



POLICIA FEDERAL ARGENTINA

Procedimiento FortiClient EMS

**Superintendencia FEDERAL DE TECNOLOGÍAS DE
LA INFORMACIÓN Y COMUNICACIONES**



FortiClient EMS

EDICIÓN 1
Tipo de Documento:
IMPLEMENTACIÓN
Versión: 2.0 / 2023
Página 2 de 17

Tabla de contenido

REQUISITOS MÍNIMOS DE HARDWARE.....	3
CREACIÓN DE WORKGROUP (GRUPO DE TRABAJO)	4
ETIQUETADO DE EQUIPOS.....	5
CREACIÓN DE PERFILES.....	6
REMOTE ACCESS	6
ZTNA DESTINATIONS.....	6
WEB FILTER.....	6
MALWARE PROTECTION.....	6
VULNERABILITY SCAN	6
SANDBOX	7
FIREWALL	7
SYSTEM SETTINGS.....	7
CREACIÓN DE POLÍTICAS	8
MANAGE POLICIES	8
CREACIÓN DE INSTALADOR	9
DEPLOYMENT & INSTALERS	9
DESINSTALACIÓN.....	10
OPCIÓN 1:.....	10
OPCIÓN 2:.....	11
CASO 1: INSTALACIÓN EMS EN EQUIPO CON INTERNET QUE SE SOLICITE VPN PARA INTRA	13
PASO 1	13
PASO 2	13
PASO 3	14
PASO 4	14
PASO 5	15
PASO 6	15
CASO 2: INSTALACIÓN EMS EN EQUIPO CON INTERNET Y QUE YA TIENE INSTALADO FORTICLIENT VPN.	16
PASO 1	16
PASO 2	16
PASO 3	17
CASO 3: INSTALACIÓN EMS EN EQUIPO CON CONECTIVIDAD INTRA.....	17
PASO 1	17
REVISIONES Y MODIFICACIONES:.....	17



FortiClient EMS

EDICIÓN 1
Tipo de Documento:
IMPLEMENTACIÓN
Versión: 2.0 / 2023
Página 3 de 17



Requisitos mínimos de hardware

FortiClient: se puede instalar en cualquiera de los siguientes sistemas operativos (versiones de 32 y 64 bits):

Procesador: Intel Core i3 o equivalente.

Memoria: 4 GB de RAM.

Disco: 10 GB.

Sistemas Operativos:

- Windows: Windows 10 (32 bits y 64 bits), Windows 8.1 (32 bits y 64 bits), Windows 8 (32 bits y 64 bits), Windows 7 (32 bits y 64 bits), Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2.
- MacOS: macOS 10.14 (Mojave), macOS 10.13 (High Sierra), macOS 10.12 (Sierra), macOS 10.11 (El Capitan), macOS 10.10 (Yosemite)



FortiClient EMS

EDICIÓN 1

Tipo de Documento:

IMPLEMENTACIÓN

Versión: 2.0 / 2023

Página 4 de 17

Creación de Workgroup (grupo de trabajo)

- Si requiere crear, modificar, eliminar o asignar una tarea específica un a grupo puede realizarlo de la siguiente manera.

The image consists of two side-by-side screenshots of the FortiClient EMS software interface, specifically the 'Endpoints' section.

Screenshot 1 (Left): Shows a context menu open over a group named 'SOC - TEST'. The menu options include: Exclude from management, Create group, Move devices..., Start full antivirus scan, Start quick antivirus scan, Update signatures, Start vulnerability scan, Patch critical/high vulnerabilities, and Clear events. A red arrow points from the 'Create group' option to the 'All Groups' item in the 'Workgroups' dropdown menu on the left, which is also circled in red.

Screenshot 2 (Right): Shows a context menu open over a group named 'SOC - TEST'. The menu options are identical to the first screenshot: Exclude from management, Create group, Move devices..., Start full antivirus scan, Start quick antivirus scan. A red arrow points from the 'Create group' option to the same 'All Groups' item in the 'Workgroups' dropdown menu on the left, which is also circled in red.



FortiClient EMS

EDICIÓN 1
Tipo de Documento:
IMPLEMENTACIÓN
Versión: 2.0 / 2023
Página 5 de 17

Etiquetado de equipos

- Luego de reportar un equipo, se debe aplicar una etiqueta para identificar si el EMS que se está ejecutando está utilizando VPN o no.

The screenshot shows the FortiClient EMS interface for managing endpoints. The main panel displays a device summary for 'SOC-W-08'. On the right, under 'Classification Tags', there is a modal dialog box. This dialog contains two sections: 'Importance Tags' (with Low, Medium, High, Critical buttons) and 'Custom Tags' (with 'CON VPN' and 'SIN VPN' listed). A red box highlights the 'Add' button in the 'Custom Tags' section, and another red arrow points to the 'CON VPN' tag in the list.



FortiClient EMS

EDICIÓN 1
Tipo de Documento:
IMPLEMENTACIÓN
Versión: 2.0 / 2023
Página 6 de 17

Creación de Perfiles

REMOTE ACCESS

The screenshot shows the FortiClient EMS interface. On the left, there's a sidebar with several options: Dashboard, Endpoints, Deployment & Installers, Endpoint Policy & Components, Endpoint Profiles (which is highlighted with a red box), and Remote Access. The main panel is titled 'Remote-Access Profiles' and shows a list of profiles with a column for 'Name' and 'Updated'. In the top right corner of this panel, there's a red '+' Add button.

ZTNA DESTINATIONS

The screenshot shows the FortiClient EMS interface. On the left, the sidebar has 'Endpoint Profiles' (highlighted with a red box), Remote Access, ZTNA Destinations (highlighted with a red box), and Web Filter. The main panel is titled 'ZTNA Destinations Profiles' and shows a list of profiles with a column for 'Name' and 'Updated'. In the top right corner of this panel, there's a red '+' Add button.

WEB FILTER

The screenshot shows the FortiClient EMS interface. On the left, the sidebar has 'Endpoint Profiles' (highlighted with a red box), Remote Access, ZTNA Destinations, Web Filter (highlighted with a red box), and Vulnerability Scan. The main panel is titled 'Web Filter Profiles' and shows a list of profiles with a column for 'Name' and 'Updated'. In the top right corner of this panel, there's a red '+' Add button.

MALWARE PROTECTION

The screenshot shows the FortiClient EMS interface. On the left, the sidebar has 'Endpoint Profiles' (highlighted with a red box), Remote Access, ZTNA Destinations, Web Filter, Vulnerability Scan, and Malware Protection (highlighted with a red box). The main panel is titled 'Malware Protection Profiles' and shows a list of profiles with a column for 'Name' and 'Updated'. In the top right corner of this panel, there's a red '+' Add button.

VULNERABILITY SCAN

The screenshot shows the FortiClient EMS interface. On the left, the sidebar has 'Endpoint Profiles' (highlighted with a red box), Remote Access, ZTNA Destinations, Web Filter, and Vulnerability Scan (highlighted with a red box). The main panel is titled 'Vulnerability Scan Profiles' and shows a list of profiles with a column for 'Name' and 'Updated'. In the top right corner of this panel, there's a red '+' Add button.



FortiClient EMS

EDICIÓN 1

Tipo de Documento:

IMPLEMENTACIÓN

Versión: 2.0 / 2023

Página 7 de 17

SANDBOX

Endpoint Profiles

Sandbox Profiles

Name

Updated

+ Add

Remote Access

ZTNA Destinations

Web Filter

Vulnerability Scan

Malware Protection

Sandbox

FIREWALL

Endpoint Profiles

Firewall Profiles

Name

Updated

+ Add

Remote Access

ZTNA Destinations

Web Filter

Vulnerability Scan

Malware Protection

Sandbox

Firewall

SYSTEM SETTINGS

Endpoint Profiles

System Settings Profiles

Name

Updated

+ Add

Remote Access

ZTNA Destinations

Web Filter

Vulnerability Scan

Malware Protection

Sandbox

Firewall

System Settings



FortiClient EMS

EDICIÓN 1
Tipo de Documento:
IMPLEMENTACIÓN
Versión: 2.0 / 2023
Página 8 de 17

Creación de Políticas

MANAGE POLICIES

The screenshot shows the 'Endpoint Policies' section of the FortiClient EMS interface. On the left, there's a sidebar with 'Dashboard', 'Endpoints', 'Deployment & Installers', and 'Endpoint Policy & Components' (which is selected and highlighted with a red box). Below that is a 'Manage Policies' button. The main area has a table titled 'Endpoint Policies' with columns for 'Name', 'Assigned Groups', 'Profile Components', 'Off-Fabric Profile C...', and 'Policy Comp...'. At the top right of this table is a '+ Add' button, which is also highlighted with a red box. To the right of the table, there's a legend for profile components: VPN (Remote), ZTNA (Default), WEB (Web Filter), VULN (Vulnerability Scan), MW (Malware Protection), and FW (Firewall).

- **Endpoint Policy**, nombrar la política.
- **Endpoint Group**, seleccionar a que grupos debe impactar (Si crea nuevos grupos y utiliza por ejemplo una política general, siempre debe agregar el nuevo grupo).
- **Profile**, seleccionar los perfiles requeridos.

The screenshot shows the 'Endpoint Policy' configuration screen. The left sidebar has 'Endpoint Policy & Components' selected (highlighted with a red box) and 'Manage Policies'. The main panel has a title 'Endpoint Policy' and a sub-section 'Endpoint Policy Name' with the value 'PRODUCTIVA'. Below it is a 'Endpoint Groups' dropdown menu with several options, one of which is highlighted with a red box. There's an 'Edit' button. The 'Profile (Off-Fabric)' section is shown with a toggle switch. The 'Profile' section lists various profiles: VPN, WEB, VULN, MW, SB, FW, and SYS. Each profile has a small icon and a status indicator. At the bottom are 'Save' and 'Cancel' buttons.



FortiClient EMS

EDICIÓN 1

Tipo de Documento:

IMPLEMENTACIÓN

Versión: 2.0 / 2023

Página 9 de 17

Creación de Instalador

DEPLOYMENT & INSTALERS

The screenshot shows the 'Deployment Packages' section of the FortiClient EMS interface. A new package named 'Instalador CON VPN' is being created. It includes two versions: 7.2.1 and 7.2.1. An 'Auto Update' checkbox is checked, and a 'Download Link' is provided.

Step 1: Version

Installer Type: Choose an official release (selected).
Release: 7.2.
Patch: 7.2.1
Keep updated to the latest patch (checkbox checked).

Step 2: General

Name: Instalador CON VPN
Notes: Tiene habilitado la VPN

Step 3: Features

Basic Security Features: Secure Access Architecture Components (SSL and IPsec VPN), Vulnerability Scan (Host vulnerability scanning), Advanced Persistent Threat (APT) Components (FortiSandbox detection and quarantine features).

Additional Security Features: Malware (AntiVirus, Anti-Exploit, Removable Media Access, Anti-Ransomware, Cloud Based Malware Outbreak Detection, Web Filtering, Application Firewall), Single Sign-On Mobility Agent, Zero Trust Network Access, Privilege Access Management.

Step 4: Advanced

Advanced: Enable desktop shortcut, Enable start menu shortcut.
Installer ID: Enable Installer ID (checkbox checked).
Endpoint Profile: Enable Endpoint VPN Profile (checkbox checked).
Remote Access Profile (PRODUCTIVA) - autoconnect.
Enable Endpoint System Profile.
System Settings Profile (PRODUCTIVA).
Invalid Certificate Action: Inherit Profile Value (Allow).

A la hora de crear y configurar un instalador, **es mandatorio configurar el paso 4**.

- **Installer ID**, se debe habilitar y seleccionar el Group Assignment Rules (Reglas de asignación de grupos) que se creó en el paso 1.



FortiClient EMS

EDICIÓN 1
Tipo de Documento:
IMPLEMENTACIÓN
Versión: 2.0 / 2023
Página 10 de 17

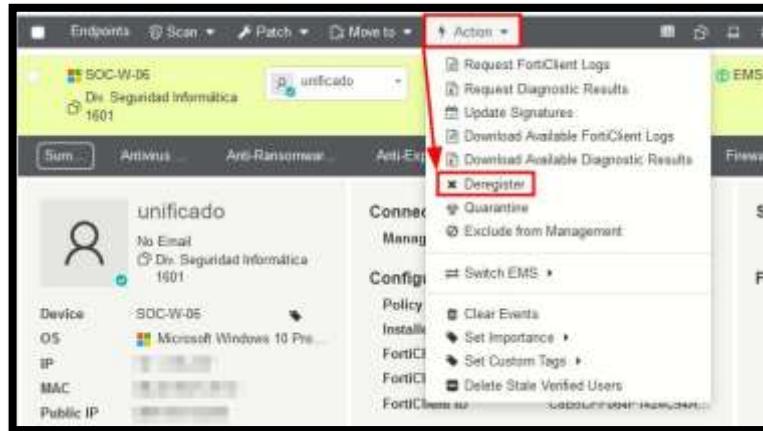
- **Endpoint Profile**, habilitar "Enable Endpoint System Profile" y seleccionar el requerido a utilizar.
Habilitar "Enable Endpoint VPN Profile" y elegir el perfil.

Desinstalación

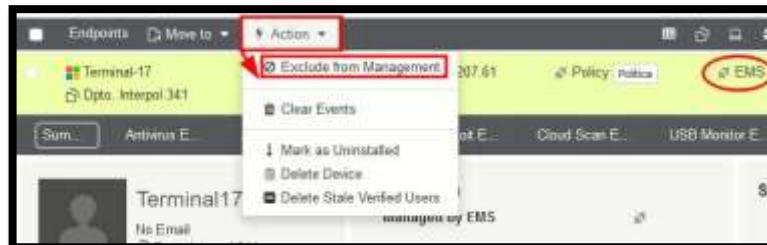
Opción 1:

Antes de desinstalar una licencia EMS, se debe cumplir los siguientes pasos.

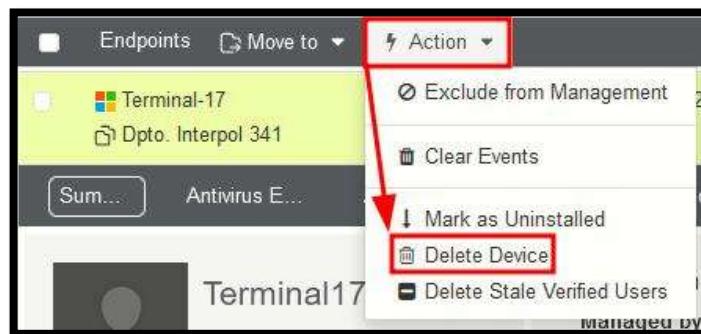
- Aplicar acción “Deregister”.



- Aplicar acción “Exclude from Management”.



- Aplicar acción “Delete Device”.





FortiClient EMS

EDICIÓN 1
Tipo de Documento:
IMPLEMENTACIÓN
Versión: 2.0 / 2023
Página 11 de 17

Opción 2:

Utilizar la herramienta **FCRemove.exe** que se encuentra en el Drive cuando no sea posible aplicar la “**Opción 1**” o se obtenga un error a la hora de “**reparar / desinstalar**” el EMS en un dispositivo.

- Iniciar los **Servicios** como *Administrador*.
 - Primero detener el servicio “*FortiClient Endpoint Protection*” y deshabilitar el inicio automático.
 - Segundo detener el servicio “*FortiClient Orquestador*” y deshabilitar el inicio automático.
 - Tercero el servicio “*FortiClient Services Scheduler*” deshabilitar el inicio automático.
 - Finalizar reiniciando el equipo.

The screenshot shows the Windows Services snap-in window. The title bar reads "Servicios". The main pane displays a list of services, with the "FortiClient Service Scheduler" service highlighted. This service is listed under the "FortiClient Service Scheduler" category. Its status is "En ejecución" (Running) and its startup type is "Deshabilitado" (Disabled). A red box highlights the "Deshabilitado" status for both the "FortiClient Service Scheduler" and the "FortiClient Endpoint Protection" services.

Nombre	Descripción	Estado	Tipo de inicio	Iniciar sesión c...
Coordinador de transacción...	Coordina las...	En ejec...	Manual	Servicio de rec...
CoreMessaging	Manages co...	En ejec...	Automático	Servicio local
CredentialEnrollmentMana...	Administrad...		Manual	Sistema local
Datos de los contactos_4259c	Indiza los da...		Manual	Sistema local
Declared Configuration(DC)...	Process Decl...		Manual (dese...	Sistema local
Detección de hardware shell	Proporciona...	En ejec...	Automático	Sistema local
Detección SSDP	Detecta disp...	En ejec...	Manual	Servicio local
DeviceAssociationBroker_42...	Enables app...		Manual	Sistema local
DevicePicker_4259c	Este servicio...		Manual	Sistema local
DevicesFlow_4259c	Permite que...		Manual	Sistema local
Diagnostic Execution Service	Executes dia...		Manual (dese...	Sistema local
DialogBlockingService	Servicio de ...		Deshabilitado	Sistema local
Directiva de extracción de t...	Permite con...		Manual	Sistema local
Disco virtual	Proporciona...		Manual	Sistema local
Dispositivo host de UPnP	Permite que...		Manual	Servicio local
DLL de host del Contador d...	Habilita a lo...		Manual	Servicio local
Energía	Administra l...	En ejec...	Automático	Sistema local
Enrutamiento y acceso rem...	Ofrece servi...		Deshabilitado	Sistema local
Estación de trabajo	Crea y mant...	En ejec...	Automático	Servicio de rec...
Examinador de equipos	Mantiene u...		Manual (dese...	Sistema local
Experiencia de calidad de a...	Experiencia ...		Manual	Servicio local
Experiencia del usuario y tel...	El servicio d...		Deshabilitado	Sistema local
Extensiones y notificacióne...	Este servicio...		Manual	Sistema local
Fax	Te permite e...		Deshabilitado	Servicio de rec...
File History Service	Protects use...		Manual (dese...	Sistema local
Filtro de teclado de Microsoft	Controla el f...		Deshabilitado	Sistema local
Firewall de Windows Defen...	Firewall de ...	En ejec...	Automático	Servicio local
FortiClient Endpoint Protect...			Deshabilitado	Sistema local
FortiClient Service Scheduler	FortiClient S...	En ejec...	Deshabilitado	Sistema local
GamelInput Service	Enables key...		Manual (dese...	Sistema local
GraphicsPerfSvc	Graphics per...		Manual (dese...	Sistema local
Hora de la red de telefonía ...	Este servicio...		Manual (dese...	Servicio local
Hora de Windows	Mantiene la ...		Manual (dese...	Servicio local



FortiClient EMS

EDICIÓN 1

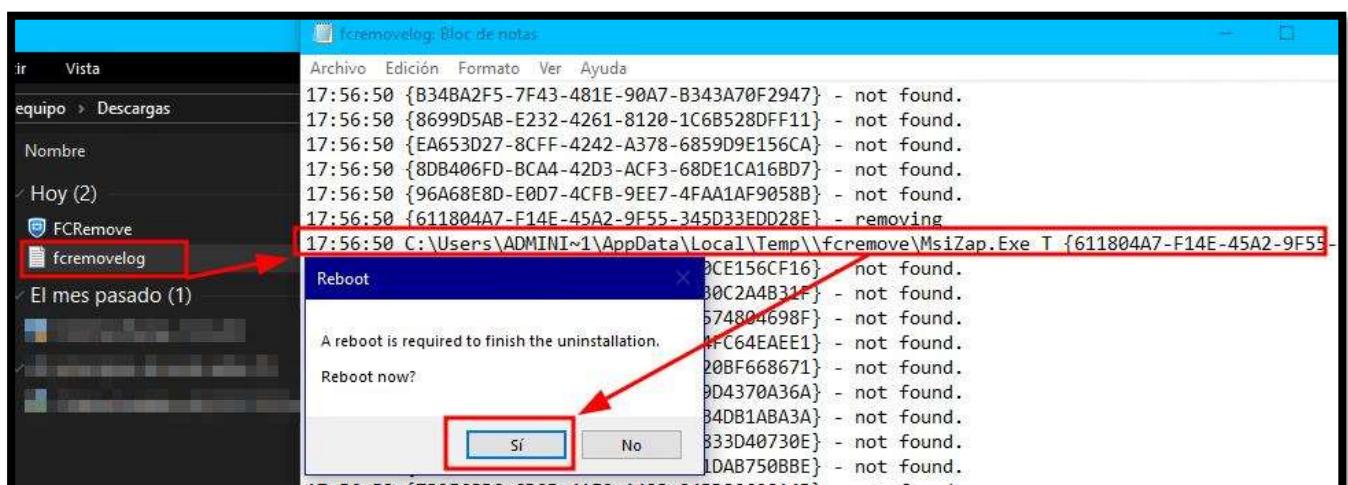
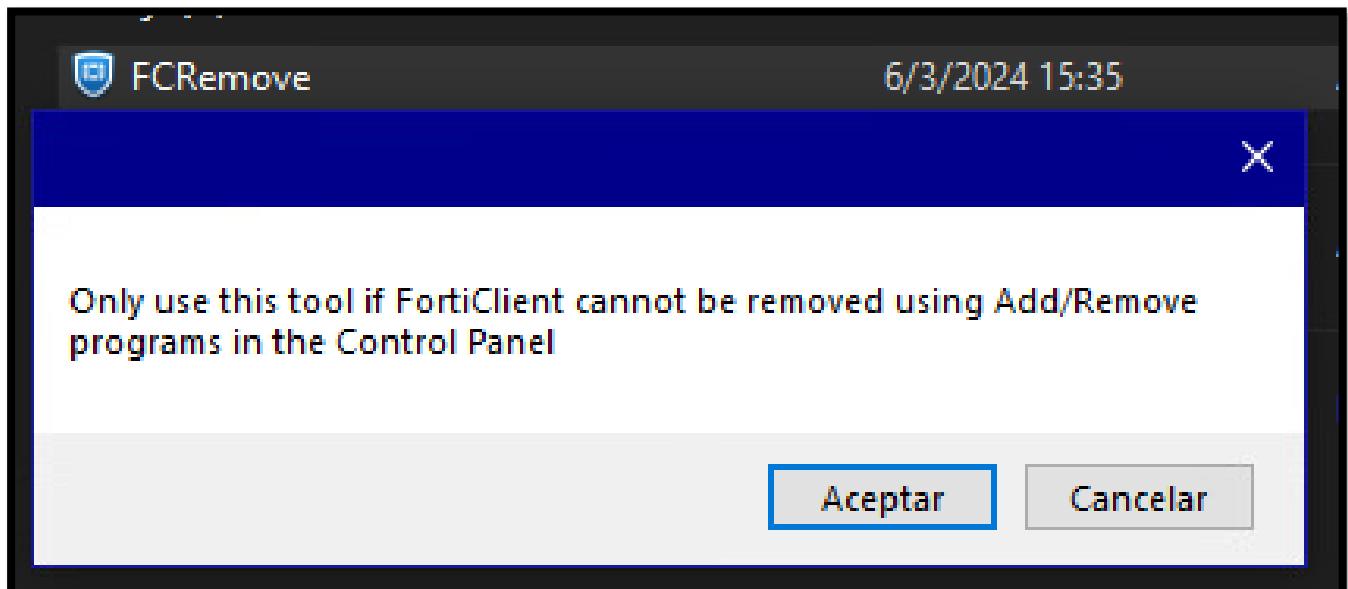
Tipo de Documento:

IMPLEMENTACIÓN

Versión: 2.0 / 2023

Página 12 de 17

- Reiniciado el dispositivo, ejecutar el programa **FCRemove.exe**.
 - En la ruta donde se ejecuta genera un archivo .txt el cual nos indica a modo informativo que se quite la llave del registro de Windows.
 - Aguardar unos instantes hasta que surja un cartel el cual solicite reinicio.





FortiClient EMS

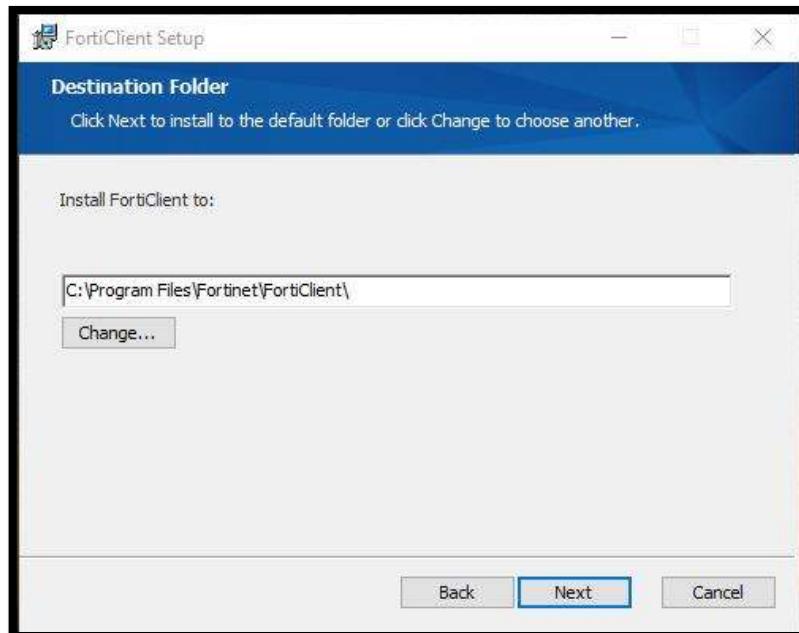
EDICIÓN 1
Tipo de Documento:
IMPLEMENTACIÓN
Versión: 2.0 / 2023
Página 13 de 17

Caso 1: Instalación EMS en equipo con INTERNET que se solicite VPN para INTRA

Paso 1



Paso 2





FortiClient EMS

EDICIÓN 1

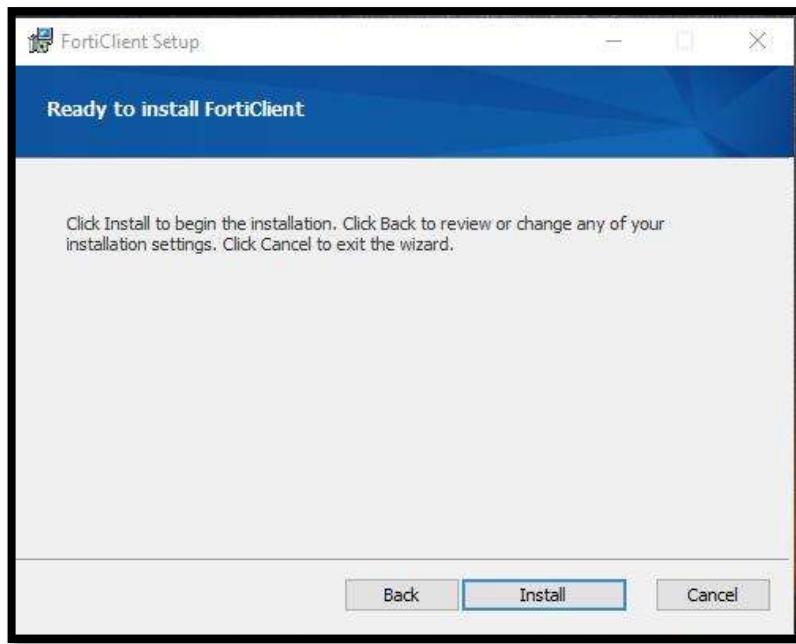
Tipo de Documento:

IMPLEMENTACIÓN

Versión: 2.0 / 2023

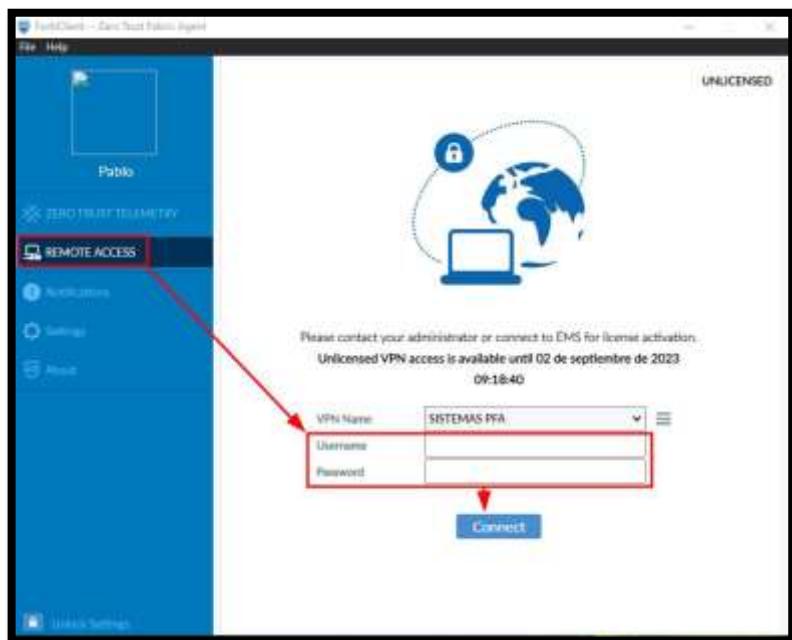
Página 14 de 17

Paso 3



Paso 4

Una vez instalado, solo se debe ingresar “**USUARIO**” y “**CONTRASEÑA**” (de no contar con dicha información, llamar a la Div. SEGURIDAD EN REDES DE DATOS).





FortiClient EMS

EDICIÓN 1

Tipo de Documento:

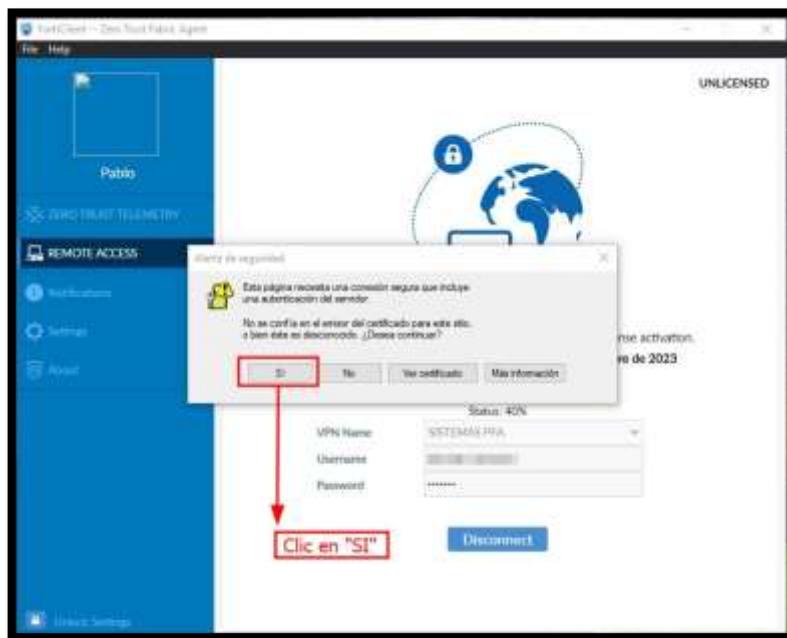
IMPLEMENTACIÓN

Versión: 2.0 / 2023

Página 15 de 17

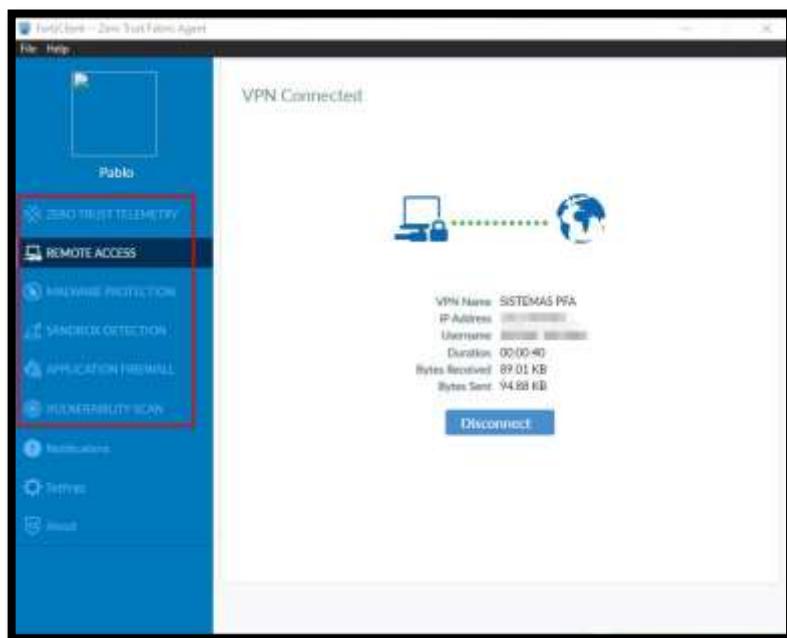
Paso 5

Aceptar la autenticación.



Paso 6

Una vez que se estableció la conexión, en el panel izquierdo de la herramienta se visualizará el componente AV en funcionamiento.





FortiClient EMS

EDICIÓN 1
Tipo de Documento:
IMPLEMENTACIÓN
Versión: 2.0 / 2023
Página 16 de 17

Caso 2: Instalación EMS en equipo con internet y que ya tiene instalado FortiClient VPN.

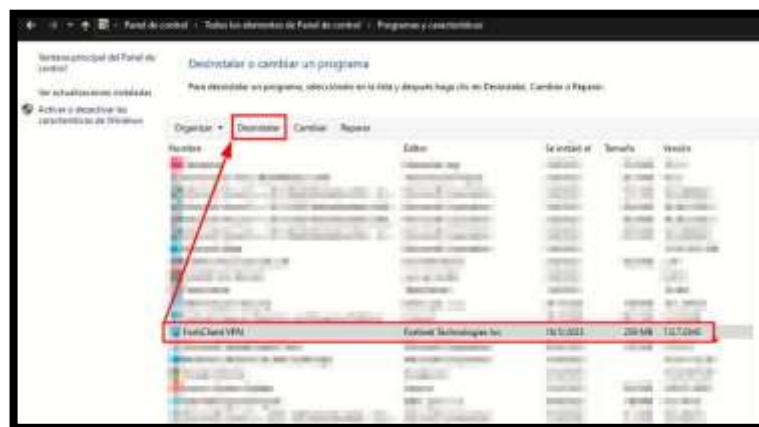
Paso 1

Identificar y tomar nota del “*nombre de usuario*” asignado a la VPN.



Paso 2

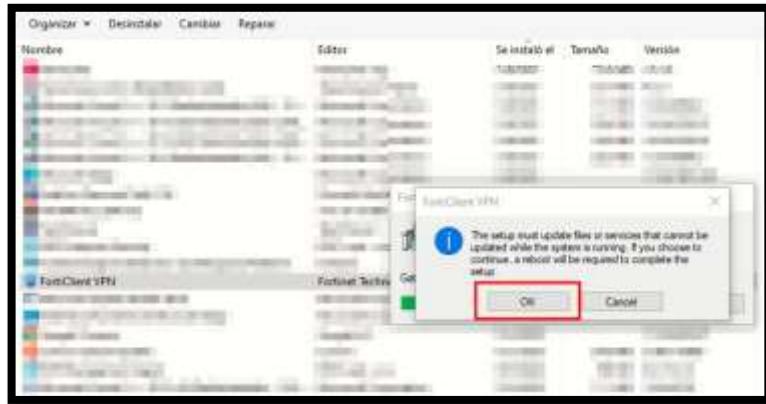
Es mandatorio que una vez cumplido el “*Paso 1 del Caso 2*”, se proceda a “desinstalar” FortiClient VPN y luego “reiniciar” el equipo.





FortiClient EMS

EDICIÓN 1
Tipo de Documento:
IMPLEMENTACIÓN
Versión: 2.0 / 2023
Página 17 de 17



Paso 3

Habiendo eliminado la VPN, proceder a instalar FortiClient EMS (*explicado en Caso 1*) y finalizada la instalación nuevamente “*ingresar el usuario y contraseña*”, acto seguido la plataforma se conectará automáticamente.

Caso 3: Instalación EMS en equipo con conectividad INTRA

Paso 1

Repetir lo mencionado en el Caso 1 pero “*no se debe configurar usuario y contraseña*” ya que, al encontrarse en la misma red, el sistema se activará por sí solo.

Revisiones y Modificaciones:

- 12/06/23
- 01/08/23
- 03/08/23
- 04/10/23
- 06/03/24