

Zertifikatsauthentifizierung konfigurieren & DUO SAML-Authentifizierung

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Schritte für DUO konfigurieren](#)

[Erstellen einer Anwendungsschutzrichtlinie](#)

[Anwendungsrichtlinie erstellen](#)

[Konfigurationsschritte für FMC](#)

[Bereitstellung des Identitätszertifikats für die FTD](#)

[Bereitstellung des IDP-Zertifikats für das FTD](#)

[Erstellen des SAML-SSO-Objekts](#)

[Erstellen einer RAVPN-Konfiguration \(Virtual Private Network\) für Remote-Zugriff](#)

[Überprüfung](#)

[Fehlerbehebung](#)

[Ausgabe 1: Die Zertifikatauthentifizierung ist fehlgeschlagen.](#)

[Ausgabe 2: SAML-Fehler](#)

Einleitung

In diesem Dokument wird ein Beispiel für die Implementierung einer zertifikatbasierten Authentifizierung und einer dualen SAML-Authentifizierung beschrieben.

Voraussetzungen

In diesem Leitfaden werden folgende Tools und Geräte verwendet:

- Cisco Firepower Threat Defense (FTD)
- Firepower Management Center (FMC)
- Interne Zertifizierungsstelle
- Cisco DUO Premier-Konto
- Cisco DUO-Authentifizierungsproxy
- Cisco Secure Client (CSC)

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Basis-VPN,
- SSL/TLS
- Public-Key-Infrastruktur
- Erfahrungen mit FMC
- Cisco Secure Client
- FTD-Code 7.2.0 oder höher
- Cisco DUO-Authentifizierungsproxy

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

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

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Schritte für DUO konfigurieren

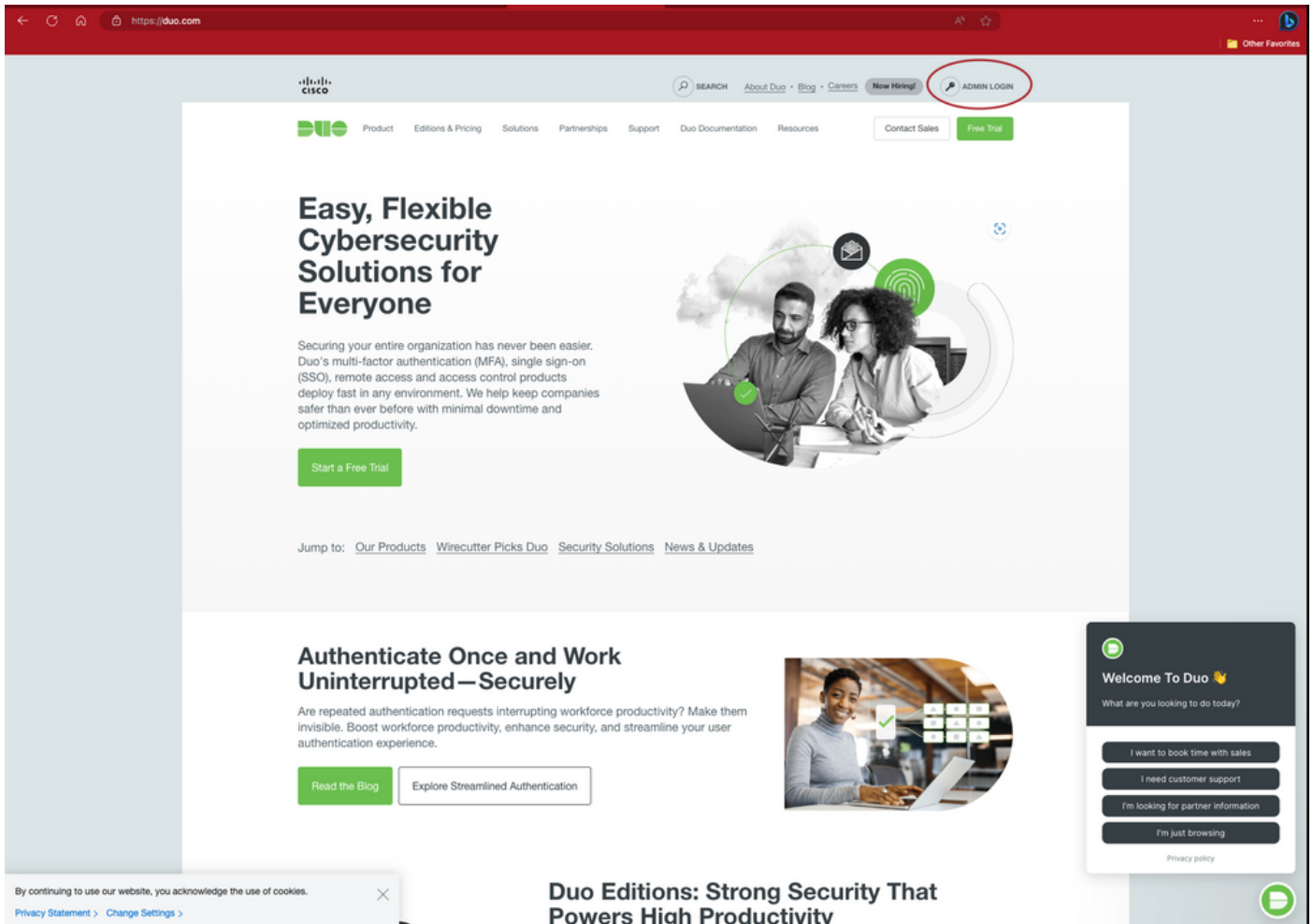
In diesem Abschnitt werden die Schritte zur Konfiguration von Cisco DUO Single Sign-on (SSO) beschrieben. Stellen Sie vor dem Start sicher, dass der Authentifizierungsproxy implementiert ist.



Warnung: Wenn kein Authentifizierungsproxy implementiert wurde, enthält dieser Link den Leitfaden für diese Aufgabe. [DUO Authentication Proxy Guide](#)

Erstellen einer Anwendungsschutzrichtlinie

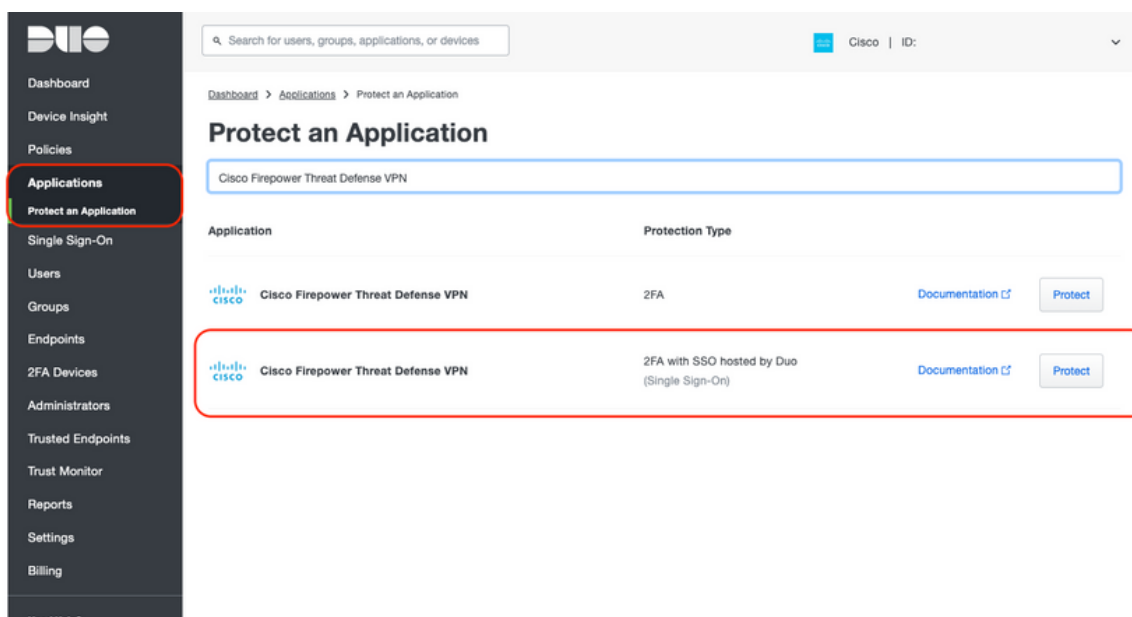
Schritt 1: Melden Sie sich über diesen Link beim Admin-Panel an [Cisco Duo](#)



Cisco DUO-Startseite

Schritt 2: Navigieren Sie zu Dashboard > Anwendungen > Eine Anwendung schützen.

Geben Sie in der Suchleiste "Cisco Firepower Threat Defense VPN" ein, und wählen Sie "Schützen".



Schützen eines Anwendungs-Screenshots

Wählen Sie die Option mit nur Schutzart "2FA mit SSO gehostet von Duo".

Schritt 3: Kopieren Sie diese URL-Informationen unter Metadaten.

- Element-ID des Identitätsanbieters
- SSO-URL
- Abmelde-URL

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

Beispiel für zu kopierende Informationen



Anmerkung: Die Links wurden im Screenshot weggelassen.

Schritt 4: Wählen Sie "Zertifikat herunterladen", um das Identitätsanbieter-Zertifikat unter "Downloads" herunterzuladen.

Schritt 5: Geben Sie die Informationen zum Service Provider ein.

Cisco FirePOWER Base-URL - Der FQDN zum Erreichen des FTD

Name des Verbindungsprofils - Name der Tunnelgruppe

Anwendungsrichtlinie erstellen

Schritt 1: So erstellen Sie eine Anwendungsrichtlinie unter Richtlinie Wählen Sie "Eine Richtlinie auf alle Benutzer anwenden", und wählen Sie dann "Oder, eine neue Richtlinie erstellen", wie im Bild gezeigt.

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

Beispiel für das Erstellen einer Anwendungsrichtlinie

Apply a Policy



Policy

Select a Policy



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

Apply Policy

Beispiel für das Erstellen einer Anwendungsrichtlinie

Schritt 2: Geben Sie unter Richtlinienname den gewünschten Namen ein, wählen Sie unter Benutzer die Option "Authentifizierungsrichtlinie" und anschließend die Option "Durchsetzen von 2FA." Speichern Sie dann mit "Richtlinie erstellen".

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

Beispiel für das Erstellen einer Anwendungsrichtlinie

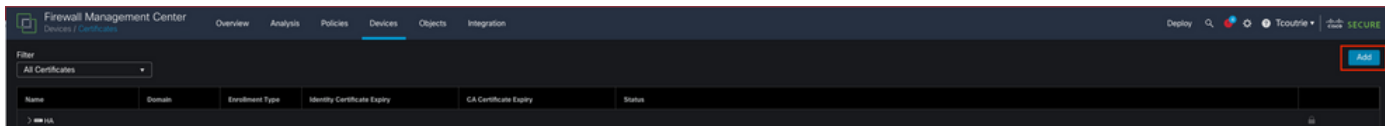
Schritt 3: Wenden Sie die Richtlinie mit "Apply Policy" (Richtlinie anwenden) im nächsten Fenster an. Führen Sie dann einen Bildlauf nach unten durch, und wählen Sie "Speichern" aus, um die DUO-Konfigurationen abzuschließen.

Konfigurationsschritte für FMC

Bereitstellung des Identitätszertifikats für die FTD

In diesem Abschnitt wird die Konfiguration und Bereitstellung des Identitätszertifikats für die FTD beschrieben, die für die Zertifikatsauthentifizierung erforderlich ist. Stellen Sie vor dem Start sicher, dass Sie alle Konfigurationen bereitstellen.

Schritt 1: Navigieren Sie zu **Geräte > Zertifikat**, und wählen Sie **Hinzufügen** aus, wie im Bild dargestellt.



Screenshot der Geräte/Zertifikate

Phase 2: Wählen Sie die FTD-Appliance aus der Dropdown-Liste aus. Klicken Sie auf das Symbol **+**, um eine neue Zertifikatsregistrierungsmethode hinzuzufügen.

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*' and 'Cert Enrollment*'. The 'Device*' dropdown is set to 'HA'. The 'Cert Enrollment*' dropdown is set to 'Select a certificate enrollment object'. A red box highlights the '+' button next to the 'Cert Enrollment*' dropdown. At the bottom right, there are two buttons: 'Cancel' and 'Add'.

Screenshot des neuen Zertifikats hinzufügen

Schritt 3: Wählen Sie die bevorzugte Methode zum Abrufen von Zertifikaten in der Umgebung über den "Anmeldungstyp" aus, wie im Bild gezeigt.

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](#)

Screenshot der neuen Seite für die Zertifikatsregistrierung



Tipp: Es stehen folgende Optionen zur Verfügung: Selbstsigniertes Zertifikat - Lokales Erstellen eines neuen Zertifikats, SCEP - Verwenden des einfachen Zertifikatsregistrierungsprotokolls, um ein Zertifikat von einer Zertifizierungsstelle zu erhalten, Manuell - Manuelles Installieren des Stamm- und Identitätszertifikats, PKCS12 -

Hochladen des verschlüsselten Zertifikatpakets mit Stamm, Identität und privatem Schlüssel.

Bereitstellung des IDP-Zertifikats für das FTD

In diesem Abschnitt wird die Konfiguration und Bereitstellung des IDP-Zertifikats für das FTD beschrieben. Stellen Sie sicher, dass Sie alle Konfigurationen bereitstellen, bevor Sie beginnen.

Schritt 1: Navigieren Sie zu Geräte > Zertifikat, und wählen Sie Hinzufügen."

Phase 2: Wählen Sie die FTD-Appliance aus der Dropdown-Liste aus. Klicken Sie auf das Symbol +, um eine neue Zertifikatregistrierungsmethode hinzuzufügen.

Schritt 3: Geben Sie im Fenster "Add Cert Enrollment" (Zertifikatsregistrierung hinzufügen) die erforderlichen Informationen ein, wie im Bild dargestellt, und klicken Sie dann auf "Save" (Speichern), wie im Bild dargestellt.

- Name: Name des Objekts
- Anmeldungstyp: Manuell
- Kontrollkästchen aktiviert: Nur CA
- Zertifizierungsstellenzertifikat: Pem Format des Zertifikats

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/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

Beispiel zum Erstellen eines Zertifikatregistrierungsobjekts



Vorsicht: Bei Bedarf kann "Prüfung auf CA-Flag in grundlegenden Einschränkungen des CA-Zertifikats überspringen" verwendet werden. Verwenden Sie diese Option mit Vorsicht.

Schritt 4: Wählen Sie das neu erstellte Zertifikatregistrierungsobjekt unter "Zertifikatregistrierung*:"

und wählen Sie dann "Hinzufügen" aus, wie im Bild gezeigt.

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

Screenshot des hinzugefügten Zertifikatregistrierungsobjekts und des Geräts



Anmerkung: Nach dem Hinzufügen wird das Zertifikat sofort bereitgestellt.

Erstellen des SAML-SSO-Objekts

In diesem Abschnitt werden die Schritte zur Konfiguration von SAML SSO über FMC beschrieben. Stellen Sie vor dem Start sicher, dass Sie alle Konfigurationen bereitstellen.

Schritt 1: Navigieren Sie zu Objekte > AAA-Server > Single Sign-on-Server, und wählen Sie "Single Sign-on-Server hinzufügen".

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 > | 🔄

Beispiel zum Erstellen eines neuen SSO-Objekts

Schritt 2: Geben Sie die erforderlichen Informationen aus "Create an Application Protection Policy" (Anwendungsschutzrichtlinie erstellen) ein

". Um fortzufahren, nachdem Sie fertig sind, wählen Sie "Speichern".

- Name*: Name des Objekts
- Element-ID des Identitätsanbieters*: Element-ID aus Schritt 3
- SSO-URL*: Anmelde-URL aus Schritt 3 kopiert
- Abmelden-URL: Abmelden-URL aus Schritt 3 kopiert
- Basis-URL: Verwenden desselben FQDN wie "Cisco FirePOWER Base URL" in Schritt 5
- Zertifikat des Identitätsanbieters*: bereitgestelltes IDP-Zertifikat
- Dienstanbieterzertifikat: Zertifikat auf der externen Schnittstelle des 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

Beispiel für ein neues SSO-Objekt.



Anmerkung: Die Links für die Element-ID, die SSO-URL und die Abmelde-URL wurden im

Screenshot weggelassen.

Erstellen einer RAVPN-Konfiguration (Virtual Private Network) für Remote-Zugriff

In diesem Abschnitt werden die Schritte zur RAVPN-Konfiguration mithilfe des Assistenten beschrieben.

Schritt 1: Navigieren Sie zu Geräte > Remotezugriff Wählen Sie "Hinzufügen" aus.

Schritt 2. Geben Sie im Assistenten den Namen des neuen RAVPN Policy Wizard ein, und wählen Sie unter VPN Protocols: Add the Targeted Devices (VPN-Protokolle: Zielgeräte hinzufügen) die Option SSL aus, wie im Bild dargestellt. Wählen Sie nach Abschluss der Aktion "Weiter" aus.

The screenshot shows the 'Remote Access VPN Policy Wizard' interface. At the top, there are five tabs: 'Policy Assignment', 'Connection Profile', 'Secure Client', 'Access & Certificate', and 'Summary'. The 'Access & Certificate' tab is currently selected. The main area is titled 'Targeted Devices and Protocols'. It contains a 'Name' field with the value 'DLO' and a 'Description' field. Below these are 'VPN Protocols' with 'SSL' selected and 'IPsec-IPv2' unselected. Under 'Targeted Devices', there is a list of available devices with 'HA' selected. A 'Next' button is visible at the bottom right. On the right side, there is a 'Before You Start' section with instructions and links for 'Authentication Server', 'Secure Client Package', and 'Device Interface'.

Schritt 1 des RAVPN-Assistenten

Schritt 2: Stellen Sie für das Verbindungsprofil die hier gezeigten Optionen ein: Wählen Sie nach Abschluss "Weiter" aus.

- Verbindungsprofilname: Verwenden Sie den Namen der Tunnelgruppe in Schritt 5 von "Erstellen einer Anwendungsschutzrichtlinie".

Authentifizierung, Autorisierung und Abrechnung (AAA):

- Authentifizierungsmethode: Client-Zertifikat und SAML
- Authentifizierungsserver:* Wählen Sie das SSO-Objekt aus, das während der Erstellung des SAML-SSO-Objekts erstellt wurde.

Client-Adressenzuweisung:

- AAA-Server verwenden (nur Bereich oder RADIUS) - Radius oder LDAP

- DHCP-Server verwenden - DHCP-Server
- IP-Adresspools verwenden - Lokaler Pool auf dem FTD

Firewall Management Center
Devices / VPN / Setup Wizard

Overview Analysis Policies **Devices** Objects Integration

Deploy Tcoute VPN SECURE

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 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 (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](#)

Schritt 2 des RAVPN-Assistenten

Tipp: Für diese Übung wird ein DHCP-Server verwendet.

Schritt 3: Wählen Sie "+", um ein Web-Bereitstellungs-Image des bereitzustellenden Cisco Secure Client hochzuladen. Aktivieren Sie dann das Kontrollkästchen für das bereitzustellende CSC-Image. wie im Bild dargestellt. Wählen Sie "Weiter" nach Abschluss.

Firewall Management Center
Devices / VPN / Setup Wizard

Overview Analysis Policies **Devices** Objects Integration

Deploy Tcoute VPN SECURE

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.

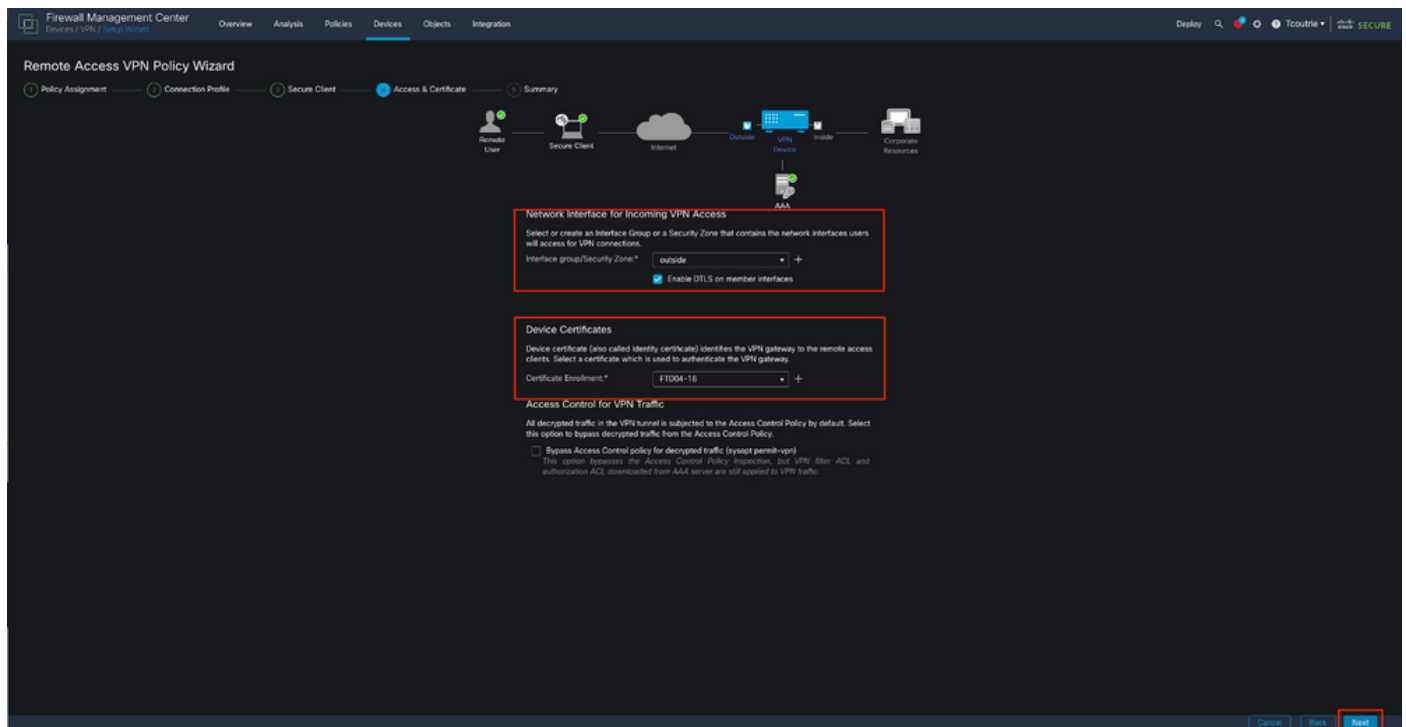
Download Secure Client packages from [Cisco Software Download Center](#).

Secure Client File Object Name	Secure Client Package Name	Operating System
☒ cisco-secure-client-macos-5.0.0.0000...	cisco-secure-client-macos-5.0.0.0000-...	Mac OS
☒ cisco-secure-client-win-5.0.0.0000...	cisco-secure-client-win-5.0.0.0000-...	Windows

Schritt 4. Setzen Sie diese Objekte (wie im Bild zu sehen): Wählen Sie "Weiter" einmal abgeschlossen.

Schnittstellengruppe/Sicherheitszone:*: Externe Schnittstelle

"Zertifikatregistrierung:": Identitätszertifikat, das während des Abschnitts "Bereitstellung des Identitätszertifikats für das FTD" dieses Leitfadens erstellt wurde

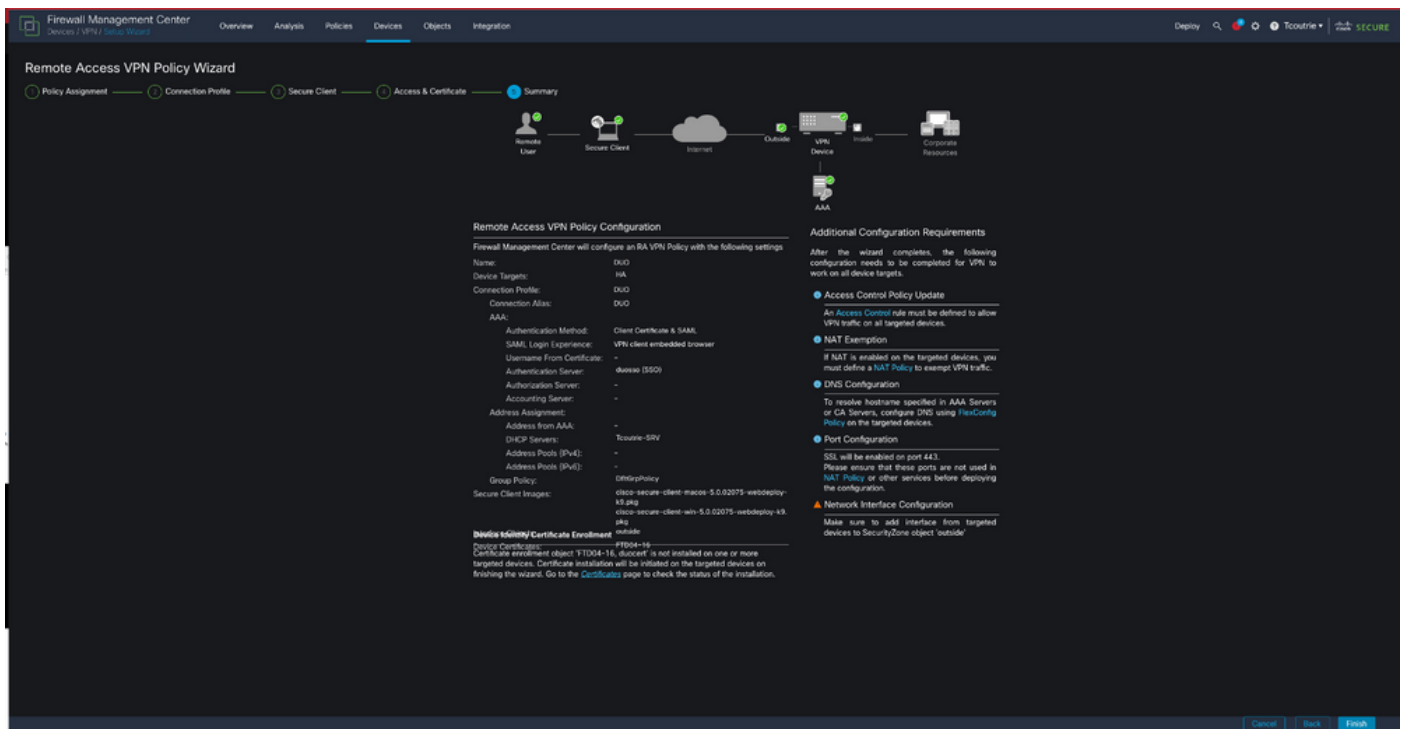


Schritt 4 des RAVPN-Assistenten

 Tipp: Wenn dies nicht erstellt wurde, fügen Sie ein neues Zertifikatregistrierungsobjekt hinzu, indem Sie auf "+" klicken.

Schritt 6: Übersicht

Überprüfen Sie alle Informationen. Wenn alles korrekt ist, fahren Sie mit 'Beenden.'



Übersichtsseite

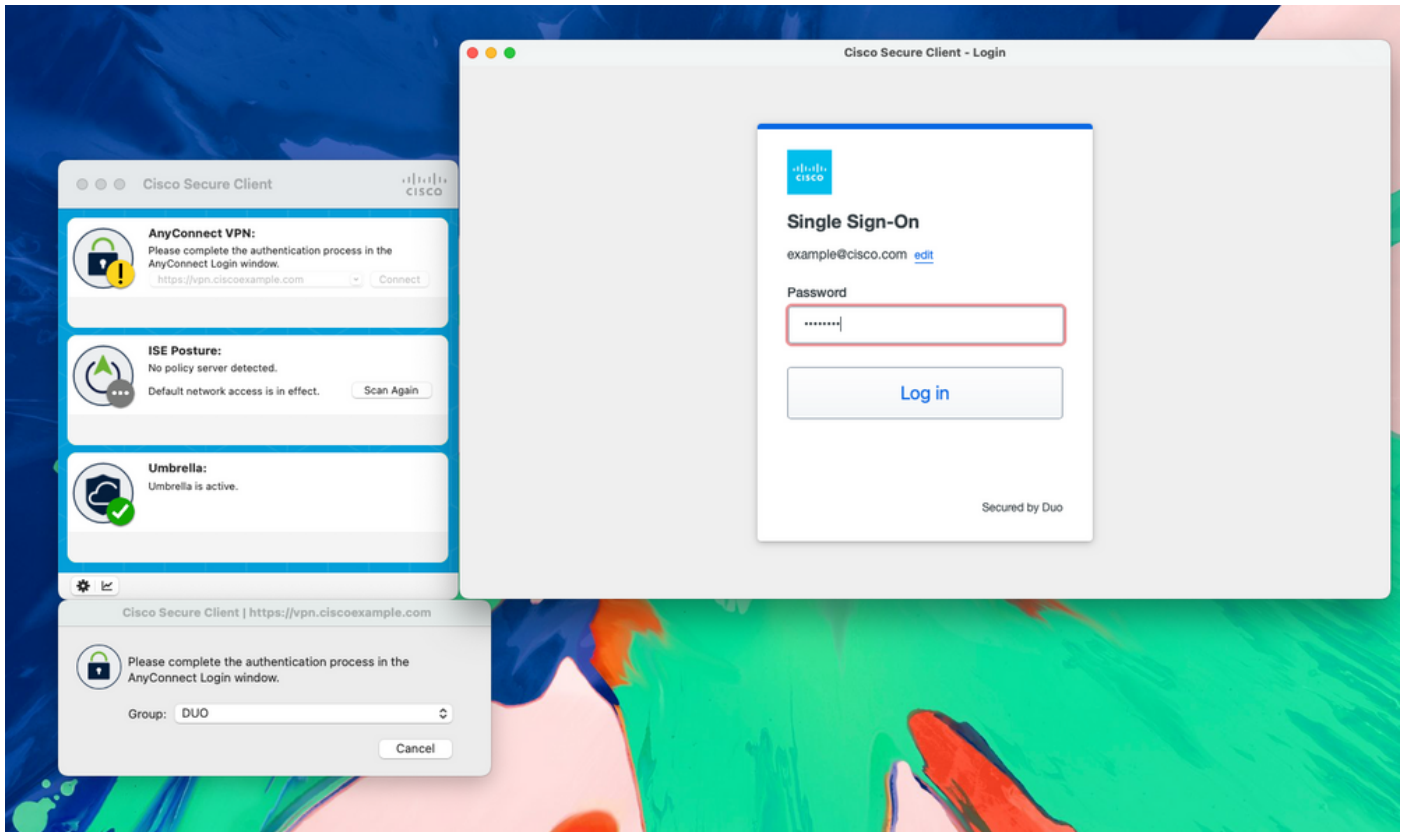
Schritt 7: Bereitstellen der neu hinzugefügten Konfigurationen

Überprüfung

In diesem Abschnitt wird beschrieben, wie Sie einen erfolgreichen Verbindungsversuch überprüfen.

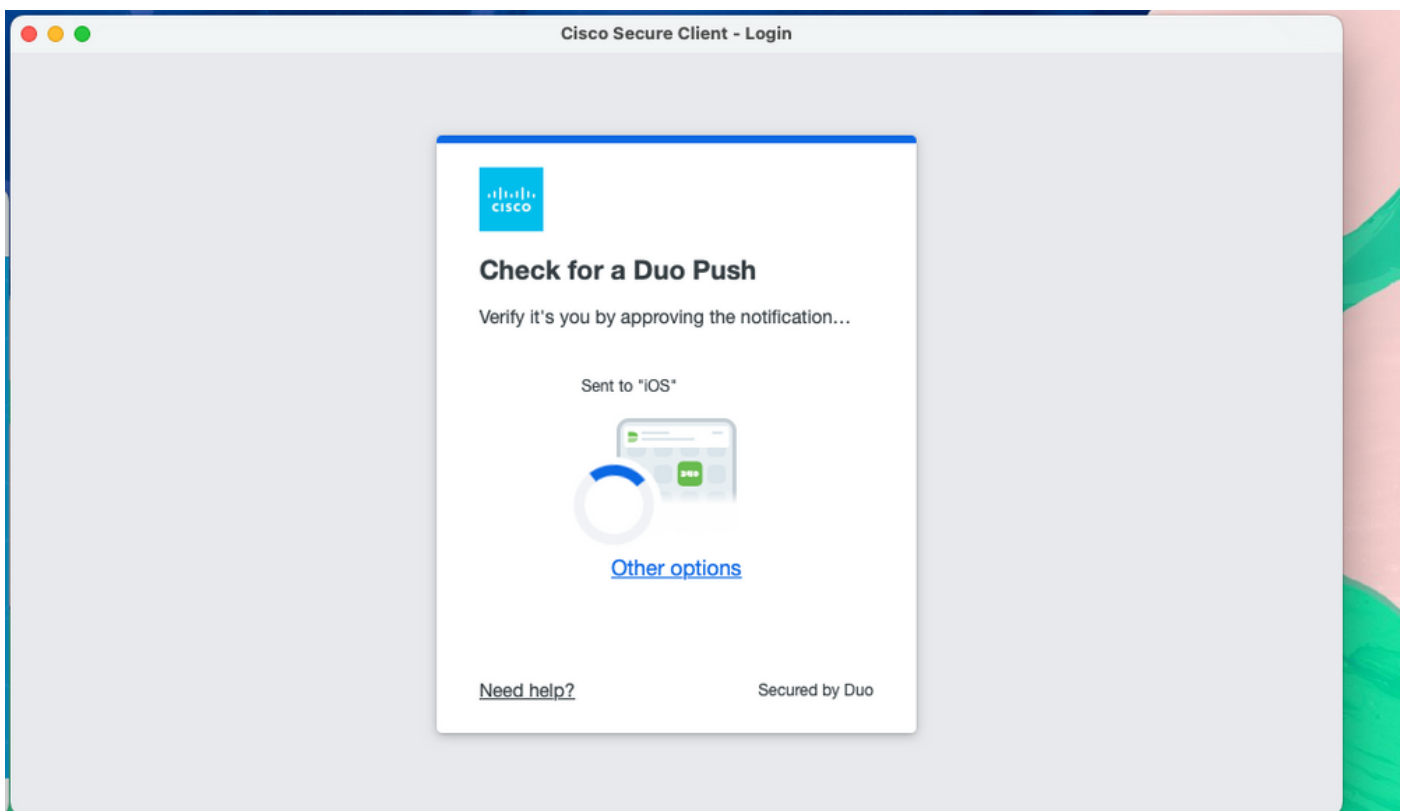
Öffnen Sie den Cisco Secure Client, geben Sie den FQDN des FTD ein, und stellen Sie die Verbindung her.

Geben Sie die Anmeldeinformationen auf der Seite SSO ein.



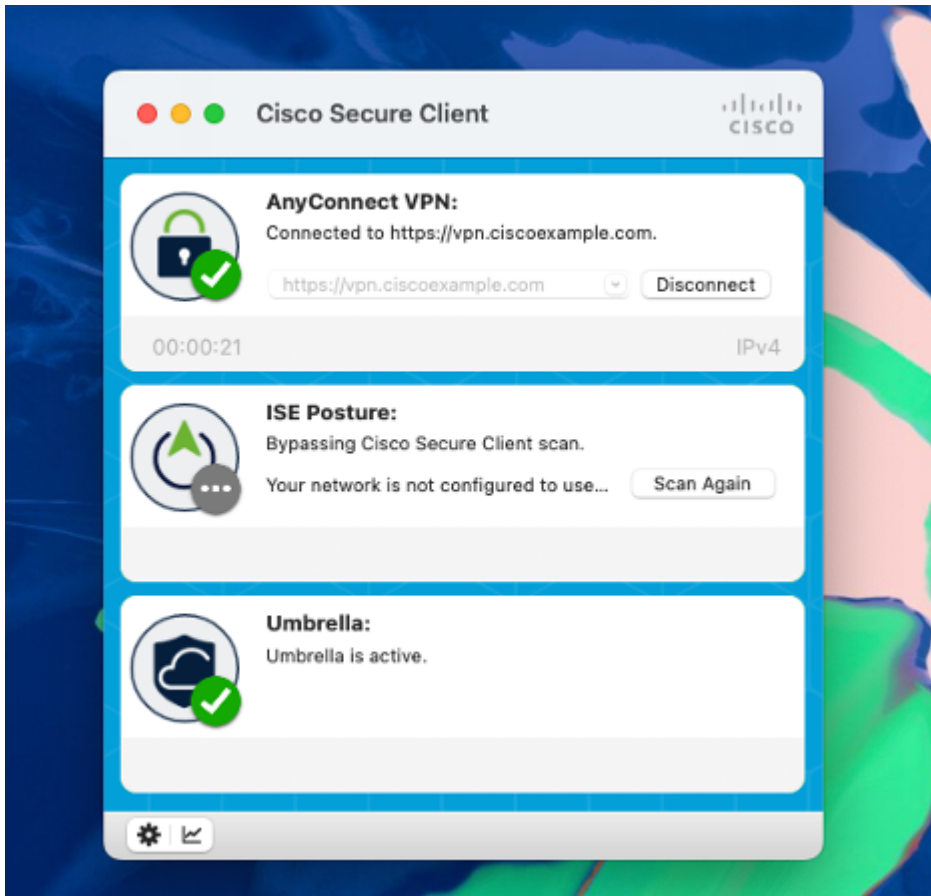
SSO-Seite über Cisco Secure Client

Akzeptieren Sie die DUO-Übertragung auf das registrierte Gerät.



DUO-Push

Verbindung erfolgreich hergestellt.



Mit FTD verbunden

Überprüfen Sie mit dem folgenden Befehl die FTD-Verbindung: `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

```

Im Ausgabebeispiel wurden einige Informationen ausgelassen.

Fehlerbehebung

Dies sind mögliche Probleme, die nach der Implementierung auftreten.

Ausgabe 1: Die Zertifikatauthentifizierung ist fehlgeschlagen.

Stellen Sie sicher, dass das Stammzertifikat auf dem FTD installiert ist.

Verwenden Sie folgende Debugging-Optionen:

debug crypto ca 14

debug aaa shim 128

debuggen aaa häufig 128

Ausgabe 2: SAML-Fehler

Diese Fehlerbehebungen können aktiviert werden, um:

debug aaa shim 128

debuggen aaa häufig 128

debug webvpn anyconnect 128

debug webvpn saml 255

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.