UNIÓN TEMPORAL **UT HC-WX SEGURIDAD 2025**

Heimcore | WEXLER

LABORATORIO DE PRUEBAS FORTICLIENTE EMS

Evidencias de Laboratorio

Versión: 0.1

Fecha: **18/03/2025**



Tabla de contenido

1. INTRODUCCIÓN 3
2. OBJETIVO 3
3. ACTIVIDADES 3
3.1 Despliegue en una arquitectura de pruebas 4
3.2 Despliegue en Cloud de pruebas 5
3.3 Políticas ZTNA habilitadas 6
3.4 FortiClient EMS para administración centralizada. 7
3.5 Integración con directorio (AD) para validación de identidad 10
3.6 Validación de registro Endpoint, aprovisionamiento y asignación automática de licencias. 11
4. CONCLUSIONES. 13

1. INTRODUCCIÓN

El presente informe tiene como propósito documentar los resultados obtenidos durante la ejecución de un laboratorio de pruebas orientado a evaluar el modelo de consumo de licenciamiento de la solución **FortiClient EMS**, específicamente en lo relacionado con la posibilidad de gestionar licencias bajo un esquema basado en usuarios y no en dispositivos. Esta validación surge como parte de la necesidad de optimizar el uso del licenciamiento disponible, considerando escenarios donde un mismo usuario puede acceder desde múltiples dispositivos, lo cual impacta directamente en la eficiencia del consumo de licencias y en la gestión operativa de la plataforma.

Durante el desarrollo del laboratorio, se realizaron pruebas controladas que permitieron analizar el comportamiento de la solución frente a distintos escenarios de autenticación, asociación de endpoints y asignación de licencias, con el fin de identificar si el modelo permite una gestión flexible orientada a usuario o si se mantiene estrictamente ligado al endpoint registrado.

Los resultados obtenidos permitirán establecer lineamientos técnicos y recomendaciones para la correcta implementación y administración del licenciamiento de **FortiClient EMS**, asegurando su alineación con los requerimientos operativos y contractuales del proyecto.

2. OBJETIVO

Evaluar el comportamiento del modelo de licenciamiento de la solución FortiClient EMS mediante la ejecución de pruebas controladas, con el fin de determinar si es viable la asignación y consumo de licencias bajo un esquema basado en usuarios en lugar de dispositivos, identificando sus implicaciones técnicas, operativas y de gestión dentro del entorno implementado.

3. ACTIVIDADES

En el entorno de pruebas se realizaron las siguientes actividades:

- Despliegue en una arquitectura de pruebas
- Despliegue en CLOUD
- Políticas ZTNA habilitadas.
- FortiClient EMS para administración centralizada.
- Integración con directorio (AD) para validación de identidad.

- Validación de registro, aprovisionamiento y asignación automática de licencias.

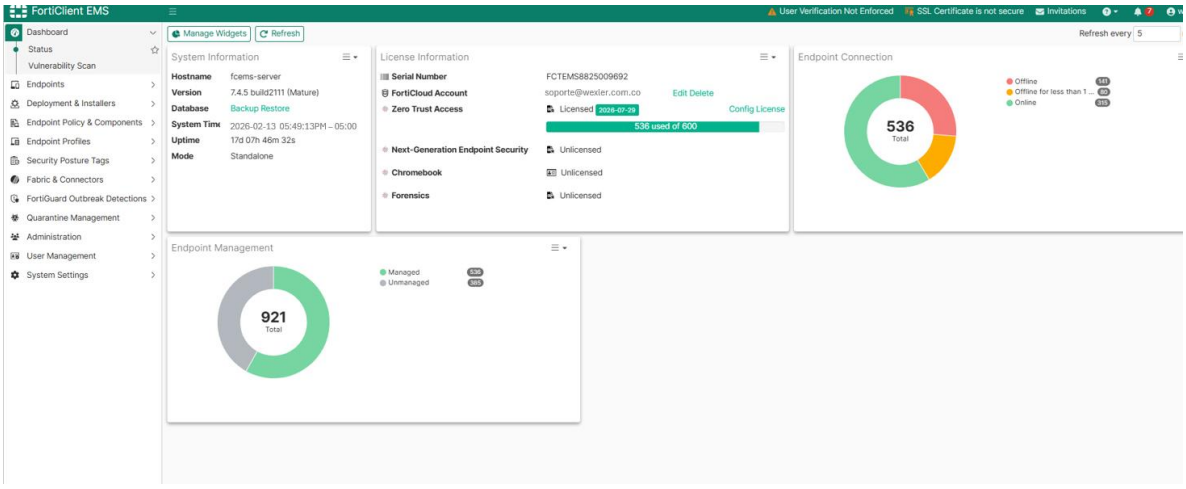
Las pruebas incluyeron:

- Proceso de enrolamiento del agente bajo esquema identity-based.
- Validación de postura del endpoint (compliance check).
- Asignación dinámica de licencias por usuario con múltiples dispositivos.
- Pruebas de desconexión, cambio de dispositivo y reasignación.
- Verificación de consumo simultáneo bajo políticas ZTNA activas.
- Validación de telemetría y trazabilidad en FortiAnalyzer.

Durante estas pruebas se identificó que, aunque históricamente Fortinet manejó un esquema de licenciamiento user-based que permitía hasta dos (2) o tres (3) agentes por usuario, la versión actualmente disponible para adquisición y activación en plataforma ya no permite la asignación efectiva bajo esa modalidad.

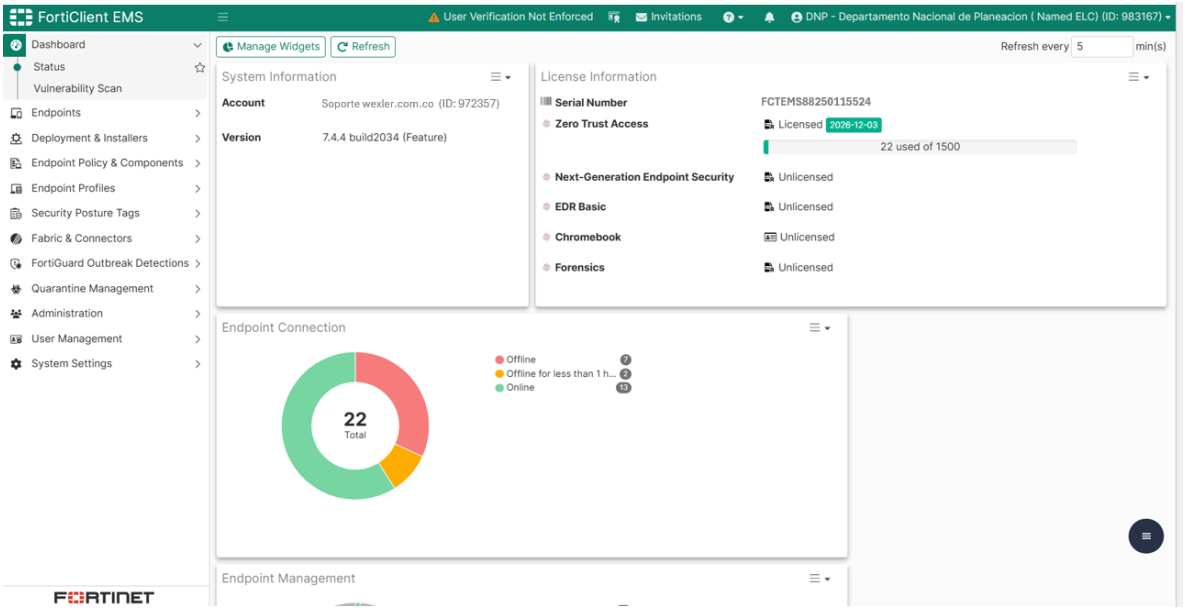
3.1 Despliegue en una arquitectura de pruebas

La plataforma FortiClient EMS, en su versión 7.4.5, fue implementada en el ambiente de pruebas en una máquina virtual con base en Linux Ubuntu Server 22.04, garantizando un entorno tecnológico robusto, validado que el rendimiento de la solución es óptimo:



3.2 Despliegue en Cloud de pruebas

también se ejecutó en el ambiente de pruebas por Cloud que otorga el Fabricante garantizando funcionamiento en una versión de 7.4.4



Durante el proceso de pruebas se evidenció que, al realizar el despliegue del agente de FortiClient por cada máquina —tanto en entornos On-Premise como Cloud—, el endpoint es registrado automáticamente en la consola de administración de FortiClient EMS una vez establece comunicación con el servicio de telemetría asociado a la licencia adquirida.

Este comportamiento confirma que el enrolamiento del agente se realiza de manera automática y centralizada, permitiendo que cada dispositivo, al momento de conectarse, sea identificado, inventariado y gestionado dentro de la plataforma sin necesidad de intervención manual adicional.

Durante este proceso, bajo un esquema identity-based, se pudo evidenciar que:

Cada endpoint que instala y activa el agente consume una licencia de manera individual, independientemente del usuario que lo opere.

La asociación principal del licenciamiento se mantiene ligada al dispositivo (endpoint) y no al usuario, incluso cuando se utilizan credenciales de autenticación.

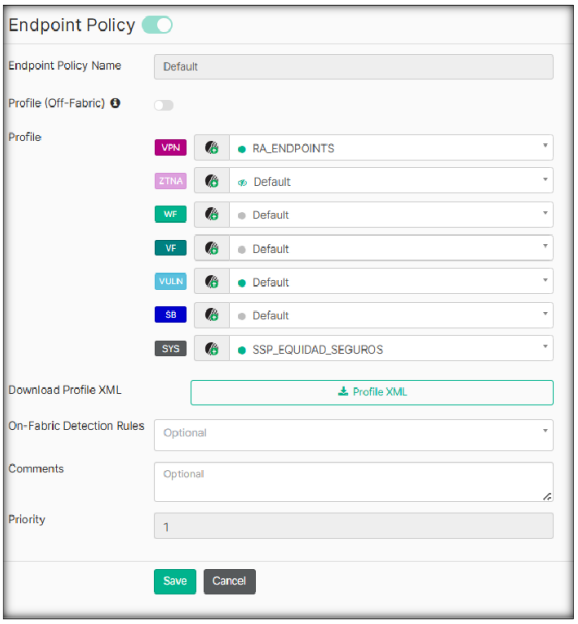
La telemetría permite validar en tiempo real el estado del endpoint (conectado, desconectado, gestionado), como se observa en los paneles de Endpoint Connection y Endpoint Management.

El sistema refleja de manera consolidada el consumo de licencias, evidenciando el número de endpoints registrados frente al total licenciado (por ejemplo, 536 de 600 licencias en uso), lo que permite un control preciso de la capacidad disponible.

3.3 Políticas ZTNA habilitadas

De acuerdo con la evidencia presentada, se observa que en la consola de FortiClient EMS, específicamente en la sección de Endpoint Policy, la herramienta maneja por defecto un esquema de asignación de políticas basado en endpoint (dispositivo) y no en usuario.

La política visualizada (denominada Default) muestra que los perfiles de seguridad —tales como VPN, ZTNA, Web Filtering (WF), Vulnerability Scan (VULN), Sandbox (SB) y System Settings (SYS)— se asocian directamente al dispositivo que se enrola en la plataforma. Esto implica que, una vez el agente es instalado y registrado, el endpoint hereda automáticamente esta política preconfigurada sin requerir una asignación manual inicial.



Durante las pruebas se pudo evidenciar que:

- La herramienta aplica políticas preestablecidas de manera automática al endpoint, basándose en su registro dentro de EMS.

- No existe, de forma nativa en esta configuración, una asociación directa de políticas por usuario, incluso cuando el esquema de autenticación pueda involucrar identidad.

- El modelo operativo está diseñado para que cada dispositivo tenga su propio conjunto de configuraciones, lo cual refuerza el enfoque device-based tanto en administración como en licenciamiento.

- Los perfiles (como VPN o ZTNA) se activan y configuran en función del endpoint, lo que permite un control granular por equipo, pero limita la flexibilidad en escenarios donde un usuario utiliza múltiples dispositivos.

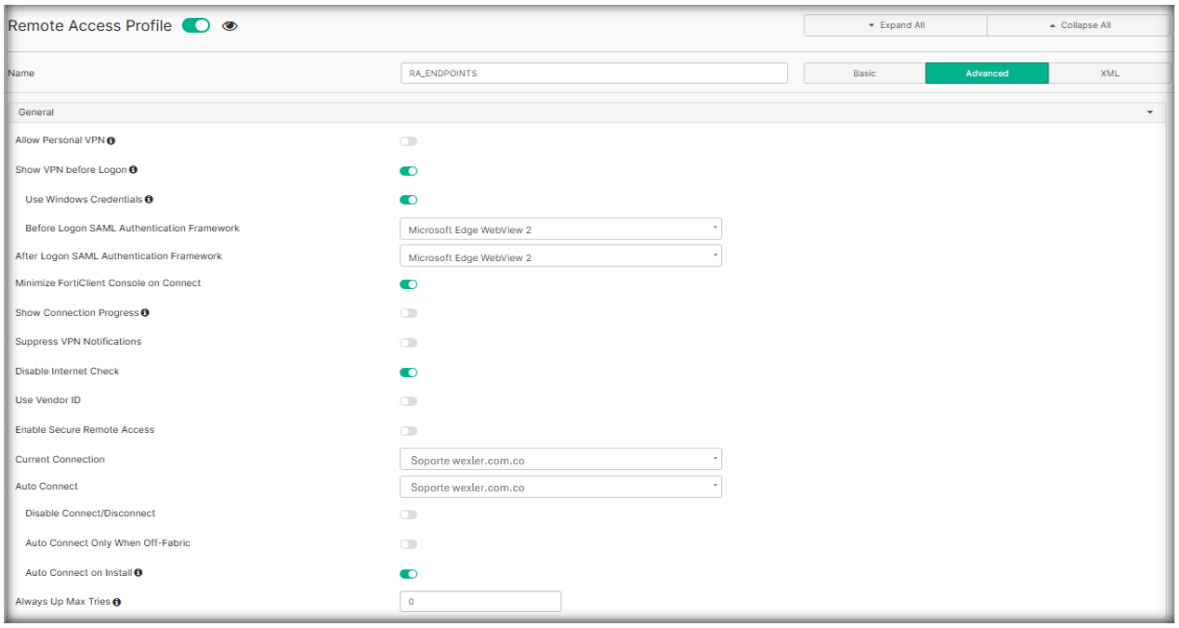
Adicionalmente, se identifica que la opción de Profile (Off-Fabric) se encuentra deshabilitada, lo cual indica que las políticas están orientadas a dispositivos que hacen parte del entorno gestionado (fabric), reforzando aún más el control por endpoint.

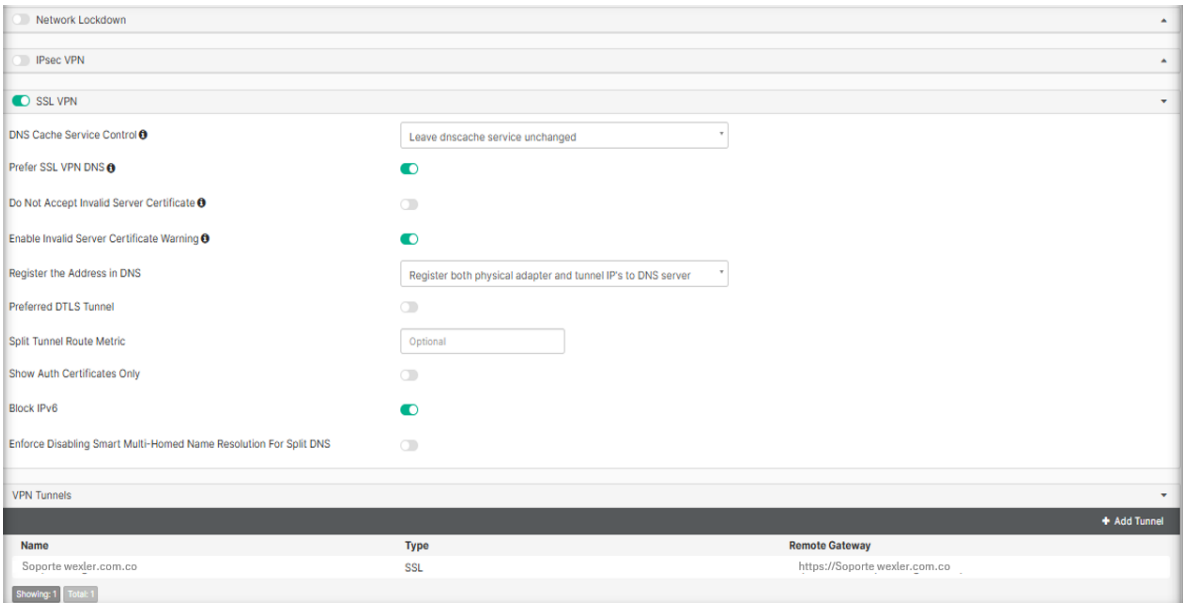
En conclusión, la configuración por defecto de FortiClient EMS establece un modelo en el cual los agentes se gestionan y se les aplican políticas basadas en el dispositivo registrado, confirmando que la herramienta no está orientada de manera nativa a un esquema de administración o licenciamiento centrado en usuario, sino en endpoint.

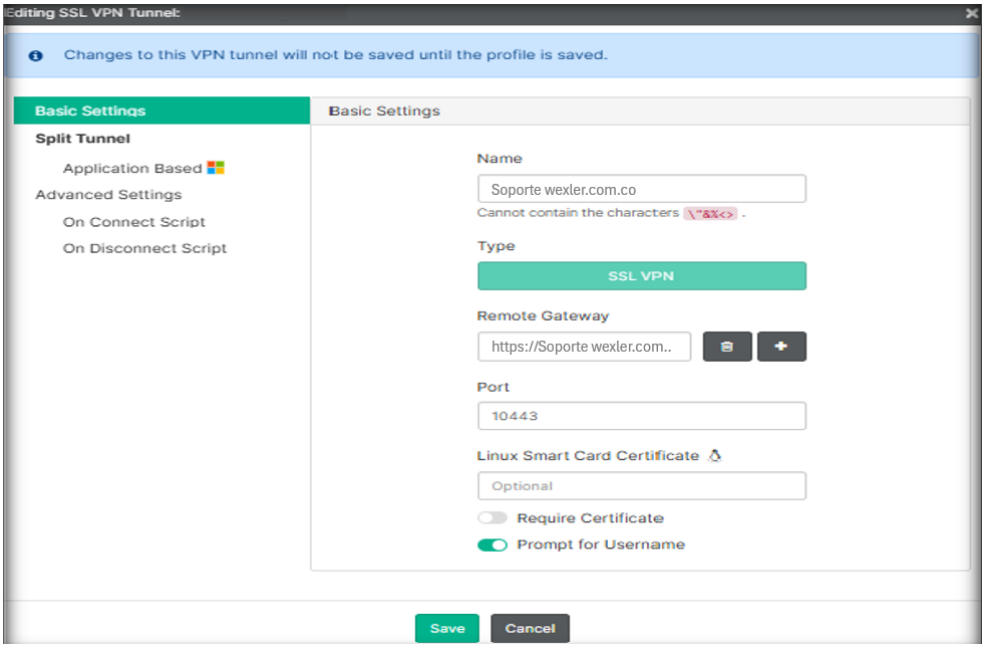
3.4 FortiClient EMS para administración centralizada.

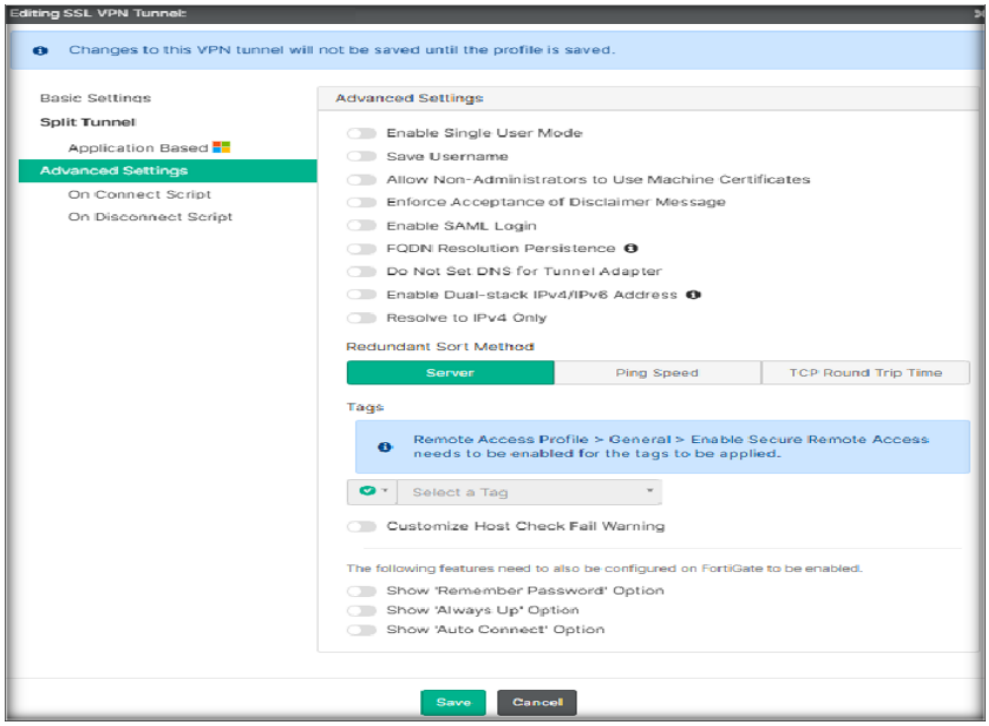
Se configuraron los Endpoints Profiles para tener acceso remoto a la VPN previamente compartida por la entidad de manera que cumpla con los siguientes criterios:

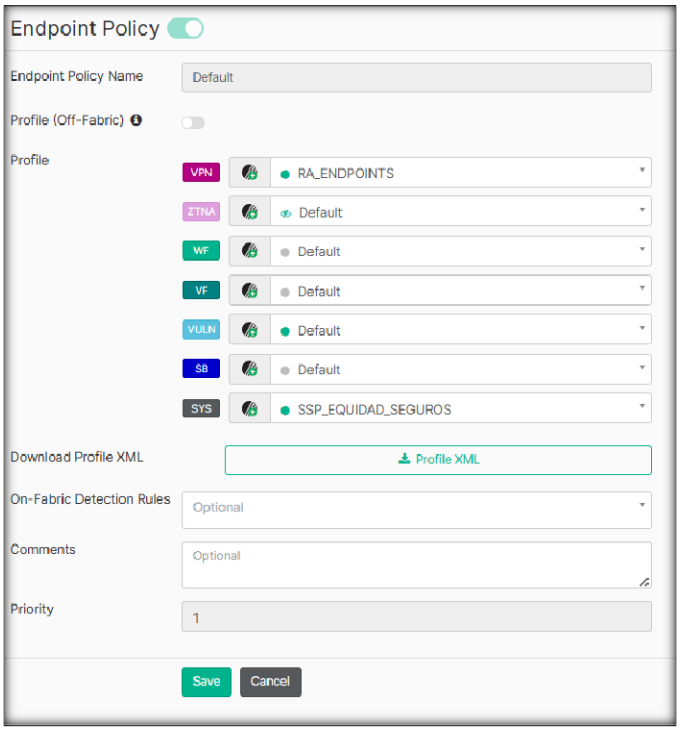
1. Se conecte con los datos de usuario de Dominio ingresados mediante Windows Logon
2. Se conecte automáticamente tras iniciar Windows
3. Minimice el agente FortiClient tras conectarse a la misma VPN
4. No muestre notificaciones
5. Prefiera los DNS de la VPN sin modificar los que ya trae el equipo desde el dominio
6. Permitir el uso únicamente del túnel de la entidad “SoporteWexler”
7. No permita desconectarse desde la EMS, sin previa autorización del departamento de TI


Remote Access Profile
Expand All
Collapse All
Name
RA_ENDPOINTS
Basic
Advanced
XML
General
Allow Personal VPN
Show VPN before Logon
Use Windows Credentials
Before Logon SAML Authentication Framework
Microsoft Edge WebView 2
After Logon SAML Authentication Framework
Microsoft Edge WebView 2
Minimize FortiClient Console on Connect
Show Connection Progress
Suppress VPN Notifications
Disable Internet Check
Use Vendor ID
Enable Secure Remote Access
Current Connection
Soporte wexler.com.co
Auto Connect
Soporte wexler.com.co
Disable Connect/Disconnect
Auto Connect Only When Off-Fabric
Auto Connect on Install
Always Up Max Tries
0


Network Lockdown
IPsec VPN
SSL VPN
DNS Cache Service Control
Leave dnscache service unchanged
Prefer SSL VPN DNS
Do Not Accept Invalid Server Certificate
Enable Invalid Server Certificate Warning
Register the Address in DNS
Register both physical adapter and tunnel IP's to DNS server
Preferred DTLS Tunnel
Split Tunnel Route Metric
Optional
Show Auth Certificates Only
Block IPv6
Enforce Disabling Smart Multi-Homed Name Resolution For Split DNS
VPN Tunnels
+ Add Tunnel
Name
Type
Remote Gateway
Soporte wexler.com.co
SSL
https://Soporte wexler.com.co
Showing: 1
Total: 1


Editing SSL VPN Tunnel:
Changes to this VPN tunnel will not be saved until the profile is saved.
Basic Settings
Split Tunnel
Application Based
Advanced Settings
On Connect Script
On Disconnect Script
Basic Settings
Name
Soporte wexler.com.co
Cannot contain the characters \"&%<> .
Type
SSL VPN
Remote Gateway
https://Soporte wexler.com..
Port
10443
Linux Smart Card Certificate
Optional
Require Certificate
Prompt for Username
Save
Cancel


Editing SSL VPN Tunnel:
Changes to this VPN tunnel will not be saved until the profile is saved.
Basic Settings
Split Tunnel
Application Based
Advanced Settings
On Connect Script
On Disconnect Script
Advanced Settings
Enable Single User Mode
Save Username
Allow Non-Administrators to Use Machine Certificates
Enforce Acceptance of Disclaimer Message
Enable SAML Login
FQDN Resolution Persistence
Do Not Set DNS for Tunnel Adapter
Enable Dual-stack IPv4/IPv6 Address
Resolve to IPv4 Only
Redundant Sort Method
Server
Ping Speed
TCP Round Trip Time
Tags
Remote Access Profile > General > Enable Secure Remote Access needs to be enabled for the tags to be applied.
Select a Tag
Customize Host Check Fail Warning
The following features need to also be configured on FortiGate to be enabled.
Show 'Remember Password' Option
Show 'Always Up' Option
Show 'Auto Connect' Option
Save
Cancel



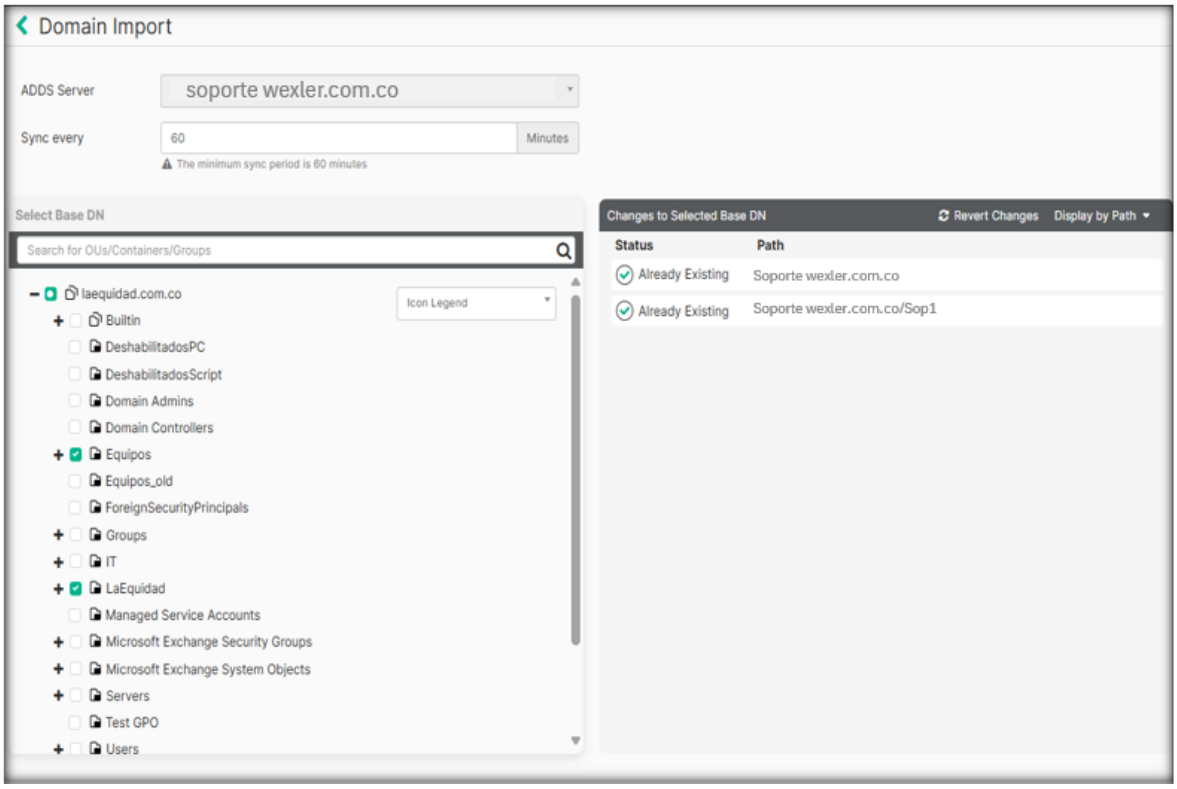
3.5 Integración con directorio (AD) para validación de identidad

Se evidenció que la solución permite la integración con servicios de directorio activo (Active Directory - AD) como mecanismo para la validación de identidad de los usuarios dentro del entorno.

Esta integración posibilita que los usuarios se autentiquen utilizando sus credenciales corporativas, centralizando la gestión de identidades y alineándose con los esquemas de seguridad organizacionales. De esta manera, se garantiza que únicamente usuarios válidos y registrados en el dominio puedan acceder a los recursos protegidos.

Adicionalmente, esta integración permite:

- Aplicar controles de acceso basados en usuarios y grupos de AD, facilitando la segmentación por roles o perfiles.
- Mejorar la trazabilidad de los accesos, asociando cada evento a un usuario del directorio.



No obstante, es importante precisar que, aunque la validación se realiza a nivel de identidad (usuario), la gestión de los agentes, la aplicación de políticas y el consumo de licencias continúan asociados al **endpoint**, manteniendo el modelo operativo basado en dispositivo.

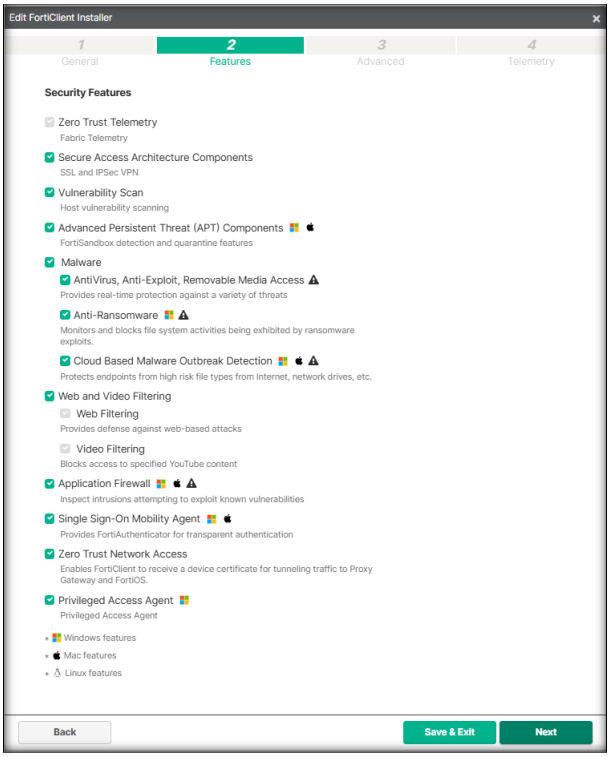
3.6 Validación de registro Endpoint, aprovisionamiento y asignación automática de licencias.

Se configuró el agente habilitando la totalidad de las funcionalidades disponibles dentro de la plataforma, con el objetivo de evaluar su comportamiento en un ambiente de pruebas controlado. Esto permitió validar de manera integral las capacidades del agente y analizar su funcionamiento bajo diferentes escenarios.

No obstante, es importante precisar que, aunque todas las funcionalidades se encuentran habilitadas a nivel de configuración, el uso efectivo de cada una está limitado al licenciamiento vigente de la compañía. En consecuencia, durante las pruebas, el agente solo hace uso de los módulos y

características que se encuentran cubiertos por las licencias activas, mientras que las demás permanecen inactivas o sin operación.

Este enfoque permite identificar el alcance real de la solución bajo el esquema de licenciamiento, así como evaluar posibles requerimientos futuros en caso de que se desee habilitar funcionalidades adicionales.



Los agentes de FortiClient para ser administrador por el FortiClient EMS requieren un código de invitación, este código se podrá ver en el menú de invitations a través de Endpoints.

4. CONCLUSIONES.

De acuerdo con los resultados obtenidos durante la ejecución del laboratorio de pruebas, se concluye que la solución FortiClient EMS opera bajo un modelo de licenciamiento orientado a dispositivos (endpoint-based) y no a usuarios. A pesar de contar con capacidades de integración con servicios de identidad, como Active Directory, y de soportar esquemas de autenticación basados en usuario, el consumo de licencias se genera de manera individual por cada endpoint que instala y registra el agente en la plataforma.

Las pruebas realizadas evidenciaron que un mismo usuario, al utilizar múltiples dispositivos, genera consumo independiente de licencias por cada uno de ellos, lo cual limita la posibilidad de implementar un modelo de licenciamiento basado en usuario dentro del esquema actual de la herramienta.

Adicionalmente, se validó que tanto la aplicación de políticas como la gestión de endpoints se encuentran diseñadas bajo este enfoque, reforzando el modelo device-based como estándar operativo de la solución.

En este sentido, se concluye que no es viable, bajo las condiciones actuales de la plataforma y el licenciamiento disponible, migrar hacia un esquema de consumo de licencias por usuario. Por lo tanto, se recomienda considerar este este tipo de consumo de licenciamiento.