

Configura & Autenticazione SAML DUO

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione delle fasi su DUO](#)

[Creare un criterio di protezione delle applicazioni](#)

[Crea criterio di applicazione](#)

[Procedura di configurazione di FMC](#)

[Distribuisce certificato di identità nell'FTD](#)

[Distribuisce certificato IDP nell'FTD](#)

[Creazione dell'oggetto SAML SSO](#)

[Crea configurazione RAVPN \(Virtual Private Network\) di accesso remoto](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Numero 1: Autenticazione del certificato non riuscita.](#)

[numero 2: Errori SAML](#)

Introduzione

Questo documento descrive un esempio di implementazione dell'autenticazione basata su certificati e dell'autenticazione DUO SAML.

Prerequisiti

Gli strumenti e i dispositivi utilizzati nella guida sono:

- Cisco Firepower Threat Defense (FTD)
- Firepower Management Center (FMC)
- CA (Certification Authority) interna
- Cisco DUO Premier Account
- Cisco DUO Authentication Proxy
- Cisco Secure Client (CSC)

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- VPN di base,
- SSL/TLS

- Infrastruttura a chiave pubblica
- Esperienza con FMC
- Cisco Secure Client
- Codice FTD 7.2.0 o superiore
- Cisco DUO Authentication Proxy

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco FTD (7.3.1)
- Cisco FMC (7.3.1)
- Cisco Secure Client (5.0.02075)
- Cisco DUO Authentication Proxy (6.0.1)
- Mac OS (13.4.1)
- Active Directory

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.

Configurazione delle fasi su DUO

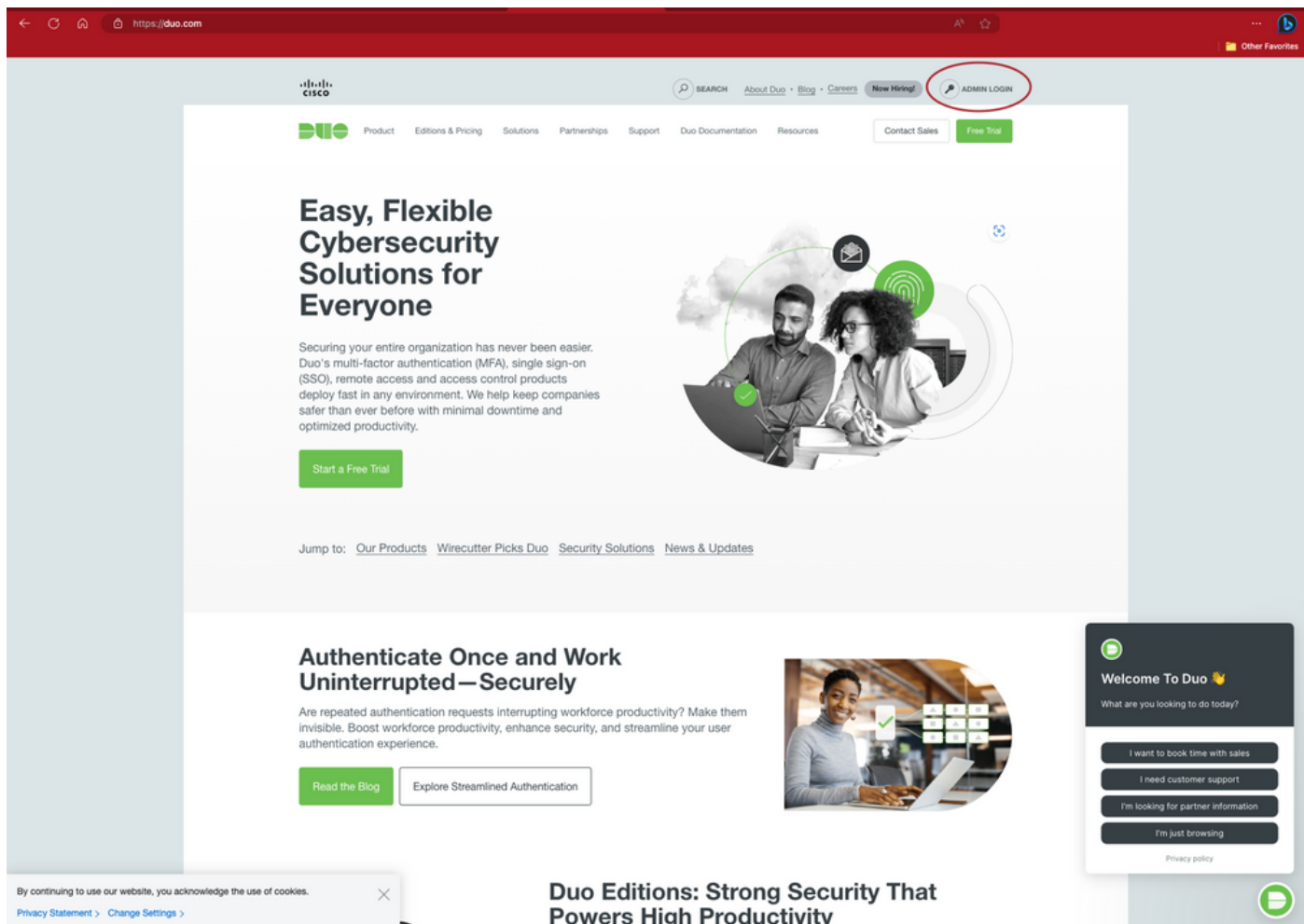
In questa sezione vengono descritti i passaggi per configurare Cisco DUO Single Sign-on (SSO). Prima di iniziare, verificare che il proxy di autenticazione sia implementato.



Avviso: Se non è stato implementato un proxy di autenticazione, questo collegamento contiene la guida per questa attività. [DUO Authentication Proxy Guide](#)

Creare un criterio di protezione delle applicazioni

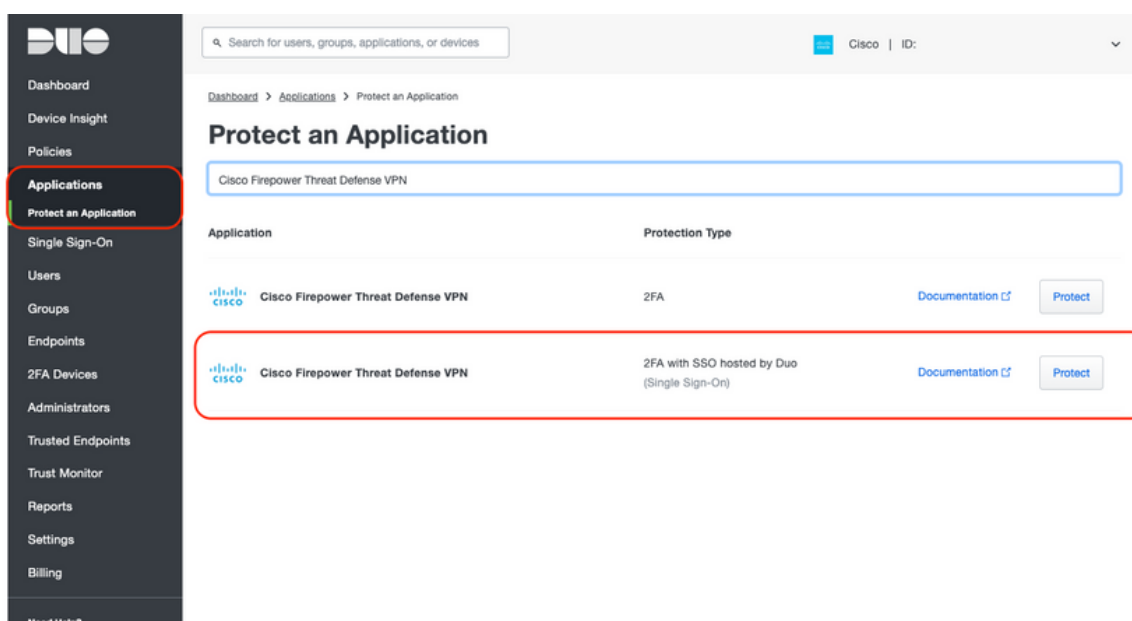
Passaggio 1. Accedere al pannello di amministrazione tramite questo collegamento a [Cisco Duo](#)



Home page Cisco DUO

Passaggio 2. Passare a Dashboard > Applicazioni > Proteggi applicazione.

Nella barra di ricerca, immettere "Cisco Firepower Threat Defense VPN" e selezionare "Proteggi".



Proteggere uno screenshot di un'applicazione

Selezionare l'opzione solo con il tipo di protezione "2FA con SSO ospitato da Duo".

Passaggio 3: Copiare queste informazioni URL in Metadati.

- ID entità provider di identità
- URL SSO
- URL di disconnessione

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

Esempio di informazioni da copiare



Nota: I link sono stati omessi dallo screenshot.

Passaggio 4. Selezionare "Scarica certificato" per scaricare il certificato del provider di identità in Download.

Passaggio 5. Inserire le informazioni sul provider di servizi

URL di base di Cisco Firepower: FQDN utilizzato per raggiungere l'FTD

Nome profilo connessione: il nome del gruppo di tunnel

Crea criterio di applicazione

Passaggio 1: Per creare un criterio di applicazione in Criterio Selezionare "Applica un criterio a tutti gli utenti", quindi selezionare "Oppure, crea un nuovo criterio" come mostrato nell'immagine.

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

Esempio di creazione di un criterio di applicazione

Apply a Policy



Policy

Select a Policy



[Or, create a new Policy.](#)

Apply Policy

Esempio di creazione di un criterio di applicazione

Passaggio 2. In Nome criterio, immettere il nome desiderato, selezionare "Criterio di autenticazione" in Utenti e selezionare "Imponi 2FA." Quindi salvare con "Crea criterio".

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

Esempio di creazione di un criterio di applicazione

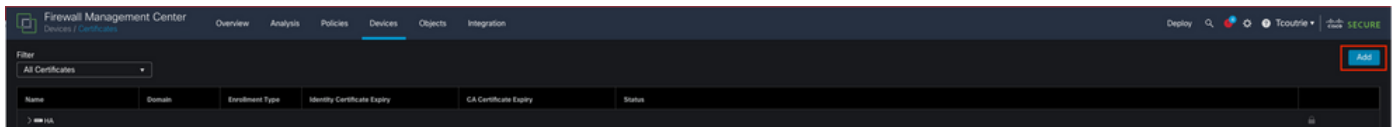
Passaggio 3. Applicare il criterio con "Applica criterio" nella finestra successiva. quindi scorrere fino alla fine della pagina e selezionare "Save" (Salva) per completare le configurazioni DUO

Procedura di configurazione di FMC

Distribuisce certificato di identità nell'FTD

In questa sezione viene descritta la configurazione e la distribuzione del certificato di identità nell'FTD necessario per l'autenticazione del certificato. Prima di iniziare, assicurarsi di distribuire tutte le configurazioni.

Passaggio 1. Passare a Dispositivi > Certificato e scegliere Aggiungi, come mostrato nell'immagine.



Schermata di dispositivi/certificati

Passaggio 2: Selezionare l'accessorio FTD dal menu a discesa dei dispositivi. Fare clic sull'icona + per aggiungere un nuovo metodo di registrazione dei certificati.

The screenshot shows the 'Add New Certificate' dialog box. It has a title bar with a question mark icon. The main text says: 'Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.' Below this, there are two dropdown menus: 'Device*' with 'HA' selected, and 'Cert Enrollment*' with 'Select a certificate enrollment object' selected. To the right of the 'Cert Enrollment*' dropdown is a red box containing a '+' icon. At the bottom right, there are two buttons: 'Cancel' and 'Add'.

Schermata Aggiungi nuovo certificato

Passaggio 3: scegliere l'opzione che rappresenta il metodo preferito per ottenere i certificati nell'ambiente tramite il "Tipo di registrazione", come mostrato nell'immagine.

Add Cert Enrollment



Name*

FTD04-16

Description

CA Information

Certificate Parameters

Key

Revocation

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](#)

Schermata della nuova pagina di registrazione del certificato



Suggerimento: Le opzioni disponibili sono: Certificato autofirmato - Genera un nuovo certificato localmente, SCEP - Utilizza il protocollo SCEP (Simple Certificate Enrollment Protocol) per ottenere un certificato da una CA, Manual - Installa manualmente il certificato radice e identità, PKCS12 - Carica il bundle di certificati crittografati con radice,

identità e chiave privata.

Distribuisci certificato IDP nell'FTD

In questa sezione viene descritto come configurare e distribuire il certificato IDP nell'FTD. Prima di iniziare, assicurarsi di distribuire tutte le configurazioni.

Passaggio 1: Passare a Dispositivi > Certificato e scegliere Aggiungi."

Passaggio 2: Selezionare l'accessorio FTD dal menu a discesa dei dispositivi. Fare clic sull'icona + per aggiungere un nuovo metodo di registrazione dei certificati.

Passaggio 3: Nella finestra Aggiungi registrazione certificato, immettere le informazioni richieste come mostrato nell'immagine, quindi "Salva" come mostrato nell'immagine.

- Nome: Nome dell'oggetto
- Tipo di iscrizione: Manuale
- Casella di controllo attivata: Solo CA
- Certificato CA: Formato Pem del certificato

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:

-----BEGIN CERTIFICATE-----
OC957DUc7tc4
b79bVzOXuqz5ZpaJHqtXV8fLOH
eIPYblyYBwSstXB+k75VHs0Voz
AkeySJCWRQXF
ISSRGu8DpUIKzKu2zd55322+wd
fkyy/WMXUJWmSXKKnnHEsOqL
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

Esempio di creazione di un oggetto di registrazione certificato



Attenzione: Se necessario, è possibile utilizzare "Ignora il contrassegno CA nei vincoli di base del certificato CA". Utilizzare questa opzione con cautela.

Passaggio 4: Selezionare l'oggetto di registrazione certificato appena creato in "Registrazione

certificato*:", quindi selezionare "Aggiungi" come mostrato nell'immagine.

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

Schermata del dispositivo e dell'oggetto di registrazione del certificato aggiunto



Nota: Dopo l'aggiunta, il certificato viene distribuito immediatamente.

Creazione dell'oggetto SAML SSO

In questa sezione vengono descritti i passaggi per configurare SAML SSO tramite FMC. Prima di iniziare, assicurarsi di distribuire tutte le configurazioni.

Passaggio 1. Passare a Oggetti > Server AAA > Server Single Sign-on e selezionare "Aggiungi server Single Sign-on".

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

esempio di creazione di un nuovo oggetto SSO

Passaggio 2. Immettere le informazioni richieste da "Crea criteri di protezione applicazione"

". Per continuare, selezionare "Salva".

- Nome*: Nome dell'oggetto
- ID entità provider di identità*: ID entità dal passaggio 3
- URL SSO*: URL di accesso copiato dal passaggio 3
- URL di disconnessione: URL di disconnessione copiato dal passaggio 3
- URL di base: Utilizzare lo stesso FQDN di "Cisco Firepower Base URL" nel passaggio 5
- Certificato del provider di identità*: Certificato IDP distribuito
- Certificato provider di servizi: Certificato sull'interfaccia esterna dell'FTD

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

Esempio di nuovo oggetto SSO.



Nota: I collegamenti ID entità, URL SSO e URL di disconnessione sono stati omessi dallo

Crea configurazione RAVPN (Virtual Private Network) di accesso remoto

In questa sezione vengono descritti i passaggi per configurare RAVPN utilizzando la procedura guidata.

Passaggio 1. Passare a Dispositivi > Accesso remoto Selezionare "Aggiungi".

Passaggio 2. Nella procedura guidata, immettere il nome della nuova Creazione guidata criteri RAVPN, selezionare SSL in Protocolli VPN: Aggiungi dispositivi di destinazione, come mostrato nell'immagine. Selezionare "Avanti" al termine.

Remote Access VPN Policy Wizard

Policy Assignment | Connection Profile | Secure Client | Access & Certificate | 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-IPv2

Targeted Devices:

Available Devices: HA

Selected Device: 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 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 Start Next

Passaggio 1 della procedura guidata RAVPN

Passaggio 2. Per il profilo di connessione, impostare le opzioni (mostrate qui): selezionare "Avanti" una volta completato.

- Nome profilo connessione: Utilizzare il nome del gruppo di tunnel nel passaggio 5 di "Creazione di un criterio di protezione dell'applicazione".

Autenticazione, autorizzazione e accounting (AAA):

- Metodo di autenticazione: Certificato client e SAML
- Server di autenticazione:* Selezionare l'oggetto SSO creato durante la creazione dell'oggetto SSO SAML.

Assegnazione indirizzo client:

- Usa server AAA (solo realm o RADIUS) - Radius o LDAP

- Usa server DHCP - Server DHCP
- Utilizza pool di indirizzi IP - Pool locale nell'FTD

Firewall Management Center
Devices / VPN / Setup Wizard

Overview Analysis Policies **Devices** Objects Integration

Deploy Tcoute

Remote Access VPN Policy Wizard

1 Policy Assignment 2 Connection Profile 3 Secure Client 4 **Access & Certificate** 5 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: Map specific field Use entire DNS Distinguished Name as username

Primary Field: Map specific field

Secondary Field: Map specific 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 (Realm 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**

Passaggio 2 della procedura guidata RAVPN



Suggerimento: In questa esercitazione viene utilizzato un server DHCP.

Passaggio 3. Selezionare "+" per caricare un'immagine di distribuzione Web di Cisco Secure Client da distribuire. Quindi selezionare la casella di controllo dell'immagine CSC da distribuire. Come mostrato nell'immagine. Selezionare "Next" (Avanti) una volta completato.

Firewall Management Center
Devices / VPN / Setup Wizard

Overview Analysis Policies **Devices** Objects Integration

Deploy Tcoute

Remote Access VPN Policy Wizard

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

Remote User Secure Client Internet Outside VPN Device Inside Corporate Resources AAA

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-5.0.02075-...	cisco-secure-client-macos-5.0.02075-...	Mac OS
☒ cisco-secure-client-win-5.0.02075-...	cisco-secure-client-win-5.0.02075-...	Windows

Cancel Back **Next**

Passaggio 4. Impostare questi oggetti (come mostrato nell'immagine): selezionare "Avanti" una volta completato.

Gruppo interfaccia/Area di sicurezza:* : Interfaccia esterna

"Registrazione certificato:*": Certificato di identità creato durante la sezione "Distribuisci certificato di identità all'FTD" di questa guida

Firewall Management Center
Devices / VPN / Remote Access

Overview Analysis Policies **Devices** Objects Integration

Deploy Search Tutorials SECURE

Remote Access VPN Policy Wizard

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

Remote User Secure Client Internet VPN Device Policy Corporate Resources AAA

Network Interface for Incoming VPN Access

Select or create an Interface Group or a Security Zone that contains the network interfaces users will access for VPN connections.

Interface group/Security Zone: outside +

☒ Enable DTLS on member interfaces

Device Certificates

Device certificate (also called identity certificate) identifies the VPN gateway to the remote access clients. Select a certificate which is used to authenticate the VPN gateway.

Certificate Enrollment: FTD04-16 +

Access Control for VPN Traffic

All decrypted traffic in the VPN tunnel is subjected to the Access Control Policy by default. Select this option to bypass decrypted traffic from the Access Control Policy.

☒ Bypass Access Control policy for decrypted traffic (except permit-vpn)

This option bypasses the Access Control Policy inspection, but VPN, Star, ACL, and authorization ACL downloaded from AAA server are still applied to VPN traffic.

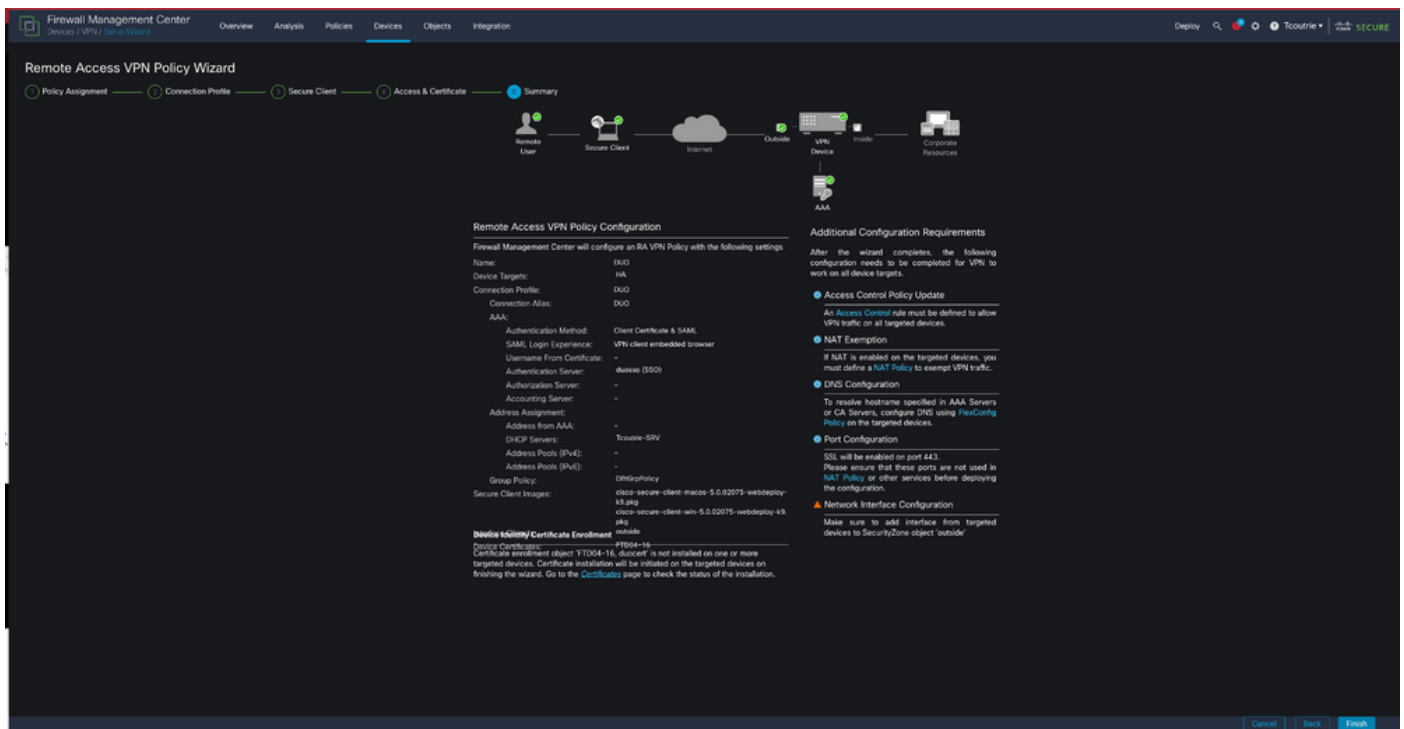
Cancel Back **Next**



Suggerimento: Se non è stato creato, aggiungere un nuovo oggetto di registrazione certificato selezionando "+".

Passaggio 6. Riepilogo

Verificare tutte le informazioni. Se tutto è corretto, continuare con "Fine".



Pagina di riepilogo

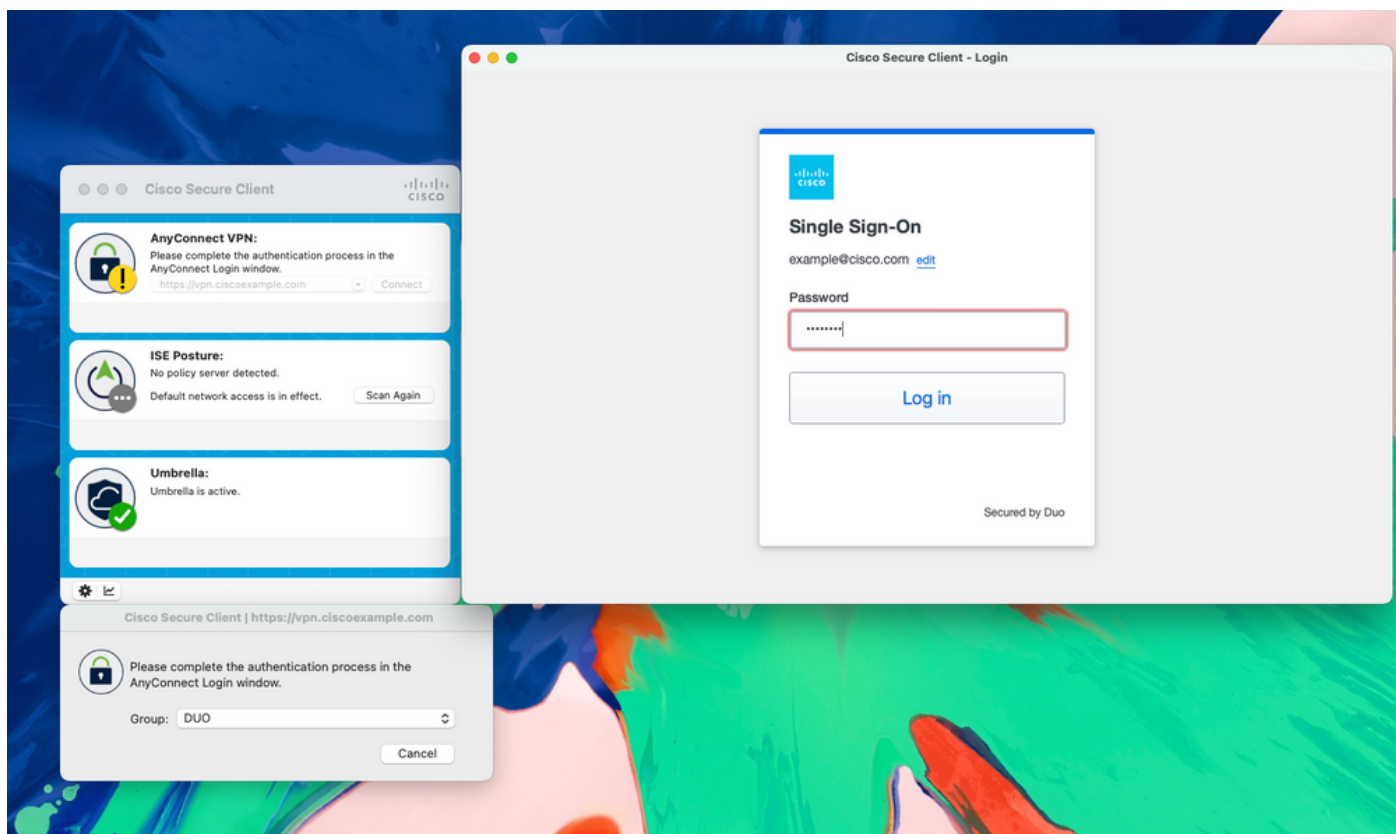
Passaggio 7. Distribuire le configurazioni appena aggiunte.

Verifica

In questa sezione viene descritta la verifica di un tentativo di connessione riuscito.

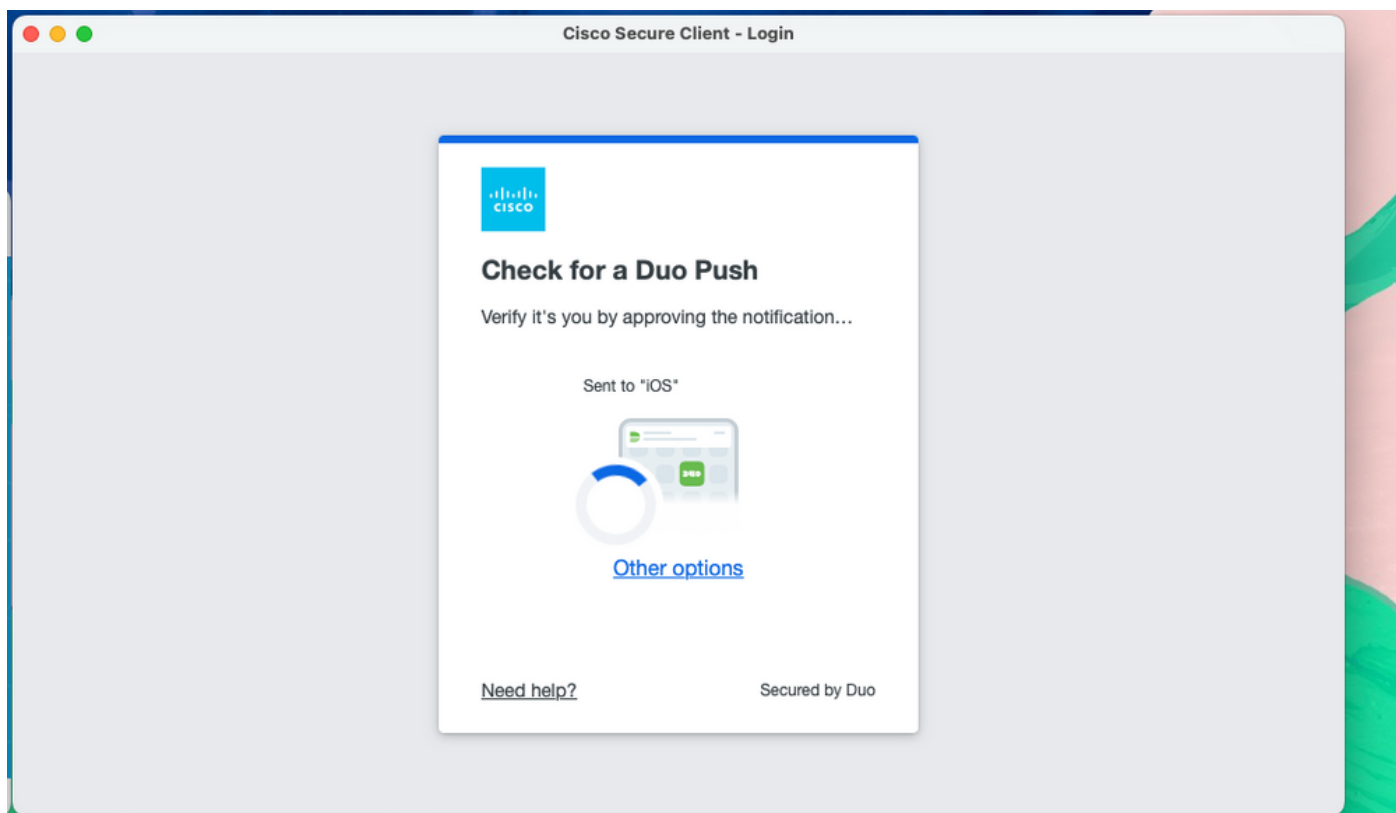
Aprire Cisco Secure Client, immettere il nome di dominio completo (FQDN) dell'FTD e connettersi.

Immettere le credenziali nella pagina SSO.



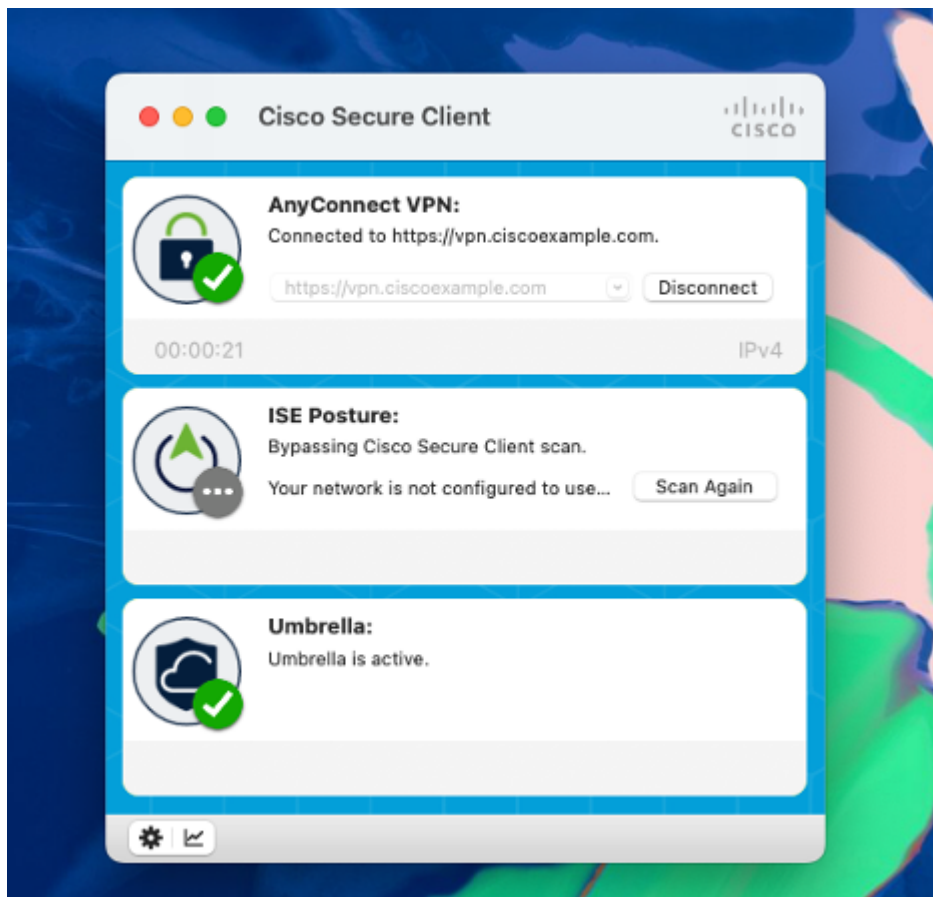
Pagina SSO tramite Cisco Secure Client

Accettare la pressione DUO sul dispositivo registrato.



Push DUO

Connessione riuscita.



Connesso a FTD

Verificare la connessione sull'FTD con il comando: `show vpn-sessiondb detail anyconnect`

```

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

```

Alcune informazioni sono state omesse dall'esempio di output

Risoluzione dei problemi

Si tratta di possibili problemi che sorgeranno dopo l'implementazione.

Numero 1: Autenticazione del certificato non riuscita.

Assicurarsi che il certificato radice sia installato sull'FTD;

utilizzare i seguenti debug:

debug crypto ca 14

debug aaa shim 128

debug aaa common 128

numero 2: Errori SAML

I seguenti debug possono essere abilitati per la risoluzione dei problemi:

debug aaa shim 128

debug aaa common 128

debug webvpn anyconnect 128

debug webvpn saml 255

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'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).