



VIRTUAL
CABLE

Doble Factor de Autenticación en UDS Enterprise (MFA)





Indice

INTRODUCCIÓN	2
Metodos de doble autenticación.....	2
1. Correo electrónico multi factor	3
1.1. Política para usuarios sin compatibilidad con MFA.....	5
1.2. Atributo mail.....	5
1.3. RESULTADOS	6
2. Desafío OTP de radius	7
3. SMS a través de HTTP	10
4. MFA basado en TOTP	13
4.1 Resultados	14
4.2 Restablecer MFA TOTP a un usuario.	15
UDS ENTERPRISE, EL SOFTWARE VDI DE VIRTUAL CABLE	16
Sobre UDS Enterprise	16
Sobre Virtual Cable	16



INTRODUCCIÓN

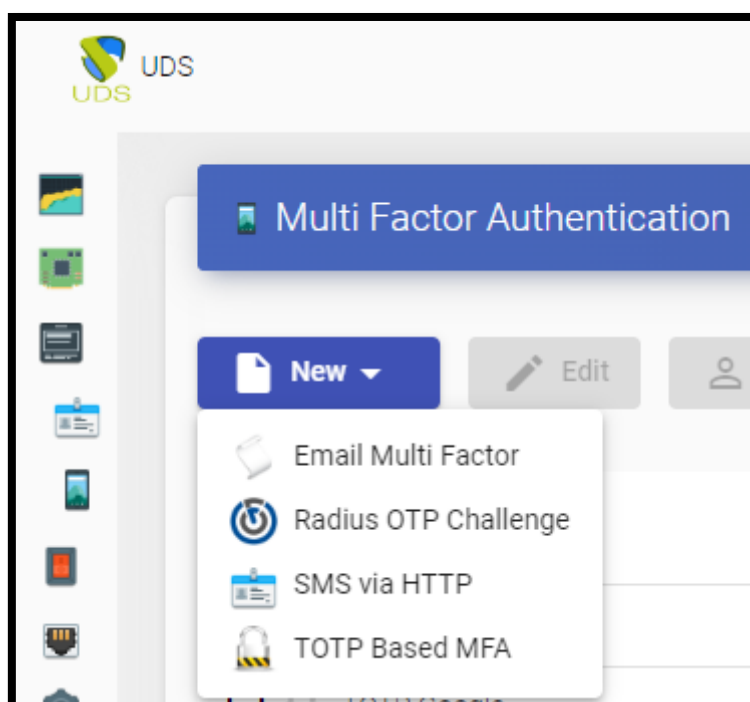
En el siguiente manual se detallan los pasos a seguir para conseguir realizar una doble autenticación a nuestros usuarios cuando accedan a la plataforma de UDS Enterprise.

Esta doble autenticación se podrá realizar en cualquiera de los autenticadores existente en UDS

NOTA: Es muy importante en el caso de usar MFA con UDS tener la hora de los appliance de UDS correctamente configurada, en caso contrario pueden aparecer errores al momento de la autenticación.

Metodos de doble autenticación

En UDS Enterprise se han incorporado 4 métodos principales de doble autenticación.



La configuración de este método se realizará en el panel de control de UDS accediendo a la pestaña "Multifactor".



1. Correo electrónico multi factor

Mediante este método, el usuario primero se autenticará con su usuario y contraseña para después ser redirigido a un segundo proceso de autenticación donde recibirá un correo electrónico con el código necesario para poder autenticarse finalmente en su plataforma UDS Enterprise.

En la configuración del mismo indicaremos lo siguientes datos como mínimo:

Edit MFA	
Main	SMTP Server
Tags	
Tags for this element	
Name *	
Correo	
Comments	
Comments for this element	
Device Caching	
0	
MFA code validity	
5	

Pestaña "Principal":

- Nombre: nombre del método.
- Cacheo del dispositivo: Tiempo en horas para almacenar en caché el dispositivo para que MFA no sea necesario nuevamente. Basado en el usuario.
- Validez del código MFA: Tiempo en minutos para permitir el uso del código MFA.



Edit MFA

Main
SMTP Server
Config

SMTP Host *
smtp.gmail.com:587

Security *
TLS

Username
noreply@udsenterprise.com

Password

Pestaña "Servidor SMTP"

En esta pestaña será donde indicaremos lo datos relacionados con nuestro servidor de correo electrónico donde este es capaz de mandar los emails correspondientes y lo tiene activado.

En este ejemplo se utiliza Gmail.

Edit MFA

Main
SMTP Server
Config

Subject *
Verification Code

From Email *
noreply@udsenterprise.com

Enable HTML
 No

Policy for users without MFA support *
Deny user login

Mail OTP Networks
Networks for Email OTP authentication

Mail text *
Bienvenido/a {username},
usted esta intentado hacer login en la plataforma UDS Enterprise.
Su código de acceso es: {code}

Mail HTML

- **Asunto:** mostrado en el correo electrónico.

- **Email de origen:** el emisor del correo electrónico.

- **Habilitar HTML:** combinado con la casilla "Correo HTML" podremos introducir condigo HTML en el correo electrónico mandado.

- **Política para usuarios sin compatibilidad con MFA:** explicado a continuación.

- **Redes OTP de correo:** las redes a las que se le aplicara el MFA, si se deja vacío se aplica a cualquier red.

- **Texto de correo:** texto plano que se mostrará en el correo electrónico.

NOTA se puede indicar {username} con el nombre de usuario, {IP} ip de origen

del usuario y el más importante: el {code} donde se rellenará el código necesario para el MFA.



1.1. Política para usuarios sin compatibilidad con MFA

Con la política elegida podremos:

- Allow user login (TODAS LAS REDES): aunque el usuario no pueda autenticarse por MFA se le **ACEPTARA** el acceso.
- Deny user login (TODAS LAS REDES): si el usuario no puede autenticarse por MFA se le **DENEGARA** el acceso. (Esta es la opción más recomendable).
- Allow user to login if it IP is in the networks list (REDES, IPs, Rangos... incluidas en el apartado REDES): si el usuario no puede autenticarse por MFA pero su IP pertenece a la lista de RED se le **ACEPTARA** el acceso.
- Deny user to login if it IP is in the networks list: si el usuario no puede autenticarse por MFA y su IP pertenece a la lista de RED se le **DENEGARA** el acceso.

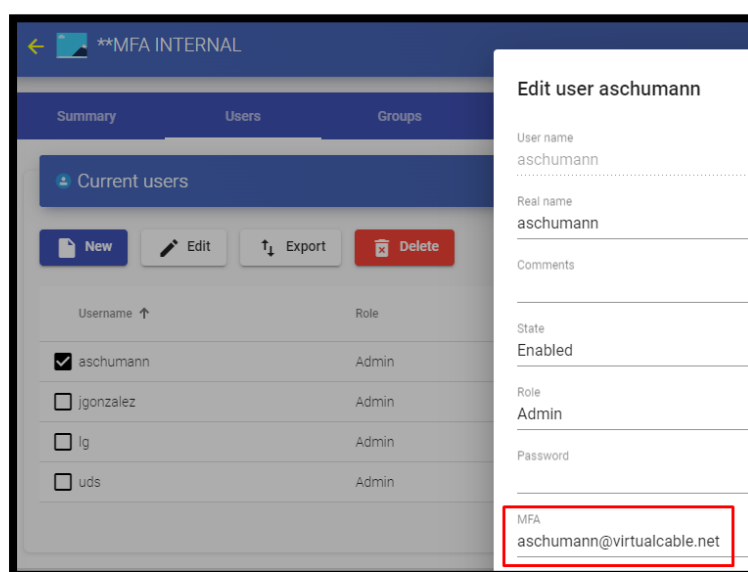
1.2. Atributo mail

Para que este tipo de método funcione correctamente se necesita el correo de destinatario para que al usuario final le lleguen los correos eléctricos.

Existen dos métodos para conseguir esta información:

Internal Database

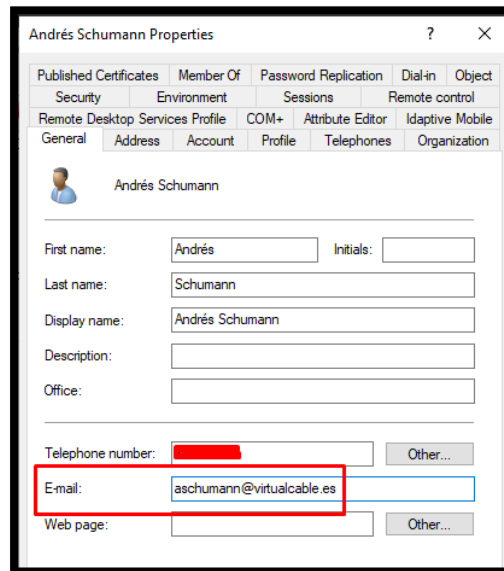
Para conseguir el mail del usuario en autenticadores como “base de datos interna” por ejemplo, deberemos indicar su mail al editar o crear un usuario en el apartado “**MFA**”:





Active Directory

En el caso de que estemos utilizando un dominio, el correo se extraerá directamente de la información / atributos del usuario en el dominio:



Andrés Schumann Properties

Published Certificates | Member Of | Password Replication | Dial-in | Object
Security | Environment | Sessions | Remote control
Remote Desktop Services Profile | COM+ | Attribute Editor | Adaptive Mobile
General | Address | Account | Profile | Telephones | Organization

Andrés Schumann

First name: Andrés Initials:

Last name: Schumann

Display name: Andrés Schumann

Description:

Office:

Telephone number: Other...

Email: aschumann@virtualcable.es

Web page: Other...

1.3. RESULTADOS

RESULTADO CON TEXTO PLANO



Verification Code Recibidos x

N noreply@udsenterprise.com
para aschumann ▾

Bienvenido/a aschumann@vc.local ,
usted esta intentado hacer login en la plataforma UDS Enterprise.

Su código de acceso es: 149607

← Responder → Reenviar



RESULTADO CON CÓDIGOP HTML



Mail HTML

```
<pre>Bienvenido/a {username} ,  
usted esta intentado hacer login en la plataforma UDS Enterprise.</pre>
```

```
<p>Su código de acceso es: <b>{code}</b></p>
```



noreply@udsenterprise.com

para aschumann ▾

Bienvenido/a aschumann@vc.local ,
usted esta intentado hacer login en la plataforma UDS Enterprise.

Su código de acceso es: **571852**

2. Desafío OTP de radius

Mediante este método, el usuario primero se autenticará con su usuario y contraseña para después ser redirigido a un segundo proceso de autenticación donde deberá introducir el código correspondiente suministrado por su servidor radius para poder autenticarse finalmente en su plataforma UDS Enterprise.



Al crear y configurar este método se deberán indicar los siguientes datos como mínimo:

New MFA

Main
Config

Tags

Tags for this element

Name *

Name of this element

Comments

Comments for this element

Host *

Radius Server IP or Hostname

Port *

1812

Secret *

Radius client secret

All users must send OTP

No

NAS Identifier *

uds-server

Device Caching

0

MFA code validity

5

Pestaña "Principal"

- Nombre: nombre del método.
- Servidor: IP o FQDN del servidor radius.
- Puerto: puerto utilizado por el servidor radius.
- Secret: generado al crear el cliente radius.
- Identificador NAS: nombre identificativo.
- Cache del dispositivo: Tiempo en horas para almacenar en caché el dispositivo para que MFA no sea necesario nuevamente. Basado en el usuario.
- Validez del código MFA: Tiempo en minutos para permitir el uso del código MFA.

Pestaña "Configuración"



New MFA

Main
Config

Radius OTP communication error action *

Allow user login

Radius OTP networks

Networks for Radius OTP authentication

User without defined OTP in server *

Allow user login

Tanto para la opción de “Acción de error de comunicación Radius OTP” como para “Usuario sin OTP definida en servidor” se define la acción que se llevara a cabo cuando el usuario no pueda realizar el OTP por algún tipo de error o no lo tenga definido en el servidor, entre las 4 opciones a elegir están:

- Allow user login (TODAS LAS REDES): aunque el usuario no pueda autenticarse por MFA se le ACEPTARA el acceso.
- Deny user login (TODAS LAS REDES): si el usuario no puede autenticarse por MFA se le DENEGARA el acceso. (Esta es la opción más recomendable).
- Allow user to login if it IP is in the networks list (REDES, IPs, Rangos... incluidas en el apartado REDES): si el usuario no puede autenticarse por MFA pero su IP pertenece a la lista de RED se le ACEPTARA el acceso.
- Deny user to login if it IP is in the networks list: si el usuario no puede autenticarse por MFA y su IP pertenece a la lista de RED se le DENEGARA el acceso.



3. SMS a través de HTTP

Mediante este método, el usuario primero se autenticará con su usuario y contraseña para después ser redirigido a un segundo proceso de autenticación donde recibirá un SMS con el código necesario para poder autenticarse finalmente en su plataforma UDS Enterprise.

En un "SMS Vía HTTP" Los parámetros mínimos por configurar son:

Pestaña "Principal":

Tags
Tags for this element
Name *
Name of this element
Comments
Comments for this element
Device Caching
0
MFA code validity
5

Nombre: Nombre que se le indicará el elemento.

Cacheo del dispositivo: Tiempo en horas para almacenar en cache el dispositivo para que el MFA no sea necesario nuevamente.

Validez del código MFA: Tiempo en minutos para permitir el uso del código MFA.



Pestaña "Servidor HTTP":

Edit MFA

Main HTTP Server HTTP Authentication HTTP Response Config

URL pattern for SMS sending *

`https://dashboard.360nrs.com/api/rest/sms`

Ignore certificate errors

No

SMS sending method *

POST

Parameters for SMS POST/PUT sending

`{"to":["{phone}"], "from":"UDSAuth", "message": "Hi {username}, your access code is {code}"}`

Headers for SMS requests

Content-Type: application/json

SMS encoding *

utf-8

Patrón de URL para envío de SMS: Patrón de URL para envío de SMS.

En la documentación de API de cada empresa o aplicación que provea esta tecnología debería existir un URL base para poder actuar y realizar acciones con la API.

Método de envío de SMS: Metodo que se usará para enviar SMS.

Parámetros para el envío de SMS POST/PUT: los datos necesarios para hacer llegar el código al usuario, deberá contener como mínimo al menos el {code} para que el usuario reciba el código de seguridad. Para un mensaje personalizado este puede contener las siguientes variables:

- * {code} - el código a enviar
- * {phone/+phone} - el número de teléfono
- * {username} - el nombre de usuario
- * {justUsername} - el nombre de usuario sin @...

Encabezados para solicitudes de SMS: la API de las diferentes tecnologías pueden necesitar unos encabezados específicos para su correcto funcionamiento por lo que se deberá leer la documentación si existe de esa tecnología específicamente.

Codificación de SMS: Codificación que se usará para el envío de SMS.



Pestaña "Autenticación HTTP":

SMS authentication method *
None
SMS authentication user or token
User or token for SMS authentication
SMS authentication password
Password for SMS authentication

Método de autenticación por SMS: Método de autenticación de la API SMS

Usuario o token de autenticación por SMS: Usuario o token para la autenticación SMS

Contraseña de autenticación de SMS: Contraseña para la autenticación SMS

Pestaña "Configuración":

SMS response error action *
Allow user login
SMS networks
Networks for SMS authentication
User without MFA policy *
Allow user login

Acción de error de respuesta de SMS: Acción que realizará el servidor en caso de error

Política para usuario sin MFA: Acción que se realizará con usuarios sin una política de MFA configurada.



4. MFA basado en TOTP

Mediante este método, el usuario primero se autenticará con su usuario y contraseña para después ser redirigido a un segundo proceso de autenticación donde deberá introducir el código TOTP generado cada cierto tiempo en nuestra aplicación como por ejemplo Google Authenticator, Microsoft, etc para poder autenticarse finalmente en su plataforma UDS Enterprise.

Al crear y configurar este método se deberán indicar los siguientes datos como mínimo:

Editar MFA	
Principal	Configuración
Etiquetas	
Etiquetas para este elemento	
Nombre *	
TOTP Google	
Comentarios	
Comentarios para este elemento	
Editor	
UDS Authenticator	
Cacheo del dispositivo	
1	
Validez del código MFA	
1	

- **Nombre:** nombre del método

- **Cache del dispositivo:** Tiempo en horas para almacenar en caché el dispositivo para que MFA no sea necesario nuevamente. Basado en el usuario.

- **Validez del código MFA:** Tiempo en minutos para permitir el uso del código MFA.



Pestaña "Configuración":

Edit MFA

Main
Config

Valid Window *

1

TOTP networks

Users within these networks will not be asked for OTP

Ventana válida: Número de códigos válidos antes y después del actual.

4.1 Resultados

Al realizar la configuración completamente pasaremos a iniciar sesión un usuario que tenga indicado en su autenticador el método elegido.

Username *

aschumann

Password

Authenticator

****MFA INTERNAL**

Authentication Code *

[Submit](#)



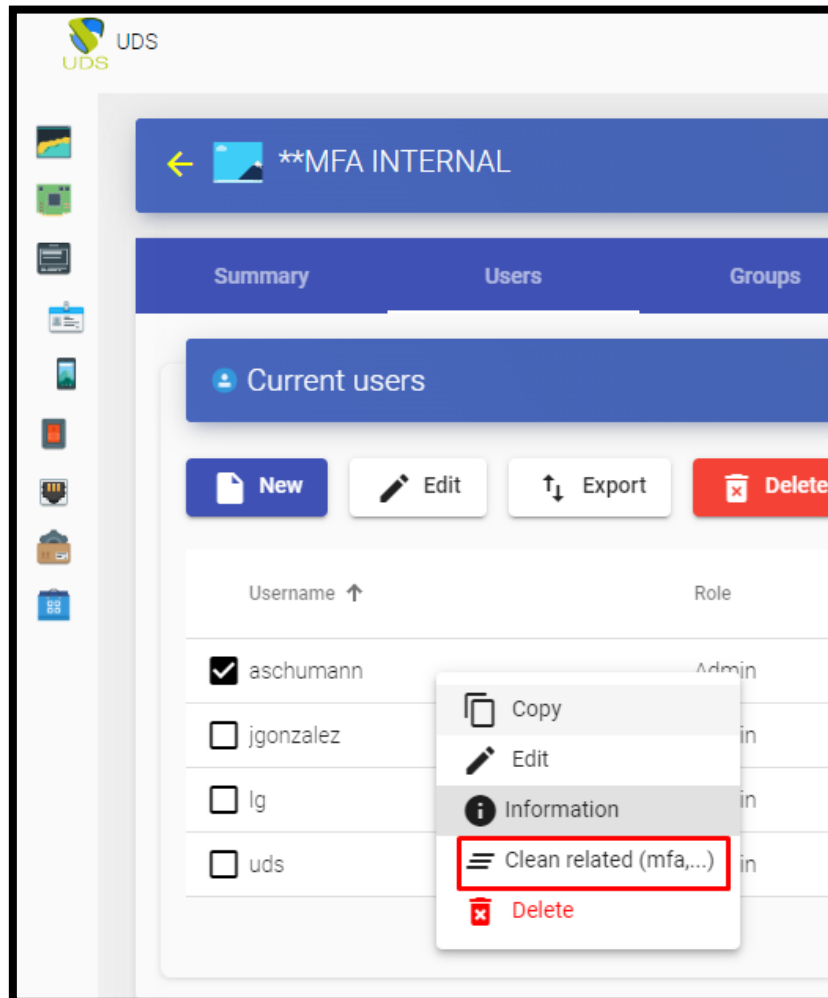
Please, use your Authenticator to add your account. (i.e. Google Authenticator, Authy, ...)

Se podrán utilizar aplicaciones como Google Authenticator, Authy,....



4.2 Restablecer MFA TOTP a un usuario.

Si por alguna razón el usuario necesita restablecer su usuario para que le vuelva a mostrar nuevamente el QR se deberá acceder al autenticador de ese usuario y hacer clic derecho sobre ese usuario y picha en **“Limpiar relacionado (mfa,...)”**





UDS ENTERPRISE, EL SOFTWARE VDI DE VIRTUAL CABLE

Sobre UDS Enterprise

[UDS Enterprise](#) es un nuevo concepto de software para crear una plataforma de **virtualización del puesto de trabajo** totalmente **personalizada**. Proporciona **acceso seguro 24x7**, desde cualquier **lugar** y **dispositivo** a todas las aplicaciones y software de una organización o centro educativo.

Permite aunar en una única consola **virtualización** de **escritorios** y **aplicaciones Windows** y **Linux**, además de **acceso remoto** a equipos Windows, Linux y macOS. Su base Open Source garantiza **compatibilidad con cualquier tecnología** de terceros. Se puede desplegar **on premise**, en nube pública, privada, híbrida o **multicloud**. Incluso **combinar** varios entornos al mismo tiempo y realizar **desbordamientos automáticos** e inteligentes para optimizar el rendimiento y la eficiencia. Todo con una **única suscripción**.

Sobre Virtual Cable

[Virtual Cable](#) es una compañía especializada en la **transformación digital** del **puesto de trabajo**. La empresa desarrolla, soporta y comercializa UDS Enterprise. Su equipo de expertos ha diseñado soluciones **VDI** a medida de **cada sector** para proporcionar una experiencia de usuario única y totalmente adaptada a las necesidades de cada perfil de usuario. Los profesionales de Virtual Cable tienen **más de 30 años de experiencia** en TI y desarrollo de software y más de 15 en tecnologías de virtualización. Cada día se despliegan **millones de escritorios virtuales Windows y Linux con UDS Enterprise en todo el mundo**.