

C I C E S E

MANUAL DE CONFIGURACIÓN DE VPN



Departamento de Redes - Dirección de Telemática

Introducción

Este documento ofrece una guía para la configuración de una conexión VPN de tipo IPSEC en dispositivos que operan utilizando el cliente de Fortinet-VPN. El seguimiento de este manual requiere de:

- El servicio de MFA en un dispositivo (manual disponible en <https://telematica.cicese.mx/servicios/servicios-vpn/>)
- Cuenta configurada en <https://balam.cicese.mx/> (manual disponible en <https://telematica.cicese.mx/servicios/servicios-vpn/>)

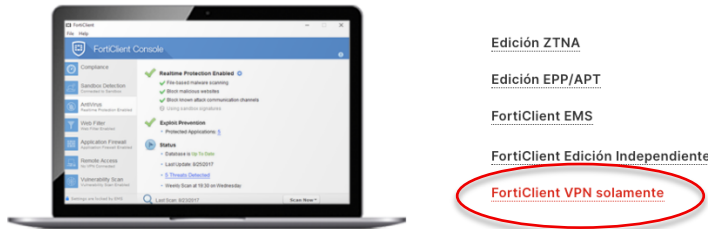
Procedimiento

La configuración se realiza a través de un programa instalador que puede descargar desde el sitio:

<https://www.fortinet.com/lat/support/product-downloads>

Seleccione la opción “VPN FortiClient solamente” (ver figura):

FortiClient se ofrece con varios niveles de capacidades, con niveles crecientes de protección. Se integra con muchos componentes clave del Fortinet Security Fabric y es administrado centralmente por el servidor de administración de endpoint (EMS)



Seleccione “Descargar VPN para su sistema operativo” (ver figura):

FortiClient VPN solamente

Actualiza tu plan a uno de los niveles Enterprise para obtener soporte, gestión centralizada, evaluación de la postura de confianza cero y más.



En ciertos navegadores la pagina oficial de Fortinet podria pedirle llenar un formulario para proceder a la descarga como el siguiente:

DESCARGUE AHORA

FortiClient VPN-only

Please complete the form below to download and get additional information on FortiClient

Nombre

Apellido

Empresa

Correo electrónico del trabajo

País o región

☐

Doy mi consentimiento para recibir comunicaciones promocionales (que pueden incluir teléfono, correo electrónico y redes sociales) de Fortinet. Entiendo que puedo inhabilitar de forma proactiva las comunicaciones con Fortinet en cualquier momento.

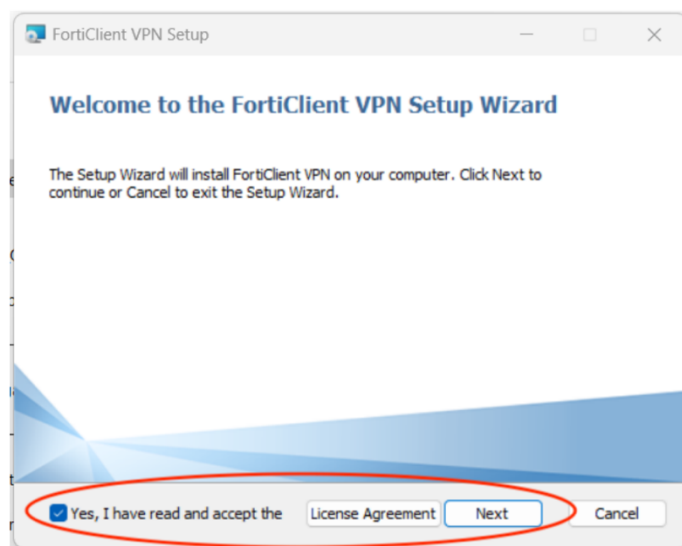
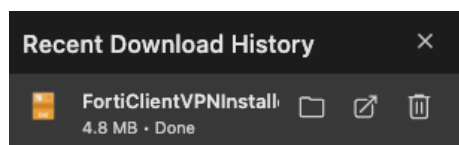
Al hacer clic en enviar, aceptas el Fortinet [Términos y Condiciones](#) & [Política de privacidad](#).

DESCARGUE AHORA

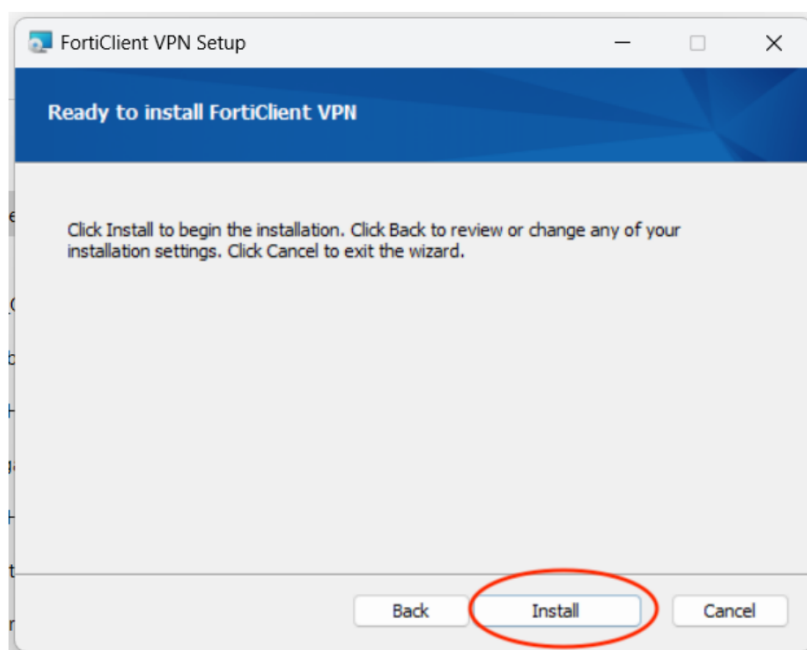
Una vez descargado el instalador, ejecute el programa que acaba de descargar (ver figura):

Manual de Configuración del Cliente de VPN FortiClient
CICESE - Departamento de Redes

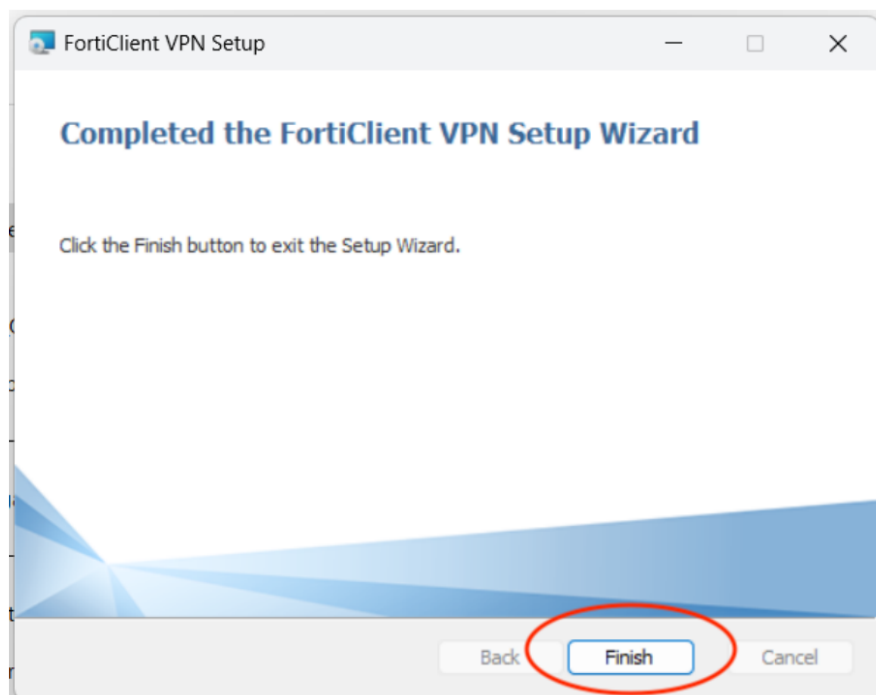
2



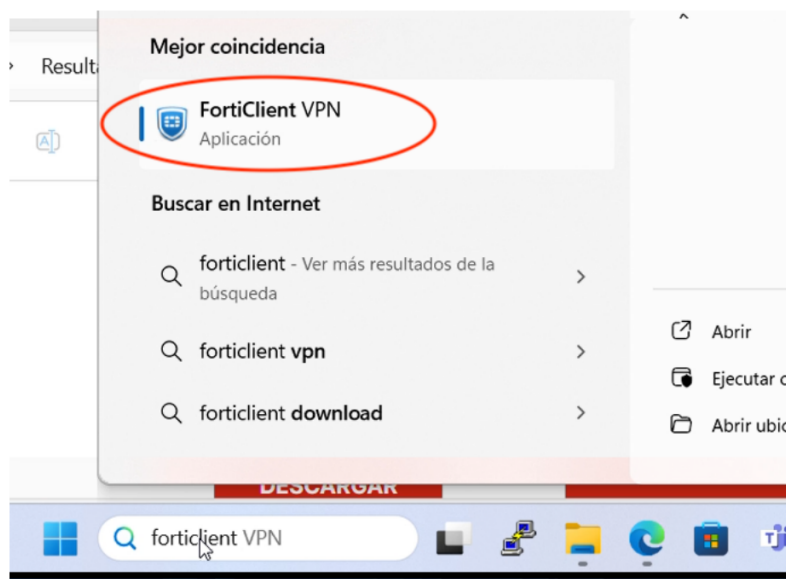
Después haga click en “Install” (ver figura):



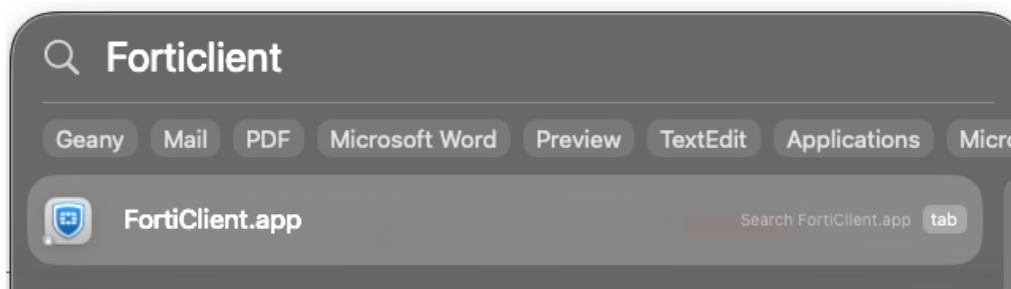
Cuando se complete la instalación, haga click en “Finish” (ver figura):



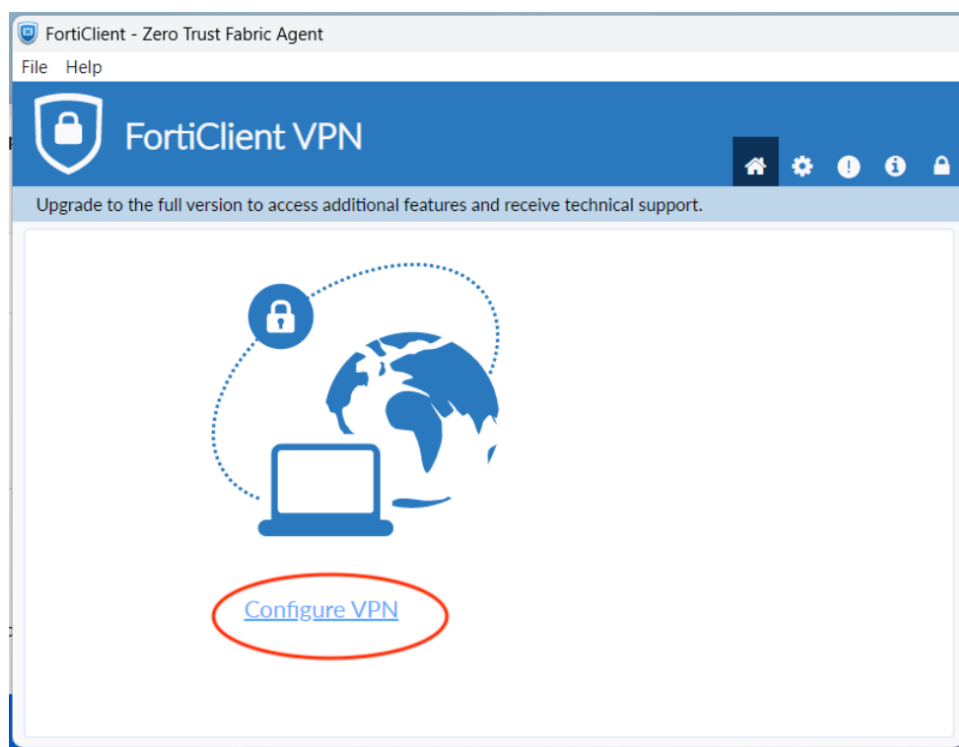
Si se encuentra utilizando un sistema operativo WINDOWS: En la barra inferior de Windows, seleccione “Buscar” (ver figura) y escriba “Forticlient VPN”, de las opciones que aparecerán arriba seleccione “Forticlient VPN, Aplicación” (ver figura):



Si se encuentra utilizando un sistema operativo MacOS: Presione su tecla de Comando “⌘” + Barra Espaciadora y escriba “Forticlient VPN”, de las opciones que aparecerán haga seleccione en “Forticlient.app,” (ver figura):



Para configurar la VPN haga click en “Configure VPN” (ver figura):



Llené los campos con la información mostrada en la siguiente figura, algunas opciones pueden resumidas, para desplegarlas presioné el icono de “+”. En el campo de “Método de autenticación” o “Authentication Method” ingrese lo siguiente “CICESE-VPN” (sin las comillas). En cuenta_de_correo escriba su usuario de correo electrónico de CICESE, sin la terminación @cicese.edu.mx) y haga click en “Save”:

FortiClient VPN

Upgrade to the full version to access additional features and receive technical support.

EDIT VPN Connection

VPN: SSL-VPN Ipssec VPN XML

Connection Name: CICESE VPN GENERAL

Description: CICESE VPN GENERAL

Remote Gateway: 158.97.249.46 ✕
 +Add Remote Gateway

Authentication Method: Pre-shared key
 CICESE-VPN

Authentication (XAuth): ☐ Prompt on login ☒ Save login ☐ Disable

Username: cuenta_de_correo(sin@cicese.edu.mx)
☐ Enable Single Sign On (SSO) for VPN Tunnel

— Advanced Settings

— VPN Settings

IKE: ☒ Version 1 ☐ Version 2

Mode: ☐ Main ☒ Aggressive

Address Assignment: ☒ Mode Config ☐ Manually Set

— Phase 1

Cancel Save

FortiClient VPN

Upgrade to the full version to access additional features and receive technical support.

— Advanced Settings

— VPN Settings

IKE: ☒ Version 1 ☐ Version 2

Mode: ☐ Main ☒ Aggressive

Address Assignment: ☒ Mode Config ☐ Manually Set

— Phase 1

IKE Proposal: Encryption AES128 Authentication SHA256

Encryption AES256 Authentication SHA1

DH Group: ☐ 1 ☐ 2 ☒ 5 ☒ 14 ☐ 15
☐ 16 ☐ 17 ☐ 18 ☐ 19 ☐ 20
☐ 21

Key Life: 86400 sec

Local ID: CICESE-VPN

☒ Dead Peer Detection

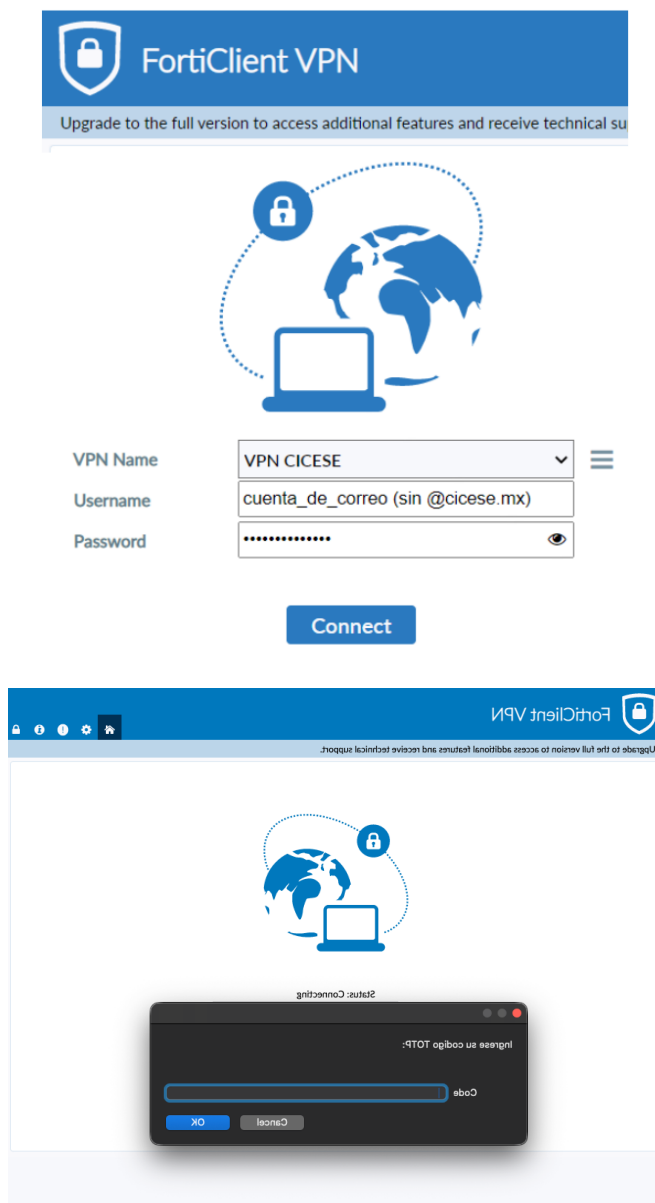
☒ NAT Traversal

+ Phase 2

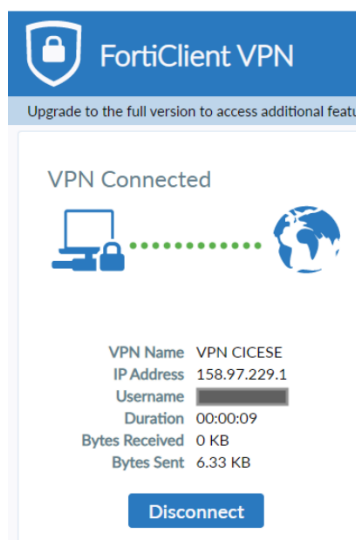
Cancel Save

Para realizar la conexión a la VPN de CICESE escriba la clave de su correo electrónico de CICESE en el campo “Password” y haga click en “Connect”, posteriormente le pedirá su código de MFA anteriormente configurado. (ver figura). **NOTA IMPORTANTE:** El servicio de VPN NO funciona estando conectado a la Red CICESE, por lo que, si intenta conectarse al servidor estando dentro de CICESE, el

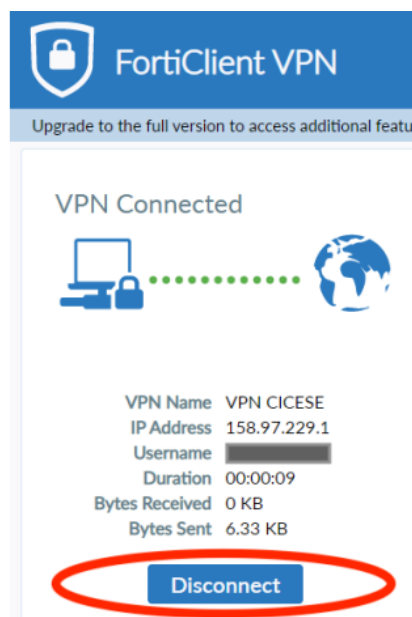
servidor no responderá y se mostrará un mensaje de error. Para probar el servicio es necesario conectarse desde una red externa.



Si la conexión se realizó correctamente, le aparecerá el mensaje de “VPN Connected”, con una dirección IP de CICESE (inicia con 158.97.229), su nombre de usuario y estadísticas de la conexión (ver figura). A partir de este momento tendrá acceso a la red interna del CICESE.



Cuando ya no requiera estar conectado a la VPN y desee terminar la conexión, regrese a la ventana de la conexión de la VPN y haga click en “Disconnect” (ver figura):



Una vez realizado el inicio de sesión este le pedirá un código de múltiple factor de autenticación los manuales para este código se pueden consultar en: <https://telematica.cicese.mx/servicios/servicios-vpn/>