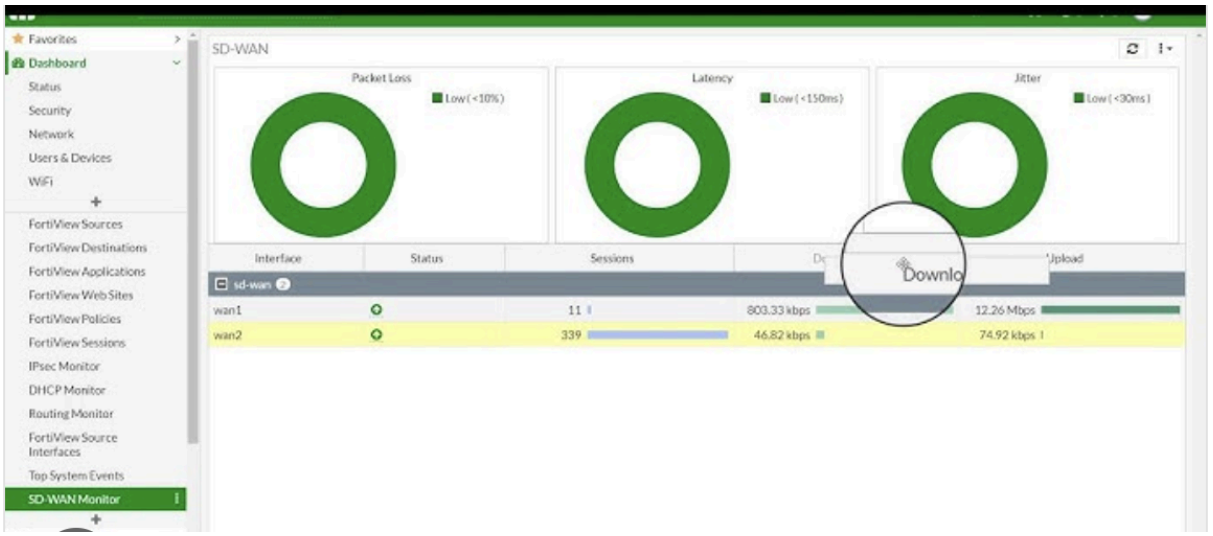
SESIONES REALIZADAS

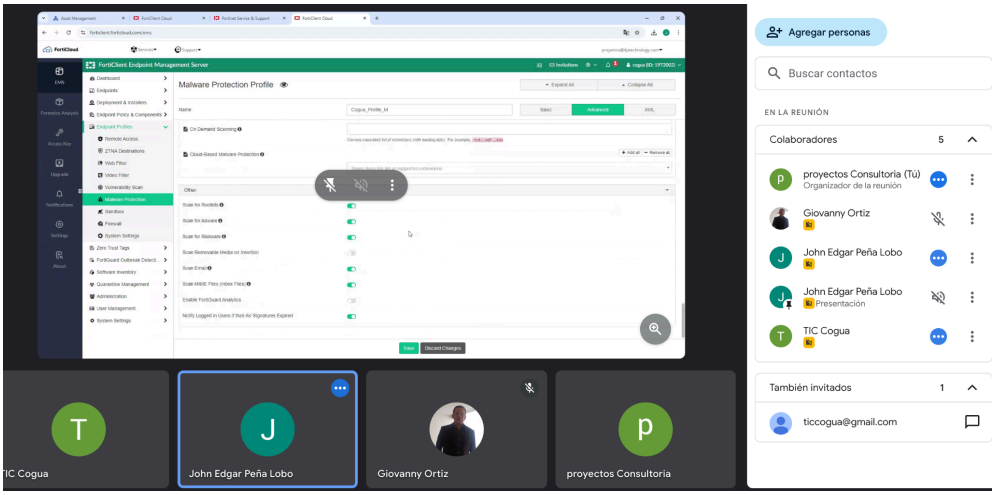
1. EL CONTRATISTA se obliga a la implementación e instalación del antivirus en los 100 equipos de cómputo de la Alcaldía de Cogua

Se instalaron 100 licencias, las cuales corresponden al total de máquinas autorizadas para instalar de la Alcaldía
Lo demás quedaron libres para uso de nuevos equipos de la Alcaldía.

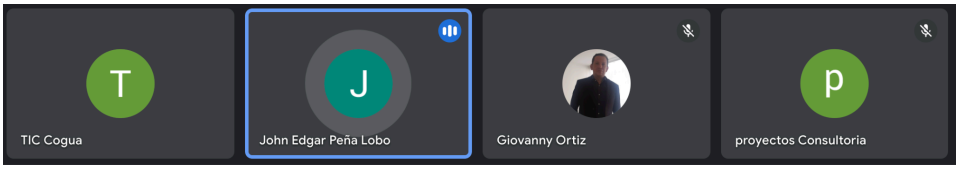


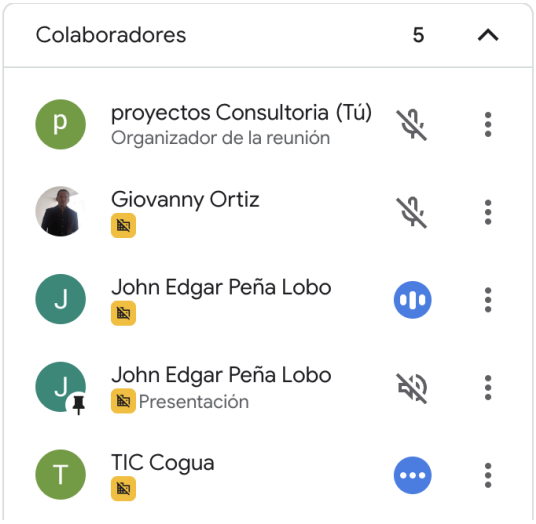
2. EL CONTRATISTA se obliga a dar soporte técnico 5X8 y entrenamiento y capacitación durante la ejecución del contrato.

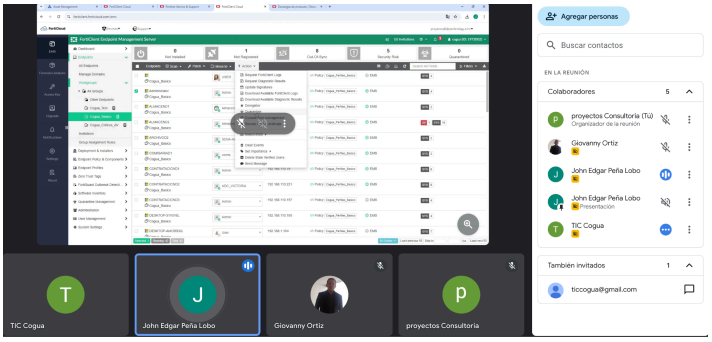
SESION DE TRANSFERENCIA DE CONOCIMIENTO CON EQUIPO TÉCNICO DE COGUA 20 DE SEPTIEMBRE











Sesión #5 y #6 Visita 24 y 25 de septiembre.

Soporte y transferencia de conocimiento presencial al técnico de Cogua Giovanny Ortiz.

Soporte 8x5
EVIDENCIAS DE SOPORTE REQUERIDOS Y SOLICITADOS.

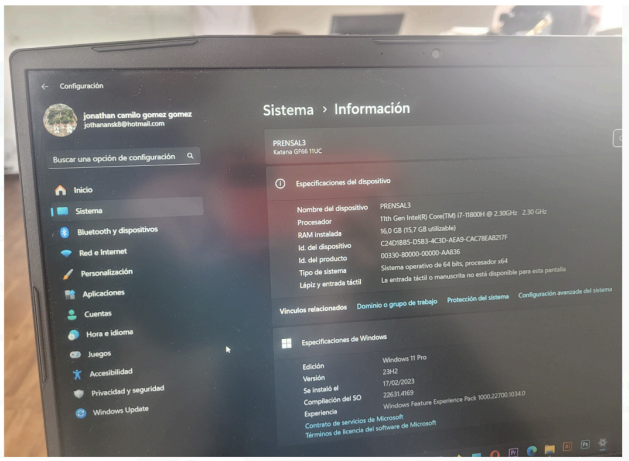
Primer Soporte , 1 hora. 4 de Octubre
Solicito Inge Giovanny Ortiz
Resolvio 4JSTECHNOLOGY

SOPORTE SOLICITADO PRA EXCLUSION DE APLICACION BLOQUEANTE

4 mensajes

proyectos Consultoria <proyectos@4jstechnology.com>
Para: tic.alcaldiacogua@gmail.com, TIC Cogua <tic@cogua-cundinamarca.gov.co>
CC: Soporte Nitromacsas <soporte_@nitromacsas.com>

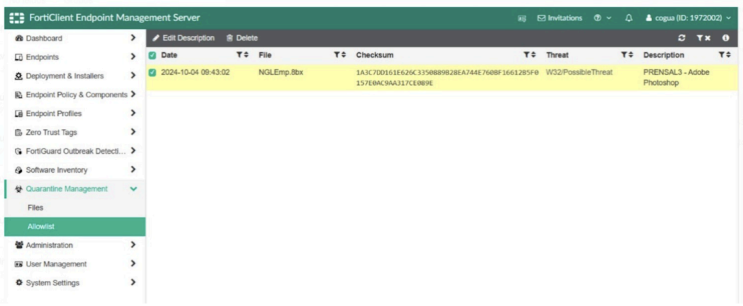
Se comunica el Ingeniero Giovanny Ortiz el 4 de Octubre reportando un bloqueo sobre la máquina de prensa



El antivirus bloqueo Photoshop y otro editor que utilizan

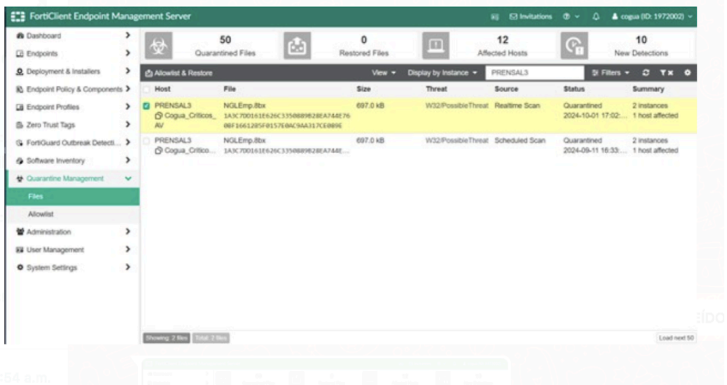
Se trabaja en la resolución de este soporte agregando la exclusión de esta aplicación en la consola para que el antivirus no la bloquee.





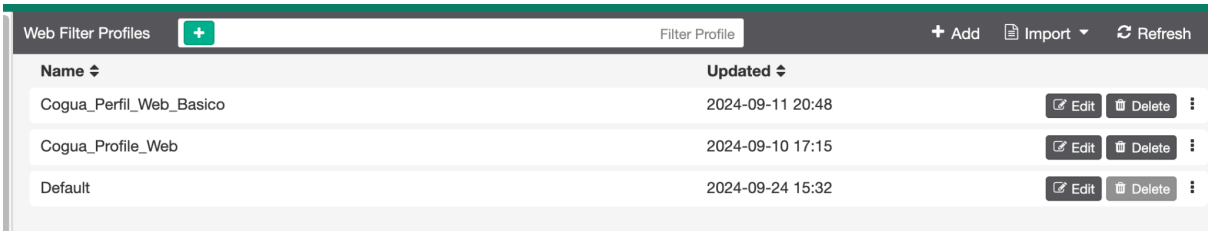
Entran aqui y seleccionan el archivo, luego le dan arriba en allow list y restore

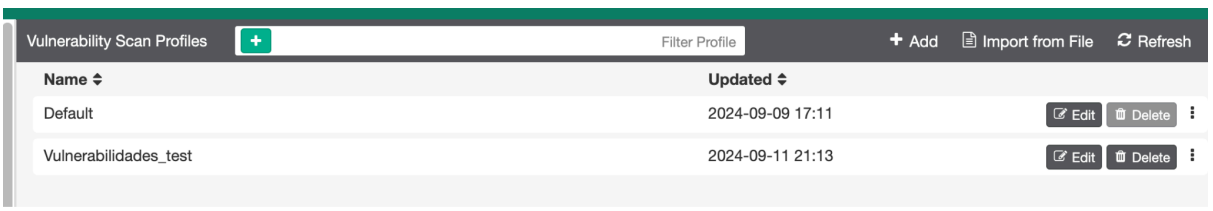
Luego pueden ir a las listas de los archivos permitidos y colocarle un nombre o una descripción



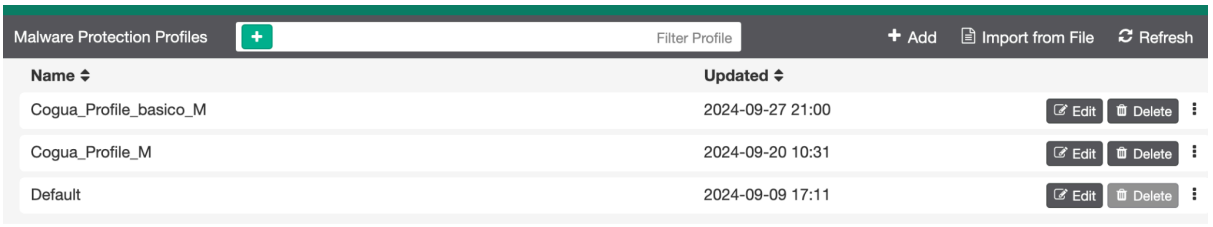
3. EL CONTRATISTA se obliga a parametrizar el equipo con las reglas de seguridad necesarias

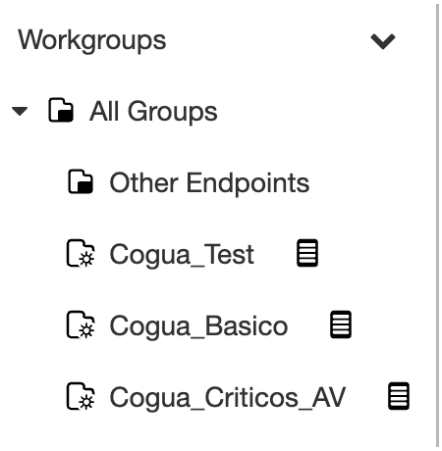
Se crearon los diferentes perfiles requeridos para cada fin a nivel de antivirus y navegación.



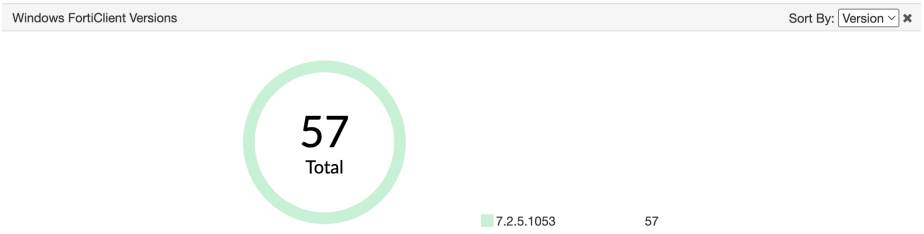








5. EL CONTRATISTA se obliga a incluir las actualizaciones directamente del fabricante Fortinet. La consola se deja en la última versión liberada por el fabricante.



6. EL CONTRATISTA se obliga con la entidad, a suministrar el software y licencia que llegara a requerir, certificados y garantizados de fábrica, cumpliendo las normas técnicas vigentes nacionales e internacionales.

El 9 de septiembre se realizaron todas las configuraciones de software y licencias requeridas para dar de alta la consola y dejarla online.

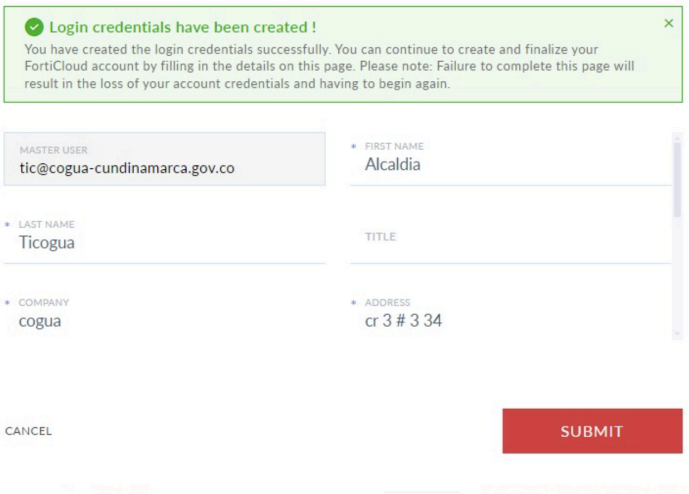
RESUMEN DE ACTIVIDADES DE REALIZADAS

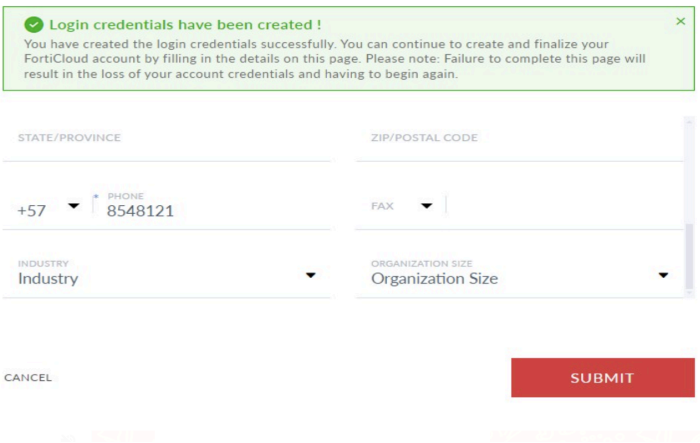
1. Registro de serial del producto.
2. Registro y activación del serial
3. Activación de usuarios sobre el portal de forticloud.
4. Activación y creación de usuarios sobre Forticloud.
5. Activación de Tenant EMS.
6. Creación de usuarios administrativos sobre EMS.
7. Configuración de la base de políticas previo a actividad de despliegue.

Anexamos evidencias.

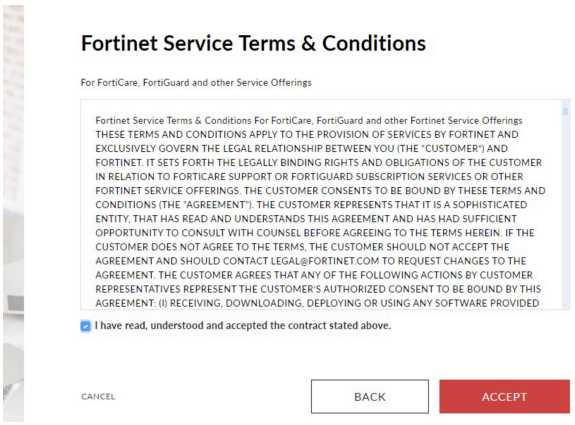
Serial de Renovación: **Serial Number**
FCTEMS8824007787

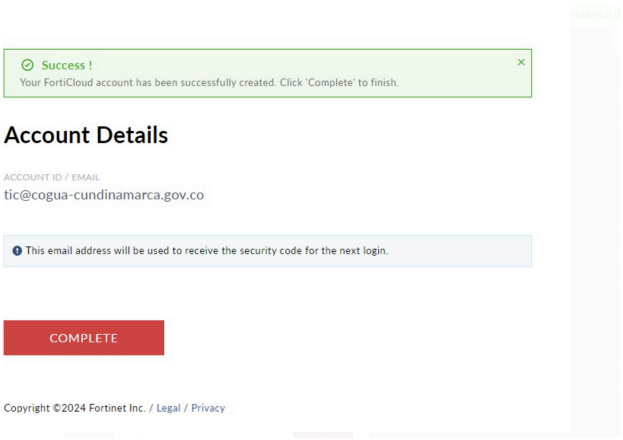
CONFIGURACION DE TENANT FORTICLIENT

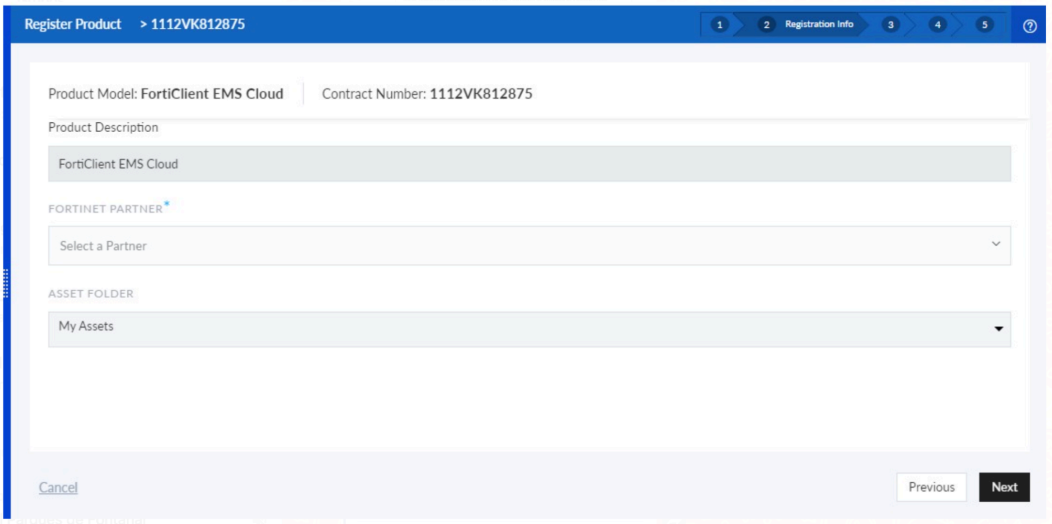




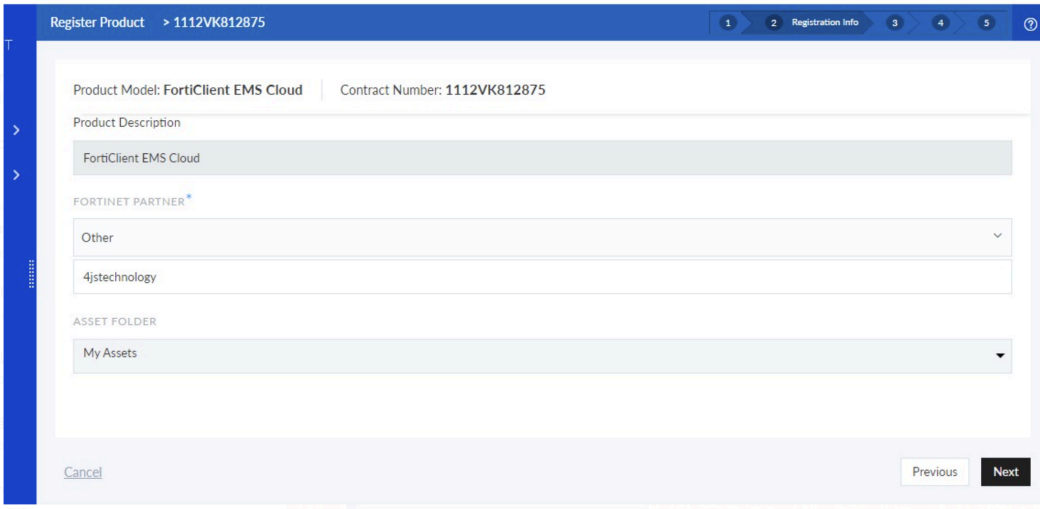

4JSTECHNOLOGY
CONECTANDONOS POR TU SEGURIDAD

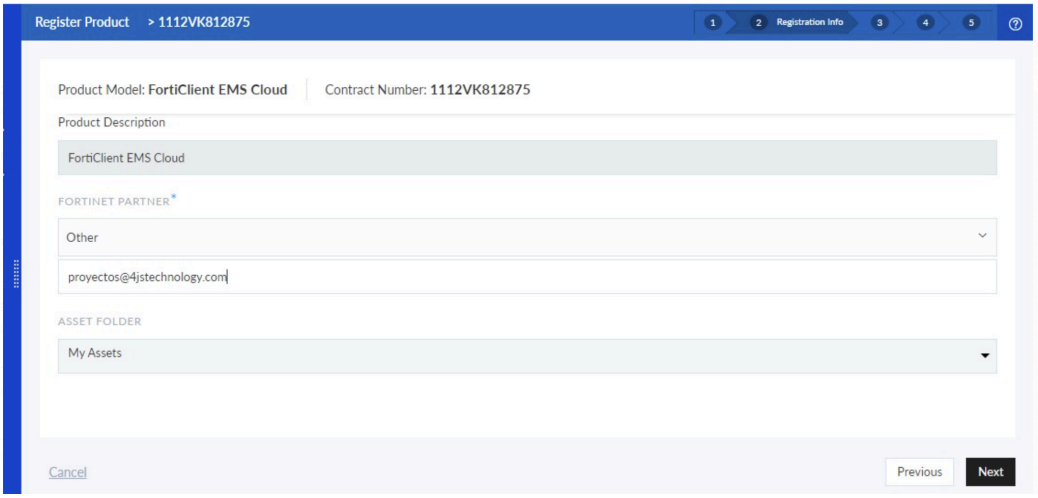

Fortinet Service Terms & Conditions
For FortiCare, FortiGuard and other Service Offerings
Fortinet Service Terms & Conditions For FortiCare, FortiGuard and other Fortinet Service Offerings
THESE TERMS AND CONDITIONS APPLY TO THE PROVISION OF SERVICES BY FORTINET AND EXCLUSIVELY GOVERN THE LEGAL RELATIONSHIP BETWEEN YOU (THE "CUSTOMER") AND FORTINET. IT SETS FORTH THE LEGALLY BINDING RIGHTS AND OBLIGATIONS OF THE CUSTOMER IN RELATION TO FORTICARE SUPPORT OR FORTIGUARD SUBSCRIPTION SERVICES OR OTHER FORTINET SERVICE OFFERINGS. THE CUSTOMER CONSENTS TO BE BOUND BY THESE TERMS AND CONDITIONS (THE "AGREEMENT"). THE CUSTOMER REPRESENTS THAT IT IS A SOPHISTICATED ENTITY, THAT HAS READ AND UNDERSTANDS THIS AGREEMENT AND HAS HAD SUFFICIENT OPPORTUNITY TO CONSULT WITH COUNSEL BEFORE AGREEING TO THE TERMS HEREIN. IF THE CUSTOMER DOES NOT AGREE TO THE TERMS, THE CUSTOMER SHOULD NOT ACCEPT THE AGREEMENT AND SHOULD CONTACT LEGAL@FORTINET.COM TO REQUEST CHANGES TO THE AGREEMENT. THE CUSTOMER AGREES THAT ANY OF THE FOLLOWING ACTIONS BY CUSTOMER REPRESENTATIVES REPRESENT THE CUSTOMER'S AUTHORIZED CONSENT TO BE BOUND BY THIS AGREEMENT: (I) RECEIVING, DOWNLOADING, DEPLOYING OR USING ANY SOFTWARE PROVIDED
I have read, understood and accepted the contract stated above.
CANCEL
BACK
ACCEPT

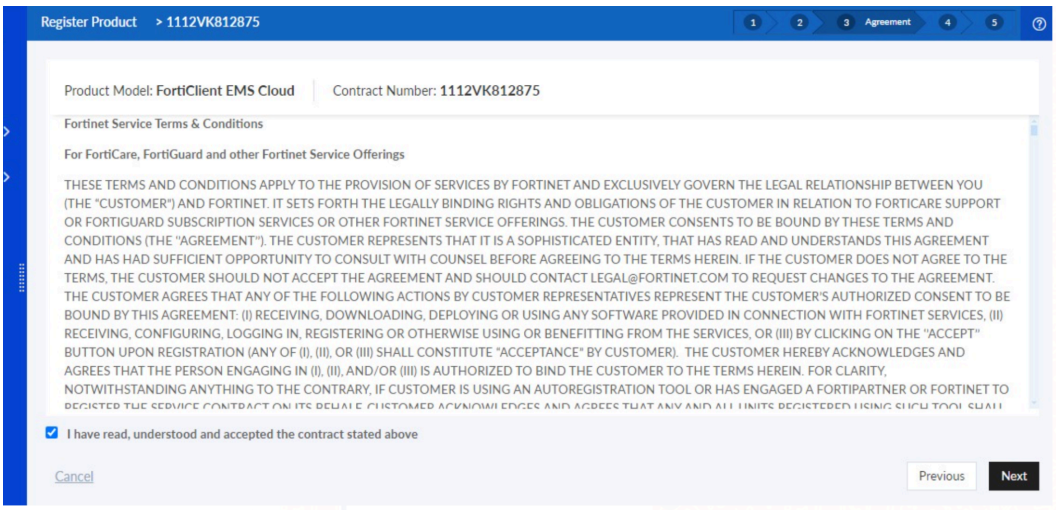

Success !
Your FortiCloud account has been successfully created. Click 'Complete' to finish.
Account Details
ACCOUNT ID / EMAIL
tic@cogua-cundinamarca.gov.co
This email address will be used to receive the security code for the next login.
COMPLETE
Copyright ©2024 Fortinet Inc. / Legal / Privacy


Register Product > 1112VK812875
1
2 Registration Info
3
4
5
Product Model: FortiClient EMS Cloud
Contract Number: 1112VK812875
Product Description
FortiClient EMS Cloud
FORTINET PARTNER*
Select a Partner
ASSET FOLDER
My Assets
Cancel
Previous
Next

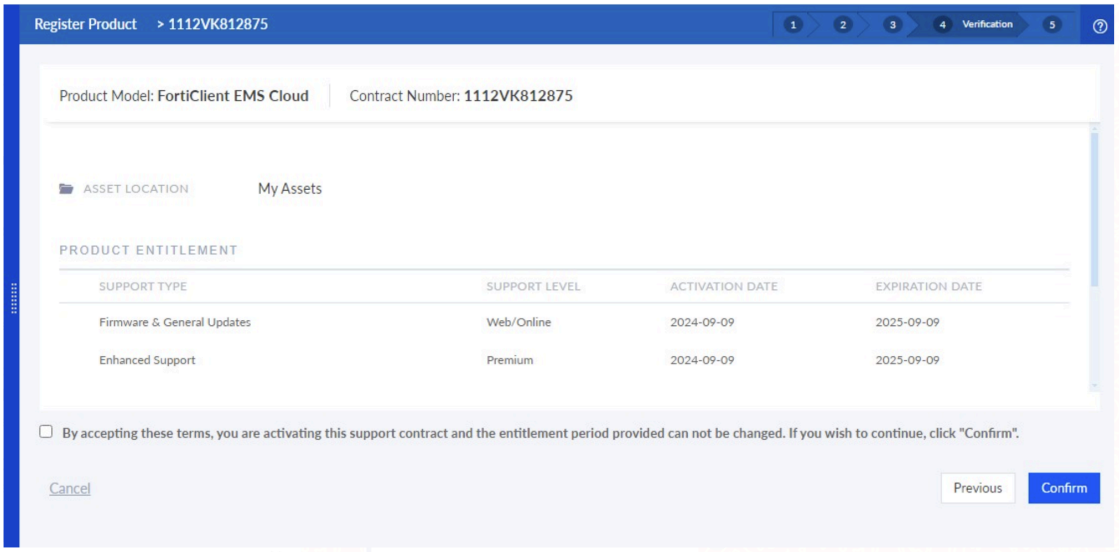

4JSTECHNOLOGY
CONECTANDONOS POR TU SEGURIDAD

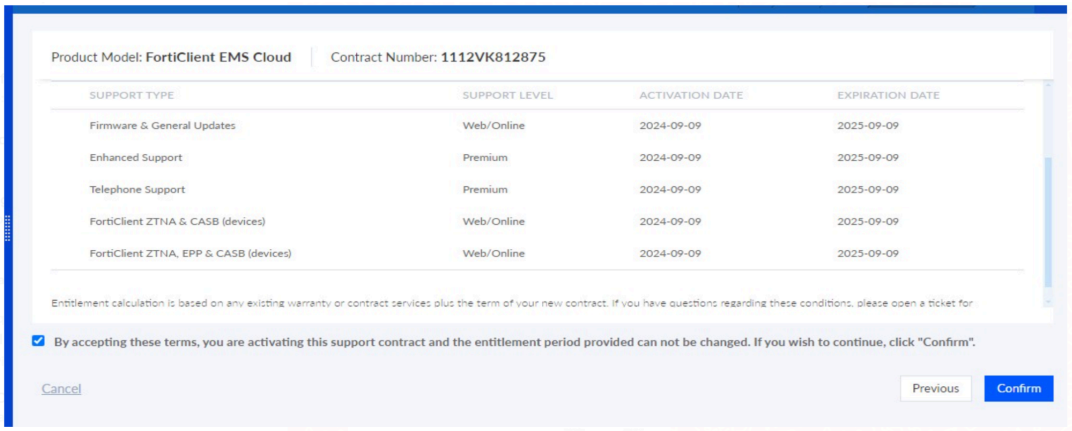

Register Product > 1112VK812875
1 2 Registration Info 3 4 5
Product Model: FortiClient EMS Cloud
Contract Number: 1112VK812875
Product Description
FortiClient EMS Cloud
FORTINET PARTNER*
Other
4jstechnology
ASSET FOLDER
My Assets
Cancel
Previous
Next

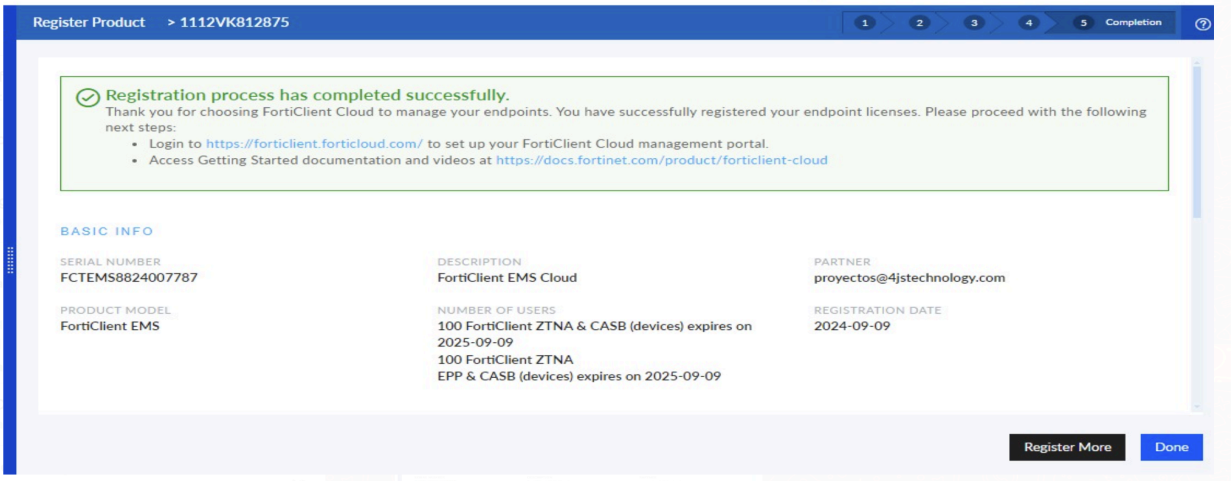

Register Product > 1112VK812875
1 2 Registration Info 3 4 5
Product Model: FortiClient EMS Cloud
Contract Number: 1112VK812875
Product Description
FortiClient EMS Cloud
FORTINET PARTNER*
Other
proyectos@4jstechnology.com
ASSET FOLDER
My Assets
Cancel
Previous
Next


Register Product > 1112VK812875
1 2 3 Agreement 4 5
Product Model: FortiClient EMS Cloud
Contract Number: 1112VK812875
Fortinet Service Terms & Conditions
For FortiCare, FortiGuard and other Fortinet Service Offerings
THESE TERMS AND CONDITIONS APPLY TO THE PROVISION OF SERVICES BY FORTINET AND EXCLUSIVELY GOVERN THE LEGAL RELATIONSHIP BETWEEN YOU (THE "CUSTOMER") AND FORTINET. IT SETS FORTH THE LEGALLY BINDING RIGHTS AND OBLIGATIONS OF THE CUSTOMER IN RELATION TO FORTICARE SUPPORT OR FORTIGUARD SUBSCRIPTION SERVICES OR OTHER FORTINET SERVICE OFFERINGS. THE CUSTOMER CONSENTS TO BE BOUND BY THESE TERMS AND CONDITIONS (THE "AGREEMENT"). THE CUSTOMER REPRESENTS THAT IT IS A SOPHISTICATED ENTITY, THAT HAS READ AND UNDERSTANDS THIS AGREEMENT AND HAS HAD SUFFICIENT OPPORTUNITY TO CONSULT WITH COUNSEL BEFORE AGREEING TO THE TERMS HEREIN. IF THE CUSTOMER DOES NOT AGREE TO THE TERMS, THE CUSTOMER SHOULD NOT ACCEPT THE AGREEMENT AND SHOULD CONTACT LEGAL@FORTINET.COM TO REQUEST CHANGES TO THE AGREEMENT. THE CUSTOMER AGREES THAT ANY OF THE FOLLOWING ACTIONS BY CUSTOMER REPRESENTATIVES REPRESENT THE CUSTOMER'S AUTHORIZED CONSENT TO BE BOUND BY THIS AGREEMENT: (I) RECEIVING, DOWNLOADING, DEPLOYING OR USING ANY SOFTWARE PROVIDED IN CONNECTION WITH FORTINET SERVICES, (II) RECEIVING, CONFIGURING, LOGGING IN, REGISTERING OR OTHERWISE USING OR BENEFITTING FROM THE SERVICES, OR (III) BY CLICKING ON THE "ACCEPT" BUTTON UPON REGISTRATION (ANY OF (I), (II), OR (III) SHALL CONSTITUTE "ACCEPTANCE" BY CUSTOMER). THE CUSTOMER HEREBY ACKNOWLEDGES AND AGREES THAT THE PERSON ENGAGING IN (I), (II), AND/OR (III) IS AUTHORIZED TO BIND THE CUSTOMER TO THE TERMS HEREIN. FOR CLARITY, NOTWITHSTANDING ANYTHING TO THE CONTRARY, IF CUSTOMER IS USING AN AUTOREGISTRATION TOOL OR HAS ENGAGED A FORTIPARTNER OR FORTINET TO
I have read, understood and accepted the contract stated above
Cancel
Previous
Next

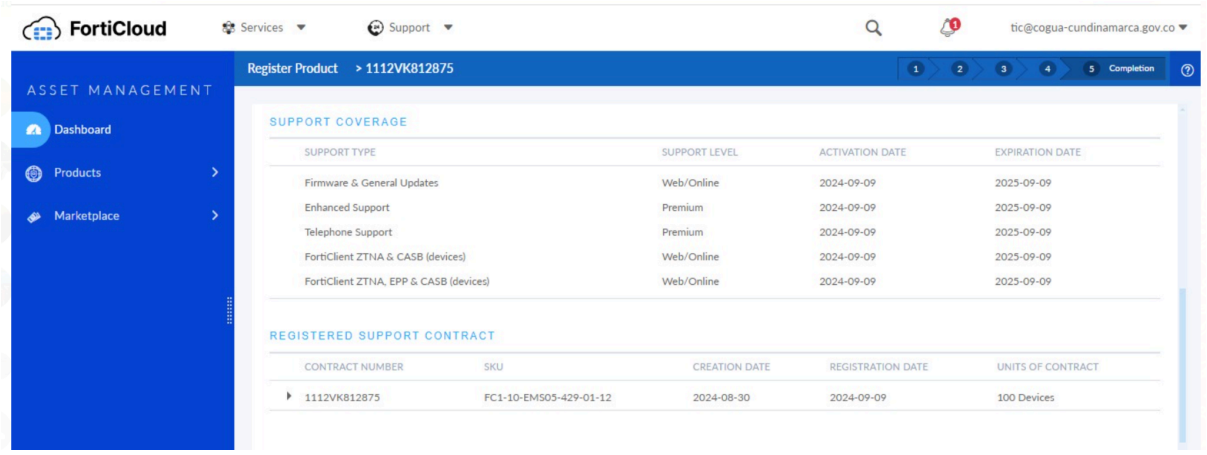

4JSTECHNOLOGY
CONECTANDONOS POR TU SEGURIDAD

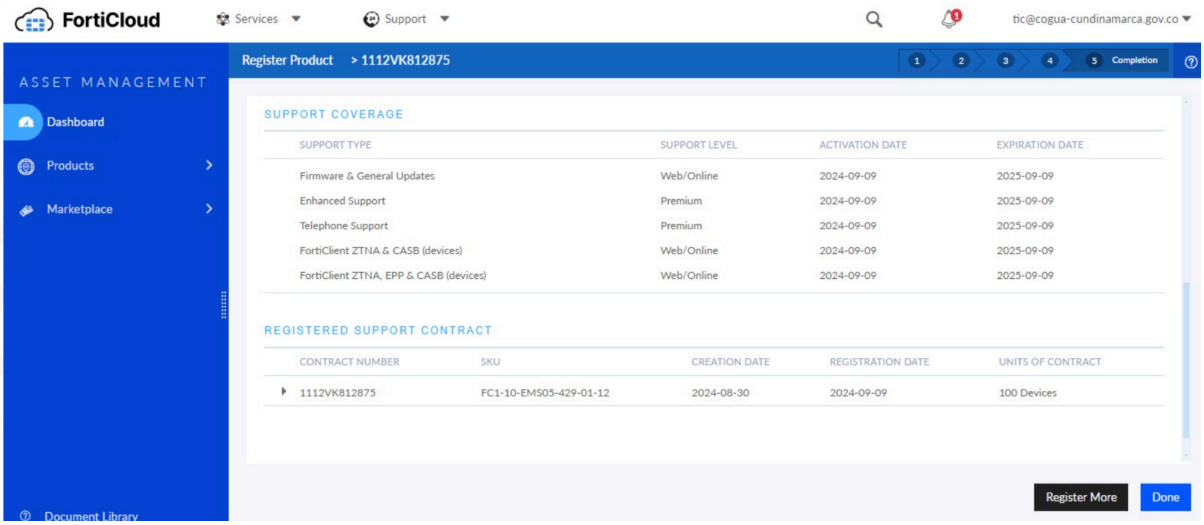

Register Product > 1112VK812875
1 2 3 4 Verification 5
Product Model: FortiClient EMS Cloud
Contract Number: 1112VK812875
ASSET LOCATION
My Assets
PRODUCT ENTITLEMENT
SUPPORT TYPE
SUPPORT LEVEL
ACTIVATION DATE
EXPIRATION DATE
Firmware & General Updates
Web/Online
2024-09-09
2025-09-09
Enhanced Support
Premium
2024-09-09
2025-09-09
By accepting these terms, you are activating this support contract and the entitlement period provided can not be changed. If you wish to continue, click "Confirm".
Cancel
Previous
Confirm

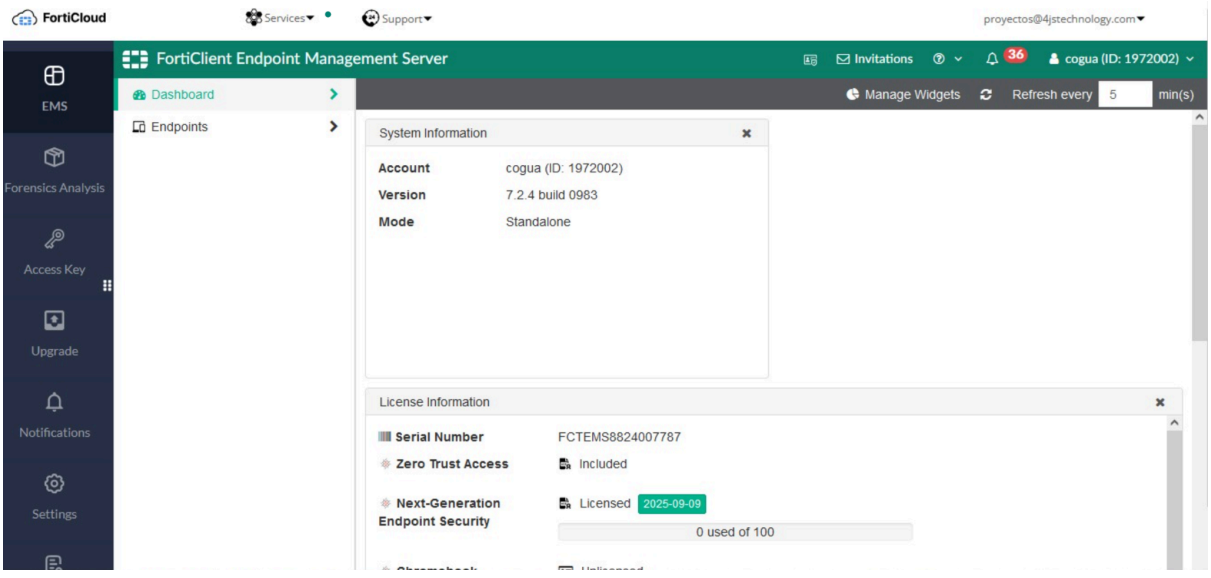

Product Model: FortiClient EMS Cloud
Contract Number: 1112VK812875
SUPPORT TYPE
SUPPORT LEVEL
ACTIVATION DATE
EXPIRATION DATE
Firmware & General Updates
Web/Online
2024-09-09
2025-09-09
Enhanced Support
Premium
2024-09-09
2025-09-09
Telephone Support
Premium
2024-09-09
2025-09-09
FortiClient ZTNA & CASB (devices)
Web/Online
2024-09-09
2025-09-09
FortiClient ZTNA, EPP & CASB (devices)
Web/Online
2024-09-09
2025-09-09
Entitlement calculation is based on any existing warranty or contract services plus the term of your new contract. If you have questions regarding these conditions, please open a ticket for
By accepting these terms, you are activating this support contract and the entitlement period provided can not be changed. If you wish to continue, click "Confirm".
Cancel
Previous
Confirm


Register Product > 1112VK812875
1 2 3 4 5 Completion
Registration process has completed successfully.
Thank you for choosing FortiClient Cloud to manage your endpoints. You have successfully registered your endpoint licenses. Please proceed with the following next steps:
Login to https://forticlient.forticloud.com/ to set up your FortiClient Cloud management portal.
Access Getting Started documentation and videos at https://docs.fortinet.com/product/forticlient-cloud
BASIC INFO
SERIAL NUMBER
FCTEMS8824007787
DESCRIPTION
FortiClient EMS Cloud
PARTNER
proyectos@4jstechnology.com
PRODUCT MODEL
FortiClient EMS
NUMBER OF USERS
100 FortiClient ZTNA & CASB (devices) expires on 2025-09-09
100 FortiClient ZTNA
EPP & CASB (devices) expires on 2025-09-09
REGISTRATION DATE
2024-09-09
Register More
Done


4JSTECHNOLOGY
CONECTANDONOS POR TU SEGURIDAD

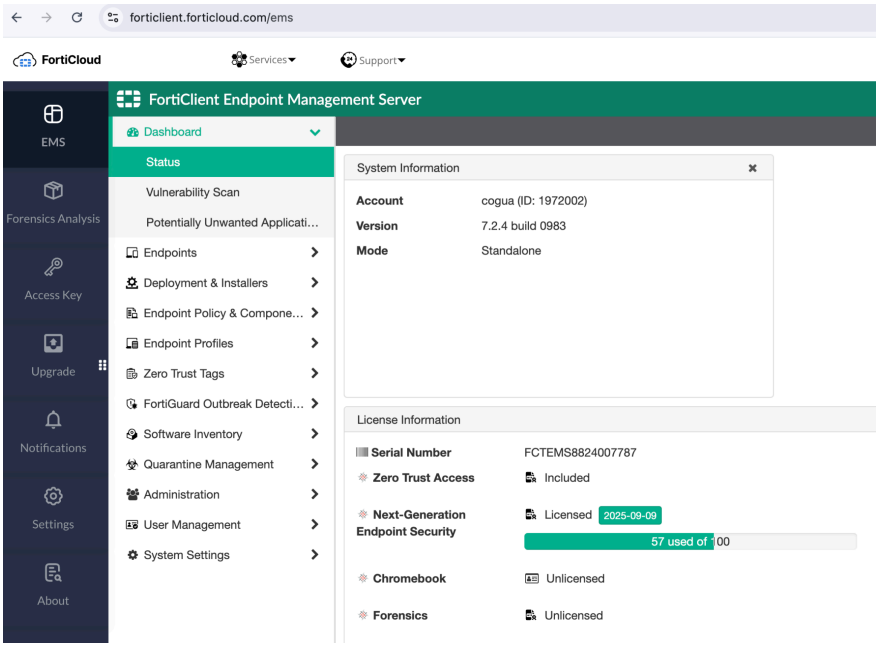

FortiCloud
Services
Support
tic@cogua-cundinamarca.gov.co
ASSET MANAGEMENT
Dashboard
Products
Marketplace
Register Product > 1112VK812875
1 2 3 4 5 Completion
SUPPORT COVERAGE
SUPPORT TYPE
SUPPORT LEVEL
ACTIVATION DATE
EXPIRATION DATE
Firmware & General Updates
Web/Online
2024-09-09
2025-09-09
Enhanced Support
Premium
2024-09-09
2025-09-09
Telephone Support
Premium
2024-09-09
2025-09-09
FortiClient ZTNA & CASB (devices)
Web/Online
2024-09-09
2025-09-09
FortiClient ZTNA, EPP & CASB (devices)
Web/Online
2024-09-09
2025-09-09
REGISTERED SUPPORT CONTRACT
CONTRACT NUMBER
SKU
CREATION DATE
REGISTRATION DATE
UNITS OF CONTRACT
1112VK812875
FC1-10-EMS05-429-01-12
2024-08-30
2024-09-09
100 Devices


FortiCloud
Services
Support
tic@cogua-cundinamarca.gov.co
ASSET MANAGEMENT
Dashboard
Products
Marketplace
Document Library
Register Product > 1112VK812875
1 2 3 4 5 Completion
SUPPORT COVERAGE
SUPPORT TYPE
SUPPORT LEVEL
ACTIVATION DATE
EXPIRATION DATE
Firmware & General Updates
Web/Online
2024-09-09
2025-09-09
Enhanced Support
Premium
2024-09-09
2025-09-09
Telephone Support
Premium
2024-09-09
2025-09-09
FortiClient ZTNA & CASB (devices)
Web/Online
2024-09-09
2025-09-09
FortiClient ZTNA, EPP & CASB (devices)
Web/Online
2024-09-09
2025-09-09
REGISTERED SUPPORT CONTRACT
CONTRACT NUMBER
SKU
CREATION DATE
REGISTRATION DATE
UNITS OF CONTRACT
1112VK812875
FC1-10-EMS05-429-01-12
2024-08-30
2024-09-09
100 Devices
Register More
Done


FortiCloud
Services
Support
proyectos@4jstechnology.com
EMS
Forensics Analysis
Access Key
Upgrade
Notifications
Settings
FortiClient Endpoint Management Server
Invitations
36
cogua (ID: 1972002)
Dashboard
Endpoints
Manage Widgets
Refresh every 5 min(s)
System Information
Account cogua (ID: 1972002)
Version 7.2.4 build 0983
Mode Standalone
License Information
Serial Number FCTEMS8824007787
Zero Trust Access Included
Next-Generation Endpoint Security
Licensed 2025-09-09
0 used of 100

7. El CONTRATISTA se obliga a garantizar el funcionamiento del antivirus en la Alcaldía Municipal de Cogua.

R/ Se deja instalado en las 100 máquinas instalada la licencia de Antivirus Forticlient Versión 7.2.5 liberada por fabricante y queda un remanente de libre uso para instalar en equipos nuevos.



8. EL CONTRATISTA se obliga a integrar la plataforma de protección contra amenazas avanzadas (antivirus), con la plataforma de Firewall de Nueva Generación (NGFW) de la entidad

R/ Esta actividad no se puede realizar hasta que la licencia de NGFW esté vigente y activa por la Entidad.

9. EL CONTRATISTA se obliga a estar disponible, y dar el soporte requerido de la bolsa de 8 horas a demanda y requerimientos TI de la entidad.

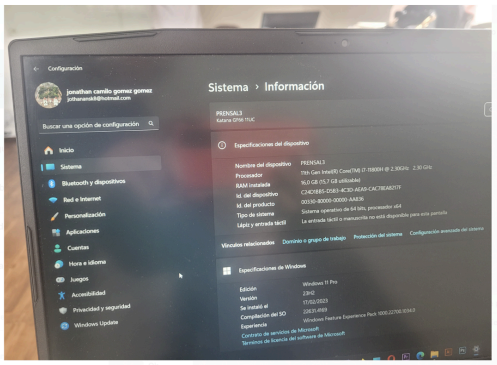
R/ La Entidad ya está en ejecución de la Bolsa de Horas de soporte, la finalización de la implementación fue el 25 de septiembre en el total de estaciones, el primer soporte se realizó el 4 de Octubre a fin de excluir una aplicación de Photoshop que generó un bloqueo en una máquina de Prensa.

Primer Soporte , 1 hora. 4 de Octubre
Solicito Inge Giovanny Ortiz
Resolvio 4JSTECHNOLOGY

SOPORTE SOLICITADO PRA EXCLUSION DE APLICACION BLOQUEANTE
4 mensajes

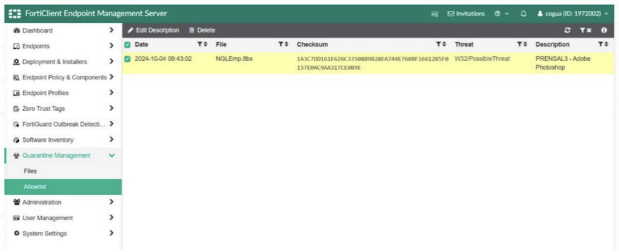
proyectos Consultoria <proyectos@4jstechnology.com>
Para: tic.alcaldiacogua@gmail.com, TIC Cogua <tic@cogua-cundinamarca.gov.co>
CC: Soporte Nitromacsas <soporte_@nitromacsas.com>

Se comunica el Ingeniero Giovanny Ortiz el 4 de Octubre reportando un bloqueo sobre la máquina de prensa



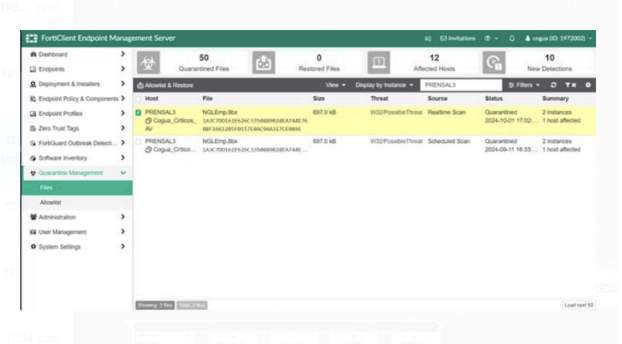
El antivirus bloqueo Photoshop y otro editor que utilizan

Se trabaja en la resolución de este soporte agregando la exclusión de esta aplicación en la consola para que el antivirus no la bloquee.



Entran aqui y seleccionan el archivo, luego le dan arriba en allow list y restore

Luego pueden ir a las listas de los archivos permitidos y colocarle un nombre o una descripción



10. EL CONTRATISTA se obliga a contratar por cuenta propia el personal idóneo y capacitado así, un líder de proyectos, ingeniero de sistemas, electrónico y/o de telecomunicaciones graduado, diploma y acta de grado, con experiencia mínima de tres años, en gestión de proyectos, y consultoría de soluciones tecnológicas, ingeniero de implementación y/o soporte de sistemas, electrónico y/o de telecomunicaciones, graduado, diploma y acta de grado, con experiencia en instalaciones, soporte y/o mantenimiento en soluciones de seguridad en



Fortinet de 2 años, con certificaciones Fortinet Certified Fundamentals, NSE4 y Scrum Foundation para la ejecución de este proyecto, adjuntar las respectivas hojas de vida y certificaciones

R/ Se hizo uso de los dos recursos solicitados por el contrato y ejecutados en el proyecto de instalación. Ingeniero de proyectos e ingeniero de implementación con las certificaciones descritas en el anexo técnico del contrato.

11. Las demás que se requieran de acuerdo con la naturaleza del contrato

R/ Se realizó apoyo presencial durante la instalación e implementación de las estaciones de la alcaldía, se realizaron más de 6 visitas presenciales a la alcaldía para la realización y apoyo del proyecto.



OTRAS EVIDENCIAS Y ANEXOS.

Usuarios:

John Edgar Peña Lobo 4:45 p.m.
support.fortinet.com
*1pyth0nt59gD

TIC Cogua 4:52 p.m.
ticcogua@gmail.com

Usuario Partner

proyectos@4jstechnology.com (adminpartner)

Hello!
Thank you for registering your FortiClient License. The FortiClient Cloud instance for tic@cogua-cundinamarca.gov.co (ID: 1972002) has been activated and is ready to use.

ACCESO FORTICLIENT CLOUD

https://forticlient.forticloud.com/static/client/index.htmL

Recursos Fortinet - Forticlient

Getting Started with FortiClient Cloud

https://video.fortinet.com/products/forticlient-ems/7.0/getting-started-with-forticlient-cloud

If you require further assistance, please contact Fortinet Support at
https://www.fortinet.com/support/contact.html

RELATED RESOURCES
Technical Documentation:



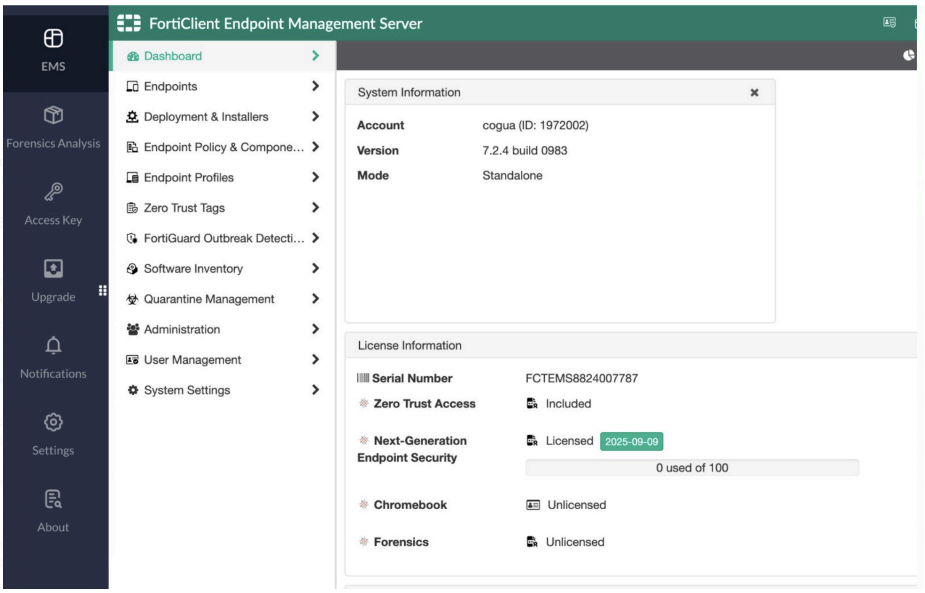
FortiClient and FortiClient EMS Documentation

Technical Videos:
FortiClient Video

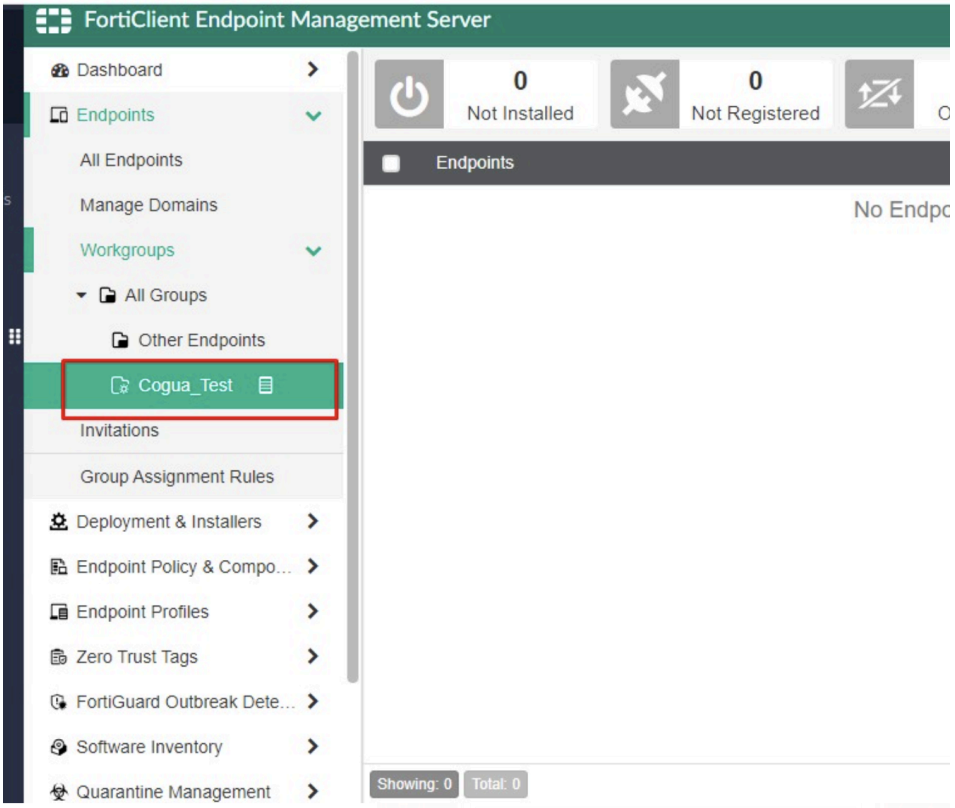
SESIÓN #2 10 DE SEPTIEMBRE

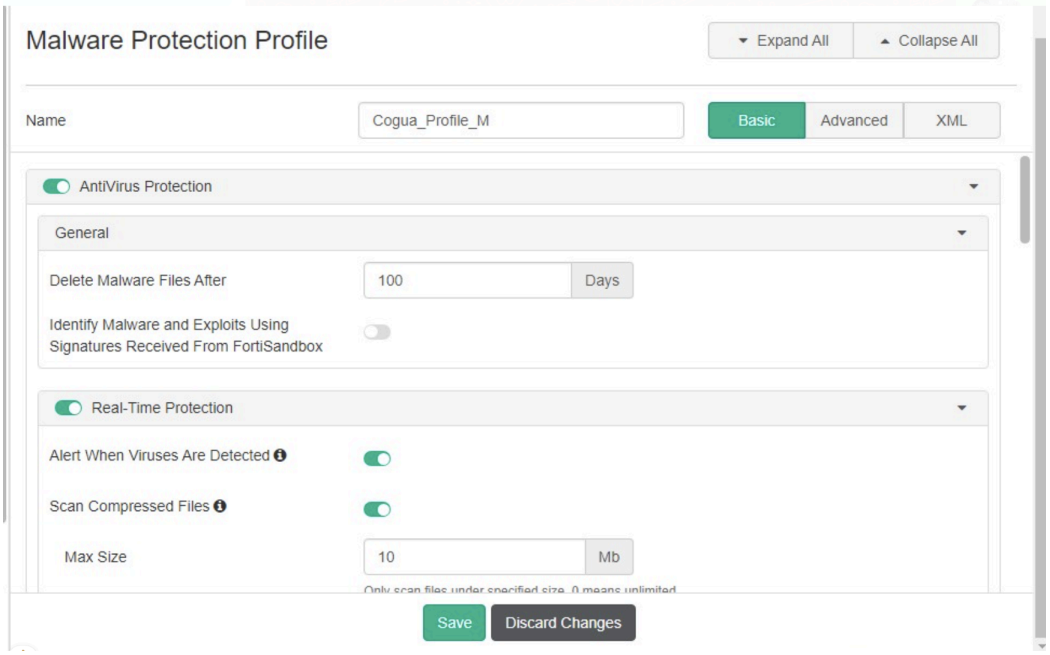
Se solicita al cliente definir grupos de usuarios y las categorías para definir las reglas de web filtering y aplicaciones de negocio.

Se trabajó en creación de algunas políticas bases, como perfil de malware, igual se creó un grupo de pruebas para probar usuarios. (anexamos evidencias)

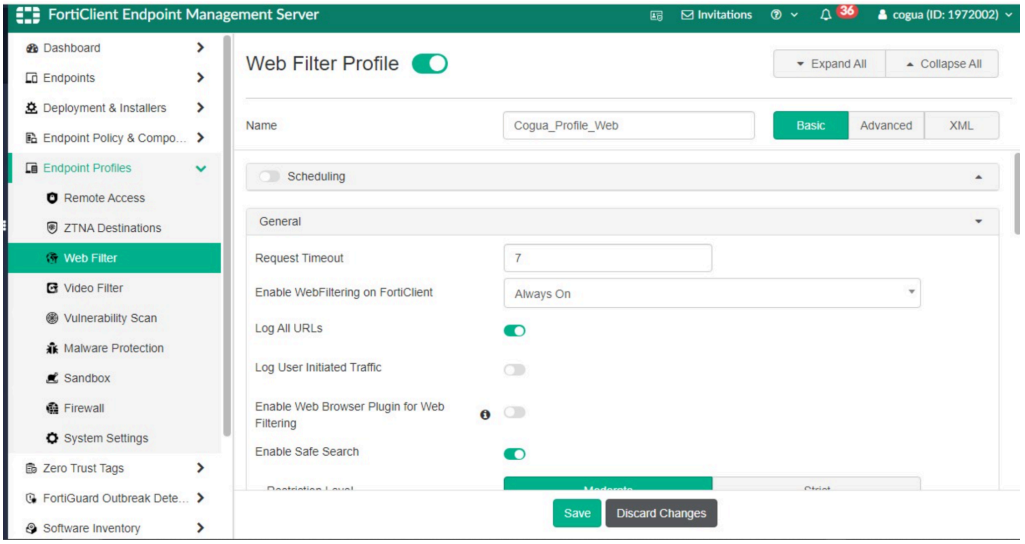


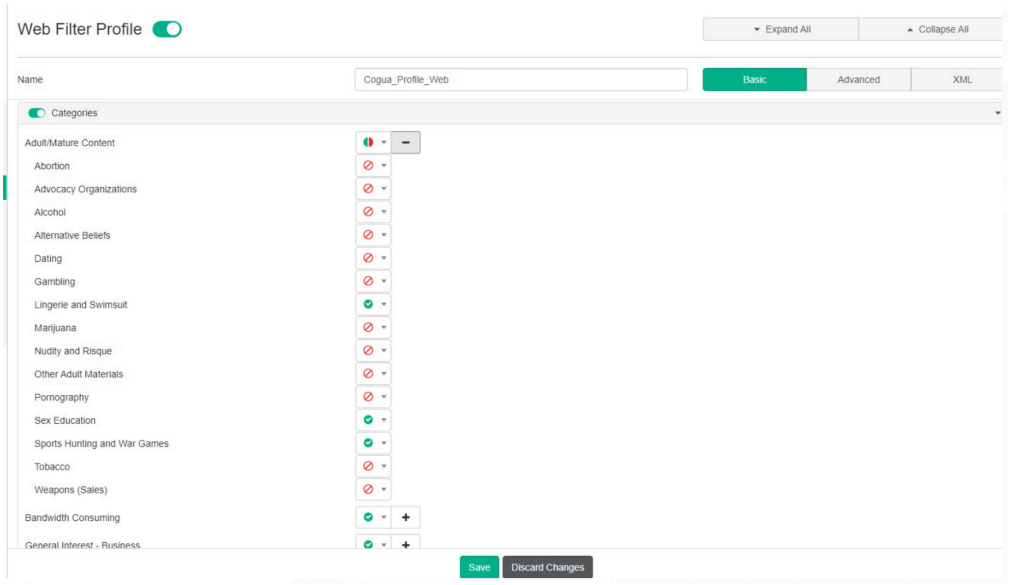

4JSTECHNOLOGY
CONECTANDONOS POR TU SEGURIDAD


FortiClient Endpoint Management Server
Dashboard
Endpoints
All Endpoints
Manage Domains
Workgroups
All Groups
Other Endpoints
Cogua_Test
Invitations
Group Assignment Rules
Deployment & Installers
Endpoint Policy & Compo...
Endpoint Profiles
Zero Trust Tags
FortiGuard Outbreak Dete...
Software Inventory
Quarantine Management
0
Not Installed
0
Not Registered
Endpoints
No Endpc
Showing: 0
Total: 0


Malware Protection Profile
Expand All
Collapse All
Name
Cogua_Profile_M
Basic
Advanced
XML
AntiVirus Protection
General
Delete Malware Files After
100
Days
Identify Malware and Exploits Using Signatures Received From FortiSandbox
Real-Time Protection
Alert When Viruses Are Detected
Scan Compressed Files
Max Size
10
Mb
Save
Discard Changes


4JSTECHNOLOGY
CONECTANDONOS POR TU SEGURIDAD


FortiClient Endpoint Management Server
Invitations
36
cogua (ID: 1972002)
Dashboard
Endpoints
Deployment & Installers
Endpoint Policy & Compo...
Endpoint Profiles
Remote Access
ZTNA Destinations
Web Filter
Video Filter
Vulnerability Scan
Malware Protection
Sandbox
Firewall
System Settings
Zero Trust Tags
FortiGuard Outbreak Dete...
Software Inventory
Web Filter Profile
Expand All
Collapse All
Name
Cogua_Profile_Web
Basic
Advanced
XML
Scheduling
General
Request Timeout
7
Enable WebFiltering on FortiClient
Always On
Log All URLs
Log User Initiated Traffic
Enable Web Browser Plugin for Web Filtering
Enable Safe Search
Save
Discard Changes


Web Filter Profile
Expand All
Collapse All
Name
Cogua_Profile_Web
Basic
Advanced
XML
Categories
Adult/Mature Content
Abortion
Advocacy Organizations
Alcohol
Alternative Beliefs
Dating
Gambling
Lingerie and Swimsuit
Marijuana
Nudity and Risque
Other Adult Materials
Pornography
Sex Education
Sports Hunting and War Games
Tobacco
Weapons (Sales)
Bandwidth Consuming
General Interest - Business
Save
Discard Changes



- Bandwidth Consuming
  - File Sharing and Storage
  - Freeware and Software Downloads
  - Internet Radio and TV
  - Internet Telephony
  - Peer-to-peer File Sharing
  - Streaming Media and Download

- Bandwidth Consuming
- General Interest - Business
  - Armed Forces
  - Business
  - Charitable Organizations
  - Finance and Banking
  - General Organizations
  - Government and Legal Organizations
  - Information and Computer Security
  - Information Technology
  - Online Meeting
  - Remote Access
  - Search Engines and Portals
  - Secure Websites
  - URL Shortening
  - Web Analytics
  - Web Hosting
  - Web-based Applications



- Health and Wellness
- Instant Messaging
- Job Search
- Meaningless Content
- Medicine
- News and Media
- Newsgroups and Message Boards
- Personal Privacy
- Personal Vehicles
- Personal Websites and Blogs
- Political Organizations
- Real Estate
- Reference
- Restaurant and Dining
- Shopping
- Social Networking
- Society and Lifestyles
- Sports
- Travel
- Web Chat

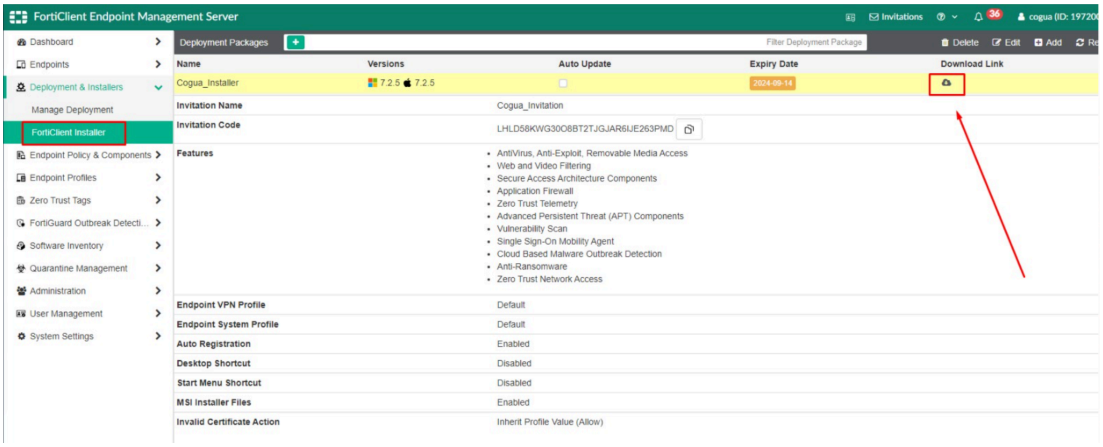
- Potentially Liable
  - Child Sexual Abuse
  - Crypto Mining
  - Discrimination
  - Drug Abuse
  - Explicit Violence
  - Extremist Groups
  - Hacking
  - Illegal or Unethical
  - Plagiarism
  - Potentially Unwanted Program
  - Proxy Avoidance
  - Terrorism



Security Risk	
Dynamic DNS	
Malicious Websites	
Newly Observed Domain	
Newly Registered Domain	
Phishing	
Spam URLs	
Unrated	
Rate IP Addresses	
Allow websites when rating error occurs	

Profile (Off-Fabric)		
Profile	VPN	Default
	ZTNA	Default
	WF	Cogua_Profile_Web
	VF	Default
	VULN	Default
	MW	Cogua_Profile_M
	SB	Default
	FW	Default
	SYS	Default
Download Profile XML		Profile XML

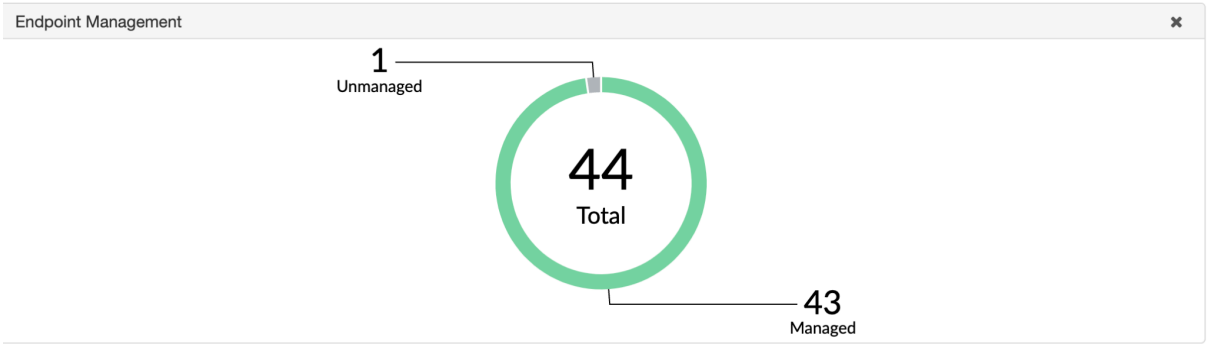
DESCARGA DE CLIENTE FORTICLIENT



19 de septiembre (Visita Presencial)

Se han realizado ya varias asistencias técnicas con el fin de realizar la instalación ya de los equipos en las diferentes sedes mencionadas y solicitadas.

A la fecha se logró ya la instalación de 44 estaciones con el agente de forticlient. se anexa evidencia.

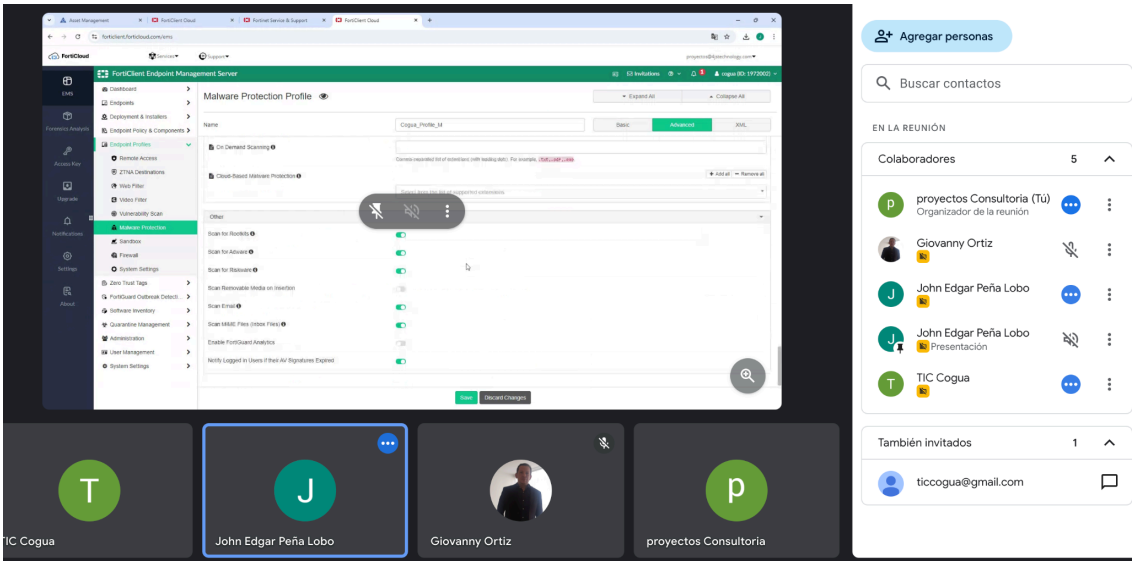


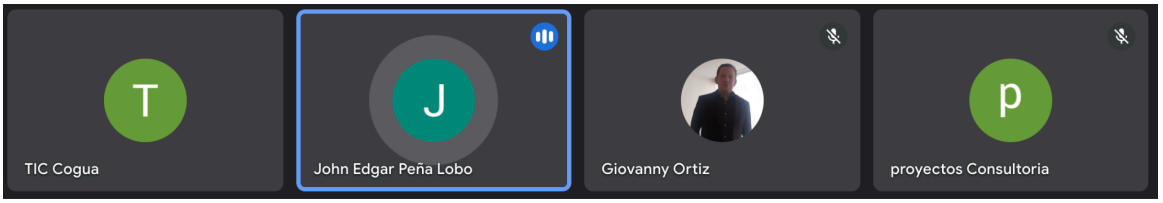
Hallazgos Generales y Recomendaciones.

1. La alcaldía debe definir cuales son los equipos restantes a los que se debe instalar el agente y su ubicación respectiva.
2. Se dejan a solicitud de la subgerencia 15 licencias para uso de equipos nuevos que están por adquirir.

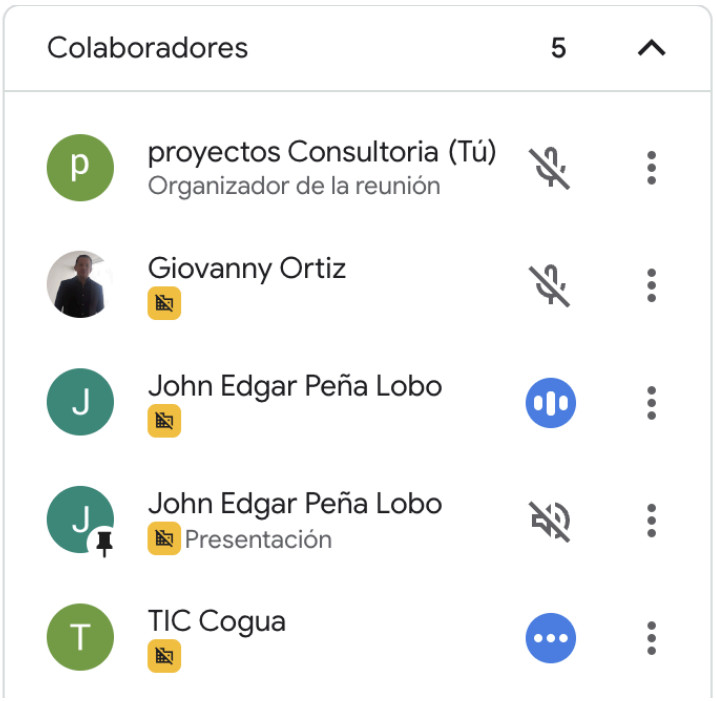
3. Se realizará transferencia de conocimiento a personal técnico el 20 de septiembre 10 am.
4. Se construyeron 3 perfiles de Antivirus, uno básico y otro para equipos críticos con el fin de evitar afectaciones en las estaciones de los usuarios.
5. Todas las actividades han sido supervisadas por el ingeniero Giovanni del área de TIC.

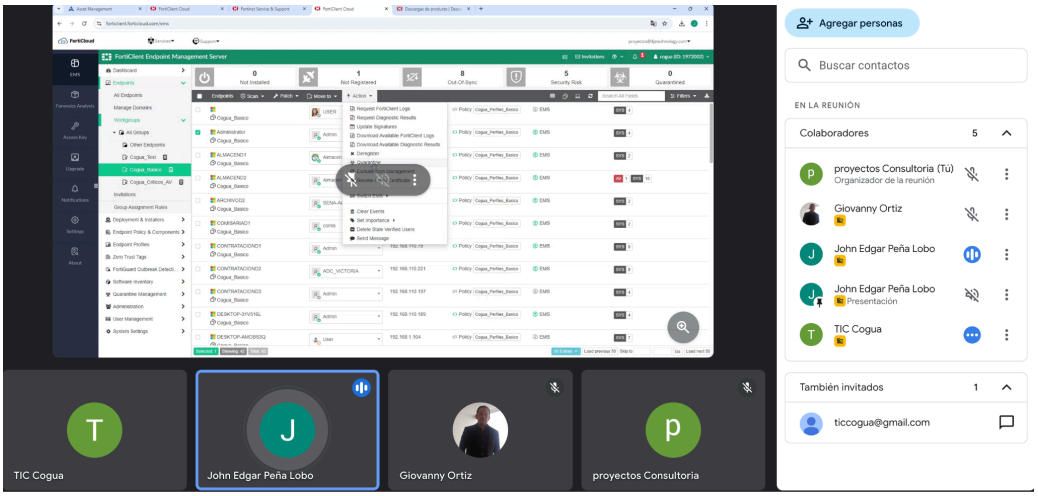
SESION DE TRANSFERENCIA DE CONOCIMIENTO CON EQUIPO TÉCNICO DE COGUA 20 DE SEPTIEMBRE











Sesión #5 y #6 Visita 24 y 25 de septiembre.

1. Se logra realizar instalación de licencia de antivirus en los edificios restantes donde existe cómputo de la alcaldía.

Inspección de Policía 3 estaciones de trabajo.
Casa de la cultura 3 estaciones de trabajo.
Deportes 4 estaciones de trabajo.



Turismo 1 estación de computo
Casa de la mujer 1 estación de computo.

Total de máquinas instaladas 100. De esta forma se abarcan el total de dependencias y estaciones de trabajo de la alcaldía.

Excepciones Realizadas.

1. Maquinas windows 7
2. Maquinas de gerentes debido a la instrucción dada por Diego Rodriguez.
3. Máquinas que no estuvieran en uso , aprobó Giovanny Ortiz.

Se anexa reporte de antivirus detectado en la máquina **SUBGENER ALD5** ya que se identificó que desde aplicaciones como Firefox, Chrome y Teams se descargaron archivos maliciosos

Se anexa reporte con evidencia del análisis realizado.

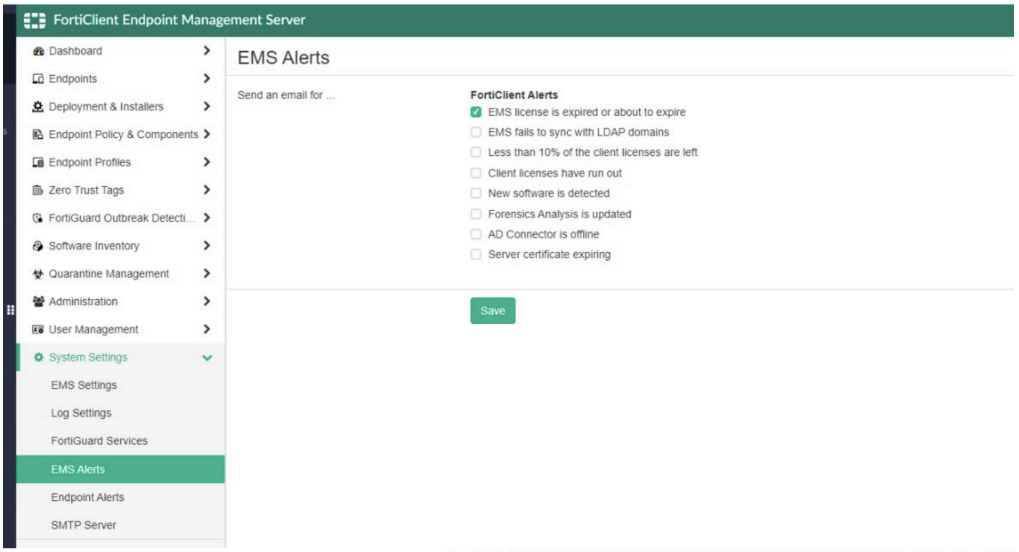


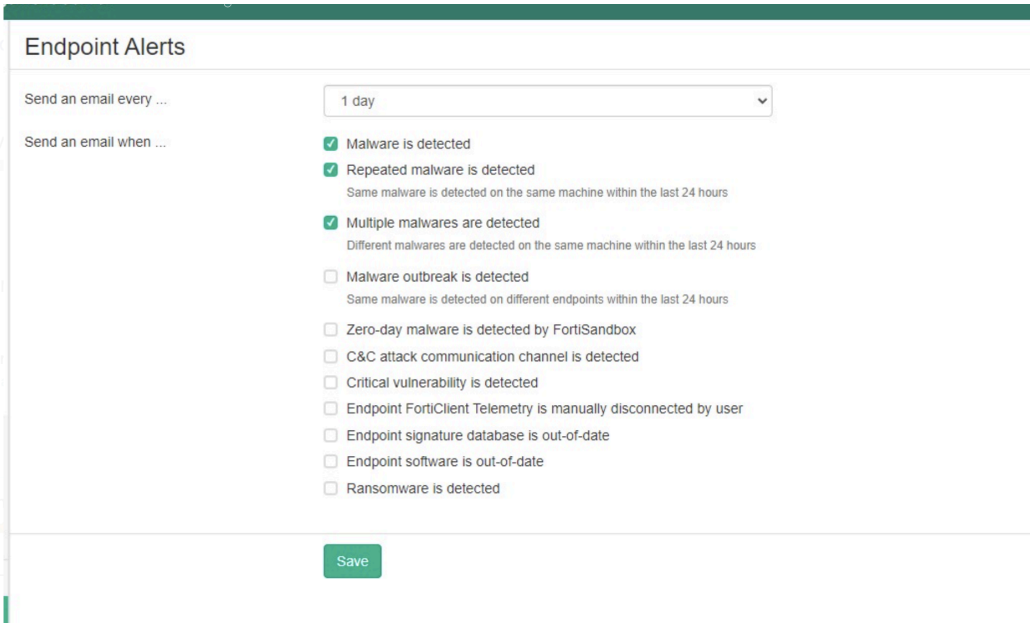
Host	Fecha	Tipo de malware	Ruta	Accion
SUBGENERALD5	21/09/2024 13:06	W32/Generic.AC.171!tr	C:\Users\ADMIN\Documents\2021\Nueva carpeta\TeamsSetupx64_s_8D9000F597191A5-7-0_.exe	El archivo fue puesto en cuarentena.
SUBGENERALD5	21/09/2024 12:35	W32/Generic.AC.171!tr	C:\Users\ADMIN\pure3401seguro260801.exe	El archivo fue puesto en cuarentena.
SUBGENERALD5	21/09/2024 12:32	W32/Generic.AC.171!tr	C:\Users\ADMIN\Downloads\L380_X64_25002_LA\WINX64\SETUP\DEVPGENP\ENPINST\ENP.exe	El archivo fue puesto en cuarentena.
SUBGENERALD5	21/09/2024 12:32	W32/Generic.AC.171!tr	C:\Users\ADMIN\Downloads\L380_X64_25002_LA\WINX64\SETUP\DEVPGENP\DevopENP.exe	El archivo fue puesto en cuarentena.
SUBGENERALD5	21/09/2024 12:32	W32/Generic.AC.171!tr	C:\Users\ADMIN\Downloads\L380_X64_25002_LA\WINX64\SETUP\SETUP64.EXE	El archivo fue puesto en cuarentena.
SUBGENERALD5	21/09/2024 12:32	W32/Generic.AC.171!tr	C:\Users\ADMIN\Downloads\L380_X64_25002_LA\WINX64\SETUP\DEVICEOP.EXE	El archivo fue puesto en cuarentena.
SUBGENERALD5	21/09/2024	W32/PossibleThreat		El archivo fue puesto

A	B	C	D	E
Host	Fecha	Tipo de malware	Ruta	Accion
SUBGENERALD5	9/21/24 13:06	W32/Generic.AC.171!tr	C:\Users\ADMIN\Documents\2021\Nueva carpeta\TeamsSetupx64_s_8D9000F597191A5-7-0_.exe	El archivo fue puesto en cuarentena.
SUBGENERALD5	9/21/24 12:35	W32/Generic.AC.171!tr	C:\Users\ADMIN\pure3401seguro260801.exe	El archivo fue puesto en cuarentena.
SUBGENERALD5	9/21/24 12:32	W32/Generic.AC.171!tr	C:\Users\ADMIN\Downloads\L380_X64_25002_LA\WINX64\SETUP\DEVPGENP\ENPINST\ENP.exe	El archivo fue puesto en cuarentena.
SUBGENERALD5	9/21/24 12:32	W32/Generic.AC.171!tr	C:\Users\ADMIN\Downloads\L380_X64_25002_LA\WINX64\SETUP\DEVPGENP\DevopENP.exe	El archivo fue puesto en cuarentena.
SUBGENERALD5	9/21/24 12:32	W32/Generic.AC.171!tr	C:\Users\ADMIN\Downloads\L380_X64_25002_LA\WINX64\SETUP\SETUP64.EXE	El archivo fue puesto en cuarentena.
SUBGENERALD5	9/21/24 12:32	W32/Generic.AC.171!tr	C:\Users\ADMIN\Downloads\L380_X64_25002_LA\WINX64\SETUP\DEVICEOP.EXE	El archivo fue puesto en cuarentena.
SUBGENERALD5	9/21/24 12:27	W32/PossibleThreat	C:\Users\ADMIN\Downloads\RADICADO	El archivo fue puesto en cuarentena.
SUBGENERALD5	9/21/24 12:17	W32/Generic.AC.171!tr	C:\Users\ADMIN\Downloads\OperaSetup.exe	El archivo fue puesto en cuarentena.
SUBGENERALD5	9/21/24 12:17	W32/Generic.AC.171!tr	C:\Users\ADMIN\Downloads\Zoom_cm_fobksunvtsZ9vvrZo4_mEc-Cxz6+ePdStAvTWHn02Ah80mGQPhzcoCDm@161OKYKsvM7EqhwA_kd813	El archivo fue puesto en cuarentena.
SUBGENERALD5	9/21/24 12:17	W32/Generic.AC.171!tr	C:\Users\ADMIN\Downloads\Firefox	El archivo fue puesto en cuarentena.
SUBGENERALD5	9/21/24 12:17	W32/Generic.AC.171!tr	C:\Users\ADMIN\Downloads\Firefox	El archivo fue puesto en cuarentena.
SUBGENERALD5	9/21/24 12:16	W32/Generic.AC.171!tr	C:\Users\ADMIN\Downloads\ChromeSetup.exe	El archivo fue puesto en cuarentena.
SUBGENERALD5	9/21/24 12:16	W32/Generic.AC.171!tr	C:\Users\ADMIN\Downloads\ChromeSetup(1).exe	El archivo fue puesto en cuarentena.
SUBGENERALD5	9/21/24 12:16	W32/Generic.AC.171!tr	C:\Users\ADMIN\Downloads\ChromeSetup(2).exe	El archivo fue puesto en cuarentena.
SUBGENERALD5	9/21/24 12:00	W32/Generic.AC.171!tr	C:\Users\ADMIN\Gupcs.exe	El archivo fue puesto en cuarentena.
SUBGENERALD5	9/21/24 11:59	W32/Generic.AC.171!tr	C:\Users\ADMIN\AppData\Roaming\Dpoksj.exe	El archivo fue puesto en cuarentena.
SUBGENERALD5	9/21/24 11:58	W32/Remcos.A!tr	C:\ProgramData\Remcos\remcos.exe	El archivo fue puesto en cuarentena.
SUBGENERALD5	9/21/24 11:57	W32/Generic.AC.171!tr	C:\Users\ADMIN\AppData\Local\Microsoft\OneDrive\24.166.0818.0003\FileCoAuth.exe	El archivo fue puesto en cuarentena.
SUBGENERALD5	9/20/24 12:15	W32/Generic.AC.171!tr	C:\Program Files (x86)\Microsoft Office\Office10\MSOHTMED.EXE	El archivo fue puesto en cuarentena.
SUBGENERALD5	9/20/24 12:10	W32/Generic.AC.171!tr	C:\Program Files (x86)\Microsoft Office\Office10\MSACCESS.EXE	El archivo fue puesto en cuarentena.

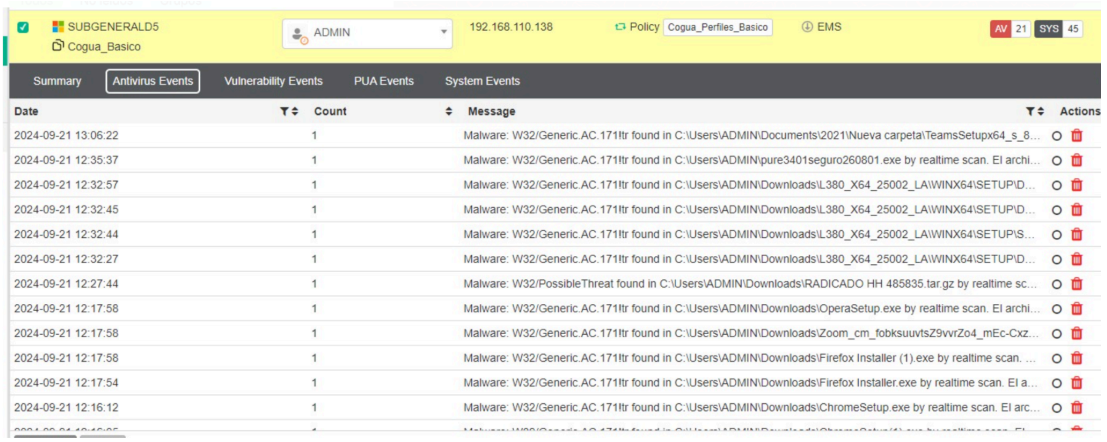


Se configuraron alertas que llegan a los administradores via Mail,









Conclusiones Generales

1. Se realizó la instalación de la licencia en 100 máquinas de la Alcaldía de Cogua.
2. Se dejaron libres 41 licencias para equipos nuevos o necesidades que requiera la Alcaldía.
3. Se trabajó en la configuración de perfiles de malware, capacitación al personal técnico y definiciones de políticas en conjunto para cada estación reportada y con el agente.
4. Se tuvo el acompañamiento por parte del Equipo.
5. se asignó clave al agente para evitar desinstalación por parte del usuario la clave asignada fue Cogua2024*
6. Se consolidaron reportes para los administradores con el fin de dar visibilidad sobre nuevos eventos de malware que se puedan generar.