



Despliegue Cisco Duo

HUNOSA - Hulleras del Norte S.A. S.M.E

Grupo CIES

Edificio Asipo II, Plaza Santa Bárbara 4, oficinas 28-19, Parque Empresarial de Asipo, 33426 Llanera, Asturias

T: 984 28 28 30

Correo el: contacto@alisee.es

Control documental

Versión	Descripción	Fecha
1	Versión 1.0	14/02/2023

1 Contenidos

1	Contenidos	2
2	General	3
3	Configuración Citrix (Netscaler)	3
3.1	Despliegue Proxy Cisco Duo.....	4
3.2	Instalación Cisco Duo.....	4
3.3	Configuración Cisco Duo Authentication Proxy	4
3.4	Configuración Netscaler	5
4	Configuración RDP	5
4.1	Instalación de forma manual	6
4.2	Instalación de forma centralizada GPO.....	7
5	Configuración Cisco Duo	8
5.1	Configuración aplicación en Cisco Duo:	8
5.2	Configuración usuarios en Cisco Duo:	10
5.2.1	Configuración manual.....	10
5.2.2	Importar usuarios.....	10
5.3	Configuración teléfonos en Cisco Duo manualmente:	10

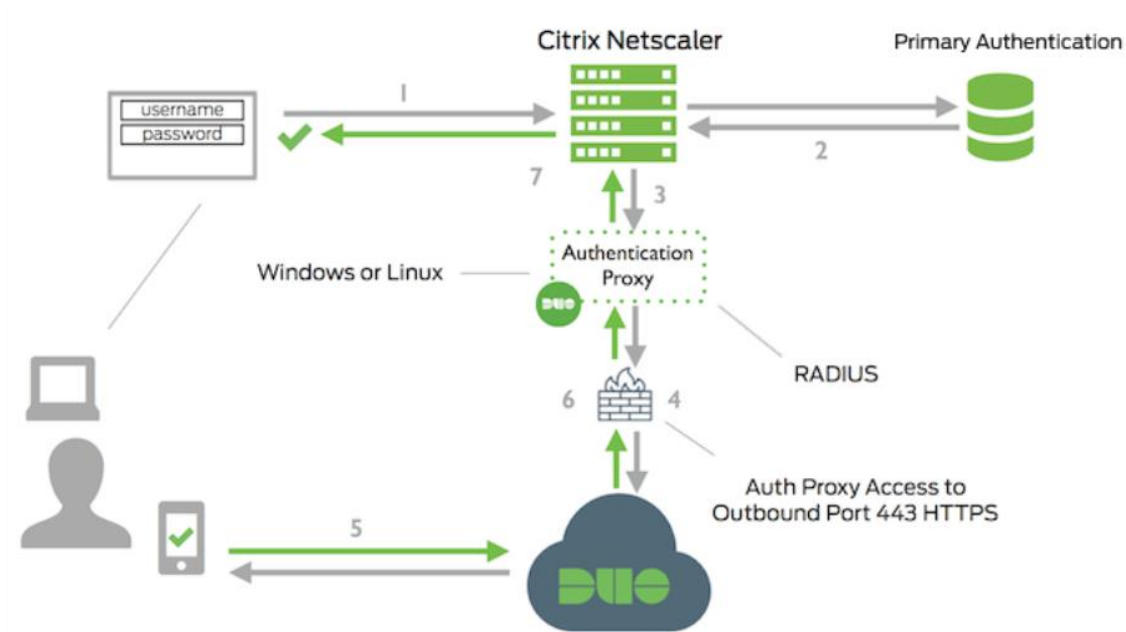
2 General

Se realiza el despliegue de la doble autenticación de Cisco Duo en Citrix (Netscaler) y en RDP para las conexiones de acceso al equipo local o para las conexiones remotas RDP.

3 Configuración Citrix (Netscaler)

Para la integración de Duo con Citrix (Netscaler), se necesita instalar un servicio de proxy local en la red de HUNOSA. Este servidor proxy actuará como un servidor RADIUS.

Una vez configurado, Duo envía a sus usuarios una solicitud de autenticación automática a través de una notificación de Duo Push o una llamada de teléfono a un dispositivo después de un inicio de sesión exitoso.



3.1 Despliegue Proxy Cisco Duo

Se despliega máquina virtual con las siguientes características:

- S.O.: Debian GNU/Linux 11 (bullseye)
- Al menos 1 CPU y 500 MB de espacio en disco
- 4 GB de RAM

3.2 Instalación Cisco Duo

Se instalan una serie de librerías necesarias para el funcionamiento:

- Build-essential
- Libffi-dev
- Perl
- Zlib1g-dev

Una vez instaladas estas librerías, se descarga Duoauthproxy y se instala.

3.3 Configuración Cisco Duo Authentication Proxy

El archivo de configuración de Cisco Duo Authentication Proxy es "authproxy.cfg" y se encuentra ubicado en "/opt/duoauthproxy/conf". La configuración del archivo se puede separa en dos partes, una en la que se establece la comunicación con el Netscaler y la otra para la comunicación con la plataforma de Cisco Duo:

```
[duo_only_client]
```

```
[radius_server_iframe]
type=citrix_netscaler_rfwebui
ikey=DIMY6690WZMAD2ECBCXN
skey=xxxxxxxxxxxxxxxxxxxxxxxxxxxx
api_host=api-api-dbbecd94.duosecurity.com
failmode=safe
client=duo_only_client
radius_ip_1=192.168.69.2
radius_secret_1=xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
port=1812
```

```
[radius_server_iframe2]
type=citrix_netscaler_rfwebui
ikey=DIMY6690WZMAD2ECBCXN
skey=xxxxxxxxxxxxxxxxxxxxxxxxxxxx
api_host=api-api-dbbecd94.duosecurity.com
failmode=safe
client=duo_only_client
radius_ip_1=192.168.69.5
radius_secret_1=xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
port=1812
```

3.4 Configuración Netscaler

Se configura en el Netscaler los datos del servidor proxy Duo:

Configure Authentication RADIUS Server

Name

SRVDUOPROXY

☒ Server Name ☐ Server IP

Server Name*

10.250.2.162

Port

1812

Secret Key*

.....

Confirm Secret Key*

.....

Test RADIUS Reachability

Test End User Connection

Transport*

UDP

Time-out (seconds)

60

More

OK

Close

Después es necesario añadirlo en la política de "Next Factor"

Authentication Virtual Server > Authentication Policy

Authentication Policy

Add Binding

Unbind

Regenerate Priorities

No action

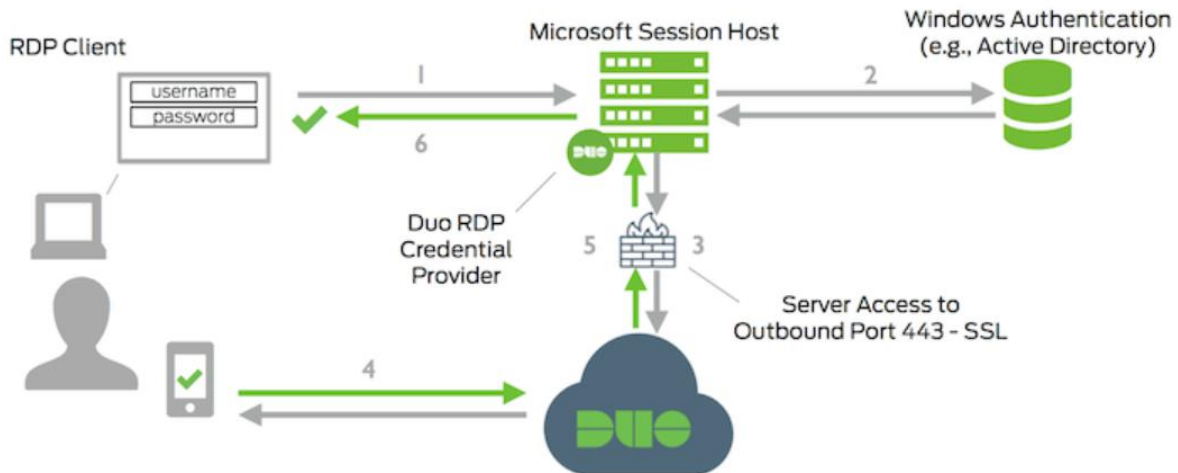
Click here to search or you can enter

	PRIORITY	POLICY NAME	EXPRESSION	ACTION	GOTO EXPRESSION	NEXT FACTOR
<input type="checkbox"/>	100	Corporate-Adv	true	LDAP-Corporative-SVRDC02	NEXT	RADIUS_DuoAuthenticationProxy

Close

4 Configuración RDP

Para la integración de Duo con RDP, es necesario instalar una aplicación en los equipos finales (servidores, equipos...), en los equipos de usuario se ha instalado manualmente, pero para los servidores se ha preparado una GPO y así poder realizar un despliegue centralizado y controlado de forma automática.



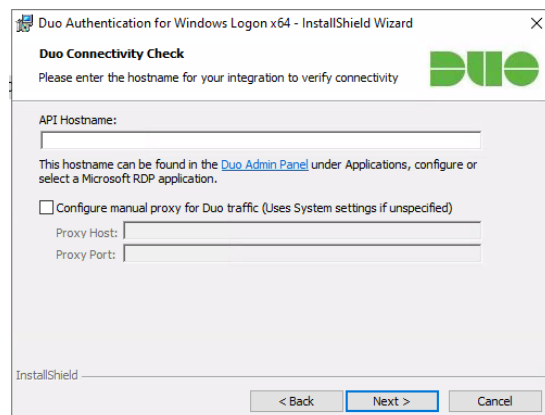
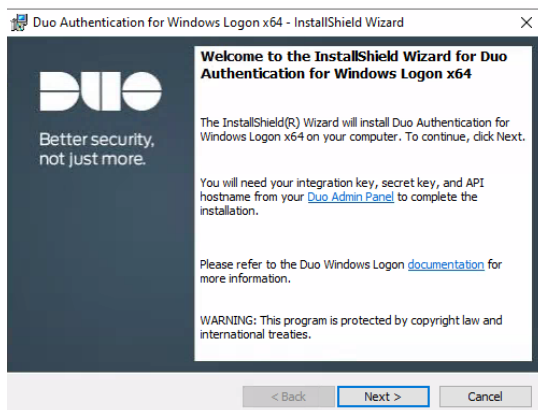
4.1 Instalación de forma manual

Descargar el instalador del siguiente enlace:

<https://duo.com/docs/checksums#duo-windows-logon>

Lanzar la ejecución del instalable descargado:

API Hostname: *api-dbbecd94.duosecurity.com*



Integration Key: *DIXP7WYF8QIU81DD3C98*

Secret Key: *xxxxxx*

5 Configuración Cisco Duo

5.1 Configuración aplicación en Cisco Duo:

Dentro de “Applications” en Cisco Duo está configurada la protección para las aplicaciones RDP-HUNOSA y NetScaler-HUNOSA . En la primera parte se pueden sacar los datos de conexión a configurar en los clientes finales y en el proxy:

RDP-HUNOSA

See the [RDP documentation](#) to integrate Duo into your Microsoft RDP deployment.

Details

Integration key [Copy](#)

Secret key [Copy](#)

Don't write down your secret key or share it with anyone.

API hostname [Copy](#)

NetScaler-HUNOSA

See the [Citrix Gateway documentation](#) to integrate Duo into your Citrix Gateway or NetScaler Gateway device.

Details

Integration key [Copy](#)

Secret key [Copy](#)

Don't write down your secret key or share it with anyone.

API hostname [Copy](#)

Se pueden configurar políticas por grupo de usuarios, estas políticas se aplicarán por encima de las políticas globales, en este caso no existen políticas específicas, por lo que la configuración que se aplica es la de la política global:

Global policy

Global Policy

This policy always applies to all applications.

[Edit Global Policy](#)

New User policy	Prompt unenrolled users to enroll whenever possible. ⓘ
Authentication policy	Require two-factor authentication or enrollment when applicable, unless there is a superseding policy configured.
Remembered devices	Don't remember devices for browser-based applications. Don't remember devices for Windows Logon.
Authorized networks	No networks.
Authentication methods	Deny: Duo Mobile passcodes. Only allow: Verified Duo Push (3-digit verification code), Phone callback, SMS passcodes, Hardware tokens, Security Keys (WebAuthn), Touch ID.

En las configuraciones globales de la aplicación se configura el texto leído en la locución al recibir la llamada telefónica para la doble autenticación:

Settings

Type Microsoft RDP

Name RDP-HUNOSA

Duo Push users will see this when approving transactions.

Username normalization

☐ None

☒ Simple

"DOMAIN\username", "username@example.com", and "username" are treated as the same user.

Controls if a username should be altered before trying to match them with a Duo user account.

Voice greeting

Bienvenido a DUO. Presione asterisco noventa y cualquier otra tecla.

Specify the message read to users who use phone callback, followed by authentication instructions. Maximum 512 characters.

Notes

For internal use. Maximum 512 characters.

En las configuraciones globales de RDP-HUNOSA también se definen el número de conexiones offline que se pueden realizar consecutivamente y los medios usados para esa autenticación.

Offline Access Settings

Offline access

☒ Offline login and enrollment is enabled

These settings will take effect the next time the application connects to the internet.

Limit access by groups

☐ Only allow offline login from users in certain groups

Select groups

If **Permitted groups** is enabled, users must also be members of a permitted group to be allowed to log in offline.

Prevent offline login after

☒

10

offline logins

☐

7

days offline

These counts reset each time the application connects to the internet.

Offline authentication methods

☒ Duo Mobile Passcode

☐ Security Key

When offline, these settings override all other authentication method policies.

5.2 Configuración usuarios en Cisco Duo:

5.2.1 Configuración manual

Username: Tiene que ser igual que el usuario del dominio

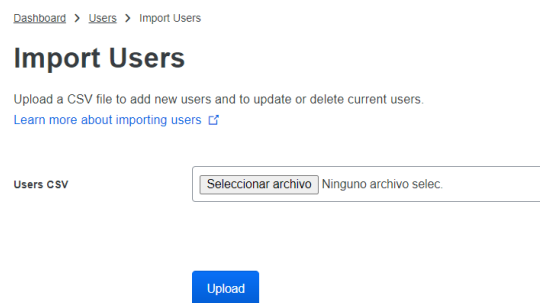
Status:

- Active: Requerido el doble factor de autenticación
- Bypass: Permite al usuario saltarse la doble autenticación
- Disabled: Al usuario se le denegará el acceso.

Groups: Se pueden organizar los usuarios por grupos y aplicar políticas específicas a esos grupos.

5.2.2 Importar usuarios

Es posible importar los usuarios a través de un archivo csv,




para ello hay que subirlos con el siguiente formato "https://duo.com/docs/importing-users":

```
username,realname,alias1,alias2,email,status,phone1,platform1,phone2,platform2,group1,group2,notes
jason,Jason Liu,jason@example.com,smithj3,jason@example.com,active,734-555-1234,iphone,734-555-1234,
sally,Sally Jones,sally@example.com,jones5,sally@example.com,disabled,(734)-555-1235,android,(734)-555-1235,
jack,Jack Cruz,jack@example.com,,jack@example.com,bypass,+17345554322,smartphone,,,StdUsers,Net
sarah,Sarah James,sarah@example.com,,sarah@example.com,active,(734) 555-2235,iphone,(734) 555-3444,
bob,Bob Rogers,bob@example.com,rogersb,bob@example.com,active,734 555 3444,landline,734 223 9834,
mary,,,,,delete,,,,,,,,,
```

5.3 Configuración teléfonos en Cisco Duo manualmente:

Acceder al usuario y en la parte de Phones añadir el dispositivo:


Add Phone

 [Learn more about Activating Duo Mobile](#)

Type

☒ Phone
☐ Tablet

Phone number

 +

Show extension field

Optional: Example: "+34 612 34 56 78"

Add Phone

Si el teléfono va con extensión es necesario marcar el campo "Show extensión field" y añadir la extensión, una vez rellenados esos campos nos aparecerán nuevos valores a configurar (retrasar segundos antes de marcar la extensión o esperar segundos después de marcar la extensión)

Extension

341

Only 0-9, #, and * are permitted.

Delay before extension

0

seconds

How long to wait after the switchboard answers the call and before the extension can be dialed.

Delay after extension

0

seconds

How long to wait after dialing the extension and before speaking."

Device name


Optional: Examples: "Work phone", "Old iPod touch"

Type

Landline


Si el teléfono introducido se utilizará para la validación 2FA a través de PUSH, es necesario su activación, para ello hay que acceder de nuevo al teléfono correspondiente y marcar la opción de "Activate Duo Mobile"


Device Info
[Learn more about Activating Duo Mobile](#)



Not using Duo Mobile

Activate Duo Mobile

 **Model**
Unknown

 **OS**
Generic Smartphone

Settings

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 +34 690 12 01 67

Expiration 24 hours after generation

Generate Duo Mobile Activation Code

Se generará un código de activación que hay que abrir desde el dispositivo móvil asociado para vincular la cuenta. Este código es una URL que se abrirá desde el móvil y se puede enviar por SMS o Email.

Send links via ☒ SMS ☐ Email

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:
<https://m-dbbecd94.duosecurity.com/activate/80QKwbFC6JoFmwYEw83O>

Send Instructions by SMS