

ةيملاعلـا ZTNA نـمـآلـا لـوصـولـا نـيـوـكـتـا مـادـخـتـسـابـاـ فـمـCـاـ رـادـمـلـا SCCـاـ

تاـيـوـتـحـمـلـا

[ةـمـدـقـمـلـا](#)

[ةـيـسـاسـأـلـا تـاـبـلـطـتـمـلـا](#)

[تابـلـطـتـمـلـا](#)

[ةـمـدـخـتـسـمـلـا تـاـنـوـكـمـلـا](#)

[ةـكـبـشـرـلـلـيـطـيـطـخـتـلـا مـسـرـلـا](#)

[ةـفـيـكـمـتـامـوـلـعـمـ](#)

[ةـمـوـعـدـلـا قـزـمـجـأـلـا](#)

[دوـقـلـا](#)

[نيـوـكـتـلـا](#)

[راـدـصـاـنـمـقـقـحـتـلـا FMC](#)

[راـدـصـاـنـمـقـقـحـتـلـا FTD](#)

[صـيـخـارـتـنـمـقـقـحـتـلـا FTD](#)

[جـوـجـصـ، لـكـشـبـاهـنـيـوـكـتـمـبـيـتـلـا DNSـيـسـاسـأـلـا مـاظـنـلـاـتـاـدـادـعـاـنـمـقـقـحـتـلـا](#)

[ةـلـيـلـعـنـاـمـأـقـبـاحـسـمـكـحـتـلـا CDOـعـاـشـنـا](#)

[ةـيـاـمـحـلـاـرـادـجـلـقـمـاعـلـاـتـاـدـادـعـاـلـاـنـيـوـكـتـنـمـدـكـأـلـلـا SCC](#)

[نـمـآلـاـلـوـصـولـاـرـجـأـتـسـمـوـنـمـآلـاـلـوـصـولـاـيـفـمـكـحـتـلـلـاـقـيـاـمـحـرـادـجـقـرـادـاـقـدـعـاـفـ، لـمـاـكـتـنـمـقـقـحـتـلـا](#)

[ةـيـاـمـحـلـاـرـادـجـلـعـافـدـبـقـعـقـوـمـCAـعـاـشـنـا \(FTD\)](#)

[نـامـآلـاـقـبـاحـسـيـفـمـكـحـتـلـلـاـقـلـيـعـنـمـضـمـلـاـقـيـاـمـحـلـاـرـادـجـقـرـادـاـزـكـرـمـ](#)

[ةـلـيـلـعـZero Trust \(uZTNA\)ـةـكـبـشـرـلـلـيـطـيـطـخـتـلـا FTDـمـادـخـتـسـابـلـيـمـعـلـاـلـلـيـجـسـتـ](#)

[نـمـآلـاـلـوـصـولـاـنـيـوـكـتـلـاـلـيـمـعـلـاـلـلـيـجـسـتـZTNA](#)

[نـمـآلـاـلـوـصـولـاـنـيـوـكـتـ](#)

[لـيـمـعـلـاـنـيـوـكـتـ](#)

[قـحـصـلـاـنـمـقـقـحـتـلـا](#)

[قـلـصـتـاذـتـامـوـلـعـمـ](#)

ةـمـدـقـمـلـا

يـرـهـاـظـلـا FTD و Secure Access ZTNA نـيـوـكـتـةـيـفـيـكـ دـنـتـسـمـلـاـاـذـهـفـصـيـ تـتـنـرـتـنـإـلـاـقـلـعـيـرـهـاـظـلـا FMCـاـوـبـهـتـرـادـاـمـتـتـيـذـلـا.

ةـيـسـاسـأـلـا تـاـبـلـطـتـمـلـا

- ةـيـاـمـحـلـاـرـادـجـمـادـخـتـسـابـدـيـدـهـتـلـاـنـعـعـافـدـلـاـوـ(FMC)ـةـيـاـمـحـلـاـنـارـادـجـةـرـادـاـزـكـرـمـرـشـنـبـجـيـ
- ثـدـحـأـرـادـصـاـوـأـ7.7.10ـجـمـانـرـبـرـادـصـاـمـادـخـتـسـابـ
- رـادـجـةـرـادـاـزـكـرـمـلـالـخـنـمـةـيـاـمـحـلـاـرـادـجـتـادـيـدـهـتـدـصـةـيـاـمـحـلـاـةـزـيـمـةـرـادـاـمـتـتـنـأـبـجـيـ
- ةـيـاـمـحـلـاـ(FMC)

تابلطتما

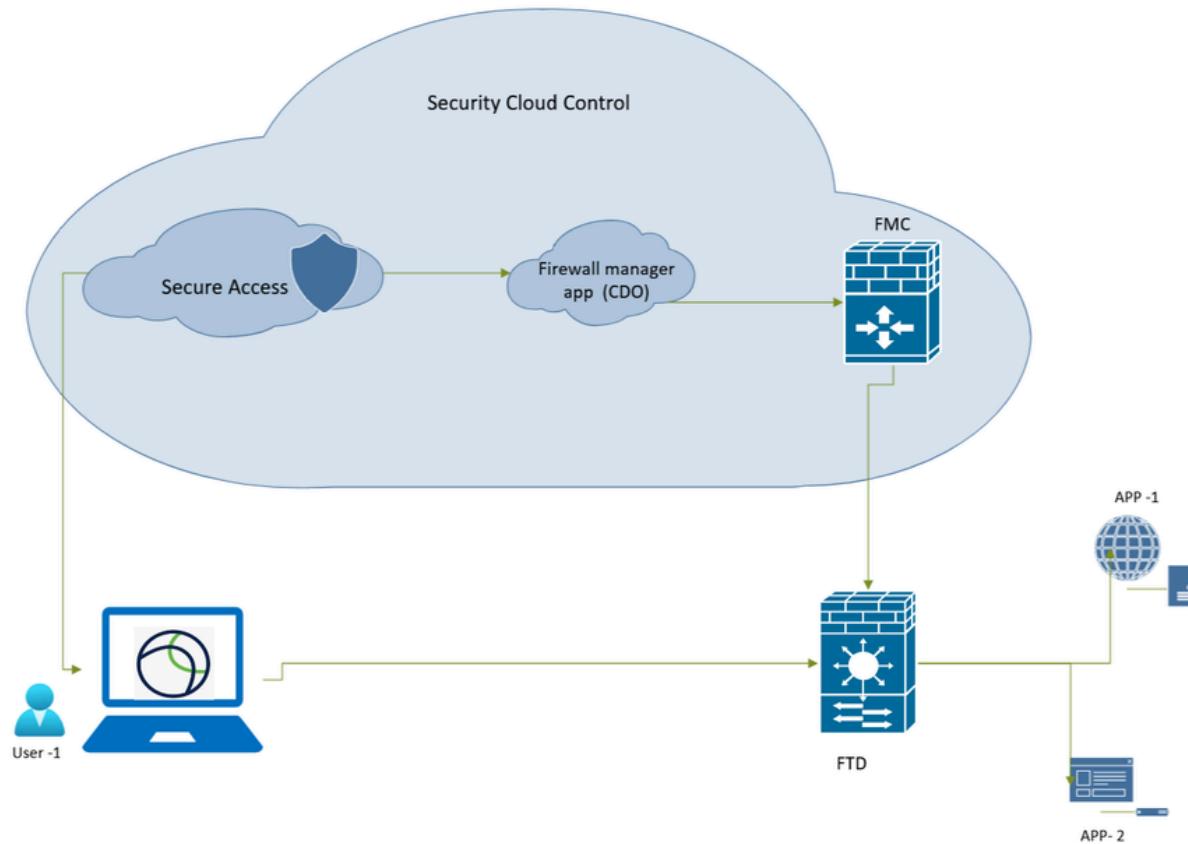
ةم دخت سملاتان وكملا

یلإ دنتسملا اذه یف ۀدراولا تامولعملاء دنتس

- نامآلا ئباقس يف مكحتلا (SCC)
 - رادصىلا، نمآلا ئيامحلى رادج ۋارادى زىرىم 7.7.10
 - Secure Firewall Threat Defense (FTD) virtual 7.7.10
 - رادصىلا Windows لىغىشتلى ماظنل 5.1.10
 - نمآلا لوصولى

ڦڻا خ ڦيلم ڻا يف ڦوجو ڦلا ڦهچ ڦلا نم ڏنٽس ڦلا اذه يف ڦراول ڦا تام ڦول ڦعمل ڦاشن ڦا مت
تن ڦاك اذا (ي ضارتفا) حوس ڦمم ڦنيو ڦوك ڦتب ڏنٽس ڦلا اذه يف ڦمدخت ڦس ڦلا ڦهچ ڦلا عيمج ٿا ڦدب
رم ڦا ي ڦا ل ڦمت ڦحمل ڦلا ر ڦي ڦث ڦأ ڦل ڦل ڦكم ڦه ڦف ڦنم ڦد ڦك ڦأ ڦف ، ڦلي ڦغ ڦش ڦتل ڦا ڦدي ڦق ڦك ڦب ڦش

ةكبس للي طختلا مسرا



ةكبشل ا ططخم - نمآلا لوصول

ةفيكم تامولع م

ةموعدملا ۆزهجانا

ننمآلا ۆيامحلا رادج ديدهت دض ۆموعدملا عافدلان جذامن:

- FPR 1150
- FPR 3105 و 3130 و 3110 و 3120 و 3140
- FPR4115,4125,4145,4112
- FPR4215,4225,4245
- ۆدحو زكارم نم ازكرم 16 عم يضارتفا (FTD) يرانلا رادجلاتادي دهت دض عافدلان زاهج
ىن دأ دحك (CPU) ۆيزكرملا ۆجلاعملان

دوبيقلان

- رصنعملا ۆكراشم
- موعدم رېغ.
- طقف یمومعملان VRF مععد متى.
- ىلارعقوم نم قفنلارورم ۆكرح ىلر ۆيملاعلان ZTNA تاسايىس ضرف متى ال زاهج .

- ةدمتعم ريغ ةعمجملا ةزهجأ.
- ةعرسب FirePOWER 4 ئسلس ئل ع تايواحك اهرشن متى يتلا FTD تافلم معدمتى ال وليك 9 و
- زج معدت ال تاسل ج ZTNA ئماعلا Jumbo تاراطإ

نيوكتلا

رادصا نم ققحتلا FMC

جمانربلا رادصا ئل ع ئيامحلا رادجل FTD جمانربو ئيامحلا رادجا زكرم ليغشت نم ققحت ئل ع 7.7.10 نوكى نأ نكمي) ئيملاعلما ZTNA ل موعدملا:

- قوف رقنا او (ينميلا ئيولعلا ئيوازلا)؟ قوف رقنا About

The screenshot shows the FMC dashboard. At the top, there's a navigation bar with a search bar, a 'Deploy' button, and several status icons (blue circle, bell with '1', gear). To the right of these is an 'admin' dropdown menu. Below the navigation bar, the main content area has three columns. The left column contains links like 'Product Content' (Secure Firewall on Cisco.com, Documentation on Cisco.com, Secure Firewall on YouTube, Secure Firewall Essentials, Partner Ecosystem). The middle column contains 'Tools' (Firewall Migration Tool, Application Detectors, Ask Cisco Community, TAC Support Cases, Software Downloads). The right column contains 'On-screen Assistance' (Page-level Help, How-Tos, What's New, Release Highlights, All New and Deprecated Features).

On-screen Assistance		
		Page-level Help
Product Content	Application Detectors	How-Tos
Secure Firewall on Cisco.com		
Documentation on Cisco.com	Support & Downloads	What's New
Secure Firewall on YouTube	Ask Cisco Community	Release Highlights
Secure Firewall Essentials	TAC Support Cases	All New and Deprecated Features
Partner Ecosystem	Software Downloads	



Firewall Management Center

Version 7.7.10 (build 8)

Model	Cisco Secure Firewall Management Center for VMware
Serial Number	None
Snort Version	2.9.24 (Build 96)
Snort3 Version	3.3.5.1000 (Build 10)
Rule Pack Version	3115
Module Pack Version	3505
LSP Version	Isp-rel-20250430-1826
VDB Version	build 400 (2024-11-26 19:30:49)
Rule Update Version	2025-04-30-001-vrt
Geolocation Version	2025-04-19-097
OS	Cisco Firepower Extensible Operating System (FX-OS) 82.17.30 (build 3)
Hostname	firepower

For technical/system questions, email tac@cisco.com phone: 1-800-553-2447 or
1-408-526-7209. Copyright 2004-2025, Cisco and/or its affiliates. All rights reserved.

[Copy](#)

[Close](#)

جـمـارـبـلـا رـادـصـا - نـمـآلـا ةـيـامـحـلـا رـادـجـ ةـرـادـا زـكـرـمـ

رادصـا نـمـ قـقـحتـلـا

مـدـخـتـسـمـ ةـجـاـوـىـلـا لـقـتـنـاـ FMC:

- [قفـرقـنـاـ > Devices > Device Management](#)

Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack
FTD1(Primary, Active) Snort 3 192.168.1.11 - Routed	Firewall Threat Defense for VMware	7.7.10	N/A	Essentials, IPS (2 more...)	ACP	
FTD2(Secondary, Standby) Snort 3 192.168.1.13 - Routed	Firewall Threat Defense for VMware	7.7.10	N/A	Essentials, IPS (2 more...)	ACP	

جـمـارـبـلـا رـادـصـا - ةـيـامـحـلـا رـادـجـ دـيـدـهـتـ دـضـ نـمـآلـا عـافـدـلـا

صيخارت نم ققحتلـا FTD

- قوف رقـنا Setting Icon > Licenses > Smart Licenses



Configuration

Users

Domains

Product Upgrades

Content Updates

Health

Monitor

Policy

Events

Exclude

Monitoring

Audit

Syslog

Statistics

Tools

Licenses

Smart Licenses

Backup/Restore

Scheduling

Import/Export

Data Purge

License Type/Device Name		License Status	Device Type	Domain	Group
> Firewall Management Center Virtual (2)		● In-Compliance			
< Essentials (2)		● In-Compliance			
> FTD-HA (2) [Performance Tier: FTDv100] Cisco Secure Firewall Threat Defense for VMware Threat Defense High Availability		● In-Compliance	High Availability - Cisco Secure Firewall Threat Defense for VMv Global		N/A
< Malware Defense (2)		● Out of Compliance			
> FTD-HA (2) [Performance Tier: FTDv100] Cisco Secure Firewall Threat Defense for VMware Threat Defense High Availability		● Out of Compliance	High Availability - Cisco Secure Firewall Threat Defense for VMv Global		N/A
< IPS (2)		● Out of Compliance			
> FTD-HA (2) [Performance Tier: FTDv100] Cisco Secure Firewall Threat Defense for VMware Threat Defense High Availability		● Out of Compliance	High Availability - Cisco Secure Firewall Threat Defense for VMv Global		N/A
< URL (2)		● Out of Compliance			
> FTD-HA (2) [Performance Tier: FTDv100] Cisco Secure Firewall Threat Defense for VMware Threat Defense High Availability		● Out of Compliance	High Availability - Cisco Secure Firewall Threat Defense for VMv Global		N/A
Carrier (0)					

ةيكلد صيخارت - ةيامحلا راج مادختساب ديدهتلا دض نمآل اعافدل

حىحص لكشب اهنيلوكت مت يتلا DNS يساسألا ماظنلا تادادعإ نم ققحتلا

رابع FTD CLI:

- ئيوكت نم ققحتل رمألا ليغشت بمق DNS:

show run dns

ييف FMC:

- ئيديج ئاسايىس عاشنا وأ ريرحتب مق وأ قوف رقنا Devices>Platform Settings،

Platform Settings	Device Type	Status
Platform,Policy	Threat Defense	Targeting 1 device(s) Up-to-date on all targeted devices

يساسألا ماظنلا ئاسايىس - ةيامحلا راج ديدهت دض نمآل اعافدل

نويوك - ئيامحلا رادج دىدەت نع نمآلما عافدىلا

وصاخلا IP ناونع لاصتا رابتخا كىنكىمى هنأ FTD ب ئاصاخ (CLI) رمأو رطس ۋەچاولالخ نم ققحت FQDN مادختساب PR ىلارنىڭ FQDN يىف بغرت تىنك اذى).

```
!dns>group Lab-DNS
ftd1# ping ise.taclab.com
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.50, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
ftd1#
```

ىلۇغ ناماً ئاباحس مەكتىرىنىڭ رجأتسم ئاشنا



ئاشنا كىلىغ نوكىي نىلف، هنويوكت مەت SCC رجأتسم لۇغلىپ كىيدل ناك اذى: ئەظحالىم دىدج رجأتسم.

ناماً ئاباحسىنىڭ مەكتىلى ىلارنىڭ لقتنى:

- **قوف رقنا** Organization > Create new organization

ۋەسىملا - ئانمآل ئاباحسلا يىف مەكتىلى

- **قوف رقنا** Create

The screenshot shows the Cisco Security Cloud Control interface. On the left, there's a sidebar with navigation links like Home, Products (Firewall, Secure Access), Platform services (Favorites, Security Devices, Shared Objects, Platform Management), and others. The main area has sections for 'Claim subscription', 'INTEGRATE IDENTITY PROVIDER (IDP)', and 'ONBOARD FIREWALL DEVICES'. A central modal window titled 'Create new organization' is open, prompting for a 'New organization name' (tac-uztha) and 'Region deployment' (North America). A red box highlights the 'Create' button at the bottom right of the modal. Below the modal, there's a 'DEFAULT LANDING PAGE' section with a 'Select' button.

ةسسؤملا عاشنإ - ةنمآل اقباحسلا يف مكحتلا

SCC و Firewall Secure Access Microapp uZTNA. نيكمل رجأتسملا تامولعم عيمجتب مق، SCC رجأتسم عاشنإ درجمب

SCC ئيامح رادجل ۋەماعل تادادعىلا نيكىت نم دكأتلارا.

ىلى لقتنانىڭ [CDO/SCC](#):

- قوف رقنا Adminstration > General Settings
- نيكىت نم دكأتل Auto onboard On-Prem FMCs from Cisco Security Cloud.



ىلى لوصوللا لواحي يذلا مدختسملل نوكى نأ بجي: ئەظحال Secure Access MicroApp Secure Access Security Cloud Control راودا.

Security Cloud Control

The screenshot shows the Cisco Security Cloud Control interface. The left sidebar includes sections for Dashboard, Monitor, Insights & Reports, Events & Logs, Manage, Objects, Security Devices, Secure Connections, and Administration. The Administration section is currently selected. The main content area is titled "Administration" and contains a "General Settings" tab (selected) and other tabs for User Management and Notification Settings. Below these tabs, there's a "Integrations" section with options for Secure Connectors, Firewall Management Center, Multicloud Defense, and Management.

The screenshot shows the "General Settings" page within the Cisco Security Cloud Control Administration interface. The "General Settings" tab is selected. The page includes several configuration options:

- Enable the option to schedule automatic deployments**: A toggle switch is off.
- Web Analytics**: A toggle switch is on.
- Auto onboard On-Prem FMCs from Cisco Security Cloud**: A toggle switch is on, highlighted with a red box. A tooltip indicates: "Ensure that your On-Prem FMCs are integrated with Cisco Security Cloud. Only the integrated On-Prem FMCs are onboarded. See [Integrate On-Prem FMC to Cisco Security Cloud](#)."
- Enable event data sharing with Talos**: A toggle switch is on.
- Tenant ID**: A dropdown menu set to "cbc".
- Secure Services Exchange Tenant ID**: A dropdown menu set to "71".
- Tenant Name**: A dropdown menu set to "CI".

سـسـفـمـلـا لـيـصـافـتـ - ظـنـمـآلـا ظـبـاحـسـلـا يـفـ مـكـحـتـلـا

رجـأـتـسـمـوـ نـمـآلـا لـوـصـوـلـا يـفـ مـكـحـتـلـا ظـيـامـحـ رـادـجـ ظـرـادـا ظـدـعـاـقـ لـمـاـكـتـ نـمـ قـقـحـتـلـا
نـمـآلـا لـوـصـوـلـا

The screenshot shows the Cisco Security Cloud Control web interface. At the top, it displays the organization details: 'Organization ID - a161c021-d64-48ab-8897-89c78be3aafe' and 'Organization - Cisco-jaiyadav - United States'. On the left sidebar, under 'Products', 'Firewall' is selected. In the main content area, there are two cards: one for 'Cisco Security Cloud Control Firewall Management Base' (Subscription ID: lab-jaiyadav-1, End date: 04/16/2026, External instance ID: 1, Quantity: 1, Region: North America) and one for 'Cisco Secure Access' (Subscription ID: lab-jaiyadav-1, End date: 04/16/2026, External instance ID: 1, Quantity: 1, Region: Global).

نمآلا لوصولا طيشنـت - ةنمآلـا ئـباـحـسـلـا يـفـ مـكـحـتـلـا

رجـاتـسـمـ عـاشـنـتـاـوـ CDOـ ىـلـعـ نـامـأـلـاـ قـبـاحـسـ يـفـ مـكـحـتـلـاـ رـاجـاتـسـمـ عـاشـنـتـاـ ۋـوطـخـلـاـ لـامـتـكـاـ دـرـجـمـبـ تـاقـيـبـطـتـ ۋـيـقـرـنـيـحـ كـنـكـمـيـ، CDOـ ىـلـعـ نـامـأـلـاـ قـبـاحـسـ يـفـ مـكـحـتـلـاـ Firewallـ وـ Secure Accessـ تـامـوـلـعـمـ ۋـحـولـ ىـلـعـ SCCـ microـ:

The screenshot shows the 'Security Devices' section of the Cisco Security Cloud Control interface. The left sidebar has a red box around the 'Firewall' and 'Secure Access' options under 'Products'. The main area shows a table with columns 'Name', 'Configuration Status', and 'Connectivity'. A large blue 'i' icon is displayed in the center, and a message below it says 'No devices or services found. You must onboard a device or service to get started.'

تـاقـيـبـطـتـ - ئـباـحـسـلـا يـفـ نـمـآلـاـ مـكـحـتـلـاـ

ةـيـامـحـلـاـ رـادـجـ تـادـيـدـهـتـ عـافـدـبـ ئـعـقـومـ CAـ ۋـدـاهـشـ عـاشـنـتـاـ (FTD)



عاـشـنـاـ مـسـقـ عـجاـنـ عـيـقـوـتـلـاـ ئـيـتـاذـ FTDـ تـادـاهـشـ مـادـخـتـسـاـ اـضـيـأـ كـنـكـمـيـ: ئـظـحـالـمـ قـيـسـنـتـبـ نـوـكـيـ نـأـ بـجـيـ. (عـيـقـوـتـلـاـ ئـيـتـاذـ ئـيـلـخـادـلـاـوـ ئـيـلـخـادـلـاـ CAـ تـادـاهـشـ يـزـكـرـمـ قـدـصـمـ عـجـرمـ تـحـتـ مـدـخـتـسـمـلـاـ ئـزـهـجـأـ نـزـخـمـ يـفـ اـدـوـجـوـمـ نـوـكـيـ نـأـ بـجـيـ وـ PKCS12ـ بـ قـوـثـوـمـ.

عاـشـنـاـ ئـزـيمـ يـفـ FTDـ مـادـخـتـسـابـ CAـ نـمـ ئـعـقـومـ ئـدـاهـشـ عـاشـنـإـلـ

- ئـلـاـ لـاقـتنـالـاـ FTD
 - ئـلـيـغـشـتـ رـمـأـ expert
- مـادـخـتـسـابـ حـاتـفـمـلـاـوـ CSRـ ئـاشـنـاـ OpenSSLـ مـادـخـتـسـابـ
 - OpenSSLـ رـمـأـ

```
openssl req -newkey rsa:2048 -nodes -keyout cert.key -out cert.csr
```

```
openssl req -newkey rsa:2048 -nodes -keyout cert.key -out cert.csr
Generating a RSA private key
-----+=====
-----+=====
writing new private key to 'cert.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:NC
Locality Name (eg, city) []:RTP
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Cisco
Organizational Unit Name (eg, section) []:TAC
Common Name (e.g. server FQDN or YOUR name) []:ftd.taclab.com
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
```

ةداهش لاعيقوت بلط

- ةعقوم CA ةداهش لىع لصح او CSR خسنا

قيسنت ىلإ ةداهش لال يوحتب مقو CA لباق نم عقوملا حاتفمل او ةداهش لامدخلتسا PKCS12

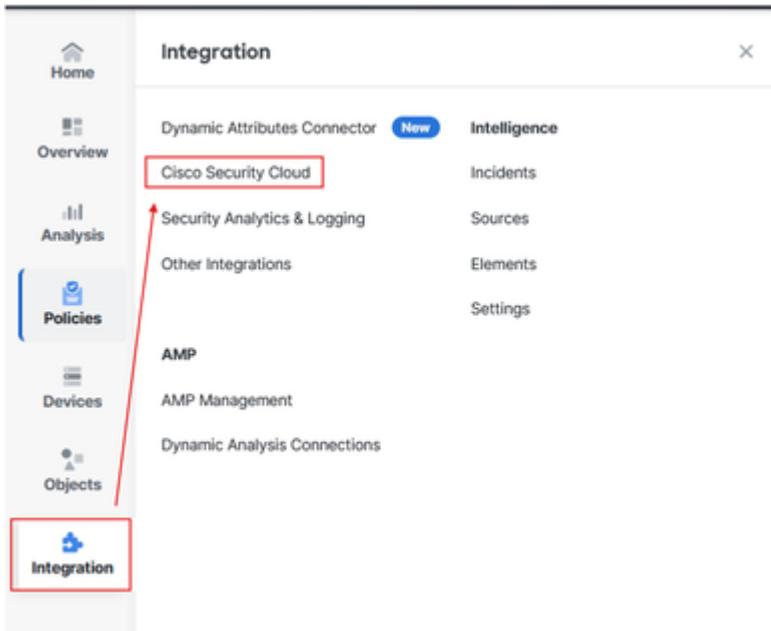
- OpenSSL:

```
openssl pkcs12 -export -out ftdcert.p12 -in cert.crt -inkey cert.key
```

- يرخأ ةادأ وأ SCP مادختساب ةداهش لاريدصت.

نامألا ةباحس يف مكحتلل ٥حوللا ىلع نمضملأا ئيامحلا رادج ةرادإ زكرم
ىلإ لقتنا FMC:

- قوف رقنا Integration> Cisco Security Cloud



و ئيامحل رادج ئارادا زكرم جمد SCC

- قوف رقنا مث ئباجسلا ۋە قطنم رتخا Enable Cisco Security Cloud

ل ئيامحل رادج ئارادا زكرم ئىلما مامضنالا ئيناكما

: ئەدىدەل بىوبتلا ۋە مالۇ يىف، ئەدىدەل ضرۇتسىم بىوبت ۋە مالۇ حەتفىيىس

- قوف رقنا Continue to Cisco SSO



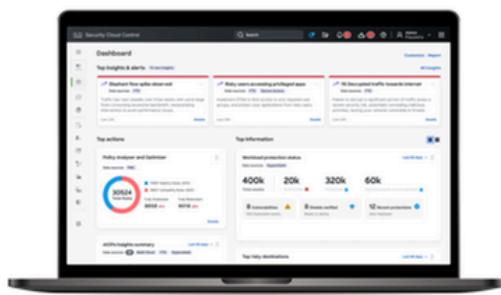
حەوت فەم ئىخأ بىوبت تامالۇ يىأ كىدل سىلىلەو SCC جراخ كنأ نم دكأت: ئەظحالىم.



Welcome to the Cisco Security Cloud

Delivered through Security Cloud Control (SCC)

Staying on top of security is easier than ever. Security Cloud Control helps you consistently manage policies across your Cisco security products. It is a cloud-based application that cuts through complexity to save time and keep your organization protected against the latest threats.



SCC complements FMC by allowing you to:

- Drive consistent policy through shared object management with FMCs
- Enable Zero-Touch Provisioning of FTDs
- View events in the cloud
- Get a centralized view of inventory across FMCs
- Leverage cloud CSDAC and Cloud Delivered FMC
- and more

To continue with cloud registration of your FMC, you will need a Cisco Security Cloud Sign On (SSO) user account.

If you don't already have a Cisco SSO account, please proceed below and Sign Up for free. Note that you will need to restart the cloud registration from your FMC after your new SSO account is created.

If you already have a Cisco SSO account, please proceed below to choose or create a free SCC account to register your FMC.

Let's get started!

1

Sign Up/Sign In with Cisco SSO

2

Register FMC with a SCC Tenant

[Continue to Cisco SSO](#)

ل ئامحلا رادج ئارادا زكرم ىلما مامضنالا ئيناكما

- **قف رقناو SCC رخأتسم رت خا**



Welcome to Security Cloud Control

To proceed with the registration of your FMC, please select a SCC tenant or enterprise to register with the FMC and verify the code displayed below matches the user code from your FMC.

Select Tenant Create Tenant

Search Tenants

cisco-jaiyadav

cisco-ngfw-us-sspt

cisco-vibobrov

default_enterprise

Grant Application Access

Compare the code below to the authorization code shown in the FMC tab. If the codes match, authorize the FMC to complete the registration. If the codes do not match, cancel registration.

8ABA15B5

FMC would like access to your SCC tenant **cisco-jaiyadav**.

- Users:** All internal users in FMC will have read-only access to this SCC tenant.
- Data:** FMC will be able to collect data using SCC APIs.

The FMC will be registered with tenant **cisco-jaiyadav**

Authorize FMC

ل ئامحلا رادى زىرىم ئىلما مامضنالا ئيناكما

- **قوف رقنا** Save

Firewall Management Center Integration / Cisco Security Cloud

Integration

Cisco Security Cloud: Enabled | Current Cloud Region: us-east-1 (US Region) | Security Services Exchange Tenant: SEC TAC | Cloud Onboarding Status: Not Available

Settings

Event Configuration

Send events to the cloud View your Events in Cisco Security Cloud

Intrusion events

File and malware events

Connection events

Security

All

Cisco AI Assistant for Security

Powered by generative AI and natural language processing, Cisco AI Assistant for Security enables you to create access control rules, query documentation and reference materials when required, and streamline your workflow. [Learn more](#)

Enable Cisco AI Assistant for Security

Policy Analyzer and Optimizer

Policy Analyzer & Optimizer evaluates access control rules to improve security and performance of the firewall. Recommendations can include removing redundant or unnecessary rules, consolidating similar rules, and reordering rules to reduce the number of rule evaluations required for each packet. [Learn more](#)

Enable Policy Analyzer and Optimizer

Cisco Security Cloud Support

Cisco cloud support services provide an enhanced support experience and maximize the value of the Cisco products. The management center establishes and maintains a secure connection to Cisco cloud to participate in additional service offerings from Cisco.

Enable Cisco Success Network

Enable Cisco Support Diagnostics

Cisco XDR Automation

Enable Cisco XDR Automation to allow a Cisco XDR user to build automated workflows that interact with various resources in the Secure Firewall Management Center. [Learn more](#)

Enable Cisco XDR Automation

Zero-Touch Provisioning (ZTP)

With ZTP, you can register your devices in management center by serial number, without performing any initial setup in the device. Management center integrates with Defense Orchestrator (DCO) for this functionality. You can either add a single device using a serial number and an access control policy, or add multiple devices simultaneously using serial numbers and a device template with preconfigured settings. [Learn more](#)

Enable Zero-Touch Provisioning

Save

ل ئيامحلا رادج ئارادا زكرم ىلا مامضنالا ئيناكما

نويحلا كلذل اونلاين Not Available Onboarding Status ۆللاح نم ۆللاح Cloud Onboarding Status ىلا بجي.

The screenshot shows the Cisco Security Cloud Integration page within the Firewall Management Center. It includes fields for Cisco Security Cloud (Enabled), Current Cloud Region (us-east-1 (US Region)), CDO Tenant (cisco-cisco-jayadav...surmpl), and Cloud Onboarding Status (Onboarding). A red box highlights the 'Cloud Onboarding Status' field.

The screenshot shows the Cisco Security Cloud Integration page within the Firewall Management Center. It includes fields for Cisco Security Cloud (Enabled), Current Cloud Region (us-east-1 (US Region)), CDO Tenant (cisco-cisco-jayadav...surmpl), and Cloud Onboarding Status (Online). A red box highlights the 'Cloud Onboarding Status' field.

ل ئيامحلا رادج ئارادا زكرم ىلا مامضنالا ۆللاح

- Platform Services > Security Devices > FTD ۆللاح نم ققحتو ىلا لقتنا

The screenshot shows the Security Devices page within the Security Cloud Control interface. The FTD tab is selected, displaying three entries: FTD-HA (FMC FTD High Availability), fmc_192.168.1.5_FT01 (FMC FTD Primary Active), and fmc_192.168.1.5_FT02 (FMC FTD Secondary Standby). All three devices are listed as Online.

ىلע نم آلا ئيامحلا رادج دىدەت دض ئيامحلا ۆللاح

ىلع FTD ۆلچسەن Zero Trust (uZTNA) ئيەملاعل ئوكبىش ىلا لوصولل تادادعىلا لىجسەن

ىلا لقتنا SCC:

- Platform Services > Security Devices > FTD > Device Management > Universal Zero Trust Network Access قوف رقنا

Security Devices

Name	Configuration Status	Connectivity
FTD-HA FMC FTD High Availability	Synced	Online
fmc_192.168.1.5_FTD1 FMC FTD Primary Active	Synced	Online
fmc_192.168.1.5_FTD2 FMC FTD Secondary Standby	Synced	Online

Device Details

- Name: FTD-HA
- Location: 192.168.1.1:443
- Model: Cisco Secure Firewall Threat Defense for VMware
- Type: FMC FTD
- Software Version: 7.7.10
- Managed By: fmc_192.168.1.5

Health

Device Management

- Device Overview
- Routing
- Interfaces
- Inline Sets
- DHCP
- VTEP
- High Availability
- Cluster
- Universal zero trust access settings**

Policies

- Access Control
- Intrusion
- Malware & File
- DNS
- Identity
- Decryption
- Prefilter
- NAT
- RA VPN

يملأ عالا ZTNA نيوكت - ةيامحلا راج ديدت دض نمآل اعافدلا

- **وصاخلا فعوملأا ةداهشلا يف اهؤاشنإ مت يتلا FTD ةداهش ليمحتو تامولعملأا ألماء ةيامحلا راج ديدت عاشناب (FTD)**

Enable Universal Zero Trust Access

Configure device for Universal Zero Trust Access

Firewall management center: FMC
Device: FTD-HA
Device FQDN: Enter device FQDN
Device identity certificate: Search and select certificate
Device interface(s): Select and search device Interface(s)
Auto deploy policy and rule enforcements to firewall device: Policy and rule enforcements will be deployed automatically to the selected device.

Quick help:

Device interface(s): For Cloud or Local enforcement

Choose an inside interface only to enable on-premises users to access private resources using the device's inside interface (also referred to as a DMZ interface).

For Local-only enforcement

Choose an inside and outside interface to enable users to access private resources regardless of user's location.

يملأ عالا ZTNA نيوكت - ةيامحلا راج ديدت دض نمآل اعافدلا

يملأ عالا ZTNA نويوك - ةيامحلا راج ديدت دض نمآل اعافدلا

يملأ عالا ZTNA نويوك - ةيامحلا راج ديدت دض نمآل اعافدلا



لک ليغشت ةداع او تارييغتلارشن متييـس، uZTNA يـلـع FTD HA نـيـكـمـت دـنـع: ةـظـحـالـمـ رـاطـإـ ـقـلـوـدـجـ نـمـ دـكـأـتـ. تـقـولـاـ سـفـنـ يـفـ (FTD) ةـيـامـحـلـاـ رـاجـ دـيدـتـ نـعـ عـافـدـلـاـ تـادـحـوـنـمـ بـسـانـمـ ةـنـايـصـ.

- تـالـجـسـلـاـ نـمـ قـقـحـتـلـلـ Workflow رـقـنـاـ

Security Devices

Name	Configuration Status	Connectivity
FTD-HA	Not Synced	Online

Device Details

- Name: FTD-HA
- Location: 192.168.1.11:443
- Model: Cisco Secure Firewall Threat Defense for VMware
- Type: FMC FTD
- Software Version: 7.730
- Managed By: FMC

Universal Zero Trust Access Settings - Last status

Device Actions

- Check for Changes
- Manage Licenses
- Workflows

ةيملأعـلـا زـنـيـوـكـتـ ةـلـاحـ - ةـيـامـحـلـا رـادـجـ دـيـدـتـ نـعـ نـمـآلـا عـافـدـلـا

Workflows

Name	Priority	Condition	Current State	Last Active	Start Time	End Time	Service
onDemandH2ZTNADeployOrchestratorStateMachine	On Demand	Active	Initiate Get Task Status Deployment Request	5/4/2025, 11:43:51 PM	5/4/2025, 11:43:00 PM	-	AEGIS

نـامـآلـا ةـبـاحـسـ يـفـ مـكـحـتـلـا لـمـعـ رـيـسـ

رـيـغـتـتـ وـرـتـ نـأـ كـنـكـمـيـ يـزـيـلـكـنـ إـلـاـ صـنـلـاـ لـيـصـافـتـ تـحـتـ Policy Deployment Status FMC.

Firewall Management Center

Deployment / Deployment History

Job Name	Deployed by	Start Time	End Time	Status	Deployment Notes
Deploy_Job_62	internaladmin	May 4, 2025 11:43 PM	May 4, 2025 11:44 PM	Completed	Security Cloud Control tr...

Transcript Details

```
FMC >> vpn-addr-assign local
FMC >> access-group CSM_FW_ACL_global
FMC >> zero-trust-hybrid
FMC >> listen-interface outside
FMC >> listen-interface inside
FMC >> proxy-fqdn ftd.taclab.com
FMC >> exit
FMC >> failover
FMC >> clear configuration session
***** INFRASTRUCTURE MESSAGES *****
["coreAllocationProfile":{"profileValue":"Universal ZTNA"}]
App/Sensor config Switch Successful in Active/Control Node;
Finalize in Data/Standby Node's App Config - Success- Node ID: [1]
```

ةـسـايـسـلـا رـشـنـ ةـلـاحـ - نـمـآلـا ةـيـامـحـلـا رـادـجـ ةـرـادـا زـكـرـمـ

نەمآلە لوصولە مادختساب لىيەتلىك ZTNA

نەمآلە لوصولە نىوكت



يە ، طب اورلا SSO و ئەدەش ئىلە دەتسەملە ZTA لىيەتلىك مادختساب كەنگەمى : ئەظحالم ئەدەشلى ئىلە دەتسەملە ZTA لىيەتلىك تاوطخ

نەمآلە لوصولە تامولۇم قىحول ئىلە لىقتىنە:

- **قوف رقنا Connect > End User Connectivity > Zero Trust Access**
- **قوف رقنا Manage**

The screenshot shows the Cisco Secure Access web interface. The top navigation bar includes the Cisco logo, 'Secure Access', and user information 'Jaikishan Yadav'. Below the navigation is a sidebar with icons for Home, Experience Insights, Connect (which is selected), and Resources. The main content area is titled 'End User Connectivity' and contains sub-sections for 'Zero Trust Access', 'Virtual Private Network', and 'Internet Security'. Under 'Zero Trust Access', there's a 'Enrollment methods' section with a note about client-based Zero Trust Access requiring endpoint devices to be enrolled. It shows options for Windows and macOS devices using SSO Authentication or Certificates, and Android and iOS devices using SSO Authentication only. A 'Manage' button is located in the top right of this section, which is highlighted with a red box.

نەمآلە لوصولە ZTA ئەدەش لىيەتلىك - نەمآلە لوصولە

- لىيەتلىك نىوكت فلم لىيزىنت و رىزجلا قىدىمىلە عەرمەلە ئەدەش لىيەتلىك

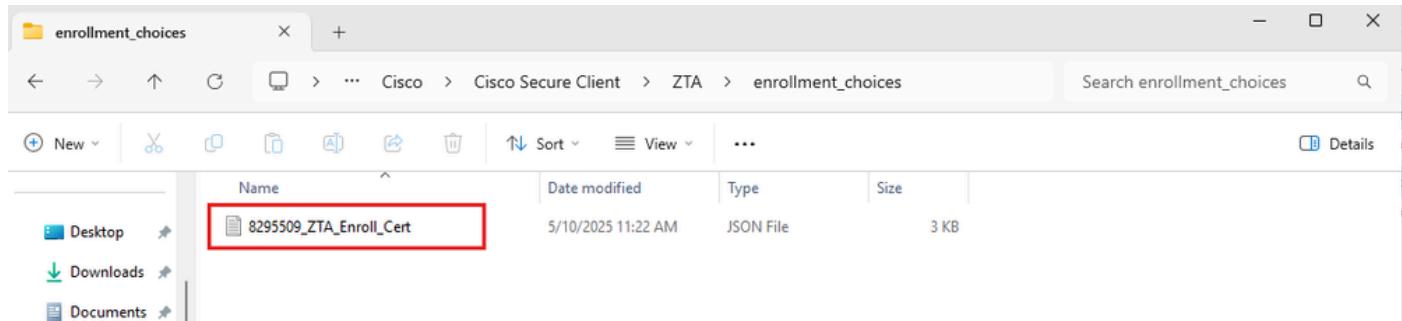
The screenshot shows the 'Windows and macOS devices' configuration page under 'Enrollment methods'. It includes sections for 'Use SSO Authentication' (with a note about requiring user action) and 'Use Certificates' (with a note about enrollment occurring without user action). There are steps for 'Upload a CA Certificate if necessary' (with a note about validating identity certificates) and 'Download the enrollment configuration file' (with a note about regenerating it each time a new CA certificate is uploaded). A 'CA Certificates' section shows a 'No CA certificates' button and a 'Upload a CA Certificate' button, with the latter highlighted with a red box. A 'Download' button for the configuration file '8295509_ZTA_Enroll_Cert.json' is also highlighted with a red box. A note at the bottom says you can also download the configuration file and Cisco Secure Client from the 'Download Cisco Secure client' page.

ةداهش ليچست - نمآلـا لوصولـا ZTA

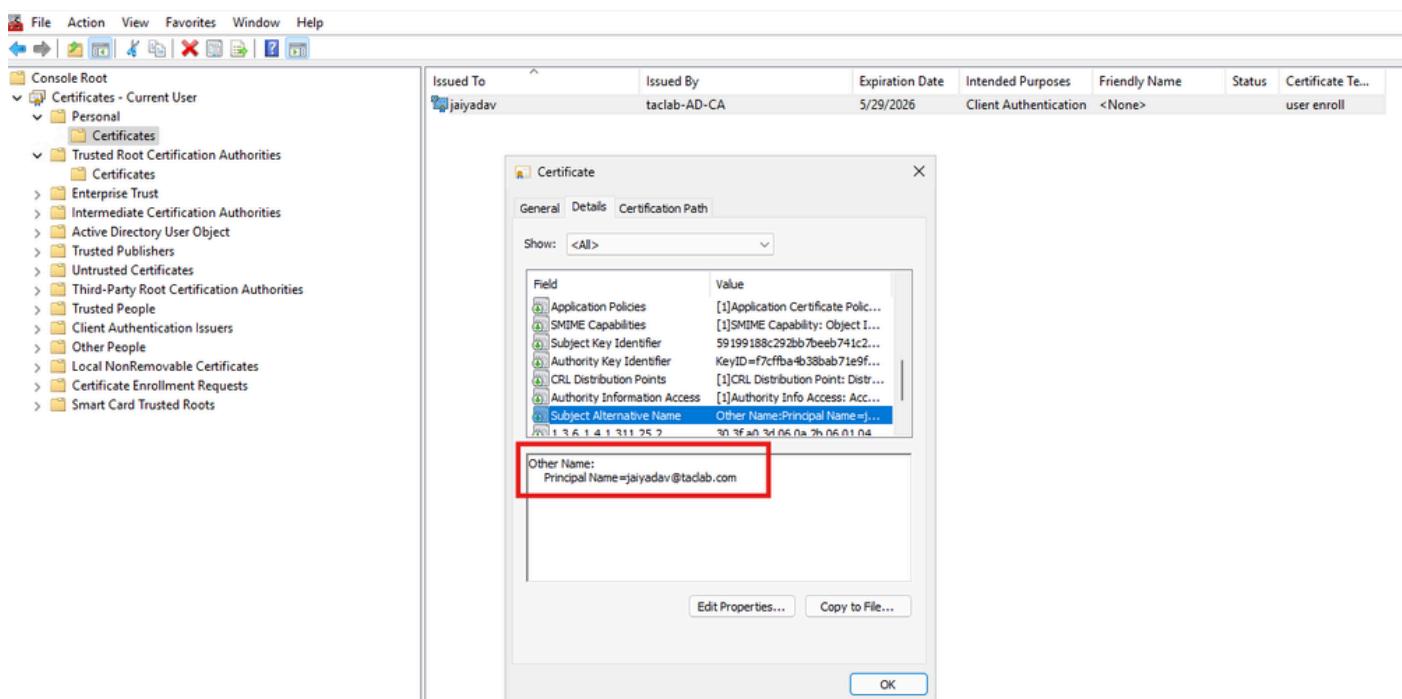
- قوف رقـنـا Save

ليـمعـلـا نـيـوـكـتـ

ىـلـا ليـجـسـتـلـا نـيـوـكـتـ فـلـمـ خـسـنـ C:\ProgramData\Cisco\Cisco Secure Client\ZTA\enrollment_choices



- يـفـ عـاشـنـا SAN Filed يـوتـحـيـ نـأـ بـجـيـ يـذـلـا Client Certicate



ةـدـاهـشـلـا تـيـبـثـتـ

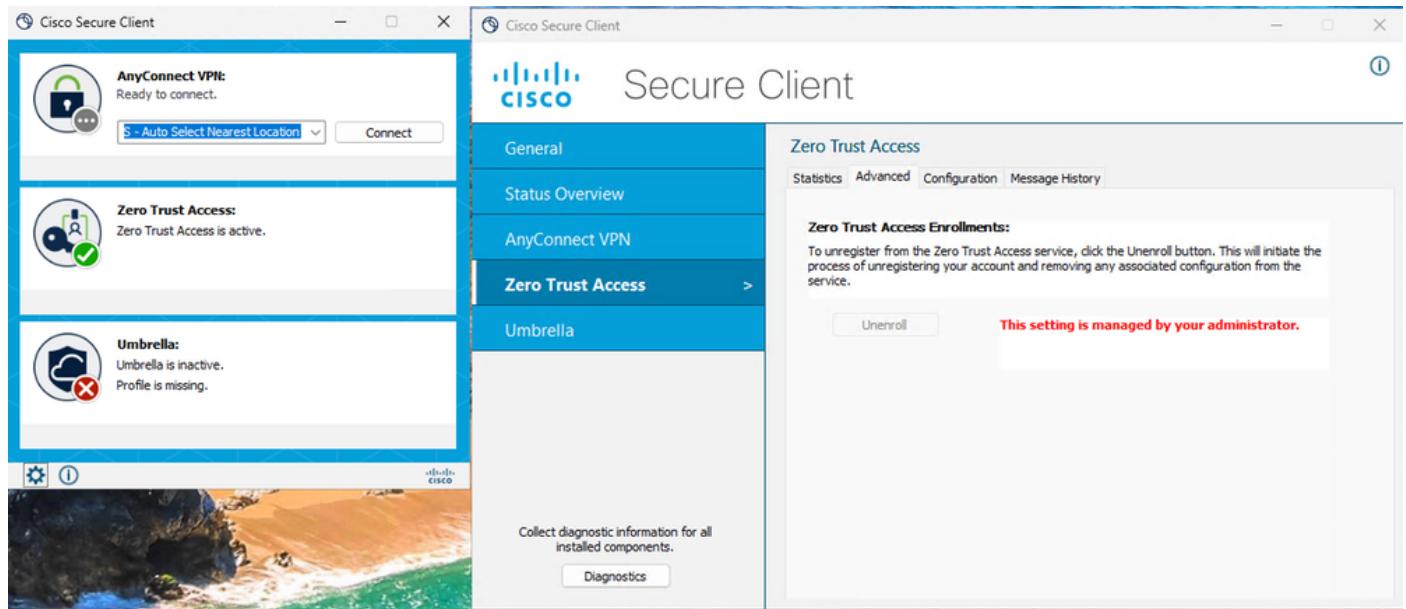
- Cisco Secure Client - Zero Trust Access Agent ليـغـشـتـ ةـدـاعـإـعـدـبـ

Services (Local)		
Name	Description	Status
Cisco Secure Client - Zero Trust Access Agent	Provides fac...	Running
Start the service	Enables opti...	
Description: Cisco Secure Client Zero Trust Access Agent Service	Enables opti...	
Cisco Secure Client - AnyConnect VPN Agent	This service ...	
Cisco Secure Client - ThousandEyes Endpoint Agent	Copies user ...	Running
Cisco Secure Client - Umbrella Agent	Cisco Secur...	Running
Cisco Secure Client - Umbrella SWG Agent	ThousandE...	Running
Cisco Secure Client - Zero Trust Acc	Cisco Secur...	
Client License Service (ClipSVC)	Provides inf...	
Clipboard User Service_11a11bf	This user se...	Running
Clipboard User Service_86240d	This user se...	Running
Cloud Backup and Restore Service_1	Monitors th...	
Cloud Backup and Restore Service_8	Monitors th...	
CNG Key Isolation	The CNG ke...	Running
COM+ Event System	Supports Sy...	Running
COM+ System Application	Manages th...	
Connected Devices Platform Service	This service ...	Running
Connected Devices Platform User Se	This user se...	Running
Connected Devices Platform User Se	This user se...	Running
Connected User Experiences and Te	The Connec...	Running

Extended / Standard /

تامدخ Windows

- ئي طمنلا ZTA ۋە دەلەج



نۇمۇلۇ لىچىسى ئەدەھىش زتا - زاتا لىچىسى

قىقىتلا نم حىصىل

(FTD) زامحىلى رادىج دىدەت ئىامحىلى uZTNA نىوكت نم قىقىتلىلى يلاتلا رمألا مىختىسأ:

```
show allocate-core profile  
show running-config universal-zero-trust
```

ةلص تاذ تامولعم

- نم تاليزنتل اوينفل ا معدلا Cisco
- نم نمآل لوصولا تامي لمعت زكرم Cisco
- ميمصت ليلد Cisco SASE

هـ لـ وـ لـ جـ رـ تـ لـ اـ هـ ذـ هـ

ةـ يـ لـ آـ لـ اـ تـ اـ يـ نـ قـ تـ لـ اـ نـ مـ مـ جـ مـ وـ عـ مـ اـ دـ خـ تـ سـ اـ بـ دـ نـ تـ سـ مـ لـ اـ اـ ذـ هـ تـ مـ جـ رـ تـ
لـ اـ عـ لـ اـ ءـ اـ حـ نـ اـ عـ يـ مـ جـ يـ فـ نـ يـ مـ دـ خـ تـ سـ مـ لـ لـ مـ عـ دـ ئـ وـ تـ حـ مـ يـ دـ قـ تـ لـ ةـ يـ رـ شـ بـ لـ اـ وـ
اـ مـ كـ ةـ قـ يـ قـ دـ نـ وـ كـ تـ نـ لـ ةـ يـ لـ آـ ةـ مـ جـ رـ تـ لـ ضـ فـ اـ نـ اـ ةـ ظـ حـ اـ لـ مـ ئـ جـ رـ يـ .ـ صـ اـ خـ لـ اـ مـ هـ تـ غـ لـ بـ
يـ لـ خـ تـ .ـ فـ رـ تـ حـ مـ مـ جـ رـ تـ مـ اـ هـ دـ قـ يـ يـ تـ لـ اـ ةـ يـ فـ اـ رـ تـ حـ اـ لـ اـ ةـ مـ جـ رـ تـ لـ اـ عـ مـ لـ اـ حـ لـ اـ وـ
ىـ لـ إـ أـ مـ ئـ اـ دـ عـ وـ جـ رـ لـ اـ بـ يـ صـ وـ تـ وـ تـ اـ مـ جـ رـ تـ لـ اـ هـ ذـ هـ ةـ قـ دـ نـ عـ اـ هـ تـ يـ لـ وـ ئـ سـ مـ
(رـ فـ وـ تـ مـ طـ بـ اـ رـ لـ اـ)ـ يـ لـ صـ أـ لـ اـ يـ زـ يـ لـ جـ نـ إـ لـ اـ دـ نـ تـ سـ مـ لـ اـ).