

Configurazione di ISE 3.3 Native Multi-Factor Authentication con DUO

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Diagramma di flusso](#)

[Configurazioni](#)

[Seleziona applicazioni da proteggere](#)

[Integrare ISE con Active Directory](#)

[Abilita Open API](#)

[Abilita origine identità MFA](#)

[Configura origine identità esterna MFA](#)

[Registra utente in DUO](#)

[Configura set di criteri](#)

[Limitazioni](#)

[Verifica](#)

[Risoluzione dei problemi](#)

Introduzione

In questo documento viene descritto come integrare la patch 1 di Identity Services Engine (ISE) 3.3 con DUO per Multi-Factor Authentication. Dalla versione 3.3 patch 1 ISE può essere configurato per l'integrazione nativa con i servizi DUO, eliminando così la necessità di un proxy di autenticazione.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di base dei seguenti argomenti:

- ISE
- DUO

Componenti usati

Le informazioni fornite in questo documento si basano su:

- Cisco ISE versione 3.3 patch 1
- DUO
- Cisco ASA versione 9.16(4)
- Cisco Secure Client versione 5.0.04032

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

Diagramma di flusso

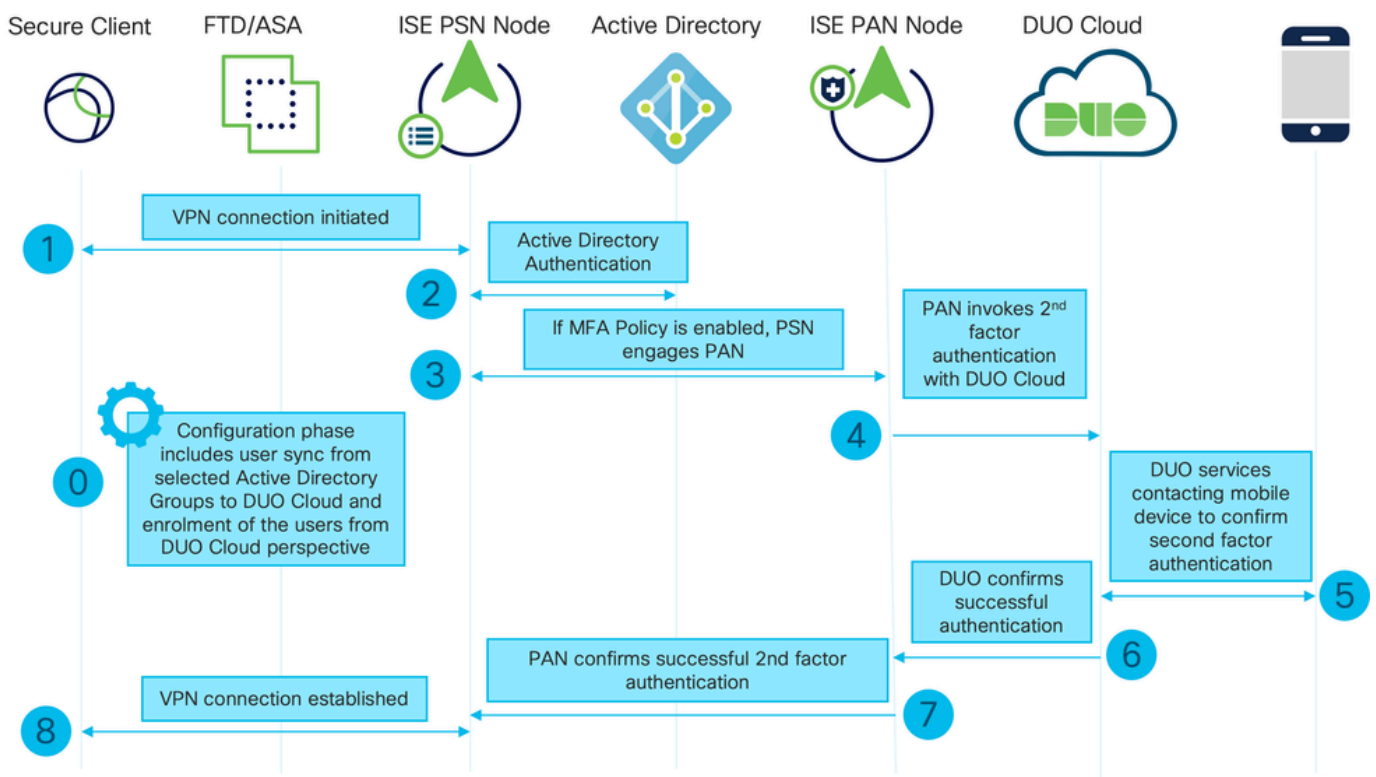


Diagramma di flusso

Passi

0. Fase di configurazione include la selezione dei gruppi di Active Directory da cui gli utenti vengono sincronizzati. La sincronizzazione viene eseguita al termine della procedura guidata di autenticazione a più fattori. Si compone di due fasi. Cerca in Active Directory per ottenere l'elenco degli utenti e di determinati attributi. Viene effettuata una chiamata a DUO Cloud con l'API Admin per spingere gli utenti in quella posizione. Gli amministratori devono registrare gli utenti. La registrazione può includere la fase opzionale di attivazione dell'utente per Duo Mobile, che consente agli utenti di utilizzare l'autenticazione one-tap con Duo Push

1. La connessione VPN viene avviata, l'utente immette il nome utente e la password e fa clic su OK. Il dispositivo di rete invia un messaggio di richiesta di accesso RADIUS a PSN

2. Il nodo PSN autentica l'utente tramite Active Directory

3. Quando l'autenticazione ha esito positivo e i criteri MFA sono configurati, il PSN avvia il PAN per contattare il cloud DUO

4. Viene effettuata una chiamata a DUO Cloud con API Auth per richiamare un'autenticazione di secondo fattore con DUO. ISE comunica con il servizio Duo sulla porta SSL TCP 443.

5. Viene eseguita l'autenticazione del secondo fattore. L'utente completa il processo di autenticazione del secondo fattore

6. DUO risponde al PAN con il risultato dell'autenticazione del secondo fattore

7. La PAN risponde al PSN con il risultato dell'autenticazione del secondo fattore

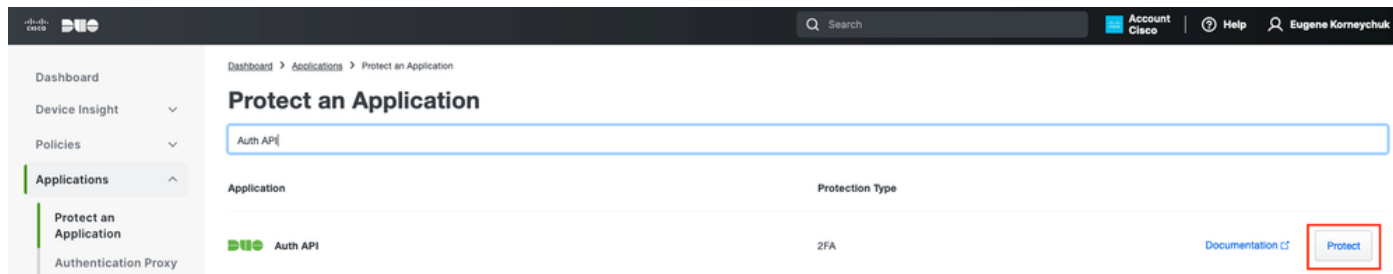
8. L'autorizzazione di accesso viene inviata al dispositivo di rete, la connessione VPN viene stabilita

Configurazioni

Seleziona applicazioni da proteggere

Passare a DUO Admin Dashboard <https://admin.duosecurity.com/login>. Eseguire l'accesso con le credenziali di amministratore.

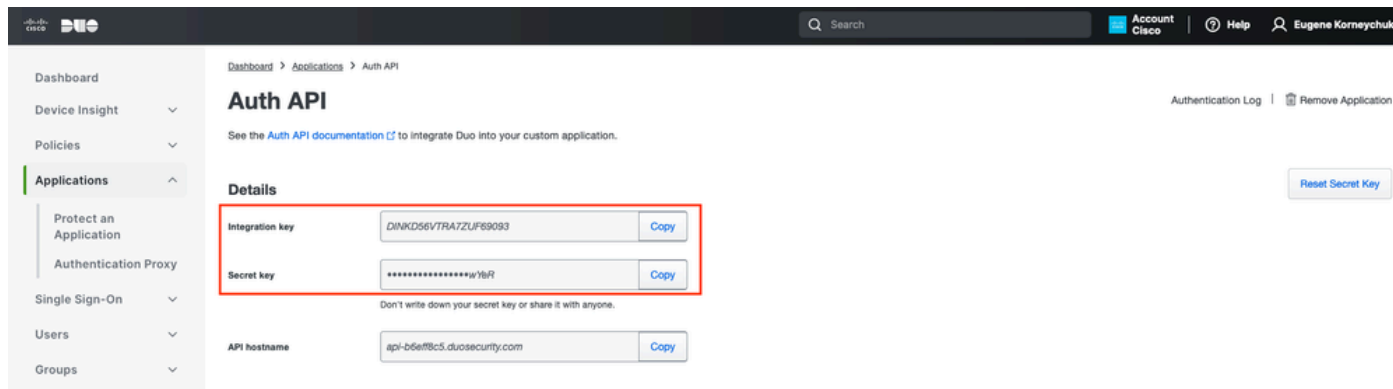
Passare a Dashboard > Applicazioni > Proteggi un'applicazione. Cercare Auth API (API di autenticazione) e selezionare Protect (Proteggi).



Application	Protection Type
Auth API	2FA

Auth API 1


Prendere nota della chiave di integrazione e della chiave segreta.

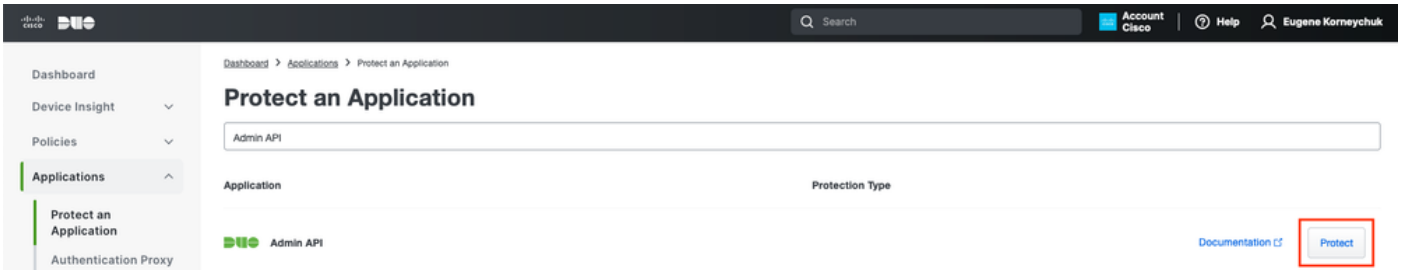


Integration key	DINKD56VTRAZUF89093	Copy
Secret key	*****u'Y8R	Copy
API hostname	api-b5e#8c5.duosecurity.com	Copy

Auth API 2

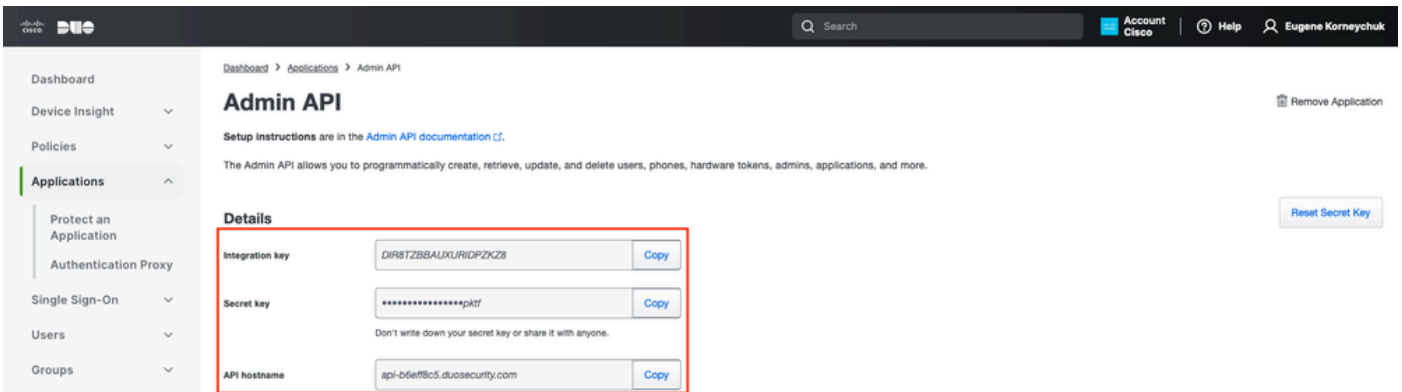
Passare a Dashboard > Applicazioni > Proteggi un'applicazione. Cercare l'API Admin e selezionare Protect (Proteggi).

 Nota: solo gli amministratori con il ruolo Proprietario possono creare o modificare un'applicazione API Admin nel pannello Duo Admin.



Auth API 1

Prendere nota della chiave di integrazione, della chiave segreta e del nome host dell'API.



API Admin 2

Configura autorizzazioni API

Passare a Dashboard > Applicazioni > Applicazione. Selezionare Admin API.

Selezionare Concedi risorsa di lettura e Concedi autorizzazioni risorsa di scrittura. Fare clic su Salva modifiche.

- Groups ▾
- Endpoints ▾
- 2FA Devices ▾
- Administrators ▾
- Trusted Endpoints
- Trust Monitor ▾
- Reports ▾
- Settings
- Billing ▾

You're using the new Admin Panel menu and left-side navigation.

[Provide feedback](#)

API hostname [Copy](#)

Settings

Type Admin API

Name

Duo Push users will see this when approving transactions.

Permissions

- Grant administrators
Permit this Admin API application to add, modify, and delete administrators and administrative units.
- Grant read information
Permit this Admin API application to read information and statistics generally used for reporting purposes.
- Grant applications
Permit this Admin API application to add, modify, and delete applications.
- Grant settings
Permit this Admin API application to read and update global account settings.
- Grant read log
Permit this Admin API application to read logs.
- Grant read resource
Permit this Admin API application to read resources such as users, phones, and hardware tokens.
- Grant write resource
Permit this Admin API application to add, modify, and delete resources such as users, phones, and hardware tokens.

API di amministrazione 3

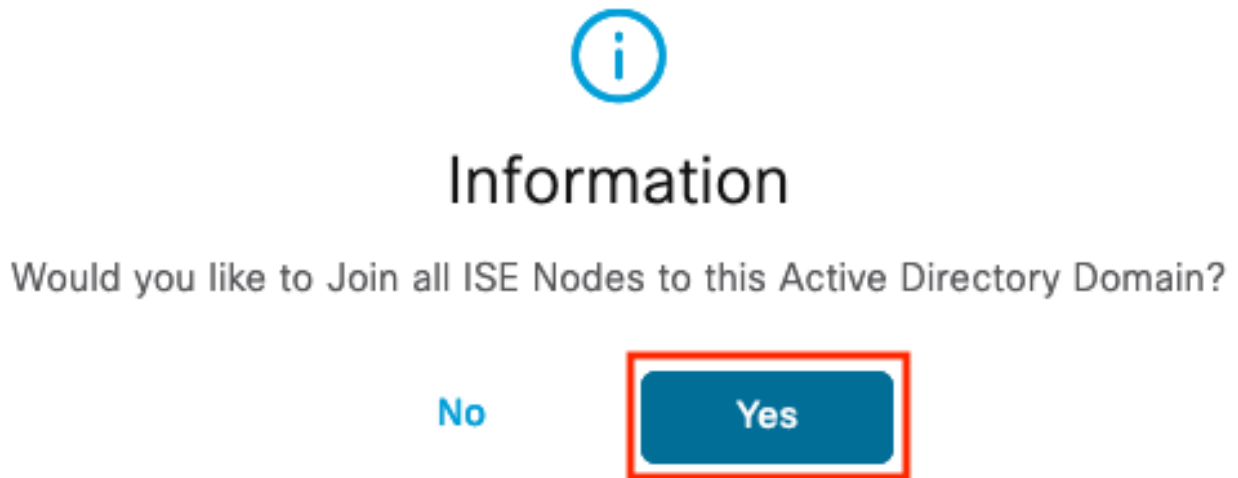
Integrare ISE con Active Directory

1. Passare a Amministrazione > Gestione delle identità > Archivi identità esterni > Active Directory > Aggiungi. Specificare il nome del punto di join, il dominio di Active Directory e fare clic su Invia.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The breadcrumb navigation is Administration / Identity Management. The main menu includes Identities, Groups, External Identity Sources (selected), Identity Source Sequences, and Settings. On the left, a tree view shows various external identity sources: Certificate Authentication, Active Directory, MFA, Identity Sync, LDAP, ODBC, RADIUS Token, RSA SecurID, SAML Id Providers, Social Login, and REST. The 'Active Directory' source is selected, and the 'Connection' configuration page is displayed. Two fields are highlighted with a red box: 'Join Point Name' with the value 'example' and 'Active Directory Domain' with the value 'example.com'. At the bottom right, there are 'Submit' and 'Cancel' buttons, with 'Submit' also highlighted by a red box.

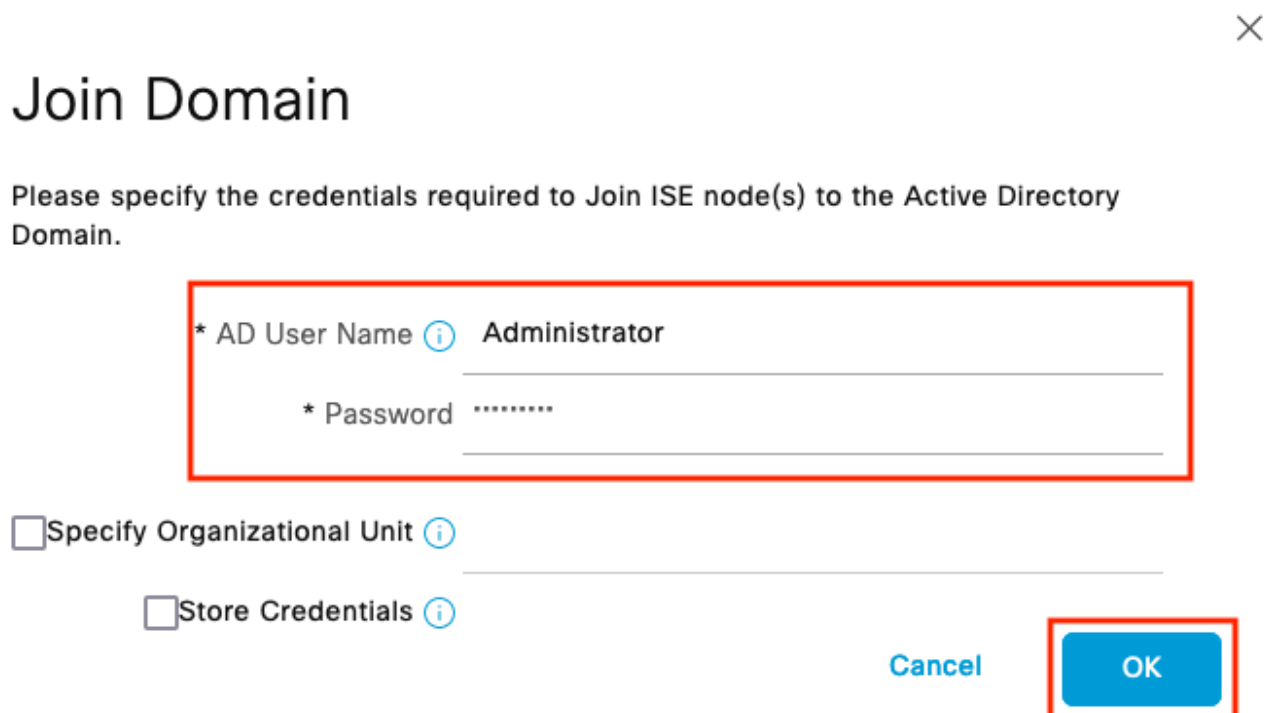
Active Directory 1

2. Quando viene richiesto di aggiungere tutti i nodi ISE a questo dominio Active Directory, fare clic su Sì.



Active Directory 2


3. Specificare il nome utente e la password di Active Directory, quindi fare clic su OK.



Active Directory 3

L'account AD richiesto per l'accesso al dominio in ISE può avere una delle seguenti caratteristiche:

- Aggiunta di workstation al diritto utente del dominio nel rispettivo dominio
- Autorizzazione Creazione oggetti computer o Eliminazione oggetti computer nei rispettivi contenitori in cui viene creato l'account del computer ISE prima che il computer venga aggiunto al dominio

 Nota: Cisco consiglia di disabilitare il criterio di blocco per l'account ISE e configurare l'infrastruttura AD in modo che invii avvisi all'amministratore se per l'account viene utilizzata una password errata. Se viene immessa una password errata, ISE non crea né modifica il proprio account computer quando necessario e quindi probabilmente nega tutte le autenticazioni.

4. Lo stato di AD è Operativo.

Connection	Allowed Domains	PassiveID	Groups	Attributes	Advanced Settings
* Join Point Name	example				i
* Active Directory Domain	example.com				i
+ Join + Leave Test User Diagnostic Tool Refresh Table					
<input type="checkbox"/>	ISE Node	ISE Node R...	Status	Domain Controller	Site
<input type="checkbox"/>	ise331.example.com	PRIMARY	<input checked="" type="checkbox"/> Operational	WIN2022.example.com	Default-First-Site-Name
<input type="checkbox"/>	ise332.example.com	SECONDARY	<input checked="" type="checkbox"/> Operational	WIN2022.example.com	Default-First-Site-Name

Active Directory 4

5. Passare a Gruppi > Aggiungi > Seleziona gruppi da directory > Recupera gruppi. Selezionare le caselle di controllo relative ai gruppi AD di propria scelta (utilizzati per sincronizzare gli utenti e per i criteri di autorizzazione), come illustrato in questa immagine.



Select Directory Groups

This dialog is used to select groups from the Directory.

Domain

Name *
Filter

SID *
Filter

Type
Filter

50 Groups Retrieved.

<input type="checkbox"/>	Name	Group SID	Group Type
<input type="checkbox"/>	example.com/Users/Cert Publishers	S-1-5-21-4068818894-3653102275-25587130...	DOMAIN LOCAL
<input type="checkbox"/>	example.com/Users/Cloneable Domain Controllers	S-1-5-21-4068818894-3653102275-25587130...	GLOBAL
<input checked="" type="checkbox"/>	example.com/Users/DUO Group	S-1-5-21-4068818894-3653102275-25587130...	GLOBAL
<input type="checkbox"/>	example.com/Users/Denied RODC Password Re...	S-1-5-21-4068818894-3653102275-25587130...	DOMAIN LOCAL
<input type="checkbox"/>	example.com/Users/DnsAdmins	S-1-5-21-4068818894-3653102275-25587130...	DOMAIN LOCAL
<input type="checkbox"/>	example.com/Users/DnsUpdateProxy	S-1-5-21-4068818894-3653102275-25587130...	GLOBAL
<input type="checkbox"/>	example.com/Users/Domain Admins	S-1-5-21-4068818894-3653102275-25587130...	GLOBAL
<input type="checkbox"/>	example.com/Users/Domain Computers	S-1-5-21-4068818894-3653102275-25587130...	GLOBAL
<input type="checkbox"/>	example.com/Users/Domain Controllers	S-1-5-21-4068818894-3653102275-25587130...	GLOBAL
<input type="checkbox"/>	example.com/Users/Domain Guests	S-1-5-21-4068818894-3653102275-25587130...	GLOBAL
<input type="checkbox"/>	example.com/Users/Domain Users	S-1-5-21-4068818894-3653102275-25587130...	GLOBAL
<input type="checkbox"/>	example.com/Users/Enterprise Admins	S-1-5-21-4068818894-3653102275-25587130...	UNIVERSAL

Cancel

Active Directory 5

6. Fare clic su Salva per salvare i gruppi AD recuperati.

Connection		Allowed Domains	PassiveID	Groups	Attributes	Advanced Settings
Edit + Add Delete Group Update SID Values						
<input type="checkbox"/>	Name	SID				
<input type="checkbox"/>	example.com/Users/DUO Group	S-1-5-21-4068818894-3653102275-2558713077-...				

Save **Reset**

Active Directory 6

Abilita Open API

Selezionare Amministrazione > Sistema > Impostazioni > Impostazioni API > Impostazioni servizio API. Abilitare Open API e fare clic su Save (Salva).

The screenshot shows the 'Identity Services Engine' Administration / System interface. The 'Settings' tab is active, and the 'API Settings' section is expanded. Under 'API Service Settings for Primary Administration Node', the 'Open API (Read/Write)' toggle is turned on and highlighted with a red box. Other settings include 'ERS (Read/Write)', 'ERS (Read)', and 'Open API (Read)'. Under 'API Service Setting for All Other Nodes', 'ERS (Read)' and 'Open API (Read)' are also visible. A 'CSRF Check' section is also present with two radio button options.

API aperta

Abilita origine identità MFA

Passare a Amministrazione > Gestione identità > Impostazioni > Impostazioni origini identità esterne. Abilitare MFA e fare clic su Salva.

Identity Services Engine Administration / Identity Management

External Identity Sources Settings

REST ID Store

To allow integration of REST identity stores with Cisco ISE, click the radio button below. It takes a few minutes to enable the REST ID Store settings. After the settings are enabled, you can add REST ID stores to Cisco ISE in the [External Identity Source](#) page.

NOTE: ISE integration with Azure AD is released as a Controlled Introduction feature and should be thoroughly tested before being used in production environment.

REST ID Store

Multi-Factor Authentication ^{BETA}

To allow the integration of Multi-Factor Authentication providers with Cisco ISE, click the MFA button.

MFA

Cancel

ISE MFA 1

Configura origine identità esterna MFA

Passare a Amministrazione > Gestione delle identità > Origini identità esterne. Fare clic su Add. Nella schermata iniziale fare clic su Let's Do It.

Identity Services Engine Add External Connector

1 Welcome 2 Connector Definition 3 Account Configurations 4 Identity Sync 5 AD Groups 6 Summary

Welcome

This wizard takes you through setting up a connection between your Duo Account and Cisco ISE to enable seamless Multi-Factor Authentication workflows.

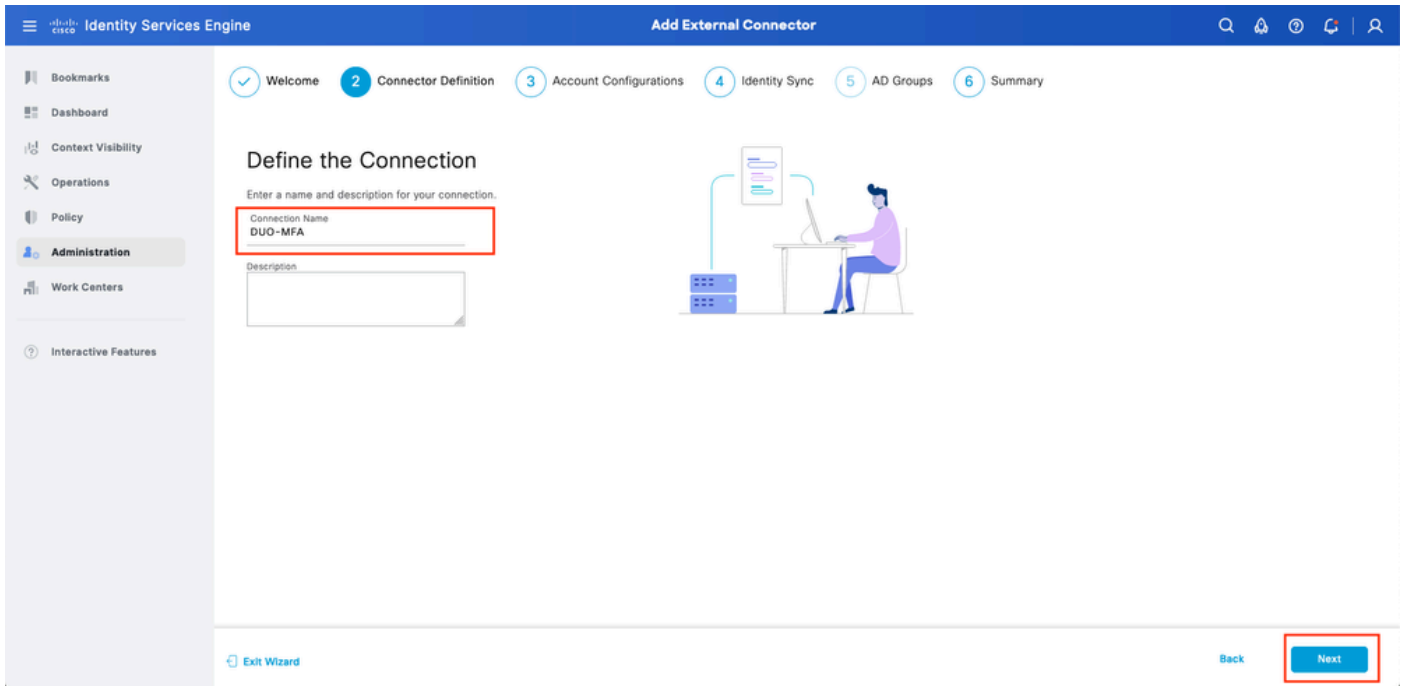
Before you begin, the following prerequisites apply:

1. Cisco ISE Advantage licenses are required.
2. The Cisco Duo license that enables MFA usage is required.
3. In your Duo portal, create a protected application that is enabled for Admin API and Authentication API usage.
4. Grant read/write access to Admin API.
5. Ensure your ISE has a stable connection to Duo (Either through direct internet or proxy).
6. For this application, note the integration keys (ikey), secret keys (skey) and API hostname values for the Admin and Authentication APIs. These values are required in the next steps of this setup wizard.

Exit Wizard

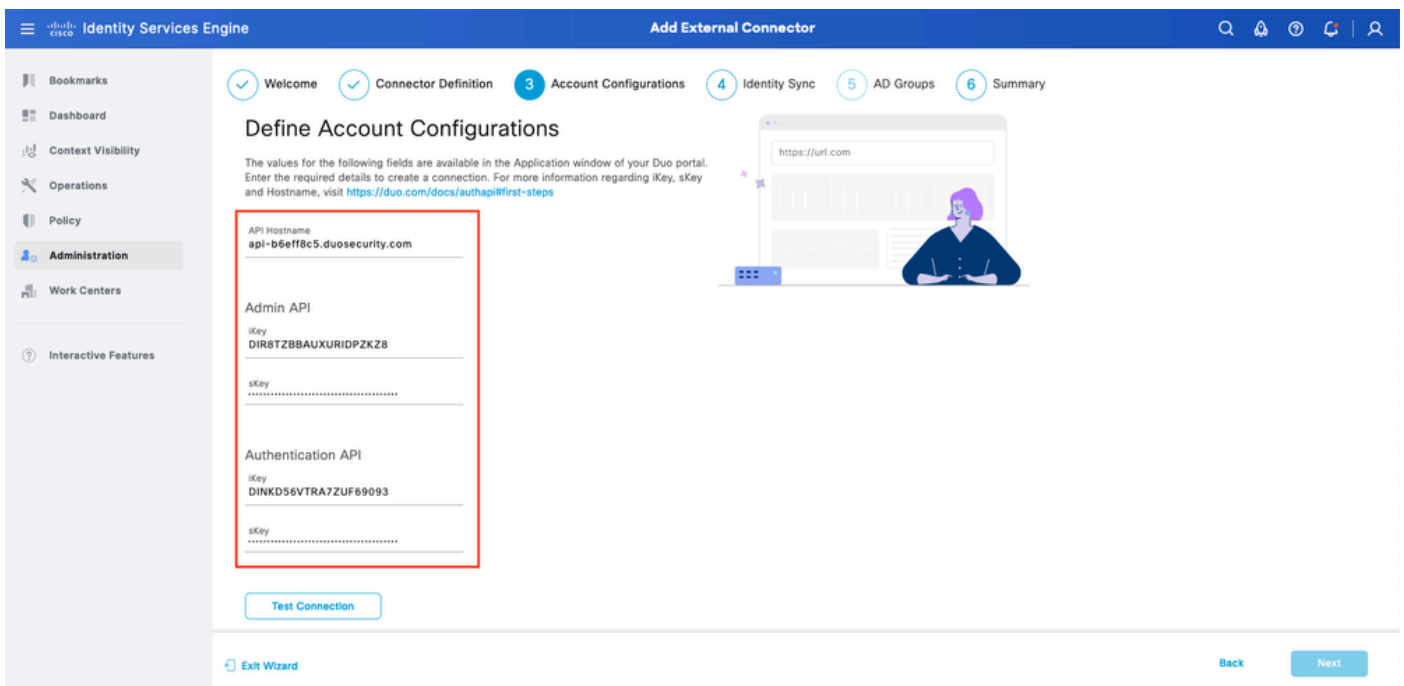
Procedura guidata ISE DUO 1

Nella schermata successiva configurare Connection Name (Nome connessione) e fare clic su Next (Avanti).



Procedura guidata ISE DUO 2

Configurare i valori di API Hostname, Admin API Integration and Secret Keys, Auth API Integration e Secret Keys da Select Applications to Protect step.



Procedura guidata ISE DUO 3

Fare clic su Test connessione. Una volta completata la verifica della connessione, fare clic su Avanti.

Test Connection

MFA Auth and Admin API Integration and Secret Keys are valid


[Exit Wizard](#)

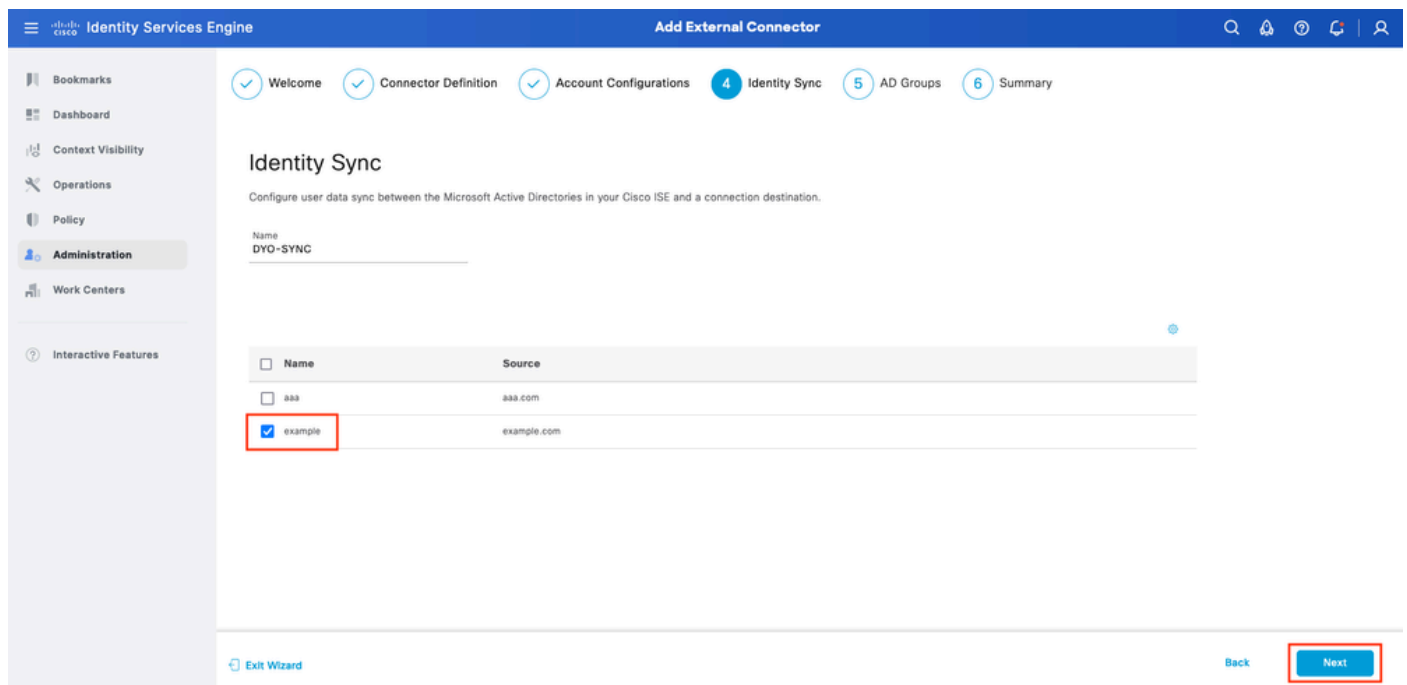
[Back](#)

Next

Procedura guidata ISE DUO 4

Configura sincronizzazione identità. Questo processo sincronizza gli utenti dai gruppi di Active Directory selezionati in Account DUO utilizzando le credenziali API fornite in precedenza. Selezionare Punto di join di Active Directory. Fare clic su Next (Avanti).

 **Nota:** la configurazione di Active Directory non rientra nell'ambito del documento. Seguire questo [documento](#) per integrare ISE con Active Directory.



Identity Sync

Configure user data sync between the Microsoft Active Directories in your Cisco ISE and a connection destination.

Name
DYO-SYNC

<input type="checkbox"/>	Name	Source
<input type="checkbox"/>	aaa	aaa.com
<input checked="" type="checkbox"/>	example	example.com

Procedura guidata ISE DUO 5

Selezionare Gruppi di Active Directory da cui si desidera sincronizzare gli utenti con DUO. Fare clic su Next (Avanti).

Identity Services Engine Add External Connector

Welcome Connector Definition Account Configurations Identity Sync **5** AD Groups 6 Summary

Select Groups from Active Directory

Select the groups that you need to sync between Cisco ISE and Duo. Edit an existing AD group from the following list, or add a new AD group in the [Active Directory](#) window and then refresh this window.

<input type="checkbox"/> Name	Source
<input checked="" type="checkbox"/> example.com/Users/DUO Group	example
<input type="checkbox"/> example.com/Builtin/Administrators	example

Exit Wizard Back **Next**

Procedura guidata ISE DUO 6

Verificare che le impostazioni siano corrette e fare clic su Done (Fine).

Identity Services Engine Add External Connector

Welcome Connector Definition Account Configurations Identity Sync AD Groups **6** Summary

Summary

Connector Definition [Edit](#)

Connection Name: DUO-MFA
VPN
TACACS

Define Account Configurations [Edit](#)

API Hostname: api-b6eff8c5.duosecurity.com
Authentication API
iKey: DIR8TZBBAUXURIDPZKZ8
sKey: *****
Admin API
iKey: DINKD56VTRA7ZUF69093
sKey: *****
Authentication: MFA Auth and Admin API Integration and Secret Keys are valid

Identity Sync [Edit](#)

Exit Wizard Back **Done**

Procedura guidata ISE DUO 7

Registra utente in DUO



Nota: la registrazione utente DUO non rientra nell'ambito del documento. Per ulteriori informazioni sulla registrazione degli utenti, consultare il [documento](#). Ai fini del presente documento, viene utilizzata la registrazione utente manuale.

Aprire DUO Admin Dashboard. Passare a Dashboard > Utenti. Fare clic sull'utente sincronizzato

da ISE.

Dashboard > Users

Users

Directory Sync | Import Users | Bulk Enroll Users [Add User](#)

Need to activate a replacement phone? [Learn more about Reactivating Duo Mobile](#).

2 Total Users **1** Not Enrolled **1** Inactive Users **0** Trash **0** Bypass Users **0** Locked Out

Select (0) ... [Export](#) Search

<input type="checkbox"/>	Username	Name	Email	Phones	Tokens	Status	Last Login
<input type="checkbox"/>	alice	alice	alice@wonderland.com	1		Active	Nov 14, 2023 1:43 AM
<input type="checkbox"/>	bob	bob				Active	Never authenticated

2 total

Registrazione DUO 1

Scorri fino ai telefoni. Fai clic su Aggiungi telefono.

Phones

You may rearrange the phones by dragging and dropping in the table. [Learn more about activating a replacement phone](#).

This user has no phones. [Add one.](#) [Add Phone](#)

Registrazione DUO 2

Immettere il numero di telefono e fare clic su Aggiungi telefono.

Configura set di criteri

1. Configurare i criteri di autenticazione

Passare a Criterio > Set di criteri. Selezionare il set di criteri per il quale si desidera abilitare l'autenticazione a più fattori. Configurare i criteri di autenticazione con l'archivio identità di autenticazione primario come Active Directory.

Status	Rule Name	Conditions	Use	Hits	Actions
ON	MAB	OR Wired_MAB Wireless_MAB	Internal Endpoints > Options	0	⚙️
ON	Dot1X	OR Wired_802.1X Wireless_802.1X	All_User_ID_Stores > Options	1	⚙️
ON	DUO Authentication	Radius-NAS-Port-Type EQUALS Virtual	example > Options	7	⚙️
ON	Default		All_User_ID_Stores > Options	7	⚙️


Set di criteri 1

2. Configurare i criteri MFA

Una volta che l'autenticazione a più fattori è stata abilitata su ISE, è disponibile una nuova sezione in ISE Policy Sets. Espandere Politica di assistenza macrofinanziaria e fare clic su + per aggiungere la Politica di assistenza macrofinanziaria. Configurare le condizioni MFA a scelta, selezionare DUO-MFA configurato in precedenza nella sezione Uso. Fare clic su Save.

The screenshot shows the Cisco Identity Services Engine (ISE) interface for configuring Policy Sets. The main content area displays a table of Policy Sets under the 'Default' policy set. A red box highlights a specific policy set named 'DUO Rule' with the condition 'Cisco-VPN3000-CVPN3000/ASA/PIX7x-Tunnel-Group-Name EQUALS RA'. The 'Use' column for this rule is set to 'DUO-MFA' and has an 'Options' dropdown menu. A 'Save' button is highlighted in the bottom right corner.

Policy ISE

 Nota: i criteri configurati in precedenza si basano sul gruppo di tunnel denominato RA. Gli utenti connessi al gruppo di tunnel RA sono obbligati a eseguire l'autenticazione a più fattori. La configurazione ASA/FTD non rientra nell'ambito di questo documento. Utilizzare questo [documento](#) per configurare ASA/FTD

3. Configurare i criteri di autorizzazione

Configurare i criteri di autorizzazione con la condizione e le autorizzazioni del gruppo di Active Directory desiderate.

The screenshot shows the Cisco Identity Services Engine (ISE) interface for configuring Authorization Policies. The main content area displays a table of Authorization Policies under the 'Authorization Policy(16)' policy set. A red box highlights a specific authorization policy named 'DUO Authorization Rule' with the condition 'example-ExternalGroups EQUALS example.com/Users/DUO Group' and the result 'PermitAccess'. A 'Save' button is highlighted in the bottom right corner.

Set di criteri 3

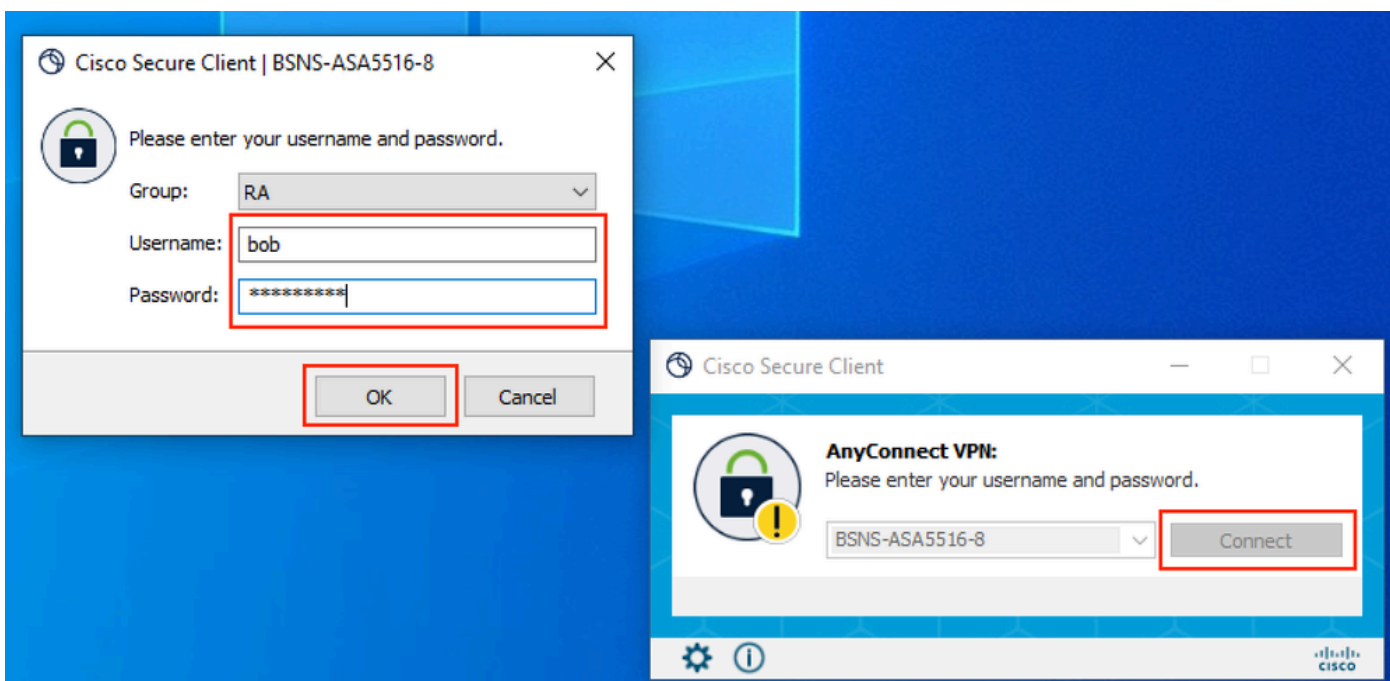
Limitazioni

Al momento della stesura del presente documento:

1. Come metodo di autenticazione di secondo fattore sono supportati solo il push DUO e il telefono
2. Non viene eseguito il push di alcun gruppo al cloud DUO. È supportata solo la sincronizzazione utente
3. Sono supportati solo i seguenti casi di utilizzo dell'autenticazione a più fattori:
 - autenticazione utente VPN
 - Autenticazione accesso amministratore TACACS+

Verifica

Aprire Cisco Secure Client, fare clic su Connect (Connetti). Specificare Nome utente e Password e fare clic su OK.



Client VPN

Gli utenti del dispositivo mobile devono ricevere una notifica Push DUO. Approvare. Connessione VPN stabilita.

1:52



Search

Accounts (8)

Add



Cisco
Cisco



Are you logging in to Auth API?

🌐 Cisco

🕒 1:52 PM

👤 bob

Registri correlati a AMF	motore delle regole	ise-psc.log	DuoMfaAuthApiUtils -::::- Richiesta inviata a Duo Client Manager DuoMfaAuthApiUtils —> Risposta Duo
Registri correlati ai criteri	prrt-JNI	port-management.log	ProcessoreRichiestaCriterioMfaRadius ProcessoreRichiestaCriteriMfaTACACS
Log relativi all'autenticazione	runtime-AAA	port-server.log	MfaAuthenticator::suAuthenticateEvent MfaAuthenticator::sendAuthenticateEvent MfaAuthenticator::onResponseEvaluatePolicyEvent
Autenticazione DUO, registri correlati a sincronizzazione ID		duo-sync-service.log	

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).