

Konfigurieren von sicherem Zugriff für RA-VPNaaS mit Duo SSO und Statusüberprüfung mit der ISE

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Netzwerkdiagramm](#)

[Konfigurieren](#)

[Duo Konfiguration](#)

[Konfiguration des sicheren Zugriffs](#)

[Konfigurieren der Radius-Gruppe auf den IP-Pools](#)

[Konfigurieren Ihres VPN-Profiles für die Verwendung von ISE](#)

[Allgemeine Einstellungen](#)

[Authentisierung, Ermächtigung und Buchhaltung](#)

[Verkehrssteuerung](#)

[Cisco Secure Client-Konfiguration](#)

[ISE-Konfigurationen](#)

[Konfiguration der Liste der Netzwerkgeräte](#)

[Konfigurieren einer Gruppe](#)

[Lokalen Benutzer konfigurieren](#)

[Policy Set konfigurieren](#)

[Autorisierung für Policy Set konfigurieren](#)

[Konfigurieren von lokalen Radius- oder Active Directory-Benutzern](#)

[Konfigurieren des ISE-Status](#)

[Statusbedingungen konfigurieren](#)

[Statusanforderungen konfigurieren](#)

[Statusrichtlinie konfigurieren](#)

[Konfiguration der Client-Bereitstellung](#)

[Client-Bereitstellungsrichtlinie konfigurieren](#)

[Erstellen der Autorisierungsprofile](#)

[Festlegen von Statusrichtlinien](#)

[Überprüfung](#)

[Statusüberprüfung](#)

[Verbindung am Rechner](#)

[So überprüfen Sie die Protokolle in der ISE](#)

[Einhaltung](#)

[Nichteinhaltung](#)

[Erste Schritte mit sicherem Zugriff und ISE-Integration](#)

[Fehlerbehebung](#)

[Herunterladen von ISE Posture Debug-Protokollen](#)

[So überprüfen Sie Protokolle für den sicheren Zugriff auf Remote-Zugriff](#)

[DART-Paket auf sicherem Client generieren](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird die Konfiguration der Statusüberprüfung für Remote-Access-VPN-Benutzer mit Identity Service Engine (ISE) und Secure Access mit Duo beschrieben.

Voraussetzungen

- [Konfiguration der Benutzerbereitstellung](#) bei sicherem Zugriff
- Duo [SSO](#) mit Authentifizierungsproxy oder Drittanbieter-IDP konfigurieren
- Verbindung der Cisco ISE mit Secure Access über den Tunnel

Anforderungen

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

- [Identity Service Engine](#)
- [Sicherer Zugriff](#)
- [Cisco Secure Client](#)
- [Guide to Two-Factor Authentication - Duo Security](#)
- ISE-Status
- Authentisierung, Ermächtigung und Buchhaltung

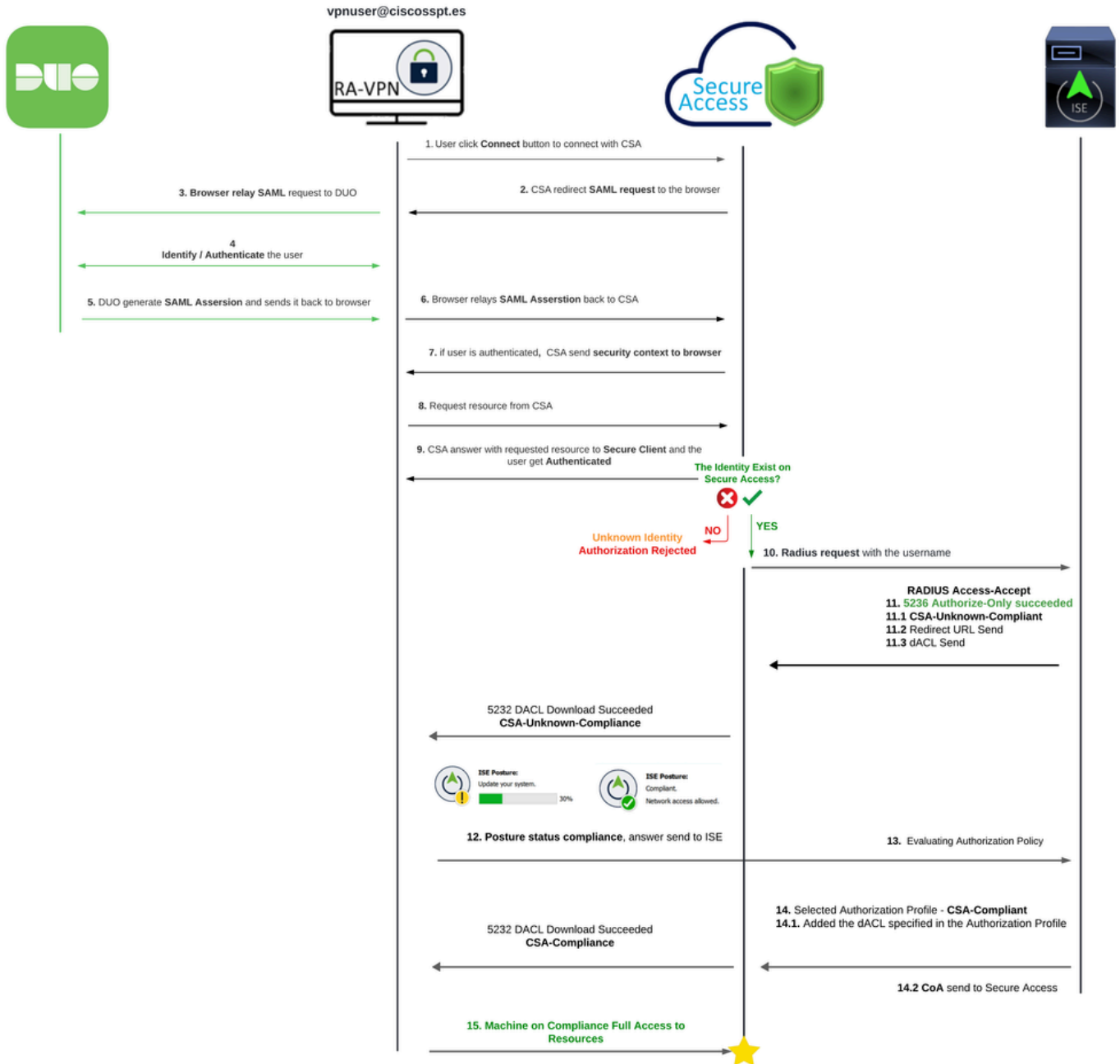
Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf:

- Identity Service Engine (ISE) Version 3.3 Patch 1
- Sicherer Zugriff
- Cisco Secure Client - AnyConnect VPN Version 5.1.2.42

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.

Hintergrundinformationen



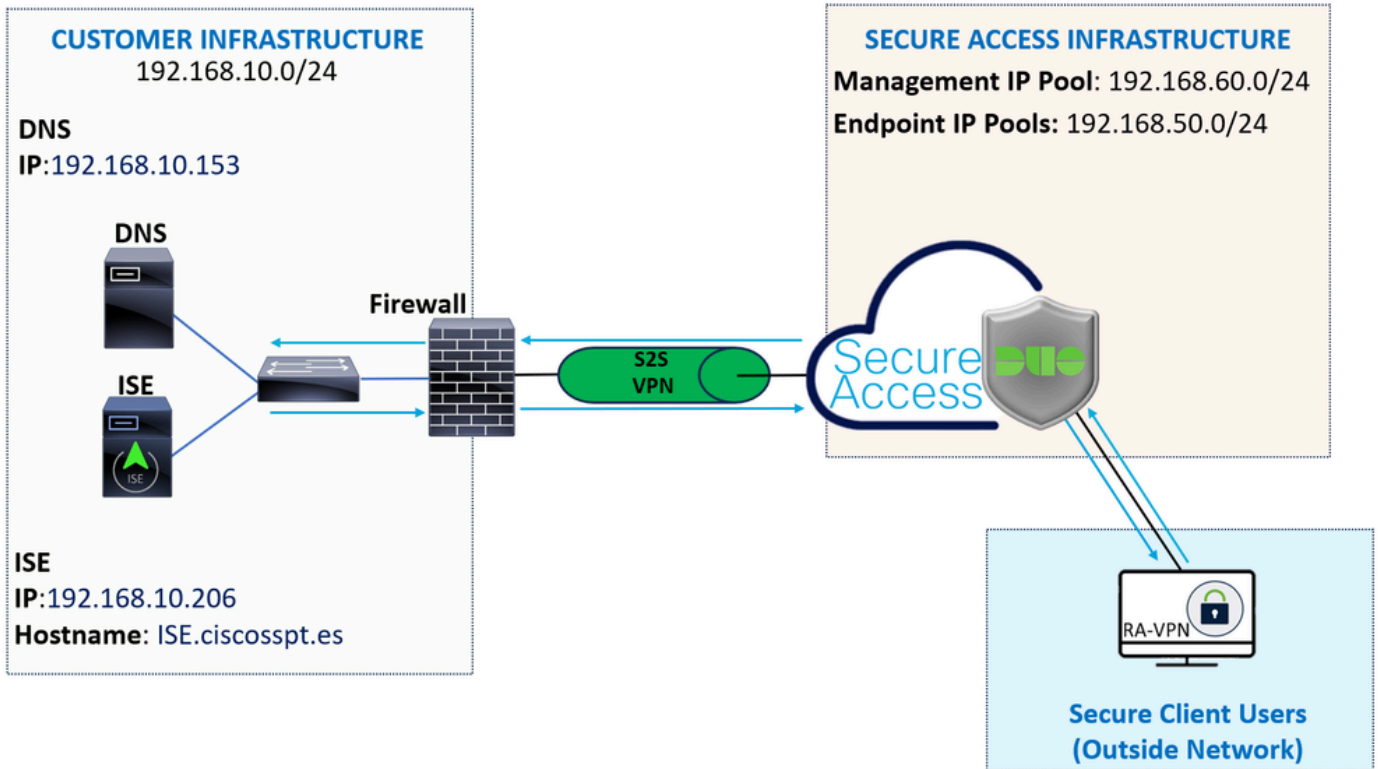
Die Integration von Duo SAML mit der Cisco Identity Services Engine (ISE) verbessert den Authentifizierungsprozess und erweitert die Cisco Secure Access-Lösungen um eine weitere Sicherheitsebene. Duo SAML bietet eine Single Sign-On (SSO)-Funktion, die den Benutzeranmeldeprozess vereinfacht und gleichzeitig hohe Sicherheitsstandards gewährleistet.

Nach der Authentifizierung über Duo SAML wird der Autorisierungsprozess von der Cisco ISE durchgeführt. Dies ermöglicht dynamische Entscheidungen bei der Zugriffskontrolle, die auf der Benutzeridentität und dem Gerätestatus basieren. Die ISE kann detaillierte Richtlinien durchsetzen, die festlegen, auf welche Ressourcen ein Benutzer zugreifen kann, wann und von welchen Geräten.



Hinweis: Um die RADIUS-Integration zu konfigurieren, müssen Sie sicherstellen, dass die Kommunikation zwischen beiden Plattformen stattfindet.

Netzwerkdiagramm



Konfigurieren



Hinweis: Bevor Sie mit der Konfiguration beginnen, müssen Sie die [ersten Schritte mit Secure Access und ISE-Integration](#) durchführen.

Duo Konfiguration

Um die RA-VPN-Anwendung zu konfigurieren, gehen Sie wie folgt vor:

Navigieren Sie zu Ihrem [Duo Admin-Bereich](#).

- Navigieren Sie zu **Applications > Protect an Application**
 - Suchen nach **Generic SAML Service Provider**
 - Klicken Sie auf **Protect**

Protect an Application

Generic SAML Service Provider

Application

Protection Type



Generic SAML Service Provider

2FA with SSO hosted by Duo
(Single Sign-On)

[Documentation](#)

Protect

Die Anwendung muss auf dem Bildschirm angezeigt werden. Merken Sie sich den Anwendungsnamen für die VPN-Konfiguration.

✓ Successfully added Generic SAML Service Provider - Single Sign-On to protected applications.
[Add another.](#)

Dashboard > Applications > Generic SAML Service Provider - Single Sign-On

Generic SAML Service Provider - Single Sign-On

[Authentication Log](#) | [Remove Application](#)

See the [Generic SSO documentation](#) to integrate Duo into your SAML-enabled service provider.

Metadata

Entity ID	<code>https://sso-5ed0a388.sso.duosecurity.com/saml2/sp/DI9818G01ZNNK5L9LR7Z/metadata</code>	Copy
Single Sign-On URL	<code>https://sso-5ed0a388.sso.duosecurity.com/saml2/sp/DI9818G01ZNNK5L9LR7Z/sso</code>	Copy
Single Log-Out URL	<code>https://sso-5ed0a388.sso.duosecurity.com/saml2/sp/DI9818G01ZNNK5L9LR7Z/slo</code>	Copy
Metadata URL	<code>https://sso-5ed0a388.sso.duosecurity.com/saml2/sp/DI9818G01ZNNK5L9LR7Z/metadata</code>	Copy

Certificate Fingerprints

SHA-1 Fingerprint	<code>05:76:95:6B:E1:7C:F7:D1:79:12:2C:23:B6:1A:63:59:32:01:88:B1</code>	Copy
SHA-256 Fingerprint	<code>CF:CB:25:7C:41:0D:81:49:E5:83:48:79:EA:6B:45:C9:9F:4A:9A:21:A9:72:32:D3:C1:7F:86:4</code>	Copy

In diesem Fall ist **Generic SAML Service Provider**.

Konfiguration des sicheren Zugriffs

Konfigurieren der Radius-Gruppe auf den IP-Pools

Um das VPN-Profil mit Radius zu konfigurieren, gehen Sie wie folgt vor:

Navigieren Sie zu Ihrem [Dashboard für sicheren Zugriff](#).



- Klicken Sie **Connect > Enduser Connectivity > Virtual Private Network**
- Klicken Sie unter der Pool-Konfiguration (**Manage IP Pools**) auf **Manage**

Manage IP Pools

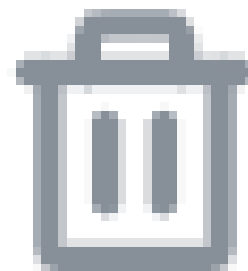
Manage

2 Regions mapped

- Wählen Sie den **IP Pool Region** und konfigurieren Sie den **Radius Server**

Pop Name	Display Name	Endpoint IP Pools	Management IP Pools	DNS Servers	RADIUS Groups
Europe (Germany)	RA VPN 1	192.168.50.0/24 256 user connections	192.168.60.0/24 256 user connections	House	 

- Zum Bearbeiten auf den Bleistift klicken



- Wählen Sie nun im Dropdown-Menü "Konfiguration" des Abschnitts "IP-Pool" unter **Radius Group (Optional)**
- Klicken Sie auf Add RADIUS Group

RADIUS Groups (optional)

Associate one RADIUS group per AAA method to this IP pool.



No RADIUS groups created

[Add RADIUS Group](#)

← Edit RADIUS Group



Add group of RADIUS servers, which will be used to control access to your VPN profiles

Change of authorization (CoA) mode ⓘ

CoA Port: 1700

Accounting

Port

1813

Accounting mode

Single

Simultaneous

Accounting update

Interim accounting update

Update interval

1

hour(s)

Settings

RADIUS Servers

You can add up to 8 servers in each group

Assign servers

ISE_CSA ×

+ Add

#	Server Name	IP Address	
1	ISE_CSA	192.168.10.206	

Group Name: Konfigurieren Sie einen Namen für Ihre ISE-Integration in Secure Access.

- **AAA method**

- **Authentication:** Aktivieren Sie das Kontrollkästchen für, **Authentication** und wählen Sie den Port als Standard 1812 aus.

- Falls Ihre Authentifizierung das Aktivieren des Kontrollkästchens erfordert Microsoft Challenge Handshake Authentication Protocol Version 2 (MCHAPv2)

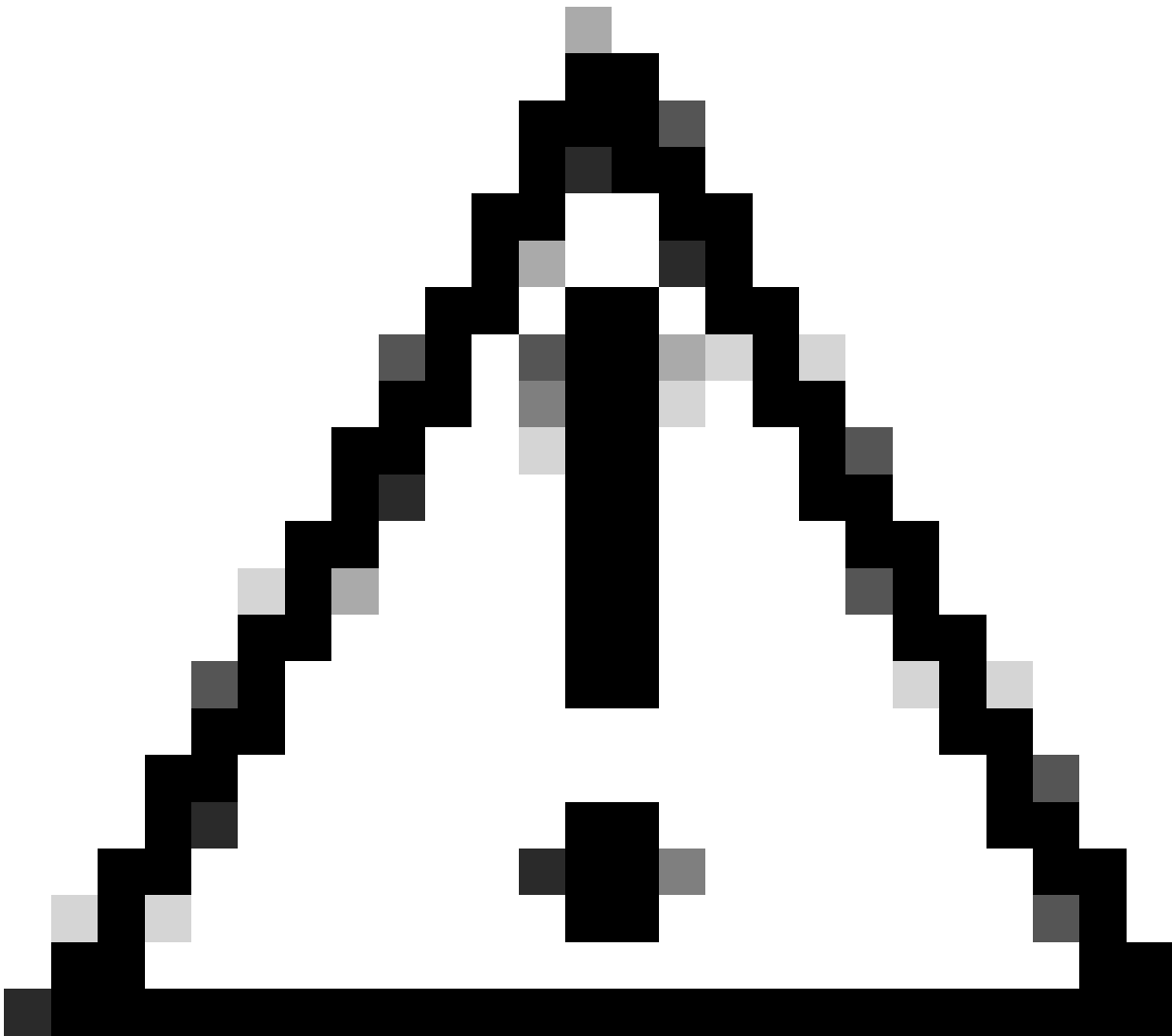
- **Authorization:** Markieren Sie das Kontrollkästchen für Authorization, und wählen Sie den Port als Standardport 1812 aus.

- Aktivieren Sie das Kontrollkästchen, **Authorization mode Only Change of Authorization (CoA) mode** um den Status und Änderungen von der ISE zuzulassen.

- **Accounting:** Aktivieren Sie das Kontrollkästchen für die Autorisierung, und wählen Sie den Port als Standard 1813 aus.

- Wählen Sie **Single or Simultaneous** (Im Einzel-Modus werden Buchhaltungsdaten nur an einen Server gesendet. Im Simultanmodus werden Accounting-Daten an alle Server in der Gruppe übertragen.)

- Aktivieren Sie das Kontrollkästchen für, **Accounting update** um die regelmäßige Generierung von RADIUS-Nachrichten für die Zwischenabrechnung und Aktualisierung zu aktivieren.



Achtung: Sowohl die Authentication als auch die **Authorization** Methoden müssen, wenn sie ausgewählt sind, denselben Port verwenden.

-
- Danach müssen Sie die (**RADIUS Servers ISE**) konfigurieren, die für die Authentifizierung über AAA verwendet wird. Siehe Abschnitt **RADIUS Servers**:
 - Klicken Sie + Add

RADIUS Servers

You can add up to 8 servers in each group

Assign servers

+ Add

#	Server Name	IP Address
---	-------------	------------

- Konfigurieren Sie dann die nächsten Optionen:

Add RADIUS Server

Server name

IP Address

Password type

Secret Key

 [Show](#)

Password

 [Show](#)

Cancel

Save & Add server

Save

- **Server Name:** Konfigurieren Sie einen Namen, um Ihren ISE-Server zu identifizieren.
 - **IP Address:** Konfigurieren Sie die IP-Adresse Ihres Cisco ISE-Geräts, die über sicheren Zugriff erreichbar ist.
 - **Secret Key:** Konfigurieren des geheimen RADIUS-Schlüssels
 - **Password:** Konfigurieren Sie Ihr Radius-Kennwort
-
- Klicken Sie unter der Assign Server Option auf Radius Server, weisen Sie Ihren Radius Server zu **Save** und wählen Sie Ihren ISE Server aus:

RADIUS Servers

You can add up to 8 servers in each group

Assign servers

^

ISE_CSA

[+ Add](#)

- Klicken Sie **Save** erneut, um die gesamte Konfiguration zu speichern.

← Edit RADIUS Group



Add group of RADIUS servers, which will be used to control access to your VPN profiles

Change of authorization (CoA) mode ⓘ

CoA Port: 1700

Accounting

Port

1813

Accounting mode

Single

Simultaneous

Accounting update

Interim accounting update

Update interval

1

hour(s)

Settings



RADIUS Servers

You can add up to 8 servers in each group

Assign servers

ISE_CSA ×



+ Add

#	Server Name	IP Address		
1	ISE_CSA	192.168.10.206		

- **Protocols: Auswahl SAML**

- Klicken Sie auf **Download Service Provider XML file**
- Ersetzen Sie die Informationen in der Anwendung, die im Schritt "[Duo Configuration](#)" konfiguriert wurde.

Service Provider

Metadata Discovery: None (manual input)

Entity ID: `https://vpn.sse.cisco.com/saml/sp/metadata/ISE_CSA_SAML`

Assertion Consumer Service (ACS) URL: `http://vpn.sse.cisco.com/+CSCOE+/saml/sp/acs?tgname=ISE_CSA_SAML`

Single Logout URL: `https://vpn.sse.cisco.com/+CSCOE+/saml/sp/logout`

- Nachdem Sie diese Informationen konfiguriert haben, ändern Sie den Namen des Duo in einen Namen, der mit der von Ihnen vorgenommenen Integration zusammenhängt

Settings

Type: Generic SAML Service Provider - Single Sign-On

Name: ISE - SAML

Duo Push users will see this when approving transactions.

- Klicken Sie **Save** auf Ihre Anwendung auf Duo.
- Sobald Sie auf Speichern klicken, müssen Sie die **SAML Metadata** durch Klicken auf die Schaltfläche **Download XML**

ISE - SAML

See the [Generic SSO documentation](#) to integrate Duo into your SAML-enabled service provider.

Metadata

Entity ID	<code>https://sso-5ed0a388.sso.duosecurity.com/saml2/sp/DIGN1FGK2GW6MVKFB45F/metadata</code>	Copy
Single Sign-On URL	<code>https://sso-5ed0a388.sso.duosecurity.com/saml2/sp/DIGN1FGK2GW6MVKFB45F/sso</code>	Copy
Single Log-Out URL	<code>https://sso-5ed0a388.sso.duosecurity.com/saml2/sp/DIGN1FGK2GW6MVKFB45F/slo</code>	Copy
Metadata URL	<code>https://sso-5ed0a388.sso.duosecurity.com/saml2/sp/DIGN1FGK2GW6MVKFB45F/metadata</code>	Copy

Certificate Fingerprints

SHA-1 Fingerprint	<code>53:0E:25:4F:29:3A:B5:DF:09:A2:0D:BB:08:C7:F6:E8:D9:DB:DE:6B</code>	Copy
SHA-256 Fingerprint	<code>C5:6F:35:44:F8:FC:74:C6:E6:2B:C1:8F:92:9C:E2:80:91:B1:61:C9:75:0B:F9:C5:4B:81:B8:F</code>	Copy

Downloads

Certificate	Download certificate	Copy certificate	Expires: 01-19-2038
SAML Metadata	Download XML		

- Laden Sie das **SAML Metadata** über Sicherer Zugriff unter der Option hoch **3. Upload IdP security metadata XML file** und klicken Sie auf **Next**

VPN Profile name


ISE_CSA_SAML

- ✓ **General settings**
Default Domain: ciscosspt.es | DNS Server: House (192.168.10.153) | Protocol: TLS / DTLS, IPsec (IKEv2)
- 2 Authentication, Authorization, and Accounting**
SAML
- ✓ **Traffic Steering (Split Tunnel)**
Connect to Secure Access | 1 Exceptions
- ✓ **Cisco Secure Client Configuration**


Authenticate with CA certificates
Select to use CA certificates to authenticate this VPN profile.


SAML Configuration

SAML Metadata XML Configuration

 **1. Download Service Provider XML file**
This XML file contains metadata required to configure your IdP.

[Download service provider XML file](#)

 **2. Generate IdP Security Metadata XML File**
a. Upload the Service Provider XML file to your IdP.
b. From your IdP, create and download an IdP Security Metadata XML file.

 **3. Upload IdP security metadata XML file**

✓ File 'ISE - SAML - IDP Metadata.xml' uploaded. [Replace](#) [Delete](#)

Manual Configuration



Cancel

Back

Next

Setzen Sie die Autorisierung fort.



Hinweis: Nachdem Sie die Authentifizierung mit SAML konfiguriert haben, autorisieren Sie sie über die ISE. Das bedeutet, dass das von Secure Access gesendete RADIUS-Paket nur den Benutzernamen enthält. Das Kennwortfeld ist hier nicht vorhanden.

Autorisierung

- ✓ **General settings**
Default Domain: ciscospt.es | DNS Server: House (192.168.10.153) | Protocol: TLS / DTLS, IKEv2
- 2 Authentication, Authorization, and Accounting**
RADIUS
- ✓ **Traffic Steering (Split Tunnel)**
Connect to Secure Access | 2 Exceptions
- ✓ **Cisco Secure Client Configuration**

Authentication, Authorization, and Accounting

Choose a configuration method to complete the SAML authentication process for this VPN profile. [Help](#)

Authentication **Authorization** Accounting

Enable Radius Authorization

Use defaults or customize groups to map to regions

Select one group for all regions

+ Group

ISE_CSA

Region	Management IP pools	Groups
RA VPN 2	192.168.80.0/24	ISE_CSA
RA VPN 1	192.168.60.0/24	ISE_CSA (default)



Cancel

Back

Next

- **Authorization**

- **Enable Radius Authorization:** Aktivieren Sie das Kontrollkästchen, um die Radius-Autorisierung zu aktivieren.

- **Wählen Sie eine Gruppe für alle Regionen aus:** Aktivieren Sie das Kontrollkästchen, um einen spezifischen Radius-Server für alle Remote Access Virtual Private Network (RA-VPN)-Pools zu verwenden, oder definieren Sie ihn separat für jeden Pool.

- Klicken Sie auf **Next**

Nachdem Sie alle **Authorization** Teile konfiguriert haben, fahren Sie bitte mit dem **Accounting** fort.



Hinweis: Wenn Sie diese Option nicht aktivieren, **Radio Authorization** kann die Statusüberprüfung nicht ausgeführt werden.

Buchhaltung

- ✓ **General settings**
Default Domain: ciscospt.es | DNS Server: House (192.168.10.153) | Protocol: TLS / DTLS, IKEv2
- 2 Authentication, Authorization, and Accounting**
RADIUS
- ✓ **Traffic Steering (Split Tunnel)**
Connect to Secure Access | 2 Exceptions
- ✓ **Cisco Secure Client Configuration**

Authentication, Authorization, and Accounting

Choose a configuration method to complete the SAML authentication process for this VPN profile. [Help](#)

Authentication Authorization Accounting

Enable Radius Accounting
Use defaults or customize groups to map to regions

Select one group for all regions + Group

ISE_CSA v

Region	Management IP pools	Groups
RA VPN 2	192.168.80.0/24	ISE_CSA v
RA VPN 1	192.168.60.0/24	ISE_CSA (default) v



Cancel

Back

Next

- **Accounting**
 - **Map Authorization groups to regions:** Wählen Sie die Regionen und wählen Sie Ihre **Radius Groups**

- Klicken Sie auf **Next**

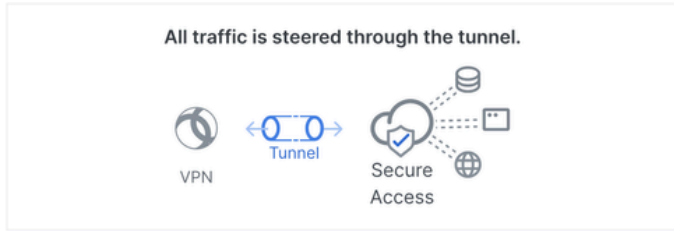
After you have done configured the Authentication, Authorization and Accounting fahren Sie bitte fort mit Traffic Steering.

Verkehrssteuerung

Unter "Traffic Steering" (Steuerung des Datenverkehrs) müssen Sie den Kommunikationstyp über Secure Access konfigurieren.

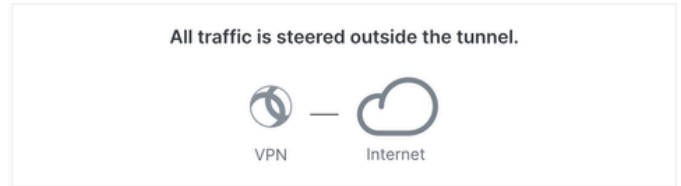
Tunnel Mode

Connect to Secure Access



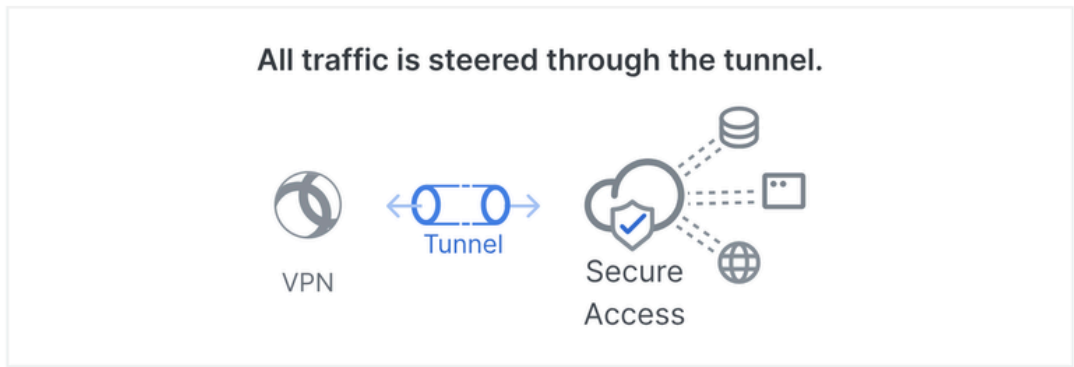
Tunnel Mode

Bypass Secure Access



- Wenn Sie möchten, **Connect to Secure Access** werden alle Internet-Datenverkehrsrouten **Secure Access**

Connect to Secure Access



Add Exceptions

Destinations specified here will be steered **OUTSIDE** the tunnel.

+ Add

Destinations	Exclude Destinations	Actions
proxy-8195126.zpc.sse.cisco.com, ztna.sse.cisco.com, acme.sse.cisco.com, devices.api.umbrella.com, sseposture-routing-commercial.k8s.5c10.org, sseposture-routing-commercial.posture.duosecurity.com, data.eb.thousandeyes.	-	-

Cancel

Back

Next

Wenn Sie Ausschlüsse für Internet-Domains oder IP-Adressen hinzufügen möchten, klicken Sie auf die + **Add** Schaltfläche und dann auf **Next**.

- Wenn Sie sich entscheiden, **Bypass Secure Access** wird der gesamte Internet-Datenverkehr über Ihren Internet-Provider geleitet, nicht über Secure Access (kein Internet-Schutz)

Tunnel Mode

Bypass Secure Access ▼

All traffic is steered outside the tunnel.



Add Exceptions

Destinations specified here will be steered **INSIDE** the tunnel.

[+ Add](#)

Destinations

Exclude Destinations

Actions



No matches found

[Cancel](#)

[Back](#)

[Next](#)



Hinweis: Fügen Sie **enroll.cisco.com** den ISE-Status hinzu, wenn Sie **Bypass Secure Access** auswählen.

In diesem Schritt wählen Sie alle privaten Netzwerkressourcen aus, auf die Sie über das VPN zugreifen möchten. Klicken Sie dazu auf + **Add**, und klicken Sie dann auf, **Next** wenn Sie alle Ressourcen hinzugefügt haben.

Cisco Secure Client-Konfiguration

Cisco Secure Client Configuration

Select various settings to configure how Cisco Secure Client operates. [Help](#)

Session Settings **3** Client Settings **13** Client Certificate Settings **2** [Download XML](#)

Banner Message
Require user to accept a banner message post authentication

Session Timeout
 days

Session Timeout Alert
 minutes before

Maximum Transmission Unit ⓘ

[Cancel](#) [Back](#) [Save](#)

In diesem Schritt können Sie alles als Standard verwalten und auf klicken, **Save** aber wenn Sie Ihre Konfiguration weiter anpassen möchten, lesen Sie bitte das [Cisco Secure Client Administratorhandbuch](#).

Name	General	Authentication, Authorization & Accounting	Traffic Steering	Secure Client Configuration	Profile URL
ISE_CSA_SAML	ciscosspt.es TLS, IPSec (IKEv2)	SAML RADIUS	Connect to Secure Access 1 Exception(s)	13 Settings	vpn.sse.cisco.com/ISE_CSA_SAML

ISE-Konfigurationen

Konfiguration der Liste der Netzwerkgeräte


Um die Authentifizierung über die Cisco ISE zu konfigurieren, müssen Sie die zulässigen Geräte konfigurieren, die Abfragen an die Cisco ISE senden können:

- Navigieren Sie zu **Administration > Network Devices**
- Klicken Sie + **Add**

Network Devices

Name CSA

Description _____

IP Address * IP : 192.168.60.0 / 24 


Device Profile  Cisco 

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol **RADIUS**

Shared Secret [Show](#)

Use Second Shared Secret 

Second Shared Secret _____ [Show](#)

CoA Port 1700 [Set To Default](#)

- **Name:** Verwenden Sie einen Namen zur Identifizierung von sicherem Zugriff.
- **IP Address:** Konfigurieren Sie die Management Interface des Schritts "[IP Pool Region](#)".
- **Device Profile** Cisco Produkte auswählen
 - **Radius Authentication Settings**
 - **Shared Secret:** Konfigurieren Sie den gleichen geheimen Schlüssel, der für den Schritt konfiguriert wurde, [Secret Key \(Geheim Schlüssel\)](#).
 - **CoA Port:** Voreinstellung; 1700 wird auch für sicheren Zugriff verwendet

Nach diesem Klick **Save**, um zu überprüfen, ob die Integration ordnungsgemäß funktioniert, fahren Sie mit der Erstellung eines lokalen Benutzers für die Integrationsverifizierung fort.

Konfigurieren einer Gruppe

Gehen Sie wie folgt vor, um eine Gruppe zur Verwendung mit lokalen Benutzern zu konfigurieren:

- Klicken Sie in **Administration > Groups**
- Klicken Sie auf **User Identity Groups**
- Klicken Sie auf + Add
- Erstellen Sie einen Namen für die Gruppe, und klicken Sie auf **Submit**

The screenshot displays the 'Identity Groups' management interface. On the left, the 'Administration' menu is open, with 'Groups' highlighted under 'Identities'. The main area shows the 'User Identity Groups' page with a 'New User Identity Group' form. The form includes a 'Name' field containing 'CSA-ISE' and a 'Description' field. Below the form is a 'Submit' button. To the right, a list of existing groups is shown, including 'ALL_ACCOUNTS (default)', 'CSA-ISE' (marked as 'GROUP CREATED'), and 'Employee'. Red numbers 1 through 6 are overlaid on the image to indicate the steps: 1. User icon, 2. Groups menu item, 3. User Identity Groups folder, 4. Add button, 5. Name field, 6. Submit button.

Lokalen Benutzer konfigurieren

So konfigurieren Sie einen lokalen Benutzer, um Ihre Integration zu überprüfen:

- Navigieren Sie zu **Administration > Identities**
- Klicken Sie **Add +**

Network Access User

* Username

Status Enabled ▼

Account Name Alias ⓘ

Email

Passwords

Password Type: ▼

Password Lifetime:

With Expiration ⓘ

Never Expires ⓘ

* Login ⓘ

Enable ⓘ

User Groups

⋮ ▼

- **Username:** Konfigurieren Sie den Benutzernamen mit einer bekannten UPN-Bereitstellung in Secure Access; dies basiert auf dem Schritt [Voraussetzungen](#)
- **Status:** Aktiv
- **Password Lifetime:** Sie können es konfigurieren **With Expiration** oder Never Expires, je nach
- **Login Password:** Passwort für den Benutzer erstellen
- **User Groups:** Wählen Sie die Gruppe erstellt auf dem Schritt, [Konfigurieren Sie eine Gruppe](#)



Hinweis: Die auf UPN basierende Authentifizierung wird in den kommenden Versionen von Secure Access geändert.

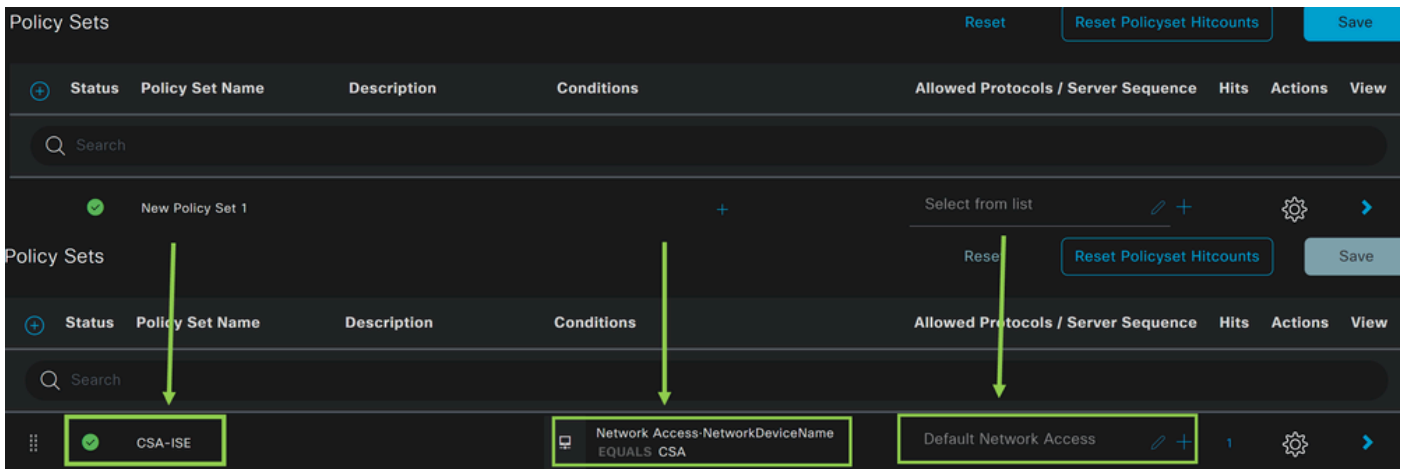
Anschließend können Sie **Save** die Konfiguration vornehmen und mit dem Schritt fortfahren **Configure Policy Set**.

Policy Set konfigurieren

Konfigurieren Sie unter dem Richtlinienatz die Aktion, die die ISE während der Authentifizierung und Autorisierung ausführt. Dieses Szenario veranschaulicht den Anwendungsfall für die Konfiguration einer einfachen Richtlinie, die den Benutzerzugriff ermöglicht. Zunächst überprüft die ISE den Ursprung der RADIUS-Authentifizierungen und überprüft, ob die Identitäten in der ISE-Benutzerdatenbank vorhanden sind, um den Zugriff zu ermöglichen.

Um diese Richtlinie zu konfigurieren, navigieren Sie zu Ihrem Cisco ISE Dashboard:

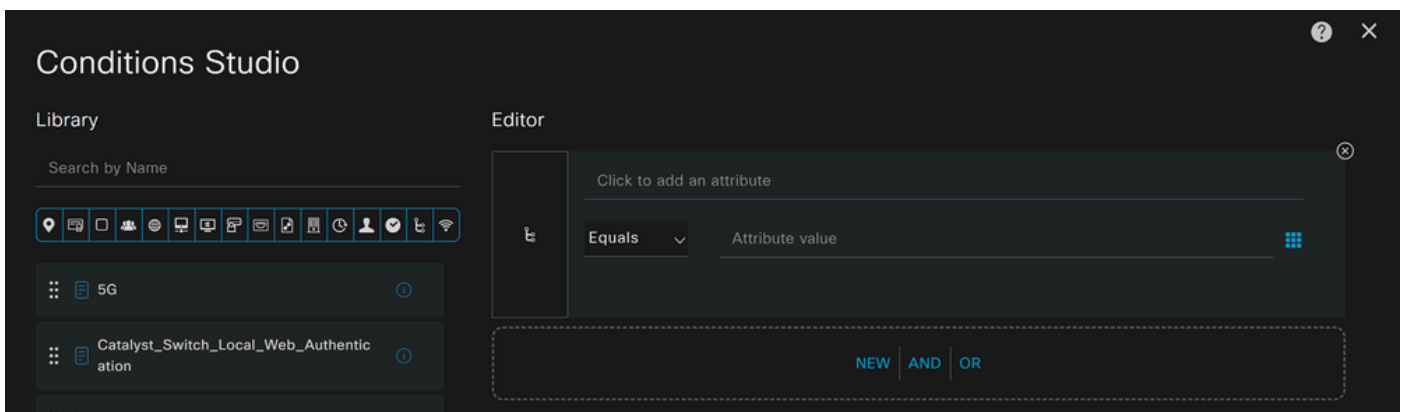
- Klicken Sie Policy > Policy Sets
- Klicken Sie auf, + um einen neuen Richtlinienatz hinzuzufügen



Erstellen Sie in diesem Fall einen neuen Richtlinienatz, anstatt ihn unter dem Standardsatz zu verwenden. Konfigurieren Sie anschließend die Authentifizierung und Autorisierung auf der Grundlage dieses Richtlinienpakets. Die konfigurierte Richtlinie ermöglicht den Zugriff auf das Netzwerkgerät, das im Schritt [Configure Network Devices List \(Liste der Netzwerkgeräte konfigurieren\)](#) definiert wurde, um zu überprüfen, ob diese Authentifizierungen von stammen, und um dann in die Richtlinie als zu gelangen **CSA Network Device List. Conditions**. Und schließlich die zulässigen Protokolle, wie **Default Network Access**.

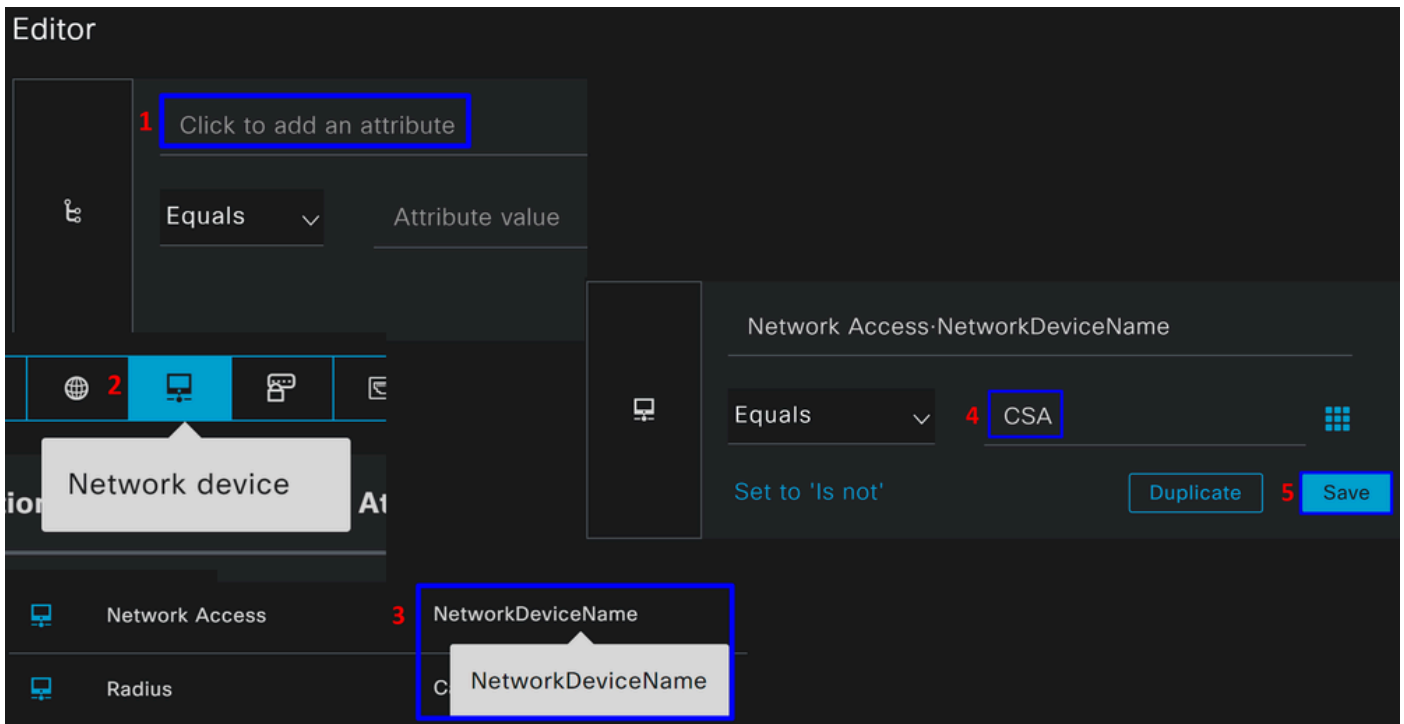
So erstellen Sie **condition** das , das mit dem Richtlinienatz übereinstimmt:

- Klicken Sie +
- Zu **Condition Studios** verfügbaren Informationen gehören:



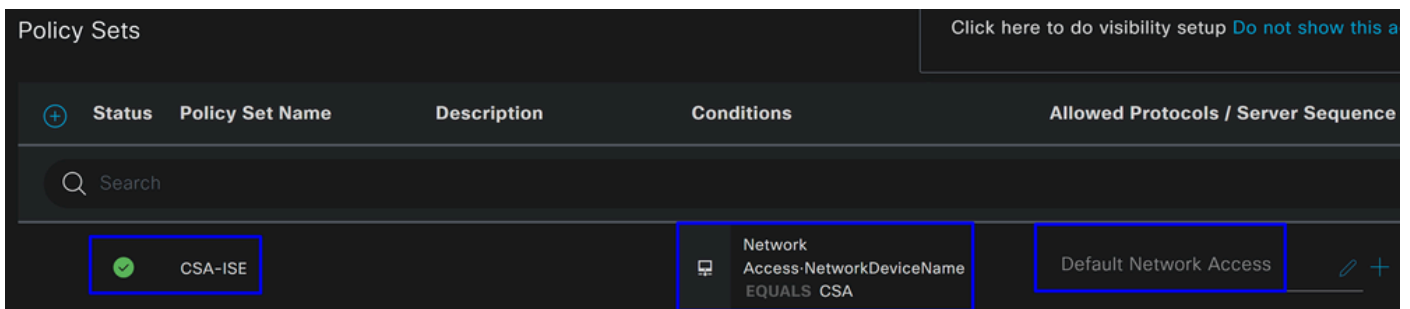
- Klicken Sie zum Erstellen der Bedingungen auf Click to add an attribute
- Klicken Sie auf die **Network Device** Schaltfläche
- Klicken Sie unter den Optionen dahinter auf **Network Access - Network Device Name** Option

- Schreiben Sie unter der Option Equals den Namen des **Network Device** unter dem Schritt [Configure Network Devices List](#)
- Klicken Sie auf **Save**

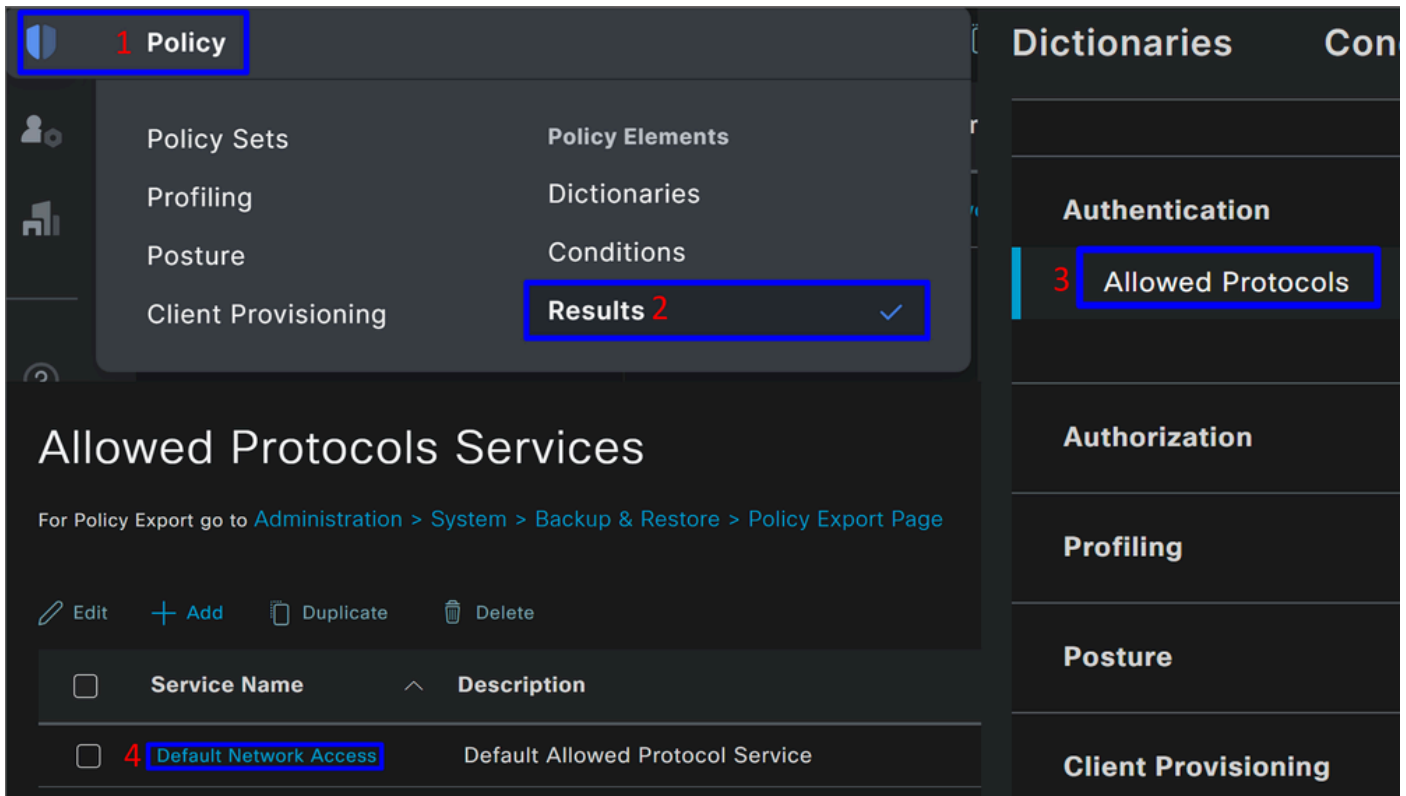


Diese Richtlinie genehmigt nur die Anforderung der Quelle, CSAs als **Authentication** und die **Authorization** Einrichtung unter dem Richtliniensatz fortzusetzen, **CSA-ISE** und überprüft außerdem die zulässigen Protokolle auf der Grundlage der **Default Network Access** für die zulässigen Protokolle.

Das Ergebnis der definierten Richtlinie muss sein:



- Um zu überprüfen, ob **Default Network Access Protocols** zulässig ist, fahren Sie mit den folgenden Anweisungen fort:
 - Klicken Sie **Policy > Results**
 - Klicken Sie **Allowed Protocols**
 - Klicken Sie **Default Network Access**

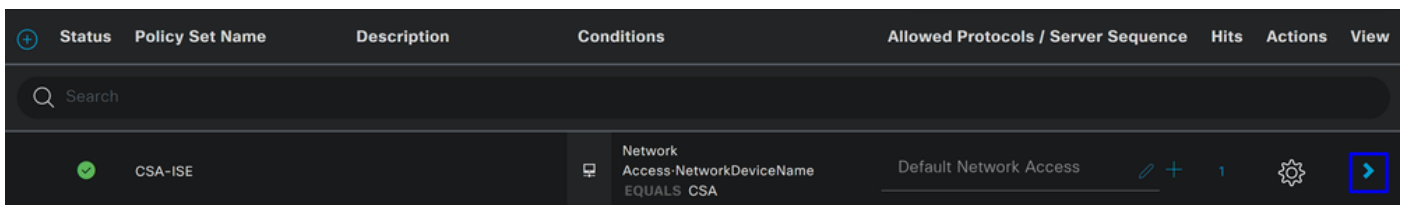


- Anschließend werden alle Protokolle angezeigt, die auf **Default Network Access**

Autorisierung für Policy Set konfigurieren

Gehen Sie wie folgt vor, um die **Authorization** Richtlinie unter **Policy Set** zu erstellen:

- Klicken Sie >



- Danach werden die **Authorization** Richtlinien angezeigt:

Policy Sets → CSA-ISE Click here to do visibility setup Do not show this again.

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	CSA-ISE		Network Access-NetworkDeviceName EQUALS CSA	Default Network Access	27
> Authentication Policy(2) > Authorization Policy - Local Exceptions > Authorization Policy - Global Exceptions > Authorization Policy(7)					

Die Richtlinie ist die gleiche, die Sie im Schritt [Configure Policy Set](#) definiert haben.

Autorisierungsrichtlinie

Sie haben viele Möglichkeiten, die Autorisierungsrichtlinie zu konfigurieren. In diesem Fall autorisieren Sie nur die Benutzer in der Gruppe, die im Schritt [Konfigurieren einer Gruppe](#) definiert ist. Im nächsten Beispiel wird die Autorisierungsrichtlinie konfiguriert:

Authorization Policy(2)

			Results		
+	Status	Rule Name	Conditions	Profiles	Security Groups
+	✓	Authorization Rule 1		Select from list	Select from list
+	+	+	+	+	+
+	✓	Authorization Secure Access	InternalUser-IdentityGroup EQUALS User Identity Groups:CSA-ISE	PermitAccess	Select from list

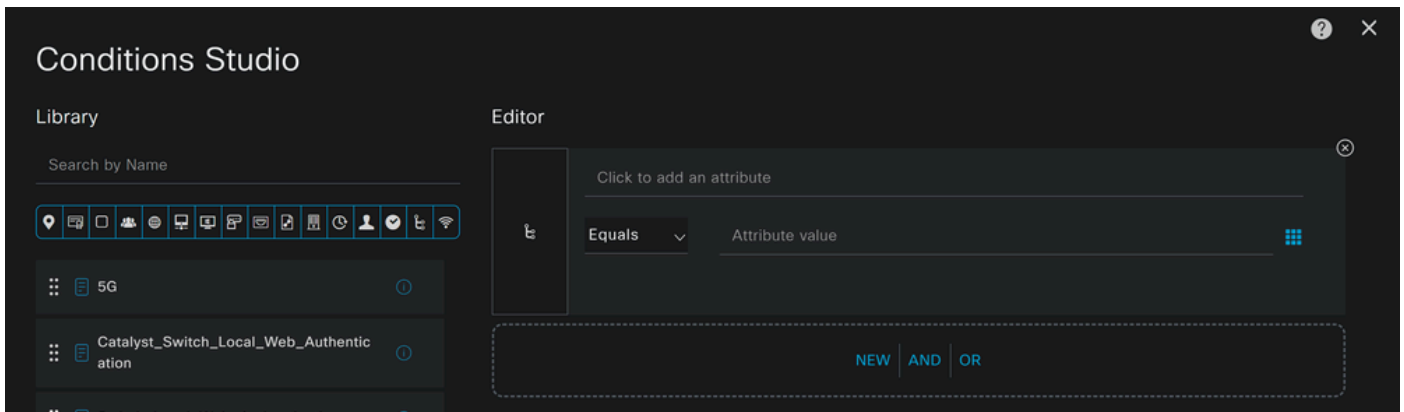
Note: Green arrows in the original image point from the top row to the bottom row for Status, Rule Name, Conditions, Profiles, and Security Groups.

- Klicken Sie **Authorization Policy**
- Klicken Sie auf, + um die Autorisierungsrichtlinie wie folgt zu definieren:

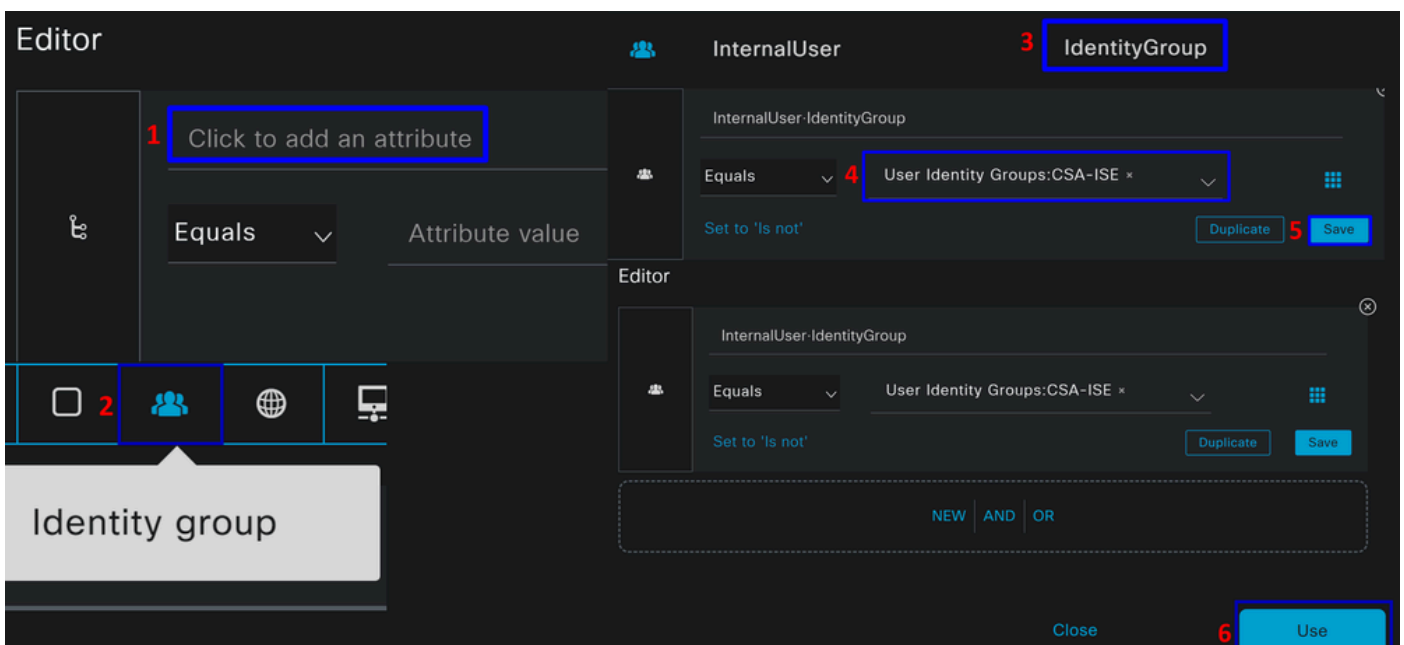
Authorization Policy(2)

			Results		
+	Status	Rule Name	Conditions	Profiles	Security Groups
+	✓	Authorization Rule 1		Select from list	Select from list

- Im nächsten Schritt ändern Sie das Rule Name, Conditions und Profiles
- Wenn Sie einen Namen **Name** konfigurieren, um die Autorisierungsrichtlinie leicht zu identifizieren
- Um das zu konfigurieren, **Condition**klicken Sie auf die Schaltfläche +
- Unter **Condition Studio**finden Sie die Informationen:



- Klicken Sie zum Erstellen der Bedingungen auf Click to add an attribute
- Klicken Sie auf die **Identity Group** Schaltfläche
- Klicken Sie unter den Optionen dahinter auf **Interner Benutzer - IdentityGroup** Option
- Verwenden Sie unter der **Equals** Option das Dropdown-Menü, um nach der für die Authentifizierung **Group** genehmigten im Schritt [Konfigurieren einer Gruppe](#) zu suchen.
- Klicken Sie auf **Save**
- Klicken Sie auf **Use**



Anschließend müssen Sie die **Profiles**, which help approve user access under the authorization policy once the user authentication matches the group selected on the policy.

- Klicken Sie unter **Authorization Policy** auf die Dropdown-Schaltfläche **Profiles**
- Nach Genehmigung suchen
- Auswählen **PermitAccess**
- Klicken Sie auf **Save**

The screenshot shows the configuration page for an authorization policy. At the top, the policy name is 'InternalUser·IdentityGroup EQUALS User Identity Groups:CSA-ISE'. A dropdown menu is open, showing the 'Profiles' section with 'PermitAccess' selected. Below this, a table lists the profiles: 'PermitAccess' (1) and 'DenyAccess' (0). The 'Save' button is highlighted in blue at the bottom right.



Anschließend haben Sie Ihre **Authorization** Richtlinie definiert. Authentifizieren Sie sich, um zu überprüfen, ob der Benutzer problemlos eine Verbindung herstellt und ob Sie die Protokolle auf Secure Access und ISE sehen können.

Um eine Verbindung zum VPN herzustellen, können Sie das auf Secure Access erstellte Profil verwenden und sich über Secure Client mit dem ISE-Profil verbinden.

- **Wie wird das Protokoll in Secure Access angezeigt, wenn die Authentifizierung genehmigt wird?**
 - Navigieren zum [Dashboard für sicheren Zugriff](#)

- Klicken Sie **Monitor > Remote Access Log**





28 Events

User	Connection Event	Event Details	Internal IP Address	Public IP Address	VPN Profile
 vpn user (vpnuser@ciscospt.es)	 Connected		192.168.50.2	151.248.21.152	ISE_CSA

- **Wie wird das Protokoll in der ISE angezeigt, wenn die Authentifizierung genehmigt wird?**

- Navigieren Sie zum **Cisco ISE Dashboard**

- Klicken Sie **Operations > Live Logs**

Status	Details	Identity	Authentication Policy	Authorization Policy	Authorization Profiles
∨		Identity	Authentication Policy	Authorization Policy	Authorization Profiles
		vpnuser@ciscospt.es	CSA-ISE	CSA-ISE >> Authorization CSA	PermitAccess
		vpnuser@ciscospt.es	CSA-ISE	CSA-ISE >> Authorization CSA	PermitAccess

Wie wird das Protokoll in Duo angezeigt, wenn die Authentifizierung genehmigt wird?

- Navigieren Sie zum [Duo Admin-Bereich](#).
- Klicken Sie **Reports > Authentication Log**

Timestamp (UTC) ▾	Result	User	Application	Risk-Based Policy Assessment	Access Device	Authentication Method
10:02:34 14 DE ABR. DE 2024	✔ Granted User approved	vpnuser	ISE - SAML	N/A	▾ iOS 17.4.1 AnyConnect 5.0.05207 Flash Not installed Java Not installed Krakow, 12, Poland 83.29.26.111 Endpoint trust is unknown because there are no active Trusted Endpoints Configurations.	▾ Duo Push Apple iPhone 15 Pro Max DPFK77EPVMXGJ7H7TMD3 Krakow, 12, Poland 83.29.26.111

Konfigurieren von lokalen Radius- oder Active Directory-Benutzern

Konfigurieren des ISE-Status

Erstellen Sie in diesem Szenario die Konfiguration, um die Endpunkt-Compliance zu überprüfen, bevor Sie den Zugriff auf interne Ressourcen gewähren oder verweigern.

Gehen Sie wie folgt vor, um die Konfiguration vorzunehmen:

Statusbedingungen konfigurieren

- Rufen Sie Ihr ISE Dashboard auf.
- Klicken Sie **Work Center > Policy Elements > Conditions**
- Klicken Sie **Anti-Malware**



Hinweis: Hier finden Sie viele Optionen, um den Status Ihrer Geräte zu überprüfen und die richtige Bewertung auf Grundlage Ihrer internen Richtlinien vorzunehmen.

Conditions



Anti-Malware

Anti-Spyware

Anti-Virus

Application

Compound

Dictionary Compound

Dictionary Simple

Disk Encryption

External DataSource

File

Firewall

Anti-Malware Condition dass die Antivirus-Installation auf dem System erkannt wird. Sie können bei Bedarf auch die Version des Betriebssystems auswählen.

The image shows two side-by-side screenshots of the 'Anti-Malware Condition' configuration interface. The left screenshot shows a form with the following fields: '* Name' (empty), 'Description' (empty), 'Compliance Module' (4.x or later), '* Operating System' (Select Operating System), and 'Vendor' (ANY). The 'Check Type' is set to 'Installation'. The right screenshot shows the same form with the following values: '* Name' (CSA-Antimalware), 'Description' (empty), 'Compliance Module' (4.x or later), '* Operating System' (Windows All), and 'Vendor' (Cisco Systems, Inc.). The 'Check Type' is also set to 'Installation'. Arrows indicate the mapping of values from the left form to the right form.

- **Name:** Verwenden Sie einen Namen, um den Anti-Malware-Zustand zu erkennen.
- **Operating System:** Wählen Sie das operative System, das Sie unter der Bedingung setzen möchten
- **Vendor:** Wählen Sie einen Anbieter oder eine BELIEBIGE
- **Check Type:** Sie können überprüfen, ob der Agent installiert ist, oder die Definitionsversion für diese Option angeben.
- Für **Products for Selected Vendor** konfigurieren Sie, was Sie über den Malwareschutz auf dem Gerät überprüfen möchten.

Baseline Condition Advanced Condition

1 You can select products either on baseline condition or advanced condition.

2

	Product Name	Minimum Version	Maximum Version	Minimum Compliant
<input type="checkbox"/>	ANY	ANY	ANY	N/A
<input checked="" type="checkbox"/>	Cisco Advanced Malware Prote...	5.x	7.x	4.2.520.0
<input checked="" type="checkbox"/>	Cisco Advanced Malware Prote...	5.x	7.x	4.3.2815.6145
<input checked="" type="checkbox"/>	Cisco Secure Endpoint	7.x	8.x	4.3.3726.6145
<input checked="" type="checkbox"/>	Cisco Secure Endpoint (x86)	7.x	8.x	4.3.3726.6145
<input type="checkbox"/>	ClamAV	0.x	ClamAV0.x	4.3.2868.6145

3 Save Reset

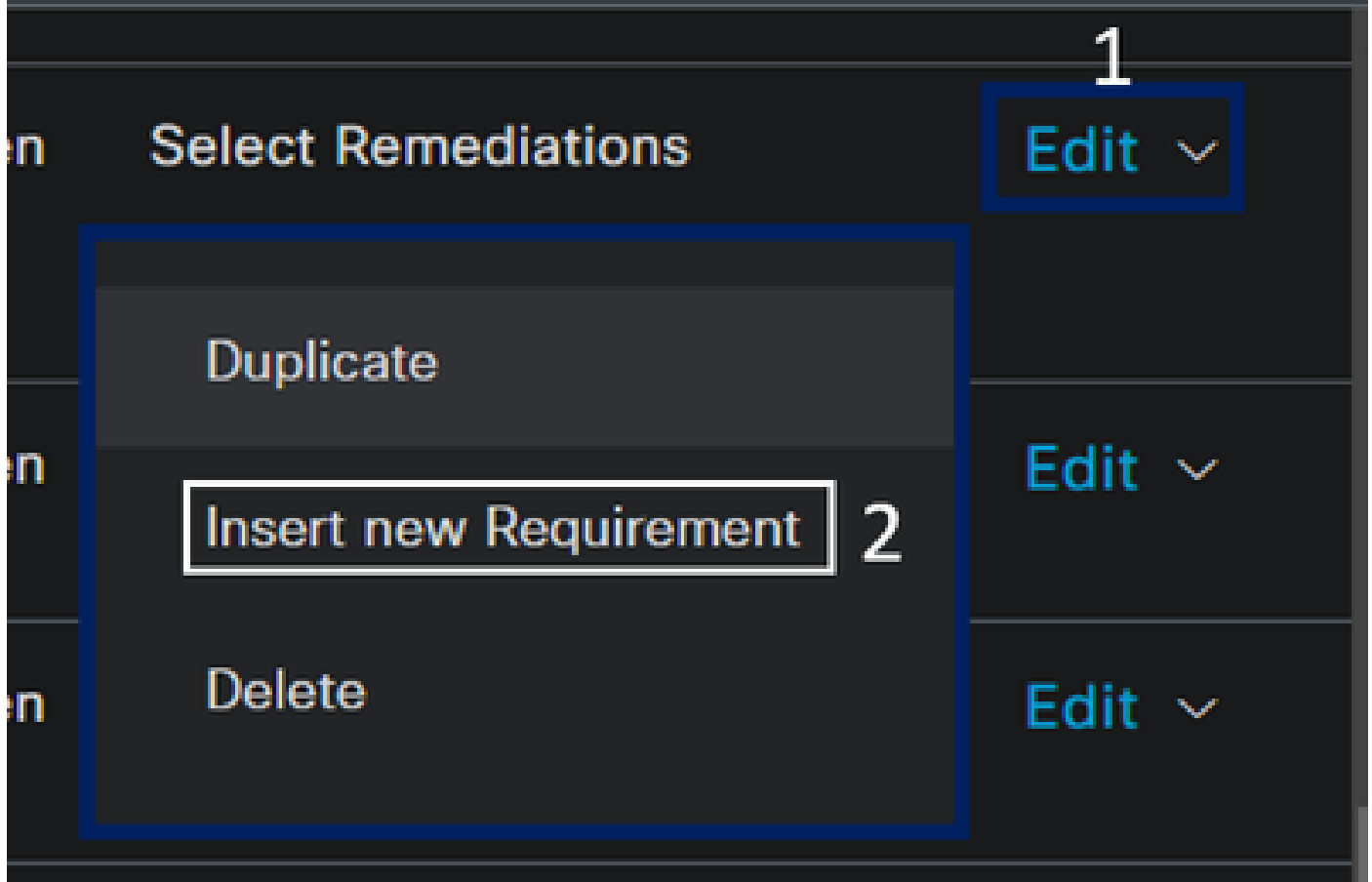
- Aktivieren Sie das Kontrollkästchen für die Bedingungen, die Sie evaluieren möchten.
- Konfigurieren Sie die zu überprüfende Mindestversion.
- Klicken Sie auf Speichern, um mit dem nächsten Schritt fortzufahren

Sobald Sie es konfigurieren, können Sie mit dem Schritt fortfahren, **Configure Posture Requirements**.

Statusanforderungen konfigurieren

- Rufen Sie Ihr ISE Dashboard auf.
- Klicken Sie **Work Center > Policy Elements > Requiriments**
- Klicken Sie auf eine **Edit** der Anforderungen, und klicken Sie auf **Insert new Requirement**

Remediations Actions



- Konfigurieren Sie unter den neuen Anforderungen die folgenden Parameter:

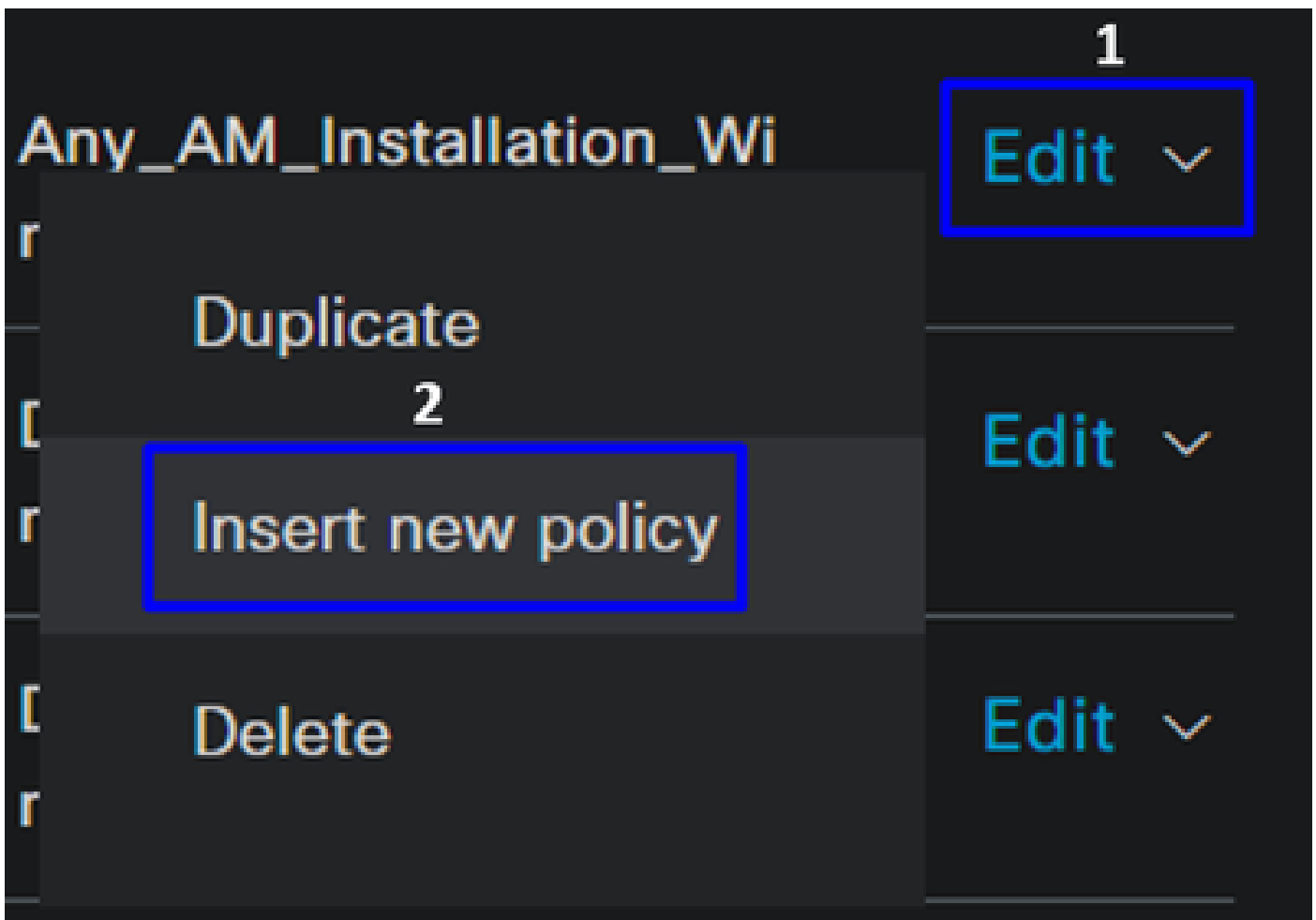
Requirements						
Name	Operating System	Compliance Module	Posture Type	Conditions	Remediations Actions	
CSA-ANTIMALWARE	for Windows All	using 4.x or later	using Agent	met if CSA-Antimalware then	Message Text Only	Edit ▾

- **Name:** Konfigurieren Sie einen Namen, um die Anti-Malware-Anforderung zu erkennen.
- **Operating System:** Wählen Sie das Betriebssystem, das Sie unter der Bedingung Schritt, [Betriebssystem](#)
- **Compliance Module:** Sie müssen sicherstellen, dass Sie das gleiche Compliance-Modul, das Sie unter der Bedingung Schritt, [Anti-Malware-Bedingung](#) haben
- **Posture Type:** Agent auswählen
- **Conditions:** Wählen Sie die Bedingung(en), die Sie im Schritt "[Statusbedingungen konfigurieren](#)" erstellt haben.
- **Remediations Actions:** Wählen Sie **Message Text Only** für dieses Beispiel aus, oder verwenden Sie eine andere Wiederherstellungsaktion.
- Klicken Sie auf **Save**

Nach der Konfiguration können Sie mit dem Schritt fortfahren, **Configure Posture Policy**

Statusrichtlinie konfigurieren

- Rufen Sie Ihr ISE Dashboard auf.
- Klicken Sie **Work Center > Posture Policy**
- Klicken Sie auf eine **Edit** der Richtlinien, und klicken Sie auf **Insert new Policy**



- Konfigurieren Sie unter der neuen Richtlinie die folgenden Parameter:

Status	Policy Options	Rule Name	Identity Groups	Operating Systems	Compliance Module	Posture Type	Other Conditions	Requirements
<input checked="" type="checkbox"/>	Policy Options	CSA-Windows-Posture	If Any	and Windows All	and 4.x or later	and Agent	and	then CSA-ANTIMALWARE

- **Status:** Aktivieren Sie das Kontrollkästchen zum Aktivieren der Richtlinie.
- **Rule Name:** Konfigurieren Sie einen Namen zur Erkennung der konfigurierten Richtlinie.

- **Identity Groups:** Wählen Sie die zu bewertenden Identitäten aus.
- **Operating Systems:** Wählen Sie das Betriebssystem basierend auf der Bedingung und den zuvor konfigurierten Anforderungen aus.
- **Compliance Module:** Wählen Sie das Compliance-Modul basierend auf der Bedingung und den zuvor konfigurierten Anforderungen aus.
- Posture Type: Agent auswählen
- **Requirements:** Wählen Sie die auf dem Schritt konfigurierten Anforderungen, [Configure Posture Requirements](#)
- Klicken Sie auf **Save**

Konfiguration der Client-Bereitstellung

Um den Benutzern das ISE-Modul bereitzustellen, konfigurieren Sie die Client-Bereitstellung so, dass die Computer mit dem ISE-Statusmodul ausgestattet werden. Auf diese Weise können Sie den Systemstatus überprüfen, sobald der Agent installiert wurde. Um mit diesem Prozess fortzufahren, gehen Sie wie folgt vor:

Navigieren Sie zu Ihrem ISE Dashboard.

- Klicken Sie **Work Center > Client Provisioning**
- Auswählen **Resources**










Bei der Clientbereitstellung müssen drei Dinge konfiguriert werden:

Zu konfigurierende Ressourcen	Beschreibung
1. Agent Resources	Secure Client-Webbereitstellungspaket.
2. Compliance Module	Cisco ISE Compliance-Modul
3. Agent Profile	Steuerung des Bereitstellungsprofils
3. Agent Configuration	Legen Sie fest, welche Module bereitgestellt werden sollen, indem Sie das Bereitstellungsportal mithilfe des Agentenprofils und der Agentenressourcen

einrichten.

Step 1 Agentenressourcen herunterladen und hochladen

- Um eine neue Agentenressource hinzuzufügen, navigieren Sie zum [Cisco Download-Portal](#), und laden Sie das Web-Bereitstellungspaket herunter. Die Web-Bereitstellungsdatei muss das Format .pkg aufweisen.

Cisco Secure Client Headend Deployment Package (Linux 64-bit) cisco-secure-client-linux64-5.1.2.42-webdeploy-k9.pkg Advisories	06-Feb-2024	58.06 MB	  
Cisco Secure Client Headend Deployment Package (Windows) cisco-secure-client-win-5.1.2.42-webdeploy-k9.pkg Advisories	06-Feb-2024	111.59 MB	  
Cisco Secure Client Headend Deployment Package (Mac OS) - Administrator rights or managed device required for install or upgrade. See Administrator Guide and Release Notes for details. cisco-secure-client-macos-5.1.2.42-webdeploy-k9.pkg Advisories	06-Feb-2024	118.88 MB	  

- Klicken Sie auf + Add > Agent resources from local disk und laden Sie die Pakete hoch.

+ Add ^ Duplicate Delete

Agent resources from Cisco site

Agent resources from local disk

Native Supplicant Profile

Agent Configuration

Agent Posture Profile

AMP Enabler Profile

Step 2 Compliance-Modul herunterladen

- Klicken Sie + Add > Agent resources from Cisco Site



Add



Duplicate



Delete

Agent resources from Cisco site

Agent resources from local disk

Native Supplicant Profile

Agent Configuration

Agent Posture Profile

AMP Enabler Profile

- Aktivieren Sie das Kontrollkästchen für jedes erforderliche Compliance-Modul, und klicken Sie auf **Save**

Download Remote Resources

<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	AnyConnectComplianceModuleLinux64 4.3.3064.0	Cisco Secure Client Linux Compliance Module 4.
<input type="checkbox"/>	AnyConnectComplianceModuleLinux64 4.3.3104.0	Cisco Secure Client Linux Compliance Module 4.
<input type="checkbox"/>	AnyConnectComplianceModuleOSX 4.3.3432.6400	Cisco Secure Client OSX Compliance Module 4.3
<input type="checkbox"/>	AnyConnectComplianceModuleOSX 4.3.3472.6400	Cisco Secure Client OSX Compliance Module 4.3
<input type="checkbox"/>	AnyConnectComplianceModuleWindows 4.3.3940.8192	Cisco Secure Client Windows Compliance Modul
<input type="checkbox"/>	AnyConnectComplianceModuleWindows 4.3.3980.8192	Cisco Secure Client Windows Compliance Modul
<input type="checkbox"/>	AnyConnectComplianceModuleWindowsARM64 4.3.3940....	Cisco Secure Client WindowsARM64 Compliance
<input type="checkbox"/>	AnyConnectComplianceModuleWindowsARM64 4.3.3980....	Cisco Secure Client WindowsARM64 Compliance

For Agent software, please download from <http://cisco.com/go/ciscosecureclient>. Use the "Agent resource from local disk" add option, to import into ISE

Cancel

Save

Step 3 Konfigurieren des Agentenprofils

- Klicken Sie + Add > Agent Posture Profile

+ Add ^

☰ Duplicate

🗑 Delet

Agent resources from Cisco site

Agent resources from local disk

Native Supplicant Profile

Agent Configuration

Agent Posture Profile

AMP Enabler Profile

- Erstellen Sie einen **Name** für **Posture Profile**

Agent Posture Profile

Name *



Description:

- Legen Sie unter "Servernamen" ein * und klicken Sie **Save** danach auf

Posture Protocol		
Parameter	Value	Description
PRA retransmission time	120 secs	This is the agent retry period if there is a Passive Reassessment communication failure
Retransmission Delay ⓘ	60 secs	Time (in seconds) to wait before retrying.
Retransmission Limit ⓘ	4	Number of retries allowed for a message.
Discovery host ⓘ		Enter any IP address or FQDN that is routed through a NAD. The NAD detects and redirects that http traffic to the Client Provisioning portal.
Discovery Backup Server List ⓘ	Choose	By default, AnyConnect sends discovery probes to all the Cisco ISE PSNs sequentially if the PSN is unreachable. Choose specific PSNs as the backup list and restrict the nodes to which AnyConnect sends discovery probes.
Server name rules * ⓘ	*	A list of wildcarded, comma-separated names that defines the servers that the agent can connect to. E.g. *.cisco.com
Call Home List ⓘ		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 ⓘ	30 secs	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

Step 4 Konfigurieren der Agentenkonfiguration

- Klicken Sie + Add > Agent Configuration

+ Add ^

📱 Duplicate

🗑️ Delete

Agent resources from Cisco site

Agent resources from local disk


Native Supplicant Profile

Agent Configuration

Agent Posture Profile

AMP Enabler Profile


- Konfigurieren Sie anschließend die folgenden Parameter:

* Select Agent Package: CiscoSecureClientDesktopWindows 5.1 

* Configuration Name:

Description:

Description Value Notes

* Compliance Module CiscoSecureClientComplianceModuleWi 

Cisco Secure Client Module Selection

ISE Posture	<input checked="" type="checkbox"/>
VPN	<input type="checkbox"/>
Zero Trust Access	<input type="checkbox"/>
Network Access Manager	<input type="checkbox"/>
Secure Firewall Posture	<input type="checkbox"/>
Network Visibility	<input type="checkbox"/>
Umbrella	<input type="checkbox"/>
Start Before Logon	<input type="checkbox"/>
Diagnostic and Reporting Tool	<input type="checkbox"/>

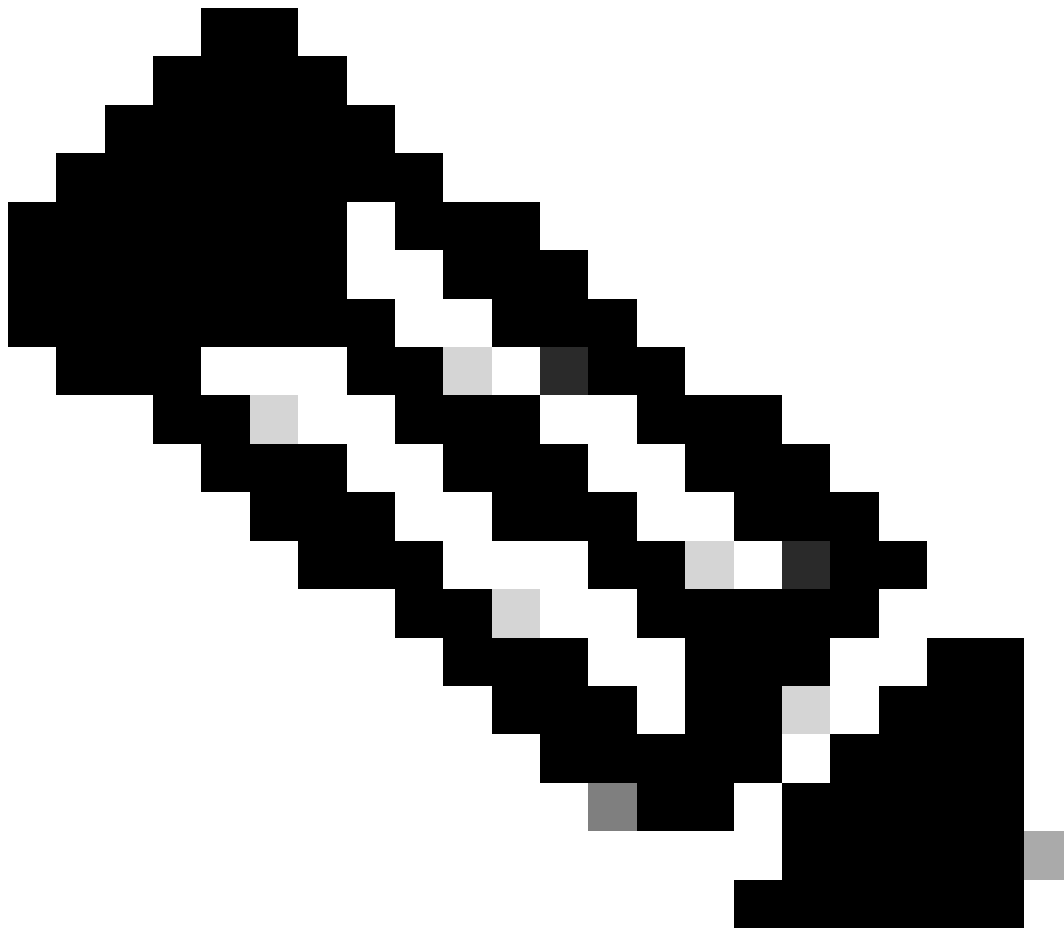
Profile Selection

* ISE Posture	1.CSA_PROFILE	▼
VPN		▼

- Select Agent Package : Wählen Sie das hochgeladene Paket für die [Step1 Download and Upload Agent-Ressourcen aus](#).
- **Configuration Name:** Wählen Sie einen Namen, um die **Agent Configuration**
- **Compliance Module:** Wählen Sie das Compliance-Modul aus, das Sie auf der Seite [Schritt 2 Compliance-Modul herunterladen](#) heruntergeladen haben.
- Cisco Secure Client Module Selection
 - **ISE Posture:** Kontrollkästchen markieren
- **Profile Selection**

- **ISE Posture:** Wählen Sie das ISE-Profil aus, das unter [Schritt 3 Konfigurieren des Agent-Profiles](#) konfiguriert wurde.

- Klicken Sie auf **Save**

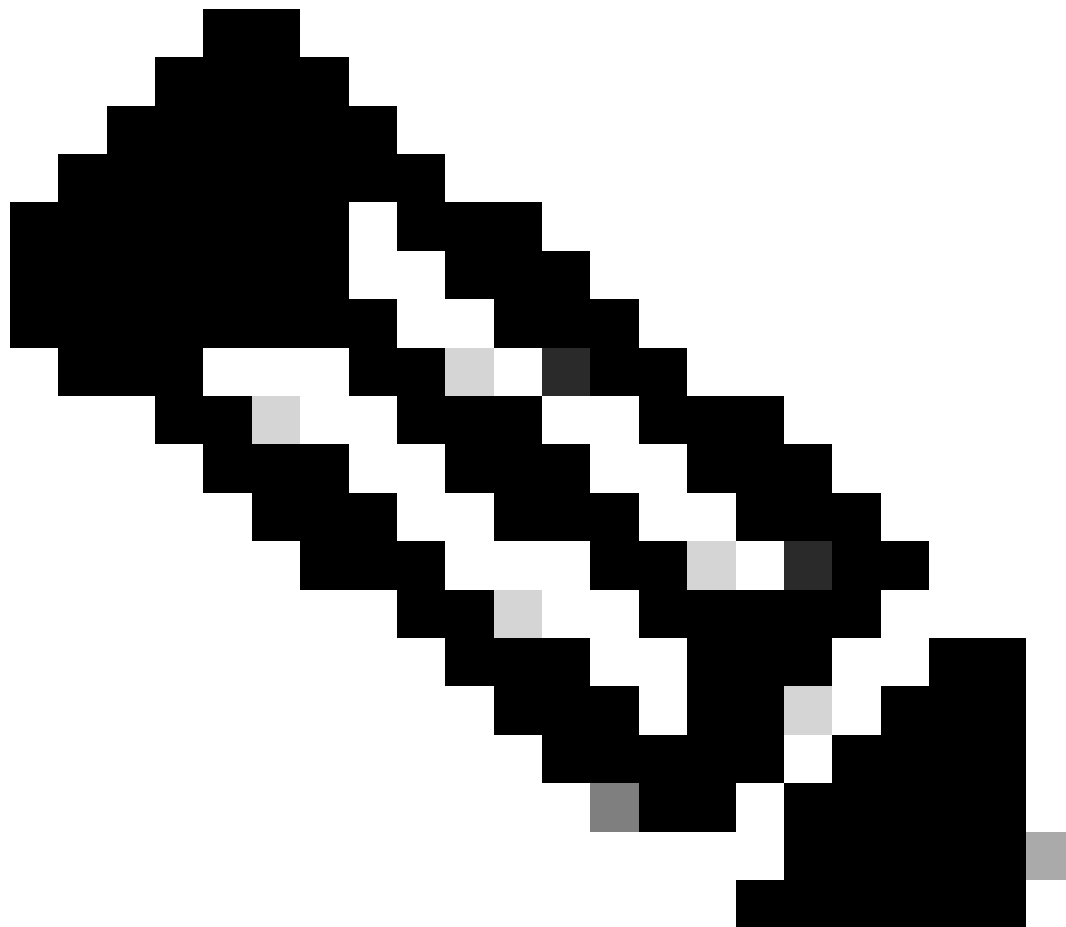


Hinweis: Es wird empfohlen, dass jedes Betriebssystem (Windows, Mac OS oder Linux) über eine unabhängige Client-Konfiguration verfügt.

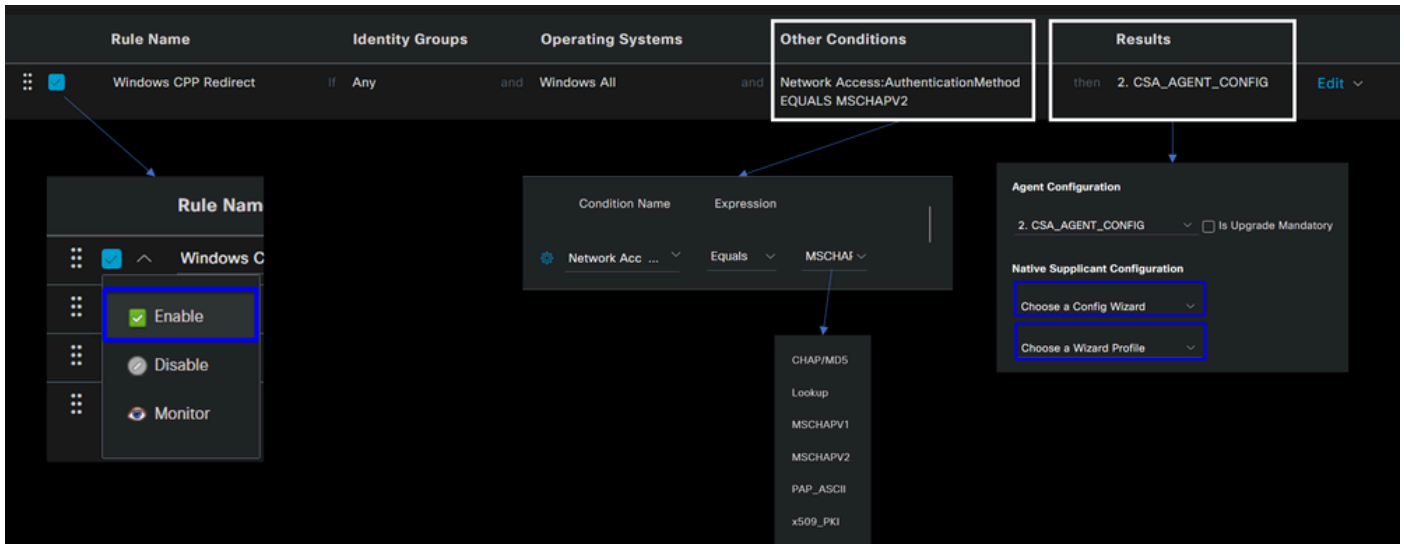
Client-Bereitstellungsrichtlinie konfigurieren

Um die Bereitstellung des ISE-Status und der im letzten Schritt konfigurierten Module zu ermöglichen, müssen Sie eine Richtlinie für die Bereitstellung konfigurieren.

- Rufen Sie Ihr ISE Dashboard auf.
- Klicken Sie **Work Center > Client Provisioning**



Hinweis: Es wird empfohlen, dass für jedes Betriebssystem (Windows, Mac OS oder Linux) eine Client-Konfigurationsrichtlinie gilt.



- **Rule Name:** Konfigurieren Sie den Namen der Richtlinie auf Basis des Gerätetyps und der Identitätsgruppenauswahl, um jede Richtlinie leicht identifizieren zu können.
- **Identity Groups:** Wählen Sie die Identitäten aus, die Sie in der Richtlinie bewerten möchten.
- **Operating Systems:** Wählen Sie das Betriebssystem basierend auf dem Agentenpaket aus, das auf dem Schritt ausgewählt wurde. [Wählen Sie Agentenpaket aus.](#)
- **Other Condition:** Wählen Sie **Network Access** basierend auf der **Authentication Method** EQUALS zu der im Schritt konfigurierten Methode, [Add RADIUS Group \(RADIUS-Gruppe hinzufügen\)](#) aus, oder lassen Sie das Feld leer.
- **Result:** Wählen Sie die unter [Schritt 4 Konfigurieren der Agentenkonfiguration](#) konfigurierte Agentenkonfiguration aus.
 - **Native Supplicant Configuration:** Wählen Sie Config Wizard und Wizard Profile
- Markieren Sie die Richtlinie als aktiviert, wenn sie nicht im Kontrollkästchen als aktiviert aufgeführt ist.

Erstellen der Autorisierungsprofile

Das Autorisierungsprofil schränkt den Zugriff auf die Ressourcen je nach dem Benutzerstatus nach dem Authentifizierungsprozess ein. Die Autorisierung muss überprüft werden, um anhand des Status zu bestimmen, auf welche Ressourcen der Benutzer zugreifen kann.

Autorisierungsprofil	Beschreibung
Konformität	Benutzerkonform - Agent installiert - Status verifiziert
Unbekannte	Benutzer nicht bekannt - Umleitung zur Installation des Agenten - Zur

Compliance	Überprüfung ausstehende Statusüberprüfung
Zugriff verweigern	Benutzer nicht konform - Zugriff verweigern

Um die DACL zu konfigurieren, navigieren Sie zum ISE Dashboard:

- Klicken Sie **Work Centers > Policy Elements > Downloadable ACLs**
- Klicken Sie **+Add**
- Erstellen Sie **Compliant DACL**

* Name: CSA-Compliant

Description: [Empty text box]

IP version: IPv4 IPv6 Agnostic ⓘ

* DACL Content:

1234567	permit ip any any
8910111	
2131415	
1617181	
9202122	
2324252	
6272829	
3031323	
3343536	
3738394	
...	

- **Name:** Fügen Sie einen Namen hinzu, der auf die DACL-konforme
- **IP version:** Auswahl **IPv4**
- **DACL Content:** Erstellen Sie eine herunterladbare Zugriffskontrollliste (DACL), die Zugriff auf alle Ressourcen des Netzwerks bietet.

<#root>

permit ip any any

Klicken Sie auf, **Save** und erstellen Sie die unbekannte Compliance-DACL.

- Klicken Sie **Work Centers > Policy Elements > Downloadable ACLs**

- Klicken Sie **+Add**
- Erstellen Sie **Unknown Compliant DACL**

*** Name**

Description

IP version IPv4 IPv6 Agnostic ⓘ

*** DACL Content**

1234567	permit udp any any eq 67
8910111	permit udp any any eq 68
2131415	permit udp any any eq 53
1617181	permit tcp any host 192.168.10.206 eq 8443
9202122	permit tcp any any eq 80
2324252	
6272829	
3031323	
3343536	
3738394	

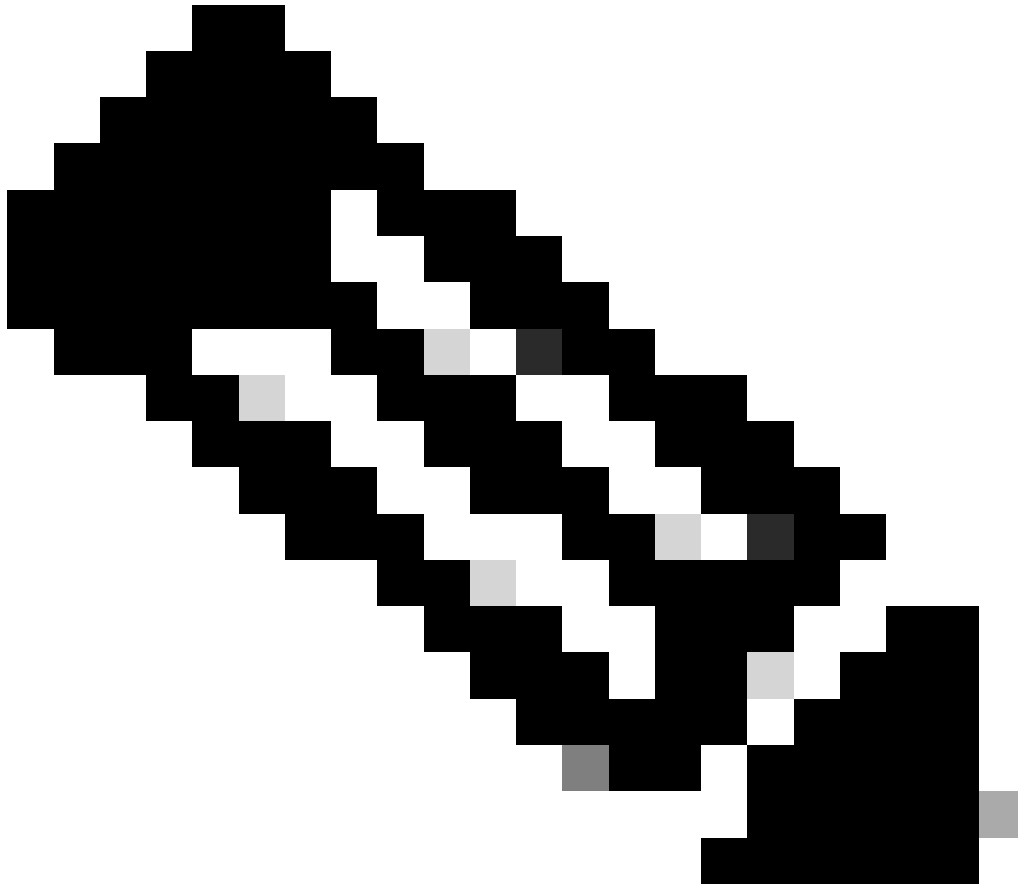
⌵ **Check DACL Syntax**

- **Name:** Fügen Sie einen Namen hinzu, der auf die DACL-Unknown-Compliant verweist.
- **IP version:** Auswahl **IPv4**
- **DACL Content:** Erstellen einer DACL mit eingeschränktem Zugriff auf Netzwerk, DHCP, DNS, HTTP und das Bereitstellungsportal über Port 8443

```

permit udp any any eq 67
permit udp any any eq 68
permit udp any any eq 53
permit tcp any any eq 80
permit tcp any host 192.168.10.206 eq 8443

```

Hinweis: In diesem Szenario entspricht die IP-Adresse 192.168.10.206 dem Cisco Identity Services Engine (ISE)-Server, und Port 8443 ist für das Bereitstellungsportal festgelegt. Dies bedeutet, dass TCP-Datenverkehr an die IP-Adresse 192.168.10.206 über Port 8443 zugelassen wird, wodurch der Zugriff auf das Bereitstellungsportal erleichtert wird.

Jetzt verfügen Sie über die erforderliche DACL zum Erstellen der Autorisierungsprofile.

Rufen Sie zum Konfigurieren der Autorisierungsprofile das ISE Dashboard auf:

- Klicken Sie **Work Centers > Policy Elements > Authorization Profiles**

- Klicken Sie **+Add**

- Erstellen Sie **Compliant Authorization Profile**

Authorization Profile

* Name


CSA-Compliant

Description

* Access Type

ACCESS_ACCEPT

Network Device Profile

 Cisco

Service Template

Track Movement

Agentless Posture

Passive Identity Tracking

✓ Common Tasks

DACL Name

CSA-Compliant

IPv6 DACL Name

ACL

ACL ID (Filter ID)

- **Name:** Erstellen Sie einen Namen, der auf das kompatible Autorisierungsprofil verweist.
- Access Type: Auswahl **ACCESS_ACCEPT**

- **Common Tasks**

- **DACL NAME:** Wählen Sie die auf dem Schritt "[Compliant DACL](#)" konfigurierte DACL aus.

Klicken **Save** und erstellen Sie Unknown Authorization Profile

- Klicken Sie **Work Centers > Policy Elements > Authorization Profiles**
- Klicken Sie **+Add**

- Erstellen Sie Unknown Compliant Authorization Profile

*** Name** CSA-Unknown-Compliant

Description

*** Access Type** ACCESS_ACCEPT

Network Device Profile Cisco

Service Template

Track Movement ⓘ

Agentless Posture ⓘ

Passive Identity Tracking ⓘ

Common Tasks

DACL Name CSA_Redirect_To_ISE

Web Redirection (CWA, MDM, NSP, CPP) ⓘ

Client Provisioning (Posture) ACL redirect Value Client Provisioning Portal (...)

- **Name:** Erstellen Sie einen Namen, der auf das unbekannte, kompatible Autorisierungsprofil verweist.
- Access Type: Auswahl **ACCESS_ACCEPT**

- **Common Tasks**

- **DACL NAME:** Wählen Sie die auf dem Schritt [Unknown Compliant DACL](#) konfigurierte DACL aus.

- **Web Redirection (CWA,MDM,NSP,CPP)**

- Auswählen **Client Provisioning (Posture)**

- **ACL:** Muss redirect

- **Value:** Wählen Sie das Standard-Bereitstellungsportal aus, oder wählen Sie es aus, wenn Sie ein anderes Portal definiert haben.



Hinweis: Der Name der Umleitungs-ACL für sicheren Zugriff für alle Bereitstellungen lautet **redirect**.

Nachdem Sie alle diese Werte definiert haben, müssen Sie etwas Ähnliches unter Attributes Details haben.

Attributes Details

Access Type = ACCESS_ACCEPT

DACL = CSA_Redirect_To_ISE

cisco-av-pair = url-redirect-acl=redirect

cisco-av-pair = url-redirect=https://ip:port/portal/gateway?sessionId=SessionIdValue&portal=

&action=cpp

Klicken Sie hier, **Save** um die Konfiguration zu beenden und mit dem nächsten Schritt fortzufahren.

Festlegen von Statusrichtlinien

Die drei Richtlinien, die Sie erstellen, basieren auf den Autorisierungsprofilen, die Sie konfiguriert haben. **DenyAccess** Sie müssen also keine weitere Richtlinie erstellen.

Richtliniensatz - Autorisierung	Autorisierungsprofil
Konformität	Autorisierungsprofil - konform
Unbekannte Compliance	Autorisierungsprofil - Unbekannt
Nicht konform	Zugriff verweigern

Rufen Sie Ihr ISE Dashboard auf.

- Klicken Sie **Work Center > Policy Sets**

- Klicken Sie auf > die Schaltfläche, um auf die von Ihnen erstellte Richtlinie zuzugreifen.

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
	CSA-ISE		Network Access-NetworkDeviceName EQUALS CSA	Default Network Access	370		

- Klicken Sie auf Authorization Policy

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
	CSA-ISE		Network Access-NetworkDeviceName EQUALS CSA	Default Network Access	370
> Authentication Policy(2)					
> Authorization Policy - Local Exceptions					
> Authorization Policy - Global Exceptions					
> Authorization Policy(4)					

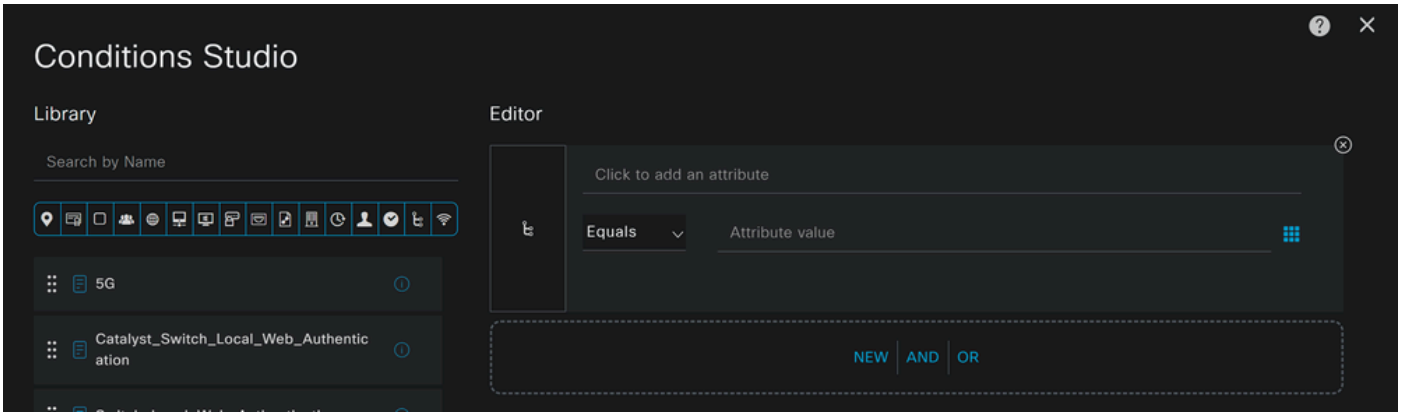
- Erstellen Sie die nächsten drei Richtlinien in der folgenden Reihenfolge:

✓	SAML-Compliant	AND	<div>Compliant_Devices</div> <hr/> <div>InternalUser-IdentityGroup EQUALS User Identity Groups:CSA-ISE</div>	CSA-Compliant
✓	SAML-Unknown-Compliant	AND	<div>Compliance_Unknown_Devices</div> <hr/> <div>InternalUser-IdentityGroup EQUALS User Identity Groups:CSA-ISE</div>	CSA-Unknown-Compliant
✓	SAML-Non-Compliant	AND	<div>Non_Compliant_Devices</div> <hr/> <div>InternalUser-IdentityGroup EQUALS User Identity Groups:CSA-ISE</div>	DenyAccess

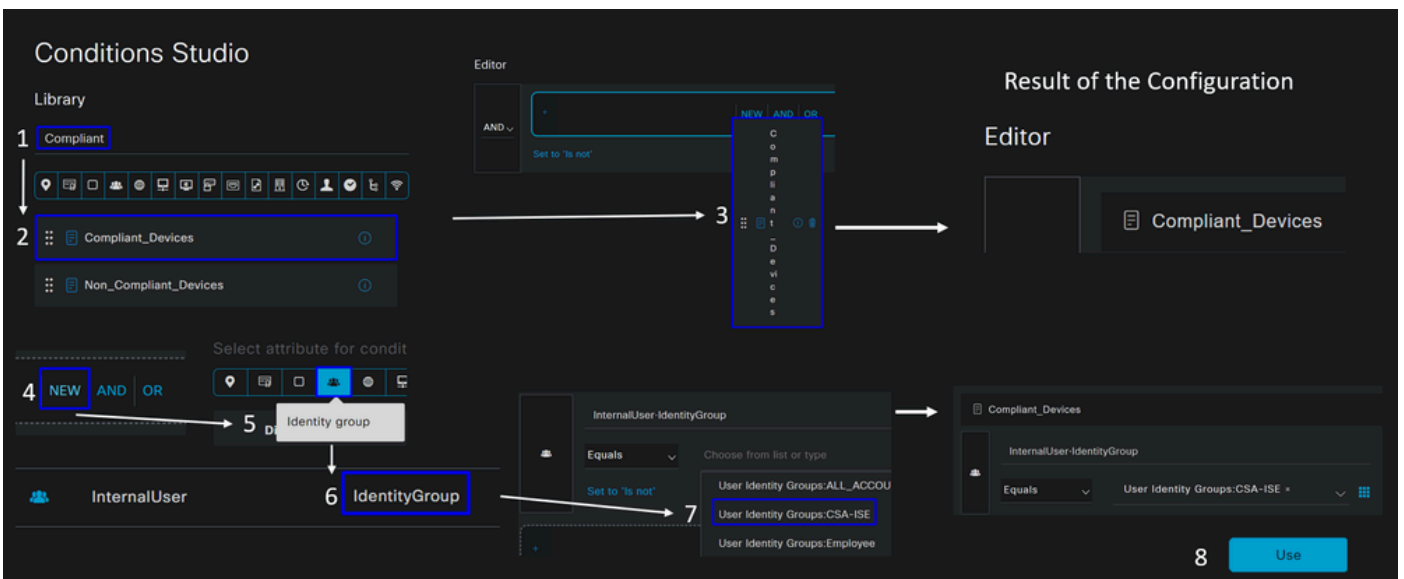
- Klicken Sie auf, + um die **CSA-Compliance** Richtlinie zu definieren:

				Results	
+ Status	Rule Name	Conditions		Profiles	Security Groups
<input type="text" value="Search"/>					
✓	Authorization Rule 1	+		Select from list	Select from list

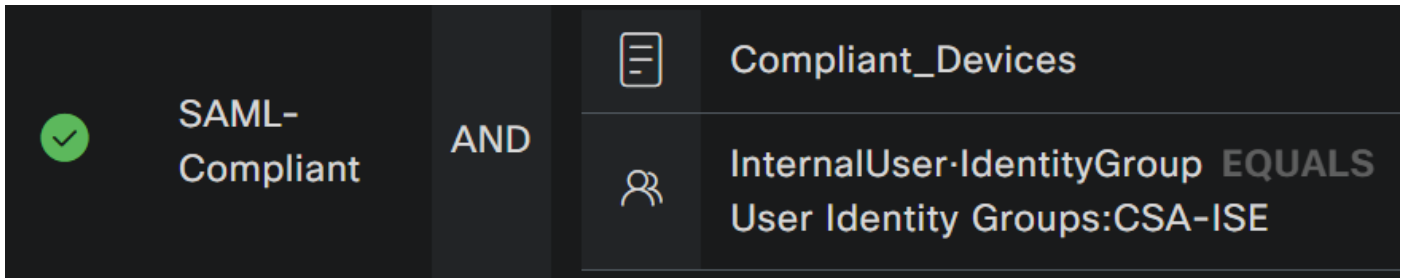
- Im nächsten Schritt ändern Sie das Rule Name, Conditions und Profiles
- Wenn Sie einen Namen **Name** konfigurieren auf **CSA-Compliance**
- Um das zu konfigurieren, **Condition**klicken Sie auf die Schaltfläche +
- Unter **Condition Studio**finden Sie die Informationen:



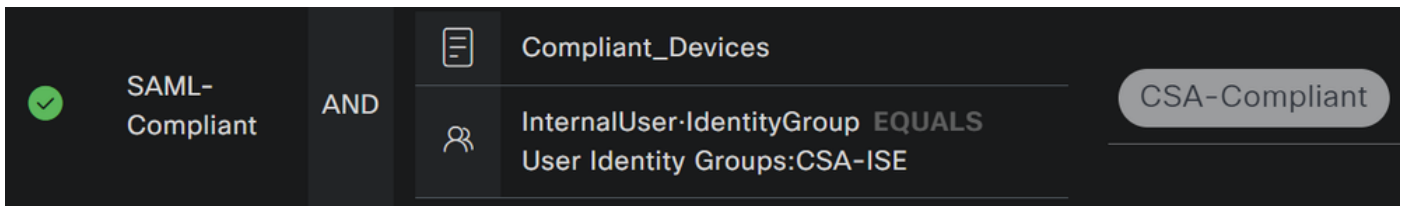
- Um die Bedingung zu erstellen, suchen Sie nach **compliant**
- Sie müssen Folgendes anzeigen: **Compliant_Devices**
- Drag & Drop unter dem **Editor**
- Klicken Sie unter Editor in **New**
- Klicken Sie auf das **Identity Group** Symbol
- Auswählen **Internal User Identity Group**
- Wählen **Equals** Sie unter die **User Identity Group** passende aus.
- Klicken Sie auf **Use**



- Als Ergebnis haben Sie das nächste Bild

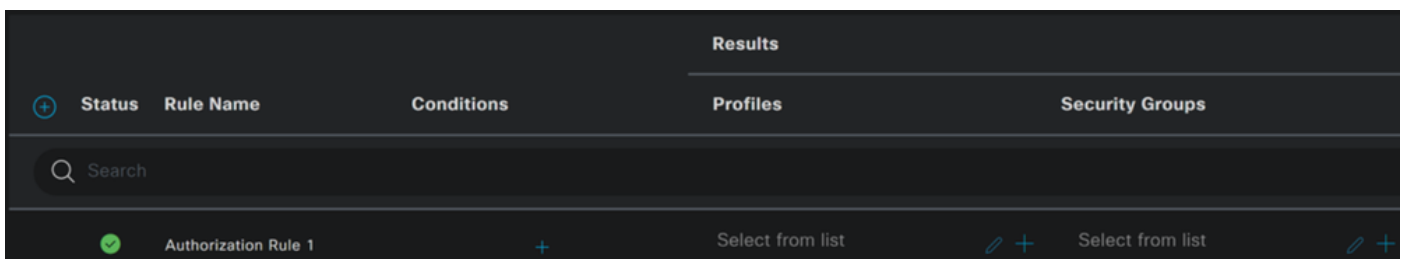


- Wählen Sie unter **Profile** Klicken Sie unter der Dropdown-Schaltfläche das auf dem Schritt konfigurierte Autorisierungsprofil für die Beschwerde aus: [Compliant Authorization Profile](#)



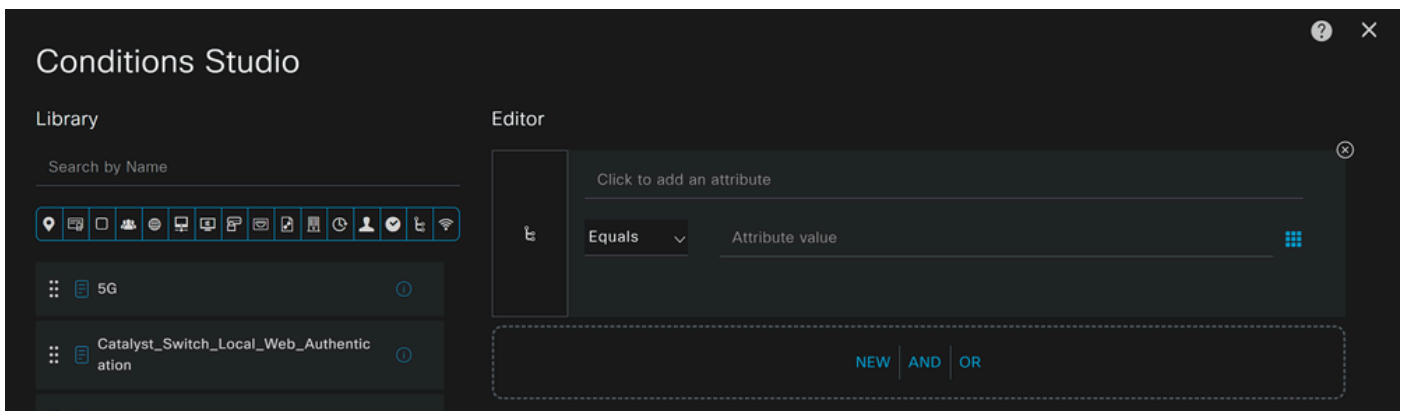
Jetzt haben Sie die konfiguriert **Compliance Policy Set**.

- Klicken Sie auf, + um die **CSA-Unknown-Compliance** Richtlinie zu definieren:

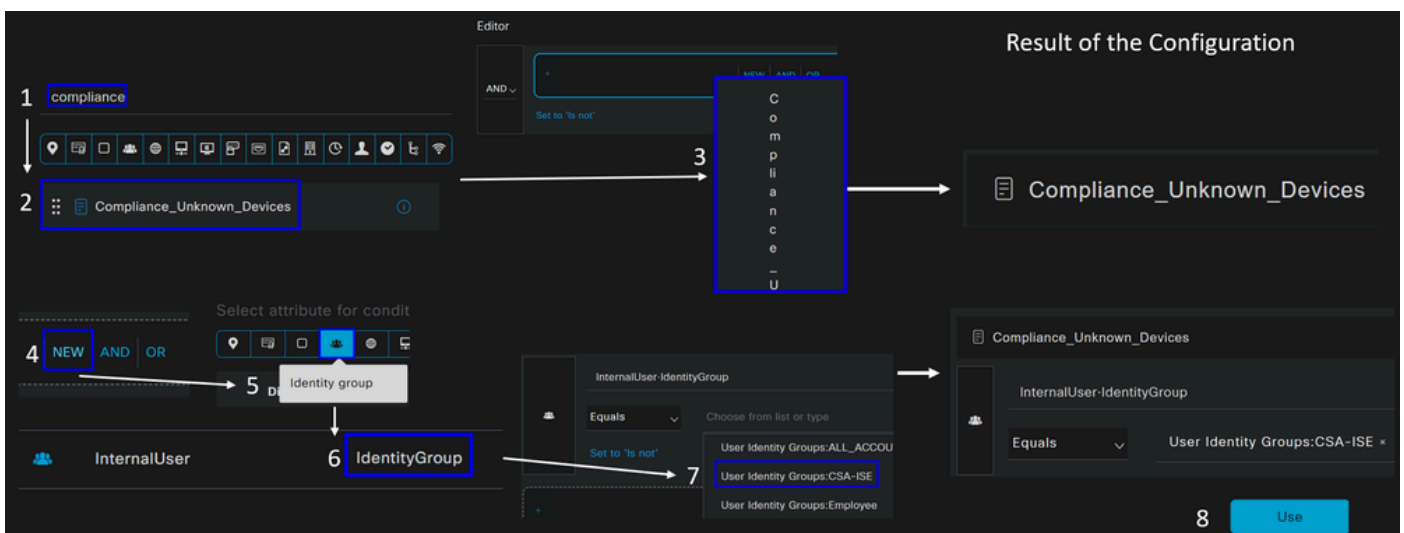


- Im nächsten Schritt ändern Sie das Rule Name, Conditions und Profiles
- Wenn Sie einen Namen **Name** konfigurieren auf **CSA-Unknown-Compliance**

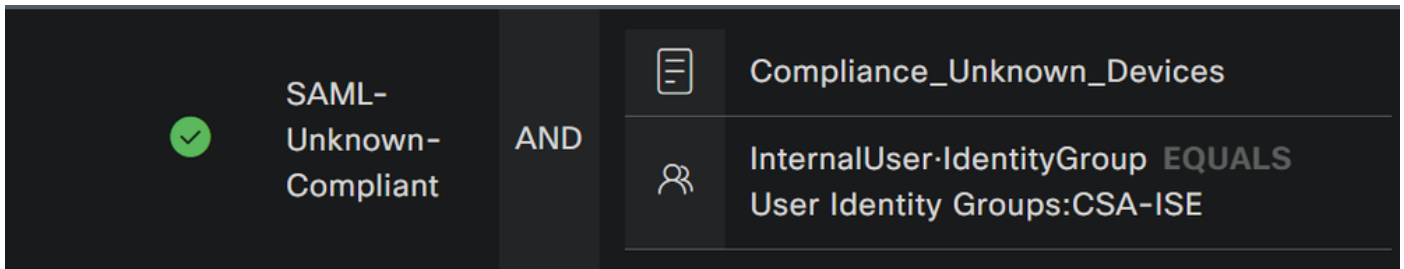
- Um das zu konfigurieren, **Condition** klicken Sie auf die Schaltfläche +
- Unter **Condition Studio** finden Sie die Informationen:



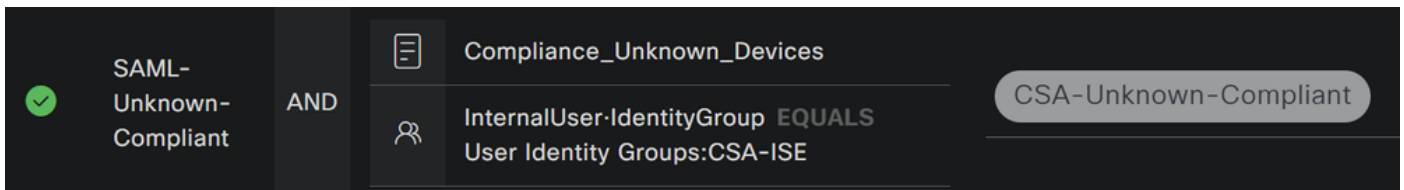
- Um die Bedingung zu erstellen, suchen Sie nach **compliance**
- Sie müssen Folgendes anzeigen: **Compliant_Unknown_Devices**
- Drag & Drop unter dem **Editor**
- Klicken Sie unter Editor in **New**
- Klicken Sie auf das **Identity Group** Symbol
- Auswählen **Internal User Identity Group**
- Wählen **Equals** Sie unter die **User Identity Group** passende aus.
- Klicken Sie auf **Use**



- Als Ergebnis haben Sie das nächste Bild

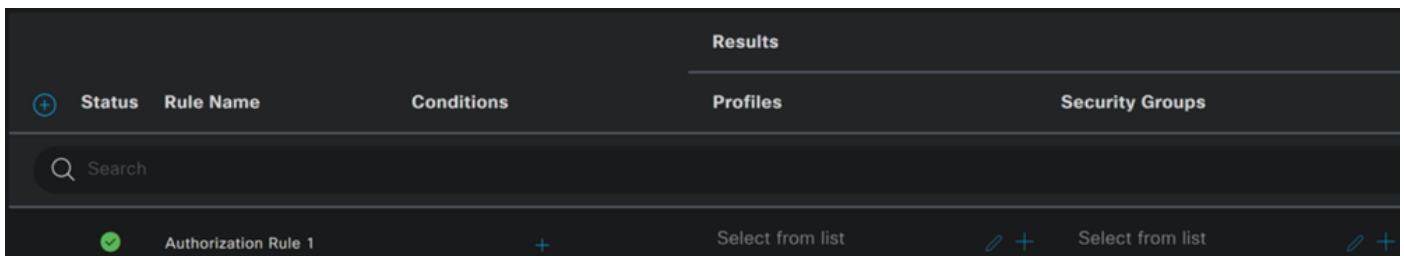


- Klicken Sie unter der Dropdown-Schaltfläche auf **Profile** und wählen Sie das auf dem Schritt konfigurierte Autorisierungsprofil für die Beschwerde aus: [Unknown Compliant Authorization Profile \(Unbekanntes konformes Autorisierungsprofil\)](#)



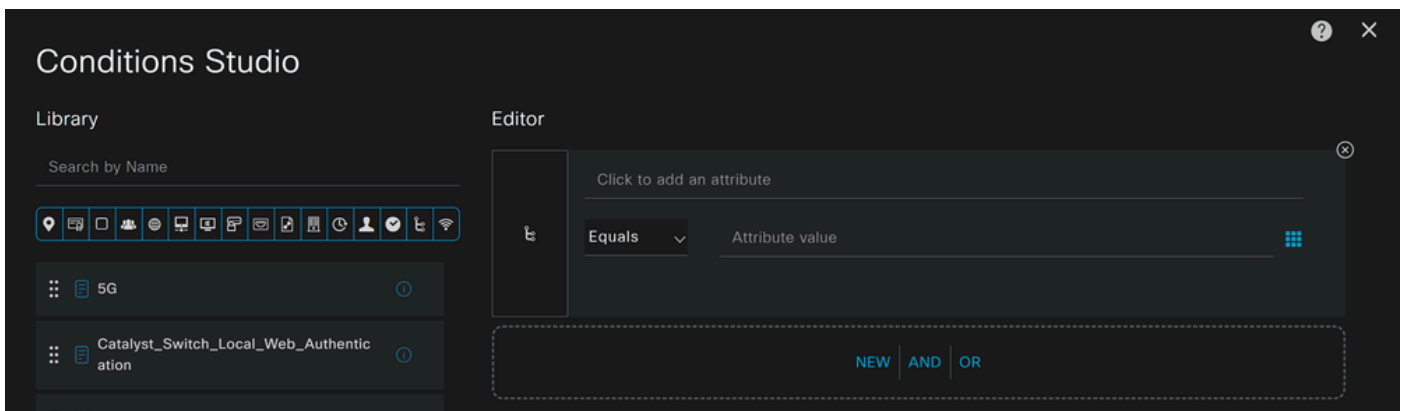
Jetzt haben Sie die konfiguriert **Unknown Compliance Policy Set**.

- Klicken Sie auf, + um die **CSA- Non-Compliant** Richtlinie zu definieren:

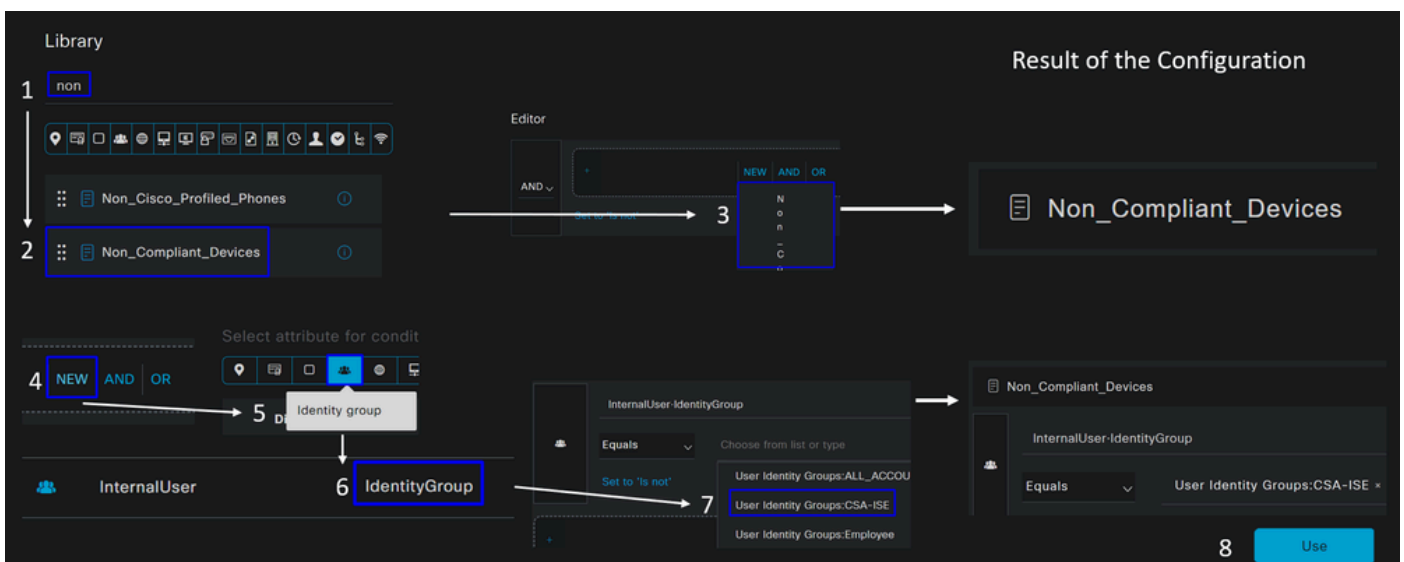


- Im nächsten Schritt ändern Sie das Rule Name, Conditions und Profiles
- Wenn Sie einen Namen **Name** konfigurieren auf **CSA-Non-Compliance**

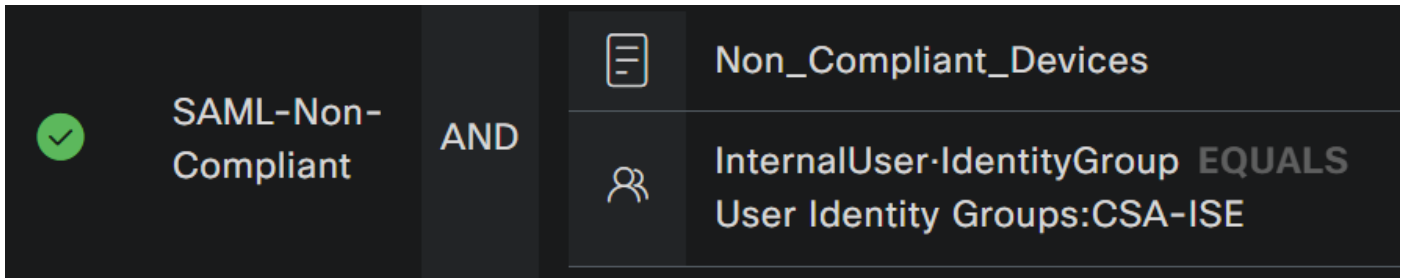
- Um das zu konfigurieren, **Condition** klicken Sie auf die Schaltfläche +
- Unter **Condition Studio** finden Sie die Informationen:



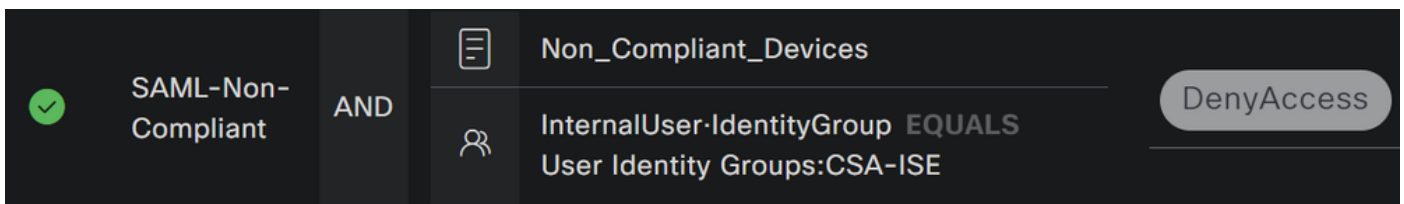
- Um die Bedingung zu erstellen, suchen Sie nach **non**
- Sie müssen Folgendes anzeigen: **Non_Compliant_Devices**
- Drag & Drop unter dem **Editor**
- Klicken Sie unter Editor in **New**
- Klicken Sie auf das **Identity Group** Symbol
- Auswählen **Internal User Identity Group**
- Wählen **Equals** Sie unter die **User Identity Group** passende aus.
- Klicken Sie auf **Use**



- Als Ergebnis haben Sie das nächste Bild



- Klicken Sie unter **Profile** dem Dropdown-Menü auf das Profil für die Autorisierung der Beschwerde. **DenyAccess**



Wenn Sie die Konfiguration der drei Profile abgeschlossen haben, können Sie die Integration mit dem Status testen.

Überprüfung


Statusüberprüfung

Verbindung am Rechner

Stellen Sie über Secure Client eine Verbindung zu Ihrer FQDN RA-VPN-Domäne bei sicherem Zugriff her.

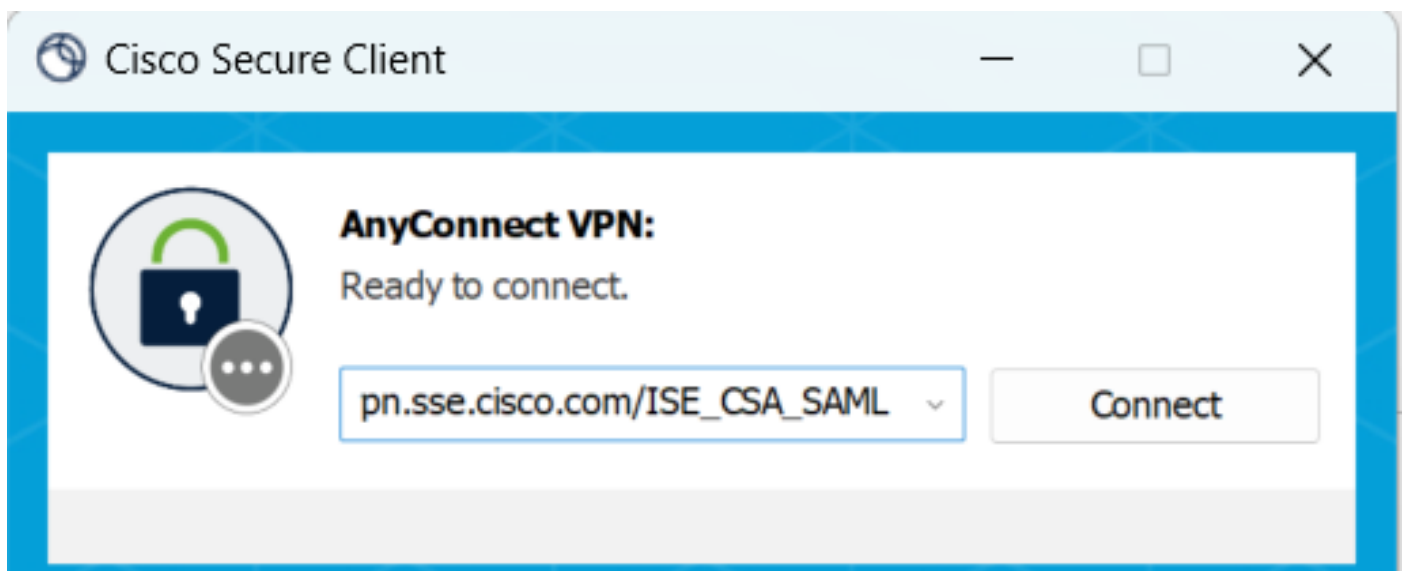
Identity	Authentication Policy	Authorization Policy	Authorization Profiles	Posture Status
#ACISACL-IP-CSA-Compliant-640b0b0a				
vphuser@cisconet.it	CSA-ISE	CSA-ISE => SAML-Compliant	CSA-Compliant	Compliant
vphuser@cisconet.it	CSA-ISE	CSA-ISE => SAML-Compliant	CSA-Compliant	Compliant
#ACISACL-IP-CSA_Redirect_To_ISE-640744f				
vphuser@cisconet.it	CSA-ISE	CSA-ISE => SAML-Unknown...	CSA-Unknown-Compliant	Pending

1. Authorization Step = Unknown Compliance
5236 Authorize-Only succeeded
2. Download CSA_Redirect_To_ISE DACL
5232 DACL Download Succeeded
3. Posture Status Is verified on the machine
4. Authorization Step - CSA-Compliant
5205 Dynamic Authorization succeeded
5. Download CSA-Compliant
5232 DACL Download Succeeded

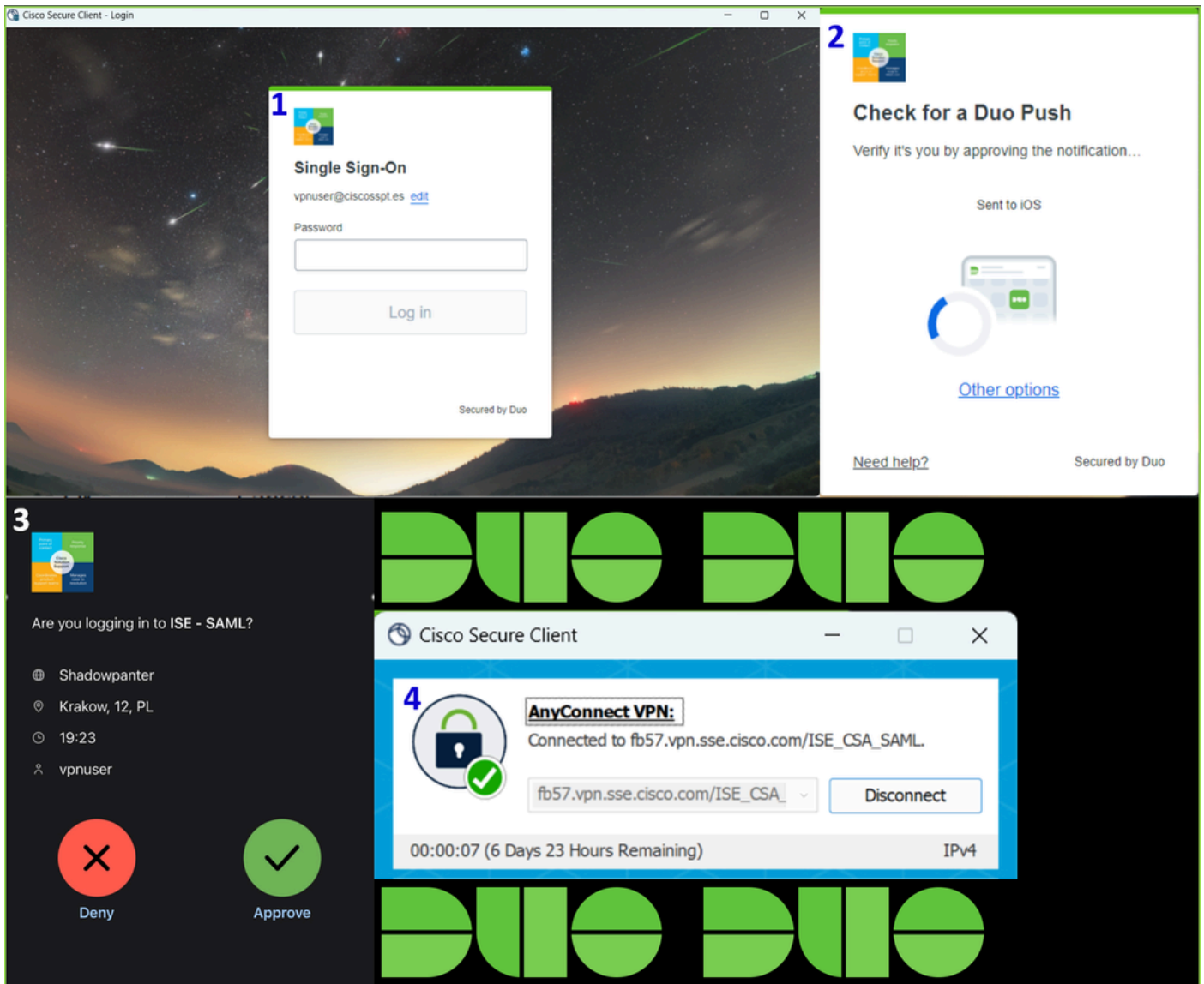


Hinweis: Für diesen Schritt muss kein ISE-Modul installiert werden.

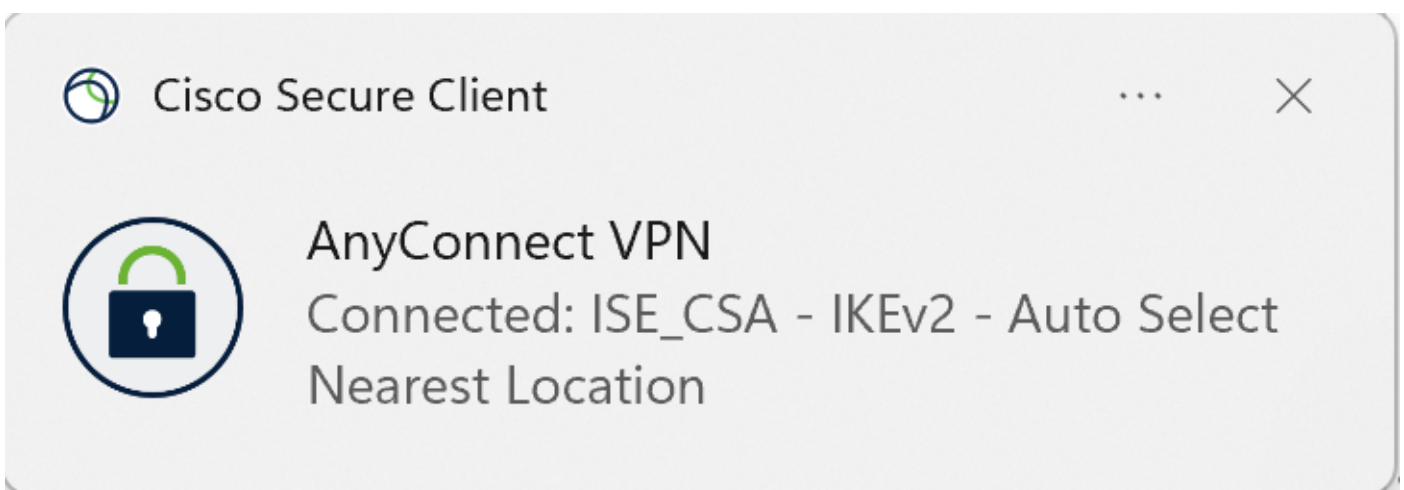
1. Verbindung über Secure Client herstellen.

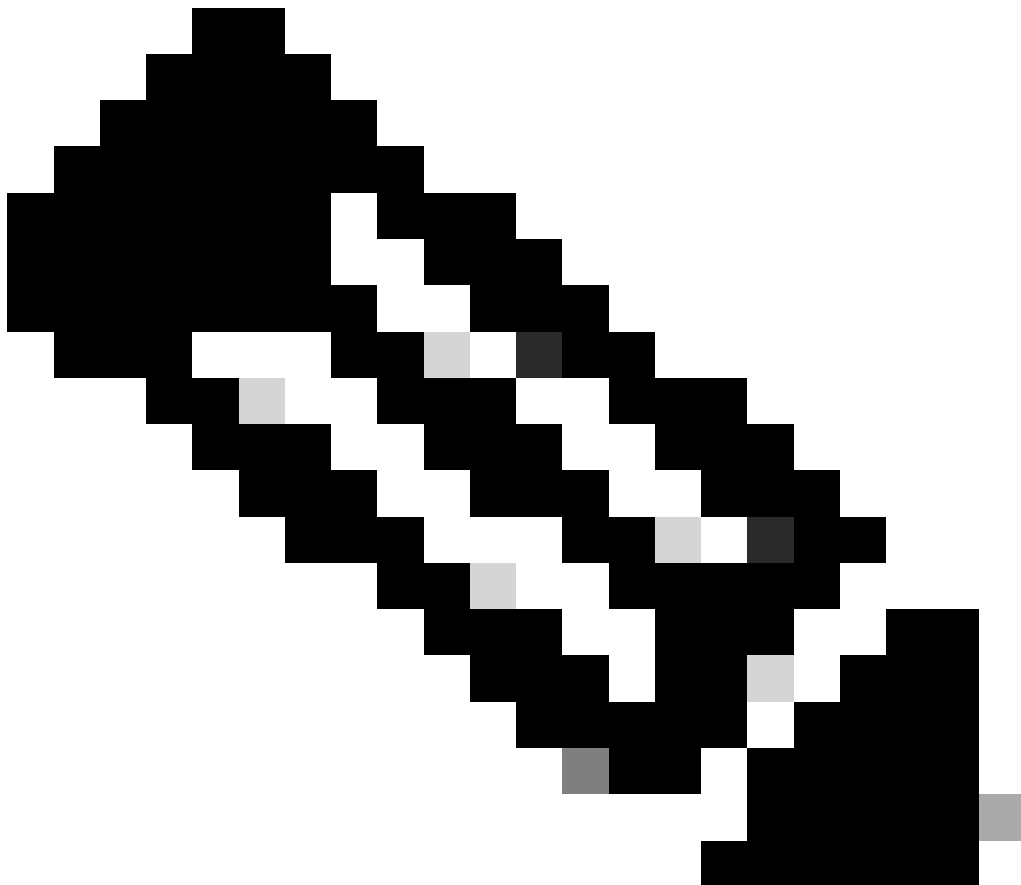
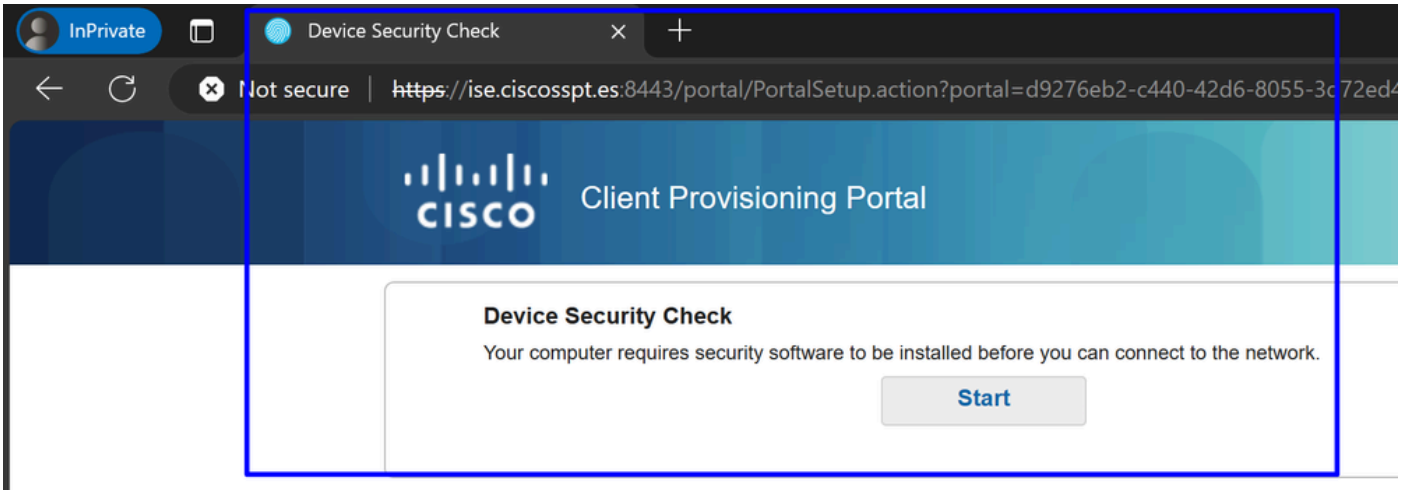


2. Geben Sie die Anmeldeinformationen für die Authentifizierung über Duo an.



3. An diesem Punkt werden Sie mit dem VPN verbunden, und meistens werden Sie wahrscheinlich zur ISE umgeleitet; wenn nicht, können Sie versuchen, zu navigieren **http:1.1.1.1**.





Hinweis: An diesem Punkt fallen Sie unter die Autorisierung - Richtlinienset [CSA-Unknown-Compliance](#), da Sie den ISE Posture

Agent nicht auf dem Computer installiert haben, und Sie werden zum ISE-Bereitstellungsportal umgeleitet, um den Agenten zu installieren.

4. Klicken Sie auf Start, um mit der Agentenbereitstellung fortzufahren.

Device Security Check

Your computer requires security software to be installed before you can connect to the network.

9 Detecting if Agent is installed and running...

5. Klicken Sie auf + **This is my first time here**.

Device Security Check

Your computer requires security software to be installed before you can connect to the network.

Unable to detect Posture Agent



+ This is my first time here



+ Remind me what to do next

6. Klicken Sie **Click here to download and install agent**



+ This is my first time here

1. You must install Agent to check your device before accessing the network. [Click here to download and install Agent](#)
2. After installation, Agent will automatically scan your device before allowing you access to the network.
3. You have 4 minutes to install and for the system scan to complete.

Tip: Leave Agent running so it will automatically scan your device and connect you faster next time you access this network.



You have 4 minutes to install and for the compliance check to complete

7. Installieren Sie den Agenten

Downloads



cisco-secure-client-ise...aBf8STpS5Nr1nzotleQ.exe

[Open file](#)

See more



Network Setup Assistant



Installation is completed.

Quit

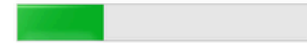
(c) 2022-2024 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc and/or its affiliates in the U.S. and certain other countries.

8. Nach der Installation des Agenten beginnt die ISE-Statusüberprüfung mit der Überprüfung des aktuellen Systemstatus. Wenn die Richtlinienanforderungen nicht erfüllt werden, wird ein Popup-Fenster angezeigt, das Sie auf die Einhaltung der Richtlinien hinweist.



ISE Posture

1 Update(s) Required



30%

Time Remaining:

3 Minutes



Action Required to Enable Access

Updates are needed on your device before you can join the network.

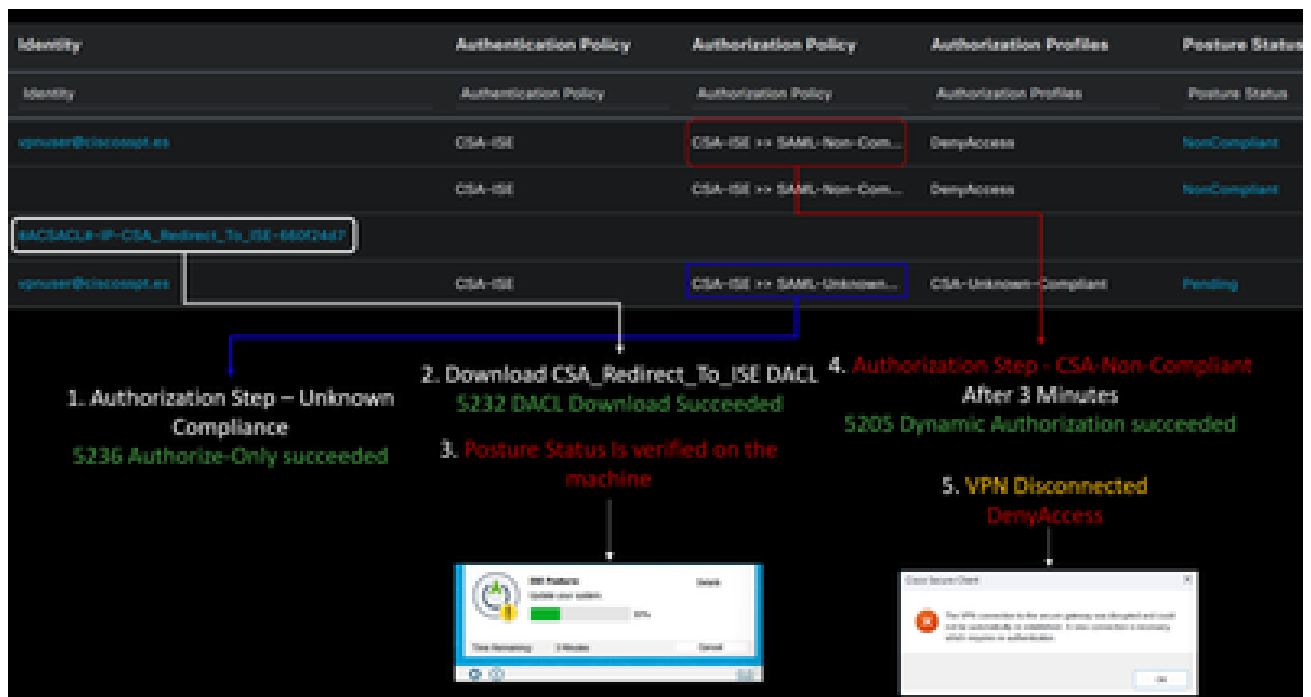
This endpoint has failed to check. Please ask your network administrator to install a Secure Endpoint.

Start

More Details

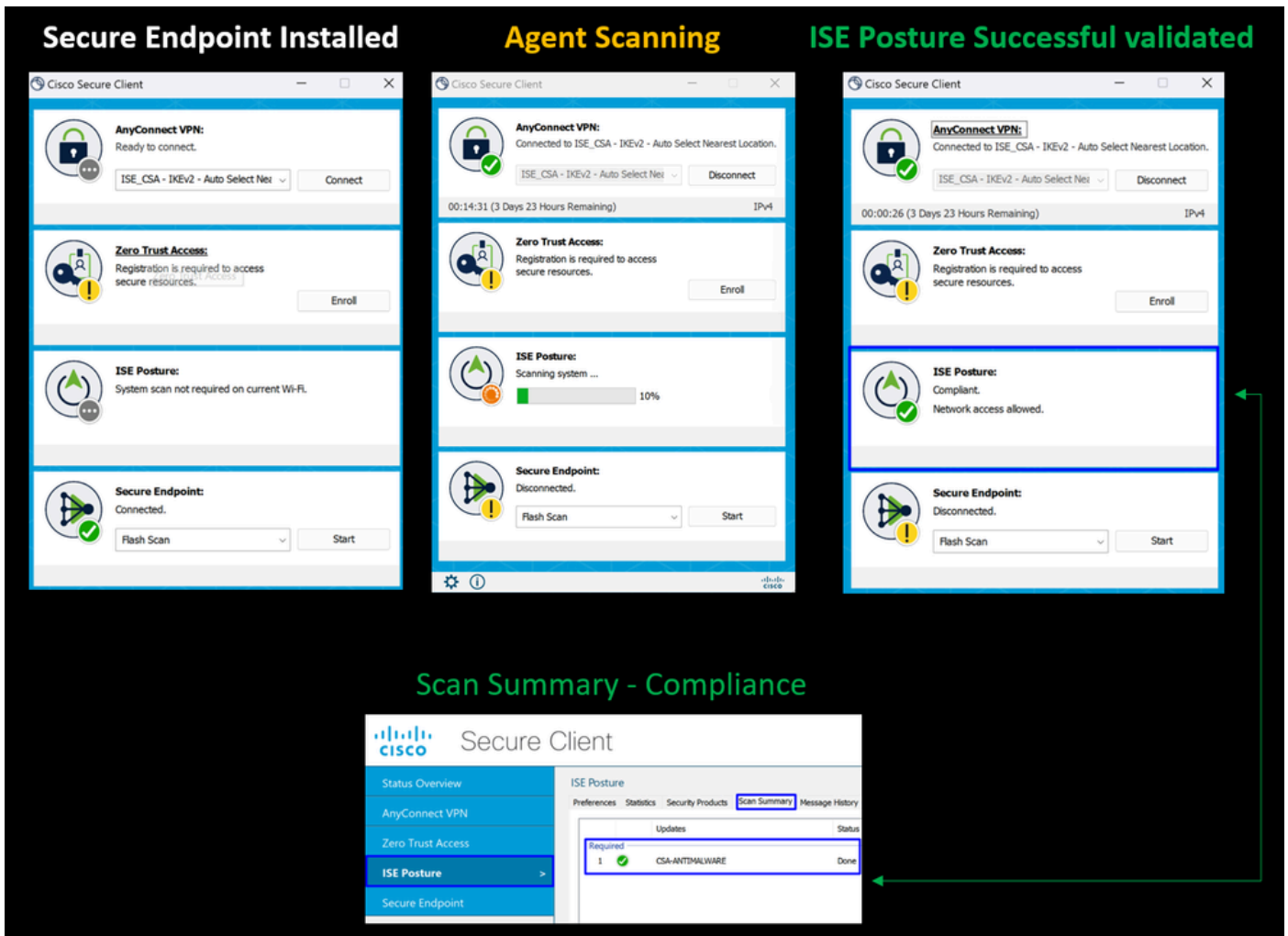


Cancel

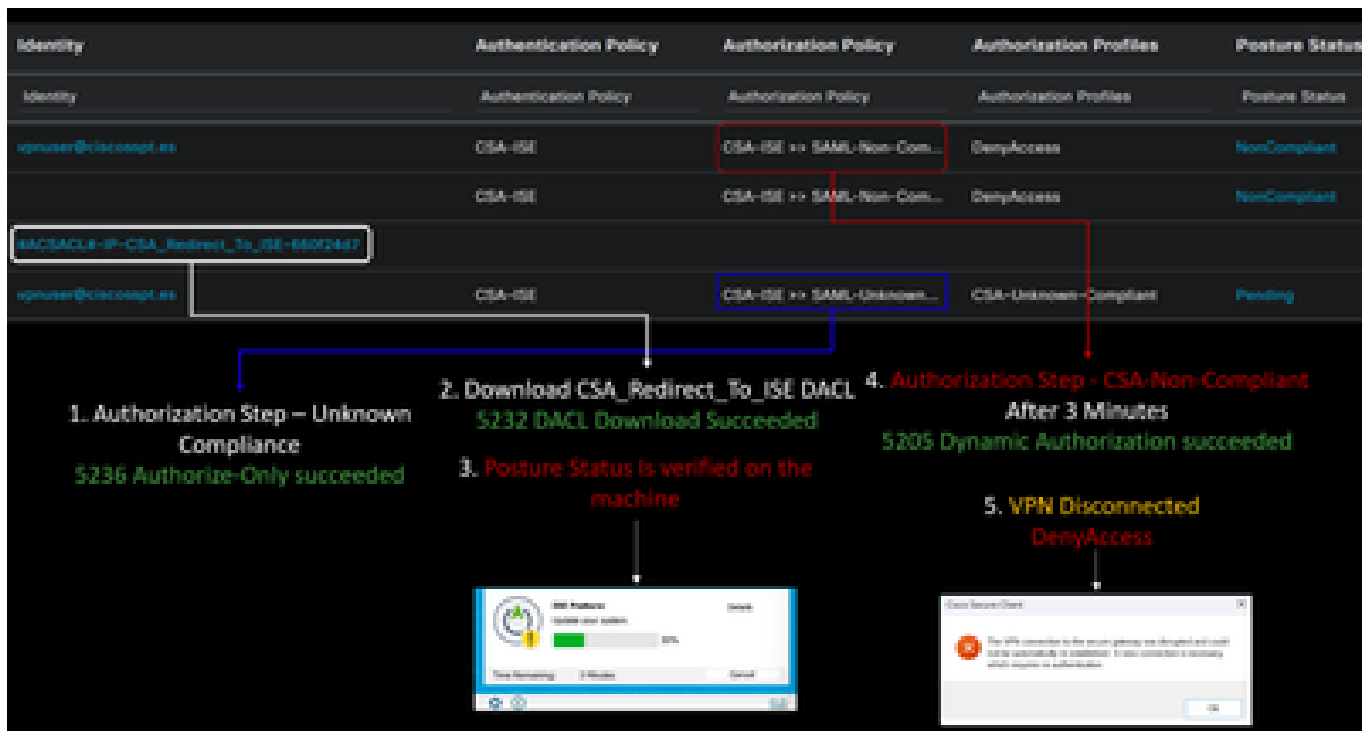


Hinweis: Wenn Sie Cancel oder die verbleibende Zeit endet, werden Sie automatisch nicht konform, fallen unter den Autorisierungsrichtliniensatz [CSA-Non-Compliance](#) und werden sofort vom VPN getrennt.

9. Installieren Sie den Secure Endpoint Agent, und stellen Sie erneut eine Verbindung mit dem VPN her.



10. Nachdem der Agent überprüft hat, dass der Computer die Anforderungen erfüllt, ändert sich Ihr Status, sodass er eine Beschwerde auslöst und Zugriff auf alle Ressourcen im Netzwerk erhält.



Hinweis: Sobald die [CSA-Konformität](#) für Sie erreicht ist, unterliegen Sie der Autorisierungsrichtlinie, und Sie haben sofort Zugriff auf alle Netzwerkressourcen.

So überprüfen Sie die Protokolle in der ISE

Um das Authentifizierungsergebnis für einen Benutzer zu überprüfen, gibt es zwei Beispiele für Compliance und Nichtkonformität. Um es in der ISE zu überprüfen, befolgen Sie die folgenden Anweisungen:

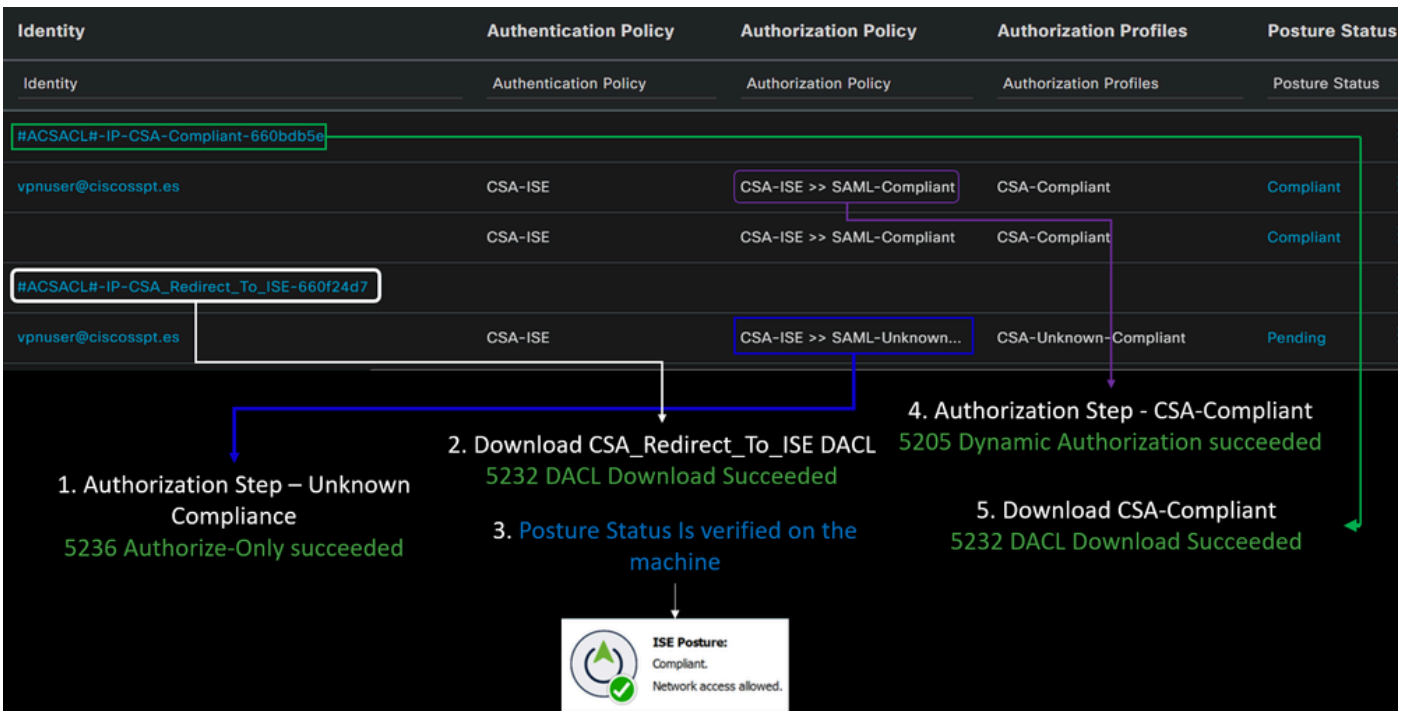
- Rufen Sie Ihr ISE Dashboard auf.
- Klicken Sie Operations > Live Logs

Misconfigured Suppliants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Counter
0	0	0	0	0

Status	Details	Identity	Authentication Policy	Authorization Policy	Authorization Profiles	Posture
		Identity	Authentication Policy	Authorization Policy	Authorization Profiles	Posture
i		vpnuser@ciscospt.es	CSA-ISE	CSA-ISE >> SAML-Non-Com...	DenyAccess	NonCom
✓		#ACSACL#-IP-CSA_Redirect_To_ISE-660f24d7	CSA-ISE	CSA-ISE >> SAML-Non-Com...	DenyAccess	NonCom
✓		vpnuser@ciscospt.es	CSA-ISE	CSA-ISE >> SAML-Unknown...	CSA-Unknown-Compliant	Pending
✓		#ACSACL#-IP-CSA-Compliant-660bdb5e	CSA-ISE	CSA-ISE >> SAML-Compliant	CSA-Compliant	Complia
✓		#ACSACL#-IP-CSA_Redirect_To_ISE-660f24d7	CSA-ISE	CSA-ISE >> SAML-Compliant	CSA-Compliant	Complia

Das nächste Szenario zeigt, wie erfolgreiche Compliance- und Nicht-Compliance-Ereignisse angezeigt werden unter **Live Logs**:

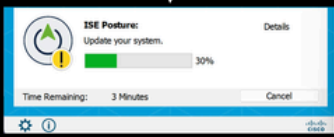

Einhaltung



Nichteinhaltung

Identity	Authentication Policy	Authorization Policy	Authorization Profiles	Posture Status
vpnuser@ciscospt.es	CSA-ISE	CSA-ISE >> SAML-Non-Com...	DenyAccess	NonCompliant
vpnuser@ciscospt.es	CSA-ISE	CSA-ISE >> SAML-Non-Com...	DenyAccess	NonCompliant
#ACSACL#-IP-CSA_Redirect_To_ISE-660f24d7				
vpnuser@ciscospt.es	CSA-ISE	CSA-ISE >> SAML-Unknown...	CSA-Unknown-Compliant	Pending

1. Authorization Step – Unknown Compliance
5236 Authorize-Only succeeded
2. Download CSA_Redirect_To_ISE DACL
5232 DACL Download Succeeded
3. Posture Status Is verified on the machine
4. Authorization Step - CSA-Non-Compliant After 3 Minutes
5205 Dynamic Authorization succeeded
5. VPN Disconnected DenyAccess

Erste Schritte mit sicherem Zugriff und ISE-Integration

Im nächsten Beispiel befindet sich die Cisco ISE unter dem Netzwerk 192.168.10.0/24, und die Konfiguration der Netzwerke, die über den Tunnel erreichbar sind, muss unter der Tunnelkonfiguration hinzugefügt werden.

Step 1: Überprüfen Sie Ihre Tunnelkonfiguration:

Navigieren Sie zu Ihrem [Secure Access Dashboard](#), um dies zu überprüfen.

- Klicken Sie **Connect > Network Connections**
- Klicken Sie auf **Network Tunnel Groups > Ihr Tunnel**

HomeFTD	Connected	Europe (Germany)	sse-euc-1-1-0	1	sse-euc-1-1-1
---------	-----------	------------------	---------------	---	---------------

- Prüfen Sie unter Zusammenfassung, ob der Tunnel den Adressraum konfiguriert hat, in dem sich Ihre Cisco ISE befindet:

Summary



Connected

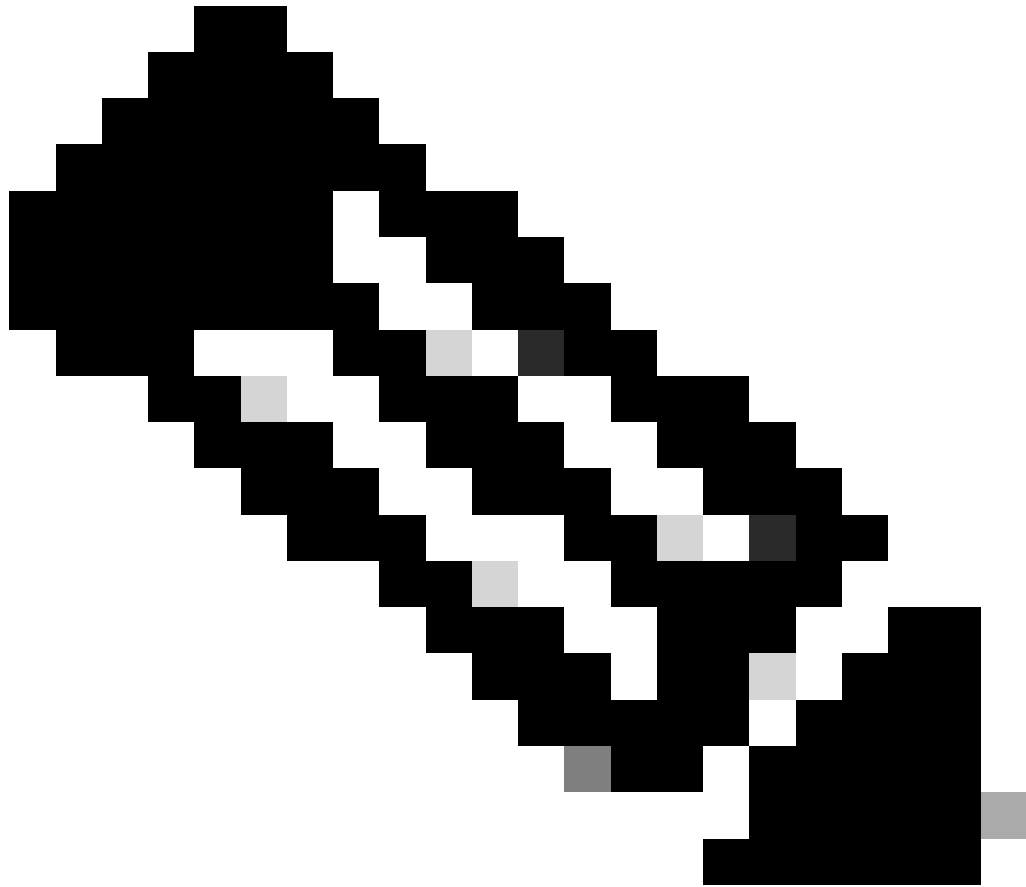
Region	Europe (Germany)
Device Type	FTD
Routing Type	Static Routing
IP Address Range	192.168.10.0/24
Last Status Update	Mar 19, 2024 11:13 AM

Step 2: Den Verkehr auf Ihrer Firewall zulassen.

Damit Secure Access das ISE-Gerät für die Radius-Authentifizierung verwenden kann, müssen Sie eine Regel von Secure Access für Ihr Netzwerk mit den erforderlichen Radius-Ports konfiguriert haben:

Regel	Quelle	Ziel	Zielport
ISE für sicheren Zugriff Management-Pool	ISE-Server	Management-IP-Pool (RA-VPN)	KAO UDP 1700 (Standard-Port)
Sicherer Access Management-IP-Pool zur ISE	Management-IP-Pool	ISE-Server	Authentifizierung, Autorisierung UDP 1812 (Standard-Port) Buchhaltung UDP 1813 (Standard-Port)
IP-Pool für sicheren Zugriff auf ISE	Endpunkt-IP-Pool	ISE-Server	Bereitstellungsportal TCP 8443 (Standard-Port)
IP-Pool für sicheren Zugriff auf DNS-SERVER	Endpunkt-IP-Pool	DNS-Server	DNS UDP und TCP 53

--	--	--	--



Hinweis: Weitere Informationen zu ISE-Ports finden Sie im [Benutzerhandbuch - Port-Referenz](#).





Hinweis: Wenn Sie Ihre ISE so konfiguriert haben, dass sie über einen Namen wie ise.ciscospt.es erkannt wird, ist eine DNS-Regel erforderlich.

Management-Pool und Endpunkt-IP-Pools

Um Ihren Management- und Endpunkt-IP-Pool zu überprüfen, navigieren Sie zu Ihrem [Secure Access Dashboard](#):

- Klicken Sie **Connect > End User Connectivity**
- Klicken Sie Virtual Private Network

- Unter **Manage IP Pools**
- Klicken Sie **Manage**

EUROPE						1	^
Pop Name	Display Name	Endpoint IP Pools	Management IP Pools	DNS Servers	RADIUS Groups		
Europe (Germany)	RA VPN 1	192.168.50.0/24 256 user connections	192.168.60.0/24 256 user connections	House	ISE_CSA		 

Schritt 3: Überprüfen der ISE-Konfiguration unter "Private Resources" (Private Ressourcen)

Damit die Benutzer, die über das VPN verbunden sind, zu navigieren **ISE Provisioning Portal** können, müssen Sie das Gerät als private Ressource konfiguriert haben, die den Zugriff ermöglicht. Damit wird die automatische Bereitstellung des Geräts über das VPN ermöglicht ISE Posture Module.

Um zu überprüfen, ob ISE korrekt konfiguriert ist, navigieren Sie zu Ihrem [Secure Access Dashboard](#):

- Klicken Sie **Resources > Private Resources**
- Klicken Sie auf die ISE-Ressource

Private Resource Name

CiscoISE

Description (optional)

Communication with Secure Access Cloud

Specify one or more addresses that will be used for communication between this resource and Secure Access. Secure Access will route traffic to this address.

[Help](#)

Internally reachable address

(FQDN, Wildcard FQDN, IP Address, CIDR)



Protocol

Port / Ranges

192.168.10.206

TCP - (HTTP/HTTPS)

Any

[+ Protocol & Port](#)

[+ IP Address or FQDN](#)

VPN connections

Allow endpoints to connect to this resource when connected to the network using VPN.

Bei Bedarf können Sie die Regel auf den Bereitstellungsportal-Port (8443) beschränken.



Hinweis: Stellen Sie sicher, dass Sie das Kontrollkästchen für VPN-Verbindungen aktiviert haben.

Schritt 4: Zulassen des ISE-Zugriffs gemäß der Zugriffsrichtlinie

Damit die Benutzer, die über das VPN verbunden sind, zu navigieren **ISE Provisioning Portal** können, müssen Sie sicherstellen, dass Sie eine konfiguriert haben, **Access Policy** damit die Benutzer, die unter dieser Regel konfiguriert sind, auf die in konfigurierte private Ressource zugreifen könnenStep3.

Um zu überprüfen, ob ISE korrekt konfiguriert ist, navigieren Sie zu Ihrem [Secure Access Dashboard](#):



- Klicken Sie **Secure > Access Policy**

- Klicken Sie auf die konfigurierte Regel, um den Zugriff für die VPN-Benutzer auf die ISE zuzulassen.

1 Specify Access

Specify which users and endpoints can access which resources. [Help](#)


Action

 Allow Allow specified traffic if security requirements are met.	 Block Block specified traffic.
-------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------


From Specify one or more sources . <input type="text" value="CSA (ciscospt.es\CSA)"/>	To Specify one or more destinations . <input type="text" value="CiscoISE"/>
Information about sources, including selecting multiple sources. Help	Information about destinations, including selecting multiple destinations. Help

Endpoint Requirements

For VPN connections:

 End-user endpoint devices that are connected to the network using VPN may be able to access destinations specified in this rule. [ⓘ](#)
Endpoint requirements are configured in the VPN posture profile. Requirements are evaluated at the time the endpoint device connects to the network. [VPN Posture Profiles](#)

For Branch connections:

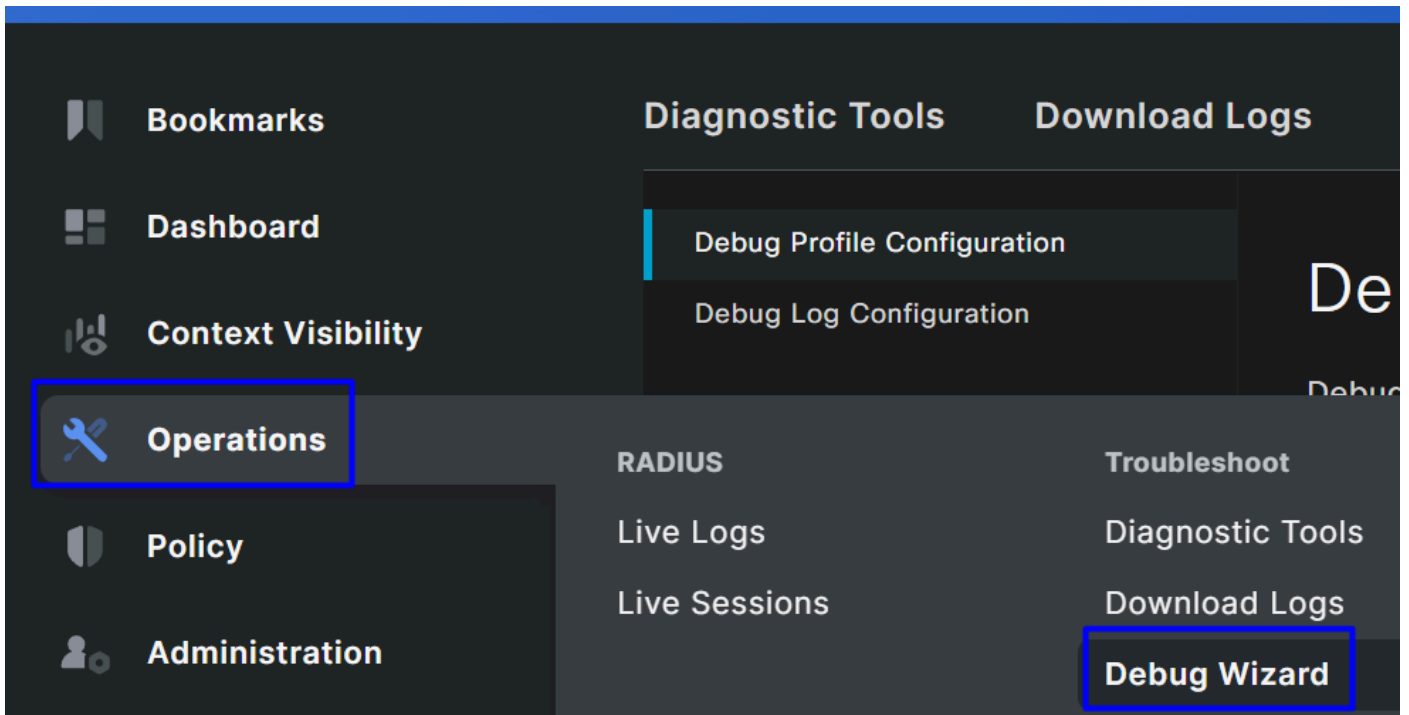
 Endpoint device posture is not evaluated for endpoints connecting to these resources from a branch network.

Fehlerbehebung

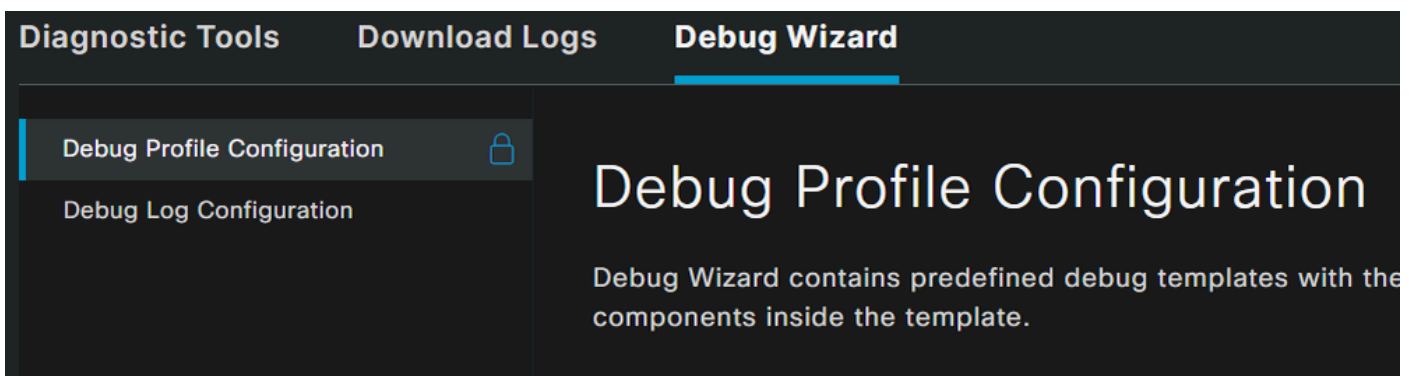
Herunterladen von ISE Posture Debug-Protokollen

So laden Sie ISE-Protokolle herunter, um ein Statusproblem zu überprüfen:

- Rufen Sie Ihr ISE Dashboard auf.
- Klicken Sie Operations > Troubleshoot > Debug Wizard



- Klicken Sie Debug Profile Configuration



- Aktivieren Sie das Kontrollkästchen für **Posture > Debug Nodes**



Add



Edit



Remove 2



Debug Nodes



Name

Des



802.1X/MAB

802



Active Directory

Acti



Application Server Issues

App



BYOD portal/Onboarding

BYO



Context Visibility

Con



Guest portal

Gue



Licensing

Lice



MnT

MnT

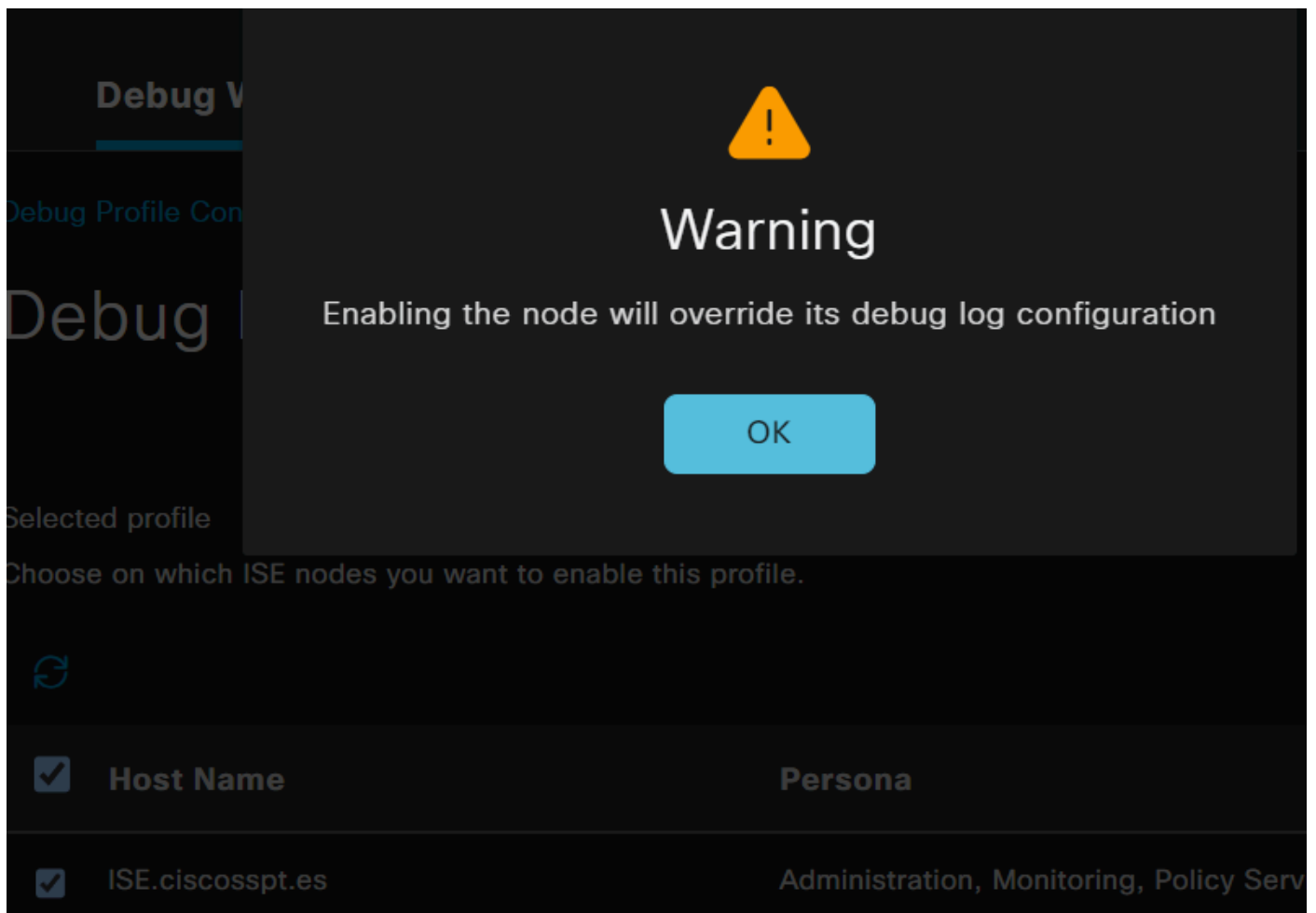
1



Posture

Pos

- Aktivieren Sie das Kontrollkästchen für die ISE-Knoten, auf denen Sie den Debugmodus aktivieren möchten, um das Problem zu beheben.



The image shows a warning dialog box overlaid on a configuration page. The dialog box has a yellow warning triangle icon and the text: "Warning", "Enabling the node will override its debug log configuration", and an "OK" button. The background page is titled "Debug V" and "Debug Profile Con". It includes a section "Selected profile" and a heading "Choose on which ISE nodes you want to enable this profile." Below this is a table with two columns: "Host Name" and "Persona". The first row has a checked checkbox, "Host Name", and "Persona". The second row has a checked checkbox, "ISE.ciscosspt.es", and "Administration, Monitoring, Policy Serv".

Host Name	Persona
<input checked="" type="checkbox"/>	Persona
<input checked="" type="checkbox"/> ISE.ciscosspt.es	Administration, Monitoring, Policy Serv

- Klicken Sie auf Save

Debug Nodes

Selected profile Posture

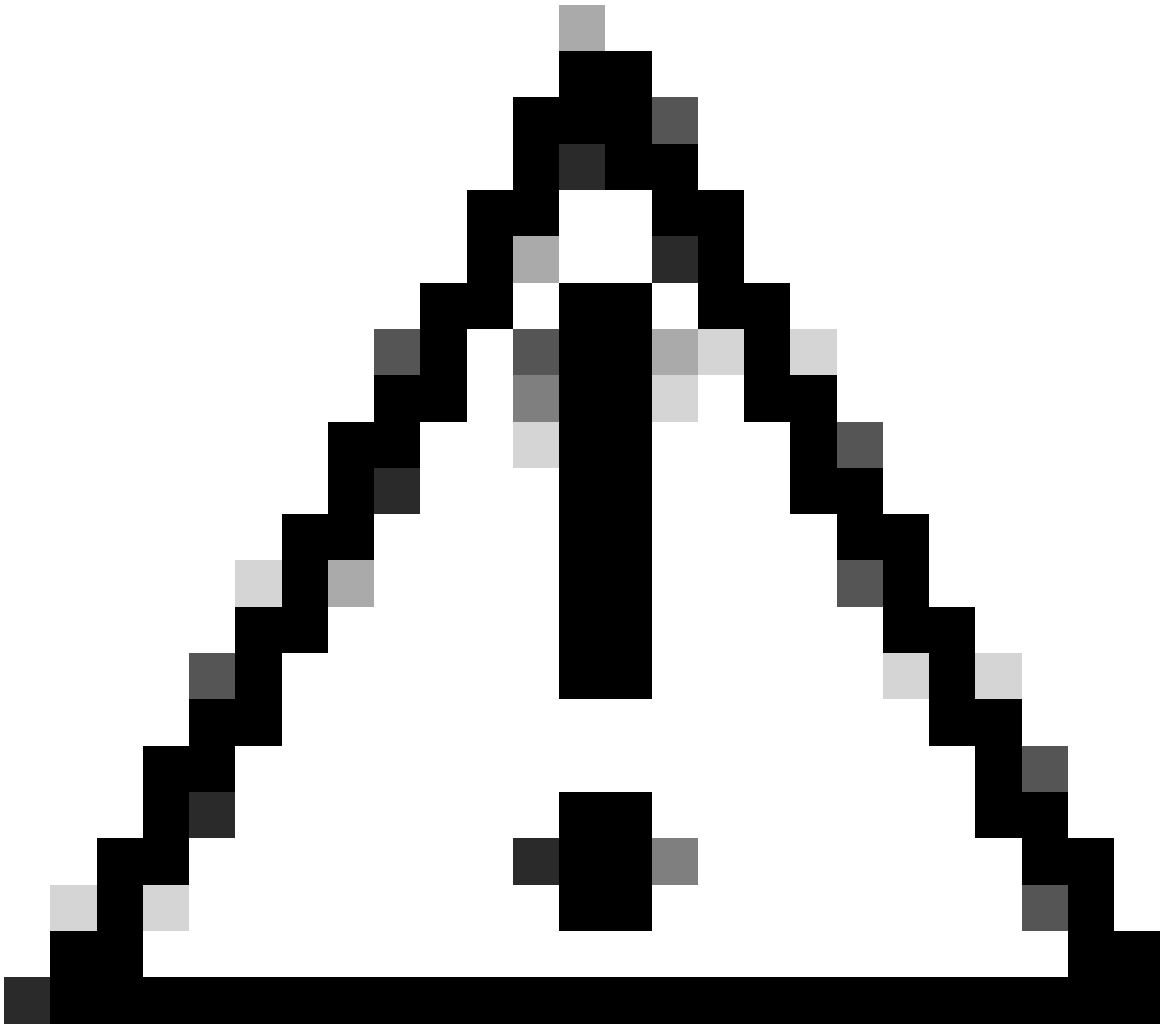
Choose on which ISE nodes you want to enable this profile.

 Filter  

<input checked="" type="checkbox"/> Host Name	Persona	Role
<input checked="" type="checkbox"/> ISE.ciscosppt.es	Administration, Monitoring, Policy Service	STANDALONE

Cancel

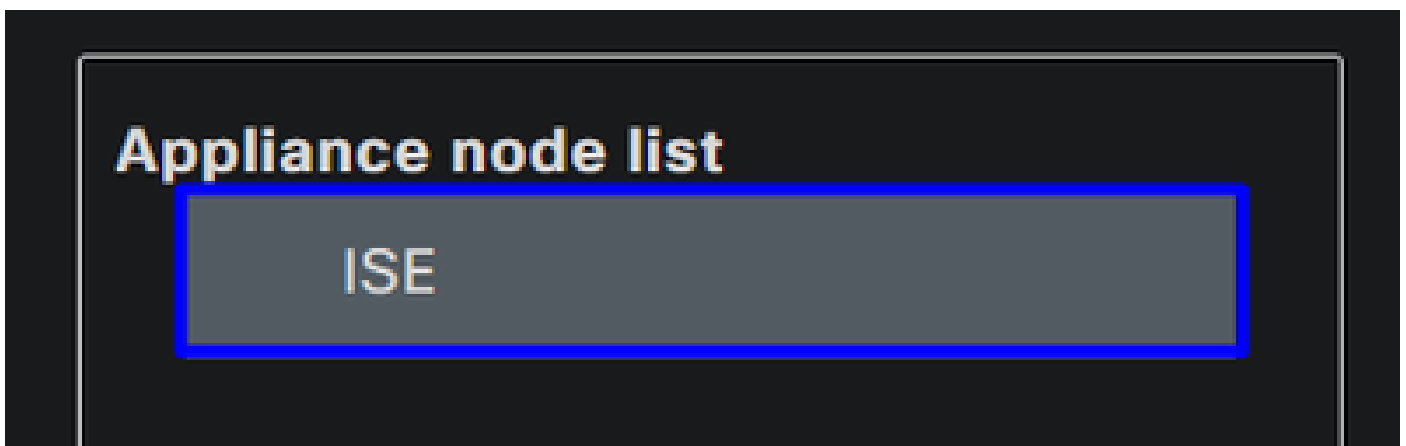
Save



Vorsicht: Nach diesem Punkt müssen Sie anfangen, das Problem zu reproduzieren; **the debug logs can affect the performance of your device.**

Wenn Sie das Problem reproduziert haben, fahren Sie mit den folgenden Schritten fort:

- Klicken Sie Operations > Download Logs
- Wählen Sie den Knoten aus, von dem Sie die Protokolle übernehmen möchten.



- Wählen Sie unter **Support Bundle** den folgenden Optionen aus:

Support Bundle

Debug Logs

- Include full configuration database ⓘ
- Include debug logs ⓘ
- Include local logs ⓘ
- Include core files ⓘ
- Include monitoring and reporting logs ⓘ
- Include system logs ⓘ
- Include policy configuration ⓘ
- Include policy cache ⓘ

From Date

(mm/dd/yyyy)

To Date

(mm/dd/yyyy)

* Note: Output from the 'show tech-support' CLI command will be included along with the selected entries.

Support Bundle - Encryption

- Public Key Encryption ⓘ
- Shared Key Encryption ⓘ

* Encryption key ⓘ

* Re-Enter Encryption key

Create Support Bundle

- Include debug logs
- Unter **Support Bundle Encryption**
 - **Shared Key Encryption**
 - Füllen **Encryption key** und **Re-Enter Encryption key**

- Klicken Sie auf **Create Support Bundle**
- Klicken Sie auf **Download**

Support Bundle - Last Generated

File Name: ise-support-bundle-ISE-admin-04-04-2024-14-27.tar.gpg

Time: Thu, 04 Apr 2024 14:35:35 UTC

Size(KB): 52165.0

[Download](#)

[Delete](#)


















Warnung: Deaktivieren Sie den Debug-Modus, der im Schritt "[Debug Profile Configuration](#)" aktiviert ist.

So überprüfen Sie Protokolle für den sicheren Zugriff auf Remote-Zugriff

Navigieren Sie zu Ihrem Secure Access Dashboard:

- Klicken Sie Monitor > Remote Access Logs

100 Events

User	Connection Event	Event Details	Internal IP Address
 vpn user (vpnuser@ciscospt.es)	 Disconnected	User Requested	192.168.50.129
 vpn user (vpnuser@ciscospt.es)	 Disconnected	Unknown	192.168.50.130
 vpn user (vpnuser@ciscospt.es)	 Connected		192.168.50.130
 vpn user (vpnuser@ciscospt.es)	 Connected		192.168.50.129
 vpn user (vpnuser@ciscospt.es)	 Disconnected	User Requested	192.168.50.1
 vpn user (vpnuser@ciscospt.es)	 Disconnected	Unknown	192.168.50.1
 vpn user (vpnuser@ciscospt.es)	 Connected		192.168.50.1
<i>Unknown Identity</i>	 Failed	AUTHORIZATION-CHECK	

DART-Paket auf sicherem Client generieren

Überprüfen Sie den folgenden Artikel, um das DART-Paket auf Ihrem Computer zu generieren:

[Cisco Secure Client Diagnostic and Reporting Tool \(DART\)](#)



Hinweis: Nachdem Sie die im Abschnitt zur Fehlerbehebung angegebenen Protokolle gesammelt haben, öffnen Sie ein Ticket bei , TAC um mit der Analyse der Informationen fortzufahren.

Zugehörige Informationen

- [Technischer Support und Downloads von Cisco](#)
- [Secure Access-Dokumentation und Benutzerhandbuch](#)

- [Software-Download für Cisco Secure Client](#)
- [Administratorleitfaden für die Cisco Identity Services Engine, Version 3.3](#)

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.