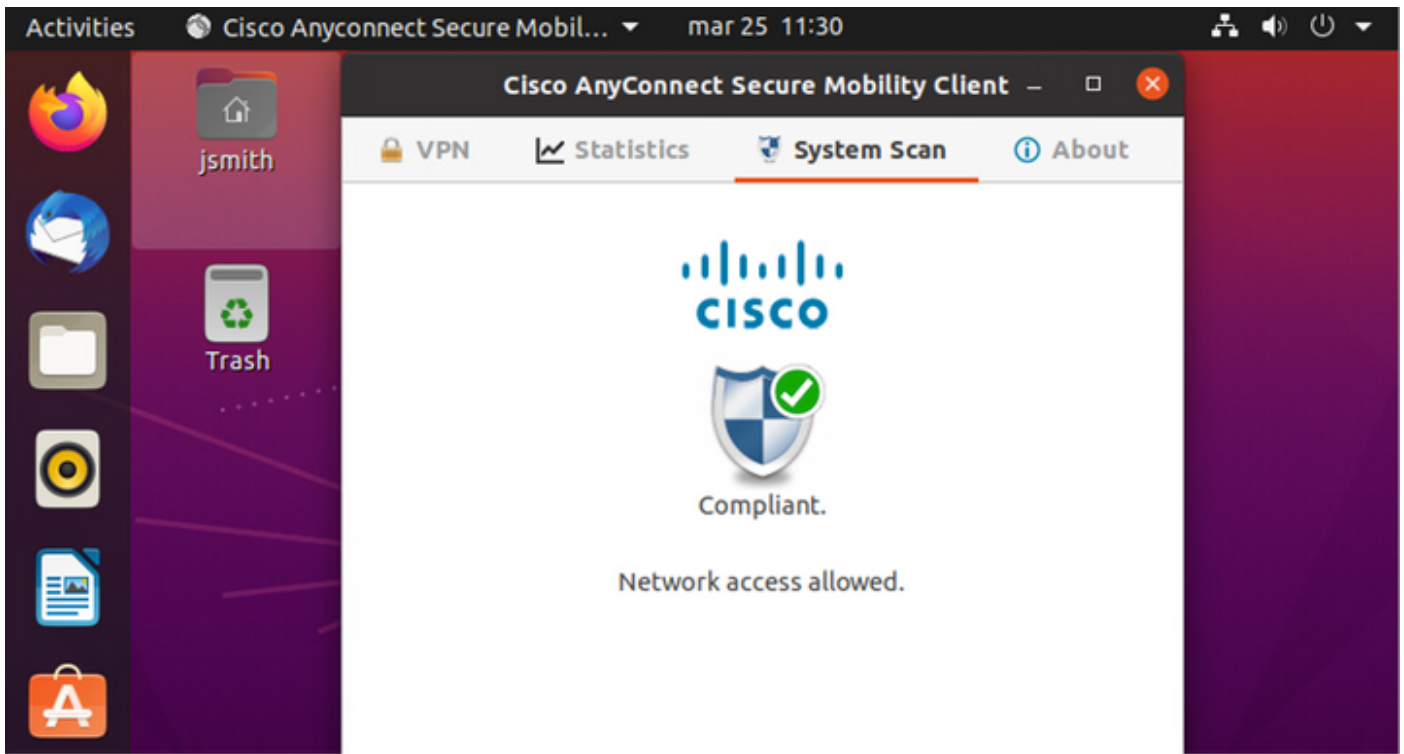
由于已知警告，即使安装了AnyConnect，也不会检测到它。使用Alt-Tab或Activities菜单切换到AnyConnect客户端。



AnyConnect尝试访问PSN以获取安全评估策略，并根据策略评估终端。

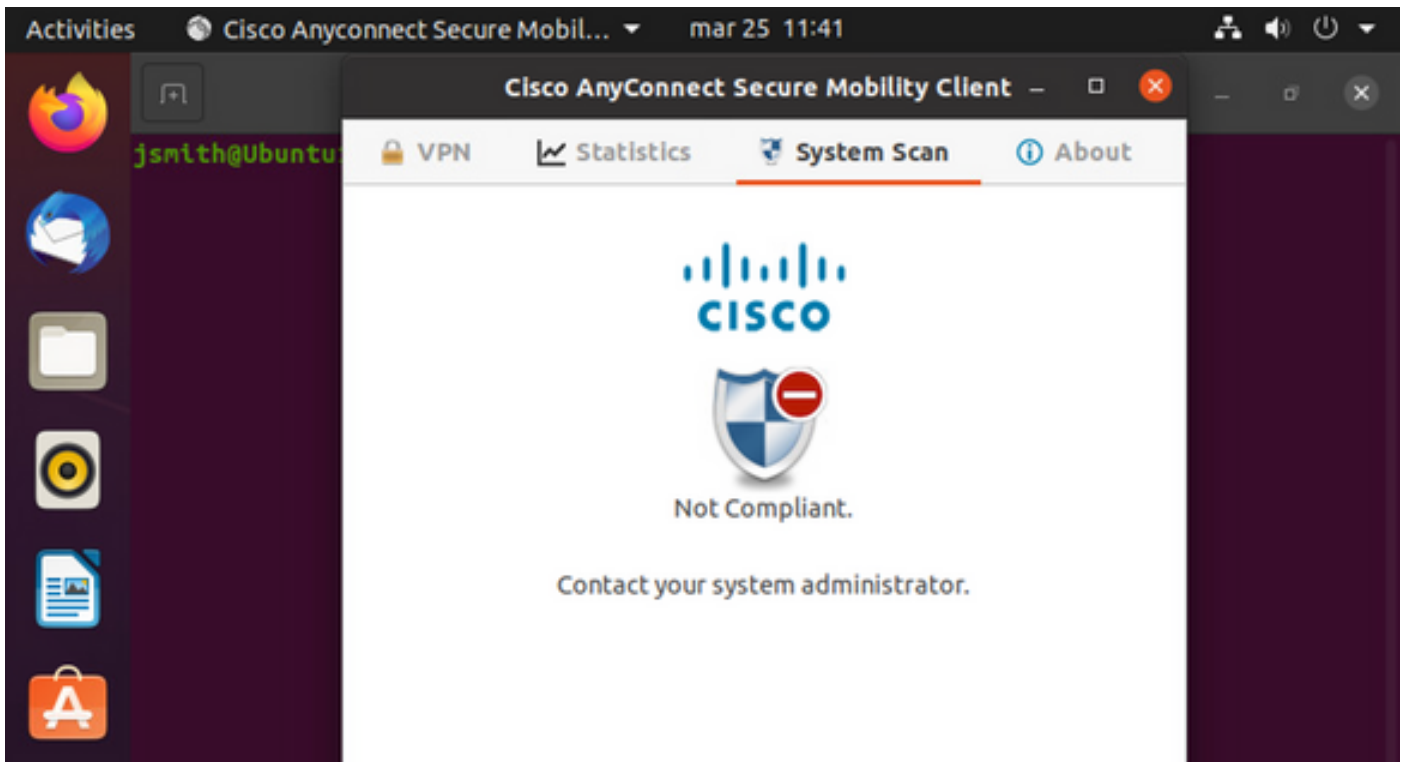


AnyConnect将其安全评估策略的确定报告回ISE。在本例中，兼容



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

另一方面，如果文件不存在，AnyConnect终端安全评估模块会将确定报告给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 Devi	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	

注意：ISE FQDN需要通过DNS或本地主机文件在Linux系统上可解析。

故障排除

show authentication sessions int fa1/0/35

重定向到位：

```

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

```


授权成功：

```
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: C0A8C883000000010008044A
  Acct Session ID: 0x00000004
  Handle: 0xEB000001

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

不合规，已移至隔离VLAN和ACL:

```
LABDEMOAC01#sh authe 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
```