

Inloggen via ISE 3.1 GUI Admin met SAML-integratie met Duo SSO en Windows AD configureren

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Identity Provider \(IDP\)](#)

[Serviceprovider \(SP\)](#)

[SAML](#)

[SAML Assertion](#)

[Flow Diagram op hoog niveau](#)

[Integratie van SAML SSO met Duo SSO configureren](#)

[Stap 1. SAML IDp configureren op ISE](#)

[Duo SSO configureren als externe SAML Identity Source](#)

[Het XML-bestand met SAML-metagegevens importeren vanuit het Duo Admin-portal](#)

[ISE-verificatiemethode configureren](#)

[Een beheergroep maken](#)

[Een RBAC-beleid voor de Admin-groep maken](#)

[Lidmaatschap Groepen toevoegen](#)

[SP-informatie exporteren](#)

[Stap 2. Duo SSO configureren voor ISE](#)

[Stap 3. Integratie van Cisco ISE met Duo SSO als generieke servicesmodule](#)

[Verifiëren](#)

[De integratie met Duo SSO testen](#)

[Problemen oplossen](#)

Inleiding

Dit document beschrijft hoe u de integratie van Cisco ISE 3.1 SAML SSO kunt configureren met een externe identiteitsprovider zoals Cisco Duo SSO.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Identity Services Engine (ISE) 3.1
- Basiskennis over implementaties van Security Assertion Markup Language (SAML) Single Sign-On (SSO) (SAML 1.1)
- Kennis van Cisco DUO SSO
- Kennis van Windows Active Directory

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

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

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Identity Provider (IDP)

Het is in dit geval de Duo SSO die een gebruikersidentiteit en toegangsrechten voor een gevraagde bron (de 'Serviceprovider') verifieert en bevestigt.

Duo SSO fungeert als een IdP, waarbij uw gebruikers worden geauthenticeerd met behulp van bestaande Active Directory (AD) op locatie met SAML 1.1 of een SAML 2.0 IDP (bijvoorbeeld Microsoft Azure) en wordt gevraagd om twee-factor-verificatie voordat toegang tot uw serviceprovider-toepassing wordt toegestaan.

Bij het configureren van een applicatie die beveiligd moet worden met Duo SSO moet u attributen van Duo SSO naar de applicatie sturen. Active Directory werkt zonder extra setup, maar als u een SAML(2.0) IDP als uw verificatiebron gebruikt, controleert u of u het hebt geconfigureerd om de juiste SAML-kenmerken te verzenden.

Serviceprovider (SP)

De gehoste bron of service waartoe de gebruiker toegang wil krijgen; Cisco ISE-toepassingsserver in dit geval.

SAML

SAML is een open standaard die IdP toestaat om de autorisatiegegevens door te geven aan SP.

SAML-transacties maken gebruik van Extensible Markup Language (XML) voor gestandaardiseerde communicatie tussen de identiteitsprovider en serviceproviders. SAML is de

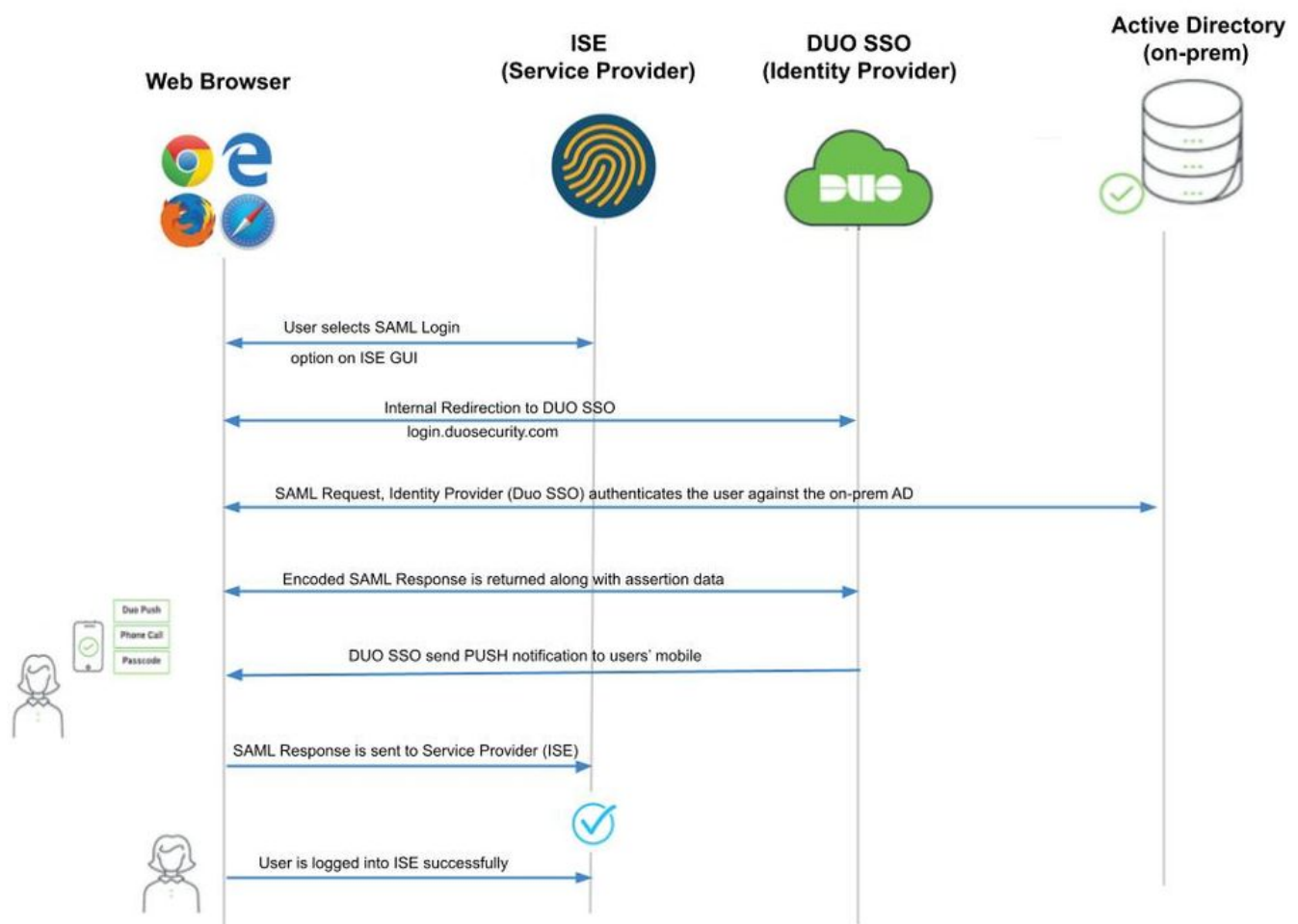
schakel tussen de authenticatie van de identiteit van de gebruiker en de autorisatie om een dienst te gebruiken.

SAML Assertion

Een SAML Assertion is het XML-document dat de IDp naar de serviceprovider stuurt die de gebruikersautorisatie bevat. Er zijn drie verschillende typen SAML Assertions - authenticatie, attribuut en autorisatiebesluit.

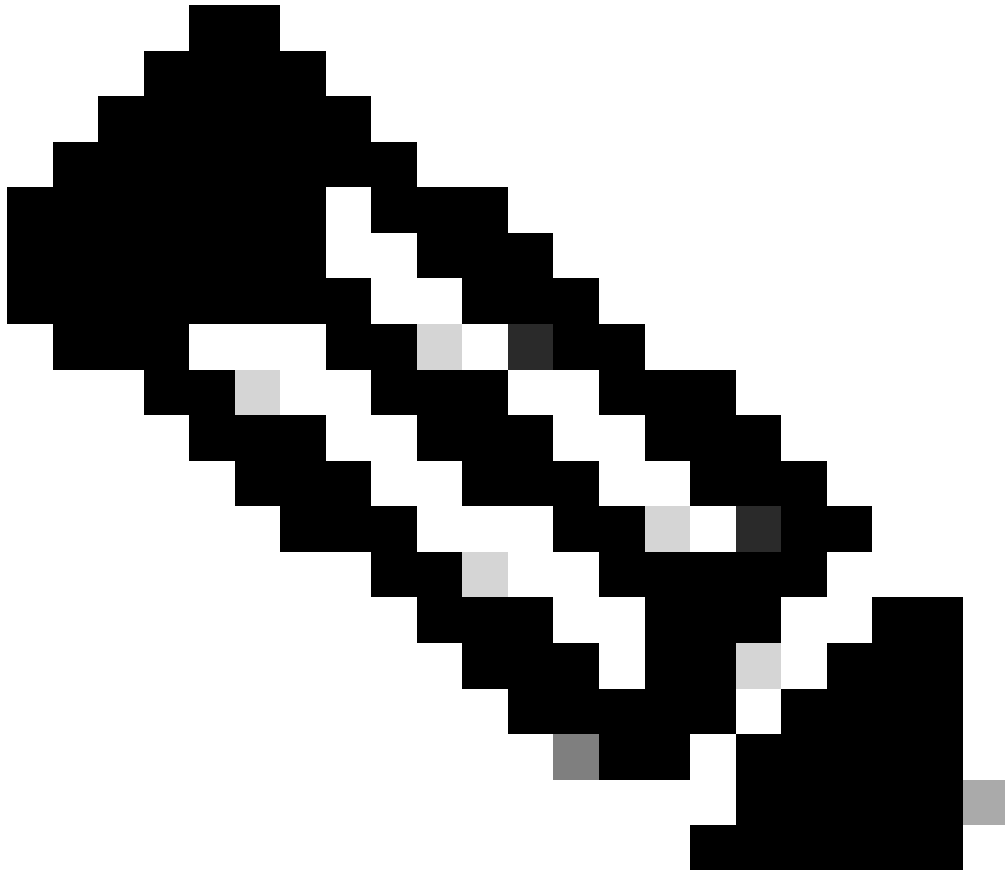
- Verificatiebeweringen bewijzen de identificatie van de gebruiker en geven de tijd aan dat de gebruiker inlogde en welke verificatiemethode zij hebben gebruikt (bijvoorbeeld Kerberos, two-factor, enzovoort).
- De attributie bewering geeft de SAML attributen, specifieke stukken gegevens die informatie geven over de gebruiker, door aan de SP.
- Een autorisatiebesluit bewering verklaart dat de gebruiker geautoriseerd is om de service te gebruiken of dat de IDp hun verzoek heeft afgewezen vanwege een wachtwoordfout of gebrek aan rechten op de service.

Flow Diagram op hoog niveau



Stroom:

1. De gebruiker meldt zich aan bij ISE met de optie Login via SAML.
 2. ISE (SAML SP) stuurt de browser van de gebruiker naar Duo SSO met een SAML-verzoekbericht.
-



Opmerking: in een gedistribueerde omgeving kunt u een Ongeldige certificaatfout en stap 3 krijgen. kan nu werken. Vandaar, voor een verdeelde omgeving, verschilt Stap 2. enigszins op deze manier:

Probleem: ISE gaat tijdelijk naar de portal van een van de PSN-knooppunten (op poort 8443).

Oplossing: om ervoor te zorgen dat ISE hetzelfde certificaat presenteert als het GUI-certificaat van de beheerder, moet u ervoor zorgen dat het systeemcertificaat dat u vertrouwt ook geldig is voor het gebruik van de portal op alle PSN-knooppunten.

3. Gebruiker logt in met primaire AD-referenties.
4. Duo SSO stuurt dit door naar AD, dat een antwoord teruggeeft aan Duo SSO.
5. Duo SSO vereist dat de gebruiker een dubbele authenticatie uitvoert door een PUSH op de mobiele telefoon te verzenden.

6. De gebruiker voltooit de Duo two-factor verificatie.
7. Duo SSO stuurt de browser van de gebruiker naar de SAML SP met een antwoordbericht.
8. De gebruiker kan nu inloggen op ISE.

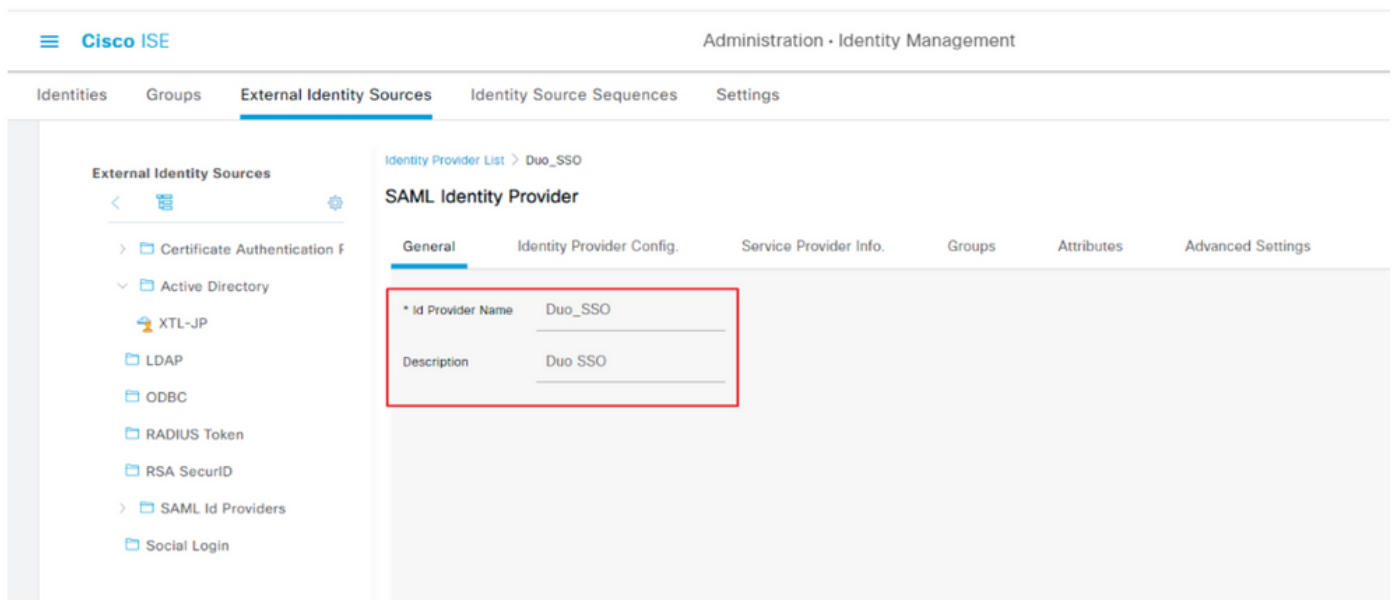
Integratie van SAML SSO met Duo SSO configureren

Stap 1. SAML IDp configureren op ISE

Duo SSO configureren als externe SAML Identity Source

Ga op ISE naar Administration > Identity Management > External Identity Sources > SAML Id Providers en klik op de knop **Toevoegen**.

Voer de naam van de IDp in en klik op **Indienen** om deze op te slaan. De IDp-naam is alleen significant voor ISE zoals in de afbeelding:



Het XML-bestand met SAML-metagegevens importeren vanuit het Duo Admin-portal

Op ISE, navigeer naar Administration > Identity Management > External Identity Sources > SAML Id Providers. > Kies de SAML IDp die u hebt gemaakt, klik op het Identity Provider Configuration en vervolgens op de knop **Bestand kiezen**.

Kies het **SSO IDP Metadata XML** bestand geëxporteerd van Duo Admin portal en klik op **Open** om het op te slaan. (Deze stap wordt ook in het gedeelte Duo van dit document vermeld.)

De SSO URL en de ondertekeningscertificaten zijn:

The screenshot shows the Cisco ISE Administration interface for Identity Management. The left sidebar lists 'External Identity Sources' with options like Certificate Authentication, Active Directory, LDAP, ODBC, RADIUS Token, RSA SecurID, SAML Id Providers, Azure, Duo_SSO, and Social Login. The main content area is titled 'SAML Identity Provider' and is currently on the 'Identity Provider Config.' tab. A red box highlights the 'Identity Provider Configuration' section, which includes an 'Import Identity Provider Config File' button with a 'Choose File' link and a 'Provider Id' field. Below this, the 'Single Sign On URL' is set to 'https://sso-19aa14ff.sso.duosecurity.com/saml2/sp/DIZA6IV4RE8UN8X5ADU6/sso' and the 'Single Sign Out URL (Post)' is 'Not supported by Identity Provider.' A 'Sianina Certificates' table is also visible, with columns for Subject, Issuer, Valid From, Valid To (Expira...), and Serial Number. The table contains one entry with a subject of 'CN=DIZA6IV4RE8UN8X5ADU6, O=Duo Security' and a serial number of '75 EC 9C 6C D5 EB 90 ...'.

ISE-verificatiemethode configureren

Navigeer naar Administration > System > Admin Access > Authentication > Authentication Method en kies de wachtwoordgebaseerde keuzerondje. Kies de gewenste IDp-naam die eerder is gemaakt in de vervolgkeuzelijst Identity Source zoals in de afbeelding:

The screenshot shows the Cisco ISE Administration interface for System > Admin Access > Authentication. The left sidebar shows 'Authentication' selected. The main content area is titled 'Authentication Method' and is currently on the 'Authentication Type' tab. A red box highlights the 'Password Based' radio button, which is selected. Another red box highlights the '* Identity Source' dropdown menu, which is set to 'SAML:Duo_SSO'.

Een beheergroep maken

Navigeer naar Administration > System > Admin Access > Authentication > Administrators > Admin Group en klik op **Super Admin** en vervolgens op de knop **Dupliceren**. Voer de **naam** van de **beheergroep in** en klik op de knop **Verzenden**.

Dit geeft Super Admin-rechten aan de Admin-groep.

Cisco ISE Administration - System

Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Backup & Restore **Admin Access** Settings

Authentication

Authorization >

Administrators >

Admin Users

Admin Groups

Settings >

Admin Groups

[Edit](#) [+ Add](#) [Duplicate](#) [Delete](#) [Reset All Ext. groups](#)

<input type="checkbox"/>	Name	External Groups Mapped	Description
<input type="checkbox"/>	ERS Operator	0	Read-only access permission to the External RESTful Services (ERS) A...
<input type="checkbox"/>	Elevated System Admin	0	Access permission for Operations tab. Includes System and data acces...
<input type="checkbox"/>	Helpdesk Admin	0	Access permission for Operations tab.
<input type="checkbox"/>	ISE Admin Group	0	Access permission for Operations, Policy and Administration tabs. Inclu...
<input type="checkbox"/>	Identity Admin	0	Access permission for Operations tab. Includes Identity Management an...
<input type="checkbox"/>	MnT Admin	0	Access permission for Operations tab.

Een RBAC-beleid voor de Admin-groep maken

Navigeer naar Administration > System > Admin Access > Authorization > RBAC Policy en kies de **acties** die overeenkomen met **het beleid van Super Admin**. Klik op de knop **.Duplicate > Add the Name field > Save**

De toegangsrechten zijn hetzelfde als het Super Admin-beleid.

Cisco ISE Administration - System License Warning

Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Backup & Restore **Admin Access** Settings

Authentication

Authorization >

Permissions >

RBAC Policy

Administrators >

Settings >

Create Role Based Access Control policies by configuring rules based on Admin groups, Menu Access permissions (menu items), Data Access permissions (primary group data elements) and other conditions. Note that multiple Menu/Data Access permissions are not allowed on a single policy. You can copy the default policies shown below, then modify them as needed. Note that system-created and default policies cannot be updated, and default policies cannot be deleted. For decision making, all applicable policies will be evaluated. The subject's permissions will be the aggregate of all permissions from each applicable policy. Permit overrides Deny. (The policies are displayed in alphabetical order of the policy name).

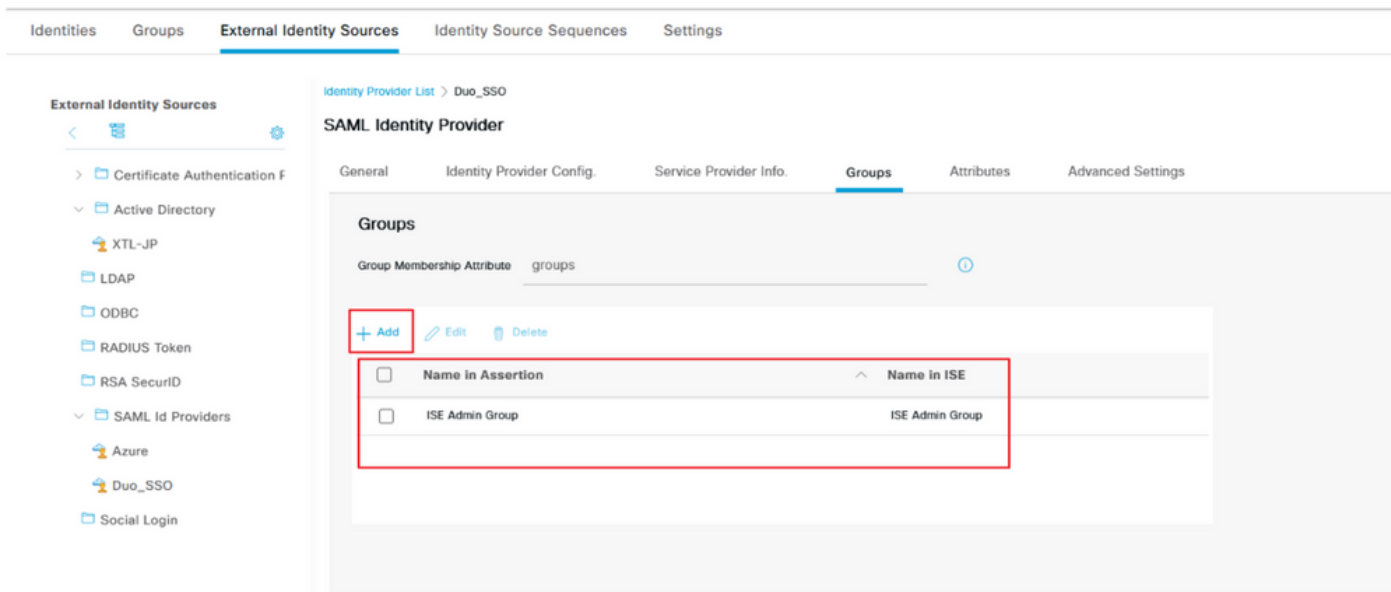
RBAC Policies

Rule Name	Admin Groups	Permissions
Customization Admin Policy	Customization Admin	Customization Admin Menu ...
Elevated System Admin Pol...	Elevated System Admin	System Admin Menu Access...
ERS Admin Policy	ERS Admin	Super Admin Data Access
ERS Operator Policy	ERS Operator	Super Admin Data Access
ERS Trustee Policy	ERS Trustee	Super Admin Data Access
Helpdesk Admin Policy	Helpdesk Admin	Helpdesk Admin Menu Access
ISE Admin Group	ISE Admin Group	Super Admin Menu Access ...
MnT Admin Policy	MnT Admin	Super Admin Menu Access
Network Device Policy	Network Device Admin	Super Admin Data Access
Policy Admin Policy	Policy Admin	RBAC Admin Menu Access ...
RBAC Admin Policy	RBAC Admin	RBAC Admin Menu Access ...
Read Only Admin Policy	Read Only Admin	Super Admin Menu Access ...
SPOG Admin Policy	SPOG Admin	Super Admin Data Access
Super Admin Policy	Super Admin	Super Admin Menu Access ...

Lidmaatschap Groepen toevoegen

Op ISE, navigeer naar Administration > Identity Management > External Identity Sources > SAML Id Providers en kies de SAML IDp die u hebt gemaakt. Klik op **Groepen** en vervolgens op de knop **Toevoegen**.

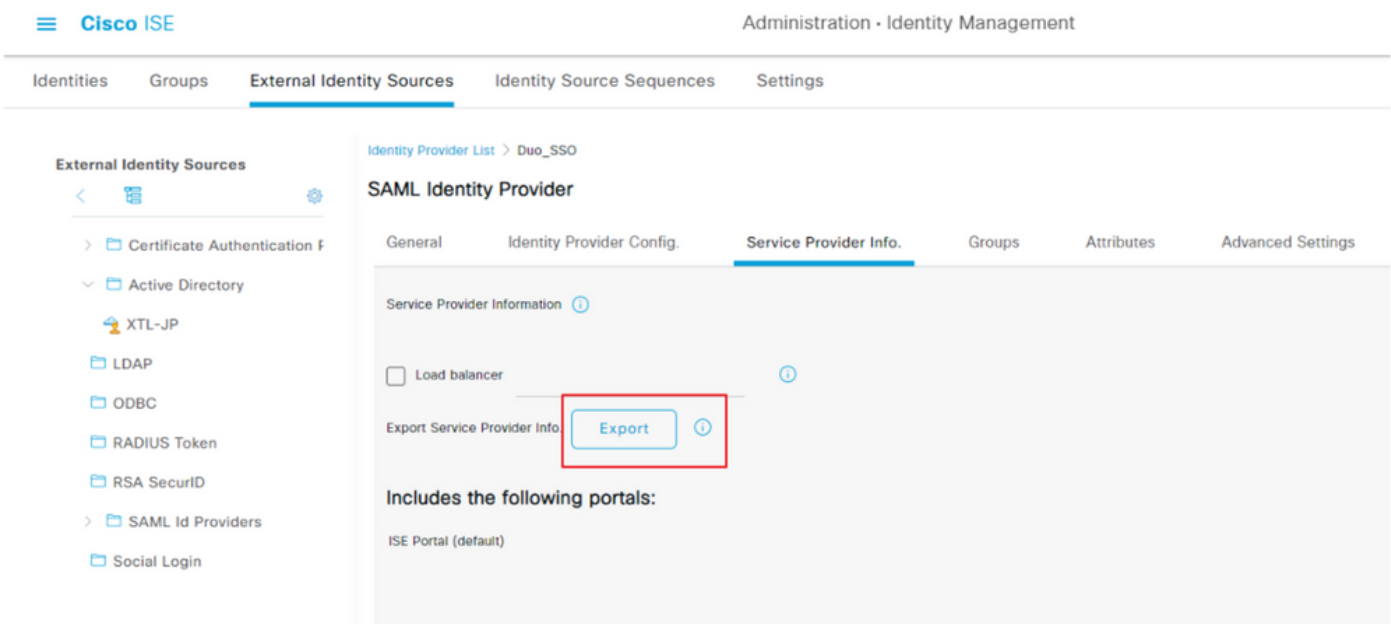
Voeg de naam toe in Assertion (naam van de ISE-beheergroep) en kies vanuit dropdown de Role-Based Access Control (RBAC) Group die is gemaakt (Stap 4.) en klik op **Openen** om het op te slaan. De SSO URL en de ondertekeningscertificaten zijn automatisch ingevuld:



SP-informatie exporteren

Navigeer naar Administration > Identity Management > External Identity Sources > SAML Id Providers > (Your SAML Provider) .

Switch het tabblad naar SP Info. en klik op de knop **Exporteren** zoals in de afbeelding:



Download het .xml bestand en sla het op. Noteer de URL van deAssertionConsumerService locatie en de waarde van **entityID** zoals deze gegevens in het Duo SSO-portal worden gevraagd.

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

Hier zijn de details/attributen van belang verzameld uit het meta-bestand dat moet worden geconfigureerd in de Duo Generic SAML Integration

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

AssertionConsumerService Location = <https://10.x.x.x:8443/portal/SSOLoginResponse.action> waar 10.x.x.x de ISE IP gevonden op het XML-bestand (Location).

AssertionConsumerService Location = <https://isenodename.com:8443/portal/SSOLoginResponse.action> waar isenodename de daadwerkelijke naam van ISE FQDN gevonden op het XML-bestand (Location) is.

Stap 2. Duo SSO configureren voor ISE

Controleer deze [KB](#) om Duo SSO met AD als verificatiebron te configureren.

Configured Authentication Sources

[+ Add source](#)

Name	Type	Status	Authentication Proxies
Active Directory	Active Directory	Enabled	Authentication Proxy

Controleer deze [KB](#) om de SSO in te schakelen met uw eigen domein.

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](#)

Stap 3. Integratie van Cisco ISE met Duo SSO als generieke servicesmodule

Controleer Stap 1 en Stap 2 van deze [KB](#) om Cisco ISE te integreren met Duo SSO als Generic SP.

Cisco ISE-SP-gegevens configureren in het Duo Admin Panel voor Generic SP:

Naam	Beschrijving
Entiteits-ID	http://CiscoISE/7fdcf239-631e-439c-a3ab-f5e56429779d
URL voor Assertion Consumer Service (ACS)	https://10.x.x.x:8443/portal/SSOLoginResponse.action

Service Provider

Entity ID *

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

The unique identifier of the service provider.

Assertion Consumer Service (ACS) URL *

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

SAML Response configureren voor Cisco ISE:

Naam	Beschrijving
NaamID-indeling	draai:oase:namen:tc:SAML:1.1:benoemde-indeling:niet gespecificeerd
Kenmerk naamID	Username

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>.

Maak een groep met de naam Cisco Admin Group in het Duo Admin Panel en voeg de ISE-gebruikers aan deze groep toe of maak een groep in Windows AD en synchroniseer hetzelfde aan het Duo Admin-paneel met behulp van de functie directory Sync.

Role-kenmerken configureren voor Cisco ISE:

Naam	Beschrijving
Naam kenmerk	groepen
SP-rol	ISE-beheergroep
Duo-groepen	ISE-beheergroep

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

In het gedeelte Settings typt u een geschikte naam op het tabblad **Name** voor deze integratie.

Settings

Type

Generic Service Provider - Single Sign-On

Name

Duo Push users will see this when approving transactions.

Klik op de knop **Opslaan** om de configuratie op te slaan en raadpleeg deze [KB](#) voor meer informatie.

Klik op **Download XML** om de SAML Metadata te downloaden.

Downloads

Certificate

[Download certificate](#)

Expires: 01-19-2038

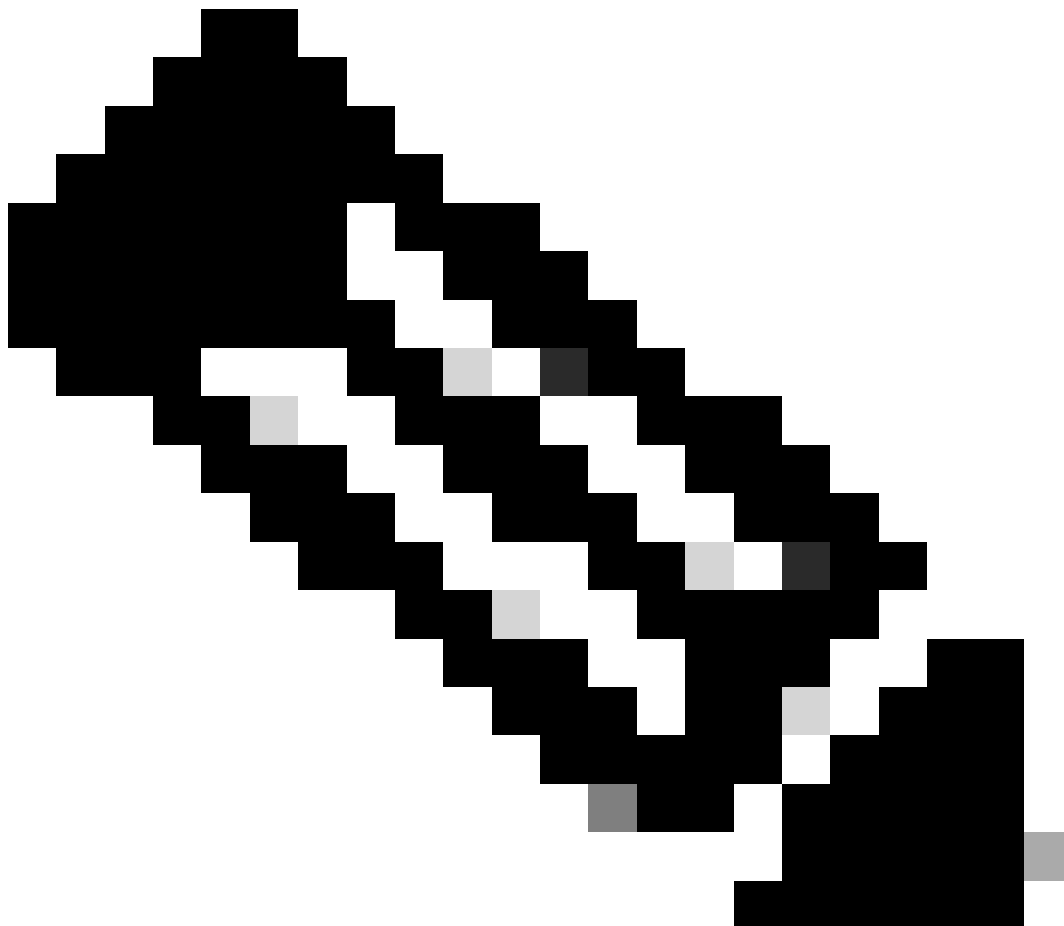
SAML Metadata

[Download XML](#)

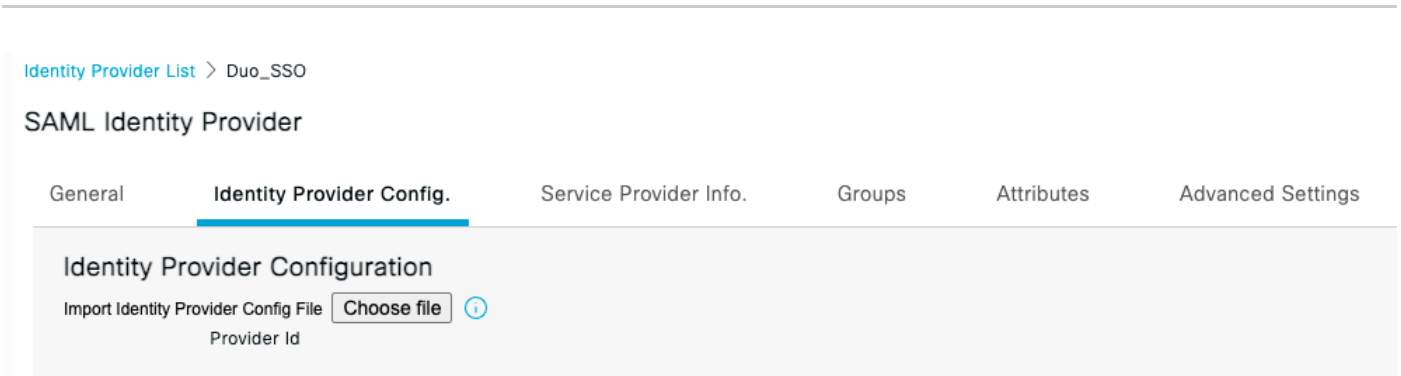
Upload SAML MetaData download van Duo Admin Panel naar Cisco ISE door naar Administration > Identity Management > External Identity Sources > SAML Id Providers > Duo_SSO te navigeren.

Switch het tabblad naar **Identity Provider Config**, en klik op de knop **Kies** bestand.

Kies het **XML**-bestand met **metagegevens dat** in Stap 8 is gedownload en klik op **Opslaan**.



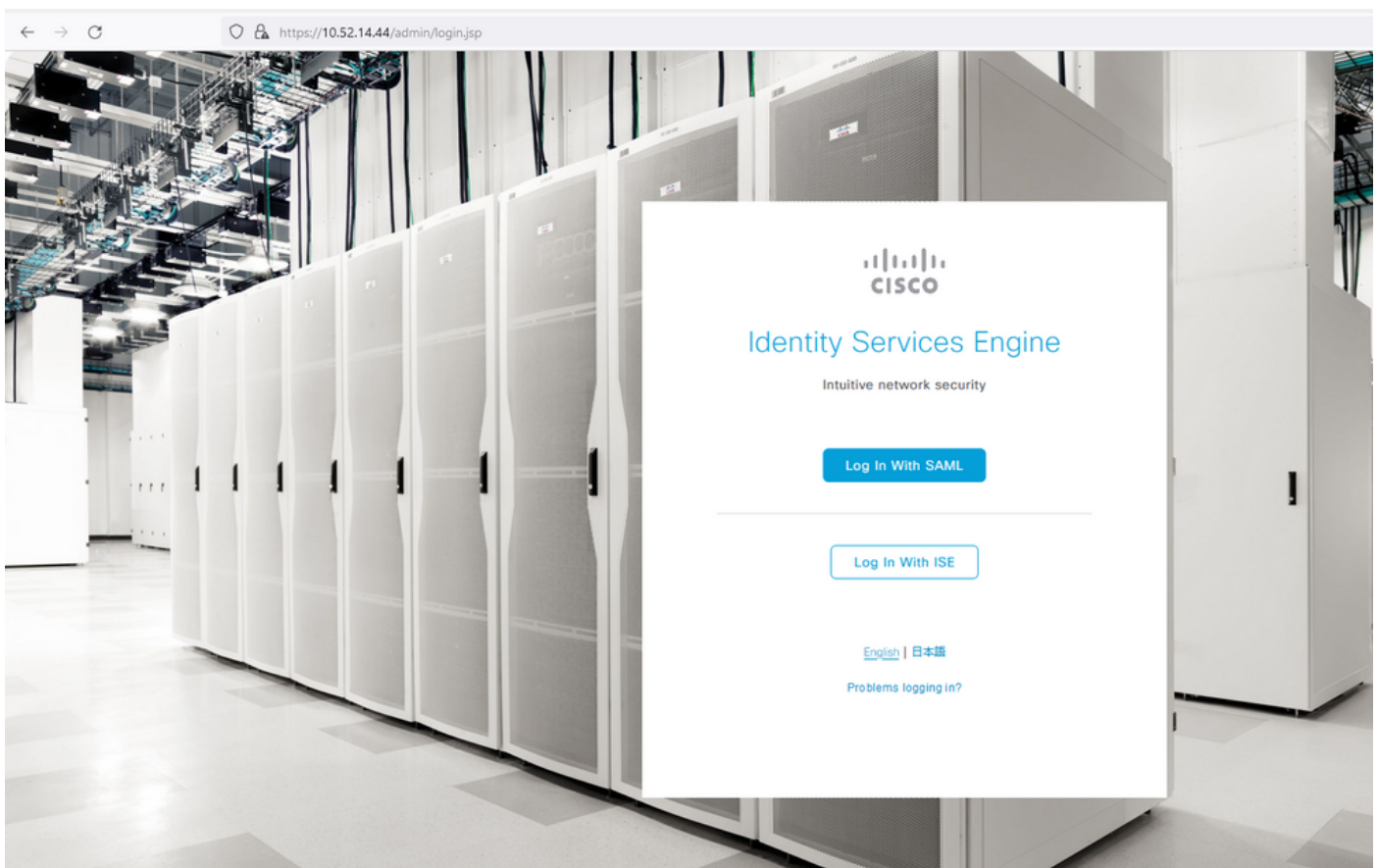
Opmerking: deze stap wordt hier vermeld onder het hoofdstuk Integratie van SAML SSO configureren met Duo SSO; Stap 2. Importeer het **SAML Metadata XML** bestand vanuit het Duo Admin portal.



Verifiëren

De integratie met Duo SSO testen

1. Log in op het **Cisco ISE-beheerpaneel** en klik op **Inloggen met SAML**.

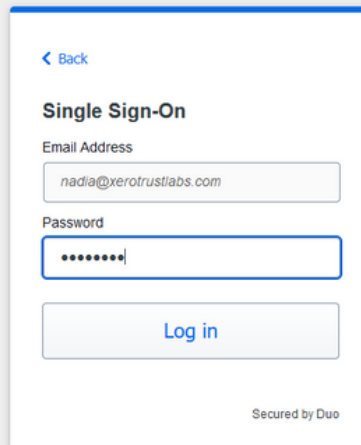


2. Ga naar de SSO-pagina, voer het **e-mailadres in** en klik op **Volgende**.



The image shows a web browser window displaying a Cisco Single Sign-On page. The page has a white background with a blue border. At the top left is the Cisco logo. Below it, the text "Single Sign-On" is displayed in bold. Underneath, the label "Email Address" is 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. Voer het wachtwoord in en klik op **Inloggen**.

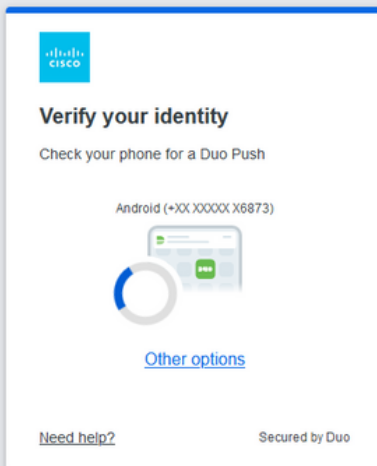


The image shows a web browser window displaying a Cisco Single Sign-On page. The page has a white background with a blue border. At the top left is a blue arrow pointing left with the text "Back". Below it, the text "Single Sign-On" is displayed in bold. Underneath, the label "Email Address" is followed by a text input field containing the email address "nadia@zerotrustlabs.com". Below that, the label "Password" is followed by a password input field containing several dots. Below the password field is a button labeled "Log in". At the bottom right of the form, it says "Secured by Duo".

4. U krijgt een Duo Push-prompt op uw mobiele apparaat.

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. Zodra u de prompt accepteert, krijgt u een venster en wordt u automatisch doorgestuurd naar de ISE-beheerpagina.

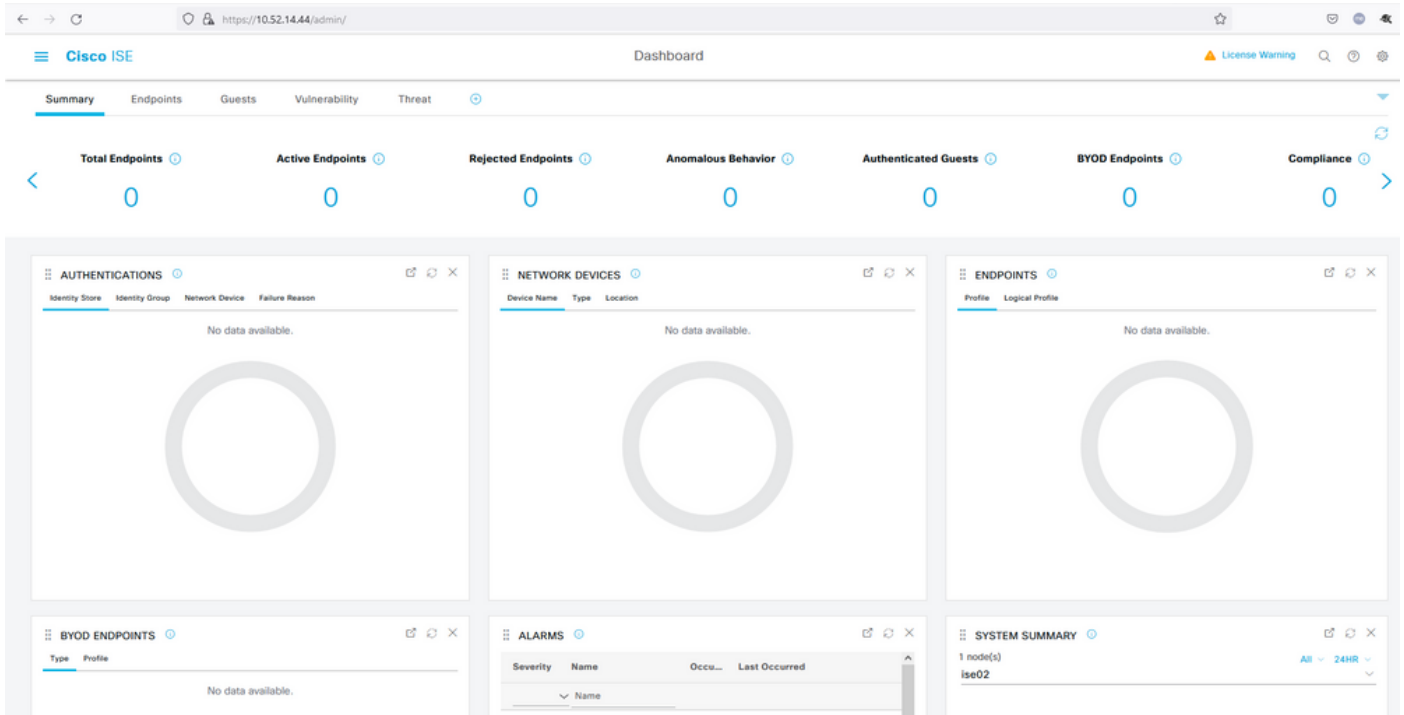


Success!

Logging you in...



Secured by Duo



Problemen oplossen

- Download de SAML tracer extensie voor Mozilla FF <https://addons.mozilla.org/en-US/firefox/addon/saml-tracer/>.
- Blader naar het SSOLoginResponse.action pakket. Onder het tabblad **SAML** ziet u een aantal attributen verzonden vanuit Duo SAML: NaamID, Ontvanger (AssertionConsumerService Location URL), en Publiek (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>MIIDDTCCAfwAwIBAgIUCbf+LB1BLJMeF6GV0B1rmdX3AVEwDQYJKoZIhvcNAQELBQAwNjEVMGMGA1UECgwMRHRvIFN1Y3VyaXR5MR0wGwYDVQDD
BRESTZPODg2UkxETUJZMzExSFBjMjEwFw0zODAxMTkwMzE0MDdaMDYxFTATBgNVBAoMDER1byBTZW51cm10eTEEdMBsGA1UEAwwURk2Tzg4N1JMRE
1CWTMxMhUqSTIwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDB03Ayuh9avw0NoQzIhQZzU9H8vu/HSKLSH30585Mukj5FnoVV50PGTuoFN4u90t
sIFULjC8eQnUsBR1PYQ5jtOV23qVnvoGyqsuHas8nbKwvzpzShzNF59p03pXkoGPuB+Du2Irrvv0opSv4vbrgKV+H/bvMqyhIA6ywfHNZedG7pbwrYBtVPDXUpnLQvtL2
/Vd9230XuXHF+k32hagRgTLub5XyT1HHQ8b4n3mQKHs6yA/KNvaB3b/AMUqAXDqaEXNG0uQENMK30wTs49
/w+r5fz7xp66muRc0IBg3xjWnnFnyujy7v5ifn1KFUFQu+86A5GbuUWCyiaKmV7CztAgMBAAGjEzARMA8GA1UdEwEB
/wQFMAMBAF8wDQYJKoZIhvcNAQELBQADggEBAH+KItcw0KtDxxBvZ5S+25a+50F4Tqd/pH56i19d2kDxInSUVsy
/Yy1FXAWge3WBke4b3JR7znD6000sZTYbF9w7H4svU2gxzdk0znXJNj2e4C5fDinvj/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_EQUALS1RS257BC24SGVHZW76GMVEZNR0YCC_LSEMI_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 Log in 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

- Administratieve Login log in op ISE: gebruikersnaam: samlUser.

- 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		10.85.48.163	16402	Administrator authentication succeeded	Administrator authentication successful

Rows/Page 1 1 Total Rows

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.