# Duo SSOおよびWindows ADとのSAML統合を使用したISE 3.1 GUI管理者ログインの設定

## 内容


[はじめに](#)

[前提条件](#)

- [要件](#)
- [使用するコンポーネント](#)

[背景説明](#)

- [アイデンティティプロバイダー(IdP)](#)
- [サービスプロバイダー(SP)](#)
- [SAML](#)
- [SAMLアサーション](#)

[高レベルフロー図](#)

[Duo SSOとのSAML SSO統合の設定](#)

- [ステップ 1：ISEでのSAML IdPの設定](#)
  - [外部SAMLアイデンティティ・ソースとしてのDuo SSOの構成](#)
  - [Duo AdminポータルからSAMLメタデータXMLファイルをインポートします](#)
  - [ISE認証方式の設定](#)
  - [管理グループの作成](#)
  - [管理グループのRBACポリシーの作成](#)
  - [グループメンバーシップの追加](#)
  - [SP情報のエクスポート](#)
- [ステップ 2：ISE用のDuo SSOの設定](#)
- [ステップ 3：Cisco ISEとDuo SSOを汎用SPとして統合](#)

[確認](#)

- [Duo SSOとの統合のテスト](#)

[トラブルシュート](#)


## はじめに

このドキュメントでは、Cisco Duo SSOなどの外部アイデンティティプロバイダーとCisco ISE 3.1 SAML SSO統合を設定する方法について説明します。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- Cisco Identity Services Engine(ISE)3.1

- Security Assertion Markup Language(SAML)シングルサインオン(SSO)導入(SAML 1.1)に関する基本的な知識
- Cisco DUO SSOの知識
- Windows Active Directoryに関する知識

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

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

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

## 背景説明

### アイデンティティプロバイダー(IdP)

この場合、要求されたリソース（「サービスプロバイダー」）に対してユーザIDとアクセス権限を確認し、アサートするのはDuo SSOです。

Duo SSOはIdPとして機能し、SAML 1.1または任意のSAML 2.0 IdP（Microsoft Azureなど）を使用して既存のオンプレミスのActive Directory(AD)でユーザを認証し、サービスプロバイダーアプリケーションへのアクセスを許可する前に2要素認証を要求します。

アプリケーションをDuo SSOで保護するように構成する場合は、Duo SSOからアプリケーションに属性を送信する必要があります。Active Directoryは追加の設定なしで動作しますが、認証ソースとしてSAML(2.0) IdPを使用した場合は、正しいSAML属性を送信するように設定されていることを確認してください。

### サービスプロバイダー(SP)

ユーザがアクセスするホステッドリソースまたはサービス。この場合はCisco ISE Application Server。

### SAML

SAMLは、SPに認証クレデンシャルを渡すためにIdPを許可するオープンスタンダードです。

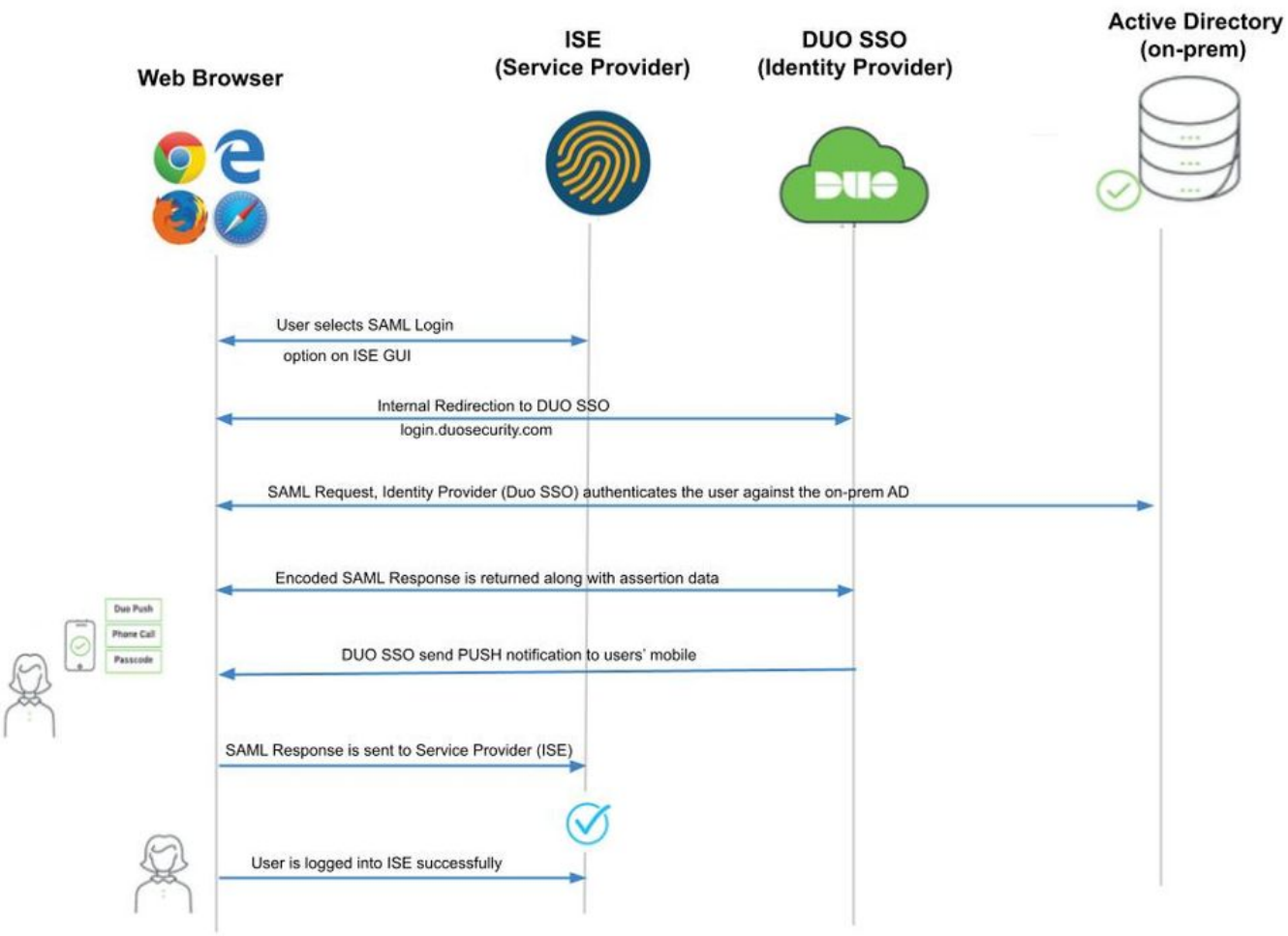
SAMLトランザクションは、IDプロバイダーとサービスプロバイダー間の標準化された通信にExtensible Markup Language(XML)を使用します。SAMLは、ユーザのIDの認証とサービスを使用するための許可の間のリンクです。

## SAMLアサーション

SAMLアサーションは、IdPがユーザ認証を含むサービスプロバイダーに送信するXMLドキュメントです。SAMLアサーションには、認証、属性、認可の決定という3つの異なるタイプがあります。

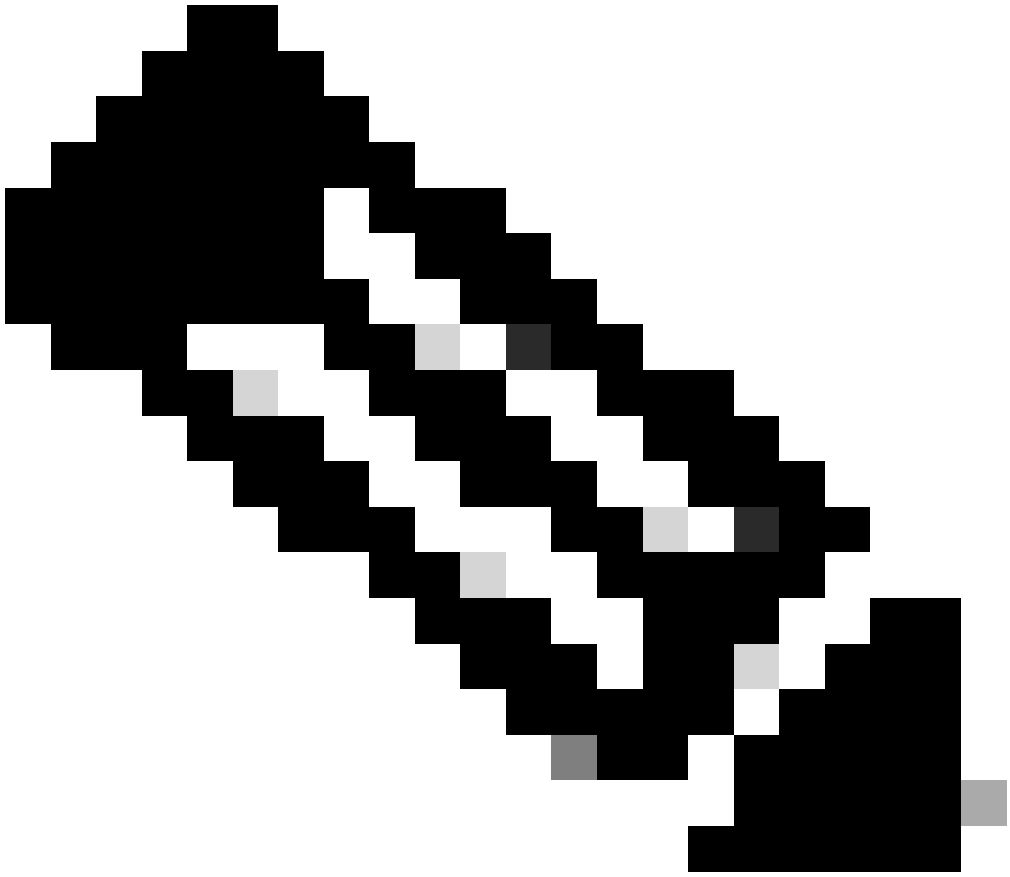
- 認証アサーションは、ユーザのIDを証明し、ユーザがログインした時間と使用した認証方法（Kerberos、二要素など）を提供します。
- アトリビューションアサーションは、SAML属性（ユーザに関する情報を提供する特定のデータ）をSPに渡します。
- 認証の決定アサーションは、ユーザがサービスを使用する権限を持っているか、パスワードの失敗またはサービスへの権限の欠如が原因でIdPが要求を拒否したかを宣言します。

# 高レベルフロー図




Flow:

1. ユーザは、Login Via SAMLオプションを使用してISEにログインします。
2. ISE(SAML SP)は、ユーザのブラウザをSAML要求メッセージを含むDuo SSOにリダイレクトします。



注：分散環境では、「Invalid Certificate」エラーが表示される場合があり、ステップ3を実行できます。したがって、分散環境の場合、手順2.は次の点で少し異なります。
問題：ISEは、いずれかのPSNノード（ポート8443）のポータルに一時的にリダイレクトします。
解決策：ISEが管理GUI証明書と同じ証明書を提示することを確認するために、信頼するシステム証明書がすべてのPSNノードでもポータル使用に対して有効であることを確認します。

3. ユーザはプライマリADクレデンシャルでログインします。
4. Duo SSOはこの応答をADに転送し、ADは応答をDuo SSOに返します。
5. Duo SSOでは、モバイルでプッシュを送信して2要素認証を完了する必要があります。
6. ユーザがDuoの2要素認証を完了します。
7. Duo SSOは、ユーザのブラウザを応答メッセージとともにSAML SPにリダイレクトします。
8. これで、ユーザはISEにログインできるようになります。

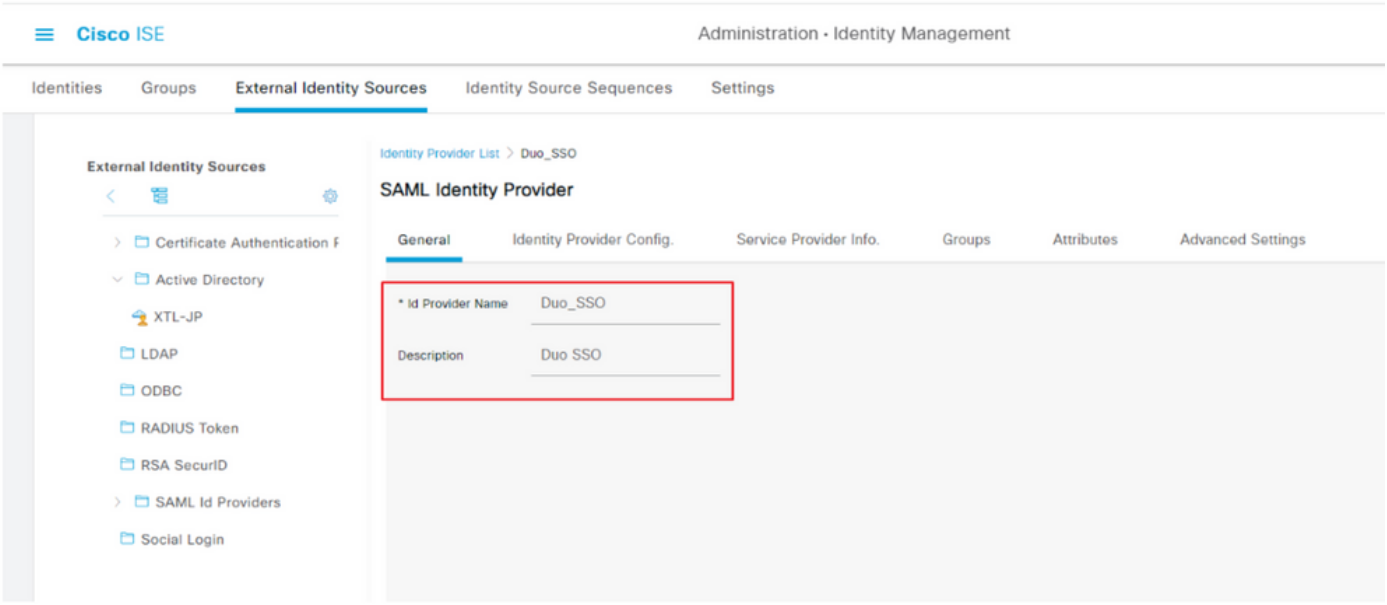
# Duo SSOとのSAML SSO統合の設定

## ステップ 1：ISEでのSAML IdPの設定

### 外部SAMLアイデンティティ・ ソースとしてのDuo SSOの構成

ISEでAdministration > Identity Management > External Identity Sources > SAML Id Providersに移動し、Addボタンをクリックします。

IdPの名前を入力し、**Submit**をクリックして保存します。IdP名は、図に示すように、ISEに対してのみ意味を持ちます。

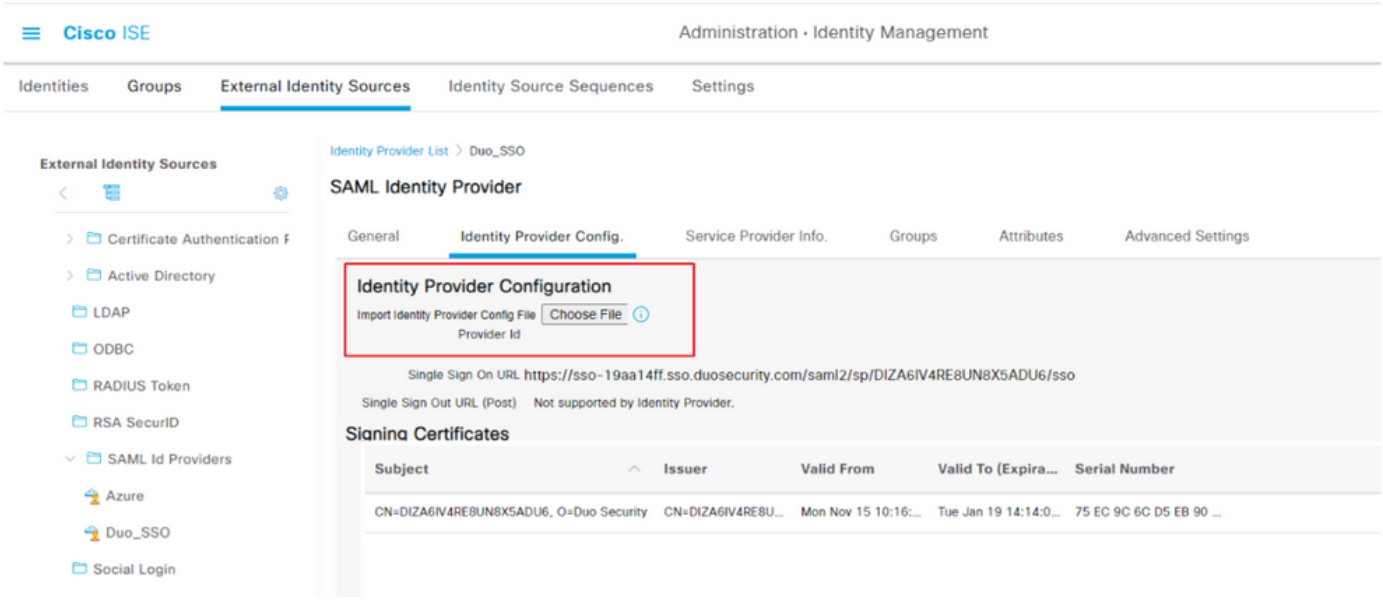



Duo AdminポータルからSAMLメタデータXMLファイルをインポートします

ISEで、Administration > Identity Management > External Identity Sources > SAML Id Providers. >作成したSAML IdPを選択します。をクリックし、 Identity Provider Configuration、ファイルの選択ボタンをクリックします。

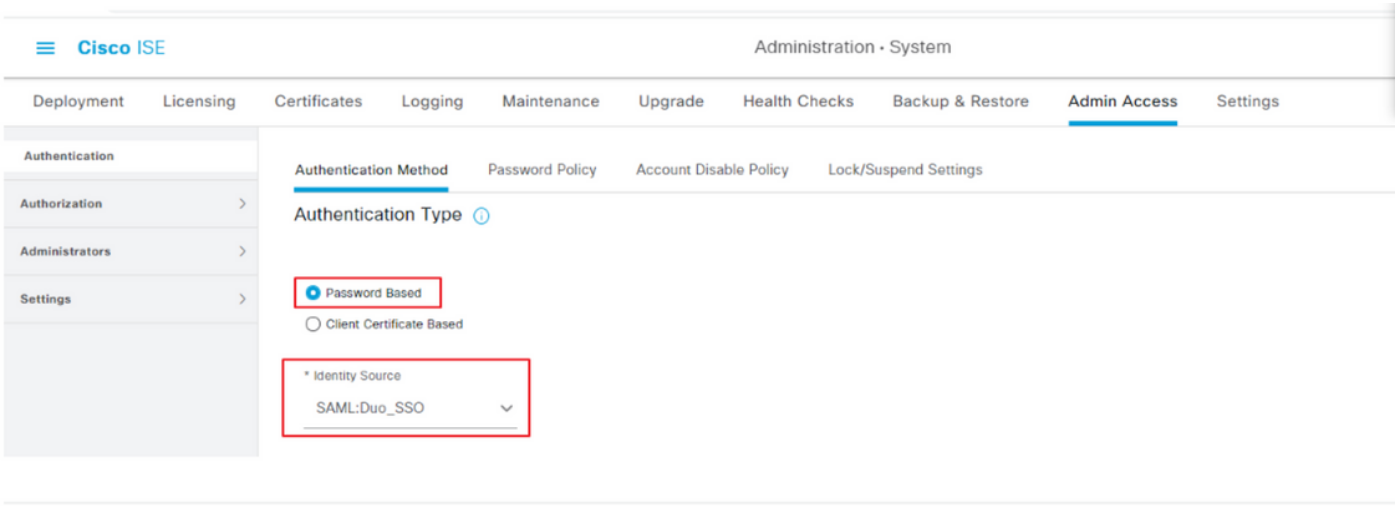
Duo Adminポータルからエクスポートされた**SSO IDP**メタデータ**XML**ファイルを選択し、**Open**をクリックして保存します。（この手順は、このドキュメントの「Duo」の項にも記載されています）。

SSO URLおよび署名証明書は次のとおりです。




ISE認証方式の設定

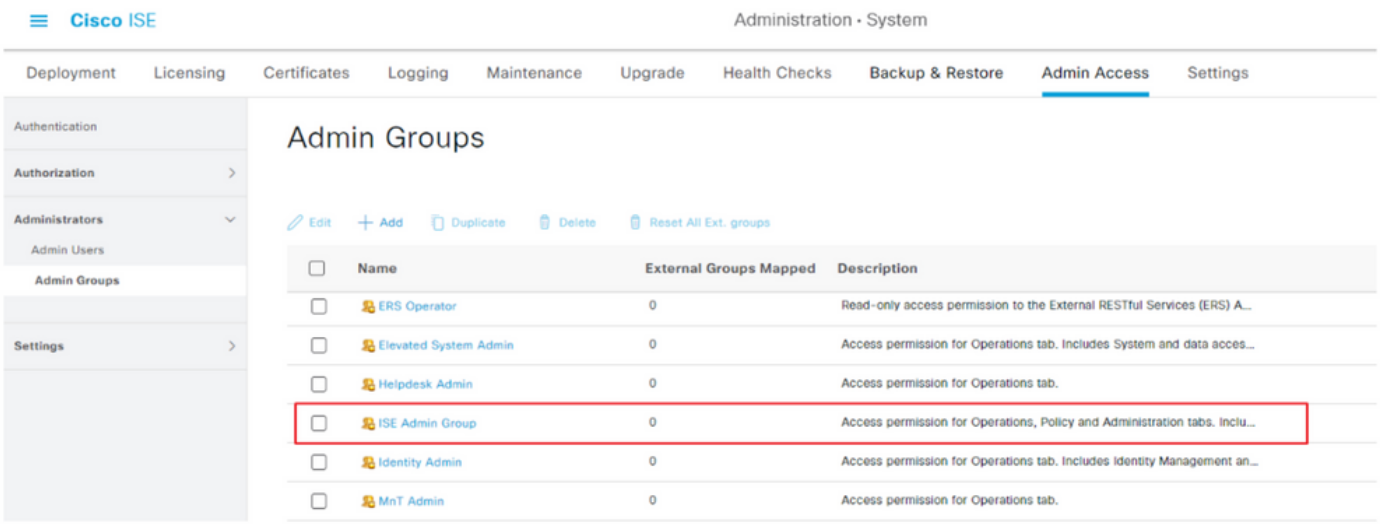
Administration > System > Admin Access > Authentication > Authentication Methodに移動し、Password-Basedオプションボタンを選択します。図に示すように、Identity Sourceドロップダウンリストから、先に作成した必要なIdP名を選択します。




管理グループの作成

Administration > System > Admin Access > Authentication > Administrators > Admin Groupに移動し、Super Adminをクリックしてから、Duplicateボタンをクリックします。**Admin group Name**を入力し、**Submit**ボタンをクリックします。

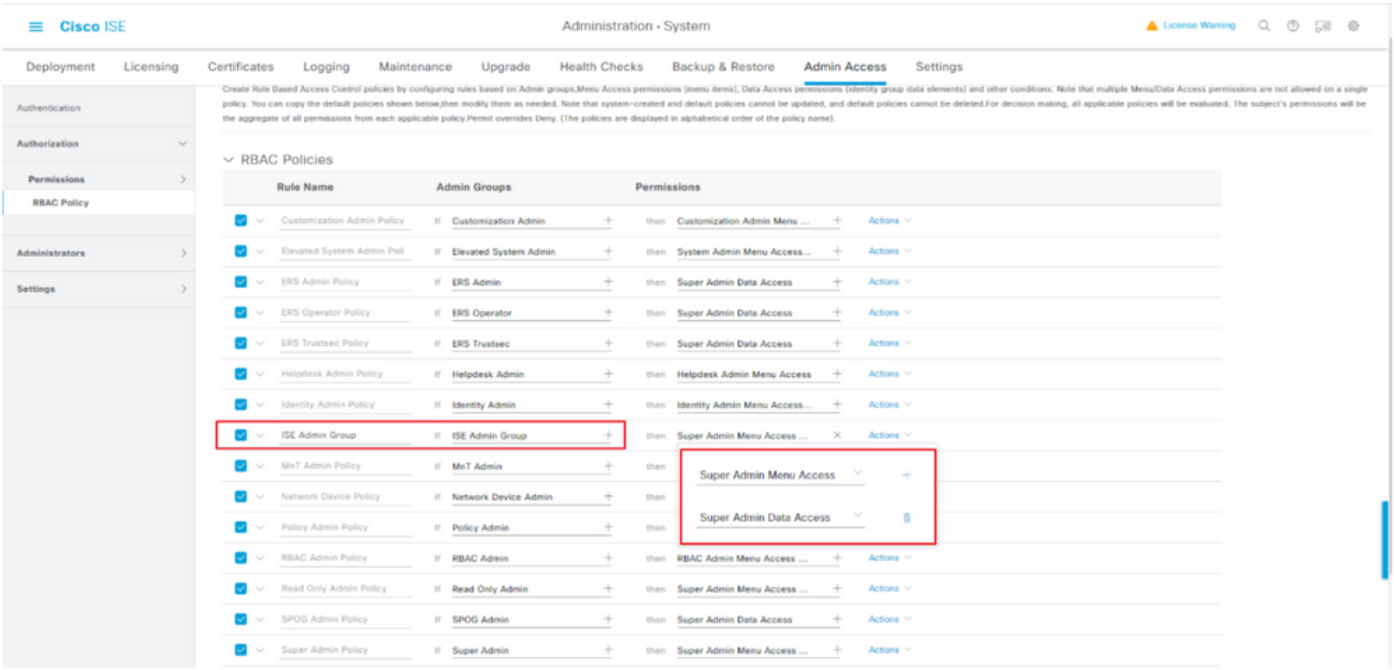
これにより、管理者グループにスーパー管理者権限が付与されます。




管理グループのRBACポリシーの作成

Administration > System > Admin Access > Authorization > RBAC Policyに移動し、Super Admin Policyに対応する**Actions**を選択します。をクリックします。Duplicate > Add the Name field > Save

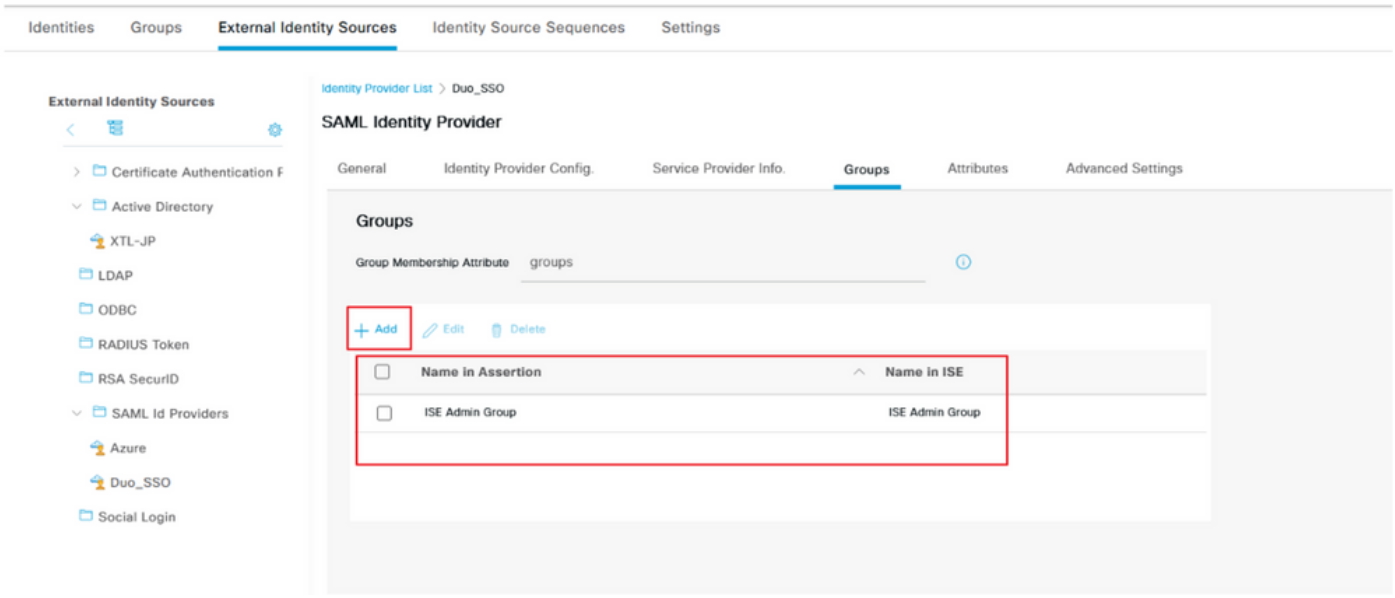
アクセスの権限は、スーパー管理者ポリシーと同じです。




グループメンバーシップの追加

ISEで、Administration > Identity Management > External Identity Sources > SAML Id Providersに移動し、作成したSAML IdPを選択します。**Groups**をクリックし、次にAddボタンをクリックします。

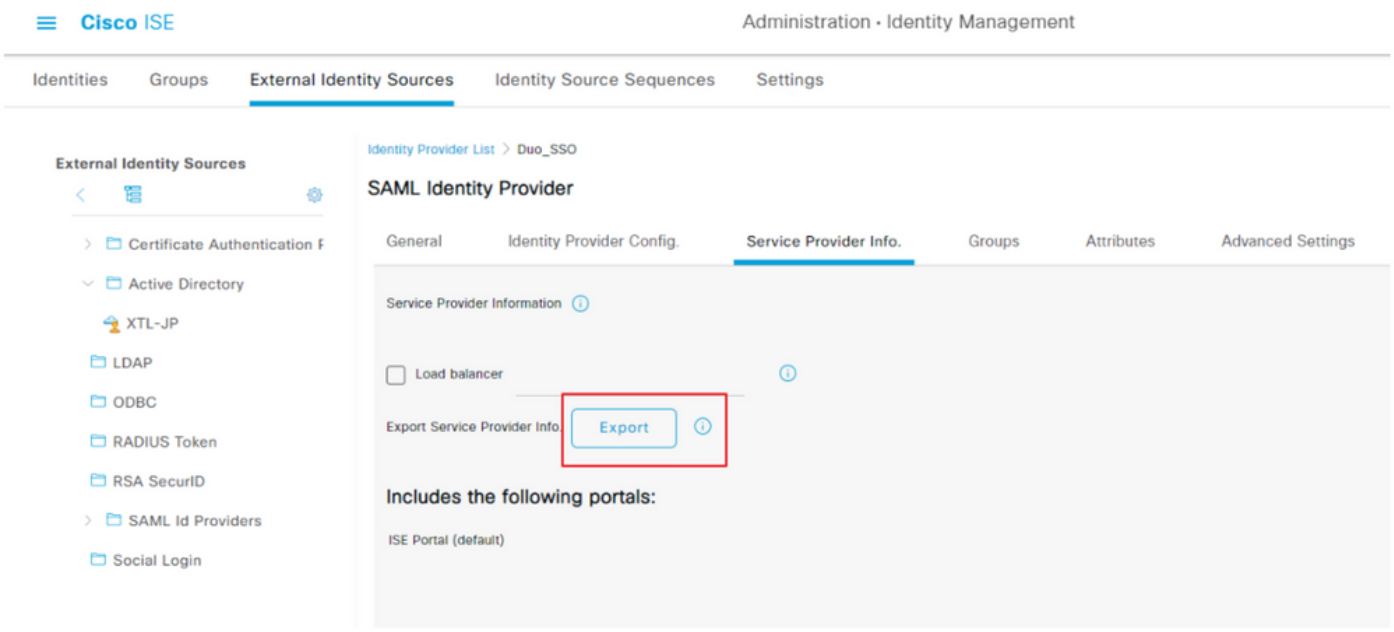
Name in Assertion（ISE管理グループの名前）を追加し、ドロップダウンから作成したロールベースアクセスコントロール(RBAC)グループを選択し（ステップ4）、**Open**をクリックして保存します。SSO URLと署名証明書は自動的に入力されます。




SP情報のエクスポート

Administration > Identity Management > External Identity Sources > SAML Id Providers > (Your SAML Provider)に移動します。

タブをSP Info.に切り替え、図に示すように**Export**ボタンをクリックします。




.xmlのファイルをダウンロードして保存します。AssertionConsumerService URLとentityIDの値をメモしてください。これらの詳細はDuo SSOポータルで必要です。

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

メタファイルから収集された対象の詳細/属性は、Duo Generic SAML統合で設定する必要があります

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

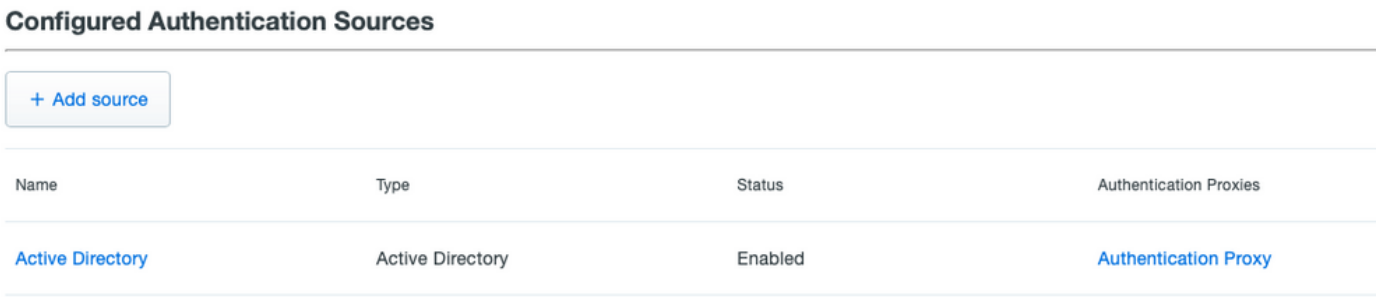
f5e56429779dです。

AssertionConsumerService Location = https://10.x.x.x:8443/portal/SSOLoginResponse.action(10.x.x.xはXMLファイルにあるISE IP（場所））。

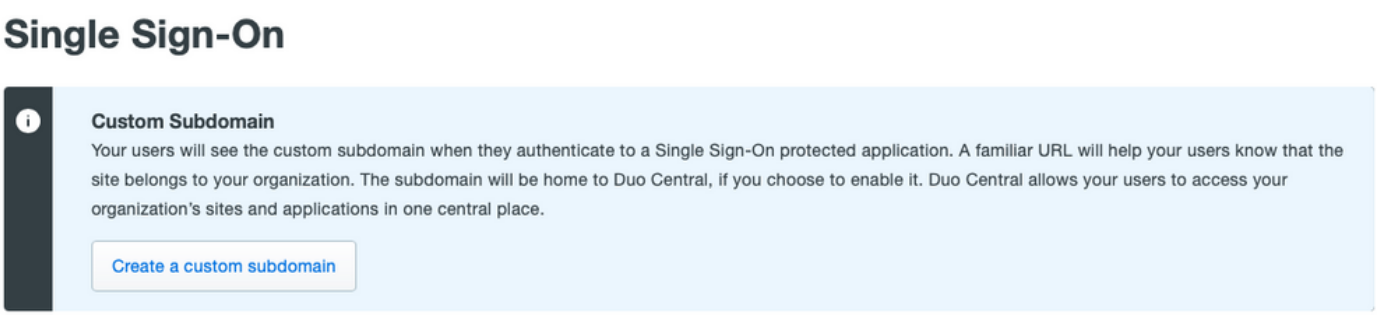
AssertionConsumerService Location = https://isenodename.com:8443/portal/SSOLoginResponse.action。ここで、isenodenameはXMLファイル(Location)で見つかった実際のISE FQDN名です。

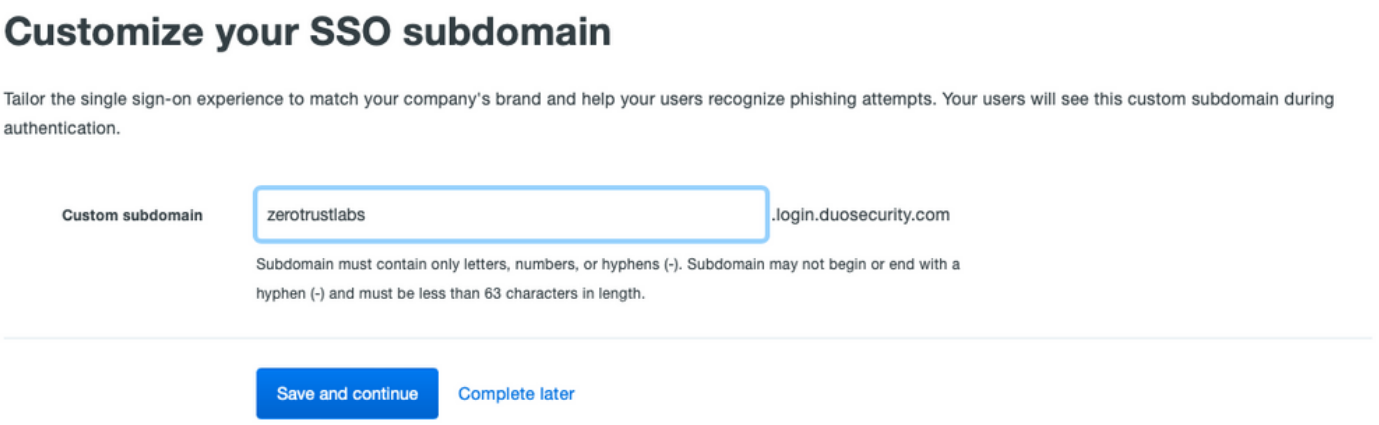
ステップ 2：ISE用のDuo SSOの設定

ADを認証ソースとして使用するDuo SSOを設定するには、このKBを確認します。




カスタムドメインでSSOを有効にするには、このKBを確認します。



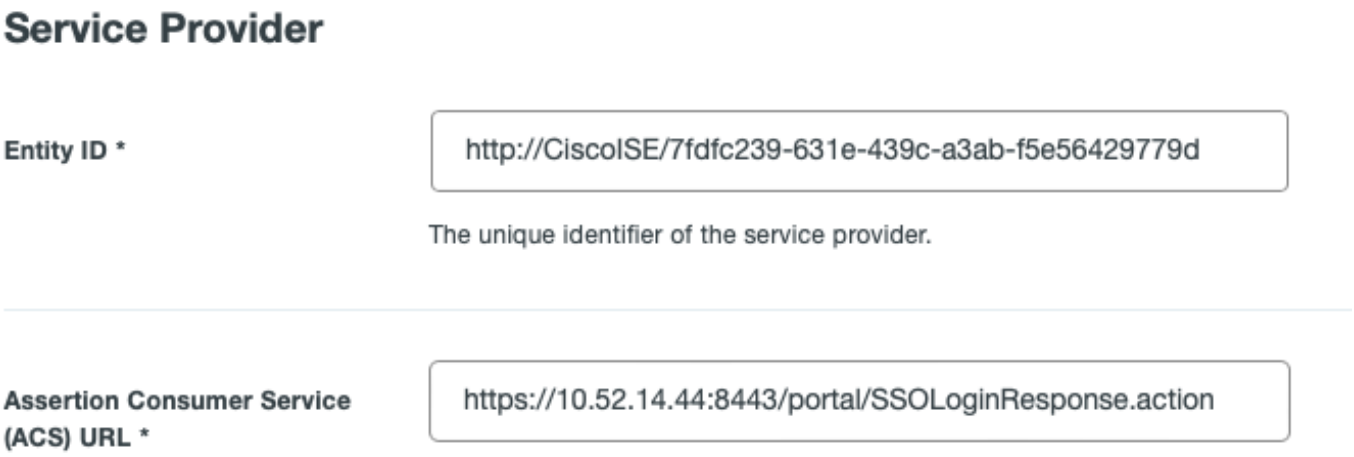




ステップ 3：Cisco ISEとDuo SSOを汎用SPとして統合

Cisco ISEとDuo SSOを一般的なSPとして統合するには、このKBのステップ1.とステップ2を確認します。

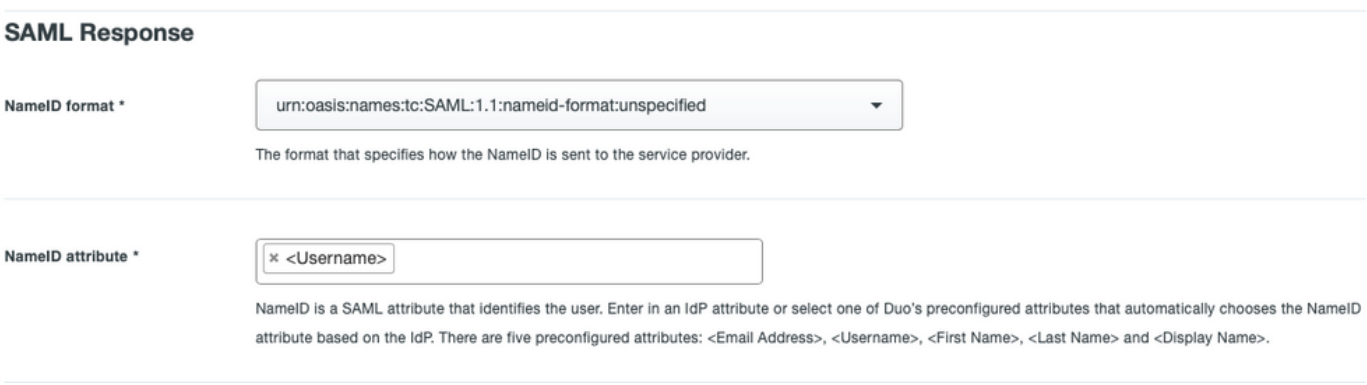
汎用SPのDuo管理パネルでCisco ISE SPの詳細を設定します。

| [名前(Name)] | 説明 |
| --- | --- |
| エンティティID | http://CiscoISE/7fdfc239-631e-439c-a3ab-f5e56429779d |
| アサーションコンシューマサービス(ACS)のURL | https://10.x.x.x:8443/portal/SSOLoginResponse.action |

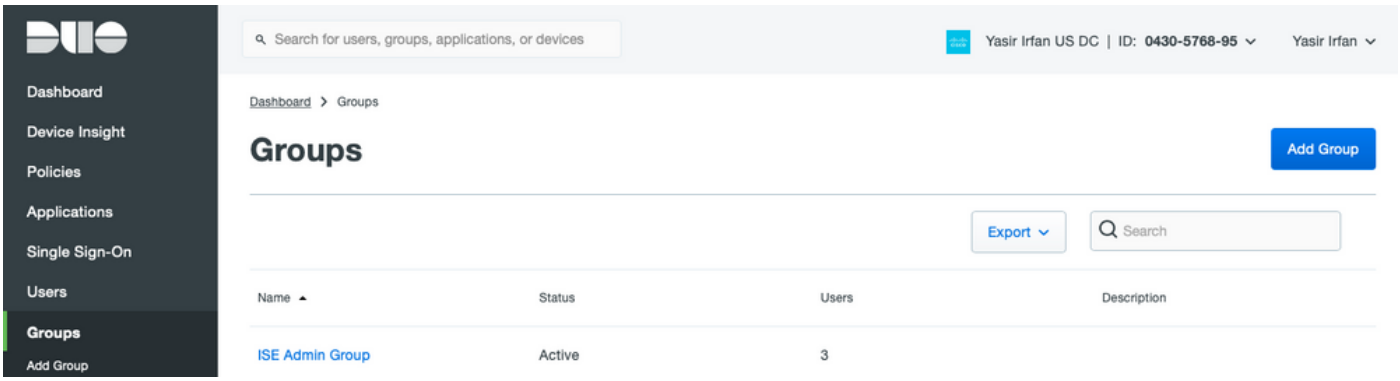



Cisco ISEのSAML応答の設定：

| [名前(Name)] | 説明 |
| --- | --- |
| NameIDの形式 | urn:oasis:names:tc:SAML:1.1:nameid-format：未指定 |
| NameID属性 | ユーザ名 |

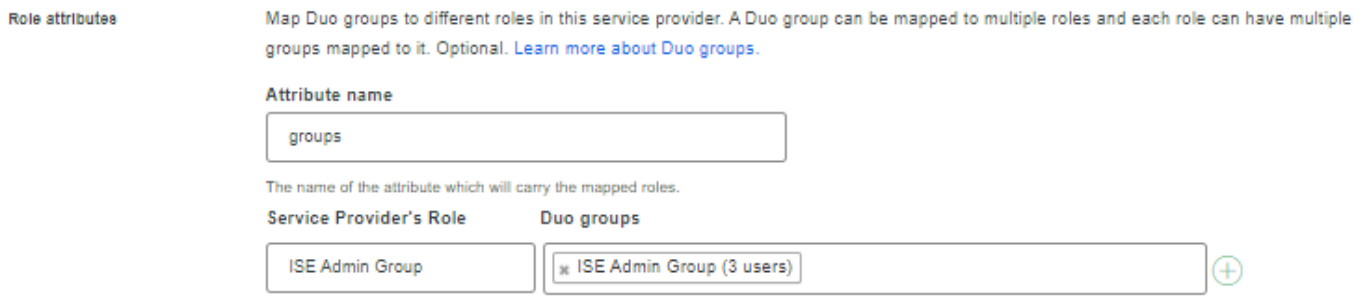



Duo Admin PanelでCisco Admin Groupという名前のグループを作成し、ISEユーザをこのグループに追加するか、Windows ADでグループを作成し、ディレクトリ同期機能を使用してDuo Admin Panelと同期します。

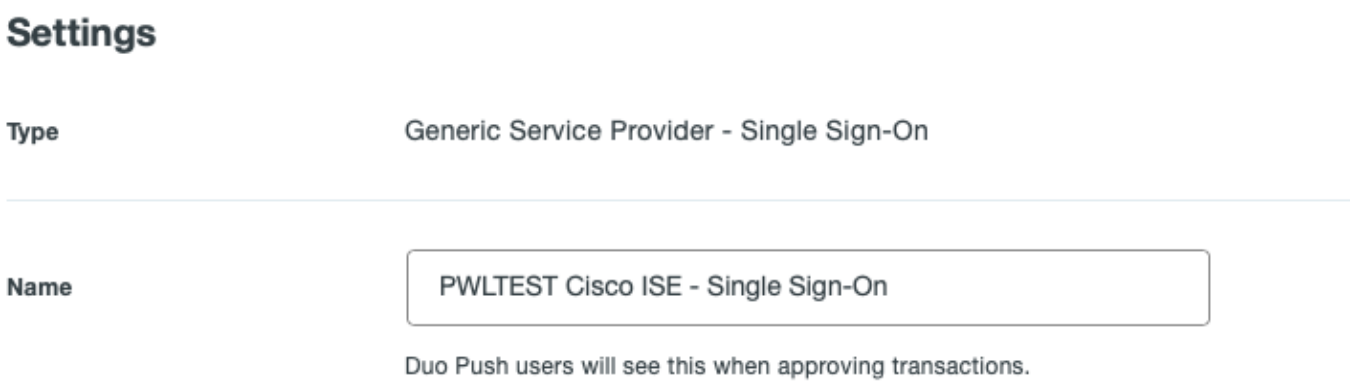



Cisco ISEのロール属性の設定：

| [名前(Name)] | 説明 |
|---|---|
| 属性名 | [グループ（groups）] |
| SPロール | ISE管理グループ |
| デュオグループ | ISE管理グループ |

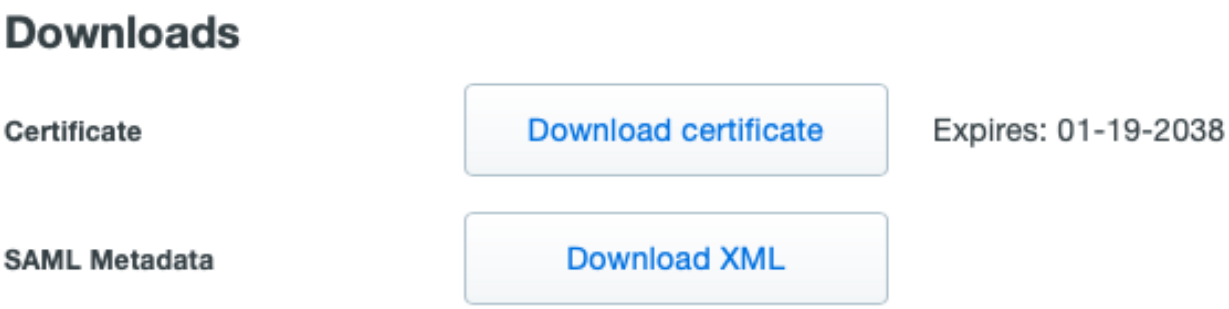



設定セクションで、この統合の名前タブに適切な名前を指定します。



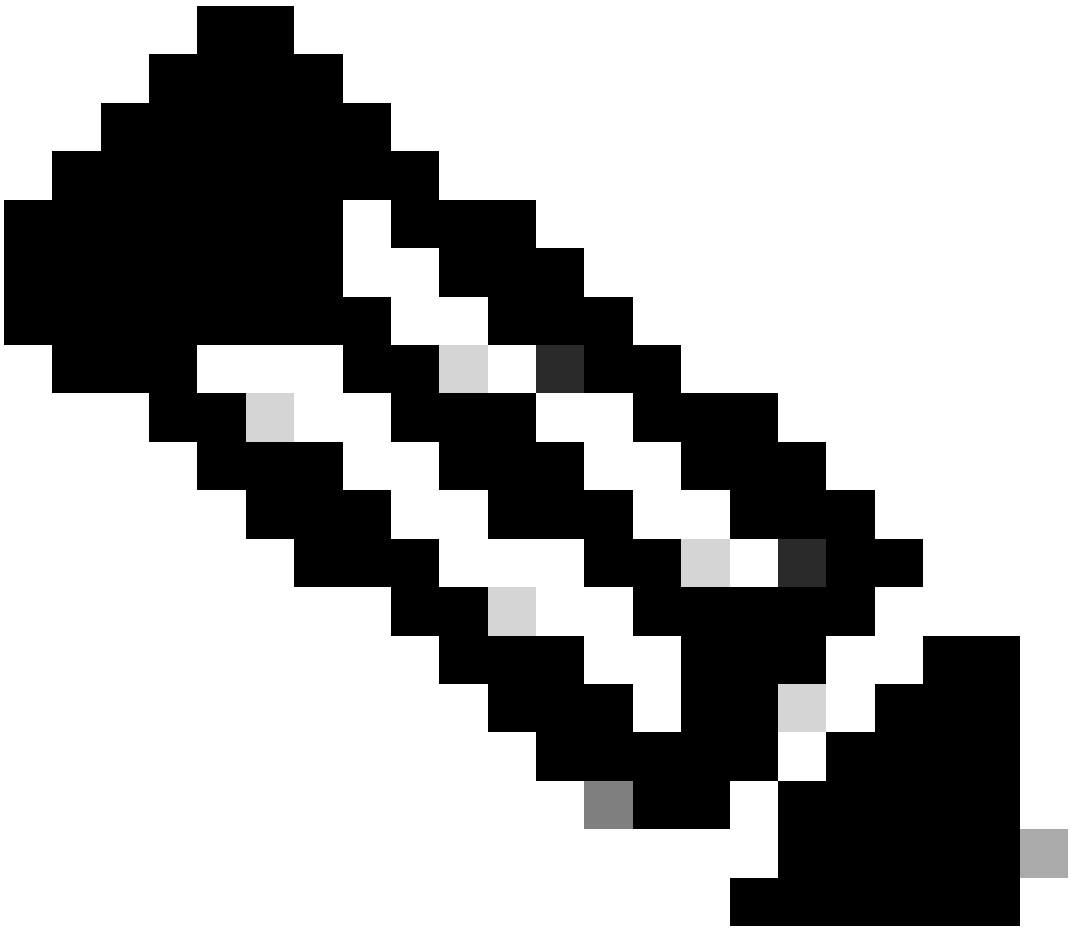

**Save**ボタンをクリックして設定を保存し、この**KB**で詳細を参照してください。

**Download XML**をクリックして、SAMLメタデータをダウンロードします。



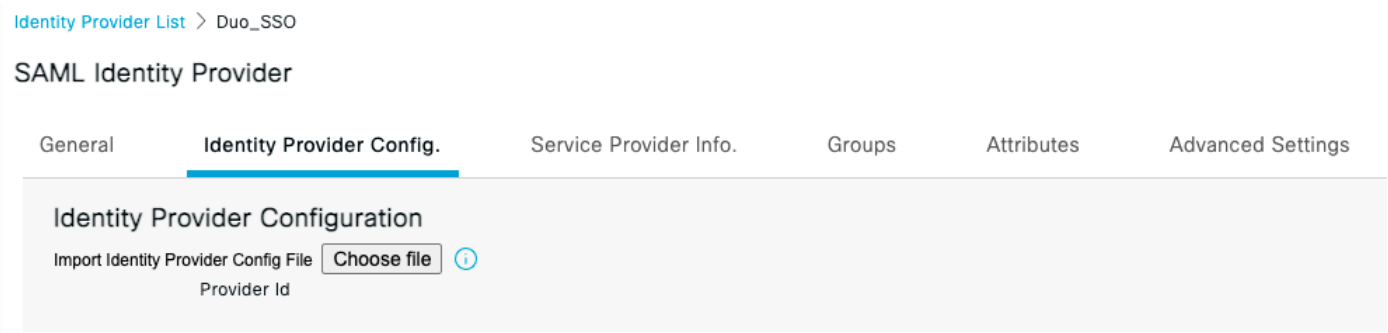

Administration > Identity Management > External Identity Sources > SAML Id Providers > Duo_SSOに移動して、Duo Admin PanelからCisco ISEにSAML MetaDataダウンロードをアップロードします。
タブを**Identity Provider Config.**に切り替え、**Choose** fileボタンをクリックします。
ステップ8でダウンロードしたメタデータ**XML**ファイルを選択し、**Save**をクリックします。

---



---

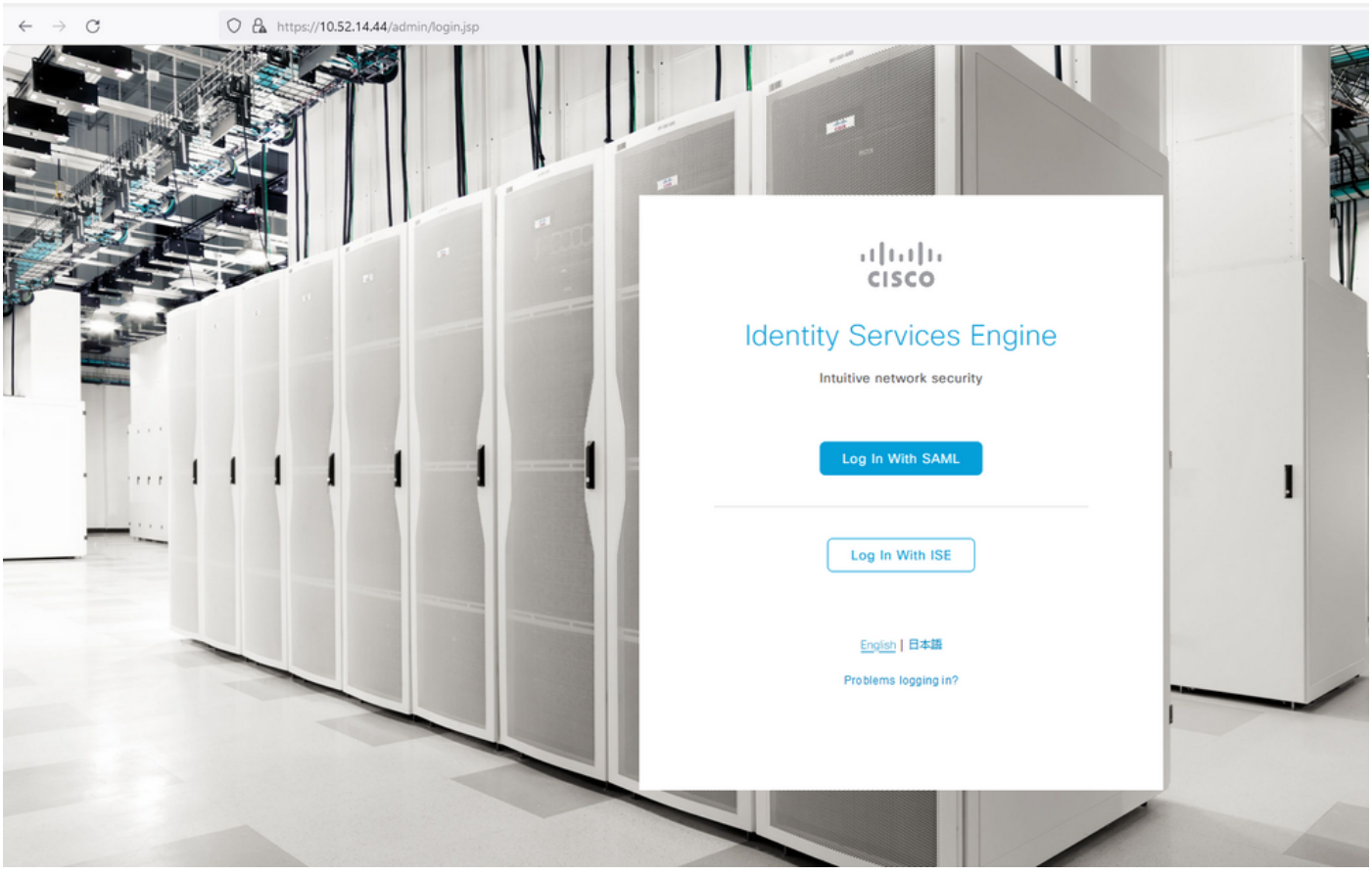
注：この手順については、「Duo SSOを使用したSAML SSO統合の設定」セクションの手順2で説明しています。Duo Adminポータルから**SAML**メタデータ**XML**ファイルをインポートします。



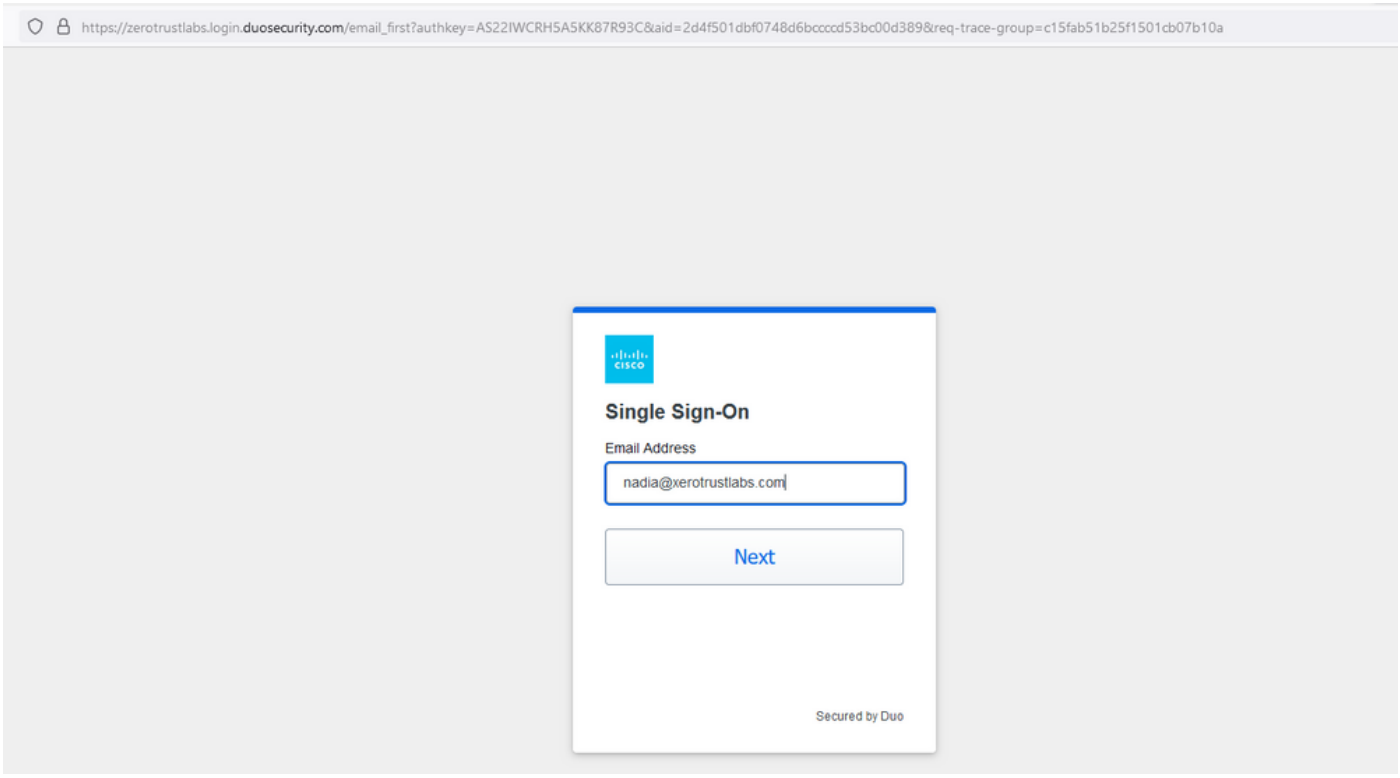

**確認**

Duo SSOとの統合のテスト

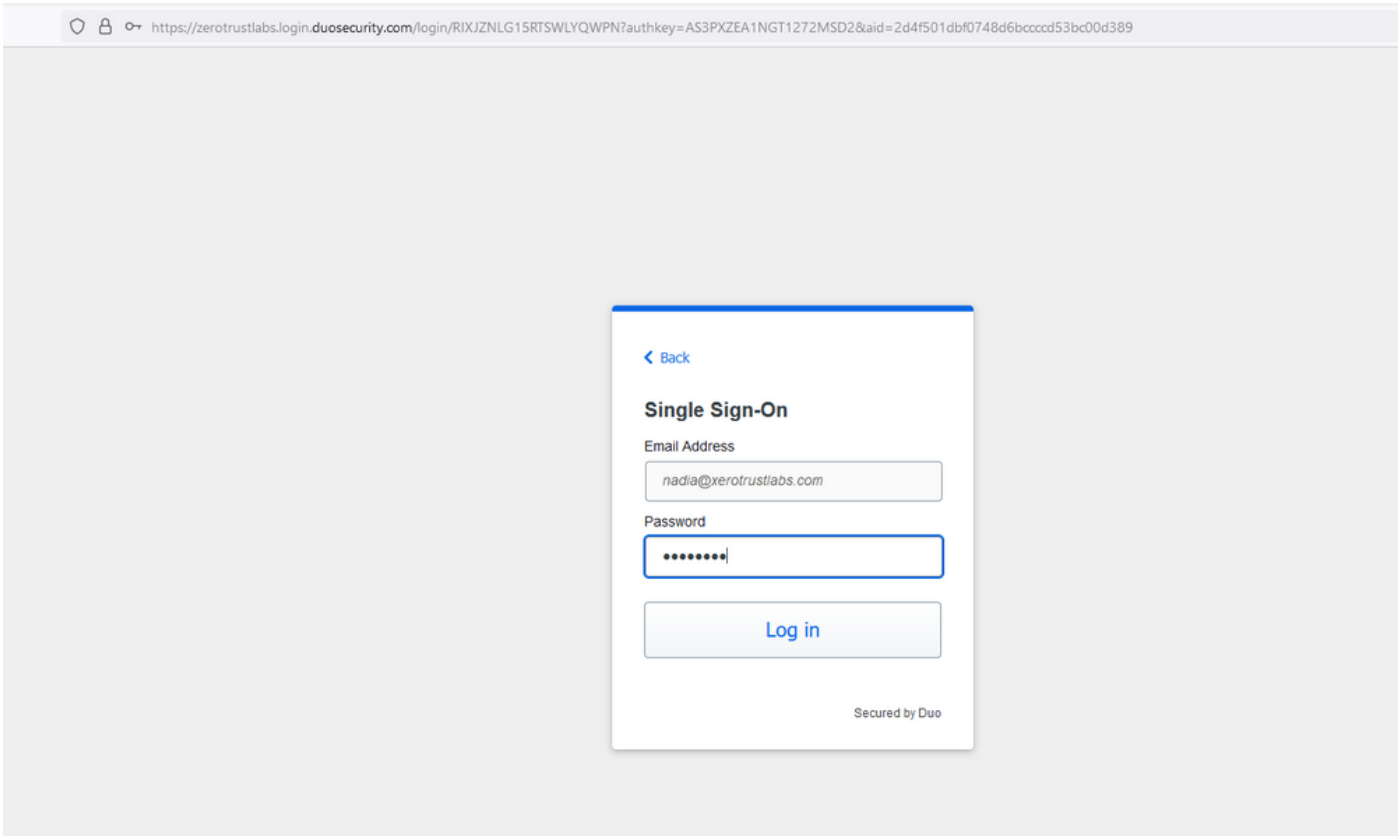
1. **Cisco ISE Admin Panel**にログインして、**Log In** With SAMLをクリックします。



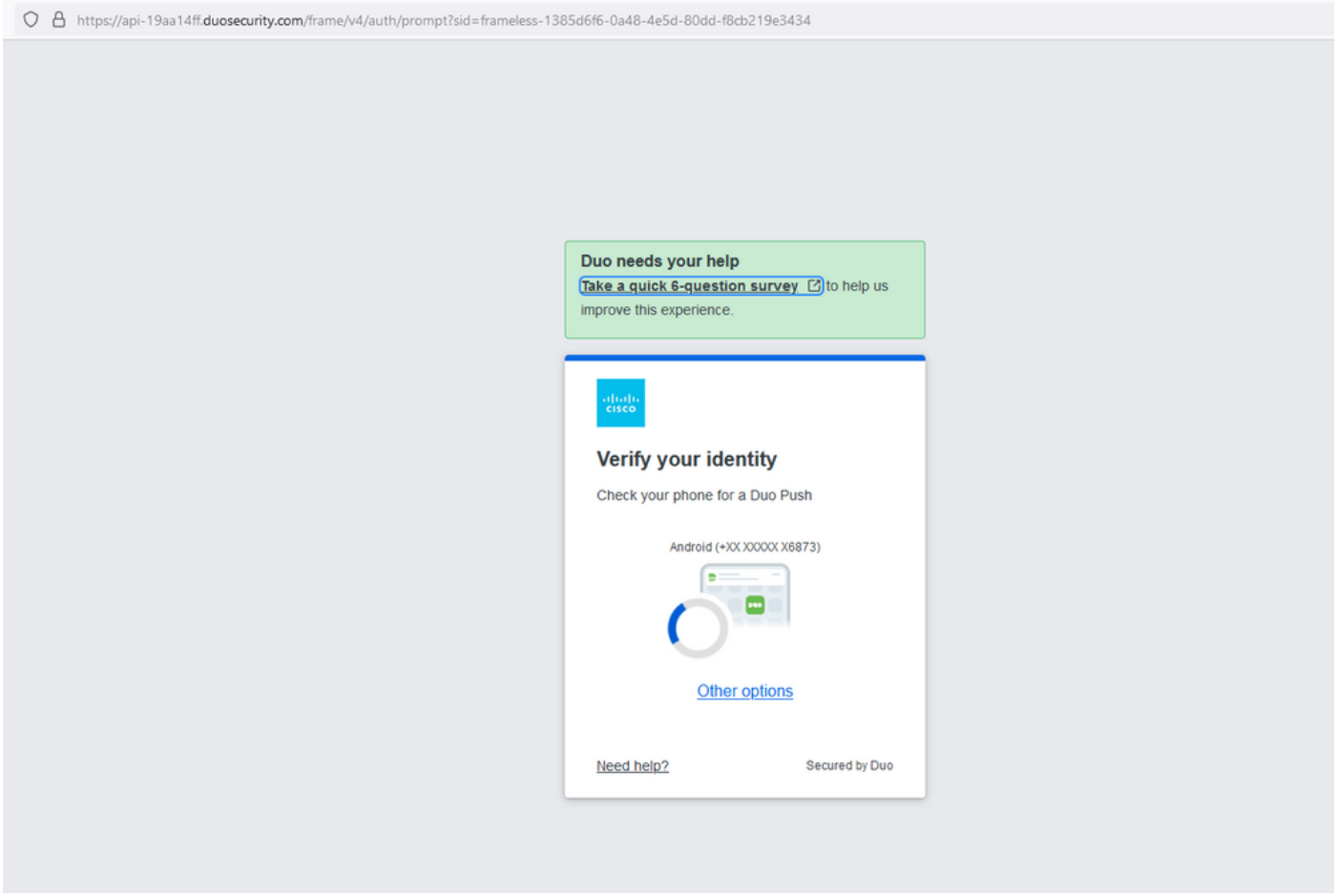

2. SSOページにリダイレクトされ、電子メールアドレスを入力して、**Next**をクリックします。



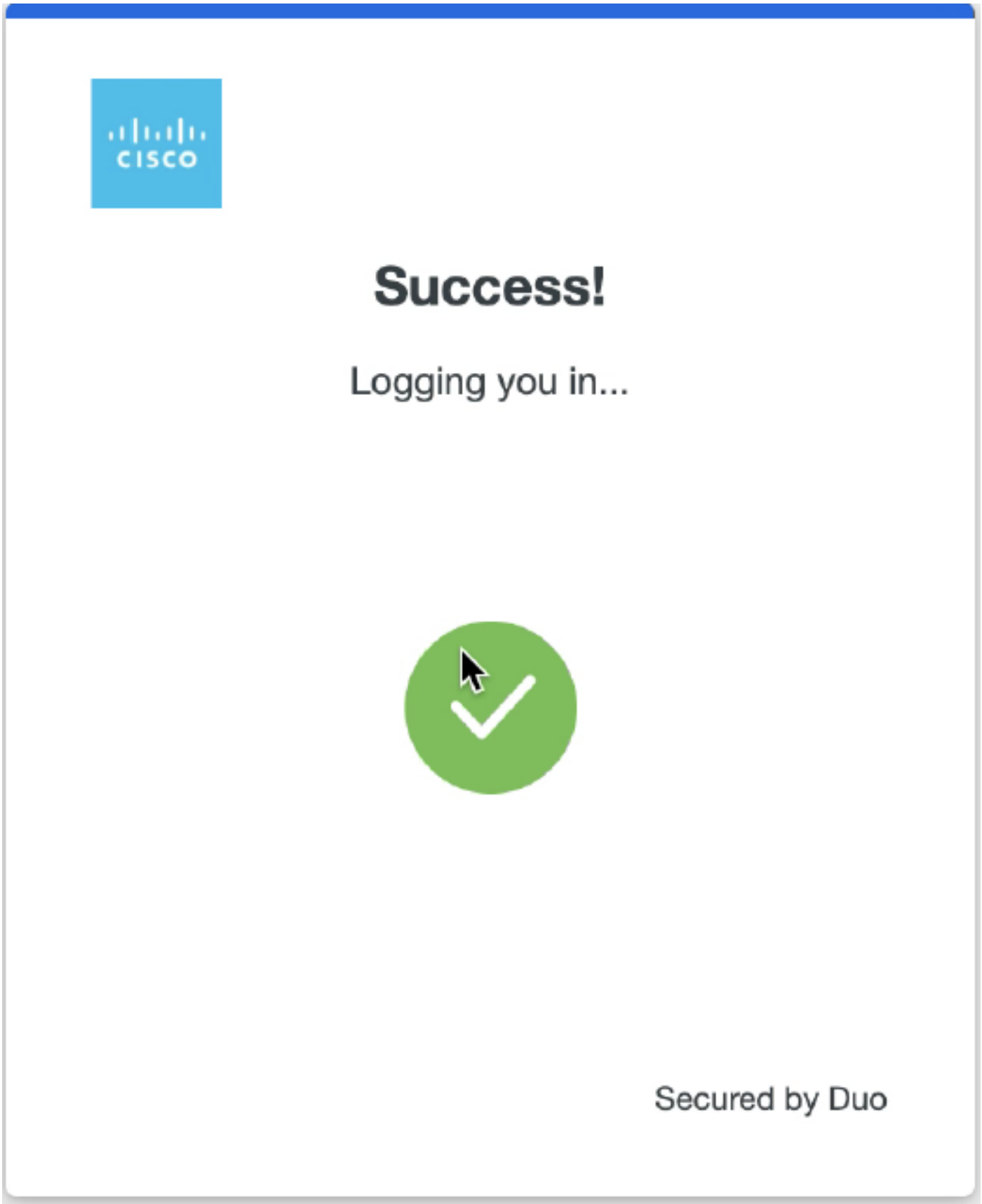

3. パスワードを入力し、**Log in**をクリックします。



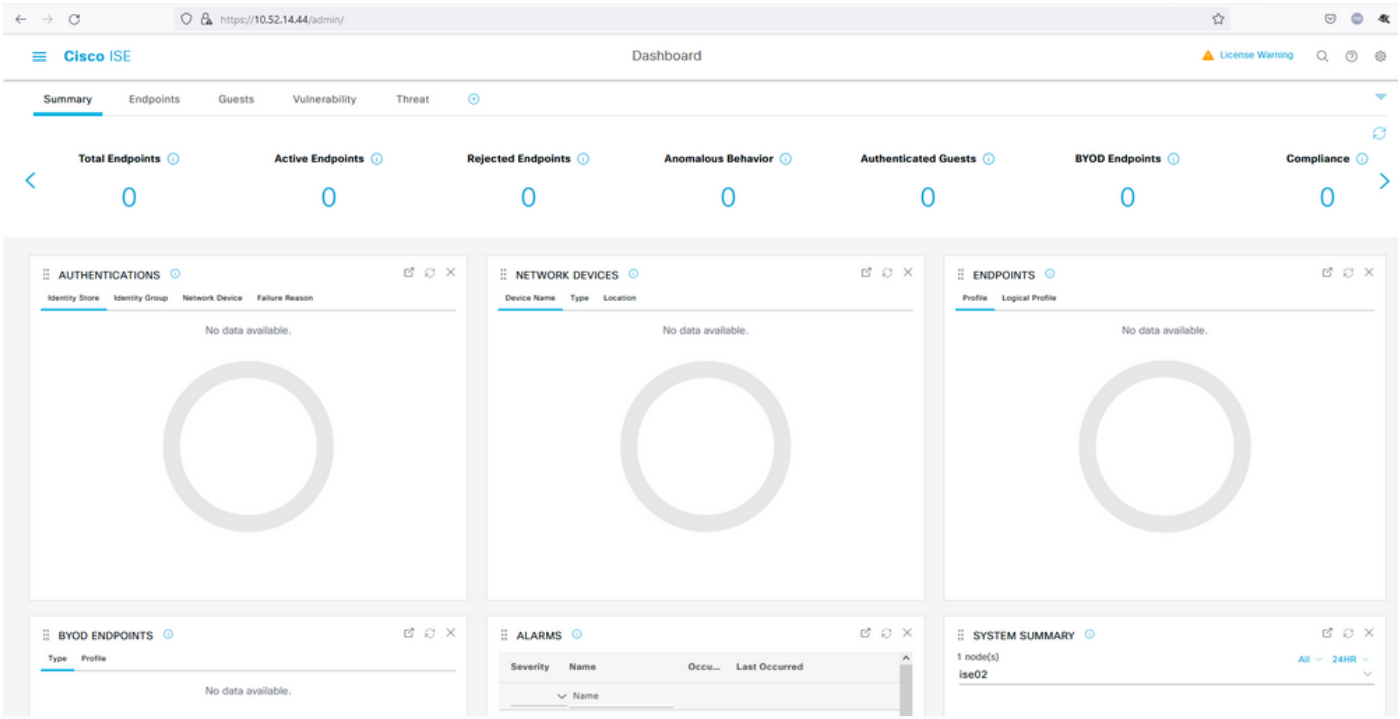

4. モバイルデバイスにDuoプッシュプロンプトが表示されます。




5. プロンプトを受け入れると、ウィンドウが表示され、ISE管理ページに自動的にリダイレクトされます。




6. ISE管理GUIアクセスページ。

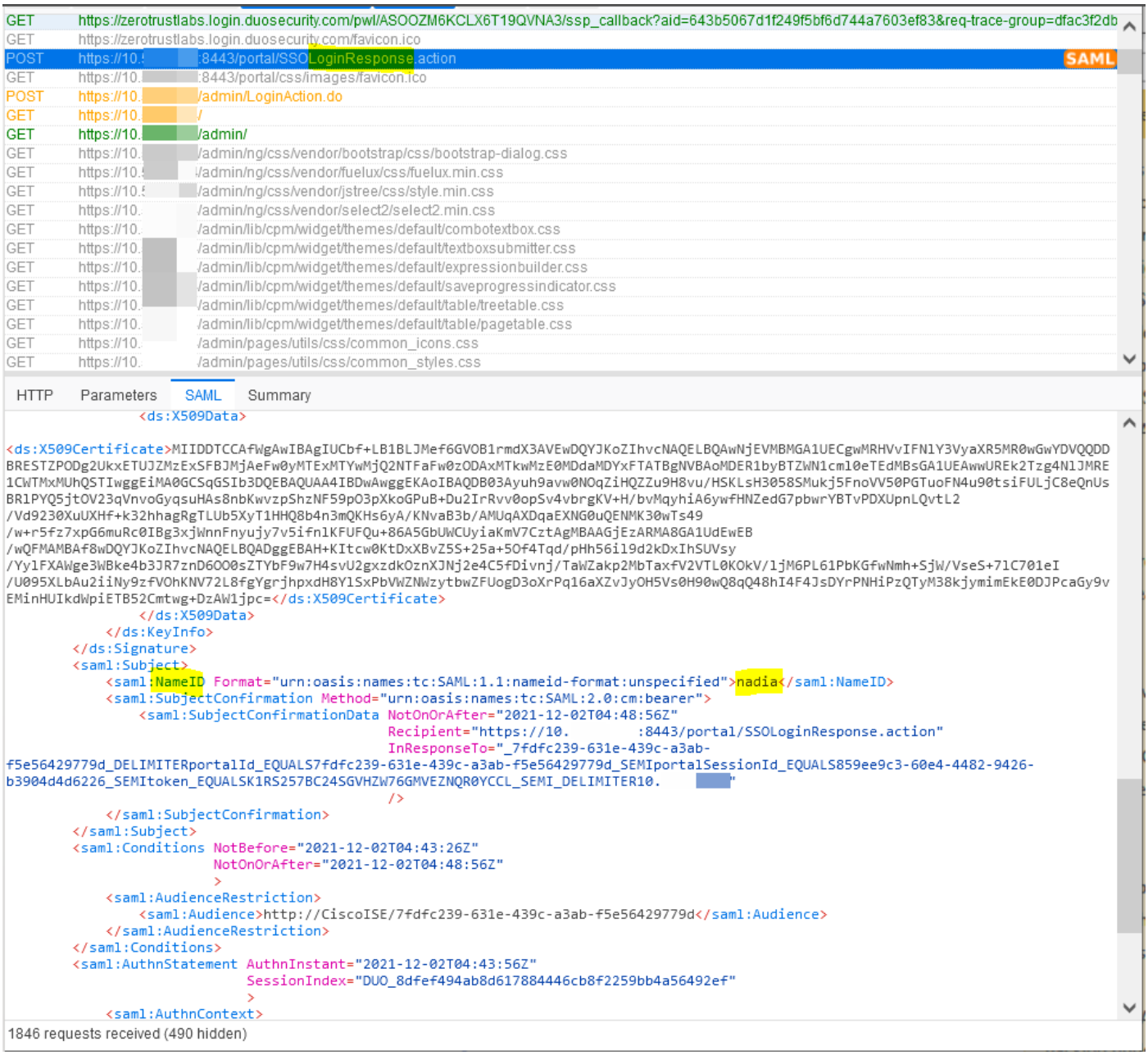



トラブルシュート

- Mozilla FF https://addons.mozilla.org/en-US/firefox/addon/saml-tracer/向けSAMLトレーサ拡張をダウンロードしてください。

SSOLoginResponse.action

- のパケットまでスクロールします。**SAML**タブの下に、Duo SAMLから送信されたNameID、Recipient（AssertionConsumerServiceロケーションURL）、Audience(EntityID)の多数の属性が表示されます。


GET https://zerotrustlabs.login.duosecurity.com/pwl/ASOOZM6KCLX6T19QVNA3/ssp_callback?aid=643b5067d1f249f5bf6d744a7603ef83&req-trace-group=dfac3f2db
GET https://zerotrustlabs.login.duosecurity.com/favicon.ico
POST https://10.[redacted]:8443/portal/SSOLoginResponse.action SAML
GET https://10.[redacted]:8443/portal/css/images/favicon.ico
POST https://10.[redacted]/admin/LoginAction.do
GET https://10.[redacted]/
GET https://10.[redacted]/admin/
GET https://10.[redacted]/admin/ng/css/vendor/bootstrap/css/bootstrap-dialog.css
GET https://10.[redacted]/admin/ng/css/vendor/fuelux/css/fuelux.min.css
GET https://10.[redacted]/admin/ng/css/vendor/jstree/css/style.min.css
GET https://10.[redacted]/admin/ng/css/vendor/select2/select2.min.css
GET https://10.[redacted]/admin/lib/cpm/widget/themes/default/combotextbox.css
GET https://10.[redacted]/admin/lib/cpm/widget/themes/default/textboxsubmitter.css
GET https://10.[redacted]/admin/lib/cpm/widget/themes/default/expressionbuilder.css
GET https://10.[redacted]/admin/lib/cpm/widget/themes/default/saveprogressindicator.css
GET https://10.[redacted]/admin/lib/cpm/widget/themes/default/table/treetable.css
GET https://10.[redacted]/admin/lib/cpm/widget/themes/default/table/pagetable.css
GET https://10.[redacted]/admin/pages/utils/css/common_icons.css
GET https://10.[redacted]/admin/pages/utils/css/common_styles.css
HTTP
Parameters
SAML
Summary
<ds:X509Data>
<ds:X509Certificate>MIIDDTCCAfWgAwIBAgIUCbf+LB1BLJMef6GVOB1rmdX3AVEwDQYJKoZIhvcNAQELBQAwNjEVMBMGA1UECgwMRHVvIFNlY3VyaXR5MR0wGwYDVQQDDBRESTZPODg2UkxETUJZMzExSFBJMjAeFw0yMTExMTYwMjQ2NTFaFw0zODAxMTkwMzE0MDdaMDYxFTATBgNVBAoMDER1byBTZWN1cml0eTEdMBsGA1UEAwwUREk2Tzg4NlJMRE1CWTMxMUhQSTIwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDB03Ayuh9avw0NOqZiHQZZu9H8vu/HSKLsH3058SMukj5FnoVV50PGTuoFN4u90tsiFULjC8eQnUsBR1PYQ5jtOV23qVnvoGyqsuHAs8nbKwvzpShzNF59pO3pXkoGPuB+Du2IrRvv0opSv4vbrgKV+H/bvMqyhiA6ywfHNZedG7pbwrYBTvPDXUpnLQvtL2/Vd9230XuUXHf+k32hhagRgTLUb5XyT1HHQ8b4n3mQKHs6yA/KNvaB3b/AMUqAXDqaEXNG0uQENMK30wTs49/w+r5fz7xpG6muRc0IBg3xjWnnFnyujy7v5ifnlKFUFQu+86A5GbUWCUyiaKmV7CztAgMBAAGjEzARMA8GA1UdEwEB/wQFMAMBAf8wDQYJKoZIhvcNAQELBQADggEBAH+KItcw0KtDxXBvZ5S+25a+5Of4Tqd/pHh56il9d2kDxIhSUVsy/Yy1FXAWge3WBke4b3JR7znD6OO0sZTYbF9w7H4svU2gxzdkOznXJNj2e4C5fDivnj/TaWZakp2MbTaxfV2VTL0KOkV/1jM6PL61PbKGfwNmh+SjW/VseS+71C701eI/U095XLbAu2iiNy9zfVOhKNV72L8fgYgrjhpxdH8Y1SxPbVWZNWzytbwZFUogD3oXrPq16aXZvJyOH5Vs0H90wQ8qQ48hI4F4JsDYrPNHiPzQTyM38kjymimEkE0DJPcaGy9vEMinHUIkdWpiETB52Cmtwg+DzAW1jpc=</ds:X509Certificate>
</ds:X509Data>
</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. :8443/portal/SSOLoginResponse.action"
InResponseTo="_7fdfc239-631e-439c-a3ab-f5e56429779d_DELIMITERportalId_EQUALS7fdfc239-631e-439c-a3ab-f5e56429779d_SEMIportalSessionId_EQUALS859ee9c3-60e4-4482-9426-b3904d4d6226_SEMItoken_EQUALSK1RS257BC24SGVHZW76GMVEZNQR0YCCL_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_8dfef494ab8d617884446cb8f2259bb4a56492ef"
>
<saml:AuthnContext>
1846 requests received (490 hidden)

- ISEのライブログ：

Cisco ISE

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 |

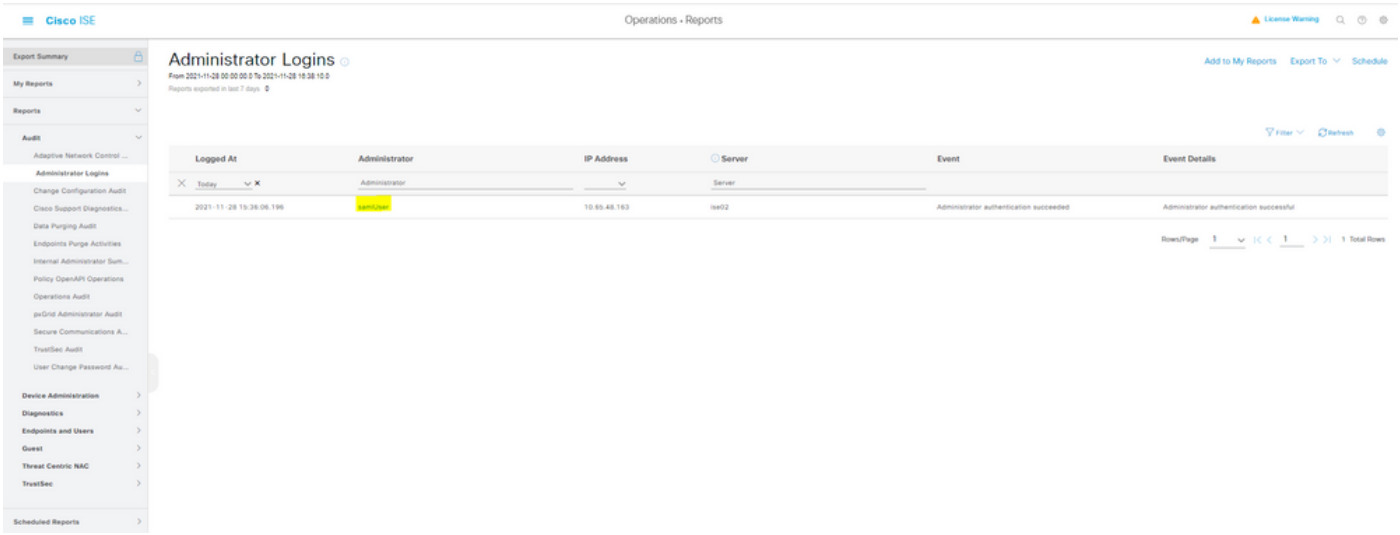
Other Attributes

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

Steps

| | |
|---|---|
| 5231 | Guest Authentication Passed |

- ISEの管理ログインログ：ユーザ名：samlUser。


Cisco ISE
Operations · Reports
License Warning
Export Summary
My Reports
Reports
Audit
Adaptive Network Control ...
Administrator Logins
Change Configuration Audit
Cisco Support Diagnostics...
Data Purging Audit
Endpoints Purge Activities
Internal Administrator Sum...
Policy OpenAPI Operations
Operations Audit
pxGrid Administrator Audit
Secure Communications A...
TrustSec Audit
User Change Password Au...
Device Administration
Diagnostics
Endpoints and Users
Guest
Threat Centric NAC
TrustSec
Scheduled Reports
Administrator Logins
From 2021-11-28 00:00:00.0 To 2021-11-28 16:38:10.0
Reports exported in last 7 days
Add to My Reports
Export To
Schedule
Filter
Refresh
Logged At
Administrator
IP Address
Server
Event
Event Details
Today
Administrator
Server
2021-11-28 15:36:06.196
samlUser
10.65.48.163
ise02
Administrator authentication succeeded
Administrator authentication successful
Rows/Page
1
1
1 Total Rows

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。