

Configurazione dell'autenticazione a due fattori Duo per l'accesso alla gestione di FMC

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Flusso di autenticazione](#)

[Spiegazione del flusso di autenticazione](#)

[Configurazione](#)

[Procedura di configurazione in FMC](#)

[Procedura di configurazione su ISE](#)

[Procedura di configurazione sul portale di amministrazione Duo](#)

[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 in Firepower Management Center (FMC).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Configurazione degli oggetti di Firepower Management Center (FMC)
- Amministrazione di Identity Services Engine (ISE)

Componenti usati

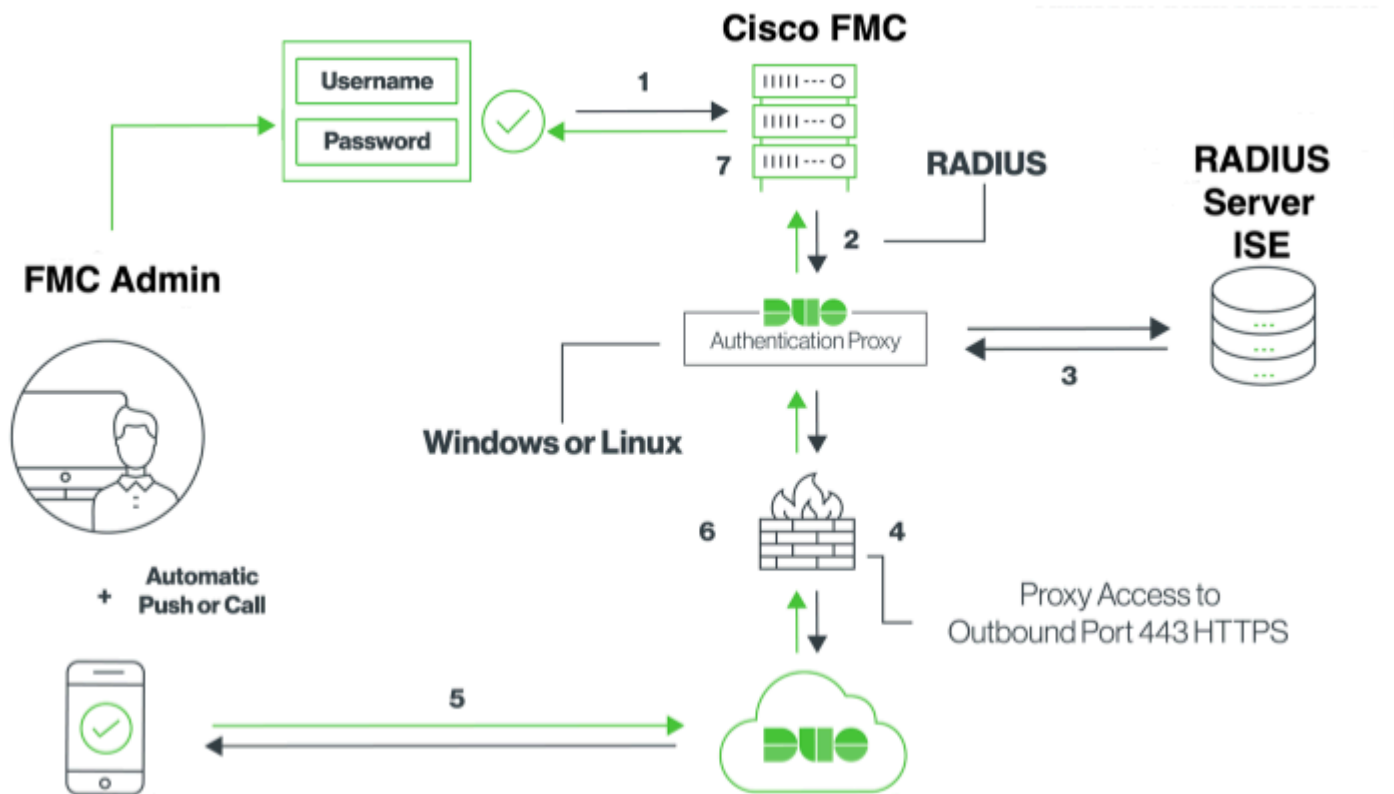
- Cisco Firepower Management Center (FMC) con versione 6.3.0
- Cisco Identity Services Engine (ISE) con versione 2.6.0.156
- Versione supportata di Windows (<https://duo.com/docs/authproxy-reference#new-proxy-install>) con connettività a FMC, ISE e Internet che funge da server proxy Duo Authentication
- Computer Windows per accedere a FMC, ISE e Duo Administration Portal
- Account Web Duo

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

L'amministratore FMC esegue l'autenticazione sul server ISE e un'ulteriore autenticazione sotto forma di notifica push viene inviata dal server Duo Authentication Proxy al dispositivo mobile dell'amministratore.

Flusso di autenticazione



Spiegazione del flusso di autenticazione

1. Autenticazione primaria avviata in Cisco FMC.
2. Cisco FMC invia una richiesta di autenticazione al proxy di autenticazione Duo.
3. L'autenticazione primaria deve utilizzare Active Directory o RADIUS.
4. Connessione del proxy di autenticazione Duo stabilita con Duo Security sulla porta TCP 443.
5. Autenticazione secondaria tramite il servizio Duo Security.
6. Il proxy di autenticazione Duo riceve la risposta di autenticazione.
7. L'accesso alla GUI del Cisco FMC è concesso.

Configurazione

Per completare la configurazione, prendere in considerazione le seguenti sezioni:

Procedura di configurazione in FMC

Passaggio 1. Selezionare **Sistema > Utenti > Autenticazione esterna**. Creare un oggetto di autenticazione esterno e impostare il metodo di autenticazione come RADIUS. Assicurarsi che l'opzione Amministratore sia selezionata in Ruolo utente predefinito come mostrato nell'immagine:

Nota: 10.106.44.177 è l'indirizzo IP di esempio del server proxy di autenticazione Duo.

Overview Analysis Policies Devices Objects AMP Intelligence

Configuration **Users** Domains Integration Update

Users User Roles **External Authentication**

External Authentication Object

Authentication Method: RADIUS

Name: DuoAuthProxy

Description:

Primary Server

Host Name/IP Address: 10.106.44.177 ex. IP or hostname

Port: 1812

RADIUS Secret Key: *****

Backup Server (Optional)

Host Name/IP Address: ex. IP or hostname

Port: 1812

RADIUS Secret Key:

RADIUS-Specific Parameters

Timeout (Seconds): 30

Retries: 3

Access Admin:

Administrator:

Security Analyst:

Security Analyst (Read Only):

Security Approver:

Threat Intelligence Director (TID) User:

Default User Role:
Access Admin
Administrator
Discovery Admin
External Database User To specify the default user role if user is not found in any group

Shell Access Filter

Administrator Shell Access User List:
(Mandatory for FTD devices) ex. user1, user2, user3

► Define Custom RADIUS Attributes

Additional Test Parameters

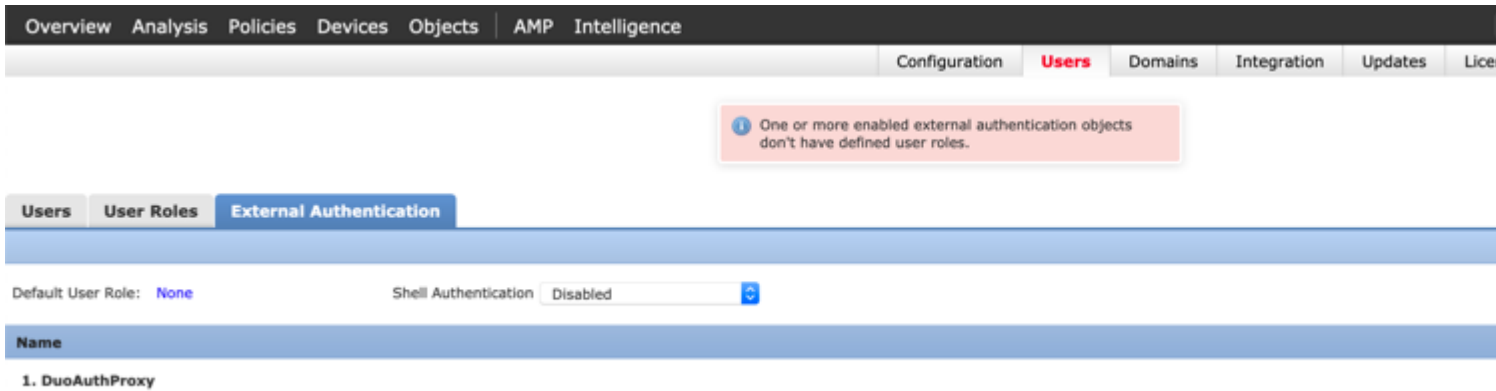
User Name:

Password:

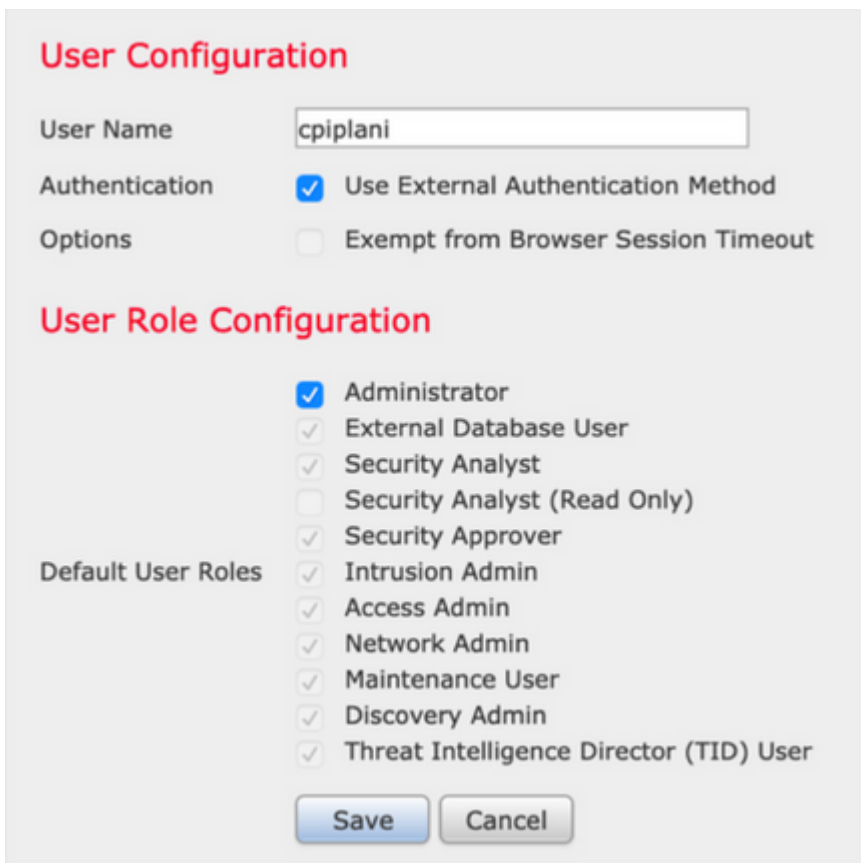
*Required Field

Save Test Cancel

Fare clic su **Save and Apply** (Salva e applica). Ignorare l'avviso come mostrato nell'immagine:



Passaggio 2. Passare a **Sistema > Utenti > Utenti**. Creare un utente e selezionare il metodo di autenticazione come esterno, come mostrato nell'immagine:



Passaggio 1. Scaricare e installare Duo Authentication Proxy Server.

Accedere al computer Windows e installare [Duo Authentication Proxy Server](#)

Si consiglia di utilizzare un sistema con almeno 1 CPU, 200 MB di spazio su disco e 4 GB di RAM

Nota: questo computer deve avere accesso a FMC, server RADIUS (ISE nel nostro caso) 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 è C:\Program Files (x86)\Duo Security Authentication Proxy\conf\authproxy.cfg

Modificare il file **authproxy.cfg** e aggiungere la configurazione seguente:

```
<#root>
```

```
[radius_client]
```

```
host=10.197.223.23
```

```
Sample IP Address of the ISE server
```

```
secret=cisco
```

Password configured on the ISE server in order to register the network device

L'indirizzo IP del CCP deve essere configurato insieme alla chiave privata RADIUS.

```
<#root>
```

```
[radius_server_auto]
```

```
ikey=xxxxxxxxxxxxxxxx
```

```
skey=xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
```

```
api_host=api-xxxxxxx.duosecurity.com
```

```
radius_ip_1=10.197.223.76
```

```
IP of FMC
```

```
radius_secret_1=cisco
```

```
Radius secret key used on the FMC
```

```
failmode=safe
```

```
client=radius_client
```

```
port=1812
```

```
api_timeout=
```

Assicurarsi di configurare i parametri ikey, skey e api_host. Per ottenere questi valori, accedere all'account Duo ([Duo Admin Login](#)) e selezionare **Applicazioni > Proteggi applicazione**. Selezionare quindi l'applicazione di autenticazione RADIUS come illustrato nell'immagine:

RADIUS

See the [RADIUS documentation](#) to integrate Duo into your RADIUS-enabled platform.

Details

Integration key	<input type="text"/>	select
Secret key	Click to view.	select
Don't write down your secret key or share it with anyone.		
API hostname	<input type="text"/>	select

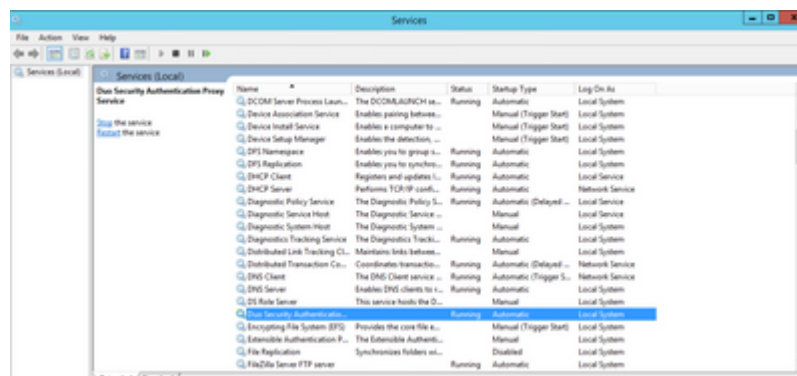
Chiave di integrazione = ikey

chiave segreta = chiave

Nome host API = api_host

Passaggio 3. Riavviare il servizio Duo Security Authentication Proxy. **Salvare** il file e **riavviare** il servizio Duo sul computer Windows.

Aprire la console Servizi di Windows (services.msc). Individuare **Duo Security Authentication Proxy Service** nell'elenco dei servizi e fare clic su **Riavvia**, come mostrato nell'immagine:



Procedura di configurazione su ISE

Passaggio 1. Selezionare **Amministrazione > Dispositivi di rete**, quindi fare clic su **Aggiungi** per configurare il dispositivo di rete come mostrato nell'immagine:

Nota: 10.106.44.177 è l'indirizzo IP di esempio del server proxy di autenticazione Duo.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Network Resources > Network Devices. The left sidebar shows 'Network Devices' with sub-items 'Default Device' and 'Device Security Settings'. The main content area is titled 'Network Devices List > DuoAuthproxy' and 'Network Devices'. The configuration form includes the following fields:

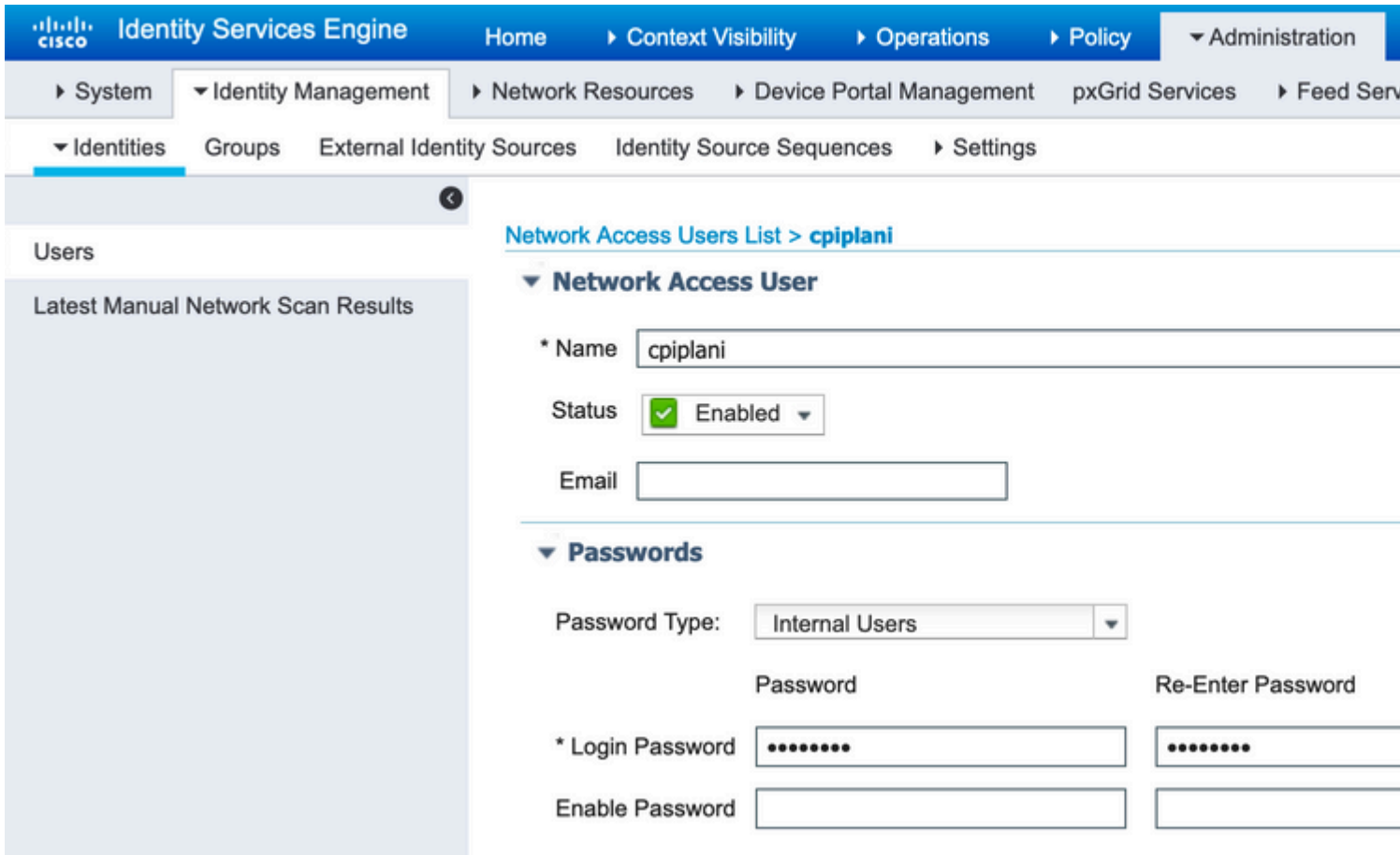
- * Name: DuoAuthproxy
- Description: (empty)
- IP Address: (dropdown menu)
- * IP: 10.106.44.177
- * Device Profile: Cisco (dropdown menu)
- Model Name: (dropdown menu)
- Software Version: (dropdown menu)

Configurare il **segreto condiviso** come indicato in **authproxy.cfg** in **segreto**, come mostrato nell'immagine:

The screenshot shows the RADIUS Authentication Settings configuration page in Cisco ISE. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Network Resources > Network Devices > RADIUS Authentication Settings. The left sidebar is the same as in the previous image. The main content area is titled 'RADIUS Authentication Settings' and 'RADIUS UDP Settings'. The configuration form includes the following fields:

- RADIUS Authentication Settings (checkbox)
- Protocol: RADIUS
- * Shared Secret: (masked with dots)
- Use Second Shared Secret: (checkbox)
- CoA Port: 1700

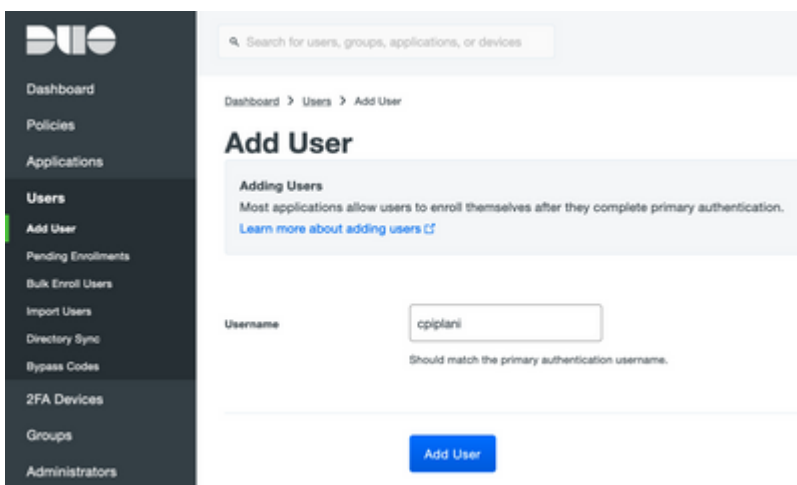
Passaggio 2. Passare a **Amministrazione > Identità**. Fare clic su **Add** (Aggiungi) per configurare l'utente Identity come mostrato nell'immagine:



Procedura di configurazione sul portale di amministrazione Duo

Passaggio 1. Creare un nome utente e attivare Duo Mobile sul dispositivo terminale.

Aggiungere l'utente nella pagina Web di amministrazione del cloud Duo. Passare a **Utenti > Aggiungi utenti** come mostrato nell'immagine:



Nota: verificare che l'utente finale abbia installato l'app Duo.

[Installazione manuale dell'applicazione Duo per dispositivi IOS](#)

[Installazione manuale di Duo Application per dispositivi Android](#)

Passaggio 2. Generazione automatica del codice.

Aggiungere il numero di telefono dell'utente come mostrato nell'immagine:

The image shows two screenshots from the Duo Admin console. The top screenshot shows a 'Phones' section with a message: 'This user has no phones. Add one.' and an 'Add Phone' button. The bottom screenshot shows the 'Add Phone' form. The breadcrumb navigation 'Dashboard > Users > ciplani > Add Phone' is highlighted with a red box. The 'Users' menu item in the left sidebar is also highlighted with a red box. The form includes a 'Type' section with radio buttons for 'Phone' (selected) and 'Tablet'. The 'Phone number' field contains '+1 201-555-5555' and has a 'Show extension field' link. An 'Add Phone' button is at the bottom.

Scegliere **Activate Duo Mobile** come mostrato nell'immagine:

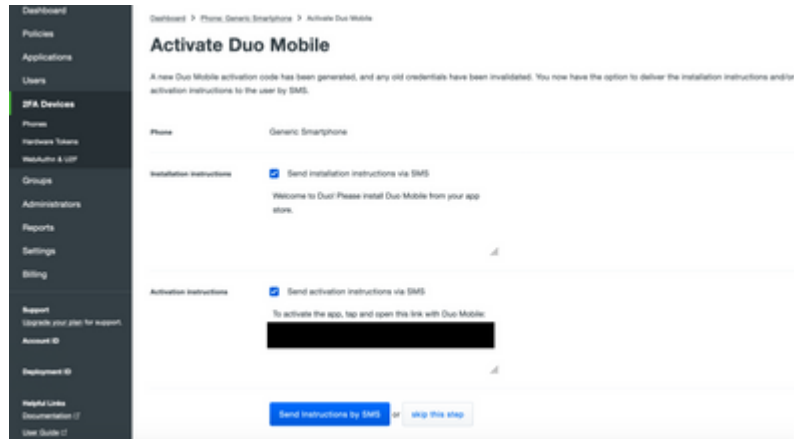
Device Info

The image shows the 'Device Info' section of the Duo Admin console. It contains three items: 1. A Duo logo icon with the text 'Not using Duo Mobile' and a blue link 'Activate Duo Mobile'. 2. A smartphone icon with the text 'Model' and 'Unknown'. 3. A green question mark icon with the text 'OS' and 'Generic Smartphone'.

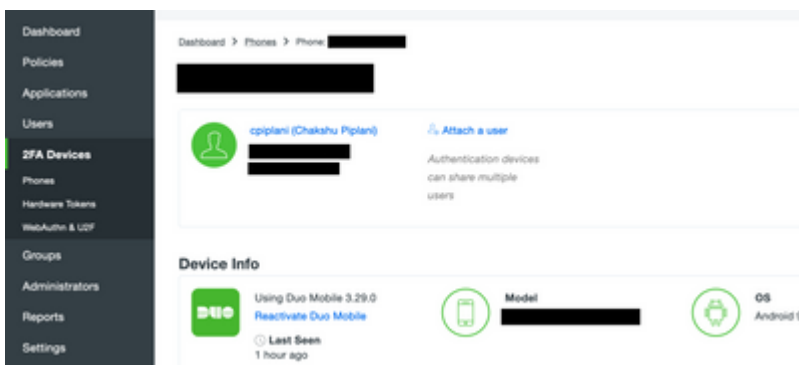
Scegliere **Generate Duo Mobile Activation Code** (Genera Duo Mobile Activation Code) come mostrato nell'immagine:

The image shows the 'Activate Duo Mobile' form in the Duo Admin console. The breadcrumb navigation is 'Dashboard > Phone, Generic Smartphone > Activate Duo Mobile'. The form title is 'Activate Duo Mobile'. Below the title is a description: '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.' A note states: 'Note: Generating an activation code will invalidate any existing Duo Mobile credentials for this device until it is activated with the new activation code.' The 'Phone' field is set to 'Generic Smartphone'. The 'Expiration' field is set to '24 hours after generation'. A blue button 'Generate Duo Mobile Activation Code' is at the bottom.

Scegliere **Send Instructions by SMS** come mostrato nell'immagine:



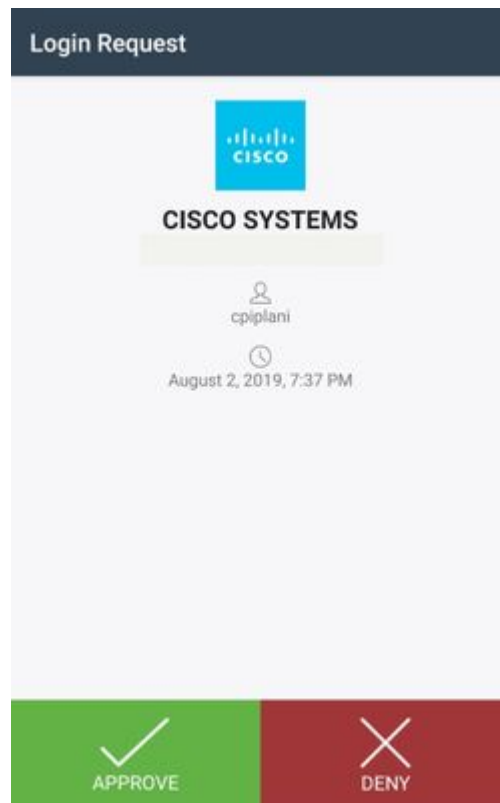
Fare clic sul collegamento nell'SMS e l'app Duo viene collegata all'account utente nella sezione Informazioni dispositivo, come mostrato nell'immagine:



Verifica

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

Accedere al FMC utilizzando le credenziali utente aggiunte nella pagina dell'identità dell'utente ISE. È necessario ottenere una notifica PUSH Duo sull'endpoint per l'autenticazione a due fattori (2FA), approvarla e FMC eseguirà l'accesso come mostrato nell'immagine:



Sul server ISE, selezionare **Operations > RADIUS > Live Log**. Individuare il nome utente utilizzato per l'autenticazione in FMC e selezionare il report di autenticazione dettagliato nella colonna dei dettagli. In questa finestra è necessario verificare se l'autenticazione ha esito positivo, come mostrato nell'immagine:

Identity Services Engine

Overview

Event	5200 Authentication succeeded
Username	cpiplani
Endpoint Id	
Endpoint Profile	
Authentication Policy	Default >> Default
Authorization Policy	Default >> Basic_Authenticated_Access
Authorization Result	PermitAccess

Authentication Details

Source Timestamp	2019-07-11 03:50:38.694
Received Timestamp	2019-07-11 03:50:38.694
Policy Server	ROHAN-ISE
Event	5200 Authentication succeeded
Username	cpiplani
User Type	User
Authentication Identity Store	Internal Users

Steps

- 11001 Received RADIUS Access-Request
- 11017 RADIUS created a new session
- 11117 Generated a new session ID
- 15049 Evaluating Policy Group
- 15008 Evaluating Service Selection Policy
- 15041 Evaluating Identity Policy
- 15048 Queried PIP - Normalised Radius.RadiusFlo
- 22072 Selected identity source sequence - All_Us
- 15013 Selected Identity Source - Internal Users
- 24210 Looking up User in Internal Users IDStore -
- 24212 Found User in Internal Users IDStore
- 22037 Authentication Passed
- 15036 Evaluating Authorization Policy
- 15048 Queried PIP - Radius.NAS-Port-Type
- 15048 Queried PIP - Network Access.UserName
- 15048 Queried PIP - IdentityGroup.Name
- 15048 Queried PIP - EndPoints.LogicalProfile
- 15048 Queried PIP - Network Access.Authentication
- 15016 Selected Authorization Profile - PermitAcces
- 22081 Max sessions policy passed
- 22080 New accounting session created in Session
- 11002 Returned RADIUS Access-Accept

Risoluzione dei problemi

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

- Controllare i debug su Duo Authentication Proxy Server. 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 quando vengono immesse credenziali non corrette e l'autenticazione viene rifiutata dal server ISE.

```
<#root>
```

```
2019-08-04T18:54:17+0530 [DuoForwardServer (UDP)] Sending request from  
10.197.223.76
```

```
to radius_server_auto
```

```
10.197.223.76 is the IP of the FMC
```

```
2019-08-04T18:54:17+0530 [DuoForwardServer (UDP)] Received new request id 4 from ('10.197.223.76', 34524)  
2019-08-04T18:54:17+0530 [DuoForwardServer (UDP)] (('10.197.223.76', 34524), 4):
```

```
login attempt for username u'cpiplani'
```

```
2019-08-04T18:54:17+0530 [DuoForwardServer (UDP)] Sending request for user u'cpiplani' to ('10.197.223.76', 34524)  
2019-08-04T18:54:17+0530 [RadiusClient (UDP)]
```

```
Got response
```

```
for id 199 from ('
```

```
10.197.223.23
```

```
', 1812);
```

```
code 3 10.197.223.23 is the IP of the ISE Server.
```

```
2019-08-04T18:54:17+0530 [RadiusClient (UDP)] (('10.197.223.76', 34524), 4): Primary credentials rejected  
2019-08-04T18:54:17+0530 [RadiusClient (UDP)] (('10.197.223.76', 34524), 4):
```

```
Returning response code 3: AccessReject
```

```
2019-08-04T18:54:17+0530 [RadiusClient (UDP)] (('10.197.223.76', 34524), 4): Sending response
```

- Ad ISE, selezionare **Operations > RADIUS > Live Logs** per verificare i dettagli dell'autenticazione.

Registra frammenti di autenticazione con esito positivo con ISE e Duo:

```
<#root>
```

```
2019-08-04T18:56:16+0530 [DuoForwardServer (UDP)] Sending request from  
10.197.223.76
```

```
to radius_server_auto
```

```
2019-08-04T18:56:16+0530 [DuoForwardServer (UDP)] Received new request id 5 from ('10.197.223.76', 34095)
2019-08-04T18:56:16+0530 [DuoForwardServer (UDP)] (('10.197.223.76', 34095), 5): login attempt for user
2019-08-04T18:56:16+0530 [DuoForwardServer (UDP)] Sending request for user u'cpiplani' to ('10.197.223.2
2019-08-04T18:56:16+0530 [RadiusClient (UDP)] Got response for id 137 from ('
```

10.197.223.23

', 1812);

code 2

<<<< At this point we have got successful authentication from ISE Server.

```
2019-08-04T18:56:16+0530 [RadiusClient (UDP)] http POST to https://api-f754c261.duosecurity.com:443/rest
2019-08-04T18:56:16+0530 [duoauthproxy.lib.http._DuoHTTPClientFactory#info] Starting factory <_DuoHTTPC
2019-08-04T18:56:17+0530 [HTTPPageGetter (TLSMemoryBIOProtocol),client] (('10.197.223.76', 34095), 5): C
2019-08-04T18:56:17+0530 [HTTPPageGetter (TLSMemoryBIOProtocol),client] Invalid ip. Ip was None
2019-08-04T18:56:17+0530 [HTTPPageGetter (TLSMemoryBIOProtocol),client] http POST to https://api-f754c26
2019-08-04T18:56:17+0530 [duoauthproxy.lib.http._DuoHTTPClientFactory#info] Starting factory <_DuoHTTPC
2019-08-04T18:56:17+0530 [duoauthproxy.lib.http._DuoHTTPClientFactory#info] Stopping factory <_DuoHTTPC
2019-08-04T18:56:30+0530 [HTTPPageGetter (TLSMemoryBIOProtocol),client] (('10.197.223.76', 34095), 5):
```

Duo authentication returned 'allow': 'Success. Logging you in...

```
2019-08-04T18:56:30+0530 [HTTPPageGetter (TLSMemoryBIOProtocol),client] (('10.197.223.76', 34095), 5):
```

Returning response code 2: AccessAccept

<<<< At this point, user has hit the approve button

```
2019-08-04T18:56:30+0530 [HTTPPageGetter (TLSMemoryBIOProtocol),client] (('10.197.223.76', 34095), 5): S
2019-08-04T18:56:30+0530 [duoauthproxy.lib.http._DuoHTTPClientFactory#info] Stopping factory <_DuoHTTPC
```

Informazioni correlate

- [Autenticazione VPN RA tramite Duo](#)
- [Documentazione e supporto tecnico â€™ Cisco Systems](#)

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).