

ىلج دحاو SSID Wireless BYOD نىوكت Windows و ISE

تاىوتحملا

[قمدملا](#)

[ةيساسال تابلطتلا](#)

[تابلطتلا](#)

[قمدمتسملا تانوكملا](#)

[ةيرطن](#)

[نىوكتلا](#)

[ISE نىوكت](#)

[\(WLC\) ةيكللسال LAN ةكبش ي ف مٌكحتلا ةدحو نىوكت](#)

[ةحصلا نم ققحتلا](#)

[ةقداصملا قفدت نم ققحتلا](#)

[يب ةصاخلا ةزهجالا ةباوب نم ققحتلا](#)

[اهجالص او ءاطخال افاشكتسا](#)

[ةماع تامولعم](#)

[لمعلا لچس ليلحت](#)

[ISE تالچس](#)

[\(spw تالچس\) ليمعلا تالچس](#)

قمدملا

ةيوهلا تامدخ كرحم ىلع (BYOD) كب صاخلا زاهجال راضح نىوكت ةيفيك دنتسملا اذه فصى جودزملا SSID و يدرفال SSID نم لك مادختساب Windows زاهج Cisco نم (ISE) ةيوهلا تامولعم.

ةيساسال تابلطتلا

تابلطتلا

ةيلاتلا عيضاوملاب ةفرعم كيديل نوكت نأب Cisco يصوت:

- Cisco ISE، رادصال 3.0 نىوكت
- Cisco WLC نىوكت
- دوياب

قمدمتسملا تانوكملا

ةيلاتلا ةيداملا تانوكملا او جماربلا تارادصال ىل دنتسملا اذه يف ةدراولا تامولعملا دنتست:

- Cisco نم 3.0 رادصال ISE
- Windows 10 ليغشتلا ماظن
- WLC و AP

ةصاخ ةي لمعم ةئي ب ي ف ةدوجوملا ةزهجال نم دنتسملا اذه ي ف ةدراولما تامولعملما عاشنإ مت تناك اذا .(يضا رتفا) حوسمم نيوكتب دنتسملا اذه ي ف ةمدختسملا ةزهجالما عيمج تادب رما يال لمحتحملما ريثاتلل كمهف نم دكاتف ،ليغشتلا دي قكتكبش

ةيرظن

حنم دعب امي فو ةزهجالما ليصوت نم لكل طقف دحاو SSID مادختسا متي دحاو SSID BYOD ي مسا مادختسا اب SSID ب مدختسملا لصتي ،الوا .ةلجسملا ةزهجالما يلا لماكلما لوصولما ةداعإ متي ،ISE يلع حاجنبا اهيلي ةقداصملا درجمبو . (MSCHAPv2) رورملا ةملاكو مدختسملا يئاهنلا لي معمل موقبي ،زاهجالما ليحست عارجإ درجمبو . BYOD لخدم يلا مدختسملا هيحوت يئاهنلا لي معمل يلع NSA تيبتت متي . ISE نم (NSA) يلاصألا بلاطلا دعاسم لي زنتب موقبي و ةيكلساللا بلاطملا نيوكتب NSA موقبي . ISE نم ةداهشلاو فيرعتلا فلم لي زنتبو مادختسا اب SSID سفلنل رخأ ةقداصمب ةيئاهنلا ةطقن موقت . ةداهشلا تيبتت ب لي معمل لي معمل نم دي دجال بلاطلا نم ISE ققحتي . EAP-TLS مادختسا اب اهلي زنت مت يئاهنلا ةداهشلا زاهجالما يلا لماكلما لوصولما حنمي و زاهجالما ليحستو EAP بولسا نم ققحتي و

Windows BYOD- ل ةدرفملا SSID تاو طخ

- ةيلاوالما EAP-MSCHAPv2 ةقداصم
- BYOD لخدم يلا هيحوتلا ةداعإ
- ةزهجالما ليحست
- NSA لي زنت
- فيرعتلا فلم لي زنت
- ةداهشلا لي زنت
- EAP-TLS ةقداصم

نيوكتلا

ISE نيوكت

كرتسملا حاتفملاو RADIUS نيوكتب مقو ISE يلع ةكبش زاهج ةفاضاب مق 1. ةوطخلا

ةكبشلا زاهج ةفاضاب > ةكبشلا ةزهجا > ةرادإ > ISE يلا لقتنا

حاتفم مادختسا يلع بلاقالما يوتحي نأ بجي . BYOD يمدختسملا ةداهش بلاقالما عاشنإ 2. ةوطخلا يضا رتفالما EAP_CERTIFICATE_TEMPLATE مادختسا كنكمي . نسمحملا لي معمل ةقداصم

Cisco ISE Administration - System

Deployment Licensing **Certificates** Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access Settings

Edit Certificate Template

* Name BYOD_Certificate_template

Description

Subject

Common Name (CN) \$UserName\$ ⓘ

Organizational Unit (OU) tac

Organization (O) cisco

City (L) bangalore

State (ST) Karnataka

Country (C) IN

Subject Alternative Name (SAN) :: MAC Address

Key Type RSA

Key Size 2048

* SCEP RA Profile ISE Internal CA

Valid Period 3652 Day(s) (Valid Range 1 - 3652)

Extended Key Usage Client Authentication Server Authentication

يكلسال فيصوتل يلصأ بلطتم فيصوت عاشنإ 3. ةوطخل

فيرعت فلم رتخاوة فاضا يلعل رقنا . ليمعلا دادم | > BYOD > لمعلا زكارم > ISE > يل لقتنا ةلدسنملا ةمئاقلا نم (NSP) يلصألا بلاطلا

دح . دحاو BYOD SSID لمعب موقت نأ لبق كلالصتا مساسفن وه SSID مساسنوكي نأ بجي انه كنكمي وأ ةقباسلا ةوطخل ي ف هؤاشنإ مت امك ةداهشلا بلاق رتخا . TLS ك لوكوتوربلا ي ضارثفالا EAP_CERTIFICATE_TEMPLATE مادختسا .

كتابلطتملاقف وزاهجالاو مدختسملا وأ مدختسملا ةقداصم دح ، ةيرايتخال تادادعإلا تحت يضارثفاك رخالا تادادعإلا كرتأ . مدختسم ةقداصمك اهنيوكت متي ، لاثلما اذه ي ف

Cisco ISE Work Centers - BYOD Evaluation Mode 46 Days

Overview Identities Identity Groups Network Devices Ext Id Sources **Client Provisioning** Portals & Components Policy Elements Policy Sets Reports More

Client Provisioning Policy

Resources

Name: WirelessNSP

Description: Wireless Profile(s)

Operating System: ALL

Wireless Profile: Multiple SSIDs can be configured. Proxy Auto-Config File URL will be used for early (pre 5.x) versions of Android.

SSID Name: BYOD-Dot1x

Proxy Auto-Config File URL:

Proxy Host/IP:

Proxy Part:

Security: WPA2 Enterprise

Allowed Protocol: TLS

Certificate Template: BYOD_Certificate_template

Optional Settings

Windows Settings

Authentication Mode: User

profile will be applied globally (i.e. to all subsequent profiles). Android 5.0 or above. used for early (pre 5.x) versions of Android.

cate Templ...

Certificate_template

Windows. زاهج ليعمل ريفوت جهن عاشن. 4. ةوطخل

ماظن دح . ليعملا دادم | سايس > ليعملا دادم | BYOD > لمعلا زكارم > ISE | لى لقتنا ةوطخل ايف هؤاشن مت يذلا NSP و WinSPWizard 3.0.0.2 دح. Windows ALL نوكل ليعغشتلا ةقباسلا.

Cisco ISE Work Centers - BYOD Evaluation Mode 46 Days

Overview Identities Identity Groups Network Devices Ext Id Sources **Client Provisioning** Portals & Components Policy Elements Policy Sets Reports More

Client Provisioning Policy

Resources

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
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 WinSPWizard 3.0.0.2 And WirelessNSP
MAC OS	If Any	and Mac OSX	and Condition(s)	then CiscoTemporalAgentOSX 4.8.00176 And MacOsXSPWizard

Save Reset

BYOD. ةزهجك ةلجسمل ريفغ ةزهجال ليوخت فيرعت فلم عاشن. 5. ةوطخل

صيصخت تافل م > ضيوفتلا حجئاتنلا > سايسلا رصانع > سايسلا ISE | لى لقتنا ةقباسلا > ضيوفتلا.

لوصلوا يف مكحتلا ةمئاق مسا ديدحتب مق. يلصألا بلاطلا ديوت دح، ةكرتشم ةمهم تحت ةيكلساللا ةيلحلم ةكبشلا يف مكحتلا رصنع لىع هؤاشن مت يذلا هيحوتلا ةداعل (ACL) BYOD لخدم عاشن كنكمي. يضارتفالا لخدملا مادختسا متي انه. ةقباسلا لىع رقناو تانوكملا و تاباوبلا > BYOD > لمعلا زكارم > ISE | لى لقتنا. صصخم.

Dictionarys Conditions **Results**

Authentication >

Authorization >

Authorization Profiles

Downloadable ACLs

Profiling >

Posture >

Client Provisioning >

* Name BYOD_Wireless_Redirect

Description

* Access Type ACCESS_ACCEPT

Network Device Profile Cisco

Service Template

Track Movement

Agentless Posture

Passive Identity Tracking

Common Tasks

Web Redirection (CWA, MDM, NSP, CPP)

Native Supplicant Provisioning ACL BYOD-Initial Value BYOD Portal (default)

ةداهش فيرعت فلم عاشنإ. 6 ةوطخلا

فيرعت فلم عاشنإ. ةداهشلا فيرعت فلم > ةيچراخلا ةيوهلا رداصم > ةرادا ISE > لىل لقتنا
يضرارتفالا ةداهشلا فيرعت فلم مادختسا وأ ديدج ةداهش

Identities Groups **External Identity Sources** Identity Source Sequences Settings

External Identity Sources

Certificate Authentication F

cert_profile

Preloaded_Certificate_Prof

Active Directory

ADJoints

LDAP

ODBC

RADIUS Token

RSA SecurID

SAML Id Providers

Social Login

Certificate Authentication Profiles List > cert_profile

Certificate Authentication Profile

* Name cert_profile

Description

Identity Store [not applicable]

Use Identity From Certificate Attribute Subject - Common N: Any Subject or Alternative Name Attributes in the Certificate (for Active Directory Only)

Match Client Certificate Against Certificate In Identity Store Never Only to resolve identity ambiguity Always perform binary comparison

في هؤاشنإ مت يذلا ةداهشلا فيرعت فلم ددحو ةيوه رداصم لس لس عاشنإب مق. 7 ةوطخلا
موقى ام دنع بولطم اذهو. يضرارتفالا ةداهشلا فيرعت فلم مادختسا وأ ةقباسلا ةوطخلا
لم الكا لوصولا لىل لوصولل BYOD لىجست دعب EAP-TLS ذيفنتب نومدختسملا

Identity Source Sequences List > For_Teap

Identity Source Sequence

Identity Source Sequence

* Name

BYOD_id_Store

Description

Certificate Based Authentication



Select Certificate Authentication Profile

cert_profile



Authentication Search List

A set of identity sources that will be accessed in sequence until first authentication succeeds

Available	Selected
Internal Endpoints	Internal Users
Guest Users	ADJoioint

ليوخت جهنو ةقداصم جهنو جهنو ةعومجم عاشنإ. 8 ةوطخل

اهظافو جهنو ةعومجم عاشنإ. تاسايسلا تاعومجم > ةسايسلا > ISE > لقتنا

ةقباسلا ةوطخل يف هؤاشنإ مت يذلا ةيوهلا ردصم لس لسست ددحو ةقداصم جهنو عاشنإ مق

نيتسايس عاشنإ بجي. ليوخت ةسايس عاشنإ

هيجوتلا ةداعإ فيرعت فلم اعاطعإ. اهيف BYOD ليجست متي مل يتلا ةزهجالل ةبسنلاب. 1. 5 ةوطخل يف هؤاشنإ مت يذلا

ةزهجالل هذه لىل لمكلا لوصول حنم. EAP-TLS ب موقتو ةلجسم BYOD نوكت يتلا ةزهجالل. 2.

Authentication Policy (1)

Status	Rule Name	Conditions	Use
+	Search		
+	Default		BYOD_id_Store > Options

> Authorization Policy - Local Exceptions

> Authorization Policy - Global Exceptions

Authorization Policy (3)

Status	Rule Name	Conditions	Results	Profiles	Security Groups
+	Search				
+	Full_Access	AND Network Access-EapAuthentication EQUALS EAP-TLS EndPoints-BYODRegistration EQUALS Yes	PermitAccess x		Select from list
+	BYOD_Redirect	EndPoints-BYODRegistration EQUALS Unknown	BYOD_Wireless_Redire... x		Select from list

WLC) ةيكل سلال LAN ةكبش في مكحت ال ةدحو نيوكت

WLC لى رADIUS م داخ نيوكت 1. ةوطخ ال

ةقداصم ال > AAA > RADIUS > نيأت ال لى لقتنا

Security

RADIUS Authentication Servers > Edit

Server Index: 7

Server Address(Ipv4/Ipv6): 10.106.32.119

Shared Secret Format: ASCII

Shared Secret: [REDACTED]

Confirm Shared Secret: [REDACTED]

Key Wrap: (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

Apply Cisco ISE Default settings:

Apply Cisco ACA Default settings:

Port Number: 1812

Server Status: Enabled

Support for CoA: Enabled

Server Timeout: 5 seconds

Network User: Enable

Management: Enable

Management Retransmit Timeout: 5 seconds

Tunnel Proxy: Enable

Realm List: [Realm List](#)

PAC Provisioning: Enable

IPSec: Enable

Cisco ACA: Enable

ةب س ا ح م ل ا > RADIUS > AAA > ن ي م أ ت ل ا ل ا ل ق ت ن ا

The screenshot shows the Cisco Security configuration interface for RADIUS Accounting Servers. The left sidebar contains a navigation tree with categories like AAA, Local EAP, and Access Control Lists. The main content area is titled 'RADIUS Accounting Servers > Edit' and shows configuration for server index 7. Key fields are highlighted with red boxes: 'Server Address(Ipv4/Ipv6)' is set to 10.106.32.119, and 'Port Number' is set to 1813. Other visible settings include Shared Secret Format (ASCII), Shared Secret (masked), Confirm Shared Secret (masked), Server Status (Enabled), Server Timeout (5 seconds), Network User (checked), Management (unchecked), Tunnel Proxy (unchecked), PAC Provisioning (unchecked), IPsec (unchecked), and Cisco ACA (unchecked).

ا ل و ط خ ل ا 2. ن ي و ك ت Dot1x SSID.

The screenshot shows the Cisco WLANs configuration interface for a profile named 'BYOD-Dot1x'. The left sidebar shows the 'WLANs' category. The main content area is titled 'WLANs > Edit 'BYOD-Dot1x'' and has tabs for General, Security, QoS, Policy-Mapping, and Advanced. The 'General' tab is active, and several fields are highlighted with red boxes: 'SSID' is set to BYOD-Dot1x, 'Status' is checked (Enabled), and 'Interface/Interface Group(G)' is set to management. Other visible settings include Profile Name (BYOD-Dot1x), Type (WLAN), Security Policies ([WPA2][Auth(802.1X)]), Radio Policy (All), Multicast Vlan Feature (unchecked), Broadcast SSID (checked), NAS-ID (none), and Lobby Admin Access (unchecked).

WLANs

- WLANs
- Advanced

WLANs > Edit 'BYOD-Dot1x'

General Security **QoS** Policy-Mapping Advanced

Layer 2 Layer 3 AAA Servers

Layer 2 Security

Security Type

MAC Filtering

WPA2+WPA3 Parameters

Policy WPA2 WPA3

Encryption Cipher CCMP128(AES) CCMP256 GCMP128 GCMP256

Fast Transition

Fast Transition

Over the DS

Reassociation Timeout Seconds

Protected Management Frame

PMF

Authentication Key Management

802.1X-SHA1 Enable

WLANs

- WLANs
- Advanced

WLANs > Edit 'BYOD-Dot1x'

General Security **QoS** Policy-Mapping Advanced

Layer 2 Layer 3 **AAA Servers**

Select AAA servers below to override use of default servers on this WLAN

RADIUS Servers

RADIUS Server Overwrite interface Enabled

Apply Cisco ISE Default Settings Enabled

Authentication Servers

Accounting Servers

Server	Enabled	IP:Port	Enabled	IP:Port
Server 1	<input checked="" type="checkbox"/>	IP:10.106.32.119, Port:1812	<input checked="" type="checkbox"/>	IP:10.106.32.119, Port:1813
Server 2	<input type="checkbox"/>	None	<input type="checkbox"/>	None
Server 3	<input type="checkbox"/>	None	<input type="checkbox"/>	None
Server 4	<input type="checkbox"/>	None	<input type="checkbox"/>	None
Server 5	<input type="checkbox"/>	None	<input type="checkbox"/>	None
Server 6	<input type="checkbox"/>	None	<input type="checkbox"/>	None

EAP Parameters

Enable

Authorization ACA Server

Accounting ACA Server

Enabled

Enabled

Server

Server

CISCO MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

WLANs > Edit 'BYOD-Dot1x'

General Security QoS Policy-Mapping **Advanced**

Allow AAA Override Enabled

Coverage Hole Detection Enabled

Enable Session Timeout 1800
Session Timeout (secs)

Aironet IE Enabled

Diagnostic Channel Enabled

Override Interface ACL IPv4 None IPv6 None

Layer2 Acl None

URL ACL None

P2P Blocking Action Disabled

Client Exclusion Enabled 180
Timeout Value (secs)

Maximum Allowed Clients 0

Static IP Tunneling Enabled

Wi-Fi Direct Clients Policy Disabled

Maximum Allowed Clients Per AP Radio 200

Clear HotSpot Configuration Enabled

DHCP

DHCP Server Override

DHCP Addr. Assignment Required

Management Frame Protection (MFP)

MFP Client Protection Optional

DTIM Period (in beacon intervals)

802.11a/n (1 - 255) 1

802.11b/g/n (1 - 255) 1

NAC

NAC State ISE NAC

Load Balancing and Band Select

Client Load Balancing

Client Band Select

Passive Client

دودح لوصول وري فو تل هي جوتال اداع ال لوصول ا ي ف م كحتال ا عمئاق ن ي و ك ت ب مق 3. ة و ط خ ل ل زاهج ل ديوزت ل

- (يضا رتفا لكش ب DHCP ب حامسالا متي) DNS و DHCP لى ل UDP رورم ة ك رح ب حامسالا
- ب لاصتالا ISE.
- ى ر خ ال رورم ل ة ك رح ض فر .

فل م ي ف اي و دي (ACL) لوصول اب م كحتال ا عمئاق ة م س ت ب تم مق مسا ي ا و ا (BYOD-Initial :م سالا ل ي و خ ت ل ل ف ي ر ع ت

CISCO MONITOR WLANs CONTROLLER WIRELESS **SECURITY** MANAGEMENT COMMANDS HELP FEEDBACK

Security

Access Control Lists > Edit

General

Access List Name BYOD-Initial

Deny Counters 0

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	Any	Any	Any	0
2	Permit	0.0.0.0 / 0.0.0.0	10.106.32.119 / 255.255.255.255	Any	Any	Any	Any	Any	0
3	Permit	10.106.32.119 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	0
4	Deny	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	0

ة ح ص ل ل ن م ق ق ح ت ل ل ا

ة ق د ا ص م ل ق ف د ت ن م ق ق ح ت ل ل ا

Live Logs Live Sessions

Misconfigured Suppliants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Counter
0	0	1	0	0

Refresh: Never | Show: Latest 20 records | Within: Last 5 minutes

Refresh | Reset Repeat Counts | Export To | Filter

Time	Status	Details	Repea...	Identity	Endpoint ID	Identity Group	Authenti...	Authorization Policy	Authorization Profiles	Ei
Nov 29, 2020 11:13:47.4...	●		0	dot1xuser	50:3E:AA:E4:8...		Wireless >...	Wireless >> Full_Access	PermitAccess	W
Nov 29, 2020 11:13:47.2...	■			dot1xuser	50:3E:AA:E4:8...	RegisteredDevices	Wireless >...	Wireless >> Full_Access	PermitAccess	W
Nov 29, 2020 11:10:57.9...	■			dot1xuser	50:3E:AA:E4:8...	Profiled	Wireless >...	Wireless >> BYOD_Redirect	BYOD_Wireless_Redirect	TF

مسامدختساب PEAP ةقداصم ءارجاب مدختسمل موقبي، ةرم لوأل لوخدلا ليجست دنع 1. BYOD. هيجوتلا ةداعإ ةدعاق هيجوت ةداعإ مدختسمل موقبي، ISE ةلاح يف رورم ةملك و مدختسم

Cisco ISE

Overview

Event	5200 Authentication succeeded
Username	dot1xuser
Endpoint Id	50:3E:AA:E4:81:B6
Endpoint Profile	TP-LINK-Device
Authentication Policy	Wireless >> Default
Authorization Policy	Wireless >> BYOD_Redirect
Authorization Result	BYOD_Wireless_Redirect

Authentication Details

Source Timestamp	2020-11-29 11:10:57.955
Received Timestamp	2020-11-29 11:10:57.955
Policy Server	isee30-primary
Event	5200 Authentication succeeded
Username	dot1xuser
User Type	User
Endpoint Id	50:3E:AA:E4:81:B6
Calling Station Id	50-3e-aa-e4-81-b6
Endpoint Profile	TP-LINK-Device
Authentication Identity Store	Internal Users
Identity Group	Profiled
Audit Session Id	0a6a21b20000009a5fc3d3ad
Authentication Method	dot1x
Authentication Protocol	PEAP (EAP-MSCHAPv2)
Service Type	Framed
Network Device	WLC1

2. EAP-ذيفنتب نأل موقيو لجمسمل زاهال الى لم دختسمل ةفاضل متت ، BYOD ليجست دع ب .
لمالك لوصول الى لصلح و TLS.

Overview

Event	5200 Authentication succeeded
Username	dot1xuser
Endpoint Id	50:3E:AA:E4:81:B6 ⓘ
Endpoint Profile	Windows10-Workstation
Authentication Policy	Wireless >> Default
Authorization Policy	Wireless >> Full_Access
Authorization Result	PermitAccess

Authentication Details

Source Timestamp	2020-11-29 11:13:47.246
Received Timestamp	2020-11-29 11:13:47.246
Policy Server	isee30-primary
Event	5200 Authentication succeeded
Username	dot1xuser
Endpoint Id	50:3E:AA:E4:81:B6
Calling Station Id	50-3e-aa-e4-81-b6
Endpoint Profile	Windows10-Workstation
Identity Group	RegisteredDevices
Audit Session Id	0a6a21b20000009a5fc3d3ad
Authentication Method	dot1x
Authentication Protocol	EAP-TLS
Service Type	Framed
Network Device	WLC1

يې ةصاخلا ةزهجالا ةباوب نم ققحتلا

ىلع عالطالا كنكمي . دامتعالا تانايب مادختساب لوخدلا لجسو MyDevices لخدم ىلى لقتنا ليجستلا ةلاحو زاهاجال مسا .

MyDevices ةباوبل URL ناوع عاشن كنكمي .

تادادع | > يې ةصاخلا ةزهجالا لخدم > تانوكملاو لخدملا > BYOD > لمعلا زكارم > ISE ىلى لقتنا لمكلا لءوملا URL ناوع لخدأ م ث لوخدلا ليجست

Manage Devices
 Need to add a device? Select **Add**. Was your device lost or stolen? Select your device from the list to manage it.
 Number of registered devices:2/5

Add **Refresh**

MAC Address...

Lost **Stolen** **Edit** **PIN Lock** **Full Wipe** **Unenroll** **Reinstate** **Delete**

<input type="checkbox"/>	MAC Address	Device Name	Description	Status
<input type="checkbox"/>	50:3E:AA:E4:81:B6	MyWindows_Device		Registered

اهحال صإو ءاطخأل فاشكتسا

ةماع تامولعم

PSN - دقع ىلع ءاطخأل احي حصت ي ف هذه ISE تانوكم نيكت مت بجي ، BYOD ءي لمعل ءبسن لباب
 ise-psc.log و filesguest.log فدهل لجلس ال . SCEP لجلس لئاسر -scep

ise-psc.log - فدهل لجلس ال فلم . ءيساسأل ءينبل لئاسر نع لوؤسم ال نوكم ال -client-webApp
 psc.log

portal-web-action- فدهل لجلس ال فلم . ليمع ال دادم ءسايس ءجالعم نع لوؤسم ال نوكم ال -
 guest.log.

guest.log - فدهل لجلس ال فلم . لخدم لب ءلصل تاذ ءادخال ءي مج -ءبواب ال

portal-session-manager - فدهل لجلس ال تافلم - ءسلجب ءقلعتم ال ءاطخأل احي حصت لئاسر -
 gues.log - لخدم ال لمع

CA-service- فدهل لجلس ال تافلم - قدصم ال ءجرم ال ءمدخ لئاسر -
 misc.log

CA-Service-CERT- فدهل لجلس ال تافلم - ءداهش لئاسر -
 misc.log و caservice.log

admin-ca- فدهل لجلس ال تافلم - ءمدخ لوؤسم لئاسر -
 caservice-misc.log

certprovisiingportal- فدهل لجلس ال تافلم - ءداهش ال ري فوت ءبواب لئاسر -
 ise-psc.log

NSF- فدهل لجلس ال تافلم - NSF ءلصل تاذ لئاسر ال -
 ise-psc.log

NSF-Session- فدهل لجلس ال تافلم - ءقؤم ال نيخت ال ءركاذب ءقلعتم لئاسر ءسلج -
 ise-psc.log

Runtime-AAA- فدهل لجلس ال فلم . ليغش ال تقو ءادخال ءي مج -
 prrt-server.log.

: ليمع ال بناج نم تالجلس لل ءبسن لباب

نوع ثحبا
C:\Users\

لمعمل لجس ليجت

ISE تالجس

داعم URL ناونعو اههيجوت داعم (ACL) لوصولو يف مكحت عمئاق عم لولوال لوصولو لوبق
BYOD لخدمل هيجوتال

Prrt-server.log-

```
Radius, 2020-12-02 05:43:52, 395, DEBUG, 0x7f433e6b8700, cntx=0008590803, sesn=isee30-  
primary/392215758/699, CPMSessionID=0a6a21b20000009f5fc770c7, user=dotlxuser, CallingStationID=50-  
3e-aa-e4-81-b6, RADIUS PACKET:: Code=2(AccessAccept) Identifier=254 Length=459 [1] User-Name -  
value: [dotlxuser] [25] Class - value: [****] [79] EAP-Message - value: [ñ [80] Message-  
Authenticator - value: [.2{wëbÜ"Åp05<Z] [26] cisco-av-pair - value: [url-redirect-acl=BYOD-  
Initial] [26] cisco-av-pair - value: [url-  
redirect=https://10.106.32.119:8443/portal/gateway?sessionId=0a6a21b20000009f5fc770c7&portal=7f8  
ac563-3304-4f25-845d-be9faac3c44f&action=nsp&token=53a2119de6893df6c6fca25c8d6bd061] [26] MS-  
MPPE-Send-Key - value: [****] [26] MS-MPPE-Recv-Key - value: [****] ,RADIUSHandler.cpp:2216
```

يل WLC ةطساوب ههيجوت ديع أو بيوع قوم يلى للاق تالال ئائالال مدخت سملال لواحي ام دنع
ISE هيجوت ةداعال URL ناونع

Guest.log -

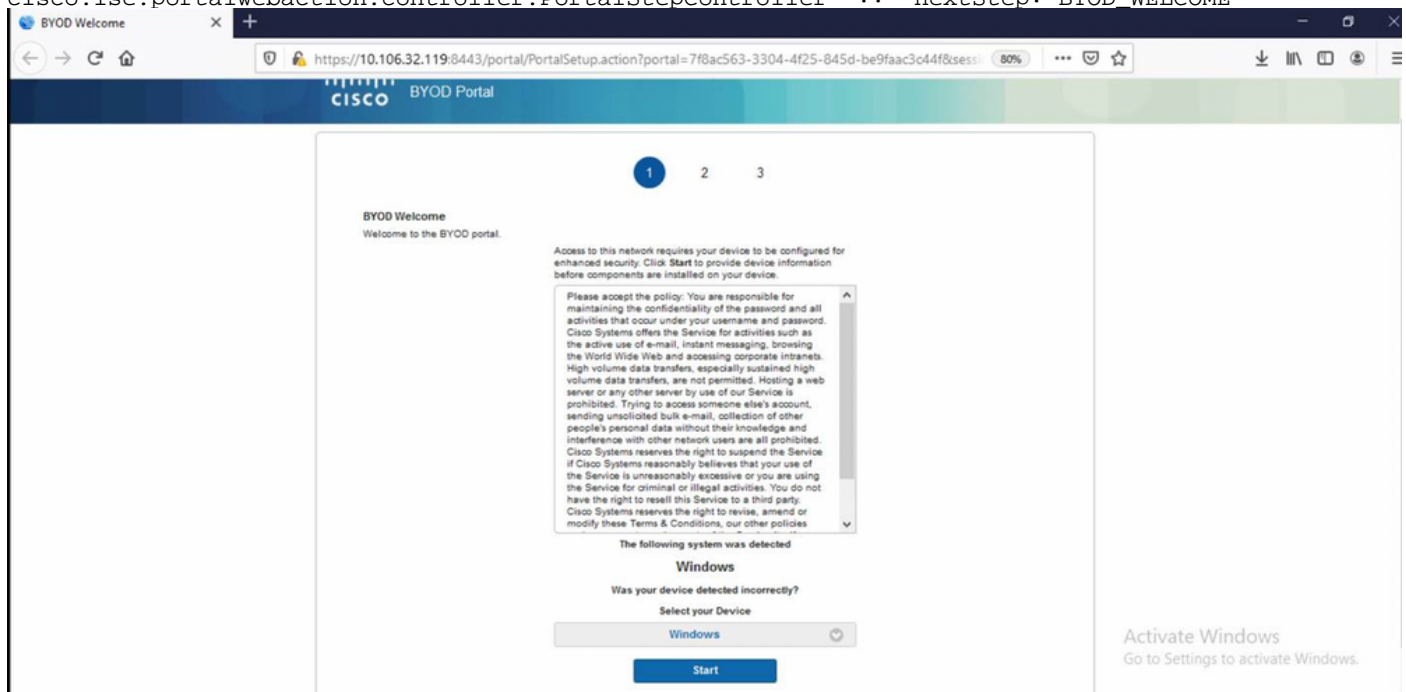
```
2020-12-02 05:43:58, 339 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-5][  
com.cisco.ise.portal.Gateway -:- Gateway Params (after update):  
redirect=www.msftconnecttest.com/redirect client_mac=null daysToExpiry=null ap_mac=null  
switch_url=null wlan=null action=nsp sessionId=0a6a21b20000009f5fc770c7 portal=7f8ac563-3304-  
4f25-845d-be9faac3c44f isExpired=null token=53a2119de6893df6c6fca25c8d6bd061 2020-12-02  
05:43:58, 339 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-5][  
cisco.ise.portalwebaction.utils.RadiusSessionUtil -:- sessionId=0a6a21b20000009f5fc770c7 :  
token=53a2119de6893df6c6fca25c8d6bd061 2020-12-02 05:43:58, 339 DEBUG [https-jsse-nio-  
10.106.32.119-8443-exec-5][ cisco.ise.portalwebaction.utils.RadiusSessionUtil -:- Session  
token successfully validated. 2020-12-02 05:43:58, 344 DEBUG [https-jsse-nio-10.106.32.119-8443-  
exec-5][ cisco.ise.portal.util.PortalUtils -:- UserAgent : Mozilla/5.0 (Windows NT 10.0;  
Win64; x64; rv:83.0) Gecko/20100101 Firefox/83.0 2020-12-02 05:43:58, 344 DEBUG [https-jsse-nio-  
10.106.32.119-8443-exec-5][ cisco.ise.portal.util.PortalUtils -:- isMozilla: true 2020-12-02  
05:43:58, 344 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-5][ com.cisco.ise.portal.Gateway -  
:- url: /portal/PortalSetup.action?portal=7f8ac563-3304-4f25-845d-  
be9faac3c44f&sessionId=0a6a21b20000009f5fc770c7&action=nsp&redirect=www.msftconnecttest.com%2Fre  
direct 2020-12-02 05:43:58, 355 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-7][  
cisco.ise.portalwebaction.controller.PortalFlowInterceptor -:- start guest flow interceptor...  
2020-12-02 05:43:58, 356 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-7][  
cisco.ise.portalwebaction.actions.BasePortalAction -:- Executing action PortalSetup via request  
/portal/PortalSetup.action 2020-12-02 05:43:58, 356 DEBUG [https-jsse-nio-10.106.32.119-8443-  
exec-7][ cisco.ise.portalwebaction.actions.PortalSetupAction -:- executeAction... 2020-12-02  
05:43:58, 360 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-7][  
cisco.ise.portalwebaction.actions.BasePortalAction -:- Result from action, PortalSetup: success  
2020-12-02 05:43:58, 360 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-7][  
cisco.ise.portalwebaction.actions.BasePortalAction -:- Action PortalSetup Complete for request  
/portal/PortalSetup.action 2020-12-02 05:43:58, 360 DEBUG [https-jsse-nio-10.106.32.119-8443-  
exec-7][ cpm.guestaccess.flowmanager.processor.PortalFlowProcessor -:- Current flow step:  
INIT, otherInfo=id: 226ea25b-5e45-43f5-b79d-fb59cab96def 2020-12-02 05:43:58, 361 DEBUG [https-  
jsse-nio-10.106.32.119-8443-exec-7][ cpm.guestaccess.flowmanager.step.StepExecutor -:- Getting  
next flow step for INIT with TranEnum=PROCEED 2020-12-02 05:43:58, 361 DEBUG [https-jsse-nio-
```



```

10.106.32.119-8443-exec-7[] cpm.guestaccess.flowmanager.step.StepExecutor -:- StepTran for
Step=INIT=> tranEnum=PROCEED, toStep=BYOD_WELCOME 2020-12-02 05:43:58,361 DEBUG [https-jsse-nio-
10.106.32.119-8443-exec-7[] cpm.guestaccess.flowmanager.step.StepExecutor -:- Find Next
Step=BYOD_WELCOME 2020-12-02 05:43:58,361 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-7[]
cpm.guestaccess.flowmanager.step.StepExecutor -:- Step : BYOD_WELCOME will be visible! 2020-12-
02 05:43:58,361 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-7[]
cpm.guestaccess.flowmanager.step.StepExecutor -:- Returning next step =BYOD_WELCOME 2020-12-02
05:43:58,362 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-7[]
cpm.guestaccess.flowmanager.adaptor.PortalUserAdaptorFactory -:- Looking up Guest user with
uniqueSubjectId=5f5592a4f67552b855ecc56160112db42cf7074e 2020-12-02 05:43:58,365 DEBUG [https-
jsse-nio-10.106.32.119-8443-exec-7[]
cpm.guestaccess.flowmanager.adaptor.PortalUserAdaptorFactory -:- Found Guest user 'dotlxuserin
DB using uniqueSubjectID '5f5592a4f67552b855ecc56160112db42cf7074e'. authStoreName in
DB=Internal Users, authStoreGUID in DB=9273fe30-8c01-11e6-996c-525400b48521. DB ID=bab8f27d-
c44a-48f5-9fe4-5187047bffc0 2020-12-02 05:43:58,366 DEBUG [https-jsse-nio-10.106.32.119-8443-
exec-7[] cisco.ise.portalwebaction.controller.PortalStepController -:- +++ updatePortalState:
PortalSession (e0d457d9-a346-4b6e-bcca-5cf29e12dacc) current state is INITIATED and current step
is BYOD_WELCOME 2020-12-02 05:40:35,611 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-6[]
com.cisco.ise.portalSessionManager.PortalSession -:- Setting the portal session state to ACTIVE
2020-12-02 05:40:35,611 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-6[]
cisco.ise.portalwebaction.controller.PortalStepController -:- nextStep: BYOD_WELCOME

```



BYOD بيحرت ةحفص يف ادبل قوف رقنا

```

2020-12-02 05:44:01,926 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-3[]
cisco.ise.portalwebaction.actions.BasePortalAction -:dotlxuser:- Executing action ByodStart via
request /portal/ByodStart.action 2020-12-02 05:44:01,926 DEBUG [https-jsse-nio-10.106.32.119-
8443-exec-3[] cisco.ise.portalwebaction.controller.PortalPreResultListener -:dotlxuser:-
currentStep: BYOD_WELCOME

```

أمة دوجوم BYOD ل ةمزاللا دراومل/اتلمل تناك اذا ام ميقيقت ب ISE موقوي، ةطقنلا هذه دنعو
 BYOD INIT. ةلا ح لىل هسفن نييعت لىل لمعوي ال

```

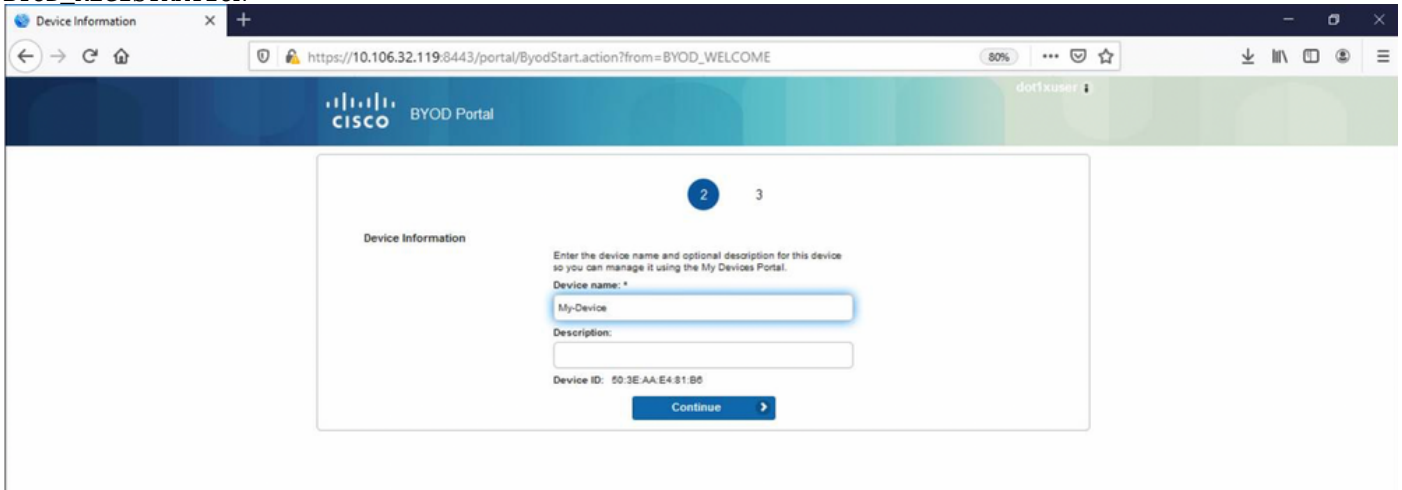
2020-12-02 05:44:01,936 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-3[]
guestaccess.flowmanager.step.guest.ByodWelcomeStepExecutor -:dotlxuser:- userAgent=Mozilla/5.0
(Windows NT 10.0; Win64; x64; rv:83.0) Gecko/20100101 Firefox/83.0, os=Windows 10 (All),
nspStatus=SUCCESS 2020-12-02 05:44:01,936 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-3[]
guestaccess.flowmanager.step.guest.ByodWelcomeStepExecutor -:dotlxuser:- NSP Downloadable
Resource data=>, resource=DownloadableResourceInfo :WINDOWS_10_ALL

```

```

https://10.106.32.119:8443/auth/provisioning/download/a2b317ee-df5a-4bda-abc3-
e4ec38ee188c/WirelessNSP.xml?sessionId=0a6a21b2000009f5fc770c7&os=WINDOWS_10_ALL null null
https://10.106.32.119:8443/auth/provisioning/download/90a6dc9c-4aae-4431-a453-81141ec42d2d/ null
null https://10.106.32.119:8443/auth/provisioning/download/90a6dc9c-4aae-4431-a453-
81141ec42d2d/NetworkSetupAssistant.exe, coaType=NoCoa 2020-12-02 05:44:01,936 DEBUG [https-jsse-
nio-10.106.32.119-8443-exec-3][] cpm.guestaccess.flowmanager.utils.NSPProvAccess -:dotlxuser:-
It is a WIN/MAC! 2020-12-02 05:44:01,936 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-3][]
cpm.guestaccess.flowmanager.step.StepExecutor -:dotlxuser:- Returning next step
=BYOD_REGISTRATION 2020-12-02 05:44:01,950 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-3][]
cisco.ise.portalwebaction.controller.PortalStepController -:dotlxuser:- +++ updatePortalState:
PortalSession (e0d457d9-a346-4b6e-bcca-5cf29e12dacc) current state is ACTIVE and current step is
BYOD_REGISTRATION 2020-12-02 05:44:01,950 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-3][]
cisco.ise.portalwebaction.controller.PortalStepController -:dotlxuser:- nextStep:
BYOD_REGISTRATION

```

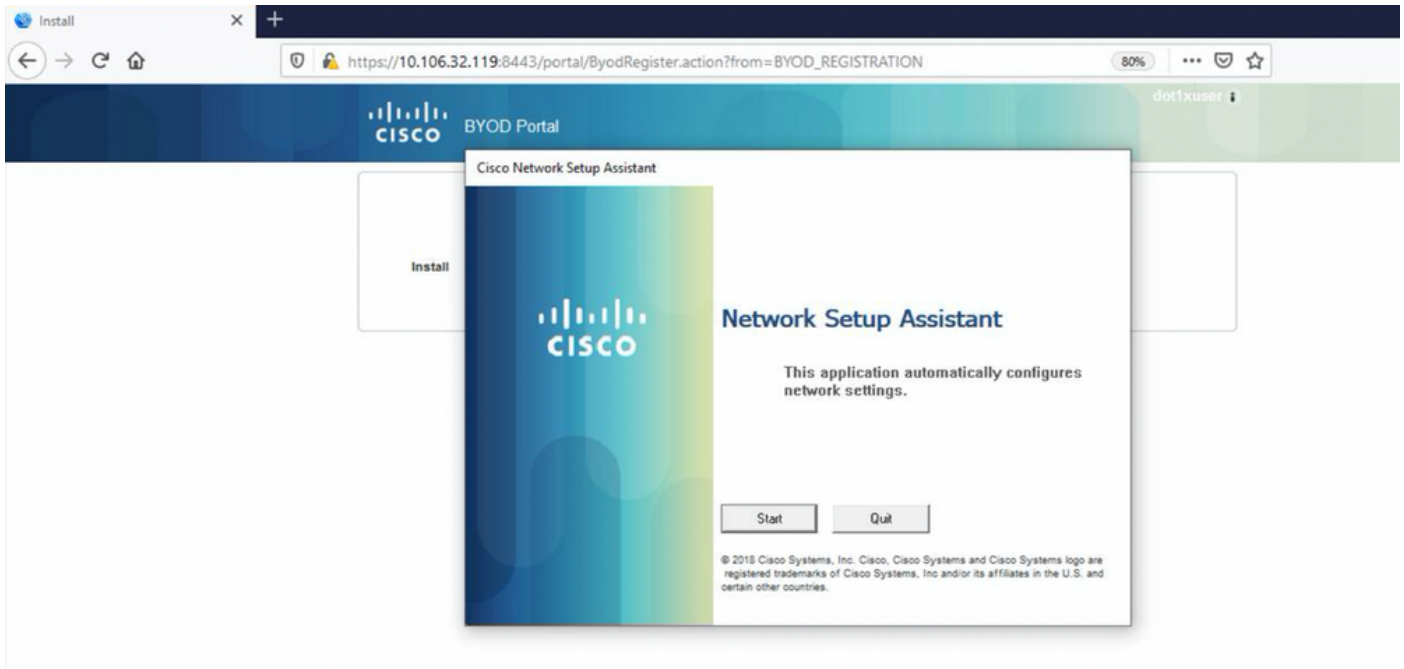


لجس تال ىل ع رقن او زا هج ل م سا ل خ د ا .

```

2020-12-02 05:44:14,682 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][]
cisco.ise.portalwebaction.actions.BasePortalAction -:dotlxuser:- Executing action ByodRegister
via request /portal/ByodRegister.action Request Parameters: from=BYOD_REGISTRATION
token=PZBMFBHX3FBPXT8QF98U717ILNOTD68D device.name=My-Device device.description= 2020-12-02
05:44:14,682 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][]
cisco.ise.portal.actions.ByodRegisterAction -:dotlxuser:- executeAction... 2020-12-02
05:44:14,682 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][]
cisco.ise.portalwebaction.actions.BasePortalAction -:dotlxuser:- Result from action,
ByodRegister: success 2020-12-02 05:44:14,682 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][]
cisco.ise.portalwebaction.actions.BasePortalAction -:dotlxuser:- Action ByodRegister Complete
for request /portal/ByodRegister.action 2020-12-02 05:44:14,683 DEBUG [https-jsse-nio-
10.106.32.119-8443-exec-1][] cpm.guestaccess.apiservices.mydevices.MyDevicesServiceImpl -
:dotlxuser:- Register Device : 50:3E:AA:E4:81:B6 username= dotlxuser idGroupID= aal3bb40-8bff-
11e6-996c-525400b48521 authStoreGUID= 9273fe30-8c01-11e6-996c-525400b48521 nadAddress=
10.106.33.178 isSameDeviceRegistered = false 2020-12-02 05:44:14,900 DEBUG [https-jsse-nio-
10.106.32.119-8443-exec-1][] cpm.guestaccess.flowmanager.step.StepExecutor -:dotlxuser:-
Returning next step =BYOD_INSTALL 2020-12-02 05:44:14,902 DEBUG [https-jsse-nio-10.106.32.119-
8443-exec-1][] cisco.ise.portalwebaction.controller.PortalStepController -:dotlxuser:- +++
updatePortalState: PortalSession (e0d457d9-a346-4b6e-bcca-5cf29e12dacc) current state is ACTIVE
and current step is BYOD_INSTALL 2020-12-02 05:44:01,954 DEBUG [https-jsse-nio-10.106.32.119-
8443-exec-3][] cisco.ise.portalwebaction.controller.PortalFlowInterceptor -:dotlxuser:- result:
success 2020-12-02 05:44:14,969 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-10][]
cisco.cpm.client.provisioning.StreamingServlet -:dotlxuser:- StreamingServlet
URI:/auth/provisioning/download/90a6dc9c-4aae-4431-a453-81141ec42d2d/NetworkSetupAssistant.exe

```

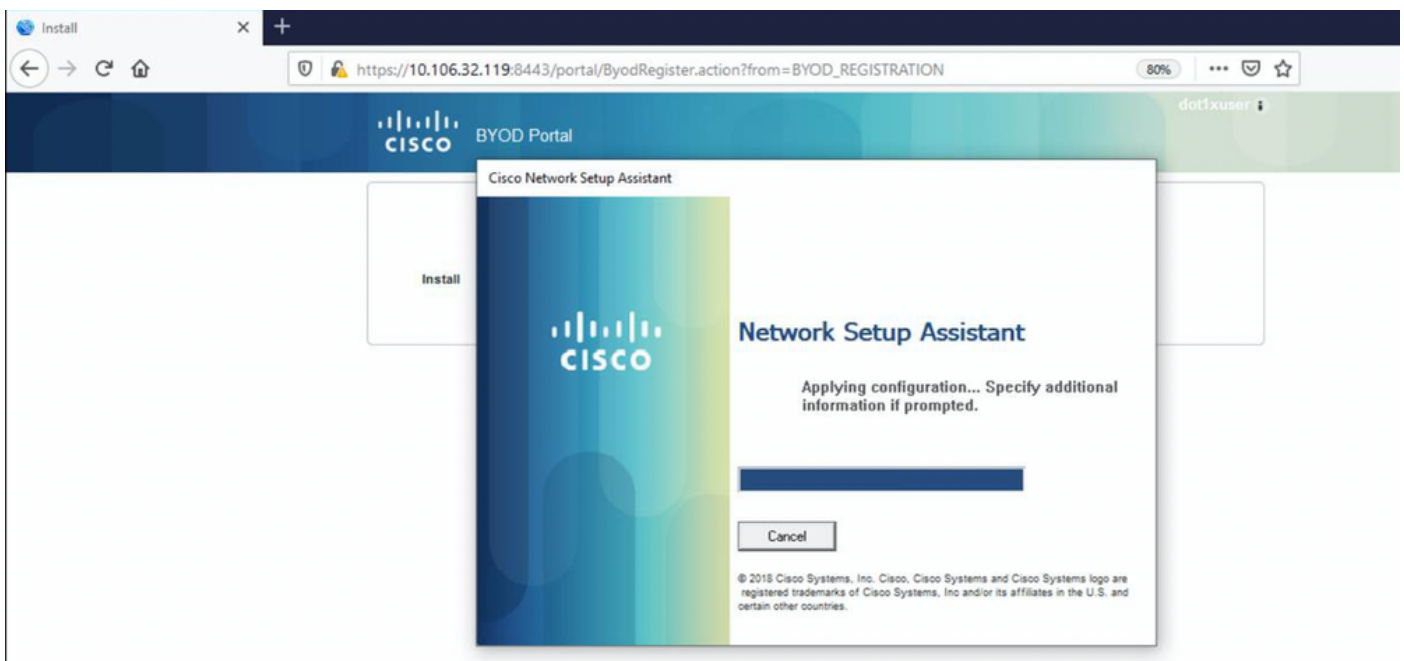


ذفنم ىلع هلېزنت مت يذلا Cisco ISE-NSP.xml نم ىوتحمل خسن يذلا لىم عملا ىلع اتقوم TCP 8905. **spwProfile.xml** م س اب فلم عاشن | متي NSA، ىلع "ءدبل" قوف مدختسم لارقني ام دنع ، نألا

Guest.log -

```
2020-12-02 05:45:03,275 DEBUG [portal-http-service15][[]
cisco.cpm.client.provisioning.StreamingServlet -::- StreamingServlet
URI:/auth/provisioning/download/a2b317ee-df5a-4bda-abc3-e4ec38ee188c/WirelessNSP.xml 2020-12-02
05:45:03,275 DEBUG [portal-http-service15][[] cisco.cpm.client.provisioning.StreamingServlet -::-
Streaming to ip:10.106.33.167 file type: NativeSPProfile file name:WirelessNSP.xml 2020-12-02
05:45:03,308 DEBUG [portal-http-service15][[] cisco.cpm.client.provisioning.StreamingServlet -::-
SPW profile :: 2020-12-02 05:45:03,308 DEBUG [portal-http-service15][[]
cisco.cpm.client.provisioning.StreamingServlet -::-
```

موقيو ةكبش للافيرت فلم نيوكتب NSA موقيو **spwProfile.xml** نم ىوتحمل ةءارق دعب
 URL ناو نع مادختس اب ةءاش ىلع لوصحلل ISE لىل هلاسراو، CSR عاشن اب
<https://10.106.32.119:8443/auth/pkclient.exe>



ise-psc.log-

```
2020-12-02 05:45:11,298 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][  
cisco.cpm.provisioning.cert.CertProvisioningFactory -::::- Found incoming certificate request for  
internal CA. Increasing Cert Request counter. 2020-12-02 05:45:11,331 DEBUG [https-jsse-nio-  
10.106.32.119-8443-exec-1][ cisco.cpm.provisioning.cert.CertProvisioningFactory -::::- Key type  
is RSA, retrieving ScepCertRequestProcessor for caProfileName=ISE Internal CA 2020-12-02  
05:45:11,331 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][  
cisco.cpm.provisioning.cert.CertRequestValidator -::::- Session user has been set to = dotlxuser  
2020-12-02 05:45:11,331 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][  
cisco.cpm.scep.util.ScepUtil -::::- Algorithm OID in CSR: 1.2.840.113549.1.1.1 2020-12-02  
05:45:11,331 INFO [https-jsse-nio-10.106.32.119-8443-exec-1][  
com.cisco.cpm.scep.ScepCertRequestProcessor -::::- About to forward certificate request  
C=IN,ST=Karnataka,L=bangalore,O=cisco,OU=tac,CN=dotlxuser with transaction id n@P~N6E to server  
http://127.0.0.1:9444/caservice/scep 2020-12-02 05:45:11,332 DEBUG [https-jsse-nio-  
10.106.32.119-8443-exec-1][ org.jscep.message.PkiMessageEncoder -::::- Encoding message:  
org.jscep.message.PkcsReq@5c1649c2[transId=4d22d2e256a247a302e900ffa71c35d75610de67,messageType=  
PKCS_REQ,senderNonce=Nonce  
[7d9092a9fab204bd7600357e38309ee8],messageData=org.bouncycastle.pkcs.PKCS10CertificationRequest@  
4662a5b0] 2020-12-02 05:45:11,332 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][  
org.jscep.message.PkcsPkiEnvelopeEncoder -::::- Encrypting session key using key belonging to  
[issuer=CN=Certificate Services Endpoint Sub CA - isee30-primary;  
serial=162233386180991315074159441535479499152] 2020-12-02 05:45:11,333 DEBUG [https-jsse-nio-  
10.106.32.119-8443-exec-1][ org.jscep.message.PkiMessageEncoder -::::- Signing message using  
key belonging to [issuer=CN=isee30-primary.anshsinh.local;  
serial=126990069826611188711089996345828696375] 2020-12-02 05:45:11,333 DEBUG [https-jsse-nio-  
10.106.32.119-8443-exec-1][ org.jscep.message.PkiMessageEncoder -::::- SignatureAlgorithm  
SHA1withRSA 2020-12-02 05:45:11,334 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][  
org.jscep.message.PkiMessageEncoder -::::- Signing  
org.bouncycastle.cms.CMSProcessableByteArray@5aa9dfcc content
```

ca-service.log -

```
2020-12-02 05:45:11,379 DEBUG [CAService-Scep][scep job 4d22d2e256a247a302e900ffa71c35d75610de67  
0x67ee11d5 request] com.cisco.cpm.caservice.CrValidator -::::- performing certificate request  
validation: version [0] subject [C=IN,ST=Karnataka,L=bangalore,O=cisco,OU=tac,CN=dotlxuser] ---  
output omitted--- 2020-12-02 05:45:11,379 DEBUG [CAService-Scep][scep job  
4d22d2e256a247a302e900ffa71c35d75610de67 0x67ee11d5 request validation]  
com.cisco.cpm.caservice.CrValidator -::::- RDN value = dotlxuser 2020-12-02 05:45:11,379 DEBUG  
[CAService-Scep][scep job 4d22d2e256a247a302e900ffa71c35d75610de67 0x67ee11d5 request]  
com.cisco.cpm.caservice.CrValidator -::::- request validation result CA_OK
```

caservice-misc.log -

```
2020-12-02 05:45:11,380 DEBUG [CAService-Scep][scep job 4d22d2e256a247a302e900ffa71c35d75610de67  
0x67ee11d5 request issuance] cisco.cpm.scep.util.ScepUtil -::::- Algorithm OID in CSR:  
1.2.840.113549.1.1.1 2020-12-02 05:45:11,380 DEBUG [CAService-Scep][scep job  
4d22d2e256a247a302e900ffa71c35d75610de67 0x67ee11d5 request issuance]  
com.cisco.cpm.scep.CertRequestInfo -::::- Found challenge password with cert template ID.
```

caservice.log -

```
2020-12-02 05:45:11,380 DEBUG [CAService-Scep][scep job 4d22d2e256a247a302e900ffa71c35d75610de67  
0x67ee11d5 request issuance] cisco.cpm.caservice.util.CaServiceUtil -::::- Checking cache for  
certificate template with ID: e2c32ce0-313d-11eb-b19e-e60300a810d5 2020-12-02 05:45:11,380 DEBUG  
[CAService-Scep][scep job 4d22d2e256a247a302e900ffa71c35d75610de67 0x67ee11d5 request issuance]  
com.cisco.cpm.caservice.CertificateAuthority -::::- CA SAN Extensions = GeneralNames: 1: 50-3E-  
AA-E4-81-B6 2020-12-02 05:45:11,380 DEBUG [CAService-Scep][scep job  
4d22d2e256a247a302e900ffa71c35d75610de67 0x67ee11d5 request issuance]  
com.cisco.cpm.caservice.CertificateAuthority -::::- CA : add SAN extension... 2020-12-02
```

```
05:45:11,380 DEBUG [CAService-Scep][scep job 4d22d2e256a247a302e900ffa71c35d75610de67 0x67ee11d5
request issuance] com.cisco.cpm.caservice.CertificateAuthority -:::::- CA Cert Template name =
BYOD_Certificate_template 2020-12-02 05:45:11,395 DEBUG [CAService-Scep][scep job
4d22d2e256a247a302e900ffa71c35d75610de67 0x67ee11d5 request issuance]
cisco.cpm.caservice.util.CaServiceUtil -:::::- Storing certificate via REST for serial number:
518fa73a4c654df282ffdb026080de8d 2020-12-02 05:45:11,395 INFO [CAService-Scep][scep job
4d22d2e256a247a302e900ffa71c35d75610de67 0x67ee11d5 request issuance]
com.cisco.cpm.caservice.CertificateAuthority -:::::- issuing Certificate Services Endpoint
Certificate: class [com.cisco.cpm.caservice.CaResultHolder] [1472377777]: result: [CA_OK]
subject [CN=dot1xuser, OU=tac, O=cisco, L=bangalore, ST=Karnataka, C=IN] version [3] serial
[0x518fa73a-4c654df2-82ffdb02-6080de8d] validity [after [2020-12-01T05:45:11+0000] before [2030-
11-27T07:35:10+0000]] keyUsages [ digitalSignature nonRepudiation keyEncipherment ]
```

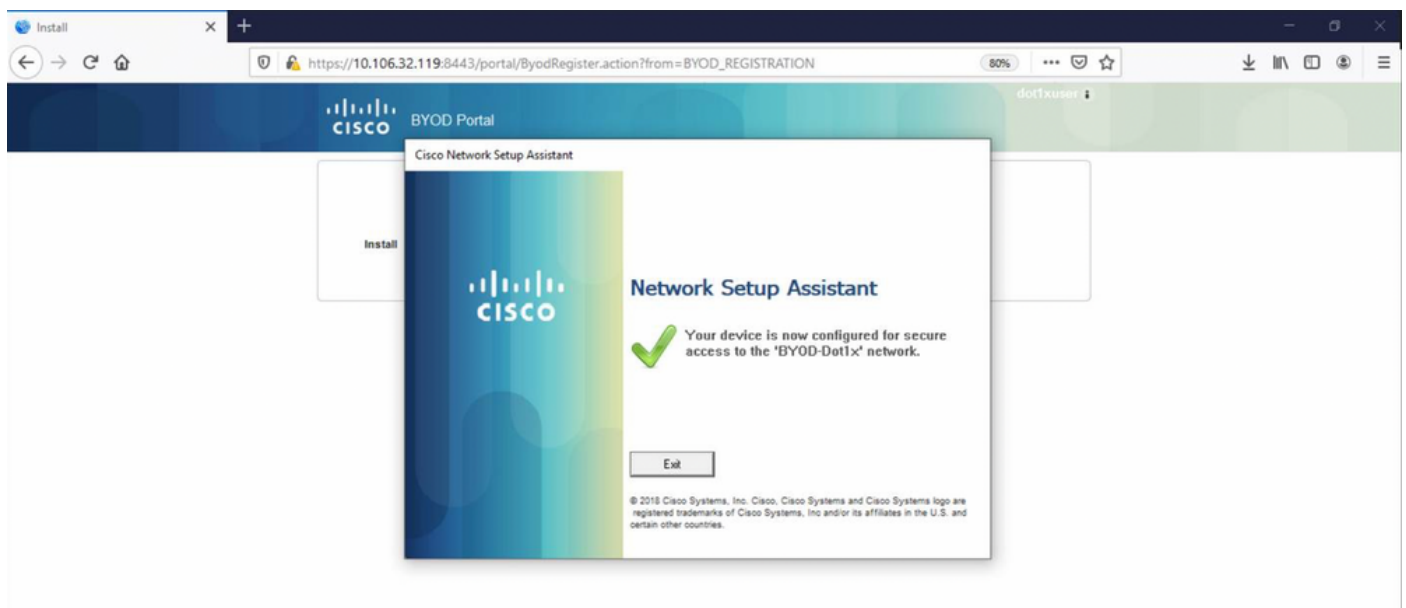
ise-psc.log -

```
2020-12-02 05:45:11,407 DEBUG [AsyncHttpClient-15-9][] org.jscep.message.PkiMessageDecoder -
::::- Verifying message using key belonging to 'CN=Certificate Services Endpoint RA - isee30-
primary'
```

caservice.log -

```
2020-12-02 05:45:11,570 DEBUG [Infra-CAServiceUtil-Thread][]
cisco.cpm.caservice.util.CaServiceUtil -:::::- Successfully stored endpoint certificate.
```

ise-psc.log -



```
2020-12-02 05:45:13,381 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-10][]
cisco.cpm.provisioning.cert.CertProvisioningFactory -:::::- Performing doGetCertInitial found
Scep certificate processor for txn id n@P~N6E 2020-12-02 05:45:13,381 DEBUG [https-jsse-nio-
10.106.32.119-8443-exec-10][] com.cisco.cpm.scep.ScepCertRequestProcessor -:::::- Polling
C=IN,ST=Karnataka,L=bangalore,O=cisco,OU=tac,CN=dot1xuser for certificate request n@P~N6E with
id {} 2020-12-02 05:45:13,385 INFO [https-jsse-nio-10.106.32.119-8443-exec-10][]
com.cisco.cpm.scep.ScepCertRequestProcessor -:::::- Certificate request Complete for
C=IN,ST=Karnataka,L=bangalore,O=cisco,OU=tac,CN=dot1xuser Trx Idn@P~N6E 2020-12-02 05:45:13,596
DEBUG [https-jsse-nio-10.106.32.119-8443-exec-10][]
cisco.cpm.provisioning.cert.CertProvisioningFactory -:::::- BYODStatus:COMPLETE_OTA_NSP
```

لوصول إلى نول صرحي و EAP-TLS م ادخ تساب ى رخأ عق داصم عالم على أدبي ةداهش لا تي بثت دع ب
لم الك لا

prrt-server.log -

Eap,2020-12-02 05:46:57,175,INFO ,0x7f433e6b8700,cntx=0008591342,sesn=isee30-
primary/392215758/701,CPMSessionID=0a6a21b20000009f5fc770c7,CallingStationID=50-3e-aa-e4-81-
b6,EAP: Recv EAP packet, code=Response, identifier=64, type=EAP-TLS, length=166
,EapParser.cpp:150 Radius,2020-12-02
05:46:57,435,DEBUG,0x7f433e3b5700,cntx=0008591362,sesn=isee30-
primary/392215758/701,CPMSessionID=0a6a21b20000009f5fc770c7,user=dotluser,CallingStationID=50-
3e-aa-e4-81-b6,RADIUS PACKET:: Code=2(AccessAccept) Identifier=5 Length=231 [1] User-Name -
value: [dotluser] [25] Class - value: [****] [79] EAP-Message - value: [E [80] Message-
Authenticator - value: [Û(ØyËöžö|kô,.)] [26] MS-MPPE-Send-Key - value: [****] [26] MS-MPPE-Recv-
Key - value: [****] ,RADIUSHandler.cpp:2216

spw (تال جس) لي م عمل تال جس

ف. في رعت الل فلم لي زنت في لي م عمل أدبي.

[Mon Nov 30 03:34:27 2020] Downloading profile configuration... [Mon Nov 30 03:34:27 2020]
Discovering ISE using default gateway [Mon Nov 30 03:34:27 2020] Identifying wired and wireless
network interfaces, total active interfaces: 1 [Mon Nov 30 03:34:27 2020] Network interface -
mac:50-3E-AA-E4-81-B6, name: Wi-Fi 2, type: unknown [Mon Nov 30 03:34:27 2020] Identified
default gateway: 10.106.33.1 [Mon Nov 30 03:34:27 2020] Identified default gateway: 10.106.33.1,
mac address: 50-3E-AA-E4-81-B6 [Mon Nov 30 03:34:27 2020] DiscoverISE - start [Mon Nov 30
03:34:27 2020] DiscoverISE input parameter : strUrl [http://10.106.33.1/auth/discovery] [Mon Nov
30 03:34:27 2020] [HTTPConnection] CrackUrl: host = 10.106.33.1, path = /auth/discovery, user =
, port = 80, scheme = 3, flags = 0 [Mon Nov 30 03:34:27 2020] [HTTPConnection] HttpSendRequest:
header = Accept: /* headerLength = 12 data = dataLength = 0 [Mon Nov 30 03:34:27 2020] HTTP
Response header: [HTTP/1.1 200 OK Location:
https://10.106.32.119:8443/portal/gateway?sessionId=0a6a21b20000009c5fc4fb5e&portal=7f8ac563-
3304-4f25-845d-
be9faac3c44f&action=nsp&token=29354d43962243bcb72193cbf9dc3260&redirect=10.106.33.1/auth/discove
ry [Mon Nov 30 03:34:36 2020] [HTTPConnection] CrackUrl: host = 10.106.32.119, path =
/auth/provisioning/download/a2b317ee-df5a-4bda-abc3-
e4ec38ee188c/WirelessNSP.xml?sessionId=0a6a21b20000009c5fc4fb5e&os=WINDOWS_10_ALL, user = , port
= 8443, scheme = 4, flags = 8388608 Mon Nov 30 03:34:36 2020] parsing wireless connection
setting [Mon Nov 30 03:34:36 2020] Certificate template: [keytype:RSA, keysize:2048,
subject:OU=tac;O=cisco;L=bangalore;ST=Karnataka;C=IN, SAN:MAC] [Mon Nov 30 03:34:36 2020] set
ChallengePwd

ل. في غش الت دي ق WLAN ة مدخ تنك اذا ام لي م عمل ق قحتي.

[Mon Nov 30 03:34:36 2020] WirelessProfile::StartWlanSvc - Start [Mon Nov 30 03:34:36 2020]
Wlansvc service is in Auto mode ... [Mon Nov 30 03:34:36 2020] Wlansvc is running in auto
mode... [Mon Nov 30 03:34:36 2020] WirelessProfile::StartWlanSvc - End [Mon Nov 30 03:34:36
2020] Wireless interface 1 - Desc: [TP-Link Wireless USB Adapter], Guid: [{65E78DDE-E3F1-4640-
906B-15215F986CAA}]... [Mon Nov 30 03:34:36 2020] Wireless interface - Mac address: 50-3E-AA-E4-
81-B6 [Mon Nov 30 03:34:36 2020] Identifying wired and wireless interfaces... [Mon Nov 30
03:34:36 2020] Found wireless interface - [name:Wi-Fi 2, mac address:50-3E-AA-E4-81-B6] [Mon
Nov 30 03:34:36 2020] Wireless interface [Wi-Fi 2] will be configured... [Mon Nov 30 03:34:37
2020] Host - [name:DESKTOP-965F94U, mac addresses:50-3E-AA-E4-81-B6]

- في رعت الل فلم قي بطت في لي م عمل أدبي

[Mon Nov 30 03:34:37 2020] ApplyProfile - Start... [Mon Nov 30 03:34:37 2020] User Id:
dotluser, sessionid: 0a6a21b20000009c5fc4fb5e, Mac: 50-3E-AA-E4-81-B6, profile: WirelessNSP
[Mon Nov 30 03:34:37 2020] number of wireless connections to configure: 1 [Mon Nov 30 03:34:37
2020] starting configuration for SSID : [BYOD-Dot1x] [Mon Nov 30 03:34:37 2020] applying
certificate for ssid [BYOD-Dot1x]

ل. في م عمل تال جس تة داهش.

```
[Mon Nov 30 03:34:37 2020] ApplyCert - Start... [Mon Nov 30 03:34:37 2020] using ChallengePwd
[Mon Nov 30 03:34:37 2020] creating certificate with subject = dotlxuser and subjectSuffix =
OU=tac;O=cisco;L=bangalore;ST=Karnataka;C=IN [Mon Nov 30 03:34:38 2020] Self signed certificate
[Mon Nov 30 03:34:44 2020] Installed [isee30-primary.anshsinh.local, hash: 5b a2 08 1e 17 cb 73
5f ba 5b 9f a2 2d 3b fc d2 86 0d a5 9b ] as rootCA [Mon Nov 30 03:34:44 2020] Installed CA cert
for authMode machineOrUser - Success Certificate is downloaded . Omitted for brevity - [Mon Nov
30 03:34:50 2020] creating response file name C:\Users\admin\AppData\Local\Temp\response.cer
[Mon Nov 30 03:34:50 2020] Certificate issued - successfully [Mon Nov 30 03:34:50 2020]
ScepWrapper::InstallCert start [Mon Nov 30 03:34:50 2020] ScepWrapper::InstallCert: Reading scep
response file [C:\Users\admin\AppData\Local\Temp\response.cer]. [Mon Nov 30 03:34:51 2020]
ScepWrapper::InstallCert GetCertHash -- return val 1 [Mon Nov 30 03:34:51 2020]
ScepWrapper::InstallCert end [Mon Nov 30 03:34:51 2020] ApplyCert - End... [Mon Nov 30 03:34:51
2020] applied user certificate using template id e2c32ce0-313d-11eb-b19e-e60300a810d5
```

يكلسال فيرعت فلم نيوكتب ISE موقري

```
[Mon Nov 30 03:34:51 2020] Configuring wireless profiles... [Mon Nov 30 03:34:51 2020]
Configuring ssid [BYOD-Dotlx] [Mon Nov 30 03:34:51 2020] WirelessProfile::SetWirelessProfile -
Start [Mon Nov 30 03:34:51 2020] TLS - TrustedRootCA Hash: [ 5b a2 08 1e 17 cb 73 5f ba 5b 9f a2
2d 3b fc d2 86 0d a5 9b]
```

صيصخت فلم

```
Wireless interface succesfully initiated, continuing to configure SSID [Mon Nov 30 03:34:51
2020] Currently connected to SSID: [BYOD-Dotlx] [Mon Nov 30 03:34:51 2020] Wireless profile:
[BYOD-Dotlx] configured successfully [Mon Nov 30 03:34:51 2020] Connect to SSID [Mon Nov 30
03:34:51 2020] Successfully connected profile: [BYOD-Dotlx] [Mon Nov 30 03:34:51 2020]
WirelessProfile::SetWirelessProfile. - End [Mon Nov 30 03:35:21 2020]
WirelessProfile::IsSingleSSID - Start [Mon Nov 30 03:35:21 2020] Currently connected to SSID:
[BYOD-Dotlx], profile ssid: [BYOD-Dotlx], Single SSID [Mon Nov 30 03:35:21 2020]
WirelessProfile::IsSingleSSID - End [Mon Nov 30 03:36:07 2020] Device configured successfully.
```

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن ت س م ل ا اذ ه Cisco ت مچرت
م ل ا ل ا اء ن ا ع مچ ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل و
ا م ك ة ق ي ق د ن و ك ت ن ل ة ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت ح 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 ع م ل ا ح ل ا و ه
ي ل ا م اء ا د ع و ج 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 ا ل ا ي ز ي ل ج ن ا ل ا دن ت س م ل ا