

Configurazione di Duo Two Factor Authentication per l'accesso alla gestione ISE

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Esempio di rete](#)

[Configurazione](#)

[Duo](#)

[Configurazione di ISE](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come configurare l'autenticazione a due fattori esterna per l'accesso alla gestione di Identity Services Engine (ISE). Nell'esempio, l'amministratore ISE esegue l'autenticazione sul token server RADIUS e un'ulteriore autenticazione sotto forma di notifica push viene inviata dal server proxy di autenticazione Duo al dispositivo mobile dell'amministratore.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Protocollo RADIUS
- Configurazione del server token ISE RADIUS e delle identità

Componenti usati

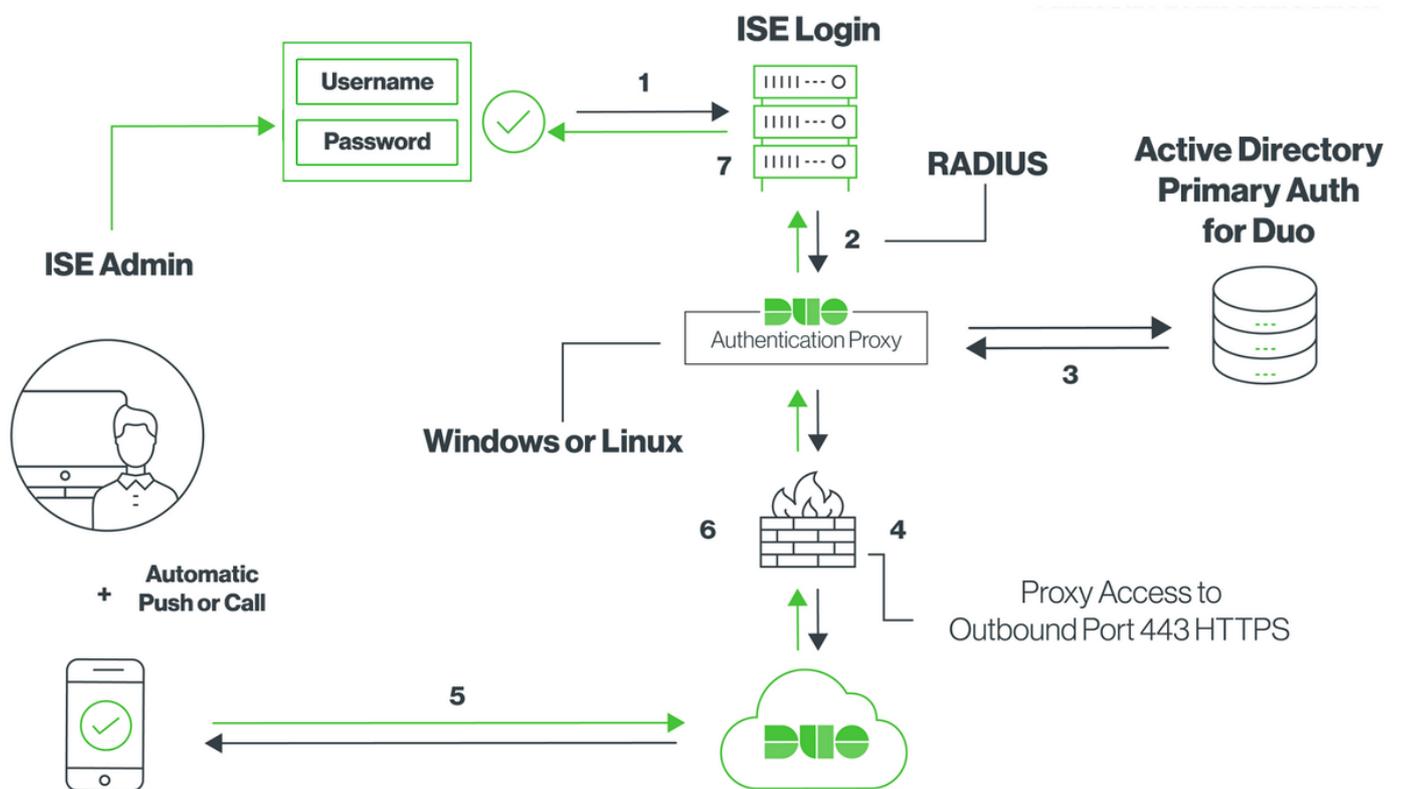
Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Identity Services Engine (ISE)
- Active Directory (AD)
- Duo Authentication Proxy Server
- Duo Cloud Service

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.

Esempio di rete



Configurazione

Duo

Passaggio 1. Scaricare e installare Duo Authentication Proxy Server in un computer Windows o Linux: <https://duo.com/docs/ciscoise-radius#install-the-duo-authentication-proxy>

Nota: Questo computer deve avere accesso ad ISE e Duo Cloud (Internet)

Passaggio 2. Configurare il file `authproxy.cfg`.

Aprire il file in un editor di testo quale Blocco note++ o WordPad.

Nota: il percorso predefinito si trova in `C:\Program Files (x86)\Duo Security Authentication Proxy\conf\authproxy.cfg`

Passaggio 3. Creare un'applicazione "Cisco ISE RADIUS" nel pannello Duo Admin: <https://duo.com/docs/ciscoise-radius#first-steps>

Passaggio 4. Modificare il file `authproxy.cfg` e aggiungere questa configurazione.

```

ikey= xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
skey= xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
api_host=api-xxxxxxx.duosecurity.com
radius_ip_1=10.127.196.189
radius_secret_1=*****
failmode=secure
client=ad_client
port=1812

```

Sample IP address of the ISE server

Passaggio 5. Configurare ad_client con i dettagli di Active Directory. Duo Auth Proxy utilizza le informazioni seguenti per l'autenticazione con AD per l'autenticazione primaria.

```

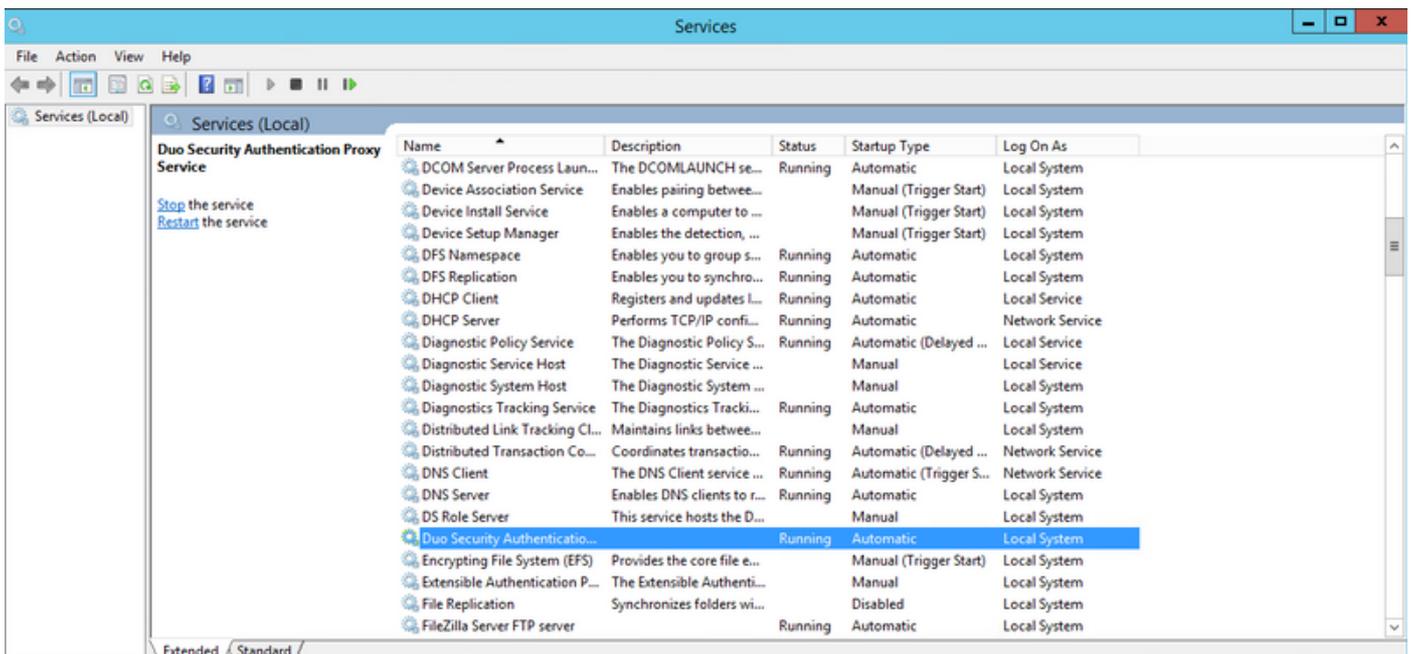
[ad_client]
host=10.127.196.230
service_account_username=< AD-username >
service_account_password=< AD-password >
search_dn=CN=Users,DC=gce,DC=iselab,DC=local

```

Sample IP address of the Active Directory

Nota: Se la rete richiede una connessione proxy HTTP per l'accesso a Internet, aggiungere i dettagli http_proxy in authproxy.cfg.

Passaggio 6. Riavviare il servizio Duo Security Authentication Proxy. Salvare il file e riavviare il servizio Duo sul computer Windows. Aprire la console dei servizi di Windows (services.msc), individuare il servizio Duo Security Authentication Proxy nell'elenco dei servizi e fare clic su Riavvia come mostrato nell'immagine:



Passaggio 7. Creare un nome utente e attivare Duo Mobile sul dispositivo terminale:

<https://duo.com/docs/administration-users#creating-users-manually>

Aggiungere l'utente al pannello di amministrazione Duo. Passare a **Utenti > aggiungi utenti**, come mostrato nell'immagine:

The screenshot shows the Duo Admin console interface. On the left is a dark sidebar with navigation options: Dashboard, Policies, Applications, Users (highlighted), Add User (highlighted), Pending Enrollments, Bulk Enroll Users, Import Users, Directory Sync, Bypass Codes, 2FA Devices, Groups, Administrators, and Reports. The main content area has a search bar at the top with the text "Search for users, groups, applications, or devices". Below it is a breadcrumb trail: Dashboard > Users > Add User. The main heading is "Add User". A section titled "Adding Users" contains the text "Most applications allow users to enroll themselves after they complete primary authentication." and a link "Learn more about adding users". Below this is a form with a "Username" label and a text input field containing "duoadmin". A note below the field says "Should match the primary authentication username." At the bottom of the form is a blue "Add User" button.

Assicurarsi che l'utente finale abbia l'app Duo installata sul telefono.

The screenshot shows the "Phones" section of the Duo Admin console. It features a heading "Phones" and a sub-heading "You may rearrange the phones by dragging and dropping in the table." On the right side, there is a blue "Add Phone" button. Below the text is a large empty box with the message "This user has no phones. [Add one.](#)"

The screenshot shows the Duo Admin console interface for adding a phone. The sidebar is the same as in the previous image, but "Users" is highlighted and "Add User" is selected. The main content area has a search bar at the top with the text "Search for users, groups, applications, or devices". Below it is a breadcrumb trail: Dashboard > Users > duoadmin > Add Phone. The main heading is "Add Phone". Under the heading, there is a "Type" section with two radio buttons: "Phone" (selected) and "Tablet". Below this is a form with a "Phone number" label and a text input field containing "+1 201-555-5555". To the right of the field is a link "Show extension field". At the bottom of the form is a blue "Add Phone" button.

Selezionare **Activate Duo Mobile**, come mostrato nell'immagine:

Device Info



Not using Duo Mobile
[Activate Duo Mobile](#)

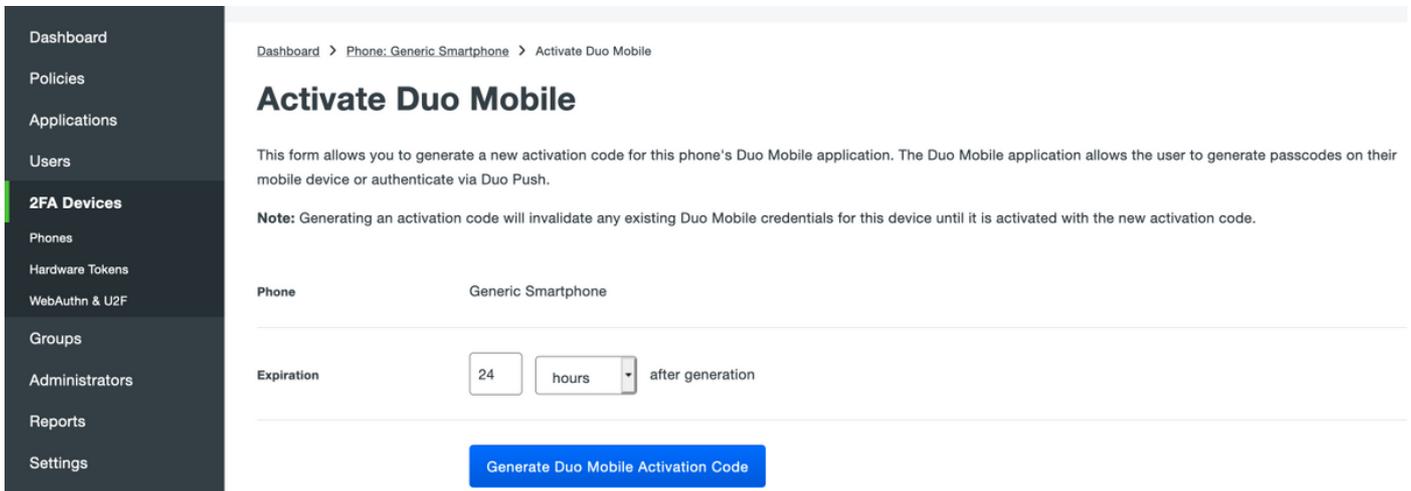


Model
Unknown



OS
Generic Smartphone

Selezionare **Generate Duo Mobile Activation Code**, come mostrato nell'immagine:



Dashboard > Phone: Generic Smartphone > Activate Duo Mobile

Activate Duo Mobile

This form allows you to generate a new activation code for this phone's Duo Mobile application. The Duo Mobile application allows the user to generate passcodes on their mobile device or authenticate via Duo Push.

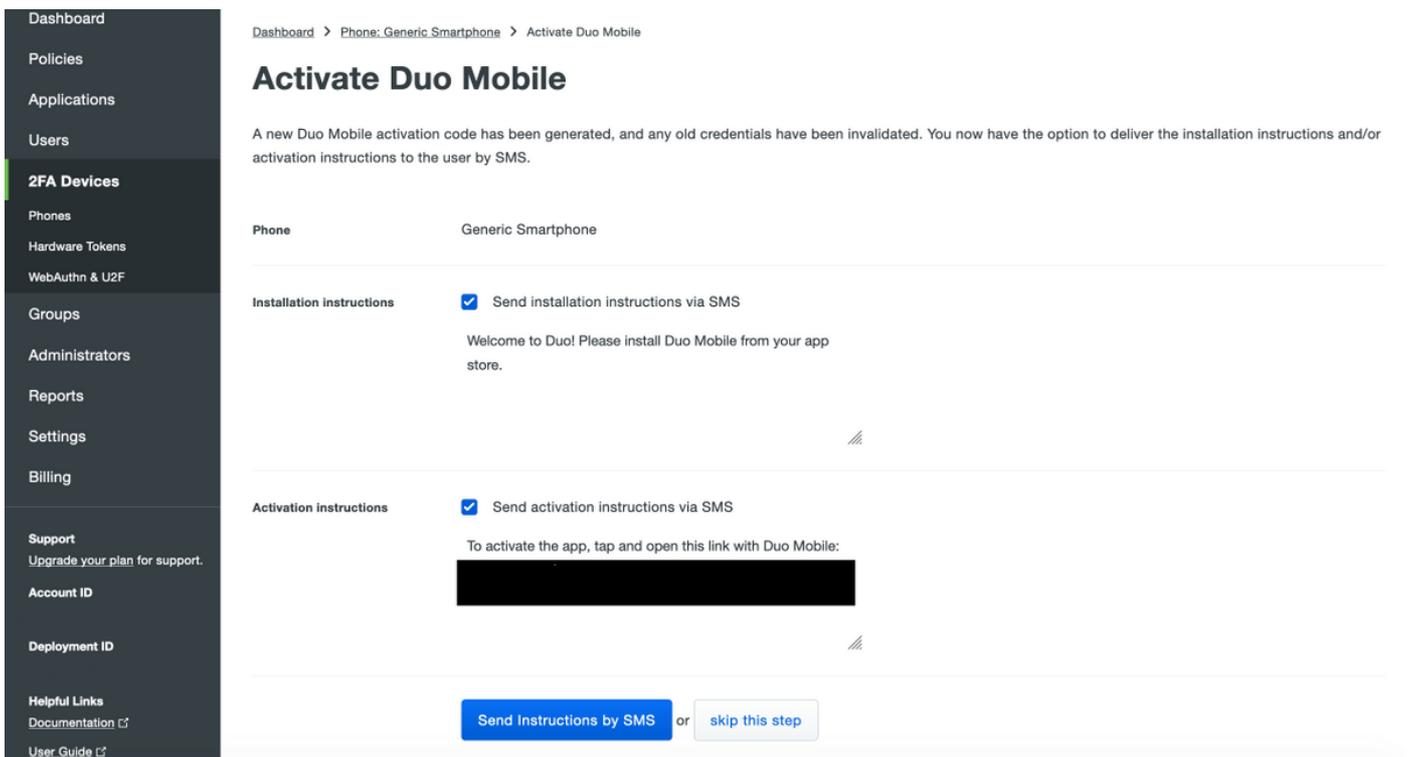
Note: Generating an activation code will invalidate any existing Duo Mobile credentials for this device until it is activated with the new activation code.

Phone: Generic Smartphone

Expiration: 24 hours after generation

[Generate Duo Mobile Activation Code](#)

Selezionare **Send Instructions by SMS (Invia istruzioni tramite SMS)**, come mostrato nell'immagine:



Dashboard > Phone: Generic Smartphone > Activate Duo Mobile

Activate Duo Mobile

A new Duo Mobile activation code has been generated, and any old credentials have been invalidated. You now have the option to deliver the installation instructions and/or activation instructions to the user by SMS.

Phone: Generic Smartphone

Installation instructions Send installation instructions via SMS

Welcome to Duo! Please install Duo Mobile from your app store.

Activation instructions Send activation instructions via SMS

To activate the app, tap and open this link with Duo Mobile:

[Redacted Link]

[Send Instructions by SMS](#) or [skip this step](#)

Fare clic sul collegamento nell'SMS e l'app Duo viene collegata all'account utente nella sezione **Informazioni dispositivo**, come mostrato nell'immagine:

The screenshot shows the Cisco Duo user interface. On the left is a dark sidebar with navigation options: Dashboard, Policies, Applications, Users, **2FA Devices** (highlighted), Phones, Hardware Tokens, WebAuthn & U2F, Groups, Administrators, Reports, Settings, and Billing. The main content area has a search bar at the top with the text "Search for users, groups, applications, or devices". Below the search bar is a breadcrumb trail: "Dashboard > Phones > Phone: [redacted]". A "Send SMS" button is visible on the right. The user profile section shows a green person icon, the name "duoadmin (NANCY)", and a blue link "Attach a user". Below this is the text "Authentication devices can share multiple users". The "Device Info" section shows a Duo Mobile 3.28.0 device with a "Reactivate Duo Mobile" link, a "Last Seen" timestamp of "29 minutes ago", a "Model" field with a redacted value, and an "OS" field showing "Android 8.0.0".

Configurazione di ISE

Passaggio 1. Integrare ISE con Duo Auth Proxy.

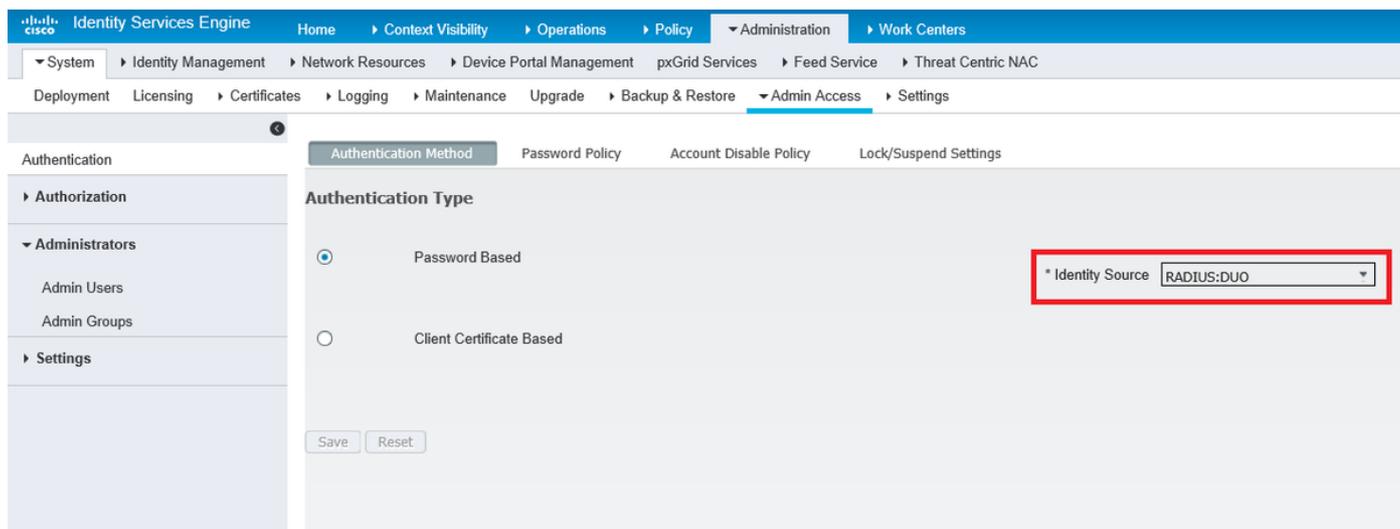
Selezionare **Amministrazione > Gestione delle identità > Origini identità esterne > Token RADIUS**, quindi fare clic su **Aggiungi** per aggiungere un nuovo server token RADIUS. Definire il nome del server nella scheda Generale, l'indirizzo IP e la chiave condivisa nella scheda Connessione, come mostrato nell'immagine:

Nota: Impostare il timeout del server su 60 secondi in modo che gli utenti dispongano di tempo sufficiente per eseguire il push

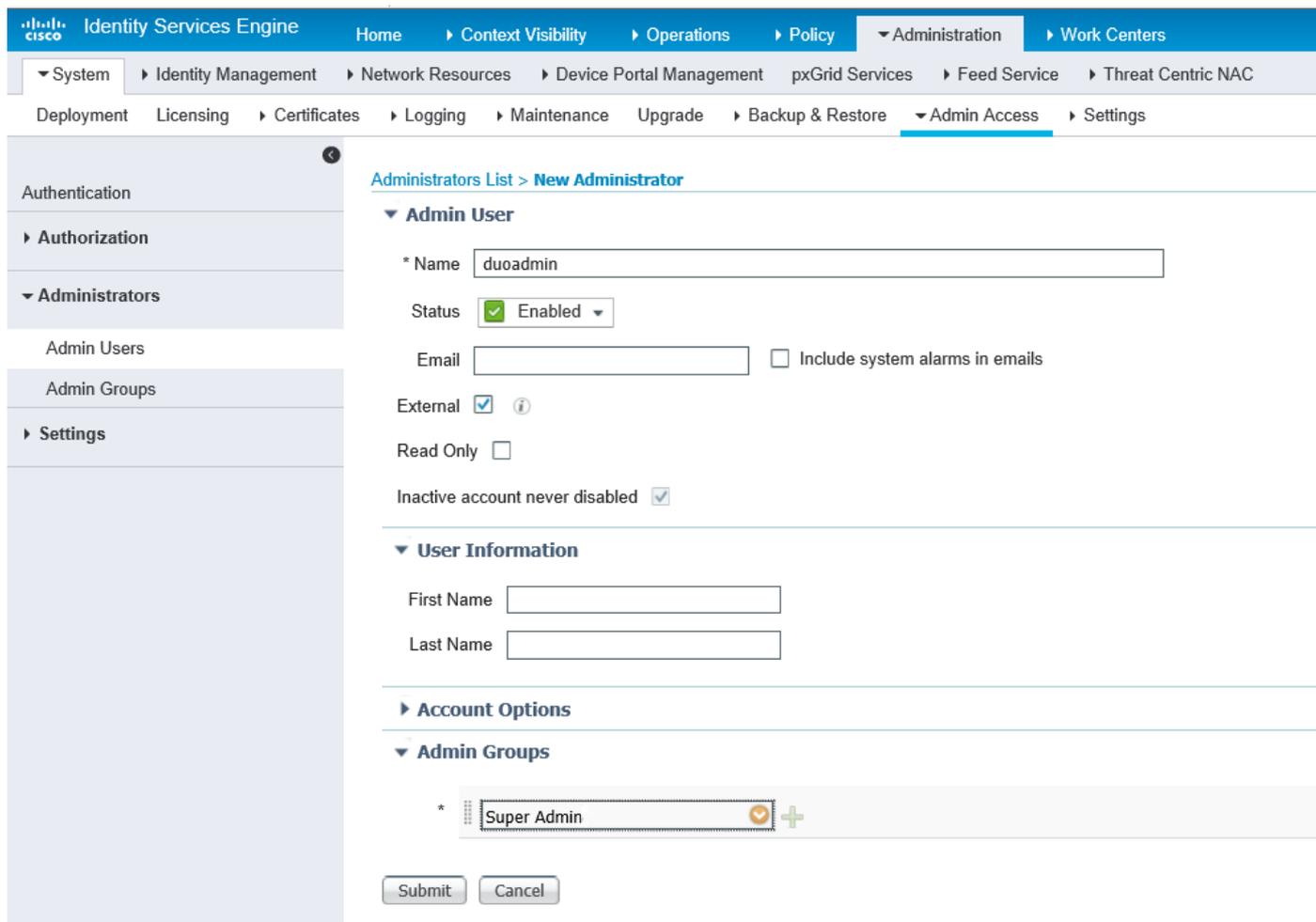
The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface. The top navigation bar includes "Identity Services Engine" and various tabs like "Home", "Context Visibility", "Operations", "Policy", "Administration", and "Work Centers". The left sidebar shows a tree view of "External Identity Sources" with categories like "Certificate Authentication Profile", "Active Directory", "RADIUS Token", and "Social Login". The main content area is titled "RADIUS Token List > DUO" and "RADIUS Token Identity Sources". It has four tabs: "General", "Connection", "Authentication", and "Authorization". The "Connection" tab is active, showing "Server Connection" options: "Safeword Server" (unchecked), "Enable Secondary Server" (unchecked), and "Always Access Primary Server First" (selected). Below this is a "Fallback to Primary Server after" field set to "5" minutes. The "Primary Server" section includes fields for "Host IP" (10.127.196.230), "Shared Secret" (masked), "Authentication Port" (1812), "Server Timeout" (60 seconds), and "Connection Attempts" (3). The "Secondary Server" section has similar fields for "Host IP", "Shared Secret", "Authentication Port" (1812), "Server Timeout" (5 seconds), and "Connection Attempts" (3). "Save" and "Reset" buttons are at the bottom.

Passaggio 2. Passare a **Amministrazione > Sistema > Accesso amministratore > Autenticazione > Metodo di autenticazione** e selezionare il server token RADIUS configurato in precedenza come

origine identità, come mostrato nell'immagine:



Passaggio 3. Passare a **Amministrazione > Sistema > Accesso amministratore > Amministratori > Amministratore utenti** e Creare un utente amministratore come esterno e fornire il privilegio di amministratore privilegiato, come mostrato nell'immagine:



Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

Aprire la GUI di ISE, selezionare RADIUS Token Server come Identity Source e accedere con

l'utente admin.



Identity Services Engine

Username

Password

Identity Source



[Problem logging in?](#)

Risoluzione dei problemi

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

Per risolvere i problemi relativi alla connettività del proxy Duo con il cloud o Active Directory, abilitare il debug sul proxy di autenticazione Duo aggiungendo "debug=true" nella sezione principale di authproxy.cfg.

I registri si trovano nel percorso seguente:

C:\Program Files (x86)\Duo Security Authentication Proxy\log

Aprire il file **authproxy.log** in un editor di testo quale Blocco note++ o WordPad.

Registra frammenti di Duo Auth Proxy che ricevono la richiesta da ISE e la inviano a Duo Cloud.

```
2019-08-19T04:59:27-0700 [DuoForwardServer (UDP)] Sending request from 10.127.196.189 to
radius_server_auto
2019-08-19T04:59:27-0700 [DuoForwardServer (UDP)] Received new request id 2 from
('10.127.196.189', 62001)
2019-08-19T04:59:27-0700 [DuoForwardServer (UDP)] (('10.127.196.189', 62001), duoadmin, 2):
login attempt for username u'duoadmin'
```

2019-08-19T04:59:27-0700 [DuoForwardServer (UDP)] **Sending AD authentication request for 'duoadmin' to '10.127.196.230'**

2019-08-19T04:59:27-0700 [duoauthproxy.modules.ad_client._ADAuthClientFactory#info] Starting factory

Frammenti di registro del proxy di autenticazione Duo non in grado di raggiungere Duo Cloud.

2019-08-19T04:59:27-0700 [duoauthproxy.modules.ad_client._ADAuthClientFactory#info] Stopping factory

2019-08-19T04:59:37-0700 [-] Duo preauth call failed

Traceback (most recent call last):

File "twisted\internet\defer.pyc", line 654, in _runCallbacks

File "twisted\internet\defer.pyc", line 1475, in getResult

File "twisted\internet\defer.pyc", line 1416, in _inlineCallbacks

File "twisted\python\failure.pyc", line 512, in throwExceptionIntoGenerator

File "duoauthproxy\lib\radius\duo_server.pyc", line 111, in preauth

File "twisted\internet\defer.pyc", line 1416, in _inlineCallbacks

File "twisted\python\failure.pyc", line 512, in throwExceptionIntoGenerator

File "duoauthproxy\lib\duo_async.pyc", line 246, in preauth

File "twisted\internet\defer.pyc", line 1416, in _inlineCallbacks

File "twisted\python\failure.pyc", line 512, in throwExceptionIntoGenerator

File "duoauthproxy\lib\duo_async.pyc", line 202, in call

File "twisted\internet\defer.pyc", line 654, in _runCallbacks

File "duoauthproxy\lib\duo_async.pyc", line 186, in err_func

duoauthproxy.lib.duo_async.DuoAPIFailOpenError: API Request Failed: DNSLookupError('api-xxxxxxx.duosecurity.com',)

2019-08-19T04:59:37-0700 [-] (('10.127.196.189', 62001), duoadmin, 3): Failmode Secure - Denied Duo login on preauth failure

2019-08-19T04:59:37-0700 [-] (('10.127.196.189', 62001), duoadmin, 3): **Returning response code 3: AccessReject**

2019-08-19T04:59:37-0700 [-] (('10.127.196.189', 62001), duoadmin, 3): Sending response

Informazioni correlate

- [Autenticazione VPN RA tramite DUO](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)