

# Configuración de Duo Two-Factor Authentication para FMC Management Access

## Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Flujo de autenticación](#)

[Flujo de autenticación explicado](#)

[Configurar](#)

[Pasos de configuración en FMC](#)

[Pasos de configuración en ISE](#)

[Pasos de configuración en Duo Administration Portal](#)

[Verificación](#)

[Troubleshoot](#)

[Información Relacionada](#)

## Introducción

Este documento describe los pasos necesarios para configurar la autenticación externa de dos factores para el acceso a la administración en Firepower Management Center (FMC).

## Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Configuración de objetos de Firepower Management Center (FMC)
- Administración de Identity Services Engine (ISE)

### Componentes Utilizados

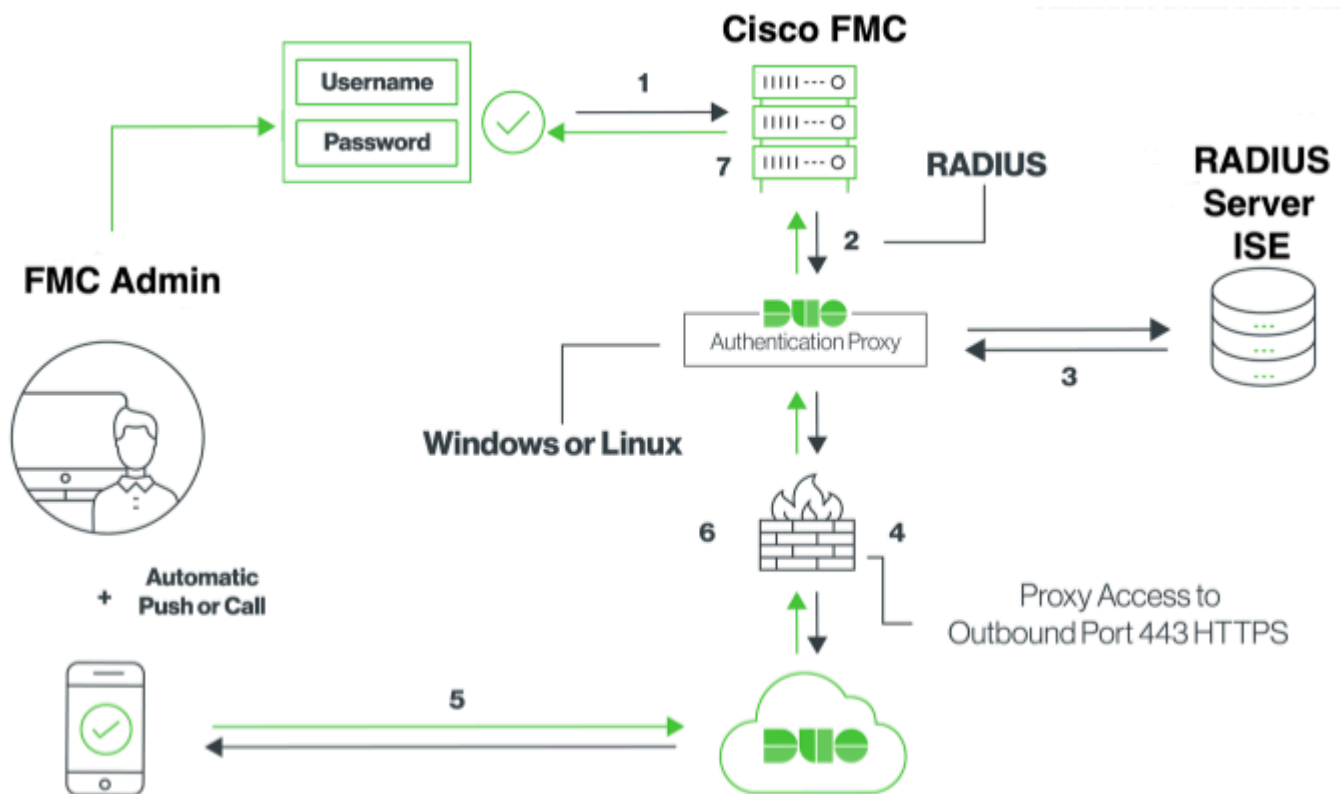
- Cisco Firepower Management Center (FMC) con la versión 6.3.0
- Cisco Identity Services Engine (ISE) que ejecuta la versión 2.6.0.156
- Versión compatible de Windows (<https://duo.com/docs/authproxy-reference#new-proxy-install>) con conectividad a FMC, ISE e Internet para actuar como servidor proxy de autenticación Duo
- Windows Machine para acceder al portal de administración de FMC, ISE y Duo
- Cuenta web Duo

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

## Antecedentes

El administrador de FMC realiza la autenticación en el servidor ISE y el servidor proxy de autenticación duo envía una autenticación adicional en forma de notificación de inserción al dispositivo móvil del administrador.

## Flujo de autenticación



## Flujo de autenticación explicado

1. Autenticación principal iniciada en Cisco FMC.
2. Cisco FMC envía una solicitud de autenticación al proxy de autenticación Duo.
3. La autenticación principal debe utilizar Active Directory o RADIUS.
4. Se ha establecido una conexión de proxy de autenticación Duo con seguridad Duo a través del puerto TCP 443.
5. Autenticación secundaria a través del servicio Duo Security.
6. El proxy de autenticación Duo recibe la respuesta de autenticación.
7. Se concede acceso a la GUI de Cisco FMC.

## Configurar

Para completar la configuración, tenga en cuenta estas secciones:

### Pasos de configuración en FMC

**Paso 1. Vaya a System > Users > External Authentication.** Cree un objeto de autenticación externa y

establezca el método de autenticación como RADIUS. Asegúrese de que Administrator esté seleccionado en Default User Role (Función de usuario predeterminada), como se muestra en la imagen:

**Nota:** 10.106.44.177 es la dirección IP de ejemplo del servidor proxy de autenticación Duo.

The screenshot shows the configuration page for an External Authentication Object in the Palo Alto Networks management console. The navigation bar at the top includes Overview, Analysis, Policies, Devices, Objects, AMP, and Intelligence. The main menu has tabs for Users, User Roles, and External Authentication. The configuration form is divided into several sections:

- External Authentication Object**
  - Authentication Method: RADIUS (dropdown)
  - Name: DuoAuthProxy
  - Description: (empty)
- Primary Server**
  - Host Name/IP Address: 10.106.44.177 (with example text "ex. IP or hostname")
  - Port: 1812
  - RADIUS Secret Key: (masked with dots)
- Backup Server (Optional)**
  - Host Name/IP Address: (empty) (with example text "ex. IP or hostname")
  - Port: 1812
  - RADIUS Secret Key: (empty)
- RADIUS-Specific Parameters**
  - Timeout (Seconds): 30
  - Retries: 3
  - Access Admin: (empty)
  - Administrator: (empty)

Security Analyst

Security Analyst (Read Only)

Security Approver

Threat Intelligence Director (TID) User

Default User Role  To specify the default user role if user is not found in any group

**Shell Access Filter**

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

► **Define Custom RADIUS Attributes**

**Additional Test Parameters**

User Name

Password

\*Required Field

Haga clic en **Guardar** y **Aplicar**. Ignore la advertencia como se muestra en la imagen:

Overview Analysis Policies Devices Objects AMP Intelligence Configuration **Users** Domains Integration Updates Licenses

**One or more enabled external authentication objects don't have defined user roles.**

Users User Roles **External Authentication**

Default User Role: **None** Shell Authentication: Disabled

**Name**

1. DuoAuthProxy

**Paso 2.** Vaya a **Sistema > Usuarios > Usuarios**. Cree un usuario y verifique el Método de autenticación como Externo, como se muestra en la imagen:

**User Configuration**

User Name:

Authentication:  Use External Authentication Method

Options:  Exempt from Browser Session Timeout

**User Role Configuration**

Default User Roles:

- Administrator
- External Database User
- Security Analyst
- Security Analyst (Read Only)
- Security Approver
- Intrusion Admin
- Access Admin
- Network Admin
- Maintenance User
- Discovery Admin
- Threat Intelligence Director (TID) User

**Paso 1.** Descargue e instale Duo Authentication Proxy Server.

Inicie sesión en la máquina Windows e instale el [servidor proxy de autenticación Duo](#)

Se recomienda utilizar un sistema con al menos 1 CPU, 200 MB de espacio en disco y 4 GB de RAM

---

Nota: Esta máquina debe tener acceso a FMC, servidor RADIUS (ISE en nuestro caso) y Duo Cloud (Internet)

---

**Paso 2. Configure el archivo authproxy.cfg.**

Abra este archivo en un editor de texto como Notepad++ o WordPad.

---

Nota: La ubicación predeterminada se encuentra en C:\Program Files (x86)\Duo Security Authentication Proxy\conf\authproxy.cfg

---

Edite el archivo **authproxy.cfg** y agregue esta configuración:

```
<#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

La dirección IP del FMC debe configurarse junto con la clave secreta 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=
```

Asegúrese de configurar los parámetros ikey, skey y api\_host. Para obtener estos valores, inicie sesión en su cuenta Duo ([Duo Admin Login](#)) y navegue hasta **Aplicaciones > Proteger una aplicación**. A continuación, seleccione la aplicación de autenticación RADIUS como se muestra en la imagen:

# RADIUS

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

## Details

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

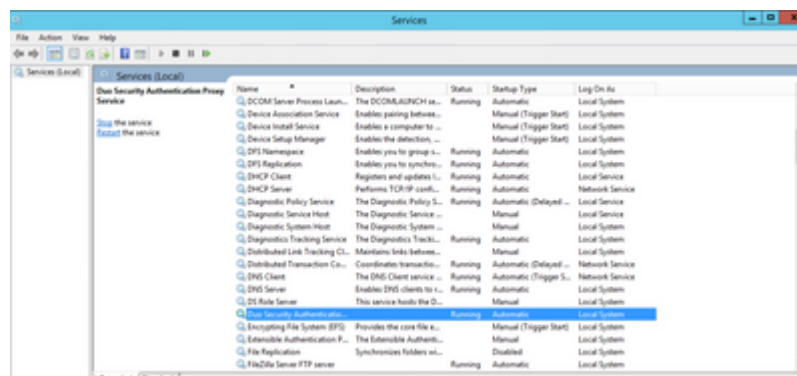
Clave de integración = ikey

clave secreta = skey

API hostname = api\_host

**Paso 3.** Reinicie el servicio Duo Security Authentication Proxy. **Guarde** el archivo y **reinicie** el servicio Duo en el equipo de Windows.

Abra la consola de Servicios de Windows (services.msc). Localice **Duo Security Authentication Proxy Service** en la lista de servicios y haga clic en **Restart** como se muestra en la imagen:



## Pasos de configuración en ISE

**Paso 1.** Navegue hasta **Administration > Network Devices**, Haga clic en **Add** para configurar el dispositivo de red como se muestra en la imagen:

**Nota:** 10.106.44.177 es la dirección IP de ejemplo del servidor proxy de autenticación 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: a required field for Name with the value 'DuoAuthproxy'; a Description field; a dropdown for IP Address with the value '10.106.44.177'; a required field for Device Profile with the value 'Cisco'; and dropdowns for Model Name and Software Version.

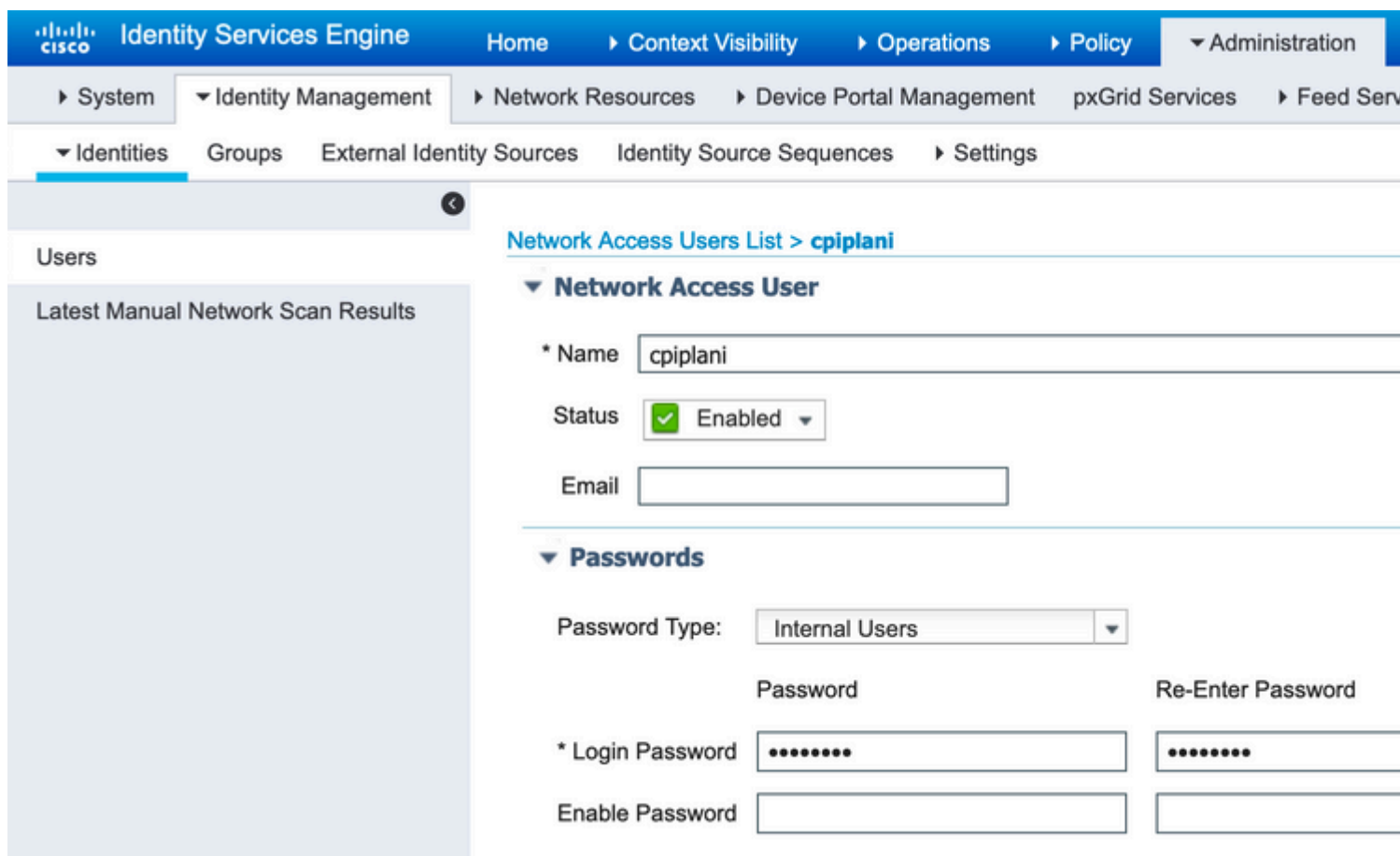
Configure el **secreto compartido** como se menciona en **authproxy.cfg** en **secret** como se muestra en la imagen:

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 shows 'Network Devices' with sub-items 'Default Device' and 'Device Security Settings'. The main content area is titled 'RADIUS Authentication Settings' and 'RADIUS UDP Settings'. The configuration form includes: a checked checkbox for RADIUS Authentication Settings; a dropdown for Protocol with the value 'RADIUS'; a required field for Shared Secret with a masked value '.....'; a checkbox for Use Second Shared Secret; and a dropdown for CoA Port with the value '1700'.

**Paso 2. Vaya a Administration > Identities.** Haga clic en **Agregar** para configurar el usuario de identidad



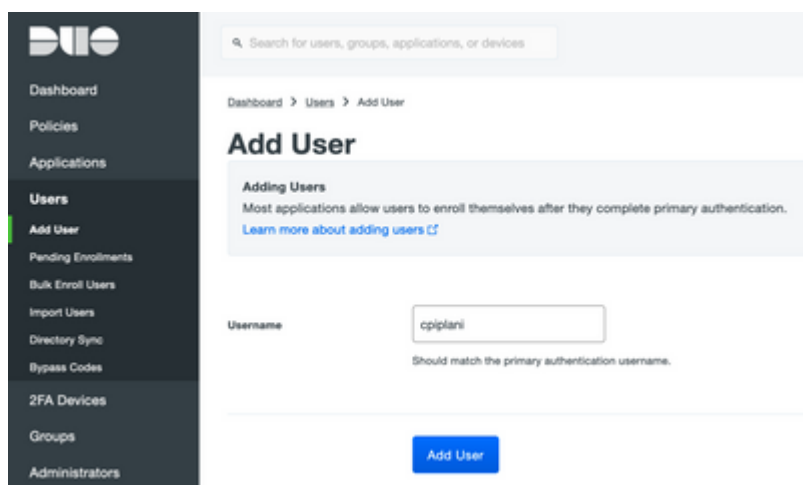
como se muestra en la imagen:



## Pasos de configuración en Duo Administration Portal

**Paso 1.** Cree un nombre de usuario y active Duo Mobile en el dispositivo final.

Agregue el usuario en la página web de administración de la nube Duo. Vaya a **Users > Add users** como se muestra en la imagen:



Nota: Asegúrese de que el usuario final tiene instalada la aplicación Duo.

## [Instalación manual de la aplicación Duo para dispositivos IOS](#)

## [Instalación manual de la aplicación Duo para dispositivos Android](#)

### **Paso 2.** Generación automática de código.

Agregue el número de teléfono del usuario como se muestra en la imagen:

The image shows two parts of the Duo Admin console. The top part is a 'Phones' section for a user, indicating they have no phones and providing an 'Add Phone' button. The bottom part is the 'Add Phone' form, which includes a search bar, a breadcrumb trail (Dashboard > Users > cpiplani > Add Phone), a sidebar menu with 'Users' and 'Add User' highlighted, and a form with the following fields: 'Type' (Phone selected, Tablet unselected), 'Phone number' (+1 201-555-5555), and a 'Show extension field' link. An 'Add Phone' button is at the bottom.

Elija **Activate Duo Mobile** como se muestra en la imagen:

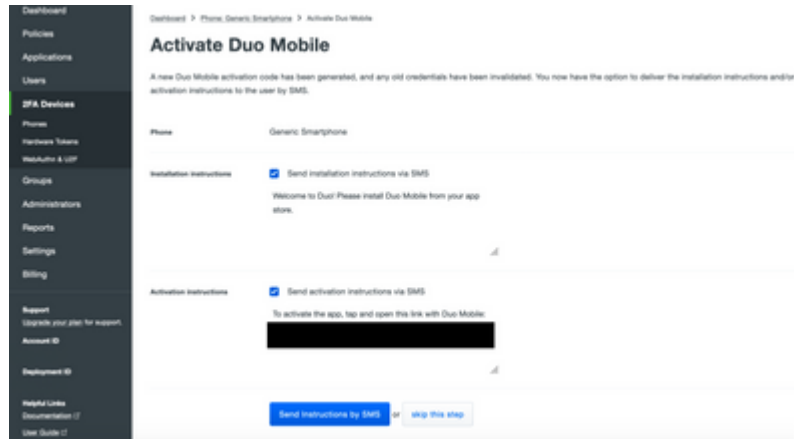
### Device Info

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 'Activate Duo Mobile' button. 2) A smartphone icon with the text 'Model Unknown'. 3) A green question mark icon with the text 'OS Generic Smartphone'.

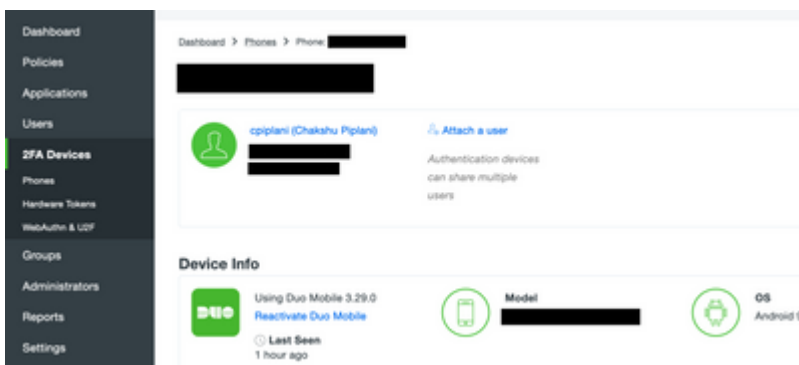
Elija **Generate Duo Mobile Activation Code** como se muestra en la imagen:

The image shows the 'Activate Duo Mobile' form in the Duo Admin console. It includes a sidebar menu with '2FA Devices' and 'Phone' highlighted. The main content area has a breadcrumb trail (Dashboard > Phone, Generic Smartphone > Activate Duo Mobile), the title 'Activate Duo Mobile', and 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.' Below this is a note: '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 form has two fields: 'Phone' (Generic Smartphone) and 'Expiration' (24 hours after generation). A blue 'Generate Duo Mobile Activation Code' button is at the bottom.

Elija **Enviar instrucciones por SMS** como se muestra en la imagen:



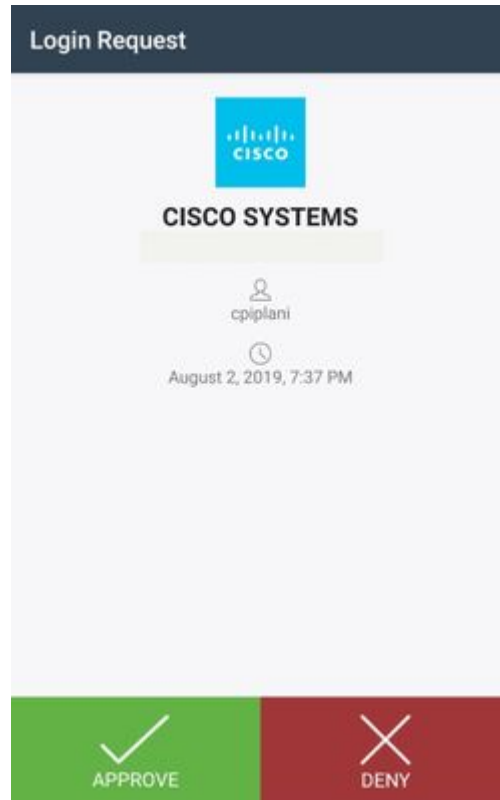
**Haga clic** en el enlace de la aplicación SMS, y Duo se vincula a la cuenta de usuario en la sección Device Info, como se muestra en la imagen:



## Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

Inicie sesión en el FMC con las credenciales de usuario que se agregaron en la página de identidad de usuario de ISE. Debe recibir una notificación Duo PUSH en el terminal para la autenticación de dos factores (2FA), aprobarla y FMC se conectará como se muestra en la imagen:



En el servidor ISE, navegue hasta **Operaciones > RADIUS > Registros en directo**. Busque el nombre de usuario utilizado para la autenticación en FMC y seleccione el informe de autenticación detallado en la columna de detalles. Aquí debe verificar si la autenticación se realiza correctamente, como se muestra en la imagen:

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

# Troubleshoot

Esta sección proporciona la información que puede utilizar para resolver problemas de su configuración.

- Verifique las depuraciones en el Servidor Proxy de Autenticación Duo. Los registros se encuentran en esta ubicación:

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

Abra el archivo **authproxy.log** en un editor de texto como Notepad++ o WordPad.

Fragmentos de registro cuando se introducen credenciales incorrectas y el servidor ISE rechaza la autenticación.

```
<#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
```

- En ISE, vaya a **Operations > RADIUS > Live Logs** para verificar los detalles de autenticación.

Fragmentos de registro de autenticación satisfactoria con ISE y 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

```

## Información Relacionada

- [Autenticación VPN de RA con Duo](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)

## Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).