

Duo ةقداصم؛ AMP و ةداهشل ةقداصم نيوكت SAML

تايوتحمل

[ةمدقملا](#)

[ةيساسال تابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكملا](#)

[يئانت ىلع تاوطخل نيوكت](#)

[تاقيبطتلا ةيامح جهن عاشنا](#)

[قيبطت ةسايس عاشنا](#)

[FMC نيوكت تاوطخ](#)

[FTD ىلا ةيول ةداهش رشت](#)

[FTD ىلا IDP ةداهش رشت](#)

[SAML SSO نئاك عاشنا](#)

[\(RAVPN\) ةرهظلا ةصاخلا دعبت نع لوصولا ةكبش نيوكت عاشنا](#)

[ةحصللا نم ققحتلا](#)

[اهجالصاو عايطال ءاشكتسا](#)

[.ةداهشل ةقداصم لشف: 1 ةلأسملا](#)

[SAML لشف: 2 رادصلال](#)

ةمدقملا

SAML ةقداصم و ةداهشل ىلا ةدنتسملا ةقداصملا ذيفنتل الاثم دنتسملا اذه حضوي ةيئانتل.

ةيساسال تابلطتملا

يه ليلدل ي ف ةمدختسملا ةزهجال او تاودال:

- Cisco نم FirePOWER (FTD) ديهت دض عافدل
- Firepower (FMC) ةرادا زكرم
- (CA) ةيلخادل ةداهشل حنم ةهج
- Cisco Duo Premier باسح
- Cisco نم DUO ةقداصم ليكو
- Cisco (CSC) نم نمالا ليمعلا

تابلطتملا

ةيلالتل عيضاوملاب ةفرعم كي دل نوكت نأب Cisco ي صوت

- ةيساسأ (VPN) ةيرهاظ ةصاخ ةكبش
- SSL/TLS
- ماعل حاتفم لل ةيساسأ ال ةينبال
- FMC عم ةبرجت
- Cisco Secure Client
- ىلعأ وأ FTD 7.2.0 زمر
- Cisco نم ةقداصم ليكو

ةمدختسم ال تانوكم ال

ةيلات ال ةيدام ال تانوكم ال اوجمارب ال تارادصا ال دن تسم ال اذه في ةدراول تامولعمل دن تست

- Cisco FTD (7.3.1)
- Cisco FMC (7.3.1)
- Cisco Secure Client (5.0.02075)
- Cisco (6.0.1) نم ةيئانث ال ةقداصم ال ليكو
- Mac OS (13.4.1)
- طشن ال لي دل

ةصاخ ةيلمعم ةئيبي في ةدوجوم ال ةزهجال نم دن تسم ال اذه في ةدراول تامولعمل عاشنإ مت تناك اذا. (يضا رتفا) حوسمم نيوكتب دن تسم ال اذه في ةمدختسم ال ةزهجال عيمج تأدب رماي ال لم تحم ال ريثأتلل كمهف نم دكأتف، ليغشت ال ديقت كتكبش

يئانث ىلع تاوطخل نيوكتب

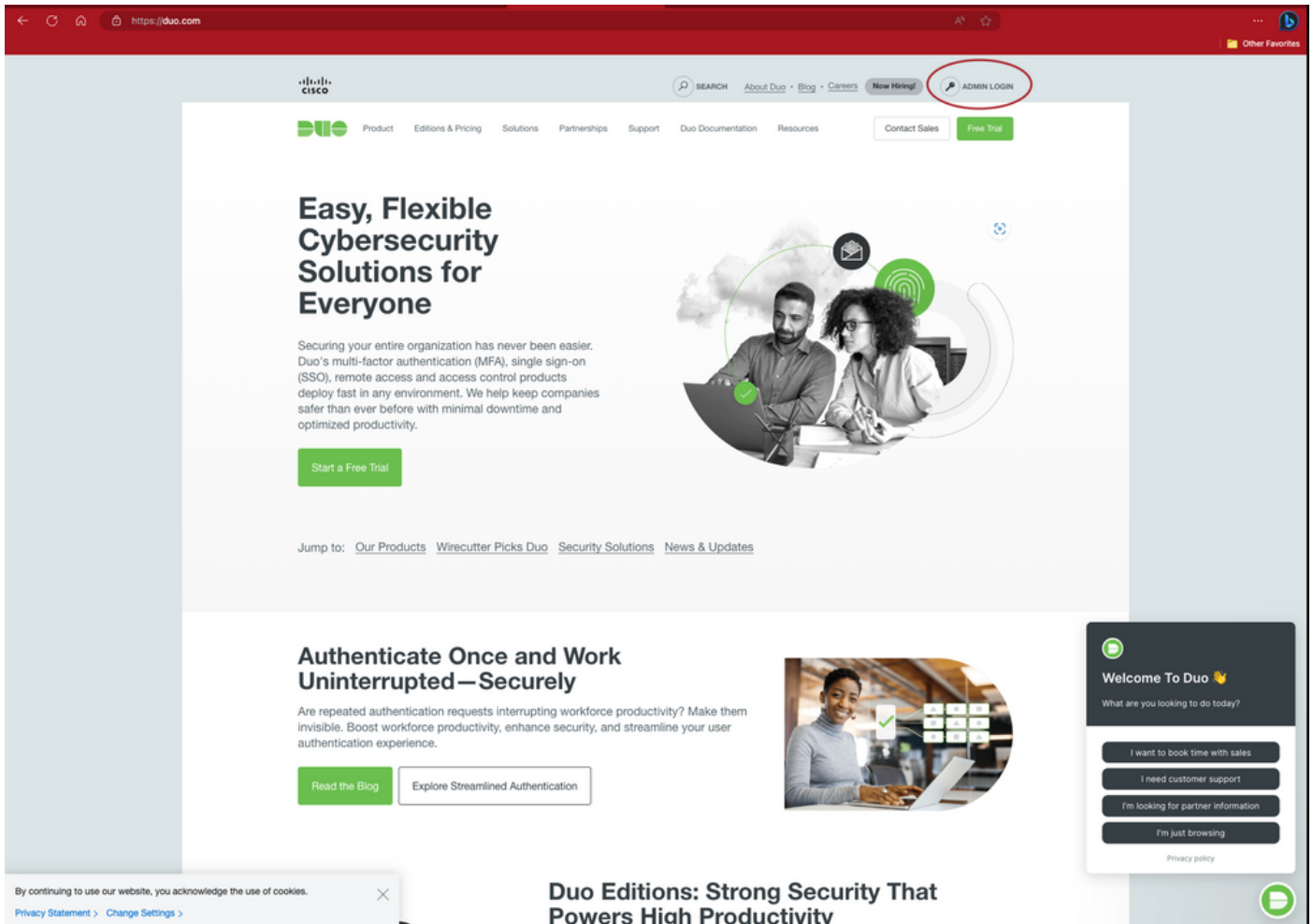
ءدب ال لبق. Cisco DUO (SSO) ل يداخال لوخدل ليچست نيوكتب تاوطخ مسقل ال اذه فصبي ةقداصم ال ليكو وظيفت نم دكأت.



هذه ليلى لىلع طابترال اذه يوتحي، ةقداصم ليكو وظيفت مدع ةلاح في: ريذحت [DUO ةقداصم ليكو وليلد](#). ةمهمل

تاقيبطت ال ةيامح هن عاشنإ

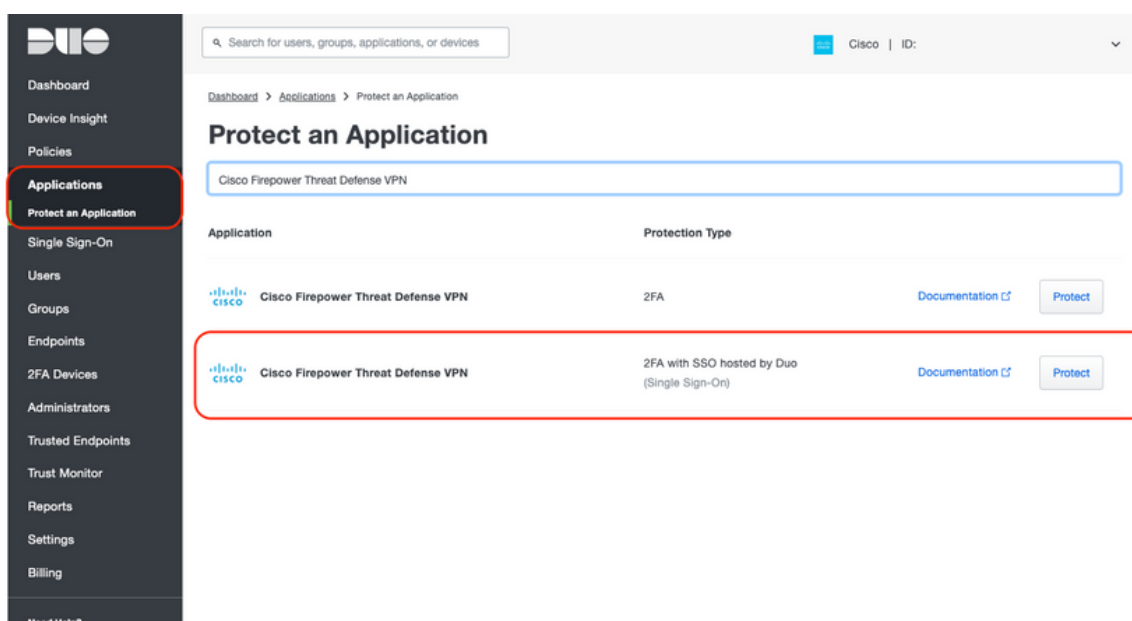
[Cisco Duo](#) طابترال اذه لالخ نم ةرادال ةحول ال لوخدل لچس 1. ةوطخل



Cisco DUO ل ةيسيئرلا ةحفصل

قيبطت ةيماح > تاقيبطت > تامولعمل ءحول ىلإ لقننا 2. ةوطخل

"ةيماح ددحو Cisco Firepower Threat Defense VPN لخدأ، ثحبل طيرش يف



قيبطت ةشاش ةطوق ةيماح

Duo". هفيضتسي يذال SSO عم 2FA طقف ةياملحلا عون عم رايلخا دح

فيعرتلا تانايب تحت هذه URL ناو نع تامولعم خسنا 3: ةوطخلا

- ةيوهلا رفوم نايبك فرعم
- URL ب صاخلا SSO
- جورخلا ليحستل URL ناو نع

See the [Cisco ASA SSO documentation](#) to integrate Duo into your SAML-enabled service provider.

Metadata

Entity ID

Copy

Sign In URL

Copy

Sign Out URL

Copy

اهخسن بولطملا تامولعملال لعل لاثم



ةشاشلا ةطقل نم تاطابترالا فذح مت: ةظحالم

تاليزنتلا نمض ةيوهلا رفوم ةداهش ليزنتل "ةداهشلا ليزنت دح 4: ةوطخلا

ةمدخلا دوزم تامولعم ألما 5: ةوطخلا

FTD لىل لوصولل FQDN مادختسا متي Cisco- نم FirePOWER ةدعاقلا URL ناو نع

قفنلا ةعومجم مسا -لاصتالا فيرعت فلم مسا

قيبطت ةسايس عاشنإ

"نيمدختسملال عيمج لعل ةسايس قيبطت" دح جهنلا نمض قيبطت جهن عاشنإل 1: ةوطخلا
ةروصلال يف حضوم وه امك "ةديج ةسايس عاشنإب مق، وأ" دح م

Policy

Policy defines when and how users will authenticate when accessing this application. Your global policy always applies, but you can override its rules with custom policies.

Group policies

Apply a policy to groups of users

Application policy

Apply a policy to all users

قيبطت ةسايس عاشنإ لعل لاثم

Apply a Policy



Policy

Select a Policy



[Or, create a new Policy](#)

Apply Policy

قېبۇتتە سەياسەت ئاشۇرۇش ئۈچۈن

، نېمەدەك سەياسەت ئاشۇرۇش "ئەقدا سەياسەت ئاشۇرۇش دېھ، بۇغۇرۇم سەياسەت ئاشۇرۇش مەقسەتتە، سەياسەت ئاشۇرۇش ئۈچۈن 2. ئورۇنلاشتۇرۇش، سەياسەت ئاشۇرۇش ئۈچۈن 2FA. "سەياسەت ئاشۇرۇش مەقسەتتە"

Create a New Policy



Policy name

MFA

Users

[New User policy](#)

☒ [Authentication policy](#)

[User location](#)

Devices

[Trusted Endpoints](#)

[Device Health application](#)

[Remembered devices](#)

[Operating systems](#)

[Browsers](#)

[Plugins](#)

Networks

[Authorized networks](#)

[Anonymous networks](#)

Authenticators

[Risk-based factor selection](#)

[Authentication methods](#)

[Duo Mobile app](#)

[Tampered devices](#)

[Screen lock](#)

[Full-disk encryption](#)

[Mobile device biometrics](#)

Authentication policy



Enforce 2FA

Require two-factor authentication or enrollment when applicable, unless there is a superseding policy configured.



Bypass 2FA

Skip two-factor authentication and enrollment, unless there is a superseding policy configured.



Deny access

Deny authentication to all users.

When enabled, this affects all users.

Choose another rule on the left to add to this policy.

Create Policy

قيبطت ةسايس عاشنإ ىلع لاثم

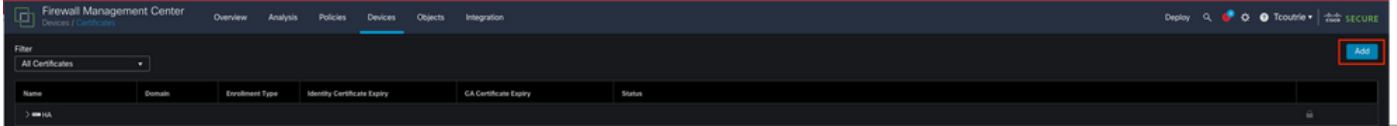
مق م ث. يلاتل راطإلإ ي "ةسايسل قيبطت مادختساب ةسايسل قيبطت ب مق 3. ةوطخلال
DUO تانيوكت ءاهنإل "ظفح ددحو ةحفصلال لفسأ ىلإ يرمرتلابل

FMC نيوكت تاوطخ

FTD إلى ةيوهل ةداهش رشن

ل بق .ةداهشل ةقداصم ل بولطم ال FTD في اهرشنو ةيوهل ةداهش نيوكت مسقلا اذه فصي .تانيوكتل اعيجم رشن نم دكأت ،ءدبل

ةروصلال في حضورم وه امك ،Add رتخأ CertificateAteand > ةزهجال إلى لقتنا 1. ةوطخل



تاداهشل/ةزهجال ةشاش ةطقل

بولسأ ةفاضال + ةنوقي إلى ع رقنا .ةزهجال ةلدسنم ال ةمئاقلا نم FTD زاهج رتخأ: 2. ةوطخل دي دج ةداهش ليجست

A screenshot of the 'Add New Certificate' dialog box. The title is 'Add New Certificate'. Below the title, there is a description: 'Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.' There are two dropdown menus: 'Device*' with 'HA' selected, and 'Cert Enrollment*' with 'Select a certificate enrollment object' selected. A red box highlights the '+' button next to the 'Cert Enrollment*' dropdown. At the bottom right, there are two buttons: 'Cancel' and 'Add'. The 'Add' button is highlighted with a red box.

ةدي دج ةداهش ةفاضال ةشاش ةطقل

ربع ةئيبلال في تاداهشل إلى ع لوصحلل ةلضفم ال ةقيرطال وه يذل رايلال رتخأ: 3. ةوطخل ةروصلال في حضورم وه امك ،"ليجستال عون

Add Cert Enrollment



Name*

FTD04-16

Description

Enrollment Type:

PKCS12 File

PKCS12 File*:

test.p12



Browse PKCS12 File

Passphrase:

.....



Validation Usage:



IPsec Client



SSL Client



SSL Server



Skip Check for CA flag in basic constraints of the CA Certificate

☐ Allow Overrides

Cancel

Save

ةدي دجال ةداهش لاي جست ةحفصل ةشاش ةطقول



SCEP - ايلحم ةدي دجال ةداهش ءاشن - ايتاذ ةعقوم ةداهش :يه ةحاتم ل تارايلخا :جملت ليلدل، CA نم ةداهش يلعل لوصلل طيسبل ةداهش لاي جست لوكوتورب مادختسا رذلابل ةرفشم ل ةداهش ل ةمزح ليمحت - PKCS12، ايوذي ةيوهلل رذل ةداهش تيبت صاخلا حاتم ل ةيوهلل او

FTD إلى IDP عداهش رشن

عيمي رشن نم دكأت، عدبلا لبق. FTD في امرشنو IDP عداهش نيوكت مسقلا اذه فصبي تانيوكتلا.

"Add. رتخاو عداهشلا > عزهجال إلى لقتنا: 1: عوطخلا

بولسأ عفاضلإ + عنوقيأ إلى لع رقنا. عزهجالل ولدسنملا عمئاقلا نم FTD زاهج رتخأ: 2: عوطخلا ديذج عداهش ليجست

ليجست عفاضلإ" عذفان نمض، عروصللا في حضوم وه امك عبولطملا تامولعملل لخدأ: 3: عوطخلا عروصللا في حضوم وه امك "ظفحا م ث"، "عقثلا

- نئاكلل مسا: مسالا
- يودي: ليجستلا عون
- طقف CA: رايتخالل عناخ نيكمتم
- عداهشلل PEM قيسنت: قحصملا عجرملا عداهش

Add Cert Enrollment

Name*

duocert

Description

CA Information

Certificate Parameters

Key

Revocation

Enrollment Type

Manual

☒ CA Only

Check this option if you do not require an identity certificate to be created from this CA

CA Certificate:

OC957DUc7tc4
b79bVzOXuqz5ZpaJHqtXV8fLOH
eIPYblyYBwSstXB+k75VHs0Voz
AkeySJCWRQXF
ISSRGu8DpUIKzKu2zd55322+wd
fkyy/WMXUJWmSXXKnnHEsOqL
GCxmfd+5OsWlo
ICCMGa5gYgEv8EHF3Y++sFg=
-----END CERTIFICATE-----

Validation Usage:

☒ IPsec Client

☐ SSL Client

☒ SSL Server

☐ Skip Check for CA flag in basic constraints of the CA Certificate

☐ Allow Overrides

Cancel

Save

ةداهش ليجست نئاك عاشنإ ىلع لاثم



ةداهشل ةيساسأل دويقلا في CA ةمالع نم ققحتلا ي طخت "مادختسا نكمي: ريذخت رذحب رايجل اذه مدختسا. رمال مزلا اذإ "CA"

دح مٲ "تاداهشل ليجست تحت ائيدح هؤاشنإ مٲ يذلا ةداهشل ليجست نئاك دح: 4 ةوطخل

ةروصلال ي ف حضوم وه امك "ةفاضل

Add New Certificate

Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

Device*:
HA

Cert Enrollment*:
duocert

Cert Enrollment Details:

Name:	duocert
Enrollment Type:	Manual (CA Only)
Enrollment URL:	N/A

Cancel

Add

فاضل ال ةداهشل ال لي ج ست زاهج و نئاكل ةشاش ةطقل



روفال لىل ع اهرشن م تي ،ةداهشل ال ةفاضل ل درج م بو :ةطخال م

SAML SSO نئاكل ءاشنل

ع ي م ج رشن ن م دكأت ،ءدبال ل بق .FMC رب ع SAML SSO ني وكت تا و ط خ م س ق ل ا ذه ف ص ي
ت ا ن ي و ك ت ل .

م دا خ ة فاضل ل د د ح و ي دا ح أ ل ل و خ د ل ل ل ي ج س ت م دا خ > AAA م دا خ > ت ا ن ئ ا ك ل ل ل ل ل ق ت ن ا . 1 ة و ط خ ل
"ي دا ح أ ل ل و خ د ل ل ل ي ج س ت .

Firewall Management Center
Objects / Object Management

Overview Analysis Policies Devices Objects Integration Deploy 🔍 ⚙️ ? Tcourtrie | cisco SECURE

AAA Server
RADIUS Server Group
Single Sign-on Server
Access List
Address Pools
Application Filters
AS Path
bfd Template
Cipher Suite List
Community List
DHCP IPv6 Pool
Distinguished Name
DNS Server Group
External Attributes
File List
FlexConfig
Geolocation
Interface
Key Chain
Network
PKI
Policy List
Port
Prefix List
Route Map

Single Sign-on Server

Add Single Sign-on Server 🔍 Filter

Single Sign-on Server contains parameters for SAML based authentication. These Single Sign-on Servers are used to authenticate users logging in through Remote Access VPN connections.

Name	
AZ	 
DUO	 

Displaying 1 - 2 of 2 rows | < > Page 1 of 1

ديج SSO نئاك عاشن ىلع لاثم

"تاقىب طتلا ةيامح ةسايس عاشن نم ةبولطم الم تامولعمل لخدأ 2. ةوطخل

".ظفح ددح ،لامتكالال درجمب ةعبات ملل ."

- نئاك الم س: *مسالا
- 3 ةوطخل نم نايلال فرعم : *ةيوهال رفوم نايلال فرعم
- 3 ةوطخل نم لوخدلا ليجستل URL ناووع خسن م ت : *SSO تامولعمل عقوم ددحم
- 3 ةوطخل نم خوسنم جورخلال ليجستل URL ناووع : جورخلال ليجستل URL ناووع
- نم FirePOWER ةدعاق ل URL ناووع "ك هس فن FQDN مدختسأ : ساسأل URL ناووع 5 ةوطخلال يف "Cisco"
- ةروشنم الم IDP ةداهش : *ةيوهال رفوم ةداهش
- ل FTD ل ةجراخلال ةهجالو ىلع ةداهش : ةمدخلال رفوم ةداهش

New Single Sign-on Server?

Name*

duosso

Identity Provider Entity ID*

SSO URL*

Logout URL

Base URL

https://vpn.ciscoexample.com

Identity Provider Certificate*

duocert

+

Service Provider Certificate

FTD04-16

+

Request Signature

--No Signature--

Request Timeout

Use the timeout set by the provide

seconds (1-7200)

☐ Enable IdP only accessible on Internal Network

☒ Request IdP re-authentication on Login

☐ Allow Overrides

Cancel

Save

يديج SSO نئاك ىل ع لاثم



جورخ لا ليحستل URL ناوع تاطابتراو SSO URL ناوعو ةدحول فرعم فذح م ت: ةطحال

ةشاشلا ةطق ل نم

RAVPN) ةيره اظلال ةصاخلا دع ب نع لوصول ةكبش نيوكت عاشنإ

جلالعمل مادختساب RAPN نيوكتل تاوطلخال مسقلا اذه فص ي

"ةفاضل دح دع ب نع لوصول > ةزهجالا لىل لقتنا 1. ةوطلخال

VPN: تالوكوتورب نمض SSL دح ،ديجال RAPN جهن جلالعمل مسلا لخدأ ،جلالعمل ي ف 2. ةوطلخال اهلامتك درجمب "يالاتلا" دح .ةروصلال ي ف حضوم وه امك ،ةفدهتسملا ةزهجالا فضأ

Remote Access VPN Policy Wizard

1 Policy Assignment 2 Connection Profile 3 Secure Client 4 Access & Certificate 5 Summary

Targeted Devices and Protocols

This wizard will guide you through the required minimal steps to configure the Remote Access VPN policy with a new user-defined connection profile.

Name*

Description

VPN Protocols:

☒ SSL ☐ IPsec-4Kiv2

Targeted Devices:

Available Devices: HA

Selected Devices: HA

Before You Start

Before you start, ensure the following configuration elements to be in place to complete Remote Access VPN Policy.

Authentication Server

Configure LOCAL or RADIUS Server Group or SSO to authenticate VPN clients.

Secure Client Package

Make sure you have Secure Client package for VPN Client downloaded or you have the relevant Cisco credentials to download it during the wizard.

Device Interface

Interfaces should be already configured on targeted devices so that they can be used as a security zone or interface group to enable VPN access.

Cancel Back Next

RAVPN جلالعمل نم 1 ةوطلخال

دح : (انه ةحضوملا) تارايلخال نييعتب مق ،لاصتالا فيرعت فلمل ةبسنلاب 2. ةوطلخال اهلامتك درجمب "يالاتلا"

- جهن عاشنإ" نم 5 ةوطلخال ي ف قفنلا ةعومجم مسلا مدختسا : لاصتالا فيرعت فلم مسلا . "تاقيبطتلا ةيامح

(AAA) ةبسا حمل او ضيوفتلاو ةقداصلما

- SAML و ليملعلا ةداهش : ةقداصلما بولسا
- "SAML SSO نئاك عاشنإ" اناثا هؤاشنإ مت يذل SSO نئاك دح : ةقداصلما مداح

ليملعلا ناو نع نييعت

- LDAP و RADIUS - (طقف RADIUS و اقاطنلا) AAA مداح مادختسا
- DHCP مداح - DHCP مداوخ مادختسا
- FTD لىل يلحمل عمجتلا - IP نيوانع تا عمجت مادختسا

Firewall Management Center
Devices / VPN / Setup Wizard

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 Tcoutfire 🔒 SECURE

Remote Access VPN Policy Wizard

Policy Assignment — Connection Profile — **Secure Client** — Access & Certificate — Summary

Connection Profile Name:

This name is configured as a connection alias, it can be used to connect to the VPN gateway

Authentication, Authorization & Accounting (AAA):

Specify the method of authentication (AAA, certificates or both), and the AAA servers that will be used for VPN connections.

Authentication Method:

Authentication Server:

SAML Login Experience: ☒ VPN client embedded browser ☐ Default OS Browser

☐ Allow connection only if username from certificate and SAML are the same

☐ Use username from client certificate for Authorization

Username from Certificate:

Primary Field:

Secondary Field:

Authorization Server:

Accounting Server:

Client Address Assignment:

Client IP address can be assigned from AAA server, DHCP server and IP address pools. When multiple options are selected, IP address assignment is tried in the order of AAA server, DHCP server and IP address pool.

☐ Use AAA Server (RADIUS or RADIUS only)

☒ Use DHCP Servers

Use DHCP Servers:

☐ Use IP Address Pools

Group Policy:

A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. Select or create a Group Policy object.

Group Policy:

[Edit Group Policy](#)

Cancel Back **Next**

RAVPN جالاعم نم 2 ةوطخل

ل.دان تلمعتسا DHCP، ربتخم اذه ل :حيملت 🔍

دح مٲ .هرشن متيس يذال Cisco Secure Client ل بيولا رشنل ةروص ليحتل "+" دح . 3 ةوطخلال درجمب "يلال دح .ةروصلال ي ف حضوم وه امك .اهرشن دارمل CSC ةروصل رايتخالال ةناخ هلامتكا .

Firewall Management Center
Devices / VPN / Setup Wizard

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 Tcoutfire 🔒 SECURE

Remote Access VPN Policy Wizard

Policy Assignment — Connection Profile — **Secure Client** — Access & Certificate — Summary

Secure Client Image

The VPN gateway can automatically download the latest Secure Client package to the client device when the VPN connection is initiated. Minimize connection setup time by choosing the appropriate OS for the selected package.

Download Secure Client packages from [Cisco Software Download Center](#).

Secure Client File Object Name	Secure Client Package Name	Operating System
☒ cisco-secure-client-macos-5.0...	cisco-secure-client-macos-5.0.02075-web...	Mac OS
☒ cisco-secure-client-win-5.0.020...	cisco-secure-client-win-5.0.02075-webde...	Windows

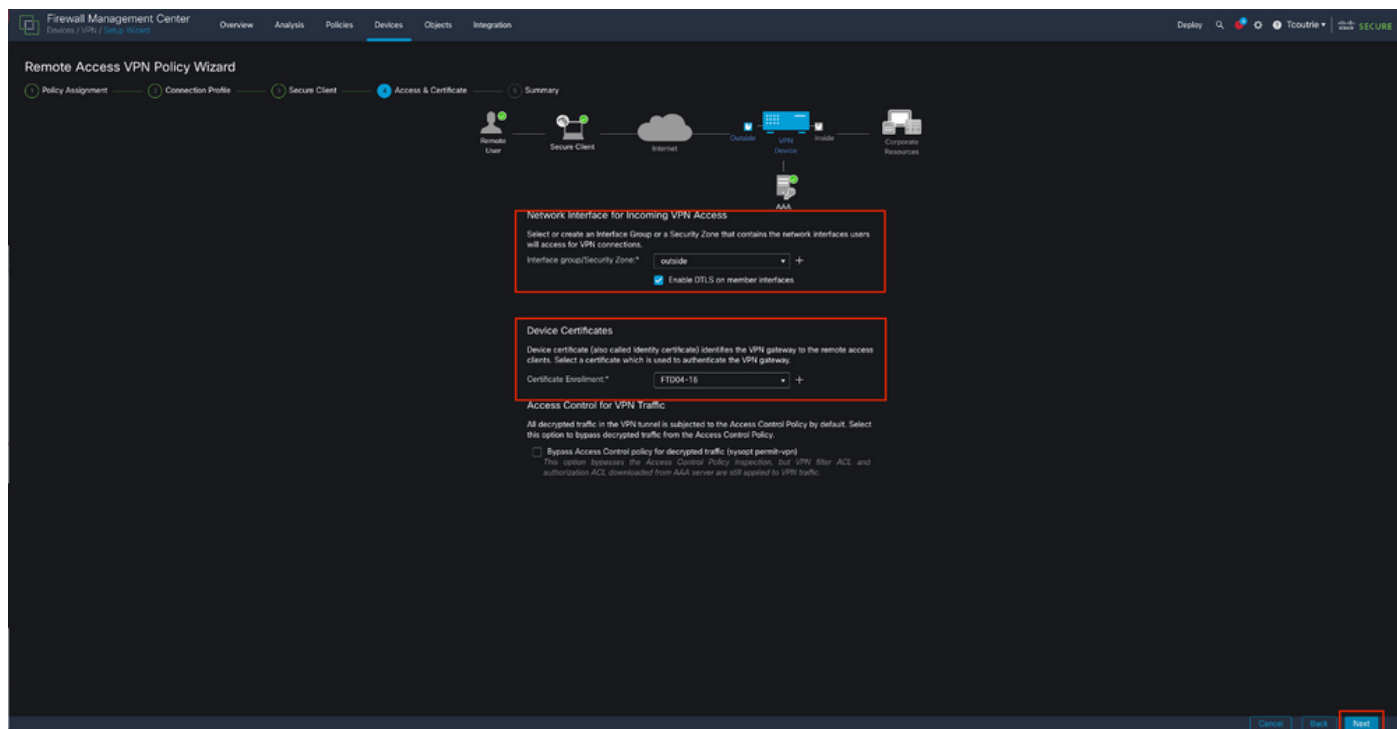
Cancel Back **Next**

RAVPN 3 ةوطخلال جالاعم

هلامتكا درجمب "يلال دح :ةروصلال ي ف رهظي امك) تانئالال هذه نييعتب مق . 4 ةوطخلال

ةيجراخل ةهجال :نامأل ةقطنم/ةهجال ةومجم

اذه نم "FTD ءزج ل ةيول ةداهش رشن" ءانثأ فيرعت ةداهش ءاشنإ م ت :ةداهش ل ليجست " ل ل ل ل

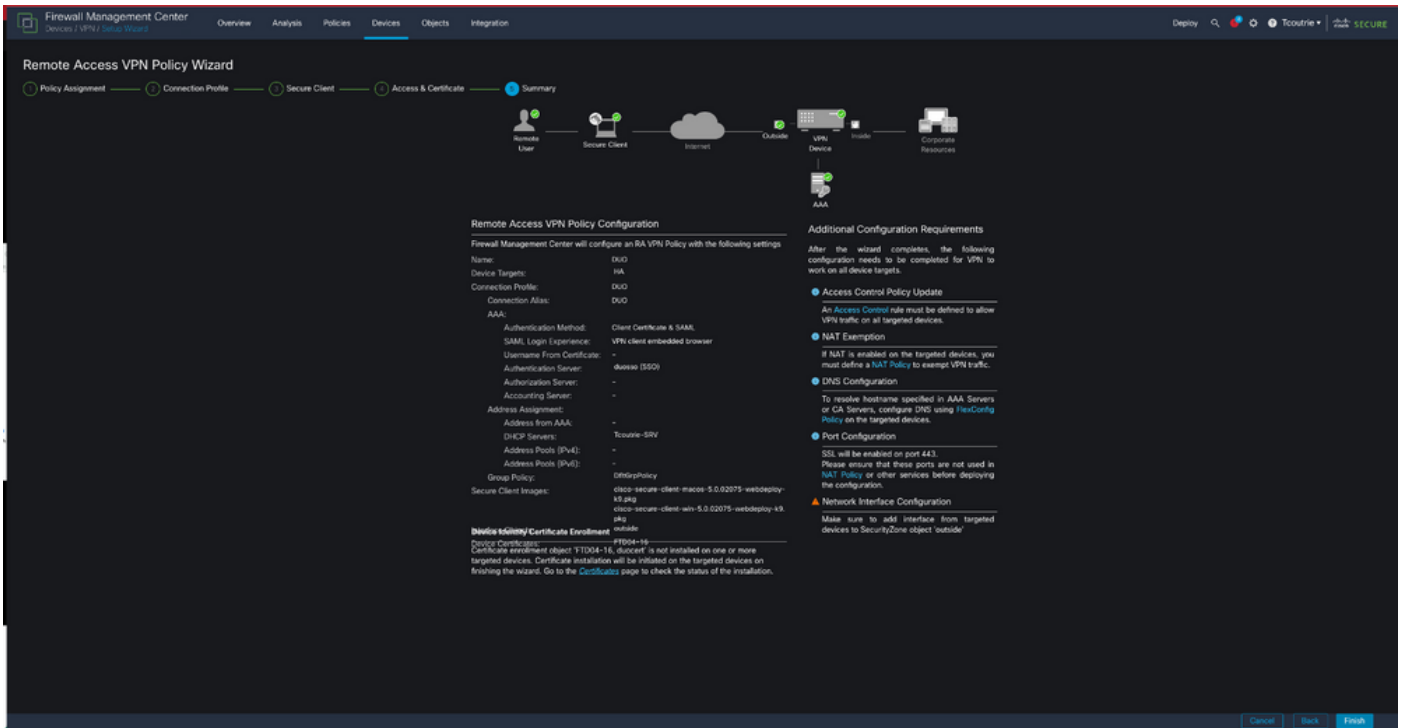


RAVPN ج اعم نم 4 ةوطخل

ديحت قيرط نع ديدج ةداهش ليجست نئاك ةفاضاب مقف ،اذه ءاشنإ م تي مل اذا :جيملت +.

صخلم 6. ةوطخل

ءاهنإ عم عبات ،ايجحص ءيش لك ناك اذا .تامولعمل ايجم نم ققحت



صخلم لمةحفص

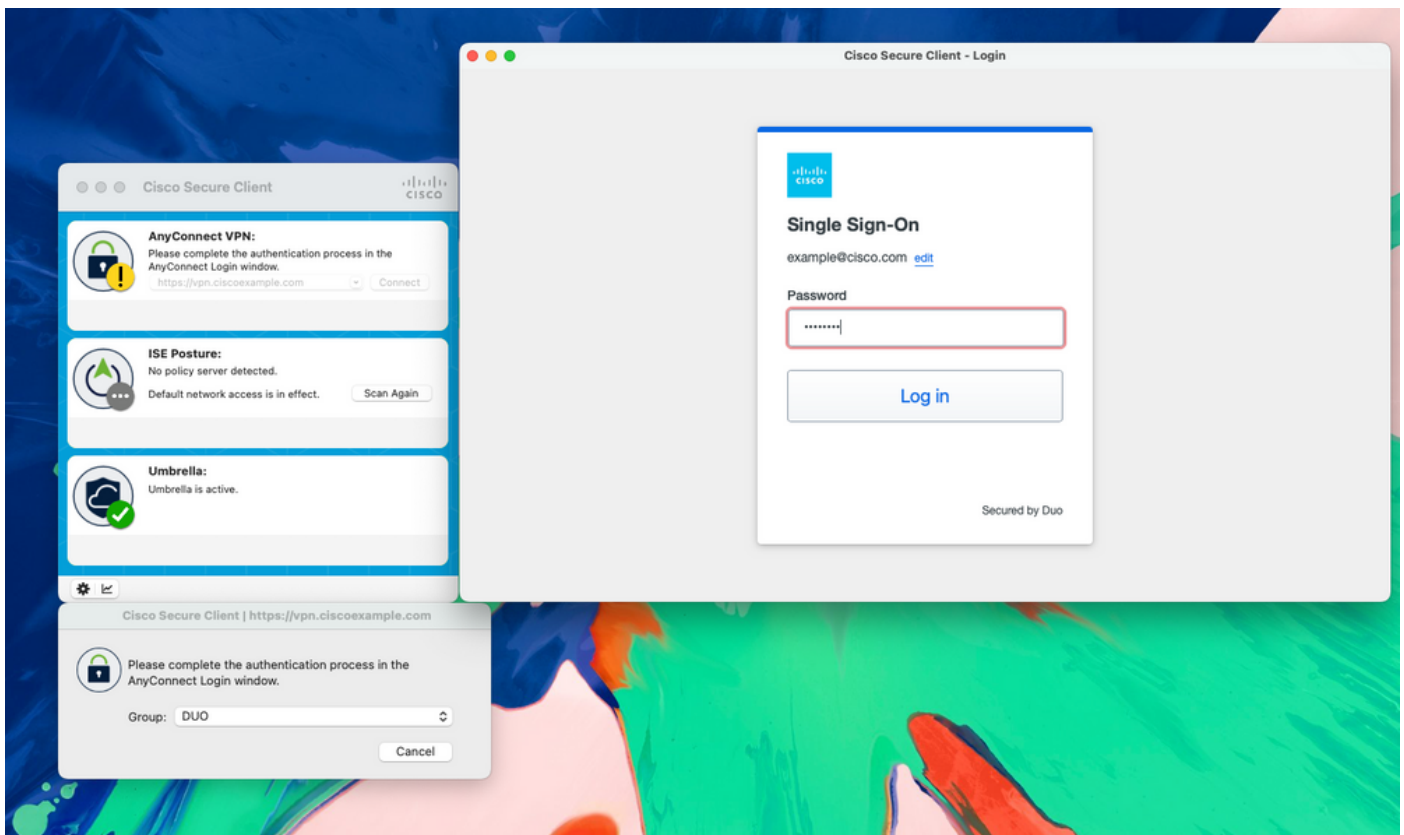
ا.ثي دح اهتفاضل تم تي تال تاني وكتال رشن ب مق 7 ة ووطخل

ةحصلال نم ققحتال

ةحجان لاصتا ةل واعم نم ققحتال مسقلا اذه حضوي

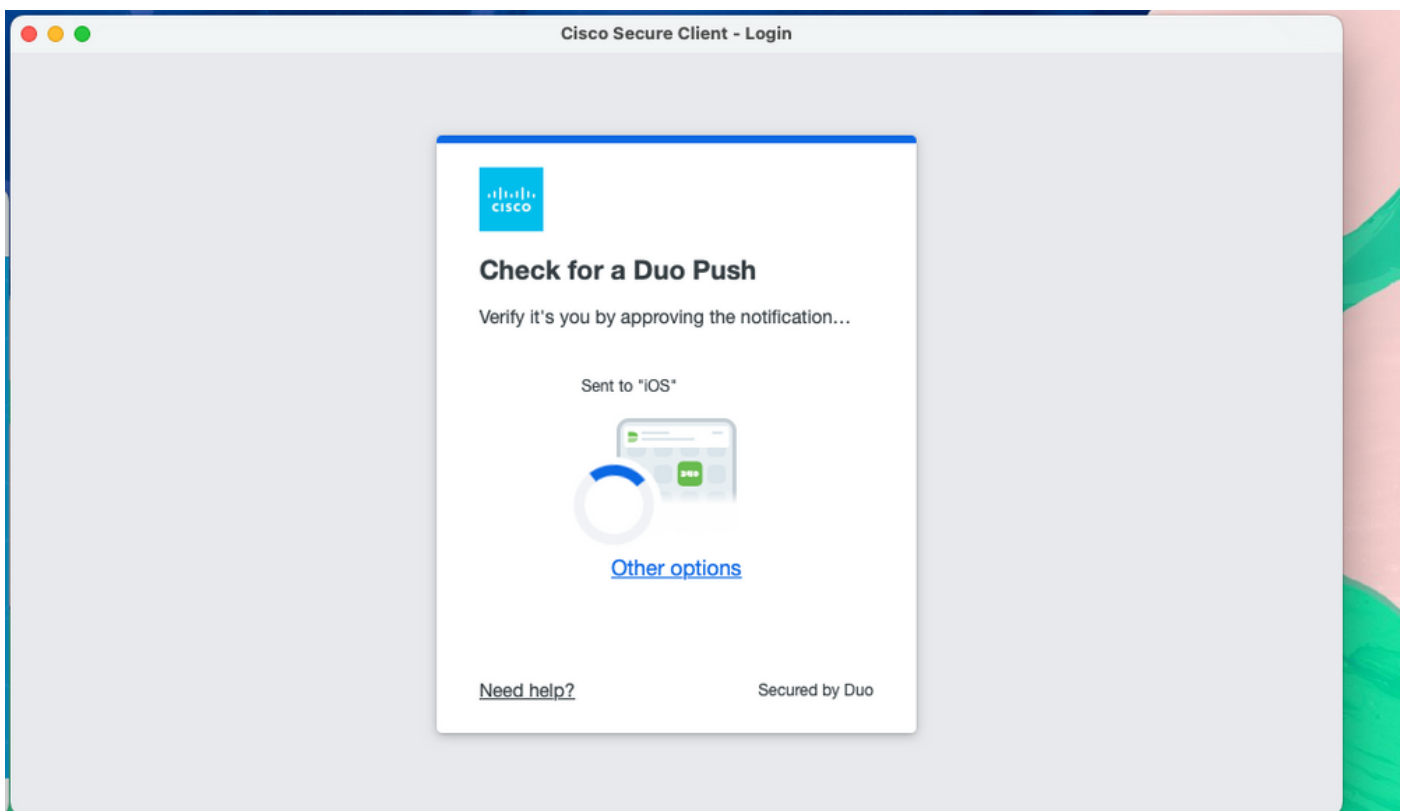
Connect و FTD لخدأو Cisco Secure Client حتفا

SSO ةحفص لىل ع دامتعالا تاناي ب لخدأ



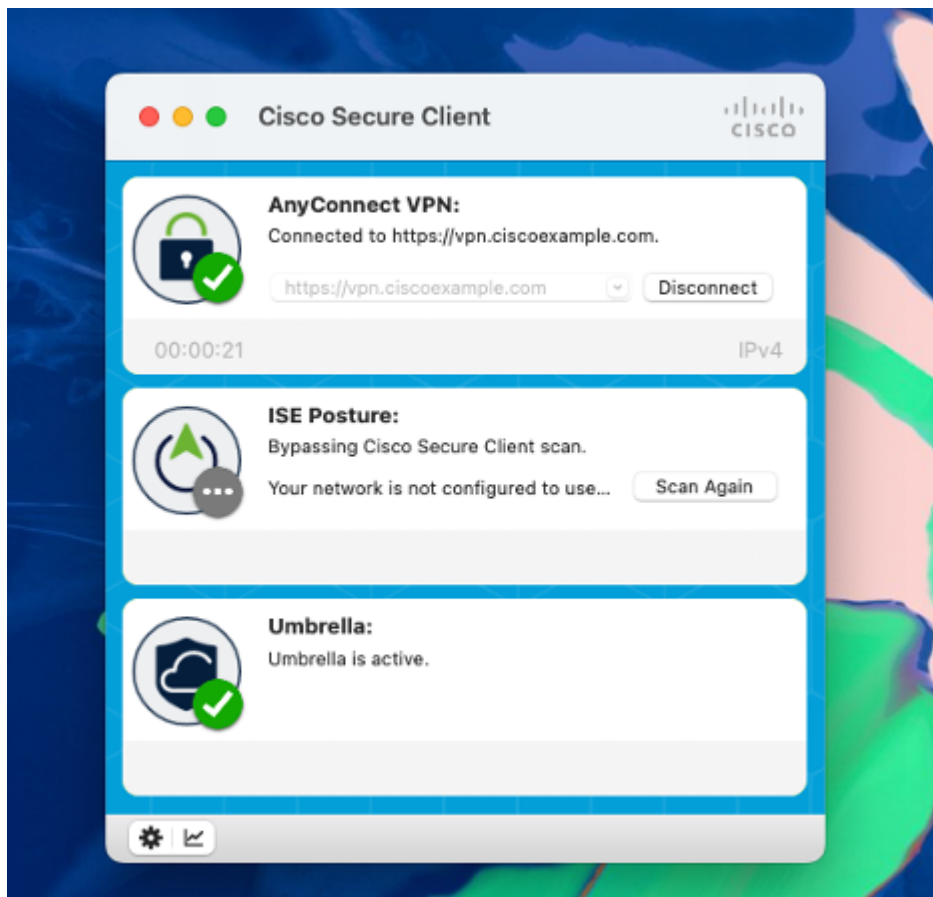
Cisco Secure Client ربح SSO ةحفص

لجسمال زاهجلا ىلإ يئانثلا عفد لبقا.



يئانث عفد

حجان لاصتا.



FTD ب ل ص ت م

show vpn-sessionDB detail AnyConnect
رم أ ل م ا د خ ت س ا ب FTD ی ل ع ل ا ص ت ا ل ا ن م ق ق ح ت

```

tcoutrie-ftd2# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username      :                               Index      : 1916
Assigned IP   :                               Public IP   :
Protocol      : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License       : AnyConnect Premium
Encryption    : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-128  DTLS-Tunnel:
Hashing       : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA256  DTLS-Tunnel: (1)SH
Bytes Tx      : 390964                      Bytes Rx     : 124114
Pkts Tx       : 1216                        Pkts Rx      : 1223
Pkts Tx Drop  : 0                          Pkts Rx Drop : 0
Group Policy  :                               Tunnel Group :
Login Time    : 23:54:41 UTC Tue Jul 18 2023
Duration      : 0h:11m:28s
Inactivity    : 0h:00m:00s
VLAN Mapping  : N/A                        VLAN         : none
Audt Sess ID  : 0a7aa95d0077c00064b72641
Security Grp  : none                       Tunnel Zone  : 0

AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:
Tunnel ID     : 1916.1
Public IP     :
Encryption    : none                      Hashing       : none
TCP Src Port  : 53859                     TCP Dst Port  : 443
Auth Mode     : Certificate and SAML
Idle Time Out: 30 Minutes                 Idle TO Left  : 18 Minutes
Client OS     : mac-intel

```

تاجزخمم للاثم نم تامولعم الم ضعب فذح مت

اهحالصإو ءاطخأل فاشكتسا

ذيفنت لا دعب أشنت ةلمتحم لئاسم هذو

ةداهشلا ةقداصم لشف 1: ةلأسم لا

FTD؛ ىلع رذجلا ةداهشلا تيبتت نم دكأت

يالاتلا ءاطخأل حيحصت مدختسأ

debug crypto ca 14

debug aaa shim 128

debug aaa عئاش 128

SAML لشف 2: رادصلإا

اهحالصإو ءاطخأل فاشكتسال هذو ءاطخأل حيحصت تايلمع نيكمت نكمي

debug aaa shim 128

debug aaa عئاش 128

debug webVPN AnyConnect 128

debug webVPN saml 255

ةمچرتل هذه ل و ح

ةيلآل ا تاي ن ق ت ل ا ن م ة و م ج م ا د خ ت س ا ب د ن ت س م ل ا ا ذ ه Cisco ت م چ ر ت م ل ا ع ل ا ا ح ن ا ع م ج 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 ا و ا م ك ة ق ي ق د ن و ك ت ن ل ة ي ل آ ة م چ ر ت ل ض ف ا ن ا ة ط 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 م چ ر ت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة م چ ر ت ل ا ع م ل ا ح ل ا و ه ي ل ا ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا م چ ر ت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م 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 د ن ت س م ل ا