

Integration von Duo SAML SSO mit AnyConnect Secure Remote Access mit ISE-Status

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Netzwerkdigramm](#)

[Datenverkehrsfluss](#)

[Konfigurationen](#)

[- Duo Admin-Portal-Konfiguration](#)

[- Duo Access Gateway \(DAG\)-Konfiguration](#)

[-ASA-Konfiguration](#)

[-ISE-Konfiguration](#)

[Überprüfung](#)

[Benutzerfreundlichkeit](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird ein Konfigurationsbeispiel für die Integration von Duo SAML SSO mit Adaptive Security Appliance (ASA) Cisco AnyConnect Secure Mobility Client für eine detaillierte Statusüberprüfung mithilfe der Cisco ISE beschrieben. Duo SAML SSO wird mithilfe von Duo Access Gateway (DAG) implementiert, das zur erstmaligen Benutzerauthentifizierung mit dem Active Directory kommuniziert und dann zur mehrstufigen Authentifizierung mit Duo Security (Cloud) kommuniziert. Die Cisco ISE wird als Autorisierungsserver für die Endpunktverifizierung mittels Statusüberprüfung verwendet.

Beitrag von Dinesh Moudgil und Pulkit Saxena, Cisco HTTS Engineer.

Voraussetzungen

Anforderungen

In diesem Dokument wird davon ausgegangen, dass die ASA voll funktionsfähig und so konfiguriert ist, dass mit dem Cisco Adaptive Security Device Manager (ASDM) oder der

Befehlszeilenschnittstelle (Command Line Interface, kurz „CLI“) Konfigurationsänderungen möglich sind.


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

- Grundlagen zu Duo Access Gateway und Duo Security
- Grundkenntnisse der VPN-Konfiguration für Remote-Zugriff auf der ASA
- Grundkenntnisse der ISE und Statusservices

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf folgenden Software-Versionen:

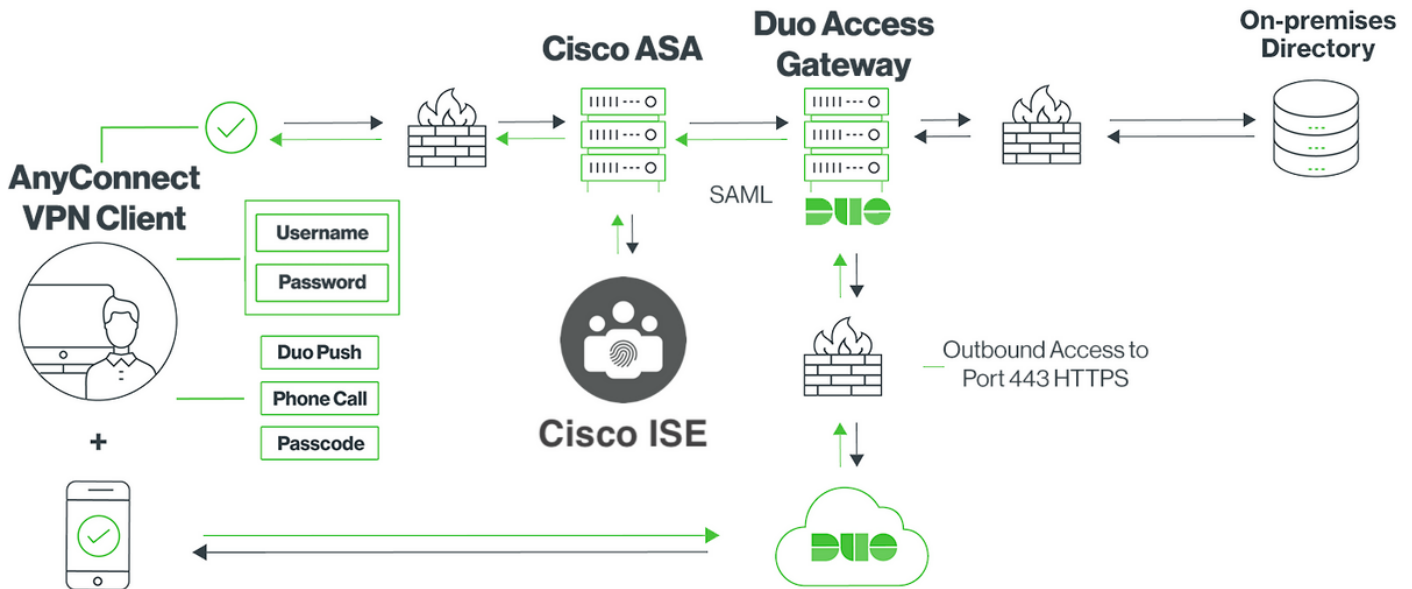
- Cisco Adaptive Security Appliance-Software Version 9.12(3)12
- Duo Access-Gateway
- Duo Security
- Cisco Identity Services Engine Version 2.6 und höher
- Microsoft Windows 10 mit AnyConnect Version 4.8.03052

 Hinweis: Für jeden in dieser Implementierung verwendeten Embedded Browser von AnyConnect ist die ASA Version 9.7(1)24, 9.8(2)28, 9.9(2)1 oder eine höhere Version jeder Version sowie die AnyConnect-Version 4.6 oder höher erforderlich.

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 Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Konfigurieren

Netzwerkdiagramm



Datenverkehrsfluss

1. AnyConnect-Client initiiert eine SSL VPN-Verbindung zur Cisco ASA
2. Cisco ASA, die für die primäre Authentifizierung mit Duo Access Gateway (DAG) konfiguriert ist, leitet den eingebetteten Browser in Anyconnect Client zur SAML-Authentifizierung an DAG um
3. AnyConnect-Client wird auf Duo Access Gateway umgeleitet
4. Sobald der AnyConnect-Client die Anmeldeinformationen eingegeben hat, wird eine SAML-Authentifizierungsanforderung erstellt und von Cisco ASA an Duo Access Gateway ausgegeben
5. Duo Access Gateway nutzt die Integration mit Active Directory vor Ort, um die primäre Authentifizierung für den AnyConnect-Client durchzuführen
6. Sobald die primäre Authentifizierung erfolgreich ist, sendet das Duo Access Gateway über den TCP-Port 443 eine Anforderung an Duo Security, um die Zwei-Faktor-Authentifizierung zu starten.
7. Der AnyConnect-Client präsentiert sich mit "Duo Interactive Prompt" und der Benutzer vollendet Duo Zwei-Faktor-Authentifizierung mit seiner bevorzugten Methode (Push oder Passcode)
8. Duo Security erhält eine Authentifizierungsantwort und sendet die Informationen an das Duo Access Gateway
9. Auf Basis der Authentifizierungsantwort erstellt Duo Access Gateway eine SAML-Authentifizierungsantwort, die eine SAML-Assertion enthält und auf den AnyConnect-Client reagiert

10. AnyConnect-Client authentifiziert erfolgreich SSL VPN-Verbindungen mit Cisco ASA
11. Nach erfolgreicher Authentifizierung sendet die Cisco ASA eine Autorisierungsanfrage an die Cisco ISE



Hinweis: Cisco ISE ist nur für die Autorisierung konfiguriert, da Duo Access Gateway die erforderliche Authentifizierung bereitstellt.

12. Die Cisco ISE verarbeitet die Autorisierungsanfrage und gibt, da der Status des Clients "Unbekannt" lautet, eine Statusumleitung mit eingeschränktem Zugriff auf den AnyConnect-Client über die Cisco ASA zurück.
13. Wenn der Anyconnect-Client über kein Compliance-Modul verfügt, wird er aufgefordert, das Modul herunterzuladen, um die Statusüberprüfung fortzusetzen.
14. Wenn der AnyConnect-Client über ein Compliance-Modul verfügt, stellt er eine TLS-Verbindung mit der Cisco ASA her, und der Statusfluss beginnt
15. Abhängig von den auf der ISE konfigurierten Statusbedingungen werden Statusüberprüfungen durchgeführt, und die Details werden vom AnyConnect-Client an die Cisco ISE gesendet.
16. Wenn sich der Status des Clients von Unbekannt zu Konformität ändert, wird von der Cisco ISE eine Anforderung zur Autorisierung (Change of Authorization, CoA) an die Cisco ASA gesendet, um dem Client den vollen Zugriff zu gewähren. Das VPN ist dann vollständig eingerichtet.

Konfigurationen

- Duo Admin-Portal-Konfiguration

Konfigurieren Sie in diesem Abschnitt die ASA-Anwendung auf dem Duo-Administratorportal.

1. Melden Sie sich bei "Duo Admin Portal" an, navigieren Sie zu "Applications > Protect an Application" (Anwendungen > Schutz einer Anwendung), und suchen Sie nach "ASA" mit dem Schutztyp "2FA with Duo Access Gateway, self-hosted" (2FA mit Duo Access Gateway, selbst gehostet). Klicken Sie ganz rechts auf "Schützen", um die Cisco ASA zu konfigurieren.

admin-77d04ebc.duosecurity.com/applications/protect/types

Search for users, groups, applications, or devices

Cisco | ID: 2010-1403-48 ciscoduobl

Dashboard > Applications > Protect an Application

Protect an Application

ASA

Application	2FA	Single Sign-On (if available)	Documentation	Action
Asana	2FA	Duo Access Gateway (self-hosted)	Documentation	Protect
Cisco ASA	2FA	Duo Access Gateway (self-hosted)	Documentation	Protect
Cisco ASA	2FA	Single Sign-On (hosted by Duo)	Documentation	Configure

2. Konfigurieren Sie unter "Service Provider" die folgenden Attribute für die geschützte Anwendung ASA.

Basis-URL	firebird.cisco.com
Tunnelgruppe	TG_SAML
Mail-Attribut	sAMAccountName, E-Mail

Klicken Sie unten auf der Seite auf "Speichern"

Device Insight

Policies

Applications

Protect an Application

Single Sign-On

Users

Groups

Endpoints

2FA Devices

Administrators

Reports

Settings

Billing

Need Help?

Chat with Tech Support

Email Support

Call us at 1-855-386-2884

Account ID
2010-1403-48

Deployment ID
DUOS7

Helpful Links
Documentation

Cisco ASA - Duo Access Gateway

Authentication Log | Remove Application

Configure Cisco ASA [Reset Secret Key](#)

To set up this application, install the Duo Access Gateway and then configure your service provider. [View Cisco ASA SAML SSO instructions](#)

Next step: [Download your configuration file](#)

Service Provider

Base URL
Enter the Cisco ASA Base URL.

Tunnel Group
Enter the Tunnel Group you are protecting with SSO.

Custom attributes Use this setting if your Duo Access Gateway authentication source uses non-standard attribute names.

Mail attribute
The attribute containing the email address of the user.

[Save Configuration](#)

In diesem Dokument werden für die restliche Konfiguration Standardparameter verwendet. Sie können jedoch entsprechend den Anforderungen des Kunden festgelegt werden. Zu diesem Zeitpunkt können zusätzliche Einstellungen für die neue SAML-Anwendung angepasst werden, z. B. das Ändern des Anwendungsnamens vom Standardwert, das Aktivieren der Self-Service-Funktion oder das Zuweisen einer Gruppenrichtlinie.

3. Klicken Sie auf den Link "Download your configuration file" (Konfigurationsdatei herunterladen), um die Einstellungen der Cisco ASA-Anwendung (als JSON-Datei) abzurufen. Diese Datei wird in späteren Schritten auf das Duo Access Gateway hochgeladen.

Device Insight
Policies
Applications
Protect an Application
Single Sign-On
Users
Groups
Endpoints
2FA Devices
Administrators
Reports
Settings
Billing

Need Help?
Chat with Tech Support
Email Support
Call us at 1-855-386-2884
Account ID
2010-1403-48
Deployment ID
DU057
Helpful Links
Documentation

Cisco ASA - Duo Access Gateway

Authentication Log | Remove Application

Configure Cisco ASA

Reset Secret Key

To set up this application, install the Duo Access Gateway and then configure your service provider. [View Cisco ASA SAML SSO instructions](#)
Next step: [Download your configuration file](#)

Service Provider

Base URL:
Enter the Cisco ASA Base URL.

Tunnel Group:
Enter the Tunnel Group you are protecting with SSO.

Custom attributes: Use this setting if your Duo Access Gateway authentication source uses non-standard attribute names.

Mail attribute:
The attribute containing the email address of the user.

Save Configuration

4. Unter "Dashboard > Anwendungen" sieht die neu erstellte ASA-Anwendung wie in der Abbildung unten dargestellt aus:

admin-77d04ebc.duosecurity.com/applications

Cisco Study | Cisco Tools | Mix | SourceFire | VPN | AAA | ASA | IFT 6.7

Search for users, groups, applications, or devices

Cisco | ID: 2010-1403-48 | ciscoduobl

Dashboard > Applications

Applications

SSO Setup Guide | Protect an Application

Export | Search

Name	Type	Application Policy	Group Policies
Cisco ASA - Duo Access Gateway	Cisco ASA - Duo Access Gateway		

1 total

5. Navigieren Sie zu "Benutzer > Benutzer hinzufügen", wie in der Abbildung dargestellt:

Erstellen Sie einen Benutzer namens "duouser", der für die AnyConnect Remote Access-Authentifizierung verwendet werden soll, und aktivieren Sie Duo Mobile auf dem Endbenutzergerät.

The screenshot shows the Duo Admin console interface. On the left is a dark sidebar with navigation options: Dashboard, Device Insight, Policies, Applications, Users (highlighted), Add User (highlighted), Pending Enrollments, Bulk Enroll Users, Import Users, Directory Sync, Bypass Codes, Groups, and Endpoints. The main content area has a search bar at the top. Below it is a breadcrumb trail: Dashboard > Users > Add User. The main heading is 'Add User'. A sub-heading 'Adding Users' is followed by a paragraph: 'Most applications allow users to enroll themselves after they complete primary authentication.' and a link 'Learn more about adding users'. Below this is a form field for 'Username' containing the text 'duouser'. A note below the field says 'Should match the primary authentication username.' At the bottom of the form is a blue 'Add User' button.

Um die Telefonnummer hinzuzufügen, wie im Bild gezeigt, wählen Sie die Option "Telefon hinzufügen".

The screenshot shows the Duo Admin console interface for adding a phone. The sidebar is the same as in the previous screenshot, but 'Add User' is no longer highlighted. The breadcrumb trail is: Dashboard > Users > duouser > Add Phone. The main heading is 'Add Phone'. A link 'Learn more about Activating Duo Mobile' is present. Below is a 'Type' section with two radio buttons: 'Phone' (selected) and 'Tablet'. Below that is a 'Phone number' section with a dropdown menu showing the Indian flag and the text '+91 9xxx-xxx-xxx'. A link 'Show extension field' is next to it. A note below the field says 'Optional. Example: "+91 91234 56789"'. At the bottom of the form is a blue 'Add Phone' button.

Aktivieren Sie "Duo Mobile" für den jeweiligen Benutzer

Device Info

[Learn more about Activating Duo Mobile](#)



Not using Duo Mobile
[Activate Duo Mobile](#)



Model
Unknown



OS
Generic Smartphone



Hinweis: Stellen Sie sicher, dass "Duo Mobile" auf dem Endbenutzergerät installiert ist.
[Manuelle Installation der Duo Anwendung für IOS Geräte](#)
[Manuelle Installation der Duo Anwendung für Android Geräte](#)

Wählen Sie "Duo-Aktivierungscode generieren" wie im Bild gezeigt:

The screenshot shows the Duo Mobile activation page in a web interface. On the left is a dark sidebar with navigation options: Dashboard, Device Insight, Policies, Applications, Users, Groups, Endpoints, 2FA Devices (highlighted), Phones, Hardware Tokens, WebAuthn & U2F, Administrators, Reports, and Settings. The main content area has a search bar at the top and a breadcrumb trail: Dashboard > Phone: [redacted] > Activate Duo Mobile. The title is "Activate Duo Mobile". Below the title is a descriptive paragraph and a note: "Note: Generating an activation code will invalidate any existing Duo Mobile credentials for this device until it is activated with the new activation code." There are two input fields: "Phone" with a red redaction box, and "Expiration" with a value of "24" and a dropdown menu set to "hours" after generation. At the bottom is a blue button labeled "Generate Duo Mobile Activation Code" with a red border.

Wählen Sie "Send Instructions by SMS" (Anweisungen per SMS senden) wie im Bild gezeigt:

- Dashboard
- Device Insight
- Policies
- Applications
- Users
- Groups
- Endpoints
- 2FA Devices**
- Phones
- Hardware Tokens
- WebAuthn & U2F
- Administrators
- Reports
- Settings
- Billing
- Need Help?
- [Chat with Tech Support](#)
- [Email Support](#)
- Call us at 1-855-386-2884

[Dashboard](#) > [Phone: +91](#) > [Activate Duo Mobile](#)

Activate Duo Mobile

A new Duo Mobile activation code has been generated, and any old credentials have been invalidated. activation instructions to the user by SMS.

Phone

Installation instructions

Send installation instructions via SMS

Welcome to Duo! Please install Duo Mobile from your app store.

Activation instructions

Send activation instructions via SMS

*To activate the app, tap and open this link with Duo Mobile:
https://m-
77d04ebc.duosecurity.com/activate/YB5ucEisJAq1YIBN5ZrT*

[Send Instructions by SMS](#)

or [skip this step](#)

Klicken Sie auf den Link in der SMS, und die Duo App wird mit dem Benutzerkonto im Abschnitt "Geräteinformationen" verknüpft, wie im Bild gezeigt:

Dashboard

Device Insight

Policies

Applications

Users

Groups

Endpoints

2FA Devices

Phones

Hardware Tokens

WebAuthn & U2F

Administrators

Reports

Settings

Billing

Need Help?
Chat with Tech Support

Search for users, groups, applications, or devices

Cisco | ID: 2010-1403-48

Duo Mobile instructions SMS'ed to +91 [redacted]

Dashboard > Phones > Phone: +91 [redacted]

+91 [redacted] Send SMS Passcodes...

Shared phone
This phone is attached to multiple users.

duouser +91 [redacted]

testing 123 +91 [redacted]

Attach a user

Authentication devices can share multiple users

Device Info
Learn more about Activating Duo Mobile

Using Duo Mobile
Reactivate Duo Mobile

Model
Unknown

OS
Generic Smartphone

- Duo Access Gateway (DAG)-Konfiguration

1. Bereitstellung von Duo Access Gateway (DAG) auf einem Server in Ihrem Netzwerk

 Hinweis: Befolgen Sie zur Bereitstellung die folgenden Dokumente:

Duo Access Gateway für Linux

<https://duo.com/docs/dag-linux>

Duo Access Gateway für Windows

<https://duo.com/docs/dag-windows>

2. Navigieren Sie auf der Startseite von Duo Access Gateway zu "Authentication Source"

3. Geben Sie unter "Quellen konfigurieren" die folgenden Attribute für Ihr Active Directory ein, und klicken Sie auf "Einstellungen speichern".

Configure Sources

Configure authentication source settings below. Changes made to non-active authentication sources will take effect when made active.

Source type	<input type="text" value="Active Directory"/> Specify the authentication source to configure.
Status:	✓ LDAP Bind Succeeded ✓ ldap://10.197.243.110
Server	<input type="text" value="10.197"/> <input type="text" value="389"/> Hostname and port of your Active Directory. The port is typically 389 for cleartext LDAP and STARTTLS, and 636 for LDAPS. Hostnames can be comma separated for failover functionality. For example: ad1.server.com,ad2.server.com,10.1.10.150
Transport type	<input checked="" type="radio"/> CLEAR <input type="radio"/> LDAPS <input type="radio"/> STARTTLS This setting controls whether the communication between Active Directory and the Duo Access Gateway is encrypted.
Attributes	<input type="text" value="sAMAccountName,mail"/> Specify attributes to retrieve from the AD server. For example: sAMAccountName,mail.
Search base	<input type="text" value="CN=Users,DC=dmoudgil,DC=local"/> The DNs which will be used as a base for the search. Enter one per line. They will be searched in the order given.
Search attributes	<input type="text" value="sAMAccountName"/> Specify attributes the username should match against. For example: sAMAccountName,mail.
Search username	<input type="text" value="iseadmin"/> The username of an account that has permission to read from your Active Directory. We recommend creating a service account that has read-only access.
Search password	<input type="password" value="••••"/> The password corresponding to the search username specified above.
<input type="button" value="Save Settings"/>	

4. Wählen Sie unter "Set Active Source" den Quelltyp als "Active Directory" aus, und klicken Sie auf "Set Active Source".

Set Active Source

Specify the source that end-users will use for primary authentication.

Source type

5. Navigieren Sie zu "Applications" (Anwendungen hinzufügen), und laden Sie im Untermenü "Add Application" (Anwendung hinzufügen) die JSON-Datei hoch, die Sie von der Duo Admin Console im Abschnitt "Configuration file" (Konfigurationsdatei) heruntergeladen haben. Die entsprechende JSON-Datei wurde in Schritt 3 unter Duo Admin Portal Configuration heruntergeladen.

Applications


Add Application

Create a SAML application in the Duo Admin Panel. Then, download the provided configuration file and upload it here.

Configuration file

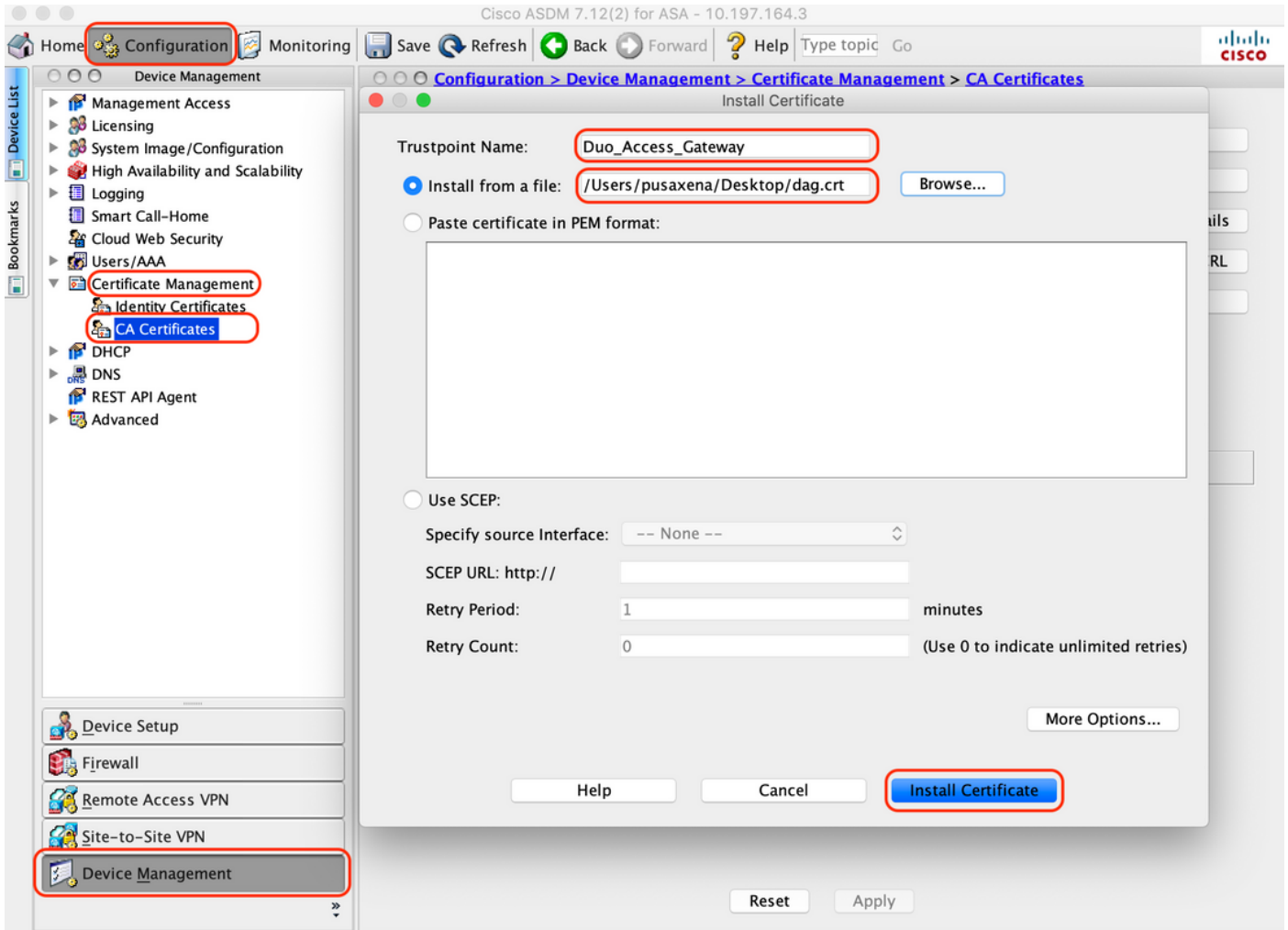
6. Sobald die Anwendung erfolgreich hinzugefügt wurde, wird sie im Untermenü "Anwendungen" angezeigt.

Applications

Name	Type	Logo	
Cisco ASA - Duo Access Gateway	Cisco ASA		<input type="button" value="Delete"/>

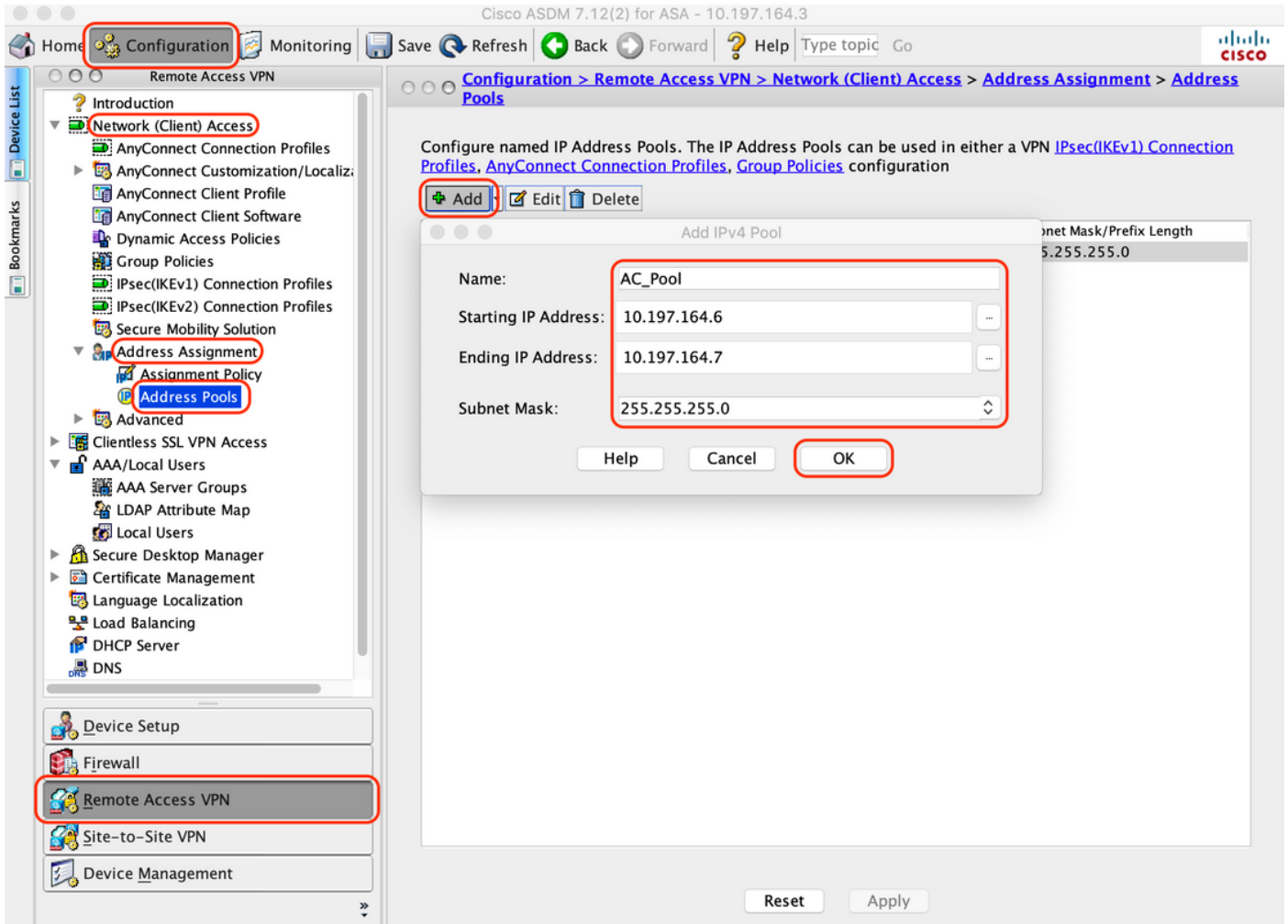
7. Laden Sie im Untermenü "Metadaten" die XML-Metadaten und das IdP-Zertifikat herunter, und notieren Sie sich die folgenden URLs, die später auf der ASA konfiguriert werden:

1. SSO-URL
2. Abmelde-URL
3. Entitäts-ID
4. Fehler-URL



2. Erstellen Sie einen lokalen IP-Pool für AnyConnect-Benutzer.

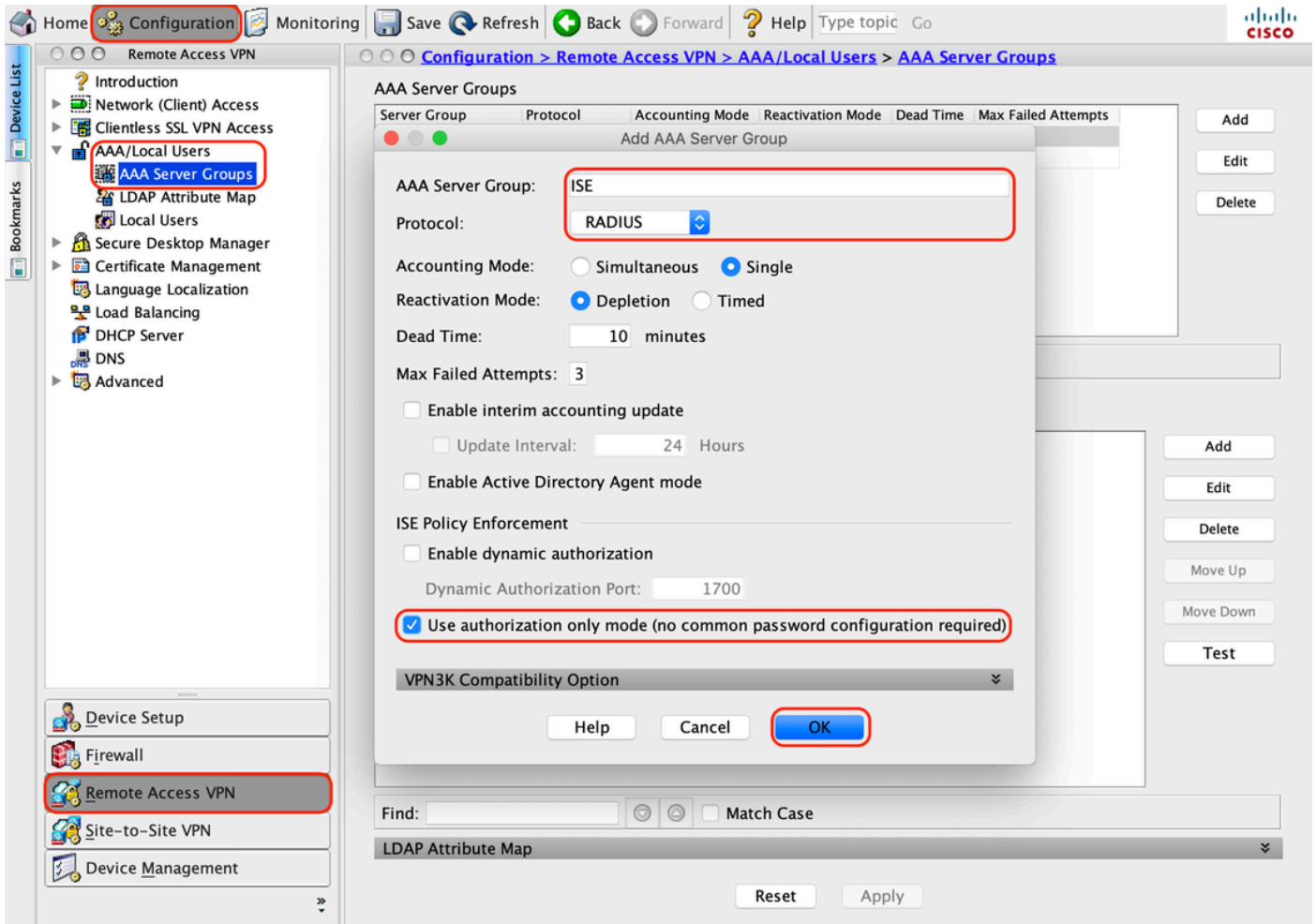
Navigieren Sie zu "Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Address Pools", und klicken Sie auf "Add".



3. Konfigurieren der AAA-Servergruppe

A.: Konfigurieren Sie in diesem Abschnitt die AAA-Servergruppe, und geben Sie Details zum AAA-Server an, der die Autorisierung durchführt.

B. Navigieren Sie zu "Configuration > Remote Access VPN > AAA/Local Users > AAA Server Groups", und klicken Sie auf "Add" (Hinzufügen).



C. Klicken Sie auf derselben Seite im Abschnitt "Server in der ausgewählten Gruppe" auf "Hinzufügen", und geben Sie die IP-Adresse des AAA-Servers an.

Cisco ASDM 7.12(2) for ASA - 10.197.164.3

Configuration > Remote Access VPN > AAA/Local Users > AAA Server Groups

Server Group	Protocol	Accounting Mode	Reactivation Mode	Dead Time	Max Failed Attempts
ISE	RADIUS	Single	Depletion	10	3
LOCAL	LOCAL				

Add AAA Server

Server Group: ISE

Interface Name: outside

Server Name or IP Address: 10.106.44.77

Timeout: 10 seconds

RADIUS Parameters

Server Authentication Port: 1645

Server Accounting Port: 1646

Retry Interval: 10 seconds

Server Secret Key: [Redacted]

Common Password: [Redacted]

ACL Netmask Convert: Standard

Microsoft CHAPv2 Capable:

SDI Messages

Message Table

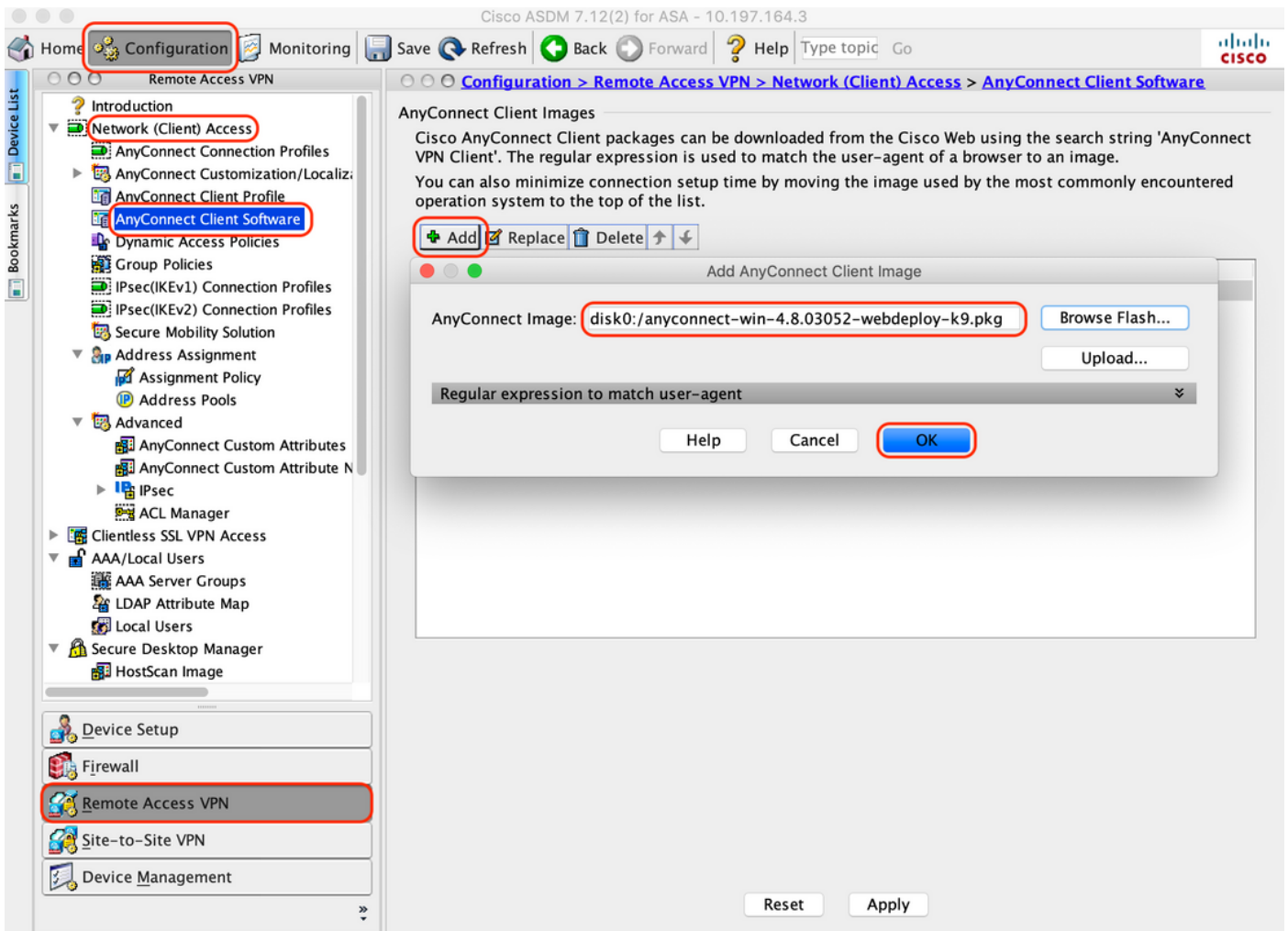
Help Cancel OK

Reset Apply

4. AnyConnect-Clientsoftware zuordnen

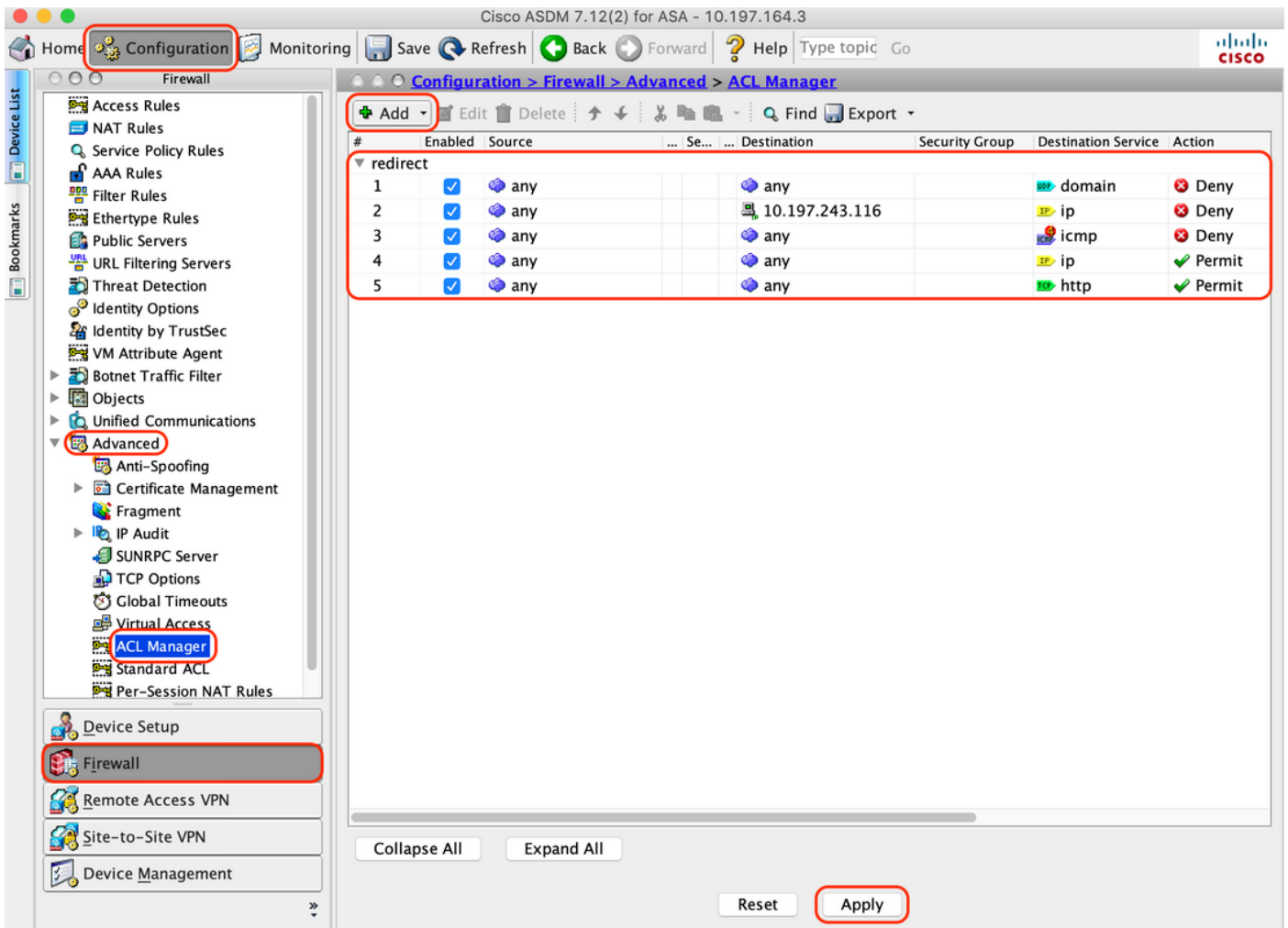
A. Map the AnyConnect client software webdeploy image 4.8.03052 for windows to be used for WebVPN

B. Navigieren Sie zu "Konfiguration > Remotezugriff-VPN > Netzwerkzugriff (Client) > AnyConnect-Clientsoftware", und klicken Sie auf "Hinzufügen".



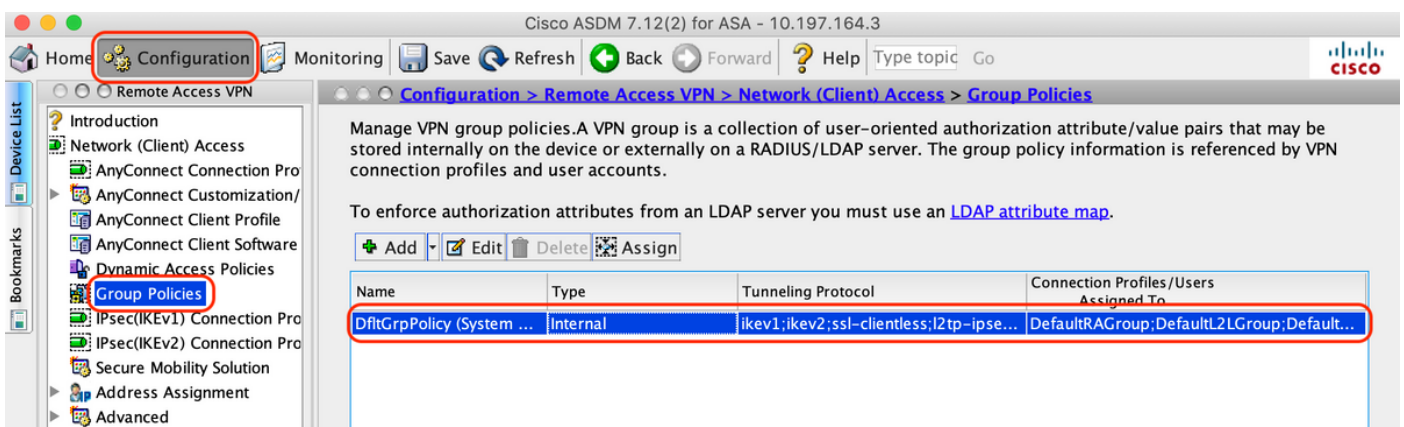
5. Konfigurieren Sie die als Ergebnis der ISE weitergeleitete ACL.

A. Navigieren Sie zu "Configuration > Firewall > Advanced > ACL Manager", und klicken Sie auf Add, um die Umleitungszugriffskontrollliste hinzuzufügen. Die Einträge sehen nach der Konfiguration wie folgt aus:



6. Bestehende Gruppenrichtlinie validieren

A. Bei dieser Konfiguration wird die standardmäßige Gruppenrichtlinie verwendet. Diese kann angezeigt werden unter: "Konfiguration > Remotezugriff-VPN > Netzwerkzugriff (Client) > Gruppenrichtlinien"

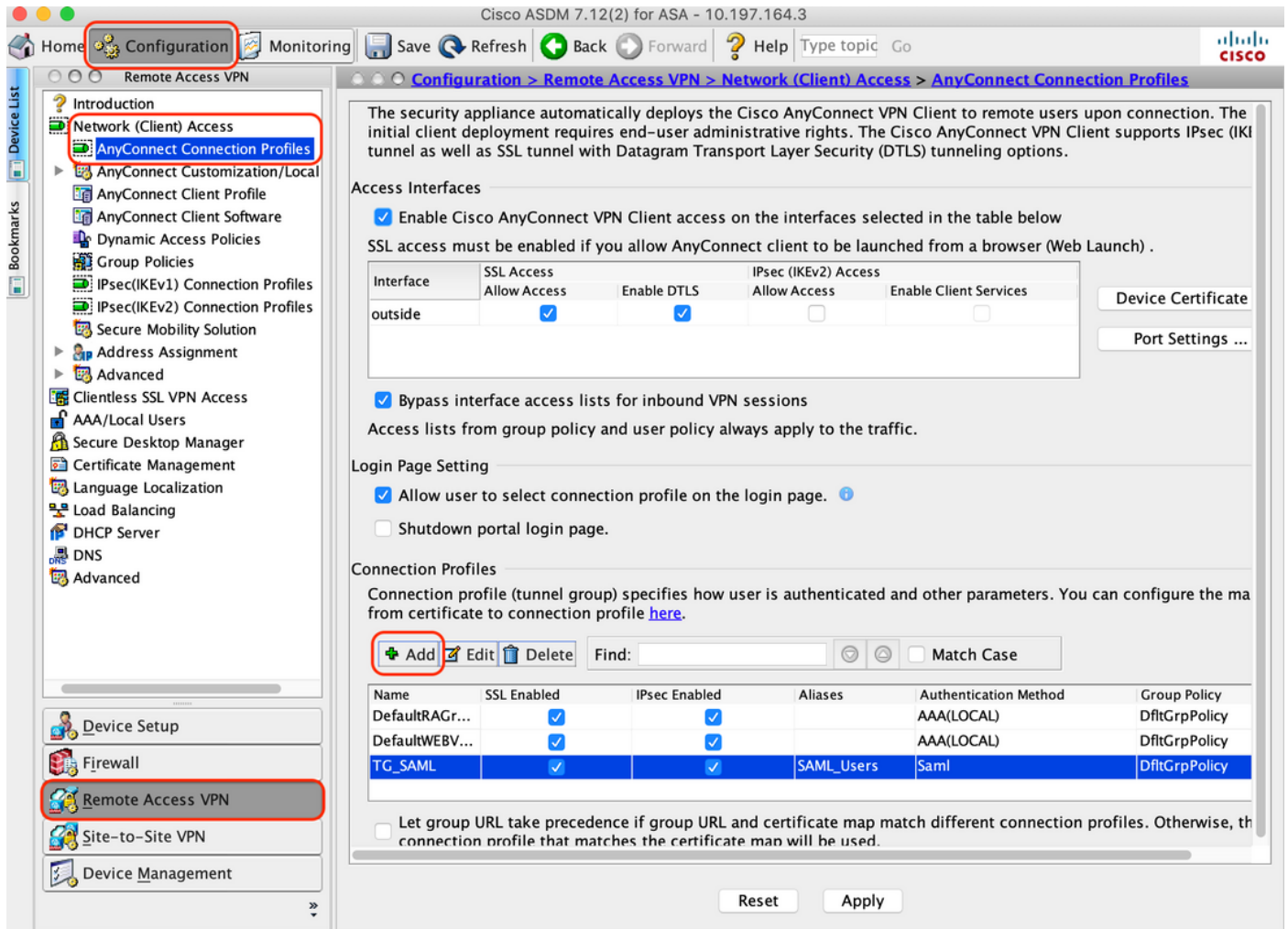


7. Verbindungsprofil konfigurieren

A. Erstellen Sie ein neues Verbindungsprofil, mit dem AnyConnect-Benutzer eine Verbindung

herstellen.

B. Navigieren Sie zu "Konfiguration > Remotezugriff-VPN > Netzwerkzugriff (Client) > AnyConnect-Verbindungsprofile", und klicken Sie auf "Hinzufügen".



C. Konfigurieren Sie die folgenden Details für das Verbindungsprofil:

Name	TG_SAML
Aliase	SAML_Benutzer
Methode	SAML
AAA-Servergruppe	Lokal
Client-Adresspools	AC-Pool
Gruppenrichtlinie	DfitGrpPolicy

Basic
▶ Advanced

Name: TG_SAML

Aliases: SAML_Users

Authentication

Method: SAML

AAA Server Group: LOCAL Manage...

Use LOCAL if Server Group fails

SAML Identity Provider

SAML Server : <https://explorer.cisco.com/dag/saml2/idp/metadata.php> Manage...

Client Address Assignment

DHCP Servers:

None DHCP Link DHCP Subnet

Client Address Pools: AC_Pool Select...

Client IPv6 Address Pools: Select...

Default Group Policy

Group Policy: DfltGrpPolicy Manage...

(Following fields are linked to attribute of the group policy selected above.)

Enable SSL VPN client protocol

Enable IPsec(IKEv2) client protocol

DNS Servers:

WINS Servers:

Domain Name:

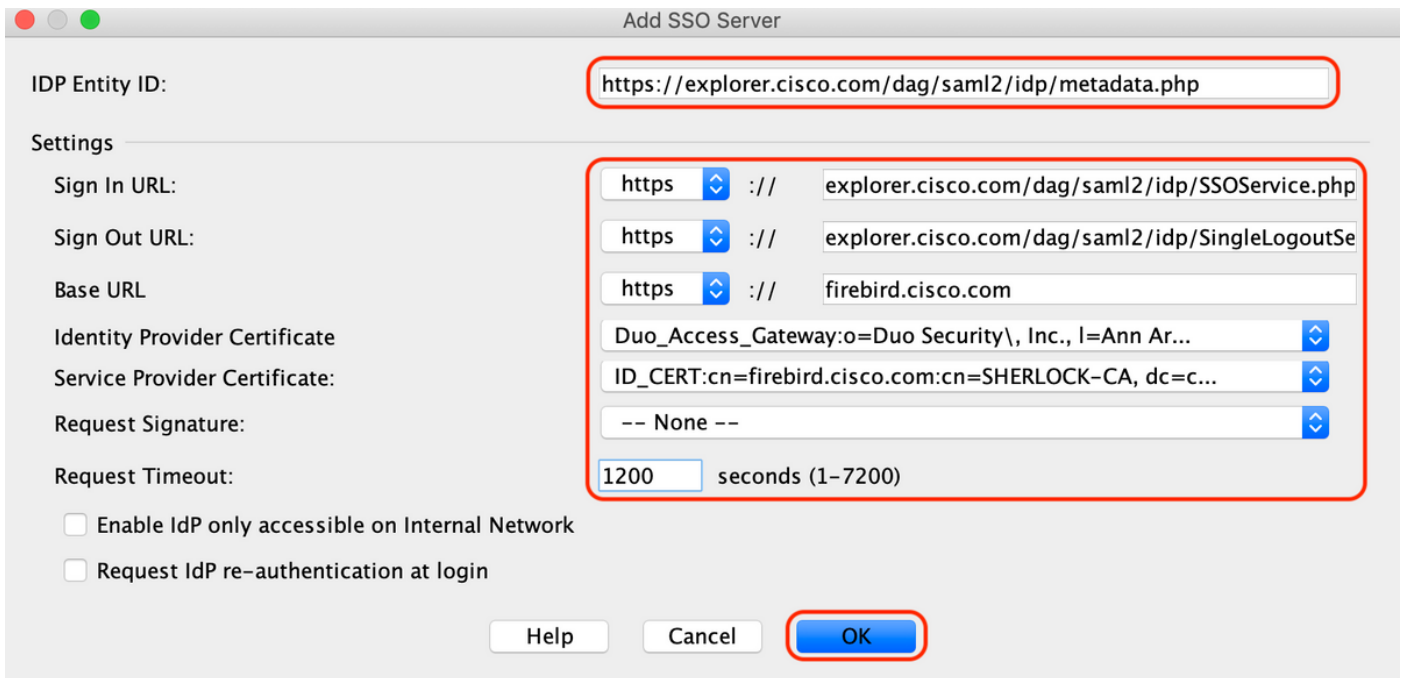
Find: Next Previous

Help Cancel OK

D. Konfigurieren Sie auf derselben Seite die Details des SAML Identity Providers, die wie folgt aussehen:

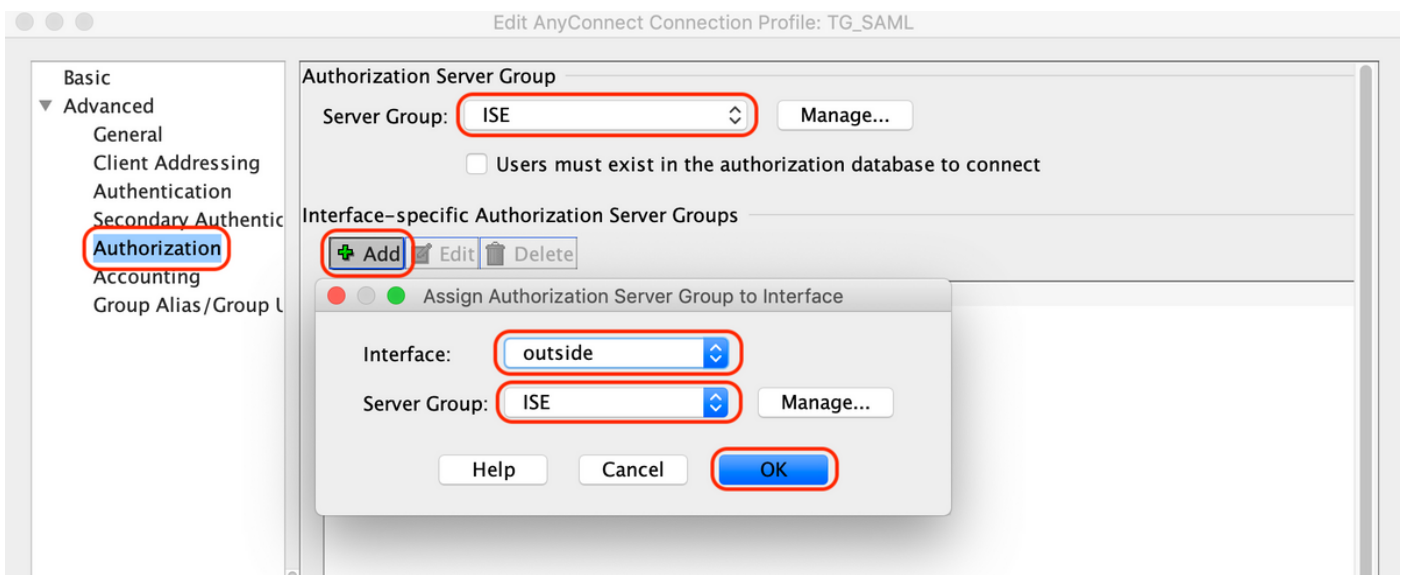
ID der IDP-Einheit	https://explorer.cisco.com/dag/saml2/idp/metadata.php
Anmelde-URL	https://explorer.cisco.com/dag/saml2/idp/SSOService.php
Abmelde-URL	https://explorer.cisco.com/dag/saml2/idp/SingleLogoutService.php?ReturnTo=https://explorer.c
Basis-URL	https://firebird.cisco.com

E. Klicken Sie auf "Verwalten > Hinzufügen"



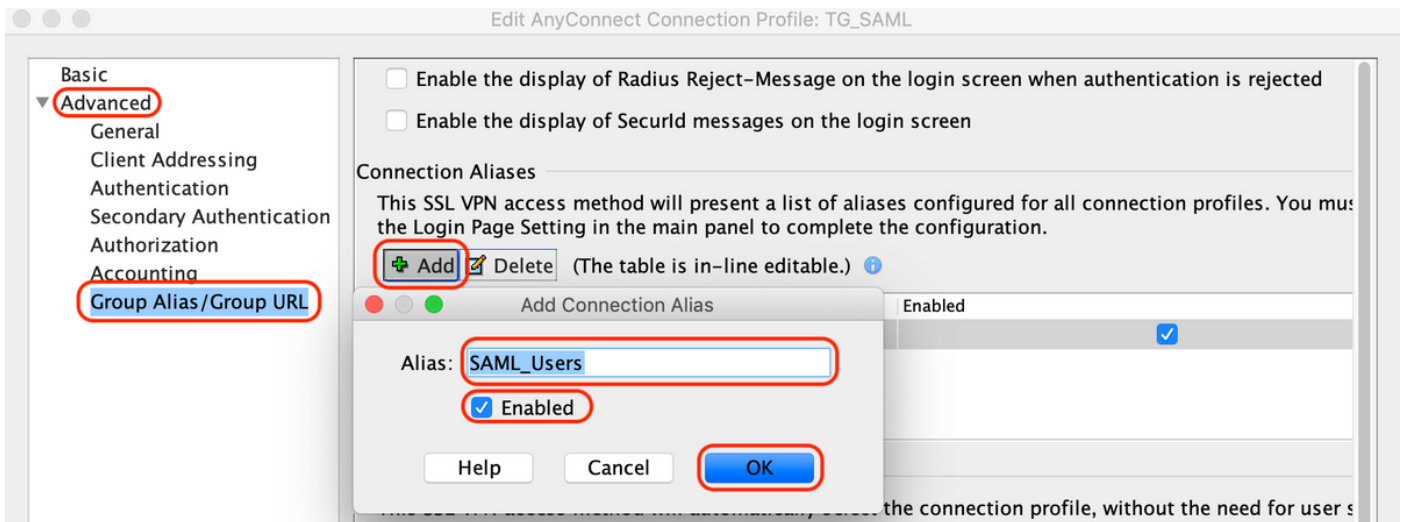
F. Definieren Sie im Abschnitt "Erweitert" für das Verbindungsprofil den AAA-Server für die Autorisierung.

Navigieren Sie zu "Erweitert > Autorisierung", und klicken Sie auf "Hinzufügen".



G. Definieren Sie unter Gruppenalias den Verbindungsalias.

Navigieren Sie zu "Erweitert > Gruppenalias/Gruppen-URL", und klicken Sie auf "Hinzufügen".



H. Damit ist die ASA-Konfiguration abgeschlossen. Dies sieht wie unten auf der Befehlszeilenschnittstelle (CLI) aus.

```

!
hostname firebird
domain-name cisco.com
!
!
name 10.197.164.7 explorer.cisco.com
name 10.197.164.3 firebird.cisco.com
!
!-----Client pool configuration-----
!
ip local pool AC_Pool 10.197.164.6-explorer.cisco.com mask 255.255.255.0
!
!-----Redirect Access-list-----
!
access-list redirect extended deny udp any any eq domain
access-list redirect extended deny ip any host 10.197.243.116
access-list redirect extended deny icmp any any
access-list redirect extended permit ip any any
access-list redirect extended permit tcp any any eq www
!
!-----AAA server configuration-----
!
aaa-server ISE protocol radius
  authorize-only
  interim-accounting-update periodic 1
  dynamic-authorization
aaa-server ISE (outside) host 10.106.44.77
  key *****
!
!-----Configure Trustpoint for Duo Access Gateway Certificate-----
!
crypto ca trustpoint Duo_Access_Gateway
  enrollment terminal
  crl configure
!
!-----Configure Trustpoint for ASA Identity Certificate-----
!
crypto ca trustpoint ID_CERT
  enrollment terminal
  fqdn firebird.cisco.com

```

```

subject-name CN=firebird.cisco.com
ip-address 10.197.164.3
keypair ID_RSA_KEYS
no ca-check
cr1 configure
!
!-----Enable AnyConnect and configuring SAML authentication-----
!
webvpn
enable outside
hsts
enable
max-age 31536000
include-sub-domains
no preload
anyconnect image disk0:/anyconnect-win-4.8.03052-webdeploy-k9.pkg 1
anyconnect enable
saml idp https://explorer.cisco.com/dag/saml2/idp/metadata.php
url sign-in https://explorer.cisco.com/dag/saml2/idp/SSOService.php
url sign-out https://explorer.cisco.com/dag/saml2/idp/SingleLogoutService.php?ReturnTo=https://explor
base-url https://firebird.cisco.com
trustpoint idp Duo_Access_Gateway
trustpoint sp ID_CERT
no signature
no force re-authentication
timeout assertion 1200
tunnel-group-list enable
cache
disable
error-recovery disable
!
!-----Group Policy configuration-----
!
group-policy DfltGrpPolicy attributes
vpn-tunnel-protocol ikev1 ikev2 l2tp-ipsec ssl-client ssl-clientless
!
!-----Tunnel-Group (Connection Profile) Configuraiton-----
!
tunnel-group TG_SAML type remote-access
tunnel-group TG_SAML general-attributes
address-pool AC_Pool
authorization-server-group ISE
accounting-server-group ISE
tunnel-group TG_SAML webvpn-attributes
authentication saml
group-alias SAML_Users enable
saml identity-provider https://explorer.cisco.com/dag/saml2/idp/metadata.php
!

```

-ISE-Konfiguration

1. Cisco ASA als Netzwerkgerät hinzufügen

Klicken Sie unter "Administration > Network Resources > Network Devices" auf "Add" (Hinzufügen).

Konfigurieren Sie den Namen des Netzwerkgeräts, die zugehörige IP-Adresse, und konfigurieren Sie unter "Radius Authentication Settings" den "Shared Secret", und klicken Sie auf "Save"

(Speichern).

[Network Devices List](#) > [ASA](#)

Network Devices

* Name

Description

* IP : /


* Device Profile 


Model Name

Software Version

* Network Device Group

Location 

IPSEC 

Device Type 

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol **RADIUS**

* Shared Secret

Use Second Shared Secret

CoA Port

RADIUS DTLS Settings

DTLS Required

Shared Secret

CoA Port

Issuer CA of ISE Certificates for CoA

DNS Name

General Settings

Enable KeyWrap

* Key Encryption Key

* Message Authenticator Code Key

Key Input Format ASCII HEXADECIMAL

TACACS Authentication Settings

SNMP Settings

Advanced TrustSec Settings

2. Installation der neuesten Statusaktualisierungen

Navigieren Sie zu "Administration > System > Settings > Posture > Updates", und klicken Sie auf "Update Now" (Jetzt aktualisieren).

Posture Updates

Web

Offline

* Update Feed URL

Proxy Address ⓘ

Proxy Port HH MM SS

Automatically check for updates starting from initial delay every hours ⓘ

▼ Update Information

Last successful update on	2020/05/07 15:15:05 ⓘ
Last update status since ISE was started	No update since ISE was started. ⓘ
Cisco conditions version	224069.0.0.0
Cisco AV/AS support chart version for windows	171.0.0.0
Cisco AV/AS support chart version for Mac OSX	91.0.0.0
Cisco supported OS version	41.0.0.0

3. Laden Sie das Compliance-Modul und das AnyConnect Headend-Bereitstellungspaket auf die ISE hoch.

Navigieren Sie zu "Richtlinie > Richtlinienelemente > Ergebnisse > Client-Bereitstellung > Ressourcen". Klicken Sie auf "Hinzufügen", und wählen Sie je nachdem, ob die Dateien von der lokalen Workstation oder von der Cisco Website abgerufen werden sollen, "Agenten-Ressourcen von der lokalen Festplatte" oder "Agenten-Ressourcen von der Cisco Website" aus.

In diesem Fall wählen Sie zum Hochladen von Dateien von der lokalen Workstation unter Kategorie "Von Cisco bereitgestellte Pakete" aus, klicken auf "Durchsuchen", wählen die erforderlichen Pakete aus und klicken auf "Senden".

In diesem Dokument wird "anyconnect-win-4.3.1012.6145-isecompliance-webdeploy-k9.pkg" als Compliance-Modul und "anyconnect-win-4.8.03052-webdeploy-k9.pkg" als AnyConnect Headend-Bereitstellungspaket verwendet.

Agent Resources From Local Disk

Category ⓘ

Browse...

▼ **AnyConnect Uploaded Resources**

Name	Type	Version	Description
AnyConnectDesktopWindows 4.8.30...	AnyConnectDesktopWindows	4.8.3052.0	AnyConnect Secure Mobility Clie...

4. AnyConnect-Posture-Profil erstellen

A. Navigieren Sie zu "Richtlinie > Richtlinienelemente > Ergebnisse > Client-Bereitstellung > Ressourcen". Klicken Sie auf "Hinzufügen", und wählen Sie "AnyConnect Posture Profile" aus.

B. Geben Sie den Namen für AnyConnect Posture Profile ein, und konfigurieren Sie den Servernamen als "*" unter "Servernamen", und klicken Sie auf "Speichern".

ISE Posture Agent Profile Settings > **Anyconnect Posture Profile**

* Name:

Description:

Posture Protocol

Parameter	Value	Notes	Description
PRA retransmission time	<input type="text" value="120"/> secs		This is the agent retry period if there is a Passive Reassessment communication failure
Retransmission Delay	<input type="text" value="60"/> secs	Default Value: 60. Acceptable Range between 5 to 300. Accept only integer Values.	Time (in seconds) to wait before retrying.
Retransmission Limit	<input type="text" value="4"/>	Default value: 4. Acceptable Range between 0 to 10. Accept only integer Values.	Number of retries allowed for a message.
Discovery host	<input type="text"/>	IPv4 or IPv6 addresses or FQDNs. IPv6 address should be without square brackets[]	The server that the agent should connect to
Server name rules	<input type="text" value="*"/>	need to be blank by default to force admin to enter a value. "*" means agent will connect to all	A list of wildcarded, comma-separated names that defines the servers that the agent can connect to. E.g. "*.cisco.com"
Call Home List	<input type="text"/>	List of IPv4 or IPv6 addresses, FQDNs with or without port must be comma-separated and with colon in between the IP address/FQDN and the port. Example: IPaddress/FQDN:Port (Port number should be the same, specified in the Client Provisioning portal)	A list of IP addresses, that defines the all the Policy service nodes that the agent will try to connect to if the PSN that authenticated the endpoint doesn't respond for some reason.
Back-off Timer	<input type="text" value="30"/> secs	Enter value of back-off timer in seconds, the supported range is between 10s - 600s.	Anyconnect agent will continuously try to reach discovery targets (redirection targets and previously connected PSNs) by sending the discovery packets till this max time limit is reached

5. AnyConnect-Konfiguration erstellen

A. Navigieren Sie zu "Richtlinie > Richtlinienelemente > Ergebnisse > Client-Bereitstellung > Ressourcen". Klicken Sie auf "Hinzufügen", und wählen Sie "AnyConnect-Konfiguration" aus.

B. Wählen Sie AnyConnect-Paket, geben Sie den Konfigurationsnamen ein, und wählen Sie das erforderliche Compliance-Modul aus.

C. Aktivieren Sie unter "AnyConnect Module Selection" das Kontrollkästchen "Diagnostic and Reporting Tool".

D. Wählen Sie unter "Profile Selection" (Profilauswahl) die Option Posture Profile und klicken Sie auf "Save" (Speichern).

* Select AnyConnect Package **AnyConnectDesktopWindows 4.8.3052.0** ▼

* Configuration Name **AnyConnect Configuration**

Description:

DescriptionValue

* Compliance Module **AnyConnectComplianceModuleWindows 4.3.1250.614** ▼

Notes

AnyConnect Module Selection

ISE Posture

VPN

Network Access Manager

Web Security

AMP Enabler

ASA Posture

Network Visibility

Umbrella Roaming Security

Start Before Logon

Diagnostic and Reporting Tool

Profile Selection

* ISE Posture **Anyconnect Posture Profile** ▼

VPN ▼

Network Access Manager ▼

Web Security ▼

AMP Enabler ▼

Network Visibility ▼

Umbrella Roaming Security ▼

Customer Feedback ▼

6. Client-Bereitstellungsrichtlinie erstellen

A. Navigieren Sie zu "Richtlinie > Client-Bereitstellung"

B. Klicken Sie auf "Bearbeiten" und wählen Sie "Regel oben einfügen".

C. Geben Sie den Regelnamen ein, wählen Sie das erforderliche Betriebssystem aus, und wählen Sie unter Results (unter "Agent" > "Agentenkonfiguration") die in Schritt 5 erstellte AnyConnect-Konfiguration aus, und klicken Sie auf "Speichern".

Client Provisioning Policy

Define the Client Provisioning Policy to determine what users will receive upon login and user session initiation:
 For Agent Configuration: version of agent, agent profile, agent compliance module, and/or agent customization package.
 For Native Supplicant Configuration: wizard profile and/or wizard. Drag and drop rules to change the order.

Rule Name	Identity Groups	Operating Systems	Other Conditions	Results
IOS	If Any and	Apple iOS All	and Condition(s)	then Cisco-ISE-NSP
Android	If Any and	Android	and Condition(s)	then Cisco-ISE-NSP
Windows_10	If Any and	Windows 10 (All)	and Condition(s)	then AnyConnect Configuration
Windows	If Any and	Windows All	and Condition(s)	then CiscoTemporalAgentWindows 4.7.00135 And WinSPWizard 2.5.0.1 And Cisco-ISE-NSP
MAC OS	If Any and	Mac OSX	and Condition(s)	then CiscoTemporalAgentOS X 4.7.00135 And MacOsXSPWizard 2.1.0.42 And Cisco-ISE-NSP
Chromebook	If Any and	Chrome OS All	and Condition(s)	then Cisco-ISE-Chrome-NSP

Save Reset

7. Eine Statusbedingung erstellen

A. Navigieren Sie zu "Richtlinie > Richtlinienelemente > Bedingungen > Status > Dateibedingung".

B. Klicken Sie auf "Hinzufügen", und konfigurieren Sie den Bedingungsnamen "VPN_Posture_File_Check", das erforderliche Betriebssystem als "Windows 10(All)", den Dateityp als "FileExistence", den Dateipfad als "ABSOLUTE_PATH" und den vollständigen Pfad und Dateinamen als "C:\custom.txt". Wählen Sie Dateioperator als "Exists" aus.

C. In diesem Beispiel wird das Vorhandensein einer Datei mit dem Namen "custom.txt" unter Laufwerk C: als Dateibedingung verwendet.

File Conditions List > VPN_Posture_File_Check

File Condition

* Name: VPN_Posture_File_Check

Description:

* Operating System: Windows 10 (All)

Compliance Module: Any version

* File Type: FileExistence

* File Path: ABSOLUTE_PATH

* File Operator: Exists

C:\custom.txt

Save Reset

8. Aktion zur Statusbehebung erstellen

Navigieren Sie zu "Policy > Policy Elements > Results > Posture > Remediation Actions" (Richtlinie > Richtlinienelemente > Ergebnisse > Status > Korrekturmaßnahmen), um eine entsprechende Dateibereinigungsaktion zu erstellen. Dieses Dokument verwendet "Nur Nachrichtentext" als Korrekturmaßnahmen, die im nächsten Schritt konfiguriert werden.

9. Statusanforderungsregel erstellen

A. Navigieren Sie zu "Richtlinie > Richtlinienelemente > Ergebnisse > Status > Anforderungen".

B. Klicken Sie auf "Bearbeiten" und wählen Sie dann "Neue Anforderung einfügen".

C. Konfigurieren Sie den Bedingungsnamen "VPN_Posture_Requirement", das erforderliche Betriebssystem als "Windows 10(Alle)", das Compliance-Modul als "4.x oder höher", den Statustyp als "AnyConnect".

D. Bedingungen wie "VPN_Posture_File_Check" (erstellt in Schritt 7) und unter "Korrekturmaßnahmen" Aktion als "Nur Nachrichtentext" auswählen und die benutzerdefinierte Nachricht für Agent-Benutzer eingeben

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The breadcrumb navigation is: Policy > Policy Elements > Results > Posture > Remediation Actions > Requirements. The 'Requirements' table is displayed with the following columns: Name, Operating System, Compliance Module, Posture Type, Conditions, and Remediations Actions. The row for 'VPN_Posture_Requirement' is highlighted with a red box. Below the table, there is a note: 'Note: Remediation Action is filtered based on the operating system and stealth mode selection. Remediation Actions are not applicable for Application Conditions (configured using the Provision By Category or Provision By Everything options), Hardware Conditions, and External Data source conditions.' At the bottom of the table, there are 'Save' and 'Reset' buttons.

Name	Operating System	Compliance Module	Posture Type	Conditions	Remediations Actions
requirement_vvrr					
Default_Hardware_Attributes_Requirement_Mac	for Mac OSX	using 4.x or later	using AnyConnect	met if Hardware_Attributes_Check	then Select Remediations
Default_Firewall_Requirement_Win	for Windows All	using 4.x or later	using AnyConnect	met if Default_Firewall_Condition_Win	then Default_Firewall_Remediation_Win
Default_Firewall_Requirement_Mac	for Mac OSX	using 4.x or later	using AnyConnect	met if Default_Firewall_Condition_Mac	then Default_Firewall_Remediation_Mac
USB_Block_temporal	for Windows All	using 4.x or later	using Temporal Agent	met if USB_Check	then Message Text Only
Any_AM_Installation_Win_temporal	for Windows All	using 4.x or later	using Temporal Agent	met if ANY_am_win_inst	then Message Text Only
Any_AM_Installation_Mac_temporal	for Mac OSX	using 4.x or later	using Temporal Agent	met if ANY_am_mac_inst	then Message Text Only
Default_AppVis_Requirement_Win_temporal	for Windows All	using 4.x or later	using Temporal Agent	met if Default_AppVis_Condition_Win	then Select Remediations
Default_AppVis_Requirement_Mac_temporal	for Mac OSX	using 4.x or later	using Temporal Agent	met if Default_AppVis_Condition_Mac	then Select Remediations
Default_Hardware_Attributes_Requirement_Win_temporal	for Windows All	using 4.x or later	using Temporal Agent	met if Hardware_Attributes_Check	then Select Remediations
Default_Hardware_Attributes_Requirement_Mac_temporal	for Mac OSX	using 4.x or later	using Temporal Agent	met if Hardware_Attributes_Check	then Select Remediations
Default_Firewall_Requirement_Win_temporal	for Windows All	using 4.x or later	using Temporal Agent	met if Default_Firewall_Condition_Win	then Default_Firewall_Remediation_Win
Default_Firewall_Requirement_Mac_temporal	for Mac OSX	using 4.x or later	using Temporal Agent	met if Default_Firewall_Condition_Mac	then Default_Firewall_Remediation_Mac
VPN_Posture_Requirement	for Windows 10 (All)	using 4.x or later	using AnyConnect	met if VPN_Posture_File_Check	then Message Text Only

10. Erstellen einer Statusrichtlinie

A. Navigieren Sie zu "Policies > Status"

B. Konfigurieren Sie den Regelnamen als "VPN_Posture_Policy_Win", das erforderliche Betriebssystem als "Windows 10(Alle)", das Kompatibilitätsmodul als "4.x oder höher", den Statustyp als "AnyConnect" und die Anforderungen als "VPN_Posture_Requirement", wie in Schritt 9 konfiguriert

Posture Policy
Define the Posture Policy by configuring rules based on operating system and/or other conditions.

Status	Policy Options	Rule Name	Identity Groups	Operating Systems	Compliance Module	Posture Type	Other Conditions	Requirements
2	Policy Options	Default_AppVis_Policy_Win	If Any	and Windows All	and 4.x or later	and AnyConnect	and	then Default_AppVis_Requirement_Win
2	Policy Options	Default_AppVis_Policy_Win_temporal	If Any	and Windows All	and 4.x or later	and Temporal Agent	and	then Default_AppVis_Requirement_Win_temporal
2	Policy Options	Default_Firewall_Policy_Mac	If Any	and Mac OSX	and 4.x or later	and AnyConnect	and	then Default_Firewall_Requirement_Mac
2	Policy Options	Default_Firewall_Policy_Mac_temporal	If Any	and Mac OSX	and 4.x or later	and Temporal Agent	and	then Default_Firewall_Requirement_Mac_temporal
2	Policy Options	Default_Firewall_Policy_Win	If Any	and Windows All	and 4.x or later	and AnyConnect	and	then Default_Firewall_Requirement_Win
2	Policy Options	Default_Firewall_Policy_Win_temporal	If Any	and Windows All	and 4.x or later	and Temporal Agent	and	then Default_Firewall_Requirement_Win_temporal
2	Policy Options	Default_Hardware_Attributes_Policy_Mac	If Any	and Mac OSX	and 4.x or later	and AnyConnect	and	then Default_Hardware_Attributes_Requirement_Mac
2	Policy Options	Default_Hardware_Attributes_Policy_Mac_temporal	If Any	and Mac OSX	and 4.x or later	and Temporal Agent	and	then Default_Hardware_Attributes_Requirement_Mac_temporal
2	Policy Options	Default_Hardware_Attributes_Policy_Win	If Any	and Windows All	and 4.x or later	and AnyConnect	and	then Default_Hardware_Attributes_Requirement_Win
2	Policy Options	Default_Hardware_Attributes_Policy_Win_temporal	If Any	and Windows All	and 4.x or later	and Temporal Agent	and	then Default_Hardware_Attributes_Requirement_Win_temporal
2	Policy Options	Default_USB_Block_Policy_Win	If Any	and Windows All	and 4.x or later	and AnyConnect	and	then USB_Block
2	Policy Options	Default_USB_Block_Policy_Win_temporal	If Any	and Windows All	and 4.x or later	and Temporal Agent	and	then USB_Block_temporal
2	Policy Options	VPN_Posture_Policy_Win	If Any	and Windows 10 (All)	and 4.x or later	and AnyConnect	and	then VPN_Posture_Requirement

Save Reset

11. Erstellen dynamischer Zugriffskontrolllisten (DACLS)

Navigieren Sie zu "Policy > Policy Elements > Results > Authorization > Downloadable ACLS" (Richtlinie > Richtlinienelemente > Ergebnisse > Autorisierung > herunterladbare ACLS), und erstellen Sie die DACLS für verschiedene Statusstatus.

In diesem Dokument werden die folgenden DACLS verwendet.

A. Status unbekannt: Ermöglicht Datenverkehr zu DNS-, PSN- und HTTP- sowie HTTPS-Datenverkehr

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Policy Sets Profiling Posture Client Provisioning Policy Elements

Dictionarys Conditions Results

Downloadable ACL List > PostureUnknown

Downloadable ACL

* Name: PostureUnknown

Description:

IP version: IPv4 IPv6 Agnostic

* DACL Content:

```

1234567 permit udp any any eq domain
8910111 permit ip any host 10.106.44.77
2131415 permit tcp any any eq 80
1617181 permit tcp any any eq 443
9202122
2324252
6272829
3031323
3343536

```

Check DACL Syntax

Save Reset

B. Status nicht konform: Verweigert den Zugriff auf private Subnetze und lässt nur Internetdatenverkehr zu

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Policy Sets Profiling Posture Client Provisioning Policy Elements

Dictionarys Conditions Results

Downloadable ACL List > PostureNonCompliant

Downloadable ACL

* Name: PostureNonCompliant

Description:

IP version: IPv4 IPv6 Agnostic

* DACL Content:

```

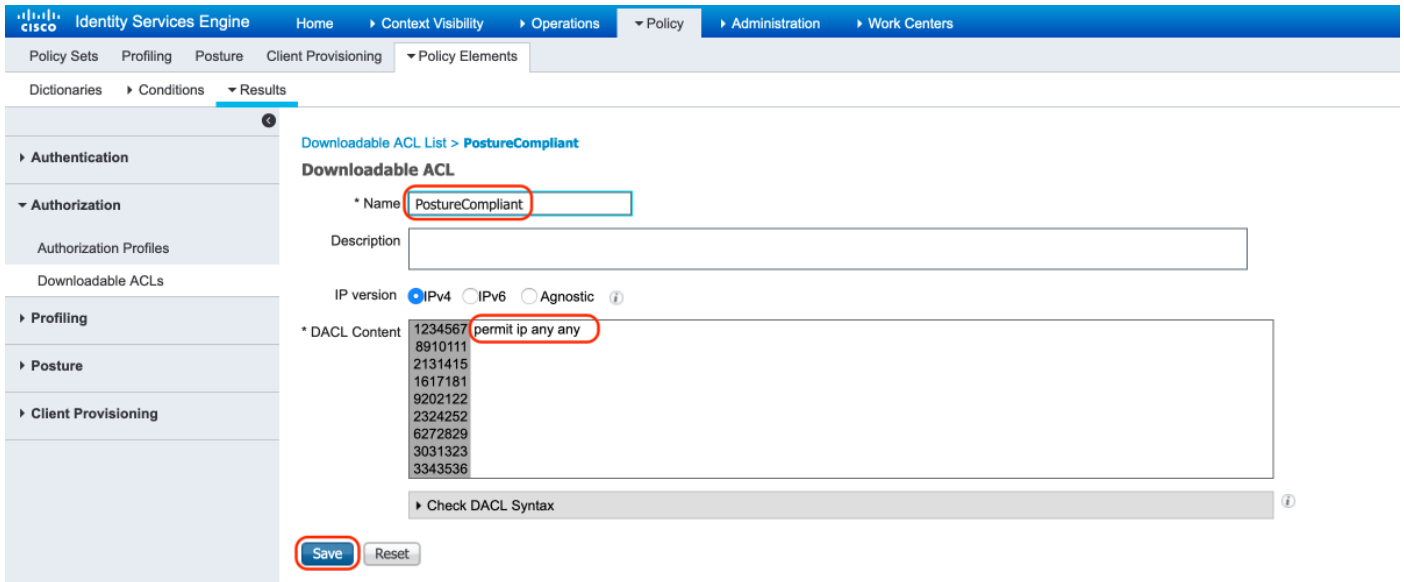
1234567 deny ip any 10.0.0.0 255.0.0.0
8910111 deny ip any 172.16.0.0 255.240.0.0
2131415 deny ip any 192.168.0.0 255.255.0.0
1617181 permit ip any any
9202122
2324252
6272829
3031323
3343536

```

Check DACL Syntax

Save Reset

C. Posture Compliant: Ermöglicht den gesamten Datenverkehr für Endbenutzer, die Posture Compliant sind

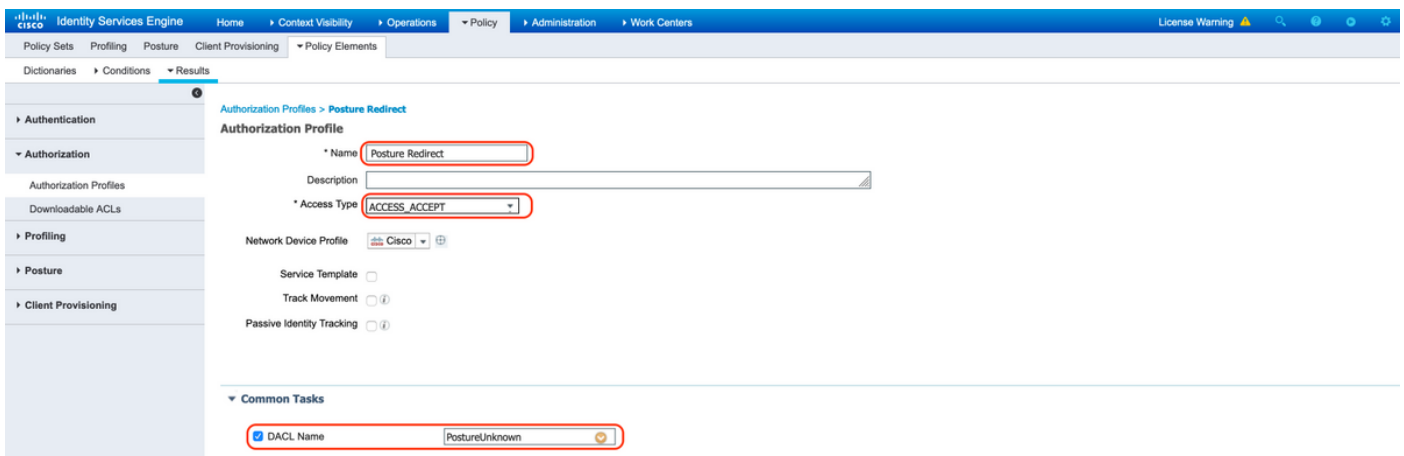


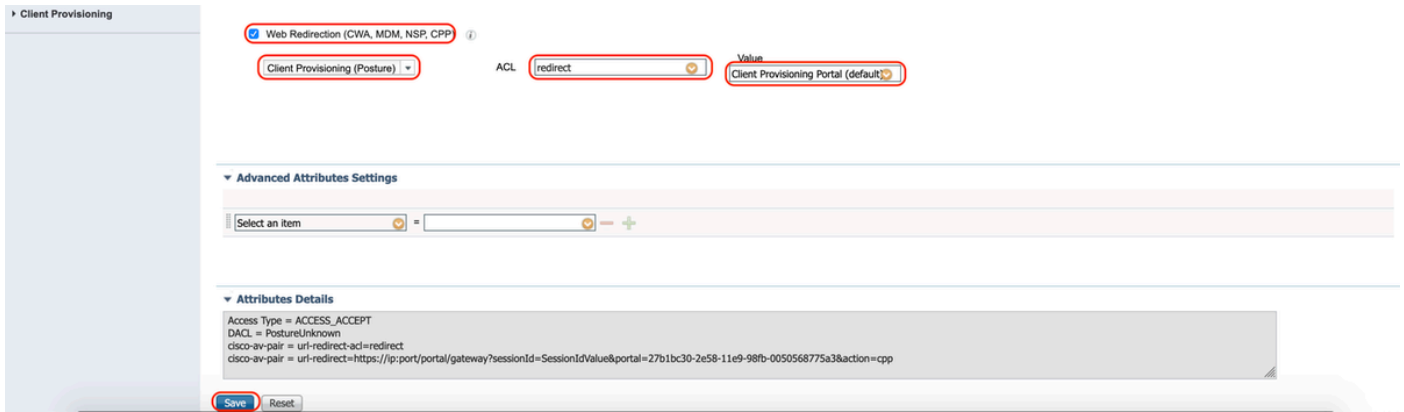
12. Autorisierungsprofile erstellen

Navigieren Sie zu "Richtlinie > Richtlinienelemente > Ergebnisse > Autorisierung > Autorisierungsprofile".

A. Autorisierungsprofil für unbekanntes Status

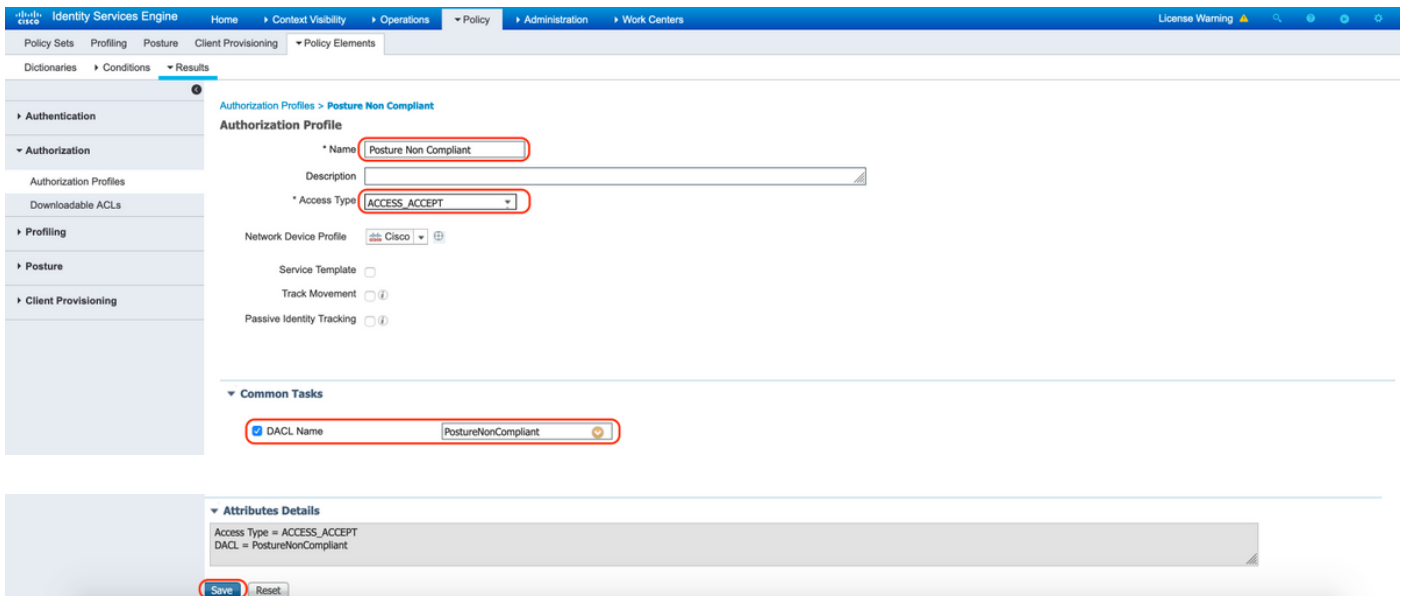
Wählen Sie DACL "PostureUnknown" (Status unbekannt), aktivieren Sie die Option Web Redirection (Webumleitung), wählen Sie Client Provisioning (Status) aus, konfigurieren Sie den Namen der Umleitungs-ACL "redirect" (Umleitung) (auf dem ASA zu konfigurieren), und wählen Sie das Client Provisioning Portal (Standard) aus.





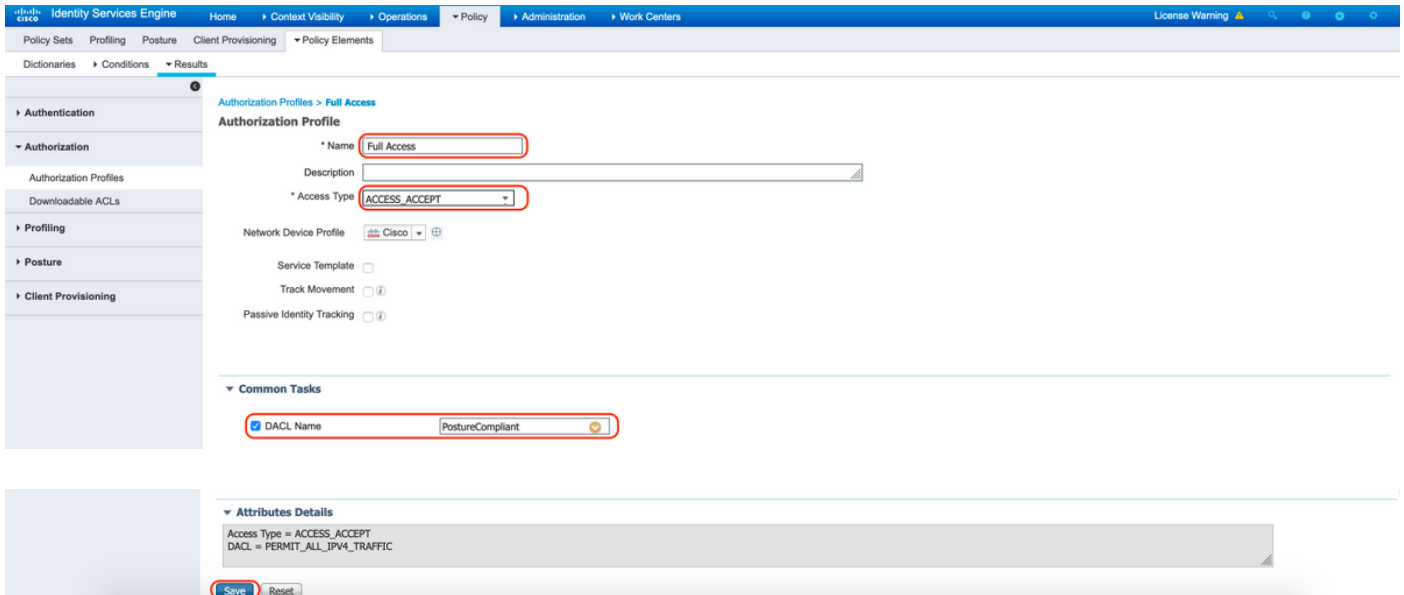
B. Autorisierungsprofil für nicht konforme Haltung

Wählen Sie DACL "PostureNonCompliant" aus, um den Zugriff auf das Netzwerk einzuschränken.



C. Autorisierungsprofil für Posture Compliant

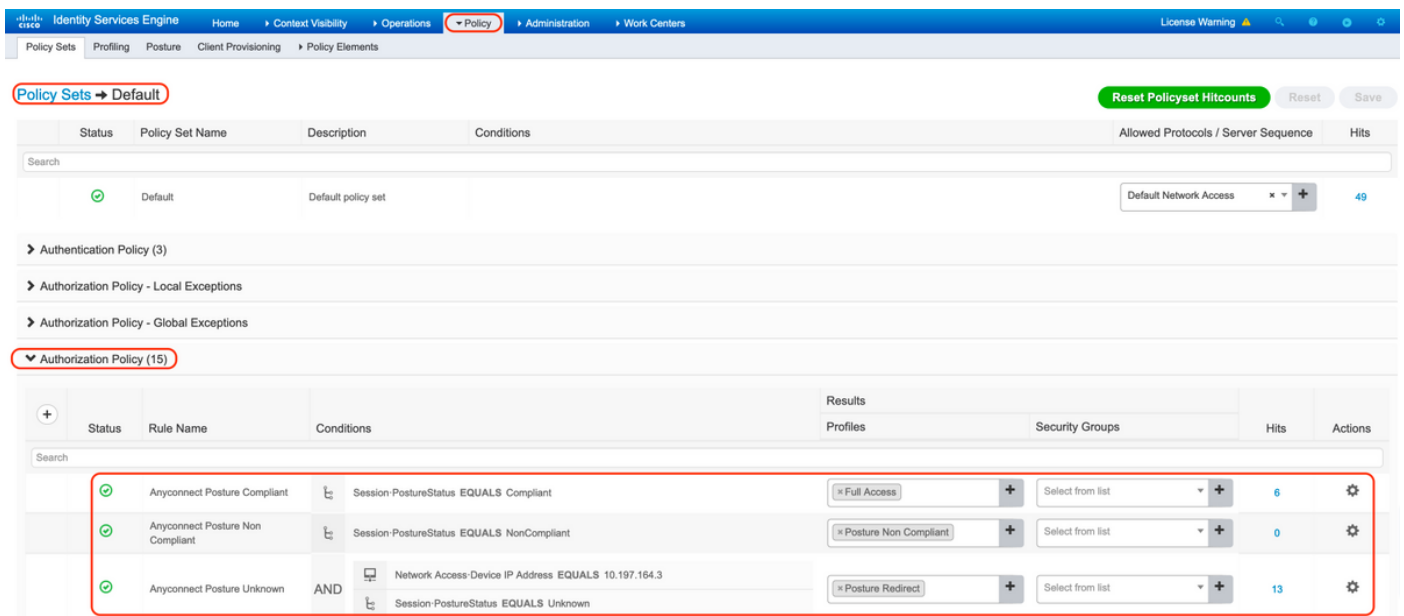
Wählen Sie DACL "PostureCompliant" aus, um vollständigen Zugriff auf das Netzwerk zu ermöglichen.



12. Autorisierungsrichtlinien konfigurieren

Verwenden Sie die im vorherigen Schritt konfigurierten Autorisierungsprofile, um drei Autorisierungsrichtlinien für "Posture Compliant", "Posture Non-Compliant" und "Posture Unknown" zu konfigurieren.

Die allgemeine Bedingung "Session: Posture Status" wird verwendet, um die Ergebnisse der einzelnen Richtlinien zu bestimmen.



Überprüfung

Verwenden Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Führen Sie den folgenden Befehl auf der ASA aus, um zu überprüfen, ob der Benutzer erfolgreich authentifiziert wurde.

```
<#root>
```

```
firebird(config)#
```

```
show vpn-sess detail anyconnect
```

Session Type: AnyConnect Detailed

```
Username      : _585b5291f01484dfd16f394be7031d456d314e3e62
Index         : 125
Assigned IP   : explorer.cisco.com      Public IP    : 10.197.243.143
Protocol      : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License       : AnyConnect Premium
Encryption    : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-256  DTLS-Tunnel: (1)AES-GCM-256
Hashing       : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA384  DTLS-Tunnel: (1)SHA384
Bytes Tx      : 16404                   Bytes Rx    : 381
Pkts Tx       : 16                       Pkts Rx    : 6
Pkts Tx Drop  : 0                         Pkts Rx Drop : 0
Group Policy  : DfltGrpPolicy              Tunnel Group :
```

TG_SAML

```
Login Time    : 07:05:45 UTC Sun Jun 14 2020
Duration      : 0h:00m:16s
Inactivity    : 0h:00m:00s
VLAN Mapping  : N/A                       VLAN        : none
Audt Sess ID  : 0ac5a4030007d0005ee5cc49
Security Grp  : none
```

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

AnyConnect-Parent:

```
Tunnel ID     : 125.1
Public IP     : 10.197.243.143
Encryption    : none                       Hashing      : none
TCP Src Port  : 57244                       TCP Dst Port : 443
Auth Mode     : SAML
Idle Time Out: 30 Minutes                   Idle TO Left : 29 Minutes
Client OS     : win
Client OS Ver : 10.0.15063
Client Type   : AnyConnect
Client Ver    : Cisco AnyConnect VPN Agent for Windows 4.8.03052
Bytes Tx      : 7973                         Bytes Rx    : 0
Pkts Tx       : 6                             Pkts Rx    : 0
Pkts Tx Drop  : 0                             Pkts Rx Drop : 0
```

SSL-Tunnel:

```
Tunnel ID     : 125.2
Assigned IP   : explorer.cisco.com      Public IP    : 10.197.243.143
Encryption    : AES-GCM-256             Hashing      : SHA384
```

Ciphersuite : ECDHE-RSA-AES256-GCM-SHA384
Encapsulation: TLSv1.2 TCP Src Port : 57248
TCP Dst Port : 443 Auth Mode : SAML
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : Windows
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.8.03052
Bytes Tx : 7973 Bytes Rx : 0
Pkts Tx : 6 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Filter Name : #ACSACL#-IP-PostureUnknown-5ee45b05

DTLS-Tunnel:

Tunnel ID : 125.3
Assigned IP : explorer.cisco.com Public IP : 10.197.243.143
Encryption : AES-GCM-256 Hashing : SHA384
Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384
Encapsulation: DTLSv1.2 UDP Src Port : 49175
UDP Dst Port : 443 Auth Mode : SAML
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : Windows
Client Type : DTLS VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.8.03052
Bytes Tx : 458 Bytes Rx : 381
Pkts Tx : 4 Pkts Rx : 6
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Filter Name :

#ACSACL#-IP-PostureUnknown-5ee45b05

ISE Posture:

Redirect URL : https://ise261.pusaxena.local:8443/portal/gateway?sessionId=0ac5a4030007d0005ee5cc49&p
Redirect ACL : redirect

Nach Abschluss der Statusüberprüfung wird der Benutzerzugriff auf den vollständigen Zugriff geändert, wie in der DACL im Feld "Filter Name" (Filtername) gezeigt.

<#root>

firebird(config)#

show vpn-sess detail anyconnect

Session Type: AnyConnect Detailed

Username : _585b5291f01484dfd16f394be7031d456d314e3e62
Index : 125
Assigned IP : explorer.cisco.com Public IP : 10.197.243.143
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-256
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384
Bytes Tx : 16404 Bytes Rx : 381

Pkts Tx : 16 Pkts Rx : 6
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : DfltGrpPolicy Tunnel Group :

TG_SAML

Login Time : 07:05:45 UTC Sun Jun 14 2020
Duration : 0h:00m:36s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : 0ac5a4030007d0005ee5cc49
Security Grp : none

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

AnyConnect-Parent:

Tunnel ID : 125.1
Public IP : 10.197.243.143
Encryption : none Hashing : none
TCP Src Port : 57244 TCP Dst Port : 443
Auth Mode : SAML
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : win
Client OS Ver: 10.0.15063
Client Type : AnyConnect
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.8.03052
Bytes Tx : 7973 Bytes Rx : 0
Pkts Tx : 6 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:

Tunnel ID : 125.2
Assigned IP : explorer.cisco.com Public IP : 10.197.243.143
Encryption : AES-GCM-256 Hashing : SHA384
Ciphersuite : ECDHE-RSA-AES256-GCM-SHA384
Encapsulation: TLSv1.2 TCP Src Port : 57248
TCP Dst Port : 443 Auth Mode : SAML
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : Windows
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.8.03052
Bytes Tx : 7973 Bytes Rx : 0
Pkts Tx : 6 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Filter Name : #ACSACL#-IP-PERMIT_ALL_IPV4_TRAFFIC-57f6b0d3

DTLS-Tunnel:

Tunnel ID : 125.3
Assigned IP : explorer.cisco.com Public IP : 10.197.243.143
Encryption : AES-GCM-256 Hashing : SHA384
Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384
Encapsulation: DTLSv1.2 UDP Src Port : 49175
UDP Dst Port : 443 Auth Mode : SAML
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : Windows
Client Type : DTLS VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.8.03052
Bytes Tx : 458 Bytes Rx : 381
Pkts Tx : 4 Pkts Rx : 6
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Filter Name :

#ACSACL#-IP-PERMIT_ALL_IPV4_TRAFFIC-57f6b0d3

Um zu überprüfen, ob die Autorisierung auf der ISE erfolgreich durchgeführt wurde, navigieren Sie zu "Operations > RADIUS > Live Logs" (Vorgänge > RADIUS > Live-Protokolle).

In diesem Abschnitt werden die relevanten Informationen zum autorisierten Benutzer angezeigt, z. B. Identität, Autorisierungsprofil, Autorisierungsrichtlinie und Status.

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authenticat...	Authorizati...	Authorization Pro...	Posture St...	IP Address	Network Device
Jun 14, 2020 07:44:59.975 AM	●	🔒	0	_585b5291f01484df1...	00:50:56:A0:D6:97	Windows10-...	Default	Anyconnect ...	Full Access	Compliant	10.197.164.7	
Jun 14, 2020 07:44:59.975 AM	✔	🔒		#ACSACL#-IP-PERMI...	10.197.243.143			Anyconnect ...	Full Access	Compliant		ASA
Jun 14, 2020 07:44:59.975 AM	✔	🔒		#ACSACL#-IP-Posture...								ASA
Jun 14, 2020 07:44:34.963 AM	✔	🔒		#ACSACL#-IP-Posture...								ASA
Jun 14, 2020 07:44:34.958 AM	✔	🔒		_585b5291f01484df1...	00:50:56:A0:D6:97	Windows10-...	Default	Default >> A...	Posture Redirect	Pending		ASA



Hinweis: Weitere Informationen zur Statusüberprüfung auf der ISE finden Sie in der folgenden Dokumentation:

<https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/215236-ise-posture-over-anyconnect-remote-access.html#anc7>

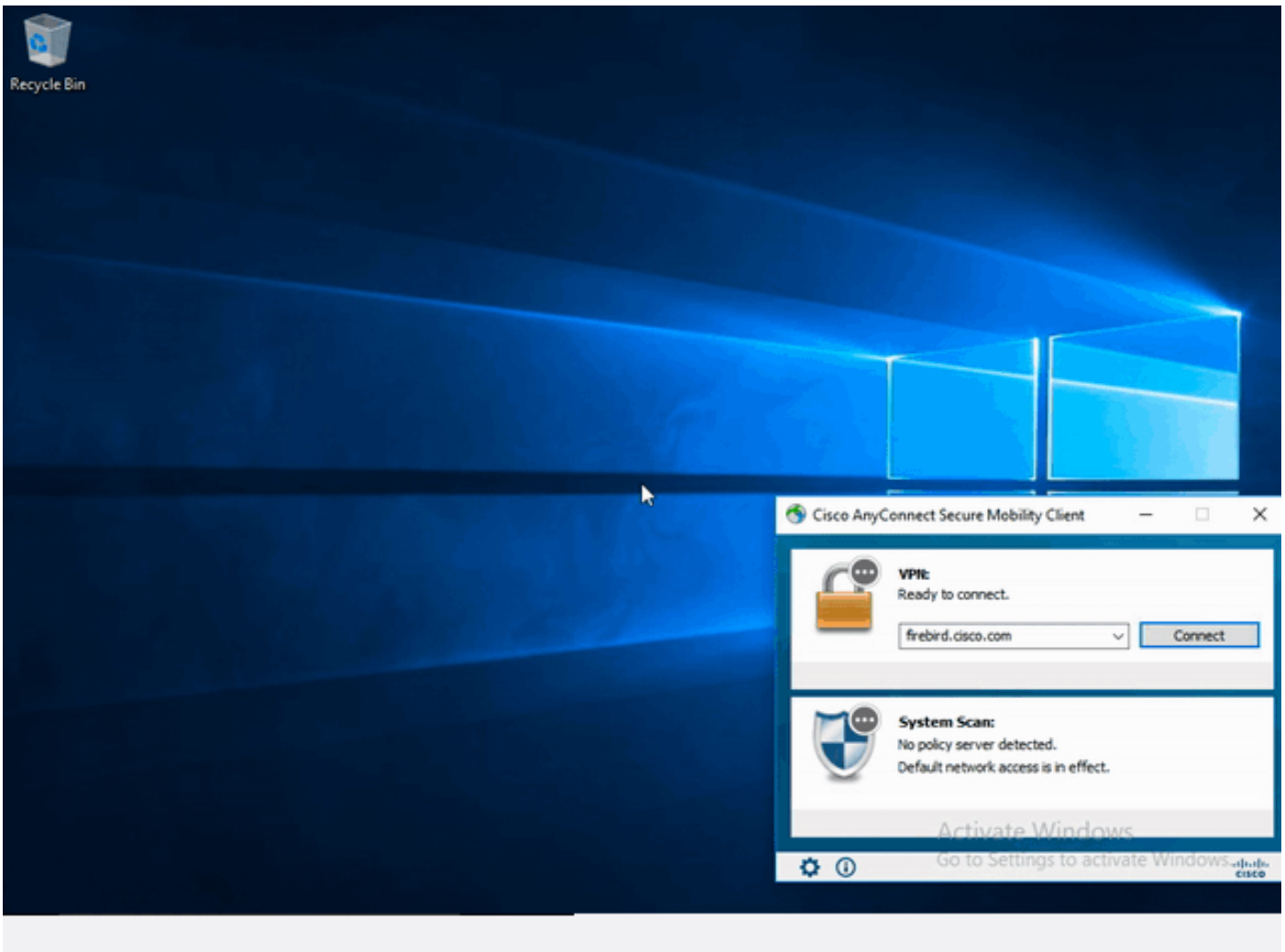
Um den Authentifizierungsstatus auf dem Duo Admin Portal zu überprüfen, klicken Sie auf "Reports" auf der linken Seite des Admin Panels, das das Authentifizierungsprotokoll anzeigt.

Weitere Informationen: <https://duo.com/docs/administration#reports>

Um die Debug-Protokollierung für Duo Access Gateway anzuzeigen, verwenden Sie den folgenden Link:


https://help.duo.com/s/article/1623?language=en_US


Benutzerfreundlichkeit



Fehlerbehebung

In diesem Abschnitt erhalten Sie Informationen zur Behebung von Fehlern in Ihrer Konfiguration.

 Hinweis: Lesen Sie den Artikel [Important Information on Debug Commands](#) (Wichtige Informationen zu Debug-Befehlen), bevor Sie debug-Befehle verwenden.

 Vorsicht: Auf der ASA können Sie verschiedene Debug-Ebenen festlegen. Standardmäßig wird Ebene 1 verwendet. Wenn Sie die Debug-Ebene ändern, kann die Ausführlichkeit der Debugs zunehmen. Gehen Sie dabei besonders in Produktionsumgebungen vorsichtig vor.

Bei den meisten SAML-Fehlerbehebungen kommt es zu Fehlkonfigurationen, die durch Überprüfen der SAML-Konfiguration oder durch Ausführen von Debugs ermittelt werden können.

"debug webvpn saml 255" kann verwendet werden, um die meisten Probleme zu beheben. In Szenarien, in denen dieses Debuggen keine nützlichen Informationen liefert, können jedoch zusätzliche Debugs ausgeführt werden:

```
debug webvpn 255
debug webvpn anyconnect 255
debug webvpn session 255
debug webvpn request 255
```

Verwenden Sie zur Behebung von Authentifizierungs- und Autorisierungsproblemen auf ASA die folgenden Debug-Befehle:

```
debug radius all
debug aaa authentication
debug aaa authorization To troubleshoot Posture related issues on ISE, set the following attributes to
```

```
posture (ise-psc.log)
portal (guest.log)
provisioning (ise-psc.log)
runtime-AAA (prrt-server.log)
nsf (ise-psc.log)
nsf-session (ise-psc.log)
swiss (ise-psc.log)
```



Hinweis: Detaillierte Informationen zum Statusverlauf und zur Fehlerbehebung bei AnyConnect und ISE finden Sie unter dem folgenden Link:

[ISE Posture Style Comparison for Pre and Post 2.2](#)

So interpretieren Sie Duo Access Gateway-Debug-Protokolle und beheben Fehler

https://help.duo.com/s/article/5016?language=en_US

Zugehörige Informationen

<https://www.youtube.com/watch?v=W6bE2GTU0Is&>

<https://duo.com/docs/cisco#asa-ssl-vpn-using-saml>

<https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/215236-ise-posture-over-anyconnect-remote-access.html#anc0>

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.