

Konfigurieren der ISE 3.1-GUI-Admin-Anmeldung mithilfe der SAML-Integration mit Duo SSO und Windows AD

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Identitätsanbieter \(IdP\)](#)

[Service Provider](#)

[SAML](#)

[SAML-Assertion](#)

[Übergeordnetes Flussdiagramm](#)

[Konfigurieren der SAML SSO-Integration mit Duo SSO](#)

[Schritt 1: Konfigurieren von SAML-IDp auf der ISE](#)

[Konfigurieren von Duo SSO als externe SAML-Identitätsquelle](#)

[SAML-Metadaten-XML-Datei aus dem Duo-Administratorportal importieren](#)

[ISE-Authentifizierungsmethode konfigurieren](#)

[Erstellen einer Administratorgruppe](#)

[Erstellen einer RBAC-Richtlinie für die Administratorgruppe](#)

[Gruppenmitgliedschaft hinzufügen](#)

[SP-Informationen exportieren](#)

[Schritt 2: Konfigurieren von Duo SSO für ISE](#)

[Schritt 3: Integration der Cisco ISE mit Duo SSO als generischem SP](#)

[Überprüfung](#)

[Testen der Integration mit Duo SSO](#)

[Fehlerbehebung](#)

Einleitung

In diesem Dokument wird die Konfiguration der Cisco ISE 3.1 SAML SSO-Integration mit einem externen Identitätsanbieter wie Cisco Duo SSO beschrieben.

Voraussetzungen

Anforderungen

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

- Cisco Identity Services Engine (ISE) 3.1
- Grundlegende Kenntnisse über SAML-Bereitstellungen (Security Assertion Markup Language) mit einmaliger Anmeldung (Single Sign-On, SSO) (SAML 1.1)
- Kenntnisse von Cisco DUO SSO
- Kenntnisse von Windows Active Directory

Verwendete Komponenten

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

- Cisco ISE 3.1
- Cisco Duo SSO
- Windows Active Directory

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

Hintergrundinformationen

Identitätsanbieter (IdP)

In diesem Fall verifiziert und bestätigt die Duo SSO eine Benutzeridentität und Zugriffsrechte für eine angeforderte Ressource (den 'Service Provider').

Duo SSO fungiert als IdP, authentifiziert Ihre Benutzer mithilfe von vorhandenem Active Directory (AD) vor Ort mit SAML 1.1 oder einer beliebigen SAML 2.0 IdP (z. B. Microsoft Azure) und fordert zur Zwei-Faktor-Authentifizierung auf, bevor der Zugriff auf die Dienstanbieteranwendung zugelassen wird.

Wenn Sie eine Anwendung für den Schutz mit Duo SSO konfigurieren, müssen Sie Attribute von Duo SSO an die Anwendung senden. Active Directory funktioniert ohne zusätzliche Einrichtung. Wenn Sie jedoch eine SAML(2.0) IdP als Authentifizierungsquelle verwendet haben, stellen Sie sicher, dass die Konfiguration für das Senden der richtigen SAML-Attribute konfiguriert ist.

Service Provider

Die gehostete Ressource oder der gehostete Service, auf die bzw. den der Benutzer zugreifen möchte; in diesem Fall der Cisco ISE-Anwendungsserver.

SAML

SAML ist ein offener Standard, der IdP zum Übergeben von Autorisierungsanmeldeinformationen an SP zulässt.

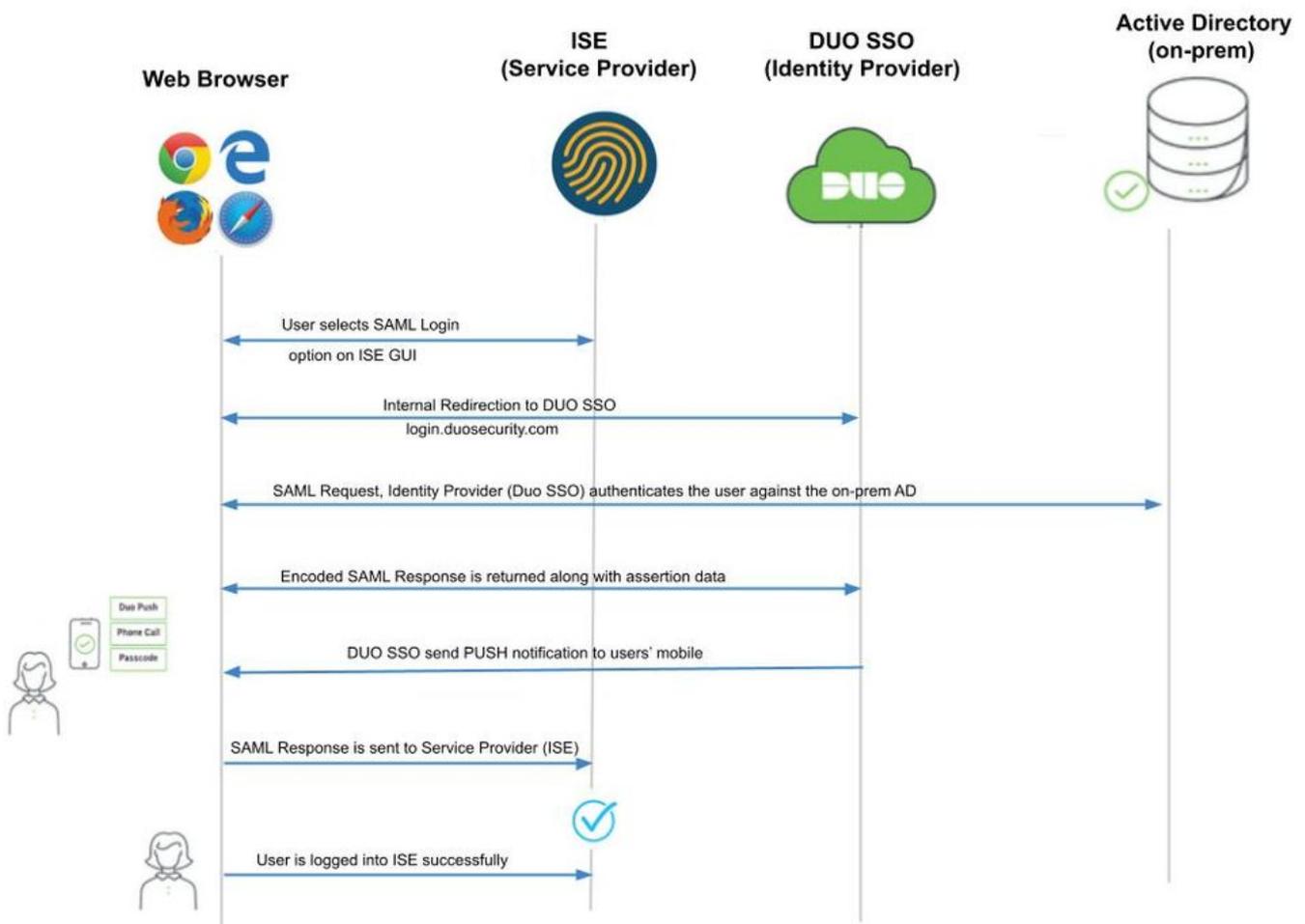
SAML-Transaktionen verwenden Extensible Markup Language (XML) für die standardisierte Kommunikation zwischen Identitätsanbieter und Dienstanbieter. SAML ist die Verbindung zwischen der Authentifizierung der Identität des Benutzers und der Autorisierung zur Nutzung eines Dienstes.

SAML-Assertion

Eine SAML Assertion ist das XML-Dokument, das von IdP an den Dienstanbieter gesendet wird, der die Benutzerautorisierung enthält. Es gibt drei verschiedene Arten von SAML-Assertionen: Authentifizierung, Attribut und Autorisierungsentscheidung.

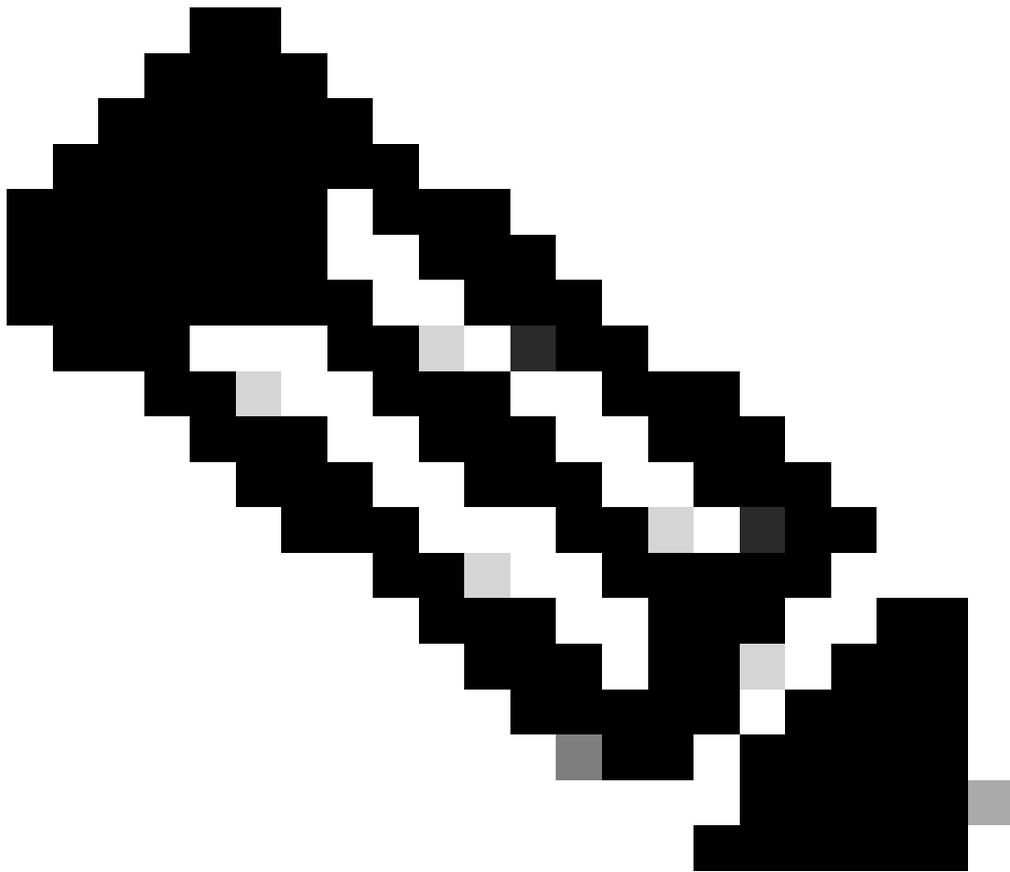
- Authentifizierungsassertionen belegen die Identifizierung des Benutzers und geben die Zeit an, zu der sich der Benutzer angemeldet hat, sowie die verwendete Authentifizierungsmethode (z. B. Kerberos, Zwei-Faktor usw.).
- Die Attributassertion übergibt die SAML-Attribute, d. h. bestimmte Datenelemente, die Informationen über den Benutzer bereitstellen, an den SP.
- Eine Autorisierungsentscheidungsassertion erklärt, ob der Benutzer zur Nutzung des Dienstes autorisiert ist oder ob die IdP ihre Anfrage aufgrund eines Kennwortfehlers oder fehlender Rechte für den Dienst abgelehnt hat.

Übergeordnetes Flussdiagramm



Fluss:

1. Der Benutzer meldet sich mit der Option Login Via SAML bei der ISE an.
2. ISE (SAML SP) leitet den Browser des Benutzers mit einer SAML-Anforderungsmeldung an Duo SSO weiter.



Hinweis: In einer verteilten Umgebung können Sie einen Fehler mit einem ungültigen Zertifikat ausgeben, und Schritt 3. kann jetzt ausgeführt werden. Daher unterscheidet sich Schritt 2. für eine verteilte Umgebung leicht in folgender Weise:
Problem: ISE leitet vorübergehend zum Portal eines der PSN-Knoten (auf Port 8443) um.

Lösung: Um sicherzustellen, dass ISE dasselbe Zertifikat wie das GUI-Zertifikat des Administrators bereitstellt, stellen Sie sicher, dass das Systemzertifikat, dem Sie vertrauen, auch für die Portalverwendung auf allen PSN-Knoten gültig ist.

-
3. Der Benutzer meldet sich mit primären AD-Anmeldeinformationen an.
 4. Duo SSO leitet diese Nachricht an AD weiter, das eine Antwort an Duo SSO zurückgibt.
 5. Duo SSO erfordert, dass der Benutzer eine Zwei-Faktor-Authentifizierung durchführt, indem er einen PUSH auf dem Mobiltelefon sendet.
 6. Der Benutzer schließt die Zwei-Faktor-Authentifizierung mit Duo ab.
 7. Duo SSO leitet den Browser des Benutzers mit einer Antwortnachricht an den SAML SP weiter.
 8. Der Benutzer kann sich jetzt bei der ISE anmelden.

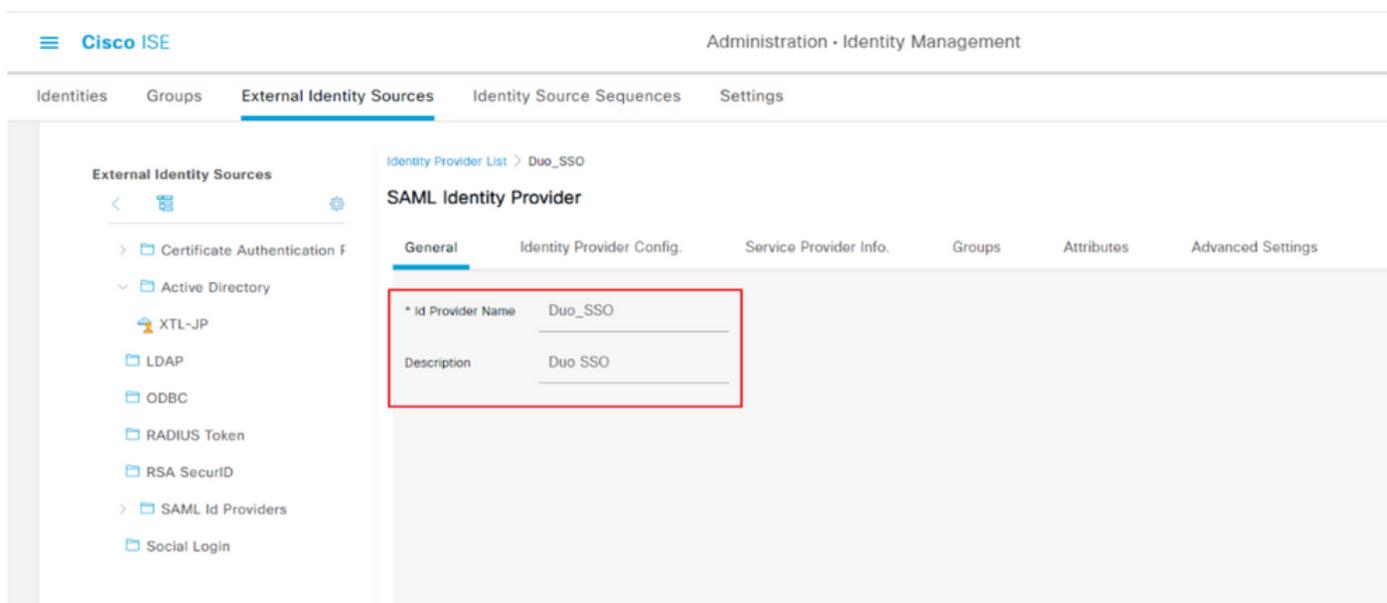
Konfigurieren der SAML SSO-Integration mit Duo SSO

Schritt 1: Konfigurieren von SAML-IDp auf der ISE

Konfigurieren von Duo SSO als externe SAML-Identitätsquelle

Navigieren Sie auf der ISE zu , Administration > Identity Management > External Identity Sources > SAML Id Providers und klicken Sie auf die Schaltfläche **Hinzufügen**.

Geben Sie den Namen der IdP ein, und klicken Sie auf **Submit (Senden)**, um sie zu speichern. Der IdP-Name ist nur für die ISE von Bedeutung, wie in der Abbildung dargestellt:



SAML-Metadaten-XML-Datei aus dem Duo-Administratorportal importieren

Navigieren Sie auf der ISE zu Administration > Identity Management > External Identity Sources > SAML Id Providers. > Choose the SAML IdP (SAML-ID auswählen), und klicken Sie auf die Identity Provider Configuration Schaltfläche und anschließend auf **Choose File (Datei auswählen)**.

Wählen Sie die **SSO IDP Metadata XML**-Datei aus dem Duo Admin-Portal exportiert und klicken Sie auf **Öffnen**, um sie zu speichern. (Dieser Schritt wird auch im Abschnitt Duo dieses Dokuments erwähnt.)

Die SSO-URL und die Signaturzertifikate sind:

The screenshot shows the Cisco ISE Administration interface for Identity Management. The left sidebar lists 'External Identity Sources' with 'Duo_SSO' selected. The main content area is titled 'SAML Identity Provider' and has tabs for 'General', 'Identity Provider Config.', 'Service Provider Info.', 'Groups', 'Attributes', and 'Advanced Settings'. The 'Identity Provider Config.' tab is active, showing an 'Identity Provider Configuration' section with a 'Choose File' button. Below this, there are fields for 'Single Sign On URL' and 'Single Sign Out URL (Post)'. A 'Samlina Certificates' table is also visible, listing certificates with columns for Subject, Issuer, Valid From, Valid To, and Serial Number.

ISE-Authentifizierungsmethode konfigurieren

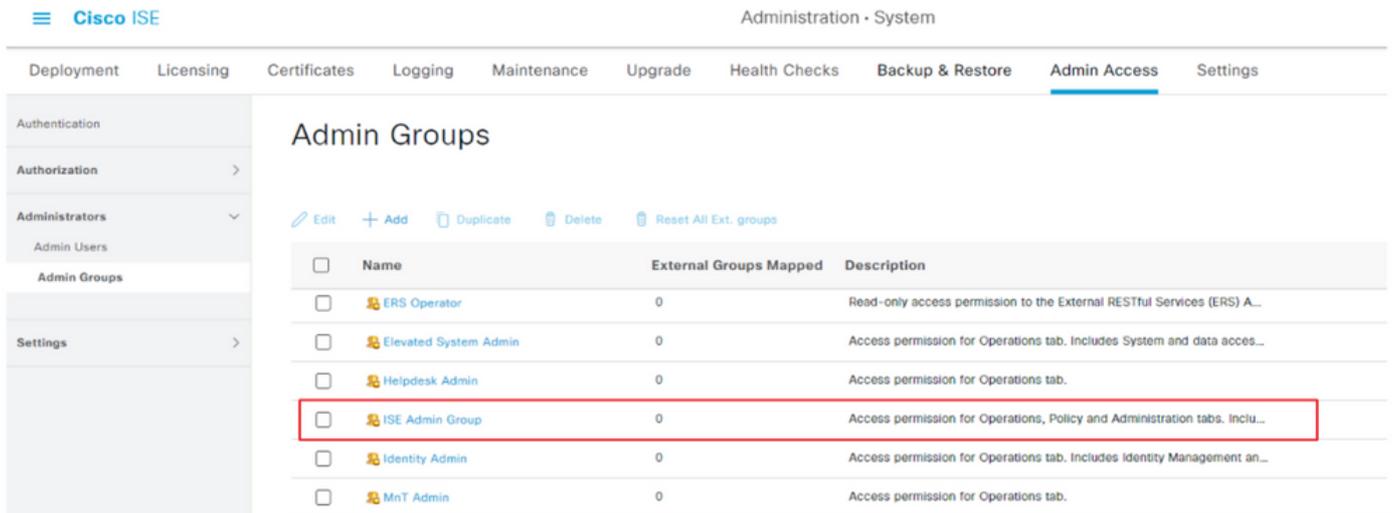
Navigieren Sie zu Administration > System > Admin Access > Authentication > Authentication Method, und wählen Sie das Optionsfeld Kennwortbasiert aus. Wählen Sie den zuvor erstellten IdP-Namen aus der Dropdown-Liste Identity Source (Identitätsquelle) aus, wie im Bild gezeigt:

The screenshot shows the Cisco ISE Administration interface for System > Admin Access > Authentication > Authentication Method. The 'Authentication Method' tab is active, showing 'Authentication Type' with two radio button options: 'Password Based' (selected) and 'Client Certificate Based'. Below the radio buttons is a dropdown menu for 'Identity Source' with 'SAML:Duo_SSO' selected. Red boxes highlight the 'Password Based' option and the 'Identity Source' dropdown.

Erstellen einer Administratorgruppe

Navigieren Sie zu Administration > System > Admin Access > Authentication > Administrators > Admin Group, und klicken Sie auf den **Super Admin** und dann auf die Schaltfläche **Duplizieren**. Geben Sie den **Namen** der **Admin-Gruppe ein**, und klicken Sie auf die Schaltfläche **Submit (Senden)**.

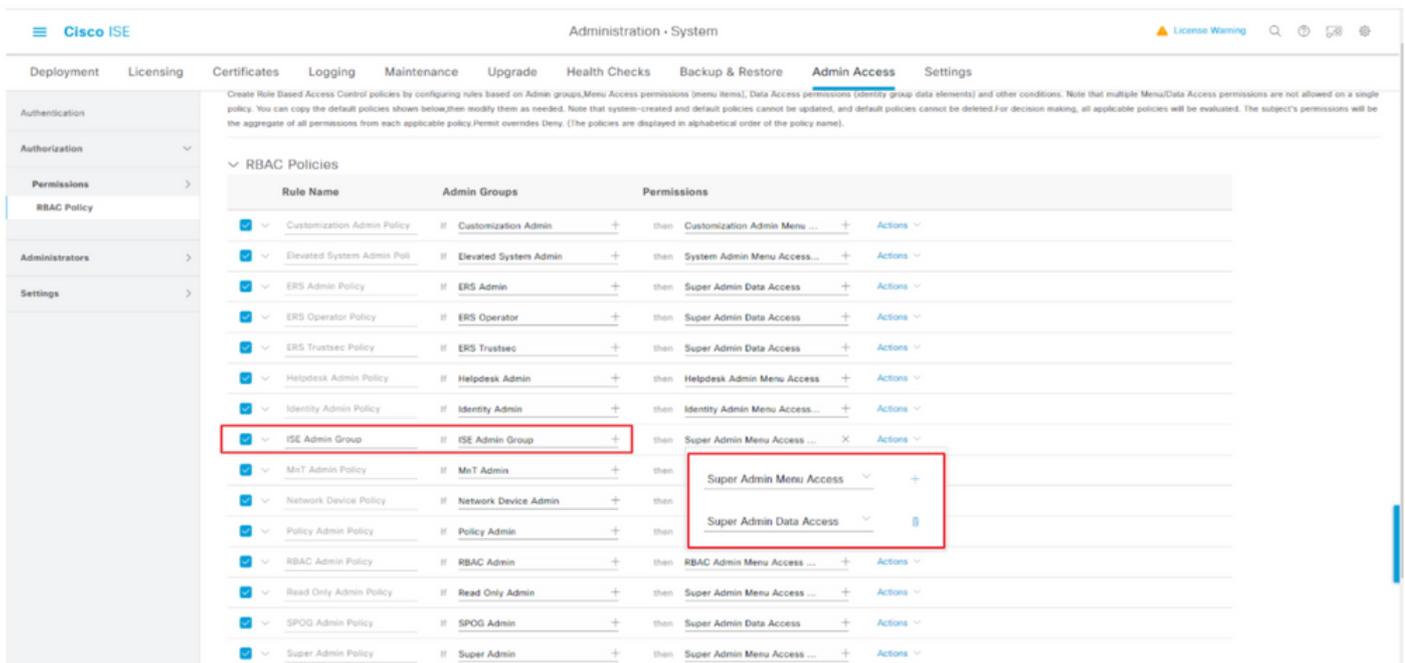
Dadurch erhält die Admin-Gruppe Super-Admin-Berechtigungen.



Erstellen einer RBAC-Richtlinie für die Administratorgruppe

Navigieren Sie zu Administration > System > Admin Access > Authorization > RBAC Policy, und wählen Sie die **Aktionen** für die **Super Admin Policy** aus. Klicken Sie auf .Duplicate > Add the Name field > Save

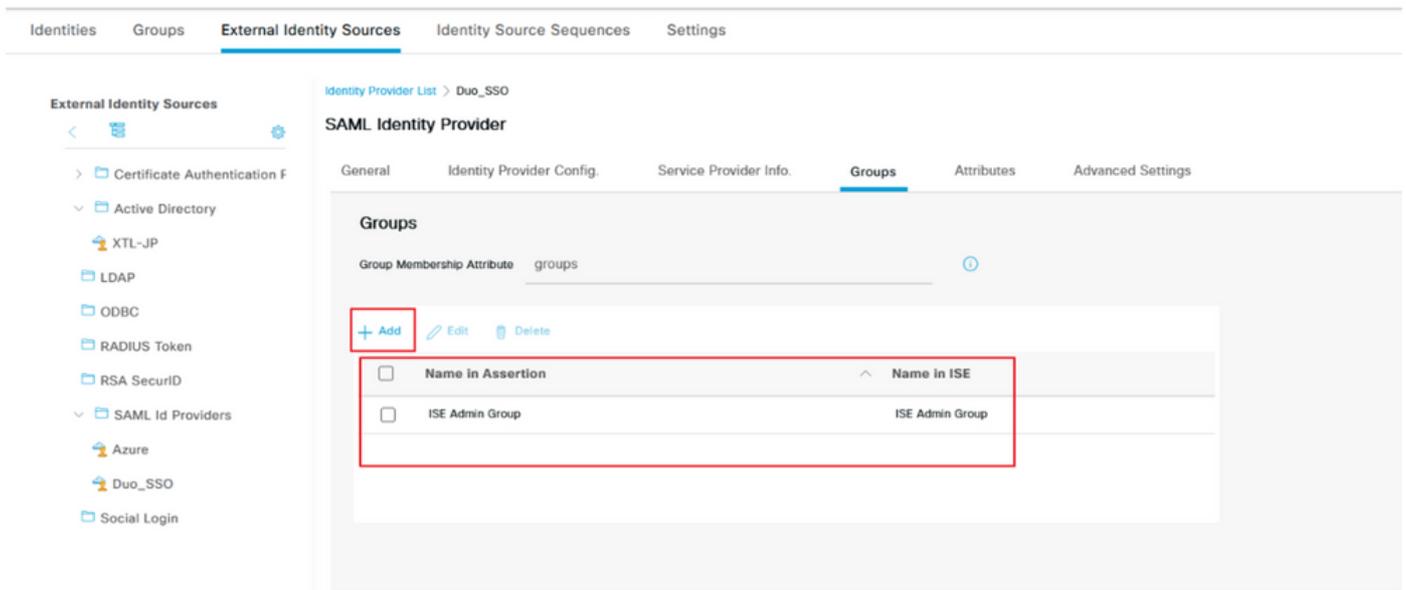
Die Zugriffsberechtigungen entsprechen den Administratorrichtlinien.



Gruppenmitgliedschaft hinzufügen

Navigieren Sie auf der ISE zu Administration > Identity Management > External Identity Sources > SAML Id Providers der von Ihnen erstellten SAML-ID, und wählen Sie sie aus. Klicken Sie auf **Gruppen** und dann auf die Schaltfläche Hinzufügen.

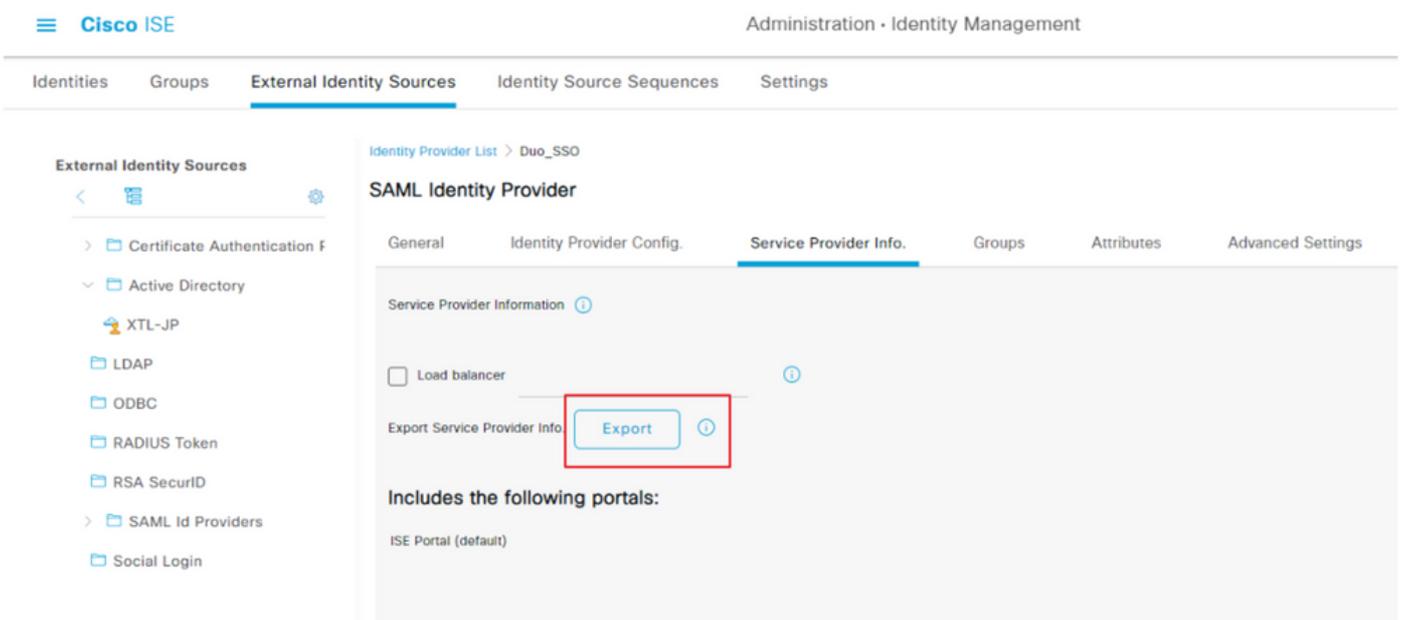
Fügen Sie den Namen in Assertion (Name der ISE-Admin-Gruppe) hinzu, und wählen Sie aus dem Dropdown-Menü die erstellte RBAC-Gruppe (Role-Based Access Control) aus (Schritt 4). Klicken Sie anschließend auf **Öffnen**, um die Gruppe zu speichern. Die SSO-URL und die Signaturzertifikate werden automatisch ausgefüllt:



SP-Informationen exportieren

Navigieren Sie zu Administration > Identity Management > External Identity Sources > SAML Id Providers > (Your SAML Provider) .

Wechseln Sie zur Registerkarte SP-Info, und klicken Sie auf die Schaltfläche **Exportieren**, wie in der Abbildung dargestellt:



Laden Sie die .xml Datei herunter, und speichern Sie sie. Notieren Sie sich die AssertionConsumerService Standort-URL und den **entityID**-Wert, da diese Details im Duo SSO-Portal erforderlich sind.

```
<?xml version="1.0" encoding="UTF-8"?><md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metada
```

Hier sind die Details/Attribute, die aus der Metadatei erfasst werden, die in der Duo Generic SAML Integration konfiguriert werden muss.

entityID = <http://CiscoISE/7fdcf239-631e-439c-a3ab-f5e56429779d>.

AssertionConsumerService Location = <https://10.x.x.x:8443/portal/SSOLoginResponse.action>, wobei 10.x.x.x die ISE-IP in der XML-Datei (Location) ist.

AssertionConsumerService Location = <https://isenodename.com:8443/portal/SSOLoginResponse.action>, wobei isenodename der tatsächliche ISE-FQDN-Name in der XML-Datei (Location) ist.

Schritt 2: Konfigurieren von Duo SSO für ISE

Überprüfen Sie diese [KB](#), um Duo SSO mit AD als Authentifizierungsquelle zu konfigurieren.

Configured Authentication Sources

Name	Type	Status	Authentication Proxies
+ Add source			
Active Directory	Active Directory	Enabled	Authentication Proxy

Überprüfen Sie diese [KB](#), um SSO mit Ihrer benutzerdefinierten Domäne zu aktivieren.

Single Sign-On

1 Custom Subdomain

Your users will see the custom subdomain when they authenticate to a Single Sign-On protected application. A familiar URL will help your users know that the site belongs to your organization. The subdomain will be home to Duo Central, if you choose to enable it. Duo Central allows your users to access your organization's sites and applications in one central place.

[Create a custom subdomain](#)

Customize your SSO subdomain

Tailor the single sign-on experience to match your company's brand and help your users recognize phishing attempts. Your users will see this custom subdomain during authentication.

Custom subdomain .login.duosecurity.com

Subdomain must contain only letters, numbers, or hyphens (-). Subdomain may not begin or end with a hyphen (-) and must be less than 63 characters in length.

[Save and continue](#) [Complete later](#)

Schritt 3: Integration der Cisco ISE mit Duo SSO als generischem SP

Überprüfen Sie Schritt 1 und Schritt 2 dieser [KB](#), um die Cisco ISE mit Duo SSO als Standard-SP zu integrieren.

Konfigurieren Sie die Details für den Cisco ISE SP im Duo-Admin-Bereich für generische SPs:

Name	Beschreibung
Entitäts-ID	http://CiscoISE/7fdfc239-631e-439c-a3ab-f5e56429779d
Assertion Consumer Service (ACS)-URL	https://10.x.x.x:8443/portal/SSOLoginResponse.action

Service Provider

Entity ID *

<http://CiscoISE/7fdfc239-631e-439c-a3ab-f5e56429779d>

The unique identifier of the service provider.

Assertion Consumer Service (ACS) URL *

<https://10.52.14.44:8443/portal/SSOLoginResponse.action>

Konfigurieren der SAML-Antwort für die Cisco ISE:

Name	Beschreibung
NameID-Format	urn:oasis:names:tc:SAML:1.1:nameid-format:nicht angegeben
NameID-Attribut	Benutzername

SAML Response

NameID format *

urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified

The format that specifies how the NameID is sent to the service provider.

NameID attribute *

× <Username>

NameID is a SAML attribute that identifies the user. Enter in an IdP attribute or select one of Duo's preconfigured attributes that automatically chooses the NameID attribute based on the IdP. There are five preconfigured attributes: <Email Address>, <Username>, <First Name>, <Last Name> and <Display Name>.

Erstellen Sie eine Gruppe namens Cisco Admin Group im Duo-Admin-Bereich, und fügen Sie die ISE-Benutzer zu dieser Gruppe hinzu, oder erstellen Sie eine Gruppe in Windows AD, und synchronisieren Sie diese mit dem Duo-Admin-Bereich über die Funktion "Verzeichnis synchronisieren".

Konfigurieren Sie Rollenattribute für die Cisco ISE:

Name	Beschreibung
Attributname	Gruppen
SP-Rolle	ISE-Administratorgruppe
Duo-Gruppen	ISE-Administratorgruppe

Role attributes Map Duo groups to different roles in this service provider. A Duo group can be mapped to multiple roles and each role can have multiple groups mapped to it. Optional. [Learn more about Duo groups.](#)

Attribute name

The name of the attribute which will carry the mapped roles.

Service Provider's Role **Duo groups**

 (+)

Geben Sie im Abschnitt Einstellungen auf der Registerkarte **Name** einen geeigneten Namen für diese Integration ein.

Settings

Type Generic Service Provider - Single Sign-On

Name

Duo Push users will see this when approving transactions.

Klicken Sie auf die Schaltfläche **Speichern**, um die Konfiguration zu speichern. Weitere Informationen finden Sie in dieser [KB](#).

Klicken Sie auf **XML herunterladen**, um die SAML-Metadaten herunterzuladen.

Downloads

Certificate

[Download certificate](#)

Expires: 01-19-2038

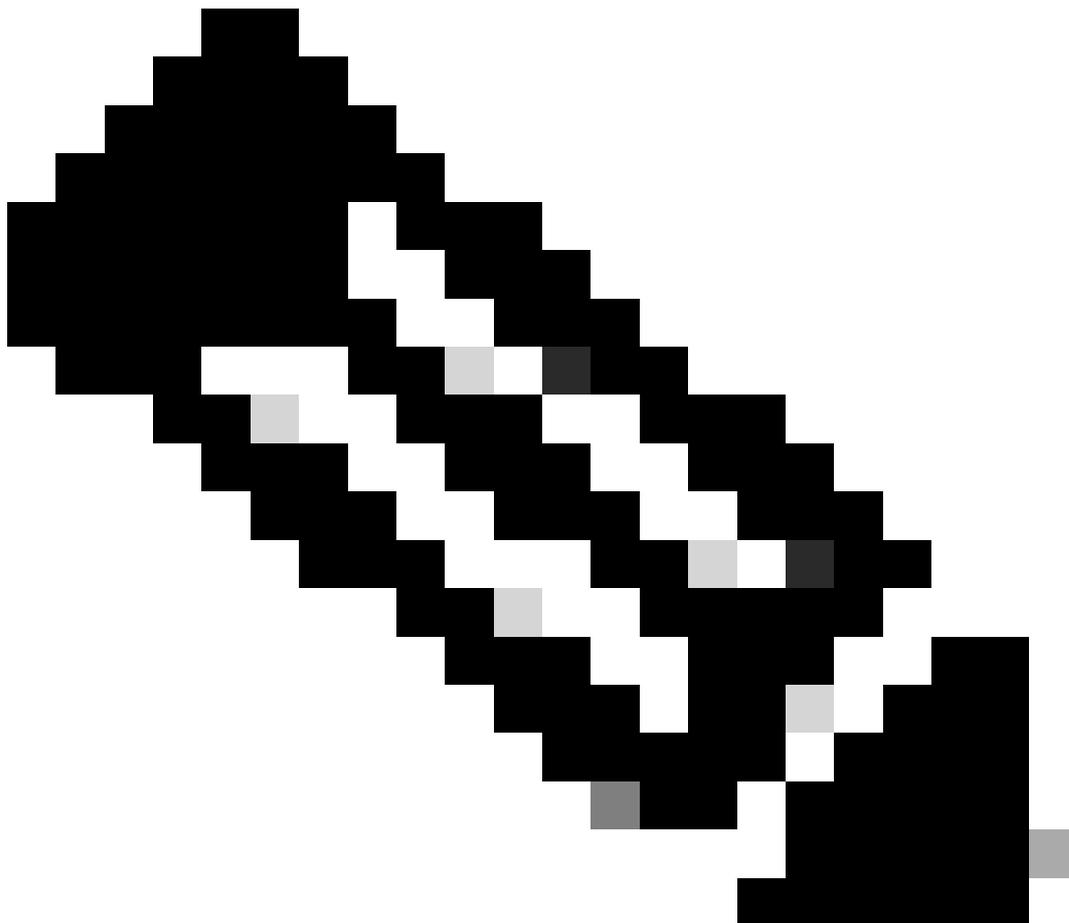
SAML Metadata

[Download XML](#)

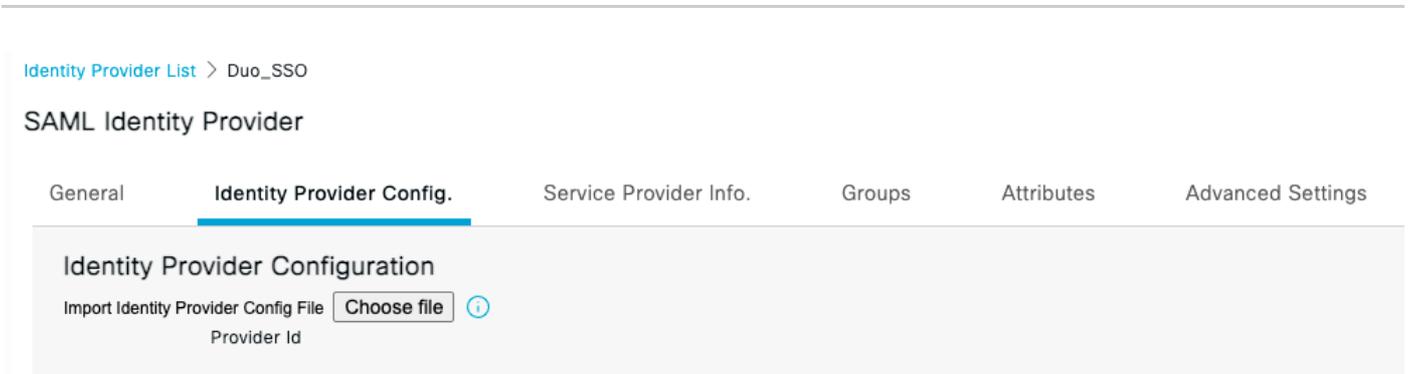
Laden Sie SAML MetaData vom Duo-Admin-Panel auf die Cisco ISE herunter, indem Sie zu navigieren Administration > Identity Management > External Identity Sources > SAML Id Providers > Duo_SSO.

Wechseln Sie auf der Registerkarte zu **Identity Provider Config**, und klicken Sie auf die Schaltfläche **Choose file**.

Wählen Sie die in Schritt 8 heruntergeladene **XML-Metadatendatei** aus, und klicken Sie auf **Speichern**.



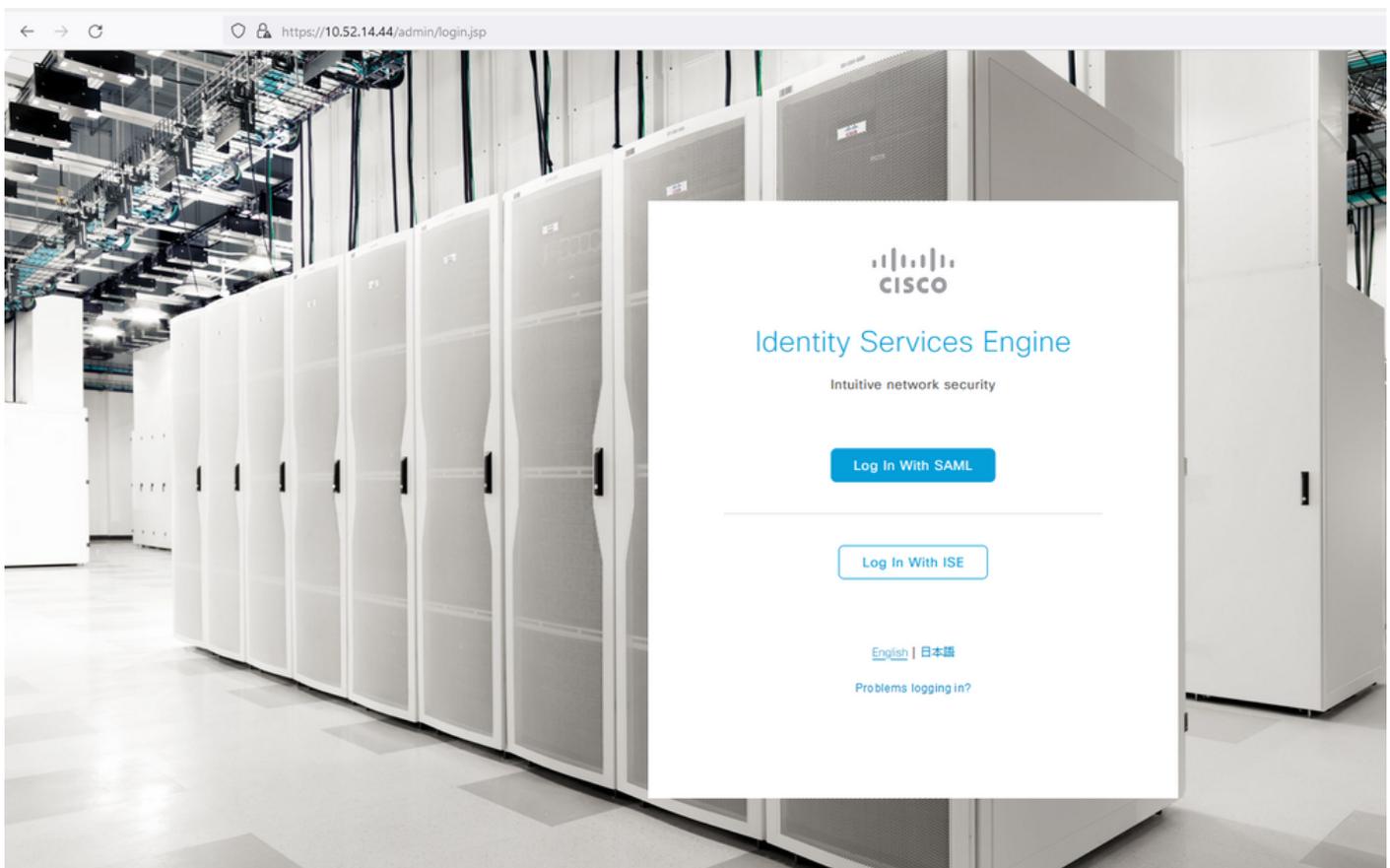
Hinweis: Dieser Schritt wird hier im Abschnitt Konfigurieren der SAML SSO-Integration mit Duo SSO; Schritt 2 beschrieben. Importieren Sie die **SAML-Metadaten-XML**-Datei aus dem Duo Admin-Portal.



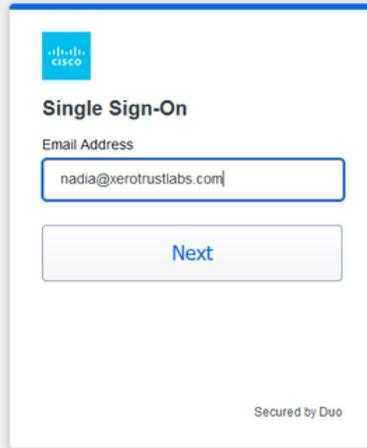
Überprüfung

Testen der Integration mit Duo SSO

1. Melden Sie sich im **Cisco ISE-Administrationsbereich an**, und klicken Sie auf **Anmelden mit SAML**.

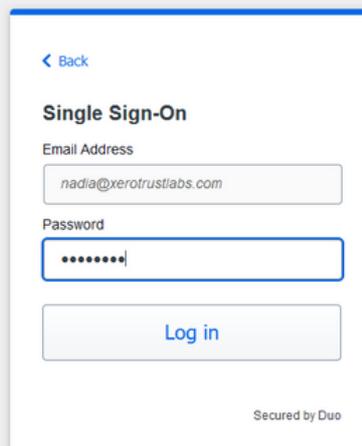


2. Umgeleitet zur SSO-Seite, geben Sie die **E-Mail-Adresse ein** und klicken Sie auf **Weiter**.



The image shows a Cisco Single Sign-On form. At the top left is the Cisco logo. Below it, the text "Single Sign-On" is displayed. Underneath, there is a label "Email Address" followed by a text input field containing the email address "nadia@zerotrustlabs.com". Below the input field is a button labeled "Next". At the bottom right of the form, it says "Secured by Duo".

3. Geben Sie das **Kennwort** ein, und klicken Sie auf **Anmelden**.

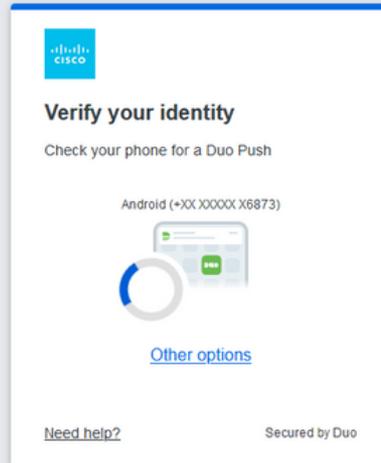


The image shows the next step of the Cisco Single Sign-On form. At the top left is a blue back arrow labeled "Back". Below it, the text "Single Sign-On" is displayed. Underneath, there is a label "Email Address" followed by a text input field containing the email address "nadia@zerotrustlabs.com". Below that is a label "Password" followed by a password input field with masked characters "••••••••". Below the password field is a button labeled "Log in". At the bottom right of the form, it says "Secured by Duo".

4. Sie erhalten eine Duo Push-Aufforderung auf Ihrem Mobilgerät.

Duo needs your help

[Take a quick 6-question survey](#) to help us improve this experience.



The image shows a white rectangular box with a blue border, representing a Duo authentication prompt. At the top left is the Cisco Duo logo. The main heading is "Verify your identity" in bold. Below it, the text says "Check your phone for a Duo Push". A phone number is displayed: "Android (+XX XXXXX X6873)". In the center, there is a graphic of a smartphone with a green push notification icon and a circular progress indicator. Below the phone number is a blue link "Other options". At the bottom left, there is a link "Need help?". At the bottom right, it says "Secured by Duo".

5. Sobald Sie die Eingabeaufforderung akzeptieren, erhalten Sie ein Fenster und werden automatisch auf die ISE-Admin-Seite weitergeleitet.

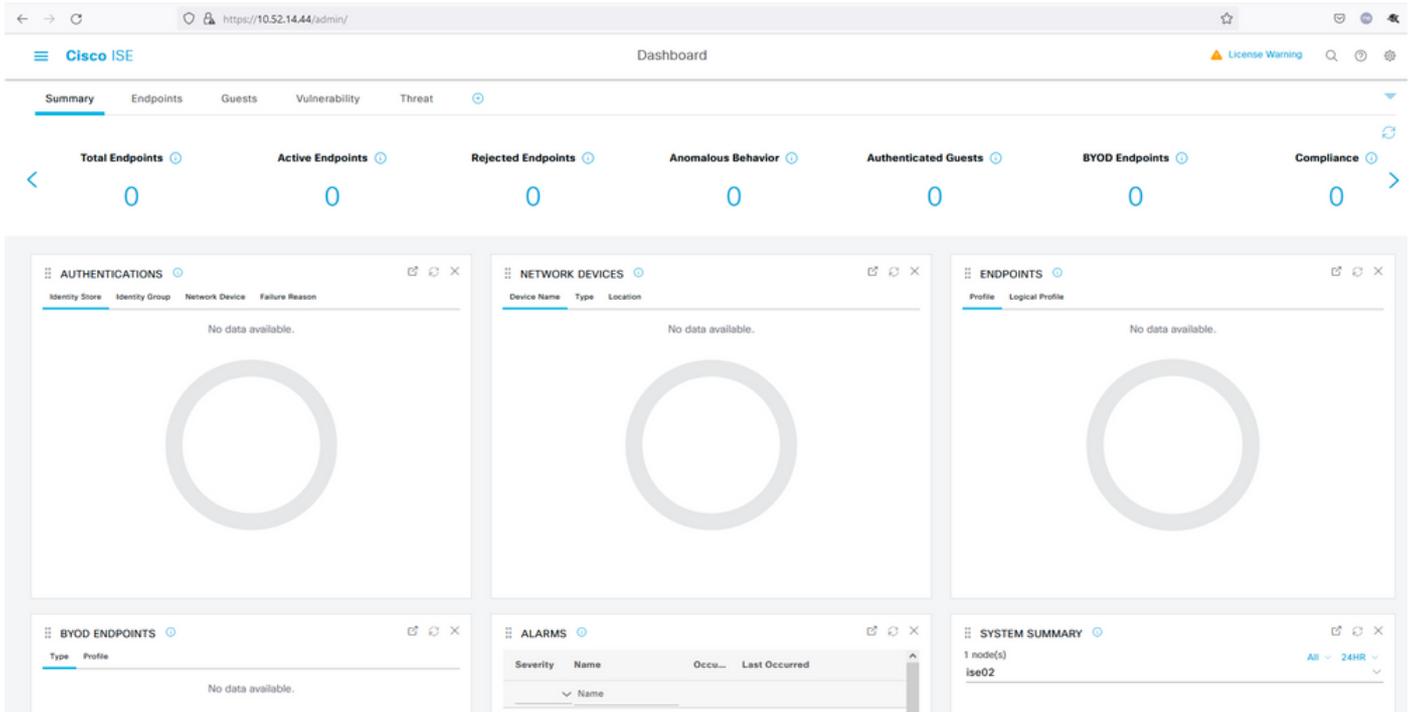


Success!

Logging you in...



Secured by Duo



Fehlerbehebung

- Laden Sie die SAML-Tracer-Erweiterung für Mozilla FF herunter <https://addons.mozilla.org/en-US/firefox/addon/saml-tracer/>.
- Blättern Sie zum SSOLoginResponse.action Paket. Auf der Registerkarte **SAML** werden mehrere Attribute angezeigt, die von Duo SAML gesendet wurden: NameID, Recipient (AssertionConsumerService Location URL) und Audience (EntityID).

```

GET https://zerotrustlabs.login.duosecurity.com/pw/ASOOZM6KCLX6T19QVNA3/ssp_callback?aid=643b5067d1f249f5bf6d744a7603ef83&req-trace-group=dfac3f2db
GET https://zerotrustlabs.login.duosecurity.com/favicon.ico
POST https://10.10.10.10:8443/portal/SSOLoginResponse.action SAML
GET https://10.10.10.10:8443/portal/css/images/favicon.ico
POST https://10.10.10.10:8443/admin/LoginAction.do
GET https://10.10.10.10:8443/admin/
GET https://10.10.10.10:8443/admin/ng/css/vendor/bootstrap/css/bootstrap-dialog.css
GET https://10.10.10.10:8443/admin/ng/css/vendor/fuelux/css/fuelux.min.css
GET https://10.10.10.10:8443/admin/ng/css/vendor/jstree/css/style.min.css
GET https://10.10.10.10:8443/admin/ng/css/vendor/select2/select2.min.css
GET https://10.10.10.10:8443/admin/lib/cpm/widget/themes/default/combobox.css
GET https://10.10.10.10:8443/admin/lib/cpm/widget/themes/default/textboxsubmitter.css
GET https://10.10.10.10:8443/admin/lib/cpm/widget/themes/default/expressionbuilder.css
GET https://10.10.10.10:8443/admin/lib/cpm/widget/themes/default/saveprogressindicator.css
GET https://10.10.10.10:8443/admin/lib/cpm/widget/themes/default/table/treetable.css
GET https://10.10.10.10:8443/admin/lib/cpm/widget/themes/default/table/pagetable.css
GET https://10.10.10.10:8443/admin/pages/utills/css/common_icons.css
GET https://10.10.10.10:8443/admin/pages/utills/css/common_styles.css

```

HTTP Parameters SAML Summary

```

<ds:X509Data>
<ds:X509Certificate>MIIDTCCAFAwIBAgIUCbf+LB1BLJMeF6GV0B1rmdX3AVEwDQYJKoZIhvcNAQELBQAwNjEVMGMGA1UECgwMRHRvIFN1Y3VyaXR5MR0wGwYDVQDD
BRESTZPODg2UkxETUJZMzExSFBJMjAeFw0yMTEyMTYwMjQNTFZlZjEwODAxMTkwMzE0MDdaMDYxFTATBgNVBAoMDER1byBTZW51cm10eTEdMBsGA1UEAwwURk2Zg4N1JMRE
1CWTMxMuhQSTIwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDB03Ayuh9avw0NoQzIhQZzu9H8vu/HSKLSH30585Mukj5FnoVV50PGTuoFN4u90tSiFULjC8eQnUs
BR1PYQ5jt0V23qVnvoGyqsuHAs8nbKwvzPshzNF59p03pXkoGPuB+Du2IrrvV0opSv4vbrgKV+H/bvMqyhIA6ywfHNZedG7pbwrYBtVPDXUpnLQvtL2
/Vd9230XuXHF+k32hagRgTLub5XyT1HHQ8b4n3mQKHs6yA/KNvaB3b/AMUqAXDqaEXNG0uQENMK30wTs49
/w+r5fz7xp66muRc0IBg3xjWnnFnyujy7v5ifn1KFUFQu+86A5GbuUWCyiaKmV7CztAgMBAAGjEzARMA8GA1UdEwEB
/wQFMAMBAF8wDQYJKoZIhvcNAQELBQADggEBAH+KItcw0KtDxXBvZ5S+25a+50F4Tqd/pHh56i19d2kDxInSUVsy
/Yy1FXAWge3WBke4b3JR7znD6000sZTYbF9w7H4svU2gxzdk0znXJNj2e4C5fDivnj/TawZakp2MbTaxfV2VTL0K0kV/1jM6PL61PbKGFwNmh+SjW/VseS+71C701eI
/U095XLbAu2iIny9zfv0hKNV72L8fgYgrjhpdxH8Y1SxPbVWZMwzytbwZFUogD30XrPq16aXZvJyOH5Vs0H90wQ8qQ48hI4F4J3DyRPNH1PzQTYM38kjymEkE0DJPcaGy9v
EMinHUkdwpiETB52Cmtwg+DzAw1jpc=</ds:X509Certificate>
</ds:X509Data>
<ds:KeyInfo>
</ds:KeyInfo>
</ds:Signature>
<saml:Subject>
<saml:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">nadia</saml:NameID>
<saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
<saml:SubjectConfirmationData NotOnOrAfter="2021-12-02T04:48:56Z"
Recipient="https://10.10.10.10:8443/portal/SSOLoginResponse.action"
InResponseTo="f5e56429779d_DELIMITERportalId_EQUALS7fdfc239-631e-439c-a3ab-f5e56429779d_SEMIportalSessionId_EQUALS859ee9c3-60e4-4482-9426-
b3904d4d6226_SEMItoken_EQUALS1RS257BC24SGVHWZ76GMVEZNR0YCCCL_SEMI_DELIMITER10."/>
</saml:SubjectConfirmation>
</saml:Subject>
<saml:Conditions NotBefore="2021-12-02T04:43:26Z"
NotOnOrAfter="2021-12-02T04:48:56Z"
>
<saml:AudienceRestriction>
<saml:Audience>http://CiscoISE/7fdfc239-631e-439c-a3ab-f5e56429779d</saml:Audience>
</saml:AudienceRestriction>
</saml:Conditions>
<saml:AuthnStatement AuthnInstant="2021-12-02T04:43:56Z"
SessionIndex="DUO_8dfe494ab8d617884446cb8f2259bb4a56492ef"
>
</saml:AuthnStatement>
</saml:AuthnContext>

```

1846 requests received (490 hidden)

- Live-Anmeldung bei ISE:

Steps

5231 Guest Authentication Passed

Overview

Event	5231 Guest Authentication Passed
Username	nadia
Endpoint Id	
Endpoint Profile	
Authorization Result	

Authentication Details

Source Timestamp	2021-11-28 15:36:03.59
Received Timestamp	2021-11-28 15:36:03.59
Policy Server	ise02
Event	5231 Guest Authentication Passed
Username	nadia
User Type	NON_GUEST
Authentication Identity Store	Duo_SSO
Identity Group	Any
Authentication Method	PAP_ASCII
Authentication Protocol	PAP_ASCII

Other Attributes

ConfigVersionId	79
IpAddress	10.65.48.163
PortalName	ISE Portal (default)
PsnHostName	ise02.xerotrustlabs.com
GuestUserName	nadia

- Administrative Anmelde-Anmeldung bei ISE: Benutzername: samIUser.

- Export Summary
- My Reports
- Reports
- Audit
 - Adaptive Network Control
 - Administrator Logins
 - Change Configuration Audit
 - Cisco Support Diagnostics
 - Data Purging Audit
 - Endpoint Purge Activities
 - Internal Administrator Sum...
 - Policy OpenAPI Operations
 - Operations Audit
 - psGrid Administrator Audit
 - Secure Communications A...
 - TrustSec Audit
 - User Change Password Au...
- Device Administration
- Diagnostics
- Endpoints and Users
- Guest
- Threat Control NAC
- TrustSec
- Scheduled Reports

Administrator Logins

From 2021-11-28 00:00:00 To 2021-11-28 18:38:10

Reports reported in last 7 days

Add to My Reports Export To Schedule

Logged At	Administrator	IP Address	Server	Event	Event Details
Today	Administrator		Server		
2021-11-28 18:38:08.199		10.85.48.183	18492	Administrator authentication succeeded	Administrator authentication successful

Rows/Page 1 1 Total Rows

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.