

Configuration de la connexion administrateur de l'interface utilisateur graphique ISE 3.1 avec l'intégration SAML avec Duo SSO et Windows AD

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Fournisseur d'identité \(IdP\)](#)

[Fournisseur de services \(SP\)](#)

[SAML](#)

[Assertion SAML](#)

[Diagramme D'Écoulement De Haut Niveau](#)

[Configuration de l'intégration SSO SAML avec Duo SSO](#)

[Étape 1. Configurer le fournisseur d'ID SAML sur ISE](#)

[Configurer Duo SSO comme source d'identité SAML externe](#)

[Importer le fichier XML de métadonnées SAML à partir du portail d'administration Duo](#)

[Configurer la méthode d'authentification ISE](#)

[Créer un groupe d'administrateurs](#)

[Créer une stratégie RBAC pour le groupe Admin](#)

[Ajouter l'appartenance aux groupes](#)

[Exporter les informations SP](#)

[Étape 2. Configuration de Duo SSO pour ISE](#)

[Étape 3. Intégrer Cisco ISE avec Duo SSO en tant que SP générique](#)

[Vérifier](#)

[Test de l'intégration avec Duo SSO](#)

[Dépannage](#)

Introduction

Ce document décrit comment configurer l'intégration SSO SAML de Cisco ISE 3.1 avec un fournisseur d'identité externe comme Cisco Duo SSO.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco ISE (Identity Services Engine) 3.1
- Connaissances de base sur les déploiements SAML (Security Assertion Markup Language) SSO (Single Sign-On) (SAML 1.1)
- Connaissance de Cisco DUO SSO
- Connaissance de Windows Active Directory

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Fournisseur d'identité (IdP)

C'est le Duo SSO dans ce cas, qui vérifie et affirme une identité d'utilisateur et des privilèges d'accès à une ressource demandée (le « Fournisseur de service »).

Duo SSO agit en tant que fournisseur d'identité, authentifiant vos utilisateurs à l'aide d'Active Directory (AD) existant sur site avec SAML 1.1 ou tout fournisseur d'identité SAML 2.0 (par exemple, Microsoft Azure) et demandant une authentification à deux facteurs avant d'autoriser l'accès à votre application de fournisseur de services.

Lors de la configuration d'une application à protéger avec Duo SSO, vous devez envoyer des attributs de Duo SSO à l'application. Active Directory fonctionne sans configuration supplémentaire, mais si vous avez utilisé un fournisseur d'identité SAML(2.0) comme source d'authentification, vérifiez que vous l'avez configuré pour envoyer les attributs SAML corrects.

Fournisseur de services (SP)

Ressource ou service hébergé auquel l'utilisateur a l'intention d'accéder ; Cisco ISE Application Server dans ce cas.

SAML

SAML est une norme ouverte qui permet au fournisseur d'identité de transmettre des informations d'identification d'autorisation au fournisseur de services.

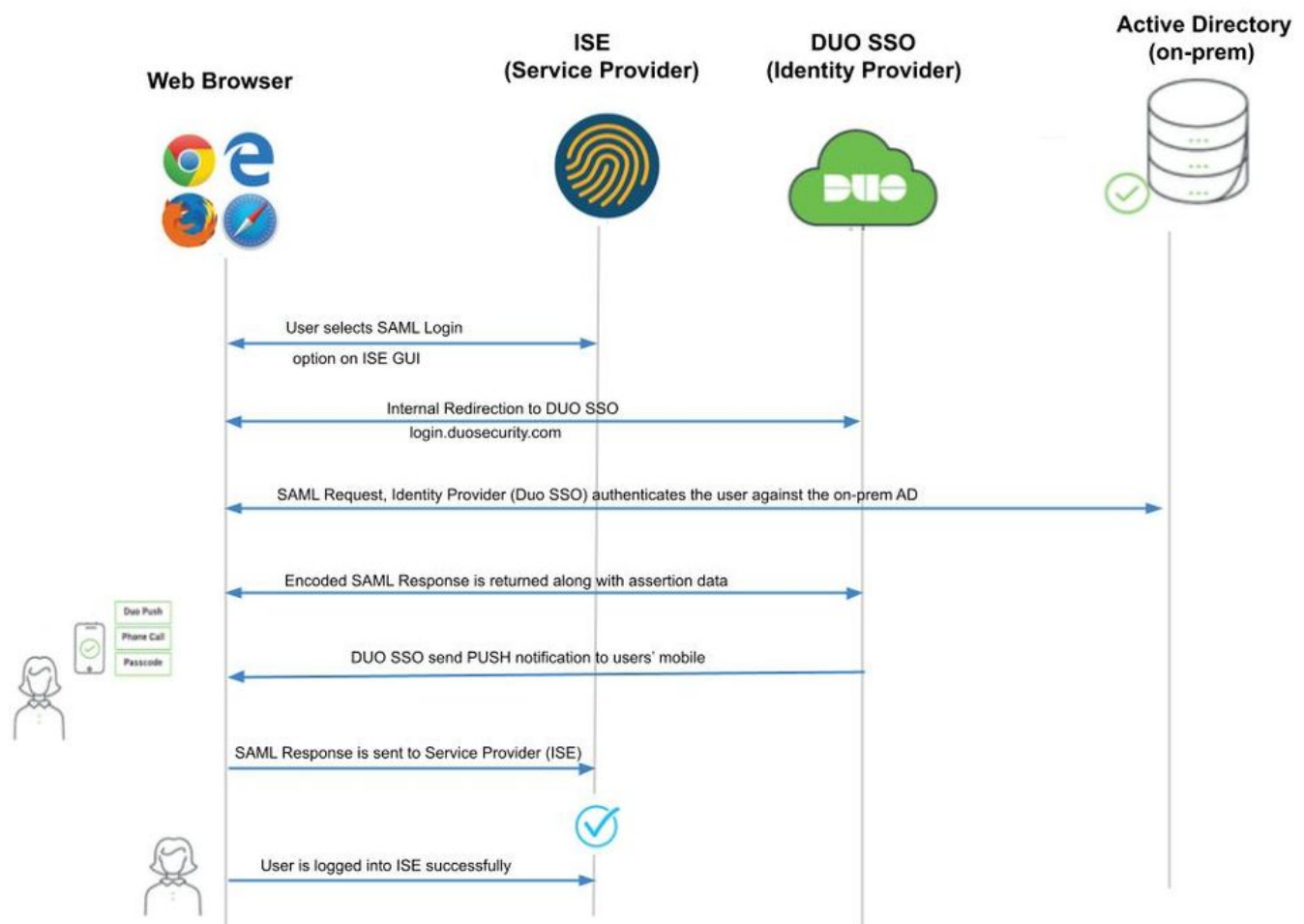
Les transactions SAML utilisent le langage XML (Extensible Markup Language) pour les communications normalisées entre le fournisseur d'identité et les fournisseurs de services. SAML est le lien entre l'authentification de l'identité de l'utilisateur et l'autorisation d'utiliser un service.

Assertion SAML

Une assertion SAML est le document XML que le fournisseur d'identité envoie au fournisseur de services qui contient l'autorisation utilisateur. Il existe trois types différents d'assertions SAML : l'authentification, l'attribut et la décision d'autorisation.

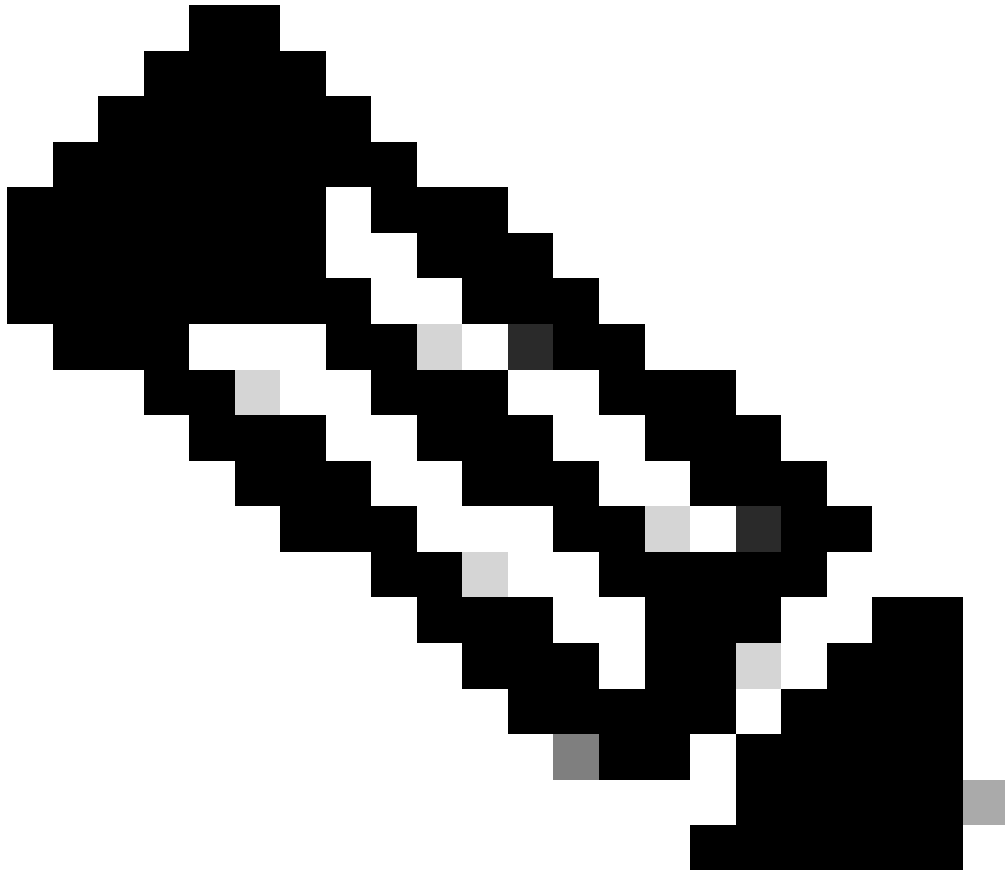
- Les assertions d'authentification prouvent l'identification de l'utilisateur et indiquent l'heure à laquelle l'utilisateur s'est connecté et la méthode d'authentification qu'il a utilisée (par exemple, Kerberos, à deux facteurs, etc.).
- L'assertion d'attribution transmet les attributs SAML, des données spécifiques qui fournissent des informations sur l'utilisateur, au SP.
- Une assertion de décision d'autorisation indique si l'utilisateur est autorisé à utiliser le service ou si le fournisseur d'identité a refusé sa demande en raison d'un échec de mot de passe ou d'un manque de droits sur le service.

Diagramme D'Écoulement De Haut Niveau



Flux :

1. L'utilisateur se connecte à ISE à l'aide de l'option Login Via SAML.
 2. ISE (SAML SP) redirige le navigateur de l'utilisateur vers Duo SSO avec un message de requête SAML.
-



Remarque : dans un environnement distribué, vous pouvez obtenir une erreur Invalid Certificate et l'étape 3. peut maintenant fonctionner. Par conséquent, pour un environnement distribué, l'étape 2 diffère légèrement de la manière suivante :
Problème : ISE redirige temporairement vers le portail de l'un des nœuds PSN (sur le port 8443).

Solution : afin de s'assurer qu'ISE présente le même certificat que le certificat de l'interface utilisateur graphique d'administration, assurez-vous que le certificat système que vous approuvez est également valide pour l'utilisation du portail sur tous les nœuds PSN.

-
3. L'utilisateur se connecte avec les informations d'identification AD principales.
 4. Duo SSO transmet ce message à AD qui renvoie une réponse à Duo SSO.
 5. Duo SSO exige que l'utilisateur effectue une authentification à deux facteurs en envoyant

une requête PUSH sur le mobile.

6. L'utilisateur termine l'authentification à deux facteurs Duo.
7. Duo SSO redirige le navigateur de l'utilisateur vers le SP SAML avec un message de réponse.
8. L'utilisateur peut désormais se connecter à ISE.

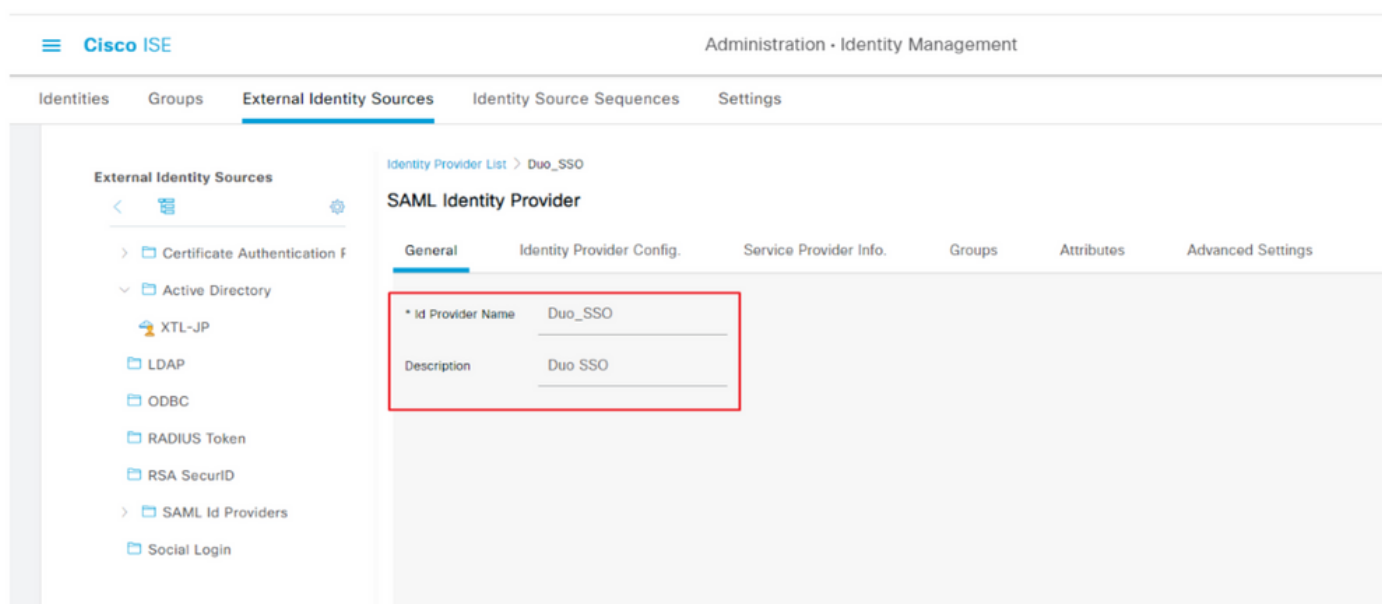
Configuration de l'intégration SSO SAML avec Duo SSO

Étape 1. Configurer le fournisseur d'ID SAML sur ISE

Configurer Duo SSO comme source d'identité SAML externe

Sur ISE, accédez à Administration > Identity Management > External Identity Sources > SAML Id Providers et cliquez sur le bouton **Add**.

Entrez le nom de l'IdP et cliquez sur **Submit** afin de l'enregistrer. Le nom du fournisseur d'identité n'est significatif que pour ISE, comme illustré dans l'image :



Importer le fichier XML de métadonnées SAML à partir du portail d'administration Duo

Sur ISE, accédez à Administration > Identity Management > External Identity Sources > SAML Id Providers. > Choisissez le fournisseur d'ID SAML que vous avez créé, cliquez sur Identity Provider Configuration, puis sur le bouton **Choisir un fichier**.

Choisissez le fichier **SSO IDP Metadata XML** exporté depuis le portail Duo Admin et cliquez sur **Open** afin de l'enregistrer. (Cette étape est également mentionnée dans la section Duo de ce document.)

L'URL SSO et les certificats de signature sont :

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 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 for the 'Provider Id' field. Below this, there are fields for 'Single Sign On URL' (https://sso-19aa14ff.sso.duosecurity.com/saml2/sp/DIZA6IV4RE8UN8X5ADU6/sso) and 'Single Sign Out URL (Post)'. A 'SAML Certificates' table is also visible with columns for Subject, Issuer, Valid From, Valid To (Expires), and Serial Number.

Configurer la méthode d'authentification ISE

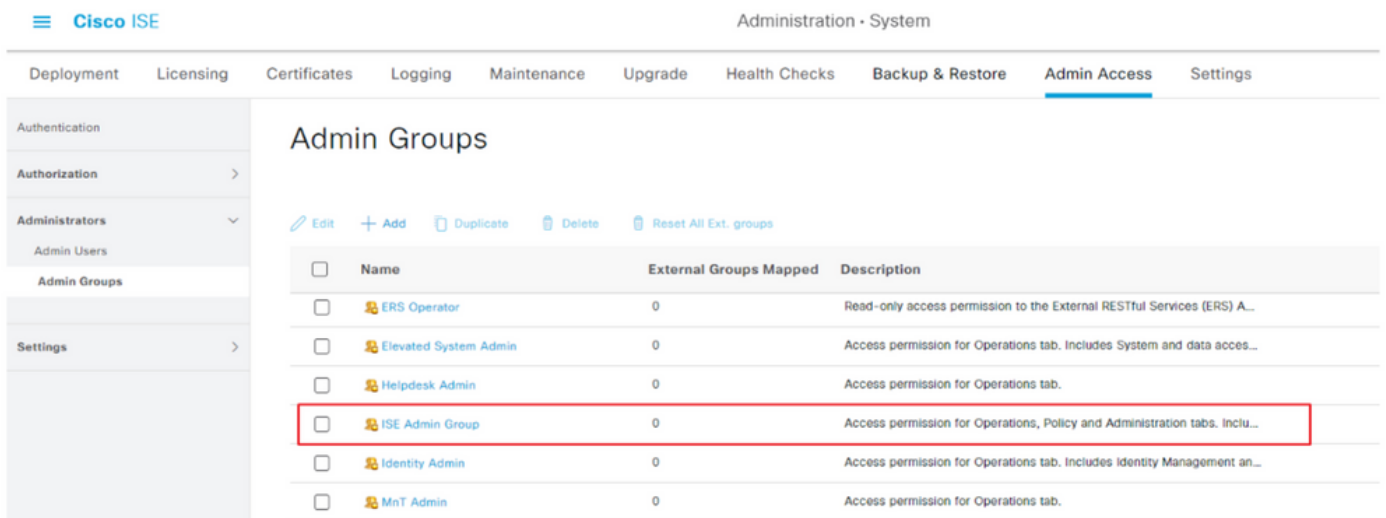
Accédez à la case d'option Password-Based (Basé sur mot de passe) Administration > System > Admin Access > Authentication > Authentication Method et sélectionnez-la. Choisissez le nom de fournisseur d'identité requis créé précédemment dans la liste déroulante Source d'identité, comme indiqué dans l'image :

The screenshot shows the Cisco ISE Administration interface for System > Admin Access. The left sidebar lists 'Authentication', 'Authorization', 'Administrators', and 'Settings'. The main content area is titled 'Admin Access' and has tabs for 'Authentication Method', 'Password Policy', 'Account Disable Policy', and 'Lock/Suspend Settings'. The 'Authentication Method' tab is active, showing an 'Authentication Type' section with two radio button options: 'Password Based' (selected) and 'Client Certificate Based'. Below this, there is a dropdown menu for '* Identity Source' with 'SAML:Duo_SSO' selected.

Créer un groupe d'administrateurs

Accédez à Administration > System > Admin Access > Authentication > Administrators > Admin Group et cliquez sur **Super Admin**, puis sur le bouton **Dupliquer**. Saisissez le **nom** du **groupe Admin** et cliquez sur le bouton **Submit**.

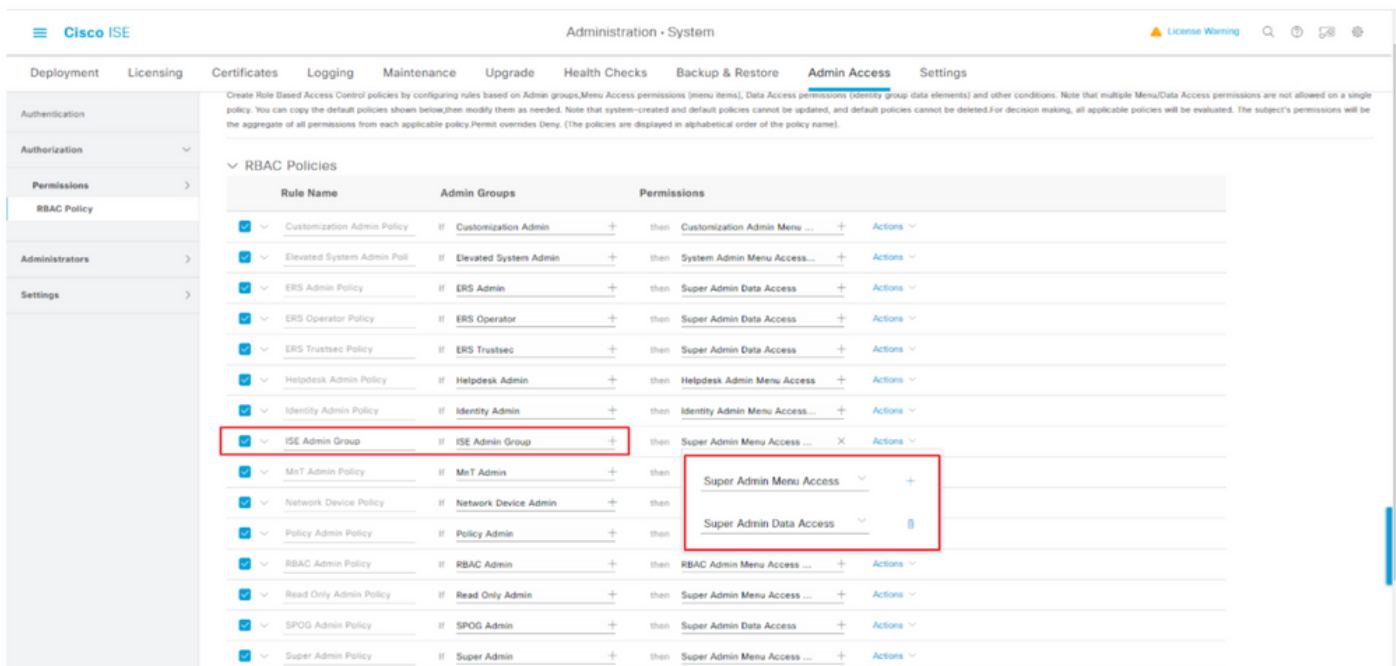
Cela permet d'accorder des privilèges de super administrateur au groupe Admin.



Créer une stratégie RBAC pour le groupe Admin

Accédez à Administration > System > Admin Access > Authorization > RBAC Policy et sélectionnez les **actions** correspondant à **Super Admin Policy**. Cliquez sur Duplicate > Add the Name field > Save.

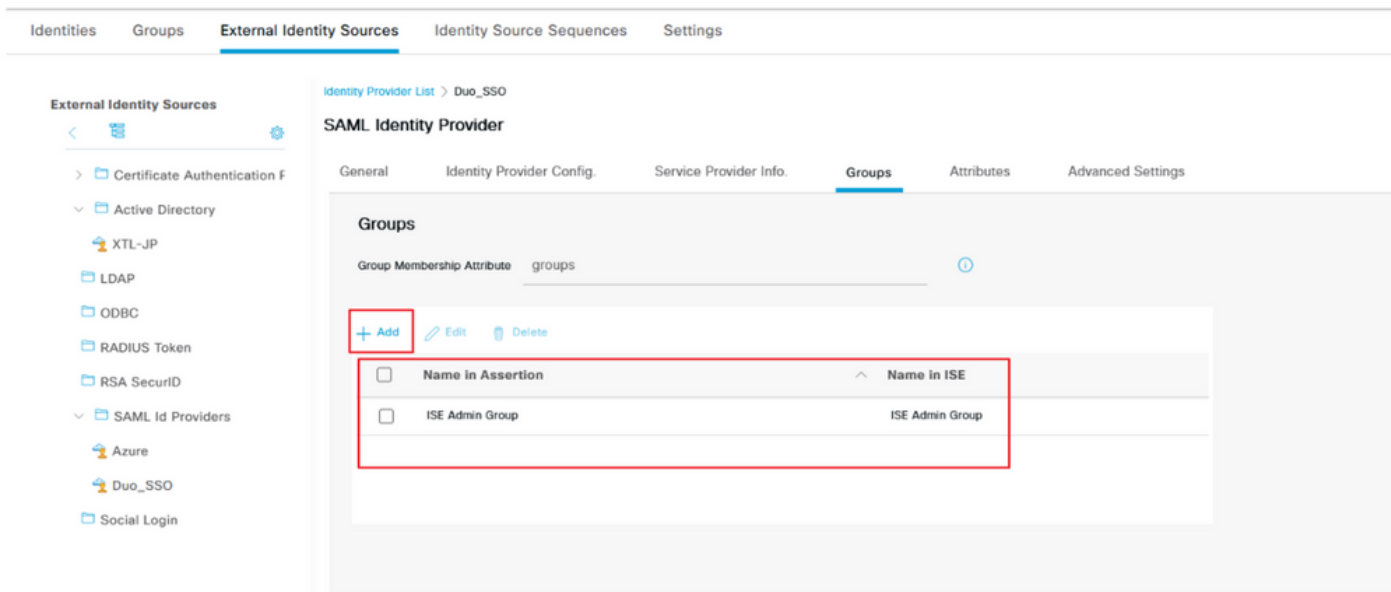
Les autorisations d'accès sont identiques à la stratégie de super administration.



Ajouter l'appartenance aux groupes

Sur ISE, accédez à Administration > Identity Management > External Identity Sources > SAML Id Providers et sélectionnez le fournisseur d'ID SAML que vous avez créé. Cliquez sur **Groups**, puis sur le bouton Add.

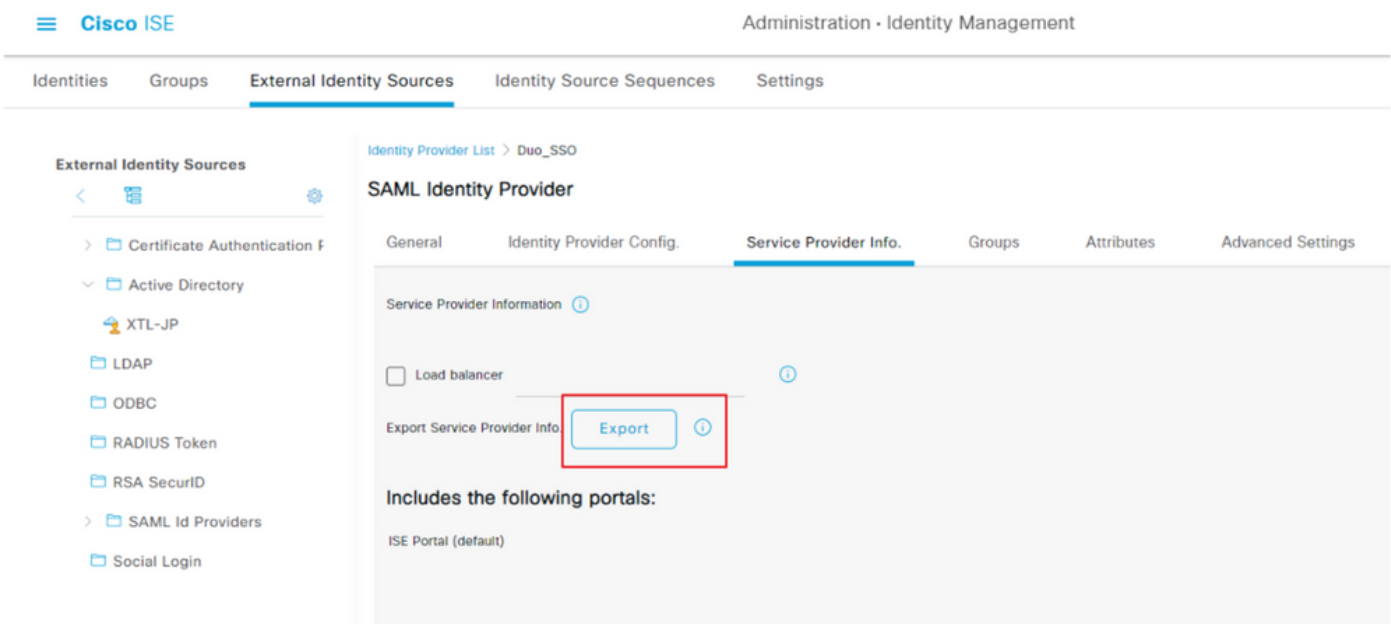
Ajoutez le nom dans l'assertion (Nom du groupe d'administration ISE) et dans la liste déroulante, choisissez le groupe de contrôle d'accès basé sur les rôles (RBAC) créé (Étape 4.0) et cliquez sur **Open** afin de l'enregistrer. L'URL SSO et les certificats de signature sont renseignés automatiquement :



Exporter les informations SP

Accédez à Administration > Identity Management > External Identity Sources > SAML Id Providers > (Your SAML Provider) .

Basculez l'onglet vers SP Info. et cliquez sur le bouton **Export** comme illustré dans l'image :



Téléchargez le fichier.xml et enregistrez-le. Notez l'URL de l'AssertionConsumerService'emplacement et la valeur **entityID** car ces détails sont requis dans le portail Duo SSO.

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

Voici les détails/attributs d'intérêt recueillis à partir du méta-fichier qui doit être configuré dans l'intégration SAML générique Duo

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

AssertionConsumerService Location = <https://10.x.x.x:8443/portal/SSOLoginResponse.action> où 10.x.x.x est l'adresse IP ISE trouvée dans le fichier XML (Location).

AssertionConsumerService Location = <https://isenodename.com:8443/portal/SSOLoginResponse.action> où isenodename est le nom de domaine complet ISE réel trouvé dans le fichier XML (Location).

Étape 2. Configuration de Duo SSO pour ISE

Cochez cette case [KB](#) afin de configurer Duo SSO avec AD comme source d'authentification.

Configured Authentication Sources

[+ Add source](#)

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

Cochez cette case [KB](#) afin d'activer l'SSO avec votre domaine personnalisé.

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

Étape 3. Intégrer Cisco ISE avec Duo SSO en tant que SP générique

Cochez les étapes 1. et 2. de cette [base de connaissances](#) afin d'intégrer Cisco ISE avec Duo SSO en tant que SP générique.

Configurez les détails de Cisco ISE SP dans le panneau d'administration Duo pour le SP générique :

Nom	Description
ID entité	http://CiscoISE/7fdfc239-631e-439c-a3ab-f5e56429779d
URL ACS (Assertion Consumer Service)	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>

Configurez la réponse SAML pour Cisco ISE :

Nom	Description
Format NameID	urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
Attribut NameID	Nom d'utilisateur

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>.

Créez un groupe appelé Groupe d'administration Cisco dans le panneau d'administration Duo et ajoutez les utilisateurs ISE à ce groupe ou créez un groupe dans Windows AD et synchronisez-le avec le panneau d'administration Duo à l'aide de la fonctionnalité de synchronisation de répertoire.

Configurez les attributs de rôle pour Cisco ISE :

Nom	Description
Nom d'attribut	groupes
Rôle SP	Groupe d'administration ISE
Groupes duo	Groupe d'administration ISE

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

+

Dans la section Paramètres, indiquez un nom approprié dans l'onglet **Nom** pour cette intégration.

Settings

Type

Generic Service Provider - Single Sign-On

Name

Duo Push users will see this when approving transactions.

Cliquez sur le bouton **Save** afin d'enregistrer la configuration et référez-vous à cette [Ko](#) pour plus de détails.

Cliquez sur **Download XML** afin de télécharger les métadonnées SAML.

Downloads

Certificate

[Download certificate](#)

Expires: 01-19-2038

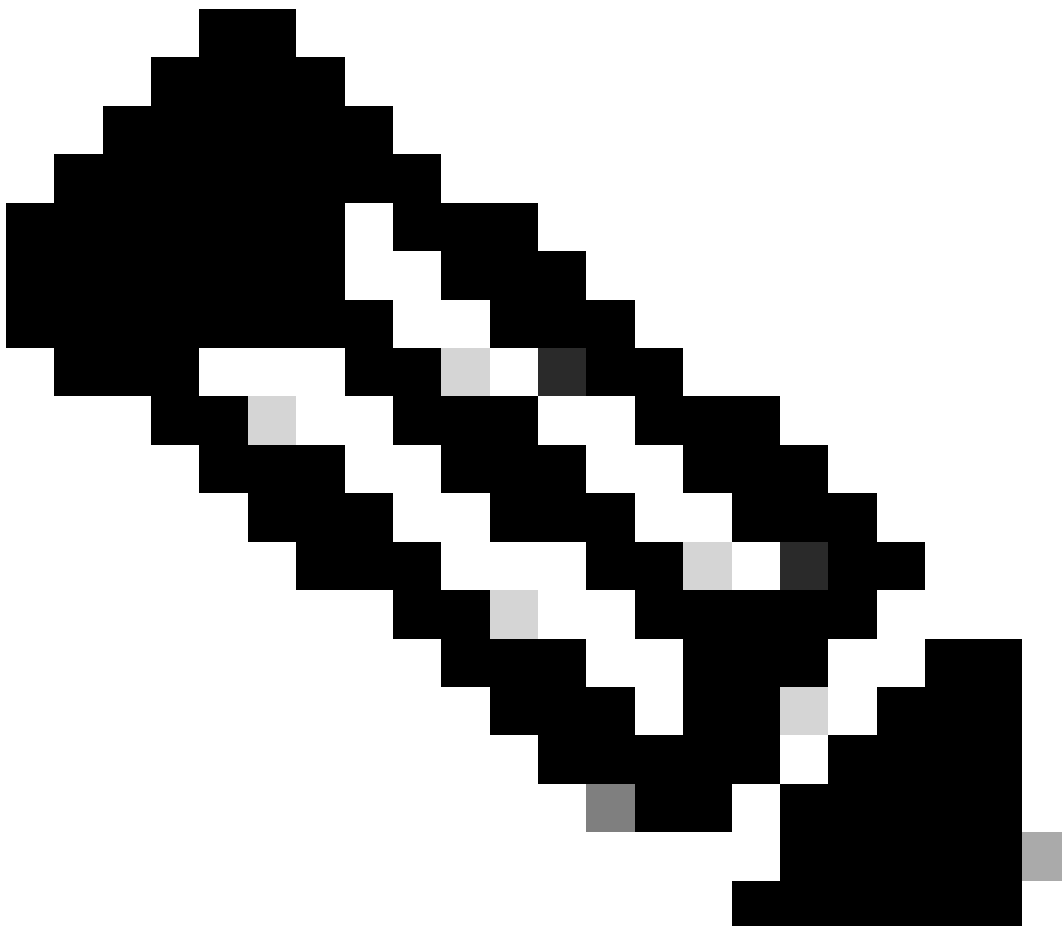
SAML Metadata

[Download XML](#)

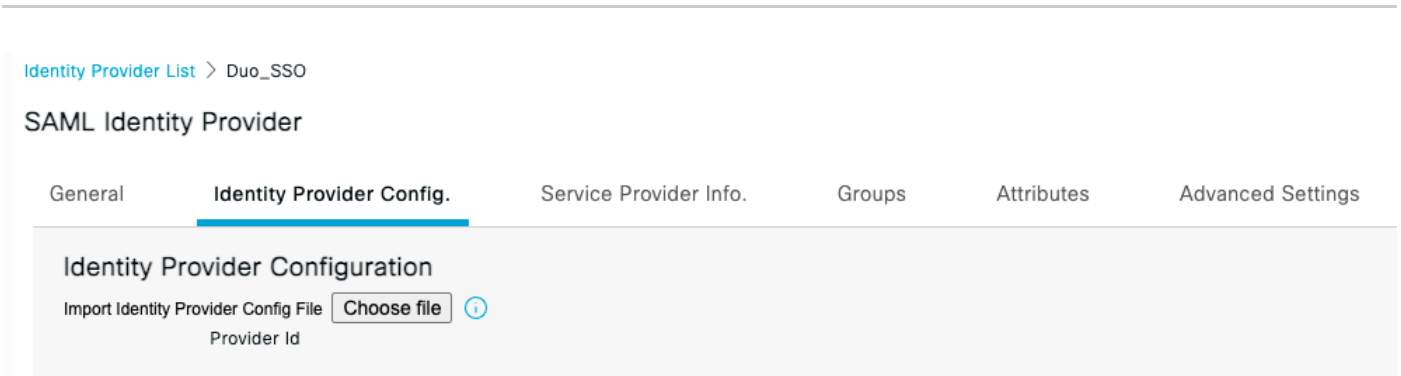
Téléchargez les métadonnées SAML à partir du panneau d'administration Duo vers Cisco ISE en naviguant jusqu'à Administration > Identity Management > External Identity Sources > SAML Id Providers > Duo_SSO.

Basculez l'onglet vers **Identity Provider Config**, et cliquez sur le bouton **Choose file**.

Sélectionnez le fichier **XML de métadonnées** téléchargé à l'étape 8. et cliquez sur **Enregistrer**.



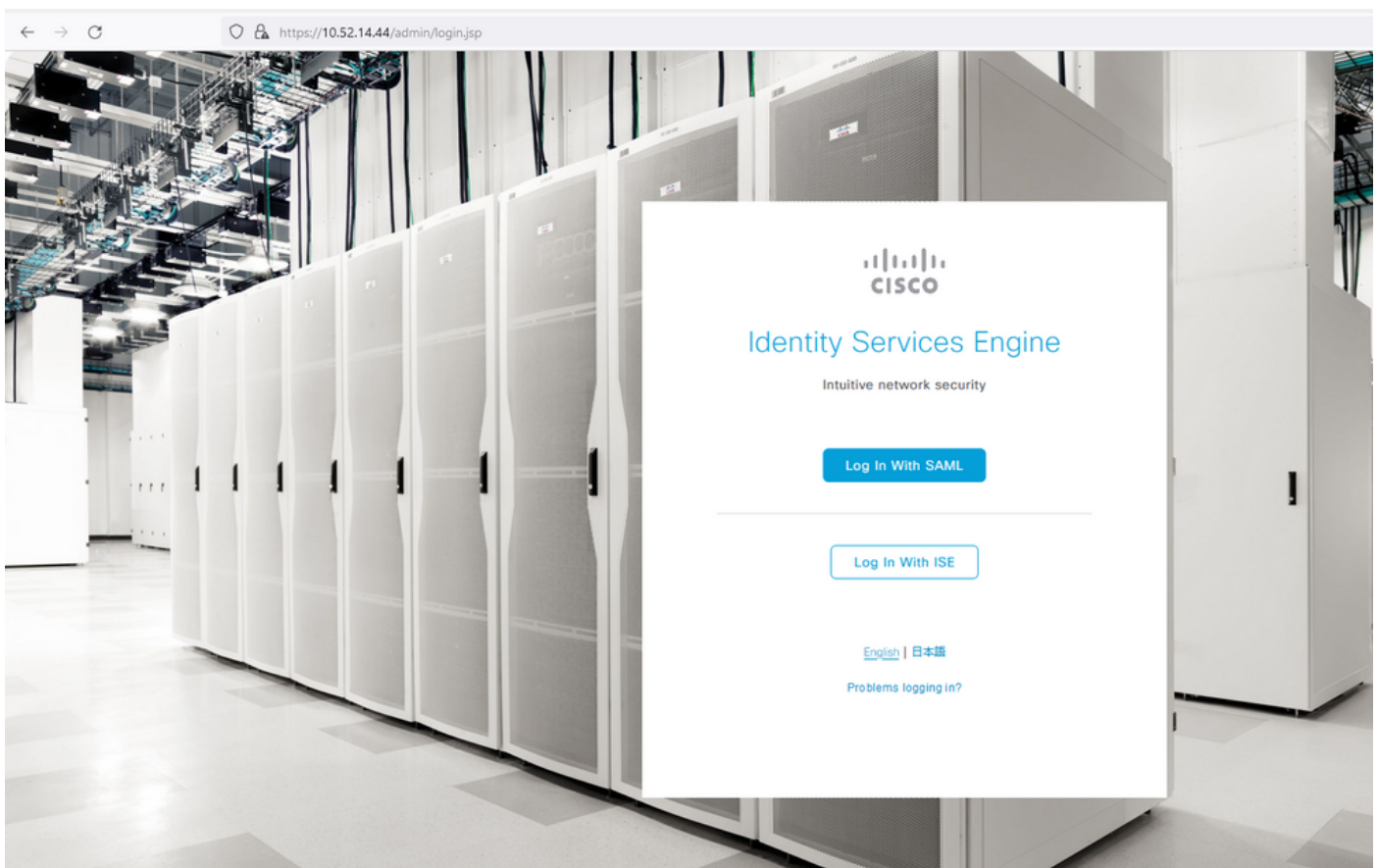
Remarque : cette étape est mentionnée ici dans la section Configurer l'intégration SSO SAML avec Duo SSO ; Étape 2. Importez le fichier **XML de métadonnées SAML** à partir du portail Duo Admin.



Vérifier

Test de l'intégration avec Duo SSO

1. Connectez-vous au **panneau d'administration de Cisco ISE** et cliquez sur **Log In With SAML**.

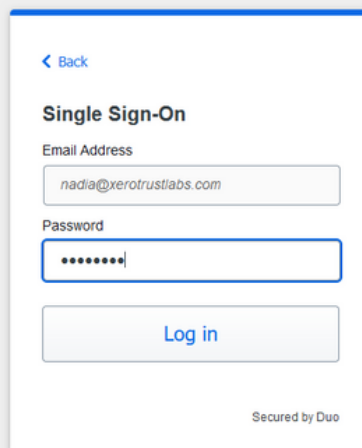


2. Redirigé vers la page SSO, saisissez l'**adresse e-mail** et cliquez sur **Next**.



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. Entrez le mot de passe et cliquez sur **Connexion**.

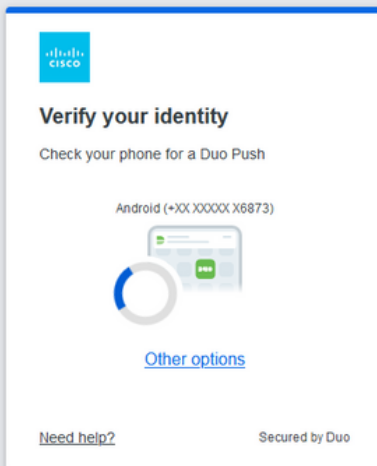


The image shows the same Cisco Single Sign-On form as in the previous step, but now with a password field. At the top left is a blue back arrow labeled "Back". Below it, the text "Single Sign-On" is displayed. Underneath, there is a label "Email Address" followed by a text input field containing the email address "nadia@zerotrustlabs.com". Below that is a label "Password" followed by a password input field 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. Vous obtenez une invite Duo Push sur votre appareil mobile.

Duo needs your help

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



The image shows a Duo authentication prompt window. At the top left is the Cisco Duo logo. The main heading is "Verify your identity". Below this, it says "Check your phone for a Duo Push". A phone number is displayed: "Android (+XX XXXXX X6873)". There is an illustration of a smartphone with a Duo push notification on the screen. Below the phone number is a link for "Other options". At the bottom left is a link for "Need help?" and at the bottom right is the text "Secured by Duo".

5. Une fois que vous avez accepté l'invite, vous obtenez une fenêtre et êtes automatiquement redirigé vers la page ISE Admin.

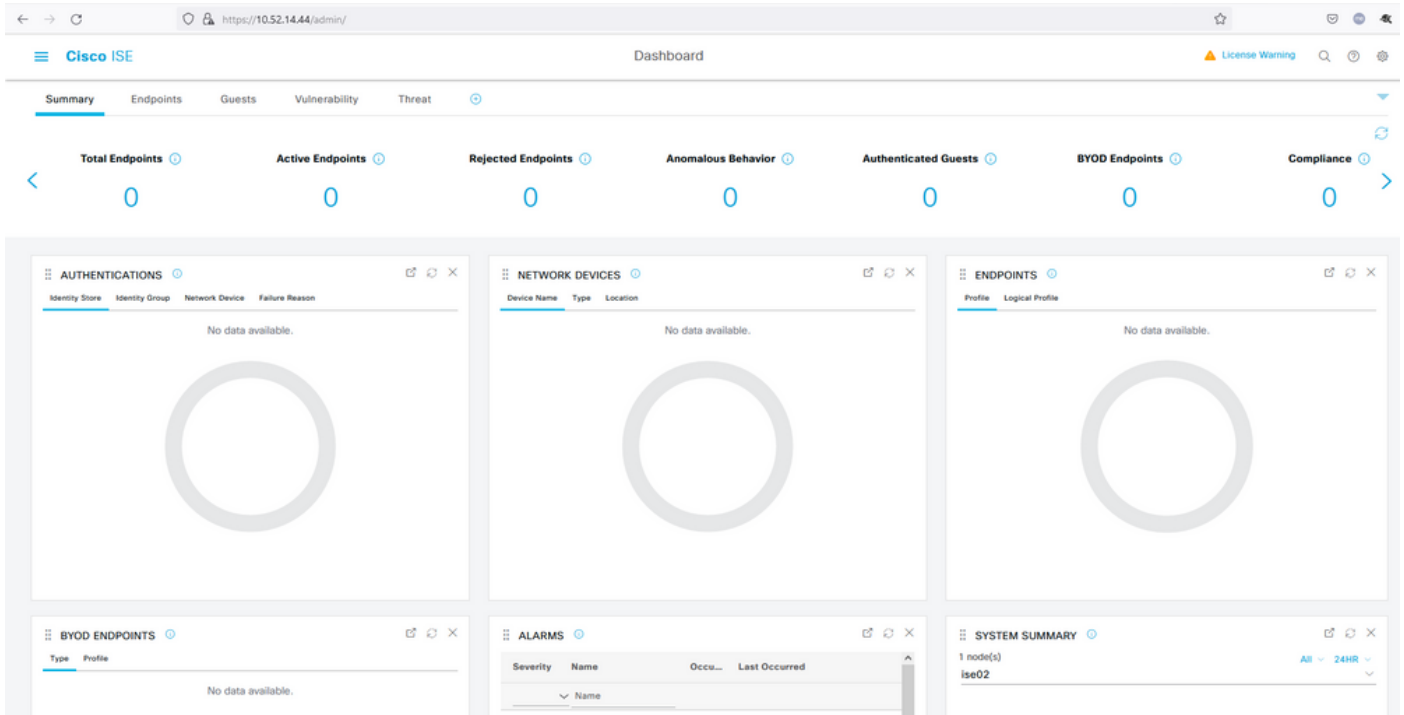


Success!

Logging you in...



Secured by Duo



Dépannage

- Téléchargez l'extension du traceur SAML pour Mozilla FF <https://addons.mozilla.org/en-US/firefox/addon/saml-tracer/>.
- Faites défiler jusqu'au paquetSSOLoginResponse.action. Sous l'onglet **SAML**, vous voyez un certain nombre d'attributs envoyés à partir de Duo SAML : NameID, Recipient (AssertionConsumerService Location URL) et 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>MIIDDTCCAfwAwIBAgIUCbf+LB1BLJMeF6GV0B1rmdX3AVEwDQYJKoZIhvcNAQELBQAwNjEVMGMA1UECgwMRHVvIFN1Y3VyaXR5MR0wGwYDVQDD
BRESTZPODg2UkxETUJZMzExSFBJMjEwFw0zODAxMTkwMzE0MDdaMDYxFTBTBGNVBAoMDER1byBTZWN1cm10eTEdMBsGA1UEAwwURk2TzG4N1JMRE
1CWTMxMUMhQSTIwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDB03Ayuh9avw0NoQzIhQZzu9H8vu/HSKLSH30585Mukj5FnoVV50PGTuoFN4u90t
sIFULjC8eQnUsBR1PYQ5jt0V23qVnvoGyqsuHAs8nbKwvzPShzNF59p03pXkoGPuB+Du2Irrvv0opSv4vbrgKV+H/bvMqyhIA6ywfHNZedG7pbwrYBtVPDXUpnLQvtL2
/Vd9230XuXHF+k32hagRgTLub5XyT1HHQ8b4n3mQKHs6yA/KNvaB3b/AMUqAXDqaEXNG0uQENMK30wTs49
/w+r5fz7xp66muRc0IBg3xjWnnFnyujy7v5ifn1KFUFQu+86A5GbuUWUyiaKmV7CztAgMBAAGjEzARMA8GA1UdEwEB
/wQFMAMBAf8wDQYJKoZIhvcNAQELBQADggEBAH+KItcw0KtDxXBvZ5S+25a+50F4Tqd/pHh56i19d2kDxInSUVsy
/Yy1FXAWge3WBke4b3JR7znD6000sZTYbF9w7H4svU2gxzdK0znXJNj2e4C5FDivnj/TaWZakp2MbTaxfV2VTL0K0kV/1jM6PL61PbKGFwNmh+Sjw/VseS+71C701eI
/U095XLbAu2iIny9zfv0hKNV72L8fgYgrjhpdxH8Y1SxPbVWzNwzytbwZFUogD30XrPq16aXZvJyOH5Vs0H90wQ8Qq48hI4F43sDYrPNH1PzQTYM38kjymEkE0DJPcaGy9v
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="_7fdfc239-631e-439c-a3ab-f5e56429779d_SEMIportalSessionId_EQUALS859ee9c3-60e4-4482-9426-
b3904d4d6226_SEMItoken_EQUALS1RS257BC245GVHWZ76GMVEZNR0YCCCL_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_8dfe9494ab8d617884446cb8f2259bb4a56492ef">
</saml:AuthnStatement>
</saml:AuthnContext>

```

1846 requests received (490 hidden)

- Connexion en direct à 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

- Connexion d'administration sur ISE : nom d'utilisateur : 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		10.65.48.163	16402	Administrator authentication succeeded	Administrator authentication successful

Rows/Page 1 1 Total Rows

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.