

Configurazione dell'accesso sicuro per Universal ZTNA con FMC gestito in locale su SCC

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Esempio di rete](#)

[Informazioni sulle parentesi](#)

[Dispositivi supportati](#)

[Limitazioni](#)

[Configurazione](#)

[Verifica versione FMC](#)

[Verifica versione FTD](#)

[Verifica licenze FTD](#)

[Verificare le impostazioni della piattaforma e il DNS configurato correttamente](#)

[Crea un tenant di controllo del cloud di sicurezza su CDO](#)

[Verificare che le impostazioni generali di SCC Firewall siano configurate](#)

[Verificare l'integrazione di Secure Access Tenant e Security Control Firewall Management Base](#)

[Genera certificato firmato CA Firewall Threat Defense \(FTD\)](#)

[Centro gestione firewall locale integrato per Security Cloud Control](#)

[Registra impostazioni Universal Zero Trust Network Access \(uZTNA\) su FTD](#)

[Registrare il client con uZTNA](#)

[Configurazione accesso sicuro](#)

[Configurazione client](#)

[Verifica](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come configurare Universal ZTNA con Secure Access e FTD virtuale gestiti da un FMC virtuale locale.

Prerequisiti

- È necessario installare Firewall Management Center (FMC) e Firewall Threat Defense (FTD) utilizzando la versione software 7.7.10 o successiva.
- Firewall Threat Defense (FTD) deve essere gestito dal Centro gestione firewall
- Firewall Threat Defense (FTD) deve essere concesso in licenza con crittografia (la

- crittografia avanzata deve essere abilitata con la funzionalità di esportazione abilitata), licenze IPS e Threat necessarie per i controlli di sicurezza
- La configurazione di base di Firewall Threat Defense (FTD) deve essere eseguita da Firewall Management Center (FMC), ad esempio interfaccia, routing e così via.
 - Per risolvere il nome di dominio completo dell'app, è necessario applicare la configurazione DNS nel dispositivo dal FMC
 - La versione di Cisco Secure Client deve essere 5.1.10 o successiva
 - Il controllo del cloud di sicurezza è fornito ai clienti con i flag delle microapplicazioni firewall e Secure Access e delle funzionalità UZTNA abilitati

Requisiti

- Tutti i dispositivi Secure Firewall Management Center (FMC), inclusi cdFMC e Firewall Threat Defense (FTD), devono eseguire il software versione 7.7.10 o successive.
- Firewall Threat Defense (FTD) deve essere gestito da Firewall Management Center; local manager Firewall Defense Manager (FDM) non è supportato
- Tutti i dispositivi Firewall Threat Defense (FTD) devono essere configurati per la modalità routing; modalità trasparente non supportata.
- I dispositivi del cluster non sono supportati.
- Sono supportati dispositivi ad alta disponibilità (HA); vengono visualizzati come un'unica entità.
- Secure Client versione 5.1.10 o successive

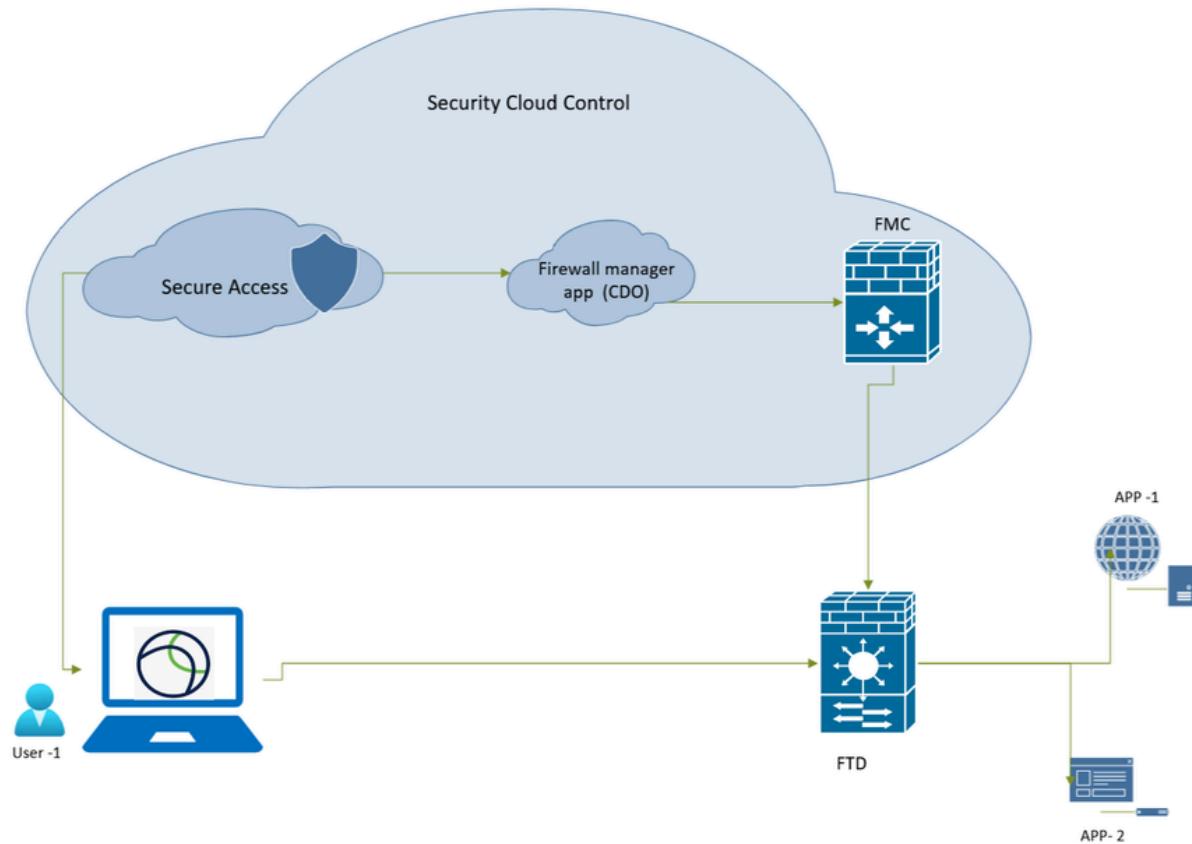
Componenti usati

Le informazioni di questo documento si basano

- Security Cloud Control (SCC)
- Secure Firewall Management Center (FMC) versione 7.7.10
- Virtual Secure Firewall Threat Defense (FTD) -100 versione 7.7.10
- Secure Client per Windows versione 5.1.10
- Accesso sicuro

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Esempio di rete



Accesso sicuro - Topologia di rete

Informazioni sulle parentesi

Dispositivi supportati

Modelli supportati di difesa dalle minacce Secure Firewall:

- FPR 1150
- FPR 3105, 3110, 3120, 3130, 3140
- FPR4115, 4125, 4145, 4112
- FPR4215, 4225, 4245
- Virtuale Firewall Threat Defense (FTD) con almeno 16 core CPU

Limitazioni

- Condivisione oggetti
- IPv6 non supportato.
- È supportata solo la VRF globale.
- I criteri ZTNA universali non vengono applicati al traffico del tunnel da sito a sito verso un dispositivo.
- I dispositivi del cluster non sono supportati.

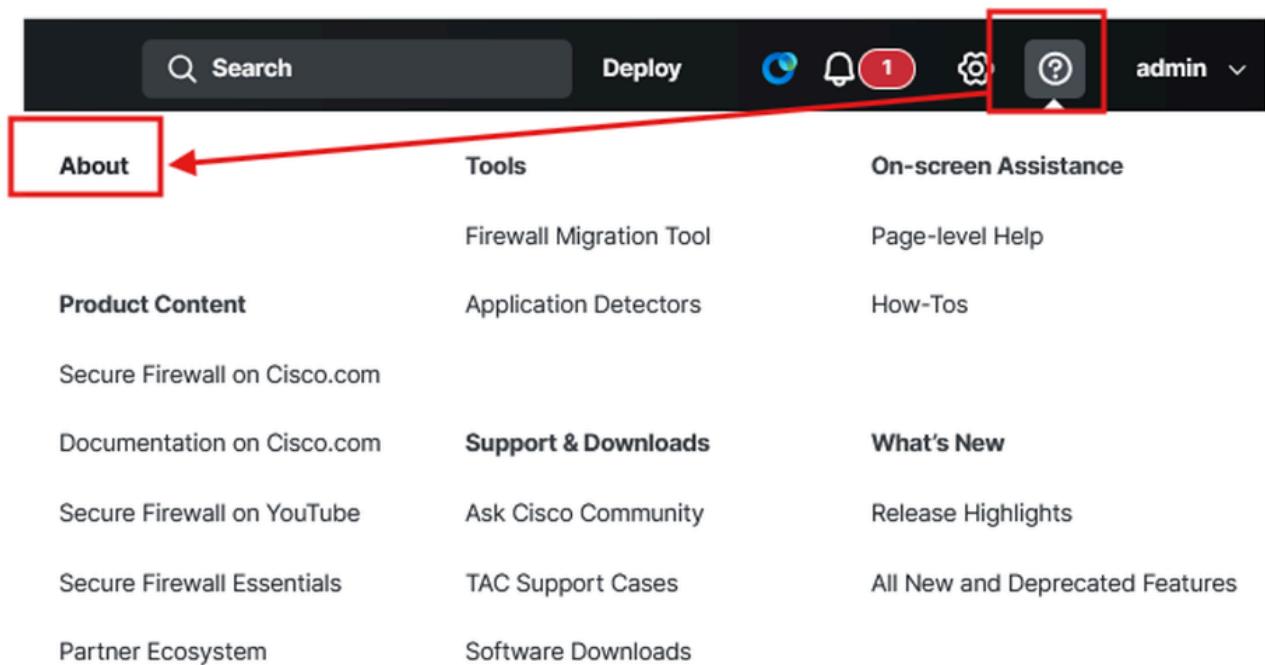
- Gli FTD distribuiti come contenitori sulle serie firepower 4K e 9K non sono supportati
- Le sessioni universali ZTNA non supportano i frame jumbo

Configurazione

Verifica versione FMC

Verificare che Firewall Management Center e Firewall FTD siano in esecuzione sulla versione software supportata per ZTNA universale (può essere 7.7.10 o superiore):

- Fare clic su ?(angolo superiore destro) e fare clic su About





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](#)

Secure Firewall Management Center - Versione software

Verifica versione FTD

Passare all'interfaccia utente di FMC:

- Fai clic su **Devices > Device Management**

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

Secure Firewall Threat Defense - Versione software

Verifica licenze FTD

- Fare clic su Setting Icon > Licenses > Smart Licenses



Configuration	Health	Monitoring
Users	Monitor	Audit
Domains	Policy	Syslog
Product Upgrades	Events	Statistics
Content Updates	Exclude	
	Monitor Alerts	Tools
Licenses		Backup/Restore
Smart Licenses		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)					

Secure Firewall Threat Defense - Licenze Smart

Verificare le impostazioni della piattaforma e il DNS configurato correttamente

Accesso all'FTD tramite CLI:

- Eseguire il comando per verificare se DNS è configurato:

```
show run dns
```

Nel CCP:

- Fai clic su Devices>Platform Settings, modifica o crea un nuovo criterio

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

Protezione da minacce firewall - Criteri piattaforma

The screenshot shows the Cisco ISE Platform Policy configuration interface. On the left, there's a sidebar with navigation links like Home, Overview, Analysis, Policies, Devices, Objects, and Integration. The main area is titled 'Platform_Policy' and has a sub-section for 'DNS'. A modal window titled 'Edit DNS Server Group' is open, showing a dropdown for 'Select DNS Group' set to 'Lab-DNS (Default)', a checked checkbox for 'Make as default', and a text input for 'Filter Domains'. Below the modal, there are fields for 'Expiry Entry Timer' (set to 1) and 'Poll Timer' (set to 240). At the bottom right of the modal are 'Cancel' and 'OK' buttons. The background shows a list of DNS resolution settings and interface objects.

Protezione da minacce del firewall - Configurazione DNS

Verificare tramite CLI FTD che sia possibile eseguire il ping dell'indirizzo IP e del nome FQDN delle risorse private (se si desidera accedere a PR utilizzando il relativo nome FQDN).

```
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#
```

Crea un tenant di controllo del cloud di sicurezza su CDO



Nota: Se è già stato configurato un tenant SCC, non è necessario creare un nuovo tenant.

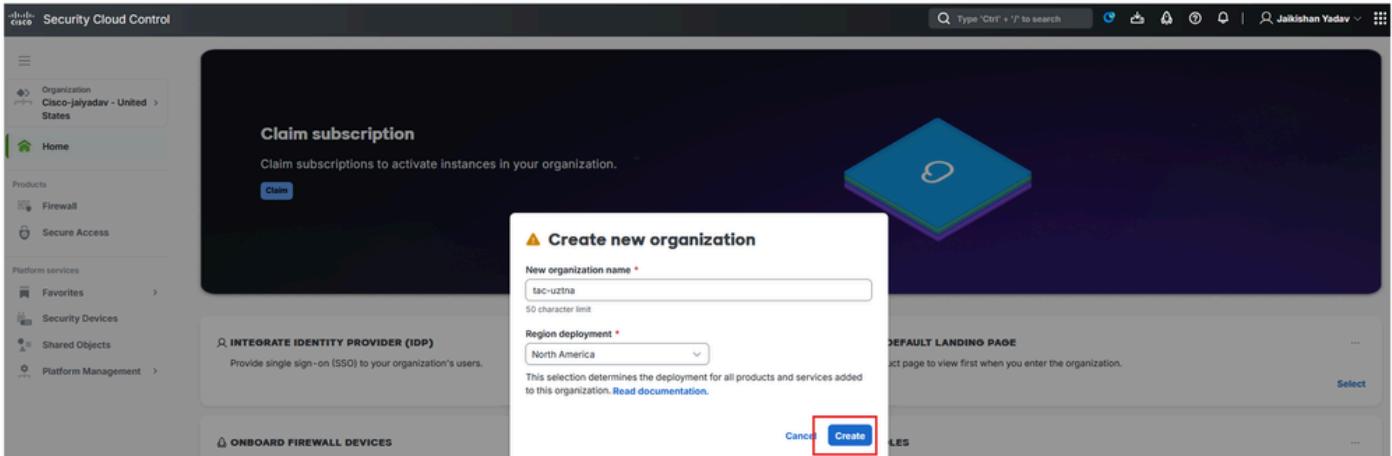
Passare a [Security Cloud Control](#):

- Fare clic su Organization > Create new organization

The screenshot shows the Security Cloud Control interface. On the left, there's a sidebar with 'Organization' (Cisco-Jaiyadav - United States), 'Home', and 'Products'. A modal window titled 'Select an organization' is open, with a search bar and a 'Create new organization' button. The main area has a dark background with a blue graphic on the right.

Secure Cloud Control - Organizzazione

- Fare clic su Create



Secure Cloud Control - Creazione di organizzazioni

Una volta creato il tenant SCC, raccogliere le informazioni sul tenant per abilitare la microapp Firewall e accesso sicuro e per abilitare uZTNA.

Verificare che le impostazioni generali di SCC Firewall siano configurate

Passare a [CDO/SCC](#):

- Fai clic su **Administration > General Settings**
- Assicurarsi che l'opzione sia **Auto onboard On-Prem FMCs from Cisco Security Cloud** **attivata**.



Nota: L'utente che tenta di accedere a Secure Access MicroApp deve disporre di ruoli di amministratore Secure Access e Security Cloud Control.

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 is 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 "Auto onboard On-Prem FMCs from Cisco Security Cloud" toggle switch is highlighted with a red box. Below it, the "Tenant ID" field (containing "cbc") and the "Secure Services Exchange Tenant ID" field (containing "?") are also highlighted with a red box. A note on the right side of the page states: "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](#)."

Secure Cloud Control - Dettagli organizzazione

Verificare l'integrazione di Secure Access Tenant e Security Control Firewall Management Base

Secure Cloud Control - Attivazione accesso sicuro

Una volta completato il passaggio [Creazione di un tenant di controllo del cloud di sicurezza su CDO](#) e [Creazione di un tenant di controllo del cloud di sicurezza su CDO](#), è possibile visualizzare le micro app di firewall e accesso sicuro sul dashboard SCC:

Controllo Secure Cloud - Micro App

Genera certificato firmato CA Firewall Threat Defense (FTD)



Nota: È inoltre possibile utilizzare i [certificati FTD](#) autofirmati FTD (fare riferimento alla sezione Generazione di certificati CA interni e autofirmati). Il certificato deve essere in formato PKCS12 e deve essere presente nell'archivio del computer dell'utente in una CA radice attendibile.

Per generare un certificato firmato da un'autorità di certificazione utilizzando FTD nella funzione build openssl:

- Passa a FTD
- Esegui `expert` comando
- Genera CSR e chiave tramite openssl
 - Comando OpenSSL:

```
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
```

Richiesta di firma del certificato

- Copiare il CSR e ottenere un certificato firmato dall'autorità di certificazione
- Usa chiave e certificato firmati CA FTD e converti il certificato nel formato PKCS12
 - Comando OpenSSL:

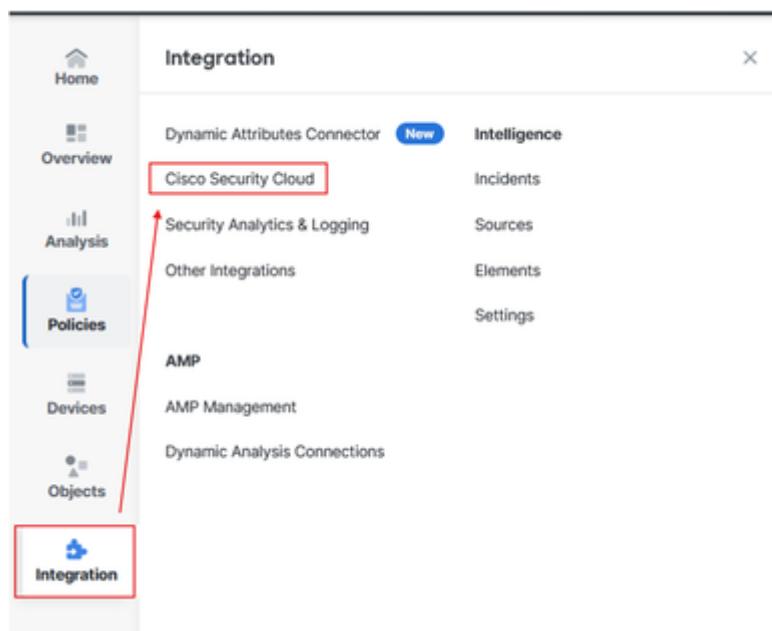
```
openssl pkcs12 -export -out ftdcert.p12 -in cert.crt -inkey cert.key
```

- Esportare il certificato utilizzando SCP o un altro strumento.

Centro gestione firewall locale integrato per Security Cloud Control

Passare al CCP:

- Fai clic su Integration > Cisco Security Cloud



Integrazione di Centro gestione firewall e SCC

- Scegliere l'area cloud, quindi fare clic su Enable Cisco Security Cloud

The screenshot shows the 'Integration' tab selected in the left sidebar. In the main content area, there's a section titled 'Cisco Security Cloud Integration'. It includes fields for 'Current Cloud Region' (set to 'us-east-1 (US Region)'), 'Security Services Exchange Tenant' (SEC TAC), and 'Cloud Onboarding Status' (Not Available). A red box highlights the 'Current Cloud Region' dropdown and the 'Enable Cisco Security Cloud' button below it. Another red box highlights the 'Enable Cisco Security Cloud' button.

Integration

Current Cloud Region: us-east-1 (US Region) Enable Cisco Security Cloud

Security Services Exchange Tenant: SEC TAC

Cloud Onboarding Status: Not Available

Settings

Event Configuration:

- Send events to the 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

Onboarding di Firewall Management Center in SCC

Verrà aperta una nuova scheda del browser nella nuova scheda:

- Fare clic su Continue to Cisco SSO



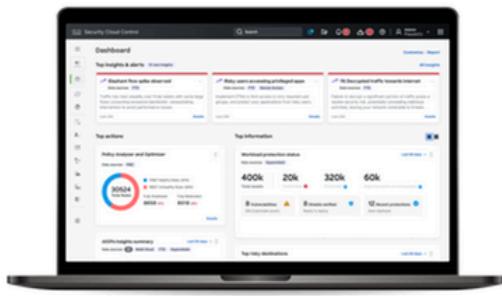
Nota: Accertarsi di essere disconnessi da SCC e di non avere altre schede aperte.



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](#)

Onboarding di Firewall Management Center in SCC

- Scegliere il tenant SCC e fare clic su Authorize FMC



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

Onboarding di Firewall Management Center in SCC

- Fare clic su 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 | Learn more ↗

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

Onboarding di Firewall Management Center in SCC

Lo stato di deve Cloud Onboarding Status essere modificato da **Not Available** a **Onboarding Online**.

The screenshot shows the 'Cisco Security Cloud Integration' section of 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...surmp), and 'Cloud Onboarding Status' (Onboarding). A red box highlights the 'Cloud Onboarding Status' field.

The screenshot shows the 'Cisco Security Cloud Integration' section of 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...surmp), and 'Cloud Onboarding Status' (Online). A red box highlights the 'Cloud Onboarding Status' field.

Stato di caricamento di Centro gestione firewall

- Passare a [SCC](#) e controllare lo stato FTD in Platform Services > Security Devices

The screenshot shows the 'Security Devices' section of the Security Cloud Control interface. Under the 'FTD' tab, there is a table listing three devices: 'FTD-HA' (Synced, Online), 'fmc_192.168.1.5_FT01' (Synced, Online), and 'fmc_192.168.1.5_FT02' (Synced, Online).

Name	Configuration Status	Connectivity
FTD-HA FMC FTD High Availability	Synced	Online
fmc_192.168.1.5_FT01 FMC FTD Primary Active	Synced	Online
fmc_192.168.1.5_FT02 FMC FTD Secondary Standby	Synced	Online

Stato di difesa dalle minacce del firewall sicuro su SCC

Registra impostazioni Universal Zero Trust Network Access (uZTNA) su FTD

Passare a SCC:

- Fare clic su Platform Services > Security Devices > FTD > Device Management > Universal Zero Trust Network Access

Screenshot of the Cisco Security Cloud Control interface showing the 'Security Devices' section.

The left sidebar shows navigation paths: Home, Products (Firewall, Secure Access), Platform services (Platform favorites, Security Devices), Shared Objects, and Platform Management.

The main area displays a table of 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

Details for the selected device (FTD-HA) are shown on the right:

- 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 (4)
- Device Management:**
 - Device Overview
 - Routing
 - Interfaces
 - Inline Sets
 - DHCP
 - VTEP
 - High Availability
 - Cluster
 - Universal zero trust access settings** (5)
- Policies:**
 - Access Control
 - Intrusion
 - Malware & File
 - DNS
 - Identity
 - Decryption
 - Prefilter
 - NAT
 - RA VPN

Secure Firewall Threat Defense - Configurazione ZTNA universale

- Compilare le informazioni e caricare il certificato FTD generato nella fase [Generate Firewall Threat Defense \(FTD\) CA signed certificate](#)

Screenshot of the Cisco Security Cloud Control interface showing the 'Enable Universal Zero Trust Access' configuration page.

The left sidebar shows navigation paths: Home, Products (Firewall, Secure Access), Platform services (Favorites, Security Devices, Shared Objects, Platform Management).

The main area shows the configuration for a device (FTD-HA):

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 (+ Add certificate)
- Device Interface(s): Select and search device Interface(s)
- Auto deploy policy and rule enforcements to firewall device

Quick help:

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). Diagram: User in a trusted network connected to Inside Interface (Local Network) of the device, which then connects to the Internet.

For Local-only enforcement: Choose an inside and outside interface to enable users to access private resources regardless of user's location. Diagram: User in a trusted network connected to Inside Interface (Local Network) of the device, which then connects to Outside Interface (Internet) of the device, which finally connects to a Remote user.

Deploy

Secure Firewall Threat Defense - Configurazione ZTNA universale

Secure Firewall Threat Defense - Configurazione ZTNA universale

Secure Firewall Threat Defense - Configurazione ZTNA universale



Nota: Quando si abilita uZTNA su FTD HA, le modifiche vengono distribuite e le unità Firewall Threat Defense (FTD) vengono riavviate contemporaneamente. Assicurarsi di pianificare una finestra di manutenzione adeguata.

- Fare clic su Workflow per controllare i registri

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

Secure Firewall Threat Defense - Stato configurazione ZTNA universale

Name	Priority	Condition	Current State	Last Active	Start Time	End Time	Service	Result
onDemandZTNADeployOrchestratorStateMachine	On Demand	Active	Initiate Get Task Status Deployment Request	5/4/2025, 11:43:51 PM	5/4/2025, 11:43:00 PM	-	AEGIS	Abort
ACTION	TIME		STARTSTATE		ENDSTATE			RESULT
EmptyOnNothingStateMachineAction	05/04/2025 11:43:01 PM / 05/04/2025 11:43:01 PM		INITIATE_UNIVERSAL_ZTNA_DEPLOY_ORCHESTRATOR		GET_DEVICE_RECORDS			SUCCESS
TriggerFmcAction	05/04/2025 11:43:01 PM / 05/04/2025 11:43:01 PM		GET_DEVICE_RECORDS		WAIT_FOR_OOB_TO_FINISH			SUCCESS
FmcOnNothingOobCompletionHandler	05/04/2025 11:43:05 PM / 05/04/2025 11:43:05 PM		WAIT_FOR_OOB_TO_FINISH		SUBMIT_CERTIFICATE_ENROLLMENT_FETCH_REQUEST			SUCCESS
FmcRequestCertEnrollmentAction	05/04/2025 11:43:05 PM / 05/04/2025 11:43:06 PM		SUBMIT_CERTIFICATE_ENROLLMENT_FETCH_REQUEST		SUBMIT_CERTIFICATE_ENROLLMENT_FETCH_REQUEST_WAIT			SUCCESS
FmcReceivedPgesAccumulator	05/04/2025 11:43:09 PM / 05/04/2025 11:43:09 PM		AVAIT_RESPONSE_FROM_EXECUTE_INCHIEQUESTS		PROCESS_FETCHED_CERTIFICATE_ENROLLMENT_DATA			SUCCESS
FmcProcessCertEnrollmentData	05/04/2025 11:43:09 PM / 05/04/2025 11:43:09 PM		PROCESS_FETCHED_CERTIFICATE_ENROLLMENT_DATA		TRIGGER_CERT_CONFIG_SYNC			SUCCESS
TriggerCertConfigSync	05/04/2025 11:43:09 PM / 05/04/2025 11:43:09 PM		TRIGGER_CERT_CONFIG_SYNC		POLL_FOR_CERT_CONFIG_SYNC_TO_FINISH			SUCCESS
CheckPollTimeOut	05/04/2025 11:43:09 PM / 05/04/2025 11:43:09 PM		POLL_FOR_CERT_CONFIG_SYNC_TO_FINISH		CHECK_CERT_CONFIG_SYNC_STATUS			SUCCESS
FetchAndProcessCertConfigSyncStatus	05/04/2025 11:43:09 PM / 05/04/2025 11:43:09 PM		CHECK_CERT_CONFIG_SYNC_STATUS		WAIT_FOR_CERT_CONFIG_SYNC_TO_FINISH			POLL_FOR_CERT_CONFIG_SYNC_TO_FINISH
NoOpSleepStateMachineAction	05/04/2025 11:43:09 PM / 05/04/2025 11:43:30 PM		WAIT_FOR_CERT_CONFIG_SYNC_TO_FINISH		POLL_FOR_CERT_CONFIG_SYNC_TO_FINISH			SUCCESS
CheckPollTimeOut	05/04/2025 11:43:30 PM / 05/04/2025 11:43:30 PM		POLL_FOR_CERT_CONFIG_SYNC_TO_FINISH		CHECK_CERT_CONFIG_SYNC_STATUS			SUCCESS
FetchAndProcessCertConfigSyncStatus	05/04/2025 11:43:30 PM / 05/04/2025 11:43:30 PM		CHECK_CERT_CONFIG_SYNC_STATUS		CLEANUP_CERT_CONFIG_SYNC_POLL_DATA			SUCCESS
CleanPollingData	05/04/2025 11:43:30 PM / 05/04/2025 11:43:30 PM		CLEANUP_CERT_CONFIG_SYNC_POLL_DATA		POLL_FOR_DEPLOYMENT_TO_FINISH_IF_ANY			SUCCESS
CheckPollTimeOut	05/04/2025 11:43:30 PM / 05/04/2025 11:43:30 PM		POLL_FOR_DEPLOYMENT_TO_FINISH_IF_ANY		GET_DEPLOY_VERSION_TIMESTAMP			SUCCESS
FmcRequestDeployVersionTimestampAction	05/04/2025 11:43:30 PM / 05/04/2025 11:43:30 PM		GET_DEPLOY_VERSION_TIMESTAMP		WAIT_FOR_DEPLOY_VERSION_TIMESTAMP			SUCCESS
FmcGetDeployVersionTimestampOrPollIfDeployingForADeviceResponseHandler	05/04/2025 11:43:33 PM / 05/04/2025 11:43:33 PM		AVAIT_RESPONSE_FROM_EXECUTE_INCHIEQUESTS		CLEANUP_EXISTING_DEPLOY_POLL_DATA			SUCCESS

Flusso di lavoro di controllo del cloud di sicurezza

In Dettagli trascrizione è possibile visualizzare Policy Deployment Status e modificare FMC.

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 tri...
FTD-HA					
Deploy_Job_61	internaladmin				Security Cloud Control tri...
Deploy_Job_60	internaladmin				Security Cloud Control tri...
Deploy_Job_59	internaladmin				Uztna specific deploymen...
Deploy_Job_58	internaladmin				Security Cloud Control tri...
Deploy_Job_57	internaladmin				Uztna specific deploymen...
Deploy_Job_56	internaladmin				Security Cloud Control tri...
Certificate_Job_9	System				Certificate deployment
Deploy_Job_55	admin				
Deploy_Job_54	admin				
Deploy_Job_53	System				High availability create

Transcript Details

```
***** 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]
```

Centro gestione firewall protetto - Stato distribuzione criteri

Registrare il client con uZTNA

Configurazione accesso sicuro



Nota: È possibile utilizzare la registrazione SSO o una registrazione ZTA basata su certificato. Di seguito sono riportati i passaggi per la registrazione ZTA basata su certificati

Passare a [Dashboard accesso protetto](#):

- Fare clic su Connect > End User Connectivity > Zero Trust Access
- Fare clic su Manage

The screenshot shows the Cisco Secure Access interface. In the top navigation bar, 'Secure Access' is selected. Under 'End User Connectivity', the 'Zero Trust Access' tab is active. On the left sidebar, 'Connect' is highlighted. The main content area displays information about enrollment methods, stating that users can access resources using client-based Zero Trust Access. It includes links for 'SSO Authentication' and 'Certificates'. A red box highlights the 'Manage' button located at the top right of this section.

Accesso sicuro - Registrazione certificato ZTA

- Carica il certificato CA radice e scarica il file di configurazione della registrazione

The screenshot shows the Cisco Secure Access interface with the following details:

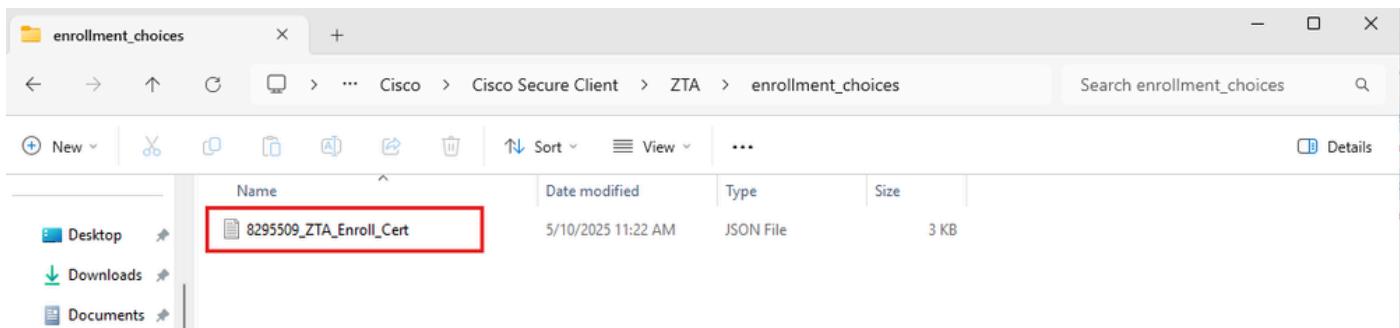
- Header:** Cisco Secure Access
- Left Sidebar:** Home, Experience Insights, Connect, Resources, Secure, Monitor, Admin, Workflows.
- Current Page:** Enrollment methods (under Zero Trust Access).
- Content:**
 - Windows and macOS devices:**
 - Use SSO Authentication:** Enrollment requires user action.
 - Use Certificates:** Enrollment occurs without user action.
 - 1. Upload a CA Certificate if necessary:** At least one uploaded root certificate or certificate chain must be able to validate identity certificates on endpoint devices during zero trust enrollment and renewal.
 - CA Certificates:** No CA certificates (button highlighted with a red box) | **Upload a CA Certificate** (button highlighted with a red box).
 - 2. Download the enrollment configuration file:** The file is regenerated each time a new CA certificate is uploaded. Deploy this file to user devices.
 - Download** 8295509_ZTA_Enroll_Cert.json (button highlighted with a red box).
 - You can also download this configuration file and Cisco Secure Client from the [Download Cisco Secure clientpage](#).
- Buttons at the bottom:** Save (highlighted with a red box), Cancel.

Accesso sicuro - Registrazione certificato ZTA

- Fare clic su Save

Configurazione client

Copiare il file di configurazione della registrazione in C:\ProgramData\Cisco\Cisco Secure Client\ZTA\enrollment_choices



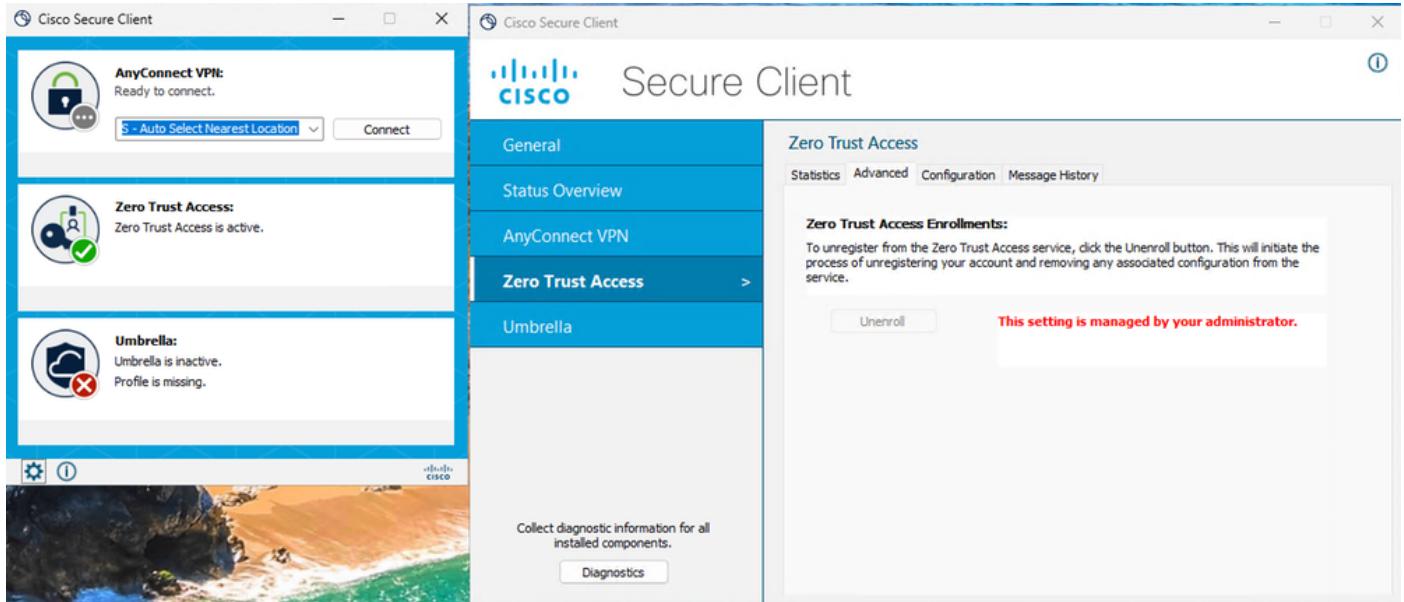
- Creare un certificato client, che deve avere un UPN nel campo SAN

Installazione certificato

- **Avvia/Riavvia** Cisco Secure Client - Zero Trust Access Agent

Servizi Windows

- **Verificare lo stato del modulo ZTA**



Accesso sicuro - Stato registrazione certificato ZTA

Verifica

Utilizzare il comando successivo per verificare la configurazione uZTNA su Firewall Threat Defense (FTD):

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

Informazioni correlate

- [Supporto tecnico Cisco e download](#)
- [Cisco Secure Access Help Center](#)
- [Guida alla progettazione di Cisco BASE](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuracy di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).