

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](#)

[トラブルシューティング](#)

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。

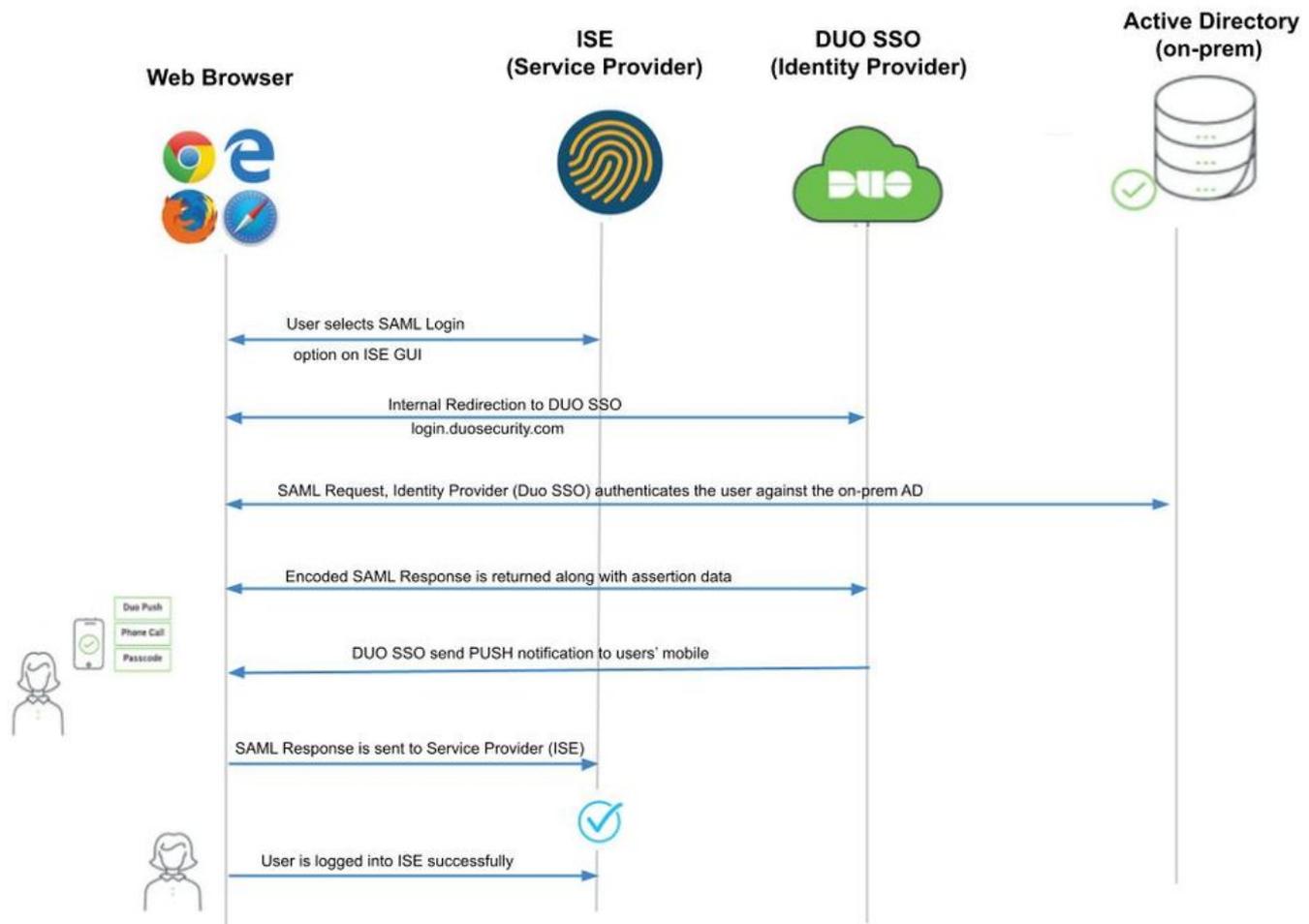
SAMLトランザクションは、IDプロバイダーとサービスプロバイダー間の標準化された通信にExtensible Markup Language(XML)を使用します。SAMLは、ユーザのIDの認証とサービスを使用するための許可の間のリンクです。

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。

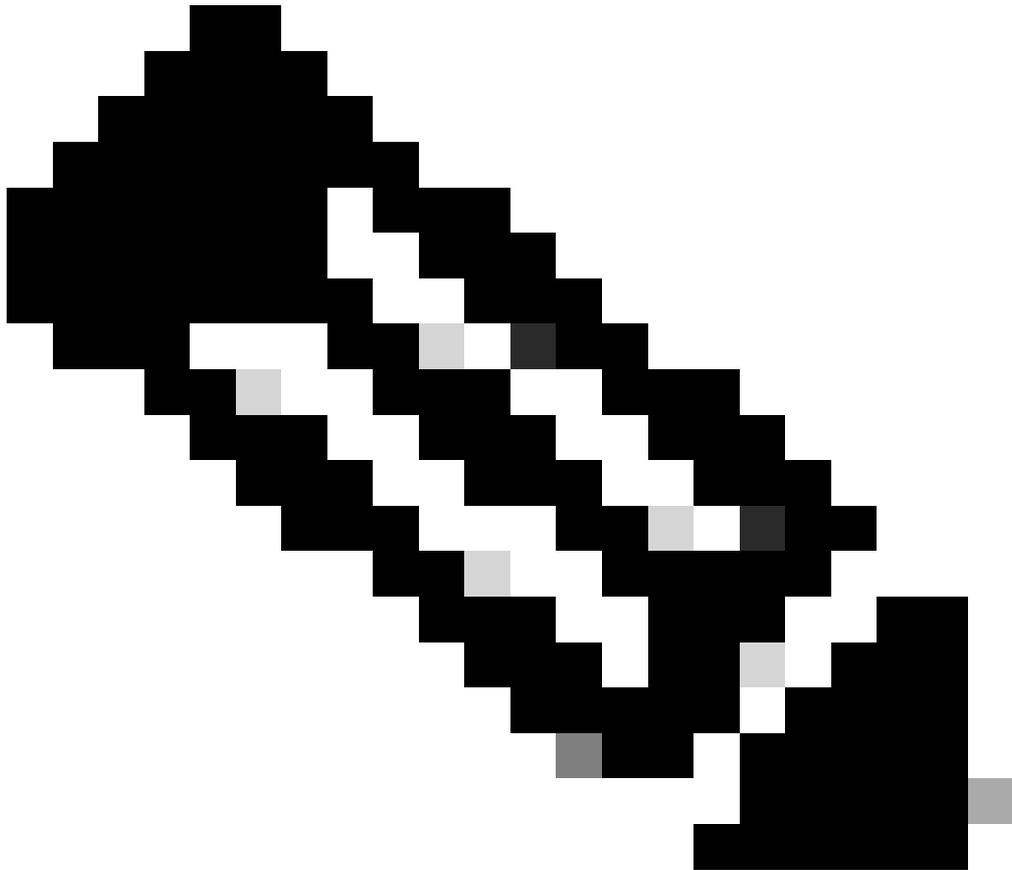
- 認証アサーションは、ユーザのIDを証明し、ユーザがログインした時間と使用した認証方法（Kerberos、二要素など）を提供します。
- アトリビューションアサーションは、SAML属性（ユーザに関する情報を提供する特定のデータ）をSPに渡します。
- 認証の決定アサーションは、ユーザがサービスを使用する権限を持っているか、パスワードの失敗またはサービスへの権限の欠如が原因でIdPが要求を拒否したかを宣言します。

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ます、ステップ3を実行できません。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。

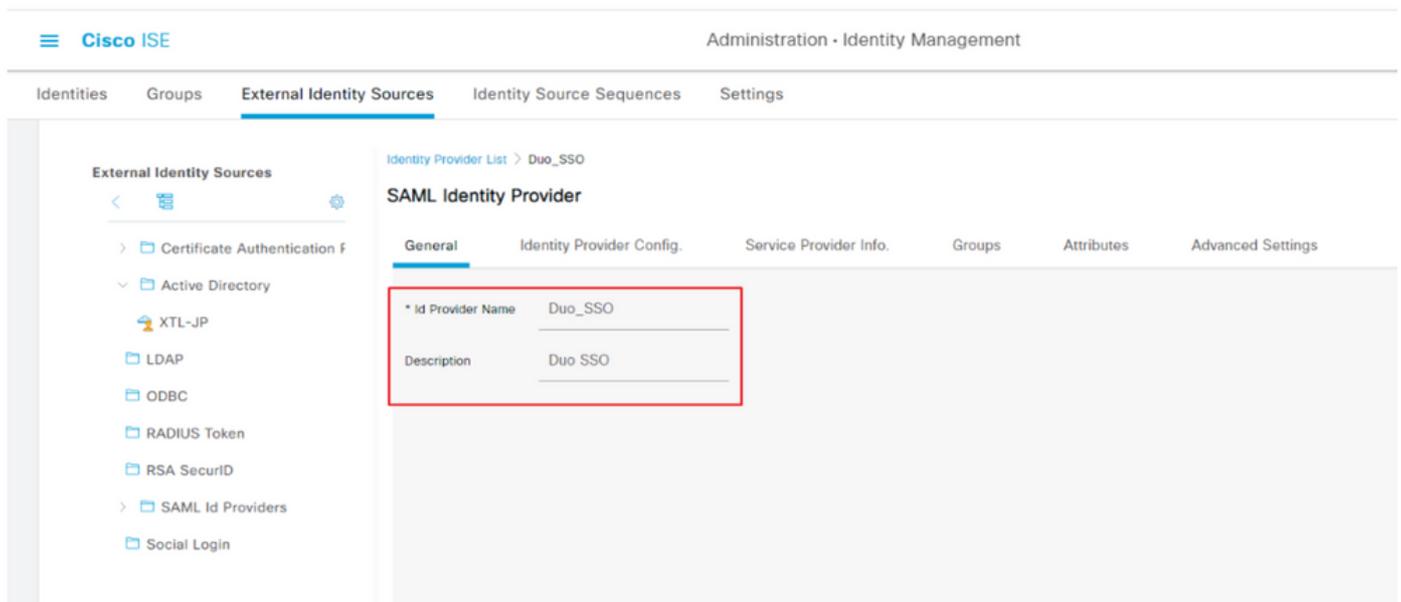
Duo SSOとのSAML SSO統合の設定

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。

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 importing a config file. 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 'Samlina Certificates' table is also visible with columns for Subject, Issuer, Valid From, Valid To, and Serial Number.

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。

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

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。

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.

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。

Administration - System

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

Create Role Based Access Control policies by configuring rules based on Admin groups, Menu Access permissions (menu items), Data Access permissions (directory 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).

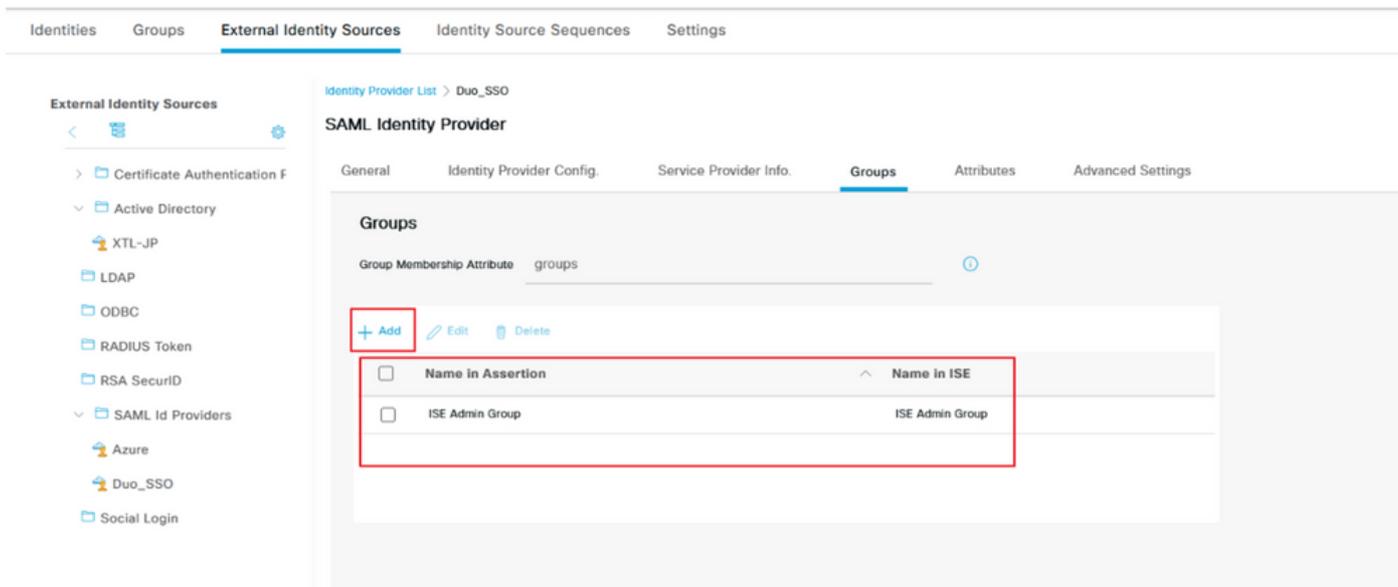
RBAC Policies

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 Trustsec Policy	ERS Trustsec	Super Admin Data Access
Helpdesk Admin Policy	Helpdesk Admin	Helpdesk Admin Menu Access
Identity Admin Policy	Identity Admin	Identity 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 ...

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。

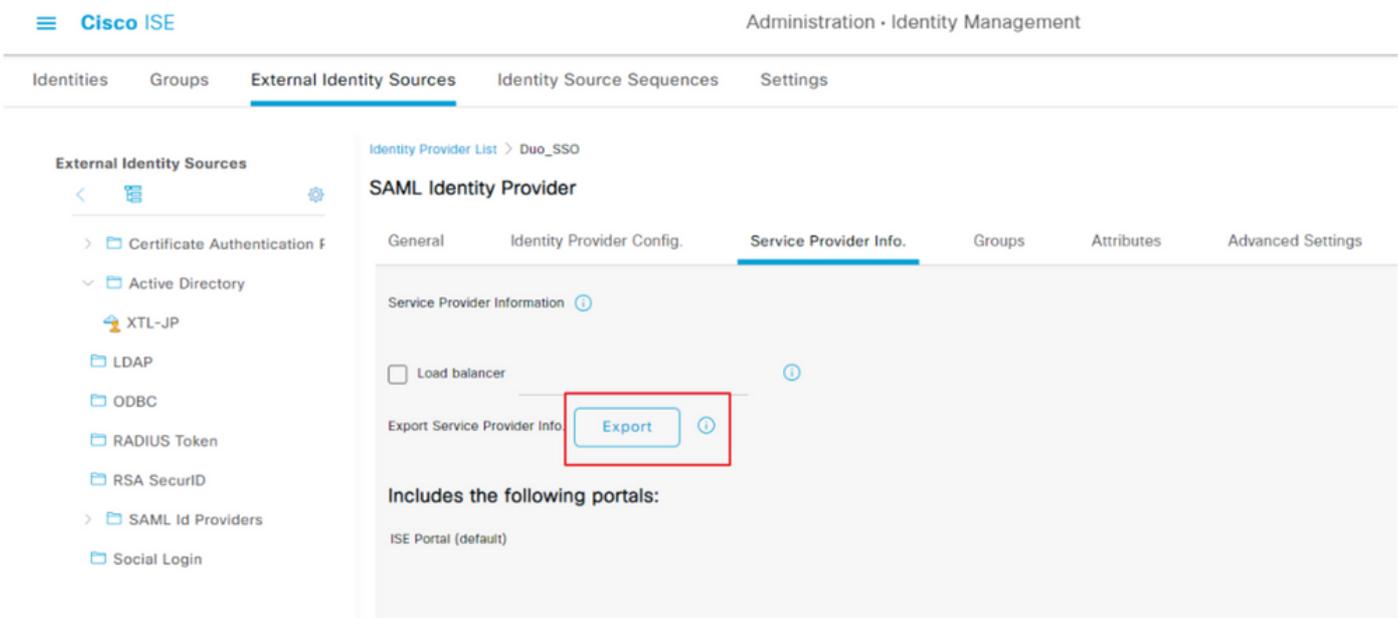
Name in Assertion (ISE管理グループの名前) を追加し、ドロップダウンから作成したロールベースアクセスコントロール (RBAC)グループを選択し (ステップ4)、Openをクリックして保存します。SSO URLと署名証明書は自動的に入力されます。



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/7fdcf239-631e-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。

Configured Authentication Sources

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

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。

Single Sign-On

i 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](#)

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/7fdcf239-631e-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

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>

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

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>.

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

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**

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。

Settings

Type Generic Service Provider - Single Sign-On

Name PWLTEST Cisco ISE - Single Sign-On

Duo Push users will see this when approving transactions.

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。

Downloads

Certificate

[Download certificate](#)

Expires: 01-19-2038

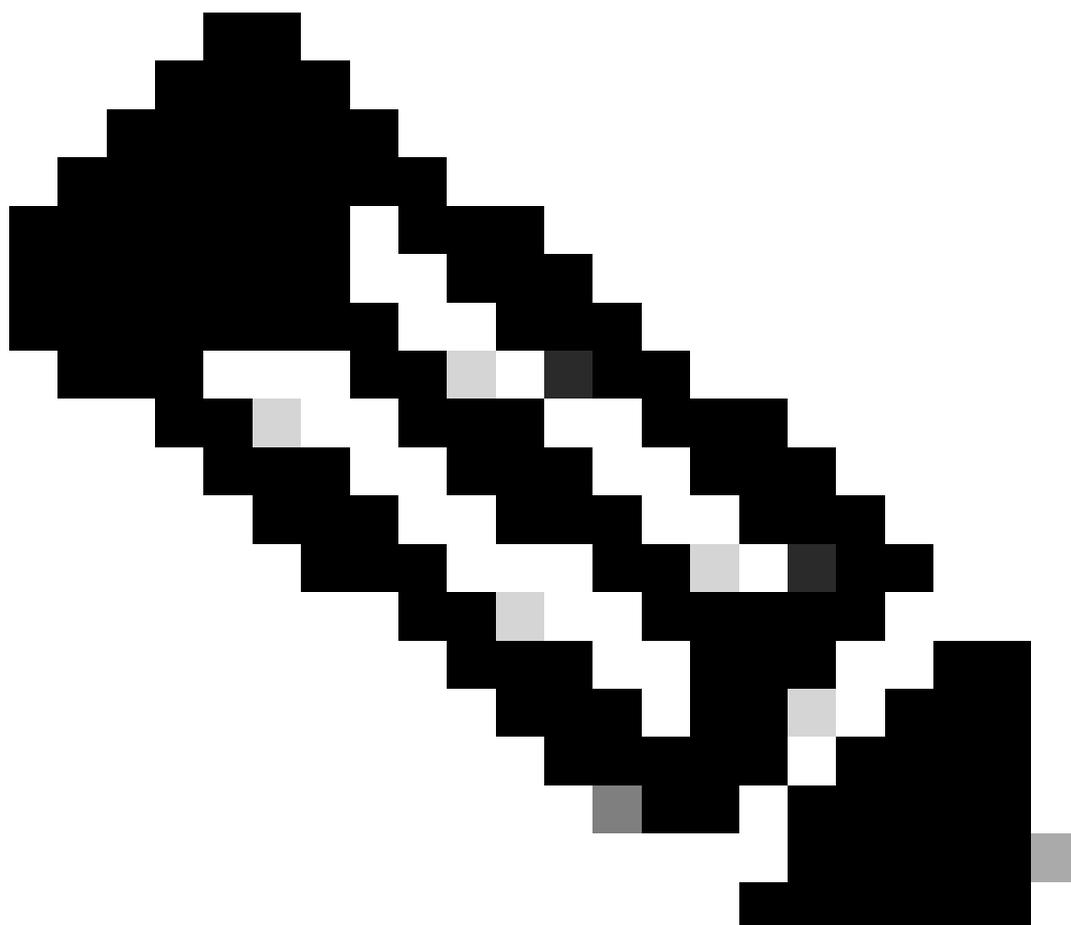
SAML Metadata

[Download XML](#)

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。

Identity Provider List > Duo_SSO

SAML Identity Provider

General **Identity Provider Config.** Service Provider Info. Groups Attributes Advanced Settings

Identity Provider Configuration

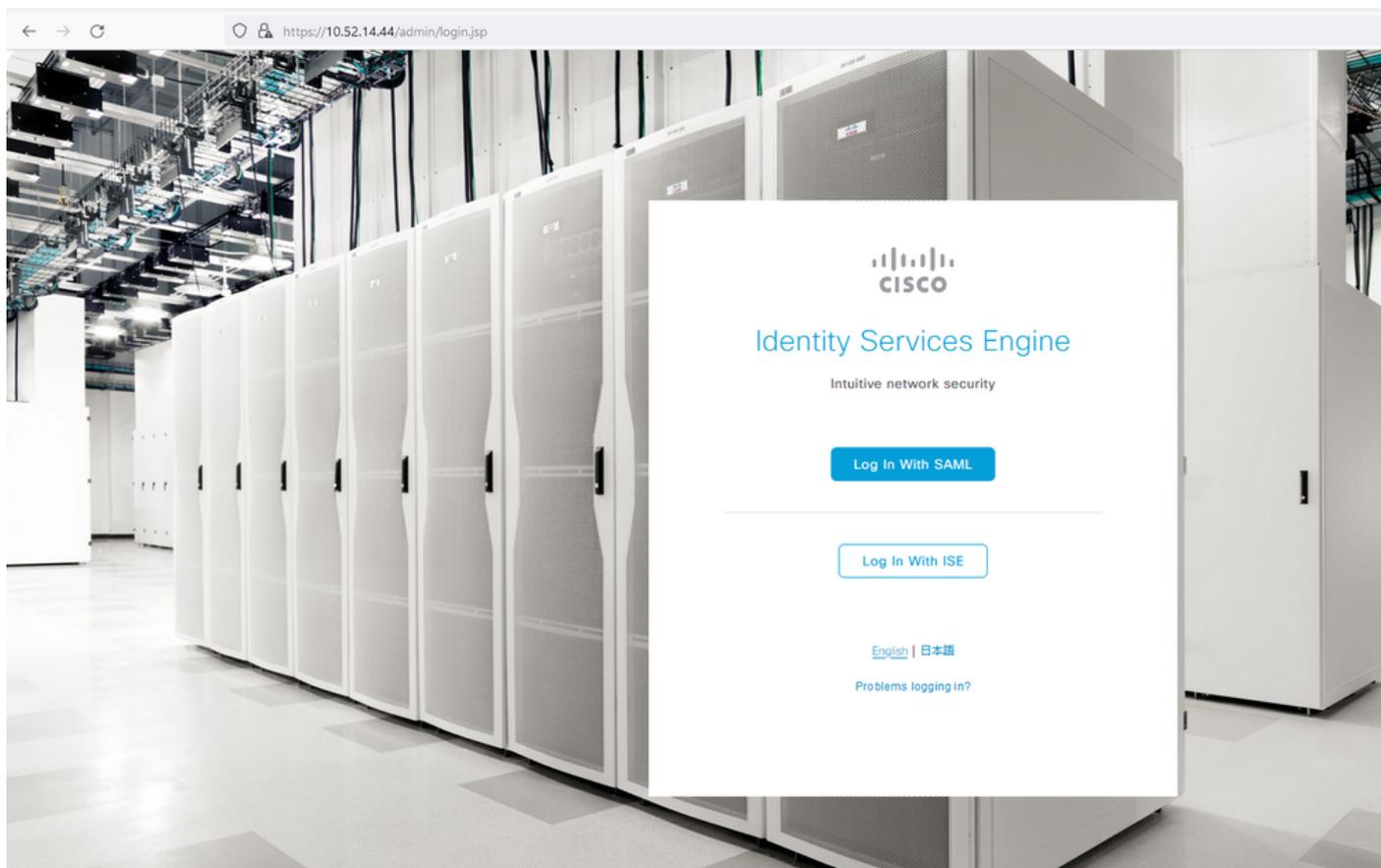
Import Identity Provider Config File ⓘ

Provider Id

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。

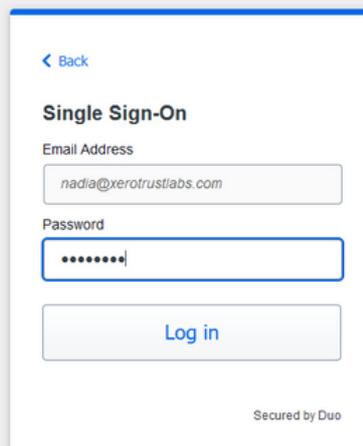


2. SSOページにリダイレクトされ、電子メールアドレスを入力して、Nextをクリックします。



The image shows a web browser window displaying a Cisco Single Sign-On page. 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. パスワードを入力し、**Log in**をクリックします。

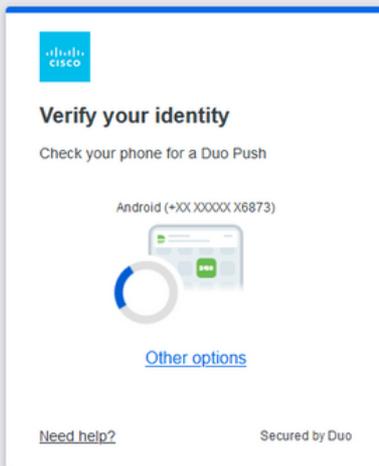


The image shows a web browser window displaying a Cisco Single Sign-On page. At the top left is a blue back arrow and the text "Back". Below it, the text "Single Sign-On" is displayed. Underneath, there is a label "Email Address" followed by a text input field containing the email address "nadia@zerotrustlabs.com".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

4. 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。

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. 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。

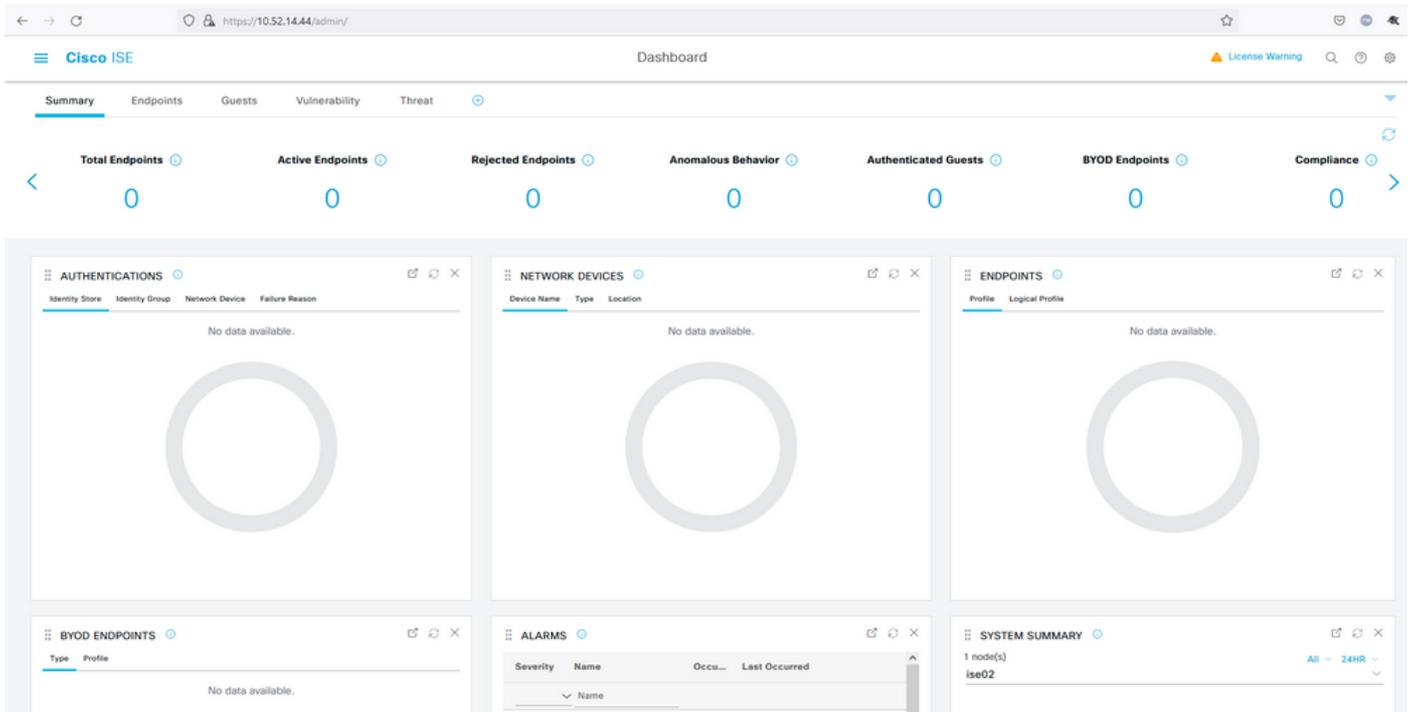


Success!

Logging you in...



Secured by Duo



トラブルシューティング

- 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口ケーションURL)、Audience(EntityID)の多数の属性が表示されます。

```

GET https://zerotrustlabs.login.duosecurity.com/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+LB1BLJMeF6GVOB1rmdX3AVEwDQYJKoZIhvcNAQELBQAwNjEVMBMGA1UECgwMRHRvIFN1Y3VyaXR5MR0wGwYDVQDD
BRESTZPODg2UkxETUJZMzExSFBJMjAeFw0yMTExMjYwMjQNTFZlFw0zODAxMTkwMzE0MDdaMDYxFTATBgNVBAoMMDER1byBTZW1cm10eTEdMBsGA1UEAwwURk2Tzg4N1JMRE
1CWTMxMuhQSTIwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDB03Ayuh9avw0NoQzIhQZzu9H8vu/HSKLSH30585Mukj5FnoVV50PGTuoFN4u90tSiFULjC8eQnUs
BR1PYQ5jt0V23qVnvoGyqsuHAs8nbKwvzPshzNF59p03pXkoGPuB+Du2IrRvv0opSv4vbrgKV+H/bvMqyhIA6ywfHNZedG7pbwrYBtVPDXUpnLQvtL2
/Vd9230XuXHF+k32hagRgTLub5XyT1HHQ8b4n3mQKHs6yA/KNvaB3b/AMUqAXDqaEXNG0uQENMK30wTs49
/w+r5fz7xp66muRc0IBg3xjWnnFnyujy7v5ifn1KFUFQu+86A5GbuUWCyiaKmV7CztAgMBAAGjEzARMA8GA1UdEwEB
/wQFMAMBAF8wDQYJKoZIhvcNAQELBQADggEBAH+KItcw0KtDxBvZ5S+25a+50F4Tqd/pHh56i19d2kDxInSUVsy
/Yy1FXAWge3WBke4b3JR7znD6000sZTYbF9w7H4svU2gxzdk0znXJNj2e4C5fDivnj/TawZakp2MbTaxfV2VTL0K0kV/1jM6PL61PbKGFwNmh+SjW/VseS+71C701eI
/U095XLbAu2iIny9zfv0hKNV72L8fgYgrjhpdxH8Y1SxPbVWZMwzytbwZFUogD30XrPq16aXZvJyOH5Vs0H90wQ8qQ48hI4F4J3DyRPNH1PzQTYM38kjymEkE0DJPcaGy9v
EMinHUkdwpiETB52Cmtwg+DzAw1jpc=</ds:X509Certificate>
</ds:X509Data>
<ds:KeyInfo>
</ds:KeyInfo>
</ds:Signature>
<saml:Subject>
<saml:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">nadia</saml:NameID>
<saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
<saml:SubjectConfirmationData NotOnOrAfter="2021-12-02T04:48:56Z"
Recipient="https://10.10.10.10:8443/portal/SSOLoginResponse.action"
InResponseTo="_7fdfc239-631e-439c-a3ab-f5e56429779d_SEMIportalSessionId_EQUALS859ee9c3-60e4-4482-9426-
b3904d4d6226_SEMItoken_EQUALS1RS257BC24SGVHWZ76GMVEZNR0YCC_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)

- ISEのライブログ：

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

- ISEの管理ログインログ：ユーザ名：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
 - pxGrid Administrator Audit
 - Secure Communications A...
 - TrustSec Audit
 - User Change Password Au...
- Device Administration
- Diagnostics
- Endpoints and Users
- Guest
- Threat Control NAC
- TrustSec
- Scheduled Reports

Administrator Logins

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

Reports reported in last 7 days

Add to My Reports Export To Schedule

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

Rows/Page 1 1 Total Rows

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。