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

Sommario

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

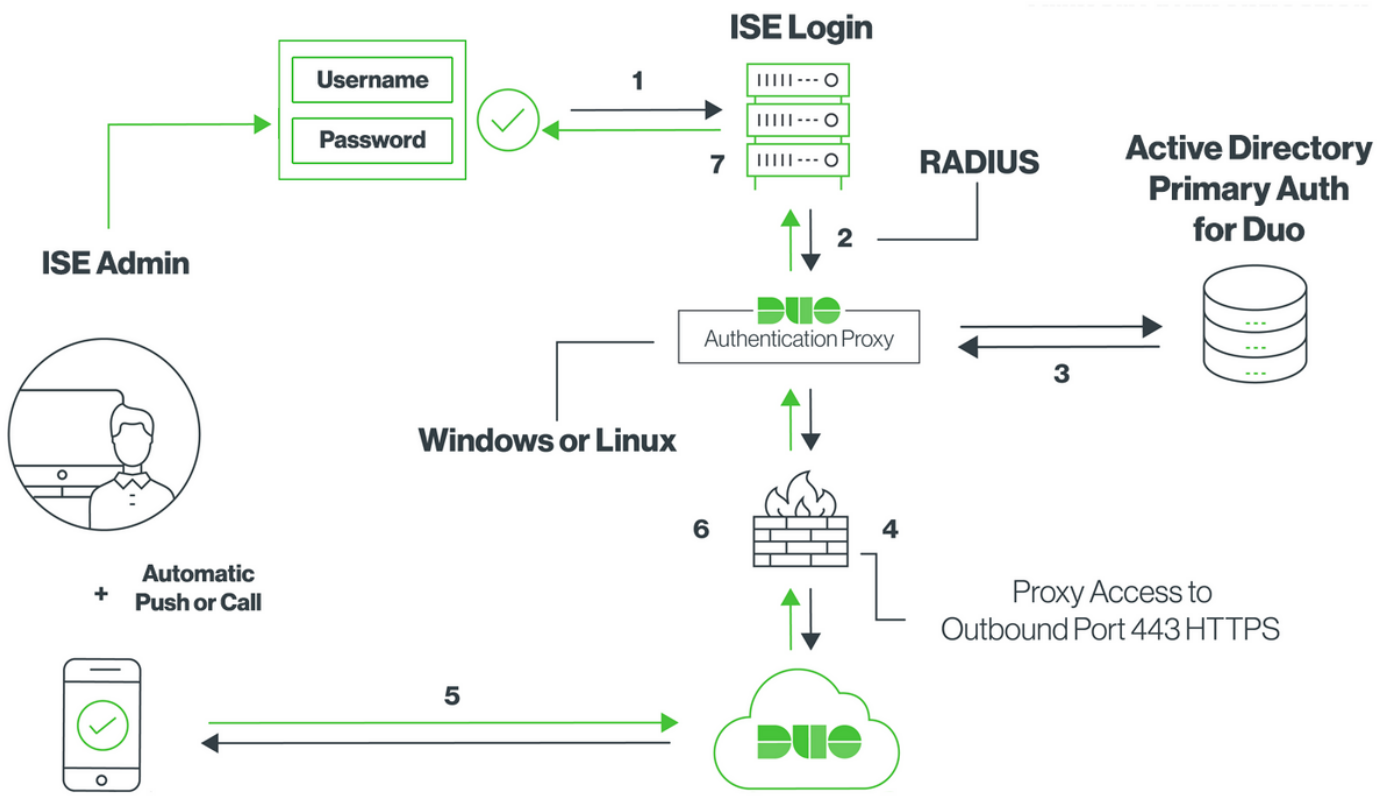
Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- 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.

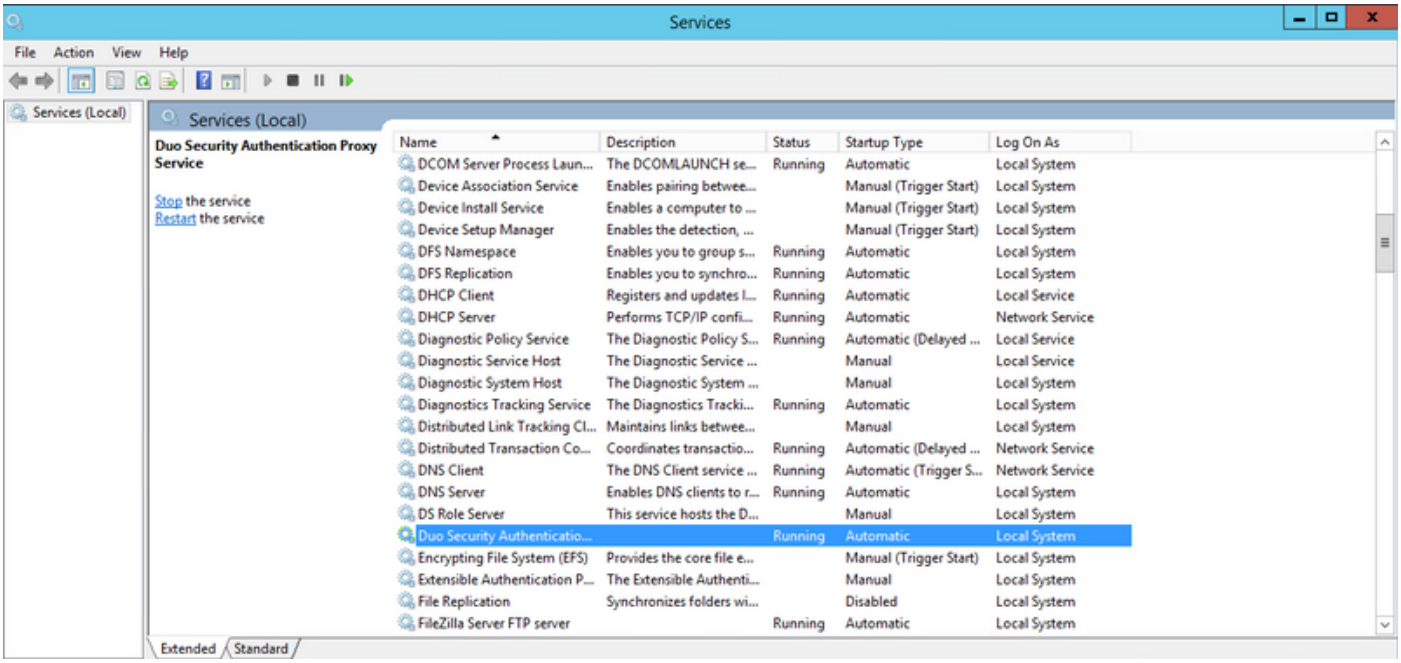
```
ikey= xxxxxxxxxxxxxxxxxxxxxxxx
skey= xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
api_host=api-xxxxxxxx.duosecurity.com
radius_ip_1=10.127.196.189                    Sample IP address of the ISE server
radius_secret_1=******
failmode=secure
client=ad_client
port=1812
```

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                           Sample IP address of the Active Directory
service_account_username=< AD-username >
service_account_password=< AD-password >
search_dn=CN=Users,DC=gce,DC=iselab,DC=local
```

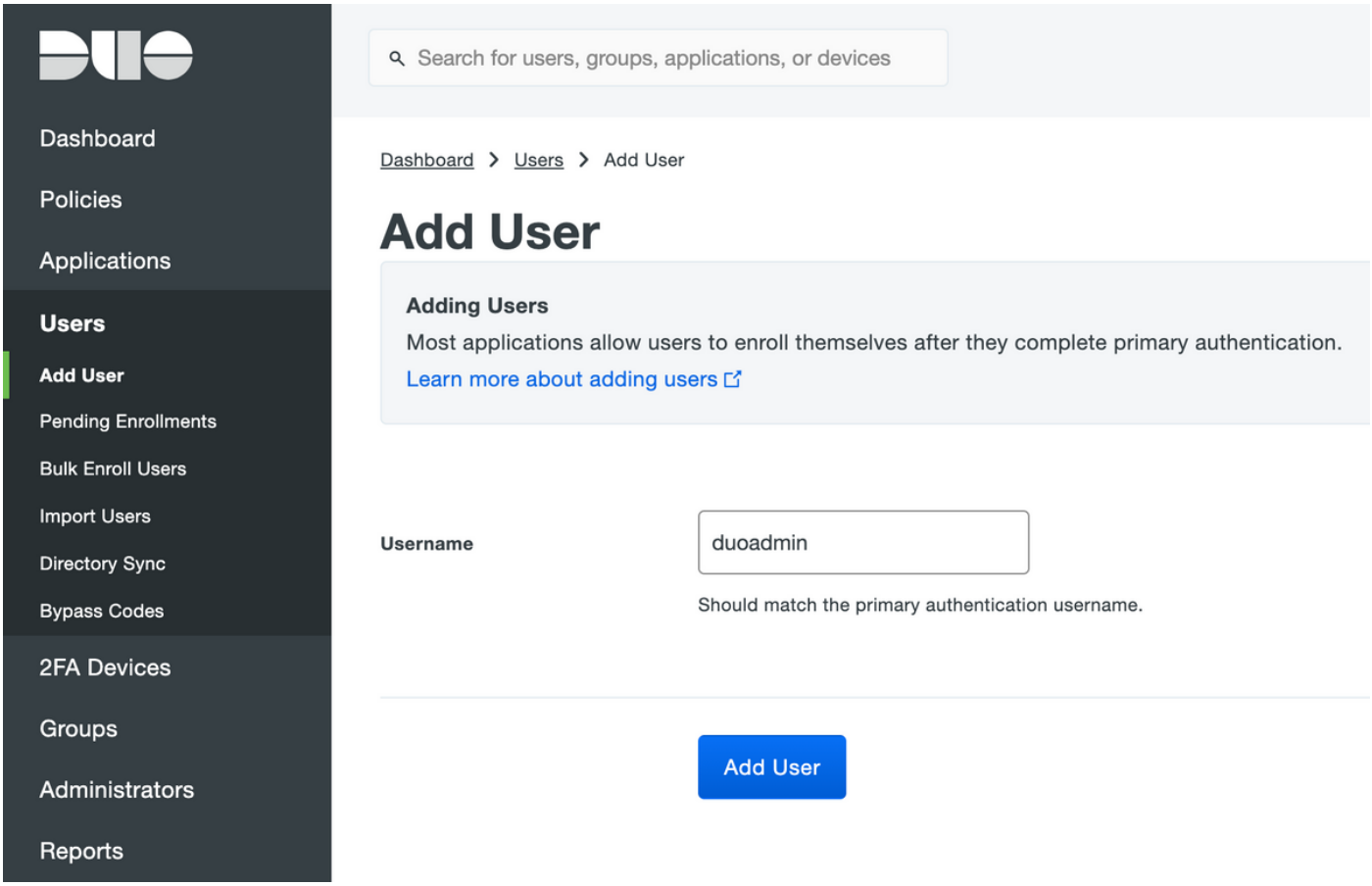
Nota: Se la rete richiede una connessione proxy HTTP per l'accesso a Internet, aggiungere i dettagli http_proxy in authproxy.cfg.

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:

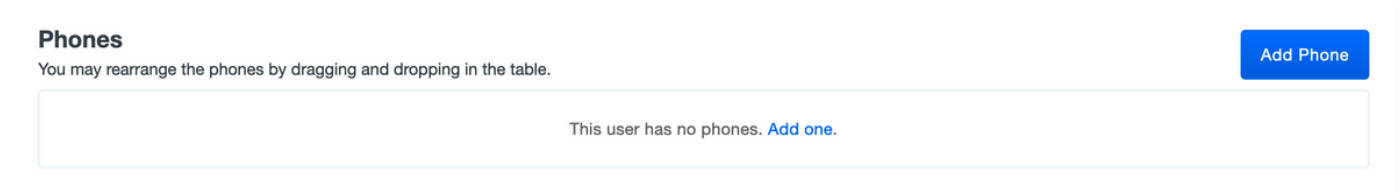


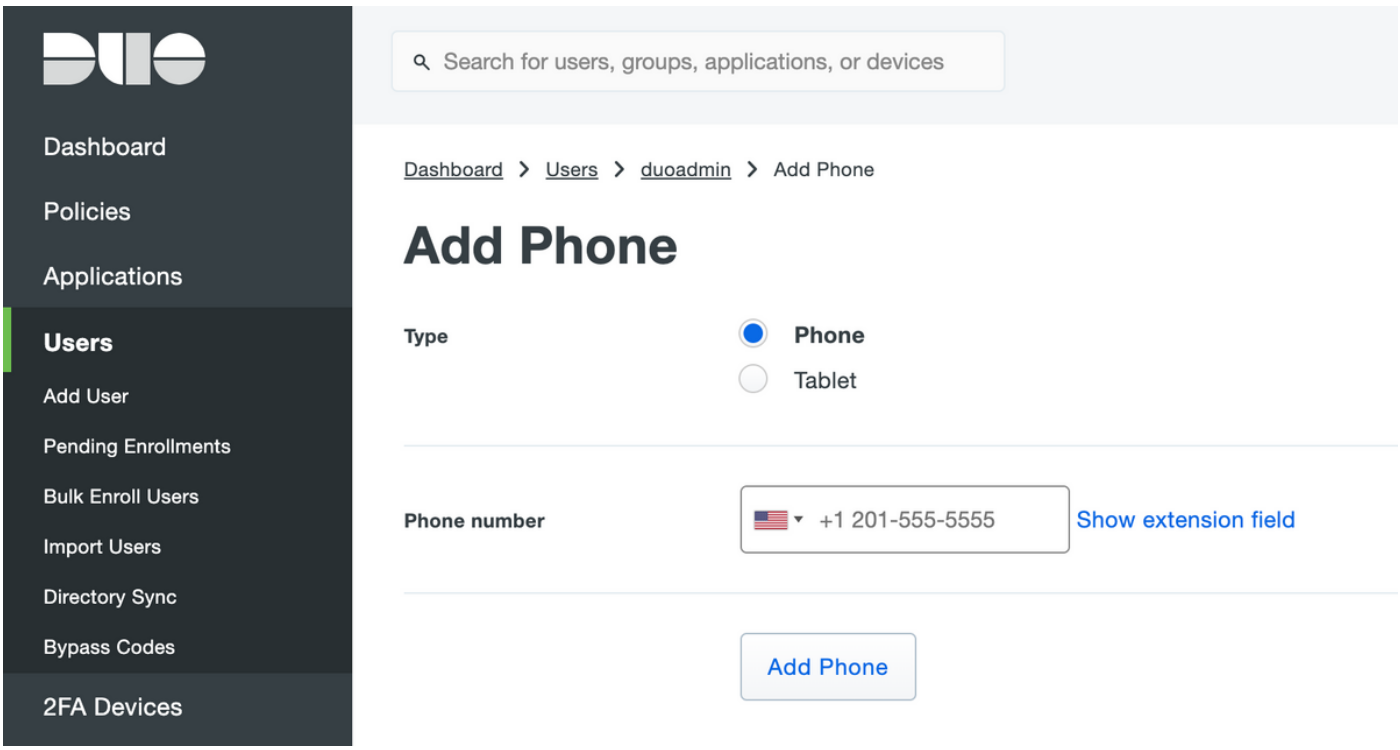
Passaggio 7. Creare un nome utente e attivare Duo Mobile sul dispositivo terminale: https://duo.com/docs/administration-users#creating-users-manually

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

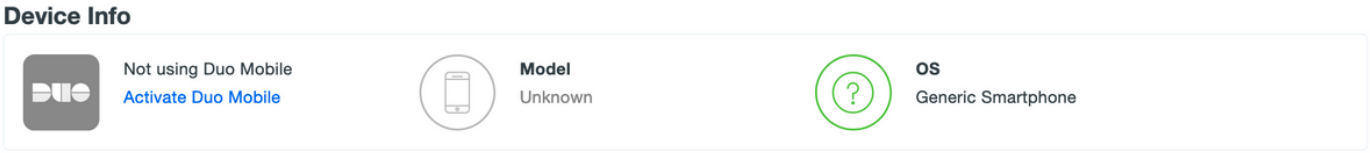


Assicurarsi che l'utente finale abbia l'app Duo installata sul telefono.

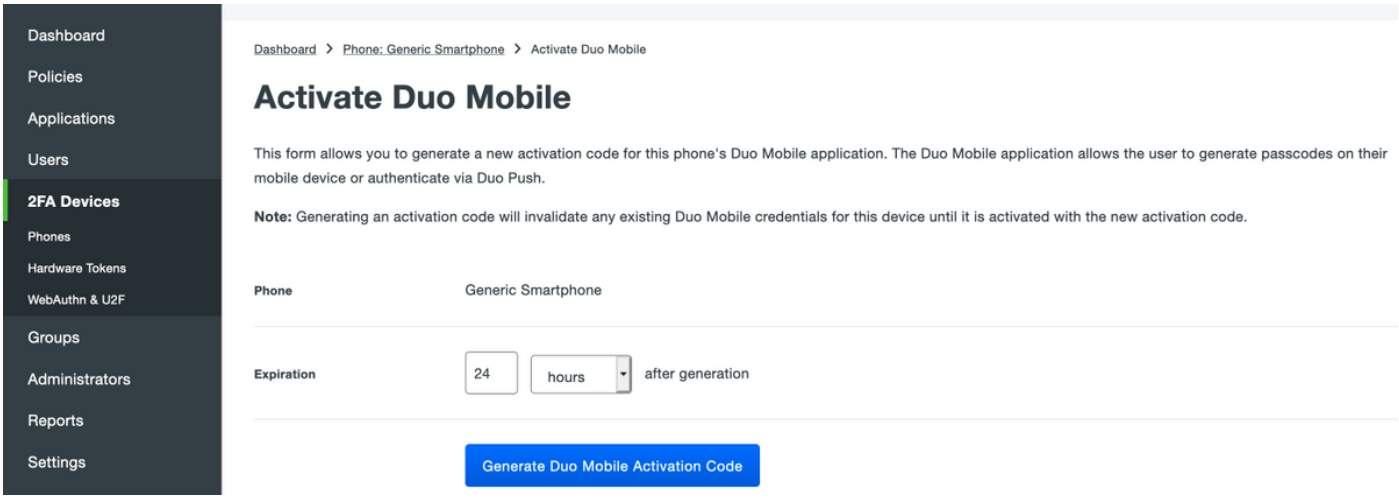




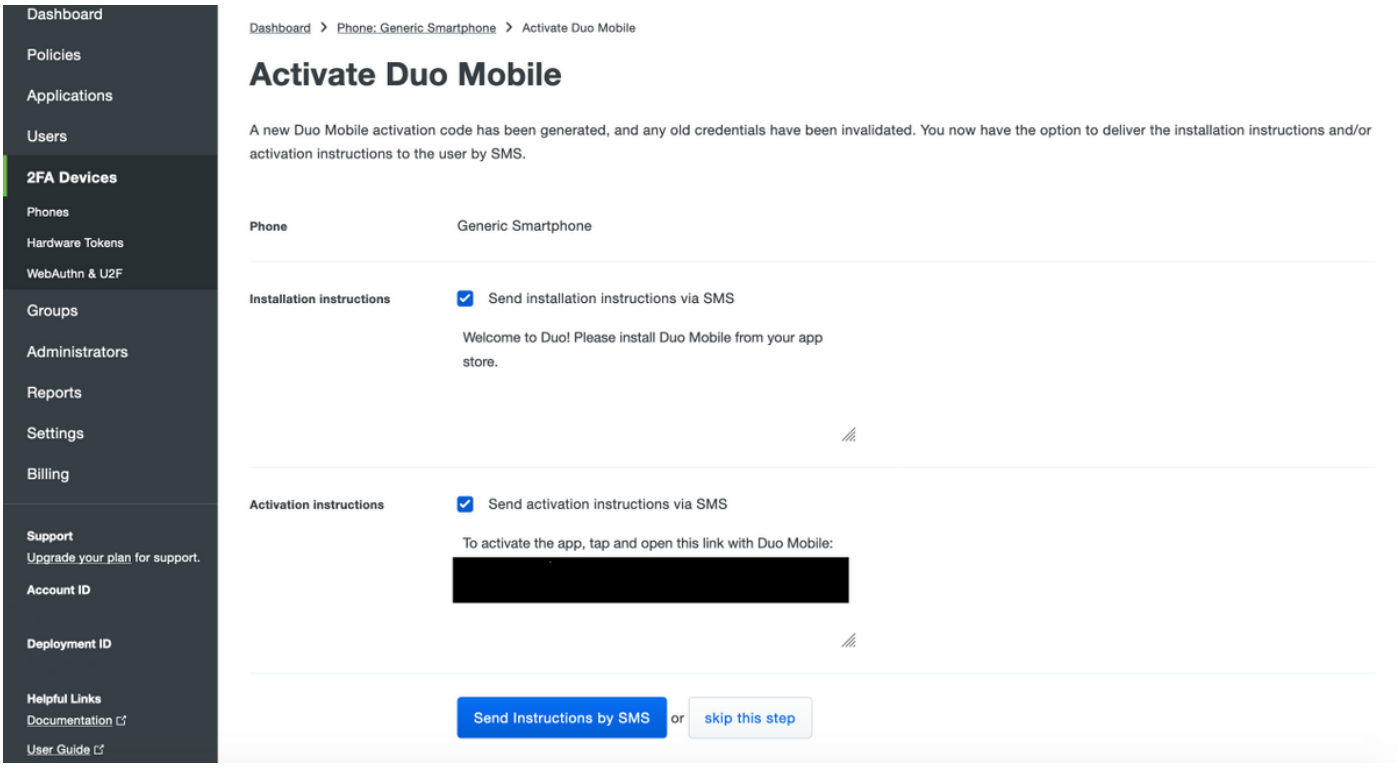
Selezionare **Activate Duo Mobile,** come mostrato nell'immagine:



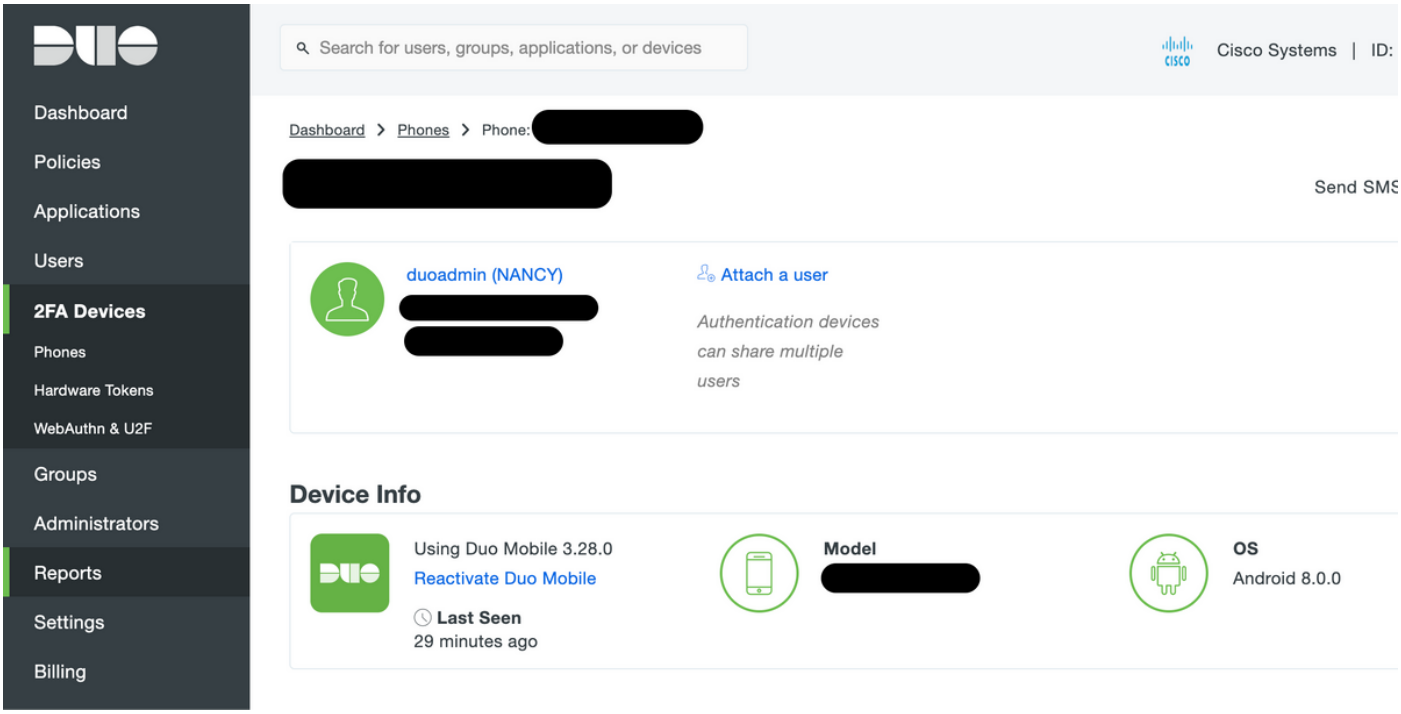
Selezionare **Generate Duo Mobile Activation Code,** come mostrato nell'immagine:



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



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

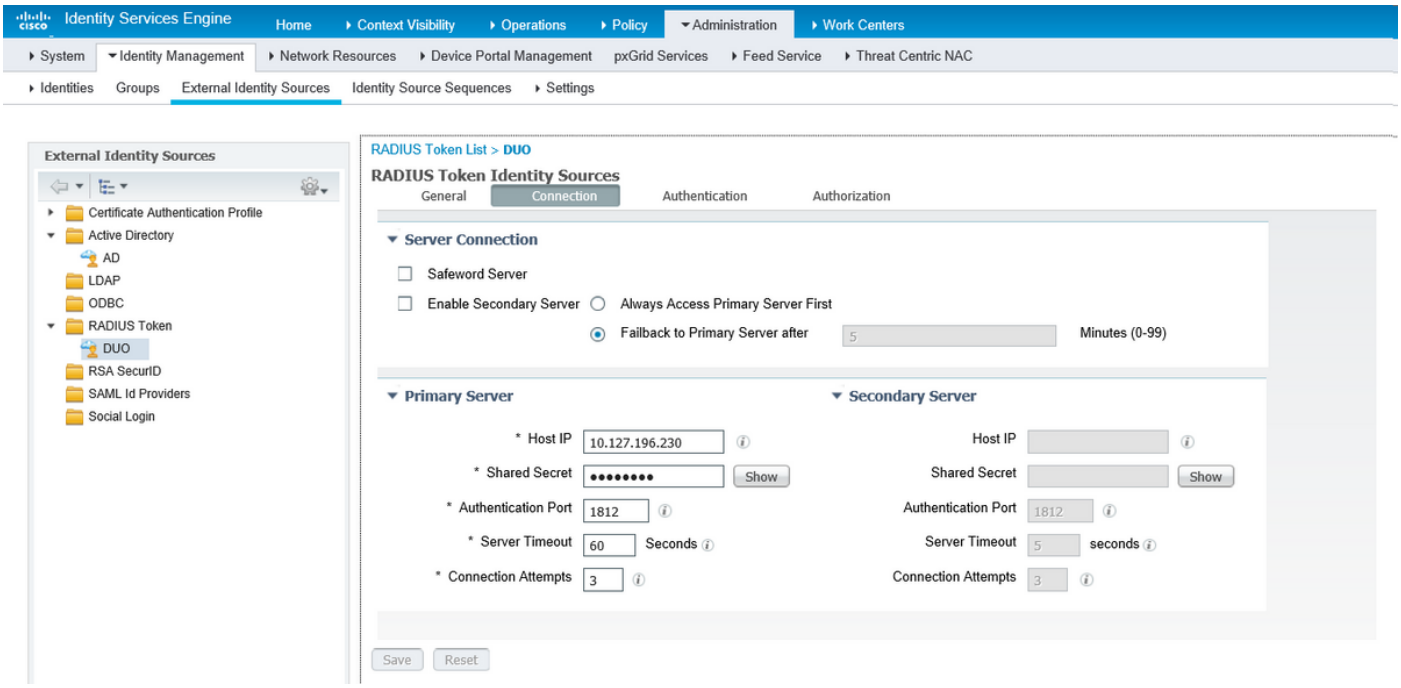


Configurazione di ISE

Passaggio 1. Integrare ISE con Duo Auth Proxy.

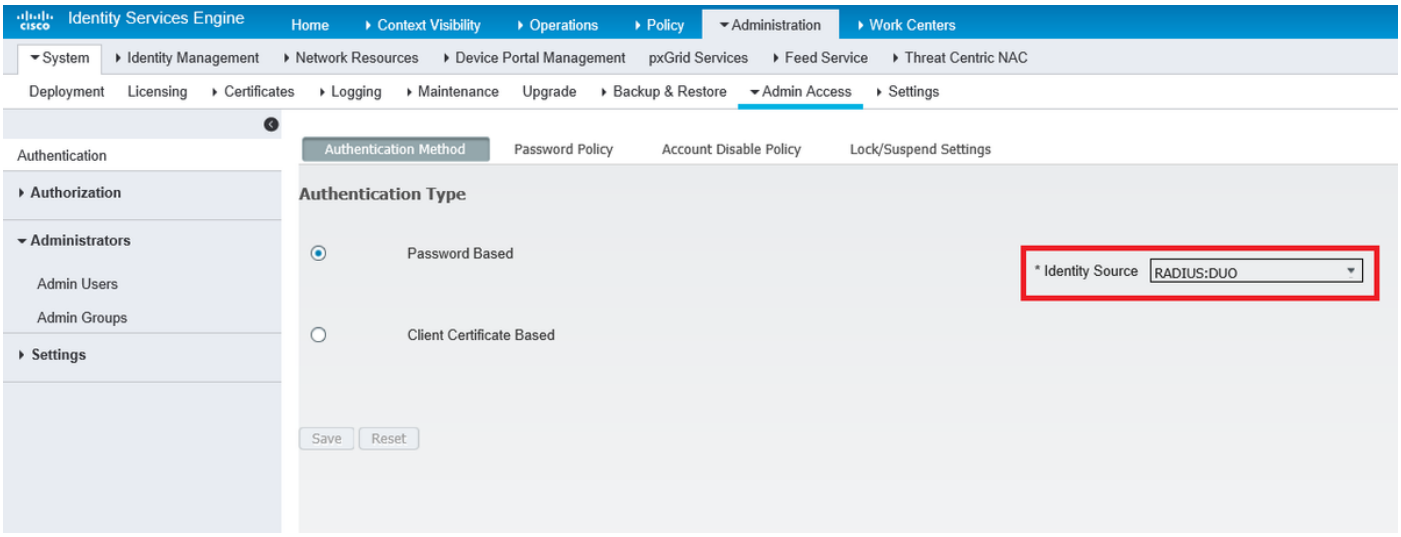
Selezionare **Amministrazione > Gestione delle identità > Origini identità esterne > Token RADIUS**, quindi fare clic su **Aggiungi** per aggiungere un nuovo server token RADIUS. Definire il nome del server nella scheda Generale, l'indirizzo IP e la chiave condivisa nella scheda Connessione, come mostrato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

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

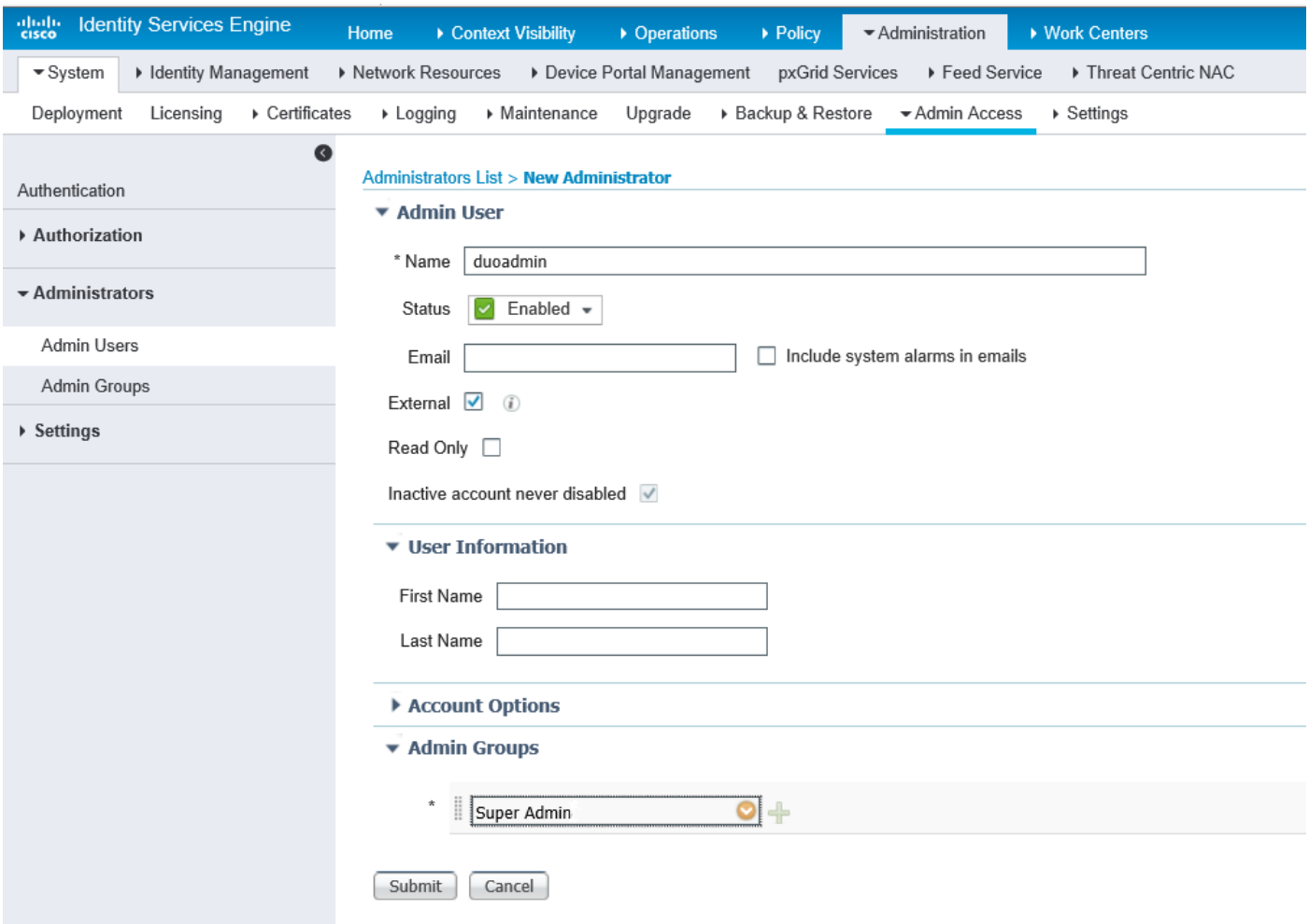


Passaggio 2. Passare a **Amministrazione > Sistema > Accesso amministratore > Autenticazione > Metodo di autenticazione** e **selezionare il** server token RADIUS configurato in precedenza come

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:

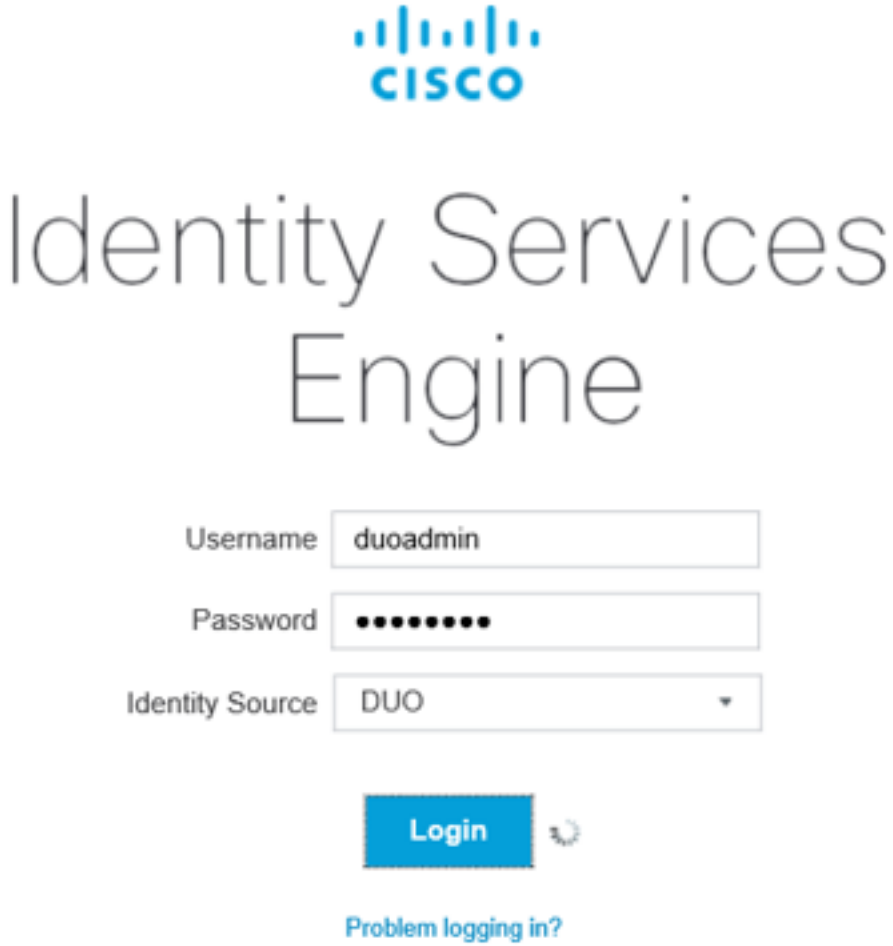


Verifica

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.



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 gotResult
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-
xxxxxxxx.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