

Configura il flusso di accesso dell'amministratore della GUI ISE ISE 3.1 tramite l'integrazione SAML SSO con Azure AD

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Provider di identità \(IdP\)](#)

[Provider di servizi \(SP\)](#)

[SAML](#)

[Asserzione SAML](#)

[Diagramma di flusso ad alto livello](#)

[Configura integrazione SAML SSO con Azure AD](#)

[Passaggio 1. Configurazione di SAML Identity Provider su ISE](#)

[1. Configurare Azure AD come origine identità SAML esterna](#)

[2. Configurazione del metodo di autenticazione ISE](#)

[3. Esporta informazioni sul fornitore di servizi](#)

[Passaggio 2. Configurare le impostazioni di Azure AD IdP](#)

[1. Creare un utente di Azure AD](#)

[2. Creare un gruppo di Azure AD](#)

[3. Assegna utente di Azure AD al gruppo](#)

[4. Creare un'applicazione Azure AD Enterprise](#)

[5. Aggiungi gruppo all'applicazione](#)

[6. Configurare un'applicazione Azure AD Enterprise](#)

[7. Configurare l'attributo di gruppo di Active Directory](#)

[8. Scarica il file XML dei metadati federativi di Azure](#)

[Passaggio 3. Carica metadati da Azure Active Directory a ISE](#)

[Passaggio 4. Configurazione dei gruppi SAML su ISE](#)

[\(Facoltativo\) Passaggio 5. Configura criteri RBAC](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Problemi comuni](#)

[Risoluzione dei problemi di ISE](#)

[Registri con nome account di accesso SAML e nomi attestazione basata su gruppo non corrispondenti](#)

Introduzione

In questo documento viene descritto come configurare l'integrazione SAML SSO di Cisco ISE 3.1 con un provider di identità esterno, ad esempio Azure Active Directory (AD).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

1. Cisco ISE 3.1
2. Distribuzioni SAML SSO
3. Azure AD

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

1. Cisco ISE 3.1
2. Azure AD

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Provider di identità (IdP)

In questo caso, è l'autorità di Azure AD che verifica e dichiara l'identità utente e i privilegi di accesso a una risorsa richiesta ("Provider di servizi").

Provider di servizi (SP)

La risorsa o il servizio ospitato a cui l'utente intende accedere, in questo caso ISE Application Server.

SAML

SAML (Security Assertion Markup Language) è uno standard aperto che consente a IdP di passare le credenziali di autorizzazione all'SP.

Le transazioni SAML utilizzano il linguaggio XML (Extensible Markup Language) per le comunicazioni standardizzate tra provider di identità e provider di servizi.

SAML è il collegamento tra l'autenticazione di un'identità utente e l'autorizzazione per utilizzare un servizio.

Asserzione SAML

Un'asserzione SAML è il documento XML che il provider di identità invia al provider di servizi che contiene l'autorizzazione utente.

Esistono tre tipi diversi di asserzioni SAML: autenticazione, attributo e decisione di autorizzazione.

- Le asserzioni di autenticazione provano l'identificazione dell'utente e forniscono l'ora di accesso dell'utente e il metodo di autenticazione utilizzato (Kerberos, a due fattori, come esempio)
- L'asserzione di attribuzione passa gli attributi SAML, parti specifiche di dati che forniscono informazioni sull'utente, al provider di servizi.
- Un'asserzione di decisione di autorizzazione dichiara se l'utente è autorizzato a utilizzare il servizio o se il provider di identità ha negato la richiesta a causa di un errore di password o di diritti insufficienti

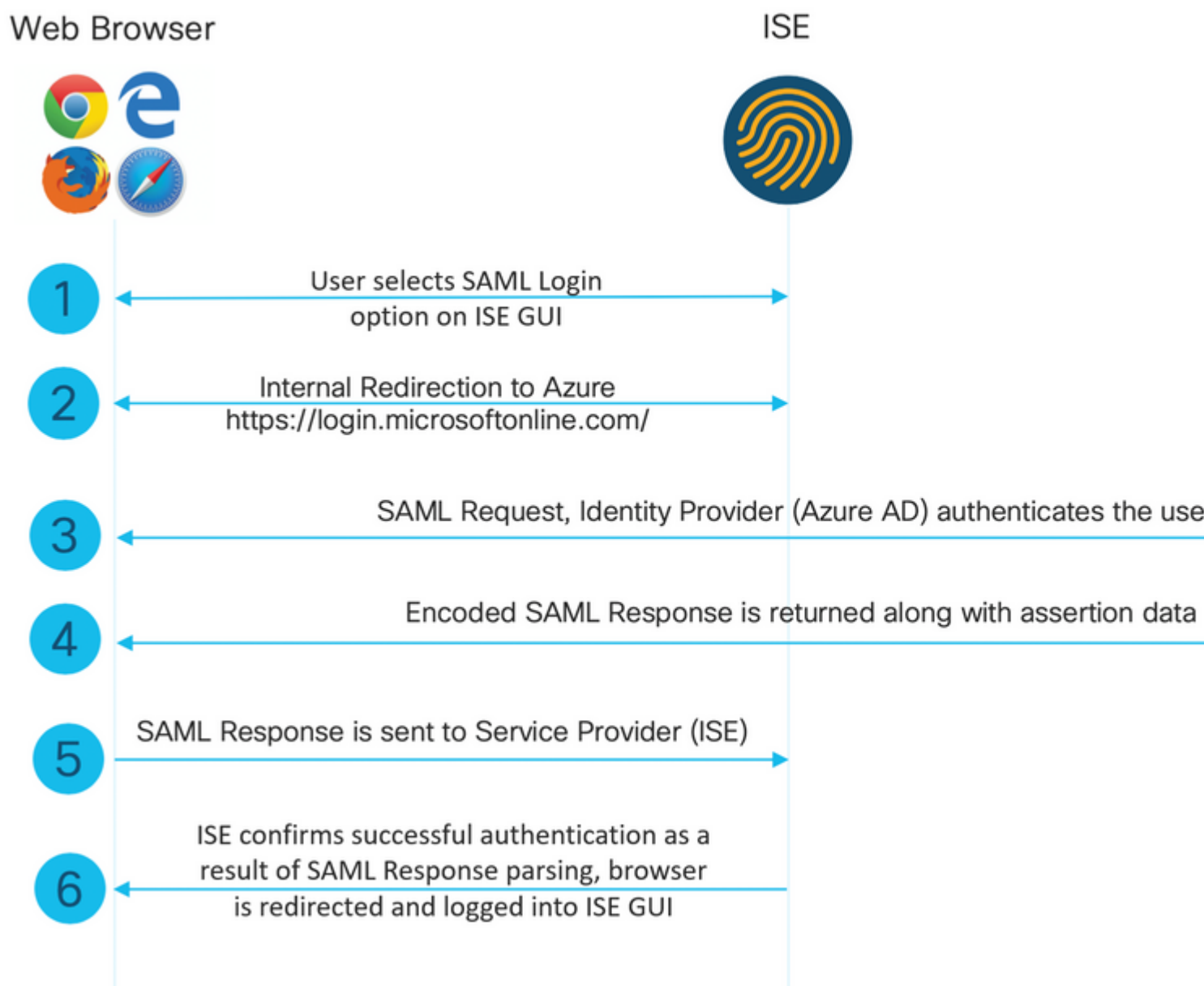
per il servizio.

Diagramma di flusso ad alto livello

SAML funziona passando informazioni su utenti, accessi e attributi tra il provider di identità, Azure AD e il provider di servizi ISE.

Ogni utente accede una volta a un Single Sign-On (SSO) con il provider di identità, quindi il provider di Azure AD passa gli attributi SAML a ISE quando l'utente tenta di accedere a tali servizi.

ISE richiede l'autorizzazione e l'autenticazione da Azure AD, come mostrato nell'immagine.



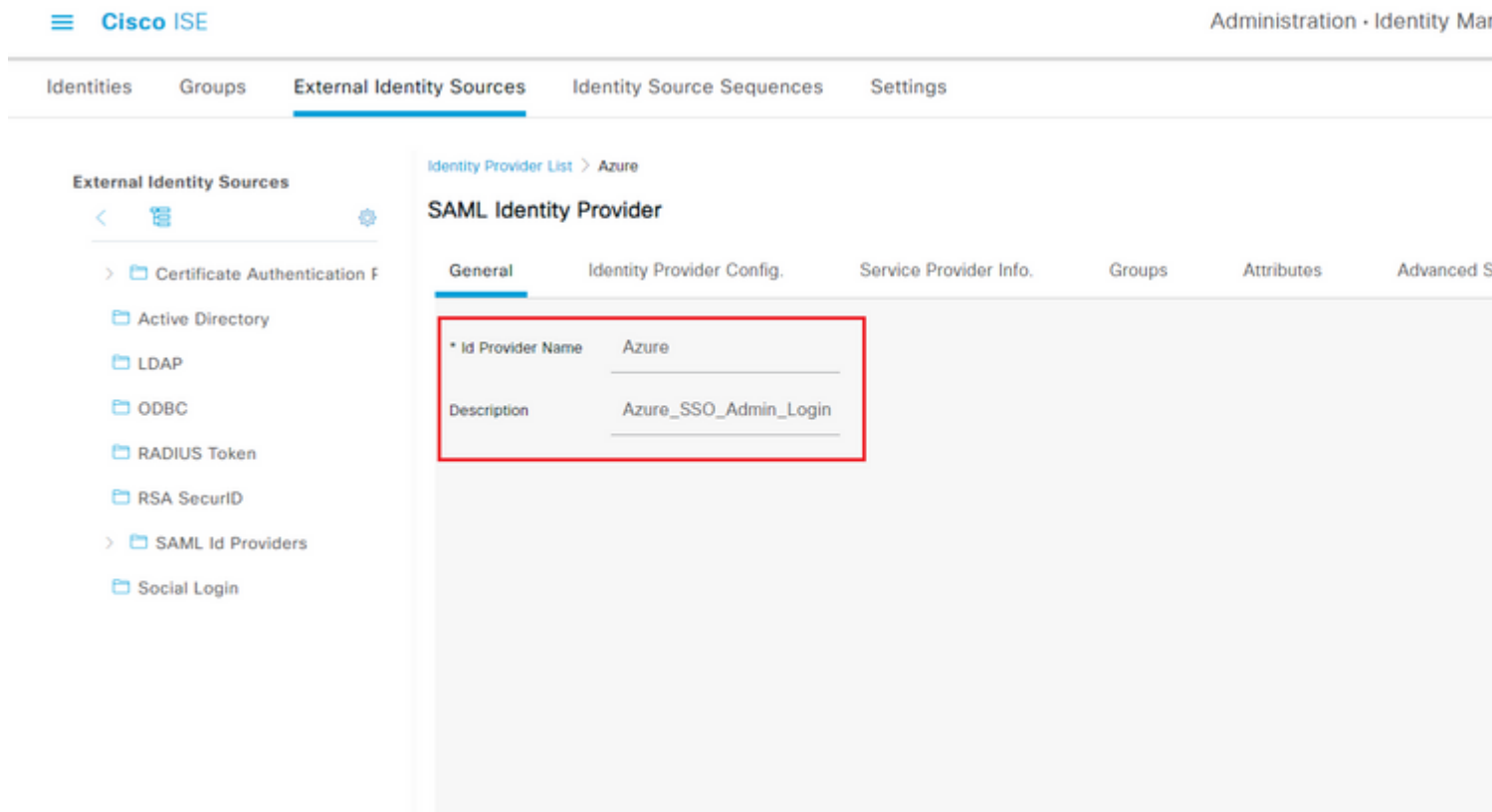
Configura integrazione SAML SSO con Azure AD

Passaggio 1. Configurazione di SAML Identity Provider su ISE

1. Configurare Azure AD come origine identità SAML esterna

In ISE, selezionare **Amministrazione > Gestione delle identità > Origini identità esterne > Provider di ID SAML** e fare clic sul pulsante **Aggiungi**.

Immettere il **nome del provider di ID** e fare clic su **Submit** (Invia) per salvarlo. Il **nome del provider di identità** è significativo solo per ISE, come mostrato nell'immagine.



2. Configurazione del metodo di autenticazione ISE

Passare a **Amministrazione > Sistema > Accesso amministratore > Autenticazione > Metodo di autenticazione** e selezionare il pulsante di opzione **Basato su password**.

Selezionare il nome del provider di ID richiesto creato in precedenza dall'elenco a discesa **Origine identità**, come mostrato nell'immagine.

- Authentication
- Authorization >
- Administrators >
- Settings >

Authentication Type ⓘ

Password Based

Client Certificate Based

* Identity Source

SAML:Azure



3. Esporta informazioni sul fornitore di servizi

Passare a **Amministrazione** > **Gestione delle identità** > **Origini identità esterne** > **Provider di ID SAML** > **[Provider SAML utente]**.

Passare alla scheda **Informazioni provider di servizi**. e fare clic sul pulsante **Esporta**, come mostrato nell'immagine.

SAML Identity Provider

General

Identity Provider Config.

Service Provider Info.

Groups

Attribute

Service Provider Information

 Load balancer (i)Export Service Provider Info. (i)[Export](#)

Includes the following portals:

Sponsor Portal (default)

Scaricare il file **.xml** e salvarlo. Prendere nota del valore **Location URL** e **entityID**.

```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntityDescriptor entityID="http://CiscoISE/0049a2fd-7047-4d1d-8907-5a05a94ff5fd" xmlns:md="urn:oasis:names:tc:SAML:2.0:protocol" WantAssertionsSigned="true" xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<md:SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol" WantAssertionsSigned="true" xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<md:KeyDescriptor use="signing">
<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:X509Data>
<ds:X509Certificate>
MIIFTjCCAzagAwIBAgINAg2amS1L6NAE8FY+tzANBgkqhkiG9w0BAQwFADA1MSMwIQYDVQQDExpT
QU1MX21zZTMtMS0xOjU5a3VtYXN1bWVtAEFw0yMTA3MTkwMzI4MDEBaFw0yMTA3MTkwMzI4MDEBa
MCUxIzAhBgNVBAMTG1NBTUxfaXN1My0xLW50aWw0LW50aWw0LW50aWw0LW50aWw0LW50aWw0LW50aWw0
AAOCAG8AMIICCGKCAgEAvila4+S0uP3j037yCOXnHAzADupfqcwcp1JQnFxfhVfnDd0ixGRt8iaQ
1zdKhpwF/BsJeSznXyaPVxFcmMFHbmyt46gQ/jjQEyt7YhyohG0t1op01qDGwtOnWZGQ+ccvqXSL
Ge1HYd1DtE1LMEcGg1mCd56GfrDcJdX0cZJmiDzizyJGKdDPf+1VM5JHCo6UNLFIIfyPmGvcCXnt
NVqsYvxSzf038ciQq1m0sqvrrYzuIUAXDWUNUg9pSGzH0fKsSsZRPxrQh+3N5DEFF1Mzybvm1FYu
9h83g4L4WJWmizETO6Vs/D0p6BSf2MPxKe790R5TfxFqJD9DnYgCnHmGooVmnSSnDsAgWebvF1uhZ
nGGkH5R0gT7v3CDrdFtRoNYAT+Yv0941KzFCSE0ssshykGSjgVn31XQ5vgDH1PvqNaYs/PWiCvmI/
wYKSTn9/hn7JM1DqOR1PGEkVjg5WbxcViejMrrIzNrIciFNz1FuggaE8tC7uyyQZa2rcmTrXGWC1
sDU4u0vFpFvrcC/lavr9Fnx7LPwXa0asvJd19SPbD+qYgshz9AI/nIXaZdioHzEQwa8pkoNRBwjZ
ef+WFC9dWiy+ctbBT0+EM06Xj1aTI1bV80mN/6LhiS8g7KpFz4RN+ag1iu6pgZ5058Zot9gqkpFw
kVS9vT4E0zwNGo7pQI8CAwEAAAN9MHswIAyDVR0RBbkwF4IVaXN1My0xLW50aWw0LW50aWw0LW50aWw0
MAwGA1UdEWFQFMBBAF8wCwYDVR0PBAQDAgLSMB0GA1UdDgQWBBIkY2z/9H9PpwSnOPGARCj5iaZ
oDAdBgNVHSUEFjAUBgggrBgEFBQcDAQYIKwYBBQUHAWIwDQYJKoZIhvcNAQEMBQADggIBAIE6mnBL
206Dkb6fHdgKd9goN8N2bj+34ybwXqvDSwGtn4NA6Hy1q7N6iJzAD/7soZfHgOT2UTgZpRF9FsHn
CGchSHqDt3bQ7g+GwlvccgreC7R46qenaonXVr1tRw11vVidcf8JQFFMxya/rIC4mxVeoo0j1F19d
rvDBH+XVEt67DnQWkuLp8zPJUuqfa4H0vdm6of3uBte0/pdUtEi6f0bqr0wCyd9Tj7KXfd2ITW
hMxaFsv8wWcVuOMDPkP9xUwwt6gFH0bE5luT4EYVuuHwMNGbZqqqb+a4uSkX/EfiDVoLSL6KI31
nf/341cuRTJUmdh9g2mppbBw0cxzoUxDm+HReSe+0JhRCyIJC0vUpdNmYC8cfAZuiV/e3wk0BLZM
lgV8FTVQSNra9LwHP/PgeNAPUCRPXSwake4rvjvMc0aS/iYdwZhziJ8zBdIBanMv5mGu1nvTET9K
EEwj9ys1IHmdqoH3Em0F0gnzR0RvsMPbJxAoTFjfoITTMdQXNHhg+w1P0KXS2GCZ29vAM52d8ZCq
UrzOVxNHKWKWER/q1GgaWvh3X/G+z1shUQDrJcBdLcZI1WKUMa6XVDj18byhBM7pFGwg4z9YJZGF
```

```
/ncHcoxFY759LA+m7Brp7FFPiGCrPW8E0v7bUMSDmmg/53NoktfJ1CckaWE87myhimj0
</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
</md:KeyDescriptor>
<md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</md:NameIDFormat>
<md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</md:NameIDFormat>
<md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:persistent</md:NameIDFormat>
<md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</md:NameIDFormat>
<md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:WindowsDomainQualifiedName</md:NameIDFormat>
<md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:kerberos</md:NameIDFormat>
<md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName</md:NameIDFormat>
<md:AssertionConsumerService index="0" Location="https://10.201.232.19:8443/portal/SSOLoginResponse.action" />
<md:AssertionConsumerService index="1" Location="https://ise3-1-19.onmicrosoft.com:8443/portal/SSOLoginResponse.action" />

</md:SPSSODescriptor>
</md:EntityDescriptor>
```

Attributi di interesse dal file XML:

entityID="<http://CiscoISE/100d02da-9457-41e8-87d7-0965b0714db2>"

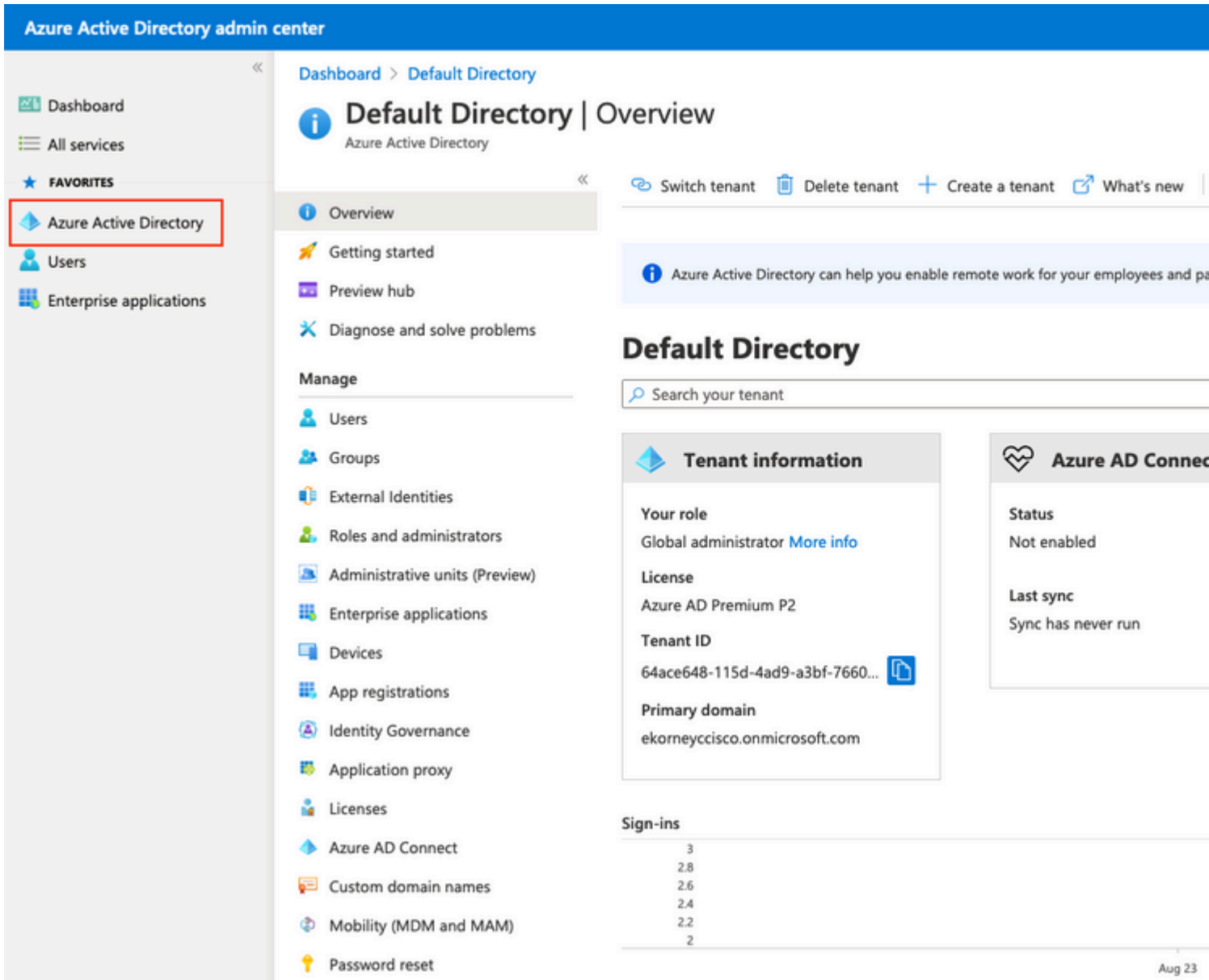
AssertionConsumerService Location="<https://10.201.232.19:8443/portal/SSOLoginResponse.action>"

AssertionConsumerService Location="<https://ise3-1-19.onmicrosoft.com:8443/portal/SSOLoginResponse.action>"

Passaggio 2. Configurare le impostazioni di Azure AD IdP

1. Creare un utente di Azure AD

Accedere al dashboard dell'interfaccia di amministrazione di Azure Active Directory e selezionare **Active Directory** come mostrato nell'immagine.



Selezionare **Users** (Utenti), fare clic su **New User** (Nuovo utente), configurare **User name (Nome utente)**, **Name (Nome)** e **Initial Password (Password iniziale)** in base alle esigenze. Fare clic su **Create** (Crea) come mostrato nell'immagine.

Identity

User name * ⓘ

mck ✓

@ gdplab2021.onmicrosoft... ▾



The domain name I need isn't shown here

Name * ⓘ

mck ✓

First name

Last name

Password

Auto-generate password

Let me create the password

Initial password

.....

Show Password

Create

2. Creare un gruppo di Azure AD

Selezionare **Gruppi**. Fare clic su **Nuovo gruppo**.

[Dashboard](#) > [Default Directory](#) > [Groups](#)



Groups | All groups

Default Directory - Azure Active Directory



+ New group



Download groups



Delete



All groups



Deleted groups



Diagnose and solve problems



This page includes previews available for your evaluation



Search groups

Mantieni tipo di gruppo come **protezione**. Configurare il **nome del gruppo** come mostrato nell'immagine.

Dashboard
All services
FAVORITES
Azure Active Directory
Users
Enterprise applications

Dashboard > TAC > Groups >

New Group

Group type * ⓘ

Security

Group name * ⓘ

ISE Admin Group

Group description ⓘ

Enter a description for the group

Azure AD roles can be assigned to the group ⓘ

Yes

No

Membership type * ⓘ

Assigned

Owners

No owners selected

Members

No members selected

3. Assegna utente di Azure AD al gruppo

Fare clic su **Nessun membro selezionato**. Scegliere l'utente e fare clic su **Seleziona**. Per creare il gruppo con un utente assegnato, fare clic su **Crea**.

Add members



Search ⓘ



mck
mck@gdplab2021.onmicrosoft.com

Selected items

No items selected

Prendere nota dell'**ID oggetto gruppo**. In questa schermata, è **576c60ec-c0b6-4044-a8ec-d395b1475d6e** per il **gruppo di amministrazione ISE**, come mostrato nell'immagine.

Dashboard >

Groups | All groups

TAC - Azure Active Directory

- All groups
- Deleted groups
- Diagnose and solve problems

Settings

- General
- Expiration
- Naming policy

+ New group | Download groups | Delete | Refresh | Columns | Previews

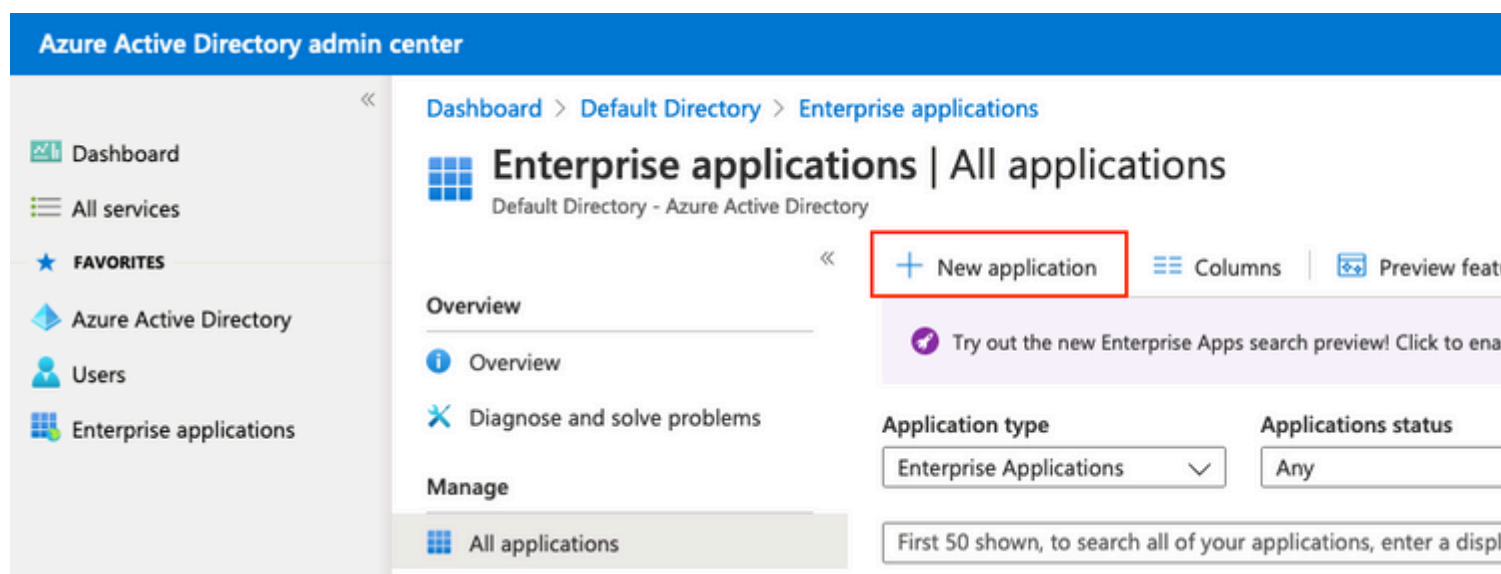
This page includes previews available for your evaluation. View previews →

Search groups | Add filters

	Name	Object Id	Group Type
<input type="checkbox"/>	ISE Admin Group	576c60ec-c0b6-4044-a8ec-d395b1475d6e	Security

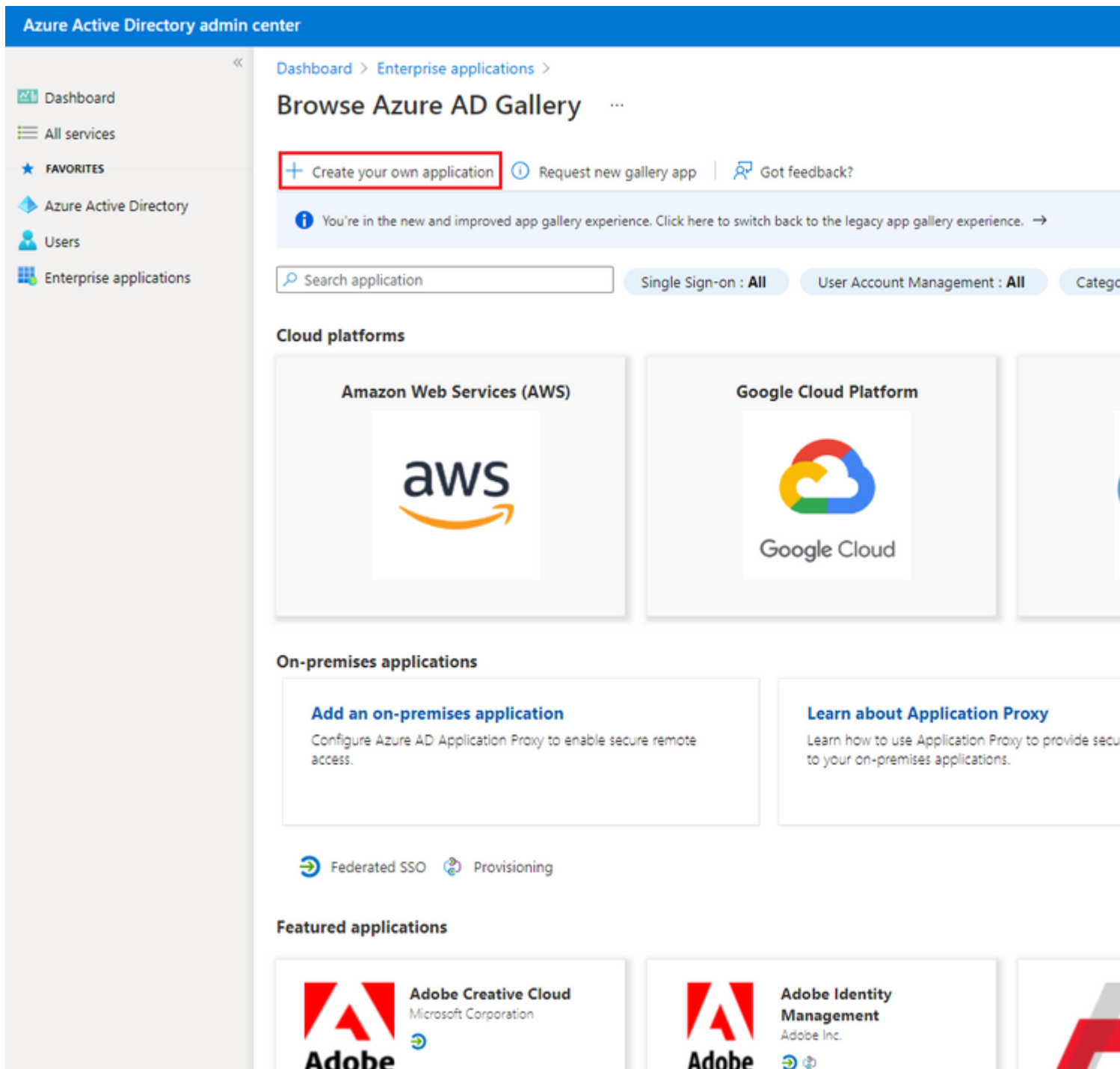
4. Creare un'applicazione Azure AD Enterprise

In AD selezionare **Applicazioni enterprise** e fare clic su **Nuova applicazione**.



The screenshot displays the Azure Active Directory admin center interface. The top navigation bar is blue and contains the text "Azure Active Directory admin center". Below this, the breadcrumb path is "Dashboard > Default Directory > Enterprise applications". The main heading is "Enterprise applications | All applications" with the subtitle "Default Directory - Azure Active Directory". On the left side, there is a navigation pane with "Enterprise applications" selected. In the main content area, the "Overview" section is active, and the "+ New application" button is highlighted with a red rectangular box. Other visible elements include a "Columns" menu, a "Preview feature" button, a notification banner about the new search preview, and filter dropdowns for "Application type" (set to "Enterprise Applications") and "Applications status" (set to "Any").

Selezionare **Crea applicazione personalizzata**.



Immettere il nome dell'applicazione e selezionare il pulsante di opzione **Integra qualsiasi altra applicazione che non si trova nella raccolta (non raccolta)** e fare clic sul pulsante **Crea** come mostrato nell'immagine.

Create your own application



What's the name of your app?

What are you looking to do with your application?

- Configure Application Proxy for secure remote access to an on-premises application
- Register an application to integrate with Azure AD (App you're developing)
- Integrate any other application you don't find in the gallery (Non-gallery)

Create

5. Aggiungi gruppo all'applicazione

Selezionare **Assegna utenti e gruppi**.

Azure Active Directory admin center

Dashboard > Enterprise applications > ISE_3_1_Admin_SSO | Overview

ISE_3_1_Admin_SSO | Overview
Enterprise Application

Overview

Deployment Plan

Manage

- Properties
- Owners
- Roles and administrators (Preview)
- Users and groups
- Single sign-on
- Provisioning
- Application proxy
- Self-service

Security

- Conditional Access

Properties

Name ⓘ
ISE_3_1_Admin_SSO

Application ID ⓘ
76b82bcb-a918-4016-aad7-...

Object ID ⓘ
22aedf32-82c7-47f2-ab34-1...

Getting Started

1. Assign users and groups
Provide specific users and groups access to the applications
[Assign users and groups](#)

Fare clic su **Aggiungi utente/gruppo**.

Azure Active Directory admin center

Dashboard > Enterprise applications > ISE_3_1_Admin_SSO

ISE_3_1_Admin_SSO | Users and groups

Overview

Deployment Plan

Manage

Properties

+ Add user/group | Edit | Remove | Update Credentials | Columns | Got feedback?

The application will appear for assigned users within My Apps. Set 'visible to users?' to no in properties to prevent this. →

First 200 shown, to search all users & groups, enter a display name.

Display Name	Object Type
--------------	-------------

Fare clic su **Utenti e gruppi**.

Add Assignment

Default Directory

Users and groups

None Selected

Select a role

User

Scegliere il gruppo configurato in precedenza e fare clic su **Seleziona**.

Nota: Selezionare il giusto gruppo di utenti o gruppi che ottengono l'accesso come previsto, come gli utenti e i gruppi menzionati qui ottengono l'accesso all'ISE una volta completata la configurazione.

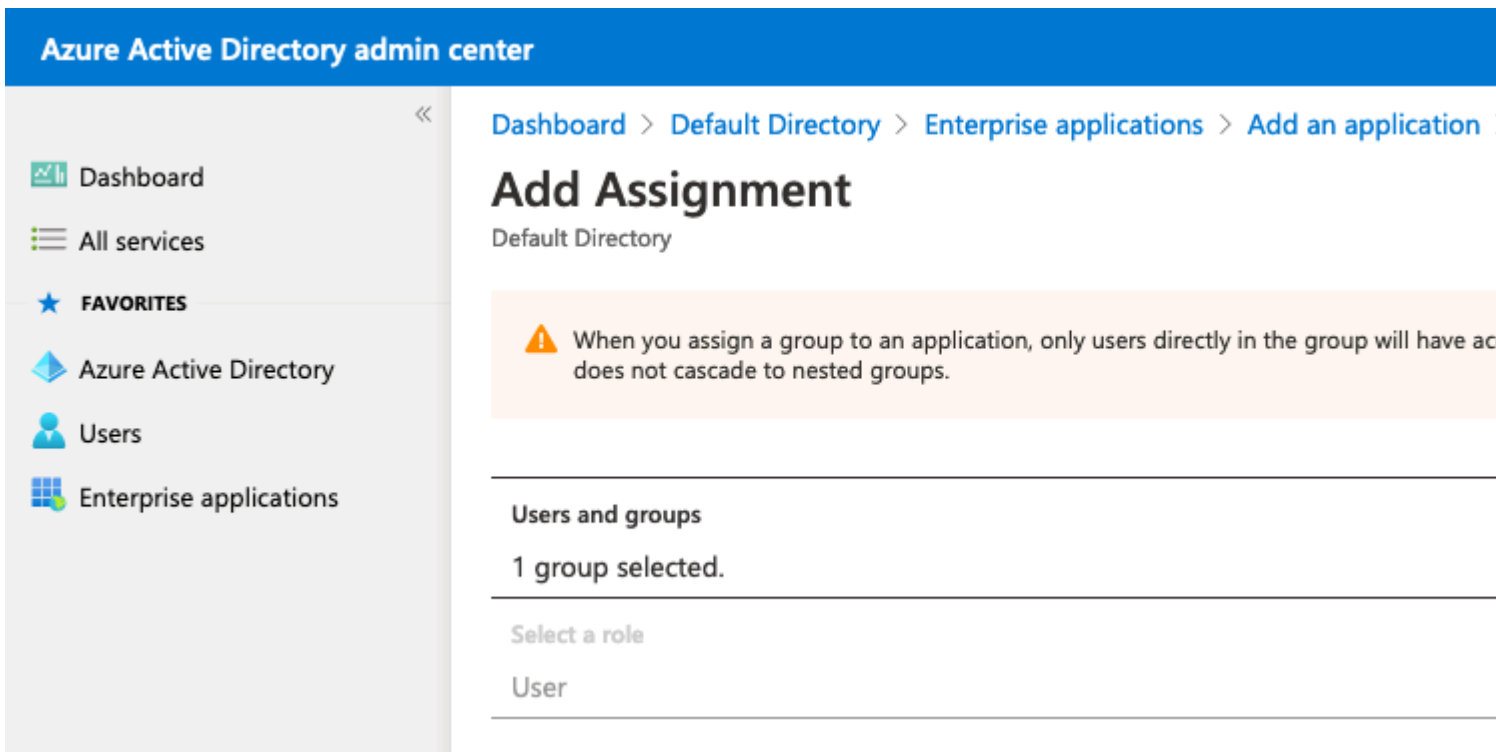
Users and groups

Search

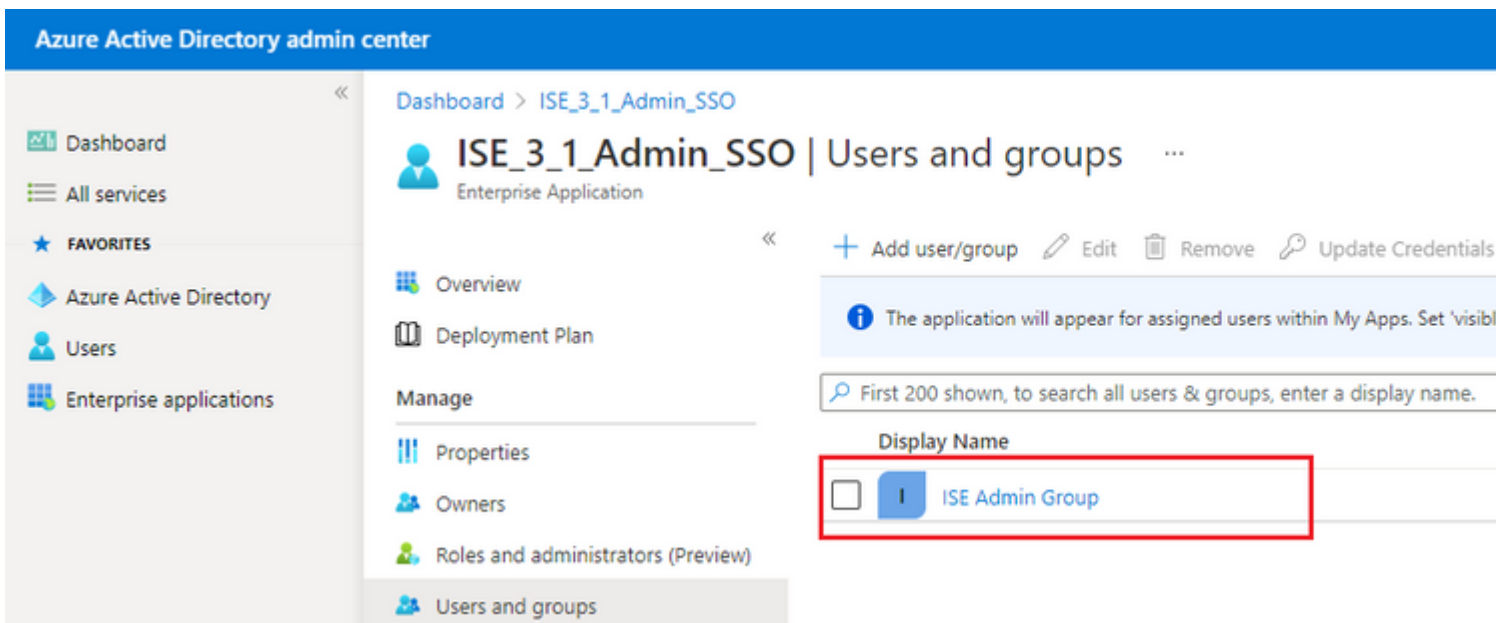
I ISE Admin Group

MC mck
mck@gdplab2021.onmicrosoft.com

Dopo aver selezionato il gruppo, fare clic su **Assegna**.



Di conseguenza, il menu **Utenti e gruppi** per l'applicazione configurata viene popolato con il gruppo selezionato.



6. Configurare un'applicazione Azure AD Enterprise

Tornare all'applicazione e fare clic su **Configura accesso Single Sign-On**.

Dashboard > Enterprise applications >

ISE_3_1_Admin_SSO | Overview

Enterprise Application

- Overview
- Deployment Plan

Manage

- Properties
- Owners
- Roles and administrators (Preview)
- Users and groups
- Single sign-on
- Provisioning
- Application proxy
- Self-service

Security

- Conditional Access

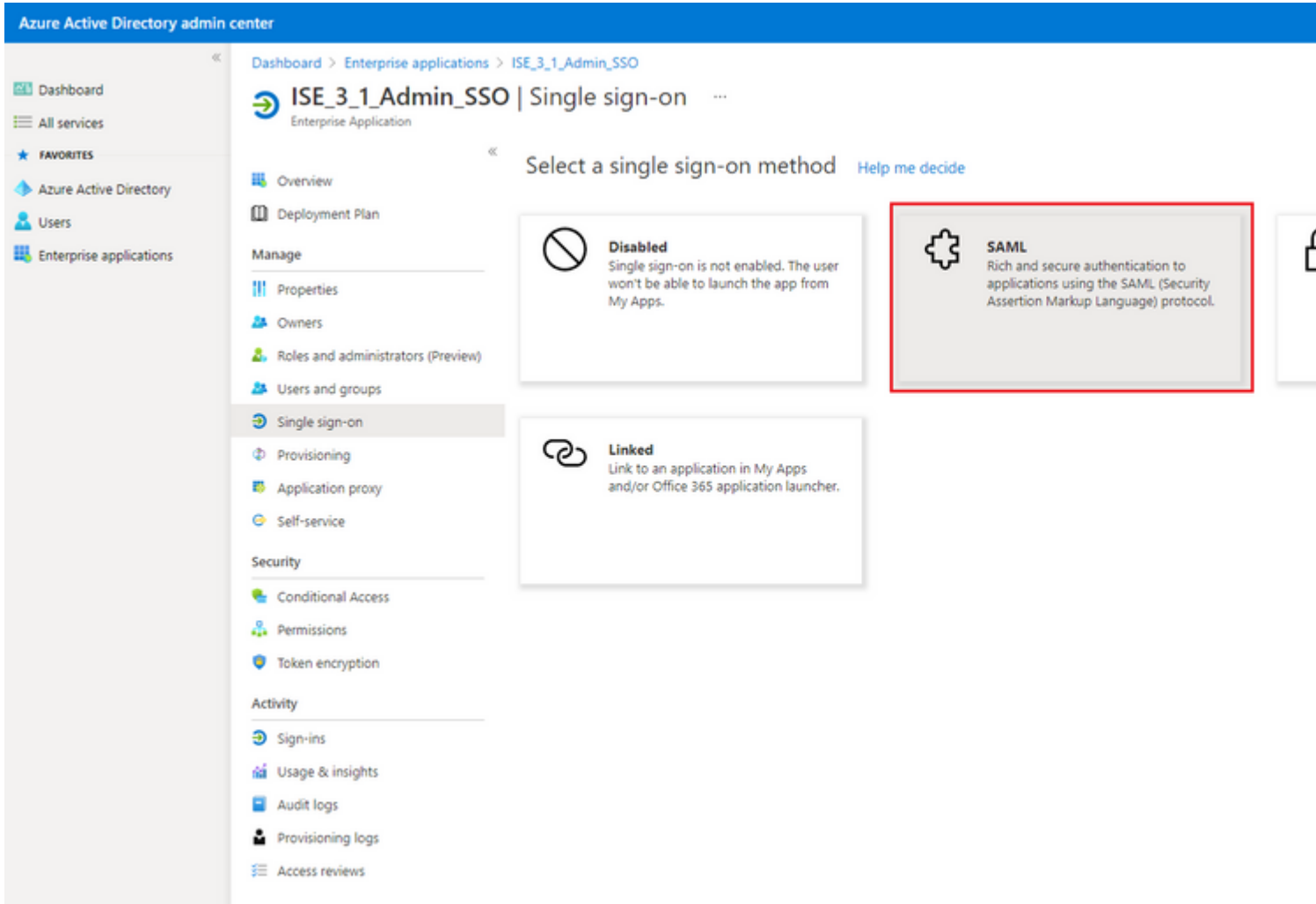
Properties

Name ⓘ	ISE_3_1_Admin_SSO
Application ID ⓘ	76b82bcb-a918-4016-aad7-...
Object ID ⓘ	22aedf32-82c7-47f2-ab34-1...

Getting Started

- 1. Assign users and groups**
Provide specific users and groups access to the applications
[Assign users and groups](#)


Selezionare **SAML** nella schermata successiva.




Fare clic su **Modifica** accanto a **Configurazione SAML di base**.

Set up Single Sign-On with SAML

Read the [configuration guide](#) for help integrating ISE30.

1 Basic SAML Configuration  Edit

Identifier (Entity ID)	Required
Reply URL (Assertion Consumer Service URL)	Required
Sign on URL	<i>Optional</i>
Relay State	<i>Optional</i>
Logout Url	<i>Optional</i>

2 User Attributes & Claims  Edit

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

Inserire l'identificatore (ID entità) con il valore di **entityID** dal file XML da step **Export Service Provider Information**. Popolare l'URL di risposta (URL servizio consumer di asserzione) con il valore di

Percorsi da AssertionConsumerService. Fare clic su **Salva**.

Nota: L'URL di risposta funge da elenco di passaggi e consente a determinati URL di fungere da origine quando vengono reindirizzati alla pagina del provider di identità.

Basic SAML Configuration



 Save

Identifier (Entity ID) *

The default identifier will be the audience of the SAML response for IDP-initiated SSO

Default


 

Reply URL (Assertion Consumer Service URL) *

The default reply URL will be the destination in the SAML response for IDP-initiated SSO

Default

Sign on URL

Relay State

Logout Url

7. Configurare l'attributo di gruppo di Active Directory

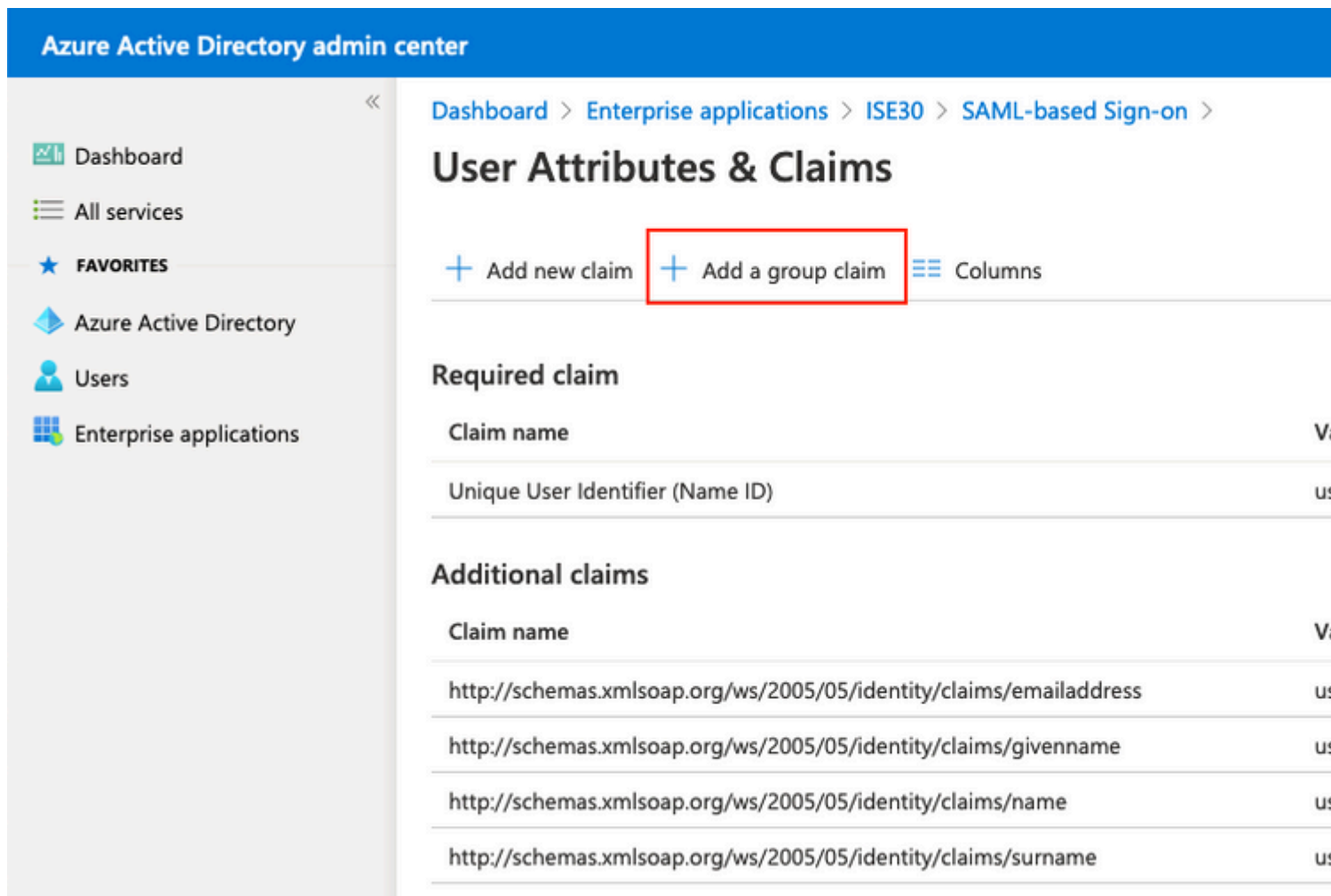
Per restituire il valore dell'attributo di gruppo configurato in precedenza, fare clic su **Modifica** accanto a **Attributi utente e attestazioni**.

User Attributes & Claims

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

 Edit

Fare clic su **Aggiungi attestazione basata su gruppo**.



Azure Active Directory admin center

Dashboard > Enterprise applications > ISE30 > SAML-based Sign-on >

User Attributes & Claims

+ Add new claim + Add a group claim Columns

Required claim

Claim name	Value
Unique User Identifier (Name ID)	us...

Additional claims

Claim name	Value
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	us...
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	us...
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	us...
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	us...

Selezionare **Gruppi protezione** e fare clic su **Salva**. Selezionare **ID gruppo** dal menu a discesa **Attributo origine**. Selezionare la casella di controllo per personalizzare il nome dell'attestazione basata su gruppo e immettere il nome **Gruppi**.

Group Claims



Manage the group claims used by Azure AD to populate SAML tokens issued to your app

Which groups associated with the user should be returned in the claim?

- None
- All groups
- Security groups
- Directory roles
- Groups assigned to the application

Source attribute *

Group ID

Advanced options

- Customize the name of the group claim

Name (required)

Groups

Namespace (optional)

- Emit groups as role claims ⓘ

Prendere nota del **nome** della **richiesta di rimborso** per il gruppo. In questo caso, si tratta di **Gruppi**.

Azure Active Directory admin center

Dashboard > Enterprise applications > ISE_3_1_Admin_SSO > SAML-based Sign-on >

User Attributes & Claims

+ Add new claim + Add a group claim Columns

Required claim

Claim name	Value
Unique User Identifier (Name ID)	user.n

Additional claims

Claim name	Value
Groups	user.g
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	user.n
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.g
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.n
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	user.s

8. Scarica il file XML dei metadati federativi di Azure

Fare clic su **Download** per XML metadati federazione nel certificato di firma SAML.

SAML Signing Certificate Edit

Status	Active
Thumbprint	B24F4BB47B350C93DE3D59EC87EE4C815C884462
Expiration	7/19/2024, 12:16:24 PM
Notification Email	chandandemo@outlook.com
App Federation Metadata Url	https://login.microsoftonline.com/182900ec-e960...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

Passaggio 3. Carica metadati da Azure Active Directory a ISE

Passare a **Amministrazione > Gestione identità > Origini identità esterne > Provider di ID SAML > [Provider SAML]**.

Passare alla scheda **Configurazione provider di identità** e fare clic su **Sfoggia**. Selezionare il file **XML dei metadati federativi** dal passaggio **Scarica XML dei metadati federativi di Azure** e fare clic su **Salva**.

The screenshot shows the Cisco ISE Administration interface. The top navigation bar includes 'Cisco ISE' and 'Administration - Identity Management'. The main navigation menu has 'Identities', 'Groups', 'External Identity Sources', 'Identity Source Sequences', and 'Settings'. The 'External Identity Sources' section is expanded, showing a list of providers: Certificate Authentication F, Active Directory, LDAP, ODBC, RADIUS Token, RSA SecurID, SAML Id Providers, and Social Login. The 'SAML Id Providers' section is selected, showing the 'Identity Provider List' for 'Azure'. The 'SAML Identity Provider' configuration page is displayed, with the 'Identity Provider Config.' tab selected. The configuration includes fields for 'Import Identity Provider Config File' (with a 'Choose File' button), 'Provider Id', 'Single Sign On URL' (https://login.microsoftonline.com/182900ec-e960-4340-bd20-e4522197...), and 'Single Sign Out URL (Redirect)' (https://login.microsoftonline.com/182900ec-e960-4340-bd20-e4522197...). Below these fields is a table titled 'Sianina Certificates' with the following data:

Subject	Issuer	Valid From	Valid To (Ex)
CN=Microsoft Azure Federated SSO Certificate	CN=Microsoft Azur...	Mon Jul 19 12:16:2...	Fri Jul 19 12:...

Passaggio 4. Configurazione dei gruppi SAML su ISE

Passare alla scheda **Gruppi** e incollare il valore di **Nome attestazione** dall'attributo **Configura gruppo di Active Directory** nell'attributo di **appartenenza al gruppo**.

External Identity Sources



- > Certificate Authentication F
- Active Directory
- LDAP
- ODBC
- RADIUS Token
- RSA SecurID
- > SAML Id Providers

Identity Provider List > Azure

SAML Identity Provider

General

Identity Provider Config.

Service Provider Info.

Groups

Groups

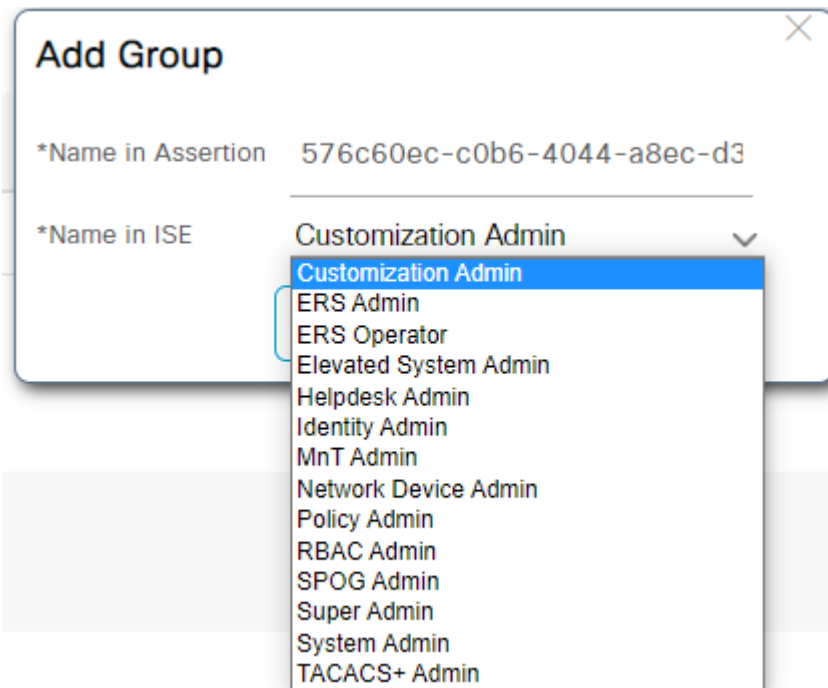
Group Membership Attribute groups

 Name in Assertion
 ^ Name in

Fare clic su **Add**. Popola **nome in asserzione** con il valore dell'**ID oggetto gruppo** del **gruppo di amministrazione ISE** acquisito in **Assegna utente di Azure Active Directory al gruppo**.

Configurare **Name in ISE** con l'elenco a discesa e selezionare il gruppo appropriato in ISE. Nell'esempio, il gruppo utilizzato è **Super Admin**. Fare clic su **OK**. Fare clic su **Salva**.

In questo modo viene creato un mapping tra il nome del gruppo in Azure e il nome del gruppo in ISE.



(Facoltativo) Passaggio 5. Configura criteri RBAC

Dalla fase precedente, esistono molti tipi diversi di livelli di accesso degli utenti che possono essere configurati su ISE.

Per modificare i criteri di controllo di accesso basati sui ruoli (RBAC), selezionare **Amministrazione** >

Sistema > Accesso amministratore > Autorizzazione > Autorizzazioni > Criteri RBAC e configurare come necessario.

Questa immagine è un riferimento alla configurazione di esempio.

▼ RBAC Policies

	Rule Name	Admin Groups	Permissions
<input checked="" type="checkbox"/> ▼	<u>Customization Admin Policy</u>	If <u>Customization Admin</u> +	then <u>Customization Admin M</u>
<input checked="" type="checkbox"/> ▼	<u>Elevated System Admin Poli</u>	If <u>Elevated System Admin</u> +	then <u>System Admin Menu Ac</u>
<input checked="" type="checkbox"/> ▼	<u>ERS Admin Policy</u>	If <u>ERS Admin</u> +	then <u>Super Admin Data Acce</u>
<input checked="" type="checkbox"/> ▼	<u>ERS Operator Policy</u>	If <u>ERS Operator</u> +	then <u>Super Admin Data Acce</u>
<input checked="" type="checkbox"/> ▼	<u>ERS Trustsec Policy</u>	If <u>ERS Trustsec</u> +	then <u>Super Admin Data Acce</u>
<input checked="" type="checkbox"/> ▼	<u>Helpdesk Admin Policy</u>	If <u>Helpdesk Admin</u> +	then <u>Helpdesk Admin Menu</u>
<input checked="" type="checkbox"/> ▼	<u>Identity Admin Policy</u>	If <u>Identity Admin</u> +	then <u>Identity Admin Menu Ac</u>
<input checked="" type="checkbox"/> ▼	<u>MnT Admin Policy</u>	If <u>MnT Admin</u> +	then <u>MnT Admin Menu Acce</u>
<input checked="" type="checkbox"/> ▼	<u>Network Device Policy</u>	If <u>Network Device Admin</u> +	then <u>Network Device Menu A</u>
<input checked="" type="checkbox"/> ▼	<u>Policy Admin Policy</u>	If <u>Policy Admin</u> +	then <u>Policy Admin Menu Acc</u>
<input checked="" type="checkbox"/> ▼	<u>RBAC Admin Policy</u>	If <u>RBAC Admin</u> +	then <u>RBAC Admin Menu Acc</u>
<input checked="" type="checkbox"/> ▼	<u>Read Only Admin Policy</u>	If <u>Read Only Admin</u> +	then <u>Super Admin Menu Acc</u>
<input checked="" type="checkbox"/> ▼	<u>SPOG Admin Policy</u>	If <u>SPOG Admin</u> +	then <u>Super Admin Data Acce</u>
<input checked="" type="checkbox"/> ▼	<u>Super Admin Policy</u>	If <u>Super Admin</u> +	then <u>Super Admin Menu Acc</u>
<input checked="" type="checkbox"/> ▼	<u>Super Admin_Azure</u>	If <u>Super Admin</u> +	then <u>Super Admin Menu Acc</u>
<input checked="" type="checkbox"/> ▼	<u>System Admin Policy</u>	If <u>System Admin</u> +	then <u>System Admin Menu Ac</u>
<input checked="" type="checkbox"/> ▼	<u>TACACS+ Admin Policy</u>	If <u>TACACS+ Admin</u> +	then <u>TACACS+ Admin Menu</u>

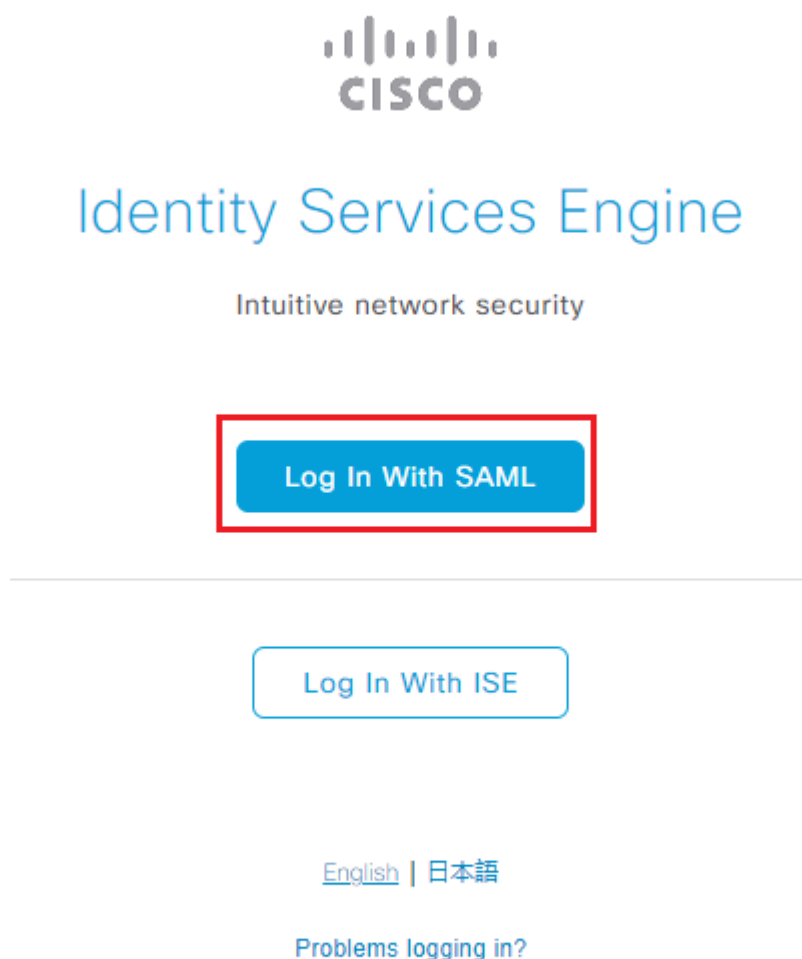
Verifica

Verificare che la configurazione funzioni correttamente.

Nota: Il test di accesso SSO SAML dalla funzionalità di test di Azure non funziona. Affinché l'SSO SAML di Azure funzioni correttamente, la richiesta SAML deve essere avviata da ISE.

Aprire la schermata del prompt di accesso con l'interfaccia grafica di ISE. Viene visualizzata una nuova opzione di **login con SAML**.

1. Accedere alla pagina di accesso all'interfaccia grafica di ISE e fare clic su **Log In with SAML**.



2. Viene visualizzata la schermata di accesso a Microsoft. Immettere le credenziali del **nome utente** di un account in un gruppo mappato ad ISE, come mostrato di seguito, e fare clic su **Avanti**, come mostrato nell'immagine.



Sign in

mck@gdplab2021.onmicrosoft.com

[Can't access your account?](#)

Next

3. Immettere la **password** per l'utente e fare clic su **Accedi**.



← mck@gdplab2021.onmicrosoft.com

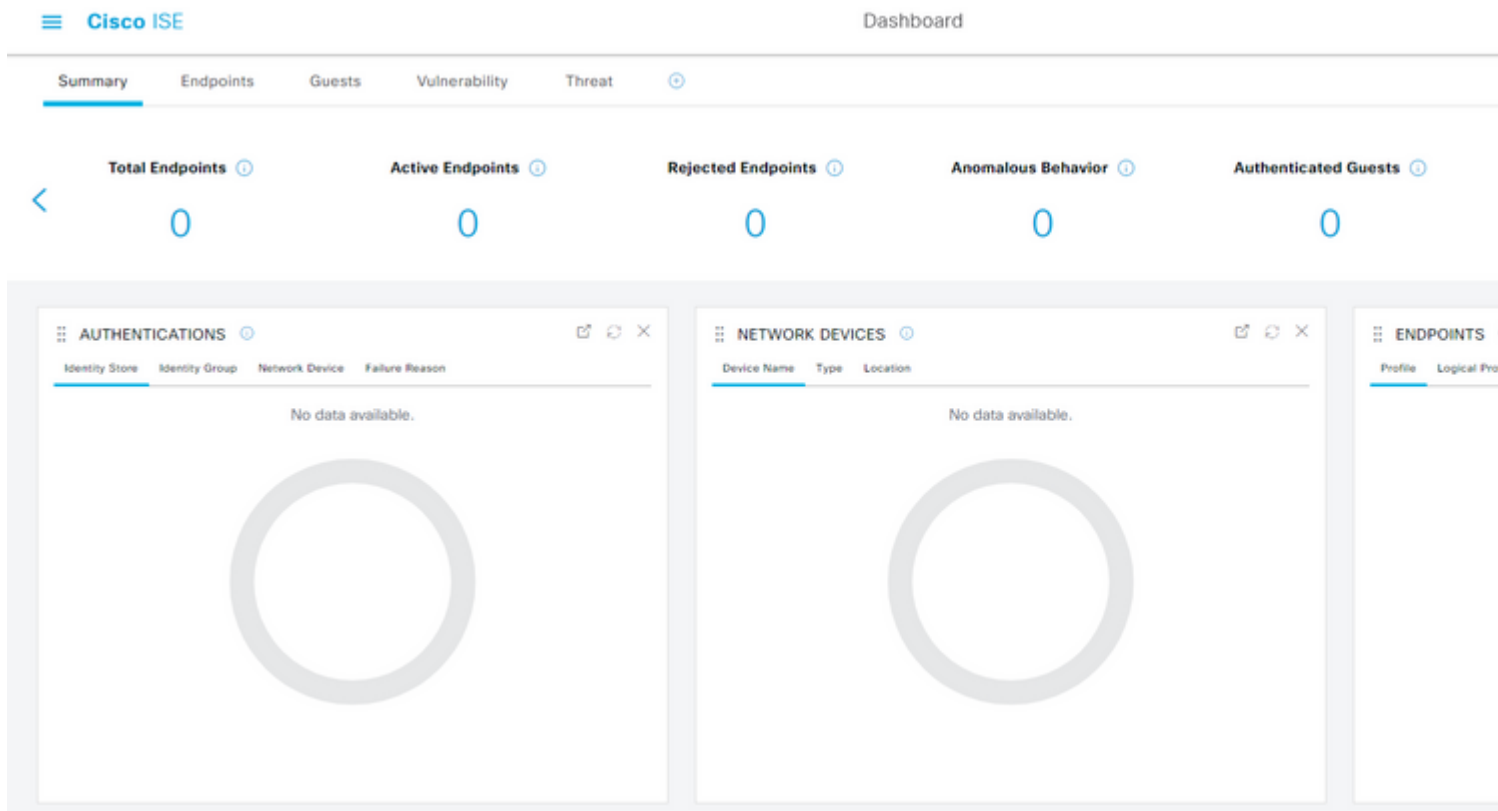
Enter password

.....

[Forgot my password](#)

Sign in

4. Ora l'utente viene reindirizzato al dashboard dell'applicazione ISE con le autorizzazioni appropriate configurate in base al gruppo ISE configurato in precedenza, come mostrato nell'immagine.



Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Problemi comuni

È fondamentale comprendere che l'autenticazione SAML viene gestita tra il browser e Azure Active Directory. È quindi possibile ottenere gli errori relativi all'autenticazione direttamente dal provider di identità (Azure) in cui l'accordo ISE non è ancora stato avviato.

Problema 1. Dopo l'immissione delle credenziali, viene visualizzato l'errore "Your account or password is correct" (Account o password errata). Qui, i dati utente non sono ancora ricevuti da ISE e il processo a questo punto rimane ancora con IdP (Azure).

Il motivo più probabile è che le informazioni sull'account non siano corrette o che la password non sia corretta. Per risolvere il problema: reimpostare la password o fornire la password corretta per l'account, come mostrato nell'immagine.



← mck@gdplab2021.onmicrosoft.com

Enter password

Your account or password is incorrect. If you don't remember your password, [reset it now](#).

Password

[Forgot my password](#)

Sign in

Numero 2. L'utente non fa parte del gruppo a cui deve essere consentito l'accesso a SAML SSO. Come nel caso precedente, i dati utente non sono ancora stati ricevuti da ISE e il processo a questo punto rimane ancora con IdP (Azure).

Per risolvere il problema: verificare che il passo di configurazione **Aggiungi gruppo all'applicazione** sia eseguito correttamente, come mostrato nell'immagine.



Sign in

Sorry, but we're having trouble signing you in.

AADSTS50105: The signed in user 'userwithoutgroup@gdplab2021.onmicrosoft.com' is not assigned to a role for the application '76b82bcb-a918-4016-aad7-b43bc4326254'(ISE_3_1_Admin_SSO).

Troubleshooting details ✕

If you contact your administrator, send this info to them.

[Copy info to clipboard](#)

Request Id: 1e15cea0-c349-4bee-922d-26299822a101

Correlation Id: 710626e0-45c1-4fad-baa6-ff7584ecf910

Timestamp: 2021-08-04T22:48:02Z

Message: AADSTS50105: The signed in user 'userwithoutgroup@gdplab2021.onmicrosoft.com' is not assigned to a role for the application '76b82bcb-a918-4016-aad7-b43bc4326254'(ISE_3_1_Admin_SSO).

Flag sign-in errors for review: [Enable flagging](#)

If you plan on getting help for this problem, enable flagging and try to reproduce the error within 20 minutes. Flagged events make diagnostics available and are raised to admin attention.

Numero 3. ISE Application Server non è in grado di gestire le richieste di accesso SAML. Questo problema si verifica quando la richiesta SAML viene avviata dal provider di identità Azure anziché dal provider di servizi ISE. Il test dell'accesso SSO da Azure AD non funziona perché ISE non supporta le richieste SAML avviate dal provider di identità.



This page isn't working

10.201.232.19 is currently unable to handle this request.

HTTP ERROR 500

ISE_3_1_Admin_SSO | SAML-based Sign-on

Enterprise Application

Overview

Deployment Plan

Manage

Properties

Owners

Roles and administrators (Preview)

Users and groups

Single sign-on

Provisioning

Application proxy

Self-service

Security

Conditional Access

Permissions

Token encryption

Activity

Sign-in logs

Usage & insights

Audit logs

Provisioning logs

Access reviews

Upload metadata file | Change single sign-on mode | Test this application

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Groups	user.groups
Unique User Identifier	user.userprincipalname

3 SAML Signing Certificate

Status	Active
Thumbprint	824F4BB47B350C93DE3D59EC87EE4C8
Expiration	7/19/2024, 12:16:24 PM
Notification Email	chandandemo@outlook.com
App Federation Metadata Url	https://login.microsoftonline.com/182
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

4 Set up ISE_3_1_Admin_SSO

You'll need to configure the application to link with Azure AD.

Login URL	https://login.microsoftonline.com/182
Azure AD Identifier	https://sts.windows.net/182900ec-e96
Logout URL	https://login.microsoftonline.com/182

[View step-by-step instructions](#)

5 Test single sign-on with ISE_3_1_Admin_SSO

Test to see if single sign-on is working. Users will need to be added to Users and group

Test single sign-on with ISE_3_1_Admin_SSO

Got feedback?

Microsoft recommends installing the My Apps Secure Sign-in Extension to allow third-party cookies if you have installed it but this message

Please make sure you have configured ISE_3_1_Admin_SSO before

~~Sign in as current user~~
~~Sign in as someone else~~ (requires browser)

Resolving errors

If you encounter an error in the sign-in page, please paste it below and retry.

What does the error look like?

Request Id: 4f8ec053-fb71-47de-a010-2786a32f1900
 Correlation Id: Saa879f5-68f1-482a-a405-ff993d8f4cb0
 Timestamp: 2018-03-06T23:54:10Z
 Message: Error AADSTSXXXX

[Get resolution guidance](#)

Numero 4. ISE visualizza un errore di accesso negato dopo un tentativo di accesso. Questo errore si verifica quando il nome attestazione del gruppo creato in precedenza nell'applicazione Azure Enterprise non corrisponde in ISE.

Per risolvere il problema: verificare che il nome dell'attestazione basata su gruppo in Azure e ISE nella scheda Gruppi provider di identità SAML sia lo stesso. Per ulteriori informazioni, fare riferimento ai passaggi 2.7 e 4. nella sezione **Configurazione di SAML SSO con Azure AD** di questo documento.



Identity Services Engine

Intuitive network security



Access Denied

Log In With SAML

Log In With ISE

[English](#) | [日本語](#)

[Problems logging in?](#)

Risoluzione dei problemi di ISE

Il livello di log dei componenti deve essere modificato su **ISE**. Passare a **Operazioni > Risoluzione dei problemi > Debug guidato > Configurazione log di debug**.

Nome componente	Livello log	Nome file di log
portale	DEBUG	guest.log

opensaml	DEBUG	ise-psc.log
saml	DEBUG	ise-psc.log

Registri con nome account di accesso SAML e nomi attestazione basata su gruppo non corrispondenti

Set di debug che visualizza lo scenario di risoluzione dei problemi di mancata corrispondenza dei nomi attestazione al momento dell'esecuzione del flusso (ise-psc.log).

Nota: tenere d'occhio le voci in **grassetto**. I registri sono stati abbreviati per motivi di chiarezza.

1. L'utente viene reindirizzato all'URL del provider di identità dalla pagina Amministrazione di ISE.

<#root>

```
2021-07-29 13:48:20,709 INFO [admin-http-pool46][] api.services.persistence.dao.DistributionDAO -:::
2021-07-29 13:48:20,712 INFO [admin-http-pool46][] cpm.admin.infra.spring.ISEAdminControllerUtils -:::
```

forwardStr for: <https://10.201.232.19/admin/LoginAction.do>

```
2021-07-29 13:48:20,839 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-7][] cpm.saml.framework.impl.SAML
2021-07-29 13:48:20,839 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-7][] cpm.saml.framework.impl.SAML
```

IDP URL: <https://login.microsoftonline.com/182900ec-e960-4340-bd20-e4522197ecf8/saml2>

```
2021-07-29 13:48:20,839 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-7][] cpm.saml.framework.impl.SAML
2021-07-29 13:48:20,839 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-7][] cpm.saml.framework.impl.SAML
2021-07-29 13:48:20,839 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-7][] cpm.saml.framework.impl.SAML
2021-07-29 13:48:20,839 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-7][] cpm.saml.framework.impl.SAML
```

SAML request - spUrlToReturnTo: <https://10.201.232.19:8443/portal/SSOLoginResponse.action>

```
2021-07-29 13:48:20,844 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-7][] cpm.saml.framework.impl.SAML
2021-07-29 13:48:20,851 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-7][] cpm.saml.framework.impl.SAML
```

2. La risposta SAML viene ricevuta dal browser.

<#root>

```
2021-07-29 13:48:27,172 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAML
2021-07-29 13:48:27,172 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAML
2021-07-29 13:48:27,172 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAML
2021-07-29 13:48:27,172 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAML
```

-:::- Decoded SAML relay state of: [_0049a2fd-7047-4d1d-8907-5a05a94ff5fd_DELIMITERportalId_EQUALS0049a2](#)

```
2021-07-29 13:48:27,177 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] opensaml.ws.message.decoder
```

-:::- Decoded SAML message

```

2021-07-29 13:48:27,182 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] opensaml.saml2.binding.decoder
2021-07-29 13:48:27,183 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] opensaml.ws.message.decoder
2021-07-29 13:48:27,183 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] opensaml.ws.message.decoder
2021-07-29 13:48:27,183 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] opensaml.common.binding.decoder
opensaml.common.binding.decoder.BaseSAMLMessageDecoder -:::- Intended message destination endpoint: https://10.201.232.19:8443/
2021-07-29 13:48:27,183 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] opensaml.common.binding.decoder
2021-07-29 13:48:27,183 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAMLMessageDecoder
2021-07-29 13:48:27,184 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] opensaml.common.binding.decoder
2021-07-29 13:48:27,184 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAMLMessageDecoder

```

3. Analisi degli attributi (asserzioni) avviata.

<#root>

```

2021-07-29 13:48:27,184 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAMLMessageDecoder
2021-07-29 13:48:27,184 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAMLMessageDecoder
2021-07-29 13:48:27,184 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAMLMessageDecoder
2021-07-29 13:48:27,184 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAMLMessageDecoder

2021-07-29 13:48:27,184 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAMLMessageDecoder

2021-07-29 13:48:27,184 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAMLMessageDecoder

2021-07-29 13:48:27,184 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAMLMessageDecoder

2021-07-29 13:48:27,184 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAMLMessageDecoder
2021-07-29 13:48:27,184 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAMLMessageDecoder
2021-07-29 13:48:27,184 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAMLMessageDecoder
2021-07-29 13:48:27,184 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAMLMessageDecoder
2021-07-29 13:48:27,184 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAMLMessageDecoder
2021-07-29 13:48:27,184 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAMLMessageDecoder
2021-07-29 13:48:27,184 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAMLMessageDecoder
2021-07-29 13:48:27,184 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAMLMessageDecoder
2021-07-29 13:48:27,184 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAMLMessageDecoder
2021-07-29 13:48:27,184 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAMLMessageDecoder
2021-07-29 13:48:27,184 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAMLMessageDecoder

[parseAttributes] Set on IdpResponse object - attribute<http://schemas.xmlsoap.org/ws/2005/05/identity/>

```

```

2021-07-29 13:48:27,184 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAMLMessageDecoder

```

4. L'attributo Group viene ricevuto con il valore **576c60ec-c0b6-4044-a8ec-d395b1475d6e**, convalida della firma.

```

2021-07-29 13:48:27,185 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAMLMessageDecoder
2021-07-29 13:48:27,185 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAMLMessageDecoder
2021-07-29 13:48:27,185 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAMLMessageDecoder
2021-07-29 13:48:27,185 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAMLMessageDecoder
2021-07-29 13:48:27,185 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAMLMessageDecoder

```

```

2021-07-29 13:48:27,185 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAM
2021-07-29 13:48:27,186 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAM
IdP URI: https://sts.windows.net/182900ec-e960-4340-bd20-e4522197ecf8/
SP URI: http://CiscoISE/0049a2fd-7047-4d1d-8907-5a05a94ff5fd
Assertion Consumer URL: https://10.201.232.19:8443/portal/SSOloginResponse.action
Request Id: _0049a2fd-7047-4d1d-8907-5a05a94ff5fd_DELIMITERportalId_EQUALS0049a2fd-7047-4d1d-8907-5a05a94ff5fd
Client Address: 10.24.226.171
Load Balancer: null
2021-07-29 13:48:27,186 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validate
2021-07-29 13:48:27,186 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validate
2021-07-29 13:48:27,186 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validate
2021-07-29 13:48:27,186 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validate
2021-07-29 13:48:27,186 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] org.opensaml.security.SAMLSignature
2021-07-29 13:48:27,186 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] org.opensaml.security.SAMLSignature
2021-07-29 13:48:27,186 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validate
2021-07-29 13:48:27,186 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] org.opensaml.xml.signature
2021-07-29 13:48:27,186 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] org.opensaml.xml.signature
2021-07-29 13:48:27,186 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] org.opensaml.xml.signature
2021-07-29 13:48:27,186 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] org.opensaml.xml.signature
2021-07-29 13:48:27,188 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] org.opensaml.xml.signature
2021-07-29 13:48:27,188 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validate
2021-07-29 13:48:27,188 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validate
2021-07-29 13:48:27,188 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validate
2021-07-29 13:48:27,188 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validate
2021-07-29 13:48:27,188 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validate
2021-07-29 13:48:27,188 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validate
2021-07-29 13:48:27,188 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validate
2021-07-29 13:48:27,188 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validate
2021-07-29 13:48:27,188 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validate
2021-07-29 13:48:27,188 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validate
2021-07-29 13:48:27,188 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAM
2021-07-29 13:48:27,188 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAM
2021-07-29 13:48:27,189 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAM
2021-07-29 13:48:27,189 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAM
2021-07-29 13:48:27,358 INFO [admin-http-pool50][] ise.rbac.evaluator.impl.MenuPermissionEvaluatorImpl

```

5. Convalida dell'autorizzazione RBAC.

```
<#root>
```

```

*****Rbac Log Summary for user samlUser*****
2021-07-29 13:48:27,360 INFO [admin-http-pool50][] com.cisco.ise.util.RBACUtil -:::- Populating cache
2021-07-29 13:48:27,368 ERROR [admin-http-pool50][] cpm.admin.infra.utils.PermissionEvaluationUtil -:::-

java.lang.NullPointerException

2021-07-29 13:48:27,369 INFO [admin-http-pool50][] cpm.admin.infra.action.LoginAction -:::- In Login
2021-07-29 13:48:27,369 INFO [admin-http-pool50][] cpm.admin.infra.action.LoginAction -:::- In Login
2021-07-29 13:48:27,369 ERROR [admin-http-pool50][] cpm.admin.infra.action.LoginAction -:::- Can't save
2021-07-29 13:48:27,369 INFO [admin-http-pool50][] cpm.admin.infra.action.LoginActionResultHandler -:::-

```

2021-07-29 13:48:27,369 INFO [admin-http-pool50][] cpm.admin.infra.spring.ISEAdminControllerUtils -:::

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).