

Linux عم Cisco ISE 3.1 ةي عضو نيوكت

تايوت حمل

[ةمدقم](#)

[ةيساس الابلطت](#)

[تابلطت](#)

[ةمدختسم التانوكم](#)

[نيوكت](#)

[ISE لىل ع تانويوكت](#)

[لوحمل لىل ع تانويوكت](#)

[ةحصل لىل نم ققحت](#)

[اوحال ص او اطاخ ال افاشكتسا](#)

ةمدقم

ةيوهل تامدخ كرحم و Linux ل فلم عضو ةسايس ذفنيو ل كشي نأ عارج ال ةقيثو اذه فص ي (ISE).

ةيساس الابلطت

تابلطت

ةيلال عيضاوم لابل ةفرعم كيدل نوكت نأب Cisco ي صوت:

- AnyConnect
- ةيوهل تامدخ كرحم (ISE)
- سكتيل

ةمدختسم التانوكم

ةيلال ةيدامل التانوكم ل اوجمارب ال تارادص ال دننتسم ل اذه يف ةدراول تامولعمل دننتست:

- AnyConnect 4.10.05085
- ISE رادص ال P1 3.1
- Linux Ubuntu 20.04
- Cisco رادص ال (15.12(3)E5) 03.07.05.E Catalyست 3650 لوحم

ةمدختسم ال ةزه ال عيجم تادب. ةصاخ ةيلمعم ةئييب يف ةدوجوم ال ةزه ال نم دننتسم ل اذه يف ةدراول تامولعمل اءاشنا م ت يال لم تحم ل ريتال ل كم هف نم دكأتف، ليغش تال دي ق كتكبش تناك اذا. (يضارثفا) حوسم نيوكتب دننتسم ل اذه يف رما.

نيوكت

ISE لىل ع تانويوكت

عضولاً ةمدخ ثي دحت 1. ةوطخل

دح. عضولاً تاثير دحت > جمارب ل تاثير دحت > تاداع ل > عضولاً > لمعل زكارم ل ل لقتنا
ةلمعل اءاتنا رظتناو نالاً "ثي دحت":

The screenshot displays the Cisco ISE Work Centers interface for Posture configuration. The 'Posture Updates' section is active, showing the 'Web' update method selected. The update feed URL is set to the default Cisco URL. There are input fields for proxy address and port, and a frequency setting for automatic updates (every 2 hours). Below the configuration fields are 'Save', 'Update Now', and 'Reset' buttons. An 'Update Information' section provides details on the last successful update and various support chart versions.

جمارب مزح لثم، Cisco.com عقوم نم اهل ليزنتب موقت جمارب ةمزح يه Cisco نم ةمدقم ل ةمزح ل
ةج او جراح هتأشنأ نيوكت وأ فيرعت فلم يه ليمعل اءاشنأ ي ل ةمزح ل AnyConnect.
اذهل ةبسن ل ل اب. عضولاً مي يقت عم مادختس ل ل ISE ل ل ه ل ي دحت دي رتو ISE مدختسم
AnyConnect Webdeploy "AnyConnect-Linux64-4.10.05085-
webdeploy-k9.pkg".

ه ب صوم ل رادصل ل ري غت نكم ي، جي حصت ل ل جمارب و تاثير دحت ل ل ارظن: ةطخال م
cisco.com عقوم ل نم ه ب صوم رادصل ل دحاً مدختس ل

AnyConnect ةمزح ل ي دحت 2. ةوطخل

دراوم ل > ليمعل ل دادم ل ل لقتنا، عضولاً لمعل زكارم ل ل خاد نم

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

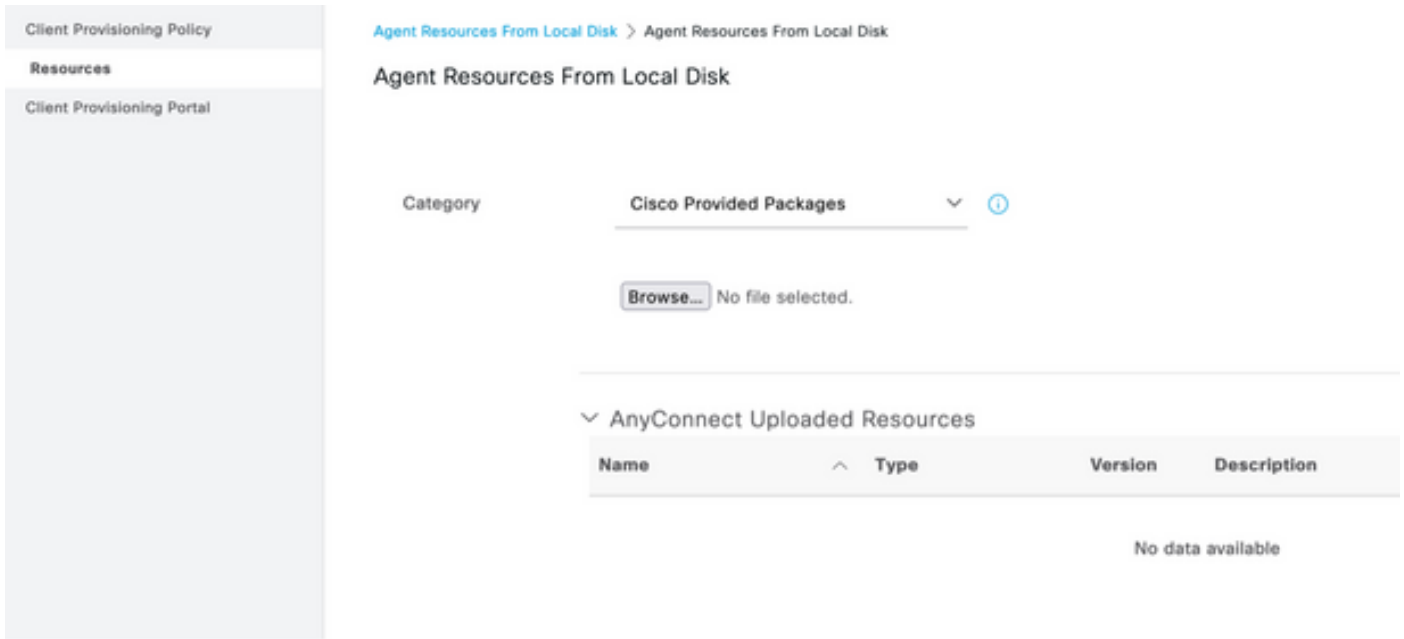
يُحلّم ال صرقل ال نم ليكوال دراوم > ةفاضل ددح 3. ةوطخل

Resources

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

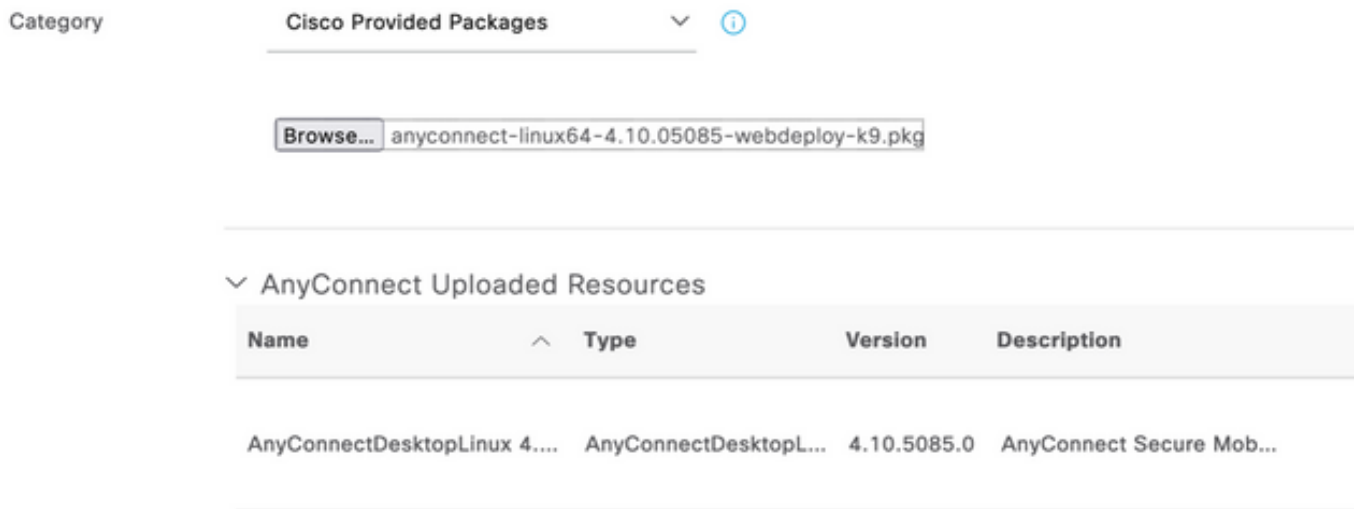
<input type="checkbox"/>	Agent resources from Cisco site
<input type="checkbox"/>	Agent resources from local disk

ةئفل ةلدسنم ال ةمئاق ال نم ةمدقم ال Cisco مزح ددح 4. ةوطخل



حفظت رقنا 5. ةوطخل

ةجالعم مت . ةقباسلا ةوطخل يف اهليزنتب تمق يتل AnyConnect مزح دحأ رتخأ 6. ةوطخل
ةمزحل لوج تامولعم ضرع متي و، AnyConnect ةروص



ةهه ةل لوصحل كنكمي ، ISE إل AnyConnect ليمحت دعب نأل . لاسرا ةل رقنا 7. ةوطخل
Cisco.com نم ىرخأل ليمعلا دراوم ةل لوصحل او ISE لاصتا

ةردقلا رفوت AnyConnect ليمع اهمدختسي ةيظمن تادحو ليمعلا دراوم نمضتت : ةظالم
لثم ةلجال نم ققحتل تاي لمع نم ةعونتم ةومجمل ةياهن ةطقن قفاوت مييقت ةل
رادجو ةراضلا جماربلا ةحفاكم جماربو سسجتلا ةحفاكم جماربو تاسوري ةل ةحفاكم
كلذ ةل امو فلملا و صارقأل ريفشتو ةيامحل

ةقيقد راطل اءلم قرغتسي . Cisco Site عقوم نم ليكولا دراوم > ةفاضل قوف رقنا 8. ةوطخل
ليمعلا ديوزتل ةروشنملا دراوملا لكب انايب عجرتسي و Cisco.com إل ISE لصي امنيب

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

كذلك إلى إضافة إلباب Linux لي غش التماظنل AnyConnect عم قفاوتل تادحو ثدحأ ددح. 9 ةوطخلل Mac و Windows ل ةيطمنلل قفاوتل ةدحو ددحت اضيأ كنكمي



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

Mac و Windows ل ني قوؤم الءالكلو ثدحأ ددح. 10 ةوطخلل

<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!

طافح ةقطق ط. 11 ةوطخل

اذه نيوكتل ليلد قاطن جراخ Windows Posture و MAC تانيوكت دجوت: ةظحالم

نآل اتقولناح دقل. ةبولطملا اعزأل اعيمج ثيدحتو ليمحتب تمق دقل، ةطقنللهذه دنع تانوكمللهذه مادختسال ةبولطملا تافصوتلاو نيوكتللا عاشنل.

AnyConnect Posture فيصوت و NAC ليلكو > ةفاضل عل رقنا. 12 ةوطخل

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

		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

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.

يه اهليلدعت بجي يتل تاملعمل

- يتليناوثلال دد ننييغت نم دادعال اذه كنكمي: VLAN ةكبش فاشتكال ينمزلال لصالال. ناو٥ 5 يه ةيصوصوال. VLAN ةكبش تارييغت نم ققحتال نيبي ةيظمنال ةدحولال اهرظتنني.
 - موقني أنكمي. ةيلعوال VLAN ةكبش رييغت فاشتكال ةقيرط يه هذ: ARP وأ ping ةقوؤمال ARP نيخت ةركاذ ةبقارم وأ ةيضاارفالال ةباوبال لاصلال راباخبال ليكوال ARP. وه هب يصوصوال دادعال. امهيلك وأ ةلهملل ةيضاارفالال ةباوبال لخالال.
 - ةياهنال ةطقن عضومتي، ةفورعم ريغ ةيانهن ةطقن ةيعضو نوكت امدنغ: حالصالال تقوؤم ةلشافال عضوال نم ققحتال تايلمع حالصال قريغتسي. عضوال مييقت قفدت لالخنم ريغ انه أنال ةياهنال ةطقن يلع ةمالع عضول بق قئاق د 4 وه يضاارفالال تقوال؛ اتقو يه ةيصوصوالا. (تاعاس 5) ةقيقد 300 ي 1 نم ميقلال حوارتن أنكمي نكلو، ةقفاوتم قريغتسي أن عقومال نم ناك اذا تاليدعت عارجا بلطتي دق كلذ أن ديبي؛ ةقيقد 15 لولطاً اتقو حالصالال.
- ةيئاقلللال ةجالعملال Linux فلم ةيعضو معدتال: ةظحالال

AnyConnect وأ ISE قئاقو يلال عوچرلا يچري، تاملعملال عيملال لماش فصو يلع لوصحلل Posture.

ددو، رايخال ددو عضوال فاشكسالا يطايتحالال خسنال ةمئاق ليكوال كولس ددح. 13 ةوطخالال ظفح ددحو PSN/لقتسملال FQDN

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

ةدقعلل IP ناونع ددح فاشتكالال فيضم > (ةيعضو) Posture تالوكوتورب تحت. 14 ةوطخالال PSN/Standalone.

FQDN وأ PSN ددح، رايخالال ددحو فاشتكالال يطايتحالال خسنال مداخ ةمئاق نم. 15 ةوطخالال ددحتلال ددحو لقتسملال

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

IP ناونع دي دحتو مداوخل ا عي مچب لاصتال * مداخال مسا دعاوق عون تحت 16 ة ووطخل لدب فرح مادختسا نكمي ،كلذ نم الدب .لزنم لاب لاصتالا ةمئاق نمض PSN/لقتسمال (اي *.acme.com) كتكبش يف ةلمتحمال PSN تالكبش عي مچ ةقباطم ل

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

AnyConnect نيوكت > ةفاضل يلع رونا 17 ة ووطخل

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 v

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

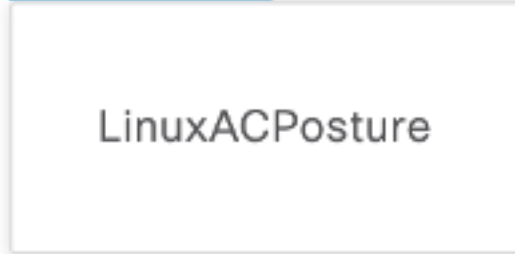
Profile Selection

* ISE Posture CPosture ▾

VPN

Network
Visibility

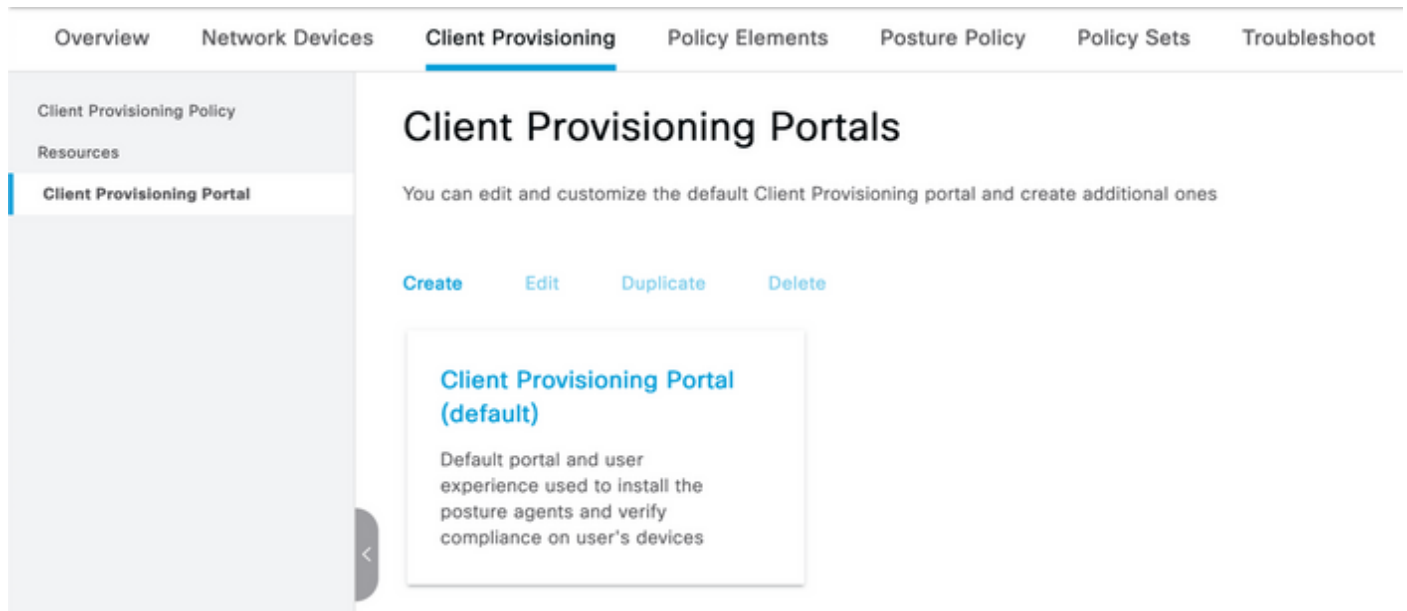
Customer
Feedback



لا سراً ددحو لفسأل ريرمتلاب مق

لا سراً قوف رقنا ،تادي دحتلال لمع نم يهتنت امدنع .18 ةوطخلال

لا سراً ددحو لفسأل ريرمتلاب مق > ليمعلا دادم | تاباوب > ليمعلا دادم | > عضولا > لمعلا زكارم ددحو .19 ةوطخلال



The screenshot shows the 'Client Provisioning Portals' configuration page. The navigation tabs include Overview, Network Devices, Client Provisioning (selected), Policy Elements, Posture Policy, Policy Sets, and Troubleshoot. The left sidebar shows 'Client Provisioning Policy' and 'Resources' with 'Client Provisioning Portal' selected. The main content area has the title 'Client Provisioning Portals' and a description: 'You can edit and customize the default Client Provisioning portal and create additional ones'. Below the description are buttons for 'Create', 'Edit', 'Duplicate', and 'Delete'. A card for the 'Client Provisioning Portal (default)' is shown, with a description: 'Default portal and user experience used to install the posture agents and verify compliance on user's devices'.

لا سراً ددحو لفسأل ريرمتلاب مق ،ذفنملاو ةهجاو لا ددحت كنكمي شيح ،لخدملا تاداع | مسق تحت .20 ةوطخلال
لا سراً ددحو لفسأل ريرمتلاب مق ،ذفنملاو ةهجاو لا ددحت كنكمي شيح ،لخدملا تاداع | مسق تحت .20 ةوطخلال

Configure authorized groups

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

Available

ALL_ACCOUNTS (default)

GROUP_ACCOUNTS (default)

OWN_ACCOUNTS (default)

>
<

Chosen

Employee

Choose all

Clear all

لېجست نېكمت رايخ نېكمت نم دكأت، لوخدل لېجست ؤحفص تادادع| نمض. 21 ؤوطخل
 ېئاقلتل لوخدل

✓ 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 v

- Require acceptance
- Require scrolling to end of AUP

ظفح ددح، نېمېلا ؤيولعلا ؤيوازلا ېف. 22 ؤوطخل

ل.لمعمل دادم| ةسايس > ل.لمعمل دادم| > عضولا > لمعمل زكارم ددح. 23 ةوطخل

هالء ةفاعضمل رتخاو CPP في IOS ةءءاق راوچب دوجومل لفسل مهسل قوف رقنا. 24 ةوطخل

LinuxPosture ةءءاق ال ةيمست. 25 ةوطخل

ل.لمعملك AnyConnect نيوكت ددح، ءءائتل لل. 26 ةوطخل

م هنال ةيطم نل قفاوتل ةءول ةلدسنم ةمءاق ىرت ال، ةلأل هذه في: ةظءالم AnyConnect نيوكت نم ءءك اهنيوكت

Client Provisioning Policy

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.

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

م قوف رقنا. 27 ةوطخل

ظفء ةقءط. 28 ةوطخل

عضولا ةسايس رصانع

ءفاضا ددح. فللمل > ءورشلل > ةسايسلل رصانع > عضولا > لمعمل زكارم ددح. 29 ةوطخل

ءيلالل ميقلل فيرءب مقو فللمل ءارش مساك TESTFile فيرءب مق. 30 ةوطخل

File Condition

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

فلمل ع قوم ىلع راسملا دمتعي: ةظحالم

ظفح ددح. 31 ةوطخلال

ثي ح ماظنلا ي ف ادوجوم فلمل ناك اذا ام ةفرعمل طرشك اذه فلمل عون ودبي. FilePresence قالطال ىلع مامتها يا دجوي ال ،رايخل اذه ديدحت عم .ءيش لك اذهو ،ادوجوم نوكي نأ ضررت في اذكهو ،ةئزجتلا ،فلمل اذخراوت نم ققحتلل

ي: لي امك ةديج ةسايس عاشن اب مقو تابلطتملا ددح. 32 ةوطخلال

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

ةجلعملل ءارجك طقف ةلاسرلا صن Linux معدي ال :ةظحالم

تابلطتملا تانوكم

- لكل سكوني ل: ليغشتلا ماظن
- قفاوتلا ةدحو: 4.x
- عضولا عون: AnyConnect
- (ليغشتلا ماظن ديدحت دعب ةرفوتم حبصت يتلا) هئالكوو قفاوتلا تادحو: طورشللا
- طورشللا عي مج رايخ اذ دعب ديدحتلل ءحاتم حبصت يتلا تاجلالم: ةجلالم تاءارج اذخراول

عضولا ةسايس > عضولا > لمعلا زكارم ددح. 33 ةوطخلال

دي دحت) LinuxPosturePolicy Define Insert New Policy ددو جهن ي أ ي (رېرحت) Edit ددح. 34 ةوطخل
 32. ةوطخل ي اهؤاشن م يتل ك تابل طتم ة فاضا نم دكأتو مساك (LinuxPosturePolicy)

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

ظفحو م ددحت. 35 ةوطخل

(ةماعل عضولا تادادع مسق) رخألا ةمهمل عضولا تادادع

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

ي لي امك عضول ةماعل تادادعإل مسق ي ةمهمل تادادعإل

- لشف ةلاح حيحصت لي م عمل يلع بجي يذلا تقولا رادقم دادعإل اذه ددحي: حالصالا تقؤم
 AnyConnect س يلو، ISE ل تقؤملا اذهو؛ AnyConnect نيوكت ي ف حالصالا تقؤم اضيأ كانه
- لماع يلع يوتحت ال يتل ةزهجالل عضولا ةلاح دادعإل اذه رفوي: يضارت فالال عضولا ةلاح
 ةمظنأ لثم، تقؤملا لماعل ليغشت اه نكمي ال يتل ليغشتال ةمظنأ وأ عضولا
 Linux. لي دنن تسمل ليغشتال
- ةزهجالل او قي بطلال طورش يلع دادعإل اذه قبطني: ةمرمت سمل ةبقارم لل ي نمزلا لصالا
 AnyConnect يلع اه ي بجي يتل تارملا ددع دادعإل ددحي. ةي اهنال ةطقن درج ب موقت يتل
 ةبقارملا تانايب لاسرا
- وأ رطلال امه دادعإل اذهل ني رايخ يوس دجوي ال: يفتللا عضو ي لو بقملا مادختسال جهن

متمي مل اذا ةعباتمل نم يفختللا عضو يف AnyConnect ءالمع رطلال عنمي . ةعباتمللا فرعتللا نود ىتح ةعباتمللاب يفختللا عضو ليمعمل ةعباتمللا حمست . AUP ب فارتعاللا ل يفختللا عضو دادعإ مادختسإ دنع دوصقملا وه نوكي ام ابلاغ يذلاو (AUP لوكوتورب ىلع AnyConnect).

مميقتللا ةداعإ تانيوكت

نيوكت ةيفيكتي تيار دقل . عضوللا لممع ريسل اماه انوكم عضوللا مميقت ةداعإ تاي لممع دعت ليمعمللا ققحتي . "عضوللا لوكوتورب" مسق يف عضوللا مميقت ةداعإل AnyConnect ليكو نيوكتللا اذه يف تقوؤملا ىللا ادانتسا ةدحمللا PSNs مادختساب لوخدلا نم يرود لكش ب

ادانتسا ، عضوللا مميقت ةداعإ ىللا ةجاح كانه تناك اذا ام PSN دحت ، PSN ىللا بلط لصي ام دنع PSN نإف ، مميقتللا ةداعإ ةي لممع ليمعمللا ررم اذا . كلت ةياهنللا ةطقن رودل ISE نيوكت ىللا اذا . عضوللا راجي نبيعت ةداعإ مميقتو ، ةياهنللا ةطقن ةي عضو عم قفاوتللا ةلاح ب ظفتحتي مميقتو ، قفاوتم ريغ ىللا ريغتت عضوللا ةلاح نإف ، مميقتللا ةداعإ يف ةياهنللا ةطقن تلشف دوجوم يعضو ريغات ي ةلازا .

ليوختللا صيصخت فلم > ليوختللا > جئاتنللا > ةسايسللا رصانع > ةسايس دح . 36 ةوطخللا ةفاضإ دح

تاملعمللا نيوكت ب مق ممل ليوختللا فيرعت فلمك wired_redirect فيرعت ب مق . 37 ةوطخللا ةيلالات

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

ظفح دح . 38 ةوطخللا

ليوختللا تاسايس نيوكت . 39 ةوطخللا

عضوللا اقبس ممل اهنيوكت ممل ليوختللا دعاوق ثالث كانه

1. فورعم ريغ زاوجللا قفاوت نأ امك ، ةقداصل ممل حاجن دنع ةقباطم لل لوالا نيوكت مميقتي .
2. ةقفاوتم ريغ ةياهنللا طاقن عم ةحجانللا ةقداصل ممل تاي لممع ةي نائللا ةدعاقللا قباطتو .

فلم مادختسإ يهو ، اهسفن ةجيتنللا ىلع نبيجللوالا ني ددعاقللا نم لك يوتحت : **ةظحالم** دادمإ لخدم ىللا ةياهنللا ةطقن هي جوت ةداعإ ىلع لمعي اقبس ممل نوك ممل ليوختللا فيرعت ليمعمللا .

3. عضوللا عم ةقفاوتم ممل ةياهنللا طاقنو ةحجانللا ةقداصل ممل ةياهنللا ةدعاقللا قباطتو . اقبس ممل همي مميقت ممل يذلل PermitAccess ضيوفت فيرعت فلم مدختستو .

مميقت يذلل MAB - يكللللا 802.1x ل نميألا مهسللا ددحو تاسايسللا ةومجم > ةسايس دح . قباصللا ربتخمللا يف هؤاشنإ

ةيلالاتللا دعاوقللا ءاشنإو ليوختللا جهن دي دحت . 40 ةوطخللا

	SISE_UnknownCompliance_Redirect	AND	<ul style="list-style-type: none"> Network_Access_Authentication_Passed Compliance_Unknown_Devices ISEAD External/Groups 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 External/Groups 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 External/Groups EQUALS ciscoise lab/Users/Domain Users 	<input type="text" value="NewAP"/> + <input type="text" value="Select from list"/> + 2

لوحه المايلع تاني وكالتا

تال د ب م ل ت ا ف ا ل ت خ ا ك ا ن ه ن و ك ت ن ا ن ك م ي . IBNS 1.0 ا ل ا ي ل ا ت ا ل ن ي و ك ت ل ا ر ي ش ي : ة ط ح ا ل م ا ر ي ث ا ت ل ق ا ع و ي ف ر ش ن ن م ض ت ي و ه و . ة ر د ا ق ل ا IBNS 2.0

```

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
```

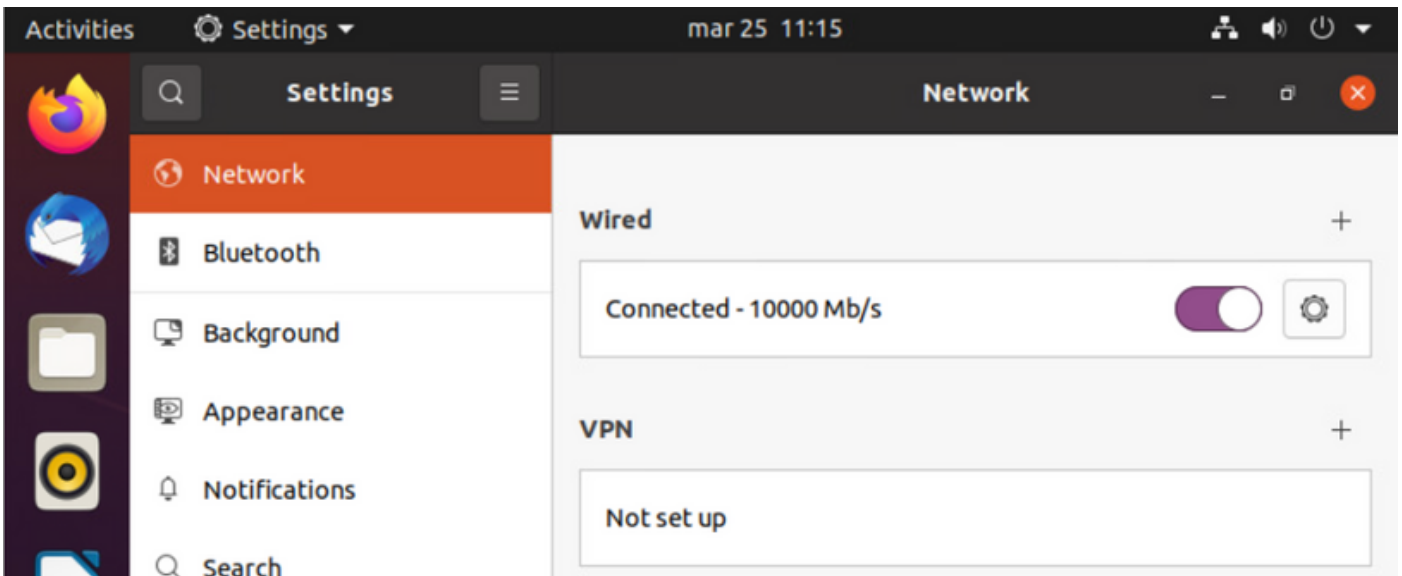
ةحصلالانم ققحتال

الانم ققحتال ISE:

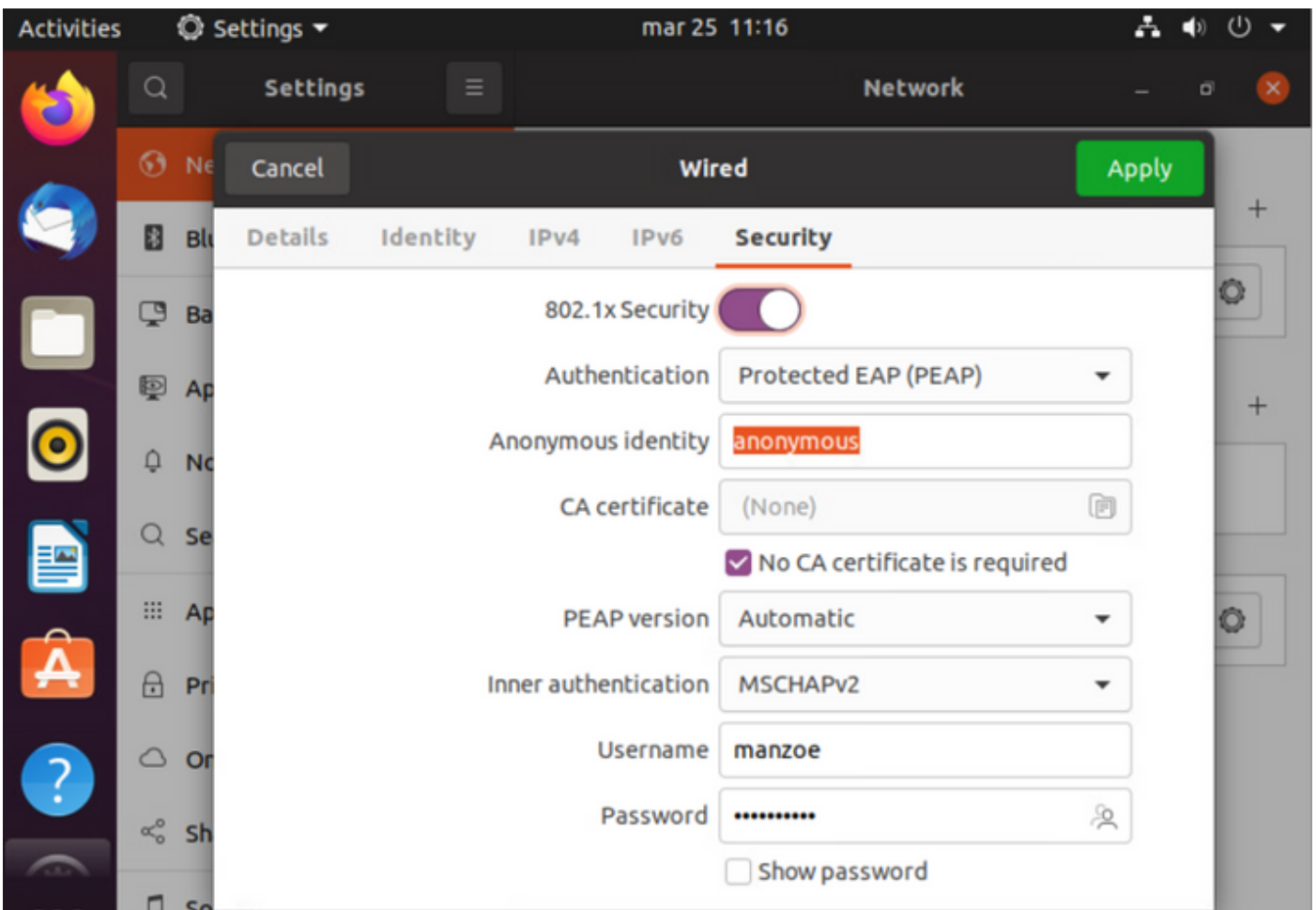
تامدخ كرحمة عىضو ISE Posture ةدحوب AnyConnect تىبثت مت دق هانأم سقلا اذه ضررت في Linux ماظن لىلع اقبس م (ISE) ةىوهال

dot1x مادختساب رتوي بمكال ةقداصم

ةكبشلال تادادع لىل لقتنا 1. ةوطخال



مدخستسما دامتعا تانايبو 802.1x ةئيهت ريفوتب مقو نيأت بيوبتلا ةمالع دح. 2 ةوطخلا



"قيبطت" قوف رقنا. 3 ةوطخلا

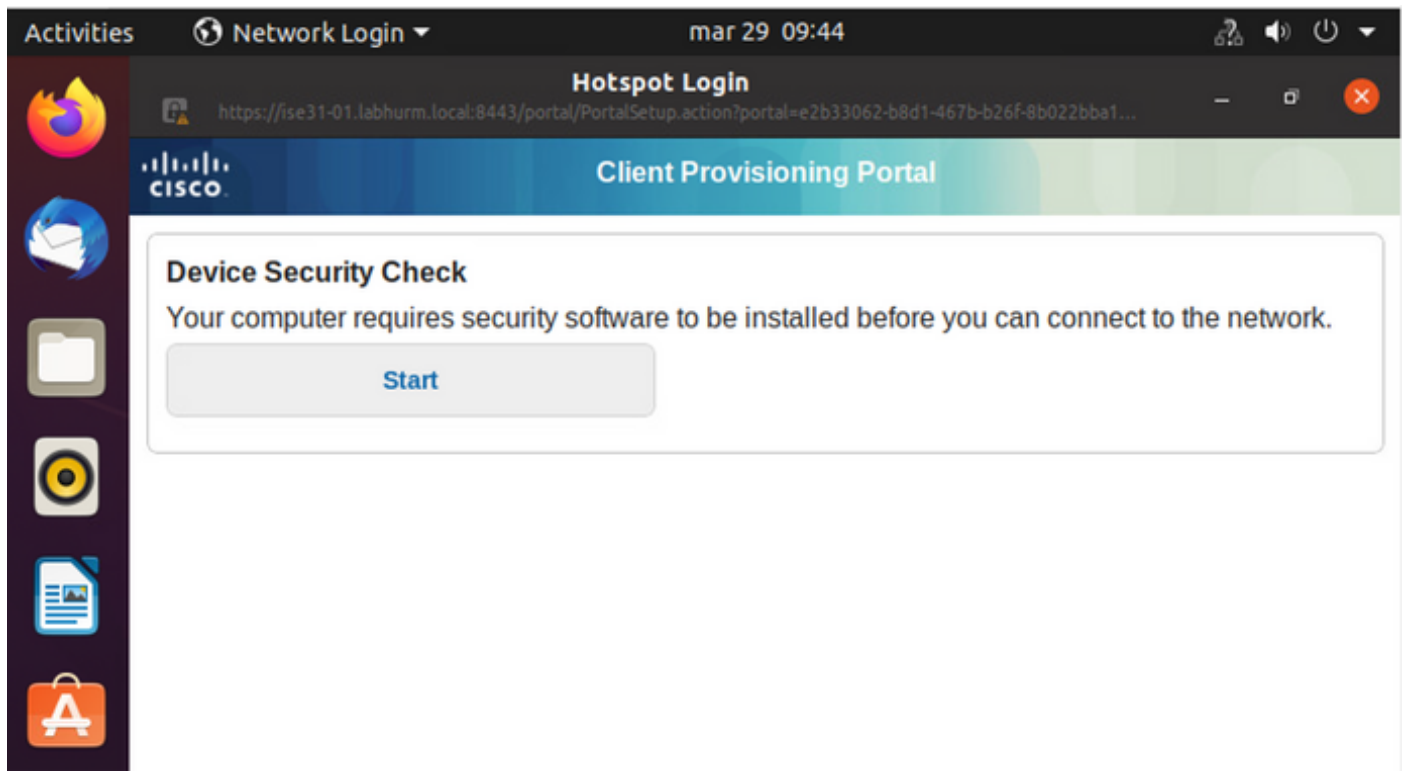
ISE لجس يف هنم ققحتلاو 802.1x ةئيهت لسلا ةكبشلاب Linux ماظن ليصوتب مق. 4 ةوطخلا
Live:

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint...	Authenti...	Authoriz...	Authoriz...	IP Address	Network De...	Device Port	Identity Group	Posture
Apr 06, 2022 08:42:08.2...	●		4	marcoe	00-0C-29-44-03-8F	Ubuntu W...	Ubuntu Po...	Ubuntu Po...	Wired_Re...			FastEthernet1...		Pending
Apr 06, 2022 08:32:48.2...	●			marcoe	00-0C-29-44-03-8F	Ubuntu W...	Ubuntu Po...	Ubuntu Po...	Wired_Re...		Cat-3750	FastEthernet1...	Workstation	Pending
Apr 06, 2022 08:32:40.8...	●			marcoe	00-0C-29-44-03-8F	Ubuntu W...	Ubuntu Po...	Ubuntu Po...	Wired_Re...		Cat-3750	FastEthernet1...	Workstation	Pending

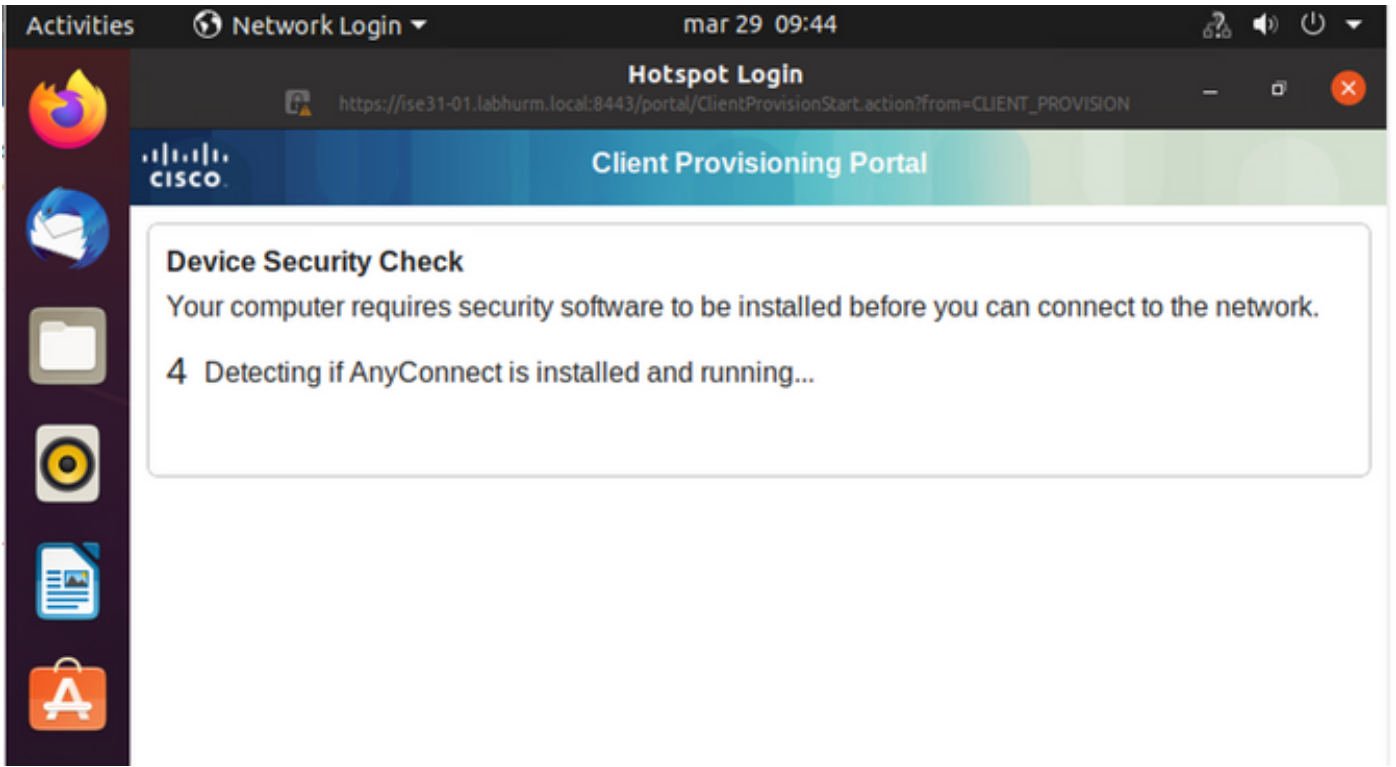
ةلاح مدخي ذلذا PSN لثم ،ةيفاضا تامولعم ضرعل يققألا ريرم تالطيرش مدختسأ يفي ISE، عضولا وأ قفدتال:

Authoriz...	Authoriz...	IP Address	Network De...	Device Port	Identity Group	Posture ...	Server
Authorizatic	Authorizatic	IP Address	Network Device	Device Port	Identity Group	Posture Sta	Server
Ubuntu Po...	Wired_Re...			FastEthernet1...		Pending	ise31-01
Ubuntu Po...	Wired_Re...		Cat-3750	FastEthernet1...	Workstation	Pending	ise31-01
Ubuntu Po...	Wired_Re...		Cat-3750	FastEthernet1...	Workstation	Pending	ise31-01

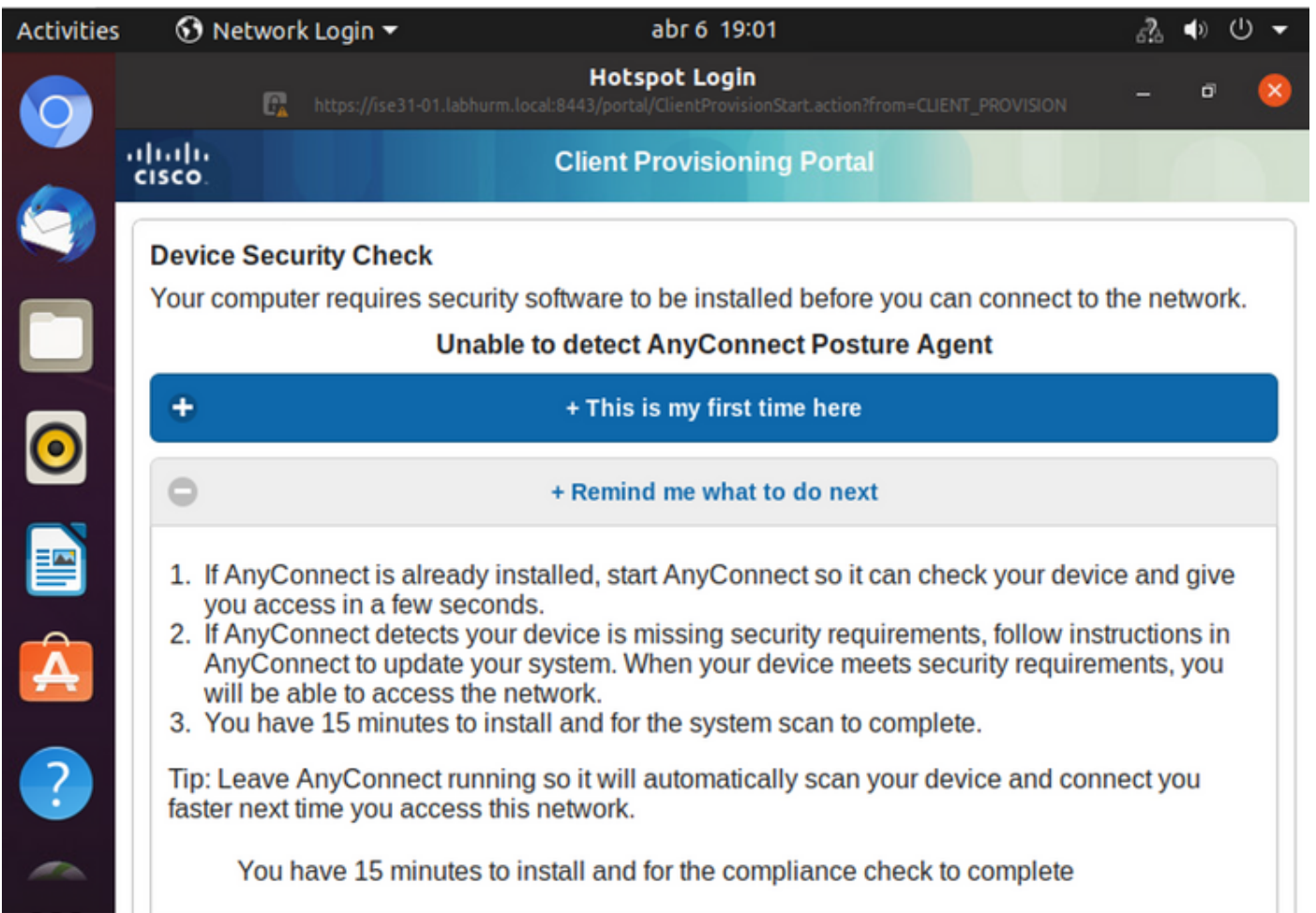
ثودح لىل ريشي لىمعال دادم لخدم مدقي وهو ،هيجوتال ةداع عقي ،Linux لىمعي في 5 ةوطخلا ةيادب رقنل وعضولا قيقت:



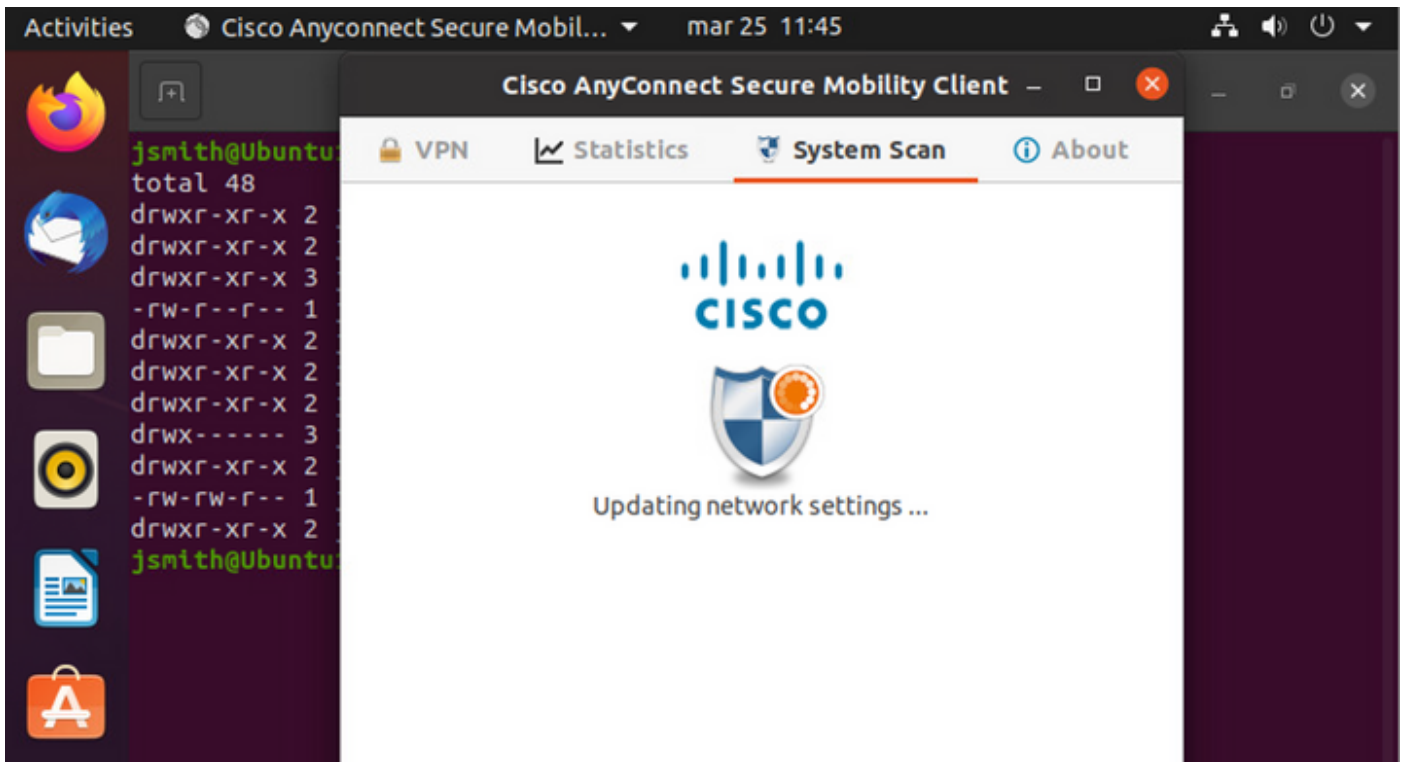
AnyConnect فاشتك لصلومال لواحي امنيب ناو ثعضب رطالتنا:



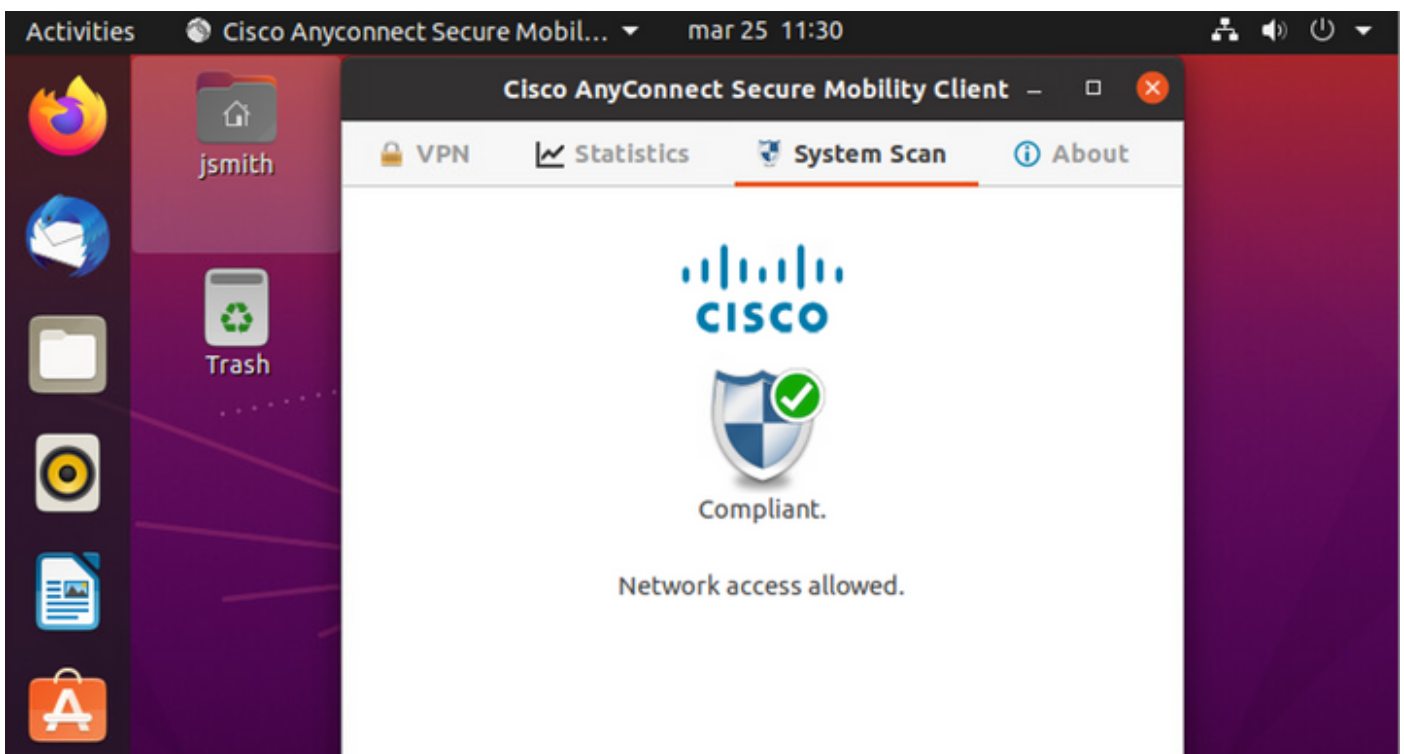
وأ Alt-Tab مَدْخَتْسَأ. هَفَشْتَكِي ال هِنِإَف، AnyConnect تِيْبَثْت مَت إِذَا يَتَح، فَوْرَعْم رِيْذَحْت بَبْسَبِ
AnyConnect لِيْمَع يَلِإ لِيْدَبْتَلَل ةَطَشْنَأَل ةَمِّيَأَق.

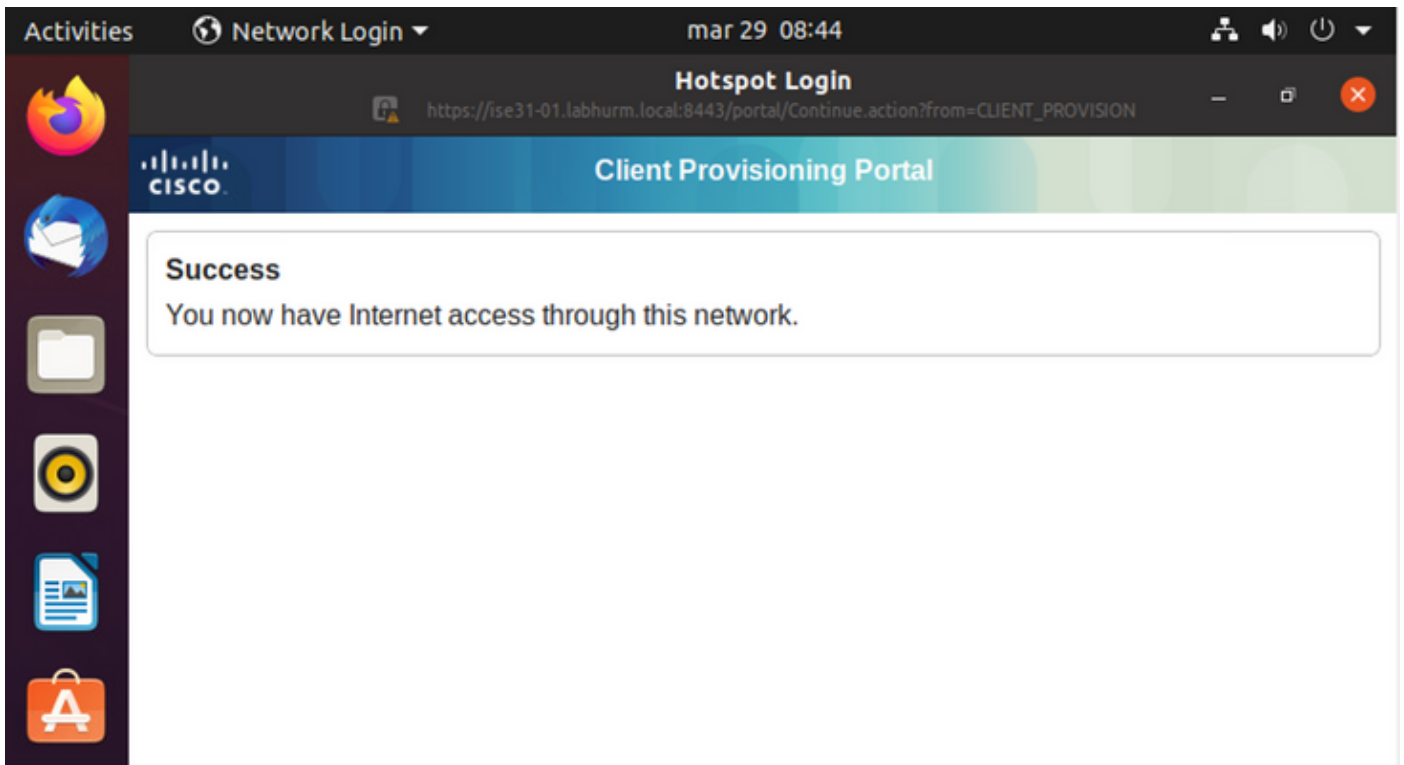


اهْدَضْ ةِيَاهِنَلَا ةَطَقْن مِيْيَقْتَو PSN عَضْو ةَسَايَس يَلِإ لَوْصَوْلَا AnyConnect لَوَاجِي.



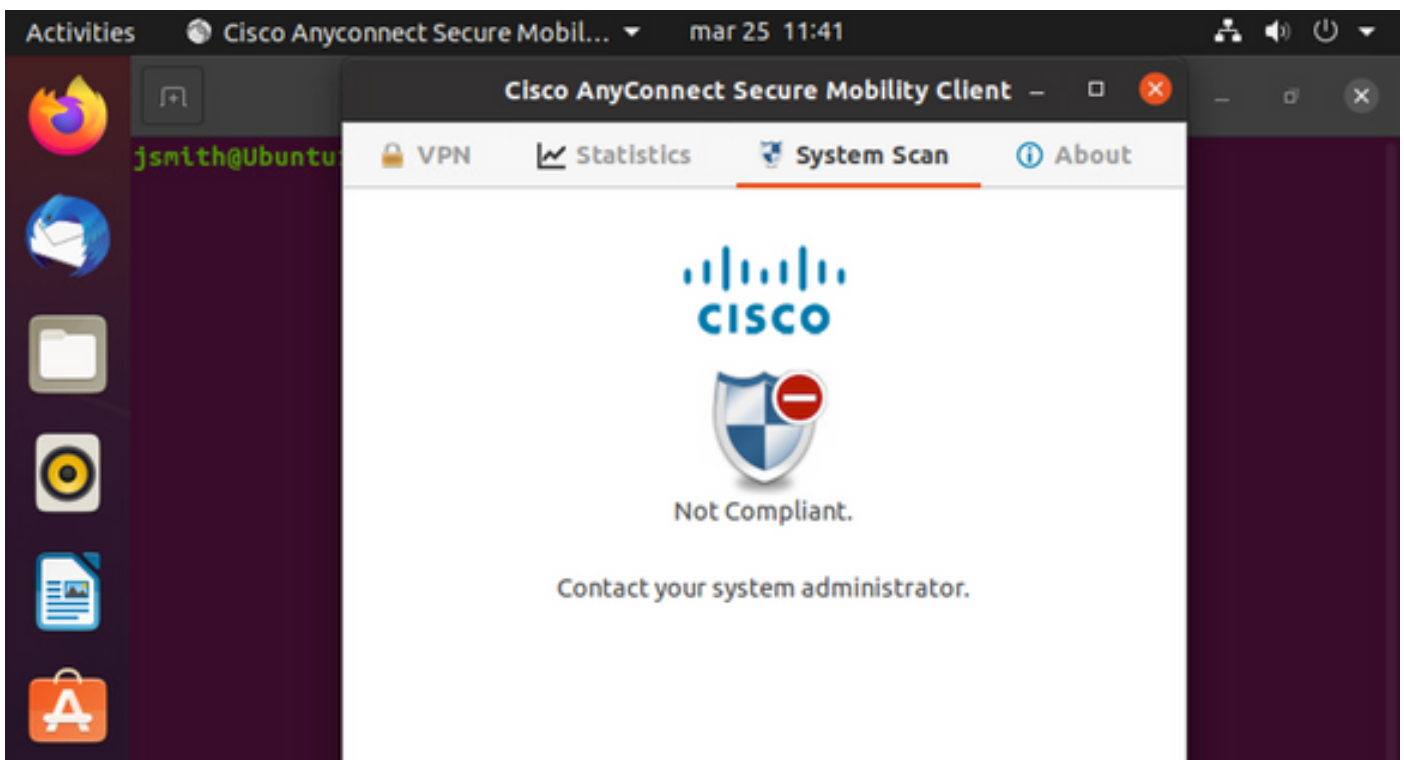
ة، لإحلال هذه في ISE. إلى إرخأ ةرم عضولا ةسايس إلى ع هم يم صت ن ع AnyConnect غل بي قفاوتم





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

نع غلبت أي عضو لل AnyConnect ةدحو نإف ،ادوجوم فل مل نكي مل اذا ،يرخأ ةي حان نم ISE لى عمي مصت الل



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	

يحلحالمال فيضمالمال فلم وأ DNS لالخالخ نم Linux ماظن ىلع فQDN ISE لجال مزلي: عطلحالمال.

اهحالصاوا عاطخال فاشكتسا

show authentication sessions int fal/0/35

عقومال في هيحوتلال اداعا:

```
LABDEMOAC01#show authentication sessions interface fastEthernet 1/0/35
  Interface: FastEthernet1/0/35
  MAC Address: 000c.2946.038f
  IP Address: 192.168.101.51
  User-Name: manzoe
  Status: Authz Success
  Domain: DATA
  Security Policy: Should Secure
  Security Status: Unsecure
  Oper host mode: multi-auth
  Oper control dir: both
  Authorized By: Authentication Server
  Vlan Group: N/A
  URL Redirect ACL: ACL_REDIRECT_AV
  URL Redirect: https://ise31-01.labhurm.local:8443/portal/gateway?sessionId=C0A8C88300000010008044A&p33062-b8d1-467b-b26f-8b022bba10e7&action=cpp&token=05a438ecb872ce396c2912fecfe0d2aa
  Session timeout: N/A
  Idle timeout: N/A
  Common Session ID: C0A8C88300000010008044A
  Acct Session ID: 0x00000004
  Handle: 0xEB000001

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

ليوختلال حجن:

```
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
```

(ACL) لوصولال في مكحتلال مئاوقو VLAN ةكبش لزع ىللالقنلال مت ،قفاوتم ريغ:

```
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
```

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة م ادخت ساب دن تسمل اذة Cisco ت مچرت
ملاعلاء انء مچ م ف ن م دخت تسمل معد و ت م م دقت ل ة يرش ب ل و
امك ة ق ق د ن و ك ت ن ل ة ل آل ة مچرت ل ض ف أن ة ظ حال م چ ر ة . ة ص ا خ ل م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت م م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا م ل ا ح ل ا و ه
ل ا ا م ا د ا د ع و چ ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص أ ل ا ي ز ي ل چ ن ا ل ا دن تسمل ا