

Configura ID REST ISE 3.0 con Azure Active Directory

Sommario

[Introduzione](#)

[Premesse](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Panoramica del flusso di alto livello](#)

[Configura Azure AD per l'integrazione](#)

[Configurazione di ISE per l'integrazione](#)

[Esempi di policy ISE per diversi scenari di utilizzo](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Problemi con il servizio di autenticazione REST](#)

[Problemi di autenticazione ID REST](#)

[Utilizzare i file di log](#)

Introduzione

In questo documento viene descritta l'integrazione di Cisco ISE 3.0 con Azure AD implementata tramite il servizio Identità REST con credenziali password del proprietario della risorsa.

Premesse

In questo documento viene descritto come configurare e risolvere i problemi relativi all'integrazione di Identity Services Engine (ISE) 3.0 con Microsoft (MS) Azure Active Directory (AD) implementata tramite il servizio ID (Identity Transfer) REST (Representative State Transfer) con l'aiuto di ROPC (Resource Owner Password Credentials).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di base dei seguenti argomenti:

- ISE
- Microsoft Azure AD

- Informazioni sull'implementazione e le limitazioni del protocollo ROPC; [collegamento](#)

Componenti usati

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

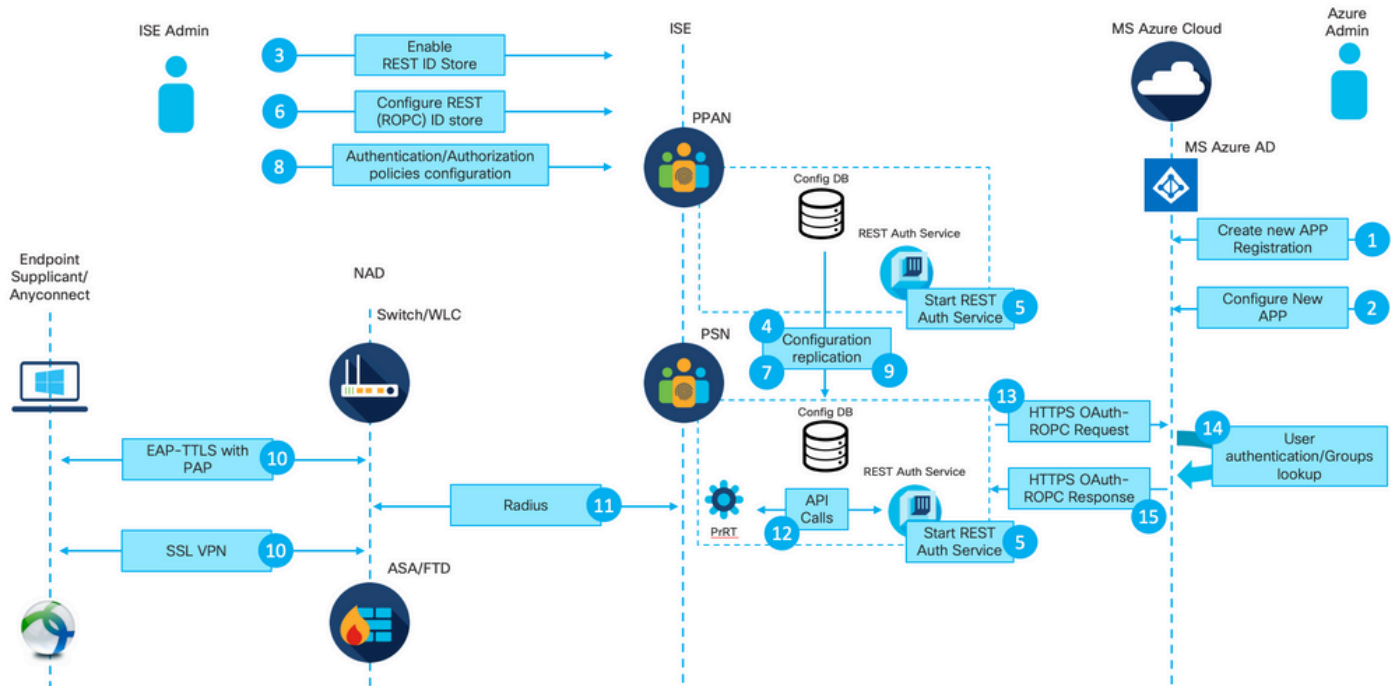
- Cisco ISE versione 3.0
- Microsoft Azure AD
- WS-C3850-24P con s/w 16.9.2
- ASA v con 9.10 (1)
- Windows 10.0.18363

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.

Configurazione

La funzionalità ISE REST ID si basa sul nuovo servizio introdotto in ISE 3.0 - Servizio di autenticazione REST. Questo servizio è responsabile della comunicazione con Azure AD tramite gli scambi ROPC OAuth (Open Authorization) per eseguire l'autenticazione utente e il recupero dei gruppi. Il servizio di autenticazione REST è disabilitato per impostazione predefinita e, dopo che è stato abilitato dall'amministratore, viene eseguito su tutti i nodi ISE nella distribuzione. Dal momento che la comunicazione del servizio di autenticazione REST con il cloud avviene quando al momento dell'autenticazione dell'utente, qualsiasi ritardo sul percorso porta una latenza aggiuntiva nel flusso di autenticazione/autorizzazione. Questa latenza è al di fuori del controllo ISE, e qualsiasi implementazione di REST Auth deve essere pianificata e testata attentamente per evitare l'impatto su altri servizi ISE.

Panoramica del flusso di alto livello



1. L'amministratore del cloud di Azure crea una nuova registrazione dell'applicazione (app). I dettagli di questa app vengono utilizzati in seguito in ISE per stabilire una connessione con Azure AD.

2. L'amministratore del cloud di Azure deve configurare l'app con:

- Crea un segreto client
- Abilita ROPC
- Aggiungì attestazioni basate su gruppo
- Definizione delle autorizzazioni API (Application Programming Interface)

3. L'amministratore ISE attiva il servizio di autenticazione REST. È necessario eseguire questa operazione prima di eseguire qualsiasi altra azione.

4. Le modifiche vengono scritte nel database di configurazione e replicate nell'intera implementazione ISE.
 5. Il servizio di autenticazione REST viene avviato su tutti i nodi.
 6. L'amministratore ISE configura l'archivio di ID REST con i dettagli del Passaggio 2.
 7. Le modifiche vengono scritte nel database di configurazione e replicate nell'intera implementazione ISE.
 8. L'amministratore ISE crea una nuova sequenza di archivio identità o modifica quella già esistente e configura i criteri di autenticazione/autorizzazione.
 9. Le modifiche vengono scritte nel database di configurazione e replicate nell'intera implementazione ISE.
 10. L'endpoint avvia l'autenticazione. In base alle specifiche del protocollo ROPC, la password utente deve essere fornita alla piattaforma Microsoft Identity in formato testo non crittografato tramite una connessione HTTP crittografata; per questo motivo, le uniche opzioni di autenticazione attualmente supportate da ISE sono:
 - Extensible Authentication Protocol-Tunneled Transport Layer Security (EAP-TTLS) con Password Authentication Protocol (PAP) come metodo interno
 - Autenticazione VPN SSL AnyConnect con PAP
 11. Scambio con ISE Policy Service Node (PSN) su Radius.
 12. Process Runtime (PrRT) invia una richiesta al servizio ID REST con i dettagli dell'utente (nome utente/password) tramite l'API interna.
 13. Il servizio ID REST invia la richiesta ROPC OAuth ad Azure AD tramite il protocollo HTTPS (HyperText Transfer Protocol Secure).
 14. Azure AD esegue l'autenticazione degli utenti e recupera i gruppi di utenti.
 15. Il risultato dell'autenticazione/autorizzazione è stato restituito all'ISE.
- Dopo il punto 15, il risultato dell'autenticazione e i gruppi recuperati vengono restituiti alla tabella PrRT, che include il flusso di valutazione delle policy e assegna il risultato finale dell'autenticazione/autorizzazione. Access-Accept con attributi dal profilo di autorizzazione o Access-Reject restituito al dispositivo di accesso alla rete (NAD).

Configura Azure AD per l'integrazione

1. Individuare AppRegistration Service come illustrato nell'immagine.

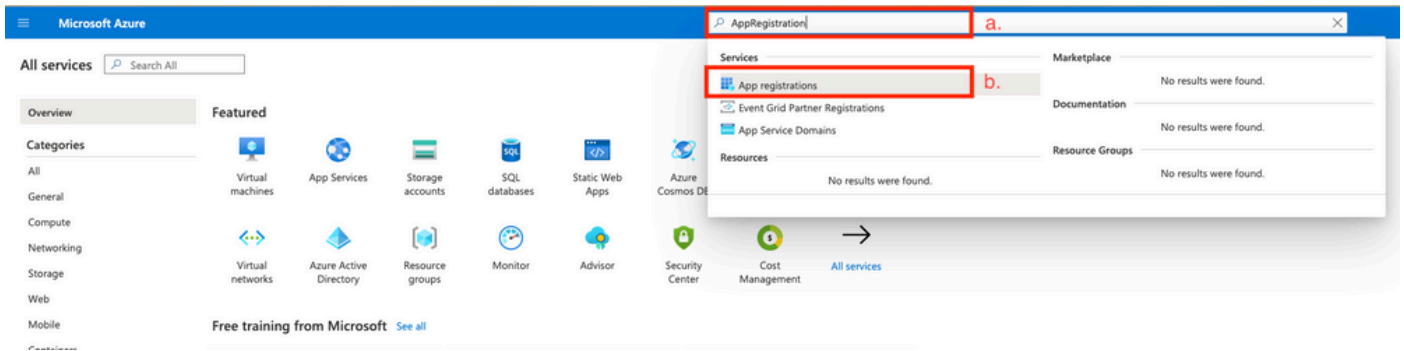


Figura 2.

a. Digitare AppRegistration nella barra di ricerca globale.

b. Fare clic sul servizio di registrazione dell'app.

2. Crea una nuova registrazione dell'app.

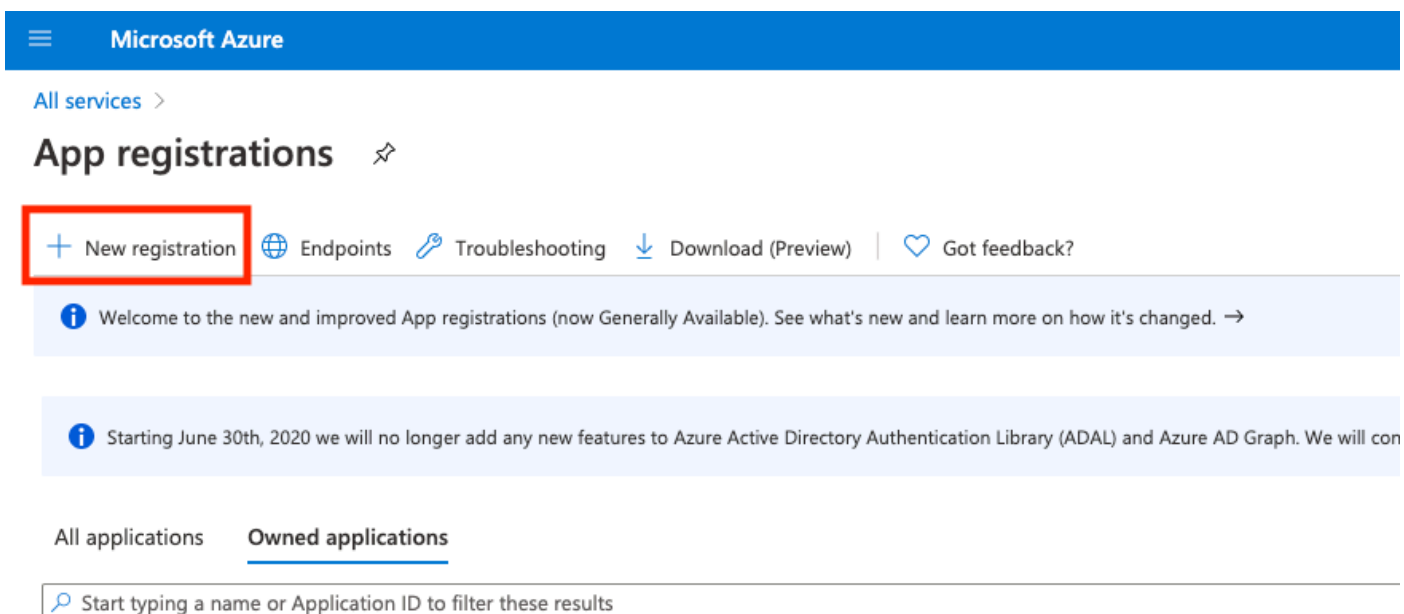


Figura 3.

3. Registra una nuova app.

Register an application

* Name

The user-facing display name for this application (this can be changed later).

✓

a.

Supported account types

Who can use this application or access this API?

- Accounts in this organizational directory only (DEMO only - Single tenant)
- Accounts in any organizational directory (Any Azure AD directory - Multitenant)
- Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- Personal Microsoft accounts only

b.

[Help me choose...](#)


Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

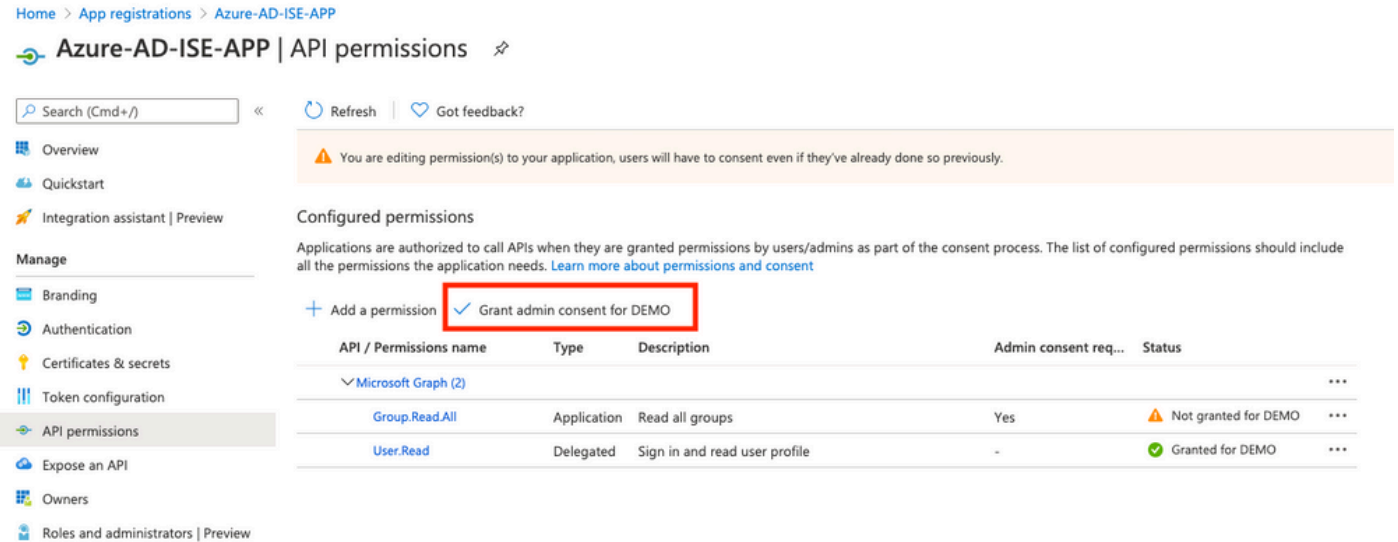
By proceeding, you agree to the [Microsoft Platform Policies](#)

c.

Figura 4.

 : i dati dei gruppi di utenti possono essere recuperati da Azure AD in più modi con l'aiuto di autorizzazioni API diverse. Il metodo descritto in questo esempio ha avuto successo nel laboratorio Cisco TAC. Usare altre autorizzazioni API se consigliato dall'amministratore di Azure AD.

16. Grant admin consent per le autorizzazioni API.



Home > App registrations > Azure-AD-ISE-APP

Azure-AD-ISE-APP | API permissions

Search (Cmd+/) Refresh Got feedback?

Overview
Quickstart
Integration assistant | Preview

Manage

Branding
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
Owners
Roles and administrators | Preview

You are editing permission(s) to your application, users will have to consent even if they've already done so previously.

Configured permissions

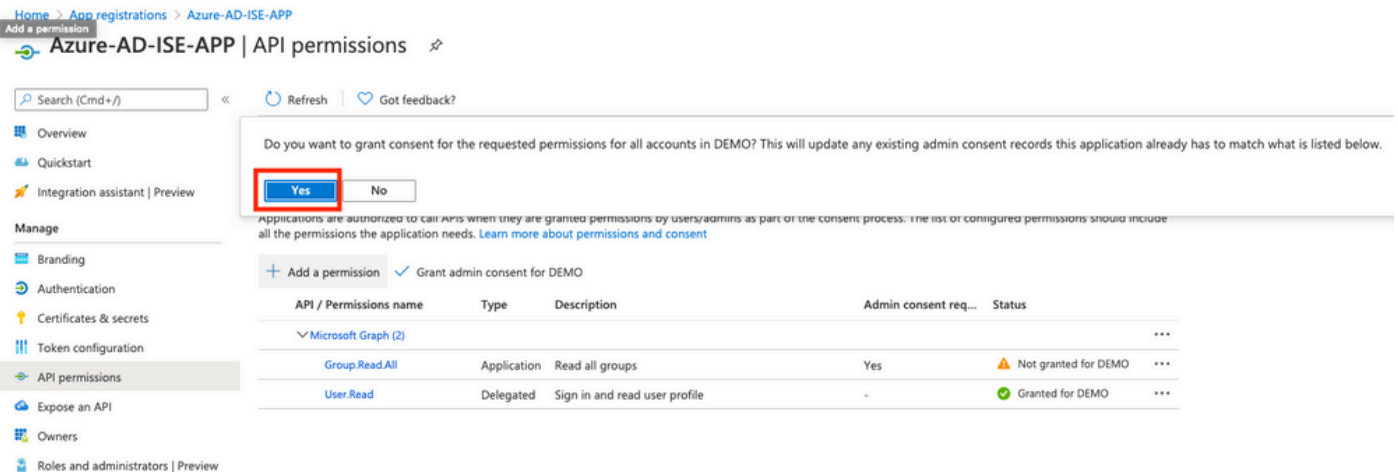
Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission Grant admin consent for DEMO

API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (2)				
Group.Read.All	Application	Read all groups	Yes	Not granted for DEMO
User.Read	Delegated	Sign in and read user profile	-	Granted for DEMO

Figura 17.

17. Confermare l'autorizzazione per l'amministratore.



Home > App registrations > Azure-AD-ISE-APP

Add a permission

Azure-AD-ISE-APP | API permissions

Search (Cmd+/) Refresh Got feedback?

Overview
Quickstart
Integration assistant | Preview

Manage

Branding
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
Owners
Roles and administrators | Preview

Do you want to grant consent for the requested permissions for all accounts in DEMO? This will update any existing admin consent records this application already has to match what is listed below.

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission Grant admin consent for DEMO

API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (2)				
Group.Read.All	Application	Read all groups	Yes	Not granted for DEMO
User.Read	Delegated	Sign in and read user profile	-	Granted for DEMO

Figura 18.

A questo punto è possibile considerare l'integrazione completamente configurata sul lato Azure AD.

Configurazione di ISE per l'integrazione

1. Passare alle impostazioni di Identity Management.

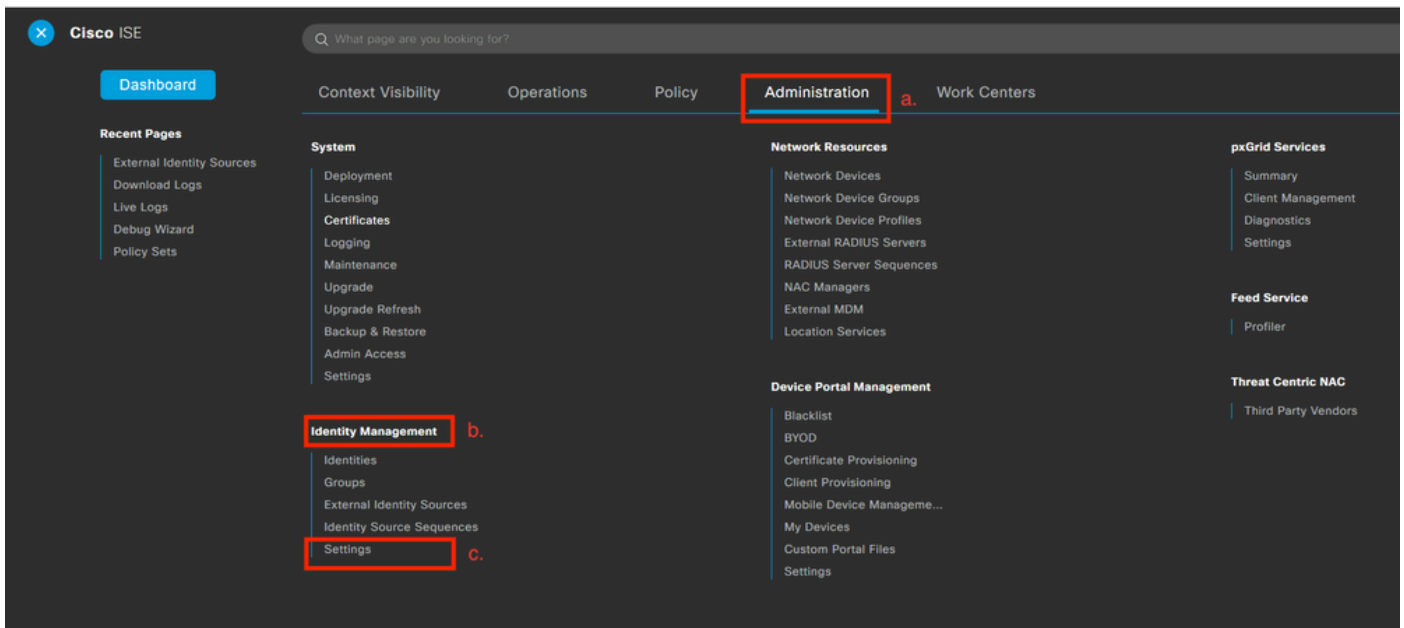


Figura 19.

Passa a Administration > Identity Management > Settings .

2. Abilitare il servizio ID REST (disabilitato per impostazione predefinita).

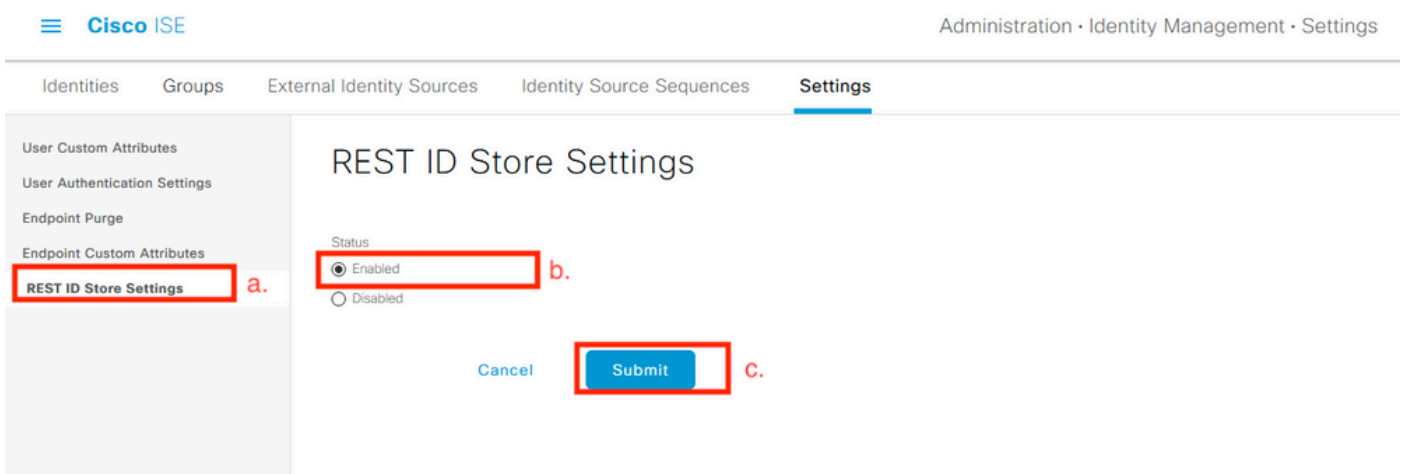


Figura 20.

Passa a REST ID Store Settings e modificare lo stato delle impostazioni dell'archivio di ID REST per Enable, quindi Submit le modifiche.

3. Creare un archivio di ID REST.

Identities Groups **External Identity Sources** Identity Source Sequences Settings

External Identity Sources

- > Certificate Authentication F
- ▼ Active Directory
 - EXAMPLE
 - LDAP
 - ODBC
 - RADIUS Token
 - RSA SecurID
- > SAML Id Providers
- Social Login
- REST (ROPC)** b.

REST (ROPC)

Refresh **+ Add** c. Duplicate Trash Edit

<input type="checkbox"/>	Name	Description	Type
No data found.			

Figura 21.

Passare alla External Identity Sources , fare clic su REST (ROPC) e fare clic su Add.

4. Configurare l'archivio di ID REST.

Identities Groups **External Identity Sources** Identity Source Sequences Settings

External Identity Sources

<

> Certificate Authentication F

▼ Active Directory

EXAMPLE

LDAP

ODBC

RADIUS Token

RSA SecurID

> SAML Id Providers

Social Login

REST (ROPC)

REST (ROPC) > New

Name * a.

Description

REST Identity Provider *
Azure

Client ID * b.

Client Secret * c.

Tenant ID * d. f.

Groups g.

Username Suffix
 e.

h.

Figura 22.


a. Definire il nome del punto vendita ID. Più tardi questo nome sarà disponibile nell'elenco dei dizionari ISE quando si configurano i criteri di autorizzazione. Inoltre, questo nome viene visualizzato nell'elenco degli archivi ID disponibili nelle impostazioni dei criteri di autenticazione e nell'elenco degli archivi ID disponibili nella configurazione di sequenza dell'archivio identità.

b. Fornire l'ID client (ottenuto da Azure AD nel passaggio 8. della sezione di configurazione dell'integrazione di Azure AD).

c. Fornire la chiave privata del client (acquisita da Azure AD nel passaggio 7. della sezione Configurazione integrazione di Azure AD).


d. Fornire l'ID tenant (acquisito da Azure AD nel passaggio 8. della sezione di configurazione dell'integrazione di Azure AD).

e. Configurare il suffisso del nome utente: per impostazione predefinita, ISE PSN utilizza un nome utente fornito dall'utente finale e fornito nel formato sAMAccountName (nome utente breve, ad esempio bob); in questo caso, Azure AD non è in grado di individuare l'utente. Suffisso nome utente è il valore aggiunto al nome utente fornito dall'utente per portare il nome utente nel formato UPN.

 Nota: il ROPC è limitato all'autenticazione dell'utente in quanto si basa sull'attributo Username durante l'autenticazione. Gli oggetti dispositivo in Azure AD non dispongono di attributi Username.

f. Fare clic su Test connessione per confermare che ISE può utilizzare i dettagli dell'app forniti per stabilire una connessione ad Azure AD.

g. Fare clic su Carica gruppi per aggiungere i gruppi disponibili nell'archivio ID di Azure AD a REST. Nell'esempio seguente viene illustrato l'aspetto dell'esperienza dell'amministratore.

 Nota: si tenga presente che l'ID bug Cisco [CSCvx00345](https://tools.cisco.com/bugcenter/bug/?bugID=CSCvx00345) è difettoso in quanto causa il mancato caricamento dei gruppi. Il difetto è risolto in ISE 3.0 patch 2.

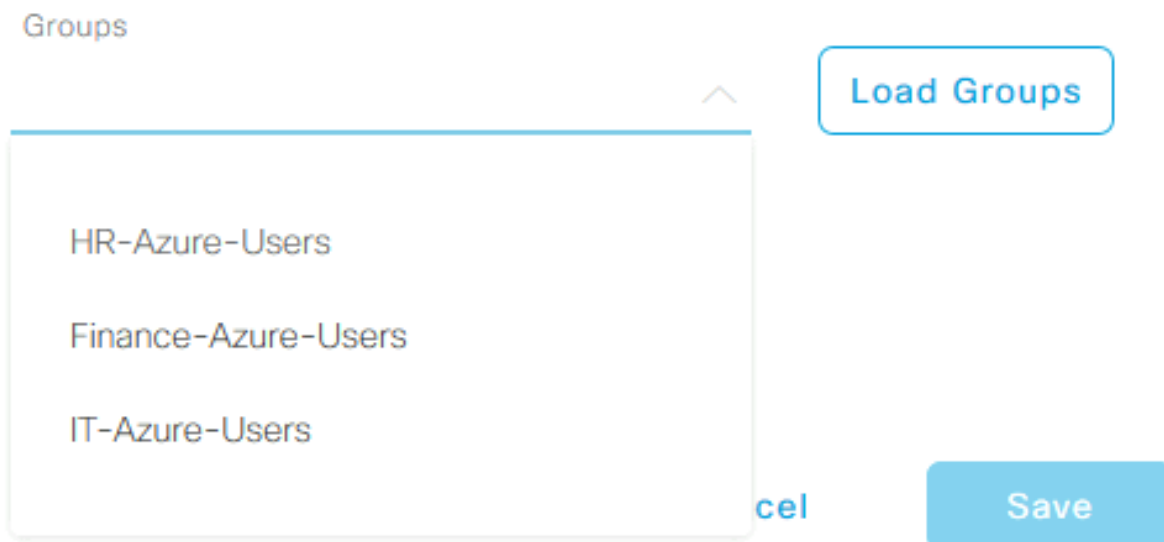


Figura 23.

h. Inviare le modifiche.

5. In questa fase, considerare la creazione di una nuova sequenza di archivio identità, che include un archivio ID REST appena creato.

6. Nel momento in cui l'archivio di ID REST o la sequenza di archivio di identità che lo contiene viene assegnata al criterio di autenticazione, modificare un'azione predefinita per Errore processo

da DROP a REJECT, come mostrato nell'immagine.

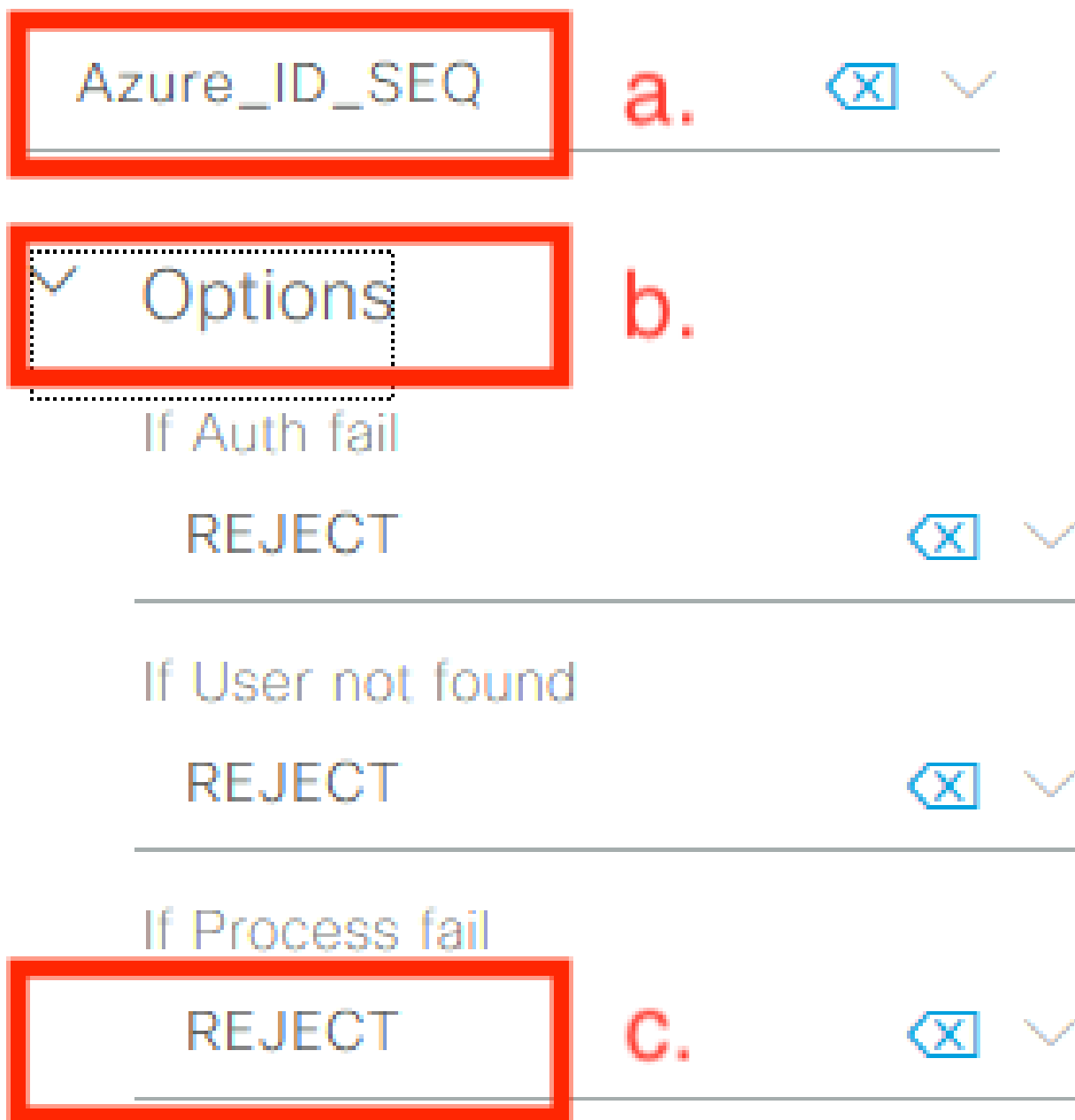


Figura 24.

- Individuare il criterio di autenticazione che utilizza l'archivio ID REST.
- Aprire l'elenco a discesa Opzioni.
- L'azione di modifica predefinita per il processo Non riuscito da DROP a REJECT.

Questa operazione è necessaria per evitare che il PSN venga contrassegnato come inattivo sul lato NAD in un momento in cui si verificano errori specifici nell'archivio ID REST, ad esempio:

- L'utente non è membro di alcun gruppo in Azure AD.

- La password dell'utente deve essere cambiata.

7. Aggiungere il dizionario dell'archivio di ID REST nei criteri di autorizzazione.

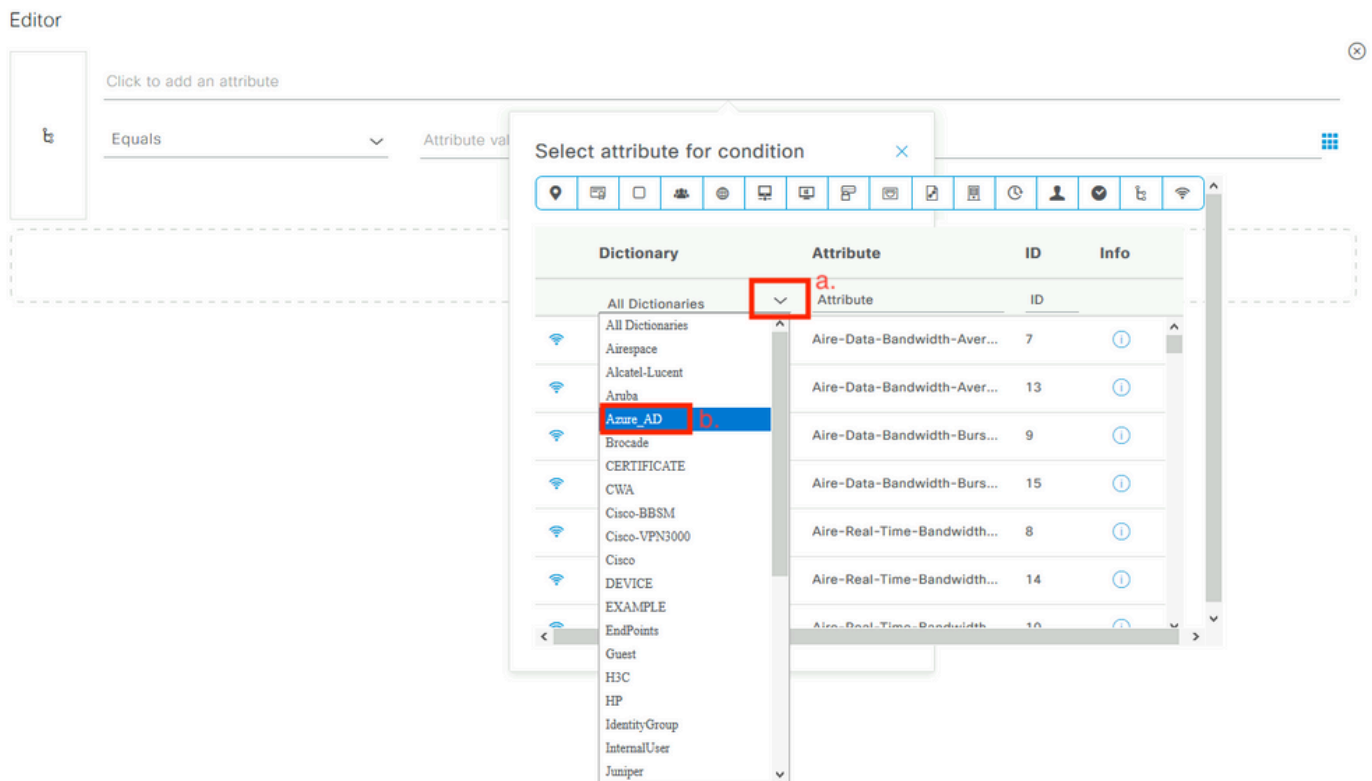


Figura 25.

a. Aprire l'elenco a discesa Tutti i dizionari.

b. Individuare il dizionario con lo stesso nome dell'archivio di ID REST.

8. Aggiungere gruppi di identità esterni (a partire da ISE 3.0, l'unico attributo disponibile nel dizionario degli archivi di ID REST è un gruppo esterno).

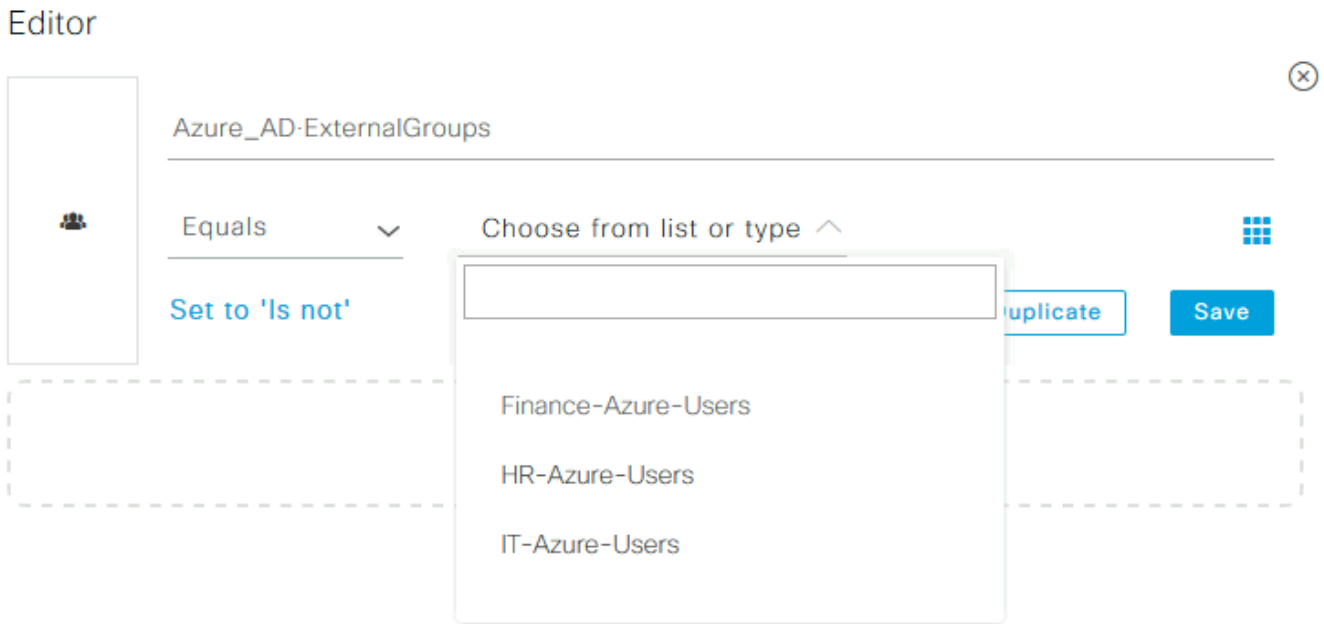


Figura 26.

Esempi di policy ISE per diversi scenari di utilizzo

Nel caso dell'autenticazione Dot1x, la condizione del tunnel EAP dal dizionario di accesso alla rete può essere utilizzata per far corrispondere i tentativi EAP-TTLS, come mostrato nell'immagine.

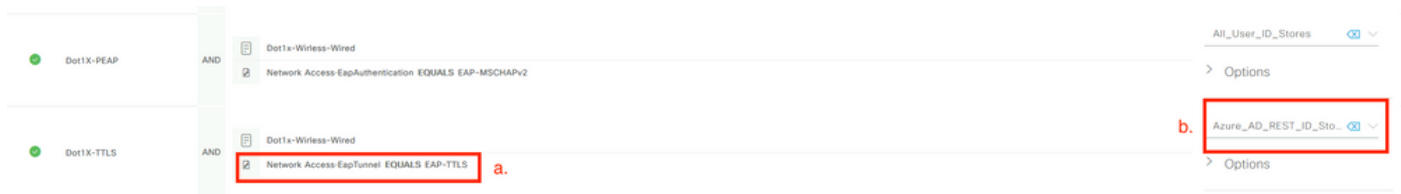


Figura 27.

a. Definire EAP Tunnel EQUAL to EAP-TTLS (Tunnel EAP uguale a EAP-TTLS) in modo che corrisponda ai tentativi che devono essere inoltrati all'archivio di ID REST.

b. Selezionare direttamente nell'archivio ID REST o la sequenza dell'archivio identità, che la contiene nella colonna Utilizza.

All'interno dei singoli criteri di autorizzazione, è possibile utilizzare i gruppi esterni di Azure AD insieme al tipo di tunnel EAP:

✓	Dot1X-TTLS-Azure-Finance	AND	<ul style="list-style-type: none"> Dot1x-Wireless-Wired Network Access-EapTunnel EQUALS EAP-TTLS Azure_AD-ExternalGroups EQUALS Finance-Azure-Users
✓	Dot1X-TTLS-Azure-HR	AND	<ul style="list-style-type: none"> Dot1x-Wireless-Wired Network Access-EapTunnel EQUALS EAP-TTLS Azure_AD-ExternalGroups EQUALS HR-Azure-Users
✓	Dot1X-TTLS-Azure-IT	AND	<ul style="list-style-type: none"> Dot1x-Wireless-Wired Network Access-EapTunnel EQUALS EAP-TTLS Azure_AD-ExternalGroups EQUALS IT-Azure-Users

Figura 28.

Per il flusso basato su VPN, è possibile utilizzare un nome di gruppo di tunnel come differenziatore:

Criteri di autenticazione:

Status	Rule Name	Conditions	Use
✓	Azure-AD	Cisco-VPN3000-CVPN3000/ASA/PIX7x-Tunnel-Group-Name EQUALS skuchere	Azure_AD_REST_ID_Sto... > Options

Criteri di autorizzazione:

✓	VPN-Azure-Finance	AND	<ul style="list-style-type: none"> Cisco-VPN3000-CVPN3000/ASA/PIX7x-Tunnel-Group-Name EQUALS skuchere Azure_AD-ExternalGroups EQUALS Finance-Azure-Users
✓	VPN-Azure-HR	AND	<ul style="list-style-type: none"> Cisco-VPN3000-CVPN3000/ASA/PIX7x-Tunnel-Group-Name EQUALS skuchere Azure_AD-ExternalGroups EQUALS HR-Azure-Users
✓	VPN-Azure-IT	AND	<ul style="list-style-type: none"> Cisco-VPN3000-CVPN3000/ASA/PIX7x-Tunnel-Group-Name EQUALS skuchere Azure_AD-ExternalGroups EQUALS IT-Azure-Users

Figura 29.

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

1. Confermare che il servizio di autenticazione REST sia in esecuzione sul nodo ISE.

Per verificare questa condizione, è necessario eseguire il comando `show application status ise` nella shell Secure Shell (SSH) di un nodo ISE di destinazione:

```
<#root>
```

```
skuchere-ise30-1/admin# show application status ise
```

```
ISE PROCESS NAME STATE PROCESS ID
-----
Database Listener running 101790
Database Server running 92 PROCESSES
Application Server running 39355
Profiler Database running 107909
ISE Indexing Engine running 115132
AD Connector running 116376
M&T Session Database running 107694
M&T Log Processor running 112553
Certificate Authority Service running 116226
EST Service running 119875
SXP Engine Service disabled
Docker Daemon running 104217
TC-NAC Service disabled
pxGrid Infrastructure Service disabled
pxGrid Publisher Subscriber Service disabled
pxGrid Connection Manager disabled
pxGrid Controller disabled
PassiveID WMI Service disabled
PassiveID Syslog Service disabled
PassiveID API Service disabled
PassiveID Agent Service disabled
PassiveID Endpoint Service disabled
PassiveID SPAN Service disabled
DHCP Server (dhcpd) disabled
DNS Server (named) disabled
ISE Messaging Service running 104876
ISE API Gateway Database Service running 106853
ISE API Gateway Service running 110426
Segmentation Policy Service disabled

REST Auth Service running 63052

SSE Connector disabled
```

2. Verificare che l'archivio di ID REST sia utilizzato al momento dell'autenticazione (controllare la sezione Passi. del report di autenticazione dettagliato).

15013 Selected Identity Source - Azure_AD

25103 Perform plain text password authentication in external REST ID store server - Azure_AD a.

25100 Connecting to external REST ID store server - Azure_AD b.

25101 Successfully connected to external REST ID store server - Azure_AD (🕒 Step latency=1660 ms) c.

25104 Plain text password authentication in external REST ID store server succeeded - Azure_AD d.

25107 REST ID store server respond with groups - Azure_AD e.

25110 User groups inserted to session cache - Azure_AD f.

22037 Authentication Passed

a. PSN avvia l'autenticazione in testo normale con l'archivio ID REST selezionato.

b. Connessione stabilita con Azure Cloud.

c. Fase di autenticazione effettiva: prestare attenzione al valore di latenza indicato qui. Nel caso in cui tutte le autenticazioni con Aure Cloud riducano la latenza significativa, questo influisce sull'altro flusso ISE e, di conseguenza, l'intera implementazione ISE diventa instabile.

d. Conferma dell'avvenuta autenticazione.

e. Conferma dei dati del gruppo presentati in risposta.

f. Contesto della sessione popolato con i dati dei gruppi di utenti. Per ulteriori informazioni sul processo di gestione delle sessioni ISE, si consiglia di leggere questo [link](#) all'articolo.

3. Confermare che siano selezionati i criteri di autenticazione/autorizzazione previsti (per questa sezione relativa alla panoramica dell'indagine nel rapporto di autenticazione dettagliato).

Overview

Event 5200 Authentication succeeded

Username bob

Endpoint Id ED:37:E1:08:57:15 ⊕

Endpoint Profile

Authentication Policy SPRT-Policy-Set >> Azure-AD

Authorization Policy SPRT-Policy-Set >> Azure-Finance

Authorization Result PermitAccess

Figura 30.

Risoluzione dei problemi

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

Problemi con il servizio di autenticazione REST

Per risolvere i problemi con il servizio di autenticazione REST, è necessario iniziare con la revisione del file ADE.log. Posizione dei pacchetti di supporto - /support/adeos/ade

Una parola chiave di ricerca per il servizio di autenticazione REST è - ROPC-control.

Nell'esempio viene mostrato come avviare il servizio di autenticazione REST:

```
2020-08-30T11:15:38.624197+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] S
2020-08-30T11:15:39.217794+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] i
2020-08-30T11:15:39.290301+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] I
2020-08-30T11:15:39.291858+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] D
2020-08-30T11:15:39.293768+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] L
2020-08-30T11:15:39.359490+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] E
2020-08-30T11:15:42.789242+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] L
2020-08-30T11:15:42.830411+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] D
2020-08-30T11:15:42.832131+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] S
2020-08-30T11:15:42.844051+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] i
2020-08-30T11:15:53.479968+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] C
2020-08-30T11:15:55.325973+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] C
2020-08-30T11:15:57.103245+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] C
2020-08-30T11:15:57.105752+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] C
2020-08-30T11:15:57.278374+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] C
```

Nei casi in cui il servizio non si avvia o si interrompe in modo imprevisto, è sempre opportuno rivedere il file ADE.log in un intervallo di tempo problematico.

Problemi di autenticazione ID REST

In caso di errori di autenticazione quando viene utilizzato l'archivio di ID REST, è sempre necessario iniziare da un report di autenticazione dettagliato. Nell'area Altri attributi è possibile visualizzare una sezione - RestAuthErrorMsg che contiene un errore restituito dal cloud di Azure:

```
RestAuthErrorMsg      Error Key - invalid_client | Error Description -
AADSTS7000218: The request body must contain the
following parameter: 'client_assertion' or 'client_secret'. Trace
ID: e33912ff-18af-4f81-acc9-efda91873900 Correlation ID:
519641db-a8ea-49df-85aa-ddd2b53a0c28 Timestamp:
2020-09-13 19:11:47Z | Error Codes - [7000218] | Error URI
- https://login.microsoftonline.com/error?code=7000218
```

Figura 31.

Utilizzare i file di log

In ISE 3.0, a causa dell'introduzione controllata della funzione ID REST, esegue il debug per abilitarla per impostazione predefinita. Tutti i log relativi all'ID REST sono archiviati in file ROPC che possono essere visualizzati tramite CLI:

```
skuchere-ise30-1/admin# sh logging application | i ropc
755573 Oct 04 2020 09:10:29 ropc/ropc.log
```

```
skuchere-ise30-1/admin# sh logging application ropc/ropc.log
23:49:31.449 [http-nio-9601-exec-6] DEBUG c.c.i.r.c.ROPCController - Starting ROPC auth flow
23:49:31.788 [http-nio-9601-exec-6] DEBUG c.c.i.r.u.ScimUtility - Found user and pass in the SCIM filter
```

In ISE 3.0 con la patch installata, notare che il nome del file è rest-id-store.log e non ropc.log. L'esempio di ricerca precedente funziona correttamente perché il nome della cartella non è cambiato.

Oppure, è possibile estrarre questi file dal pacchetto di supporto ISE.

Di seguito sono riportati un paio di esempi di registro che mostrano diversi scenari lavorativi e non lavorativi:

1. Errore del certificato quando il grafico di Azure non è considerato attendibile dal nodo ISE. Questo errore può essere visualizzato quando i gruppi non vengono caricati nell'impostazione

dell'archivio di ID REST.

```
20:44:54.420 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.HttpClientWrapper - Start proxy load for URI 'https
20:44:54.805 [http-nio-9601-exec-7] ERROR c.c.i.r.p.a.AzureIdentityProviderFacade - Couldn't fetch appl
javax.net.ssl.SSLHandshakeException: sun.security.validator.ValidatorException: No trusted certificate
at sun.security.ssl.Alerts.getSSLException(Alerts.java:192)
at sun.security.ssl.SSLSocketImpl.fatal(SSLSocketImpl.java:1946)
at sun.security.ssl.Handshaker.fatalSE(Handshaker.java:316)
at sun.security.ssl.Handshaker.fatalSE(Handshaker.java:310)
at sun.security.ssl.ClientHandshaker.serverCertificate(ClientHandshaker.java:1639)
```

Questo problema indica che il certificato Microsoft graph API non è considerato attendibile da ISE. In ISE 3.0.0.458 non è installata una CA radice globale DigiCert G2 nell'archivio attendibile. Ciò è documentato nel difetto

- ID bug Cisco [CSCvv80297](https://tools.cisco.com/bugcenter/bug/?bugID=CSCvv80297) Per risolvere questo problema, è necessario installare DigiCert Global Root G2 CA nell'archivio attendibile ISE e contrassegnarlo come attendibile per i servizi Cisco.

Il certificato può essere scaricato da qui - <https://www.digicert.com/kb/digicert-root-certificates.htm>

2. Segreto applicazione errato.

```
10:57:53.200 [http-nio-9601-exec-1] DEBUG c.c.i.r.e.c.CertificateCache - SSLContext initialized with tr
10:57:54.205 [http-nio-9601-exec-1] ERROR c.c.i.r.u.RestUtility - Error response in 'POST' request. Sta
10:57:54.206 [http-nio-9601-exec-1] ERROR c.c.i.r.c.ROPCController - Request related Error
com.cisco.ise.ROPC.entities.exceptions.InvalidApplicationAuthException: AADSTS7000215: Invalid client s
Trace ID: 99cc29f7-502a-4aaa-b2cf-1daeb071b900
Correlation ID: a697714b-5ab2-4bd1-8896-f9ad40d625e5
Timestamp: 2020-09-29 09:01:36Z - Error Codes: [7000215]
at com.cisco.ise.ROPC.providers.azure.AzureIdentityProviderFacade.authenticateApplication(AzureIdentity
```

3. ID APP errato.

```
21:34:36.090 [http-nio-9601-exec-4] DEBUG c.c.i.r.e.c.CertificateCache - SSLContext initialized with tr
21:34:36.878 [http-nio-9601-exec-4] ERROR c.c.i.r.u.RestUtility - Error response in 'POST' request. Sta
21:34:36.879 [http-nio-9601-exec-4] ERROR c.c.i.r.c.ROPCController - Request related Error
com.cisco.ise.ROPC.entities.exceptions.InvalidApplicationAuthException: AADSTS700016: Application with
Trace ID: 6dbd0fdd-0128-4ea8-b06a-5e78f37c0100
Correlation ID: eced0c34-fcc1-40b9-b033-70e5abe75985
Timestamp: 2020-08-31 19:38:34Z - Error Codes: [700016]
```

4. Utente non trovato.

```
10:43:01.351 [http-nio-9601-exec-2] ERROR c.c.i.r.u.RestUtility - Error response in 'POST' request. Sta
10:43:01.352 [http-nio-9601-exec-2] ERROR c.c.i.r.c.ROPCController - Request related Error
com.cisco.ise.ROPC.entities.exceptions.ROPCResponseErrorException: {"error":"invalid_grant","error_desc
at com.cisco.ise.ROPC.providers.azure.AzureIdentityProviderFacade.authenticateUser(AzureIdentityProvide
at com.cisco.ise.ROPC.providers.azure.AzureROPCFlow.authenticateUser(AzureROPCFlow.java:100)
at com.cisco.ise.ROPC.providers.azure.AzureROPCFlow.doEntireFlow(AzureROPCFlow.java:69)
at com.cisco.ise.ROPC.controllers.ROPCController.ROPCAuthFlow(ROPCController.java:168)
at com.cisco.ise.ROPC.controllers.ROPCController.get(ROPCController.java:85)
at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
at sun.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:62)
at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43)
at java.lang.reflect.Method.invoke(Method.java:498)
```

5. La password dell'utente è scaduta. In genere ciò può accadere per l'utente appena creato perché la password definita dall'amministratore di Azure deve essere modificata al momento dell'accesso a Office365.

```
10:50:55.096 [http-nio-9601-exec-4] ERROR c.c.i.r.u.RestUtility - Error response in 'POST' request. Sta
10:50:55.097 [http-nio-9601-exec-4] ERROR c.c.i.r.c.ROPCController - Request related Error
com.cisco.ise.ROPC.entities.exceptions.ROPCResponseErrorException: {"error":"invalid_grant","error_desc
at com.cisco.ise.ROPC.providers.azure.AzureIdentityProviderFacade.authenticateUser(AzureIdentityProvide
at com.cisco.ise.ROPC.providers.azure.AzureROPCFlow.authenticateUser(AzureROPCFlow.java:100)
at com.cisco.ise.ROPC.providers.azure.AzureROPCFlow.doEntireFlow(AzureROPCFlow.java:69)
at com.cisco.ise.ROPC.controllers.ROPCController.ROPCAuthFlow(ROPCController.java:168)
at com.cisco.ise.ROPC.controllers.ROPCController.get(ROPCController.java:85)
at sun.reflect.GeneratedMethodAccessor53.invoke(Unknown Source)
at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43)
at java.lang.reflect.Method.invoke(Method.java:498)
```

6. Impossibile caricare i gruppi a causa di autorizzazioni API errate.

```
12:40:06.624 [http-nio-9601-exec-9] ERROR c.c.i.r.u.RestUtility - Error response in 'GET' request. Stat
"error": {
"code": "Authorization_RequestDenied",
"message": "Insufficient privileges to complete the operation.",
"innerError": {
"date": "2020-08-30T10:43:59",
"request-id": "da458fa4-cc8a-4ae8-9720-b5370ad45297"
}
}
}'
```

7. L'autenticazione non riesce quando il ROPC non è consentito nel lato di Azure.

```
11:23:10.824 [http-nio-9601-exec-2] DEBUG c.c.i.r.e.c.CertificateCache - SSLContext initialized with tr
11:23:11.776 [http-nio-9601-exec-2] ERROR c.c.i.r.u.RestUtility - Error response in 'POST' request. Sta
11:23:11.777 [http-nio-9601-exec-2] ERROR c.c.i.r.c.ROPCController - Request related Error
com.cisco.ise.ROPC.entities.exceptions.ROPCResponseErrorException: {"error":"invalid_client","error_des
```

```
at com.cisco.ise.ROPC.providers.azure.AzureIdentityProviderFacade.authenticateUser(AzureIdentityProviderFacade.java:100)
at com.cisco.ise.ROPC.providers.azure.AzureROPCFlow.authenticateUser(AzureROPCFlow.java:100)
at com.cisco.ise.ROPC.providers.azure.AzureROPCFlow.doEntireFlow(AzureROPCFlow.java:69)
at com.cisco.ise.ROPC.controllers.ROPCController.ROPCAuthFlow(ROPCController.java:168)
at com.cisco.ise.ROPC.controllers.ROPCController.get(ROPCController.java:85)
at sun.reflect.GeneratedMethodAccessor53.invoke(Unknown Source)
at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43)
at java.lang.reflect.Method.invoke(Method.java:498)
```

8. L'autenticazione non riesce perché l'utente non appartiene ad alcun gruppo sul lato di Azure.

```
21:54:55.976 [http-nio-9601-exec-5] DEBUG c.c.i.r.e.c.CertificateCache - SSLContext initialized with tr
21:54:57.312 [http-nio-9601-exec-5] ERROR c.c.i.r.p.a.AzureROPCFlow - Missing claims in the id token: "
21:54:57.313 [http-nio-9601-exec-5] ERROR c.c.i.r.c.ROPCController - Server Error
com.cisco.ise.ROPC.entities.exceptions.JsonParseException: Json exception: Missing claims in the id tok
at com.cisco.ise.ROPC.providers.azure.AzureROPCFlow.validateIdTokenPayload(AzureROPCFlow.java:93)
```

9. Autenticazione degli utenti e recupero dei gruppi completati.

```
11:46:03.035 [http-nio-9601-exec-7] DEBUG c.c.i.r.c.ROPCController - Starting ROPC auth flow
11:46:03.037 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.ScimUtility - Found user and pass in the SCIM filter
11:46:03.037 [http-nio-9601-exec-7] DEBUG c.c.i.r.c.ROPCController - Getting the right ROPC handler for
11:46:03.037 [http-nio-9601-exec-7] DEBUG c.c.i.r.c.ROPCController - Getting user groups from handler
11:46:03.038 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.HttpClientWrapper - Start building http client
11:46:03.039 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.HttpClientWrapper - Start proxy load for URI 'https
11:46:03.039 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.HttpClientWrapper - Start check if host is bypass
11:46:03.039 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.HttpClientWrapper - Iterating bypass hosts '192.168
11:46:03.040 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.HttpClientWrapper - Proxy server found with address
11:46:03.040 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.HttpClientWrapper - Start adding proxy credentials
11:46:03.040 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.HttpClientWrapper - No credentials found for proxy
11:46:03.040 [http-nio-9601-exec-7] DEBUG c.c.i.r.e.c.CertificateCache - Created SSLContext with TLSv1.
11:46:03.041 [http-nio-9601-exec-7] DEBUG c.c.i.r.e.c.CertificateCache - SSLContext initialized with tr
11:46:04.160 [http-nio-9601-exec-7] DEBUG c.c.i.r.c.ROPCController - The ROPCHandlerResponse is: {
"schemas" : [ "urn:ietf:params:scim:schemas:core:2.0:User" ],
"userName" : "username",
"name" : {
"formatted" : "bob"
},
"displayName" : "bob",
"groups" : [ {
"value" : "17db2c79-fb87-4027-ae13-88eb5467f25b"
} ],
"roles" : [ ]
}
```

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).