CONFIGURAR OPCIONES DE MFA EN LA CUENTA DE USUARIO

Antes de empezar con la configuración del cliente de VPN para MFA es recomendable que el usuario tenga configuradas las opciones para recibir el segundo factor de autenticación.

Si es la primera vez que va a usar este sistema de MFA, siga estos pasos, que figuran a continuación. Si ya está usando el MFA para otros servicios de M365, puede obviar este paso previo y puede pasar directamente al apartado 2 para la configuración del MFA para el cliente de VPN (forticlient) de este documento.

<u>1.- CONFIGURAR LAS OPCIONES Y EL MODO DE AUTENTICACIÓN MFA QUE SE PEDIRÁ EN LAS</u> <u>APLICACIONES.</u>

 Acceder a <u>https://aka.ms/mfasetup</u> Se presentará una pantalla similar a la siguiente. De entre las opciones que se presenta, os recomendamos activar al menos 2 (Teléfono de autenticación y Aplicación de autenticación o token).

UNIVERSIDAD DE LA RIOJA	fernando@unirioja.es	?
Comprobación de seguridad adicional Contraseñas de aplicación		
Al iniciar sesión con su contraseña, ahora también deberá responder desde un dispositivo registra sesión solo con una contraseña robada. Ver vídeo para saber cómo proteger su cuenta	ado. De este modo, los hackers tendrán más dificultades para iniciar	
¿cuál es su opción preferida?		
Se usará esta opción de configuración de forma predeterminada.		
Notificarme a través de la aplicac 🗸		
¿cómo desea responder?		
Seleccione y configure una o más de estas opciones. Más información		
Teléfono de autenticación * España (+34) V		
□ Teléfono de la oficina (no use un teléfono Lync) Ext	tensión	
☐ Teléfono de autenticación Seleccione su país o región ✓		
Aplicación autenticadora o token Configurar aplicación autenticadora		
Guardar cancelar		
Sus números de teléfono sólo se usarán para proteger su cuenta. Se aplicará la tarifa estándar de	teléfono y SMS.	

 Para el uso de la Aplicación de Autenticación, se necesitará instalar en el dispositivo móvil una APP (Microsoft Authenticator, Google Authenticator, otras).
 Recomendamos instalar "Microsoft Authenticator" que está disponible para Android e iOS.



3. Para integrar la autenticación MFA de la VPN, escanear el código QR que se proporcionará por Microsfoft que se genera en el apartado 1 de este documento en *"Configurar aplicación autenticadora"*.

2.- CONFIGURACIÓN DE DOBLE FACTOR DE AUTENTICACIÓN EN CLIENTE VPN (FORTICLIENT)

Para la configuración del 2FA en el acceso al servicio de VPN de la UR con el SW forticlient, seguir los siguientes pasos:

- El PAS y PDI no necesita hacer este paso. Los alumnos tienen que autosuscribirse al grupo que permite el acceso por vpn: fwgs_vpn_alum_ok.
 En este <u>enlace</u> puedes ver un video de cómo hacerlo.
 Una vez hecho tendrás que esperar a que se sincronicen los sistemas de gestión de identidad. Como se realiza cada hora tendrás que esperar eso como máximo para acceder.
- 2. Instalar el software

En función del dispositivo y/o sistema operativo desde el que va a acceder, descargue e instale en el equipo **la última versión** del cliente de VPN que le corresponda <u>para Windows 10 o superior</u> <u>Mac OS 11 Big Sur o superior</u> <u>Linux tipo Debian</u> <u>Linux tipo Redhat</u>

- 3. Una vez instalado, inicie FortiClient, marque la casilla de verificación y haga clic en el botón "*Aceptar*".
- 4. En la siguiente pantalla, deberá hacer clic en "Configurar VPN".





- 5. En la nueva pantalla, deberá completar la información como se especifica a continuación y se ve en la siguiente captura. Después hacer clic en "*Guardar*".
 - a. Seleccione la pestaña "VPN SSL"
 - b. Nombre de conexión "VPN Unirioja"
 - c. Descripción "Conexión VPN Unirioja"
 - d. Gateway Remoto: "boo.unirioja.es"
 - e. Personalizar puerto: 10443
 - f. Enable SSO for VPN Tunel

FortiClient		-		×
Archivo Ayuda				
FortiClient VPN	*	٠	•	
Upgrade to the full version to access additional features	and receive technical support.			
Nueva Conexió	n VPN			
VPN	VPN SSL VPN IPsec XML			
Nombre de Conexión	VPN Unirioja			
Descripción	Conexión VPN Unirioja			
Gateway Remoto	boo.unirioja.es * *Adicionar Gateway Remoto * Personalizar puerto 10443 Enable Single Sign On (SSO) for VPN Tunnel * Use external browser as user-agent for saml user authentication Cancelar Guardar			

6. Una vez creada la conexión VPN, haga clic en "SAML Login".

FortiClient	-		×
Archivo Ayuda			
FortiClient VPN	*	i i	
opprate to the full version to access additional relatics and receive technical support.			
Ombre de VPN VPN Unirioja SAML Login			

7. Luego ingrese los datos de su CUASI: "Nombre_Usuario y contraseña".

FortiClient	– 🗆 X
Archivo Ayuda	
FortiClient VPN	# © 0 A
Upgrade to the full version to access a 😨 FortiClient (49) — 🗆	×
	*
UNIVERSIDAD DE LA RIOJA	
Selección de la cuenta	
@unirioia.es	:
Usar otra cuenta	
Términos de uso Privacidad y cookies ····	-

8. Se le pedirá que autorice el inicio de sesión con Multi-Factor Authentication (MFA) utilizando el método de su elección: Token, llamada telefónica, SMS, aprobación. Estos son las posibles opciones:

ur	UNIVERSIDAD DE LA RIOJA
	@unirioja.es
Com	pruebe su identidad
0	Aprobar una solicitud en la aplicación Microsoft Authenticator
123	Usar un código de verificación
\Box	Enviar un mensaje de texto al +XX XXXXXXXX
R	Llamar al +XX XXXXXXXXX
Más info	ormación
¿Están a Compru	ctualizados los métodos de verificación? ébelo en https://aka.ms/mfasetup
	Cancelar
Inicio d	e sesión en Office365

9. En la siguiente imagen aparece la opción de "aprobación", por lo que según el método elegido, pueden aparecer otro tipo de pantallas diferentes.

FortiClient Archivo Ayuda		-		×	
FortiClient VPN	ñ	٠	•	0 A	
Upgrade to the full version to access a line inclar sesión en la cuenta – C X					
@unirioja.es					
Aprobar la solicitud de inicio de					
Abra la aplicación de Microsoft Authenticator y					l
apruebe la solicitud para iniciar sesión.					l
No puedo usar mi aplicación Microsoft Authenticator en este momento					l
Más información —					l
Inicio de sesión en Office365					

10. Si se encuentra bloqueado en una pantalla con una cuenta atrás, o no le conecta al servicio de VPN, cierre la ventana "Inicio sesión en la cuenta" y haga clic de nuevo en "Inicio de sesión SAML".

FortiClient				_		×
FortiClient VP	N				•	0
Upgrade to the full version to access a	FortiClient (120) Redirecting to remote id in 3 second If you were not redirecting	- D	×			
FortiClient Archivo Ayuda FortiClient VPN	١			-	•	×
Upgrade to the full version to access add	Itonal features and receive technical support.	✓ =				

11. Ante la aparición de pregunta de "¿Quiere mantener la sesión iniciada?" que aparece en la siguiente ventana, pulse "NO", ya que en caso contrario no se le volverá a pedir la autenticación, y cualquier otra persona que use ese equipo podrá establecer la VPN con sus credenciales.



12. Si ha configurado bien el perfil y ha introducido correctamente los datos de autenticación, debería estar conectado.

FortiClient		-	×
Archivo Ayuda			
FortiClient VPN		* •	Ð 🔒
Upgrade to the full version to access additional features and receive technical su	ipport.		
VPN Conectada			
Nombre de VPN Dirección IP Nombre de Usuario Duración Bytes Recibidos Bytes Enviados Desco	VPN Unirioja 10.140. 00:00:12 11.99 KB 15.95 KB		

13. Cuando haya finalizado la sesión de VPN, recuerde desconectar el cliente.