

Socialización configuración segura de acceso VPN – FortiClient

Desde Jhon Hader Rodríguez Perdomo <Jhon.Rodriguez@icbf.gov.co>

Fecha Mié 10/06/2026 16:17

Para Diego Andres Pulecio Barahona <Diego.Pulecio@icbf.gov.co>

CC Paola Sabogal Valdes <Paola.Sabogal@icbf.gov.co>

Cordial saludo, Diego.

De manera atenta me permito compartir la información relacionada con la configuración segura del acceso a la **VPN** institucional mediante **FortiClient**, para su conocimiento y apoyo en caso de que algún colaborador de la **Regional Guaviare** requiera orientación durante el proceso.

De acuerdo con la guía socializada, los colaboradores que cuenten con permisos de VPN deberán verificar que la conexión tenga habilitadas las siguientes opciones:

1. **Puerto personalizado:** 10443
2. **Inicio de sesión único SSO para el túnel VPN:** habilitado
3. **Autenticación mediante cuenta institucional Microsoft 365**
4. **Validación mediante doble factor de autenticación MFA**
5. En caso de aplicar, uso del navegador externo como agente de usuario para autenticación SAML.

Es importante tener presente que esta configuración aplica únicamente para los colaboradores que tienen permisos de acceso VPN autorizados, por lo cual no corresponde realizar configuraciones a usuarios que no cuenten previamente con dicho permiso.

Agradezco tener en cuenta esta información para el acompañamiento en sitio, especialmente cuando los usuarios reporten inconvenientes de acceso a la VPN o dudas frente al inicio de sesión con su cuenta institucional.

Cliente ZTNA

EDIT VPN

VPN SSL

VPN IPsec

XML

Nombre de Conexión

VPN_ICBF

Descripción

Remote Gateway

181.59.43.4

X

+ Adicionar Gateway Remoto

☒ Personalizar puerto

10443

Inicio único de sesión

☒ Habilite el inicio de sesión único (SSO) para el túnel VPN

☒ Use un navegador externo como agente de usuario para la autenticación de usuario SAML

☐ Enable auto-login with Azure Active Directory

Certificado de Cliente

Ninguno

▼

☐ Habilitar dirección Dual-stack IPv4/IPv6

Traffic Keep Strategy

Ninguno

▼

Cancel

Save

Edit VPN Connection

Cliente VPN Normal

VPN

SSL-VPN

IPsec-VPN

XML

Connection Name

VPN-ICBF

Description

Remote Gateway

181.59.43.4

X

+Add Remote Gateway

☒ Customize port

10443

☒ Enable Single Sign On (SSO) for VPN Tunnel

☐ Use external browser as user-agent for saml user authentication

☐ Enable auto-login with Azure Active Directory

Cancel

Save

Configura tu acceso a la VPN de forma segura



Para fortalecer la seguridad en tu conexión, sigue estos pasos:

- Activa el inicio de sesión único (SSO) en Forticlient.
- Ingresa con tu cuenta de Microsoft 365.
- Valida tu acceso mediante doble verificación (MFA).

Aplica únicamente para **colaboradores con permisos de VPN.**

DTi con Bienestar Digital

Quedo atento a cualquier novedad que se presente durante el proceso.

Cordialmente,



Jhon Hader Rodríguez Perdomo
Contratista
Grupo Interno de Trabajo de Gestión Misional
ICBF Sede Regional Guaviare
Av. Colonizadores No. 23 – 106
Teléfono: 601 4377630 Ext. 880003
www.icbf.gov.co

Clasificación de la información: **CLASIFICADA**