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

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)

la ressource ou le service hébergé auquel l'utilisateur a l'intention d'accéder ; Serveur d'applications Cisco ISE 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.

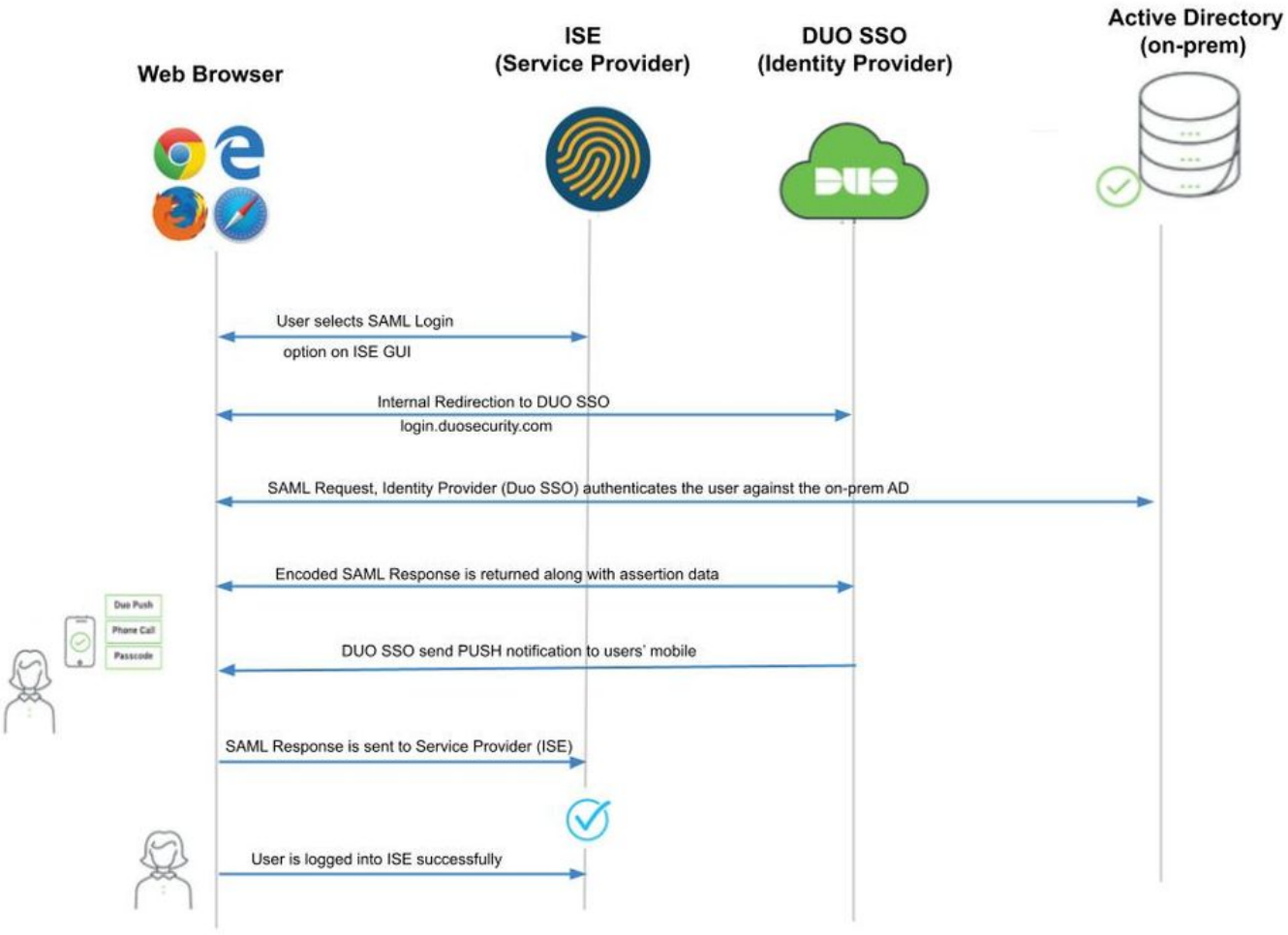
Les transactions SAML utilisent le langage XML (Extensible Markup Language) pour les communications normalisées entre le fournisseur d'identité et les fournisseurs de services. SAML est le lien entre l'authentification de l'identité de l'utilisateur et l'autorisation d'utiliser un service.

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.

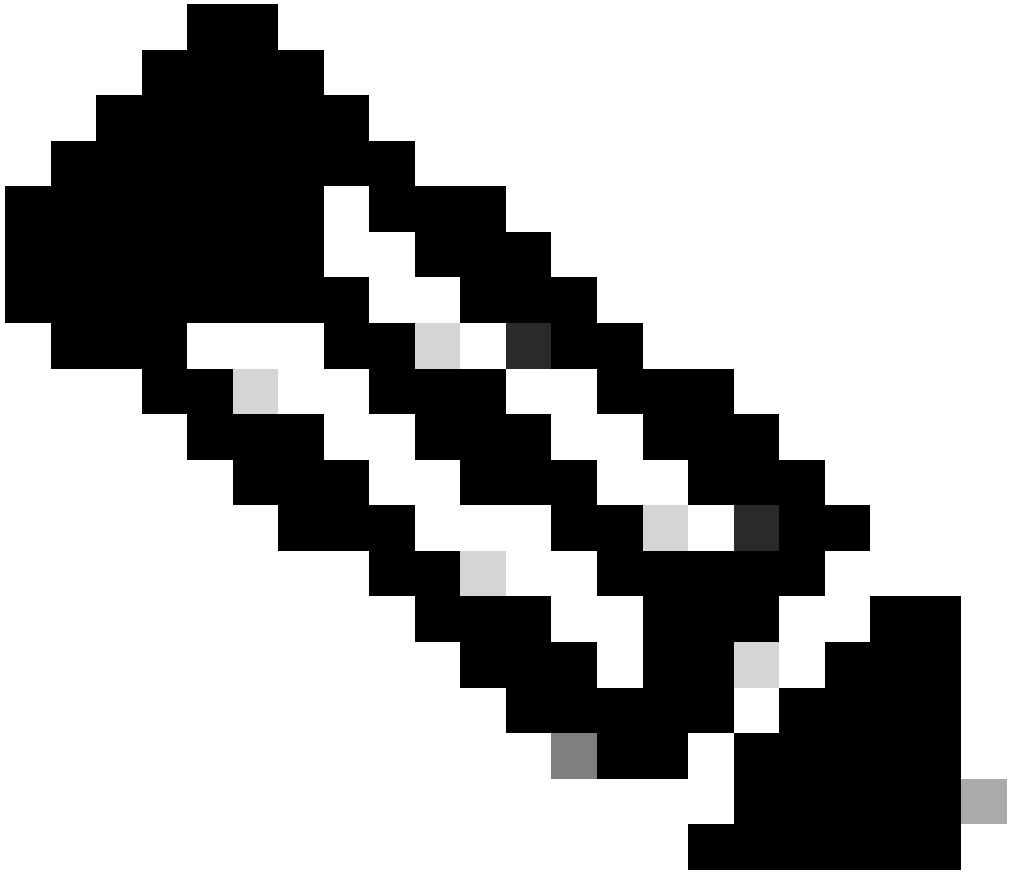
- Les assertions d'authentification prouvent l'identification de l'utilisateur et indiquent l'heure à laquelle l'utilisateur s'est connecté et la méthode d'authentification qu'il a utilisée (par exemple, Kerberos, à deux facteurs, etc.).
- L'assertion d'attribution transmet les attributs SAML, des données 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 noeuds 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 noeuds 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.

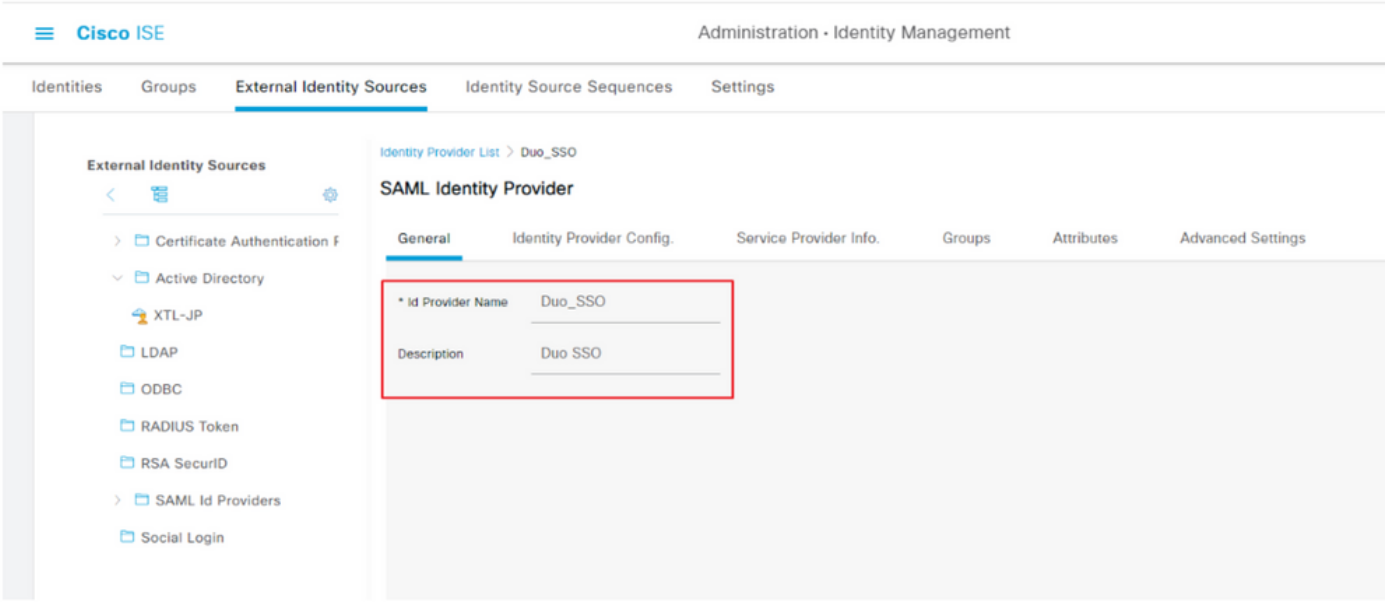
Configuration de l'intégration SSO SAML avec Duo SSO

Étape 1 : configuration du fournisseur d'accès SAML sur ISE

Configurer Duo SSO comme source d'identité SAML externe

Sur ISE, accédez àAdministration > Identity Management > External Identity Sources > SAML Id Providerset 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 :

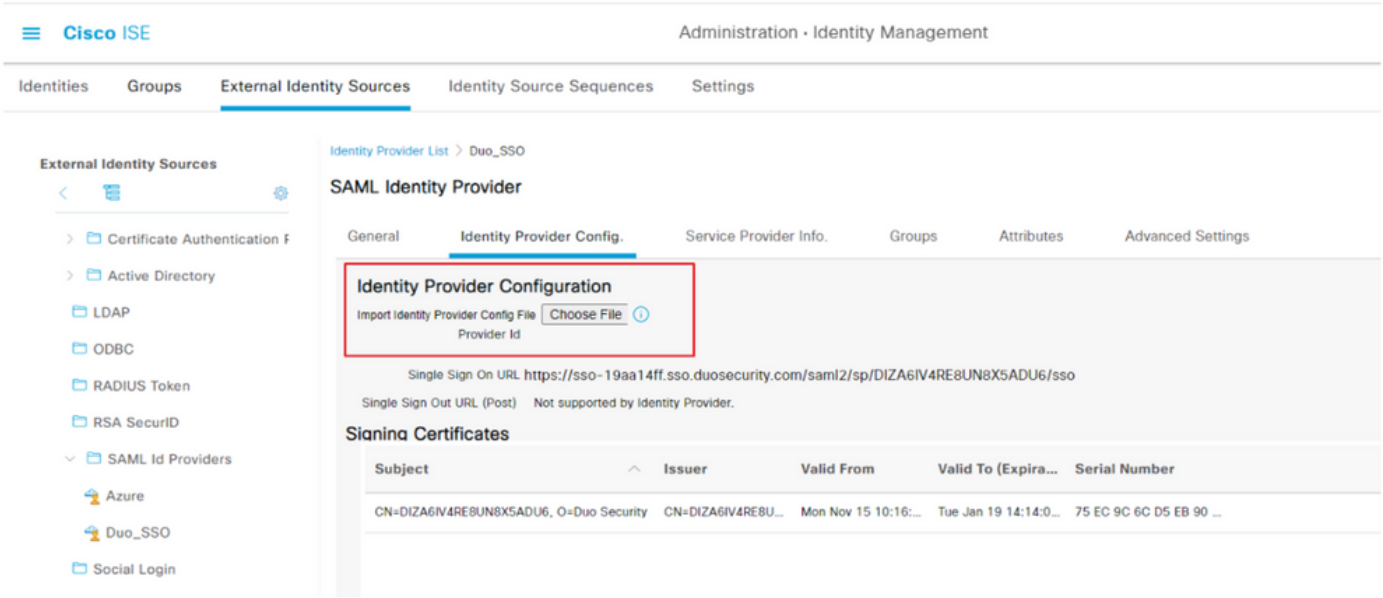


Importer le fichier XML de métadonnées SAML à partir du portail d'administration Duo

Sur ISE, accédez àAdministration > 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.

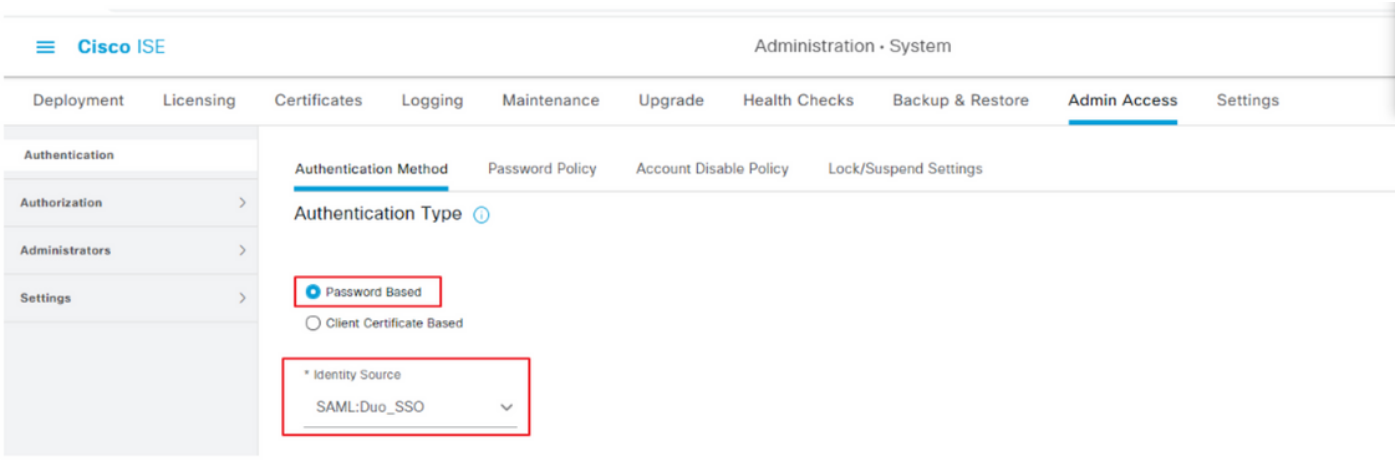
Choisissez le fichier SSO IDP Metadata XML exporté depuis le portail Duo Admin et cliquez sur Open afin de l'enregistrer. (Cette étape est également mentionnée dans la section Duo de ce document.)

L'URL SSO et les certificats de signature sont :



Configurer la méthode d'authentification ISE

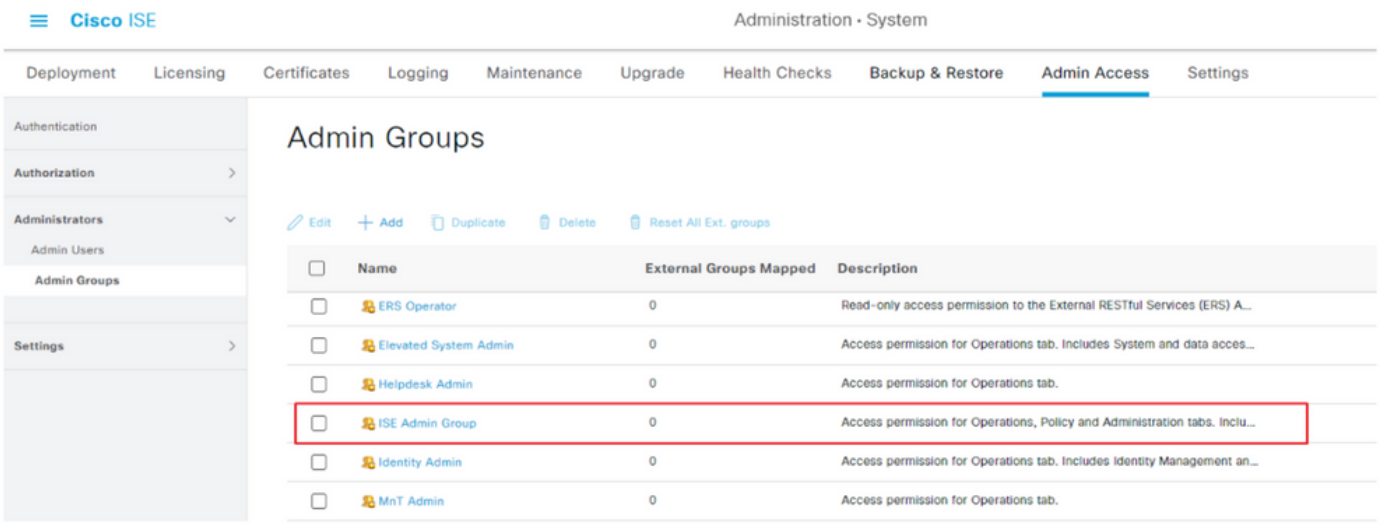
Accédez à la case d'option Password-Based (Basé sur mot de passe)Administration > System > Admin Access > Authentication > Authentication Methodet sélectionnez-la. Choisissez le nom de fournisseur d'identité requis créé précédemment dans la liste déroulante Source d'identité, comme indiqué dans l'image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



Créer un groupe d'administrateurs

Accédez àAdministration > System > Admin Access > Authentication > Administrators > Admin Groupet cliquez sur Super Admin, puis sur le bouton Dupliquer. Saisissez le nom du groupe Admin et cliquez sur le bouton Submit.

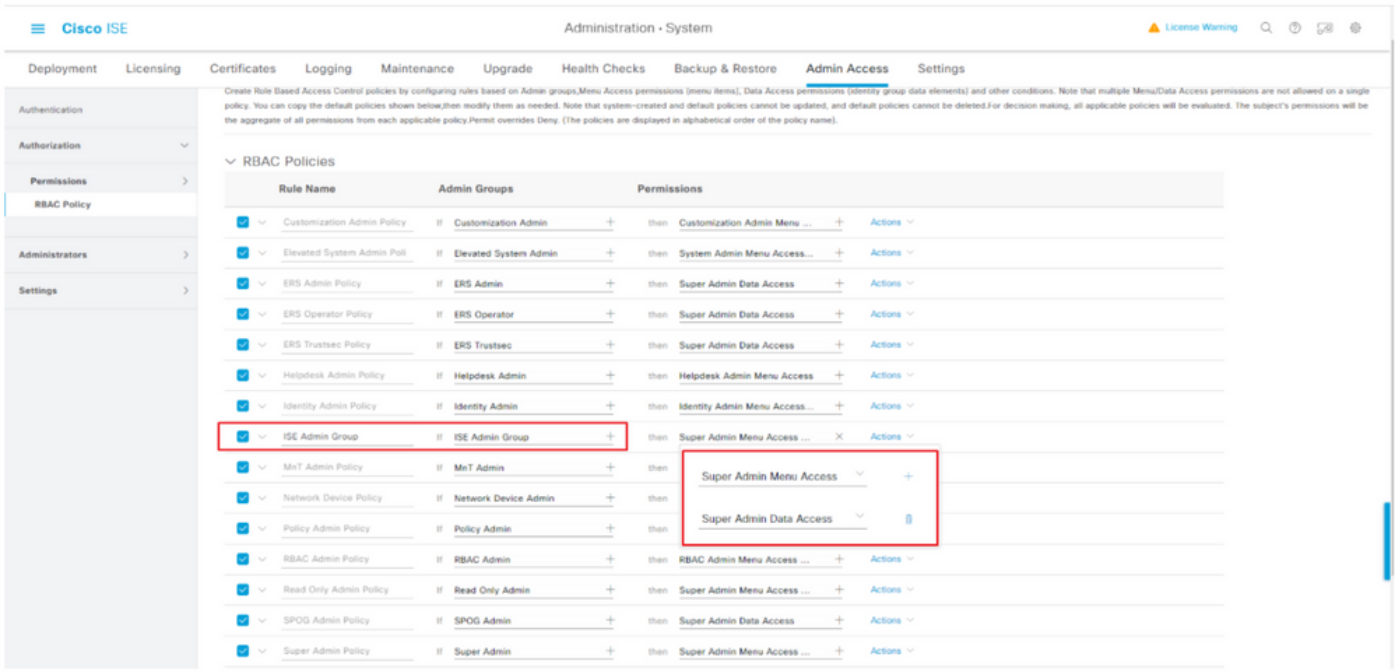
Cela permet d'accorder des privilèges de super administrateur au groupe Admin.



Créer une stratégie RBAC pour le groupe Admin

Accédez àAdministration > System > Admin Access > Authorization > RBAC Policyet sélectionnez les actions correspondant à Super Admin Policy. Cliquez surDuplicate > Add the Name field > Save.

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

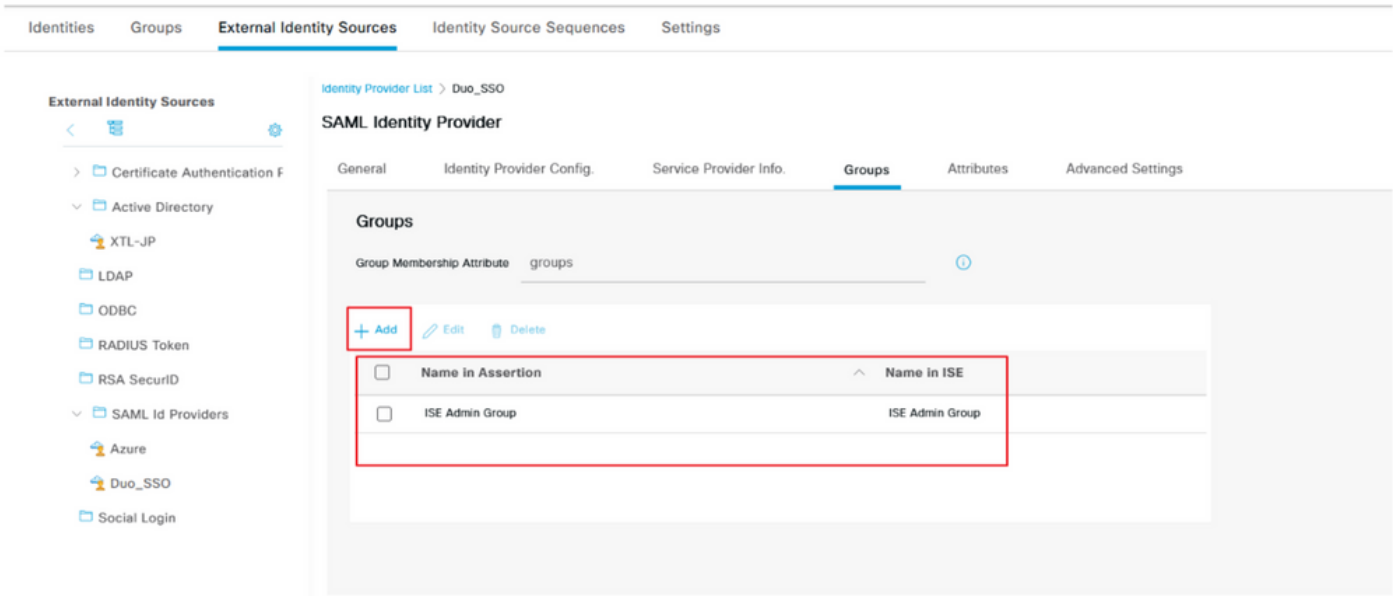


Ajouter l'appartenance aux groupes

Sur ISE, accédez àAdministration > Identity Management > External Identity Sources > SAML Id Providerset 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

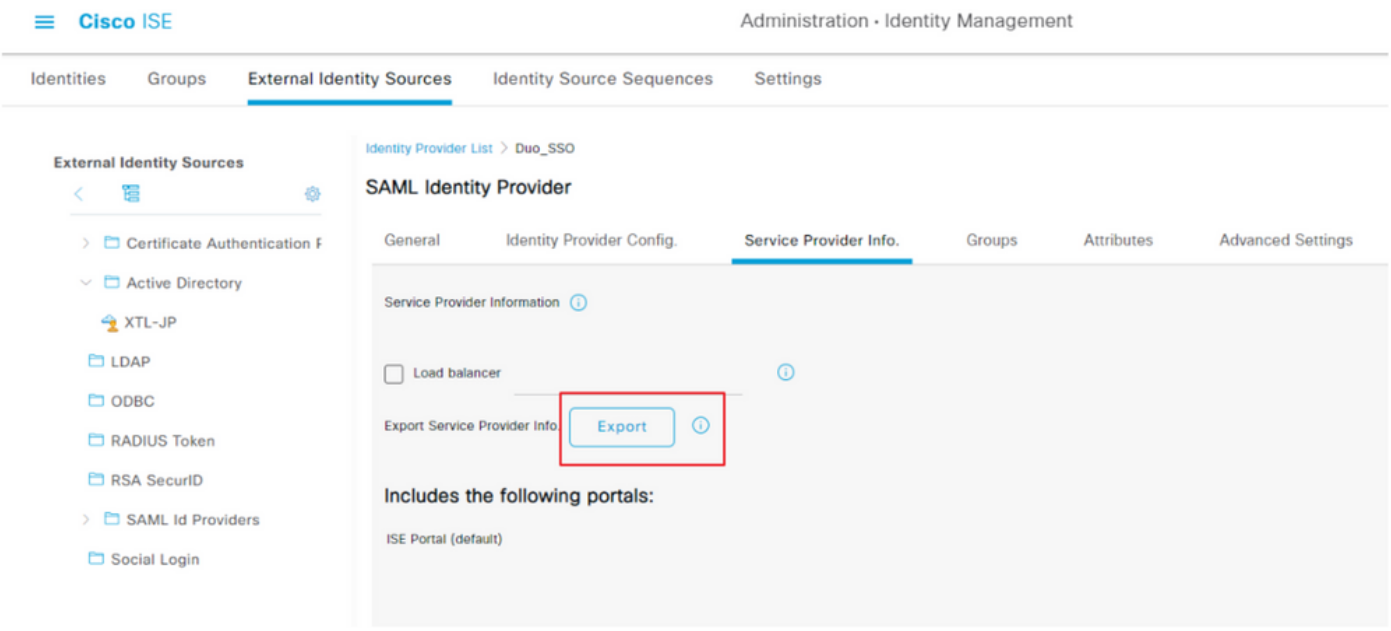
automatiquement :



Exporter les informations SP

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

Basculez l'onglet sur Infos SP. et cliquez sur le bouton Export (Exporter) comme illustré dans l'image :



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

MIIFUzCCAzugAwIBAgIMNOUWtIWSUFWaealmMA0GCSqGSIb3DQEBDAUAMCcxJTAjBgNVBAMTHFNB
TUxfaXNlMDIueGVyb3RydXN0bGFicy5jb20wHhcNMjExMTE1MjI1OTM0WhcNMjYxMTE0MjI1OTM0
WjAnMSUwIwYDVQQDExxTQU1MX2lzZTAyLnhlcm90cnVzdGxhYnMuY29tMIICIjANBgkqhkiG9w0B
AQEFAAOCAg8AMIICCgKCAgEAxw7scSLMH1ApI3O/7+vWsGP4schoJJHlVeJKHuJVgm19SXViW8Ab
WL9hQEXDr+U/zzp7fAq0YjckeNJg6VMhasao5tY4cutrAZK2F/kYvdVN+0N2cJUSTdJZNdKO+hcj
VmUgClUi6Xa4PJNw+1yhj8PwrDlpzfgXZLi3wlo5sMRGrg8NeSbShPJVakIEF2FoI0hXTOOSH4ZN
sD4q99dzrAv2m6y74vtUOGqwX4RRMOdvr7DIMNd2U/trh41QT85SY5c7Ol6fRWtY9omZBdUOS2JC
ihWnC9ug7FEOqdPm2h5KiZvxJck9OqVXDHvtRKctW5gwzfX8Hu7DQKqs9Oh04HRUxg2GEiuiXCQZ
5p63KfoRly5oW5OUKOLIMdyhDl+8uP+n+Jo3ufR8lKe42+/rws5Ct1hg4jozddutKkw2vyxMEg5/
ZpAz/goRIOmBN4r3n3FNGZV1uTfbb1Mz8yvY61ccGgTU1/Iynt9maNHxjbFtAP+HaiMPisfTKDRJ
OLx91v+xKpb+opcOxqVK1qOUs0yGVvfycaFNZ3jP5wBNBzSAi7cvXk7sIW9WM7DC84OjC/r9EbaX
Wll7MLV+16Z+FeDnzhzFVjq/cb61eNvXKKwDFryFqBnDLLJGmJuZQ/EgROwkvseR8tNE3qIYVhOe
qfCKZUpWtZ+lGLDD3r50p9UCAwEAAaN/MHOwIgYDVR0RBBswGYIXaXNlMDIueGVyb3RydXN0bGFi
cy5jb20wDAYDVR0TBAUwAwEB/zALBgNVHQ8EBAMCAuwwHQYDVR0OBBYEFAoHeqyYR5r0XpOVXODT
WdpDycOoMB0GA1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjANBgkqhkiG9w0BAQwFAAOCAgEA
aoIIkyS8slDwjQrRsUVyPi17LvlOTleCUQBrnr5WNUWlaXIB7Cb9qrG9D2ced72miH6vUcxine78
V4loTsgVu3tVlslQrOLW2eNLSbaN1XqbVUl1sCZkA4wGt8uLPX0t8UYysecEPFXD0NiKGPoIMaFg
3pP5525cJpeLRkgHjw1Z2qT54lsGd8Gdq6V666kliAt73kPwfDiZf/uDsCI+euIHDywLdOad51kJ
RWAsZO7tgxK3tJO9z7JU4oY1fI26DUN43++Ap3KSaDiz9gYJ3fFjR9hP/nF/ywyOOHO5MgHqhsMo
+zBMADukmprYC8qd+Oz76+NQ6TLXgUer7NQMty68tQYP4riupvc26CEmgEZ592jBgDdt2tkY9An4
Fl/rqJPhX2RISLdUt50NcBbIZVOJ/IjkqHj9UG1E/U8qYy3krWvZV+VV5ChVNzwiVTWFCEOHNOTh
l/yYdAAsODUBbwTqgJL1G3hNo+dA3LAgg/XKENFr+tt3LQOkwPAtjKFQsIX/4sgMetV4KSqUI3HZ
qw5uOt9WT578SZ5p1u/qj2cfx2wdqRVk5vSij6TxOpXIaCuY2L5YfeIMP/K49K+DecMBxCrKygNT
vGXOPkVG/yqgQ9OIfQZ1OD3/NZxGyBJdzSSkjHxiUdWf4lWj1tVU+qav8M3imsCRvcZJppaKJNo=

urn:oasis:names:tc:SAML:2.0:nameid-format:transient

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

urn:oasis:names:tc:SAML:2.0:nameid-format:persistent

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

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

urn:oasis:names:tc:SAML:2.0:nameid-format:kerberos

urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName
```

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

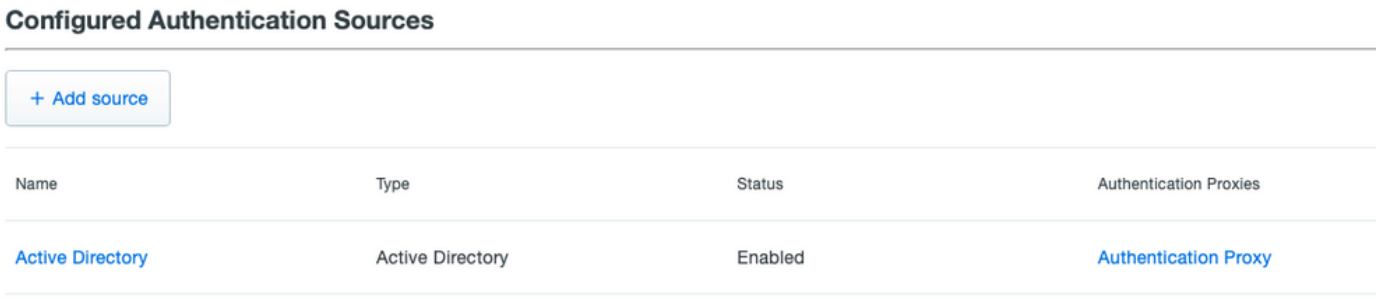
entityID = http://CiscoISE/7fdfc239-631e-439c-a3ab-f5e56429779d.

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).

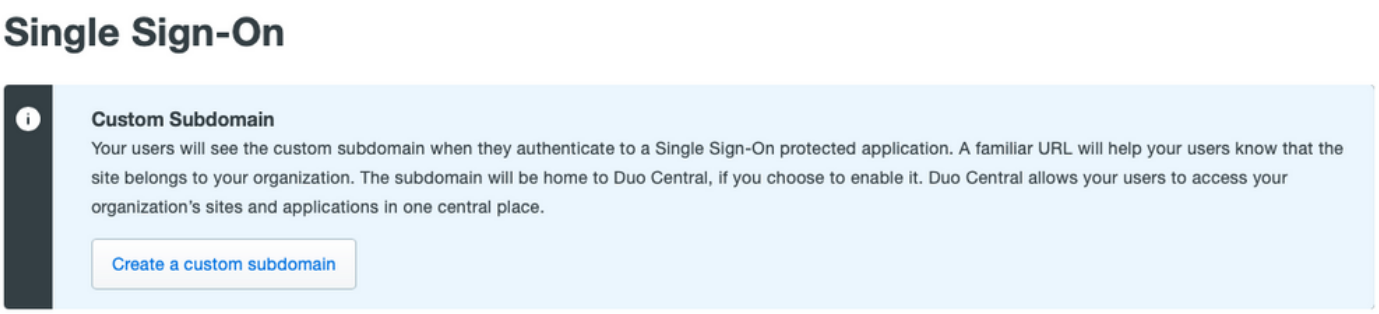
AssertionConsumerService Location = https://isenodename.com:8443/portal/SSOLoginResponse.action où isenodename est le nom de domaine complet ISE réel trouvé sur le fichier XML (Location).

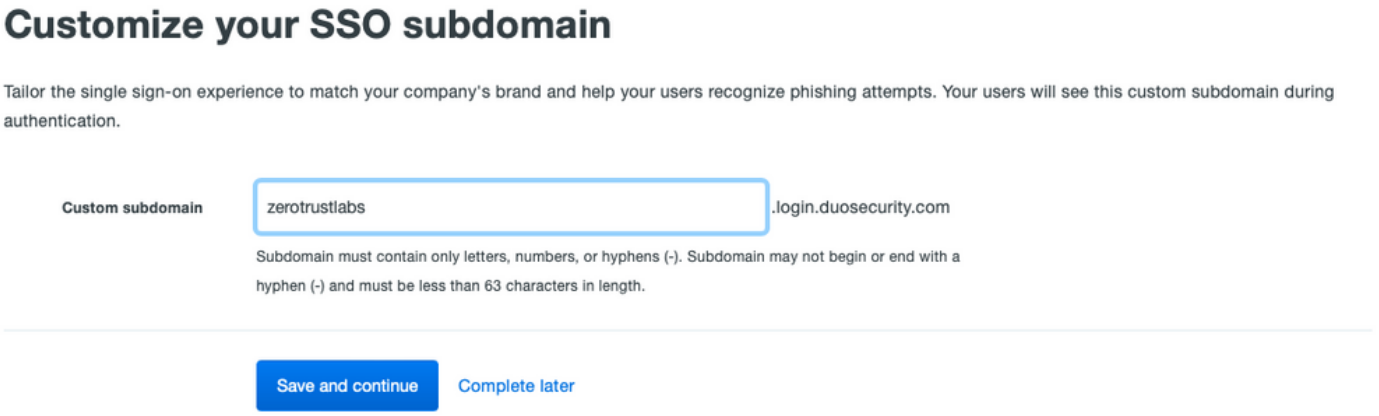
Étape 2 : configuration de Duo SSO pour ISE

Cochez cette case KB afin de configurer Duo SSO avec AD comme source d'authentification.



Cochez cette case KB afin d'activer l'SSO avec votre domaine personnalisé.





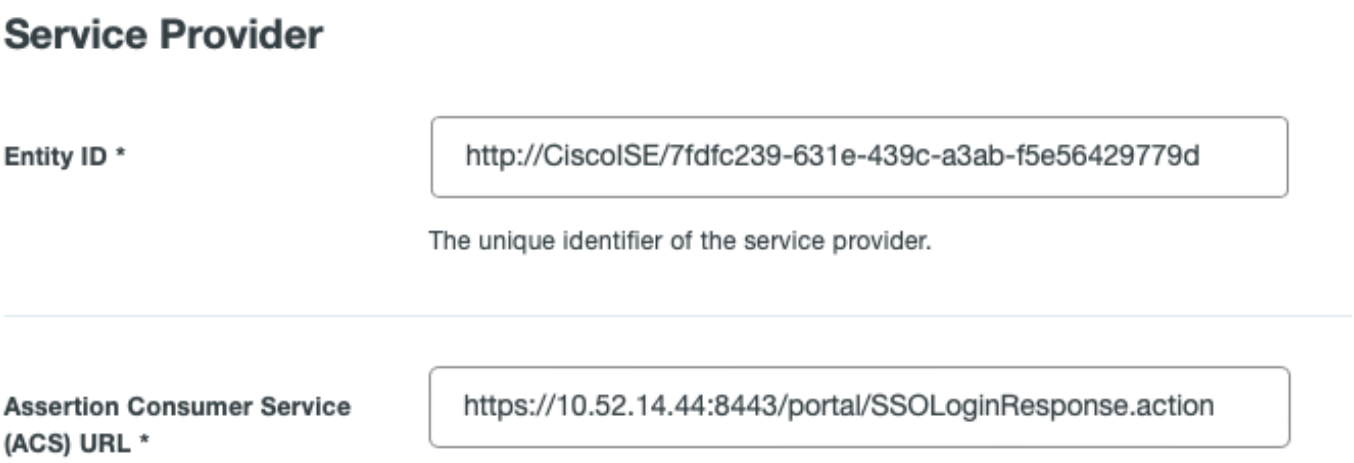
Étape 3. Intégration de Cisco ISE avec Duo SSO en tant que SP générique

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 :

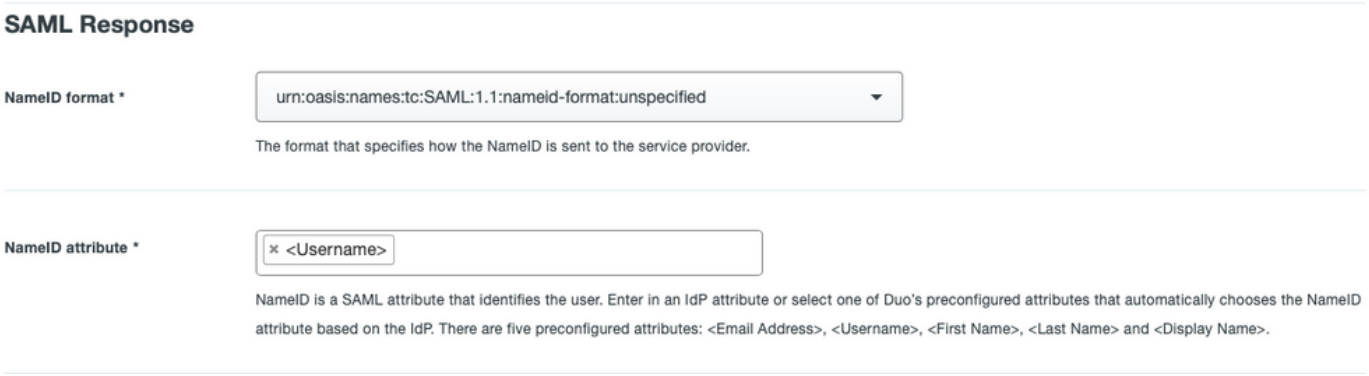
Nom	Description
ID entité	http://CiscoISE/7fdfc239-631e-439c-a3ab-f5e56429779d
URL ACS (Assertion Consumer	https://10.x.x.x:8443/portal/SSOLoginResponse.action

Service)	

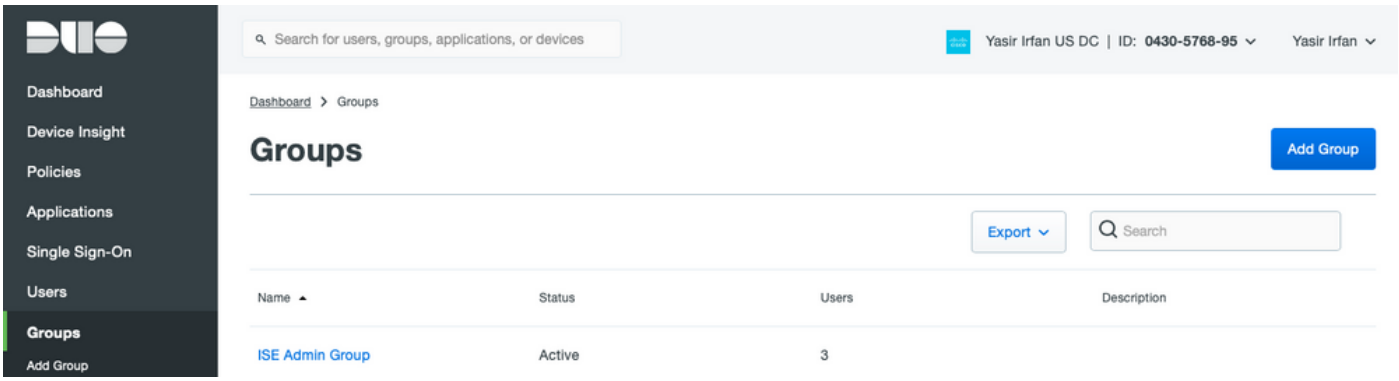


Configurez la réponse SAML pour Cisco ISE :

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

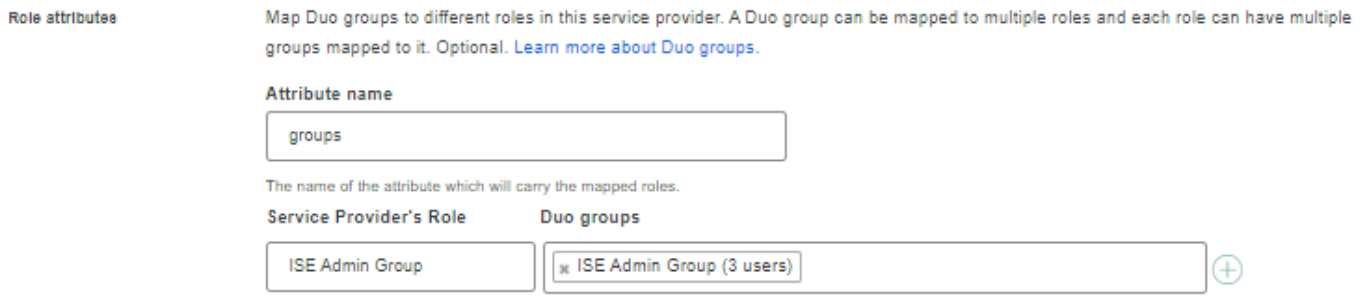


Créez un groupe appelé Groupe d'administration Cisco dans le panneau d'administration Duo et ajoutez les utilisateurs ISE à ce groupe ou créez un groupe dans Windows AD et synchronisez-le avec le panneau d'administration Duo à l'aide de la fonctionnalité de synchronisation de répertoire.

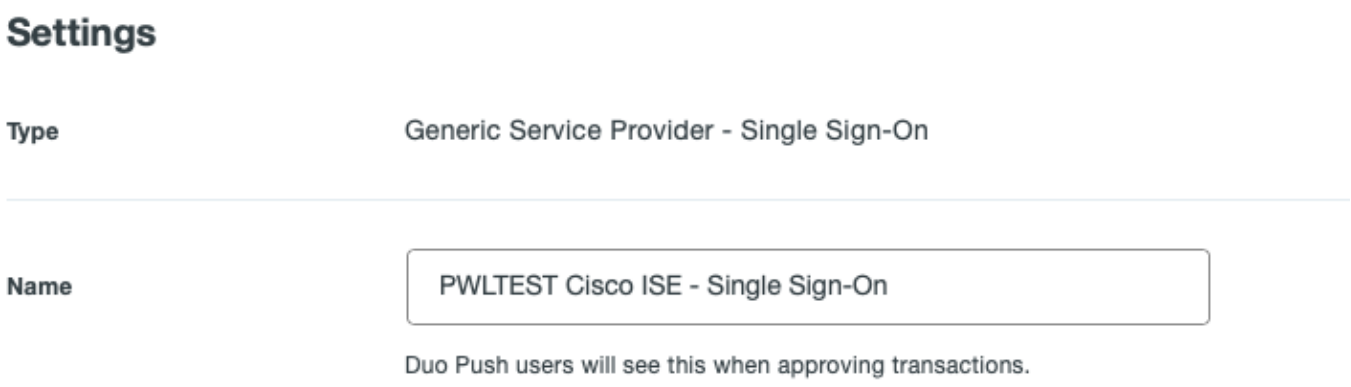


Configurez les attributs de rôle pour Cisco ISE :

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



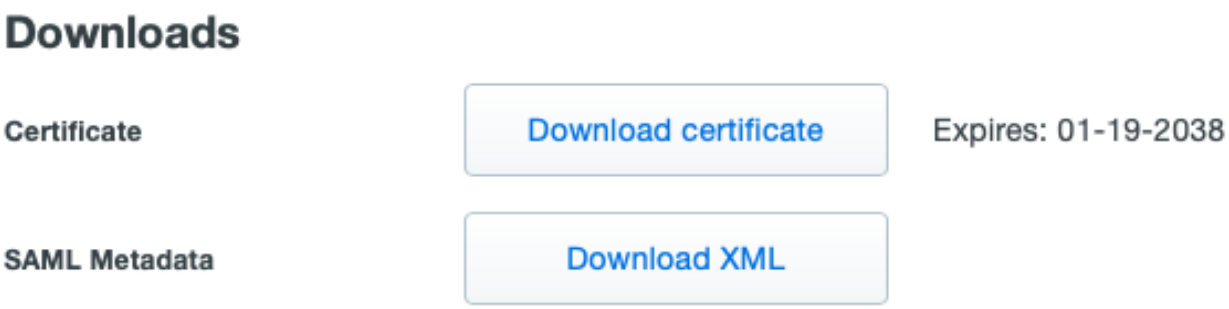
Dans la section Paramètres, indiquez un nom approprié dans l'onglet Nom pour cette intégration.



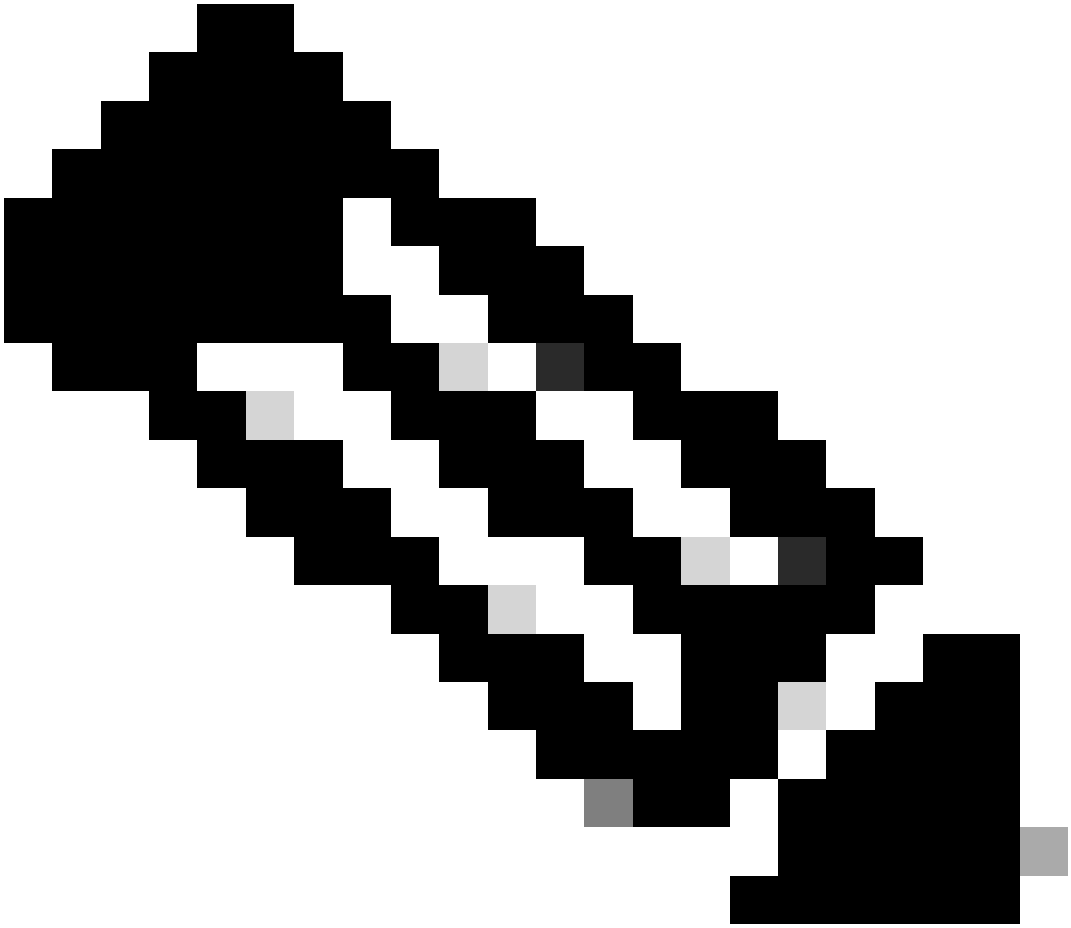
Cliquez sur le bouton Save afin d'enregistrer la configuration et référez-vous à cette Ko pour plus

de détails.

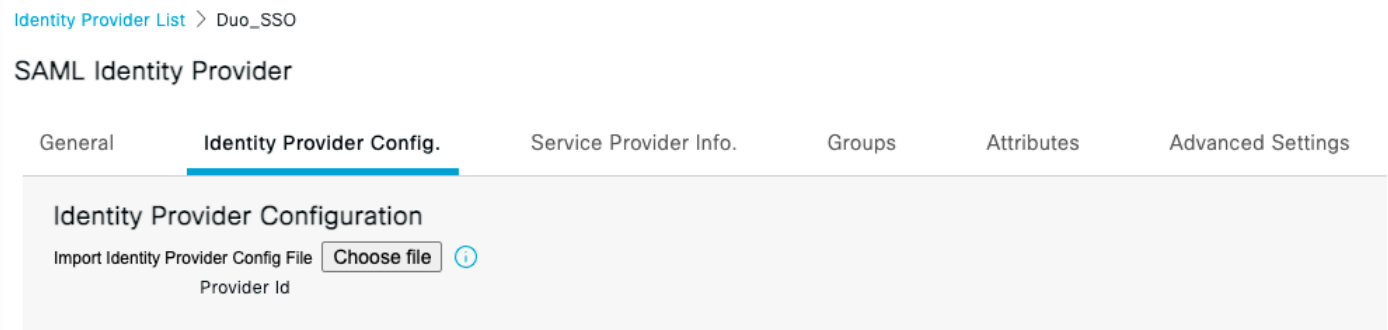
Cliquez sur Download XML afin de télécharger les métadonnées SAML.



Téléchargez les métadonnées SAML à partir du panneau d'administration Duo vers Cisco ISE en naviguant jusqu'àAdministration > Identity Management > External Identity Sources > SAML Id Providers > Duo_SSO.
Basculez l'onglet vers Identity Provider Config. et cliquez sur le bouton Choisir un fichier.
Sélectionnez le fichier XML de métadonnées téléchargé à l'étape 8. et cliquez sur Enregistrer.



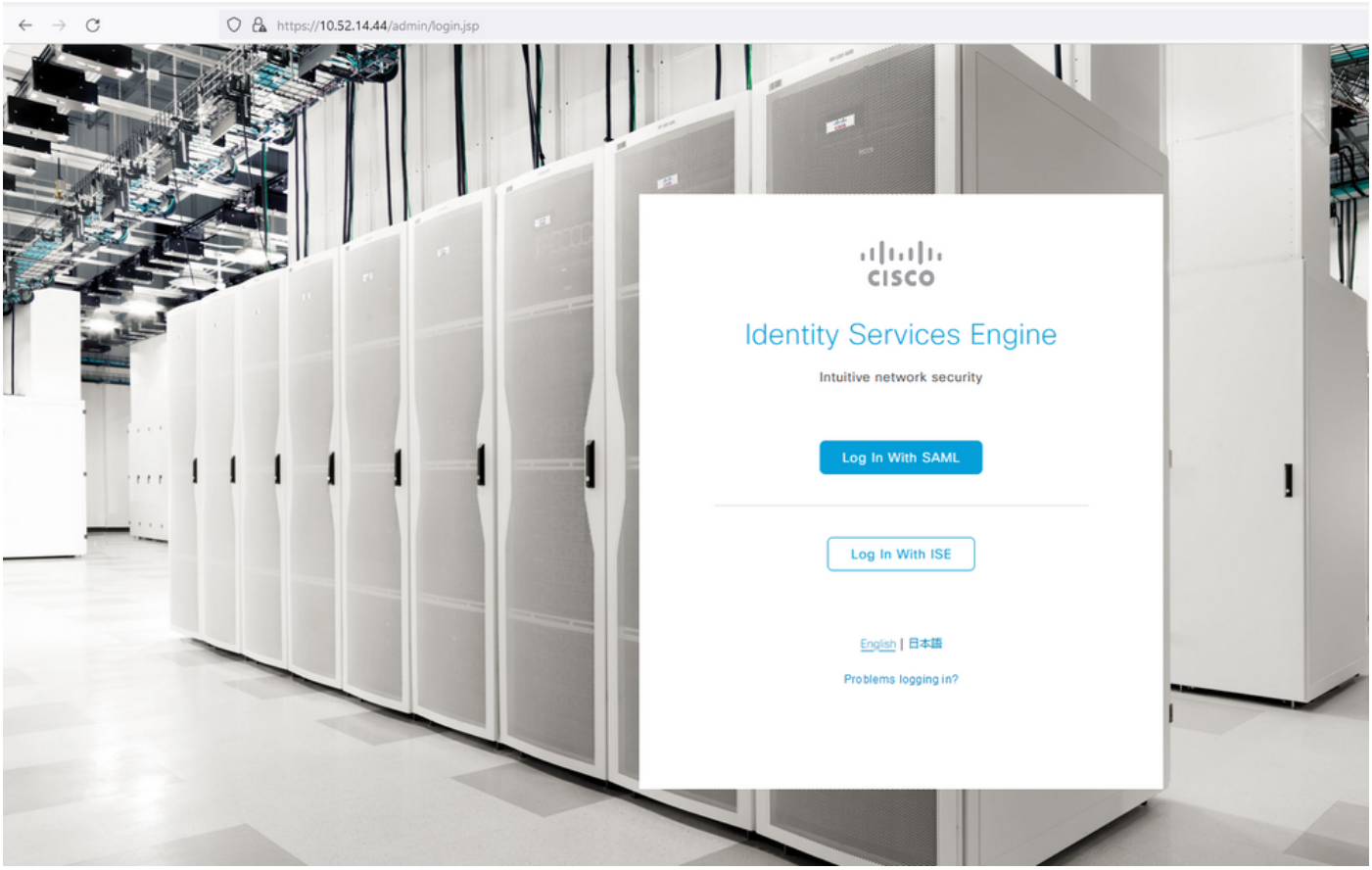
> Remarque : Cette étape est mentionnée ici dans la section Configurer l'intégration SSO SAML avec Duo SSO ; Étape 2 : importation du fichier XML de métadonnées SAML à partir du portail Duo Admin



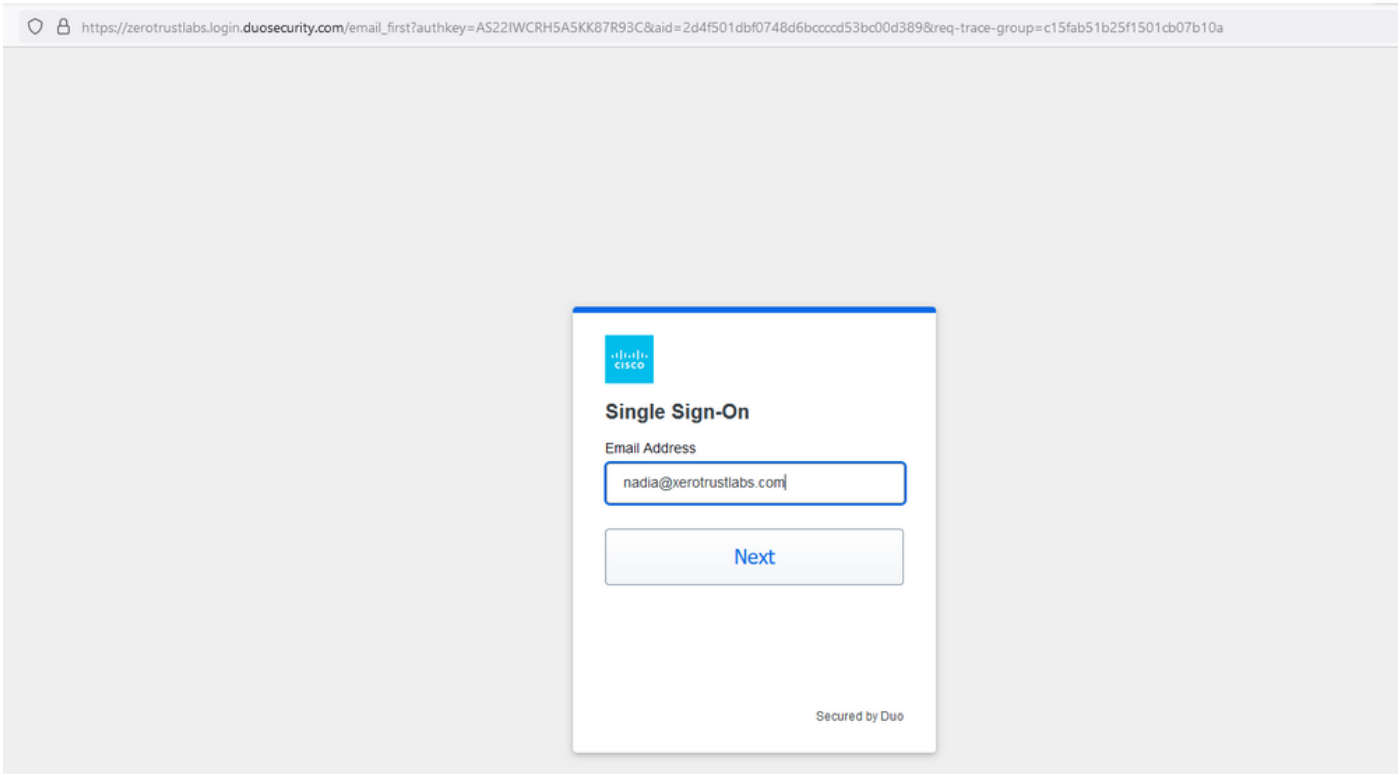
Vérifier

Test de l'intégration avec Duo SSO

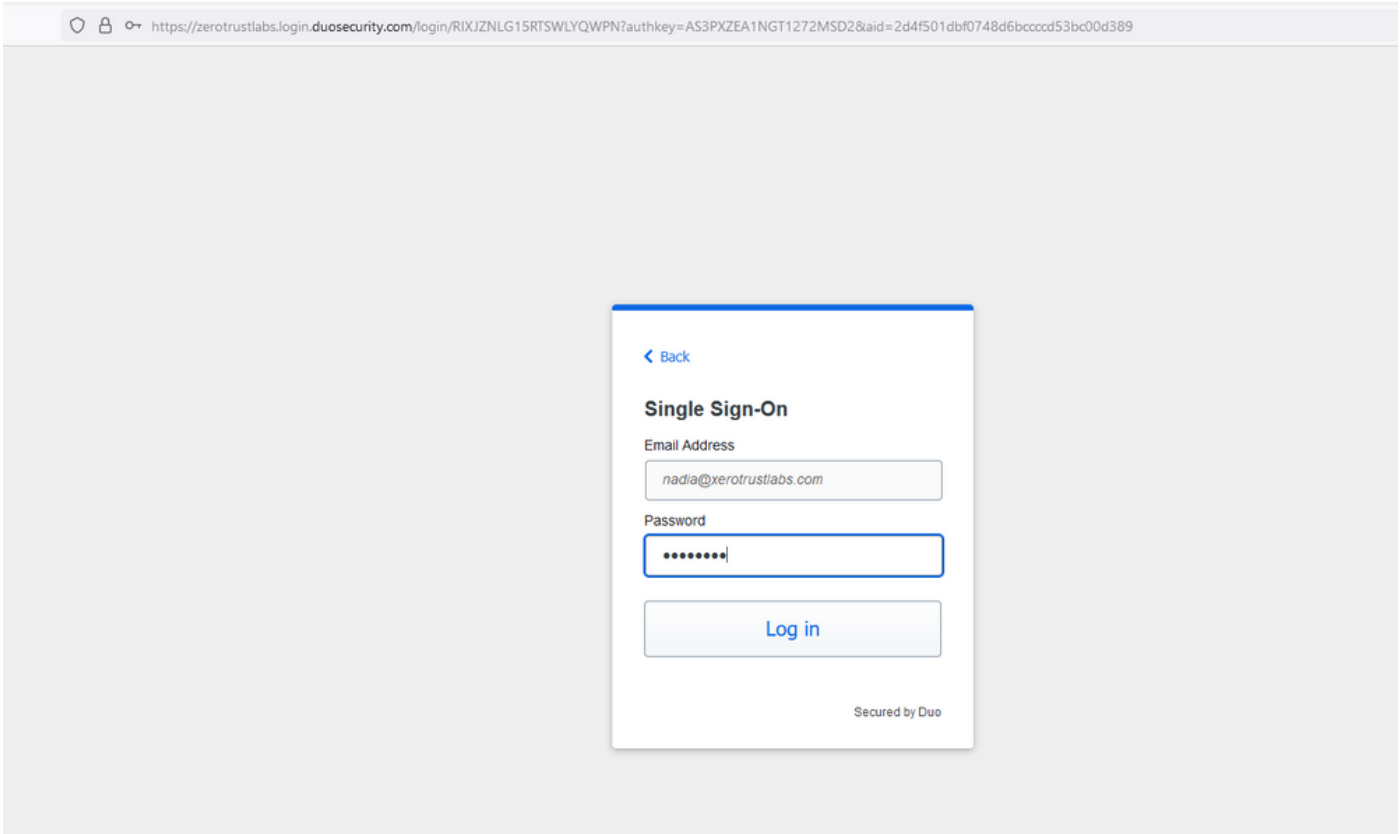
1. Connectez-vous au panneau d'administration de Cisco ISE et cliquez sur Log In With SAML.



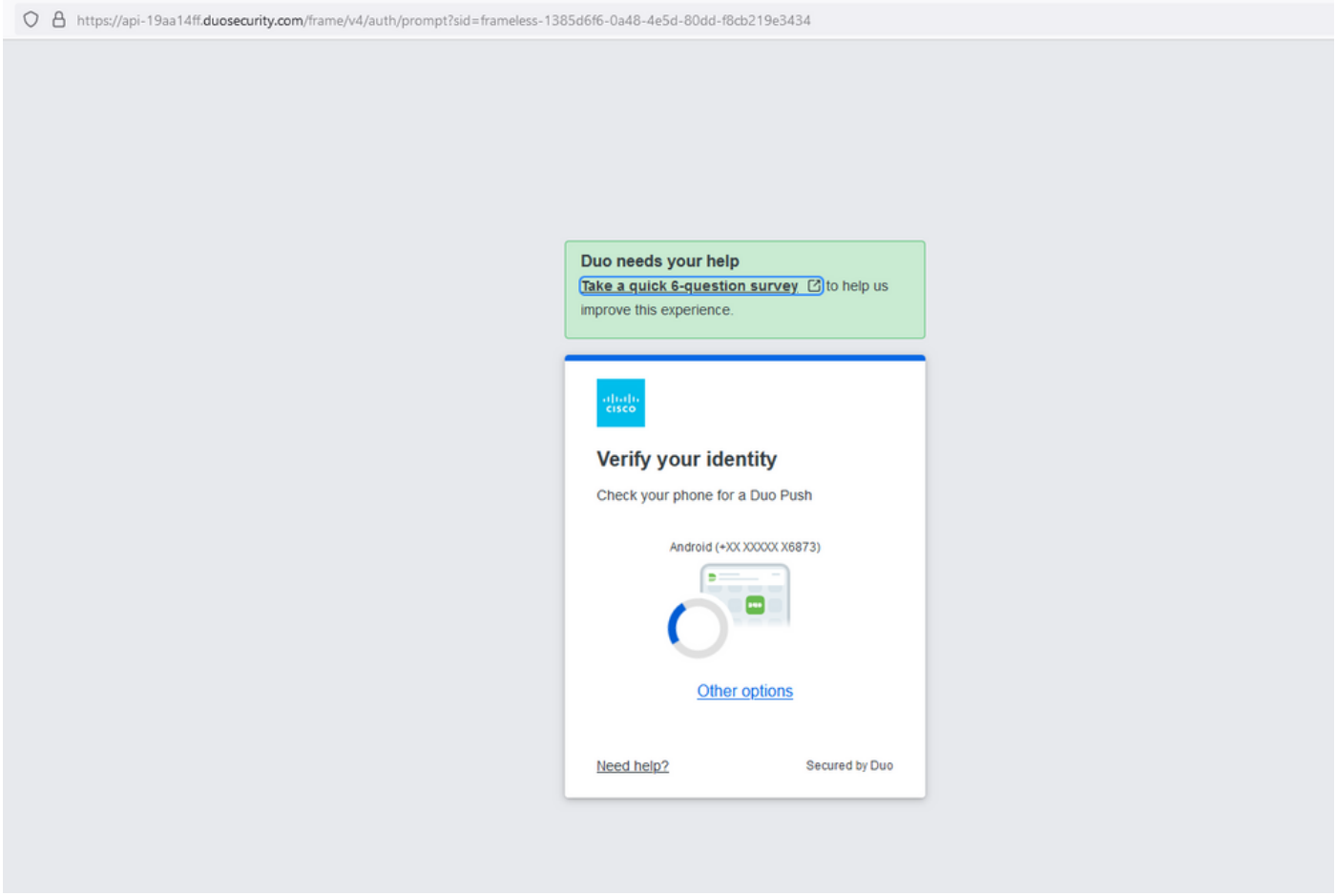
2. Redirigé vers la page SSO, saisissez l'adresse e-mail et cliquez sur Next.



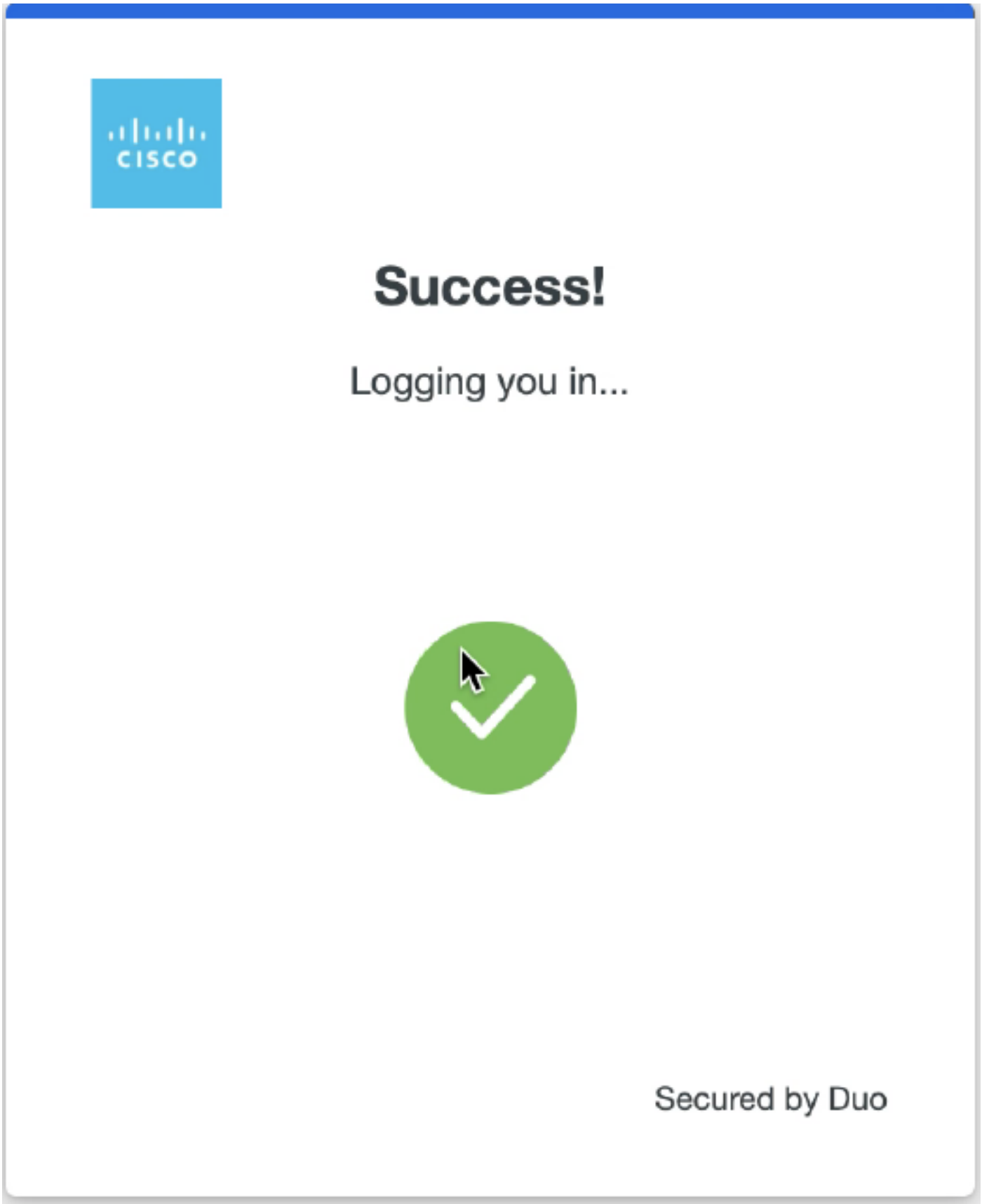
3. Entrez le mot de passe et cliquez sur Connexion.



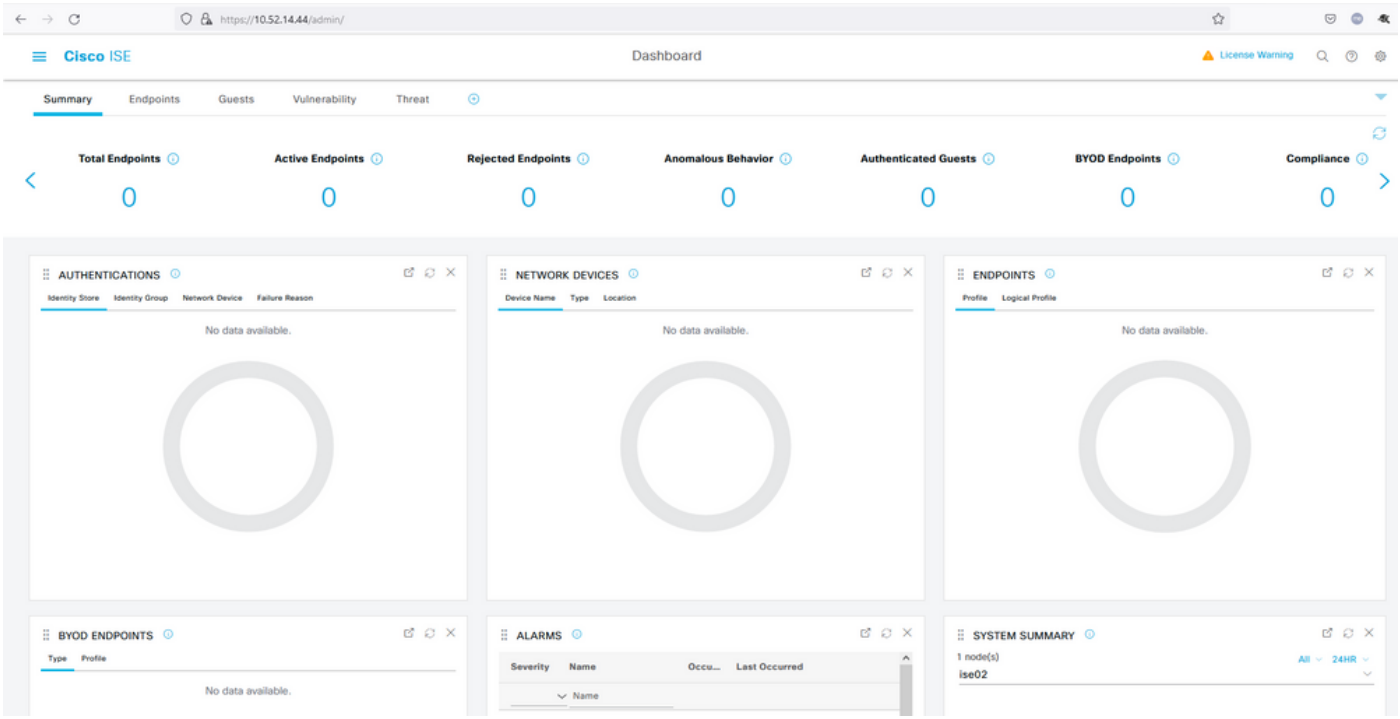
4. Vous obtenez une invite Duo Push sur votre appareil mobile.



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

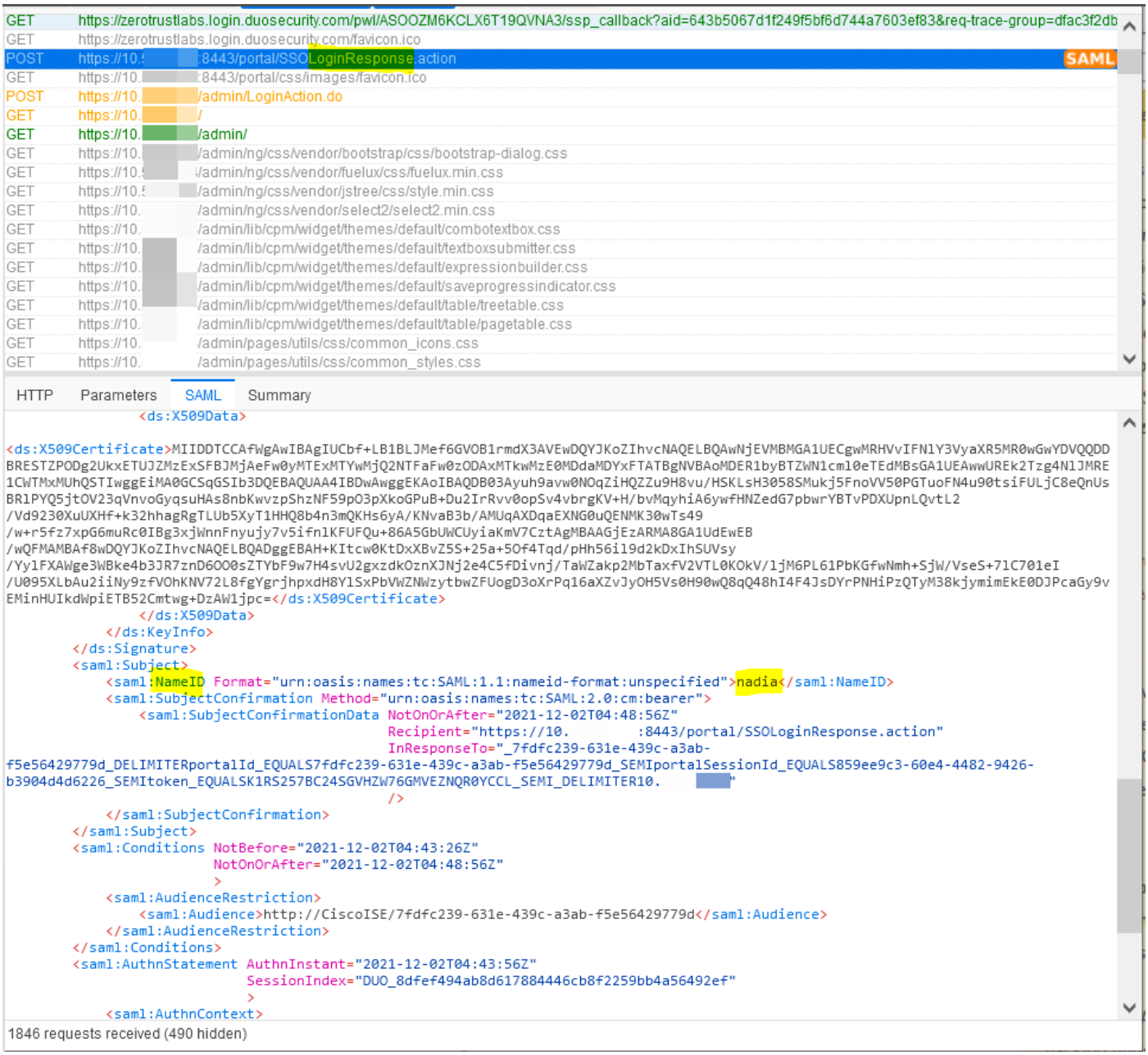


6. Page d'accès à l'interface utilisateur ISE Admin.



Dépannage

- Téléchargez l'extension du traceur SAML pour Mozilla FF https://addons.mozilla.org/en-US/firefox/addon/saml-tracer/.
- Faites défiler jusqu'au paquet`SSOLoginResponse.action`. Sous l'onglet SAML, vous voyez un certain nombre d'attributs envoyés à partir de Duo SAML : NameID, Recipient (URL d'emplacement AssertionConsumerService) et Audience (EntityID).



- Connexion en direct à ISE :

Cisco ISE

Overview

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

Steps

5231	Guest Authentication Passed

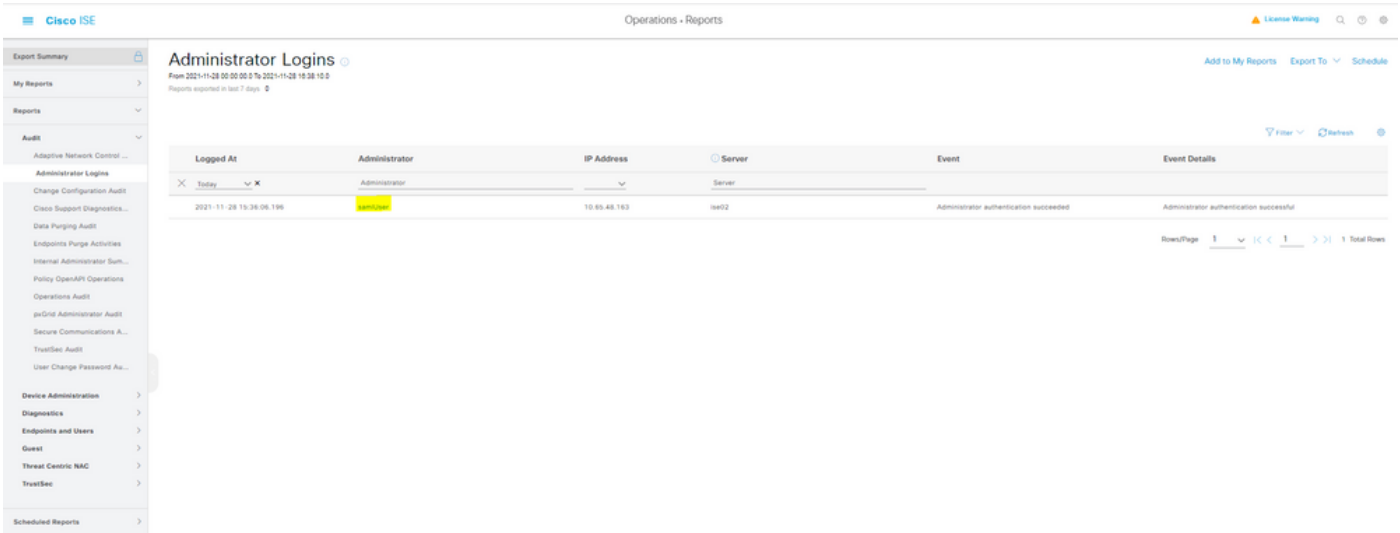
Authentication Details

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 à ISE : username (nom d’utilisateur) : samlUser.



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.