



MARCO Federal Managed Computer Services



Cybersecurity Maturity Model Certification Initiative



ONOPA Project Management
Information System
Administration Handbook

Document No
ONOPA IT-100

Effective Date
7/19/2021

Review Date
7/20/2021

Version
4

Page No.
Live Doc]

[MOJVII 301-00 Access Control Policy](#)
[MOJVII 302-00 Security Awareness Training Policy](#)
[MOJVII 303-00 Audit Accountability Policy](#)

[MOJVII 305-00 Configuration Management Policy](#)
[MOJVII 306-00 Contingency Planning Policy](#)
[MOJVII 307-00 Identification and Authentication Policy](#)
[MOJVII 308-00 Incident Response Policy](#)
[MOJVII 309-00 IT Maintenance Policy](#)
[MOJVII 310-00 Media Protection Policy](#)

[MOJVII 313-00 Physical and Environmental Protection](#)
[MOJVII 314-00 Risk Assessment Policy](#)

[MOJVII 316-00 Systems and Communications Protection Policy](#)

[ONOPA 301 Access Control Policy](#)
[ONOPA 302 Security Awareness Training Policy](#)
[ONOPA 303 Audit Accountability Policy](#)

[ONOPA 305 Configuration Management Policy](#)
[ONOPA 306 Contingency Planning Policy](#)
[ONOPA 307 Identification and Authentication Policy](#)
[ONOPA 308 Incident Response Policy](#)
[ONOPA 309 IT Maintenance Policy](#)
[ONOPA 310-00 Media Protection](#)

[ONOPA 313-00 Physical & Environmental Protection](#)

Operations

Element		
Essential Practices Statement	OPMIS	CMMC
1. General Operations		
Hardware and Software Inventories		
<p>Maintain current hardware and software inventories.</p> <p><u>Reason:</u> Hardware inventories should be maintained to identify assets. Inventories should be used to facilitate:</p> <ul style="list-style-type: none"> • resource sharing, • software distribution and maintenance, • asset control, • hardware security, and • repair or replacement of hardware. <p>Software inventories should be maintained to identify assets. Inventories should be used to identify:</p> <ul style="list-style-type: none"> • software for replacement or upgrades, • authorized users, • license compliance, and • unauthorized software. 		
Software Licensing		
<p>Maintain current software licensing and enforce compliance with licensing agreements.</p> <p><u>Reason:</u> Software licensing and compliance with licensing requirements minimizes the legal and financial risks associated with using unlicensed software. As noted above under inventories, an inventory of all software is a key component to controlling this issue, as are detection and protection techniques.</p>		

Equipment Removal/Data Destruction		
<p>Establish formal procedures and controls for the secure removal and disposal of information assets. Essential controls include:</p> <ul style="list-style-type: none"> • Requiring authorization for removal of equipment, information, or software. • Ensuring all data and software are removed or destroyed prior to equipment disposal. • Ensuring information and equipment to be removed or destroyed is stored in a secure area. 		

Operations		
Element		
Essential Practices Statement	OPMIS	CMMC
<p><i>Information can be compromised through careless disposal or re-use of equipment. Therefore, storage devices containing sensitive information, as defined by the institution's data classification system, should be physically destroyed or securely overwritten. These actions help protect the institution from liability by providing security for confidential information, as well as compliance with licensing agreements.</i></p>		
2. Network Operations		
Intrusion Detection		
<p>Establish processes to detect, correct, and report unauthorized system access. Essential elements of the process include:</p> <ul style="list-style-type: none"> • Detecting external and internal intrusions, • Logging incidents, • Real-time monitoring, • Reporting to management and FCA, • Conducting an impact analysis, • Establishing an intrusion response process and team, and • Updating and maintaining the system. 		

<p><u>Reason:</u></p> <p><i>Using an Intrusion Detection System (IDS) enhances an institution's ability to determine if its preventive and protective measures are performing as expected. An IDS also provides some protection against legal liability as it can show an institution took "reasonably" expected steps to prevent damage, loss, or theft of privileged information.</i></p>		
Web Site Monitoring		
<p>Review the web site to detect unauthorized changes and implement corrective action if necessary.</p> <p><u>Reason:</u></p> <p><i>Ensure the web site is available and its integrity is maintained and reputation risk is minimized.</i></p>		
Internet Use Monitoring		
<p>Establish, monitor, and enforce Internet Usage policies and procedures.</p> <p><u>Reason:</u></p> <p><i>Ongoing monitoring of internet usage allows management to:</i></p> <ul style="list-style-type: none"> <i>Protect corporate resources (e.g., employee time, network resources);</i> 		

Operations		
Element		
Essential Practices Statement	OPMIS	CMMC
<ul style="list-style-type: none"> <i>Prevent inappropriate use (e.g., gambling, pornography, stock trading, downloading files, etc.);</i> <i>Limit legal liability; and</i> <i>Minimize reputation risk.</i> 		

Internet Data Transmissions		
<p>Identify and classify all internet transmissions. Secure data transmissions of confidential and sensitive information as defined in the institution's data classification system.</p> <p><u>Reason:</u> <i>Unless encrypted, information sent via the internet is exposed to disclosure, theft or modification and creates potential legal exposure and reputation damage. To address these concerns FCA issued Regulation 609.950(c) – Electronic Communications in May 2002. This regulation requires institutions to ensure electronic communications represent “good business practices.”</i></p>		
Network Traffic Monitoring		
<p>Monitor network faults, performance, configuration, security, and accounting management.</p> <p><u>Reason:</u> <i>The network system is an integral part of communications infrastructure. Problems affect many or all users quickly and visibly. Projections of future capacity requirements should be made to ensure that adequate processing power and storage are available. A network administrator should monitor network efficiency statistics, ensure that files are backed up regularly and stored off-site, establish and maintain adequate virus protection, review network activity reports, and react to network alerts and alarms.</i></p>		
Monitoring Network and Firewall Exploits		
<p>Regularly review the technical alerts/advisories and recommended solutions provided to monitor new threats and implement timely corrective measures to firewalls, network operating systems, and applications.</p> <p><u>Reason:</u> <i>To protect the confidentiality, integrity, and availability of data and systems, network administrators must constantly monitor new exploits and ensure that measures to protect against them are applied to systems. Computer hackers and intruders continue to exploit newly discovered holes in firewalls and network systems and devise new attacks.</i></p>		

Operations

Element		
Essential Practices Statement	OPMIS Reference	CMMC
Patch Management		
<ul style="list-style-type: none"> Implement a patch management program that includes: Monitoring vulnerabilities and patches for all software identified in the systems inventory Evaluating the impact of the patches on the institution's information technology systems and environment, Testing the patches to validate expected functionality, and Installing the patches throughout the network. <p><u>Reason:</u></p> <p><i>Inadequate patching of software vulnerabilities exposes an institution to significant risk. Although software vendors often develop an update or "patch" to correct identified weaknesses, it is the software user's responsibility to update systems or install patches in a timely manner. Flaws in software code that could cause a program to malfunction generally result from programming errors that occur during software development. The increasing complexity and size of software programs contribute to the growth in software flaws. By exploiting software vulnerabilities, hackers and others who spread malicious code can</i></p>		
Network Architecture		
<p>Maintain current diagram of network architecture.</p> <p><u>Reason:</u></p> <p><i>The network diagram depicts the current network layout and design. It is a tool that the network administrator uses to identify inter-relationships, enforce security, detect problems, minimize risk, and help restore operations.</i></p>		

Operations

Element

Essential Practices Statement

OPMIS Reference

CMMC

1. General Operations

Hardware and Software Inventories

Maintain current hardware and software inventories.

Reason:

Hardware inventories should be maintained to identify assets. Inventories should be used to facilitate:

- resource sharing,
- software distribution and maintenance,
- asset control,
- hardware security, and
- repair or replacement of hardware.

Software inventories should be maintained to identify assets. Inventories should be used to identify:

- software for replacement or upgrades,
- authorized users,
- license compliance, and
- unauthorized software.

Software Licensing

Maintain current software licensing and enforce compliance with licensing agreements.

Reason:

Software licensing and compliance with licensing requirements minimizes the legal and financial risks associated with using unlicensed software. As noted above under inventories, an inventory of all software is a key component to controlling this issue, as are detection and protection techniques.

Equipment Removal/Data Destruction

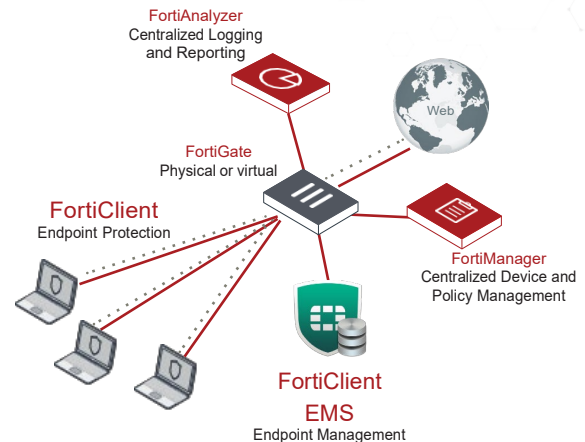
Establish formal procedures and controls for the secure removal and disposal of information assets. Essential controls include:

- Requiring authorization for removal of equipment, information, or software.
- Ensuring all data and software are removed or destroyed prior to equipment disposal.
- Ensuring information and equipment to be removed or destroyed is stored in a secure area.

FortiClient

Lock down visibility and control of your software and hardware inventory across the entire security fabric. Identify vulnerable or compromised hosts and track all details of systems and user profiles across your attack surface.

FortiClient's Security Fabric Integration, ensures that all fabric components – FortiGate, FortiAnalyzer, EMS, Managed AP, Managed Switches, Sandbox – have a unified view of endpoints in order to provide tracking & awareness, compliance enforcement and reporting. **Advanced Threat Protection** automates prevention of known and unknown threats through built-in host-based security stack and integration with FortiSandbox. Easy to use **Secure Remote Access & Mobility** via SSL and IPsec VPN. FortiClient connects every endpoint to form a cohesive security fabric.



6 Devices

Total

2 Devices

Out of Sync

3 Devices

Not Compliant

4 Devices

Security Risk

Scan

Exclude

Move to

Delete

Device

User

IP

Endpoint Connection

Endpoint Profile

acac03cb.lpt.aol

Group: PM

Wendy

172.172.3.203

FortiTelemetry to FGT (FGT3445456765)

Managed by EMS

Installer

Config

Gateway IP List

JeffC-Laptop

Group: Web

Jeff

172.28.1.108

FortiTelemetry to FGT (FGT1345653678)

Managed by EMS

Installer

Config

Gateway IP List

Andrew's PC

Group: Docs

Andrew

172.18.72.40

FortiTelemetry to FGT (FGT3762288377)

Managed by EMS

Installer

Config

Gateway IP List

Endpoint Details

Endpoint Summary

Anti-Virus Events

Vulnerability Events

Web Filter Events

System Events

Device

Andrew

172.18.72.40

Device: Andrew's PC

Mac Address: 00:21:15:B1:S2

OS: Windows 10

Last Seen: 09-19-2016 19:23:11

Location: On Net

Endpoint Connection

FortiTelemetry to FGT3762288377

Managed by EMS

Compliance

Compliance Status

Quarantine Reason:

Infected with Botnet

Details

Removable Media Access

Exempted

EMS for Central Management

- Simple & User Friendly UI
- Remote FortiClient Deployment
- Realtime Dashboard
- Software Inventory Management
- Active Directory Integration
- Central Quarantine Management
- Automatic Group Assignment
- Automatic Email Alerts
- Supports Custom Groups
- Remote Triggers

FortiClient Benefits:

Unified endpoint features including compliance, protection, and secure access into a single, modular lightweight client.

End-to-end threat visibility and control by natively integrating endpoint into the Security Fabric architecture.

Advanced threat protection against exploits and advanced malware, powered by FortiGuard along with FortiSandbox integration.

Integrated patch management and vulnerability shielding to harden all endpoints.

Simplified management and policy enforcement with Enterprise Management Server (EMS) and FortiGate, respectively.

Advanced Threat Protection

As a next-generation endpoint protection solution, FortiClient helps connect endpoints to FortiSandbox, which uses **behavior-based analysis** to automatically analyze in real-time all files downloaded to FortiClient endpoints. Millions of FortiClient and FortiSandbox users worldwide share information about known and unknown, malware with cloud-based **FortiGuard**. FortiGuard automatically shares the intelligence with other FortiSandbox units and FortiClient endpoints to **prevent attacks** from known and unknown malware.

Security Fabric Integration

As a key piece of the **Fortinet Security Fabric**, FortiClient integrates the endpoints into the Fabric for early detection and prevention of advanced threats and delivers endpoint visibility, compliance control, vulnerability management and automation. With 6.0, FortiOS & FortiAnalyzer leverages **FortiClient endpoint telemetry** intelligence to identify Indicator of Compromise (IoC). With the **Automation** capability, admins can investigate real-time and set policies to automate responses including quarantining suspicious or compromised endpoints to contain incidents and stem outbreaks. Fortinet's endpoint compliance & vulnerability management features **simplifies the enforcement** of enterprise security policies preventing endpoints from becoming easy attack targets.

Secure Remote Access & Mobility

FortiClient uses SSL and IPSec VPN to provide **secure, reliable access** to corporate networks and applications from virtually any internet connected remote location. FortiClient simplifies remote user experience with built-in **auto-connect and always-up** VPN features. Two-Factor authentication can also be used to provide additional layer of security. Feature like, VPN auto-connect, Always up, Dynamic VPN Gateway Selection and split-tunneling ensures smooth user experience on all device types connecting from home or public places.

Anti-Exploit

This behavioral-based detection technology **protects against zero-day attacks** that target applications with zero-day or unpatched vulnerabilities.



Protects against zero-day attacks targeting undiscovered or unpatched application vulnerabilities

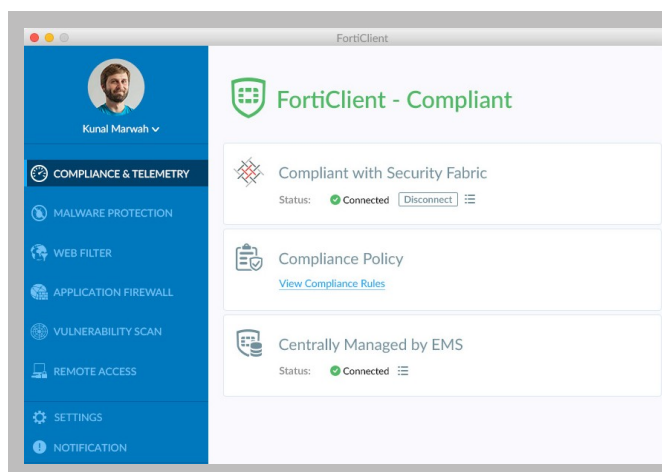
Detects various memory techniques used in an exploit, such as ROP, HeapSpray, bufferoverflow

File-less Attacks powershell & other scripted attacks

Shields web browsers, Java/Flash plug-ins, Microsoft Office applications, and PDF Reader

Identifies and Blocks exploit kits, prevents drive-by downloads

Signature-less solution



Feature Highlights

EMS provides ability to centrally manage Windows, Mac, Linux, Chrome, iOS and Android endpoints



FortiGate provides awareness and control over all your endpoints



Remote FortiClient Deployment

that allows administrators to remotely deploy endpoint software and perform controlled upgrades.

Centralized Client Provisioning makes deploying FortiClient configuration to thousands of clients an effortless task with a click of a button.

Software Inventory Management provides visibility into installed software applications and licence management to improve security hygiene. You can use inventory information to detect and remove unnecessary or outdated applications that might have vulnerabilities to reduce your attack surface.

Windows AD Integration helps sync organisations AD structure into EMS so same OUs can be used for endpoint management.

Realtime Endpoint Status always provides current information on endpoint activity & security events.

Vulnerability Dashboard helps manage organizations attack surface. All vulnerable endpoints are easily identified for administrative action.

Telemetry provides real-time endpoint visibility (including user avatar) on FortiGate console so administrators can get a comprehensive view of the whole network. Telemetry also ensures that all fabric components have a unified view of the endpoints.

Compliance Enforcement can be used to enforce organisations security policies. Only authorized and compliant endpoints with no security risks are granted access.

Endpoint Quarantine

helps to quickly disconnect a compromised endpoint from the network and stop it from infecting other assets.

Automated Response

helps detect and isolate suspicious or compromised endpoints without manual intervention

FortiClient EMS and FortiGate Endpoint Licenses

	FORTICLIENT EMS LICENSE	FORTIGATE ENDPOINT TELEMETRY & COMPLIANCE LICENSE
PROVISIONING		
Centralized Client Provisioning	✓	
Client Software Updates	✓	
Windows AD Integration	✓	
FortiTelemetry Gateway IP List	✓	
Software Inventory	✓	
Automatic Group Assignment	✓	
COMPLIANCE ENFORCEMENT AND SECURITY FABRIC INTEGRATION		
Fortinet Security Fabric Integration		✓
Security Posture Check		✓
Vulnerability Compliance Check		✓
Minimum System Compliance		✓
Authorized Device Detection		✓
Automated Endpoint Quarantine	✓	✓
REMOTE CONTROL		
On-demand Antivirus Scan	✓	
On-demand Vulnerability Scan	✓	
Host Quarantine	✓	✓
TELEMETRY AND MONITORING		
Client Information (client version, OS IP/MAC address, profile assigned, user avatar)	✓	✓
Client Status	✓	✓
Reporting	✓ (To FortiAnalyzer)	✓ (To FortiAnalyzer)



AC

Information Security Policies are the foundation for information technology security at MARCO-ONOPA JVII. The policies set out the information security standards required by NIST 800-171, w...

[Go to this Sway](#)



AT

Information Security Policies are the foundation for information technology security at MARCOONOPA JVII (MOJVII). The policies set out the information security standards required by NIST 80...

[Go to this Sway](#)



AU

[Go to this Sway](#)



SA

Information Security Policies are the foundation for information technology security at MARCO-ONOPA JVII (MOJVII). The policies set out the information security standards required by NIST 8...

[Go to this Sway](#)



CM

[Go to this Sway](#)



CP

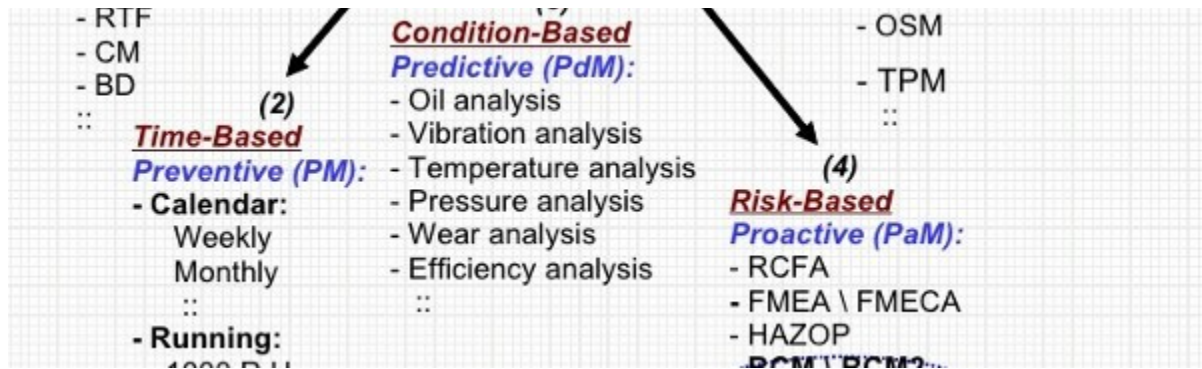
[Go to this Sway](#)



IA

Information Security Policies are the foundation for information technology security at MARCO-ONOPA JVII (MOJVII). The policies set out the information security standards required by NIST 8...

[Go to this Sway](#)



MA

Information Security Policies are the foundation for information technology security at MARCO-ONOPA JVII (MOJVII). The policies set out the information security standards required by NIST 8...

[Go to this Sway](#)



MP

Information Security Policies are the foundation for information technology security at MARCO-ONOPA JVII (MOJVII). The policies set out the information security standards required by NIST 8...

[Go to this Sway](#)



PE

Information Security Policies are the foundation for information technology security at MARCO-ONOPA JVII (MOJVII). The policies set out the information security standards required by NIST 8...

[Go to this Sway](#)



RA

Information Security Policies are the foundation for information technology security at MARCO-ONOPA JVII (MOJVII). The policies set out the information security standards required by NIST 8...

[Go to this Sway](#)



SC

Information Security Policies are the foundation for information technology security at MARCO-ONOPA JVII (MOJVII). The policies set out the information security standards required by NIST 8...

[Go to this Sway](#)



PL

Information Security Policies are the foundation for information technology security at MARCO-ONOPA JVII (MOJVII). The policies set out the information security standards required by NIST 8...

[Go to this Sway](#)

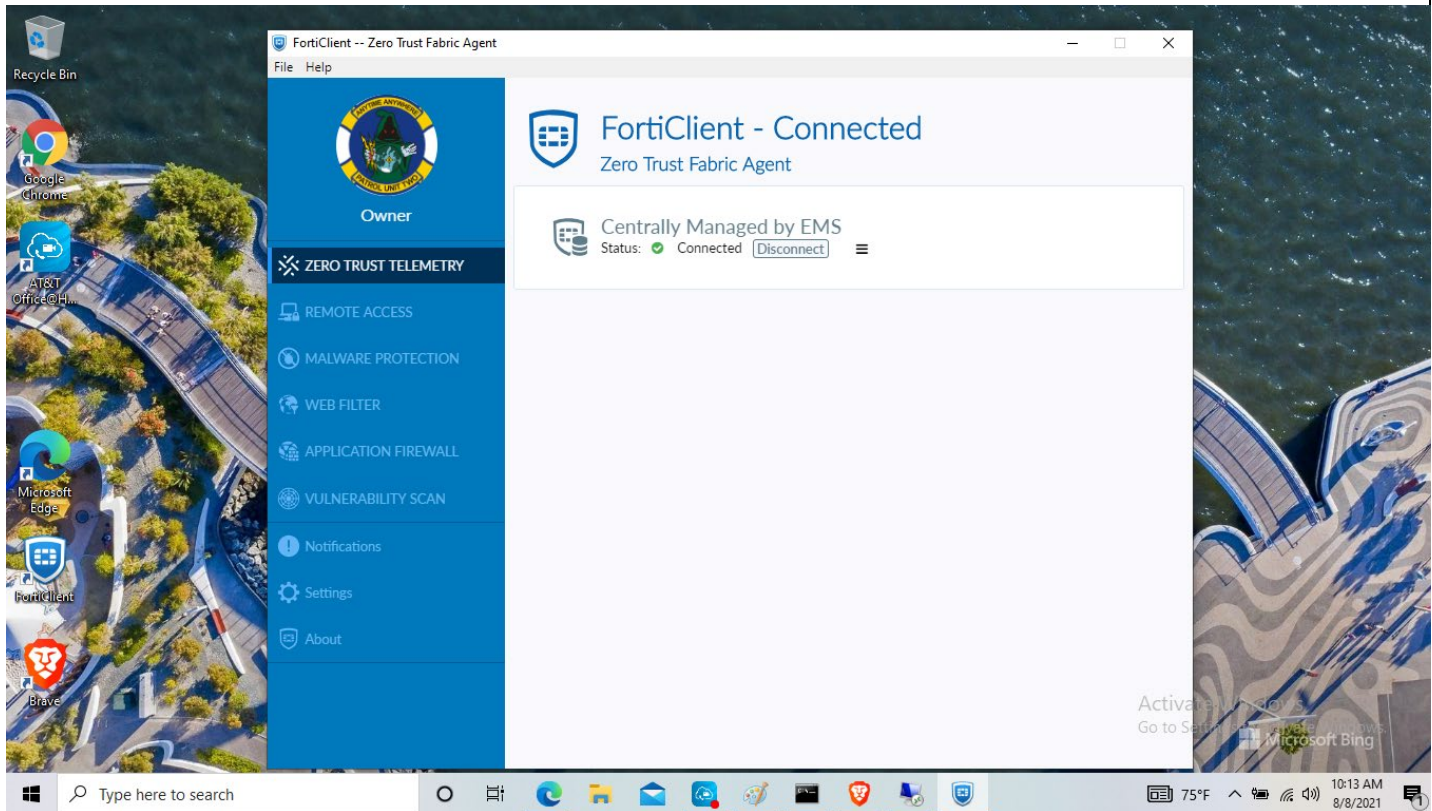


SI

Information Security Policies are the foundation for information technology security at MARCOONOPA JVII (MOJVII). The policies set out the information security standards required by NIST 80...

[Go to this Sway](#)

OPMIS Network Administrator Handbook



Conflicts with third party AV products

The AV feature in FortiClient is known to conflict with other similar products in the market.

- You should not use FortiClient's AV feature with other AV products.
- If not using FortiClient's AV feature, you should exclude the FortiClient installation folder from scanning for the third-party AV product.

During a new installation of FortiClient, the installer searches for other registered third-party software and, if any is found, warns users to uninstall them before proceeding with the installation. There is also an option to disable FortiClient Real Time Protection (RTP).

Perimeter-based security zero-trust model

Every time a device or user is automatically trusted, it places an organization's data, applications, and intellectual property at risk. Organizations should implement a zero-trust strategy that focuses on three key elements:

1. Know every device on the network.
2. Know every user that accesses the network.

Know how to protect assets on and off the network



Conflicting Antivirus Software



The following antivirus software has been detected on your computer. To maintain system stability, the conflicting antivirus should be uninstalled before installing FortiClient. Alternatively you can disable the FortiClient real-time protection feature. However, this is not recommended.

Avira Desktop

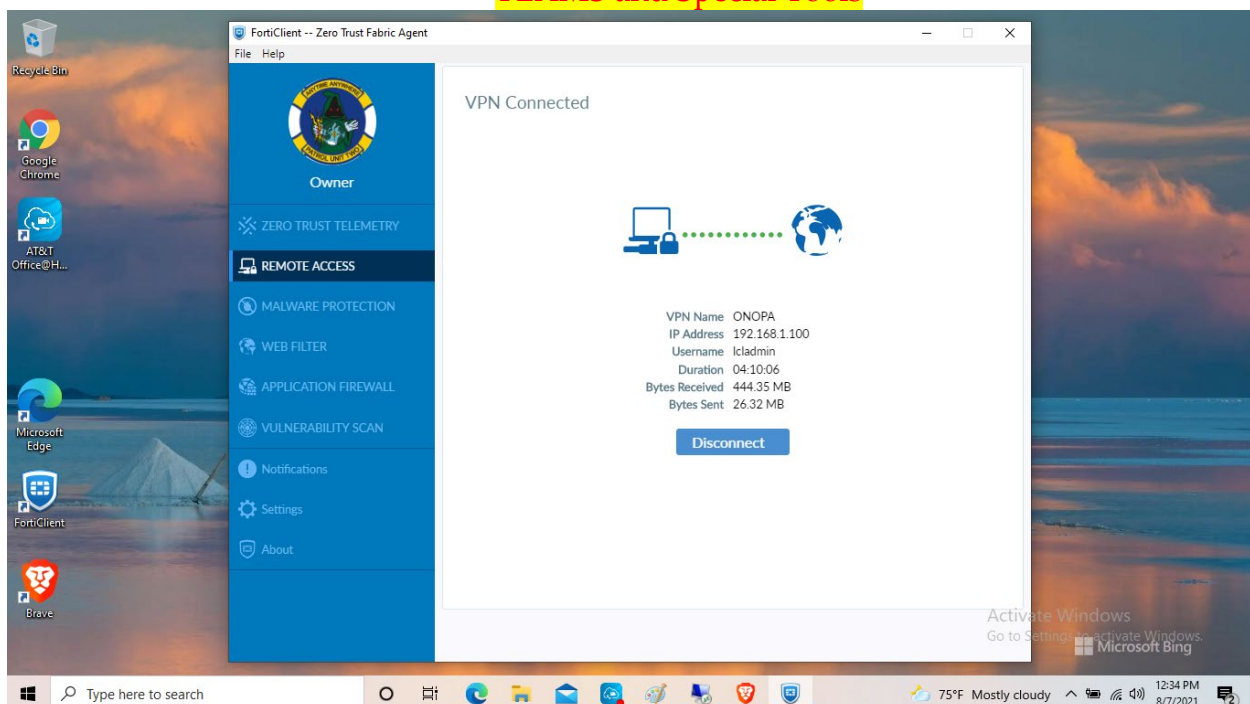
- ☐ Exit the current installation. I will uninstall all other antivirus product(s) before installing FortiClient.
- ☒ Disable FortiClient real-time protection.

Back

Next

Cancel

Only authorized ONOPA VPN users can access backend resources, Remote Desktop Services, TEAMS and Special Tools



Fortinet Security Fabric

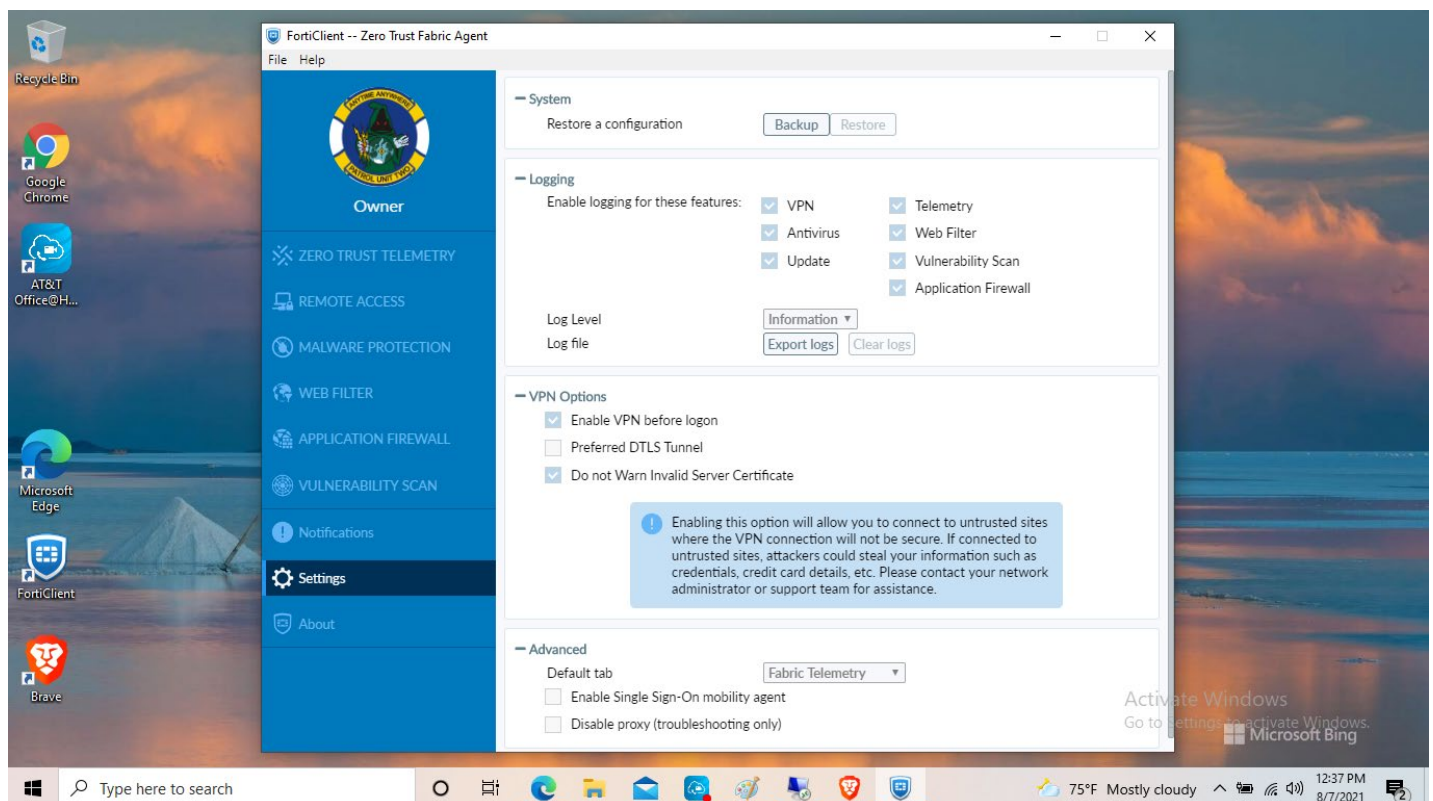
The [Fortinet Security Fabric](#) continuously assesses the risks automatically adjusts to provide comprehensive real-time across the digital attack surface and cycle.

Powered by FortiOS, the Fabric is the industry's highest-integrated cybersecurity platform with a rich ecosystem. enables consistent security across the extended digital surface. Seamless interoperability, complete visibility, and control are now possible for hybrid deployments including software, and X-as-a-Service across networks, endpoints,



and protection

performing
The Fabric attack
granular
hardware,
and clouds.



The Fabric is Built on Three Key Attributes



Broad

Reduce risk and manage the entire digital attack surface

Fortinet Security portfolio enables coordinated threat detection and policy enforcement across the entire digital attack surface and lifecycle with converged networking and security across edges, clouds, endpoints, and users.

Integrated

Close the security gaps and reduce complexity

Integrated and unified security, operations, and performance across different technologies, locations, deployments enables complete visibility. It also security of all form factors including hardware appliances, virtual machines, cloud-delivered, and X-as-a-Service. Fabric-ready Partner products are included in the Fabric ecosystem.



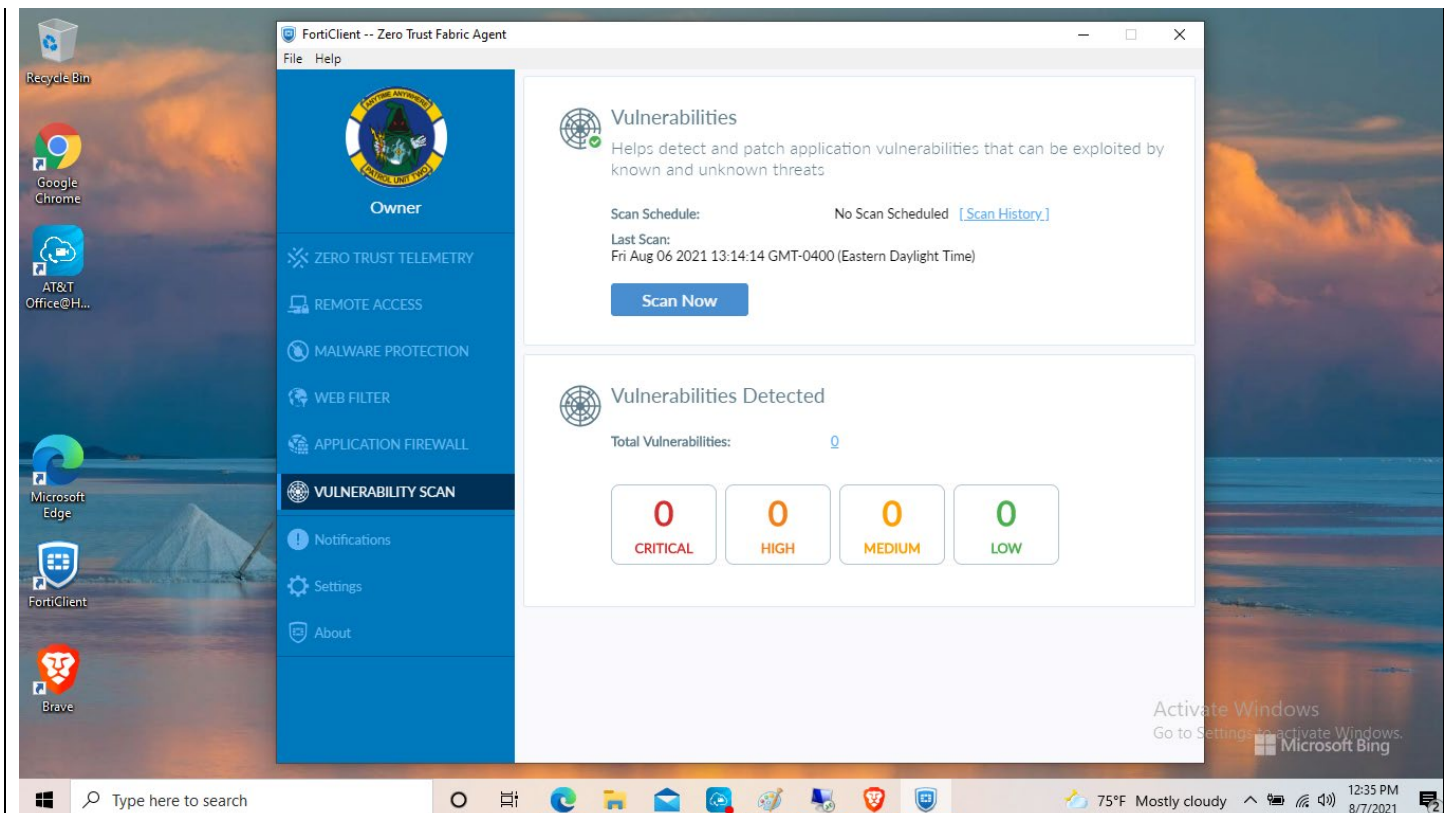
and
tightens



Automated

Faster time to prevention and efficient operations

A context aware, self-healing network and security posture leverages cloud-scale and advanced AI to automatically deliver near-real-time, user-to-application coordinated protection across the Fabric.





The Key Pillars of the Fortinet Security Fabric

One operating system drives the Fortinet Security Fabric, which supports more deployment models than any other solution. These include physical, virtual, cloud, and X-as-a-Service environments. And it encompasses the industry's broadest ecosystem and product portfolio, spanning endpoints, networks, and clouds.

Security-Driven Networking

Security-Driven Networking enables digital innovation with the convergence of networking and security into a single, integrated system that can expand to any edge.

Fortinet was named a Leader in both the [November 2020 Gartner Magic Quadrant for Network Firewalls](#) and the [September 2020 Gartner Magic Quadrant for WAN Edge Infrastructure](#). Our FortiGate next-generation firewall is the single product that achieved Leader status in both reports.

[Learn More](#)



Zero Trust Access

Fortinet Zero Trust Access (ZTA) supports taking a zero-trust approach, verifying who and what is on your network. With the new updates in FortiOS 7.0 every [FortiGate](#) customer using the FortiClient Agent can now employ zero trust network access (ZTNA) capabilities right out of the box. Management is simplified by using the same adaptive, application access policy whether users are on or off the network.

[Learn More](#)

Adaptive Cloud

Consistent, cloud native security with auto-scaling is provided across multi-cloud environments. Adaptive Cloud Security allows for usage of resources with auto-scaling, dynamic load-balancing, and user experience visibility. In addition, our context-aware policy is these environments providing coordinated threat response via with FortiGuard AI-powered security services.



and within effective application extended into integration

[Learn More](#)

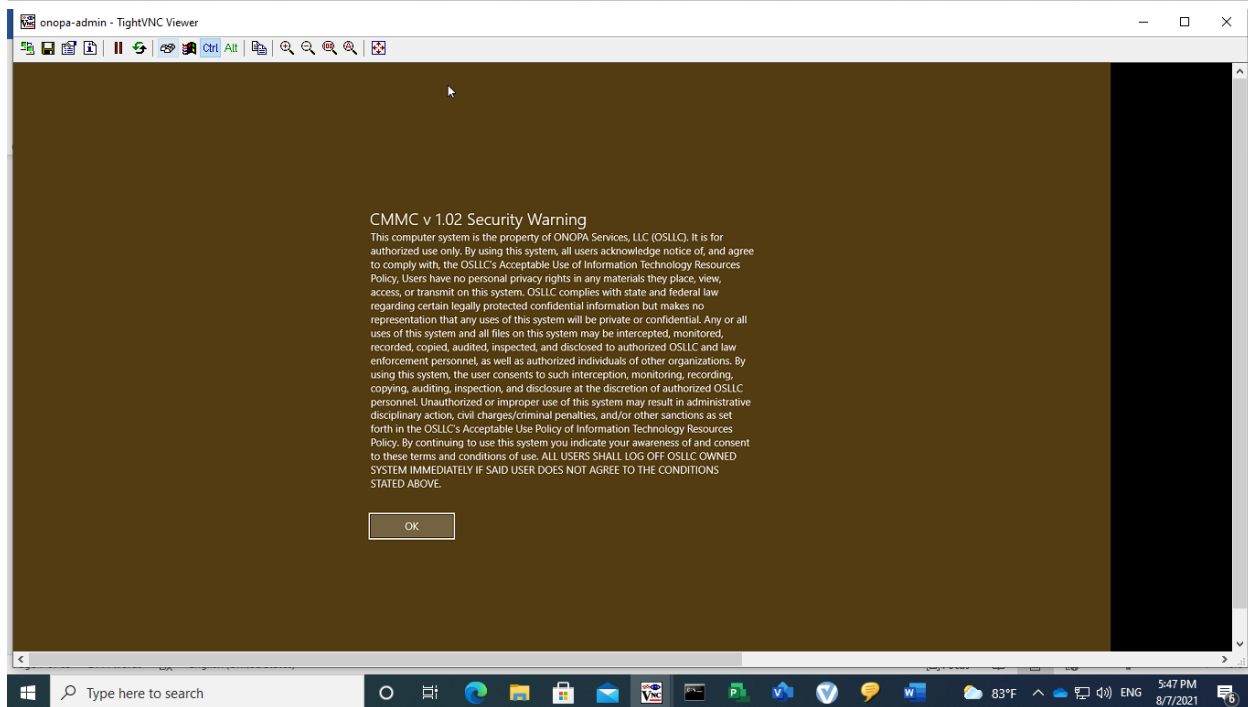
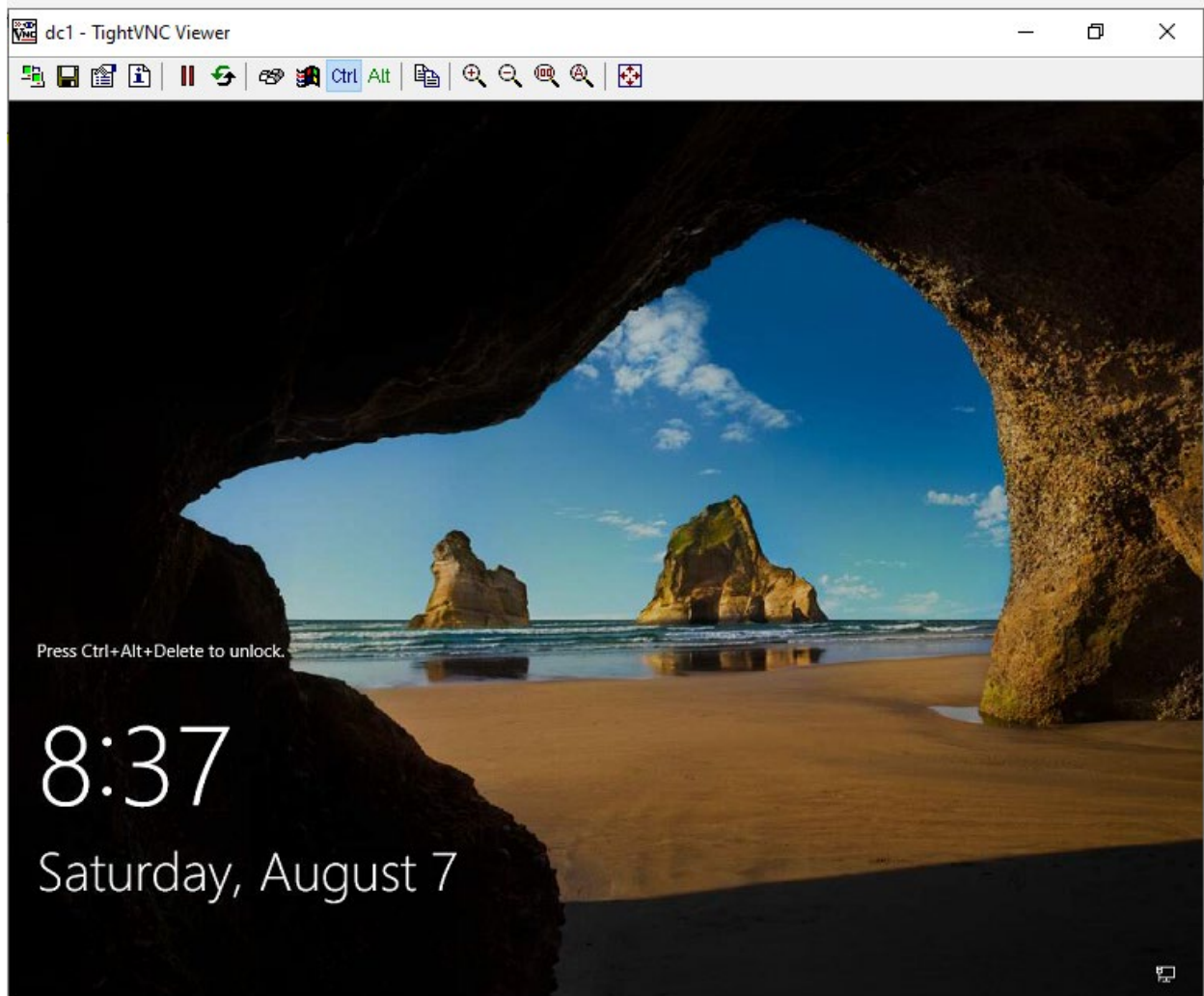
Fabric-level Functions

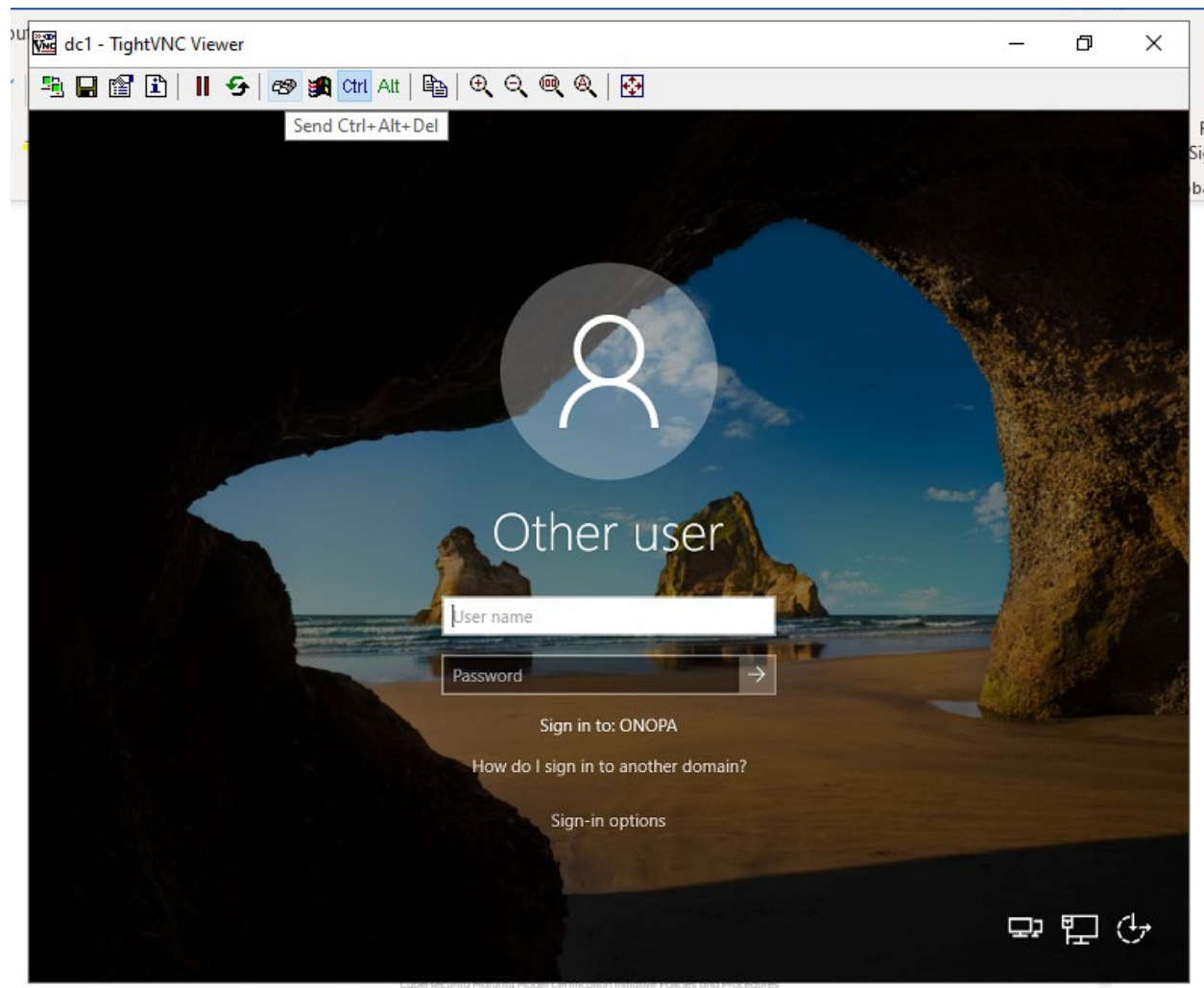
Fortinet Fabric Management Center

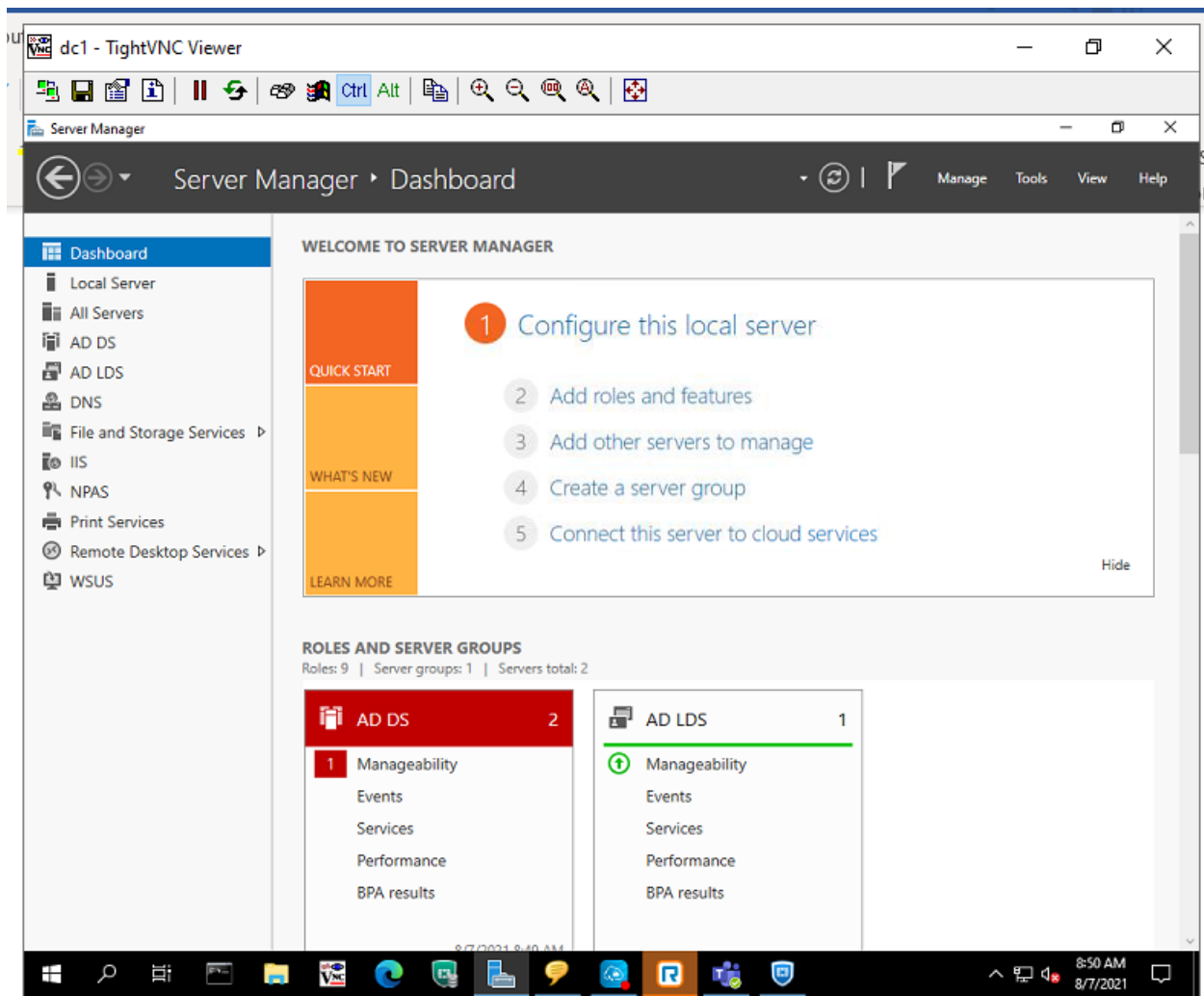


The Fabric Management Center enables centralized management, network automation and orchestration, and Security Fabric Analytics. A unified console across networks, endpoints, and clouds improves efficiency, reduces risk, and lowers total cost of ownership.

[Learn More - NOC](#)







dc1 - TightVNC Viewer

Server Manager

Server Manager ▸ Dashboard

Dashboard

- Local Server
- All Servers
- AD DS
- AD LDS
- DNS
- File and Storage Services
- IIS
- NPAS
- Print Services
- Remote Desktop Services
- WSUS

WELCOME TO SERVER MANAGER

AD DS - Manageability Detail View

1 Manageability Hide Alert Criteria

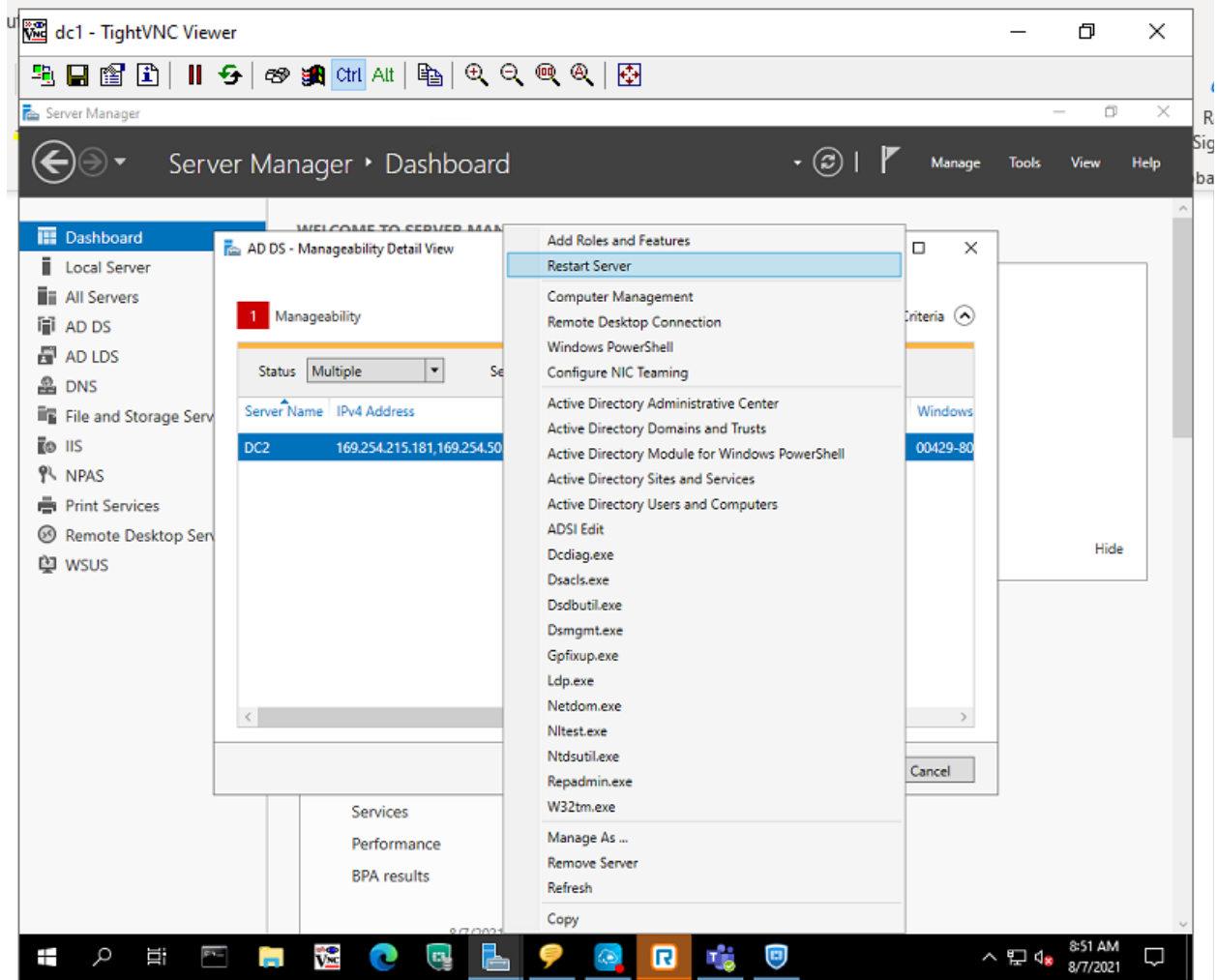
Status: Multiple Servers: All

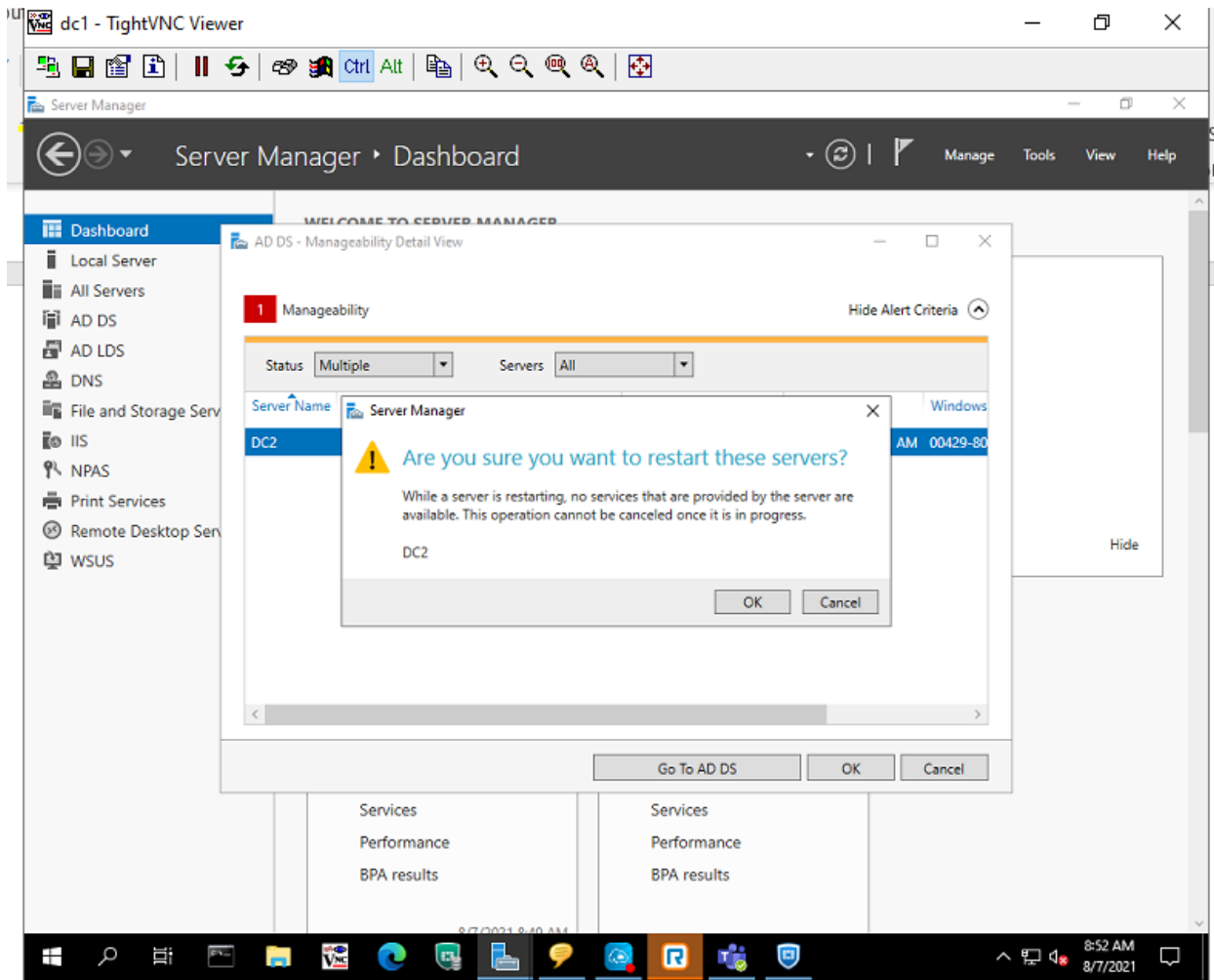
Server Name	IPv4 Address	Manageability	Last Update	Windows
DC2	169.254.215.181,169.254.50.219,192.168.1.12	Online - Restart pending	8/7/2021 8:49:01 AM	00429-80

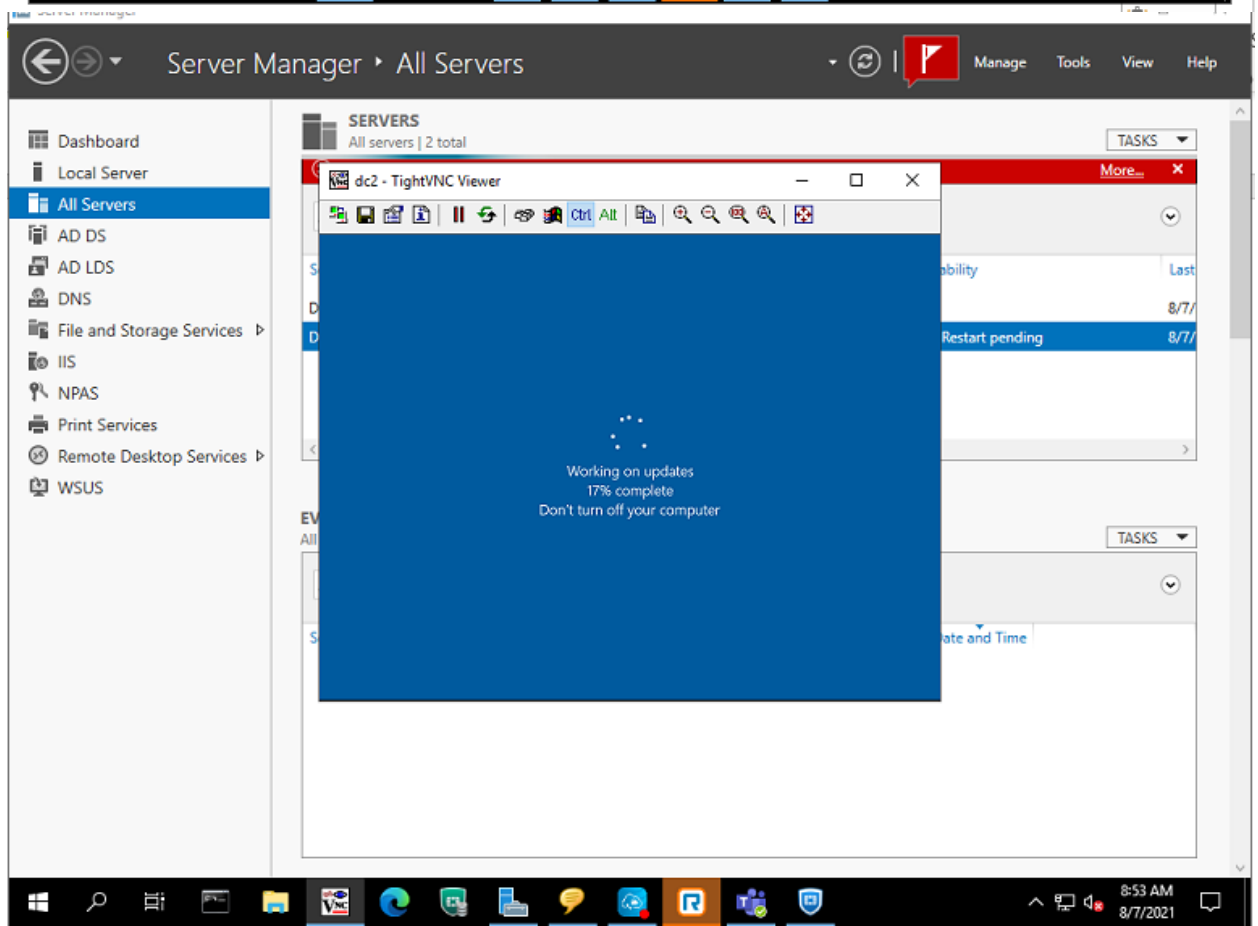
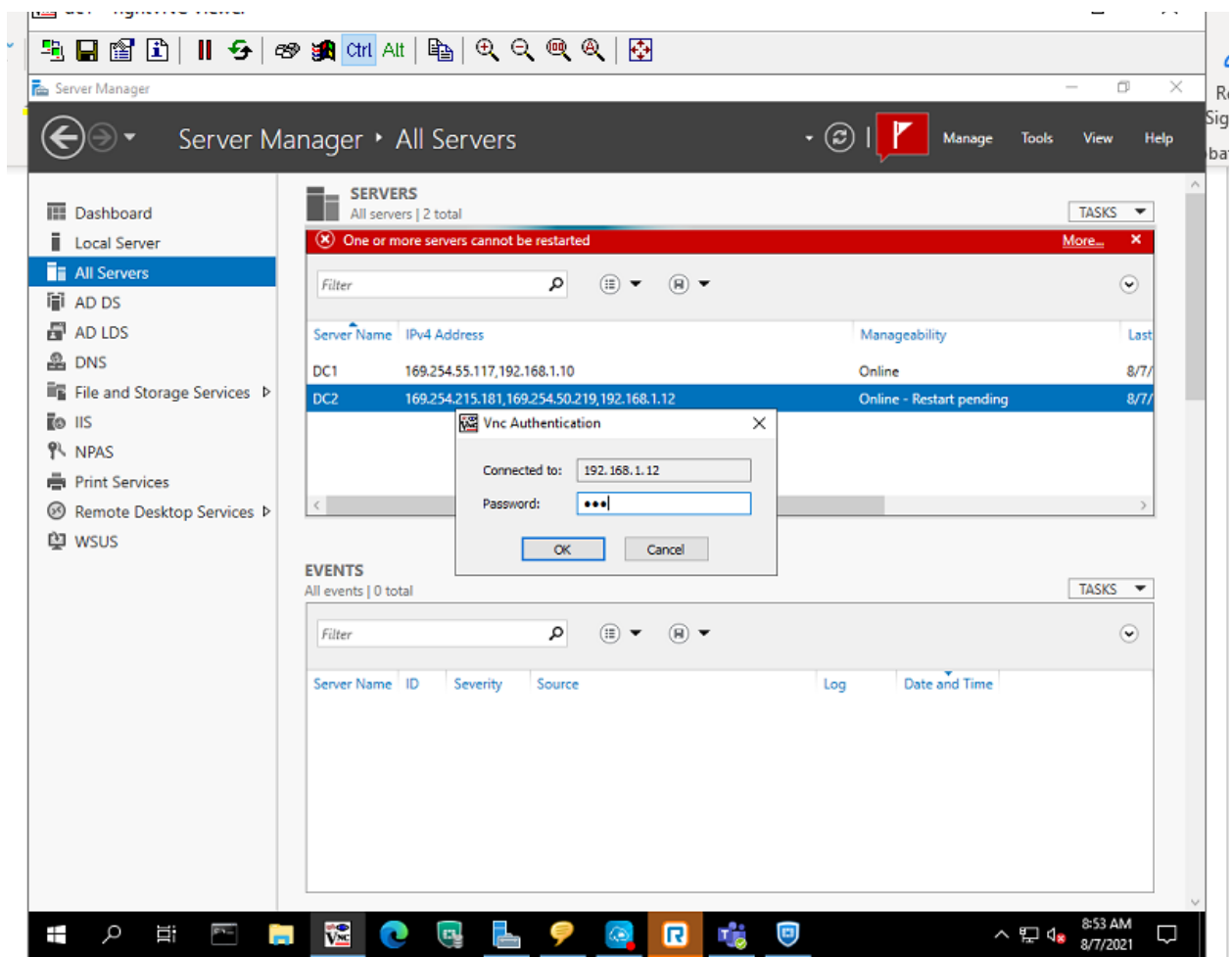
Go To AD DS OK Cancel

Services Performance BPA results

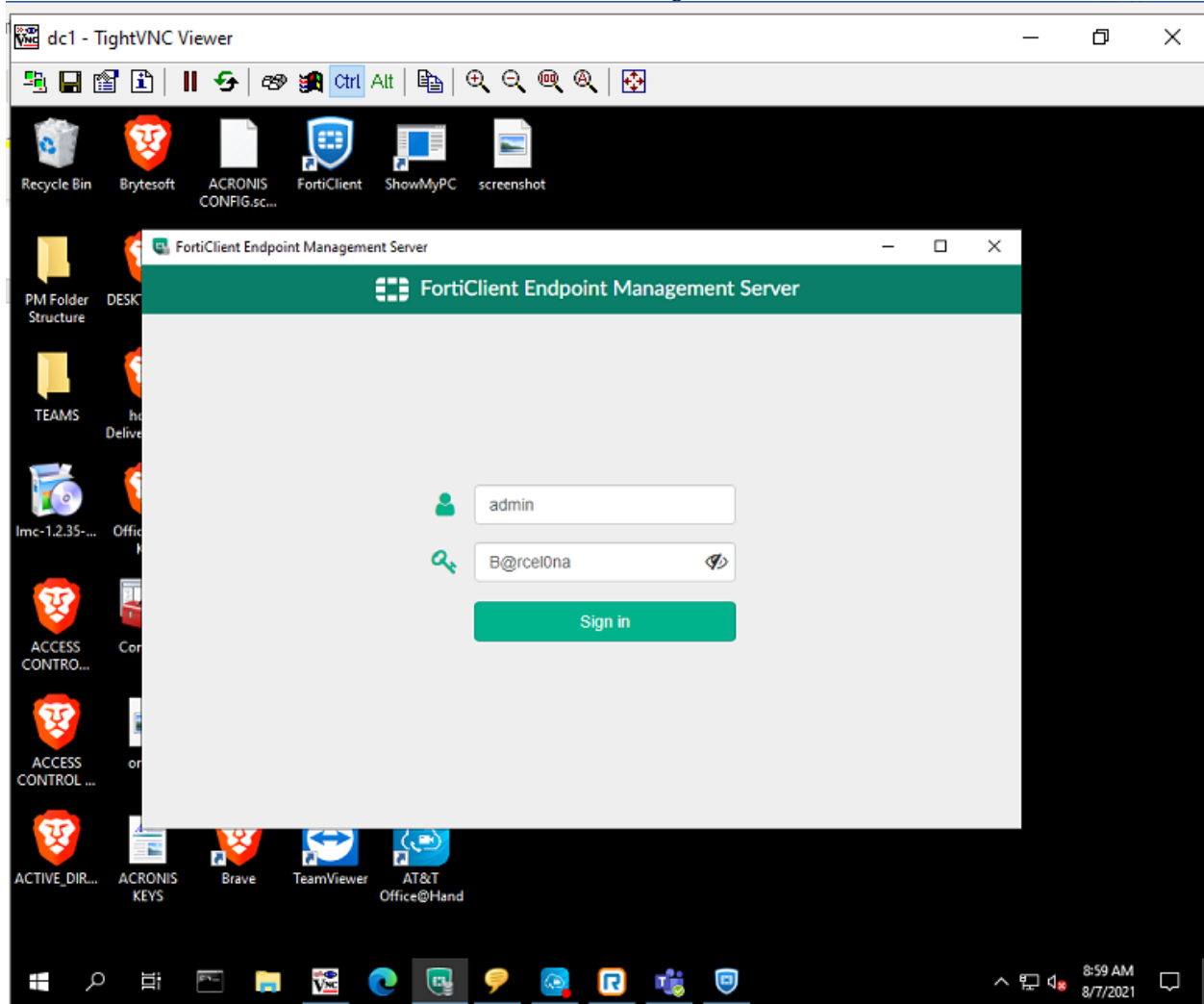
8/7/2021 8:51 AM







Fortinet End Point Management Server



Enterprise Wide Vulnerability Scan

dc1 - TightVNC Viewer

FortiClient Endpoint Management Server

Invitations 100% admin

Dashboard

Status

Vulnerability Scan

Endpoints

Deployment & Installers

Endpoint Policy & Components

Endpoint Profiles

Zero Trust Tags

Software Inventory

Quarantine Management

Administration

System Settings

Current Vulnerabilities Summary

6 Critical Vulnerabilities on 6 Hosts

0 Low

1 Medium

2 High

6 Critical

Total View 9

9 Third Party App

0 Operating System

0 Service

0 Browser

0 User Config

0 Microsoft Office

0 Other

Endpoint Scan Status

11 Total

6 Vulnerable

5 Secured

File Home Insert Design Layout

Calibri (Body) 11

dc1 - TightVNC Viewer

FortiClient Endpoint Management Server

Invitations 100% admin

Dashboard

Status

Vulnerability Scan

Endpoints

Deployment & Installers

Endpoint Policy & Components

Endpoint Profiles

Zero Trust Tags

Software Inventory

Quarantine Management

Administration

System Settings

Affected Endpoints

Hostname	Username	Last Seen	Scan Time
ENGINEERING1	asupplegate	2021-08-07 08:59:41	2021-08-06 13:54:34
DC2	dbermudez	2021-08-07 09:00:37	2021-08-07 09:00:31
ANDRE	abermudez	2021-08-06 16:59:09	2021-08-06 13:07:02
DESKTOP-JSCFAJIT	kzeller	2021-08-05 12:46:20	2021-08-03 08:52:20
Onopa-Admin	Autumn	2021-08-07 08:59:41	2021-08-06 13:21:06
DESKTOP-3JOBAJG	jafet	2021-08-03 19:05:27	2021-08-02 12:11:36

Showing 6

Page 5 of 5 32 words English (United States)

Type here to search

78°F

9:01 AM 8/7/2021

AutoSave Document2 - Word Search Anthony@ Sullivan AS

File Home Insert Design Layout

Clipboard Font

dc1 - TightVNC Viewer

FortiClient Endpoint Management Server

Dashboard 1 Not 1 Not 7 Out-Of 8 Security 0 Quarantined

Endpoints

All Endpoints

Manage Domains

Domains

Workgroups

Invitations

Group Assignment Rules

Deployment & Installers

Endpoint Policy & Components

Endpoint Profiles

Zero Trust Tags

Software Inventory

Quarantine Management

Administration

System Settings

Owner

IT Department
ITDEPT@ONOPA
(915) 504-1323
ONOPA CMMC

Device: DESKTOP-4KH...

OS: Microsoft Windows

IP: 192.168.1.100

MAC: 00-09-0f-aa-00-01

Public IP: 2607:fbb0:4002:cof:1

Connection: Managed by EMS

Configuration

Policy: Default

Profile: Default

Off-Fabric Profile: Not assigned

Installer: ONOPA CMMC...

FortiClient Version: 7.0.0.0029

FortiClient Serial Number: FCT80005351...

FortiClient ID: 986F0A88A6F

Status: Managed

Features

Antivirus enabled

Anti-Ransomware enabled

Cloud Based Malware Outbreak Detection enabled

Sandbox installed

Sandbox Cloud installed

Web Filter enabled

Showing 13 Total: 13

9:03 AM 8/7/2021

Page 6 of 6 32 words English (United States)

Type here to search

AutoSave Document2 - Word Search Anthony@ Sullivan AS

File Home Insert Design Layout

Clipboard Font

dc1 - TightVNC Viewer

FortiClient Endpoint Management Server

Dashboard Add Import From File Refresh

Endpoints

Local Profiles

Default 2021-08-05 10:22

MCBCL 2021-08-02 07:37

Manage Profiles

Import from FortiGate/FortiMan...

Zero Trust Tags

Software Inventory

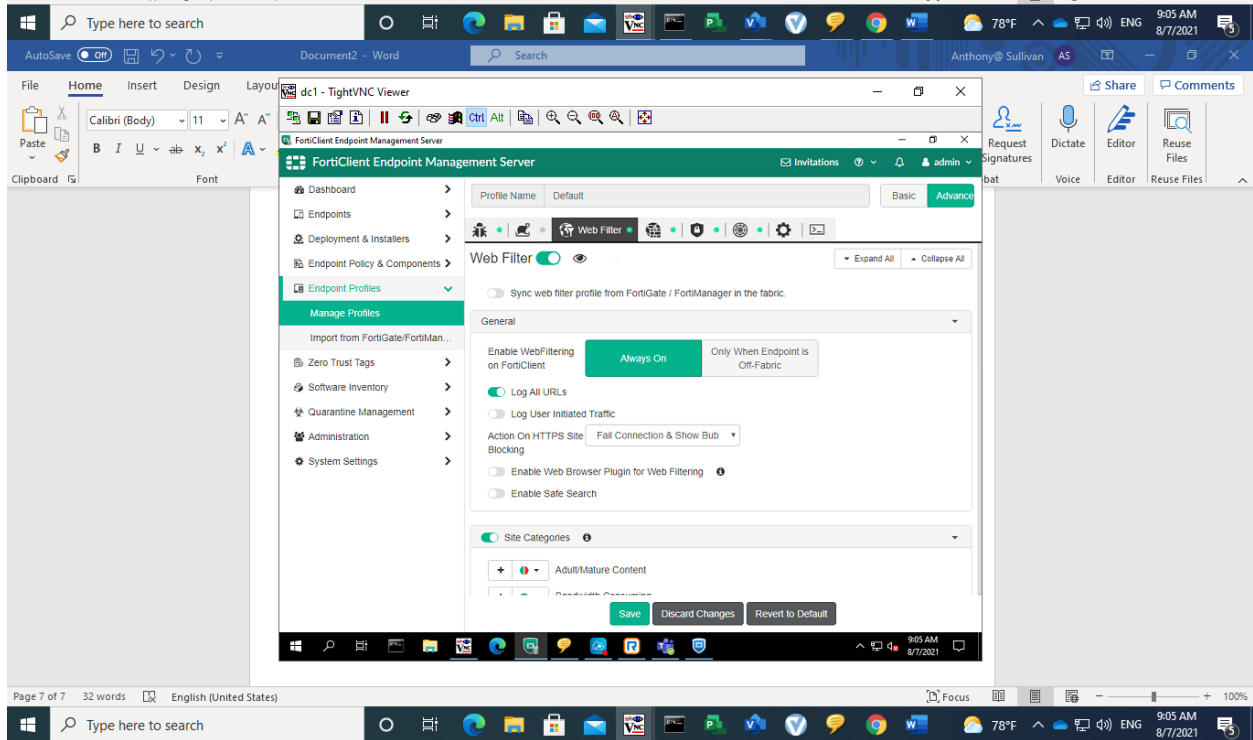
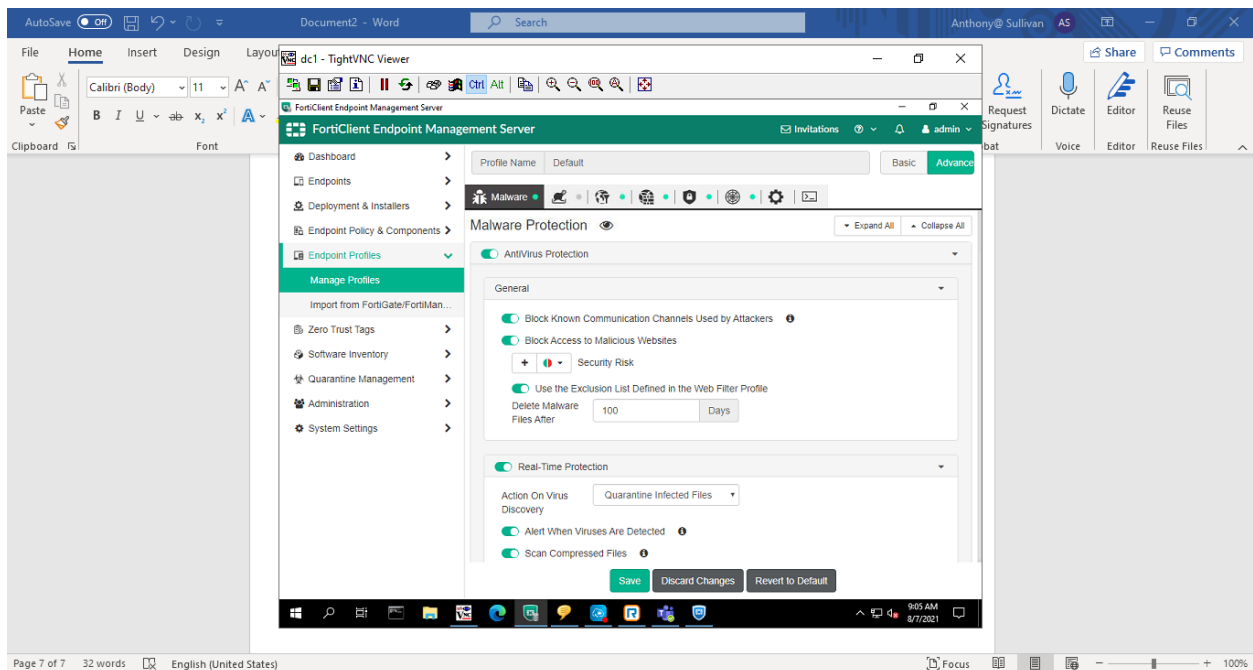
Quarantine Management

Administration

System Settings

Showing 2

9:04 AM 8/7/2021



dc1 - TightVNC Viewer

FortiClient Endpoint Management Server

FortiClient Endpoint Management Server

Invitations admin

Dashboard Endpoints Deployment & Installers Endpoint Policy & Components Endpoint Profiles Manage Profiles Import from FortiGate/FortiMan... Zero Trust Tags Software Inventory Quarantine Management Administration System Settings

Profile Name Default Basic Advance

Application Firewall

General

Notification Bubbles on User's Desktop When Applications Are Blocked

Detect & Block Exploits

Categories

Botnet Business Cloud.IT Collaboration Email Game General Interest Industrial Mobile

Save Discard Changes Revert to Default

AutoSave Document2 - Word Anthony@ Sullivan AS

File Home Insert Design Layout

Calibri (Body) 11

Paste

Clipboard Font

dc1 - TightVNC Viewer

FortiClient Endpoint Management Server

FortiClient Endpoint Management Server

Invitations admin

Dashboard Endpoints Deployment & Installers Endpoint Policy & Components Endpoint Profiles Manage Profiles Import from FortiGate/FortiMan... Zero Trust Tags Software Inventory Quarantine Management Administration System Settings

Profile Name Default Basic Advance

VPN

Allow Personal VPN

Disable Connect/Disconnect

Show VPN before Login

Use Windows Credentials

Minimize FortiClient Console on Connect

Show Connection Progress

Suppress VPN Notifications

Use Vendor ID

Current Connection ONOPA

Auto Connect ONOPA

Auto Connect Only When Off-Fabric

Always Up Max Tries 0

Save Discard Changes Revert to Default

Page 8 of 9 32 words English (United States)

Type here to search

Focus

78°F

9:07 AM 8/7/2021

AutoSave 09 Document2 - Word Search Anthony@ Sullivan AS

File Home Insert Design Layout

Clipboard Font

dc1 - TightVNC Viewer

FortiClient Endpoint Management Server

Dashboard Endpoints Deployment & Installers Endpoint Policy & Components Endpoint Profiles Manage Profiles Import from FortiGate/FortiMan... Zero Trust Tags Software Inventory Quarantine Management Administration System Settings

Profile Name Default Basic Advance

Vulnerability Scan

Scanning

Scan on Registration Scan on Vulnerability Signature Update Scan for OS Updates Enable Proxy

Automatic Maintenance

Scheduled Scan

Automatic Patching Patch Level All Automatic patching may require endpoint reboot.

Save Discard Changes Revert to Default

9:07 AM 8/7/2021

Page 9 of 9 32 words English (United States)

Type here to search

AutoSave 09 Document2 - Word Search Anthony@ Sullivan AS

File Home Insert Design Layout

Clipboard Font

dc1 - TightVNC Viewer

FortiClient Endpoint Management Server

Dashboard Endpoints Deployment & Installers Endpoint Policy & Components Endpoint Profiles Manage Profiles Import from FortiGate/FortiMan... Zero Trust Tags Software Inventory Applications Hosts Quarantine Management Administration System Settings

11 Hosts 4 Operating Systems

Host	User	OS	IP	Application	Last Instal...
ANDRE	abermudez	Microsoft Windows 10 Profes...	192.168.1.219	169	2021-08-05
DAVID	dbermudez	Microsoft Windows 10 Profes...	192.168.1.200	136	2021-08-06
DC2	dbermudez	Microsoft Windows Server 20...	192.168.1.12	52	2021-08-06
DESKTO...	jafet	Microsoft Windows 10 Profes...	192.168.1.202	198	2021-08-01
DESKTO...	Owner	Microsoft Windows 10 Enterp...	192.168.1.100	118	2021-08-07
DESKTO...	autum	Microsoft Windows 10 Profes...	192.168.1.101	115	2021-08-05
DESKTO...	kzeller	Microsoft Windows 10 Profes...	192.168.1.212	174	2021-08-05
DESKTO...	Dawn Nel...	Microsoft Windows 10 Profes...	192.168.1.100	115	2021-08-05
ENGINEE...	aaplegate	Microsoft Windows 10 Profes...	192.168.1.205	224	2021-08-07
Onopa-Ad...	Autumn	Microsoft Windows 10 Profes...	192.168.1.220	178	2021-08-06
Onopa-FL...	dnelson	Microsoft Windows 10 Profes...	192.168.1.211	161	2021-08-05

Showing: 11 Hosts Total: 11 hosts

9:08 AM 8/7/2021

AutoSave Document2 - Word Search Anthony@ Sullivan AS

File Home Insert Design Layout

Paste Calibri (Body) 11 A⁺ A⁻ B I U Clipboard Font

dc1 - TightVNC Viewer

FortiClient Endpoint Management Server

Invitations 8 1 1 8

Dashboard > Endpoints > Deployment & Installers > Endpoint Policy & Components > Endpoint Profiles > Zero Trust Tags > Software Inventory > Quarantine Management > Files > Allowlist > Administration > System Settings >

View Display by instance Search All Fields Filters

Host	File	Size	Threat	Source	Status	Summary
DESKTOP... ONOP...	AWInstaller_8257_1207... 77AA471F59528A7A5F7...	733.9 kB	Riskware/...	Realtime ...	Quarantined 2021-08-0... 2 hosts aff...	7 instances
DESKTOP... ONOP...	mcgc64_yxeepsuox.dll 668B9A06F8B8020FED...	4.4 MB	Riskware/...	Realtime ...	Quarantined 2021-08-0... 1 host affe...	1 instance
DESKTOP... ONOP...	mcie64_bekmxuau.dll 80D8E6156770A95C77...	3.7 MB	Riskware/...	Realtime ...	Quarantined 2021-08-0... 1 host affe...	1 instance
DESKTOP... ONOP...	mcie64_laairfob.dll 88D41E484787DF54BD...	1.1 MB	Adware/W...	Realtime ...	Quarantined 2021-08-0... 1 host affe...	1 instance
DESKTOP... ONOP...	chromeplg.dll 78E4C801A6B82CE6C7B...	2.3 MB	Riskware/...	Realtime ...	Quarantined 2021-08-0... 1 host affe...	1 instance
DESKTOP... ONOP...	svcbboot_vtbecpyu.dll 52A7D85D06F4118CF87...	250.8 kB	Riskware/...	Realtime ...	Quarantined 2021-08-0... 1 host affe...	1 instance
DESKTOP... ONOP...	Unconfirmed 835013 cr... 77AA471F59528A7A5F7...	733.9 kB	Riskware/...	Realtime ...	Quarantined 2021-08-0... 2 hosts aff...	7 instances
DESKTOP... ONOP...	Unconfirmed 774838 cr... 77AA471F59528A7A5F7...	733.9 kB	Riskware/...	Realtime ...	Quarantined 2021-08-0... 2 hosts aff...	7 instances

Showing: 8 files Total: 8 files Load next 50

9:09 AM 8/7/2021

Page 10 of 10 32 words English (United States)

AutoSave Document2 - Word Search Anthony@ Sullivan AS

File Home Insert Design Layout

Paste Calibri (Body) 11 A⁺ A⁻ B I U Clipboard Font

dc1 - TightVNC Viewer

FortiClient Endpoint Management Server

Invitations 8 1 1 8

Dashboard > Endpoints > Deployment & Installers > Endpoint Policy & Components > Endpoint Profiles > Zero Trust Tags > Software Inventory > Quarantine Management > Administration > System Settings > EMS Settings > Log Settings > FortiGuard Services > EMS Alerts > Endpoint Alerts > SMTP Server > Custom Messages > Feature Select

Feature Select

- ☒ Malware Protection
 - ☒ Antivirus 0
 - ☒ Anti-Ransomware 0
 - ☒ Anti-Exploit 0
 - ☒ Cloud Based Malware Detection 0
 - ☒ Removable Media Access 0
- ☒ Sandbox Detection 0
- ☒ Web Filter 0
- ☒ Application Firewall 0
- ☒ VPN 0
- ☒ Vulnerability Scan 0

Save Cancel

9:10 AM 8/7/2021

Page 10 of 10 32 words English (United States)

Microsoft Office Home

Privacy error

fortinet 60f - Google Search

Fortinet FAD-60F | Fortinet Forti...

Not secure | 192.168.1.5/admin

Your connection is not private

Attackers might be trying to steal your information from **192.168.1.5** (for example, passwords, messages, or credit cards). [Learn more](#)

NET::ERR_CERT_AUTHORITY_INVALID

To get Chrome's highest level of security, [turn on enhanced protection](#)

Hide advanced

Back to safety

This server could not prove that it is **192.168.1.5**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

[Proceed to 192.168.1.5 \(unsafe\)](#)

Type here to search

79°F 9:22 AM 8/7/2021

Microsoft Office Home

FortiVoice

fortinet 60f - Google Search

Fortinet FAD-60F | Fortinet Forti...

Not secure | 192.168.1.5/admin/AdminLogin.html

Please Login

Name

Password

☐ Remember me

Log In

Type here to search

79°F 9:23 AM 8/7/2021

Microsoft Office Home x FortiVoice x fortinet 60f - Google Search x Fortinet FAD-60F | Fortinet Forti... x +

192.168.1.5/admin/Admin.html#/dashboard/vx_status

FortiVoice 20E FortiVoice

admin

Dashboard Status Call Statistics Console +Manage Widget Reset Widget

Monitor > System > Phone System > Managed System > Security > Extension > Trunk > Call Routing > Call Feature > Log & Report

System Information

Serial number: FO20E25G20000104

Up time: 2 day(s) 23 hour(s) 0 minute(s) 17 second(s)

System time: Sat, Aug 7, 2021 09:23:42 EDT [\[Change...\]](#)

Reboot time: Wed, Aug 4, 2021 10:23:25 EDT

Firmware version: v6.0.9(GA), build272, 2021.06.02 [\[Update...\]](#)

System configuration: [\[Backup...\]](#) [\[Restore...\]](#)

Deployment mode: PBX

Current administrator: admin (2 in total) [\[Details...\]](#)

Endpoint: Total/Limit: 5/25

Log disk: Capacity 2736 MB, Used 68 MB (2.52%), Free 2667 MB

Storage disk: Capacity 10 GB, Used 4121 MB (37.65%), Free 6827 MB

Phones not assigned: 0

System Resource

CPU usage: 8%

Memory usage: 28%

Log disk usage: 2%

Storage usage: 37%

License Information

[\[Update License...\]](#)

Recent Call

Direction: --All-- Disposition: --All--

From (Name)	From	To (Name)	To	Start
Unavailable	7868377619	AA: auto_atten...	0000000	2021-08-06 18...
Unavailable	13214500201	AA: auto_atten...	0000000	2021-08-06 13...
Unavailable	14075535775	AA: auto_atten...	0000000	2021-08-06 12...
David Bermudez	7706	3864792081	7706	2021-08-06 11...
CARR RIGGS INGR	13213979872	AA: auto_atten...	0000000	2021-08-06 10...
Operator	7701	David Bermudez	7706	2021-08-06 10...
Operator	7701	Operator	7701	2021-08-06 10...
Andre Bermudez	7711	3864792081	3864792081	2021-08-06 09...

Start

Type here to search

Microsoft Office Home x FortiVoice x fortinet 60f - Google Search x Fortinet FAD-60F | Fortinet Forti... x +

192.168.1.5/admin/Admin.html#/pbx/ext_device

FortiVoice 20E FortiVoice

admin

Dashboard Phone Multi-cell Device

+ New... Edit... Delete + Action... Filter: --None--

Option: --All--

1 / 1 Page size: 50 Total: 5

Extens...	MAC Address	Phone Model	Phone Profile	Management	Number	Display Name	Status	IP	Phone Info
	04:d5:90:16:71:94	FortiFone-175	Default-FortiFon...	Assigned - Main	7711	Andre Bermudez		192.168.1.225	Fortinet FortiFon...
	04:d5:90:16:74:de	FortiFone-175	Default-FortiFon...	Assigned - Main	7703	Kirk Zeller		192.168.1.206	Fortinet FortiFon...
	04:d5:90:16:74:e2	FortiFone-175	Default-FortiFon...	Assigned - Main	7702	Dawn Nelson		192.168.1.214	Fortinet FortiFon...
	04:d5:90:16:74:e9	FortiFone-175	Default-FortiFon...	Assigned - Main	7706	David Bermudez		192.168.1.229	Fortinet FortiFon...
	e0:23:ff:1b:8f:76	FortiFone-675i	Default-FortiFon...	Assigned - Main	7701	Operator		192.168.1.209	Fortinet FON-67...

Microsoft Office Home x FortiVoice x fortinet 60f - Google Search x Fortinet FAD-60F | Fortinet Forti... x +

Not secure | 192.168.1.5/admin/Admin.html#/pbx/numlist

FortiVoice 20E FortiVoice admin

Dashboard Monitor System Phone System Setting Contact Audio Profile Device Review Managed System Security Extension Trunk Call Routing Call Feature Log & Report

Number MWI Auditor Network Summary DID Handling Referenced Extension

Extension type: All Referred type: All

1 / 1 Page size: 50 Selected: 1 / 5

Number	Display Name
7711 (IP extension)	Andre Bermudez
Reference Object	Referenced Role
SANFORD (User group)	Group member
7711 (Extension)	Message waiting light(mwl) notification subscriber
7706 (IP extension)	David Bermudez
Reference Object	Referenced Role
SANFORD (User group)	Group member
7706 (Extension)	Message waiting light(mwl) notification subscriber
7703 (IP extension)	Kirk Zeller
Reference Object	Referenced Role
SANFORD (User group)	Group member
7702 (IP extension)	Dawn Nelson
Reference Object	Referenced Role
SANFORD (User group)	Group member
7702 (Extension)	Message waiting light(mwl) notification subscriber
7701 (IP extension)	Operator
Reference Object	Referenced Role

Type here to search

Microsoft Office Home x FortiVoice x fortinet 60f - Google Search x Fortinet FAD-60F | Fortinet Forti... x +

Not secure | 192.168.1.5/admin/Admin.html#/voip_trunks/trunks_sip

FortiVoice 20E FortiVoice admin

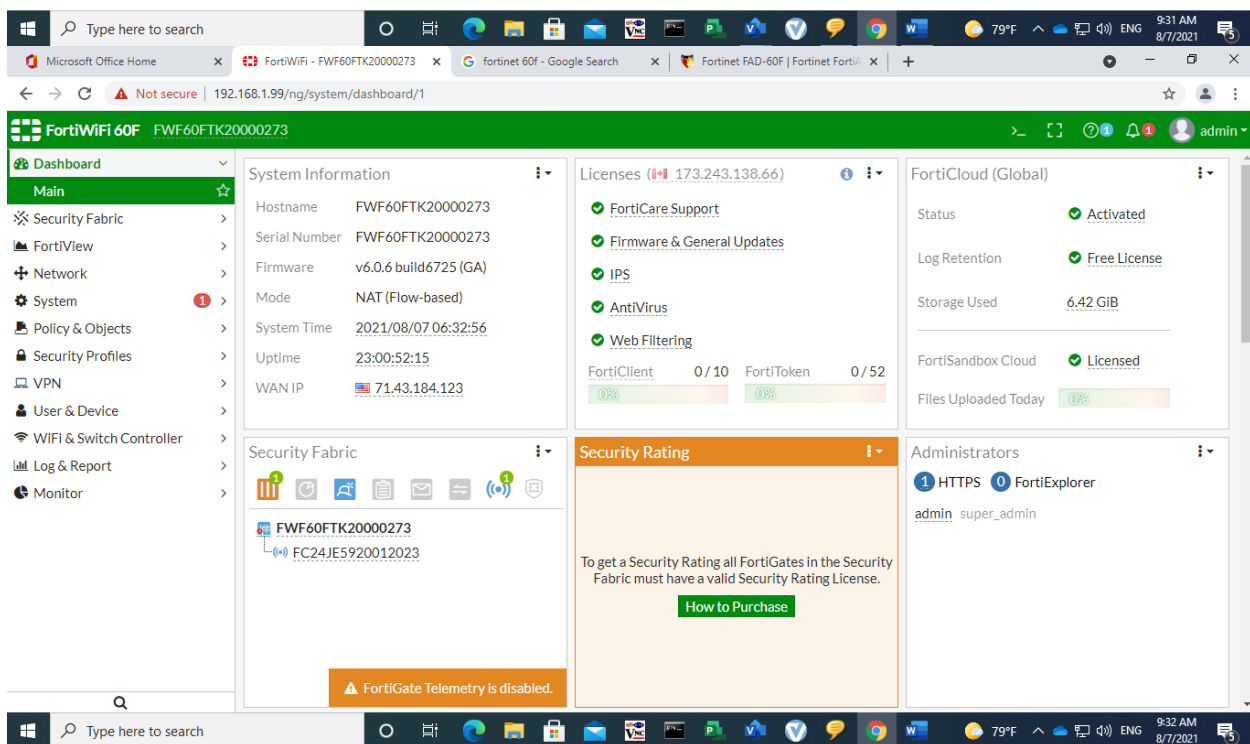
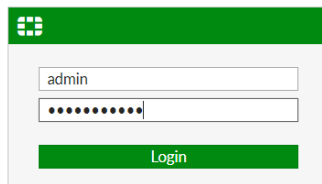
Dashboard Monitor System Phone System Managed System Security Extension Trunk Call Routing Call Feature Log & Report

SIP

+ New... Edit... Delete Test FortiCall

1 / 1 Page size: 50 Total: 4

Enabled ...	Name	Server	Port	SIP Setting	Status
<input checked="" type="checkbox"/>	ATT101	sipringcentral.com	5060	sip_setting_default	In service
<input checked="" type="checkbox"/>	ATT102	sipringcentral.com	5060	sip_setting_default	In service
<input checked="" type="checkbox"/>	ATT103	sipringcentral.com	5060	sip_setting_default	In service
<input checked="" type="checkbox"/>	ATT104	sipringcentral.com	5060	sip_setting_default	In service



Microsoft Office Home x FortiWiFi - FWF60FTK20000273 x fortinet 60f - Google Search x Fortinet FAD-60F | Fortinet Forti... x +

192.168.1.99/ng/page/p/system/interface/

FortiWiFi 60F FWF60FTK20000273

admin

- Dashboard
- Security Fabric
- FortiView
- Network
- Interfaces
- DNS
- Packet Capture
- SD-WAN
- Performance SLA
- SD-WAN Rules
- Static Routes
- System
- Policy & Objects
- Security Profiles
- VPN
- User & Device
- WiFi & Switch Controller
- Log & Report
- Monitor

FortiWiFi 60F

INTERNAL

1 2 3 4 5 A B DMZ WAN1 WAN2

+ Create New Edit Delete

By Type By Role Alphabetically

Status	Name	Members	IP/Netmask	Type	Access	Ref.
Hardware Switch (1)						
	fortilink	1 2 3 4 5 A B	Dedicated to FortiSwitch	Hardware Switch (2)	PING CAPWAP	2
Physical (3)						
	dmz		10.10.10.1 255.255.255.0	Physical Interface	PING HTTPS FMG-Access CAPWAP	0
	wan1		71.43.184.123 255.255.255.248	Physical Interface	FortiTelemetry	7
	wan2		0.0.0.0 0.0.0.0	Physical Interface		0
Software Switch (2)						
	lan	internal, wifi (SSID: ONOPA)	192.168.1.99 255.255.255.0	Software Switch (2)	PING HTTPS SSH FMG-Access CAPWAP FortiTelemetry	7
	wgt.root	wgtn.8.wifi	0.0.0.0 0.0.0.0	Software Switch (1)		0
WiFi (2)						
	wifi (SSID: ONOPA)			WiFi SSID		3
	wgtn.8.wifi		0.0.0.0 0.0.0.0	VLAN		1

Type here to search

Microsoft Office Home x FortiWiFi - FWF60FTK20000273 x fortinet 60f - Google Search x Fortinet FAD-60F | Fortinet Forti... x +

192.168.1.99/ng/firewall/policy/policy/standard

FortiWiFi 60F FWF60FTK20000273

admin

+ Create New Edit Delete Policy Lookup Search

Interface Pair View By Sequence

ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log
lan → SSL-VPN tunnel interface (ssl.root) 1									
6	Reach_Back	all	REACHBACK	always	ALL	ACCEPT	Disabled		UTM
lan → wan1 3									
5	Fortivoice_ATT	Fortivoice_Internal	ATT	always	ALL	ACCEPT	Enabled		UTM
2	test	testadd	testadd2	always	ALL	ACCEPT	Enabled		All
1		all	all	always	ALL	ACCEPT	Enabled		All
SSL-VPN tunnel interface (ssl.root) → lan 1									
3	ssl to internal	all	Internal	always	ALL	ACCEPT	Enabled	AV default WEB default DNS default APP default SSL certificate-inspection	All
wan1 → lan 1									
4	ATT_Fortivoice	all	FortivoiceVIP	always	SIP	ACCEPT	Disabled		All
Implicit 1									
0	Implicit Deny	all	all	always	ALL	DENY			Disabled

Type here to search

Microsoft Office Home x FortiWiFi - FWF60FTK20000273 x fortinet 60f - Google Search x Fortinet FAD-60F | Fortinet Forti... x

192.168.1.99/ng/firewall/service

FortiWiFi 60F FWF60FTK20000273

admin

- Dashboard
- Security Fabric
- FortiView
- Network
- System
- Policy & Objects
 - IPv4 Policy
 - Addresses
 - Wildcard FQDN
 - Addresses
 - Internet Service Database
 - Services**
 - Schedules
 - Virtual IPs
 - IP Pools
 - Traffic Shapers
 - Traffic Shaping Policy
- Security Profiles
 - VPN
 - User & Device

92

Type here to search

Microsoft Office Home x FortiWiFi - FWF60FTK20000273 x fortinet 60f - Google Search x Fortinet FAD-60F | Fortinet Forti... x

192.168.1.99/ng/page/p/utm/antivirus/profile/edit/default/

FortiWiFi 60F FWF60FTK20000273

admin

Edit AntiVirus Profile

Name: default

Comments: Scan files and block viruses. 29/255

Scan Mode: Quick Full

Detect Viruses: Block Monitor

APT Protection Options

Treat Windows Executables in Email Attachments as Viruses: ☒

Send Files to FortiSandbox Cloud for Inspection: None Suspicious Files Only All Supported Files

Do not submit files matching types: +

Do not submit files matching file name patterns: +

Use Virus Outbreak Prevention Database: ☒

Use FortiSandbox Database: ☒

Include Mobile Malware Protection: ☒

Apply

Type here to search

Microsoft Office Home x FortiWiFi - FWF60FTK20000273 x fortinet 60f - Google Search x Fortinet FAD-60F | Fortinet Forti... x

192.168.1.99/ng/log/view/forward_traffic

FortiWiFi 60F FWF60FTK20000273

admin

- Network
- System
- Policy & Objects
- Security Profiles
- VPN
- User & Device
- WiFi & Switch Controller
- Log & Report
 - Forward Traffic
 - Local Traffic
 - Sniffer Traffic
 - System Events
 - Router Events
 - VPN Events
 - User Events
 - Endpoint Events
 - HA Events
 - Security Rating Events
 - WiFi Events

#	Date/Time	Source	Destination	Application Name	Security Events	Result
1	3 hours ago	192.168.1.10	8.8.8.8 (dns.google)	DNS		✓ Accept: s
2	3 hours ago	ENGINEERING1	8.8.8.8 (dns.google)	DNS		✓ 74 B / 20
3	3 hours ago	192.168.1.205	8.8.8.8 (dns.google)	DNS		✓ Accept: s
4	3 hours ago	ONOPA-FINANCE	13.35.105.49 (d17ndjuagurpsr.cloudfront.net)	HTTPS		✓ 1.67 kB /
5	3 hours ago	ONOPA-ADMIN	204.79.197.203 (www.msn.com)	HTTPS		
6	3 hours ago	ONOPA-FINANCE	162.125.5.13 (client-env.dropbox-dns.com)	HTTPS		
7	3 hours ago	192.168.1.5	199.255.120.214 (sip10.ringcentral.biz)	UDP/5090		✓ Accept: s
8	3 hours ago	ENGINEERING1	104.46.162.226 (global.asimov.events.data.trafficmanager.net)	HTTPS		
9	3 hours ago	ONOPA-ADMIN	52.96.189.2 (acdc-direct.office.com)	HTTPS		✓ 207.07 kt
10	3 hours ago	192.168.1.205	210.7.96.12	UDP/8888		✓ Accept: s
11	3 hours ago	192.168.1.205	210.7.96.14	UDP/8888		✓ Accept: s
12	3 hours ago	192.168.1.205	83.231.212.83	UDP/8888		✓ Accept: s
13	3 hours ago	192.168.1.205	83.231.212.82	UDP/8888		✓ Accept: s
14	3 hours ago	192.168.1.205	173.243.138.194 (service.fortiguard.net)	UDP/8888		✓ Accept: s
15	3 hours ago	192.168.1.205	173.243.138.195	UDP/8888		✓ Accept: s
16	3 hours ago	192.168.1.205	209.222.147.43	UDP/8888		✓ Accept: s
17	3 hours ago	192.168.1.205	66.117.56.38	UDP/8888		✓ Accept: s
18	3 hours ago	192.168.1.205	12.34.97.71	UDP/8888		✓ Accept: s
19	3 hours ago	192.168.1.205	66.117.56.37	UDP/8888		✓ Accept: s
20	3 hours ago	192.168.1.211	162.125.5.13 (client-env.dropbox-dns.com)	HTTPS		✓ Accept: s

Start

Type here to search

Microsoft Office Home x FortiWiFi - FWF60FTK20000273 x fortinet 60f - Google Search x Fortinet FAD-60F | Fortinet Forti... x

192.168.1.99/ng/page/p/utm/wf/profile/edit/default/

FortiWiFi 60F FWF60FTK20000273

admin

Edit Web Filter Profile

☒ FortiGuard category based filter

Pre-configured filters **Custom** G PG-13 R

Show ☐ All

- ☒ Local Categories
- ☐ Potentially Liable
- ☐ Adult/Mature Content
- ☒ Bandwidth Consuming
- ☐ Security Risk
- ☒ General Interest - Personal
- ☒ General Interest - Business
- ☐ Unrated

Static URL Filter

URL Filter ☐

Block malicious URLs discovered by FortiSandbox ☐

Web Content Filter ☐

Rating Options

Allow websites when a rating error occurs ☒

Apply

Type here to search

80°F 9:39 AM 8/7/2021

Microsoft Office Home x FortiWiFi - FWF60FTK20000273 x fortinet 60f - Google Search x Fortinet FAD-60F | Fortinet Forti... x +

192.168.1.99/ng/page/p/utm/dns/profile/edit/default/

FortiWiFi 60F FWF60FTK20000273

admin

- Dashboard
- Security Fabric
- FortiView
- Network
- System
- Policy & Objects
- Security Profiles
 - AntiVirus
 - Web Filter
 - DNS Filter**
 - Application Control
 - Intrusion Prevention
 - FortiClient Compliance
 - SSL/SSH Inspection
 - Web Rating Overrides
 - Custom Signatures
- VPN
- User & Device
- WiFi & Switch Controller
- Log & Report

Edit DNS Filter Profile

Redirect botnet C&C requests to Block Portal ☒ 39803 domains in [botnet package](#).

Enforce 'Safe search' on Google, Bing, YouTube ☐

☐ FortiGuard category based filter

Static Domain Filter

Domain Filter ☒

+ Create Edit Delete Search

Domain	Type	Action	Status
amazon.com	Simple	Allow	Enable
kdp.amazon.com	Simple	Allow	Enable
facebook.com	Simple	Redirect to Block Portal	Enable

External IP Block Lists ☐

Options

Redirect Portal IP ☒ Use FortiGuard Default Specify 0.0.0.0

Allow DNS requests when a rating error occurs ☒

Apply

Microsoft Office Home x FortiWiFi - FWF60FTK20000273 x fortinet 60f - Google Search x Fortinet FAD-60F | Fortinet Forti... x +

192.168.1.99/ng/utm/appctrl/sensor/edit/default

FortiWiFi 60F FWF60FTK20000273

admin

- Dashboard
- Security Fabric
- FortiView
- Network
- System
- Policy & Objects
- Security Profiles
 - AntiVirus
 - Web Filter
 - DNS Filter
 - Application Control**
 - Intrusion Prevention
 - FortiClient Compliance
 - SSL/SSH Inspection
 - Web Rating Overrides
 - Custom Signatures
- VPN
- User & Device
- WiFi & Switch Controller
- Log & Report

Edit Application Sensor

110 Cloud Applications require deep inspection.
1 policies are using this profile. [\[View Application Signatures\]](#)

Deep Inspection is disabled on the following policies:
[ssl to Internal](#)

Name default [View Application Signatures]

Comments Monitor all applications. 25/255

Categories

All Categories

Business (152, 6)	Cloud.IT (58, 1)	Collaboration (264, 16)
Email (77, 12)	Game (85)	General.Interest (231, 7)
Mobile (3)	Network.Service (331)	P2P (56)
Proxy (173)	Remote.Access (93)	Social.Media (115, 32)
Storage.Backup (161, 20)	Update (49)	Video/Audio (155, 16)
VoIP (24)	Web.Client (24)	Unknown Applications

Application Overrides

Apply

Microsoft Office Home x FortiWiFi - FWF60FTK20000273 x fortinet 60f - Google Search x Fortinet FAD-60F | Fortinet Forti... x

Not secure | 192.168.1.99/page/p/utm/ips/sensor/edit/default/

FortiWiFi 60F FWF60FTK20000273 admin

Dashboard > Security Fabric > FortiView > Network > System > Policy & Objects > Security Profiles > AntiVirus > Web Filter > DNS Filter > Application Control > Intrusion Prevention > FortiClient Compliance > SSL/SSH Inspection > Web Rating Overrides > Custom Signatures > VPN > User & Device > WiFi & Switch Controller > Log & Report >

Edit IPS Sensor

Name: default [View IPS Signatures]

Comments: Prevent critical attacks. 25/255

Block malicious URLs: ☒

IPS Signatures

+ Add Signatures Delete Edit IP Exemptions

Name	Exempt IPs	Severity	Target	Service	OS	Action	Packet Logging
No matching entries found							

IPS Filters

+ Add Filter Edit Filter Delete

Filter Details				Action	Packet Logging
Severity:				Default	

Rate Based Signatures

Enable	Signature	Threshold	Duration (seconds)	Track By	Action	Block Duration (minutes)
<input type="checkbox"/>	Apache.OpenMeetings.NetTest.DoS	10	3	Any	Block	None
<input type="checkbox"/>	Apache.OpenMeetings.NetTest.Download.Upload.size.DoS	10	5	Any	Block	None

Apply

Microsoft Office Home x FortiWiFi - FWF60FTK20000273 x fortinet 60f - Google Search x Fortinet FAD-60F | Fortinet Forti... x

Not secure | 192.168.1.99/page/p/utm/endpoint/profile/edit/default/

FortiWiFi 60F FWF60FTK20000273 admin

Dashboard > Security Fabric > FortiView > Network > System > Policy & Objects > Security Profiles > AntiVirus > Web Filter > DNS Filter > Application Control > Intrusion Prevention > FortiClient Compliance > SSL/SSH Inspection > Web Rating Overrides > Custom Signatures > VPN > User & Device > WiFi & Switch Controller > Log & Report >

Edit FortiClient Compliance Profile

Telemetry Data

Non-compliance action: Block Warning

Endpoints must send telemetry data to FortiGate for Security Fabric. Unregistered endpoints will be issued a warning.

Specify Compliance Criteria

Endpoint Compliance on: EMS FortiGate

☒ Endpoint Vulnerability Scan on Client

Vulnerability level: High

Non-compliance action: Block Warning

☒ System Compliance

Minimum FortiClient version: ☐

Upload Logs to FortiAnalyzer: ☒ Traffic ☒ Vulnerability ☒ Event

Check Running Applications: ☐

Non-compliance action: Block Warning

Apply

Microsoft Office Home x FortiWiFi - FWF60FTK20000273 x fortinet 60f - Google Search x Fortinet FAD-60F | Fortinet Forti... x +

192.168.1.99/ng/user/group

FortiWiFi 60F FWF60FTK20000273

admin

- Dashboard
- Security Fabric
- FortiView
- Network
- System
- Policy & Objects
- Security Profiles
- VPN
- User & Device
 - User Definition
 - User Groups
 - Guest Management
 - Device Inventory
 - Custom Devices & Groups
 - LDAP Servers
 - RADIUS Servers
 - Authentication Settings
 - FortiTokens
- WiFi & Switch Controller
- Log & Report

Group Name	Group Type	Members	Ref.
Guest-group	Firewall	lcladmin Abermudez dbermudez dnelson autumn	2
SSO_Guest_Users	Fortinet Single Sign-On (FSSO)		1

Type here to search

Microsoft Office Home x FortiWiFi - FWF60FTK20000273 x fortinet 60f - Google Search x Fortinet FAD-60F | Fortinet Forti... x +

192.168.1.99/ng/user/device

FortiWiFi 60F FWF60FTK20000273

admin

- Dashboard
- Security Fabric
- FortiView
- Network
- System
- Policy & Objects
- Security Profiles
- VPN
- User & Device
 - User Definition
 - User Groups
 - Guest Management
 - Device Inventory
 - Custom Devices & Groups
 - LDAP Servers
 - RADIUS Servers
 - Authentication Settings
 - FortiTokens
- WiFi & Switch Controller
- Log & Report

Status	Device	User	Address	Interfaces	OS
Online	FortiAP		192.168.1.213 (DHCP)	lan	
Online	S124EN5920019922		192.168.1.227 (DHCP)	lan	FortiGate
Online	S124EN5920019922		192.168.1.227	lan	FortiOS/FortiSwitch / v6.2.3 build 0202
iOS device 3					
Offline	Lucass-MacBook-Pro		192.168.1.230 (DHCP)	lan	Mac OS X
Offline	Tims-Air		192.168.1.215	lan	Mac OS X
Offline	Zacharys-MacBook-Pro		192.168.1.215 (DHCP)	lan	Mac OS X
Linux PC 1					
Other identified device 1					
Printing device 2					
VoIP phone 4					
Windows device 13					
Server 5					
Online	68:69:2e:03:7b:8b		192.168.1.5	lan	TLS/SSL Server
Online	DC1		192.168.1.110	lan	TLS/SSL Server (Windows / XP (x86))
Online	ENGINEERING1		192.168.1.205 (DHCP)	lan	Web Server (Windows / XP (x86))
Online	ONOPA-ADMIN		192.168.1.220	lan	Samba Server (Windows 10 / 2016)

Type here to search

80°F 9:44 AM 8/7/2021

Microsoft Office Home x FortiWiFi - FWF60FTK20000273 x fortinet 60f - Google Search x Fortinet FAD-60F | Fortinet Forti... x +

Not secure | 192.168.1.99/ng/user/ftoken

FortiWiFi 60F FWF60FTK20000273

admin

- Dashboard
- Security Fabric
- FortiView
- Network
- System
- Policy & Objects
- Security Profiles
- VPN
- User & Device
 - User Definition
 - User Groups
 - Guest Management
 - Device Inventory
 - Custom Devices & Groups
 - LDAP Servers
 - RADIUS Servers
 - Authentication Settings
 - FortiTokens**
 - WiFi & Switch Controller
 - Local WiFi Radio

Type	Serial Number	Status	User	Drift	Comments
Mobile Token	FTKMOB17A8BEF3CC	Available		0	
Mobile Token	FTKMOB17A8D6C6C5	Available		0	
Mobile Token	FTKMOB17A26D2AAF	Available		0	
Mobile Token	FTKMOB17A2165FA1	Available		0	
Mobile Token	FTKMOB17AB1E4E3E	Available		0	
Mobile Token	FTKMOB17ACF3C362	Available		0	
Mobile Token	FTKMOB17AFFA296D	Available		0	
Mobile Token	FTKMOB17B0CBBB51	Available		0	
Mobile Token	FTKMOB17B2BFFF33	Available		0	
Mobile Token	FTKMOB17B235DED0	Available		0	
Mobile Token	FTKMOB17B515F452	Available		0	
Mobile Token	FTKMOB17C0FB4D6A	Available		0	
Mobile Token	FTKMOB17C38BEA0F	Available		0	
Mobile Token	FTKMOB17C81E3A37	Available		0	
Mobile Token	FTKMOB17C138DD29	Available		0	
Mobile Token	FTKMOB17C8419D30	Available		0	
Mobile Token	FTKMOB17CE91CCA2	Available		0	

0% 52

Type here to search

Microsoft Office Home x FortiWiFi - FWF60FTK20000273 x fortinet 60f - Google Search x Fortinet FAD-60F | Fortinet Forti... x +

Not secure | 192.168.1.99/ng/page/p/wifi/managed_ap/

FortiWiFi 60F FWF60FTK20000273

admin

- Dashboard
- Security Fabric
- FortiView
- Network
- System
- Policy & Objects
- Security Profiles
- VPN
- User & Device
- WiFi & Switch Controller
 - Local WiFi Radio
 - Managed FortiAPs**
 - SSID
 - FortiAP Profiles
 - WIDS Profiles
 - Security Profile Groups
 - Managed FortiSwitch
 - FortiSwitch VLANs
 - FortiSwitch Ports
 - FortiSwitch Security

Access Point	Status	Connected Via	SSIDs	Channel	Clients	OS Version	FortiAP Profile	Radio	Group
FC24JE5920012023	Online	192.168.1.213 - lan	Radio 1: All Radio 2: All	Radio 1: 6 Radio 2: 149	Radio 1: 1 Radio 2: 0	FC24JE-v5.4-build0203 A new firmware version is available	FAPC24JE-default		0

1/10 Managed FortiAPs AP Radio Group

<< < 1 /1 > >> [Total: 1]

Type here to search

Microsoft Office Home x FortiWiFi - FWF60FTK20000273 x fortinet 60f - Google Search x Fortinet FAD-60F | Fortinet Forti... x +

Not secure | 192.168.1.99/ng/page/p/wifi/ssid/edit/wifi/

FortiWiFi 60F FWF60FTK20000273

admin

- Dashboard
- Security Fabric
- FortiView
- Network
- System
- Policy & Objects
- Security Profiles
- VPN
- User & Device
- WiFi & Switch Controller**
 - Local WiFi Radio
 - Managed FortiAPs
 - SSID**
 - FortiAP Profiles
 - WIDS Profiles
 - Security Profile Groups
 - Managed FortiSwitch
 - FortiSwitch VLANs
 - FortiSwitch Ports
 - FortiSwitch Security

Edit Interface

Type: WiFi SSID
Traffic Mode: Tunnel

Tags: Add Tag Category

WiFi Settings

SSID: ONOPA
Security Mode: WPA2 Personal
Pre-shared Key: fortinet
Client Limit: ☐
Multiple Pre-shared Keys: ☐
Broadcast SSID: ☒
Schedule: always
Block Intra-SSID Traffic: ☐
Broadcast Suppression: ☒
ARPs for known clients
DHCP Uplink

Filter clients by MAC Address

OK Cancel

Microsoft Office Home x FortiWiFi - FWF60FTK20000273 x fortinet 60f - Google Search x Fortinet FAD-60F | Fortinet Forti... x +

Not secure | 192.168.1.99/ng/page/p/wifi/ap_profiles/

FortiWiFi 60F FWF60FTK20000273

admin

- Dashboard
- Security Fabric
- FortiView
- Network
- System
- Policy & Objects
- Security Profiles
- VPN
- User & Device
- WiFi & Switch Controller**
 - Local WiFi Radio
 - Managed FortiAPs
 - SSID
 - FortiAP Profiles**
 - WIDS Profiles
 - Security Profile Groups
 - Managed FortiSwitch
 - FortiSwitch VLANs
 - FortiSwitch Ports
 - FortiSwitch Security

+ Create New Edit Clone Delete Search View All Profiles

Name	Platform(s)	Radio 1	Radio 2	Comments	Ref.
11ac-only	Local WiFi Radio	5GHz 802.11ac/n			1
11n-only	Local WiFi Radio	2.4GHz 802.11n/g			0
FAPC24JE-default	FAP-C24JE	2.4GHz 802.11n/g/b	5GHz 802.11ac/n/a		1
FORTIAP	FAP-220B, FAP-221B	5GHz 802.11n/a [36, 40, 44 ...]	2.4GHz 802.11n/g [1, 6, 11]		0
FORTI_DAVID	FAP-220B, FAP-221B	5GHz 802.11n/a [36, 40, 44 ...] (w) wifi	2.4GHz 802.11n/g [1, 6, 11]	LOCATED DAVIDS OFFICE	0

Microsoft Office Home x FortiWiFi - FW60FTK20000273 x fortinet 60f - Google Search x Fortinet FAD-60F | Fortinet Forti... x

Not secure | 192.168.1.99/ng/wifi/utm-profile/

FortiWiFi 60F FW60FTK20000273

admin

- Dashboard
- Security Fabric
- FortiView
- Network
- System
- Policy & Objects
- Security Profiles
- VPN
- User & Device
- WIFI & Switch Controller
 - Local WIFI Radio
 - Managed FortiAPs
 - SSID
 - FortiAP Profiles
 - WIDS Profiles
 - Security Profile Groups
 - Managed FortiSwitch
 - FortiSwitch VLANs
 - FortiSwitch Ports
 - FortiSwitch Security

+ Create New View Clone Delete Search

Name	Security Profiles	Logging	Scan Botnets
PHONES	IPS: high_security APP: block-high-risk AV: wifi-default WEB: wifi-default	Enabled	Blocked
wifi-default	IPS: wifi-default APP: wifi-default AV: wifi-default WEB: wifi-default	Enabled	Blocked

Type here to search

Microsoft Office Home x FortiWiFi - FW60FTK20000273 x fortinet 60f - Google Search x Fortinet FAD-60F | Fortinet Forti... x

Not secure | 192.168.1.99/ng/log/view/forward_traffic

FortiWiFi 60F FW60FTK20000273

admin

- Network
- System
- Policy & Objects
- Security Profiles
- VPN
- User & Device
- WIFI & Switch Controller
- Log & Report
 - Forward Traffic
 - Local Traffic
 - Sniffer Traffic
 - System Events
 - Router Events
 - VPN Events
 - User Events
 - Endpoint Events
 - HA Events
 - Security Rating Events
 - WIFI Events
 - Compliance Events

Refresh Add Filter

#	Date/Time	Source	Destination	Application Name	Security Events	Result
1	3 hours ago	192.168.1.10	8.8.8.8 (dns.google)	DNS		Accept: s
2	3 hours ago	ENGINEERING1	8.8.8.8 (dns.google)	DNS		74 B / 20
3	3 hours ago	192.168.1.205	8.8.8.8 (dns.google)	DNS		Accept: s
4	3 hours ago	ONOPA-FINANCE	13.35.105.49 (d17ndjuagurpsr.cloudfront.net)	HTTPS		1.67 kB /
5	3 hours ago	ONOPA-ADMIN	204.79.197.203 (www.msn.com)	HTTPS		
6	3 hours ago	ONOPA-FINANCE	162.125.5.13 (client-env.dropbox-dns.com)	HTTPS		
7	3 hours ago	192.168.1.5	199.255.120.214 (sip10.ringcentral.biz)	UDP/5090		Accept: s
8	3 hours ago	ENGINEERING1	104.46.162.226 (global.asimov.events.data.trafficmanager.net)	HTTPS		
9	3 hours ago	ONOPA-ADMIN	52.96.189.2 (acdc-direct.office.com)	HTTPS		207.07 k
10	3 hours ago	192.168.1.205	210.7.96.12	UDP/8888		Accept: s
11	3 hours ago	192.168.1.205	210.7.96.14	UDP/8888		Accept: s
12	3 hours ago	192.168.1.205	83.231.212.83	UDP/8888		Accept: s
13	3 hours ago	192.168.1.205	83.231.212.82	UDP/8888		Accept: s
14	3 hours ago	192.168.1.205	173.243.138.194 (service.fortiguard.net)	UDP/8888		Accept: s
15	3 hours ago	192.168.1.205	173.243.138.195	UDP/8888		Accept: s
16	3 hours ago	192.168.1.205	209.222.147.43	UDP/8888		Accept: s
17	3 hours ago	192.168.1.205	66.117.56.38	UDP/8888		Accept: s
18	3 hours ago	192.168.1.205	12.34.97.71	UDP/8888		Accept: s
19	3 hours ago	192.168.1.205	66.117.56.37	UDP/8888		Accept: s
20	3 hours ago	192.168.1.211	162.125.5.13 (client-env.dropbox-dns.com)	HTTPS		Accept: s

Microsoft Office Home x FortiWiFi - FWF60FTK20000273 x fortinet 60f - Google Search x Fortinet FAD-60F | Fortinet Forti... x +

Not secure | 192.168.1.99/ng/log/view/system_events

FortiWiFi 60F FWF60FTK20000273

Network System Policy & Objects Security Profiles VPN User & Device WiFi & Switch Controller Log & Report Forward Traffic Local Traffic Sniffer Traffic System Events Router Events VPN Events User Events Endpoint Events HA Events Security Rating Events WiFi Events Compliance Events

User: admin Add Filter

#	Date/Time	Level	User	Message	Log Description
1	3 hours ago		admin	Administrator admin logged in successfully from https(192.168.1.205)	Admin login successful
2	3 hours ago		admin	Administrator admin timed out on https(192.168.1.205)	Admin logout successful
3	3 hours ago		admin	Administrator admin logged in successfully from https(192.168.1.205)	Admin login successful
4	13 hours ago		admin	Administrator admin logged out from https(192.168.1.10)	Admin logout successful
5	13 hours ago		admin	Administrator admin logged in successfully from https(192.168.1.10)	Admin login successful
6	Thursday		admin	Administrator admin logged out from https(192.168.1.10)	Admin logout successful
7	Thursday		admin	Administrator admin logged in successfully from https(192.168.1.10)	Admin login successful
8	Wednesday		admin	Administrator admin logged out from https(192.168.1.10)	Admin logout successful
9	Wednesday		admin	Administrator admin logged in successfully from https(192.168.1.10)	Admin login successful
10	Wednesday		admin	Configuration is changed in the admin session	Configuration changed
11	Wednesday		admin	Administrator admin timed out on https(192.168.1.101)	Admin logout successful
12	Wednesday		admin	Edit user.local autumn	Object attribute configured
13	Wednesday		admin	User admin changed local user autumn setting from GUI(192.168.1.101)	User changed
14	Wednesday		admin	Rename user.local autumn to autumn	Object configured
15	Wednesday		admin	Administrator admin logged in successfully from https(192.168.1.101)	Admin login successful
16	Tuesday		admin	Administrator admin logged out from https(192.168.1.10)	Admin logout successful
17	Tuesday		admin	Administrator admin logged in successfully from https(192.168.1.10)	Admin login successful
18	Tuesday		admin	Administrator admin timed out on https(192.168.1.218)	Admin logout successful
19	Tuesday		admin	Administrator admin logged in successfully from https(192.168.1.218)	Admin login successful
20	Monday		admin	Administrator admin logged out from https(192.168.1.10)	Admin logout successful
21	Monday		admin	Administrator admin logged in successfully from https(192.168.1.10)	Admin login successful

< > 1 /1 > [Total: 27]

Microsoft Office Home x FortiWiFi - FWF60FTK20000273 x fortinet 60f - Google Search x Fortinet FAD-60F | Fortinet Forti... x +

Not secure | 192.168.1.99/ng/log/view/user_events

FortiWiFi 60F FWF60FTK20000273

Network System Policy & Objects Security Profiles VPN User & Device WiFi & Switch Controller Log & Report Forward Traffic Local Traffic Sniffer Traffic System Events Router Events VPN Events User Events Endpoint Events HA Events Security Rating Events WiFi Events Compliance Events

User: autumn, dbernandez, dnelson Add Filter

#	Date/Time	Level	User	Action	Message	Group
1	20 hours ago		autumn	auth-logout	User autumn removed from auth logon	
2	20 hours ago		autumn	auth-logon	User autumn added to auth logon	
3	20 hours ago		autumn	auth-logout	User autumn removed from auth logon	
4	20 hours ago		autumn	auth-logon	User autumn added to auth logon	
5	Thursday		dnelson	auth-logout	User dnelson removed from auth logon	
6	Thursday		dnelson	auth-logon	User dnelson added to auth logon	
7	Thursday		autumn	auth-logout	User autumn removed from auth logon	
8	Thursday		dnelson	auth-logout	User dnelson removed from auth logon	
9	Thursday		dnelson	auth-logon	User dnelson added to auth logon	
10	Thursday		dbernandez	auth-logout	User dbernandez removed from auth logon	
11	Thursday		dbernandez	auth-logon	User dbernandez added to auth logon	
12	Thursday		dbernandez	auth-logout	User dbernandez removed from auth logon	
13	Thursday		dbernandez	auth-logon	User dbernandez added to auth logon	
14	Thursday		autumn	auth-logon	User autumn added to auth logon	
15	Thursday		dnelson	auth-logout	User dnelson removed from auth logon	
16	Thursday		dnelson	auth-logon	User dnelson added to auth logon	
17	Wednesday		autumn	auth-logout	User autumn removed from auth logon	
18	Wednesday		dnelson	auth-logout	User dnelson removed from auth logon	
19	Wednesday		autumn	auth-logon	User autumn added to auth logon	
20	Wednesday		dnelson	auth-logon	User dnelson added to auth logon	
21	Wednesday		dnelson	auth-logout	User dnelson removed from auth logon	

< > 1 /1 > [Total: 22]

Microsoft Office Home x FortiWiFi - FWF60FTK20000273 x fortinet 60f - Google Search x Fortinet FAD-60F | Fortinet Forti... x +

Not secure | 192.168.1.99/ng/log/view/security_rating

FortiWiFi 60F FWF60FTK20000273

Network > System > Policy & Objects > Security Profiles > VPN > User & Device > WiFi & Switch Controller > Log & Report > Forward Traffic > Local Traffic > Sniffer Traffic > System Events > Router Events > VPN Events > User Events > Endpoint Events > HA Events > Security Rating Events > WiFi Events > Compliance Events

#	Date/Time	Level	Log Description	Result	Security Score
1	3 hours ago	Security Rating summary	1 5 0 1 29	+380	
2	6 hours ago	Security Rating summary	1 5 0 1 29	+380	
3	10 hours ago	Security Rating summary	1 5 0 1 29	+380	
4	14 hours ago	Security Rating summary	1 5 0 1 29	+380	
5	18 hours ago	Security Rating summary	0 10 2 1 45	+640	
6	22 hours ago	Security Rating summary	0 11 2 1 44	+620	
7	Yesterday	Security Rating summary	0 10 2 1 45	+610	
8	Yesterday	Security Rating summary	0 10 2 1 45	+640	
9	Thursday	Security Rating summary	0 10 2 1 45	+640	
10	Thursday	Security Rating summary	0 10 2 1 45	+640	
11	Thursday	Security Rating summary	0 10 2 1 45	+640	
12	Thursday	Security Rating summary	0 10 2 1 45	+640	
13	Thursday	Security Rating summary	0 11 2 1 44	+600	
14	Thursday	Security Rating summary	0 10 2 1 45	+650	
15	Wednesday	Security Rating summary	0 11 2 1 44	+630	
16	Wednesday	Security Rating summary	0 11 2 1 44	+630	
17	Wednesday	Security Rating summary	0 10 2 1 45	+630	
18	Wednesday	Security Rating summary	0 11 2 1 44	+570	
19	Wednesday	Security Rating summary	0 10 2 1 45	+660	
20	Wednesday	Security Rating summary	0 10 2 1 45	+660	
21	Tuesday	Security Rating summary	0 10 2 1 45	+660	

https://192.168.1.99/ng/log/view/security_rating

Type here to search

81°F 10:08 AM 8/7/2021

Microsoft Office Home x FortiWiFi - FWF60FTK20000273 x fortinet 60f - Google Search x Fortinet FAD-60F | Fortinet Forti... x +

Not secure | 192.168.1.99/ng/log/view/compliance

FortiWiFi 60F FWF60FTK20000273

Router Events > VPN Events > User Events > Endpoint Events > HA Events > Security Rating Events > WiFi Events > Compliance Events > AntiVirus > Web Filter > DNS Query > Application Control > Intrusion Prevention > Anomaly > Learning Report > FortiCloud Reports > Log Settings > Threat Weight > Email Alert Settings > Monitor

#	Date/Time	Level	Message	Result
1	10 hours ago	Check SSH-SSL deep inspection with WF enabled drops traffic from servers with invalid server certificates	✓	
2	10 hours ago	Check that Spyware / Malicious sites are being blocked by a WF policy	✗	
3	10 hours ago	Check that Phishing-related sites are being blocked by a WF policy	✗	
4	10 hours ago	Check that Bot net-related sites are being blocked by a WF policy	✗	
5	10 hours ago	Check that proxy related sites are being blocked by a WF policy	✗	
6	10 hours ago	Check that Hacking-related sites are being blocked by a WF policy	✗	
7	10 hours ago	Check that Spam-related sites are being blocked by a WF policy	✗	
8	10 hours ago	Check that P2P file sharing sites-related sites are being blocked by a WF policy	✗	
9	10 hours ago	Check that the IPS module has an updated IPS signature package	✓	
10	10 hours ago	Check that FGT performs IPS inspection on all traffic	✗	
11	10 hours ago	Check that there are no general exclusions to the activated IPS protections	✗	
12	10 hours ago	Check that the IPS Profile includes Protocol Anomalies protections	✗	
13	10 hours ago	Check the Severity-based Protections in the IPS Policy	✗	
14	10 hours ago	Check the IPS protection is enabled on Firewall policy	✗	
15	10 hours ago	Check the default IPS profiles have the default action set to block	✗	
16	10 hours ago	Check that all audit trails include date, time and user identification	✓	
17	10 hours ago	Check the dropped out-of-state TCP packets are logged	✓	
18	10 hours ago	Check that a message is displayed to locked out Administrators	✓	
19	10 hours ago	Check that Administrators' accounts are unlocked after 30 minutes	✗	
20	10 hours ago	Check that Administrators are locked out after 3 login failures	✓	
21	10 hours ago	Check that each Firewall rule has a Comment defined	✗	

Type here to search

81°F 10:09 AM 8/7/2021

Microsoft Office Home x FortiWiFi - FWF60FTK20000273 x fortinet 60f - Google Search x Fortinet FAD-60F | Fortinet Forti... x

192.168.1.99/ng/log/view/av

FortiWiFi 60F FWF60FTK20000273

Router Events VPN Events User Events Endpoint Events HA Events Security Rating Events WiFi Events Compliance Events **AntiVirus** Web Filter DNS Query Application Control Intrusion Prevention Anomaly Learning Report FortiCloud Reports Log Settings Threat Weight Email Alert Settings Monitor

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20

#	Date/Time	Service	Source	File Name	Virus/Botnet	User
1	Thursday	SMB	Icladmin (192.168.1.100)	FortiFone Import Onopa Directory.xlsx		Icladmin
2	Thursday	CIFS	192.168.1.100	FortiFone Import Onopa Directory.xlsx		
3	Thursday	SMB	Icladmin (192.168.1.100)	FortiFone Import Onopa Directory.xlsx		Icladmin
4	Thursday	CIFS	192.168.1.100	FortiFone Import Onopa Directory.xlsx		
5	Thursday	SMB	Icladmin (192.168.1.100)	FortiFone Import Onopa Directory.xlsx		Icladmin
6	Thursday	CIFS	192.168.1.100	FortiFone Import Onopa Directory.xlsx		
7	Thursday	SMB	Icladmin (192.168.1.100)	FortiFone Import Onopa Directory.xlsx		Icladmin
8	Thursday	CIFS	192.168.1.100	FortiFone Import Onopa Directory.xlsx		
9	Thursday	CIFS	192.168.1.100	FortiFone Import Onopa Directory.xlsx		
10	Thursday	SMB	Icladmin (192.168.1.100)	FortiFone Import Onopa Directory.xlsx		Icladmin
11	Thursday	SMB	Icladmin (192.168.1.100)	FortiFone Import Onopa Directory.xlsx		Icladmin
12	Thursday	SMB	Icladmin (192.168.1.100)	FortiFone Import Onopa Directory.xlsx		Icladmin
13	Wednesday	CIFS	192.168.1.100	ARB Cyber Threat Intelligence and Incident Response Report.pdf		
14	Wednesday	CIFS	192.168.1.100	21-X-0358 Vulnerability Assessment White Paper USAF Red Team FINAL.pdf		
15	Wednesday	CIFS	192.168.1.100	Mr. Sullivan's Resume updated.pdf		
16	Wednesday	CIFS	192.168.1.100	AOWC Cyber Threat Intelligence and Incident Response Report.pdf		
17	Wednesday	SMB	Icladmin (192.168.1.100)	21-X-0358 Vulnerability Assessment White Paper USAF Red Team FINAL.pdf		Icladmin
18	Wednesday	SMB	Icladmin (192.168.1.100)	Mr. Sullivan's Resume updated.pdf		Icladmin
19	Wednesday	SMB	Icladmin (192.168.1.100)	ARB Cyber Threat Intelligence and Incident Response Report.pdf		Icladmin
20	Wednesday	SMB	Icladmin (192.168.1.100)	AOWC Cyber Threat Intelligence and Incident Response Report.pdf		Icladmin

1 /1 [Total: 20]

Microsoft Office Home x FortiWiFi - FWF60FTK20000273 x fortinet 60f - Google Search x Fortinet FAD-60F | Fortinet Forti... x

192.168.1.99/ng/dhcp/monitor

FortiWiFi 60F FWF60FTK20000273

Network System Policy & Objects Security Profiles VPN User & Device WiFi & Switch Controller Log & Report **Monitor** Routing Monitor DHCP Monitor SD-WAN Monitor IPsec Monitor SSL-VPN Monitor Firewall User Monitor Quarantine Monitor FortiClient Monitor WiFi Client Monitor Rogue AP Monitor WiFi Health Monitor

Refresh Revoke Reservation

Interface	Device	MAC	IP	Host Information	Expires	Status
lan	FortiAP	e0:23:ff:ef:1e:dc	192.168.1.213	VCI: FortiAP-FC24JE Hostname: FortiAP	2021/08/14 05:42:28	Leased out
lan	HPECC622	48:0f:cf:a6:e8:d7	192.168.1.201	VCI: Hewlett-Packard OfficeJet Hostname: HPECC622	2021/08/13 20:08:32	Leased out
lan	ANDRE	e0:2b:e9:f4:99:6c	192.168.1.219	VCI: MSFT 5.0 Hostname: ANDRE	2021/08/13 16:59:02	Leased out
lan	David_PC	b4:ae:2b:39:9e:7d	192.168.1.200	VCI: MSFT 5.0 Hostname: DAVID	2021/08/13 13:28:22	Leased out
lan	ENGINEERING1	a4:bb:6d:d9:32:87	192.168.1.205	VCI: MSFT 5.0 Hostname: ENGINEERING1	2021/08/13 13:08:23	Leased out
lan	Lucass-MacBook-Pro	38:f9:d3:c6:df:36	192.168.1.230	Hostname: Lucass-MBP	2021/08/13 12:00:07	Leased out
lan	Zacharys-MacBook-Pro	38:f9:d3:c6:45:70	192.168.1.215	Hostname: Zacharys-MBP	2021/08/13 11:57:47	Leased out
lan	WIN-74KB634JUQI	8c:c8:4b:21:cc:05	192.168.1.207	VCI: MSFT 5.0 Hostname: DESKTOP-4KHPPKN	2021/08/13 11:55:27	Leased out
lan	04:d5:90:16:74:e2	04:d5:90:16:74:e2	192.168.1.214		2021/08/13 10:10:51	Leased out
lan	04:d5:90:16:74:e9	04:d5:90:16:74:e9	192.168.1.229		2021/08/13 10:10:08	Leased out
lan	04:d5:90:16:71:94	04:d5:90:16:71:94	192.168.1.225	VCI: FortiFone FON-175	2021/08/13 10:09:36	Leased out
lan	S124EN5920019922	e0:23:ff:96:a3:da	192.168.1.227	VCI: FortiSwitch-124E Hostname: S124EN5920019922	2021/08/12 22:21:31	Leased out

10:15 AM 8/7/2021

Microsoft Office Home x FortiWiFi - FWF60FTK20000273 x fortinet 60f - Google Search x Fortinet FAD-60F | Fortinet Forti... x +

Not secure | 192.168.1.99/ng/vpn/ssl/monitor

FortiWiFi 60F FWF60FTK20000273

admin

- Network
- System
- Policy & Objects
- Security Profiles
- VPN
- User & Device
- WiFi & Switch Controller
- Log & Report
- Monitor
 - Routing Monitor
 - DHCP Monitor
 - SD-WAN Monitor
 - IPsec Monitor
 - SSL-VPN Monitor**
 - Firewall User Monitor
 - Quarantine Monitor
 - FortiClient Monitor
 - WiFi Client Monitor
 - Rogue AP Monitor
 - WiFi Health Monitor

Refresh

Username	Last Login	Remote Host	Active Connections
lcladmin	2021/08/07 08:24:14	71.46.253.149	Tunnel: 192.168.1.100

1 / 1 [Total: 1]

Type here to search

Microsoft Office Home x FortiWiFi - FWF60FTK20000273 x fortinet 60f - Google Search x Fortinet FAD-60F | Fortinet Forti... x +

Not secure | 192.168.1.99/ng/wifi/health-monitor/dashboard

FortiWiFi 60F FWF60FTK20000273

admin

- Network
- System
- Policy & Objects
- Security Profiles
- VPN
- User & Device
- WiFi & Switch Controller
- Log & Report
- Monitor
 - Routing Monitor
 - DHCP Monitor
 - SD-WAN Monitor
 - IPsec Monitor
 - SSL-VPN Monitor
 - Firewall User Monitor
 - Quarantine Monitor
 - FortiClient Monitor
 - WiFi Client Monitor
 - Rogue AP Monitor
 - WiFi Health Monitor**

Active Clients

Both

- FWF60F-WIFI0
- FC24JE5920012023

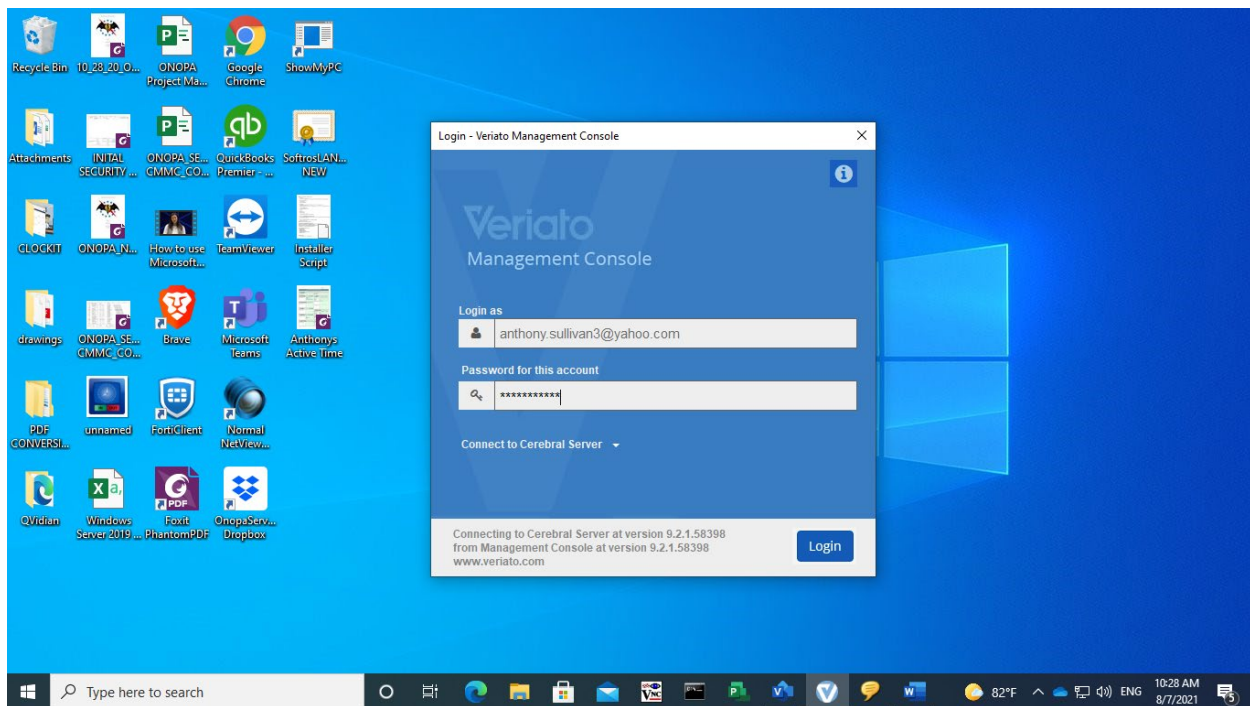
1 1

Total active clients 2

AP Status

- Uptime > 24 hours
- Rebooted within 24 hours
- Down/Missing

2



Home - Veriato Management Console

Veriato Cerebral

Maintenance has expired. Renew now to update.

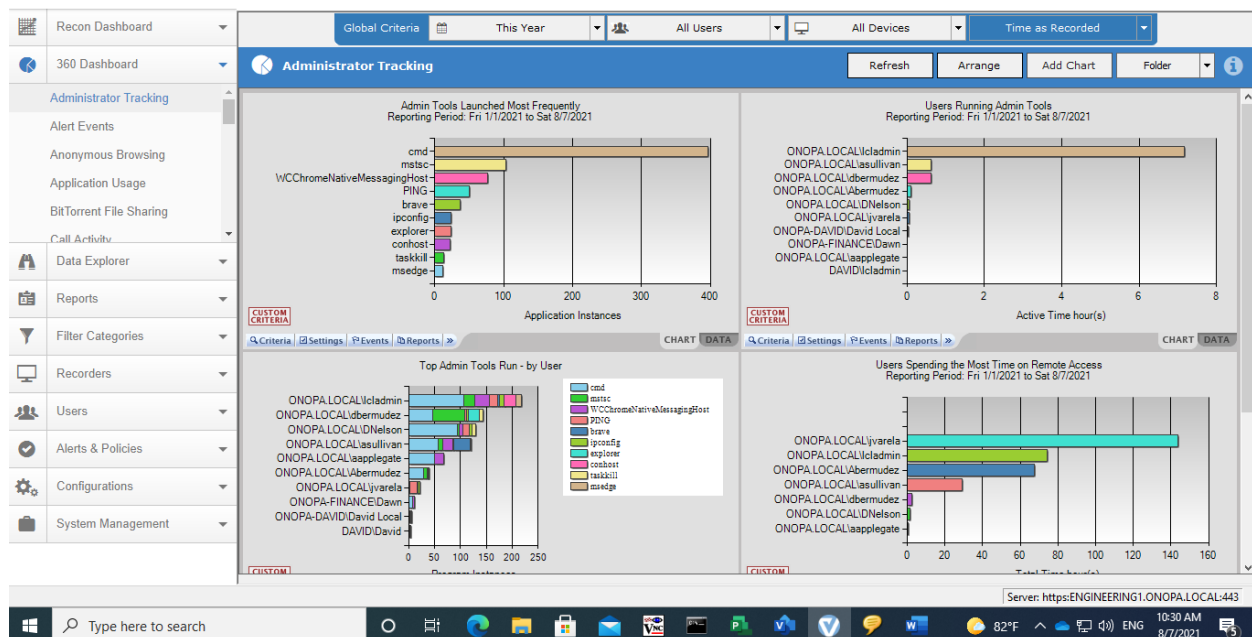
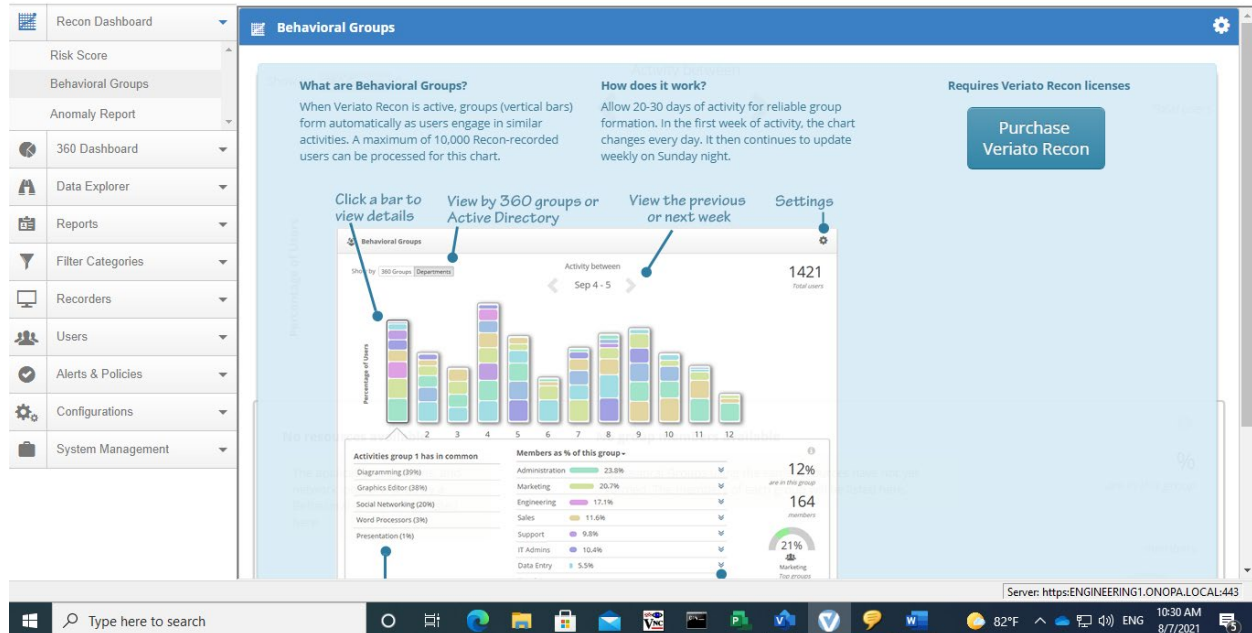
Showing: 08/06/2021 All Groups Selected in this group: Abermudez

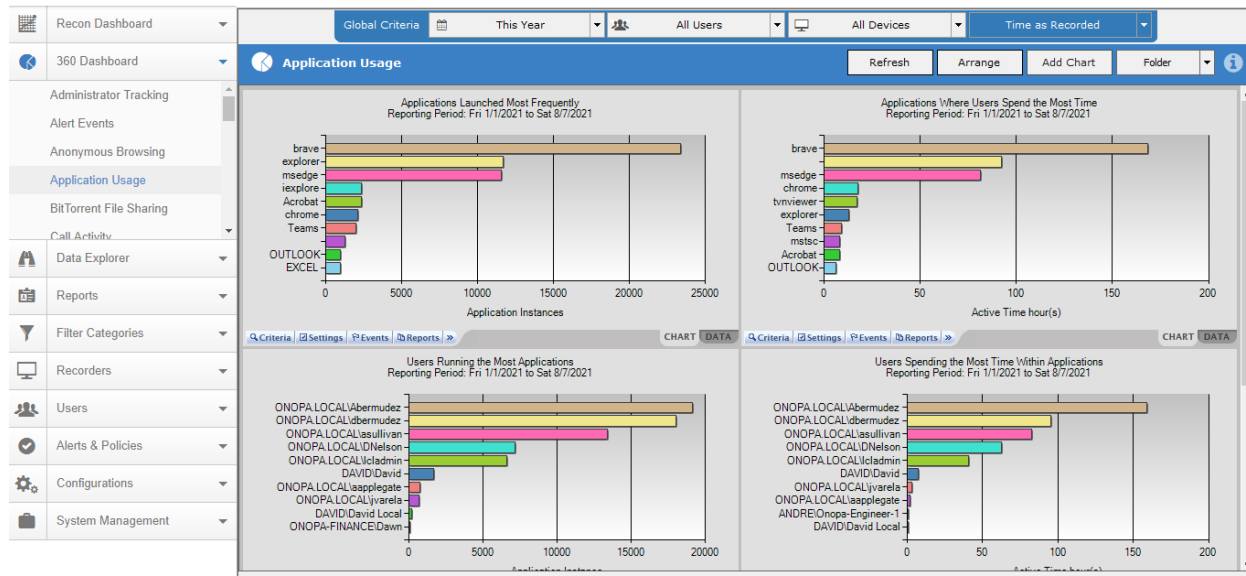
Top Risk Scores (All)

SCORES IN EACH LEVEL ON 08/06/2021: HIGH RISK 0 POSSIBLE RISK 0 LOW RISK 4

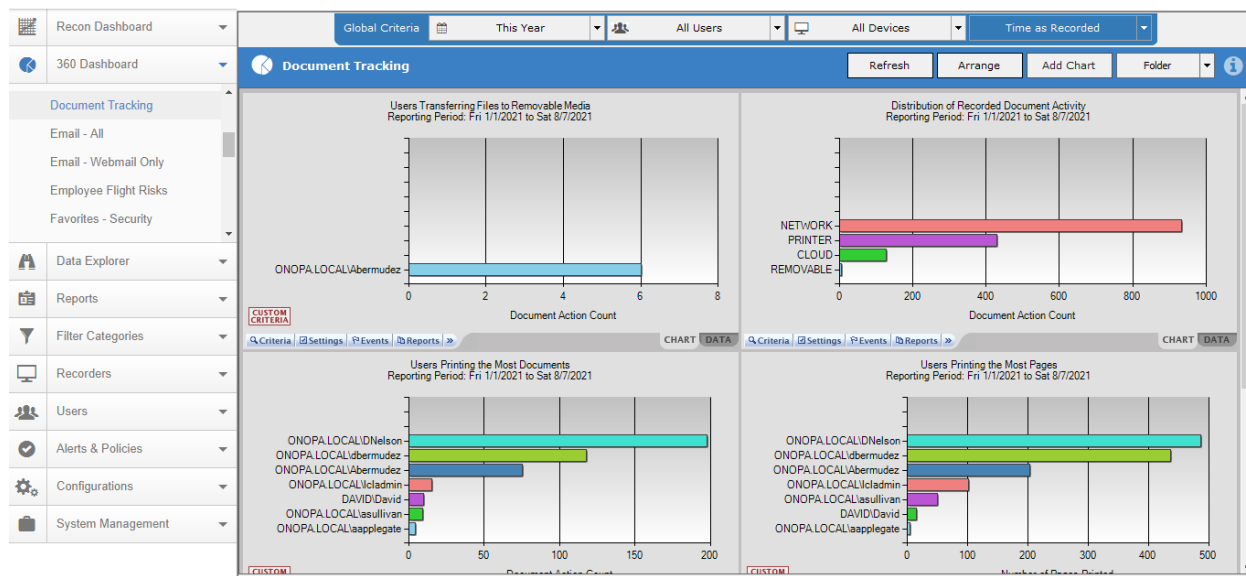
NAME	TREND	SCORE	Accidental Leak	Espionage	Financial Fraud	Opportunistic Data...	Sabotage
Abermudez	▲	22					
DNelson	▼	-0					
lcladmin	▼	-0					
dbermudez	▼	0					

Server: https://ENGINEERING1.ONOPA.LOCAL:443

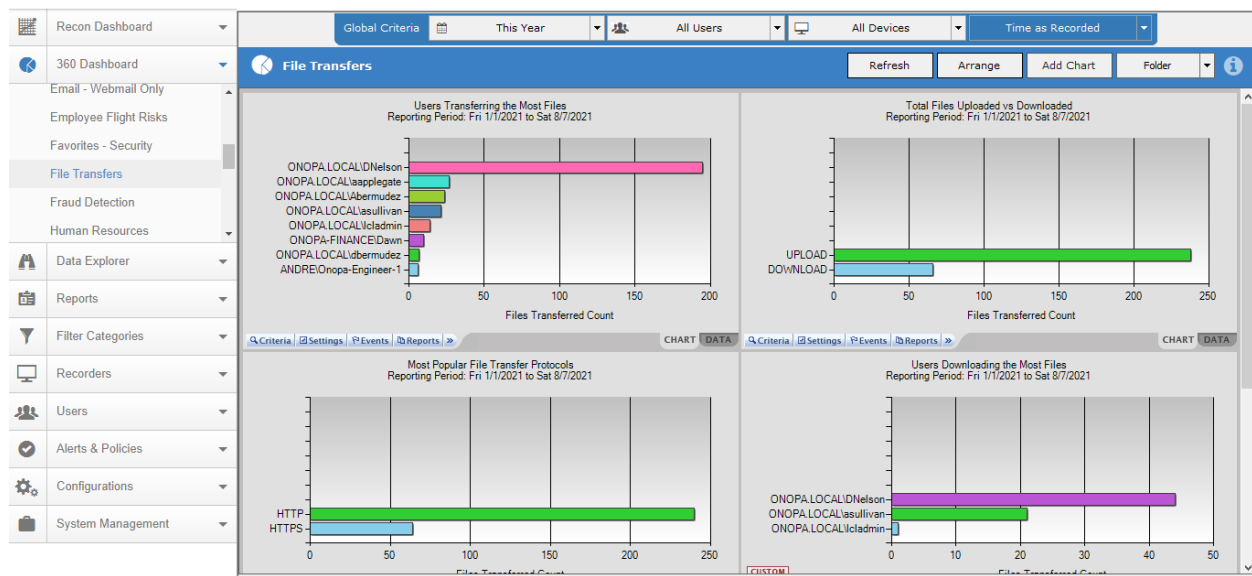
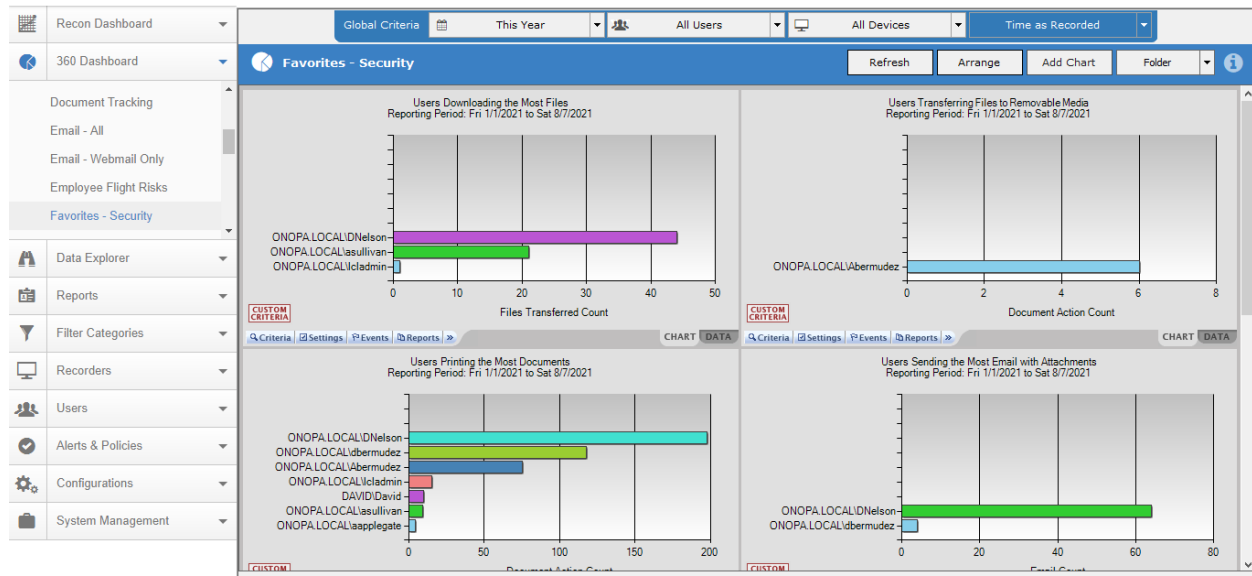


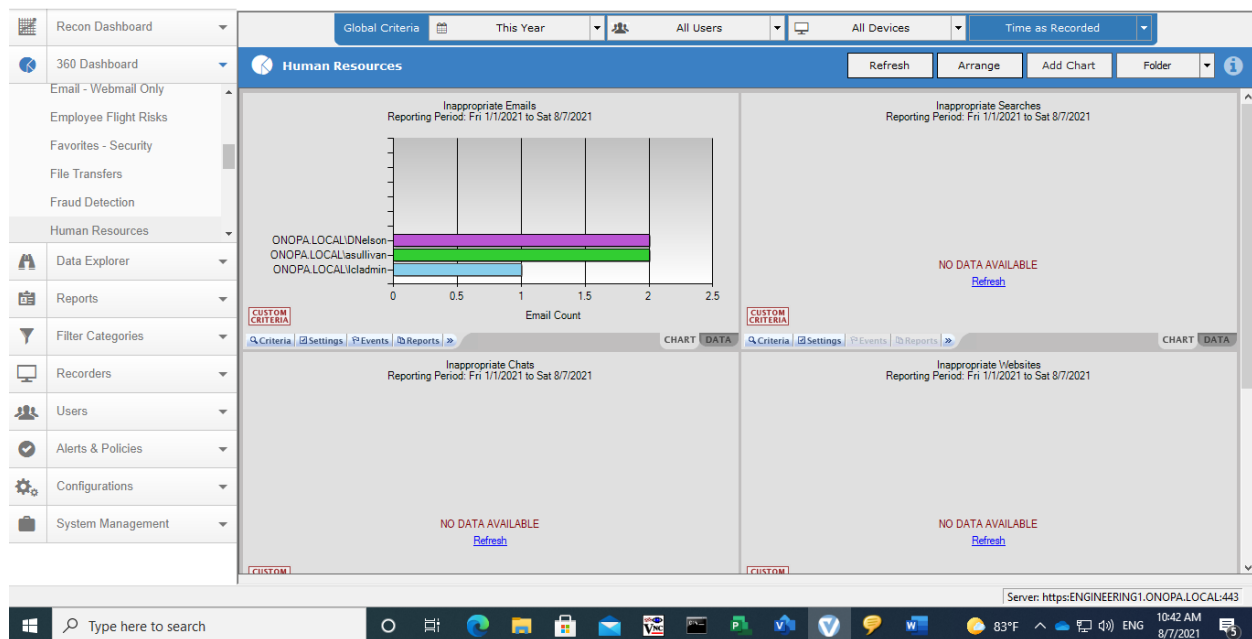
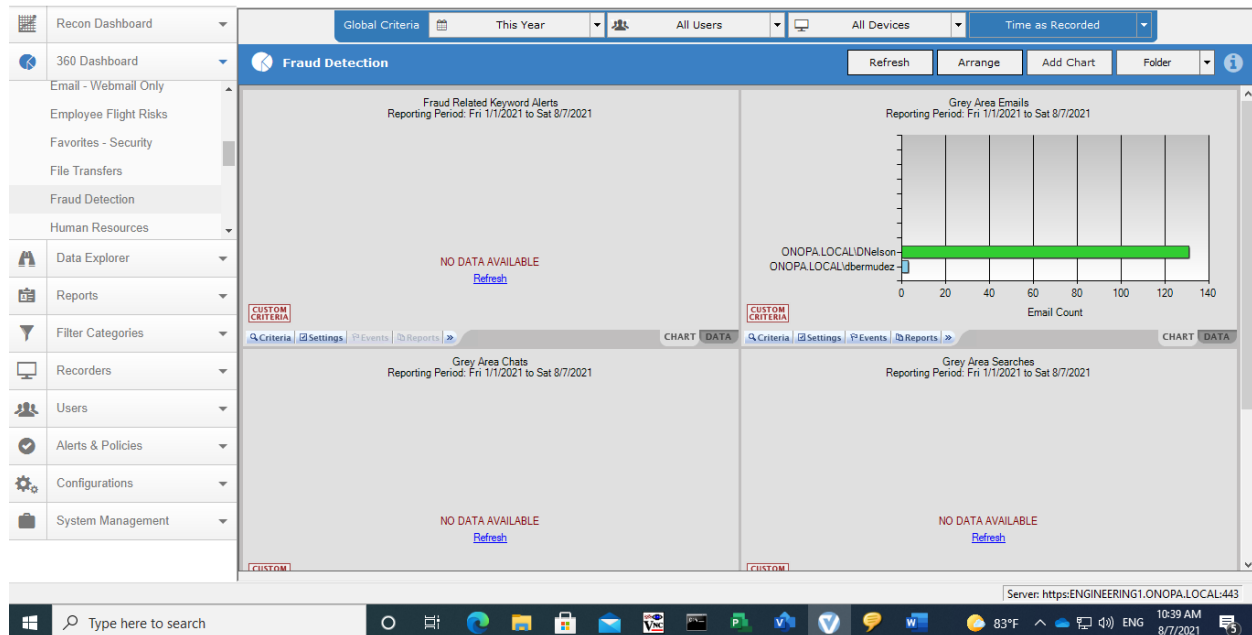


Server: https://ENGINEERING1.ONOPA.LOCAL:443



Server: https://ENGINEERING1.ONOPA.LOCAL:443





Inappropriate Emails - Events

File Edit View Data Windows

Navigate

- Load Events
- Criteria
- Grouping

Summary

Name	Events	In	Out	Attachments
Count:				

Events (Email Events => ONOPA.LOCAL\asullivan => 05/29/2021 - Fri)

Recorded T...	Device	Application	Attach...	Sent/Recei...	Type	From Name	From Address	To	Subject	CC	BC
10:02:31 AM	ENGINEER1...	OUTLOOK	0	Rcvd	MAPI	Isaac Elyahou	success@at...	IT Departm...	[VIDEO] Tic...		
10:02:31 AM	ENGINEER1...	OUTLOOK	0	Rcvd	MAPI	Proofpoint ...	do-not-repl...	IT Departm...	Quarantine ...		

Record 2 of 2

"Fortinet"
bounce-63730.html-27385936-85245-514006124-821213@bounce.s11.exacttarget.com

How to handle a ransomware attack

27 May 21 - 09:53 AM

[Preview](#)
[Release](#)
[Release & Approve](#)
[Block](#)

Inappropriate Searches
Reporting Period: Fri 1/1/2021 to Sat 8/7/2021

NO DATA AVAILABLE
[Refresh](#)

Inappropriate Websites
Reporting Period: Fri 1/1/2021 to Sat 8/7/2021

NO DATA AVAILABLE
[Refresh](#)

Server: https://ENGINEERING1.ONOPA.LOCAL:443

Recon Dashboard

Global Criteria This Year All Users All Devices Time as Recorded

Keystrokes

Refresh Arrange Add Chart Folder

Users Typing the Most Keystrokes
Reporting Period: Fri 1/1/2021 to Sat 8/7/2021

User	Formatted Keystroke Count
ONOPA.LOCAL\bermudez	~90000
ONOPA.LOCAL\bermudez	~85000
ONOPA.LOCAL\asullivan	~25000
ONOPA.LOCAL\cladmin	~20000
ONOPA.LOCAL\cladmin	~15000
ONOPA.LOCAL\cladmin	~10000
ONOPA.LOCAL\cladmin	~5000
ONOPA.LOCAL\cladmin	~2000
ONOPA.LOCAL\cladmin	~1000
ONOPA.LOCAL\cladmin	~500
ONOPA.LOCAL\cladmin	~200
ONOPA.LOCAL\cladmin	~100
ONOPA.LOCAL\cladmin	~50
ONOPA.LOCAL\cladmin	~20
ONOPA.LOCAL\cladmin	~10
ONOPA.LOCAL\cladmin	~5
ONOPA.LOCAL\cladmin	~2
ONOPA.LOCAL\cladmin	~1
ONOPA.LOCAL\cladmin	~0

Programs Receiving the Most Keystrokes Typed
Reporting Period: Fri 1/1/2021 to Sat 8/7/2021

Program	Formatted Keystroke Count
msedge	~85000
brave	~80000
brave	~75000
brave	~70000
brave	~65000
brave	~60000
brave	~55000
brave	~50000
brave	~45000
brave	~40000
brave	~35000
brave	~30000
brave	~25000
brave	~20000
brave	~15000
brave	~10000
brave	~5000
brave	~2000
brave	~1000
brave	~500
brave	~200
brave	~100
brave	~50
brave	~20
brave	~10
brave	~5
brave	~2
brave	~1
brave	~0

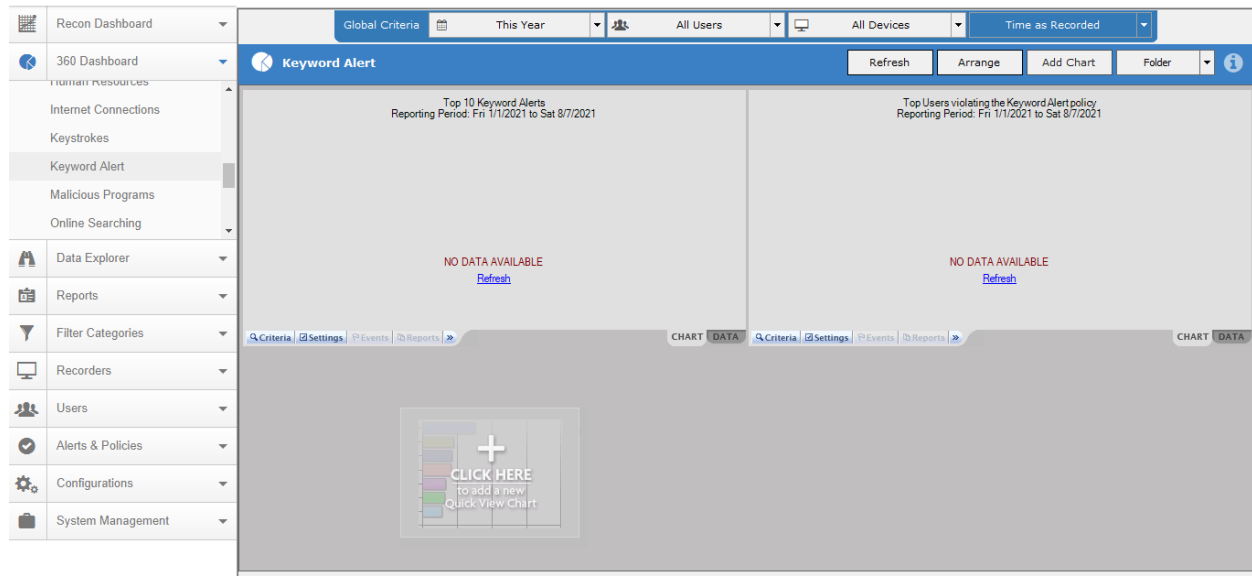
Trend of Keystrokes Typed (Last 10 Days)
Reporting Period: Wed 7/28/2021 to Sat 8/7/2021

Keystroke Count

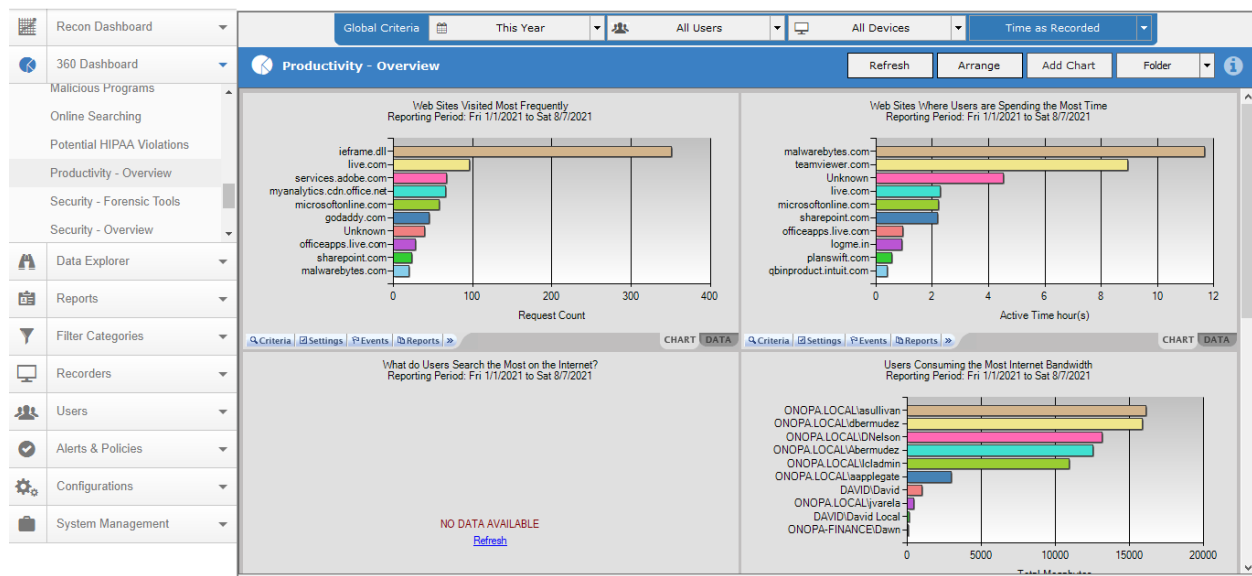
BANDWIDTH
Reporting Period: Fri 1/1/2021 to Sat 8/7/2021

Domain	Total Keystrokes
dropbox.com	~9000
blob.core.windows.net	~8500
office365.com	~8000
ENGINEERING1	~7500
office.com	~7000
teams.cdn.office.net	~6500
sharepoint.com	~6000
ONOPA.LOCAL	~5500
officeapps.live.com	~5000

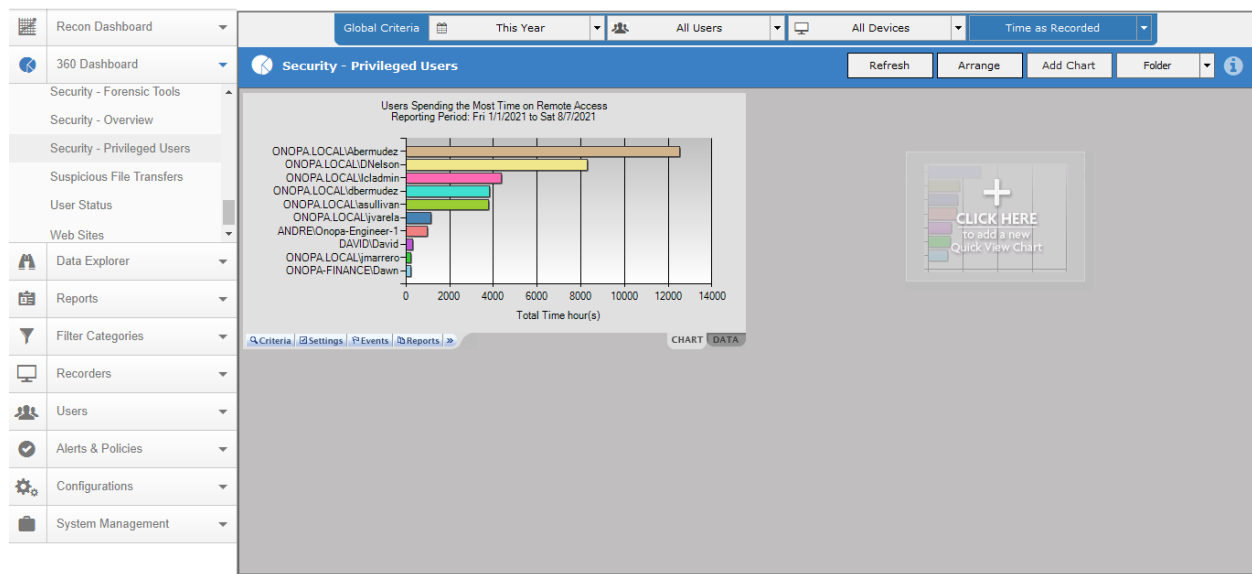
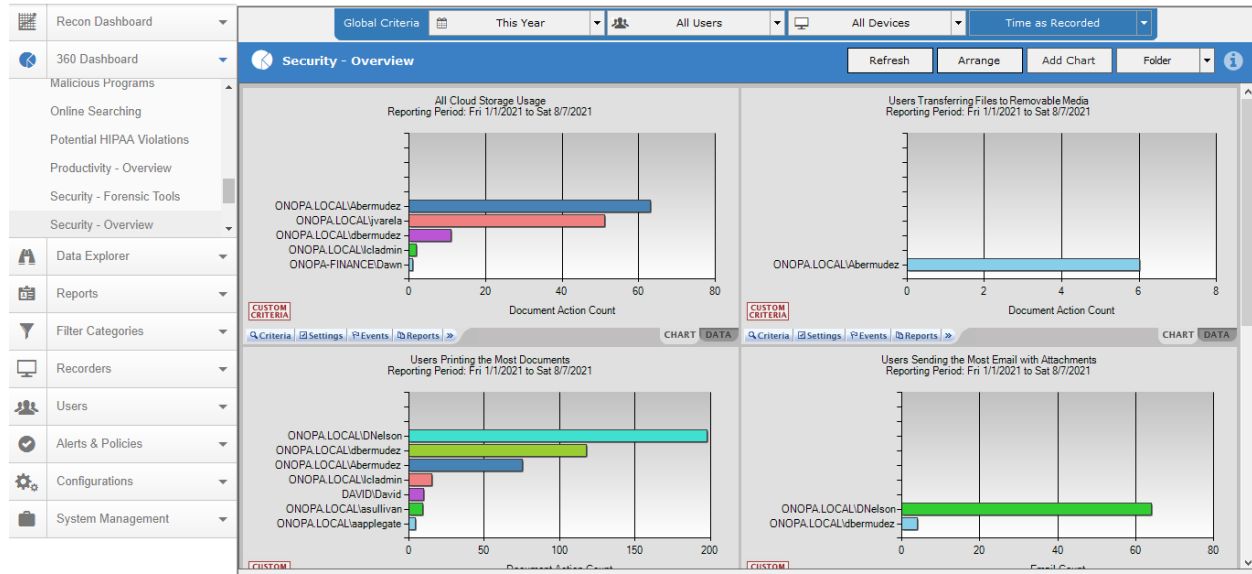
Server: https://ENGINEERING1.ONOPA.LOCAL:443



Server: https://ENGINEERING1.ONOPA.LOCAL:443



Server: https://ENGINEERING1.ONOPA.LOCAL:443



Recon Dashboard

360 Dashboard

Security - Forensic Tools

Security - Overview

Security - Privileged Users

Suspicious File Transfers

User Status

Web Sites

Data Explorer

Reports

Filter Categories

Recorders

Users

Alerts & Policies

Configurations

System Management

Global Criteria

This Year

All Users

All Devices

Time as Recorded

Suspicious File Transfers

Refresh

Arrange

Add Chart

Folder

Email Activity after Business Hours
Reporting Period: Thu 8/22/2013 to Mon 12/2/2013 between 7:00 PM and 11:59 PM

NO DATA AVAILABLE
[Refresh](#)

Custom Criteria

Criteria Settings Events Reports

CHART DATA

Email Activity before Business Hours
Reporting Period: Thu 8/22/2013 to Mon 12/2/2013 between 12:00 AM and 7:00 AM

NO DATA AVAILABLE
[Refresh](#)

Custom Criteria

Criteria Settings Events Reports

CHART DATA

Chat Activity after Business Hours
Reporting Period: Thu 8/22/2013 to Mon 12/2/2013 between 7:00 PM and 11:59 PM

NO DATA AVAILABLE
[Refresh](#)

Custom Criteria

Criteria Settings Events Reports

CHART DATA

Chat Activity before Business Hours
Reporting Period: Thu 8/22/2013 to Mon 12/2/2013 between 12:00 AM and 7:00 AM

NO DATA AVAILABLE
[Refresh](#)

Custom Criteria

Criteria Settings Events Reports

CHART DATA

Server: https://ENGINEERING1.ONOPA.LOCAL:443

Recon Dashboard

360 Dashboard

Security - Forensic Tools

Security - Overview

Security - Privileged Users

Suspicious File Transfers

User Status

Web Sites

Data Explorer

Reports

Filter Categories

Recorders

Users

Alerts & Policies

Configurations

System Management

Global Criteria

This Year

All Users

All Devices

Time as Recorded

User Status

Refresh

Arrange

Add Chart

Folder

User Time Sheet
ONOPA.LOCAL\vaullkvan

Device	Date	8 AM	9 AM	10 AM	11 AM	12 PM	1 PM	2 PM	3 PM	4 PM	5 PM
DC1	01/18/2021 - Mo										
DC2	01/18/2021 - Mo										
DC2	01/15/2021 - Fri										
DC2	01/14/2021 - Thu										
DC2	01/13/2021 - W										
ENGINEERING1	01/18/2021 - Mo										
ENGINEERING1	01/15/2021 - Fri										
ENGINEERING1	01/14/2021 - Thu										

Zoom: 100%

Logged In & Active

Logged In & Inactive

Recording Interrupted

Clock Change

Criteria Settings Events Reports

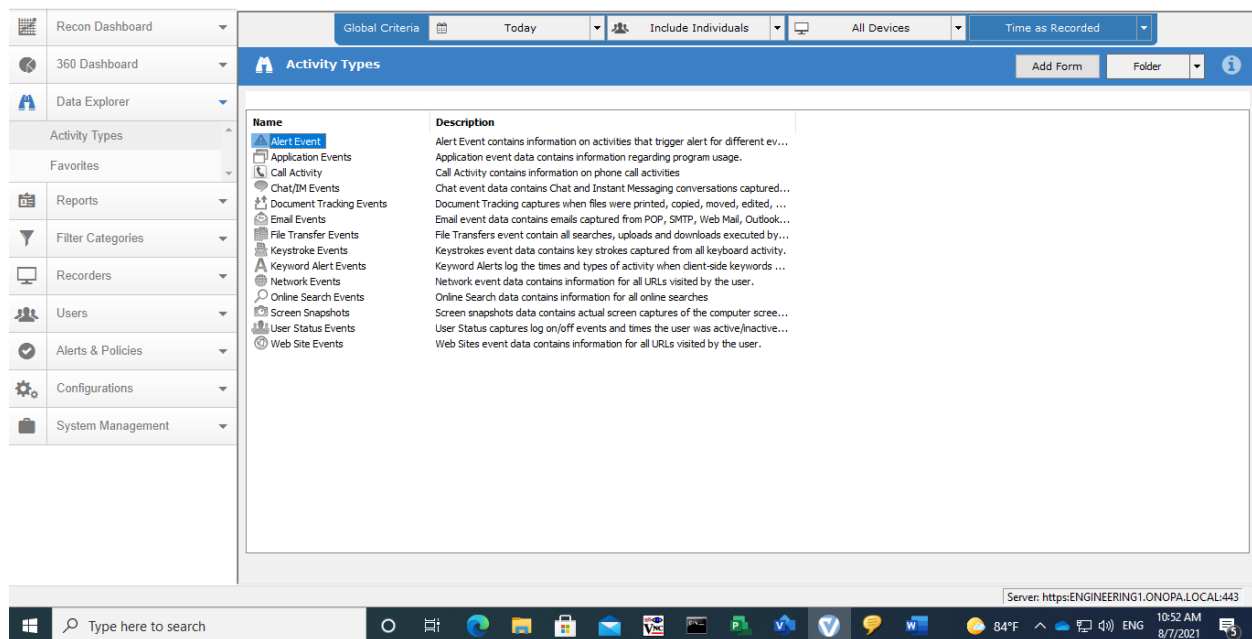
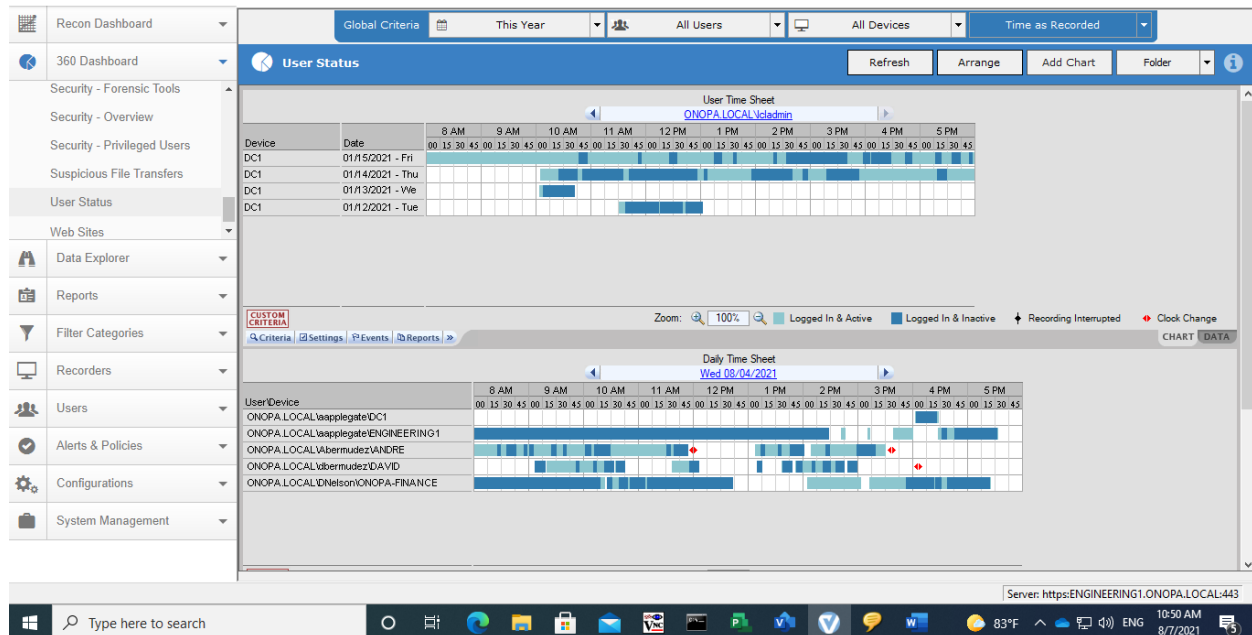
CHART DATA

Daily Time Sheet
Sat 08/07/2021

User/Device	8 AM	9 AM	10 AM	11 AM	12 PM	1 PM	2 PM	3 PM	4 PM	5 PM
N/A										

No Data Available for this Date

Server: https://ENGINEERING1.ONOPA.LOCAL:443



Application Events

FileEditViewDataWindows

Summary

Load EventsCriteriaGrouping

Load EventsPrintExportShow Columns

Application Events

ANDRE\Onopa-Engineer-1

DAVID\David

DAVID\David Local

DAVID\ldadmin

ONOPA-DAVID\David Local

ONOPA-FINANCE\Dawn

ONOPA.LOCAL\aspplegate

ONOPA.LOCAL\abermudez

ONOPA.LOCAL\asullivan

ONOPA.LOCAL\abermudez

ONOPA.LOCAL\Nelson

ONOPA.LOCAL\lmarrero

ONOPA.LOCAL\lvarela

ONOPA.LOCAL\ldadmin

Name	Events	Instances	Active Time	Focus Time	Total Time
ANDRE\Ono...	79	79	0:47:01	0:53:15	971:01:18
DAVID\David	1,677	1,677	7:20:57	9:16:25	289:34:55
DAVID\David Local	180	180	0:39:11	0:59:13	35:54:44
DAVID\ldadmin	48	48	0:12:35	0:12:35	1:43:42
ONOPA-DAVID\David Local	740	740	1:52:50	4:33:08	116:14:35
ONOPA-LO...	19,140	19,140	159:14:28	270:06:09	12524:11:43
ONOPA-LO...	13,397	13,397	82:42:48	170:46:16	3777:33:10
ONOPA-LO...	18,020	18,020	95:23:05	135:15:12	3816:25:33
ONOPA-LO...	7,139	7,139	62:14:20	629:57:39	8311:55:23
ONOPA-LO...	8	8	0:00:59	0:11:13	228:38:27
ONOPA-LO...	672	672	2:59:11	71:20:48	1129:49:03
ONOPA-LO...	6,591	6,591	40:34:53	122:05:24	4372:42:18
ONOPA-DA...	25	25	0:09:40	0:09:40	2:11:32
ONOPA-FIN...	87	87	0:31:43	1:03:17	200:02:40
Count: 14	67,803	67,803	454:43:41	1416:50:14	35777:59:03

Events (Application Events)

View Screen SnapshotsPrintExportShow Columns

Start Time	Device	Application	Application ...	Active Time	Focus Time	Total Time	Window Ca...	Platform	View Screenshot
------------	--------	-------------	-----------------	-------------	------------	------------	--------------	----------	-----------------

To view events, select a specific item above and click the Load Events button. To drill down on an item, click on the tree [-] button, or double click on the item.

Record 0 of 0

Application Events

FileEditViewDataWindows

Summary

Load EventsCriteriaGrouping

Load EventsPrintExportShow Columns

Application Events

ANDRE\Onopa-Engineer-1

DAVID\David

DAVID\David Local

DAVID\ldadmin

ONOPA-DAVID\David Local

ONOPA-FINANCE\Dawn

ONOPA.LOCAL\aspplegate

ONOPA.LOCAL\abermudez

ONOPA.LOCAL\asullivan

ONOPA.LOCAL\abermudez

ONOPA.LOCAL\Nelson

ONOPA.LOCAL\lmarrero

ONOPA.LOCAL\lvarela

ONOPA.LOCAL\ldadmin

08/07/2021 - Sat

08/06/2021 - Fri

Name	Events	Instances	Active Time	Focus Time	Total Time
01/12/2021...	19	19	0:04:35	0:11:14	1:28:05
01/13/2021...	20	20	0:05:30	0:05:30	32:29:37
01/14/2021...	304	304	4:38:55	10:18:21	327:54:40
01/15/2021...	839	839	8:37:14	15:46:04	161:21:02
01/31/2021...	1	1	0:00:00	0:00:00	11:56:30
02/04/2021...	7	7	0:00:00	0:00:00	16:07:37
02/05/2021...	1	1	0:00:00	0:00:00	0:00:01
02/06/2021...	1	1	0:00:00	0:00:00	20:27:25
02/07/2021...	1	1	0:00:00	0:00:00	16:07:36
02/09/2021...	2	2	0:00:00	0:00:00	0:26:00
02/21/2021...	5	5	0:01:41	0:01:41	0:21:08
02/22/2021...	6	6	0:00:10	0:00:10	0:00:22
02/24/2021...	21	21	0:14:34	0:14:34	0:30:04
02/27/2021...	1	1	0:00:00	0:00:00	10:11:17
Count: 73	6,591	6,591	40:34:53	122:05:24	4372:42:18

Events (Application Events -> ONOPA.LOCAL\ldadmin -> 01/12/2021 - Tue)

View Screen SnapshotsPrintExportShow Columns

Start Time	Device	Application	Application ...	Active Time	Focus Time	Total Time	Window Ca...	Platform	View Screenshot
11:34:10 AM	DC1	brave	01/12/2021...	0:00:00	0:00:00	0:00:01	localhost:9...	Windows S...	View Screen Snapshots
11:34:28 AM	DC1	brave	01/12/2021...	0:00:00	0:00:00	0:00:00	Untitled - Br...	Windows S...	View Screen Snapshots
11:37:16 AM	DC1	explorer	01/12/2021...	0:00:00	0:00:00	0:00:20	Internet Ex...	Windows S...	View Screen Snapshots
12:16:23 PM	DC1	explorer	01/12/2021...	0:00:00	0:00:00	0:00:00	Users (\DC2)	Windows S...	View Screen Snapshots
12:16:29 PM	DC1	explorer	01/12/2021...	0:00:00	0:00:00	0:00:00	ldadmin	Windows S...	View Screen Snapshots
11:34:08 AM	DC1	brave	01/12/2021...	0:00:01	0:00:01	0:00:02	Untitled - Br...	Windows S...	View Screen Snapshots
12:16:29 PM	DC1	explorer	01/12/2021...	0:00:01	0:00:01	0:00:02	Favorites	Windows S...	View Screen Snapshots
12:16:31 PM	DC1	explorer	01/12/2021...	0:00:02	0:00:02	0:00:03	ldadmin	Windows S...	View Screen Snapshots
12:16:34 PM	DC1	explorer	01/12/2021...	0:00:02	0:00:02	0:00:02	Documents	Windows S...	View Screen Snapshots
12:43:07 PM	DC1	explorer	01/12/2021...	0:00:02	0:00:02	0:00:03	Videos	Windows S...	View Screen Snapshots
12:16:18 PM	DC1	explorer	01/12/2021...	0:00:05	0:00:05	0:00:05	DC2	Windows S...	View Screen Snapshots
12:16:23 PM	DC1	explorer	01/12/2021...	0:00:06	0:00:06	0:00:06	Users	Windows S...	View Screen Snapshots
12:15:53 PM	DC1	explorer	01/12/2021...	0:00:09	0:00:09	0:00:09	File Explorer	Windows S...	View Screen Snapshots

Record 1 of 19

Application Events

File Edit View Data Windows

Navigate

Load Events Criteria Grouping

Summary

Load Events Print Export Show Columns

Name	Events	Instances	Active Time	Focus Time	Total Time
01/12/2021...	19	19	0:04:35	0:11:14	1:28:05
01/13/2021...	20	20	0:05:30	0:05:30	32:29:37
01/14/2021...	304	304	4:38:55	10:18:21	327:54:40
01/15/2021...	839	839	8:37:14	15:46:04	161:21:02
01/31/2021...	1	1	0:00:00	0:00:00	11:56:30
02/04/2021...	7	7	0:00:00	0:00:00	16:07:37
02/05/2021...	1	1	0:00:00	0:00:00	0:00:01
02/06/2021...	1	1	0:00:00	0:00:00	20:27:25
02/07/2021...	1	1	0:00:00	0:00:00	16:07:36
02/09/2021...	2	2	0:00:00	0:00:00	0:26:00
02/21/2021...	5	5	0:01:41	0:01:41	0:21:08
02/22/2021...	6	6	0:00:10	0:00:10	0:00:22
02/24/2021...	21	21	0:14:34	0:14:34	0:30:04
02/27/2021...	1	1	0:00:00	0:00:00	10:11:17
Count: 73	6,591	6,591	40:34:53	122:05:24	4372:42:18

Events (Application Events -> ONOPA.LOCAL\jldadmin -> 01/15/2021 - Fri)

View Screen Snapshots Print Export Show Columns

Start Time	Device	Application	Application ...	Active Time	Focus Time	Total Time	Window Ca...	Platform	View Screenshot
------------	--------	-------------	-----------------	-------------	------------	------------	--------------	----------	-----------------

To view events, select a specific item above and click the Load Events button. To drill down on an item, click on the tree [-] button, or double click on the item.

Record 0 of 0

Application Events

File Edit View Data Windows

Navigate

Load Events Criteria Grouping

Summary

Load Events Print Export Show Columns

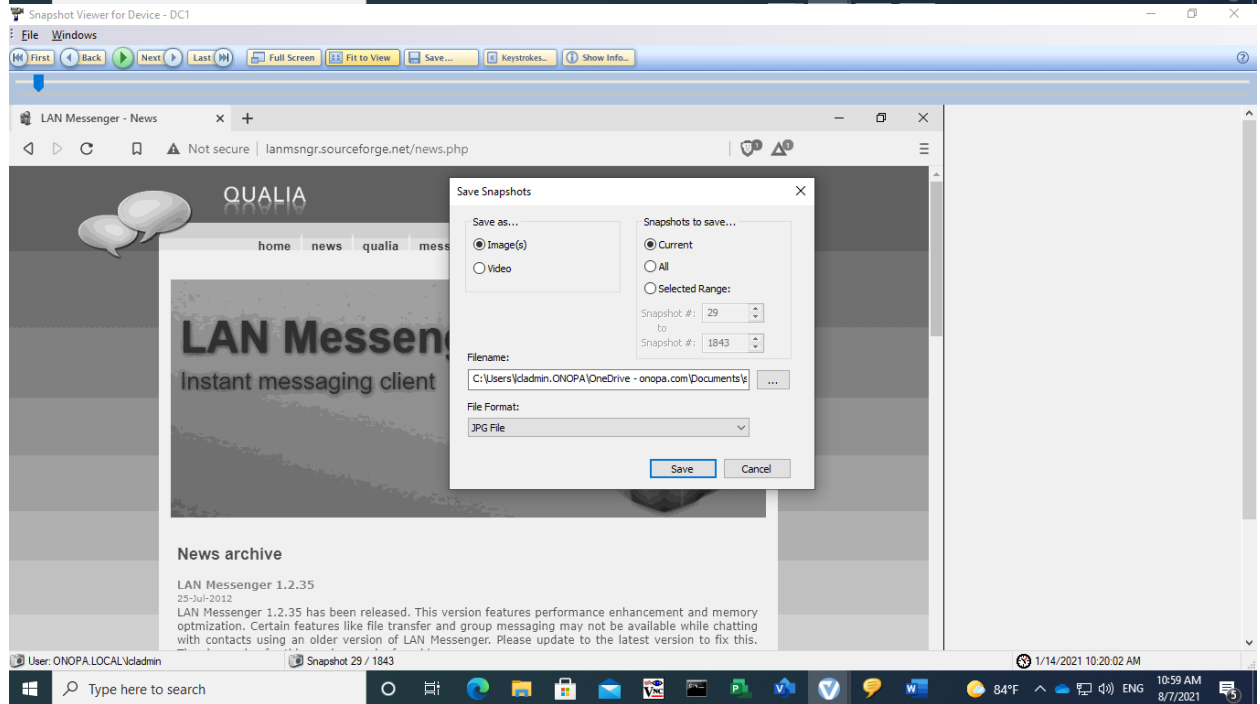
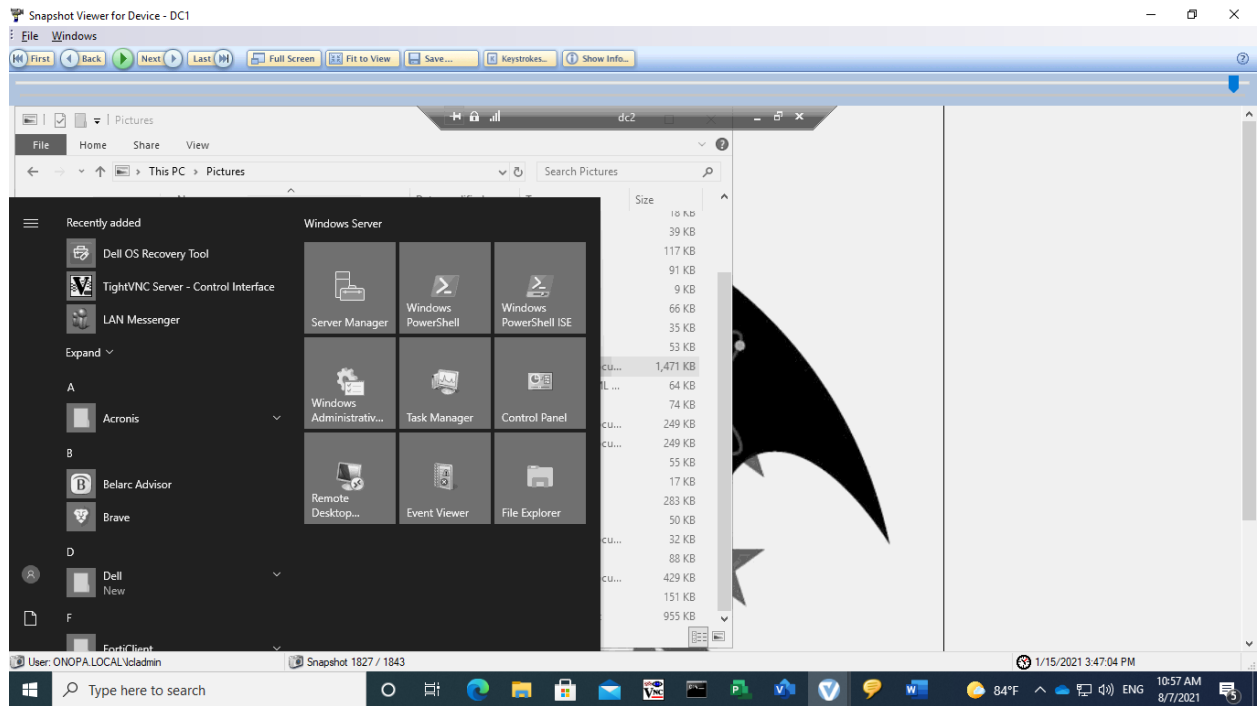
Name	Events	Instances	Active Time	Focus Time	Total Time
01/12/2021...	19	19	0:04:35	0:11:14	1:28:05
01/13/2021...	20	20	0:05:30	0:05:30	32:29:37
01/14/2021...	304	304	4:38:55	10:18:21	327:54:40
01/15/2021...	839	839	8:37:14	15:46:04	161:21:02
01/31/2021...	1	1	0:00:00	0:00:00	11:56:30
02/04/2021...	7	7	0:00:00	0:00:00	16:07:37
02/05/2021...	1	1	0:00:00	0:00:00	0:00:01
02/06/2021...	1	1	0:00:00	0:00:00	20:27:25
02/07/2021...	1	1	0:00:00	0:00:00	16:07:36
02/09/2021...	2	2	0:00:00	0:00:00	0:26:00
02/21/2021...	5	5	0:01:41	0:01:41	0:21:08
02/22/2021...	6	6	0:00:10	0:00:10	0:00:22
02/24/2021...	21	21	0:14:34	0:14:34	0:30:04
02/27/2021...	1	1	0:00:00	0:00:00	10:11:17
Count: 73	6,591	6,591	40:34:53	122:05:24	4372:42:18

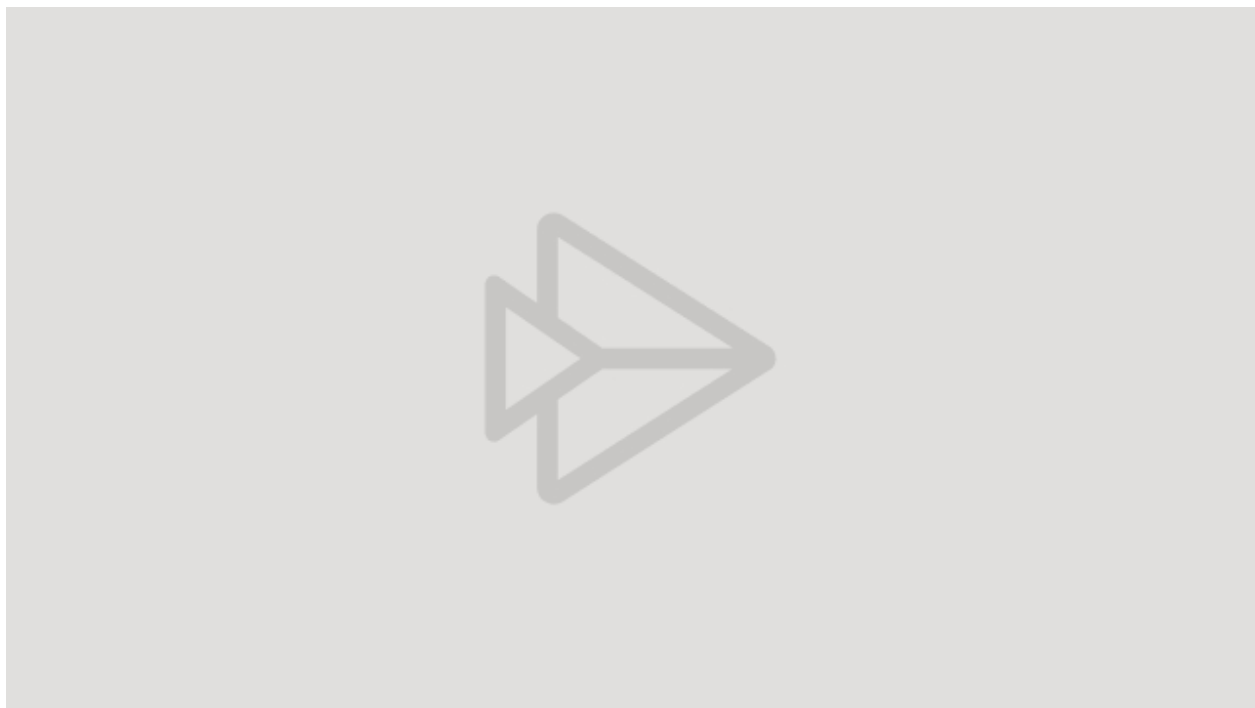
Events (Application Events -> ONOPA.LOCAL\jldadmin -> 01/15/2021 - Fri)

View Screen Snapshots Print Export Show Columns

Start Time	Device	Application	Application ...	Active Time	Focus Time	Total Time	Window Ca...	Platform	View Screenshot
03:43:04 PM	DC1		01/15/2021...	0:00:00	0:00:00	0:00:02	Windows S...	Windows S...	View Screen Snapshots
06:55:41 PM	DC1		01/15/2021...	0:00:01	0:00:01	0:00:06	Windows S...	Windows S...	View Screen Snapshots
10:59:40 AM	DC1		01/15/2021...	0:00:00	0:00:00	0:00:02	Windows S...	Windows S...	View Screen Snapshots
01:33:14 PM	DC1		01/15/2021...	0:00:01	0:00:01	0:00:02	Windows S...	Windows S...	View Screen Snapshots
06:56:01 PM	DC1		01/15/2021...	0:00:01	0:00:01	0:00:02	Windows S...	Windows S...	View Screen Snapshots
06:56:03 PM	DC1		01/15/2021...	0:00:00	0:00:00	0:00:00	Windows S...	Windows S...	View Screen Snapshots
11:18:05 AM	DC1		01/15/2021...	0:00:00	0:00:00	0:00:01	Windows S...	Windows S...	View Screen Snapshots
02:07:45 PM	DC1		01/15/2021...	0:00:00	0:00:00	0:00:01	Windows S...	Windows S...	View Screen Snapshots
01:11:50 PM	DC1		01/15/2021...	0:00:01	0:00:01	0:00:03	Windows S...	Windows S...	View Screen Snapshots
09:29:44 AM	DC1		01/15/2021...	0:00:01	0:00:01	0:00:02	Windows S...	Windows S...	View Screen Snapshots
10:21:32 AM	DC1		01/15/2021...	0:00:01	0:00:01	0:00:01	Windows S...	Windows S...	View Screen Snapshots
05:03:37 PM	DC1		01/15/2021...	0:00:00	0:00:00	0:00:01	Windows S...	Windows S...	View Screen Snapshots
06:58:04 AM	DC1	hrave	01/15/2021...	0:00:05	0:00:05	0:00:05	Untitled4 - Pr...	Windows S...	View Screen Snapshots

Record 1 of 839





- Recon Dashboard
- 360 Dashboard
- Data Explorer
- Reports
- Filter Categories
- Recorders
- Users
- Alerts & Policies
 - Alerts - Anomalies
 - Alerts - Events
 - Alerts - Keywords
 - Alerts - Operators
 - Policies - Geofencing
 - Policies - Recording
- Configurations
- System Management

Alert Type > Users > Keywords > Action > Summary

Keyword Alert Action

Process this alert

☒ Daily ☐ Hourly ☐ Every Alert

Scan for alert conditions once a day.

When this alert is triggered:

☒ Notify user

Display popup notification at the user's own desktop.

Note : Users will know they are being monitored!

☒ Send email to

Add

Email Rate: Set by process rate.

Send email once a day if the alert is triggered.

Note : Regardless of rate setting, new alerts from devices that have been offline will be compiled into a single, daily email.

Microsoft Office Home SharePoint

netorg7844005.sharepoint.com/_layouts/15/sharepoint.aspx?

SharePoint Search in SharePoint

Create site Create news post

Following

- CMPROPOSALS
- ONOPA TRAINING
- LMS365 SANDBOX
- TEST CATALOG
- WIDGET TEST CATALOG

See all

Recent

- ONOPA TRAINING
- CMMC
- CMPROPOSALS
- LMS365 SANDBOX

News from sites

See all

NIST SPECIAL PUBLICATION 800-171

CMMC

SWAY

IT Department yesterday

7 views

ONOPA TRAINING

Home

IT Department 7/22/2021

2 views

MCBCL Team

MCBCL

IT Department 5/19/2021

Frequent sites

See all

CMMC

ONOPA TRAINING

ITDEPT

Type here to search

Microsoft Office Home ONOPA TRAINING - Home

netorg7844005.sharepoint.com/sites/ONOPATRAINING

SharePoint Search this site

OT ONOPA TRAINING

Course Catalog My Training Dashboard Home Documents Pages Site contents Edit

Following Share

New Page details Analytics

Draft saved 7/22/2021 Edit Republish

ONOPA COURSE CATALOG

VIEW COURSES →

Cyber Awareness Challenge 2021

Sharable Content Object Reference Model

SCORM LEARN

LMS365 VIDEOS

Type here to search

85°F 11:37 AM 8/7/2021

SharePoint

Search this site

OT ONOPA TRAINING

Course Catalog

My Training Dashboard

Home

Documents

Pages

Site contents

Edit

Following

Share

New

Send to

Promote

Page details

Analytics

Published 7/21/2021

Edit

Search Course Catalog

Categories

Products

(17)

Scenarios

(4)

Get started

(2)

Adoption Tools

(1)

Course Type

e-Learning

(24)

Tools

★★★★★ 0 ratings

Type: e-Learning

Contact(s): IT Department

Lists

★★★★★ 0 ratings

Type: e-Learning

Contact(s): IT Department

Office for the web

★★★★★ 0 ratings

Type: e-Learning

Contact(s): IT Department

Arrange by: Newest Courses First

Show more

SharePoint

Search this site

OT ONOPA TRAINING

Course Catalog

My Training Dashboard

Home

Documents

Pages

Site contents

Edit

New

Send to

Promote

Page details

Analytics

Published 7/21/2021

Edit

Webinar

(0)

Training Plan

(0)

Access

★★★★★ 0 ratings

Type: e-Learning

Contact(s): IT Department

View Course

Accessibility

★★★★★ 0 ratings

Type: e-Learning

Contact(s): IT Department

View Course

Sway

★★★★★ 0 ratings

Type: e-Learning

Contact(s): IT Department

View Course

Microsoft Forms

★★★★★ 0 ratings

Type: e-Learning

Contact(s): IT Department

View Course

Planner

★★★★★ 0 ratings

Type: e-Learning

Contact(s): IT Department

View Course

Microsoft 365 Basics

★★★★★ 0 ratings

Type: e-Learning

Contact(s): IT Department

View Course

Microsoft Office Home

Course Catalog

netorg7844005.sharepoint.com/sites/ONOPATRAINING/SitePages/CourseCatalog.aspx

SharePoint

Search this site

ONOPA TRAINING

Course Catalog

My Training Dashboard

Home

Documents

Pages

Site contents

Edit

New

Send to

Promote

Page details

Analytics

Published 7/21/2021

Edit

Yammer

0 ratings

Type: e-Learning

Contact(s): IT Department

View Course

Microsoft Teams

0 ratings

Type: e-Learning

Contact(s): IT Department

View Course

SharePoint

0 ratings

Type: e-Learning

Contact(s): IT Department

View Course

OneNote

0 ratings

Type: e-Learning

Contact(s): IT Department

View Course

PowerPoint

0 ratings

Type: e-Learning

Contact(s): IT Department

View Course

Excel

0 ratings

Type: e-Learning

Contact(s): IT Department

View Course

Type here to search

85°F

11:40 AM 8/7/2021

SharePoint

Home

LMS365

SharePoint

Not following

Share

New

Send to

Page details

Analytics

Published 8/4/2021

Edit

SharePoint

0 ratings

Course Management

Course Description

SharePoint

Learning Modules

SharePoint Online Quick Start

Build and customize intranet sites, collaborate with others, manage your daily routine with workflows, and store your information

Not Started

Enroll to Course

Category: Products

Type: e-Learning

Course ID: SharePoint

Contact(s): IT Department

Microsoft Office Home CMMC - Home x +

netorg7844005.sharepoint.com/sites/CMMC

SharePoint Search this site

CMMC Home Documents Pages SWAY Site contents Edit

+ New Page details Analytics Published 1/21/2021 Edit

end boring meetings

CMMC Certification

LEARN MORE →

How to use Microsoft Teams

IT Planning

Group Policy Objects

Managed IT

Type here to search

SharePoint Search this site

85°F 11:42 AM 8/7/2021

CMMC Home Documents Pages SWAY Site contents Edit

+ New Page details Analytics Published 1/21/2021 Edit

```
mirror_mod.use_x = False
mirror_mod.use_y = True
mirror_mod.use_z = False
operation = "MIRROR_Z"
mirror_mod.use_x = False
mirror_mod.use_y = False
mirror_mod.use_z = True

selection at the end -add
obj.select= 1
obj.select=1
context.scene.objects.active
("Selected" + str(modifier
mirror_ob.select = 0
bpy.context.selected_obj
data.objects[one.name].sel
int( please select
MIRROR CLASSES -----
```


Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

LEARN MORE →

SharePoint Search this site


CMMC Home Documents Pages SWAY Site contents Edit

+ New Page details Analytics Published 1/21/2021 Edit



Awareness Training for CMMC Requirements


[LEARN MORE →](#)



SharePoint Search this site


CMMC Home Documents Pages SWAY Site contents Edit

+ New Page details Analytics Published 1/21/2021 Edit



Cybersecurity Maturity Model Certification


[LEARN MORE →](#)



SharePoint Search this site

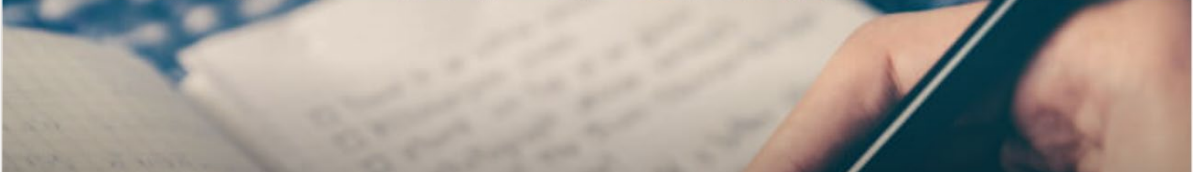
CMMC Home Documents Pages SWAY Site contents Edit

+ New Page details Analytics Published 1/21/2021 Edit



Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events

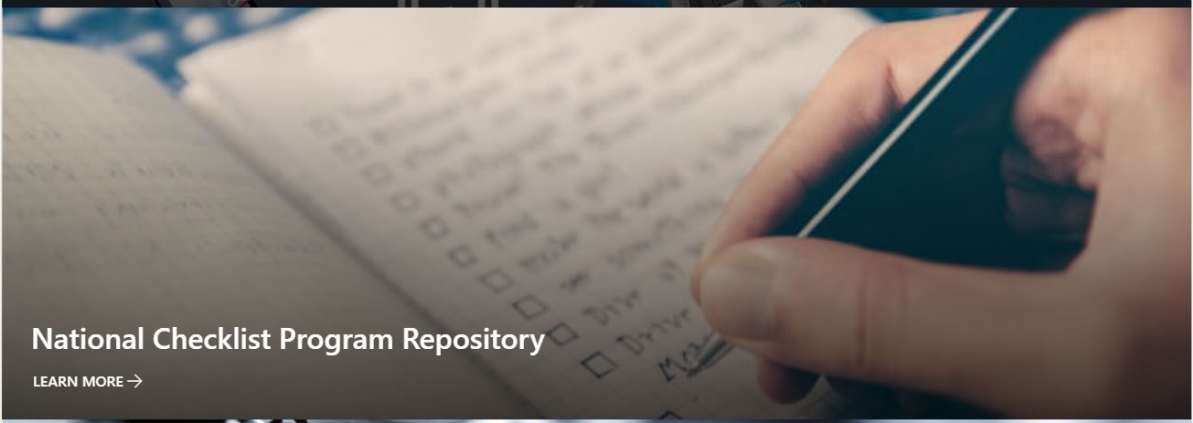
[LEARN MORE →](#)



SharePoint Search this site


CMMC Home Documents Pages SWAY Site contents Edit

+ New Page details Analytics Published 1/21/2021 Edit



National Checklist Program Repository

[LEARN MORE →](#)




Microsoft Office Home | CMMC - Home | NCP - National Checklist Program Ch... | A Guide to the Cybersecurity Maturity

netorg7844005.sharepoint.com/sites/CMMC

SharePoint | Search this site

CMMC Home Documents Pages SWAY Site contents Edit

+ New Page details Analytics Published 1/21/2021 Edit



Policy and Prodedures

LEARN MORE →

Type here to search

Microsoft Office Home | CYBER Security Aw... | Group Policy Objects - | What is Managed IT Si... | Planning for IT Archiv... | NCP - National Checkli... | A Guide to the Cybers...

netorg7844005.sharepoint.com/sites/onopa.com/SitePages/CYBER-Security-Awareness.aspx

SharePoint | Search this site

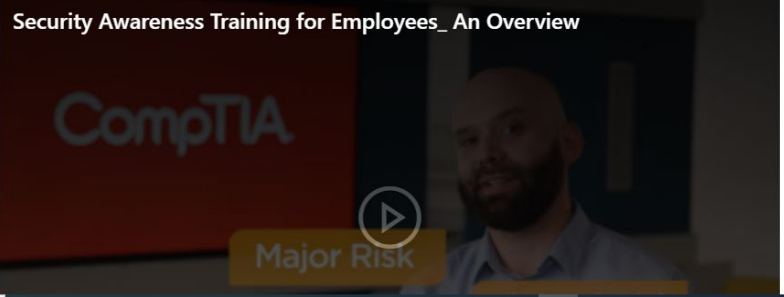
onopa.com Public group ☆ Not following 37 members

Home Conversations Documents Notebook Pages Site contents Recycle bin Edit

+ New Discard changes Send to Promote Page details Draft saved 1/16/2021 Edit Update news

CYBER Security Awareness

IT Department



Security Awareness Training for Employees_ An Overview

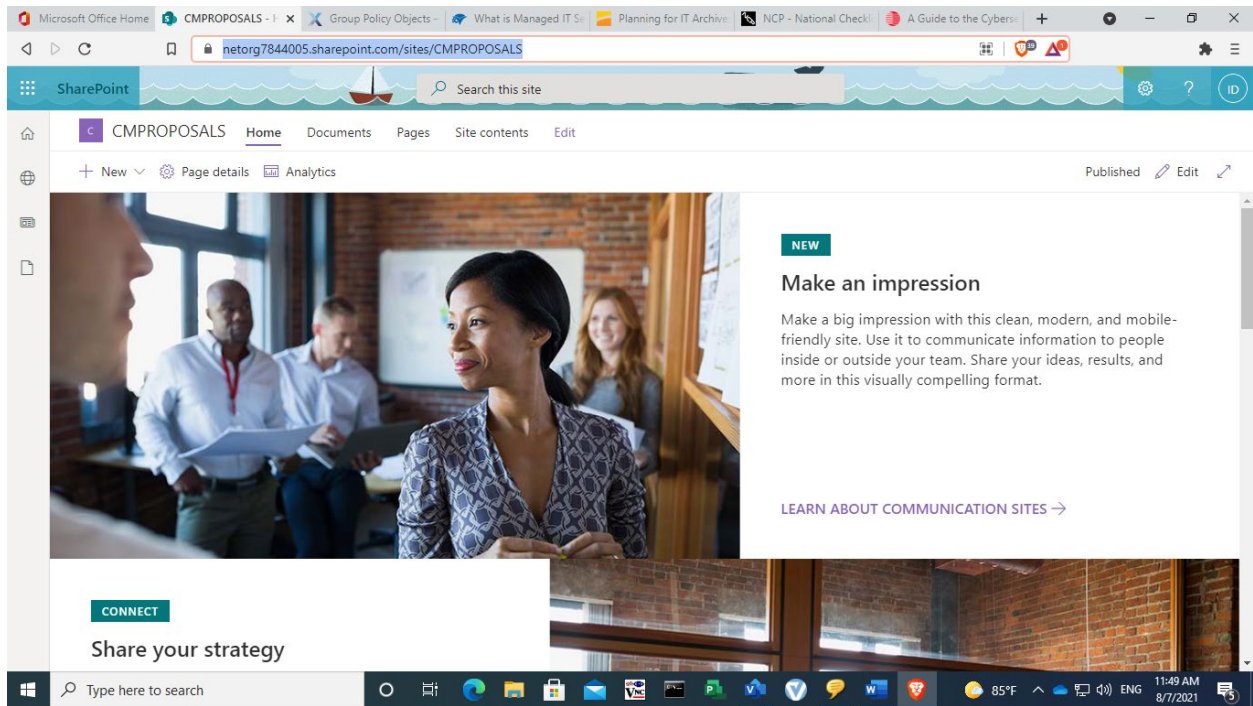
CompTIA

Major Risk

Type here to search

85°F 11:47 AM 8/7/2021

<https://netorg7844005.sharepoint.com/sites/CMPROPOSALS>



Module 1: Windows Server Administration Overview

This module describes how to distinguish different Windows Server 2019 editions and techniques for deployment, servicing, and activation. The module also introduces Windows Server Core and compares it with the Desktop Experience version. The module describes tools and concepts for administering Windows Server, such as Windows Admin Center, PowerShell, and delegation of privileges.

Lessons

- Overview of Windows Server administration principles and tools
- Introducing Windows Server 2019
- Windows Server Core Overview

Lab: Deploying and configuring Windows Server

- Deploying and configuring Server Core
- Implementing and using remote server administration

After completing this module, students will be able to:

- Describe Windows Server as well as techniques for deployment, servicing, and activation.
- Describe Windows Server Core, its specifics, and ways to administer it.

Module 2: Identity Services in Windows Server

This module introduces identity services and describes Active Directory Domain Services (AD DS) in a Windows Server environment. The module describes how to deploy domain controllers in AD DS, as well as the Azure Active Directory (AD) and the benefits of integrating Azure AD with AD DS. The module also covers Group Policy basics and how to configure group policy objects (GPOs) in a domain environment. Finally, the modules describe the role of Active Directory certificate services and certificate usage.

Lessons

- Overview of AD DS
- Deploying Windows Server domain controllers
- Overview of Azure AD
- Implementing Group Policy
- Overview of Active Directory Certificate Services

Lab : Implementing identity services and Group Policy

- Deploying a new domain controller on Server Core
- Configuring Group Policy
- Deploying and using certificate services

After completing this module, students will be able to:

- Describe AD DS in a Windows Server environment.
- Deploy domain controllers in AD DS.
- Describe Azure AD and benefits of integrating Azure AD with AD DS.
- Explain Group Policy basics and configure GPOs in a domain environment
- Describe the role of Active Directory certificate services and certificate usage

Module 3: Network Infrastructure services in Windows Server

This module describes how to implement core network infrastructure services in Windows Server. The modules cover how to deploy, configure and manage DNS and IPAM. The modules also describe how to use Remote Access Services.

Lessons

- Deploying and managing DHCP
- Deploying and managing DNS services
- Deploying and managing IPAM

Lab: Implementing and configuring network infrastructure services in Windows Server

- Deploying and configuring DHCP
- Deploying and configuring DNS

After completing this module, students will be able to:

- Describe, deploy, and configure DHCP service.
- Deploy, configure, and manage DNS.
- Describe, deploy, and manage IPAM.

Module 4: File Servers and Storage management in Windows Server

This module describes how to configure file servers and storage in Windows Server. The module covers file sharing and deployment of Storage Spaces technology. The module describes how to implement data deduplication, iSCSI-based storage in Windows Server, and finally, how to deploy DFS.

Lessons

- Volumes and file systems in Windows Server
- Implementing sharing in Windows Server
- Implementing Storage Spaces in Windows Server
- Implementing Data Deduplication
- Implementing iSCSI
- Deploying Distributed File System

Lab: Implementing storage solutions in Windows Server

- Implementing Data Deduplication
- Configuring iSCSI storage
- Configuring redundant storage spaces
- Implementing Storage Spaces Direct

After completing this module, students will be able to:

- Implement sharing in Windows Server
- Deploy Storage Spaces technology
- Implement the data deduplication feature

- Implement iSCSI-based storage
- Deploy and manage Distributed File System (DFS)

Module 5: Hyper-V virtualization and containers in Windows Server

This module describes how to implement and configure Hyper-V VMs and containers. The module covers key features of Hyper-V in Windows Server, describes VM settings, and how to configure VMs in Hyper-V. The module also covers security technologies used with virtualization, such as shielded VMs, Host Guardian Service, admin-trusted and TPM-trusted attestation, and KPS.

Lessons

- Hyper-V in Windows Server
- Configuring VMs
- Securing virtualization in Windows Server
- Containers in Windows Server
- Overview of Kubernetes

Lab: Implementing and configuring virtualization in Windows Server

- Creating and configuring VMs
- Installing and configuring containers

After completing this module, students will be able to:

- Describe the key features of Hyper-V in Windows Server.
- Describe VM settings and deploy and configure VMs in Hyper-V.
- Explain the use of security technologies for virtualization.
- Describe and deploy containers in Windows Server.
- Explain the use of Kubernetes on Windows.

Module 6: High Availability in Windows Server

This module describes current high availability technologies in Windows Server. The module describes failover clustering and considerations for implementing it, and how to create and configure failover clustering. The module also explains stretch clusters and options for achieving high availability with Hyper-V VMs.

Lessons

- Planning for failover clustering implementation
- Creating and configuring failover cluster
- Overview of stretch clusters
- High availability and disaster recovery solutions with Hyper-V VMs

Lab: Implementing failover clustering

- Configuring iSCSI storage
- Configuring a failover cluster
- Deploying and configuring a highly available file server
- Validating the deployment of the highly available file server

After completing this module, students will be able to:

- Describe failover clustering and the considerations for implementing it.
- Create and configure failover clusters.
- Describe stretch clusters.
- Describe options to achieve high availability with Hyper-V VMs.

Module 7: Disaster recovery in Windows Server

This module describes disaster recovery technologies in Windows Server and how to implement them. The module covers how to configure and use Hyper-V Replica and describes Azure Site Recovery. The module also covers how to implement Windows Server backup and describes the Azure Backup service.

Lessons

- Hyper-V Replica
- Backup and restore infrastructure in Windows Server

Lab: Implementing Hyper-V Replica and Windows Server Backup

- Implementing Hyper-V Replica
- Implementing backup and restore with Windows Server Backup

After completing this module, students will be able to:

- Describe and implement Hyper-V Replica.
- Describe Azure Site Recovery.
- Describe and implement Windows Server backup.
- Describe the Azure Backup service.

Module 8: Windows Server security

This module describes Windows Server security features and how to implement them. The module covers credentials used in Windows Server and explains how to implement privileged access protection. In addition to describing methods and technologies for hardening Windows Server security, the module explains how to configure Just Enough Administration (JEA) and how to secure SMB traffic. Finally, the module covers Windows Update, its deployment and management options.

Lessons

- Credentials and privileged access protection in Windows Server
- Hardening Windows Server
- Just Enough Administration in Windows Server
- Securing and analyzing SMB traffic
- Windows Server update management

Lab: Configuring security in Windows Server

- Configuring Windows Defender Credential Guard
- Locating problematic accounts
- Implementing LAPS

After completing this module, students will be able to:

- Describe credentials used in Windows Server.
- Explain how to implement privileged access protection.
- Describe methods and technologies to harden security in Windows Server.
- Describe and configure Just Enough Administration (JEA).
- Secure SMB traffic in Windows Server.
- Describe Windows Update and its deployment and management options.

Module 9: Remote Desktop Services in Windows Server

This module describes key Remote Desktop Protocol (RDP) and Virtual Desktop Infrastructure (VDI) features in Windows Server. The module covers how to deploy session-based desktops and describes personal and pooled virtual desktops.

Lessons

- Remote Desktop Services Overview
- Configuring a session-based desktop deployment
- Overview of personal and pooled virtual desktops

Lab: Implementing RDS in Windows Server

- Implementing RDS
- Configuring RemoteApp collection settings
- Configuring a virtual desktop template

After completing this module, students will be able to:

- Describe Remote Desktop Services (RDS) in Windows Server.
- Describe and deploy session-based desktops.

- Describe personal and pooled virtual desktops.

Module 10: Remote access and web services in Windows Server

This module describes how to implement virtual private networks (VPNs), Network Policy Server (NPS), and Microsoft Internet Information Services (IIS). The module provides an overview of remote access services and describes Always On VPN functionality, as well as how to configure NPS and Web Server (IIS) in Windows Server.

Lessons

- Overview of RAS in Windows Server
- Implementing VPNs
- Implementing NPS
- Implementing Always On VPN
- Implementing Web Server in Windows Server

Lab: Deploying network workloads

- Implementing Web Application Proxy
- Implementing VPN in Windows Server
- Deploying and Configuring Web Server

After completing this module, students will be able to:

- Describe VPN options in Windows Server.
- Describe Always On VPN functionality.
- Describe and configure NPS.
- Describe and configure Web Server (IIS).

Module 11: Monitoring, performance, and troubleshooting

This module describes how to implement service and performance monitoring and apply troubleshooting in Windows Server. The module highlights monitoring tools and describes how to monitor performance, including event logging and how to perform event logging monitoring for troubleshooting purposes.

Lessons

- Overview of Windows Server monitoring tools
- Using Performance Monitor
- Monitoring event logs for troubleshooting

Lab: Monitoring and troubleshooting Windows Server

- Establishing a performance baseline
- Identifying the source of a performance problem
- Viewing and configuring centralized event logs
- Identifying the source of a performance problem
- Describe monitoring tools in Windows Server.
- Describe performance monitoring and use it in Windows Server.
- Describe event logging and perform event logging monitoring for troubleshooting purposes.

Module 12: Upgrade and migration in Windows Server

This module describes how to perform upgrades and migrations for AD DS, Storage, and Windows Server. The module covers tools to use for AD DS migration. The module also covers the Storage Migration Service, and finally, Windows Server migration tools and usage scenarios.

Lessons

- AD DS migration
- Storage Migration Service
- Windows Server migration tools

Lab: Migrating Server workloads

- Selecting a process to migrate server workloads
- Planning how to migrate files by using Storage Migration Service

After completing this module, students will be able to:

- Describe tools to use for AD DS migration.
- Describe the Storage Migration Service.
- Describe Windows Server migration tools and their usage scenarios.