

DO NOT REPRINT
© FORTINET



FortiClient EMS Study Guide

for FortiClient EMS 7.0

DO NOT REPRINT

© FORTINET

Fortinet Training

<https://training.fortinet.com>

Fortinet Document Library

<https://docs.fortinet.com>

Fortinet Knowledge Base

<https://kb.fortinet.com>

Fortinet Fuse User Community

<https://fusecommunity.fortinet.com/home>

Fortinet Forums

<https://forum.fortinet.com>

Fortinet Support

<https://support.fortinet.com>

FortiGuard Labs

<https://www.fortiguards.com>

Fortinet Network Security Expert Program (NSE)

<https://training.fortinet.com/local/staticpage/view.php?page=certifications>

Fortinet | Pearson VUE

<https://home.pearsonvue.com/fortinet>

Feedback

Email: askcourseware@fortinet.com

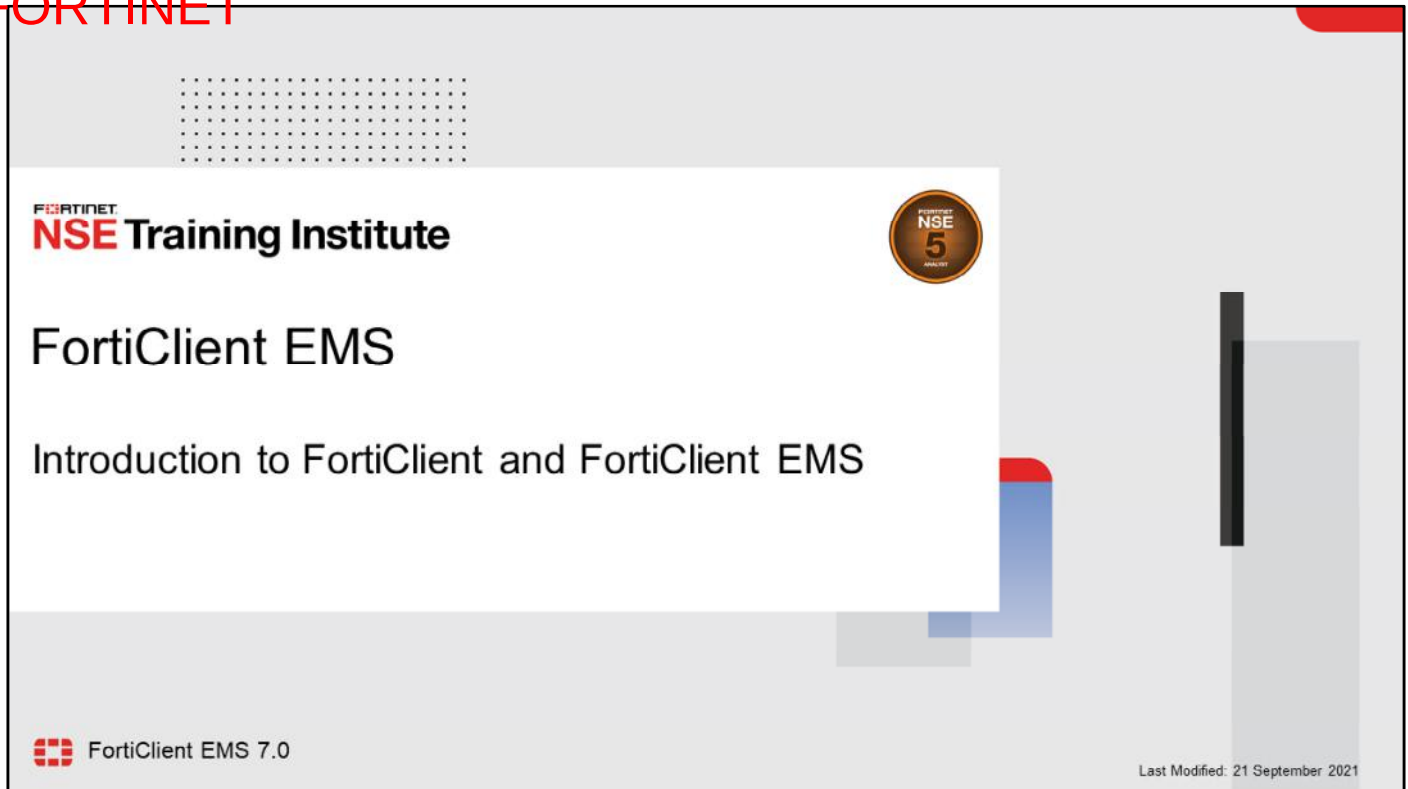


9/21/2021

TABLE OF CONTENTS

01 Introduction to FortiClient and FortiClient EMS.....	4
02 Installation and Licensing.....	43
03 FortiClient EMS Configuration and Administration.....	75
04 FortiClient Deployment.....	135
05 FortiClient Provisioning Using FortiClient EMS.....	160
06 ZTNA.....	231
07 Diagnostics and Troubleshooting.....	292

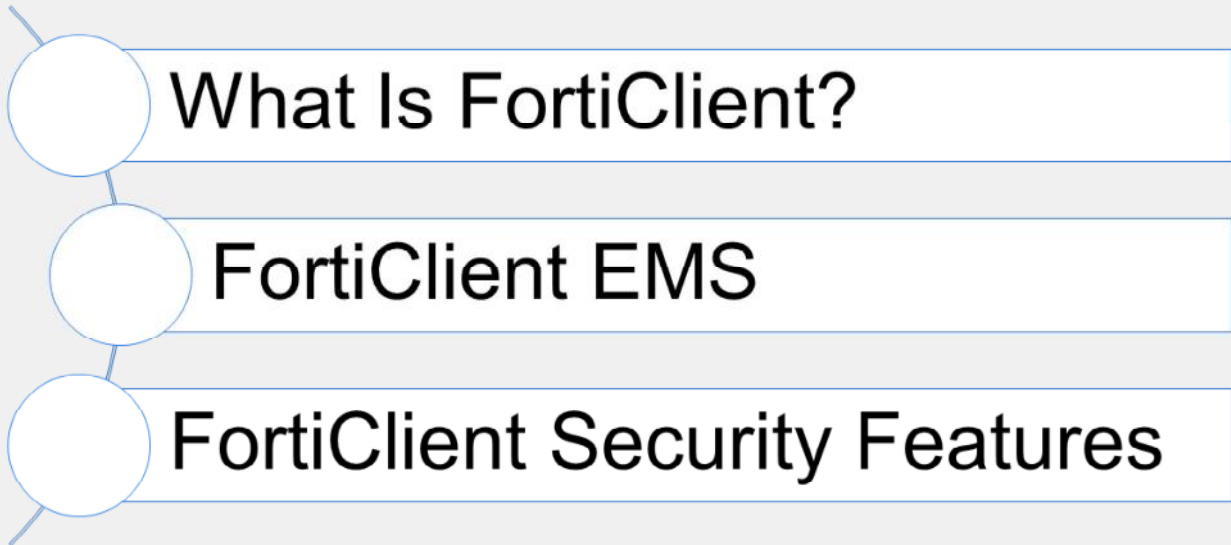
DO NOT REPRINT
© FORTINET



In this lesson, you will learn how to integrate FortiClient into your existing network, and manage the security of multiple endpoint devices from a single management console, such as FortiClient Enterprise Management Server (EMS).

DO NOT REPRINT
© FORTINET

Lesson Overview



In this lesson, you will learn about the topics shown on this slide.

DO NOT REPRINT
© FORTINET

What Is FortiClient?

Objectives

- Know when and why FortiClient endpoint security is needed
- Understand FortiClient
- Understand FortiClient Editions
- Understand FortiClient EMS

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating a competent understanding of what FortiClient is and what it does, you will be able to understand how FortiClient fits into your network.

DO NOT REPRINT
© FORTINET

Endpoint Network Security

- FortiClient endpoint protection



Many single-purpose endpoint security software applications → Leads to high cost and complexity



Fortinet NSE Training Institute

© Fortinet Inc. All Rights Reserved.

4

In a typical endpoint network security solution, multiple instances of single-purpose software applications are used. Each application provides a specific service, including antivirus protection, web filtering, VPN access, application firewall, and so on.

Many endpoint security solutions are not capable of providing central management, central logging, and other features.

When several different applications are used, most times they all are made by different vendors. Using applications from multiple vendors can introduce unwanted complexity, create many potential points of failure, and increase the cost of initial installation and ongoing operation.

On the other hand, FortiClient offers comprehensive endpoint protection for your Windows-based and Mac-based desktops, laptops, file servers, and mobile devices. FortiClient can safeguard your systems with advanced security technologies and provide a single management console.

DO NOT REPRINT
© FORTINET

Why You Need Endpoint Security

- Traditional antivirus protection is not enough:
 - It cannot stop advanced threats
 - It puts data and organizations at risk
 - It doesn't provide central monitoring and visibility into individual endpoints
- Potential threats as well as incidents of stolen information and stolen identities are increasing exponentially
- More people are using remote access to connect to work:
 - No control over the remote and mobile devices
 - No control over removable media
- Threats are coming from inside your network
 - Infected and compromised mobile devices – laptop, removable media
 - Downloading files using VPN
 - Downloading password-encrypted files

Traditional antivirus software can protect your endpoints from known viruses, but may be unable to detect and protect against advanced threats. This can result in data being lost or compromised.

Present day attackers use advanced methods to hijack your identity, such as social media accounts, and access your banking information. Sometimes, this information is browser or application-based, and antivirus software can do a little to protect it.

More and more people connect to corporate networks from Wi-Fi hotspots, providing no control over remote or mobile devices.

Not only do threats come from outside your network, people often take mobile devices inside your network, which may be compromised. They also use your VPN to download files, which may contain potential issues.

This is why you need endpoint security!

DO NOT REPRINT
© FORTINET

Endpoint Security

- Protection of an individual workstation or device
- Endpoint security includes a wide range of security features:
 - Malware, grayware, virus, spyware, key logger protection
 - Application firewall
 - Network protection
 - Vulnerability management
 - Input/output data control
 - Central monitoring, provisioning, and logging
- In sync with latest signatures and application updates
- Enforcement of endpoint compliance

Standard security software can provide basic protection, but endpoint security provides basic security plus much more.

Endpoint security provides an antivirus program and much more to protect your devices and it creates a barrier between your network and the outside. Endpoint security provides antivirus updates, antimalware, IPS/IDS signatures, and updates.

Endpoint security also forces endpoint compliance, which requires endpoint devices to comply with specific criteria before they can gain access to the network.

DO NOT REPRINT
© FORTINET

FortiClient

- Provides a comprehensive network security solution for endpoints while improving your visibility and control
 - Allows you to manage security of multiple endpoints from the FortiClient EMS
 - Allows you to manage endpoints locally or remotely, stationary or mobile, using FortiClient EMS
 - Supports multiple platform protection:
 - Windows devices
 - Mac OS devices
 - Linux OS devices
 - iOS devices
 - Android mobile devices
 - Chromebook

FortiClient provides comprehensive endpoint protection for your Windows-based, Mac-based, and Linux-based desktops, laptops, file servers, and mobile devices such as iOS and Android. It helps you to safeguard your systems with advanced security technologies, all of which you can manage from a single management console.

FortiClient enables every device—local or remote, stationary or mobile—to integrate with your FortiClient EMS and FortiGate. FortiClient supports Windows, Mac OS, Linux, iOS, Android mobile devices and Chromebook, and also integrates your home offices, mobile workers, and visiting partners.

DO NOT REPRINT
© FORTINET

FortiClient (Contd)

- FortiClient is used with EMS to use all APT and security features
- FortiClient must connect to FortiClient EMS to activate the license
- You can change FortiClient configurations only from the management device
- FortiClient is either used with FortiClient EMS only or in the Security Fabric
- Enforces endpoint compliance and provides endpoint awareness
- Automates prevention of known and unknown threats
- Provides secure remote access

FortiClient must be used with FortiClient EMS. FortiClient must connect to FortiClient EMS to activate its license and become provisioned by the endpoint profile that the administrator configured in FortiClient EMS. You cannot use any FortiClient features until FortiClient is connected to FortiClient EMS and licensed.

When FortiClient is connected only to FortiClient EMS, FortiClient EMS provisions and manages FortiClient. FortiClient EMS also sends zero-trust tagging rules to FortiClient, and uses the results from FortiClient to dynamically group endpoints in EMS. Only FortiClient EMS can control the connection between FortiClient and FortiClient EMS. However, FortiClient cannot participate in the Fortinet Security Fabric.

FortiClient in the security fabric connects to FortiClient EMS to receive a profile of configuration information as part of an endpoint policy. FortiClient EMS is connected to FortiGate to participate in the Security Fabric. FortiClient EMS sends FortiClient endpoint information to FortiGate. FortiGate can also receive dynamic endpoint group lists from FortiClient EMS and use them to build dynamic firewall policies.

FortiClient automates prevention of known and unknown threats through its built-in, host-based security stack and integration with FortiSandbox.

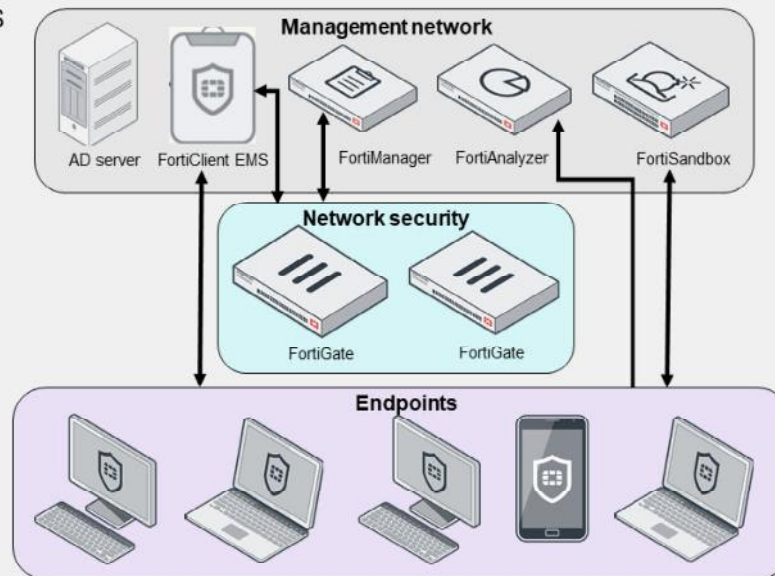
FortiClient also provides secure remote access to corporate assets through VPN.

DO NOT REPRINT
© FORTINET

FortiClient (Contd)

- Fortinet products can work together to support FortiClient

- FortiClient EMS
- FortiManager
- FortiGate
- FortiAnalyzer
- FortiSandbox



Fortinet
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

9

The following Fortinet products can work together to support FortiClient:

FortiClient EMS: FortiClient EMS runs on a Windows server. EMS manages FortiClient endpoints by deploying FortiClient (Windows) and endpoint policies to endpoints, and the endpoints can connect FortiClient Telemetry to EMS. FortiClient endpoints can connect to EMS to participate in the Security Fabric. FortiClient endpoints connect to EMS to be managed in real time.

FortiManager: FortiManager provides central FortiClient management for FortiGate devices that FortiManager manages. When endpoints are connected to managed FortiGate devices, you can use FortiManager to monitor endpoints from multiple FortiGate devices.

FortiGate: FortiGate provides network security. EMS defines compliance verification rules for connected endpoints and communicates the rules to endpoints and FortiGate. FortiGate uses the rules and endpoint information from EMS to dynamically adjust security policies. When using FortiManager, FortiGate communicates between EMS and FortiManager.

FortiAnalyzer: FortiAnalyzer can receive logs, and Windows host events directly from endpoints connected to EMS, and you can use FortiAnalyzer to analyze the logs and run reports. FortiAnalyzer receives other FortiClient data from EMS.

FortiSandbox: FortiSandbox offers capabilities to analyze new, previously unknown, and undetected virus samples in real time. Files sent to it are scanned first, using a similar antivirus engine and signatures available on FortiOS and FortiClient. If the file is not detected but is an executable file, it is run in a Microsoft Windows VM and monitored. The file is given a rating or score based on its activities and behavior in the VM.

DO NOT REPRINT
© FORTINET

FortiSASE SIA Deployment

- SASE-SIA (Security-as-a-Service-Secure Internet Access)
 - Security-as-a-Service is deployed by FortiClient SASE edition
 - Cloud-based platform
 - Managed by FortiGuard advanced protection
 - Provides FWaaS, IPS, DLP, DNS, and sandboxing to off-fabric remote users
 - Only supported with FortiClient Cloud (Hosted EMS)
 - Supports Windows, Mac, and Linux operating systems

FortiSASE SIA is a Security-as-a-Service deployed via FortiClient SASE deployment. This scalable cloud-based platform is easy to manage and powered by Fortinet's award-winning FortiGuard advanced protection services allowing customers to extend FWaaS, IPS, DLP, DNS, SWG, sandboxing off-fabric remote users. FortiSASE SIA offers up-to-date, real-time protection to terminate client traffic, scan traffic for known and unknown threats, and enforce corporate security policies for users anywhere. All features of EPP/ATP are included in a FortiSASE deployment. This deployment is only supported with FortiClient Cloud.

DO NOT REPRINT
© FORTINET

FortiClient Editions

- FortiClient provides visibility and control for:
 - Zero Trust Network Access
 - Secure Access Service Edge
- FortiClient comes in four different editions:
 - ZTNA (Zero Trust Network Access)
 - EPP/APT (Endpoint Protection Platform/Advanced Persistent Threat)
 - Managed Service
 - Chromebook

FortiClient Security Fabric integration provides endpoint visibility through telemetry and ensures that all fabric components, FortiGate, FortiAnalyzer, EMS, Managed APs, Managed Switches, and Sandbox have a unified view of endpoints in order to provide tracking and awareness, compliance enforcement, and reporting. Secure remote connectivity is provided by either traditional VPN tunnels or new, automatic ZTNA tunnels.

FortiClient comes in four different editions:

- ZTNA (Zero Trust Network Access)
- EPP/APT (Endpoint Protection Platform/Advanced Persistent Threat)
- Managed Service
- Chromebook

DO NOT REPRINT
© FORTINET

FortiClient Editions (Contd)

	VPN/ZTNA	EPP/APT	MANAGED	Chrome
Zero Trust Agent				
Zero Trust Network Access (ZTNA)	✓	✓	✓	
Central Management using FortiClient Cloud	✓	✓	✓	✓
Central Logging and Reporting	✓	✓	✓	✓
SSL VPN with MFA*	✓	✓	✓	
IPSec VPN with MFA*	✓	✓	✓	
SSO Mobility Agent	✓	✓	✓	
IT Hygiene				
Vulnerability Agent and Remediation	✓	✓	✓	
FortiGuard Web Filtering	✓	✓	✓	✓
USB Device Control	✓	✓	✓	

* Multi-factor Authentication

This slide shows the comparison table of FortiClient editions.

FortiClient ZTNA works with FortiOS to enable secure, granular access to applications whether the user is on-fabric or off-fabric. Each session is initiated with an automatic, encrypted tunnel from FortiClient to the FortiOS proxy point for user and device verification. If verified, access is granted for that session. Two-Factor authentication can also be used to provide an additional layer of security. With ZTNA, organizations benefit from both a better remote access solution and a consistent policy for controlled access to applications both on and off the network.

EPP/APT: includes all features detailed for the Zero Trust Network Access (ZTNA) license, as well as antivirus (AV), antiransomware, anti-exploit, cloud-based malware detection, application firewall, software inventory, and advanced threat protection through FortiClient Cloud Sandbox.

The managed service includes all features detailed for ZTNA and EPP editions, as well as initial FortiClient cloud provisioning with the customer, to set up and configure their FortiClient cloud environment, endpoint onboarding, security fabric setup and integration, and endpoint vulnerability monitoring

Chromebook: license allows management of one Google Chromebook user. If the number of Chromebooks that the EMS is managing exceeds the number of Chromebook licenses available, FortiClient EMS licenses the additional Chromebooks using any available Fabric Agent licenses.

DO NOT REPRINT
© FORTINET

FortiClient Editions (Contd)

	VPN/ZTNA	EPP/APT	MANAGED	Chrome
Endpoint Security (EPP)				
FortiSandbox (On-premises or PaaS)	✓	✓	✓	
FortiClient Cloud Sandbox		✓	✓	
AI-powered NGAV		✓	✓	
Automated Endpoint Quarantine		✓	✓	
Ransomware Protection		✓	✓	
Managed FortiClient Service				
Endpoint On-boarding			✓	
Initial Provisioning			✓	
Security Fabric Setup/Integration			✓	
Vulnerability Monitoring			✓	
Endpoint Security Monitoring			✓	

This slide is the continuation of the comparison table.

DO NOT REPRINT
© FORTINET

Knowledge Check

1. What is endpoint security?
 - A. Traditional antivirus software
 - ✓ B. A comprehensive network security solution for endpoints

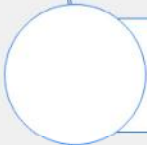
2. Which FortiClient connection participates in the Security Fabric?
 - ✓ A. EMS and FortiGate
 - B. EMS only

DO NOT REPRINT
© FORTINET

Lesson Progress



What Is FortiClient?



FortiClient EMS



FortiClient Security Features

Good job! You now know more about what FortiClient is and what it does.

Now, you will learn about FortiClient EMS.

DO NOT REPRINT
© FORTINET

The slide features a light gray background with a white rectangular area on the left containing the title and objectives. To the right of this area are several gray rectangular blocks of varying sizes and a small grid of dots. A red and blue L-shaped graphic is positioned between the white area and the gray blocks. The Fortinet logo and 'NSE Training Institute' text are in the bottom left, and the number '16' is in the bottom right.

FortiClient EMS Introduction

Objectives

- Understand the purpose of FortiClient EMS
- Identify FortiClient EMS components

FORTINET
NSE Training Institute

16

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating a competent understanding of the components and management functions of FortiClient EMS, you will be able to understand the purpose of FortiClient EMS.

FortiClient EMS

- FortiClient EMS is a security management solution that enables:
 - Scalable and centralized management of multiple endpoints (computers)
 - Efficient and effective administration of endpoints running FortiClient
- Provides visibility across the network to securely share information and assign security profiles to endpoints
- Works with the FortiClient Web Filter extension to provide web filtering for Google Chromebook users
- Designed to meet the needs of small to large enterprises that deploy FortiClient on endpoints and/or provide web filtering for Google Chromebook users

FortiClient EMS is a security management solution that enables scalable and centralized management of multiple endpoints (computers). It also provides efficient and effective administration of endpoints running FortiClient, and visibility across the network to securely share information and assign security profiles to endpoints. It is designed to maximize operational efficiency and includes automated capabilities for device management and troubleshooting.

FortiClient EMS also works with the FortiClient Web Filter extension to provide web filtering for Google Chromebook users.

The benefits of deploying FortiClient EMS include:

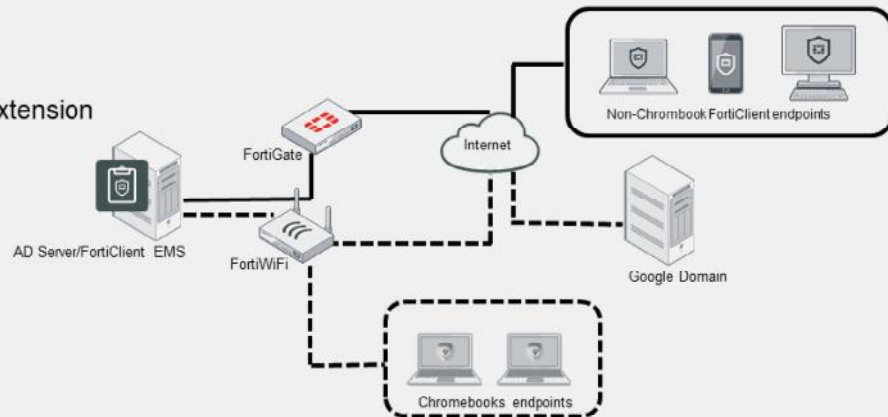
- Remotely deploying FortiClient software to Windows computers
- Updating profiles for endpoint users regardless of access location
- Administering FortiClient endpoint connections, such as accepting, disconnecting, and blocking connections
- Managing and monitoring endpoints, such as status, system, and signature information
- Identifying outdated versions of FortiClient software
- Defining web filtering rules in a profile, and remotely deploying the profile to the FortiClient Web Filter extension on Google Chromebook endpoints

You can manage endpoint security for Windows and macOS platforms using a unified organizational security policy. An organizational security policy provides a full, understandable view of the security policies defined in the organization. You can see all policy rules, assignments, and exceptions in a single unified view. FortiClient EMS is part of the Fortinet Endpoint Security Management suite, which ensures comprehensive policy administration and enforcement for an enterprise network.

DO NOT REPRINT
© FORTINET

FortiClient EMS—Components

- FortiClient EMS provides the infrastructure to install and manage FortiClient software on endpoints
- FortiClient protects endpoints from viruses, threats, and risks
- FortiClient EMS components are:
 - FortiClient EMS
 - Database
 - FortiClient
 - FortiClient Web Filter extension



Fortinet
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

18

The following components make up FortiClient EMS:

- **FortiClient EMS:** manages FortiClient on endpoints that connect to your network. It also manages the FortiClient Web Filter extension installed on Google Chromebook endpoints, which are connected to your Google domain. It includes two types of software:
 - Console software that manages security profiles, FortiClient on endpoints, and Chromebook endpoints
 - Server software that provides secure communication between endpoints and the console and between Chromebook endpoints and the Google Admin console
- **Database:** stores security profiles and events. Also stores user information retrieved from the Google Admin console for Chromebooks. The SQL database is installed as part of the FortiClient EMS installation
- **FortiClient:** helps enforce security and protection on endpoints. It runs on servers, desktops, and portable computers you want to secure
- **FortiClient Web Filter extension:** communicates with FortiClient EMS and enforces web filtering on Google Chromebook endpoints

In the EMS lesson, you will learn about FortiClient EMS in more detail, and explore all the features and options.

DO NOT REPRINT
© FORTINET

Knowledge Check

1. Which component is a FortiClient EMS component?
☐ A. FortiGate
☒ B. FortiClient
2. Which system requires a FortiClient Web Filter extension ?
☐ A. Linux
☒ B. Chromebook

DO NOT REPRINT
© FORTINET

Lesson Progress



What Is FortiClient?



FortiClient EMS



FortiClient Security Features

Good job! You now understand FortiClient EMS.

Now, you will learn about FortiClient security features and what they do.

DO NOT REPRINT
© FORTINET

FortiClient Security Features

Objectives

- Identify FortiClient security features

FORTINET
NSE Training Institute

21

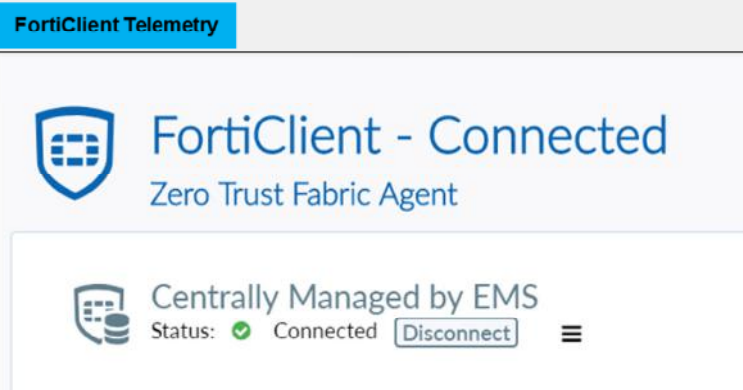
After completing this section, you should be able to achieve the objective shown on this slide.

By demonstrating a competent understanding of the key features of FortiClient, you will be able to use FortiClient features and operation modes in your network.

DO NOT REPRINT
© FORTINET

Zero Trust Telemetry—FortiClient Telemetry

- Displays whether FortiClient telemetry is connected to EMS
- Tab is used to manually connect FortiClient telemetry to EMS and to disconnect
- FortiClient Telemetry
 - FortiClient uses server IP address/FQDN or invitation code to connect FortiClient Telemetry



The **FortiClient Telemetry** tab displays whether FortiClient Telemetry is connected to EMS. You can use the **FortiClient Telemetry** tab to manually connect FortiClient Telemetry to EMS and to disconnect FortiClient Telemetry from EMS.

FortiClient can use a gateway IP address to connect FortiClient Telemetry to FortiClient EMS.

DO NOT REPRINT
© FORTINET

Zero Trust Telemetry—FortiClient Telemetry (Contd)

- Telemetry data
 - Hardware information, such as MAC addresses
 - Software information, such as the OS version on the endpoint
 - Identification information, such as username, avatar, and hostname
 - Vulnerability information that the vulnerability scanning module reports
- FortiClient automatically launches and connects telemetry to EMS after installation
- You can also manually enter the EMS IP address
- FortiClient can remember up to 20 IP addresses for EMS
- You must disconnect FortiClient telemetry to:
 - Connect another EMS
 - To disable and uninstall FortiClient

When FortiClient Telemetry is connected to EMS, FortiClient collects the hardware information (MAC addresses), software information (OS version on the endpoint), identification information (username, avatar, and hostname), and vulnerability information that the vulnerability scanning module reports about the endpoint and its workload, and sends it to EMS. When EMS participates in the Security Fabric, the Security Fabric uses the information to understand the endpoint and its workload to better protect it.

After installation, FortiClient automatically launches and connects telemetry to the EMS server that created the installed deployment package. You can also manually enter the EMS IP address or invitation code to connect. When you confirm the telemetry connection to EMS, you can instruct FortiClient to remember the EMS IP address. If a connection key is required, FortiClient remembers the connection key too. FortiClient can remember up to 20 IP addresses for EMS.

When you instruct FortiClient to forget an IP address for EMS, FortiClient Telemetry does not use the IP address to automatically connect to EMS when rejoining the network. You must disconnect FortiClient Telemetry from EMS to connect to another EMS or to disable and uninstall FortiClient.

DO NOT REPRINT
© FORTINET

Zero Trust Telemetry—Compliance

- Compliance depends on FortiClient EMS and FortiOS
- Because of changes to the license, all three components must be on 7.0.0
 - FortiClient 7.0.0
 - FortiClient EMS 7.0.0
 - FortiOS 7.0.0
- Administrator can define verification rules based on criteria:
 - Certificates
 - Logged-in domain
 - Files present
 - OS versions
 - Running processes
 - Registry keys
- FortiClient EMS dynamically groups the endpoints based on compliance verification rules
- FortiOS creates dynamic firewall policies

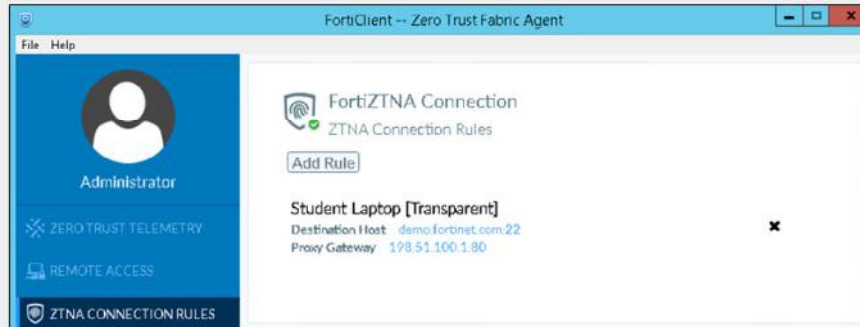
In FortiClient 7.0.0, compliance depends on FortiClient EMS and FortiOS. This feature is available only if you are using FortiClient 7.0.0 with FortiClient EMS 7.0.0 and FortiOS 7.0.0. Because of changes to the license, you can't have a mixed version environment.

The administrator can define compliance verification rules on FortiClient EMS based on criteria, such as certificates, the logged-in domain, files present, OS versions, running processes, and registry keys. When a FortiClient endpoint registers on the FortiClient EMS, FortiClient EMS dynamically groups the endpoint based on the compliance verification rules. FortiOS can receive the dynamic endpoint groups from FortiClient EMS and use them to create dynamic firewall policies. The endpoint may be unable to access the network based on the compliance verification rules.

DO NOT REPRINT
© FORTINET

ZTNA Connection Rules

- Provide secure encrypted connection without using VPN
- FortiClient works with FortiGate, which acts as local proxy gateway
- Secure connection (HTTPS) uses a certificate received from EMS includes FortiClient UID
- The UID is used to identify the device and, based on configuration, FortiGate allows or denies the access



Fortinet
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

25

ZTNA connection rules on FortiClient create a secure encrypted connection to protected applications without using VPN. FortiClient uses the FortiGate device application proxy feature to create a secure connection through HTTPS using a certificate received from EMS that includes the FortiClient UID. FortiGate acts as a local proxy gateway.

FortiGate retrieves the UID to identify the device and check other endpoint information that EMS provides to FortiGate, which can include other identity and posture information. The FortiGate allows or denies the access as applicable.

DO NOT REPRINT
© FORTINET

ZTNA Connection Rules (Contd)

- For TCP forwarding to non-web-based applications, you must define ZTNA connection rules
- It includes:
 - Rule Name
 - Destination Host (resource server IP address)
 - Proxy Gateway (FortiGate IP address)
 - Mode

The screenshot shows a 'Create Ztna Rule' window with the following configuration:

Ztna Rule Configuration	
Rule Name	Student Laptop
Destination Host	demo.fortinet.com:22
Proxy Gateway	198.51.100.1:80
Mode	Transparent

Buttons: Create

Fortinet
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

26

On the **ZTNA Connection Rules** tab, for TCP forwarding to non-web-based applications, you must define ZTNA connection rules in FortiClient.

You must configure the following:

- Rule Name: allows you to enter the desired name for a rule.
- Destination Host: allows you to enter the IP address or FQDN and port number of the destination host/server.
- Proxy Gateway: allows you to enter the FortiGate device access IP address and port number.
- Mode: allows you to select **Transparent** mode for a connection.

FortiClient Malware Protection

- Includes antivirus protection, anti-ransomware, cloud-based malware protection, anti-exploit and removable media access
- FortiClient AV includes:
 - Botnet communication detection
 - Enhanced real-time protection
- FortiClient can scan:
 - System files
 - Executable files
 - Removable media
 - DLL files and drivers
 - System memory
- File-based malware, malicious websites, phishing, and spam URL protection is included in antivirus protection

FortiClient has enhanced capabilities for the detection of malware. The protection includes antivirus protection, anti-ransomware, cloud-based malware protection, anti-exploit and removable media access

In FortiClient antivirus, when you enable the botnet feature, FortiClient monitors and compares network traffic on a compromised system with a list of known command and control servers, and blocks it.

The real-time protection (RTP) feature on FortiClient uses tight integration with Microsoft Windows to monitor files locally or over a network file system, as they are being downloaded, saved, run, copied, renamed, opened, or written to.

FortiClient can scan system files, executable files, removable media, dynamic-link library (DLL) files, memory, and drivers. FortiClient also scans for and removes rootkits. File-based malware, malicious websites, phishing, and spam URL protection is part of the antivirus component.

DO NOT REPRINT
© FORTINET

FortiClient Web Filter

- Web Filter allows you to take action on web traffic based on URL category or custom URL filters
 - Block
 - Allow
 - Warn
 - Monitor
- FortiGuard distribution network (FDN) handles URL categorization
- Custom URL filter exclusion list overrides FDN
- Use web browser plugin for HTTPS web filtering on endpoints
 - Improves detection and enforcement of HTTPS sites

After FortiClient is registered to EMS, Web Filter configuration settings are pushed from the management device and are read-only on the FortiClient console.

Web Filter features allow you to block, allow, warn, and monitor web traffic based on URL category or custom URL filters. URL categorization is handled by the FDN. You can create a custom URL filter exclusion list, which overrides the FDN category.

The EMS administrator can enable a web browser plugin for HTTPS web filtering on the endpoint. This improves detection and enforcement of Web Filter rules on HTTPS sites. After this option is enabled, you must open the browser to approve installing the new plugin. The plugin is supported only for the Google Chrome browser on Windows platforms.

DO NOT REPRINT
© FORTINET

Remote Access—SSL and IPsec

- FortiClient supports both IPsec and SSL VPN
 - Can configure on the FortiClient console
 - Use EMS to provision VPN configuration
- Simplified VPN configuration
- Supports two-factor authentication with FortiToken
- Allows you to create multiple VPN profiles
- Allows you to activate VPN before login (Windows and AD environment)
- Allows you to create redundant IPsec and priority-based SSL VPNs (Windows and Mac OS)



Remote Access

VPN Name: Student_SSL

Username:

Password:

Token:

Buttons: FTM Push, OK, Cancel

Two-factor authentication
with FortiToken

Fortinet
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

29

FortiClient supports both IPsec and SSL VPN connections to your network for remote access. The FortiClient EMS administrator can provision client VPN connections in the FortiClient profile (EMS endpoint profile) or the endpoint user can configure new connections on the FortiClient console.

You can also configure two-factor authentication using FortiToken for enhanced security for both types of VPNs on your FortiGate device for FortiClient VPN connections.

FortiClient VPN features are not limited to basic configuration and provisioning, but can be used for advanced configurations. For example, you can automatically connect to a VPN when FortiClient is launched, or you can map or unmap a network drive when a tunnel is connected or disconnected, respectively.

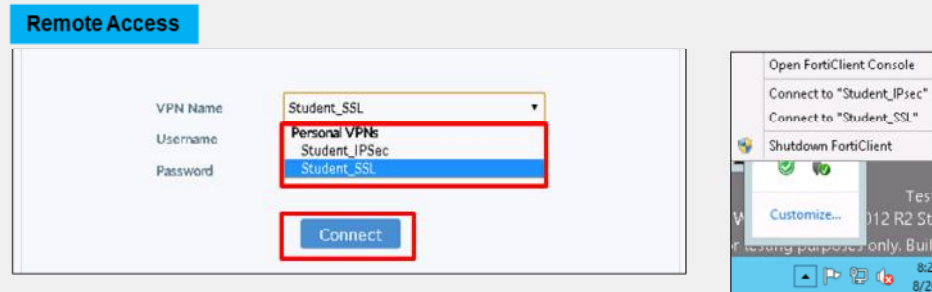
You can also configure FortiClient to connect to a VPN before the login in (either logging in to a Windows account, or through an AD environment). Advanced features like redundant IPsec VPN and priority-based SSL VPN are also supported on FortiClient for Windows and Mac OS.

DO NOT REPRINT
© FORTINET

Remote Access—Connect to VPN

- You can connect to VPN from the:

- FortiClient console
- FortiClient icon in system tray



To connect to a VPN (IPsec or SSL), select the VPN name from the drop-down list on the FortiClient console. Enter your username, password, and then click **Connect**. Optionally, in the system tray, right-click the FortiClient icon and select the VPN connection you want to connect to. When connected, the console displays the connection status, duration, and other relevant information.

Note that provisioned VPN connections are listed under **Corporate VPN**. Locally configured VPN connections are listed under **Personal VPN**.

DO NOT REPRINT
© FORTINET

Application Firewall

- Application control:
 - Application firewall
 - Block specific application traffic
- Read-only profile in the FortiClient console:
 - Allows you to view blocked applications—past 7 days
- Capable of recognizing network activity (application traffic):
 - Allows you to create rules to block or allow traffic per application or category

Application Firewall

Application Firewall Enabled
1 Violation in the Last 7 Days

Application Profile

- Block: Botnet/Social Media
- Allow: All Other Unknown Applications

Violations

Program	Application	Category	Count	Last Time
Firefox	Facebook	Social Media	3	9/16/2019 7:29:06 AM

Fortinet
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

31

You can use the application firewall feature to detect and take actions against network traffic, depending on the application that is generating the traffic. The application firewall uses IPS protocol decoders to analyze and detect application traffic, even on non-standard ports.

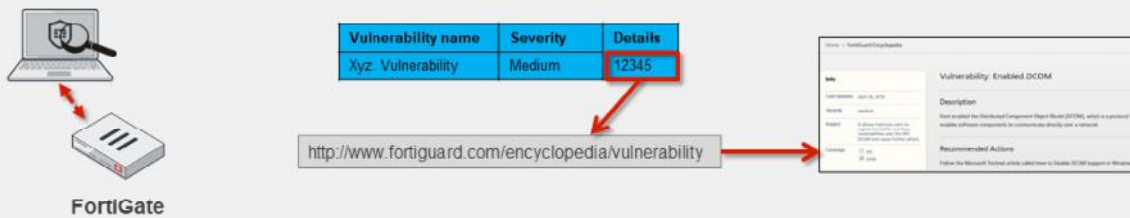
FortiClient can recognize the traffic generated by a large number of applications. You can create rules to block or allow application traffic on FortiGate or EMS, based on the category or application. The rules are then pushed to the managed FortiClient.

Application firewall settings are read-only on the FortiClient console. You can view blocked applications for the past seven days.

DO NOT REPRINT
© FORTINET

Vulnerability Management

- Vulnerability management
 - List of vulnerabilities detected
 - One-click link to install patches and resolve as many identified vulnerabilities as possible
 - List of patches that require manual installation by the endpoint user to resolve vulnerabilities
- Managed by EMS, an administrator may configure and lock vulnerability scanning for you



Fortinet NSE Training Institute

© Fortinet Inc. All Rights Reserved.

32

When endpoint users are transferring data over the internet, hackers can exploit vulnerabilities in endpoint devices, and use those vulnerabilities to gain unauthorized access to the system.

FortiClient can perform a vulnerability scan to search endpoint devices to identify weaknesses, provide details about the impact of those weaknesses and recommend actions to protect the applications running on the endpoint devices.

FortiClient communicates with the FortiGuard Center to get the signature updates.

After the scan is complete, FortiClient displays the list of vulnerabilities and details. You can click an item in the list, such as release date, severity, impact, and recommended actions, to name a few.

DO NOT REPRINT
© FORTINET

Logging

- Logging
 - VPN, application firewall, antivirus, web filter, update, and vulnerability scan logging
 - Export or clear logs
 - Default logging level is **Information**

Logging Level	Description
Emergency	The system becomes unstable
Alert	Immediate action is required
Critical	Functionality is affected
Error	An error condition exists and functionality could be affected
Warning	Functionality could be affected
Notice	Information about normal events
Information	General information about system operations
Debug	Debug FortiClient

You can export the log file (.log) from FortiClient.

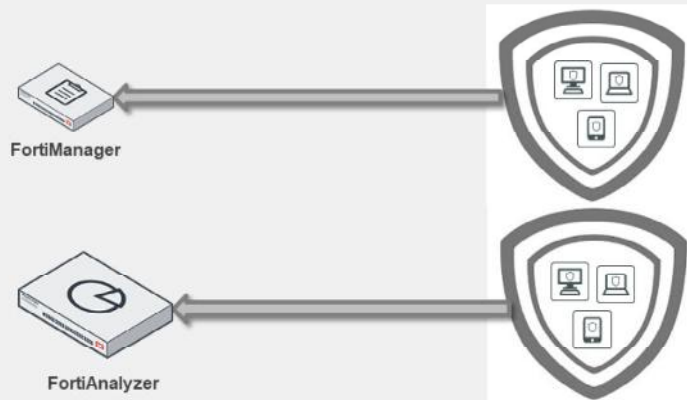
FortiClient provides options for logging levels, such as information, notice, or emergency. When FortiClient is managed by FortiClient EMS, the administrator can configure the XML configuration to set the logging levels.

The default logging level on FortiClient is **Information**.

DO NOT REPRINT
© FORTINET

Logging and Software Inventory

- Logging and Software Inventory
 - Upload logs to FortiAnalyzer or FortiManager
 - FortiClient must be registered to FortiClient EMS to upload logs to FortiAnalyzer or FortiManager
- Use TCP port 514



Fortinet NSE Training Institute

© Fortinet Inc. All Rights Reserved.

34

You can configure FortiClient to send logs and software inventory reports to FortiAnalyzer or FortiManager. You need the following products:

- FortiClient
- FortiClient EMS
- FortiAnalyzer or FortiManager

FortiClient uses TCP port 514 to upload to FortiAnalyzer or FortiManager. FortiClient collects information on regular software installed on the endpoint and sends the information to EMS and FortiAnalyzer. FortiClient sends the software inventory information when it first registers on EMS and when it first sends data to FortiAnalyzer. If software changes occur on the endpoint, such as installing new software, updating existing software, or removing existing software, FortiClient sends an updated inventory to EMS and FortiAnalyzer.

FortiClient Telemetry must connect to EMS for FortiClient to upload logs and software inventory reports to FortiAnalyzer or FortiManager.

Note that you must enable logging on FortiManager. By default, this feature is disabled.

DO NOT REPRINT
© FORTINET

Feature Support

	WINDOWS (all variants)	MAC OS X	ANDROID	IOS	CHROMEBOOK	LINUX
Security Fabric Components						
Endpoint Telemetry	✓	✓	✓	✓	✓	✓
Compliance Enforcement using Dynamic Access Control	✓	✓	✓	✓		✓
Endpoint Audit and Remediation with Vulnerability Scanning	✓	✓				✓
Automated Endpoint Quarantine	✓	✓				
Host Security and VPN Components						
Antivirus	✓	✓				✓
Cloud-based Threat Detection	✓					
Anti-Exploit	✓					
Sandbox Detection (on-prem)	✓	✓				✓
Sandbox Cloud Detection	✓					
Web Filtering	✓	✓	✓	✓	✓	
Application Firewall	✓	✓				
IPsec VPN	✓	✓	✓			
SSL VPN	✓	✓	✓	✓		✓
Others						
Remote Logging and Reporting	✓	✓		✓	✓	✓
Windows AD SSO Agent	✓	✓				
USB Device Control	✓	✓				✓
PLUS - Add Sandbox Cloud Subscription for Proactive Advanced Threat Detection						

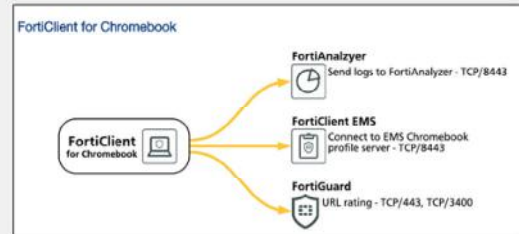
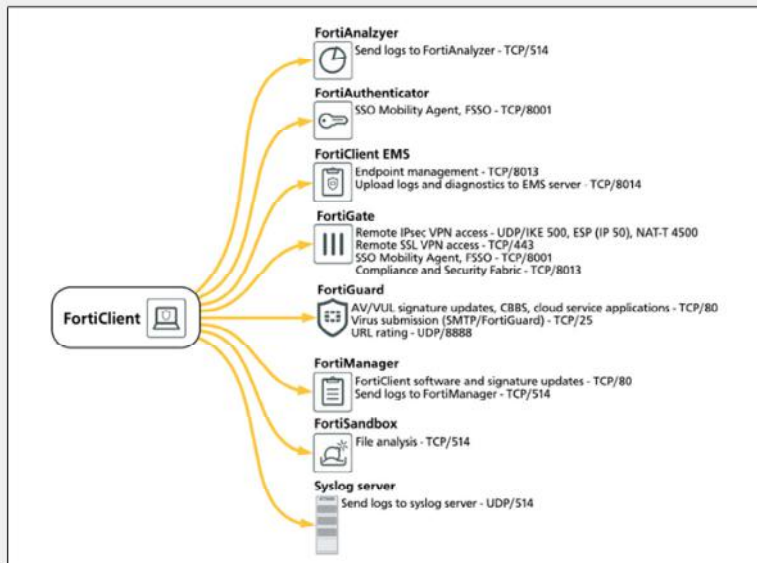
FortiClient 7.0.0 supports a number of features, such as VPNs, antivirus, web filtering, and more. When FortiClient is registered with FortiGate or FortiClient EMS, it enhances comprehensive security, helping you to safeguard your systems with advanced security technologies, which are all managed from a single management console with easy provisioning, monitoring, and auditing.

You can also customize the FortiClient installation and use VPN auto-connect to ensure that FortiClient creates a VPN connection to FortiGate when it is considered to be off-net. FortiClient also supports configuration provisioning for iOS (.mobileconfig files) in addition to FortiClient configuration provisioning.

DO NOT REPRINT
© FORTINET

FortiClient Ports

• Ports



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

36

You use FortiClient ports to communicate with other Fortinet products.

Note that Chromebook port TCP 3400 for URL rating is only used with EMS.

DO NOT REPRINT
© FORTINET

Knowledge Check

1. Which features are included in FortiClient malware protection?
 - A. Antivirus, vulnerability scan, and sandbox integration
 - ✓ B. Antivirus, anti-exploit, and cloud-based malware

2. Which VPN types are supported in FortiClient?
 - A. IPsec and PPTP
 - ✓ B. IPsec and SSL

DO NOT REPRINT
© FORTINET

Lesson Progress



What Is FortiClient?



FortiClient EMS



FortiClient Features

Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in this lesson.

DO NOT REPRINT
© FORTINET

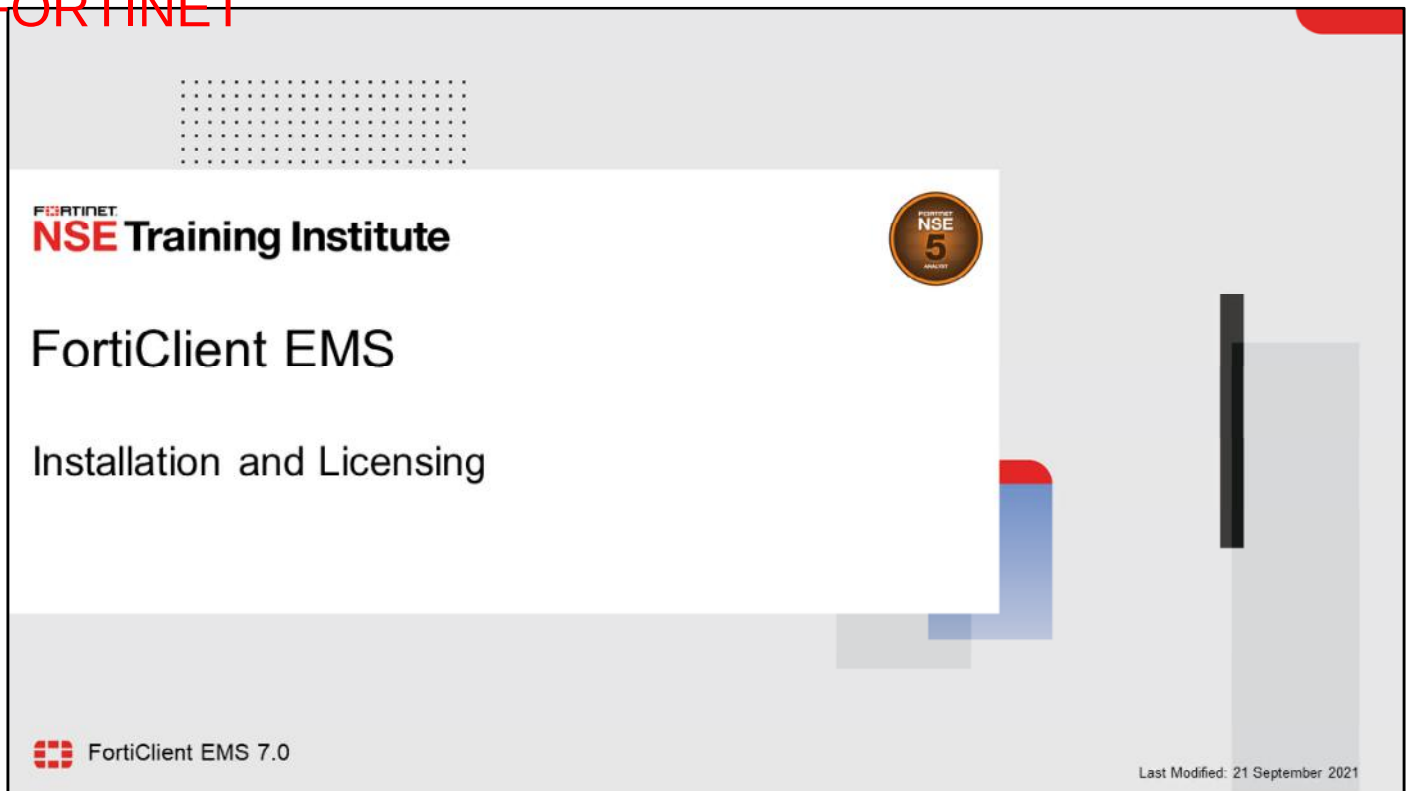
Review

- ✓ Know when and why FortiClient endpoint security is needed
- ✓ Understand FortiClient
- ✓ Understand FortiClient Editions
- ✓ Understand FortiClient EMS
- ✓ Understand the purpose of FortiClient EMS
- ✓ Identify FortiClient EMS components
- ✓ Identify FortiClient security features

This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned how to use FortiClient features and options to install and use FortiClient to secure endpoints in your network.

DO NOT REPRINT
© FORTINET



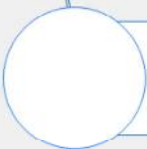
In this lesson, you will learn how to install FortiClient and FortiClient EMS. You will also learn about FortiClient editions and FortiClient EMS operation modes.

DO NOT REPRINT
© FORTINET

Lesson Overview



FortiClient Installation



FortiClient EMS Installation



FortiClient EMS Operation Modes

In this lesson, you will learn about the topics shown on this slide.

DO NOT REPRINT
© FORTINET

FortiClient Installation

Objectives

- Identify FortiClient installation files and tools

FORTINET
NSE Training Institute

3

After completing this section, you should be able to achieve the objective shown on this slide.

By demonstrating competence in identifying and understanding FortiClient installation options, tools, and features, you will be able to select the appropriate options, editions, and tools to install FortiClient in your network.

FortiClient Firmware Images and Tools

- Windows
 - FortiClientSSOSetup_7.0.0.xxxx.zip FSSO-only installer (32-bit).
 - FortiClientSSOSetup_7.0.0.xxxx_x64.zip FSSO-only installer (64-bit)
 - FortiClientTools_7.0.X.XXXX.zip for Windows contains:
 - FortiClientVirusCleaner
 - SupportUtils
 - VPNAutomation
 - SSLVPNcmdline
- Mac OS
 - FortiClientTools_7.0.X.XX_macosx.tar for Mac OS contains:
 - OnlineInstaller
 - RemoveFCTID
- Linux
 - forticlient_7.0.x.xxxx_amd64.deb
 - forticlient_7.0.0.xxxx_x86_64.rpm
 - forticlient_vpn_server_7.0.0.xxxx_amd64.deb
 - forticlient_vpn_server_7.0.0.xxxx_x86_64.rpm

The files mentioned are available in the firmware image file folder on the Fortinet Support Portal.

The FortiClient tools package contains various tools you can use to customize your FortiClient installation. The FortiClientVirusCleaner tool was developed to identify and cleanse systems of viruses.

SupportUtils folder contains various tools:

- RemoveFCTID.exe: is a tool to remove the unique identifier
- FCRemove.exe: is a cleanup tool for use only if the **Add/Remove Programs** applet fails to remove FortiClient
- ReinstallNIC.exe: is a tool for use on Windows 7 if DHCP address allocation is slow
- FortiClient_Diagnostic_Tool.exe: is a tool to gather information, such as the FortiClient connection to FortiGuard Distribution Server (FDS), general system information, and installed feature information, all of which can be useful for troubleshooting

VPNAutomation includes FCCOMIntDLL.tlb, which is a type of library needed for building applications that use the FortiClient IPsec VPN COM interface, and SSLVPNcmdline includes FortiSSLVPNClient.exe, which is a command line tool for controlling SSL-VPN tunnels.

The Mac OS X FortiClient tools file contains an online installer which downloads and installs the latest FortiClient file from the public FDS, and RemoveFCTID.exe to remove the unique identifier.

For files in the Linux folder, refer to this slide.

DO NOT REPRINT

© FORTINET

Installation Packages

- MSI and EXE files are available on EMS when administrator creates a deployment package
- Administrator provides a download link or files
 - FortiClient_7.0.X_x64.exe
 - FortiClient_7.0.X_x86.exe
 - FortiClientSetup_7.0.X.XXXX.zip–FortiClient.msi and language transforms for Microsoft Windows (32-bit)
 - FortiClientSetup_7.0.X.XXXX_x64.zip–FortiClient.msi and language transforms for Microsoft Windows (64-bit)
- MSI package can be deployed using Microsoft Active Directory (AD) server or Microsoft SCCM 2012
- FortiClient_7.0.X_macosx.dmg for Mac OS

In 7.0.0 or later, the FortiClient (Windows and MacOS) installers are available on EMS. You can configure and select installed features and options on EMS. The administrator configures a FortiClient deployment package in EMS that includes an EXE and MSI file. The administrator specifies which modules to install in the deployment package. The EMS administrator will provide a download link to the FortiClient installation files.

MSI installers are supported in Microsoft Windows environments only.

FortiClientSetup_7.0.X.zip: A zip package containing `FortiClient.msi` and language transforms for 32-bit Windows. Some properties of the MSI package can be customized with a custom installer.

FortiClientSetup_7.0.X_x64.zip: A zip package containing `FortiClient.msi` and language transforms for 64-bit Windows. Some properties of the MSI package can be customized with a custom installer.

The MSI installer in the ZIP file package is customizable for a larger rollout to many computers in an organization.

DO NOT REPRINT

© FORTINET

FortiClient Installation

- Installing FortiClient on infected systems
 - FortiClient installer always runs a quick AV scan on the target host system
 - If the system is clean, the installation proceeds as usual
 - Viruses found during installation are quarantined before installation continues
- Installing FortiClient as part of cloned disk images
 - Must remove the unique identifier from the FortiClient application using a cloned hard disk image
 - FortiGate will encounter problems if multiple FortiClient applications are deployed with the same identifier
 - Run `RemoveFCTID.exe`
- Installing FortiClient using the CLI
 - You can install FortiClient using the CLI
 - Installation options available are shown in the table

Option	Description
<code>/quiet</code>	Installation is in quiet mode and requires no user interaction
<code>/passive</code>	Installation is in unattended mode, showing only the progress bar
<code>/norestart</code>	Does not restart the machine after installation is complete
<code>/promptrestart</code>	Prompts you to restart the machine if necessary
<code>/forcerestart</code>	Always restarts the machine after installation
<code>/uninstall</code>	Uninstalls FortiClient
<code>/log"<LogFile>"</code>	Creates a log file with the specified name

The FortiClient installer always runs a quick AV scan on the target host system before proceeding with the complete installation. If the system is clean, the installation proceeds as normal. Any virus found during this step is quarantined before installation continues. In case a virus on an infected system prevents you from downloading the new FortiClient package, use the following process:

1. Boot into **Safe mode with networking**. This is required for the FortiClient installer to download the latest signature packages from the Fortinet Distribution Network.

2. Run the FortiClient installer.

The installer scans the entire file system. If a virus is found, it is quarantined. When the scan is complete, reboot into normal mode and run the FortiClient installer to complete the installation, (Windows does not allow FortiClient installation to complete in safe mode).

If you configure computers using a cloned hard disk image, you must remove the unique identifier from the FortiClient application. You will encounter problems with FortiGate if you deploy multiple FortiClient applications with the same identifier. You must use the following steps:

1. Install the FortiClient application.
2. Right-click the FortiClient icon in the system tray, and select **Shutdown FortiClient**.
3. From the folder where you expanded the `FortiClientTools.zip` file, run `RemoveFCTID.exe`. The `RemoveFCTID` tool requires administrative rights. Do not include the `RemoveFCTID` tool as part of a login script.
4. Shut down the computer. Do not reboot the Windows operating system on the computer before you create the hard disk image. The FortiClient identifier is created before you log in.
5. Create the hard disk image and deploy it, as needed.

You can also install FortiClient using the CLI. The table on this slide summarizes the installation options available when using the CLI. For example, `FortiClientSetup_7.0.0.1131_x64.exe /quiet /log"Log"` installs FortiClient 7.0.0 build 1131 in quiet mode, creating a log file with the name `Log`.

DO NOT REPRINT

© FORTINET

FortiClient Installation (Contd)

- You can deploy FortiClient using Microsoft AD servers
 - The required MSI and MST packages are available on the EMS server
- GPO is used for both deployment and uninstall process, general steps to deploy:
 - Create a distribution point
 - Create a shared network folder and set permissions to allow access to distribution package
 - Copy FortiClient MSI installer package
 - Copy FortiClient MST package
 - Create a group policy object
 - Select the groups you would like to install on FortiClient
 - Assign the package
 - Assign the package by selecting the path of your distribution point and the FortiClient installer file
 - FortiClient will be installed on the next client computer reboot
- Manual uninstallation requires the administrator to disconnect FortiClient from EMS
- Upgrade:
 - The EMS administrator controls the upgrade process on Windows OS endpoints
 - The endpoint user can postpone the reboot for 24 hours

You can deploy FortiClient installation using Microsoft AD servers. On your domain controller, create a distribution point and a shared network folder to distribute the FortiClient MSI installer file that is available from FortiClient EMS. Set file permissions on the shared folder to allow access to the distribution package. Now copy the FortiClient MSI installer and MST package into this shared folder.

In your domain, add a new organizational unit (OU) and move all the computers you want to distribute the FortiClient software to, into the newly-created OU. Create a group policy object (GPO), and then create the FortiClient installer package. Force a GPO update. The software is installed on the next reboot of the client computer. You can also wait for the client computer to poll the domain controller for GPO changes and install the software then.

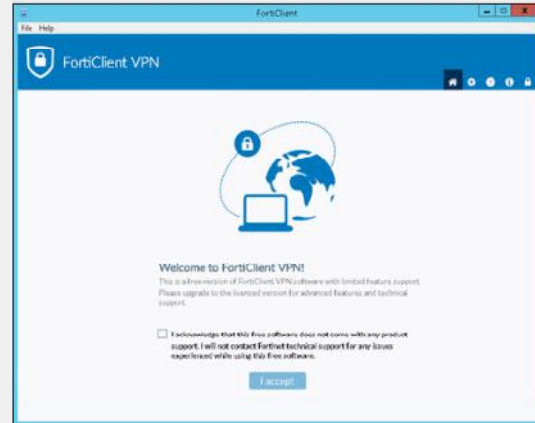
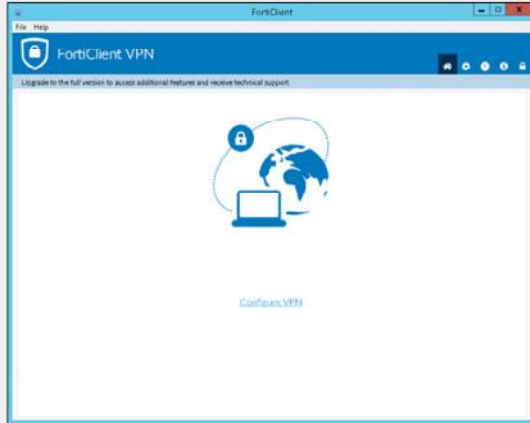
To uninstall FortiClient, you can either use a GPO or manual process. To do a manual uninstall, disconnect FortiClient from EMS. The endpoint is no longer managed by FortiClient EMS. Click **Unlock** to unlock the configuration and then shut down FortiClient. After FortiClient is shut down, uninstall FortiClient using the Windows **Add/Remove Programs** application.

An administrator will control FortiClient upgrades for you. When an administrator deploys a FortiClient upgrade from FortiClient EMS to endpoints running a Windows operating system, an **Upgrade Schedule** dialog opens on the endpoint to let endpoint users schedule the upgrade and mandatory endpoint reboot. If FortiClient is not installed on the endpoint, a reboot is not required for the installation, and the *Upgrade Schedule dialog does not open*. The endpoint user can postpone the reboot for a maximum of 24 hours. Before the mandatory reboot occurs, a FortiClient dialog opens giving you a 15 minute warning.

DO NOT REPRINT
© FORTINET

VPN-Only Installation

- There is a VPN-only client available
- You can download the installation files from www.fortinet.com



FortiClient 7.0.0 offers a free VPN-only version that you can use for VPN-only connectivity to FortiGate. You can download the VPN-only application from www.fortinet.com. You cannot use the VPN-only client with the FortiClient Single Sign-On Mobility Agent (SSOMA). To use VPN and SSOMA together, you must purchase an FortiClient EMS license.

DO NOT REPRINT
© FORTINET

Knowledge Check

1. During installation, which FortiClient component is selected by default, and cannot be removed?
 - A. Advanced persistent threat
 - ✓ B. Zero Trust Telemetry

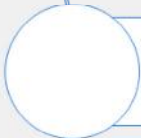
2. Which installation package can you use to install a custom FortiClient?
 - ✓ A. MSI package
 - B. Online installer

DO NOT REPRINT
© FORTINET

Lesson Progress



FortiClient Installation



FortiClient EMS Installation



FortiClient EMS Operation Modes

Good job! You now know about FortiClient installation files and tools.

Now, you will learn about FortiClient EMS installation.

DO NOT REPRINT
© FORTINET

FortiClient EMS Installation

Objectives

- Understand system requirements
- Identify license types
- Identify services and ports
- Identify the FortiClient EMS installation file
- Understand installation using a GUI and a CLI

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in installing and licensing FortiClient EMS, you will be able to understand system requirements, and identify license types, services, and ports. You will also know how to use the FortiClient EMS installation file to install FortiClient EMS using the GUI and the CLI.

DO NOT REPRINT
© FORTINET

FortiClient EMS—System

- System requirements:
 - The minimum system requirements for FortiClient EMS are as follows:
 - Microsoft Windows Server 2008 R2 or later
 - 2.0 GHz 64-bit processor, dual core (or two virtual CPUs)
 - 4 GB RAM (8 GB RAM, or more, is recommended)
 - 40 GB free hard disk
 - Gigabit (10/100/1000baseT) Ethernet adapter
 - Internet access
- Management capacity:
 - FortiClient EMS is intended for use by enterprises
 - FortiClient has the capacity to manage a large number of endpoints
 - Fortinet recommends you have at least 200

You should read the *FortiClient EMS Release Notes* to become familiar with the relevant software components and other important information about the product.

Internet access is required during installation. This becomes optional after installation is complete. FortiClient EMS accesses the internet to obtain information about FortiGuard engine and signature updates.

Note that you should install only FortiClient EMS and the default services for the operating system on the server. You should not install additional services on the same server as FortiClient EMS.

DO NOT REPRINT

© FORTINET

FortiClient EMS—Licenses

- Types of FortiClient EMS license bundles for Windows, macOS, and Linux endpoints
 - Endpoint protection platform (EPP)
 - Zero trust network access (ZTNA)
- Must purchase a minimum of 25 endpoint licenses
- Chromebook licenses
 - A Chromebook license allows management of one Google Chromebook user
- Component applications
 - Common services or applications do not require a license
- Managed services license
 - FortiClient Managed services to streamline the configuration, deployment, and monitoring of FortiClient agents

The following are the latest license bundles:

- EPP is a full license that offers all FortiClient features. Includes all features detailed for the ZTNA license, as well as antivirus (AV), anti-ransomware, anti-exploit, cloud-based malware detection, application firewall, software inventory, and advanced threat protection via FortiClient Cloud Sandbox.
- ZTNA includes support for fabric agent for endpoint telemetry, security posture check through ZTNA tagging, remote access (SSL and IPsec VPN), vulnerability scan, web filter, threat protection through sandbox (appliance only) and USB device control. Each purchased ZTNA license allows management of one FortiClient Windows, macOS, Linux, iOS, Android, or Chromebook endpoint.

You must purchase a minimum of 25 endpoint licenses.

A Chromebook license allows management of one Google Chromebook user. You must purchase a minimum of 25 Google Chromebook user licenses.

Fortinet also offers FortiClient managed services to streamline the configuration, deployment, and monitoring of FortiClient agents in the cloud. Services include initial FortiClient cloud provisioning, endpoint onboarding, security fabric setup and integration, and endpoint vulnerability monitoring. This also includes BPS (Best Practice Service) which is an account-based annual subscription providing access to a specialized team that delivers remote guidance on deployment, upgrades, and operations.

FortiClient EMS uses one license seat per logged-in user. If the user logs out, the license seat times out (default timeout value is 30 days), and the license is released. At this point, another user can use this license seat.

FortiClient EMS—Services and Ports

- You must enable the required ports and services for use by FortiClient EMS

Communication	Usage	Protocol	Port	Incoming/Outgoing	How to customize
FortiClient Telemetry	FortiClient endpoint management	TCP	8013 (default)	Incoming	Installer/GUI
Samba (SMB) service	FortiClient EMS uses the SMB service during FortiClient initial deployment	TCP	445	Outgoing	N/A
Distributed Computing Environment / Remote Procedure Calls(DCE/RPC)	The FortiClient EMS server connects to endpoints using RPC for FortiClient initial deployment	TCP	135 1024-5000 49152-65535	Outgoing	You can configure ranges
AD server connection	Retrieving workstation and user information	TCP	389 (LDAP) or 636(LDAPS)	Outgoing	GUI
FortiClient download	Downloading FortiClient deployment packages created by FortiClient EMS	TCP	10443 (default)	Incoming	Installer
Apache/HTTPS	Web access to FortiClient EMS	TCP	443	Incoming	Installer
FortiGuard	FortiGuard AV, vulnerability, and application version updates	TCP	80	Outgoing	N/A
SMTP server/email	Alerts for FortiClient EMS and endpoint events. When an alert is triggered, EMS sends an email notification	TCP	25 (default)	Outgoing	GUI
FortiClient endpoint probing	FortiClient EMS uses ICMP for endpoint probing during FortiClient initial deployment.	ICMP	N/A	Outgoing	N/A
Communication with FortiOS	EMS is the server that opens up the port for FortiOS to connect to as a client	TCP	8015	Incoming	N/A
FSSO	Connection to FortiOS	TCP	8000	Incoming	N/A

The table on this slide shows the ports and services that are required by FortiClient EMS to communicate with endpoints and servers running associated applications. You do not need to enable port 8013 and port 10443 on the server because the FortiClient EMS installation opens these.

FortiClient EMS—Services and Ports (Contd)

- FortiClient EMS services and ports to manage Chromebooks

Communication	Usage	Protocol	Port	Incoming/Outgoing	How to customize
The following ports and services only apply when using FortiClient EMS to manage Chromebooks:					
FortiClient on Chrome OS	Connecting to FortiClient EMS	TCP	8443 (default) You can customize this port.	Incoming	GUI
G suite API/Google Domain directory	Retrieving Google domain information using API calls	TCP	443	Outgoing	N/A
The following ports and services should be enabled for use on Chromebooks when using FortiClient for Chromebooks:					
FortiClient EMS	Connecting to the profile server	TCP	8443 (default)	Outgoing	Via Google Admin console when adding the profile
FortiGuard	Rating URLs	TCP	443, 3400	Outgoing	N/A
FortiAnalyzer	Sending logs to FortiAnalyzer	TCP	8443	Outgoing	N/A

The table on this slide shows the ports and services that are required by FortiClient EMS to communicate with Chromebook endpoints or Chromebook endpoints to communicate with FortiClient EMS.

FortiClient EMS—Services and Ports (Contd)

- FortiClient EMS services and ports to connect to FortiGuard to download signatures updates

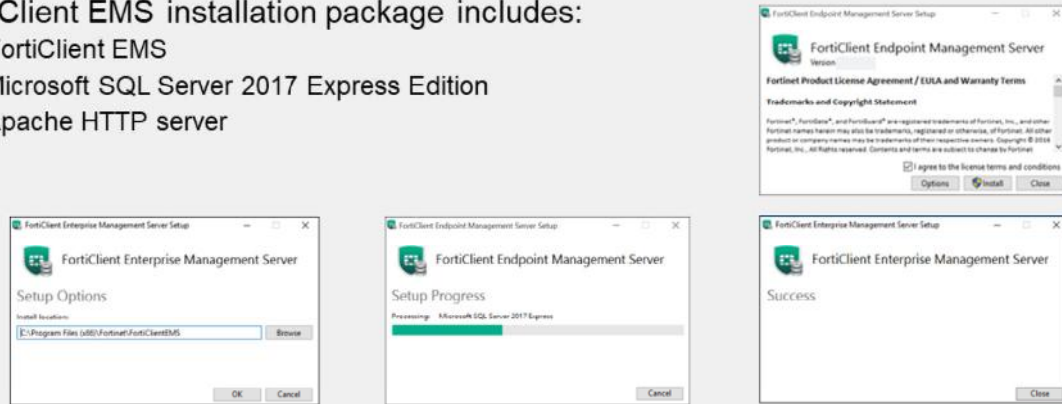
Usage	ServerURL Global	U.S.	Europe	Protocol	Port	Incoming/Outgoing
AV/vulnerability signature update	forticlient.fortinet.net	usforticlient.fortinet.net	N/A	TCP	80	Outgoing
AV/vulnerability signature updates with FortiGuard Anycast	fctupdate.fortinet.net	fctusupdate.fortinet.net	fcteuupdate.fortinet.net	TCP	443	Outgoing

The table on this slide shows the ports and services that are required by FortiClient EMS to communicate with FortiGuard to download AV and vulnerability scan engine and signature updates. FortiClient EMS can connect to legacy FortiGuard or FortiGuard Anycast.

DO NOT REPRINT
© FORTINET

FortiClient EMS—Installation File

- The installation file is available for download from the www.fortinet.com:
 - FortiClientEndpointManagementServer_7.0.xxxxx_x64.exe
- You can also receive the installation file from a sales representative
- FortiClient EMS installation package includes:
 - FortiClient EMS
 - Microsoft SQL Server 2017 Express Edition
 - Apache HTTP server



Fortinet
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

17

FortiClient EMS is available for download from the Fortinet Support website. You can also receive the installation file from a sales representative. The installation file available for FortiClient EMS is shown in this slide.

Note that local administrator rights and internet access are required to install FortiClient EMS.

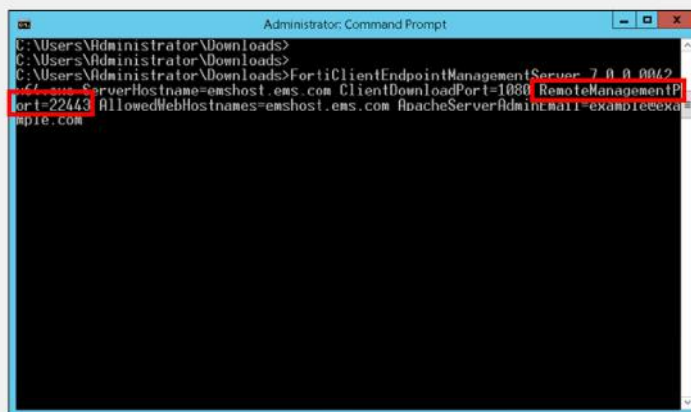
DO NOT REPRINT
© FORTINET

FortiClient EMS—Installation Using the CLI

- You can install FortiClient EMS using the CLI

- CLI options are:

- AllowedWebHostnames
- ApacheServerAdminEmail
- BackupDir
- ClientDownloadPort
- RemoteManagementPort
- InstallFolder
- InstallSQL
- ScriptDB
- ServerHostname
- SQLAuthType
- SQLCmdlineOptions="//INSTANCEDIR



```
Administrator: Command Prompt
C:\Users\Administrator\Downloads>
C:\Users\Administrator\Downloads>
C:\Users\Administrator\Downloads>FortiClientEndpointManagementServer 7.0.0.8042
-ServerHostname=emshost.ems.com ClientDownloadPort=1080 RemoteManagementP
ort=22443 AllowedWebHostnames=emshost.ems.com ApacheServerAdminEmail=exam
ple@example.com
```

You can install FortiClient EMS using the CLI.

The `AllowedWebHostnames` command allows you to configure the host name. The default value is `localhost, 127.0.0.1`. To clear this value, first enter `AllowedWebHostnames=*`, then enter the desired `AllowedWebHostnames` value. Otherwise, the value entered will be appended to `localhost, 127.0.0.1`.

In `ApacheServerAdminEmail` option, you can configure the Apache server administrator's email address. By default, this is `admin@yourcompany.com`. The `BackupDir` option allows you to enter the desired backup directory path for the SQL server. Similarly, `ClientDownloadPort` allows you to enter the customized HTTP port number and `RemoteManagementPort` allows you to enter the HTTPS port number. The default values are 80 (HTTP) and 443.

The image on this slide, shows FortiClient EMS installation using the CLI with a custom port (port 22443) for remote access.

For details on other CLI commands, refer to the *FortiClient EMS Administration Guide*.

Installation Using the CLI (Contd)

- CLI options:

- SQLCmdlineOptions="/INSTANCENAME"
- SQLEncryptConnection
- SQLPort
- SQLServer
- SQLServerInstance
- SQLService
- SQLTrustServerCertificate
- SQLUser
- SQLUserPassword
- WindowsUser
- WindowsUserPassword

FortiClientEnterpriseManagement_7.0.X.XXXX_x
64.exe

ServerHostname = emshost.ems.com

ClientDownloadPort = 11443

RemoteManagementPort = 22443

AllowedWebHostnames = emshost.ems.com

ApacheServerAdminEmail = example@example.com

Example of a customized
CLI installation

- Allows you to enable specific options during installation, such as customizing the SQL Server Express installation directory, using custom port numbers, and so on

Installation using the CLI allows you to enable specific options during installation, such as customizing the SQL Server Express installation directory, using custom port numbers, and so on.

Take a look at the example of a customized configuration during CLI installation, shown on the slide. Here, we use different ports for FortiClient download (11443) and management (22443) because default ports (10443 and 443) are used by pre-existing services running on Windows server.

DO NOT REPRINT
© FORTINET

FortiClient EMS—Uninstalling

- You can uninstall FortiClient EMS:
 - If migrating one EMS on-premise environment to another
 - If conflicting with another application or services
 - To perform fresh installation to resolve issues cause by upgrade or compatibility
- FortiClient EMS has dependencies on other applications
 - Browser for SQL Server 2017
 - Microsoft ODBC Driver 13 for SQL Server
 - Microsoft SQL Server 2012 Native Client
 - Microsoft SQL Server 2017 (64-bit)
 - Microsoft SQL Server 2017 Setup (English)
 - Microsoft SQL Server 2017 T-SQL Language Service
 - Microsoft Visual C++ 2017 Redistributable (x64) - 14.11.25325.0
 - Microsoft Visual C++ 2017 Redistributable (x86) - 14.11.25325.0
 - Microsoft VSS Writer for SQL Server 2017

You can uninstall FortiClient EMS in the following cases:

- If migrating one EMS on-premises environment to another new server
- If conflicting with another application or services running on server
- If performing a fresh installation to resolve issues cause by upgrade or compatibility

FortiClient EMS can be uninstalled using the Windows **Add or Remove Program**. FortiClient EMS installs the dependencies. If other applications on the same computer are not using them, you can uninstall them manually, after removing FortiClient EMS. The list of dependencies are shown on this slide.

DO NOT REPRINT
© FORTINET

Knowledge Check

1. What minimum amount of disk space does Fortinet require for FortiClient EMS?
✓ A. 40GB
B. 200GB

2. Which port is used by FortiClient for telemetry?
A. 10443
✓ B. 8013

DO NOT REPRINT
© FORTINET

Lesson Progress



FortiClient Installation



EMS Installation



FortiClient EMS Operation Modes

Good job! You now understand the system requirements to install FortiClient EMS. You also learned about license types, services, the FortiClient EMS installation file, as well as how to install FortiClient EMS using the GUI and CLI.

Now, you will learn about the FortiClient EMS operation modes.

DO NOT REPRINT
© FORTINET

The slide features a light gray background with a white rectangular area on the left containing the title and objectives. To the right of this area are several decorative gray rectangles of varying sizes and a vertical cyan bar with a red top. A small grid of dots is visible near the bottom right of the white area. The Fortinet logo and 'NSE Training Institute' text are in the bottom left, and the number '23' is in the bottom right.

FortiClient EMS Operation Modes

Objectives

- Understand FortiClient EMS operation modes
- Understand FortiClient Cloud

FORTINET
NSE Training Institute

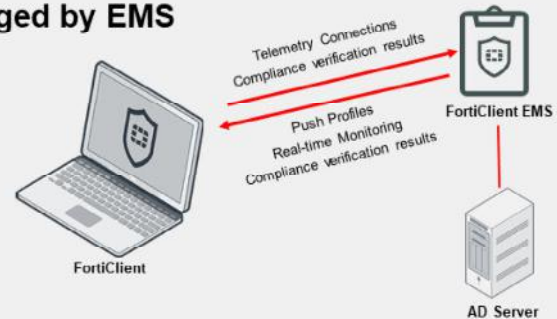
23

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence understanding FortiClient EMS operation modes and FortiClient Cloud, you will be able to use it effectively in your network.

Standalone Mode Without Security Fabric

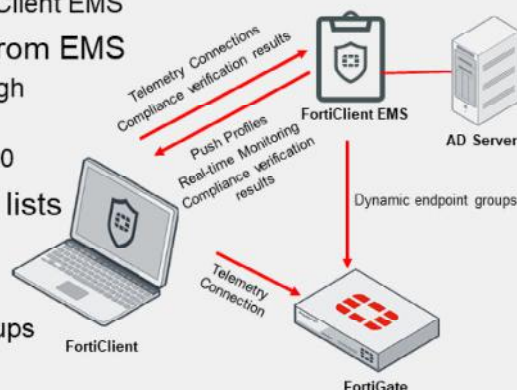
- FortiClient EMS provides FortiClient endpoint provisioning
- FortiClient endpoints connect zero trust telemetry to FortiClient EMS to receive configuration information from FortiClient EMS
- EMS sends Zero Trust Tagging rules to FortiClient
- EMS controls the connection between FortiClient and EMS
- FortiClient settings are locked
- Endpoint status shows as **Centrally Managed by EMS**



FortiClient EMS in standalone mode provides FortiClient endpoint provisioning. FortiClient endpoints connect FortiClient Telemetry to FortiClient EMS to receive configuration information in an endpoint profile, as part of an endpoint policy from FortiClient EMS. FortiClient EMS also sends compliance verification rules to FortiClient, and uses the results from FortiClient to dynamically group endpoints in EMS. Only EMS can control the connection between FortiClient and EMS. Any changes to the connection must be made from EMS, not from FortiClient. When FortiClient is connected to EMS, FortiClient settings are locked, so the endpoint user cannot change any configuration.

Integrated Mode With Security Fabric

- FortiClient EMS
 - Provides FortiClient endpoint provisioning
 - Connects to FortiGate to participate in the Security Fabric
 - Sends FortiClient endpoint information to the FortiGate
- FortiClient endpoints connect zero trust telemetry
 - To EMS to receive configuration information from FortiClient EMS
- FortiClient can also receive a device certificate from EMS
 - To securely encrypt and tunnel TCP and HTTPS through HTTPS to the FortiGate
 - This feature requires FortiClient 7.0.0 and FortiOS 7.0.0
- FortiGate also receives dynamic endpoint group lists from EMS
 - To build dynamic firewall policies
 - Use updates to adjust the policies based on those groups
 - Requires FortiOS 6.2 or a later version



You can integrate FortiGate with FortiClient EMS. In this scenario, FortiClient Zero Trust Telemetry connects to FortiClient EMS to receive a profile of configuration information as part of an endpoint policy and FortiClient EMS is connected to the FortiGate to participate in the Security Fabric. FortiClient EMS sends FortiClient endpoint information to the FortiGate.

FortiClient can also receive a device certificate from FortiClient EMS. FortiClient can use the device certificate to securely encrypt and tunnel TCP and HTTPS traffic through HTTPS to the FortiGate. This feature requires FortiClient 7.0.0 or a later, and FortiOS 7.0.0 or later.

FortiGate also receives dynamic endpoint group lists from FortiClient EMS and uses them to build dynamic firewall policies. FortiClient EMS sends group updates to FortiOS, and FortiOS uses the updates to adjust the policies based on those groups. This feature requires FortiOS version 6.2.0 or a later.

Note that FortiGate does not provide configuration information for FortiClient and the endpoint. An administrator must configure FortiClient using an FortiClient EMS endpoint policy.

DO NOT REPRINT
© FORTINET

FortiClient Cloud

- Fortinet-hosted EMS solution
- Component of FortiSASE SIA
- Use cloud-based SaaS endpoint management service
- Provides protection for remote, off-net endpoints
- Requirements:
 - FortiCloud account with FortiClient Cloud subscription
 - Internet access
 - Web browser
- You can manage the following:
 - Windows
 - macOS
 - Linux
 - iOS
 - Android

A cloud-based SaaS endpoint management service called FortiClient Cloud is available. This is a Fortinet-hosted EMS solution. You can execute EMS functions from the cloud-based FortiClient EMS. You must complete the following steps to create a cloud-based EMS instance under your FortiCloud user account:

1. Register a FortiClient Cloud subscription to your FortiCloud account.
2. Register a FortiClient license contract for management by FortiClient Cloud to your FortiCloud account.

FortiClient Cloud is a component of FortiSASE SIA, a cloud-based SaaS service that offers protection for remote, off-net endpoints. FortiSASE SIA works only with a new FortiClient Cloud instance. You cannot apply a FortiSASE SIA license to an existing FortiClient Cloud instance.

The following items are required to initiate a FortiClient Cloud instance:

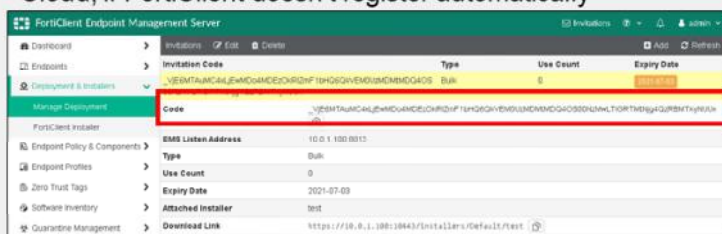
- A FortiCloud account with FortiClient Cloud subscription
- Access to create a FortiClient Cloud instance
- A browser to access FortiClient Cloud GUI

Note that you can create only one FortiClient Cloud instance per FortiCloud account. You can manage the following endpoints:

- Windows
- macOS
- Linux
- iOS
- Android

FortiClient Cloud (Contd)

- The following actions are required to deploy FortiClient (Windows OS) when using FortiClient Cloud
 - Administrator creates deployment package and note the invitation code
 - Administrator creates an invitation and sends the code for registration
 - Administrator shares the FortiClient installer files or sends a FortiClient download link
 - Enduser installs FortiClient on their device
 - Enduser uses invitation code to register to FortiClient Cloud, if FortiClient doesn't register automatically
- You can connect FortiGate as a fabric device to FortiClient Cloud
- Limitations of FortiClient Cloud
 - Manage and provision up to 20000 endpoints
 - Initial FortiClient deployment for Active Directory devices not supported



FortiNSE Training Institute

© Fortinet Inc. All Rights Reserved.

27

When installing FortiClient on the Windows endpoint from a deployment package created in FortiClient Cloud, the administrator carries out some actions, while the endpoint user carries out others, as shown on this slide. Since you can not create deployment packages for FortiClient Linux, iOS, or Android endpoints, you must use the invitation code provided by the administrator, to join FortiClient Cloud. You can type the code in the **Join FortiClient Cloud** field on the **Zero Trust Telemetry** tab in FortiClient.

FortiGate can connect to FortiClient Cloud as a Security Fabric device. You must authorize a connection request from FortiGate, to allow a fabric connection between FortiClient Cloud and the FortiGate.

Although FortiClient Cloud functions are the same as those for an on-premises FortiClient EMS, there are some limitations:

- FortiClient Cloud can support only up to 20000 endpoints. If there are more than 20000 endpoints, you must use an on-premises FortiClient EMS.
- Active directory (AD) integration is supported but FortiClient cloud does not currently support initial FortiClient deployment to AD devices.

DO NOT REPRINT
© FORTINET

FortiClient Cloud (Contd)

Feature	FortiClient Cloud	On-premise EMS
Security Fabric Integration		
Share endpoint telemetry data with FortiGate and FortiAnalyzer	FortiGate connector	FortiGate and FortiAnalyzer connector
Dynamic access control	Yes	Yes
Zero Trust tags	Yes	Yes
FortiSASE SIA support	Yes	No
Secure remote access		
IPSec and SSL VPN agents	Yes	Yes
SSO	Yes	Yes
Web Filter		
Web Filter	Yes	Yes
Web Filter for iOS and Android	Yes	Yes
Import WF policy from FortiOS	Yes	Yes
Browser plugin support	Depends on the endpoint OS and installed FortiClient version	Depends on the endpoint OS and installed FortiClient version

The table on this slide shows a comparison of FortiClient Cloud and on-premises FortiClient EMS.

DO NOT REPRINT
© FORTINET

FortiClient Cloud (Contd)

Feature	FortiClient Cloud	On-premise EMS
Endpoint hardening, visibility, and discovery		
Vulnerability scan	Yes	Yes
Patching	Yes	Yes
Application inventory	Yes	Yes
Application control	Yes	Yes (6.4.2 and later versions)
Endpoint protection and prevention		
Antimalware	Yes (CPRL)	Yes (CPRL)
Antiexploit	Yes	Yes
Application Firewall	Yes	Yes
Fileless malware scanning through AMSI	Yes	Yes (6.4.2 and later versions)
Sandbox integration	Yes	Yes
Deployment and management console		
Management console	Cloud-based management console	On-premise, self-hosted by customer. Requires WinServer

This slide shows a continuation of the comparison table.

DO NOT REPRINT
© FORTINET

Knowledge Check

1. Which type of information does FortiClient EMS in standalone mode not support?
 - A. FortiClient configuration information
 - ✓ B. Group updates to adjust policies

2. Which of these devices provide tagging?
 - A. FortiGate
 - ✓ B. FortiClient EMS

DO NOT REPRINT
© FORTINET

Lesson Progress



FortiClient Installation



FortiClient EMS Installation



FortiClient EMS Operation Modes

Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in this lesson.

DO NOT REPRINT
© FORTINET

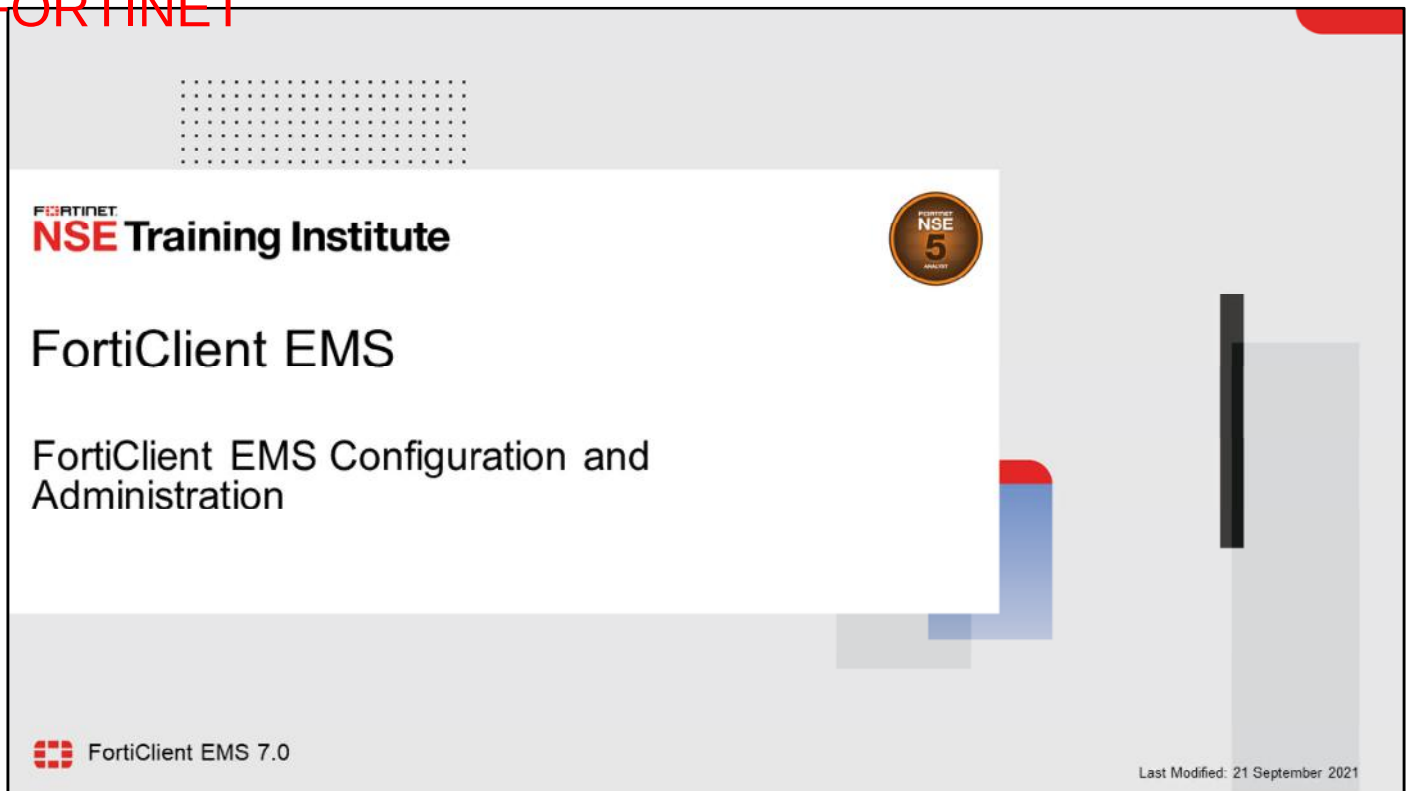
Review

- ✓ Identify FortiClient installation files and tools
- ✓ Understand system requirements
- ✓ Identify license types
- ✓ Identify services and ports
- ✓ Identify the FortiClient EMS installation file
- ✓ Understand installation using a GUI and CLI
- ✓ Understand FortiClient EMS operation modes
- ✓ Understand FortiClient Cloud

This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned how to install FortiClient and FortiClient EMS. You also learned about FortiClient editions, FortiClient EMS Cloud, and operation modes.

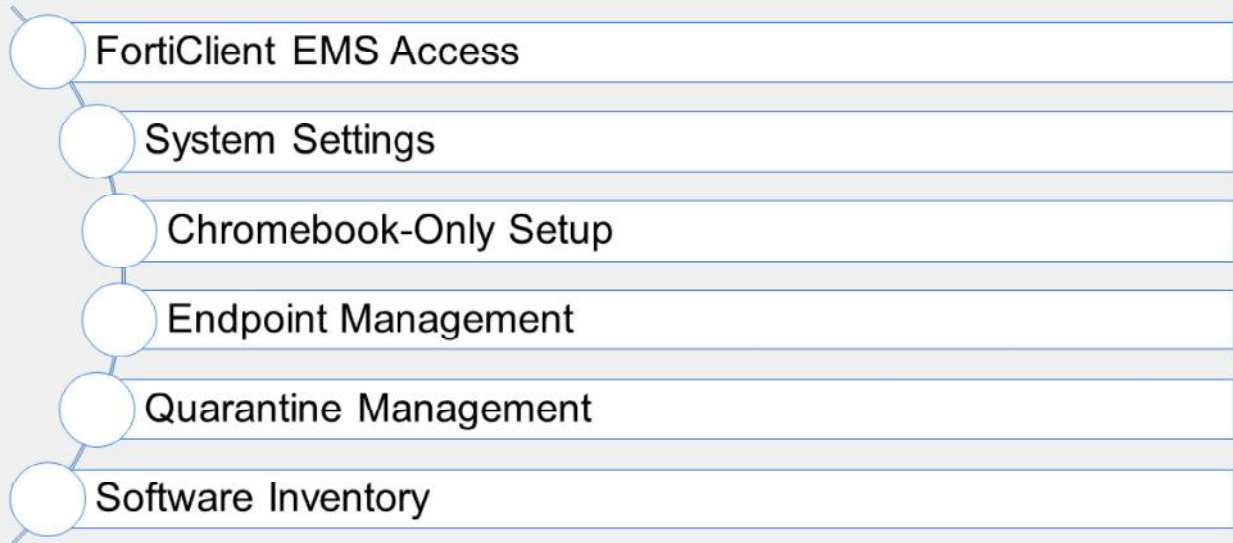
DO NOT REPRINT
© FORTINET



In this lesson, you will learn how to configure and administer FortiClient EMS. You will also learn how to manage a large number of endpoints.

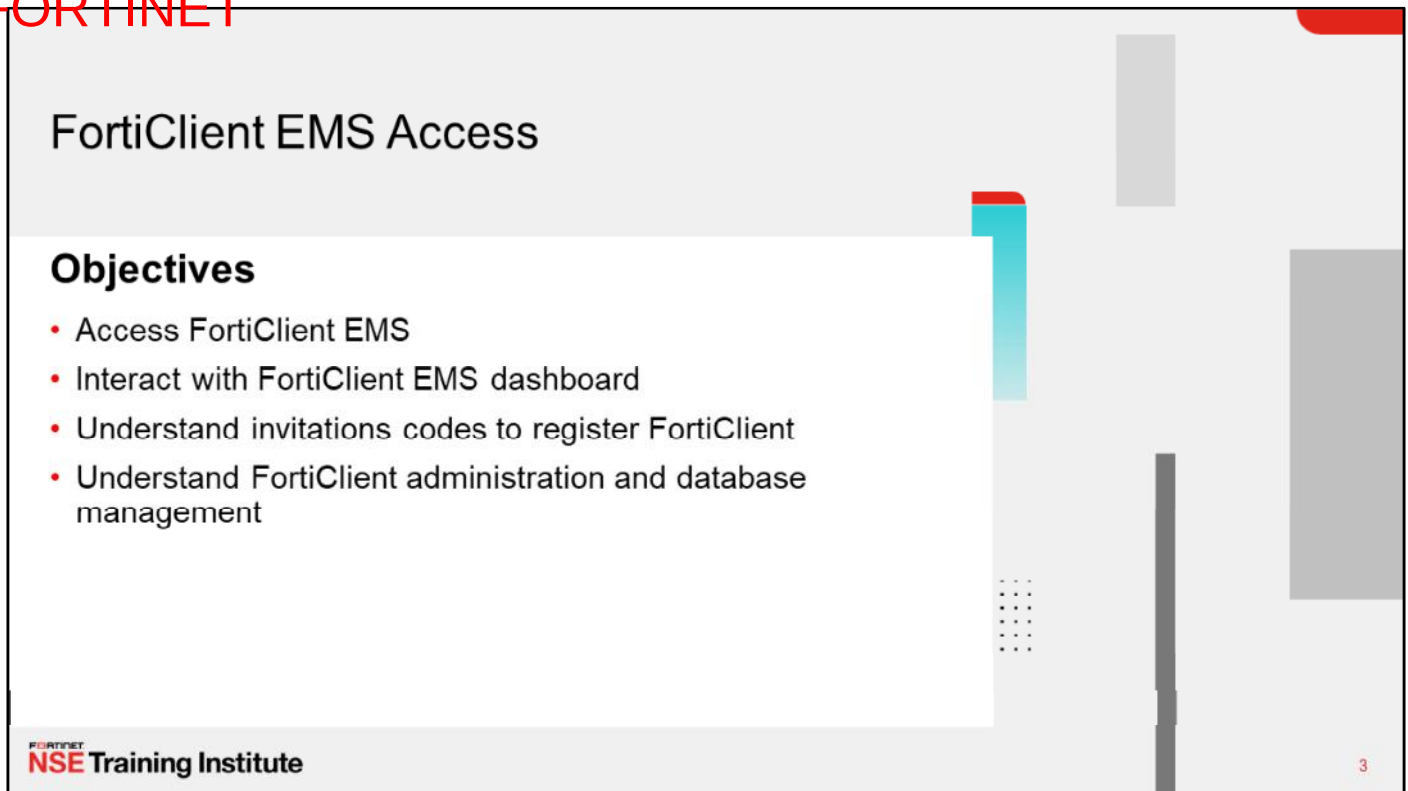
DO NOT REPRINT
© FORTINET

Lesson Overview



In this lesson, you will learn about the topics shown on this slide.

DO NOT REPRINT
© FORTINET



FortiClient EMS Access

Objectives

- Access FortiClient EMS
- Interact with FortiClient EMS dashboard
- Understand invitations codes to register FortiClient
- Understand FortiClient administration and database management

FORTINET
NSE Training Institute

3

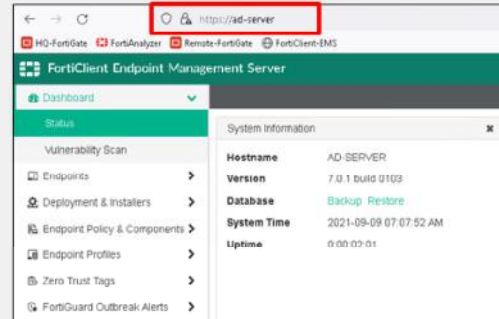
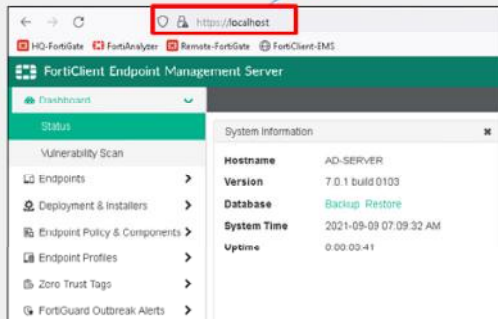
After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in understanding the management functions of FortiClient EMS, you will be able to perform FortiClient EMS administration and database management, and identify its components.

DO NOT REPRINT
© FORTINET

Endpoint Network Security

- Access FortiClient EMS by launching the application
- Access using a web browser
 - From EMS server: `https://localhost`
 - Remotely using server hostname – `https://<server_name>`



Fortinet NSE Training Institute

© Fortinet Inc. All Rights Reserved.

4

You can access FortiClient EMS by launching the FortiClient EMS application or by using a supported web browser. On the FortiClient EMS server, type `access localhost` via `https` in the web browser, and, if accessing remotely, use the server hostname or FQDN to access the page over the web.

You can get the server name by running the command `ipconfig /all` on the server. The host name will appear in the Windows IP configuration. If you are unable to access the server remotely, make sure you are able to ping `servername`, which you can do by adding it to the DNS entry or Windows host file. You may have to modify the firewall rules to allow the connection.

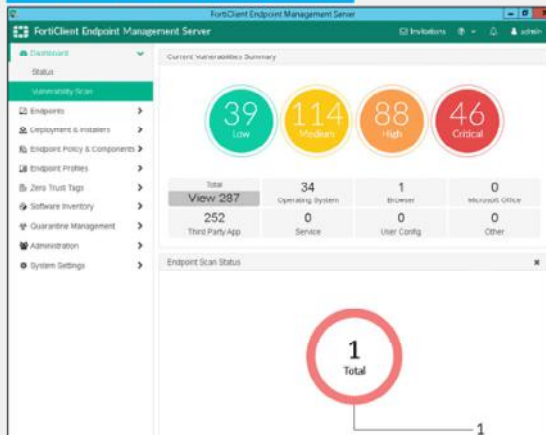
DO NOT REPRINT
© FORTINET

Dashboard

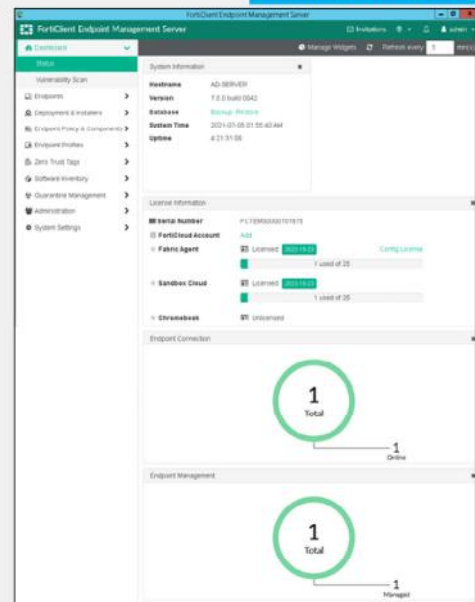
- You use the EMS dashboard to view summary information about:

- System
- Endpoints
- Vulnerability scan on endpoints

Dashboard > Vulnerability Scan



Dashboard > Status



Fortinet NSE Training Institute

© Fortinet Inc. All Rights Reserved.

5

You use the dashboard to view summary information about the system and endpoints. You can also view summary information about vulnerability scans on endpoints.

In the FortiClient EMS dashboard, you see the system and license information widget:

- System information widget: displays hostname, version, database, system time, and uptime information of the FortiClient EMS
- License information widget: displays FortiClient EMS serial number, FortiCloud account, zero trust security license, next-generation endpoint security license, and Chromebook license information

Status page charts and widgets display number of pie charts. Each pie chart provides a summary of endpoint information. You can click any section of the pie charts or any row in the table to display more details. The details include endpoint activity (on-fabric or off-fabric status), endpoint alerts, endpoint connection status, managed Windows, Mac FortiClient version, and OS version. It also shows antivirus, sandbox, vulnerability, and web detection.

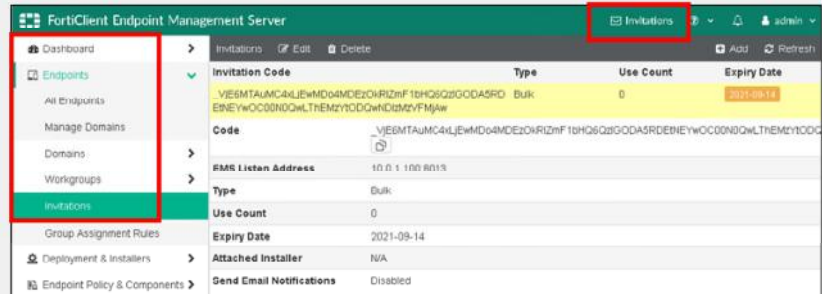
The **Vulnerability Scan** dashboard displays a number of charts and widgets containing a summary of vulnerability scan information collected from endpoints.

When Chromebook management is enabled on the **EMS settings** page, you can also view the Chromebook status. Chromebook status displays a number of charts. Each chart provides a summary of Chromebook information.

DO NOT REPRINT
© FORTINET

Invitations

- An invitation code is used to register FortiClient in the following scenarios:
 - To register FortiClient Linux, iOS, or Android because you cannot create deployment package
 - To register a FortiClient device that doesn't automatically register to FortiClient EMS after installation
- End users can enter the invitation codes to connect
- Invitation codes can be configured by clicking:
 - **Invitations** in the upper-right corner
 - **Endpoints > Invitations**



Fortinet NSE Training Institute

© Fortinet Inc. All Rights Reserved.

6

You can use an invitation code in the following scenarios:

- To register a FortiClient Linux, iOS, or Android endpoint to FortiClient EMS. Since you cannot create a deployment package for these operating systems in FortiClient EMS, this is the only way to register these endpoints to FortiClient EMS.
- To register a FortiClient device that does not automatically register to FortiClient EMS after installation.

End users enter invitation codes to connect FortiClient to FortiClient EMS. If you have configured SMTP settings, you can enable the option to send invitation codes as email notifications. You can send the email notification individually or in bulk. Sending individual invitation codes is a best practice, because it limits any unexpected endpoints from connecting to FortiClient EMS.

Create a new installer to include an installer with the invitation. End users use this installer to install FortiClient on their endpoint and use the invitation code to connect to FortiClient EMS if their FortiClient did not connect automatically after installation.

DO NOT REPRINT
© FORTINET

Administration

- Default user account is admin
 - Has complete access to all FortiClient EMS permissions, including modification, user permissions, approval, discovery, and deployment
 - Has access to all configured Windows and LDAP servers and users, and has the authority to configure user privileges and permissions
 - By default, the admin user account has no password; you should add a password to increase security
- You can view the default admin account and all other admin users added to FortiClient EMS on the **Administrators** page

Administration > Administrators

Users	Edit	+ Add	Refresh
Name	Source	Role	
admin	Builtin	Super Administrator	
Name	admin		
Type	Builtin		
Role	Super Administrator		
Trusted hosts	Disabled		
Last login or activation	2021-07-15 12:40		
Comments			

Fortinet NSE Training Institute

© Fortinet Inc. All Rights Reserved.

7

The default user named *admin* has complete access to all FortiClient EMS permissions, including modification, user permissions, approval, discovery, and deployment. The admin user has access to all configured Windows and LDAP servers and users, and has the authority to configure user privileges and permissions. If you are not authorized to perform certain tasks or access certain devices, the related menu items, items in content pages, and buttons are hidden or disabled. In addition, a message informs you that you do not have permission to view the selected information or perform the selected operation.

By default, the admin user account has no password. You must add a password to increase security.

Administration (Contd)

- You can configure local, Windows, and LDAP user accounts
- The Windows users list is derived from the host server on which FortiClient EMS is installed
- The LDAP users list is derived from servers in the AD domain imported into FortiClient EMS
- You can use admin roles to define permissions for administrator accounts
- You can use four default roles or create a new role
 - Super administrator
 - Standard administrator
 - Endpoint administrator
 - Restricted administrator

Administration > Admin Roles > +Add

Admin Role

Name Required

Description Optional

Endpoint permissions (0/14)

- ☐ Manage LDAPs
- ☐ Manage custom groups
- ☐ Block/interact/quarantine/register endpoints
- ☐ View group assignment rules
- ☐ View endpoint filter bookmarks
- ☐ View quarantine management
- ☐ View software inventory
- ☐ Manage Google domains
- ☐ Run commands on endpoints
- ☐ Manage and assign endpoint policies
- ☐ Manage group assignment rules
- ☐ Manage endpoint filter bookmarks
- ☐ Manage quarantine management
- ☐ Manage software inventory

Policy permissions (0/11)

You can configure local, Windows, and LDAP admin user accounts. The local admin account store in FortiClient EMS local database. The Windows users list is derived from the host server on which FortiClient EMS is installed. The LDAP users list is derived from those in the AD domain imported into EMS.

You can use admin roles to define the permissions for each administrator account in FortiClient EMS. You can use one of the four default admin roles in FortiClient EMS or create a new admin role to assign to an administrator account.

The four default roles are:

- Super administrator
- Standard administrator
- Endpoint administrator
- Restricted administrator

Each admin role can include permissions from three categories: endpoint permissions, policy permissions, and settings permissions. For admin roles that are not authorized for certain tasks or devices, EMS hides or disables the related menu items, items in content pages, and buttons.

DO NOT REPRINT
© FORTINET

Administration (Contd)

- **User Settings** allows you to configure a user account:
 - Inactivity timeout
 - Allowed inactive days
 - Password maximum age

Administration > User Settings

User Settings

Inactivity timeout	30	minutes
Enter 0 to disable.		
Allowed inactive days	0	days
Users not logged in for X days will be marked as disabled. Enter 0 to disable.		
Maximum password age	0	days
Enter 0 to disable. This setting only applies to builtin and EMS users.		
Save		

Fortinet
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

9

You can also configure user settings on EMS. The **Inactivity timeout** setting specifies how long to keep inactive users logged into FortiClient EMS. When the time expires, EMS automatically logs the user out. To keep inactive users logged into FortiClient EMS indefinitely, type a value of 0.

The **Allowed inactive days** setting specifies the number of days of inactivity after which to disable a user account. For example, if this field is set to 10 and a user does not log into FortiClient EMS for ten days, EMS disables their account so that they cannot log into FortiClient EMS. A user with super administrator permissions can reactivate their account.

Maximum password age setting specifies the number of days after which the user is forced to change their password. You can disable the setting by setting the value to 0. This setting only applies to built-in users such as the admin user and EMS users.

**DO NOT REPRINT
© FORTINET**

Administration (Contd)

- SAML SSO
 - Enables SAML SSO to allow users to log in to FortiClient EMS using FortiGate as an identity provider (IdP)
 - Only FortiGate is supported

Administration > SAML SSO

SAML SSO [Expand All] [Collapse All]

Enable SAML SSO: ☒ ⚠ SAML SSO is designed to be used with FortiGate. Custom IdPs are not supported.

Service Provider Settings

SP Address: Use Current B...

SP Certificate: [Upload] [X]

Identity Provider Settings

IdP Address:

Prefix:

IdP Certificate: [Upload] [X]

Save

You can also enable SAML SSO to allow users to log in to FortiClient EMS using a FortiGate as an identity provider (IdP). You can only use the SAML SSO feature in FortiClient EMS with FortiGate as the IdP. FortiClient EMS does not support using FortiAuthenticator as an IdP, or using custom IdPs.

DO NOT REPRINT
© FORTINET

Administration (Contd)

- Fabric devices

- You can view all FortiGate devices
- You can deny or authorize FortiGate

Administration > Fabric Devices

Fabric Devices Deny Edit Delete			
Serial Number	Last Seen IP	Last Seen Time	Authorized
FGVM02TM19001113	10.0.1.254	2021-06-30 06:04:53	✓
Serial Number: FGVMO2TM19001113			
Last Seen IP: 10.0.1.254			
Last Seen Time: 2021-06-30 06:04:53			
Authorized: ✓ Authorized			
Send tag info from all FortiClients: Disabled			
Filter tag info from additional FortiGates: N/A			

- Log viewer

- You can view and download FortiClient EMS logs
- Logs are downloaded as zip file

Administration > Log Viewer

Date	Level	Source	Message	Occurrences
2021-07-15 12:40:21	Info	Console	admin has logged in from :: 1.	1 time since 2021...
2021-07-15 12:40:08	Warning	Console	Session has expired or does not exist.	3 times since 202...
2021-07-15 12:27:34	Info	Update Service	No updates available	11 times since 20...
2021-07-15 06:49:30	Warning	Console	Session has expired or does not exist.	1 time since 2021...
2021-07-15 06:25:08	Info	Update Service	No updates available	3 times since 202...
2021-07-15 06:07:00	Info	Console	admin updated Deployment Package Installer_6.4	1 time since 2021...
2021-07-15 06:02:34	Info	Console	admin updated Profile: Default from UI	1 time since 2021...
2021-07-15 06:01:46	Info	Console	admin has logged in from :: 1.	1 time since 2021...
2021-07-15 05:25:24	Info	Update Service	No updates available	1 time since 2021...
2021-07-15 04:56:03	Warning	Console	Session has expired or does not exist.	3 times since 202...
2021-07-15 04:25:30	Info	Update Service	No updates available	3 times since 202...
2021-07-15 03:58:24	Info	Console	admin updated Profile: Default from UI	2 times since 202...
2021-07-15 03:56:16	Info	Console	admin updated Deployment Package Installer_6.4	3 times since 202...
2021-07-15 03:31:45	Info	Update Service	No updates available	1 time since 2021...
2021-07-15 03:30:56	Info	Console	admin updated Deployment Package Installer_6.4	3 times since 202...
2021-07-15 03:30:40	Info	Console	admin updated Deployment Package Installer	1 time since 2021...

In the FortiClient EMS **Administration** window, you can view all FortiGate devices that the FortiClient EMS has authorized in the **Fabric Devices** window. After FortiGate is added, you can change the status to deny or authorize. These fabric devices only appear when FortiClient EMS is part of the Security Fabric.

The **Log Viewer** option allows you to view and download FortiClient EMS logs. The log viewer page includes logs from all the FortiClient EMS processes such as the GUI console, service update, AD service, EMS service, and so on. You can also apply filters to see specific FortiClient EMS logs. The raw logs are downloaded as zip file to your computer.

DO NOT REPRINT
© FORTINET

Database Management

- You can back up and restore the FortiClient EMS database

Dashboard > Status > Backup

Back Up Database

Password Required

Confirm password Required

Your password must be:

- At least 8 characters long
- And has 3 out of the 4 following:
 - At least one uppercase letter (A-Z)
 - At least one lowercase letter (a-z)
 - At least one number (0-9)
 - At least one symbol (e.g. !@#)

Dashboard > Status > Restore

Restore Database

File Browse... Required

Password Required

FortiClient database management allows you to back up and restore the database, as shown on this slide. The options are available on the FortiClient EMS **Dashboard > Status** window. A password is required to perform a backup. The same password will be used to restore the database using the same backup. When the database is restored, a message appears. The message instructs you to wait for the restored database to reload. You must wait until the database is completely restored.

Note that restore will work only if the database was backed up using the same version number.

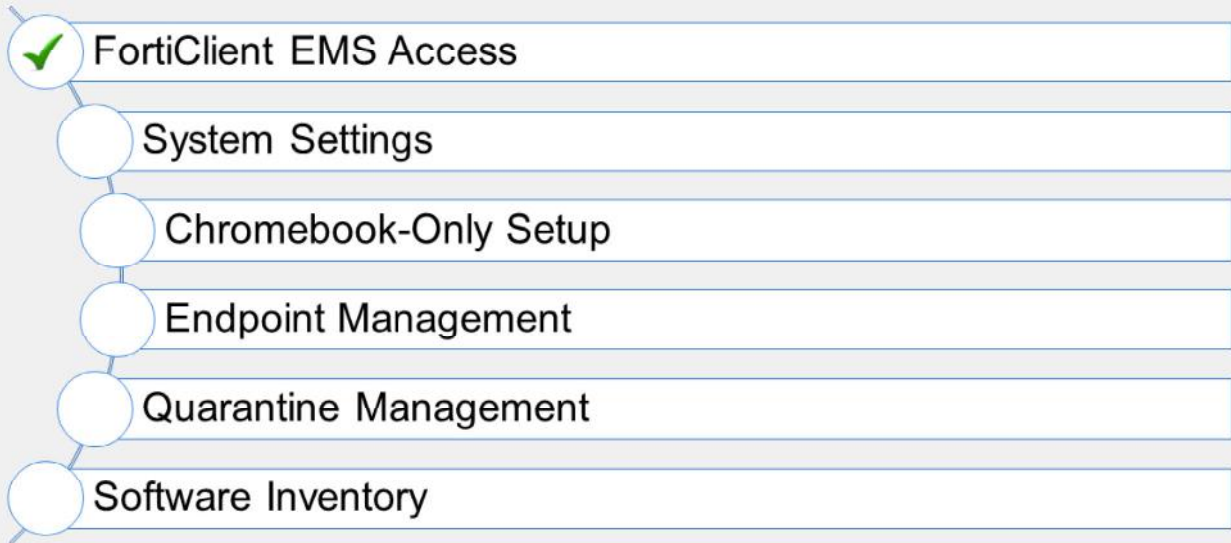
DO NOT REPRINT
© FORTINET

Knowledge Check

1. Which method is used to provision iOS endpoint?
☐ A. AD
☒ B. Invitation code
2. What is the default administrator account password?
☐ A. Fortinet
☒ B. There is no default password

DO NOT REPRINT
© FORTINET

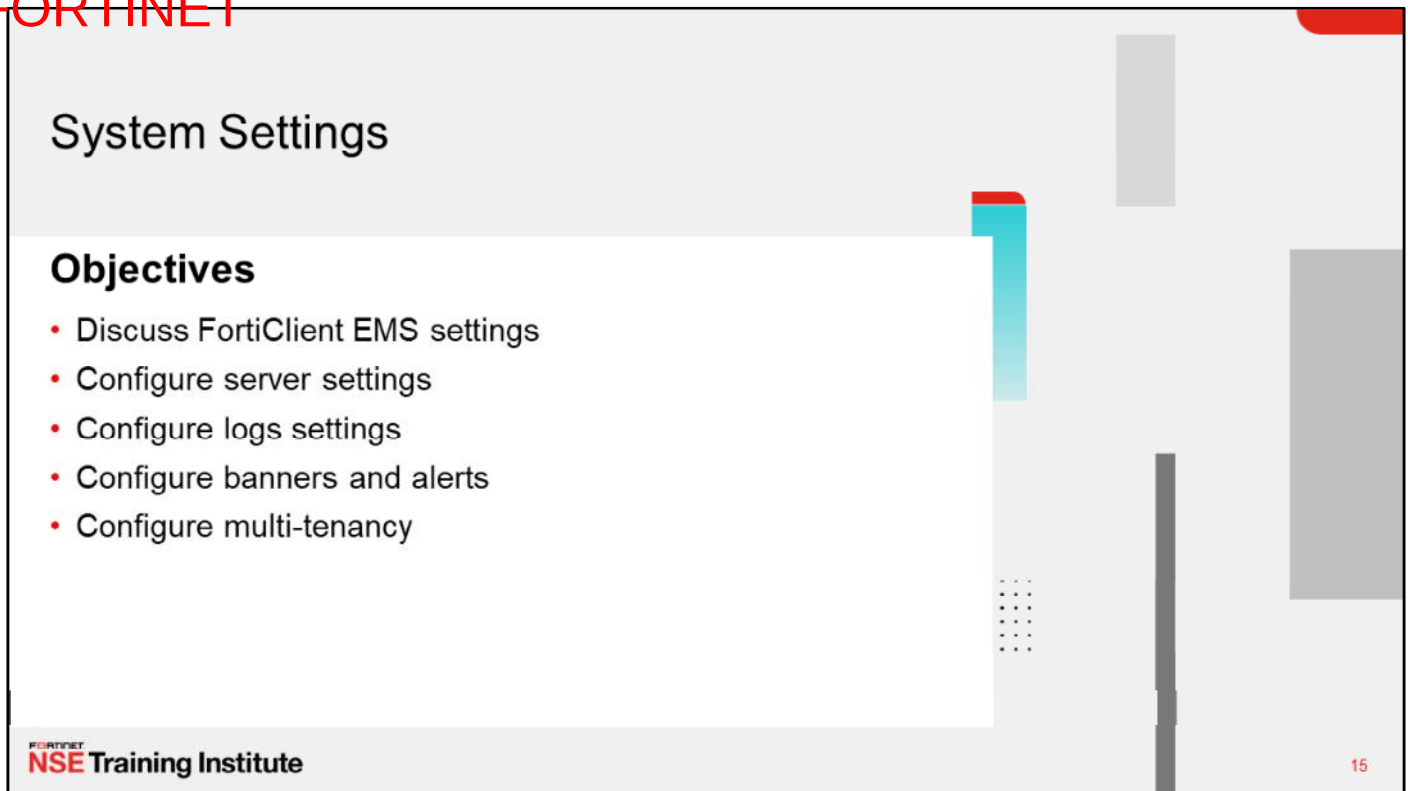
Lesson Progress



Good job! You now know how to access the FortiClient EMS GUI. You also learned about FortiClient EMS components, FortiClient administration, and database management.

Now, you will learn about system settings for FortiClient EMS.

DO NOT REPRINT
© FORTINET



System Settings

Objectives

- Discuss FortiClient EMS settings
- Configure server settings
- Configure logs settings
- Configure banners and alerts
- Configure multi-tenancy

FORTINET
NSE Training Institute

15

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in FortiClient EMS system settings, you will be able to configure the server, logs, FortiGuard, endpoints, login banner, EMS alerts, endpoint alerts, SMTP server, and custom messages settings.

Shared Settings

- You can change the default IP address and port, and configure other server settings for FortiClient EMS

- Shared Settings:**

- Shared between FortiClient EMS managing Windows, MacOS, Linux endpoints, and Chromebook endpoints
- Shared settings include:
 - Hostname
 - Listen on IP
 - Use FQDN
 - Remote HTTPS access
 - SSL certificate
 - EMS CA certificate (ZTNA)

System Settings > EMS Settings > Shared Settings

The FortiClient EMS **Shared Settings** option is shared between Windows, MacOS, Linux, and Chromebook endpoints. You can configure the FortiClient EMS hostname, IP address, and FQDN. When you enable the **Use FQDN** option, FortiClient can connect using either the specified IP address in the **Listen on IP Addresses** field, or the specified FQDN.

The **Remote HTTPS access** option specifies settings for remote administration access to FortiClient EMS. You can enable or disable remote HTTPS access to FortiClient EMS. When you select **Remote HTTPS access**, the HTTPS port, predefined hostname, management IP and port for proxy, and custom hostname options are available. The pre-defined hostnames includes server binding names or IP addresses. FortiClient EMS responds to all the names that are defined in this field.

The **SSL certificate** option displays the SSL certificate currently imported. If you have already uploaded an SSL certificate, the page displays the **Replace** button.

The **EMS CA certificate (ZTNA)** requires the ZTNA or EPP license and only applies for endpoints running FortiClient 7.0.0 and later versions.

EMS Settings

• EMS Settings:

- These settings are used by FortiClient EMS managing Windows, MacOS, and Linux endpoints
 - Listen on port
 - FortiOS Connector port
 - Enable TLS 1.0/1.1
 - FortiClient download URL
 - Enforce invitation-only registration for
 - Sign software packages
 - Configure EMS server list
 - Connect to local subnets only
 - Enable login banner

System Settings > EMS Settings > EMS Settings

On the **EMS Settings** window, you can configure the **Listen on port** setting by typing a new port number in the field. FortiClient will connect using the specified port. By default, it displays port 8013 for the FortiClient EMS server.

You can also enable or disable TLS 1.0 or 1.1 for file downloads. Windows 7 uses old TLS versions.

In the **FortiClient download URL** field you can see the URL on which FortiClient installers created on FortiClient EMS will be made available for download.

You can use the **Enforce invitation-only registration for** option to deregister a FortiClient endpoint that does not satisfy the requirement. You can select all, none, or FortiClient version 7.0.0 or later for endpoints using invitation-only registration.

The **Sign software packages** option allows you to digitally sign Windows FortiClient software installers with a code signing certificate created by or uploaded to FortiClient EMS.

The **Configure EMS server list** allows you to select a specific FortiClient EMS IP address or FQDN that FortiClient uses to register.

The **Connect to local subnets only** option allows connections to FortiClient EMS local subnets.

When you select the **Enable login banner** check box, a message appears on the login screen before a user logs in to FortiClient EMS. The **Preview** section displays a preview of the message when you type a message in a **Message** box.

DO NOT REPRINT
© FORTINET

EMS for Chromebooks Settings

- **EMS for Chromebooks Settings:**
 - These settings are used by FortiClient EMS managing Chromebook endpoints
 - **Listen on port**
 - **User inactivity timeout**
 - **Profile update interval**
 - **SSL certificate**
 - **Service account**

System Settings > EMS Settings > EMS Settings

Fortinet
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

18

The **EMS for Chromebooks Settings** window also includes the **Listen on port** setting, which, like EMS settings, displays the default port for the FortiClient EMS server for Chromebooks. You can change the port by typing a new port number. The default port is 8443.

You can also configure the **User inactivity timeout** setting, which is the number of hours of inactivity after which the user is timed out. **Profile update interval** specifies the profile update interval, in seconds.

SSL certificate displays the SSL certificate currently imported. If you have already uploaded an SSL certificate, the page displays the **Replace** button. **Service account** displays the service account ID currently in use. You must enter an account ID and private key to update the account. Note that you must add an SSL certificate to FortiClient EMS to allow Chromebooks to connect to FortiClient EMS.

DO NOT REPRINT
© FORTINET

Endpoints Settings

- Endpoints Settings:
 - FortiClient telemetry connection key
 - Keep alive interval
 - Offline timeout
 - Delete timeout
 - License timeout
 - Automatically upload avatars
 - Enable endpoint snapshot reports

EMS Settings > EMS Settings > Endpoints Settings

The screenshot displays the 'Endpoints Settings' configuration window. It includes the following fields and options:

- FortiClient telemetry connection key:** A text input field with the value 'Optional' and a small icon to the right.
- Keep alive interval:** A numeric input field with the value '60' and a unit dropdown set to 'seconds'.
- Offline timeout:** A numeric input field with the value '5' and a unit dropdown set to 'keep alive intervals'.
- Delete timeout:** A numeric input field with the value '30' and a unit dropdown set to 'days'.
- License timeout:** A numeric input field with the value '45' and a unit dropdown set to 'days'.
- Automatically upload avatars:** A checkbox that is checked. Below it, a note states: 'When this is enabled, FortiClient will upload user avatars to all FortiGate, FortiAnalyzer, and EMS servers it is registered to.'
- Enable endpoint snapshot reports:** An unchecked checkbox.

When the FortiClient endpoint is registered to FortiClient EMS, it consumes a license seat. You can configure a license timeout value in days. If an endpoint disconnects from EMS, the license seat is retained in anticipation that the endpoint will reconnect.

If the endpoint does not reconnect within the given timeout, its connection record is removed from FortiClient EMS. If the endpoint is removed, switched off, or goes offline, and does not re-establish a telemetry connection to FortiClient EMS within the **Delete timeout** value, the endpoint is deleted from FortiClient EMS, even if FortiClient on the endpoint shows that it is still connected. The default license timeout value is 45 days. The maximum allowed value is 90 days. The License Timeout value releases the license after the given timeout.

The **Automatically upload avatars** option allows FortiClient to upload user avatars to all of the devices, and the **Enable endpoint snapshot reports** setting enables the endpoint snapshot report. You can set the interval for the snapshots, it must be between 300 and 86400 seconds.

DO NOT REPRINT
© FORTINET

Log Settings

- You can specify what level of log messages to capture
- You can specify when to automatically delete logs and alerts

System Settings > Log Settings

Log Settings

Log level
Info

Automatically clear logs older than
30
days
Clear all now

Automatically clear alerts older than
30
days
Clear all now

Automatically clear events older than
30
days
Clear all now

Clear Chromebook events older than
7
days
Clear now

This applies to Chromebooks only.

Save

Fortinet
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

20

In the **Log Settings** section, you can specify what level of log messages to capture in the logs for FortiClient EMS. For example, if you select **Info** in the **Log level** drop-down list, all log messages from **Info** to **Emergency** are added to the FortiClient EMS logs. Generally, the level you want to use is **Info** because it includes most of the logs the system generates (except **Debug**) including administrator login or logout activity. **Emergency** logs only generate when the system is unstable and do not include other system logs. Depending on the type of log and the needs of your organization, you may want to log only specific levels of system logs.

You can also specify when to automatically delete logs, alerts, and events. By default, it is 30 days for all logs, alerts, and other OS events, and seven days for Chromebook events.

You can click **Clear now** to immediately delete all FortiClient EMS logs, alert, or events.

DO NOT REPRINT
© FORTINET

FortiGuard Services

- FortiGuard Settings:
 - Server Location
 - FortiManager
 - Cloud Services

System Settings > FortiGuard Services

Software and Signature Update Services

FortiGuard

Server Location: ☐ Global ☐ US ☐ Europe

Port:

Enable SSL: ☒

[View Signature List](#)

☒ Use FortiManager for client software/signature updates

IP address/hostname:

Port:

Fallover port:

Timeout: seconds

Fallover: ☒

Cloud Services

FortiCloud

Region:

Time Offset:

Fortinet
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

21

The FortiGuard settings include **Server Location**, which allows you to configure the FortiGuard server location to **Global**, **US**, or **Europe**. Europe is only available if you have selected the **Enable SSL** checkbox.

You can also enable the **Use FortiManager for client software/signature updates** option, which allows you to use FortiManager for client software and signature updates. If you select **Fallover**, this enables failover to FDN, when FortiManager for FortiClient is not available. The settings in the **Endpoints** window allows you to add the FortiClient telemetry connection key for FortiClient EMS. FortiClient must provide this key during connection. You can also configure keep alive intervals. FortiClient sends short and full keep alive messages to FortiClient EMS at the specified intervals. The **Cloud Services** section provides options that allow you to connect FortiCloud, and you can select region and time offset.

DO NOT REPRINT
© FORTINET

Alerts

• EMS Alerts

- Send alerts for EMS events

System Setting > EMS Alerts

EMS Alerts

Send an email for ...

Version Alerts

- ☐ New EMS version is available for deployment
- ☐ New FortiClient version is available for deployment

FortiClient Alerts

- ☐ EMS license is expired or about to expire
- ☐ EMS fails to sync with LDAP domains
- ☐ Less than 10% of the client licenses are left
- ☐ Client licenses have run out
- ☐ New software is detected

Save

• Endpoint Alerts

- Send alerts for EMS events

System Setting > Endpoint Alerts

Endpoint Alerts

Send an email every ... 2 hours

Send an email when ...

- ☐ Malware is detected
- ☐ Repeated malware is detected
- ☐ Multiple malwares are detected
- ☐ Malware outbreak is detected
- ☐ Zero-day malware is detected by FortiSandbox
- ☐ C&C attack communication channel is detected
- ☐ Critical vulnerability is detected
- ☐ Endpoint FortiClient Telemetry is manually disconnected by user
- ☐ Endpoint signature database is out of date
- ☐ Endpoint software is out-of-date

Save

You can view the alerts FortiClient EMS generates. Examples of events that generate an alert are shown on this slide. A red label is associated with the **Alert** icon when new notifications are available or received. It is cleared when you view the alert. You select the **Alert** icon (a bell) in the toolbar to view alerts. You can use the **Filter** icon in each column heading to apply filters, and the **Clear Filters** icon to remove the filters.

You can also set up an SMTP server to enable alerts for FortiClient EMS or endpoint events. When an alert is triggered, EMS sends an email notification.

The **EMS Alerts** window allows you to send an email notification for version and FortiClient alerts. This slide shows all of the alerts that are available on the **EMS Alerts** window.

On the **Endpoint Alerts** window, you enable the option to send an email alert for the endpoints. This slide shows all the endpoint events that you can select to generate email alerts. You can also select a time interval to send alert emails. By default, it is set to 30 minutes.

DO NOT REPRINT
© FORTINET

Alerts (Contd)

- Viewing alerts

You can view alerts FortiClient EMS generates by clicking a bell icon. Examples of events that generate an alert include:

- New version of FortiClient is available
- FortiClient deployment failed
- Failure to check for signature updates
- Error encountered when downloading AD server entries
- Error encountered when scanning for local computers

You can view the alerts FortiClient EMS generates. Examples of events that generate an alert are shown on this slide. A red label is associated with the **Alert** icon when new notifications are available or received. It is cleared when you view the alert. You click the **Alert** icon (a bell) in the toolbar to view alerts. You can use the **Filter** icon in each column heading to apply filters, and the **Clear Filters** icon to remove the filters.

DO NOT REPRINT
© FORTINET

SMTP Server

- **SMTP Server**

- When an alert is triggered, EMS sends an email notification to the configured email address(es)

System Setting > SMTP Server

SMTP Server

Server

Port

Security ☒ None ☐ STARTTLS ☐ SMTPS ☐ Auto Detect

From

Reply-to

Subject

Recipients

Test subject

On the **SMTP Server** window, you can set up an SMTP server to enable alerts for EMS and endpoint events. All the options available for SMTP server configuration are shown on this slide. You can choose to encrypt SMTP traffic using STARTTLS or SMTPS. Selecting one of the encryption options will enable the username and password fields on the GUI.

Custom Messages

- You can customize messages that display on endpoints in certain situations
- Customize endpoint quarantine message:
 - You can customize the message that displays on an endpoint when it has been quarantined by FortiClient EMS
- Customize web filter messages:
 - You can customize the messages that display on an endpoint on in-browser web filter result pages
 - There are different types of web filter messages:
 - Blocklisted page
 - Blocked page
 - Blocked FortiGuard inaccessible page
 - Warning page
 - Warning FortiGuard inaccessible page
 - You can also upload images for logo and icon fields

You can customize messages that display on endpoints in certain situations, such as when FortiClient EMS has quarantined the endpoint. For example, you can customize the message to include your organization's help desk phone number so that users can contact the network administrator about their machine.

You can also customize the messages that display on an endpoint in in-browser web filter result pages. In **Custom Messages**, select **WebFilter Custom Messages**. The left panel displays the customization fields, while the right panel previews the custom messages as they will appear in a web browser when using the latest version of FortiClient. The types of web filter messages are: blocklisted page, blocked page, blocked FortiGuard inaccessible page, warning page, and warning FortiGuard inaccessible page.

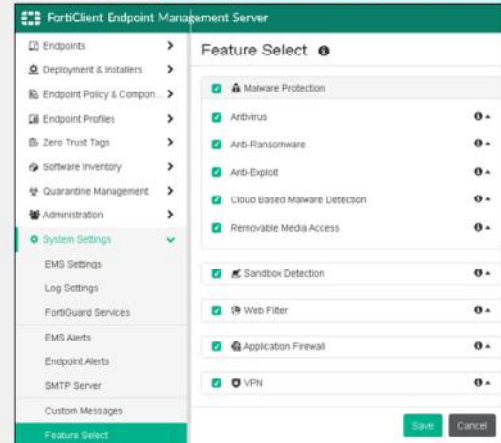
In the left pane, enable or disable the fields and enter the desired messages. You can also upload images for logo and icon fields. The right pane displays previews of the messages.

DO NOT REPRINT
© FORTINET

Feature Select

- **Feature Select**
 - You can choose which features to show and hide in FortiClient EMS
 - Only features that are selected are available for configuration in FortiClient EMS
 - Only FortiClient EMS super administrator can enable and disable features on the **Feature Select** pane

System Settings > Feature Select



Fortinet
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

26

On the **Feature Select** pane, you can choose which features to show and hide. Only features that are enabled on the **Feature Select** window are available for configuration in other areas of FortiClient EMS.

For example, if you disable **Web Filter** on the **Feature Select** window, the **Web Filter** tab will not appear on endpoint profiles, and the option to enable web filter logs on the system settings will also not be available.

Also, when you enable web filter in a deployment package, and the deployment package installs web filter on the endpoint, the **Web Filter** option does not appear in the FortiClient GUI because it is disabled.

The **Web Filter Detection** widget on the status dashboard and option to import a profile from FortiGate/FortiManager are also not available.

Only a FortiClient EMS super administrator can enable and disable features on the **Feature Select** window. Other FortiClient EMS users can view which features are enabled and disabled on the Feature Select page, but cannot modify the configuration.

If you previously enabled a feature on an endpoint, but you later disable the feature on the **Feature Select** window, FortiClient EMS then disables the feature on the endpoint.

DO NOT REPRINT
© FORTINET

Multi-Tenancy

- You can create multiple sites
 - To provide granular access
 - To assign different administrators to different sites
 - To separate endpoint data from configuration data
- FortiClient EMS supports up to 500 multitenancy sites
- When multi-tenancy is enabled, fabric connectors must use an FQDN to connect to FortiClient EMS
- You must enable **Manage Multiple Customer Sites**
 - FortiClient EMS forces the GUI to restart for the changes to take effect
- Initially there are two sites:
 - Global
 - Default



Fortinet
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

27

In the FortiClient EMS multi-tenancy setup, you can create multiple sites to provide granular access to different sites for different administrators and separate endpoint data and configuration into different sites. The sites are completely separate from each other and cannot share data between them. For example, if an administrator only has access to Site A, they cannot view data from any other site.

FortiClient EMS supports up to 500 multi-tenancy sites. When multi-tenancy is enabled, Fabric connectors must use an FQDN to connect to EMS, where the FQDN hostname matches a site name in EMS (including "Default site").

You would use multi-tenancy in an MSSP environment to conserve resources and use the same license (the total number of FortiClient licenses are shared between sites). This will also work well in enterprise environments that use segmentation and different ADs for different departments.

You must enable **Manage Multiple Customer Sites** in FortiClient EMS system settings. FortiClient EMS forces the GUI to restart for the changes to take effect. After restarting, the EMS GUI displays the global dashboard. When you initially enable multi-tenancy, there are two sites: global, where you can set and view global settings; and default, which contains the endpoints that belong to your original FortiClient EMS instance. The settings associated with your original FortiClient instance are retained. To switch between sites, select the site name in the upper-right corner, then select the desired site from the drop-down list.

After you enable multi-tenancy, all previously created administrators, except the default admin user, become administrators for the default site.

Multi-Tenancy (Contd)

- You can add a new site by
 - Site select list in the upper-right corner or
 - On **Administration > Configure Sites**



- In the **Add FortiClient EMS Site** dialog box:
 - Enter desired site name
 - Number of available licenses for assignment
- When multi-tenancy is enabled:
 - Some settings are available only from the global level and others are available only from site level
- You can configure the administrator as a non-multi-tenant setup, but with different roles

 A screenshot of the 'Add FortiClient EMS Site' dialog box. It has a title bar with a close button. The form contains:

- A 'Name' field with 'Site-A' entered.
- A prompt: 'Provide a name for this site.'
- An 'Assign Licenses' section with two checkboxes: 'Zero Trust Security' (unchecked) and 'Next-Generation Endpoint Security' (checked).
- A license count field showing '15'.
- A note: '25 Next-Generation Endpoint Security license(s) available'.
- A 'Chromebook' checkbox (unchecked).
- 'Save' and 'Cancel' buttons at the bottom.

To add a new site, select **Configure Sites** from the site selection list, as shown on this slide. You can also open the **Configure Sites** page in **Administration** to create new site. This page displays all sites and their license usage. You must configure name. You must also release the number of licenses from the *Default* site before assigning number of licenses to a new site.

When multi-tenancy is enabled, you can configure some settings only from the global level, and other settings only from the site level. You cannot view site-level settings from the global site. For descriptions of the settings, see the FortiClient *EMS Administration Guide* document.

From the global site, you can configure the administrator. When adding a new administrator from the global site, you can create a local administrator or configure a Windows or LDAP user. When adding a new administrator from the site level, you can configure only an LDAP user. Administrator names from the same source (FortiClient EMS, LDAP, or Windows) must be unique across all sites. Administrators can have the same name if they are from different sources. In multi-tenancy, you get an additional administrator role besides super and settings administrator—it is site administrator.

The site administrator has access to specified sites only, with no access to the global site. A site administrator can have access to multiple sites. By default, a site administrator is a super administrator for all sites that they have access to. A site administrator can configure the site license and system settings, including server settings. You can modify the site administrator's available configuration options for a site by assigning them a different admin role for that site after you log in to the site. The mentioned administrator roles are specific to global administrator management when multi-tenancy is enabled.

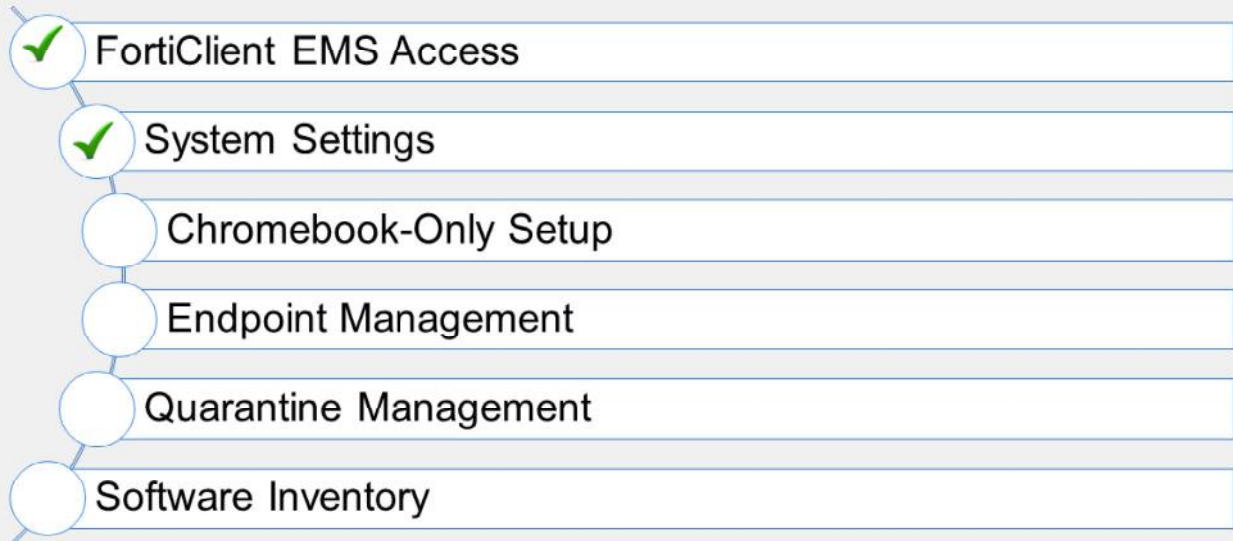
DO NOT REPRINT
© FORTINET

Knowledge Check

1. By default, which port does a FortiClient EMS managing a Chromebook endpoint listen on?
✓ A. 8443
B. 8013

DO NOT REPRINT
© FORTINET

Lesson Progress



Good job! You now understand the system settings for FortiClient EMS.

Now, you will learn how to set up FortiClient EMS for Chromebook only.

DO NOT REPRINT
© FORTINET

Chromebook-Only Setup

Objectives

- Discuss the Google Admin console setup
- Configure service account credentials

FORTINET
NSE Training Institute

31

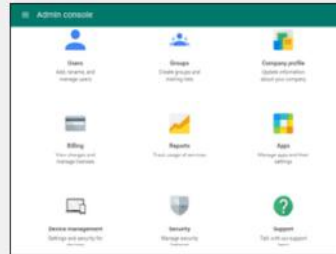
After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in setting up FortiClient EMS to manage Chromebooks, you will be able to configure the Google Admin console setup and service account credentials.

DO NOT REPRINT
© FORTINET

Admin Console Setup

- Logging in to the Google Admin console



- FortiClient Web Filter extension

- You must add extension ID `igbgpehnbmhdgjbhkkpedommgmfbeao` to enable the web filter feature for Chromebook endpoints



Log in to the Google Admin console using your Google domain admin or G Suite account. Note that a Google account set up through an organization like work, school, a club, or maybe family or friends, is called a G Suite account.

After the FortiClient Web Filter extension is added, on the **Chrome Web Store** window, search for the extension ID shown on this slide. The extension name appears as **FortiClient Chromebook Web Filter Extension**.

Note that FortiClient EMS software is not available for public use. You can enable the feature only by using the extension ID that is shown in this slide.

DO NOT REPRINT
© FORTINET

Admin Console Setup

- Configure the FortiClient Web Filter extension to enable communication
- FortiClient EMS hosts the services that assign endpoint profiles of web filtering policies
- FortiClient EMS is the profile server
- Create text file about FortiClient EMS as profile server and upload to admin console
- Example:

```
{  
  "ProfileServerUrl":{"Value": https://ems.mydomain.com:8443"}  
}
```

You must configure the FortiClient Chromebook Web Filter extension to enable the Google Admin console to communicate with FortiClient EMS. FortiClient EMS hosts the services that assign endpoint profiles of web filtering policies to groups in the Google domain. FortiClient EMS also handles the logs and web access statistics sent from the FortiClient web filter extensions.

You must add FortiClient EMS details as profile server in the Google Admin console as shown on this slide.

For details about configuration setup, see the *FortiClientEMS Administration Guide*.

DO NOT REPRINT
© FORTINET

Add Root Certificates

- Add root certificates
 - Chromebook needs to trust the EMS certificate to establish HTTPS connection between the Chromebook web extension and FortiClient EMS
 - You can use both public or private CA certificates
- FortiClient extensions use HTTPS connections to communicate
- HTTPS connections require SSL certificates

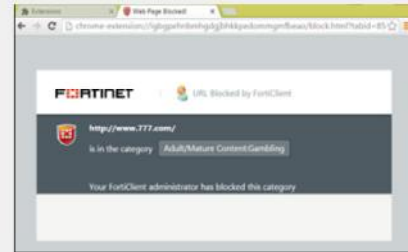
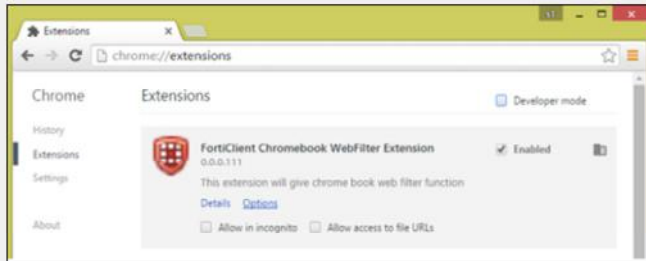
The FortiClient Chromebook Web Filter extension communicates with FortiClient EMS using HTTPS connections. You must obtain an SSL certificate and add it to FortiClient EMS to allow the Chromebook extension to trust FortiClient EMS.

If you use a public SSL certificate, you need to add only the public SSL certificate to FortiClient EMS. If you prefer to use a certificate that is not from a common certificate authority (CA), you must add the SSL certificate to FortiClient EMS, and push your certificate's root CA to the Google Chromebooks. Otherwise, the HTTPS connection between the FortiClient Chromebook Web Filter extension and FortiClient EMS will not work.

For more details about certificates, see the *FortiClientEMS Administration Guide*.

Admin Console Setup

- Disable access to Chrome developer tools
 - Block user from disabling FortiClient Web Filter extension
- Disallow incognito and guest mode
 - Extensions are bypassed with incognito mode
- Block Task Manager
 - Users can stop extension



You must disable developer tools and disallow incognito mode, and guest mode. Disabling access to Chrome developer tools blocks users from disabling the FortiClient web filter extension. When users browse in incognito mode, extensions are bypassed. Guest mode doesn't provide profile information and deletes browsing activity after the user closes the browser window.

You must also block **Task Manager** for managed Google domains to prevent the user from stopping the FortiClient web extension. The Google Chrome browser has a built-in task manager that allows you to see how much memory and CPU web pages, extensions, and Google processes are using while Chrome is running. When the **Task Manager** opens, it displays a list of all open tabs, extensions, and processes currently being used by Chrome, and the user can end any process.

After you add the Google domain to FortiClient EMS, the Google Admin console automatically pushes the FortiClient Web Filter extension to the Chromebooks when users log in to the Google domain.

You can verify that the feature has become available on the Chromebooks by opening the Google Chrome browser. Type `chrome://extensions` to check FortiClient extension and visit any gambling site, such as `http://www.777.com`, and confirm the site is blocked.

Service Account

- FortiClient EMS includes the following default service account credentials generated by the Google Developer console:

Option	Default setting	Where used
Client ID	102515977741391213738	Google Admin console
Email address	account-1@forticlientwebfilter.iam.gserviceaccount.com	FortiClient EMS
Service account certificate	A certificate in PEM format for the service account credentials	FortiClient EMS

- Must add the client ID default value to the Google Admin console—no other configuration for service account credentials is required
- Add service account credentials to the Google Admin console and FortiClient EMS
- Fortinet recommends unique service account credentials for improved security

FortiClient EMS requires service account credentials generated by the Google Developer console. You can use the default service account credentials provided with FortiClient EMS. To configure the default service account credentials, you must add the client ID default value to the Google Admin console. No other configuration for service account credentials is required. These settings allow Google to trust FortiClient EMS, which enables FortiClient EMS to retrieve information from the Google domain.

Note that the service account credentials are a set. If you change one credential, you must change the other two credentials.

When using unique service account credentials for improved security, you must complete the following steps to add the unique service account credentials to the Google Admin console and FortiClient EMS:

- Create unique service account credentials using the Google Developer console.
- Add the unique service account credentials to the Google Admin console.
- Add the unique service account credentials to FortiClient EMS.

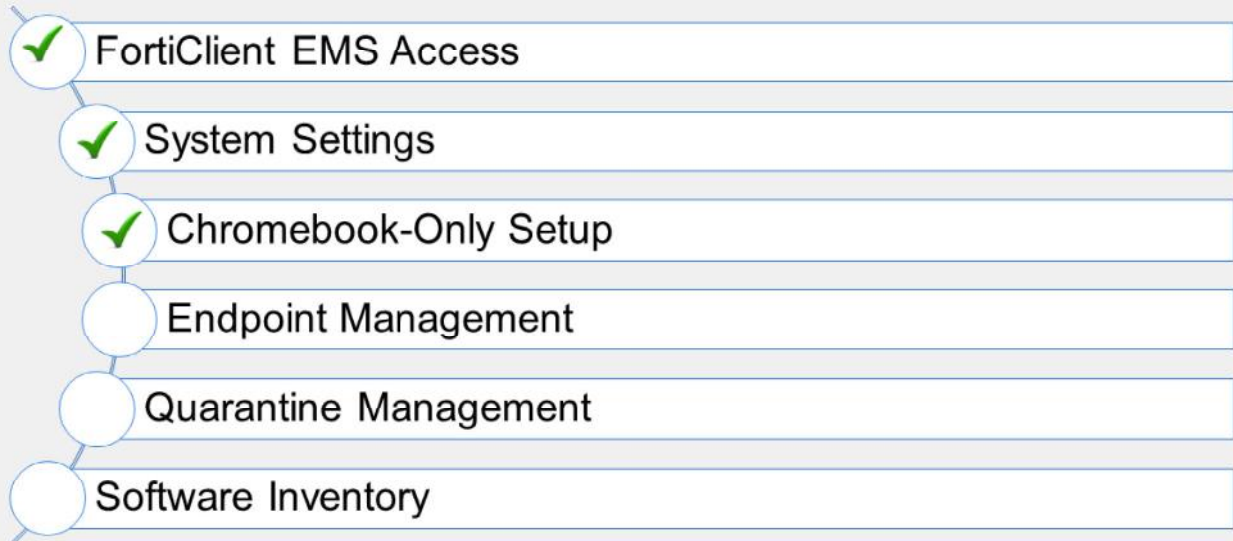
DO NOT REPRINT
© FORTINET

Knowledge Check

1. Which type of Google account do you need to access the Google Admin console?
✓ A. G Suite
B. Personal
2. Which connection does the FortiClient Chromebook web filter extension use to communicate?
✓ A. HTTPS
B. HTTP

DO NOT REPRINT
© FORTINET

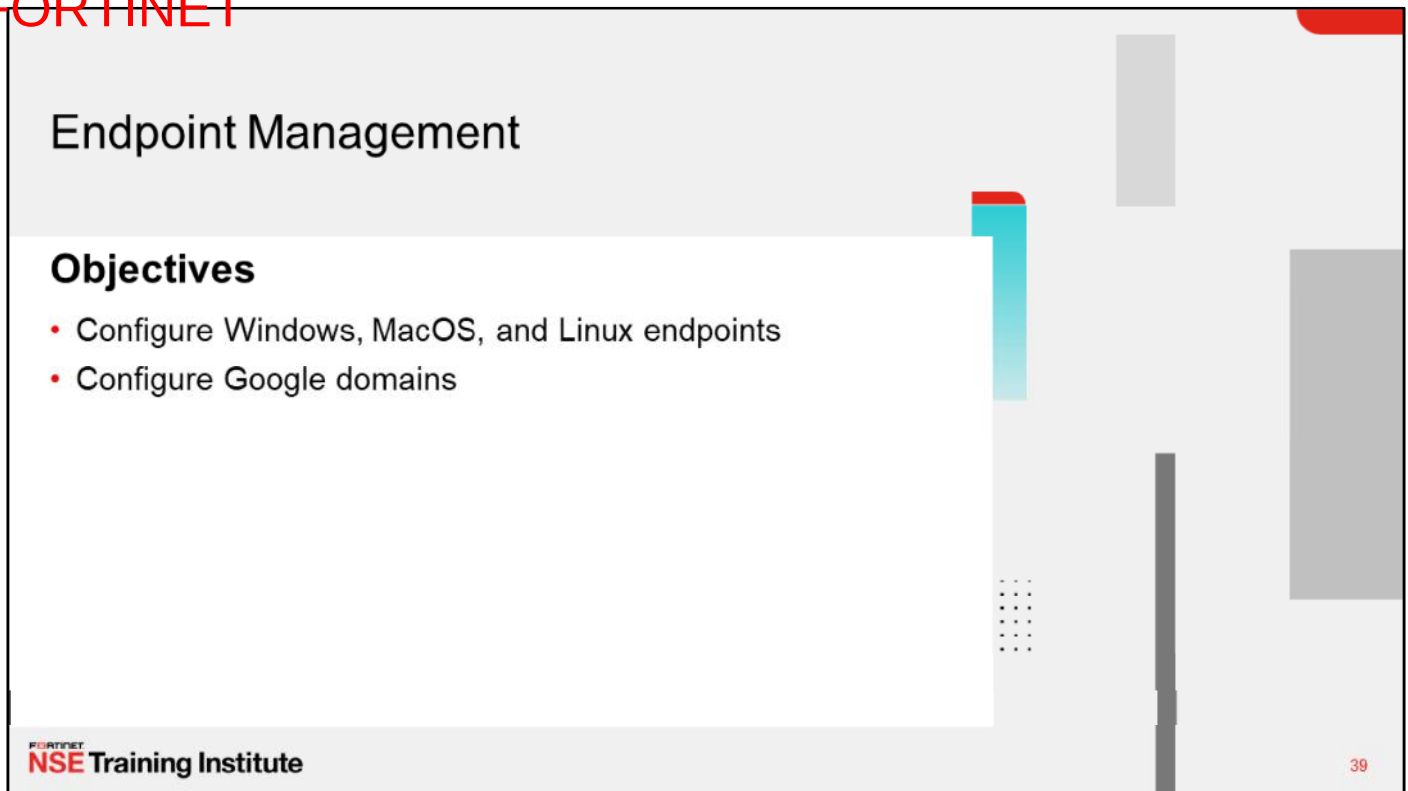
Lesson Progress



Good job! You now understand how to configure FortiClient EMS to manage Chromebooks.

Now, you will learn about endpoint management.

DO NOT REPRINT
© FORTINET



Endpoint Management

Objectives

- Configure Windows, MacOS, and Linux endpoints
- Configure Google domains

FORTINET
NSE Training Institute

39

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in using FortiClient for endpoint management, you will be able to configure Windows, macOS, and Linux endpoints, as well as Google domains.

DO NOT REPRINT
© FORTINET

Endpoint Management

- Windows, MacOS, and Linux endpoints
 - FortiClient EMS needs to determine which devices to manage
 - Information can come from an active directory (AD) server, Windows workgroup, or manual FortiClient connection
- Creating groups
 - You can create groups to organize endpoints
 - You can also rename and delete groups
- Adding endpoints
 - You can add endpoints using an AD service
 - Endpoint users can manually connect FortiClient Telemetry to FortiClient EMS

FortiClient EMS needs to identify which devices to manage. For Windows and macOS, device information can come from an AD server, Windows workgroup, or manual FortiClient connection. The Linux endpoint doesn't communicate with the AD server.

On FortiClient EMS, you can create the domain or workgroup, and then rename and delete groups.

You can import endpoints manually from an AD server. You can import and synchronize information about computer accounts with an LDAP or LDAPS service. You can add endpoints by identifying endpoints that are part of an AD domain server.

Note that after importing endpoints from an AD server, you can edit the endpoints. These changes are not synced back to the AD server.

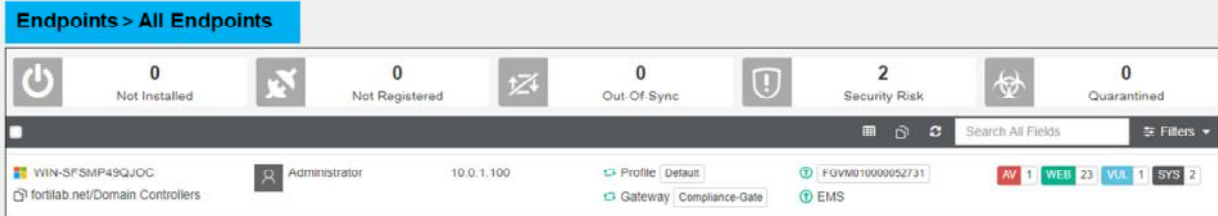
Endpoint users can also manually connect FortiClient Telemetry to FortiClient EMS by specifying the IP address for FortiClient EMS on FortiClient. This process is sometimes called registering FortiClient to FortiClient EMS.

DO NOT REPRINT
© FORTINET

Endpoint Management (Contd)

- Viewing endpoints

- You can view the list of endpoints in a domain or workgroup on the **Endpoints** pane
- You can view details about each endpoint on the **Client Details** pane



After you add endpoints to FortiClient EMS, you can view the list of endpoints in a domain or workgroup on the **Endpoints** pane. You can also view details about each endpoint on the **Client Details** pane, and use filters to access endpoints with specific qualities.

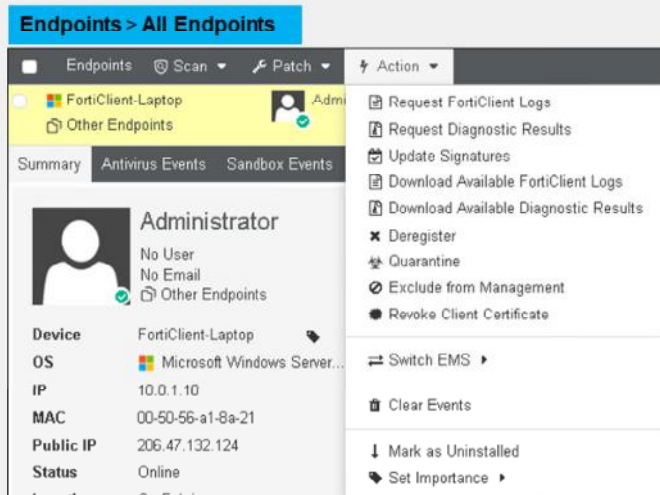
You can save filter settings as bookmarks, then select the bookmarks to use them.

DO NOT REPRINT
© FORTINET

Endpoint Management (Contd)

• You can do the following from the **Endpoints** pane:

- Run antivirus scans on endpoints
- Run vulnerability scans on endpoints
- Patch vulnerabilities on endpoints
- Request FortiClient logs
- Request the FortiClient diagnostic results
- Update signatures
- Download available FortiClient logs
- Download available diagnostic results
- Disconnect and connecting endpoints
- Quarantine endpoints
- Quarant an endpoint from FortiOS using EMS
- Exclude endpoints from management
- Delete endpoints



On the **Endpoints** pane, you can perform the actions that are shown in this slide. FortiClient EMS can run antivirus and vulnerability scans. All the scanning starts on the endpoints with the next FortiClient Telemetry communication. You can also view the history of vulnerability scans for each endpoint on the **Client Details** pane.

FortiClient EMS can automatically patch software if a vulnerability requires the endpoint user to download and install a software to patch a vulnerability. The FortiClient console displays the information.

FortiClient can upload a log file from one or several endpoints requested by FortiClient EMS. The log file is uploaded to the hard drive on the computer running FortiClient EMS, and file is not visible in the FortiClient EMS GUI.

You can use FortiClient EMS to run the FortiClient diagnostic tool on one or multiple endpoints, and export the results to the hard drive on the computer on which you are running FortiClient EMS. The exported information is not visible in the FortiClient EMS GUI.

FortiClient EMS can also quarantine, disconnect and connect, exclude from management, and delete endpoints.

Endpoint Management (Contd)

- Provisioning FortiClient Android endpoints for central management
 - Use FortiClient EMS invitation codes
 - Use a third-party QR code generator to create a QR code to distribute to FortiClient (Android) users
 - Scan the QR code from their devices
 - QR codes can contain the FortiClient EMS server's hostname or IP address, port number, and a connection key
- Google Domains
 - **Google Domains** is only available if FortiClient EMS manages Chromebooks
 - You can add, view, edit, and delete domains

You can either use FortiClient EMS invitation codes or a QR code to provision Android devices. You can send invitation codes or create a QR code to distribute to FortiClient (Android) users. FortiClient (Android) users can type the code or scan the QR code from their devices to automatically enable FortiTelemetry and attempt a connection to the specified FortiClient EMS server. Invitation or QR codes can contain the FortiClient EMS server hostname or IP address, port number, and a connection key. Only the FortiClient EMS hostname/IP address is required; all other fields are optional.

FortiClient EMS needs to identify which devices to manage. Device information comes from the Google Admin console. The **Google Domains** option is available if **EMS for Chromebooks Settings** is selected in the EMS server settings.

You can add domains on the **Manage Domains** page on the FortiClientEMS. After you add domains to FortiClient EMS, you can view, edit, and delete them.

Note that this section is applicable only if you are using FortiClient EMS to manage Google Chromebooks.

DO NOT REPRINT
© FORTINET

Group Assignment Rules

- Rules automatically place endpoints into groups based on:
 - Installer ID
 - IP address
 - OS
- FortiClient EMS automatically places endpoints that do not apply for any group assignment rule into the **Other Endpoints** group
- FortiClient EMS admin can disable or enable and delete group assignment rules

Endpoints > Group Assignment Rules

Endpoints > Workgroups > All Groups

Fortinet NSE Training Institute

© Fortinet Inc. All Rights Reserved.

44

You can use group assignment rules to automatically place endpoints into custom groups based on their installer ID, IP address, or OS.

Creating a FortiClient deployment package includes an option to specify an installer ID. For example, say you want all endpoints located in your company's headquarters to be moved on the same endpoint group. You can configure a FortiClient deployment package with an "HQ" installer ID, then deploy this deployment package to the desired endpoints.

The **IP Address** option allows you to create a group assignment rule that automatically moves all endpoints within a specified subnet or IP address range into the same custom group.

The **OS** option automatically moves all endpoints that have a specific OS installed into the custom group.

When the endpoints' FortiClient connects to FortiClient EMS, FortiClient EMS places the endpoints in the desired group.

If a newly connected endpoint does not match any group assignment rule and belongs to an imported AD domain, the endpoint is moved into the OU to which it belongs in the AD domain tree. If no AD domain has been imported, or the endpoint also does not belong to the imported AD domain, it is placed in the **Other Endpoints** group.

FortiClient EMS automatically places endpoints that do not apply to any group assignment rule into the **Other Endpoints** group.

DO NOT REPRINT
© FORTINET

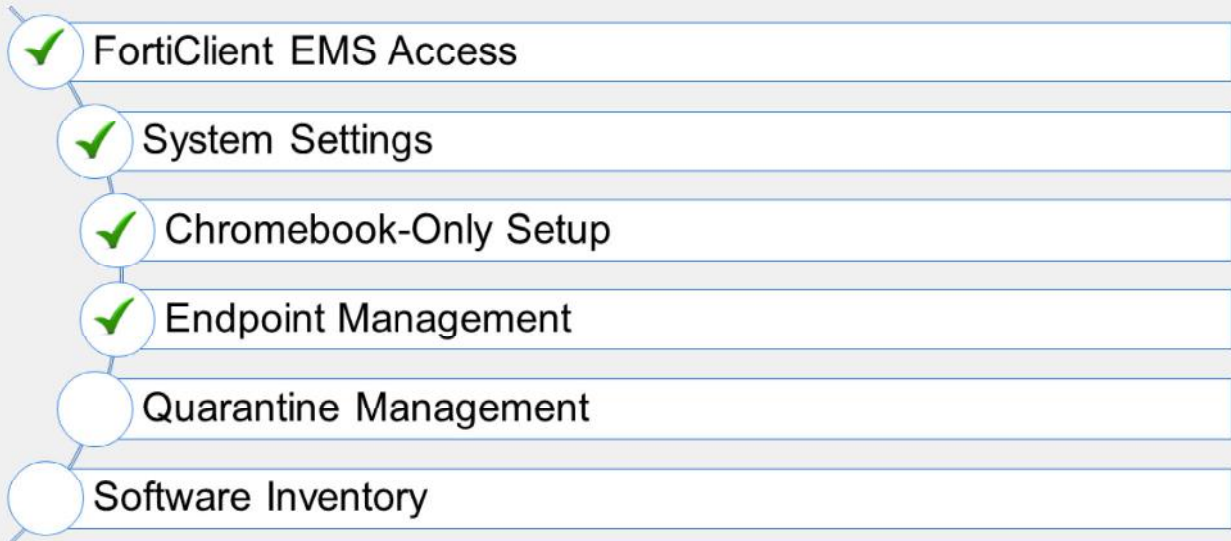
Knowledge Check

1. Which two methods can you use to add endpoints to FortiClient EMS?
 - ✓ A. Microsoft Active Directory (AD) server and manual connection from FortiClient
 - B. Import XML configuration from FortiGate and FortiClient

2. Which network device is required to manually quarantine an endpoint?
 - A. Chromebook Web Filter extension
 - ✓ B. FortiClient EMS

DO NOT REPRINT
© FORTINET

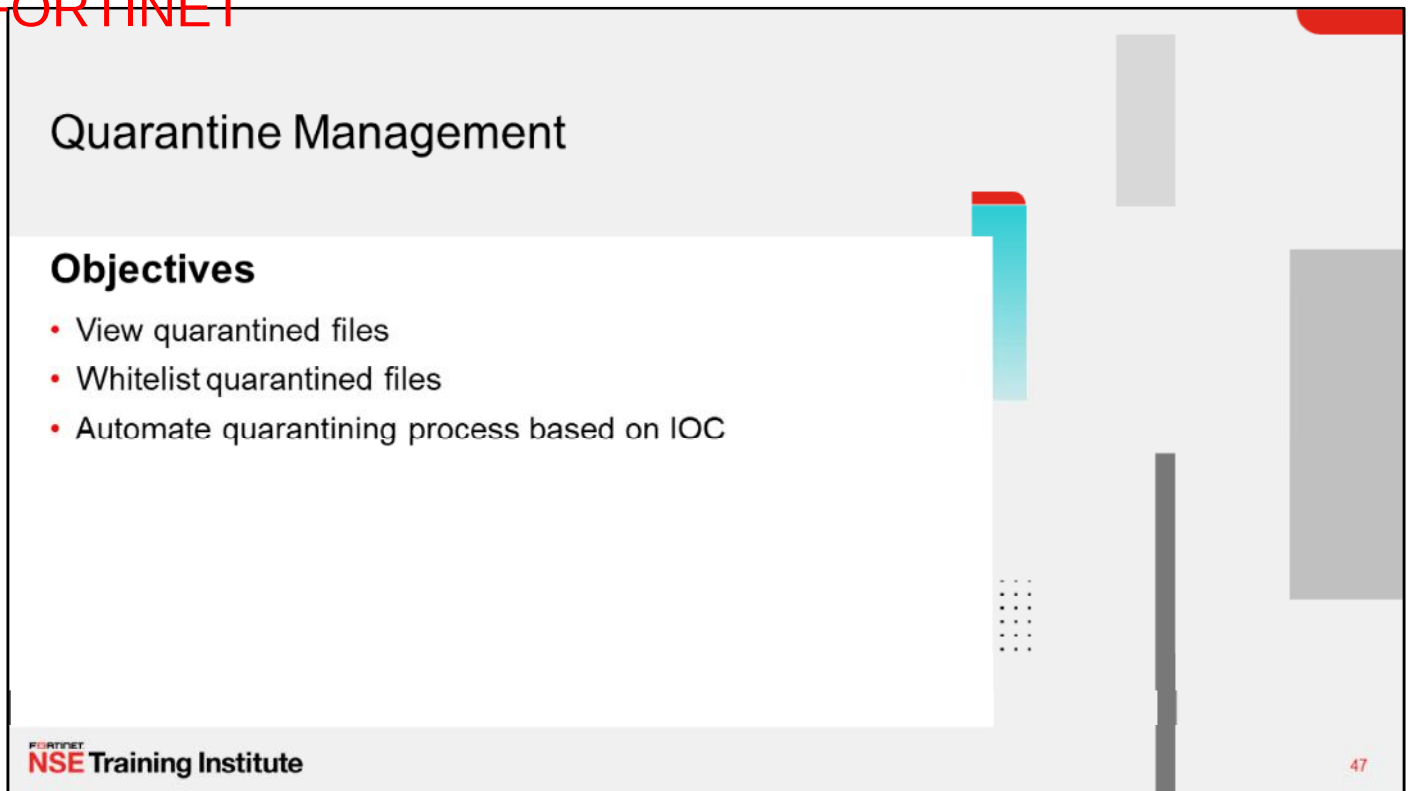
Lesson Progress



Good job! You now understand endpoint management for Windows, macOS, Linux, and Chromebook user endpoints on FortiClient EMS.

Now, you will learn about quarantine management.

DO NOT REPRINT
© FORTINET



Quarantine Management

Objectives

- View quarantined files
- Whitelist quarantined files
- Automate quarantining process based on IOC

FORTINET
NSE Training Institute

47

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in using FortiClient EMS to manage quarantined files, you will be able to view and allowlist quarantined files.

DO NOT REPRINT
© FORTINET

View Quarantined and Allowlist Files

- Viewing quarantined files
 - FortiClient sends quarantined file information to FortiClient EMS
 - You can view the list of quarantined files on the **Files** pane
 - You can filter the file list
- Allowlisting quarantined file
 - You can allowlist and restore quarantined files from EMS
 - You can view the lost allowlisted files in the **Allowlist** pane
 - You can filter, edit the file description, and delete allowlisted files

On the **Files** pane, the FortiClient EMS administrator can view quarantined file information for all managed endpoints, and whitelist files from FortiClient EMS, if needed.

FortiClient sends quarantined file information to FortiClient EMS. After FortiClient quarantines files on endpoints and sends the quarantined file information to FortiClient EMS, you can view the list of quarantined files in **Quarantine Management** on the **Files** pane. You can also view details about each quarantined file and use filters to access quarantined files that have specific qualities.

You can allowlist and restore quarantined files from EMS. This releases the files from quarantine and makes them accessible on the endpoint with the next telemetry communication between FortiClient EMS and FortiClient. The file status changes to **Quarantined & Allowlisted**.

Note that the FortiClient console doesn't allow you to restore and delete quarantined files. These options are grayed out on the FortiClient GUI.

DO NOT REPRINT
© FORTINET

Quarantine Automation

- You can enable the Security Fabric with FortiClient and EMS
- As Fabric Agent FortiClient:
 - Integrate endpoints with the Security Fabric
 - Automate response to contain incidents
- Fabric Agent with the Security Fabric:
 - Provides endpoint information
 - Runs vulnerability scan and patching
 - Identifies risky endpoints
 - Provides application inventory
- Based on IoC verdicts, FortiClient EMS and FortiOS can automate the process of quarantining suspicious endpoints

Many of you have heard of the Security Fabric. The Security Fabric uses FortiTelemetry to link different security sensors and tools together to collect, coordinate, and respond to malicious behaviour anywhere it occurs on your network, in real-time.

The Fabric Agent connects endpoints with the Security Fabric, and delivers endpoint visibility and control by sharing endpoint telemetry and compliance status with the Security Fabric. It also has vulnerability management capabilities to extend the scanning process to either the managed FortiGate or FortiClient EMS.

In the Security Fabric topology, you can see the compromised and quarantined endpoints. You can obtain the visibility and details about these endpoints from devices such as FortiAnalyzer, where indicator of compromise (IoC) verdicts are based on a threshold value that is reached or exceeded, at which point an endpoint becomes a risk, must be quarantined, and is confirmed to be compromised.

In addition to quarantining malicious files, submitting objects to FortiSandbox for analysis, and applying patches, by integrating with the Security Fabric, FortiClient can also automate the process of quarantining suspicious or compromised endpoints.

The benefits of quarantine automation include containing threats and incidents, and controlling outbreaks.

DO NOT REPRINT
© FORTINET

Quarantine Automation (Contd)

- You can quarantine an endpoint from FortiOS using EMS using an API
- The following network components are required:
 - FortiGate
 - FortiAnalyzer
 - FortiClient EMS
 - FortiClient
- Security Fabric, which includes the above network devices, can automatically quarantine an endpoint on which an IoC is detected

The screenshot shows the 'Security Fabric > Automation' configuration page. The 'Edit Automation Stitch' window is open, showing a stitch named 'Compromised Host Quarantine' with a status of 'Enable'. The stitch contains the following steps:

- Trigger:** Compromised Host Quarantine
- Action:** Compromised Host Quarantine_quarantine
- Action:** Compromised Host Quarantine_quarantine-forticlient

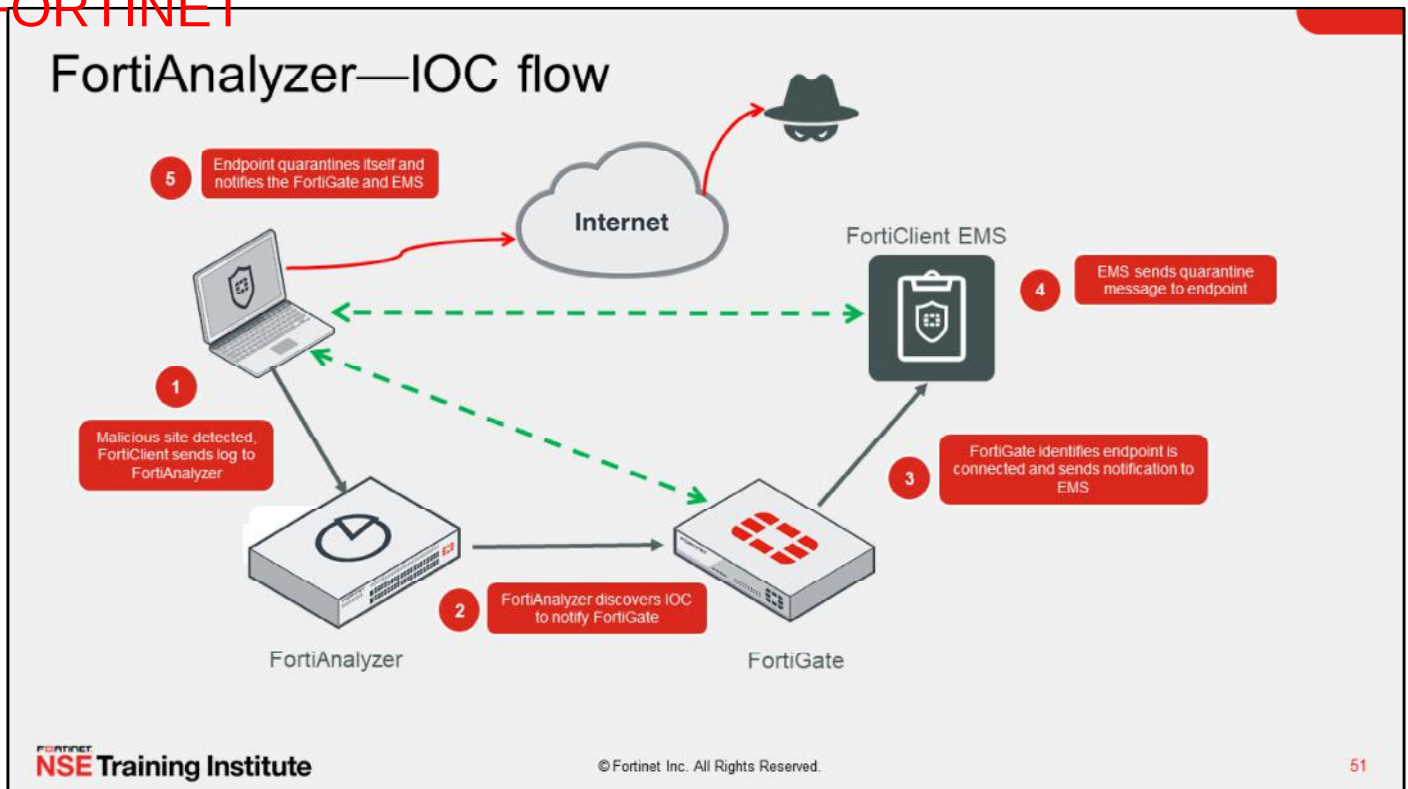
Each step is highlighted with a red box. The 'Add delay' button is visible between the steps. The 'OK' button is at the bottom right.

The Security Fabric offers visibility of endpoints at various monitoring levels. When the Security Fabric includes network devices listed here, you can configure the system to automatically quarantine an endpoint on which an IoC is detected. This requires the following network devices:

- FortiGate
- FortiAnalyzer
- FortiClient EMS
- FortiClient

You must connect FortiClient to both the EMS and FortiGate. FortiGate and FortiClient must both be sending logs to FortiAnalyzer. You must configure the EMS IP address on the FortiGate, as well as administrator login credentials.

DO NOT REPRINT
© FORTINET



51

This configuration functions as follows:

1. FortiClient sends logs to FortiAnalyzer.
2. FortiAnalyzer discovers IoCs in the logs and notifies FortiGate.
3. FortiGate identifies if FortiClient is a connected endpoint, and if it has the login credentials for the FortiClient EMS that FortiClient is connected to. With this information, FortiGate sends a notification to FortiClient EMS to quarantine the endpoint.
4. FortiClient EMS searches for the endpoint and sends a quarantine message to it.
5. The endpoint receives the quarantine message and quarantines itself, blocking all network traffic. The endpoint notifies FortiGate and EMS of the status change.

Executing automation:

The following command triggers the quarantine action on the endpoint at `endpoint_ip_address`:

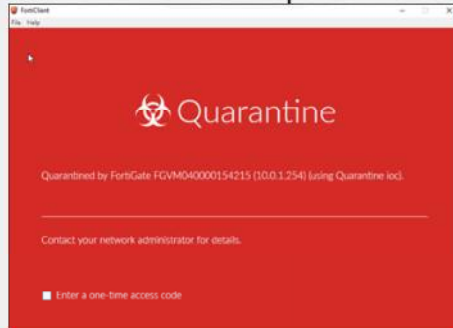
- `diag endpoint forticlient-ems-rest-api queue-quarantine-ipv4 endpoint_ip_address`

Note that this feature is not supported on FortiClient (Linux).

DO NOT REPRINT
© FORTINET

Quarantine Automation

- FortiClient must connect to the EMS
- FortiGate must have an EMS IP address and credentials to log in
- FortiAnalyzer must receive logs from both FortiGate and FortiClient
- Quarantine is done at the network interface driver level (IPS)
- Communication with FortiClient EMS remains open to unquarantined endpoint
- Telemetry to FortiGate remains established to update the status



Fortinet
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

52

You must meet the following prerequisites for FortiClient, EMS, and FortiGate:

1. FortiClient must be installed on the endpoint and connected to the EMS.
2. On FortiClient EMS, an endpoint profile and gateway list using the FortiGate IP address, must be assigned to the endpoint. It also needs an endpoint policy that is configured with the desired profile and telemetry gateway list for the desired endpoint group, and the **Remote HTTPS access** option must be enabled.
3. FortiGate must use the following configuration to quarantine an endpoint.
 - Automation trigger
 - Automation action
 - Automation stitch
 - EMS firewall address object (if using a FortiOS version earlier than 6.2.0)
 - Endpoint control FCT-EMS object

For more details about FortiGate automation configuration, see the *FortiClientEMS 7.0 Administration Guide*.

DO NOT REPRINT
© FORTINET

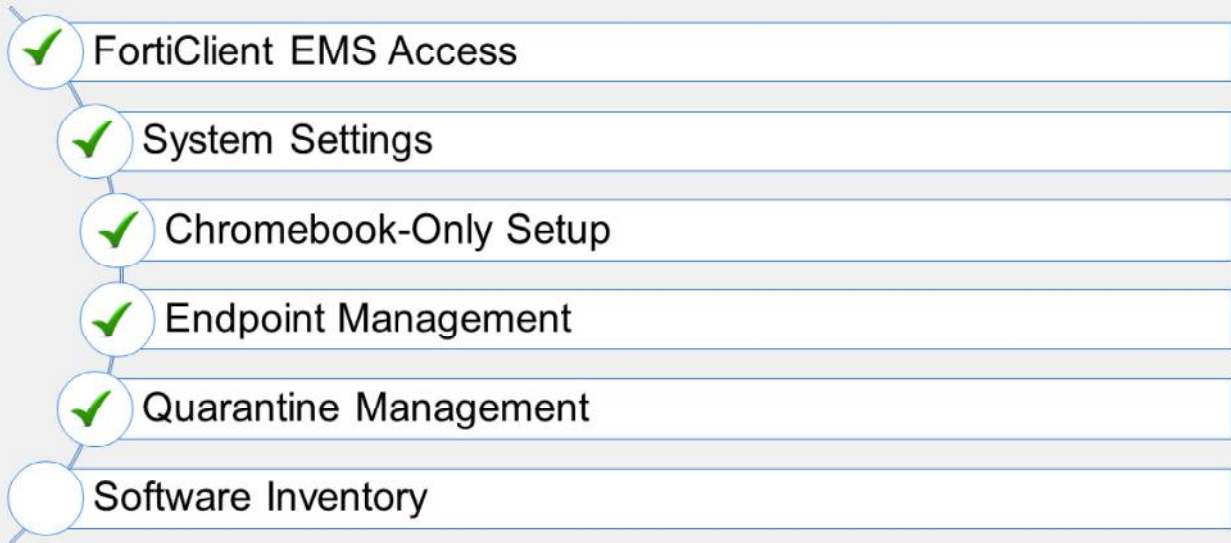
Knowledge Check

1. Which network component is required to automate endpoint quarantine?
✓ A. FortiAnalyzer
B. FortiSandbox

2. Which network device enforces quarantine and notifies the network of status changes?
A. FortiClient EMS
✓ B. FortiClient

DO NOT REPRINT
© FORTINET

Lesson Progress



Good job! You now know how to configure endpoint quarantine management.

Now, you will learn about software inventory.

DO NOT REPRINT
© FORTINET

The slide features a light gray background with a white rectangular area on the left containing the text. To the right of this area is a vertical cyan bar with a red top section. Further right are several gray rectangular blocks of varying sizes. At the bottom left is the Fortinet NSE Training Institute logo, and at the bottom right is the number 55.

Software Inventory

Objectives

- View installed applications

FORTINET
NSE Training Institute

55

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in using FortiClient EMS to view the software inventory on endpoints, you will be able to identify what applications are installed.

Applications

- You can centrally view a list of software installed on all endpoints
- The list includes details for each application, such as vendor and version information
- **Applications**
 - Shows information about installed applications for all managed endpoints
 - You can filter by application

Software Inventory > Applications

6 Total Applications		5 Total Vendors		6 New Detections	
Name	Vendor	Version	First Detected	Last Installed	Install Count
FortiClient	Fortinet Inc.	6.0.0.0036	2018-04-16	2018-04-10	1
Google Chrome	Google Inc.	65.0.3325.181	2018-04-16	2018-04-16	1
Mozilla Firefox 59.0.2 (x64 en-US)	Mozilla	59.0.2	2018-04-16		1
Mozilla Maintenance Service	Mozilla	59.0.2	2018-04-16		1
Notepad++ (64-bit x64)	Notepad++ Team	7.5.6	2018-04-16		1
Skype version 8.19	Skype Technologies S.A.	8.19	2018-04-16	2018-04-16	1

You can centrally view a list of software installed on all endpoints. The list includes details for each application, such as vendor and version information. You can view this information by application or by vendor, on the **Applications** pane, or by host on the **Hosts** pane. FortiClient sends installed application information to FortiClient EMS.

The FortiClient EMS administrator can view installed application information for all managed endpoints on the **Applications** pane.

The **Applications** pane also shows the total number of application installed, vendors, and newly installed applications. You can view the application names alphabetically, or by vendor. You can also apply filters by application name, vendor name, and version number.

DO NOT REPRINT
© FORTINET

Hosts

- **Hosts**

- Shows information about installed applications for all managed endpoints by host
- You can filter by host

Software Inventory > Hosts

Host	User	OS	IP	Application Count	Last Installation
DESKTOP-8K1R2V5	Admin	Microsoft Windows 10 Enterprise	10.0.1.10	7	2019-09-18

Name	Vendor	Version	Install Date
Adobe Reader X	Adobe Systems Incorporated	10.0.0	2019-09-18
FortiClient	Fortinet Technologies Inc	6.2.1.0831	2019-09-18
Microsoft Visual C++ 2008 Redistributable ...	Microsoft Corporation	9.0.30729.6161	2019-09-18
Microsoft Visual C++ 2008 Redistributable ...	Microsoft Corporation	9.0.30729.4148	2019-09-18
Mozilla Firefox 69.0 (x86 en-GB)	Mozilla	69.0	2019-08-27
Mozilla Maintenance Service	Mozilla	69.0	2019-09-18
VMware Tools	VMware, Inc.	10.0.6.3595377	2019-09-18

The FortiClient EMS administrator can view installed applications information for all managed endpoints by host on the **Hosts** pane.

The **Hosts** pane shows the total number of applications, OS details, and lists of the software installed on the endpoints. You can also view other details about the hosts, as shown on this slide image.

You can apply filters by host name, user name, OS name, and IP address.

DO NOT REPRINT
© FORTINET

Knowledge Check

1. Which pane shows information about installed applications for all managed endpoints?
✓ A. Application pane
B. Host pane

DO NOT REPRINT
© FORTINET

Lesson Progress



Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in this lesson.

DO NOT REPRINT
© FORTINET

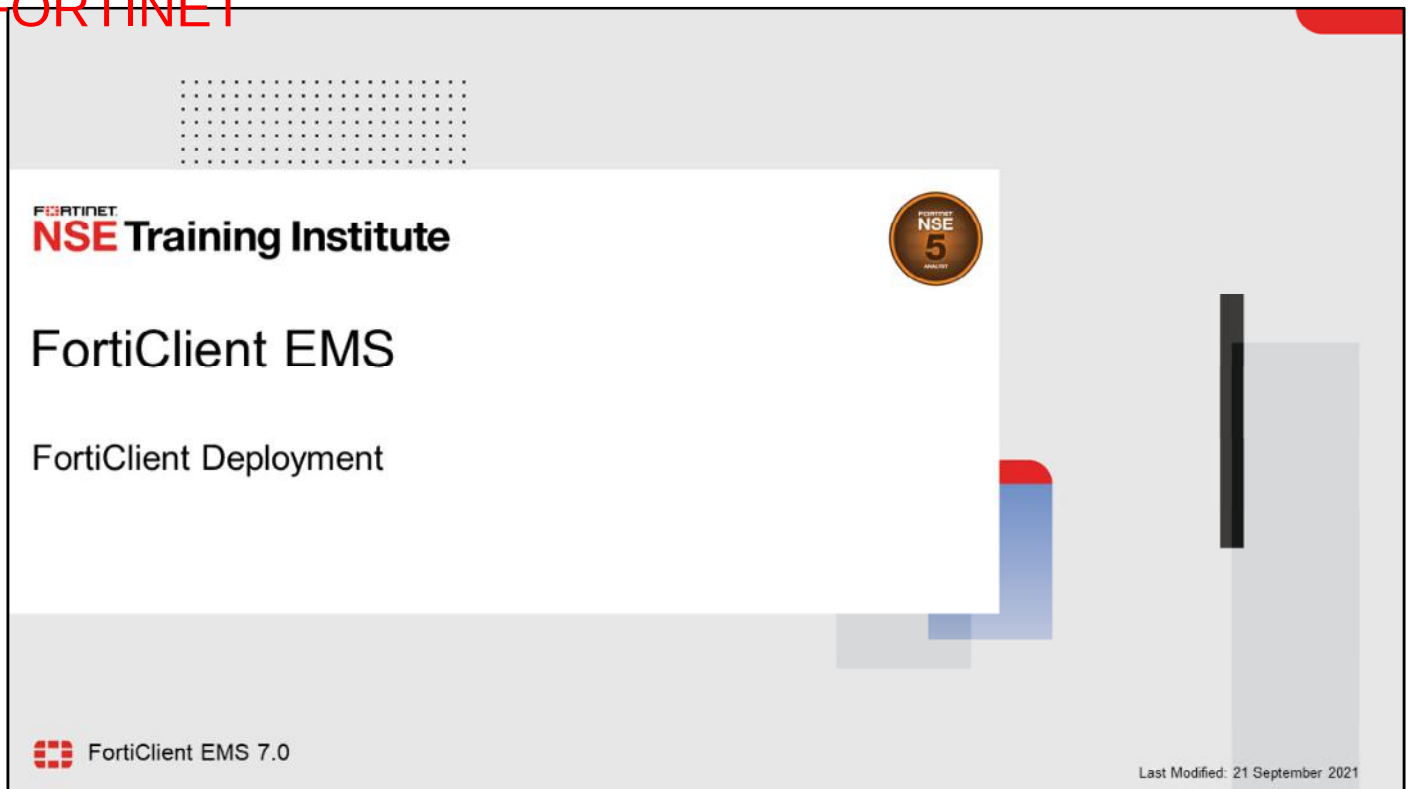
Review

- ✓ Access FortiClient EMS
- ✓ Understand FortiClient administration and database management
- ✓ Configure FortiClient EMS server, logs settings, banners, and alerts settings
- ✓ Configure FortiClient EMS to manage Chromebooks
- ✓ Manage FortiClient EMS endpoints
- ✓ View quarantined and allowlist quarantined files
- ✓ Manage the FortiClient EMS quarantine process
- ✓ View the FortiClient software inventory

This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned how to install, configure, and administer FortiClient EMS. You also learned how to manage a large number of endpoints.

DO NOT REPRINT
© FORTINET

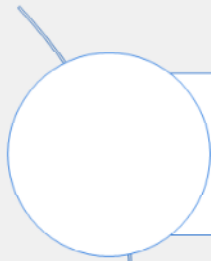


In this lesson, you will learn how to deploy FortiClient and manage deployment packages using FortiClient EMS.

By demonstrating competence in FortiClient deployment, you will be able to deploy FortiClient endpoints using EMS in Windows Active Directory environment, as well as prepare and manage different types of installation files.

DO NOT REPRINT
© FORTINET

Lesson Overview



Deployment



Managing Installers

In this lesson, you will learn about the topics shown on this slide.

By demonstrating competence in FortiClient deployment, you will be able to prepare Windows Active Directory (AD) server and endpoints, as well as implement different deployment types. You will also be able to deploy various types of FortiClient endpoint using FortiClient EMS and MacOS.

DO NOT REPRINT
© FORTINET

Deployment

Objectives

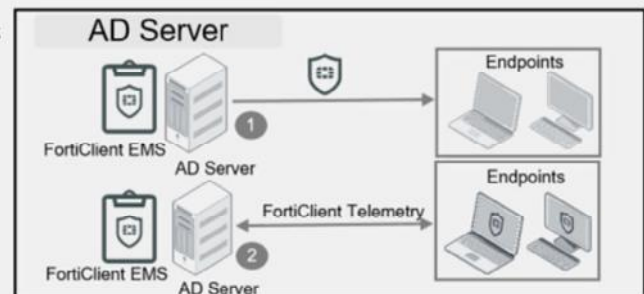
- Understand deployment methods
- Prepare the Windows AD server for deployment
- Prepare the Windows endpoint
- Understand deployment types
- Manage deployment configuration

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in FortiClient deployment, you will be able to prepare Windows AD server and endpoints, as well as implement different deployment types.

Deployment Methods

- There are two methods you can use to add FortiClient to EMS:
 - Windows AD
 - Workgroups
- AD
 - An AD setup provides central management and control (group policies)
 - You can deploy initial installation of Windows FortiClient but can not deploy macOS FortiClient
 - After installation endpoints are connected to EMS, you can deploy:
 - Upgrades
 - Removals
 - Replacement of FortiClient for Windows and macOS



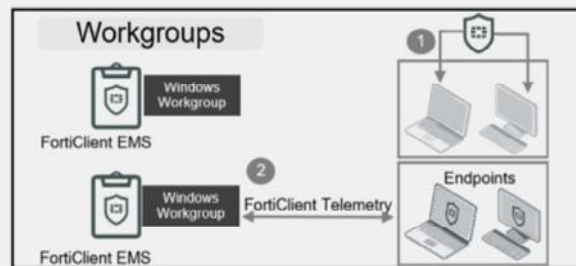
There are two methods that you can use to add FortiClient to EMS: Windows AD and workgroups.

AD setup provides central management and control (group policies) for the Windows endpoint. It is generally used in large setups to implement corporate policies such as resource usage and access control.

When using an AD server, you can deploy an initial installation of FortiClient (Windows) to endpoints, but you cannot deploy an initial installation of FortiClient (macOS). After FortiClient for Windows or macOS is installed on endpoints and endpoints are connected to FortiClient EMS, you can deploy upgrades, removals, and replacements of both FortiClient for Windows and macOS using AD servers.

Deployment Methods (Contd)

- Workgroup
 - A collection of computers on a LAN that share common resource and responsibility
 - You cannot deploy an initial installation
 - You can use workgroups to uninstall and update FortiClient on endpoints



A Windows workgroup is a collection of computers on a local area network (LAN) that share common resources and responsibilities. Being a peer-to-peer (P2P) network design, each workgroup computer may both share and access resources if configured to do so. Workgroups are designed for small LANs. This setup doesn't have a centralized server and all the Windows endpoints in LAN need to be configured as individually machines.

When using workgroups, you cannot deploy an initial installation of FortiClient to endpoints. However, after FortiClient is installed on endpoints and endpoints are connected to FortiClient EMS, you can use workgroups to uninstall and update FortiClient on endpoints.

DO NOT REPRINT
© FORTINET

Prepare the AD Server

- You must install and prepare the AD server before you deploy FortiClient installation
 - Configure a group policy under **Group Policy Management**
 - Use the default domain policy, or create a new one to assign to the OU that contains endpoint
 - Configure Windows services in the **Group Policy Management Editor**
 - **Task Scheduler: Automatic**
 - **Windows Installer: Manual**
 - **Remote Registry: Automatic**
 - Configure deployment rules for Windows firewall
 - Allow inbound connection for SMB-In and RPC
 - Configure Windows firewall domain profile settings
 - Allow inbound file and printer sharing exception
 - Allow inbound remote administration exception
 - Allow ICMP exceptions
 - Allow inbound echo request

To deploy FortiClient from FortiClient EMS, you must prepare the AD server for deployment and deploy FortiClient on the endpoints. Before you can successfully deploy a FortiClient installation, ensure you install and prepare the AD server by completing the tasks shown on this slide.

Note that you cannot use FortiClient EMS to deploy an initial installation of FortiClient to endpoints (macOS and workgroup computers). However, after FortiClient is installed on the endpoints, and the endpoints are connected to FortiClient EMS, you can use FortiClient EMS to uninstall and update FortiClient on endpoints.

DO NOT REPRINT
© FORTINET

Prepare Windows Endpoints

- You must prepare the Windows endpoint before deploying FortiClient installation
 - Configure Windows services to the following settings:
 - **Task Scheduler: Automatic**
 - **Windows Installer: Manual**
 - **Remote Registry: Automatic**
 - Configure Windows firewall rules to:
 - Allow inbound connection for file and printer sharing (SMB-In)
 - Allow inbound connection for remote scheduled tasks management (RPC)
- AD administrator account use for AD group deployments
- An installer URL is shared for non-AD deployments
 - Can download and install FortiClient manually

You must enable and configure the following services on each Windows endpoint before FortiClient deployment:

- **Task Scheduler: Automatic**
- **Windows Installer: Manual**
- **Remote Registry: Automatic**

The Windows firewall must allow SMB-in and RPC traffic for inbound connections.

For AD group deployments, an AD administrator account is required. For non-AD deployments, the installer URL can be shared with users, who can then download and install FortiClient manually. You can locate the installer URL in the **Manage Installers** pane.

Note that when you are adding endpoints using an AD domain server, FortiClient EMS automatically resolves endpoint IP addresses during initial deployment of FortiClient. FortiClient EMS can deploy FortiClient (Windows) to AD endpoints that do not have FortiClient installed, as well as upgrade existing FortiClient installations, if the endpoints are already connected to the EMS server.

You can execute `gpresult.exe /H gpresult.html` on any AD client to verify if you have an issue pushing the group policy to the endpoints.

Deploying FortiClient

- Deploy a FortiClient installation from FortiClient EMS using an AD server
 - Add the AD server to FortiClient EMS by adding a domain
 - Add a FortiClient installer package to FortiClient EMS
 - Add a profile
 - Select the FortiClient installer package
 - Configure FortiClient features in the profile
 - Assign the profile to the AD domain to push the FortiClient installation process on the endpoints
 - Verify the deployment by monitoring FortiClient connections to the FortiClient EMS
- Deploying initial installations of FortiClient (macOS)
 - Create a custom FortiClient (macOS) installer on FortiClient EMS and send the installer download link to users so they can install FortiClient manually
 - Use a third-party application to perform initial deployment of FortiClient (macOS) to endpoints
- Deploying FortiClient upgrades from EMS
 - You can deploy a FortiClient software update from EMS
 - Prompt appears on endpoint when installer package is about to be deployed

You can deploy FortiClient on Windows endpoints using an AD server: For successful deployment of FortiClient installation from FortiClient EMS using an AD server, you must prepare the AD server, add the AD server to FortiClient EMS as a domain, add an installer package to FortiClient EMS, add a profile (which includes the installer package and configured FortiClient features), and assign the profile to a branch of the AD domain to push the installation. You can verify the deployment by monitoring FortiClient connections to the EMS.

FortiClient EMS cannot be used to deploy initial installations of FortiClient (macOS). You can deploy an initial installation of FortiClient (macOS) by doing one of the options that are shown on this slide. After FortiClient (macOS) is installed on endpoints, and you have connected FortiClient Telemetry to FortiClient EMS, you can use FortiClient EMS to replace, upgrade, and uninstall FortiClient.

You can also deploy a FortiClient software update from FortiClient EMS when endpoints running older version. A prompt appears on the FortiClient endpoint when an installer package is requested to be deployed. The prompt instructs the user to choose an upgrade option: **Upgrade Now** or **Upgrade Later**. If you select the **Upgrade Now** option, FortiClient performs the upgrade and automatically restarts your computer. If you select the **Upgrade Later**, the user can indicate the time to start the upgrade. The default is 8:00 PM. Your computer automatically restarts after the upgrade.

If no option is selected, the upgrade occurs, by default, at 8:00 PM. After FortiClient EMS uninstalls the previous version, it asks if the user wants to reboot now or reboot later.

Deployment Configuration

- You can create a deployment configuration
- A deployment configuration includes the following fields:
 - Name
 - Endpoints group
 - Action
 - Deployment Package
 - Start time
 - Unattended installation
 - Reboot when need
 - Reboot when no users are logged in
 - Notify user
 - Username and password
- An endpoint is eligible for multiple deployments and two factors determine which one to apply:
 - The deployment configuration enable on FortiClient EMS
 - The priority level

Deployment & Installers > Manage Deployment

Name	Installer
Versions	Windows 7 0.0, Mac 7.0.0
Auto Update	Enabled
Managed by EMS	10.0.1.100/0013
Auto Registration	Enabled
Desktop Shortcut	Enabled
Start Menu Shortcut	Enabled

You can create a deployment configuration on FortiClient EMS. An administrator can select different configuration options when deploying FortiClient. You can configure the configuration deployment name, select endpoint groups, take action to install or uninstall FortiClient, and select deployment installer.

The EMS administrator can also select start time to install FortiClient. An unattended installation option restrict user from changing installation schedule and if required, the device reboots without warning.

The **Reboot When Needed** option reboots the endpoint to install FortiClient when needed and the **Reboot When No Users Are Logged In** option allows the endpoint to reboot without prompt, if no endpoint user is logged into FortiClient.

The **Notify Users and Let Them Decide When To Reboot When Users Are Logged In** option notifies the end user if a reboot of the endpoint is needed and allows the user to decide what time to reboot the endpoint. Disable this option to reboot the endpoint without notifying the user.

The username and password allows you to enter the admin credentials for the AD. The credentials allow FortiClient EMS to install FortiClient on endpoints using AD.

You can also enable or disable the deployment using the **Enable the Deployment** option.

When an endpoint is eligible for multiple endpoint deployment configurations, two factors determine which configuration EMS applies to the endpoint:

- EMS applies deployment configurations to endpoints only if the configurations are enabled on the EMS.
- If an endpoint is eligible for multiple enabled configurations, FortiClient EMS applies the configuration with the first priority level to the endpoint.

DO NOT REPRINT
© FORTINET

Knowledge Check

1. What Windows services are required on the server and the client?
✓ A. Remote Registry and Task Manager
B. Remote Access and FortiClient Proxy Service

2. Which one you can use to deploy the initial FortiClient installation?
✓ A. Domain
B. Workgroup

DO NOT REPRINT
© FORTINET

Lesson Progress

The diagram shows a vertical sequence of two steps. The first step, 'Deployment', is marked with a green checkmark in a circle, indicating it is completed. The second step, 'Managing Installers', is marked with an empty circle, indicating it is pending. A vertical line connects the two circles, and a horizontal line extends from the 'Deployment' circle to its text box.

- Deployment
- Managing Installers

FORTINET
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

11

Good job! You now understand FortiClient deployment methods and types.

Now, you will learn about how to manage FortiClient installers and the deployment package.

DO NOT REPRINT
© FORTINET

Managing Installers

Objectives

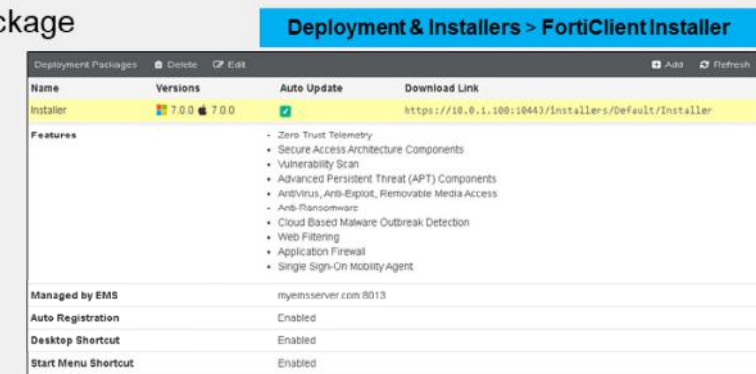
- Understand deployment packages
- Understand FortiClient installers

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in working with deployment packages and installers, you will be able to create deployment packages, installers, and manage on FortiClient EMS.

Deployment Packages

- Use to deploy FortiClient to endpoints
- Deployment packages include:
 - FortiClient installer, which determines release and patch
 - FortiClient features to be installed on the endpoints
- You can specify which FortiClient features to include and then disable them later in a profile
- You can not edit the deployment package
- To add a package you can select
 - Version
 - General
 - Features
 - Advanced
 - Telemetry



You can create deployment packages to deploy FortiClient to endpoints. Deployment packages include the FortiClient installer, which determines the FortiClient release and patch to install on the endpoint, as well as which FortiClient features are installed on the endpoint.

You can also specify what FortiClient features to include in the deployment package for the endpoint. You can include a feature in the deployment package, then disable the feature in the profile. Because the feature is included in the deployment package, you can update the profile later to enable the feature on the endpoint.

After you add a package to the FortiClient EMS, you can not edit it. You can delete the package and edit the deployment package outside of the FortiClient EMS and then can add the edited deployment package to the FortiClient EMS. When adding a package you can select an installer type, release version, patch, and enable FortiClient to automatically update to the latest release, and installer's name and notes.

In **Features** section, you can select options to enable zero-trust telemetry (enabled by default and can't be disabled); secure success (SSL and IPsec VPN); APT, and additional security features such as antivirus protection, web filtering, SSO agent, and cloud-based malware detection.

The **Advanced** section allows you to enable automatic registration, desktop shortcut, installer ID, and endpoint profile. The **Telemetry** tab displays the hostname and IP address of the FortiClient EMS server, which will manage FortiClient after it is installed on the endpoint.

You can view the deployment packages in the **Deployment & Installers** pane. You can view more details or delete packages in the **Deployment Packages** pane.

FortiClient Setup and Modules

- When an administrator creates a FortiClient deployment package in EMS, they choose which setup type and modules to install
 - Zero trust telemetry
 - Secure access architecture components
 - Advanced persistent threat (APT) components
 - Additional Security Features

Setup type	Description	Impact on FortiClient
Zero trust telemetry	Enabled by default and installs FortiClient with Telemetry enabled.	Displays the following tabs: - Zero Trust Telemetry - Selected optional security feature
Secure access architecture components	Optional. Supports SSL and IPsec VPN access.	Displays the Remote Access tab.
Vulnerability scan	Optional. Supports vulnerability scanning, and vulnerability remediation.	Displays Vulnerability Scan tab.
Advanced persistent threat (APT) components	Optional. Supports FortiSandbox and quarantine features.	Enables the Sandbox Detection tab to connect to FortiSandbox
Additional security features	Optional. Supports AntiVirus, Anti-Exploit, Anti-Ransomware, Web Filtering, Application Firewall, SSO mobility agent, and cloud-based malware outbreak detection. The administrator may select one, more, or all security features.	Displays the following tabs when all security features are selected: - Malware Protection - Web Filter - Application Firewall When Single Sign On is selected, FortiClient supports the SSO feature. When a security feature is not selected, the tab is hidden from view in FortiClient.

When the administrator creates a FortiClient deployment package in EMS, they choose which setup type and modules to install:

- Zero trust telemetry (Selected by default, you must also select one of the other security feature to create package)
- Secure access architecture components
- Vulnerability scan
- Advanced persistent threat (APT) components
- Additional security features

The impact of the options are shown on this slide. The administrator can use an FortiClient EMS profile to disable installed components on FortiClient but cannot use an FortiClient EMS profile to enable uninstalled components on FortiClient.

For example, if the administrator creates the FortiClient EMS installer with APT components selected, the **Sandbox Detection** tab is enabled on FortiClient. The administrator can use an EMS profile to disable **Sandbox Detection**. However, if the installer did not include APT components, the **Sandbox Detection** tab is disabled on FortiClient and the administrator cannot use an EMS profile to enable **Sandbox Detection**.

DO NOT REPRINT
© FORTINET

Zero Trust Telemetry

- Zero Trust Telemetry:
 - Enabled by default, you cannot disable
 - Installs FortiClient telemetry
 - Must select another FortiClient feature with zero trust telemetry to create a package



By default, zero trust telemetry feature is selected and enabled when you select a installer file. This setup installs telemetry component to FortiClient. You must also select one of the other security feature to create package.

Telemetry provides endpoint visibility and ensures that all fabric components—FortiGate, FortiAnalyzer, FortiClient EMS, managed APs, managed switches, and sandbox have a unified view of endpoints in order to provide tracking and awareness, compliance enforcement, and reporting.

Secure Access Architecture Components

- Secure access architecture components:
 - Support remote access (SSL and IPsec VPN)
 - Useful to connect remote users after initial FortiClient installation to activate FortiClient license
 - This is optional feature



The secure access architecture component installs FortiClient with the **Remote Access** tab. FortiClient provides flexible options for VPN connectivity. It supports both secure sockets layer (SSL) and internet protocol security (IPsec) VPNs.

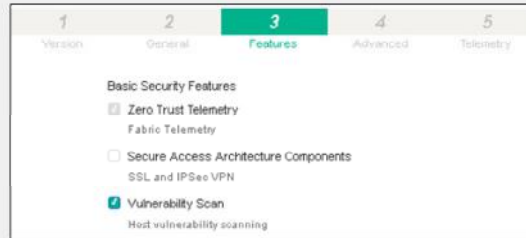
If you enable this feature for a deployment package and include a preconfigured VPN tunnel in the included endpoint profile, users who use this deployment package to install FortiClient can connect to this preconfigured VPN tunnel for three days after their initial FortiClient installation. This is useful for remote users, as it allows them to connect to the corporate network to activate their FortiClient license. If the user does not activate their FortiClient license within the three days, all FortiClient features, including VPN, stop working on their device.

Note that this is an optional feature.

DO NOT REPRINT
© FORTINET

Vulnerability Scan

- Vulnerability scan:
 - Enables vulnerability scan feature
 - Provides endpoint hygiene
 - Reduces attack surface



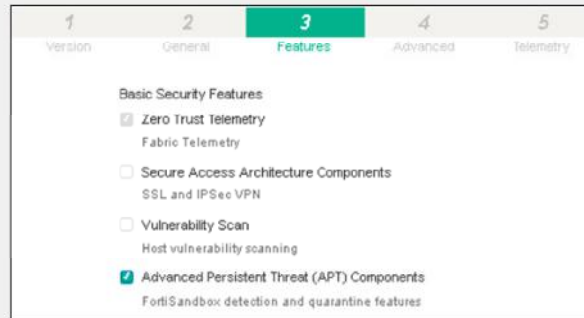
The vulnerability scan feature enables host vulnerability scanning on FortiClient. FortiClient helps organizations reduce attack surface with vulnerability scanning and optional auto-patching. Combined with the zero-trust access principles, this approach can enhance an organization's hygiene and security posture.

All vulnerable endpoints are easily identified on FortiClient EMS for remediation. This feature is optional.

DO NOT REPRINT
© FORTINET

APT Components

- APT Components:
 - Installs FortiClient with APT components
 - Integrates FortiSandbox with FortiClient
 - Provides FortiSandbox detection and quarantine feature

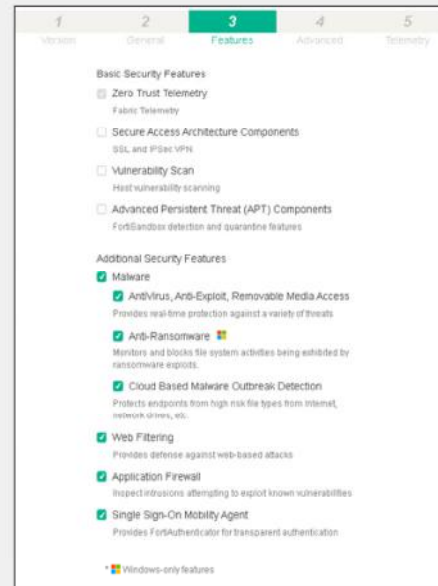


The APT components feature enables FortiSandbox integration with FortiClient. By integrating with FortiSandbox and leveraging FortiGuard global threat intelligence, FortiClient prevents advanced malware and vulnerabilities from being exploited.

FortiClient integrates with FortiSandbox to analyze all downloaded files in real time to FortiClient endpoints. FortiClient and FortiSandbox users worldwide share information about known and unknown malware with FortiGuard threat intelligence platform. FortiGuard automatically shares the intelligence with FortiClient endpoints to protect against emerging threats.

Additional Security Features

- Additional security feature enables:
 - Malware
 - Antivirus, antiexploit, removeable media access
 - Anti-ransonsomware (Windows only)
 - Cloud-based malware outbreak detection
 - Web filtering
 - Application firewall
 - Single sign-on mobility agent



The **Additional Security Features** option enables the malware, web filtering, application firewall and single sign-on mobility agent.

Malware includes antivirus, anti-exploit, removable media access, anti-ransomware, and cloud-based malware outbreak detection. These feature provide real time protection against a variety of threats such as file system activities exhibited by ransomware exploits or high risk file types from internet and network drives.

Web Filtering provides defence against web-based attacks.

Application Firewall inspects intrusions that attempt to exploit known vulnerabilities.

Single Sign-On Mobility Agent enables transparent authentication or single sign-on feature. This setup requires FortiAuthenticator.

Deployment Packages

- Deploy different installer IDs using same deployment package
 - Suitable for environment with large number of endpoints
 - Requires FortiClient installation using CLI
- Cli command for .msi file
 - `msiexec /i forticlient.msi GROUP_TAG=<installer_ID>`
- Cli command for .exe file
 - `FortiClientSetup.exe /v"GROUP_TAG=<installer_ID>"`
- For example, HR, marketing and office management endpoints using same deployment package respectively:
 - `FortiClientSetup.exe /v"GROUP_TAG=<HR>"`
 - `FortiClientSetup.exe /v"GROUP_TAG=<Marketing>"`
 - `FortiClientSetup.exe /v"GROUP_TAG=<OM>"`

You can include an installer ID in a FortiClient deployment package. After FortiClient installation, the endpoint connects to FortiClient EMS and FortiClient EMS groups the endpoint according to the installer ID group assignment rule. You can configure one installer ID for each deployment package.

In an environment with a large number of endpoints, you may have multiple installer IDs that you want to use to group endpoints automatically in FortiClient EMS after installation. Since you can configure each deployment package with only one installer ID, it may be inefficient to create a deployment package for each installer ID.

Instead, you can use the same deployment package on multiple endpoints, providing different installer IDs in the CLI depending on which group you want FortiClient EMS to place the endpoint in. When these endpoints connect to FortiClient EMS, FortiClient EMS groups them according to the installer ID provided in the CLI.

This process consists of the following steps:

1. Create a deployment package in FortiClient EMS. Do not configure an installer ID.
2. Create installer ID group assignment rules to automatically move endpoints into the desired groups.
3. Install FortiClient on endpoints using the CLI commands show on this slide:

Consider that you want to deploy the same deployment package but different installer IDs for the HR, marketing, and office management teams at your organization. In this scenario, you would use EMS to create an deployment package without an installer ID and an installer ID group assignment rule for each endpoint group. Then, you can install FortiClient on the endpoints using the deployment package and CLI command as shown on this slide.

After the endpoints connect to FortiClient EMS, FortiClient EMS automatically places them into groups based on their installer IDs (for example HR, marketing, and office management).

FortiClient Installers

- FortiClient installers are available from:
 - FortiGuard
 - Custom FortiClient installers
- FortiGuard Distribution Network (FDN)
 - FortiClient EMS automatically connects to FDN
 - To provide access to FortiClient installers you can use with deployment packages
 - Download manually if no connection to FDN
 - You can download installer to use from these locations:
 - <https://support.fortinet.com>

FortiClient EMS automatically connects to FDN to provide access to FortiClient installers that you can use with FortiClient EMS profiles. If a connection to FDN is not available, you must manually download FortiClient installers to use with FortiClient EMS.

You can download FortiClient installers to use with FortiClient EMS from the Fortinet Support site.

After you add a FortiClient installer to FortiClient EMS, you cannot edit it. You can delete the installer from FortiClient EMS, and edit the installer outside of FortiClient EMS. You can then add the edited installer to FortiClient EMS.

DO NOT REPRINT
© FORTINET

Custom Installers

- Adding custom FortiClient installers
 - You can create a custom installer and add to FortiClient EMS
 - Manually download and add to EMS if no connection to FDN
 - Option to select Windows or Mac OS installer
 - Supports both MSI or ZIP files for Windows
 - Supports DMG files for macOS
 - You can not upload FortiClient free VPN client installer

Deployment & Installers > FortiClient Installer > +Add

Add FortiClient Installer

Name
Required
Provide a memorable name for this set of installation files.

☒ Upload Windows Installers

Windows 64-Bit Installer (ZIP or MSI)
Browse... Required

Windows 32-Bit Installer (ZIP or MSI)
Browse... Required

☐ Upload Mac Installer

Upload Cancel

You can create a custom FortiClient installer and add it to FortiClient EMS. Alternately, if a connection to FDN is not available, you may need to manually download a FortiClient installer and add it to FortiClient EMS.

There are options to select Windows or Mac installer. Windows installers must be MSI or ZIP files and macOS must be DMG files. You cannot upload the FortiClient free VPN client installer.

After you add FortiClient installers to FortiClient EMS, you can view them in the **FortiClient Installers** pane. By default, this page lists installers from FortiGuard first, then from uploaded installers. The following information is displayed for each installer:

- Name
- Versions
- Type

DO NOT REPRINT
© FORTINET

Knowledge Check

1. By what method can you add a custom installer to FortiClient EMS?
 - A. Connection to FDS
 - ✓ B. Manual upload

2. What is required to import a certificate from FortiGate?
 - A. FortiGate configuration file
 - ✓ B. FortiGate log in details

DO NOT REPRINT
© FORTINET

Lesson Progress



Deployment



Managing Installers

Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in this lesson.

DO NOT REPRINT
© FORTINET

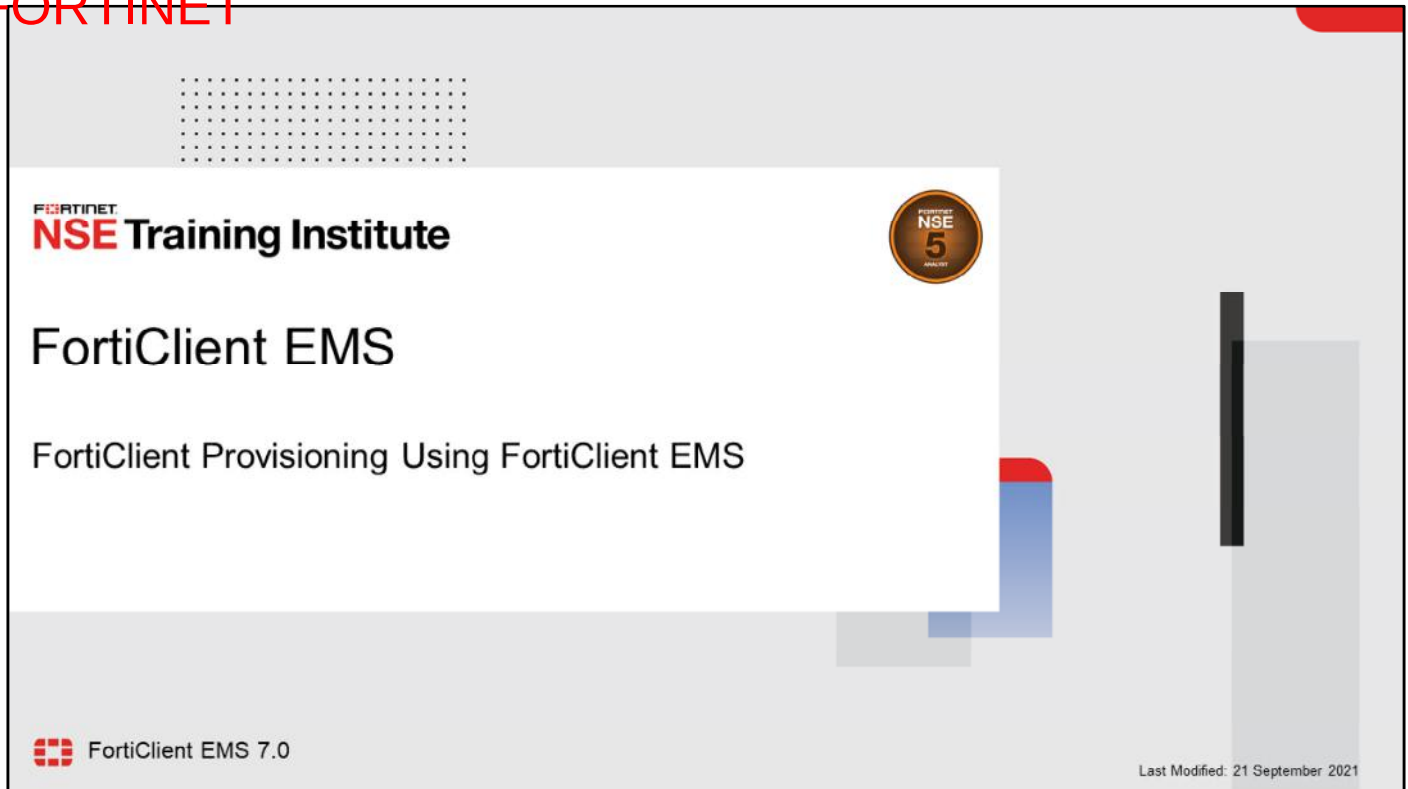
Review

- ✓ Understand deployment methods
- ✓ Prepare the AD server for deployment
- ✓ Prepare the Windows endpoint
- ✓ Understand deployment types
- ✓ Manage deployment configuration
- ✓ Understand deployment packages
- ✓ Understand FortiClient installers

This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned about deployment types, configuration, and packages.

DO NOT REPRINT
© FORTINET

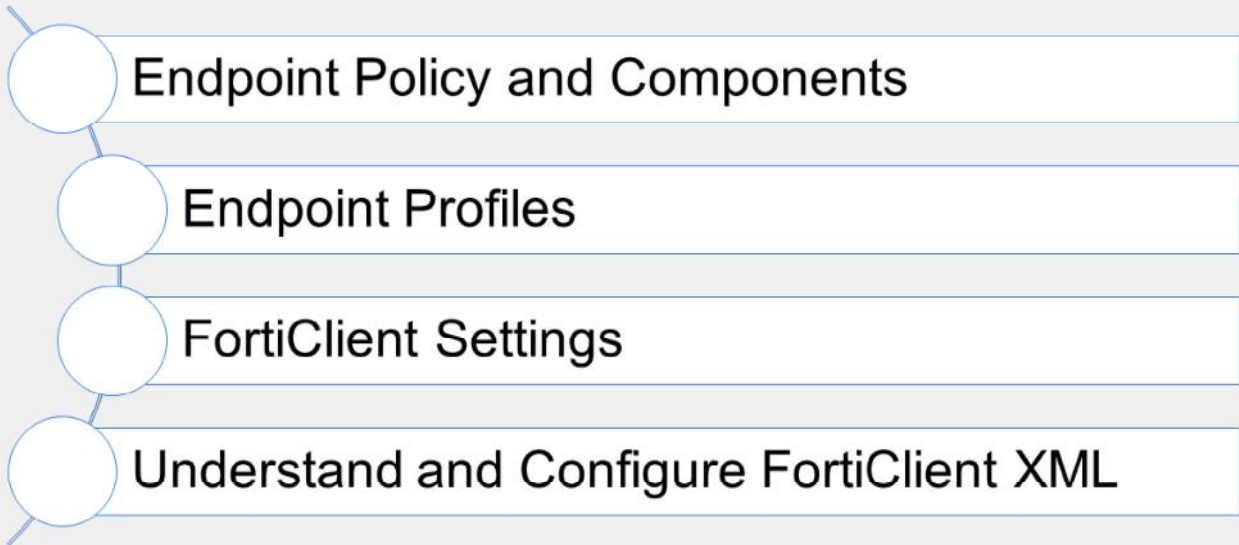


In this lesson, you will learn how to provision FortiClient on endpoints using FortiClient EMS.

By demonstrating competence in FortiClient provisioning, you will be able to create endpoint policy and profiles, as well as enable different FortiClient features and settings.

DO NOT REPRINT
© FORTINET

Lesson Overview



In this lesson, you will learn about the topics shown on this slide.

DO NOT REPRINT
© FORTINET

Endpoint Policy and Components

Objectives

- Understand endpoint policy
- Configure and edit endpoint policy
- Manage CA certificates
- Configure on-fabric detection rules

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in configuring and editing endpoint policy, you will be able to use endpoint policy to apply an endpoint profile to endpoint groups or users.

DO NOT REPRINT
© FORTINET

Endpoint Policy

- Default policy:
 - When you install FortiClient EMS, a default policy is created
 - By default, the endpoint policy assigns a default endpoint profile to unassigned endpoint groups or AD device groups that are part of the initial installation
 - You can modify a default policy but you cannot disable or delete it
 - Default policy only supports changing on and off fabric setting

Endpoint Policy & Components > Manage Policies

Endpoint Policy

Endpoint Policy Name	Default
Profile	Default
Profile (Off-Fabric)	Optional
On-Fabric Detection Rules	Optional
Comments	Optional
Enable the Policy	☒

Save **Cancel**

An endpoint policy assigns endpoint profiles to endpoint groups or users of Windows, macOS, and Linux endpoints. The **Manage Policies** page provides a comprehensive summary of which endpoint policies are applied to which endpoint groups or AD device groups (computers).

When you install FortiClient EMS, a default policy is created. By default, the default policy assigns a default endpoint profile to unassigned endpoint groups or AD device groups, or to groups or users that do not match any other policy configured on FortiClient EMS on initial setup.

You can edit a default policy but you cannot disable it or delete it. You can modify only on-fabric and off-fabric endpoint profiles on the default policy.

Note that when a user switches accounts between a local non-domain account and a domain account on the same machine, FortiClient EMS may not apply the correct policy to the endpoint.

DO NOT REPRINT
© FORTINET

Endpoint Policy (Contd)

- You can also create a new endpoint policy to assign the following to endpoint groups or users:
 - Endpoint profiles
 - On-fabric detection rules
- You can do the following on FortiClient EMS:
 - Add an endpoint policy
 - Edit an endpoint policy
 - Delete an endpoint policy
 - Enable or disable an endpoint policy
- Chromebook policy
 - Assign an endpoint profile to groups of Chromebook endpoints
 - A Chromebook profile is available only if the FortiClient EMS is configured to manage Chromebooks endpoints

Endpoint Policy & Components > Manage Policies

Endpoint Policy

Endpoint Policy Name:

Endpoint Groups:

Users:

Profile:

Profile (Off-Fabric):

On-Fabric Detection Rules:

Comments:

Enable the Policy: ☒

You can create new endpoint policies to assign endpoint profiles to endpoint groups or AD users.

In the screen capture shown on this slide, you can see that endpoints that belong to the domain **trainingAD** group and **All Groups** include workgroup endpoints that have the endpoint profiles configured in the endpoint policy. You must select an on-fabric profile on the policy, but an off-fabric profile is optional. FortiClient EMS pushes these settings to the endpoint with the next Telemetry communication. In this example, endpoints in the trainingAD group are applicable for the **Student Policy**. FortiClient EMS applies only the **Training Policy** to the group.

You can add, edit, delete, enable, or disable a policy on the **Manage Policies** page.

You can also create Chromebook policies to assign endpoint profiles and telemetry gateway lists to groups of Chromebook endpoints. The **Manage Chromebook Policies** page provides a comprehensive summary of which policies are applied to which groups within the Google domain. This option is available only if the **FortiClient EMS for Chromebooks Settings** option is enabled on the FortiClient EMS server.

Chromebook policies function identically to Windows, macOS, and Linux endpoint policies, except that they are applied to Chromebook endpoints and can include only a Chromebook profile, not a telemetry gateway list.

Endpoint Policy—Policy Priority

- An endpoint can be eligible for multiple endpoint policies
- The factors that determine which policy to apply are as follows:
 - The policy must be enabled on FortiClient EMS
 - If an endpoint is eligible for multiple enabled policies, FortiClient uses the following criteria, in the following order, to decide which policy to assign to the endpoint.
 - If a policy has been directly assigned to the user, FortiClient applies it
 - If a policy has been assigned to a group container, user group, or both, FortiClient applies the policy with the highest priority level
 - If multiple inherited policies have been assigned to a parent container or group, FortiClient assigns the policy with the highest priority level
- To change endpoint policy priority, click **Change Priority** and then move to the desired position

Endpoint Policy & Components > Manage Policies

Name	Assigned Groups	Profile	Policy Components	Endpoint	Pri.	Enab...
Training	All Groups trainingAD training lab	PROFILE Fortine... OFF-FABRIC Defa...	On-F...	3	1	☒
AD-Group	trainingAD training lab	PROFILE Fortine... OFF-FABRIC Defa...		9	2	☒

Priority has changed after moving AD-Group policy above Training policy

Name	Assigned Groups	Profile	Policy Components	Endpoint	Pri.	Enab...
AD-Group	trainingAD training lab	PROFILE Fortine... OFF-FABRIC Defa...		2	1	☒
Training	All Groups trainingAD training lab	PROFILE Fortine... OFF-FABRIC Defa...	On-F...	1	2	☒

An endpoint can be eligible for multiple endpoint policies. When an endpoint is eligible for multiple endpoint policies, the following factors determine which endpoint policy FortiClient EMS applies to the endpoint:

- FortiClient EMS applies endpoint policies to endpoints only if those policies are enabled on the **Endpoint Policy & Components Manage Policies** page.
- If an endpoint is eligible for multiple enabled endpoint policies, FortiClient EMS determines which policy to apply using the following criteria, in the following order:
 - If a policy is directly assigned to the user (configured in the **Users** field for the endpoint policy), FortiClient EMS assigns that policy to the endpoint.
 - If there are policies assigned to the group container, or user group, or both, FortiClient EMS assigns the policy with the highest priority level to the endpoint.
 - If there are inherited policies assigned to the group container, or user group, or both (policies assigned to a parent container or group), FortiClient EMS assigns the policy with the highest priority level to the endpoint.

In the example shown on this slide, the AD group **TrainingAD** is eligible for both the **Training** and **AD-Group** policies. In this scenario, FortiClient EMS applies the first eligible endpoint policy, **Training**, to the AD group because it has the highest priority level. In order to apply a more restrictive policy (**AD-Group**) to endpoints, the administrator must move the policy so that it has a higher priority level than the **Training** policy.

To change priority level, on the **Manage Policies** page, click **Change Priority**, select a policy, and then move the selected policy up or down, depending on your requirements.

DO NOT REPRINT
© FORTINET

Managing CA Certificates

- You can upload or import a CA certificate into FortiClient EMS
- You can upload locally by browsing to the file

Endpoint Policy & Components > CA Certificates

Upload Local Certificate

Browse...

Upload Cancel

- Importing a certificate from FortiGate requires the following:
 - A FortiGate IP address
 - A VDOM
 - A login username
 - A login password

Import Certificates from FortiGate

IP address/hostname
IP Port

VDOM
root

Username
Required

Password

Import Cancel

Fortinet
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

7

FortiClient EMS allows you to upload or import a CA certificate. You can upload the certificate manually by browsing the CA certificates files on your local computer. Alternatively, you can import a certificate from FortiGate. You will need to provide the FortiGate IP address, VDOM information, and login credentials.

FortiClient EMS will use the HTTPs port to import certificates.

On-Fabric Detection Rules

- On-fabric detection rules:
 - FortiClient EMS uses rules to determine on-fabric or off-fabric endpoints
 - Depending on the status, FortiClient EMS can apply a different endpoint profile
- You can select one of the following rule sets:
 - DHCP Server
 - DNS Server
 - FortiClient EMS Connection
 - Local IP/Subnet
 - Default Gateway
 - Ping Server
 - Public IP
 - Connection Media
 - VPN Tunnel

Endpoint Policy & Components > On-fabric Detection Rules

On-Fabric Rule Set

Name: ON-Fabric

Enabled: ☒

Comments: Optional

Rules: ☒ Edit Rule ☒ Delete Rule

Rule Type	Criteria
Ping Server	IP: 8.8.8.8

You can configure on-fabric detection rules for endpoints. FortiClient EMS uses the rules to determine if the endpoint is on-fabric or off-fabric. Depending on the endpoint on-fabric status, FortiClient EMS may apply a different profile to the endpoint, as configured in the applied endpoint policy. A rule set is available for on-fabric detection.

The DHCP server allows you to configure the IP address, the MAC address, or both, of the DHCP server. You can also configure the DHCP code. The DHCP code is synonymous with option 224 in FortiOS 6.0, which was the FortiGate serial number. Now, the DHCP code can be any string configured in the DHCP server as option 224. You may still use the FortiGate serial number as the DHCP code, if desired. FortiClient EMS considers the endpoint as satisfying the rule if it is connected to a DHCP server that matches the specified configuration. You can configure multiple IP and MAC addresses and DHCP codes. If you select a DNS server, FortiClient EMS considers the endpoint as satisfying the rule if it is connected to a DNS server that matches the specified configuration. You can configure multiple IP addresses for the DNS server.

If **FortiClient EMS Connection** is selected as the detection type, FortiClient EMS considers the endpoint as satisfying the rule if it is online with FortiClient EMS. The local IP/subnet allows you to configure a range of IP addresses considered as local IP addresses. Configuring the gateway MAC address is optional. FortiClient EMS considers the endpoint as satisfying the rule if its Ethernet or wireless IP address is within the range specified, and if its default gateway MAC address matches the one specified, if it is configured.

The default gateway option allows you to configure the gateway IP address. FortiClient EMS considers the endpoint as satisfying the rule if its default gateway configuration matches the IP address specified and MAC address. Again, the MAC address is optional.

DO NOT REPRINT
© FORTINET

On-Fabric Detection Rules (Contd)

Endpoint Policy & Components > On-fabric Detection Rules > Add Rule

The screenshot displays the 'Add New Rule' dialog in FortiClient EMS. It shows three different detection rules configured:

- DHCP Server Rule:** The 'Detection Type' is 'DHCP Server'. The 'IP Address' field is highlighted with a red box. A callout labeled 'DHCP server' points to the 'DHCP Code' field.
- Ping Server Rule:** The 'Detection Type' is 'Ping Server'. The 'IP Address' field is highlighted with a red box. A callout labeled 'Ping server' points to the 'IP Address' field.
- Connection Media Rule:** The 'Detection Type' is 'Connection Media'. The 'Ethernet' field is highlighted with a red box. A callout labeled 'Connection media' points to the 'Ethernet' field.

Each rule has an 'Add Rule' button and a 'Cancel' button.

Fortinet NSE Training Institute

© Fortinet Inc. All Rights Reserved.

9

For ping server detection, FortiClient EMS considers the endpoint as satisfying the rule if it can access the server at the specified IP address. The public IP option allows you to use the public IP address or WAN IP address of an endpoint. FortiClient EMS considers the endpoint as satisfying the rule if its public (WAN) IP address matches the one specified. You can configure multiple addresses.

If you select **Connection Media** as the detection type, you have the option to select a connection status, such as **Connected**, or **Not Connected** for the Ethernet connection, the Wi-Fi connection, or both. The Wi-Fi option also requires the **SSID** and security type of the wireless connection. FortiClient EMS considers the endpoint as satisfying the rule if its network settings match all configured fields.

Note that on-fabric detection rules do not apply to endpoints running FortiClient 6.2.1 and earlier versions.

In the VPN tunnel option, you can type an SSL or IPsec VPN tunnel name. FortiClient EMS considers the endpoint as satisfying the rule if it is connected to a VPN tunnel with a matching name. You can configure tunnels by pressing the + button.

This slide shows some of the detection types and their options.

DO NOT REPRINT
© FORTINET

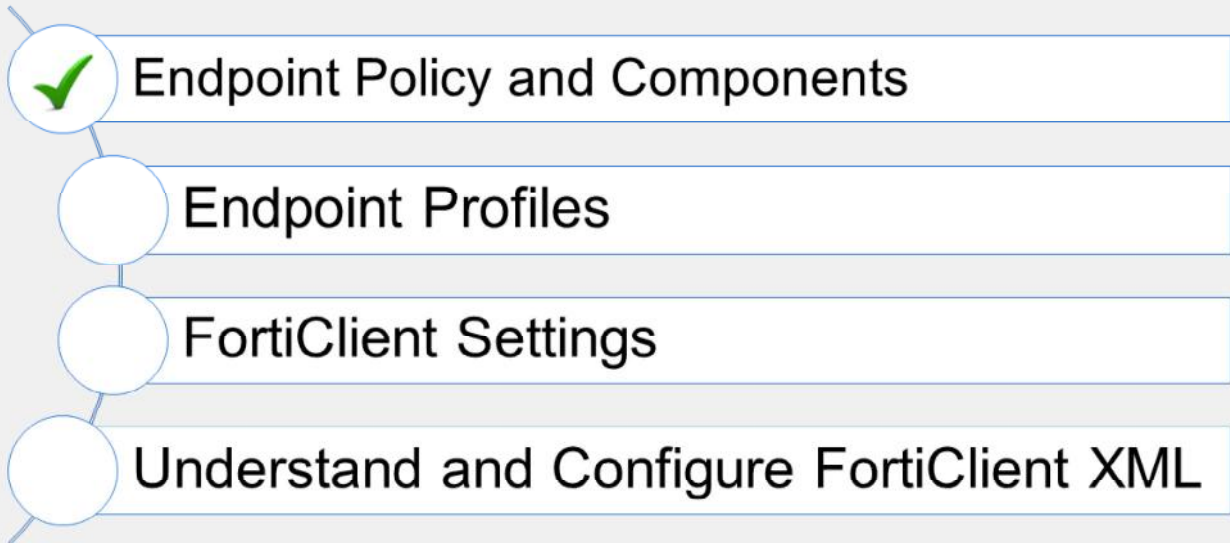
Knowledge Check

1. Which endpoint policy is applied to workgroups and domains that have no endpoint policy assigned?
☐ A. Custom endpoint policy
☒ B. Default endpoint policy

2. Which on-fabric detection rule can you select based on access to the specified IP address?
☒ A. Ping server
☐ B. DHCP server

DO NOT REPRINT
© FORTINET

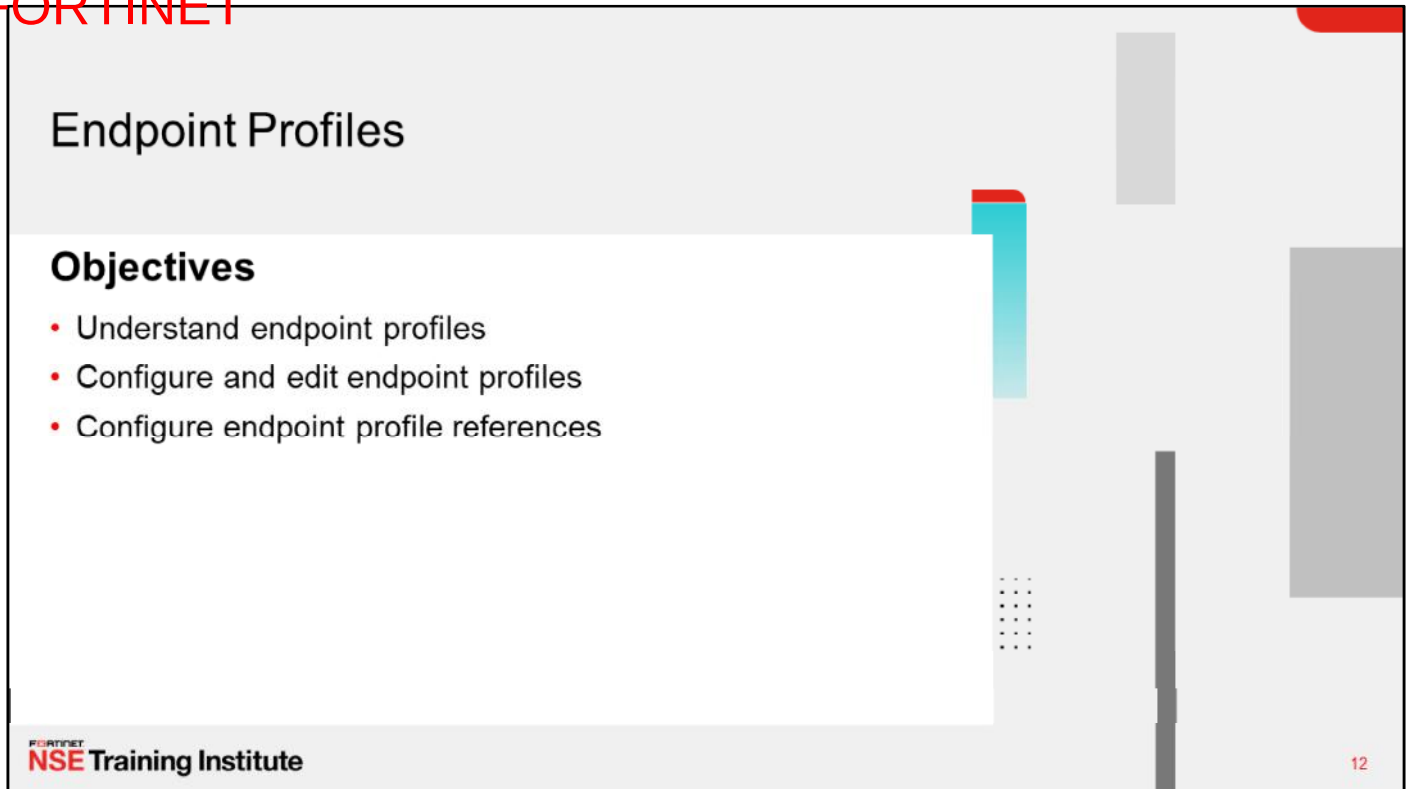
Lesson Progress



Good job! You now understand endpoint policy and its components.

Now, you will learn about endpoint profiles.

DO NOT REPRINT
© FORTINET



Endpoint Profiles

Objectives

- Understand endpoint profiles
- Configure and edit endpoint profiles
- Configure endpoint profile references

FORTINET
NSE Training Institute

12

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in configuring, editing, assigning, and managing endpoint profiles, you will be able to use endpoint profiles to define the features installed on FortiClient endpoints.

DO NOT REPRINT
© FORTINET

Endpoint Profiles—Default Profile

- When you install FortiClient EMS, a default profile is created
- The default profile is designed to provide effective levels of protection
- There is only one default profile for the following operating systems:
 - Windows
 - macOS
 - Linux endpoints
- Chromebook has a separate default profile because of different supported features
- You can also edit the default profiles
 - To edit the default profile for Chromebooks, click **Endpoint Profiles > Local Chromebook Profiles**, and click the **Default - Chromebooks** profile.
 - To edit the default profile for other endpoints, click **Endpoint Profiles > Local Profiles**, and click the **Default** profile.

When you install FortiClient EMS, a default profile is created. By default, this profile is applied to any groups you create. The default profile is designed to provide effective levels of protection. There are separate default profiles for Windows, macOS, and Linux endpoints and for Chromebook endpoints.

You can create and configure separate profiles for Windows, macOS, and Linux endpoints and for Chromebook endpoints. You can also edit the default profiles as shown on this slide.

You can edit, to add, or remove settings in the default profile. You can also revert to the default settings by clicking **Revert to Default**.

DO NOT REPRINT
© FORTINET

Configure and Create Profiles

- To use specific features, such as application firewall, either create a new profile or edit the default profile
- Consider the following when creating profiles:
 - Use default settings within a profile
 - Consider the endpoint role when changing the default profile or creating new profiles
 - Create a separate group and profile for endpoints requiring long-term special configuration
 - Use FortiClient EMS for all central profile settings, and set options for within the group
 - FortiClient EMS can only apply profile to a group
- In FortiClient EMS you can create endpoint profiles to achieve desired settings

The default profile is designed to provide effective levels of protection. To use specific features, such as application firewall, create a new profile or edit the default profile.

Note that an individual FortiClient must belong to a group before the settings can be pushed to them.

Configure and Create Profiles (Contd)

- Profiles to configure FortiClient
 - Exclude any installation or uninstallation of FortiClient software on endpoints
 - Only to configure FortiClient software on endpoints
- Creating profiles with XML
 - You can configure FortiClient profile settings by using XML or a custom XML configuration in XML editor
 - The custom XML file must include all settings required by the endpoint

Endpoint Profiles > Manage Profiles > +Add

Fortinet NSE Training Institute

© Fortinet Inc. All Rights Reserved.

15

You can create endpoint profiles to configure FortiClient. This profile excludes any installation or uninstallation of FortiClient software on endpoints, and is used to configure FortiClient software on endpoints.

You can also configure FortiClient profile settings in FortiClient EMS by using XML or a custom XML configuration by using the XML editor on FortiClient EMS. The custom XML file must include all settings required by the endpoint at the time of deployment.

DO NOT REPRINT
© FORTINET

Endpoint Profiles—Import Profiles

- Importing FortiGate web filter profiles
 - You can import a FortiClient web filter profile into FortiClient EMS
- Importing FortiClient profiles from FortiManager
 - You can import web filter profiles from FortiManager into FortiClient EMS
- Importing a profile from XML file
 - You can import XML profile configuration file and upload to FortiClient EMS

Endpoint Profiles > Manage Profiles > Import

You can import a FortiClient web filter profile from FortiGate and FortiManager devices into FortiClient EMS, then edit the profile in FortiClient EMS to add a FortiClient installer or other configuration details.

To import profiles successfully from FortiOS to FortiClient EMS, the HTTPS port on FortiGate and FortiManager must be open.

You need the IP address and port number of the FortiGate or FortiManager device from which the profile is being imported. You also need a VDOM name from the FortiGate or FortiManager, if applicable; login username; and password to connect.

You can also import the XML configuration file to create a profile. If the profile has a feature enabled that is disabled in **Feature Select**, FortiClient EMS displays a warning that the feature will not be enabled on endpoints that the profile is deployed to. To enable this feature on the endpoint, you must enable the feature in **Feature Select**.

DO NOT REPRINT
© FORTINET

Profile for Chromebooks

- Chromebook profiles support
 - Web filtering by categories
 - Block and allow lists
 - Safe search
- You can create different profiles and assign them to different groups in the Google domain
- Default profile applies to any domains you add
- Viewing profiles
 - Newly created endpoint profiles are listed under **Endpoint Profiles** in the left pane
 - You can view endpoint profiles and their settings

Chromebook profiles support web filtering by categories, block and allow lists, and safe search. You can create different profiles and assign them to different groups in the Google domain. When you install FortiClient EMS, a default profile is created. This profile is applied to any domains you add to FortiClient EMS.

The search engine provides a safe search feature that blocks inappropriate or explicit images from search results. The safe search feature helps block most adult content. FortiClient EMS supports safe search for most common search engines, such as Google, Yahoo, and Bing.

The profile in FortiClient EMS controls the safe search feature.

DO NOT REPRINT
© FORTINET

Managing Profiles

- The profile settings are automatically pushed to the endpoints
- Unassigned domain or workgroup gets default profile
- You can manage profiles from the **Endpoint Profiles** pane
- You can
 - Edit profiles
 - Clone profiles
 - Sync profile changes
 - Edit sync schedules
 - Delete profiles

When you assign the profile using endpoint policy to domains or workgroups, the profile settings are automatically pushed to the endpoints in the domain or workgroup. If you do not assign a profile to a specific domain or workgroup, the default profile is automatically applied. After editing an existing profile assigned to endpoints or domains, the changes are also automatically pushed to the endpoints or Chromebooks when you save the profile.

When you clone a profile, all the content displays in the content pane, and you can save the cloned profile with a new name.

For profiles imported from FortiGate or FortiManager, you can manually sync profiles so they are updated with the latest changes from the FortiGate or FortiManager device that they were imported from. You can also edit the sync schedule time.

You can also delete any newly created profile. But note that you cannot delete the default profile and the assigned profiles.

DO NOT REPRINT
© FORTINET

Profile Name

- Only the **Web Filter** and **System Settings** tabs are available for Chromebooks
- You can give a name to a profile
- There are two display options for configuration
 - Basic
 - Advanced

Endpoint Profiles > Manage Profiles > +Add

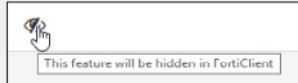
For Chromebooks, only the **Web Filter** and **System Settings** tabs are available. All other tabs are exclusive to Windows, macOS, and Linux endpoints.

The **Profile Name** allows you to enter a name and select a display option. The **Basic** display option shows all the GUI options. The **Advanced** display option enables the XML configuration tab to configure a profile using XML. This option is available only for Windows, macOS, and Linux profiles.

DO NOT REPRINT
© FORTINET

Profile References—Eye Icon

- The eye icon is available on the following features:
 - Malware Protection
 - Sandbox
 - Web Filter
 - Application Firewall
 - VPN
 - Vulnerability Scan
- Use the eye icon to show or hide the features from the end user in FortiClient



The eye icon is available on the following FortiClient features:

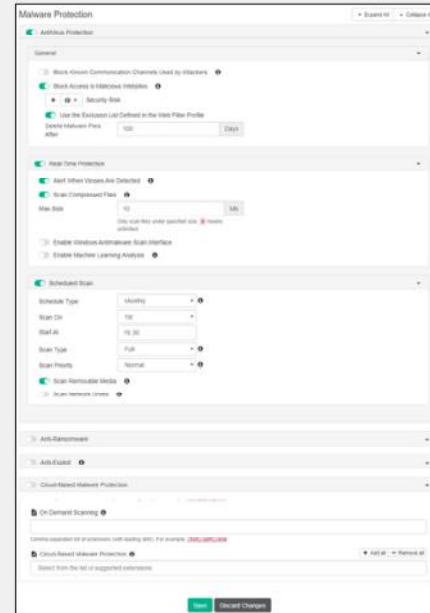
- Malware Protection
- Sandbox
- Web Filter
- Application Firewall
- VPN
- Vulnerability Scan

You can use the eye icon to show or hide the feature from the end user, in FortiClient. When you select hide, the feature will still run in the background, but the endpoint user cannot see it. It is very useful when inspecting the traffic without the user's knowledge.

Malware Protection

- On the **Malware Protection** tab, you can enable **Antivirus Protection** to see the following sections and options:

- **General**
- **Real-Time Protection**
- **On Demand Scanning**
- **Scheduled Scan**
- **Anti-Ransomware**
- **Anti-Exploit**
- **Cloud Based Malware Detection**
- **Removable Media Access**
- **Exclusions**
- **Other**



You can enable antivirus protection on FortiClient. Some options display only if you enable **Advanced**.

In the general settings, you enable or disable options that will block communication to known channels, block access to malicious websites, and identify malware and exploits using signatures from FortiSandbox.

In real-time protection settings, FortiClient can take different actions on virus discovery. You can also select file size and scan files accessed by a user or system process, such as read or write. On-demand scanning integrates FortiClient into the Windows Explorer menu. You can pause scanning when a computer is running on battery power, and automatically submit suspicious files to FortiGuard for analysis. You can also select schedule type, scan type, and priority. You can also select removable media and network drives for scanning.

Anti-ransomware protects specific files, folders, or file types on your endpoints from unauthorized changes.

The anti-exploit option enables the anti-exploit engine to monitor commonly used applications for attempts to exploit known vulnerabilities. You can exclude applications from anti-exploit detection and enable system tray notifications.

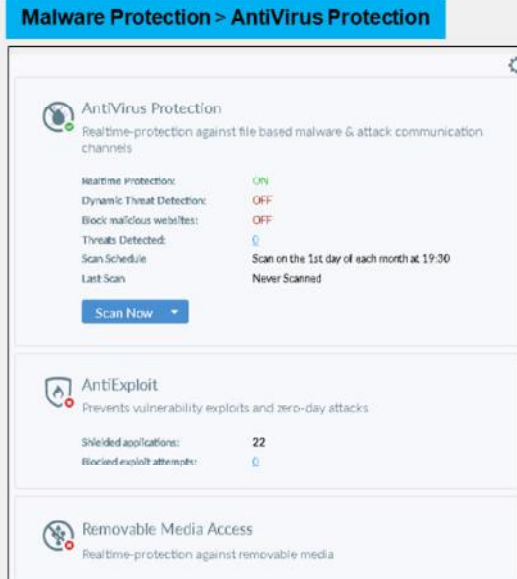
You can enable cloud-based malware outbreak detection. The cloud-based malware protection feature helps protect endpoints from high risk file types that come from external sources, such as the internet or network drives, by querying FortiGuard to determine whether files are malicious.

You can also enable controlling access to removable media devices and file or folder exclusions from antivirus scanning. The **Other** option enables scanning for rootkits, adware, riskware, email, media on insertion, and advanced heuristics signature. You must use the **Advanced** view to see the **Other** option.

DO NOT REPRINT
© FORTINET

Antivirus Dashboard

- Settings
 - View real-time protection
 - Show the status of the database
 - Initiate a scan on demand
- By default, **Malware Protection** is disabled on the FortiClient EMS **Default** endpoint profile



Once malware is enabled on the endpoint profile and pushed to FortiClient, you can view available options on the anti-virus dashboard on the FortiClient console.

You can view the real-time protection status, view if the database is up-to-date, or perform an on-demand antivirus scan. Malware protection is disabled, by default, on the FortiClient EMS **Default** endpoint profile.

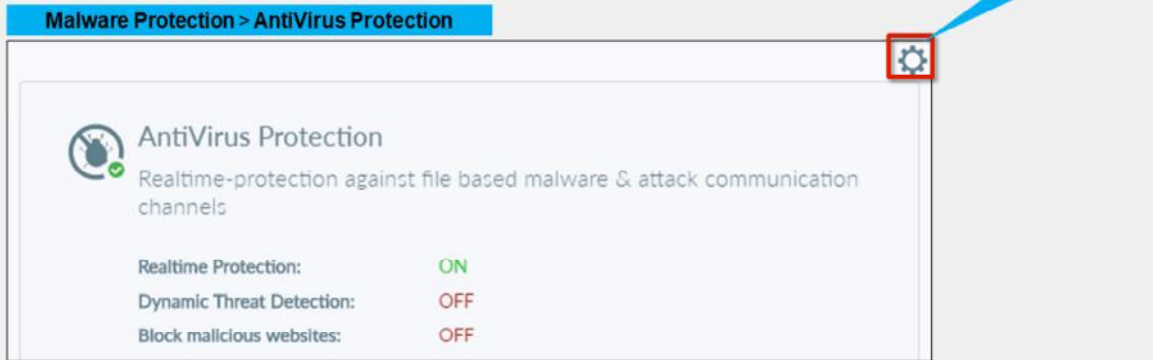
FortiClient automatically disables RTP after installation when one of the following is true:

- The OS is a server
- Exchange Server is detected
- SQL Server is detected

DO NOT REPRINT
© FORTINET

Configuring Antivirus Options

- FortiClient EMS endpoint profile allows you to configure AV options
- You can click the **Settings** icon to view the configuration
 - Shows real-time protection status
 - Shows scheduled scan
 - Shows an exclusion list



As you know, FortiClient security features are licensed with FortiClient EMS. Without a connection to FortiClient EMS, the features disappear. You can only configure AV options on an endpoint profile in FortiClient EMS to make changes.

You can click the **Settings** icon to view most of the antivirus configuration. On real-time protection, you can configure settings to specify what to scan. When a virus is detected during real-time monitoring, it is automatically quarantined. If you have another antivirus program installed, FortiClient displays a warning message stating that your system may lock up or become unstable because of conflicts between the different antivirus products. You should uninstall all conflicting antivirus software before installing FortiClient or enabling antivirus real-time protection.

You can also enable scheduled antivirus scans that automatically scan your workstation at a scheduled time. An exclusion list allows you to include files and folders that you don't want included in an antivirus scan.

DO NOT REPRINT
© FORTINET

Configuring Real-Time Protection Settings

- You can use real-time protection settings to:
 - Scan files as they are downloaded or copied to my system
 - Dynamic threat detection using threat intelligence data
 - Block malicious websites
 - You must also enable FortiProxy on FortiClient
 - Block known communication channels used by attackers

Malware Protection > AntiVirus Protection

AntiVirus Protection ☒

Settings

- ☒ Scan files as they are downloaded or copied to my system
 - ☐ Antimalware Scan Interface (AMSI)
- ☐ Dynamic threat detection using threat intelligence data
- ☒ Block malicious websites
 - Security Risk
 - ☒ Malicious Websites
 - ☒ Phishing
 - ☒ Spam URLs
 - ☒ Dynamic DNS
 - ☒ Newly Observed Domain
 - ☒ Newly Registered Domain
- ☒ Block known attack communication channels

Scheduled Scan

Schedule Type: Monthly

Scan On: 1

Start (HH-MM): 19:30

Scan Type: Full Scan

☐ Disable Scheduled Scan

Exclusions

Add/remove files or folders to exclude from scanning:

Fortinet
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

24

This slide shows the configuration of the real-time protection on FortiClient. To enable real-time protection, you must select **Scan files as they are downloaded or copied to my system**. Why?

When you download software from the internet, there is always a chance that you could download applications or programs that will try to inject malware, grayware, or viruses into your system.

You can also enable command and control (C&C) detection using IP reputation database signatures. It checks network traffic against known C&C IP addresses, plus port number combinations.

Block malicious websites blocks all access to malicious websites. You must select **FortiProxy (Disable Only When Troubleshooting)** on the **System Settings** tab before you can enable this option.

You can configure one of the actions for the **Security Risk** site category, which includes block, warn, allow, and monitor. You can also select to view all the subcategories, and configure individual actions (**Block, Warn, Allow, Monitor**) for each subcategory. The security risk category contains the following subcategories:

- Dynamic DNS
- Malicious Websites
- Newly Observed Domain
- Newly Registered Domain
- Phishing
- Spam URLs

DO NOT REPRINT
© FORTINET

Configuring Schedule Scan and Exclusions

- You can schedule scans to occur daily, weekly, or monthly and select from these scan types:

- Quick Scan
- Full Scan
- Custom Scan

Malware Protection > AntiVirus Protection

☒ Scheduled Scan

Schedule Type	Monthly
Scan On	1st
Start At	07:30 PM
Scan Type	Full
Scan Priority	Normal



- You can create an exclusions list and add files and folders that will be excluded from the antivirus scan

Exclusion setting configured on the FortiClient EMS

Exclusions

Paths: One fully qualified path per line. For example, C:\path\to\file.exe, C:\path\to\file.txt, etc.

Paths to Excluded Folders

C:\Documents

Paths to Excluded Files

Scheduled Scan

Schedule Type: Monthly

Scan On: 1

Start (HH:MM): 19:30

Scan Type: Full Scan

☐ Disable Scheduled Scan

Exclusions

Add/remove files or folders to exclude from scanning: Add Remove

C:\Documents\

Configuration pushed to FortiClient

Fortinet NSE Training Institute

© Fortinet Inc. All Rights Reserved.

25

You can configure daily, weekly, and monthly scans as well as selecting one of the scan types on this slide. **Quick Scan** scans only executable files, DLLs, and drivers that are currently running for threats. **Full Scan** performs a full system scan including all files, executable files, DLLs, and drivers for threats, and **Custom Scan** allows you to select a specific file folder on your local hard disk drive (HDD) to scan for threats. All three scan types run the rootkit detection engine to detect and remove rootkits.

By default, FortiClient is scheduled to run full system scans monthly. It is recommended that you run a full system scan on your endpoint, as specified by the default settings. Using the default settings provides the best balance between protecting your endpoint from network threats and supporting the best overall performance. If the default settings do not meet your needs, you can adjust and fine-tune the settings accordingly.

Note that if you configure monthly scans to occur on the 31st of each month, the scan occurs on the first day of the month for those months with fewer than 31 days.

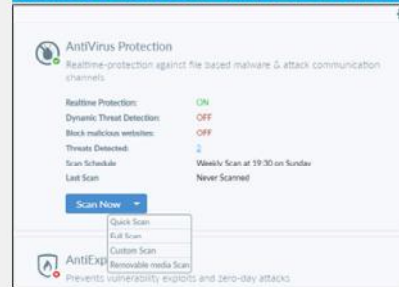
If you want to exclude specific files or folders from the antivirus scan, but still want to perform an antivirus scan on the rest of the system, you can configure an exclusions list. The files and folders that you add to this list are excluded from antivirus scanning.

On-Demand Antivirus Scanning

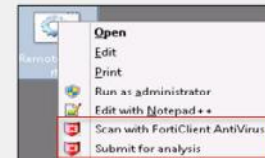
- You can click the **Scan Now** button to view on-demand antivirus scanning. You can select from these scan types:

- Custom Scan
- Full Scan
- Quick Scan
- Removable Media Scan

Malware Protection > AntiVirus Protection



- You can scan a specific file or folder and submit a file for analysis by right-clicking that file on your workstation
 - You can submit up to five files a day to FortiGuard for analysis
 - FortiClient uses the SMTP port to upload files



You can also run an on-demand antivirus scan on the FortiClient Console. There are four types of scans:

- Custom Scan:** runs the rootkit detection engine to detect and remove rootkits. It allows you to select a specific file folder on your local hard disk drive (HDD) to scan for threats.
- Full Scan:** runs the rootkit detection engine to detect and remove rootkits. It then performs a full system scan of all files, executable files, DLLs, and drivers.
- Quick Scan:** runs the rootkit detection engine to detect and remove rootkits. It scans only the following for threats: executable files, DLLs, and drivers that are currently running.
- Removable Media Scan:** runs a full scan on removable media. You cannot schedule scans for removable media.

You can view the date of the last scan run. You can perform a virus scan on a specific file or folder on your workstation by right-clicking the file or folder and selecting **Scan with FortiClient AntiVirus** and **Submit for analysis**. You can submit up to five files per day to FortiGuard for analysis. FortiClient uses SMTP port 25 to upload files. The port must be open on the network firewall. The FortiGuard team does not provide feedback for the files submitted, but creates signatures for the malicious files detected.

Note that the **Submit for Analysis** option is available only when you select an individual file.

View Threats Detected

- The **Threats Detected** link allows you to view:

- Quarantined files
- Site violations
- Real-time protection events

Malware Protection > AntiVirus Protection



- Viewing quarantined files allows you to view details, view logs, or submit the suspicious file to FortiGuard
- When you view site violations, you can view website violations and submit them for recategorization
- The **Realtime Protection** link opens the `realtime_scan.log`

On the FortiClient console, the **Threats Detected** link allows you to view quarantined threats, site violations, and real-time protection events. Each link provides further information about the threat or violation.

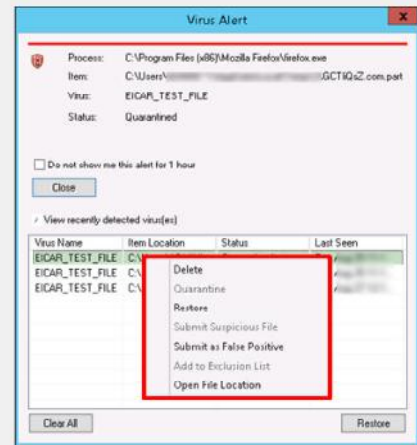
The **Quarantined Files** link allows you to view, submit, or see details of the quarantined file. You can also view the original file location, view the virus name, submit the suspicious file to FortiGuard, and view logs. Only the FortiClient EMS administrator can delete, allowlist, and restore quarantined files.

The **Site Violations** link allows you to view site violations, which are part of FortiClient antivirus, and submit requests to have the site recategorized. It allows you to view site violation details, including the website name, category, date and time, user name, and status.

When an antivirus real-time protection event occurs, it is logged in the `realtime_scan.log` and you can open it in any text editor. By default, real-time protection events open in the default viewer.

Virus Alert

- A warning message opens when a virus is detected while downloading a file through a web browser.
 - Deny access or quarantine the infected file
 - Right-click a file to access the context menu
- File action on quarantined file includes:
 - **Delete**: deletes a quarantined or restored file
 - **Quarantine**: quarantines a restored file
 - **Restore**: restores file and adds to exclusion list
 - **Submit Suspicious File**: submits a file to FortiGuard as a suspicious file
 - **Submit as False Positive**: submits a quarantined file to FortiGuard as a false positive
 - **Add to Exclusion List**: adds a restored file to the exclusion list
 - Any files in the exclusion list are not scanned
 - **Open File Location**: opens the file location on your workstation



If FortiClient detects a virus file that is being downloaded through a web browser, FortiClient presents a warning message if the action on virus discovery is either set to **Deny Access To Infected File** or **Quarantine Infected File**. When the file discovery action is quarantined, you can take one of the actions shown on this slide. FortiClient locks the file on a specified location shown on the file details page until any action is taken. In version 6.2, restore and allowlist is done on FortiClient EMS quarantine management.

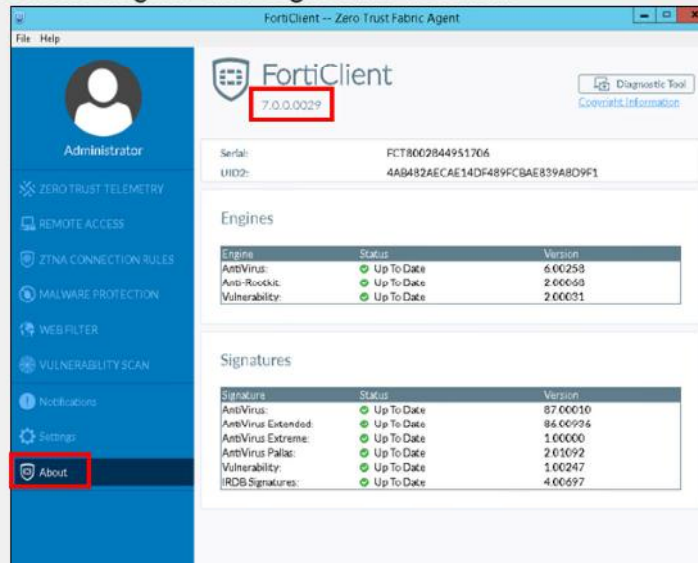
When the action is set to **Deny Access to Infected Files**, a message is displayed stating that users are not permitted to download the file because it is infected.

Note that if you do not select **Alert when viruses are detected**, the virus alert dialog box does not open when you attempt to download a file that contains a virus through a web browser.

DO NOT REPRINT
© FORTINET

FortiClient Engine and Signature Version

- You can view FortiClient engine and signature versions



Fortinet
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

29

You can view the current FortiClient version, engine, and signature information by selecting **About**.

You can use FortiManager for client software and signature updates when registered on FortiGate or FortiClient EMS.

DO NOT REPRINT
© FORTINET

Anti-Ransomware

- Protects specific file, folders, or file types
- Settings include:
 - Protected folder
 - Protected files types
 - Action
 - Bypass valid signer

List of Protect Folders

List of Protect File Types

Malware Protection > Anti-Ransomware

Protected Folders

Path
☒ C:\Users\USERNAME\Documents\
☐ C:\Users\USERNAME\Pictures\
☐ C:\Users\USERNAME\Videos\
☐ C:\Users\USERNAME\Music\
☐ C:\Users\USERNAME\Desktop\
☐ C:\Users\USERNAME\Favorites\

+ Add Folder

Protected File Types

cmd, csv, dll, dmg, docm, docx, dot, dotm, dotx, elf, eml, exe, gz, lqy, iso, jar, jsx

Comma-separated list of extensions (without leading dots). For example, txt, pdf, exe

Action

Terminate ransomware behavior with Anti-R

Bypass Valid Signer

Add Protected Folder

Folder Path

For example, C:\Users\Public\Documents etc.

Add Cancel

Fortinet
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

30

Anti-ransomware protects specific files, folders, or file types on your endpoints from unauthorized changes. The anti-ransomware section includes options for protected folder, file types, and action valid signer.

You can select the desired folders from the existing list, or create a custom directory to protect. Use the **Add Folder** button to add a new folder. FortiClient anti-ransomware protects all content in the selected folders against unauthorized changes.

There is also a list of file types that are protected. You can add additional file types to protect from suspicious activity, separating each file type with a comma. Please note, do not include the leading dot when entering a file type. For example, to include text files, you would enter `txt`, as opposed to `.txt`.

When anti-ransomware detects suspicious activity, it displays a pop-up window asking the user if they want to terminate the process. If the user selects yes, FortiClient terminates the suspicious process. If the user selects no, FortiClient allows the process to continue. However, If the user does not select an option, FortiClient waits for the configured action timeout, then does one of the following, as configured:

- Blocks access and warns the user if suspicious activity is detected: FortiClient terminates the suspicious process.
- Warns the user and resumes after the timeout: FortiClient allows the process to continue.

Bypass Valid Signer enables FortiClient to exclude a process from the selected anti-ransomware action if it has a valid signer.

Anti-Exploit Detection

- Protects vulnerable endpoints from unknown exploit attacks
- FortiClient monitors the behavior of popular applications, such as web browsers
 - Internet Explorer
 - Chrome
 - Firefox
 - Opera
- Protects against memory-based attacks and drive-by download attacks

Malware Protection > AntiExploit

AntiExploit ☒

Settings

Shielded applications: 5

Blocked exploit attempts: 0

Protected Application List

Application	Filename
Microsoft Word	winword.exe
Microsoft Excel	excel.exe
Microsoft PowerPoint	powerpnt.exe
Microsoft Equation Editor	EQNEDT32.exe
Microsoft Outlook	outlook.exe

Applications listed on FortiClient console that are protected

Application Exclusion List

22 Applications

Microsoft help and Support Center

Microsoft PowerPoint

Microsoft Windows Based Script Host

Microsoft Word

Mozilla Firefox

Opera Internet Browser Plugin Wrapper

Opera Internet Browser Plugin Wrapper (32 bit)

Plugin Container for Firefox

Windows Help

1 Excluded Applications

Opera Internet Browser

Application excluded from monitoring

The anti-exploit detection protects vulnerable endpoints from unknown exploit attacks. FortiClient monitors the behavior of popular applications, such as web browsers (Internet Explorer, Chrome, Firefox, Opera), Java/Flash plug-ins, Microsoft Office applications, and PDF readers, to detect exploits that use zero-day or unpatched vulnerabilities to infect the endpoint. Once detected, FortiClient terminates the compromised application process.

The anti-exploit detection feature also protects the endpoint from memory-based attacks and drive-by download attacks. It also detects and blocks unknown and known exploit kits.

This slide shows the list of commonly used application in the anti-exploit section. You can also exclude an application from being monitored by moving it to the **Excluded Applications** box. In this example, the Opera internet browser is excluded.

Anti-exploit is a signature-less solution.

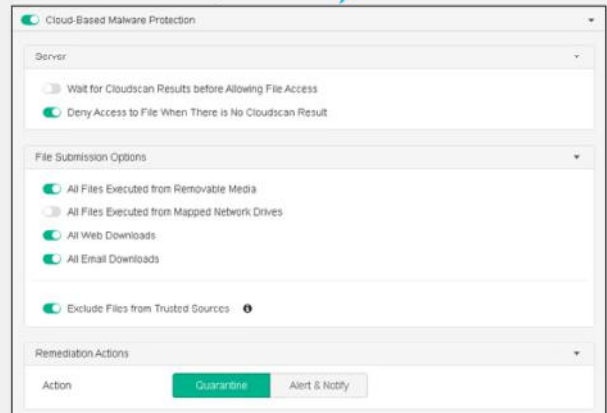
DO NOT REPRINT
© FORTINET

Cloud-Based Malware Protection

- Helps protect endpoints from high-risk file types
- Query FortiGuard to determine if a file is malicious
- Generate a SHA1 checksum for the file
- FortiGuard compares the checksum against the checksum library
- Only submit high risk file types, such as:
 - .exe
 - .doc
 - .pdf
 - .dll

Configuration options on FortiClient EMS

Malware Protection > Cloud Based Malware Protection



Fortinet
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

32

The cloud-based malware protection feature helps protect endpoints from high-risk file types coming from external sources, such as the internet or network drives, by querying FortiGuard to identify whether files are malicious. When a file is downloaded or executed, FortiClient generates a SHA1 checksum for the file. FortiClient sends the checksum to FortiGuard, where it is compared against the FortiGuard checksum library to identify if it is malicious. If the checksum is found in the library, FortiGuard communicates to FortiClient that the file is deemed malware. By default, FortiClient quarantines the file.

This feature submits only high risk file types, such as .exe, .doc, .pdf, and .dll, to FortiGuard. You can enable this feature independently of antivirus protection. By default, the list of high-risk file types is the same as the list of file types submitted to FortiSandbox.

This slide shows the options you can select for cloud-based malware protection:

For **Server** settings, you can either select to wait for cloudscan result and then allow access if the result times out, or deny access to file when there is no result at all. Time out happens if FortiClient EMS cannot reach FortiGuard.

The **File Submission Options** section allows you to select the source from which files need to submit for analysis. The source can be removable media like USB, mapped network drives, web downloads, and email downloads. You can also exclude files from trusted sources by enabling **Exclude Files from Trusted Sources**.

Remediation Actions allows you to select either **Quarantine** or **Alert & Notify** when a malicious file is detected. This action applies when FortiClient quarantines the file, depending on if FortiGuard reports the file as malicious.

DO NOT REPRINT
© FORTINET

Removable Media Access

- FortiClient controls access to removable media devices
 - USB drives
 - External hard drives
- FortiClient can allow, block, or monitor devices

Malware Protection > Removable Media Access

Removable Media Access

Realtime-protection against removable media

Action: Monitor

Status shows on FortiClient console

Create rule for specific device

Default action

Removable Media Access

Show bubble notifications

As Simple: Perform case-insensitive matching against classes, manufacturers, vendor IDs, product IDs, revisions.

Regular Expression: Use Perl Compatible Regular Expressions (PCRE) to perform matching against classes, manufacturers, vendor IDs, product IDs, revisions.

Description	Description			
Class	Any	Manufacturer	Any	
Vendor ID	Any	Product ID	Any	
Revision	Any			

Default removable media access

Fortinet
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

33

Removable Media Access section controls access to removable media devices, such as USB drives or external hard drives. You can also configure rules to allow or block specific removable devices. Rules for specific devices require the class, manufacturer, vendor ID, product ID, and revision information. You can find the desired values for the device in one of the following ways:

- Microsoft Windows Device Manager: select the device and view its properties.
- USBDeview

FortiClient can allow, block, or monitor access to removable media devices based on the rules, as configured by the FortiClient EMS administrator. Access control or action for devices that do not match any configured rules are control by **Default removable media access** settings. In the example on this slide, action **Monitor** is selected as the default action and there is no rule configured for a specific device. With this configuration, FortiClient will log the connections to the endpoint for all the removable devices that connect to it.

Malware Protection—Exclusion

- **Exclusion:**

- Enable exclusion from AV scan
- Supports wildcards and path variables for files and folders to exclude

- Exclusion lists are case-sensitive

- FortiClient EMS support the following wildcards and variables:

- Wildcards:

- Edb*.jrs

Exclude a range of file names with specified extension

- *.jrs

Exclude all files with specified extension

- Path variable:

- %allusersprofile%
- %appdata%
- %localappdata%
- %systemroot%
- %systemdrive%
- %userprofile%
- %windir%

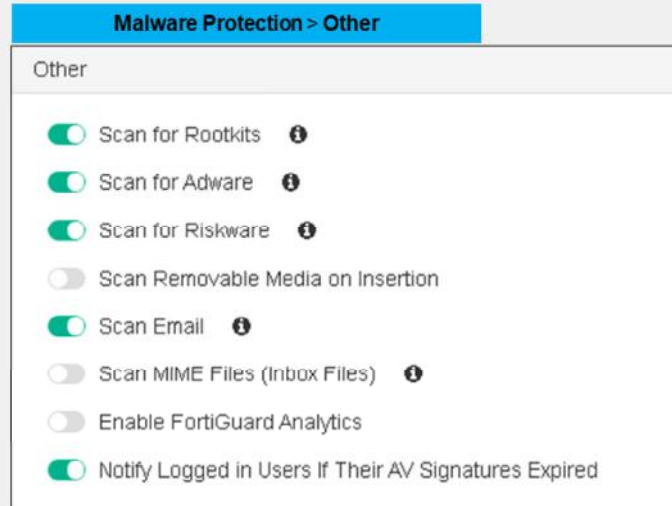
The **Exclusion** option enables exclusions from AV scanning. FortiClient EMS supports using wildcards and path variables to specify files and folders to exclude from scanning. The wildcards and variable FortiClient EMS support are shown on this slide.

Note that combinations of wildcards and variables are not supported. A longer exclusion list affects AV performance. It is recommended to keep the exclusion list as short as possible. Exclusion lists are case-sensitive.

DO NOT REPRINT
© FORTINET

Malware Protection—Others

- Other enables scanning of:
 - Rootkits
 - Adware
 - Riskware
 - Email
 - Removable media on insertion
 - Advanced heuristics signature
 - MIME files(Inbox files)
- Enable FortiGuard Analytics
- Notify user about expire AV signatures



The **Other** section allows you to enable scanning of rootkits, adware, riskware, email, media on insertion, advanced heuristics, and MIME files. It also enables FortiGuard analytics that automatically sends suspicious files to FortiGuard for analysis.

You can also enable notifications for expired AV signatures for logged in FortiClient users.

DO NOT REPRINT
© FORTINET

Sandbox Detection

- FortiClient supports integration with FortiSandbox both on-premises or in the cloud
- FortiClient sends files to FortiSandbox for further analysis if they are not detected locally
- Endpoint users can also manually submit files to FortiSandbox for scanning
- Access to files can be blocked until the FortiSandbox scanning result is returned

Fortinet
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

36

FortiClient supports integration with FortiSandbox both on-premises or in the cloud. When configured, FortiSandbox automatically scans files downloaded on the endpoint, or from removable media attached to the endpoint, or mapped network drives. FortiClient also automatically scans files downloaded with an email client on the endpoints, or from the internet. In each case, if the file is not detected locally, and FortiSandbox integration is configured, FortiClient sends the file to FortiSandbox for further analysis. Endpoint users can also manually submit files to FortiSandbox for scanning. FortiClient periodically downloads the latest AV signatures from FortiSandbox, and applies them locally to all real-time and on-demand AV scanning. FortiClient can send a maximum of 300 files daily to FortiSandbox Cloud. If multiple files are submitted around the same time, FortiClient sends one file to FortiSandbox Cloud, waits until it receives the verdict for that file, then sends the next file to FortiSandbox Cloud. In the case of FortiSandbox, the total number of files sent by FortiClient is limited to hardware specifications.

DO NOT REPRINT
© FORTINET

Sandbox Detection (Contd)

- On the **Sandbox** tab in the endpoint profile, you can enable **Sandbox Detection**
- Options available are:
 - Server
 - File Submission Options
 - Remediation Actions
 - Exceptions
 - Inclusions
 - Other

Fortinet
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

37

You can enable **Sandbox Detection** on the FortiClient EMS. Some options display only if you enable **Advanced**.

When you enable FortiSandbox, the following options are available:

- **Server** allows you to select FortiSandbox in the network, and file access options based on results.
- In the **File Submission Options** section, you can select file resources like removable media, network drives, web downloads, and email downloads.
- **Remediation Actions** allows you to select the **Quarantine** or **Alert & Notify** action for infected files.
- **Exceptions** allows you to exclude files from trusted sources and specific files or folders.
- **Inclusions** allows you to include folders and files for FortiSandbox submission.
- **Other** hides sandbox scan option from Windows context menu.

In addition to configuring the options shown on this slide, you must also configure the connection to FortiClient EMS on FortiSandbox. On FortiSandbox, click **Scan > Devices**, and search for and authorize FortiClient EMS using its serial number. You can find the FortiClient EMS serial number on the **System Information** widget on the Dashboard.

DO NOT REPRINT
© FORTINET

Configuring Sandbox Detection

- You can click the **Settings** icon to view the sandbox configuration on the FortiClient console
 - Submission
 - Access
 - Remediation
 - Exceptions

Sandbox Detection

Sandbox Detection ☒

Settings

IP:

☐ Wait for FortiSandbox results before allowing file access

☐ Deny access to file when there is no sandbox result

FortiSandbox Submission Options

☒ All files executed from mapped network drives

☒ All files executed from removable media

☒ All web downloads

☒ All email downloads (Ex. Outlook)

Remediation Options

☒ Quarantine infected files

☐ Alert & Notify only

Exclusions

☐ Exclude files from trusted sources

☐ Exempt specified files / folders

Inclusions

☐ Include specified files / folders

Fortinet
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

38

You can click the **Settings** icon to view the sandbox configuration on the FortiClient console. These options include:

Wait for FortiSandbox results before allowing file access: Select to wait for FortiSandbox analysis results before files can be accessed.

Deny Access to file when there is no sandbox result: Select to deny access to files when FortiClient cannot reach FortiSandbox for file analysis, or no result.

You can view the following FortiSandbox submission options:

All files executed from mapped network drives: Select to submit all files that are executed on mapped network drives to FortiSandbox for analysis. Clear the checkbox to disable this feature.

All files executed from removable media: Select to submit all files executed on removable media, such as USB drives, to FortiSandbox for analysis. Clear the checkbox to disable this feature.

All web downloads: Select to submit all web downloads on the endpoint to FortiSandbox for analysis.

All email downloads (Ex. Outlook): Select to submit all email downloads on the endpoint to FortiSandbox for analysis.

DO NOT REPRINT
© FORTINET

Configuring Sandbox Detection (Contd)

- You can click the **Settings** icon to view the sandbox configuration on the FortiClient console

- Submission
- Access
- Remediation
- Exceptions

Sandbox Detection

Sandbox Detection ☒

Settings

IP:

☐ Wait for FortiSandbox results before allowing file access

☐ Deny access to file when there is no sandbox result

FortiSandbox Submission Options

☒ All files executed from mapped network drives

☒ All files executed from removable media

☒ All web downloads

☒ All email downloads (Ex. Outlook)

Remediation Options

☒ Quarantine infected files

☐ Alert & Notify only

Exclusions

☐ Exclude files from trusted sources

☐ Exempt specified files / folders

Inclusions

☐ Include specified files / folders

Fortinet
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

39

You can view the following remediation options:

Quarantine infected files: Select to quarantine infected files.

Alert & Notify only: Select to alert and notify the endpoint user about infected files, but not quarantine infected files.

You can view the following exclusion options:

Exclude files from trusted sources: Select to exclude files from trusted sources from FortiSandbox analysis.

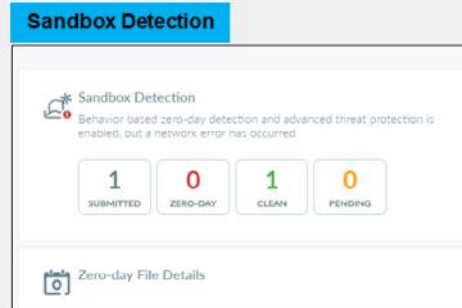
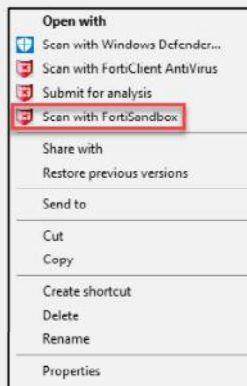
Exempt specified files / folders: Select to exempt specified files and/or folders from FortiSandbox analysis. You must also create the exclusion list.

Note that all the configuration changes are done on the FortiClient EMS endpoint profile. For example, you can also include files with no extension but they must be configured through XML configuration.

DO NOT REPRINT
© FORTINET

On-Demand Scan and Viewing Results

- Scanning with FortiSandbox on demand
- Viewing FortiSandbox scan results



You can send files to FortiSandbox for scanning on demand when FortiSandbox is enabled and online.

FortiSandbox scan results display on the **Malware Protection** page. When a virus is detected, FortiClient creates a notification alert that displays the number of files. Access to files can be blocked until the FortiSandbox scanning result is returned. When scanning is complete, FortiSandbox can quarantine infected files, or alert and notify the endpoint user of infected files without quarantining the files.

The **SUBMITTED** box shows the number of files submitted to FortiSandbox for scanning. The **ZERO-DAY** box shows the number of detected zero-day files. The **CLEAN** box shows the number of files identified as clean after FortiSandbox scanning, and the **PENDING** box shows the number of files waiting for FortiSandbox scanning.

**DO NOT REPRINT
© FORTINET**

View, Submit, Restore, and Delete Quarantined Files

- Endpoint user can view files quarantined by FortiSandbox
- Endpoint user can also see details of quarantined files and submit them for another analysis

Malware Protection > Sandbox Quarantined Files

Quarantined Files

Filename	Date Quarantined
4f352679-7f20-4ae5-a54e-481a656076a0.tmp	2018/11/14 12:03:36
90CF8C63A855C3864064CE36EB492D9C7...	2018/11/14 16:05:40
bymP5I2.com.ppt	2018/11/14 16:05:40

Send file ...

Infected file:

C:\Program Files\Fortinet\FortiClient\quarantine\QuarantFile43a31d8_2172

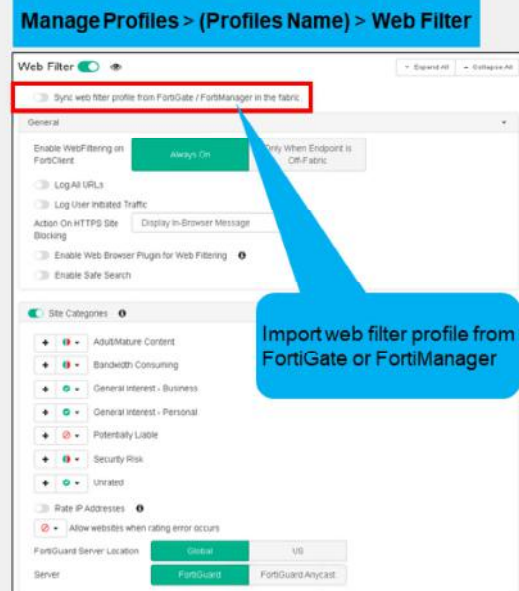
You can view files quarantined by FortiSandbox. Endpoint users can submit files to FortiSandbox only for scanning and checking details of quarantined files.

The maximum age for quarantined files is specified in the `<quarantine></quarantine>` XML tags.

FortiClient sends quarantined file information to FortiClient EMS. If the FortiClient EMS administrator allowlists the file (in the case of a false positive), FortiClient EMS sends the allowlist information to FortiClient. After FortiClient receives the allowlist information, it releases the file from quarantine.

Web Filter

- You must enable FortiProxy to use web filter options
- Web Filter:**
 - Enables web filtering for on and/or off-fabric client
 - You can select site categories from FortiGuard
 - You can select actions for entire site categories and subcategories
 - Rate IP address
 - FortiClient requests site rating by URL and IP separately
 - Provides additional security against attempts to by FortiGuard
 - Configure action to take when FortiGuard is unavailable
 - Exclusion List
 - You can configure actions for specific URLs and URL types
 - It bypasses action configured for site categories



The **Web Filter** tab enables web filtering options. For Windows, macOS, and Linux profiles, you must enable **FortiProxy (Disable Only When Troubleshooting)** on the **System Settings** tab to use the **Web Filter**.

General settings include **Enable WebFiltering on FortiClient** that allows FortiClient to perform web filtering even when it is on-net with FortiGate in the network also configured with a web filter profile. This option is available only for Windows and macOS profiles. This setting affects the **Block Access to Malicious Websites** setting in AntiVirus protection.

Log All URLs enables logging for all URLs access by endpoint user. You can also enable **Log User Initiated Traffic** to include user information in web filtering logs.

Show Bubble Notification When HTTPS Site Is Blocked enables the showing of a bubble notification when a HTTPS site is blocked. Select **Enable Web Browser Plugin for HTTPS Web Filtering** to improve detection and enforcement of web filter rules on HTTPS sites.

You can also enable the safe search option for search engines like Google search or YouTube.

Site Categories enables site categories from FortiGuard. When site categories are disabled, FortiClient is protected by the exclusion list. For all categories below, you can configure an action for the entire site category by selecting either **Block**, **Warn**, **Allow**, or **Monitor**. Each site category is shown on this slide.

You can also import a web filter profile from FortiOS or FortiManager into FortiClient EMS, then synchronize the web filter profile settings to an endpoint profile on FortiClient EMS.

DO NOT REPRINT
© FORTINET

Web Filter (Contd)

- Filter URL and resolve IP address at the same time
- Create an exclusion list with actions:
 - Allow
 - Block
 - Monitor
- FortiClient is protected by the exclusion list when no site categories are enabled

Manage Profiles > (Profiles Name) > Web Filter

Rate IP Addresses ⓘ

⌵ Allow websites when rating error occurs

Exclusion List ⓘ

Aa Simple: Perform a case-insensitive matching against URLs.

?* Wildcard: ? matches any character once. For example, the pattern 123??? will match 123a or 123abc, but not 123abcdef. * matches zero or more characters.

.* Regular Expression: Use Perl Compatible Regular Expressions (PCRE) to perform matching against URLs.

⌵	www.facebook.*	.*	🗑️ + ⬆️ ⬇️
----------------	----------------	----	--

Fortinet NSE Training Institute

© Fortinet Inc. All Rights Reserved.

43

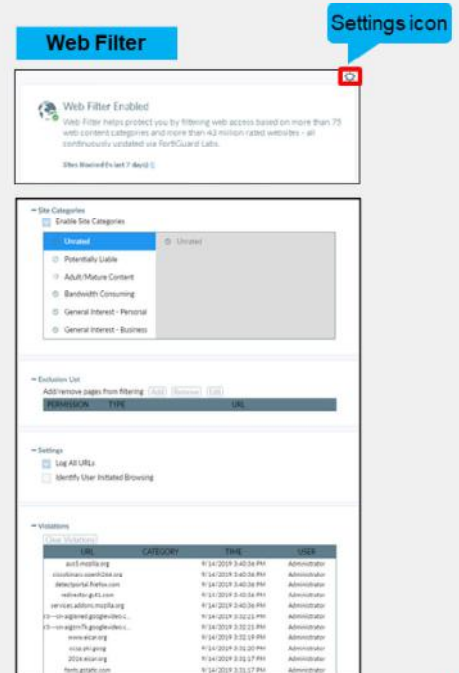
In **Rate IP Addresses**, you can filter URLs and resolved IP addresses at the same time and select the action for rating errors.

Note that if you enable the **Allow websites when rating error occurs** option, FortiClient will block all URLs, including the captive portal authentication page. This will prevent users from getting access to the authentication page.

The **Exclusion List** option allows you to select an action, and enter specific URLs and their type, such as simple, wildcard, or regular expression.

Web Filter—Settings and Violations

- You can click the settings icon to see the current configuration
 - Site categories
 - Exclusion list
 - Settings
 - Violations: view and clear
- Exclusion List** tab
 - Allows you to add URLs that are overridden from the FDN category
 - Three types to choose: Simple, Wildcard, Regular Expression
 - Three actions to choose: Block, Allow, Monitor
- Settings** allows you to view the following:
 - Log all URLs
 - Identify User Initiated Browsing
- Violations**
 - Allows you to view web filter violations



The endpoint user can view the current configuration by clicking the settings icon on FortiClient console. The FortiClient EMS administrator can configure a web security profile to **Allow**, **Block**, **Warn**, or **Monitor** web traffic based on website categories and subcategories.

What if you want to exempt a URL that is part of a category, but you still want to take action on that category as a whole?

The FortiClient EMS administrator can configure an exclusion list to which the administrator can add websites and set the permissions to allow, block, and monitor. An administrator can also configure simple, wildcard, or regular expressions as a type. If the website is part of a blocked category, an allow or monitor permission in the exclusion lists allows the user to access the specific URL. Note that when site categories are disabled, FortiClient is protected by the exclusion list only.

When you configure web filter general settings, you can choose to log all URLs with an assigned action, and the logged files can be downloaded. You can also select to log only user-initiated browsing.

You can view site violations and violation details, including the website name, category, date and time, and username. The violation shows only if the action is set to **block** or **warn** for FortiGuard site categories, and **block** for the exclusion list.

DO NOT REPRINT
© FORTINET

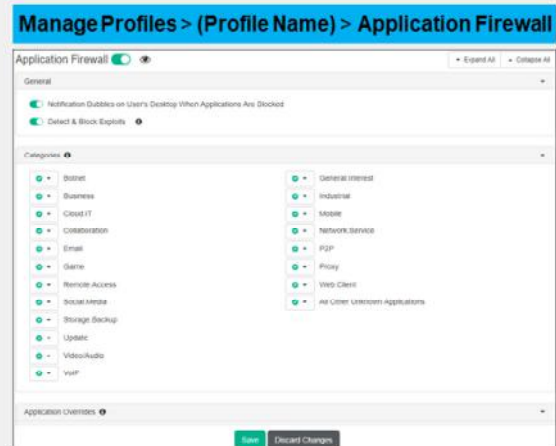
Application Firewall

- Enable **Application Firewall** to enforce application control on endpoints
 - Enables notification when applications are blocked
 - Inspects network traffic for intrusions
 - Enables FortiClient firewall to allow, block, or monitor applications
 - Uses signatures to identify applications
 - Applications are divided into categories
 - Actions you can take:
 - Block
 - Allow
 - Monitor

Application Overrides		
Application Signature	Category	Action
☐ Adobe Creative Cloud	Storage Backup	☐ Block
Remove Signatures Add Signatures		

Signature doesn't
require deep inspection

Requires Deep Inspection



Fortinet
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

45

Application Firewall tab enables or disables application control.

In the **General** section, you can enable bubble notifications for blocked applications. You can also enable the inspection of network traffic for intrusions attempting to exploit known vulnerabilities.

In the **Categories** section, you can select the following actions on the categories shown in this slide image:

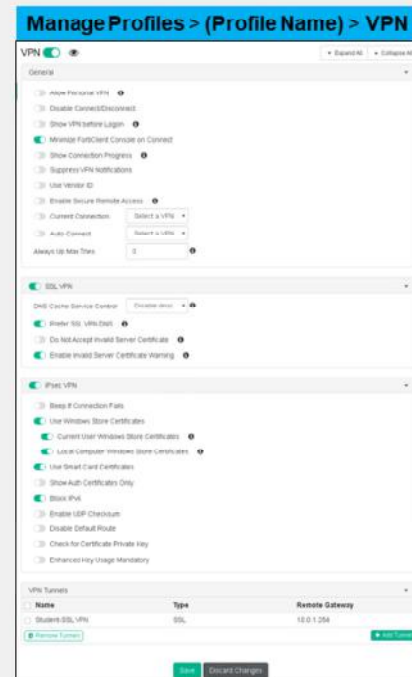
- Block
- Allow
- Monitor

The **Application Overrides** option allows the FortiClient firewall to allow, block, or monitor applications based on their signatures. You can delete an application and add a signature to an application. Note that FortiClient does not include SSL deep inspection. FortiClient cannot apply signatures marked as **Require Deep Inspection**, do not use these signatures in a profile.

DO NOT REPRINT
© FORTINET

VPN

- Enables VPN provisioning
- Supports IPsec and SSL VPN
- Allows you to add VPN tunnels
- Disable option to connect/disconnect
- You can enable SSL VPN DNS cache server control
- IPsec can use Windows Store Certificates
- Configure basic and advanced VPN settings



Fortinet NSE Training Institute

© Fortinet Inc. All Rights Reserved.

46

The **VPN** tab, enable or disable VPN use on endpoints. There are general and specific VPN type settings available to configure.

The **General** section allows you to enable or disable various VPN-related settings. You can also select a maximum number of attempts. These options are applied to both SSL and IPsec VPN.

SSL VPN includes the **DNS Cache Service Control** setting. You can select to disable, leave unchanged, or restart the DNS cache control service. You can also override the DNS server to SSL VPN DNS IP.

You can also enable or disable different IPsec VPN options that are shown on this slide.

VPN (Contd)

- VPN tunnels
 - You can add IPsec or SSL VPN profiles
 - There are basic and advanced settings
- SSL VPN
 - You can add multiple remote gateway IPs
 - Default access port is 443
 - Select certificate for additional security
 - On-connect script and on-disconnect script
- IPsec VPN
 - You can add multiple remote gateway IPs
 - Authentication method
 - VPN settings
 - Phase1 and 2 settings
 - On connect and on disconnect script

VPN > +Add Tunnel > SSL VPN

VPN > +Add Tunnel > IPsec VPN

You can add VPN profiles for both SSL and IPsec.

The SSL VPN settings include remote gateway IP, SSL port number, and options to request the certificate and prompt for the user name. There is also an option to enter connect and disconnect scripts. This option must also be enabled on FortiGate.

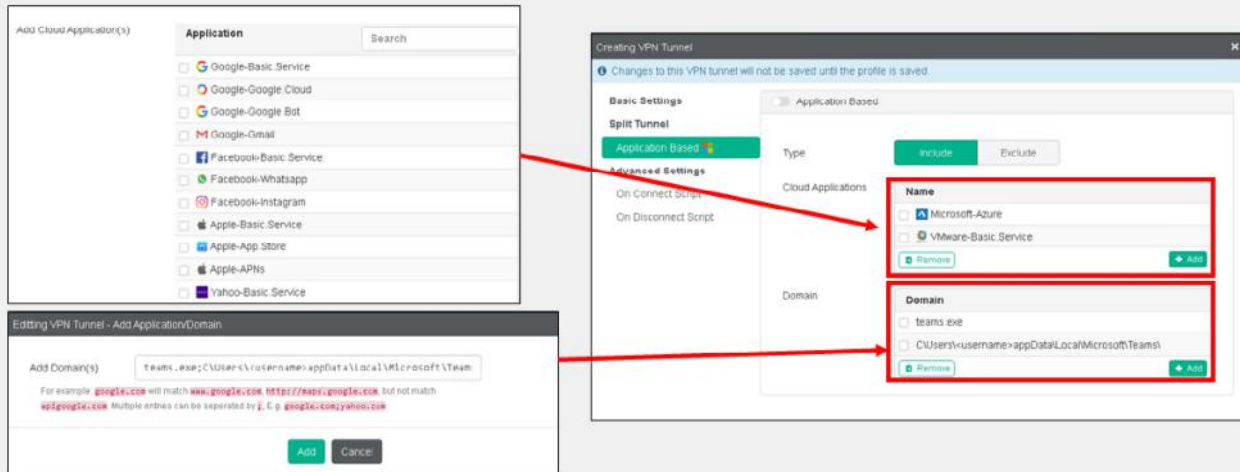
The IPsec VPN settings includes remote gateway IP, authentication method, pre-shared key (if **Pre-Shared Key** is selected for **Authentication Method**), and prompt username. You can select the IPsec mode (**Main** or **Aggressive**), and options such as **Mode Config**, **Manual Set**, **DHCP over IPsec**, **DNS server**, and so on in the **VPN Settings** pane.

You can also configure phase 1 and phase 2 settings. You can select the encryption and authentication algorithms used to generate keys for protecting negotiations and add encryption and authentication algorithms as required, and algorithms that will be proposed to the remote VPN peer. You need to select a minimum of one and a maximum of two combinations. The remote peer or client must be configured to use at least one of the proposals that you define.

DO NOT REPRINT
© FORTINET

VPN—Application-Based Split Tunnel

- FortiClient supports source application-based split tunnel
- You can specify which application traffic to exclude from the VPN tunnel
- This is supported on Windows endpoints only



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

48

FortiClient (Windows) supports source application-based split tunnel, where you can specify which application traffic to exclude from the VPN tunnel. You can exclude high bandwidth-consuming applications.

For example, you can exclude applications like Microsoft Office 365, Microsoft Teams, Skype, GoToMeeting, Zoom, and so on.

You must configure these settings in the endpoint profile in EMS. This feature does not support explicitly including traffic in the VPN tunnel.

The example shown on this slide shows that the application Microsoft Teams is specified by its name, full path, or directory where it is installed. Multiple entries can be separated by a semi-colon (;).

DO NOT REPRINT
© FORTINET

Remote Access—IPsec VPN

- Easy configuration to create, edit, or delete VPN connections
 - Authentication settings – prompt on login, save login (only username), or disable
 - Allows you to configure VPN settings, phase 1 settings, and phase 2 settings
- Configure many advanced configurations when managed by FortiGate or FortiClient FortiClient EMS
 - Redundant IPsec VPN connections
 - Save password
 - Auto connect
 - Always up

Remote Access > IPsec VPN

Edit VPN Connection

VPN: SSL-VPN **IPsec VPN**

Connection Name:

Description:

Remote Gateway: ✖

[Add Remote Gateway](#)

Authentication Method: Pre-shared key

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

[Advanced Settings](#)

You can also configure IPsec VPN directly on the FortiClient console when the FortiClient EMS administrator allows you to add personal VPN connections. This allows you to create, edit, save, or delete IPsec VPN connections. You can create and save multiple IPsec connections. Because this configuration is one side of IPsec VPN, the configuration settings must match the FortiGate IPsec configuration in order to connect and access remote resources.

When a personal VPN is not allowed by the FortiClient EMS administrator, the endpoint profile VPN tab allows you to provision these configurations, along with advanced configurations, such as redundant IPsec VPN connections, save password, auto connect, and always up, to name a few.

DO NOT REPRINT
© FORTINET

Remote Access—SSL VPN

- Create, edit, or delete a VPN connection
 - Save the login information – username
 - Configure authentication – prompt on login, save login (only username), or disable (only when **Client Certificate** option is enabled)
- When managed by FortiClient EMS, perform advanced configuration:
 - Priority-based SSL VPN connections
 - SSL VPN portal on FortiGate allows:
 - Save password
 - Auto connect
 - Always up
- Supports DTLS
 - If required, falls back to TCP over TLS
 - Windows only

Remote Access > IPsec VPN

Edit VPN Connection

VPN: SSL VPN IPsec VPN

Connection Name:

Description:

Remote Gateway: ✕

+ Add Remote Gateway

☒ Customize port:

Client Certificate: None ▼

Authentication: ☒ Prompt on login ☐ Save login

☐ Do not Warn Invalid Server Certificate

Fortinet
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

50

The SSL VPN configuration is similar to the IPsec configuration, where you configure one side of the tunnel and the other side is configured on FortiGate.

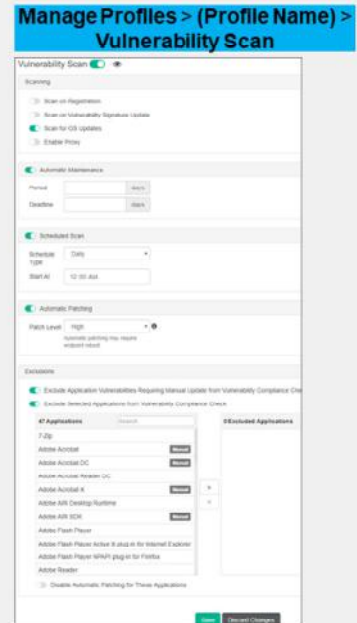
When personal VPN is not allowed by the FortiClient EMS administrator, the endpoint profile VPN tab allows you to provision these configurations, along with advanced configurations on SSL VPN portals, and many more.

DTLS is a Windows-only feature and is not recommended for slower networks. DTLS settings must also be enabled on FortiGate SSL VPN settings.

DO NOT REPRINT
© FORTINET

Vulnerability Scan

- The **Vulnerability Scan** tab enables scanning on endpoints
 - Scanning on connecting to FortiGate
 - Scan for OS and vulnerability signature updates
 - Configure automatic maintenance
 - Configure scheduled scans
 - Configure automatic patching
 - Create exclusion list



Fortinet
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

51

You can select vulnerability scan for endpoints after connecting to FortiGate, when updating a vulnerability signature, and for OS updates.

You can also select the **Enable Proxy** setting to enable proxy.

The **Automatic Maintenance** setting allows you to configure the vulnerability scan to run as part of Windows automatic maintenance. Adding FortiClient vulnerability scans to the Windows automatic maintenance queue allows the system to choose an appropriate time for the scan.

You can also schedule scans. In the **Schedule Type** drop-down list, you can select **Daily**, **Weekly**, or **Monthly**. In the **Scan On** field, you can configure the day the scan will run. This setting applies if the schedule is set to **Monthly**. You can also specify the time the scan will start.

Automatic Patching allows patches to be installed automatically when vulnerabilities are detected. You can select patch severity level such as **Critical**, **High**, **Medium**, **Low** or **All**.

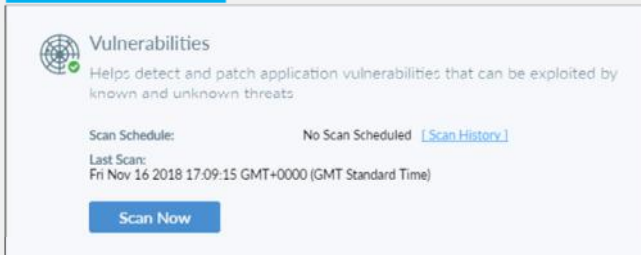
The **Exclusions** section contains options that allow you to exclude applications. The options are shown in the image on this slide. These options do not exclude applications from vulnerability scanning. When the **Disable Automatic Patching for These Applications** button is enabled in exclusion, it disables automatic patching for the applications excluded from the vulnerability compliance check.

DO NOT REPRINT
© FORTINET

Vulnerability Scan (Contd)

- Scan on demand
 - You can scan on demand.
 - FortiClient displays a summary of vulnerabilities found on the endpoint
 - If any detected vulnerabilities require you to manually install remediation patches, the list of affected software is also displayed

Vulnerability Scan



If compliance is enabled for FortiClient, and FortiClient EMS compliance rules require it, all automatic and manual software patches must be installed within a time frame that maintains compliant status and network access. The default time frame is one day.

However, the FortiGate administrator may choose a different time frame. Contact your system administrator to learn how long you have to fix vulnerabilities.

Vulnerability Scan (Contd)

- Automatically fix detected vulnerabilities
 - You can automatically install software patches by clicking **Fix Now**, or review detected vulnerabilities before installing software patches



3rd Party App (7)

APPLICATIONS	SEVERITY	RECOMMENDED ACTION
Adobe Reader X 10.0.0.395 (1)	Critical	Manual Install
Wireshark 2.4.2.0 (1)	Critical	Manual Install
Java JRE 8.0.910.54 (132)	Critical	Auto Patch
Java JRE 8.0.910.12 (115)	Critical	Auto Patch
NotepadPlusPlus 6.9.1.0 (1)	High	Manual Install
PutTY release 0.70 (64-bit) 0.70.0.0 (1)	Medium	Manual Install
VMware Tools 10.0.8.3746311 (1)	Low	Manual Install

- Review detected vulnerabilities before fixing them
- Manually fixing detected vulnerabilities
 - In some cases, FortiClient cannot automatically install software patches, and you must manually download and install software patches
- Viewing vulnerability scan history

Scan History

Vulnerability Patch History

Time	Applications	Status
08/18/2021 9:04:49 AM (11)	Adobe Reader X 10.0.0.395 (1)	Unpatched
	Firefox 89.0.2.7843 (1)	Patched
	Internet Explorer 11.0.31 (1)	Unpatched
	Java JRE 8.0.910.12 (115)	Unpatched
	Java JRE 8.0.910.14 (132)	Unpatched
	NotepadPlusPlus 6.9.1.0 (1)	Unpatched
	Operating System (5)	Unpatched
	PutTY release 0.70 (64-bit) 0.70.0.0 (1)	Unpatched
	VMware Tools 10.0.8.3746311 (1)	Unpatched
	Windows Server 2012 (59)	Unpatched
	Wireshark 2.4.2.0 (1)	Unpatched
07/23/2021 3:42:18 AM (11)	Adobe Reader X 10.0.0.395 (1)	Unpatched
	Firefox 89.0.2.7843 (1)	Unpatched
	Internet Explorer 11.0.31 (1)	Unpatched
	Java JRE 8.0.910.12 (115)	Unpatched
	Java JRE 8.0.910.14 (132)	Unpatched
	NotepadPlusPlus 6.9.1.0 (1)	Unpatched
	Operating System (5)	Unpatched
	PutTY release 0.70 (64-bit) 0.70.0.0 (1)	Unpatched
	VMware Tools 10.0.8.3746311 (1)	Unpatched
	Windows Server 2012 (59)	Unpatched
	Wireshark 2.4.2.0 (1)	Unpatched

Vulnerability scan identifies vulnerabilities on the endpoint that should be fixed by installing software patches. You can automatically install software patches by clicking **Fix Now**, or you can review detected vulnerabilities before installing software patches. Any software patches that cannot be automatically installed are also listed. You should manually download and install software patches for the vulnerable software.

FortiClient updates vulnerability scan signatures at specific intervals or daily. For intervals, you must select the value in hours. The minimum is 1 and the maximum is 24. For daily, you must select a specific time of the day. FortiClient does not support push updates.

When the scan is complete, FortiClient displays a summary of vulnerabilities found on the endpoint. If any detected vulnerabilities require you to manually install remediation patches, the list of affected software is also displayed.

You can view the history of the last seven vulnerability scans and patches. You can view the history to see what software was identified as vulnerable and whether patches for the vulnerabilities were installed.

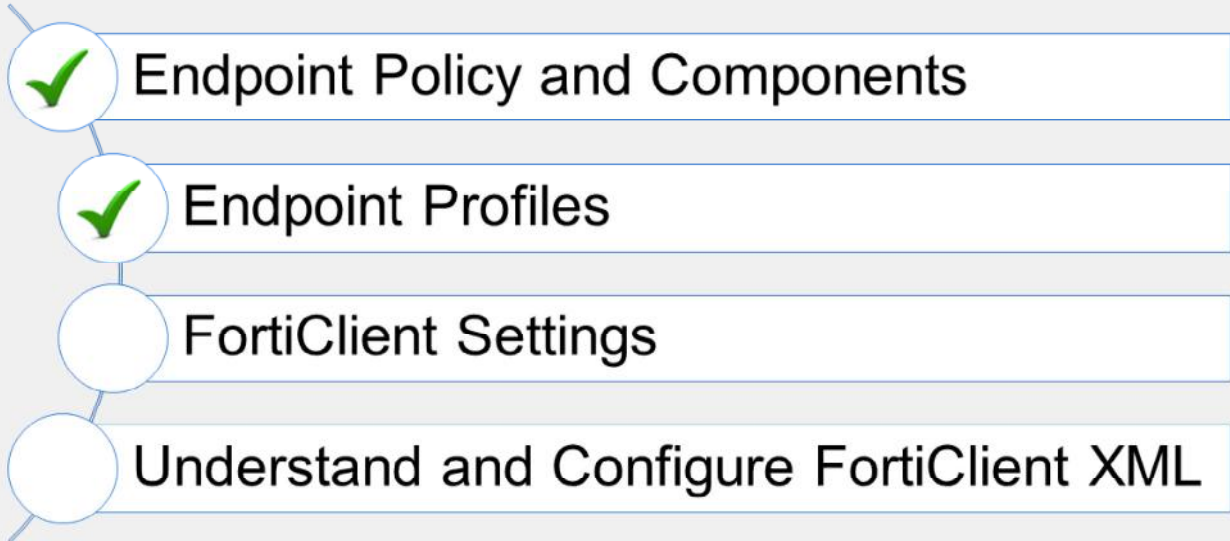
DO NOT REPRINT
© FORTINET

Knowledge Check

1. What is the default log level configured on FortiClient?
☐ A. Critical
☒ B. Information
2. Which components does FortiClient single sign-on mobility require?
☒ A. FortiAuthenticator
☐ B. FortiClient EMS
3. Which of these features uses FortiProxy?
☐ A. Application firewall
☒ B. Web filter

DO NOT REPRINT
© FORTINET

Lesson Progress



Good job! You now understand FortiClient endpoint profiles

Now, you will learn how to configure FortiClient settings.

DO NOT REPRINT
© FORTINET

The slide is titled "FortiClient Settings" in a large, bold, black font. Below the title, the word "Objectives" is written in a bold, black font. Under "Objectives", there is a single bullet point: "• Configure FortiClient settings". The slide has a light gray background with a white rectangular area containing the text. In the bottom left corner, there is a logo for "NSE Training Institute" with the FortiNet logo above it. In the bottom right corner, the number "56" is displayed in red. The slide is decorated with several gray and red geometric shapes, including a large gray rectangle on the right side and a red shape in the top right corner.

FortiClient Settings

Objectives

- Configure FortiClient settings

FORTINET
NSE Training Institute

56

After completing this section, you should be able to achieve the objective shown on this slide.

By demonstrating competence in configuring FortiClient settings, you will be able to configure different FortiClient settings to suit your requirements.

System Settings

- Use the options in the **System Settings** tab to define the appearance of the user interface

- UI**

- Dashboard banner
 - Lock password
 - Backing up FortiClient configuration
 - Hide system tray
 - Show Zero Trust Tag on FortiClient GUI
 - Language

- Log**

- Select log level
 - Select feature for which logs will be generated
 - Select logs upload to FortiAnalyzer/FortiManager

- Proxy**

- Use proxy server for FortiGuard updates and virus submission

Manage Profiles > (Profile Name) > System Settings

The screenshot shows the 'System Settings' window for a specific profile. It is divided into three main sections: UI, Log, and Proxy. The UI section has several toggle switches for user interface elements. The Log section has a 'Level' dropdown menu and a 'Features' list where various logging features can be enabled or disabled. The Proxy section has two toggle switches for using a proxy for updates and virus submission.

The majority of these configuration options are available only for Windows, macOS, and Linux profiles. Options such as **Upload Logs to FortiAnalyzer/FortiManager** are available for all endpoints. Some options are available only when you enable the **Advanced** view.

The **UI** section specifies how the FortiClient user interface appears when installed on endpoints.

The **Log** section specifies log settings such as **Level** and **Features** for which logs will generate. There are different log levels available for FortiClient. They include **Info**, **Emergency**, **Alert**, **Critical**, **Notice**, **Debug**, and so on.

You can also select **Client-Based Logging When On-Net**, this includes local log messages when client is on-net, and **Upload Logs to FortiAnalyzer/FortiManager**. This will require the IP address of the FortiAnalyzer or FortiManager and other settings such as upload schedule, log generation timeout, and log retention policy in days. You can also select to upload event logs from FortiClient endpoints.

The **Proxy** section allows you to enable access to FortiGuard servers and submit viruses to FortiGuard using the configured proxy. You can select proxy type, IP, port, username, and password.

System Settings (Contd)

- **Update**
 - Specify whether FortiManager or Micro-FortiGuard server updates FCT
 - Enables FortiClient software update
 - Select update action, scheduling, and server location and type
- **FortiProxy**
 - You must enable **FortiProxy** to use the web filter options as well as some antivirus options
 - Enables **HTTPS Proxy** to inspect https traffic
 - Email server and client comforting
- **Endpoint Control**
 - Specify settings for endpoints
 - You can enable
 - **Show Bubble Notifications**
 - **Silent registration**
 - **On-Net Subnets**

In the **Update** section, you can specify whether FortiManager is used for FortiClient updates. You can also select FortiClient software updates, the update schedule, FortiGuard server location and type, and anycast.

You must enable FortiProxy to use the web filter options as well as some antivirus options. You can enable **HTTPS Proxy**. If disabled, FortiProxy no longer inspects HTTPS traffic. It also enables other useful options that are shown on this slide.

The **Endpoint Control** section specifies the settings for the endpoint. You can refer to this slide for all the options available. For example, an administrator can enable **Disable Disconnect** to disallow users from disconnecting the FortiClient telemetry connection to FortiClient EMS.

System Settings (Contd)

- **User Identity Settings**
 - Enables users to specify their identity in FortiClient
 - Manually entering their details
 - Logging in to their social media account
- **ZTNA Settings**
 - Enables ZTNA connection feature on FortiClient GUI
- **Other**
 - Enable to select and install a CA certificate on endpoints
 - Select to enable single sign-on (SSO) mobility agent
- **iOS**
 - Enable and browse for `.mobileconfig` file to distribute the configuration profile
- **Privacy**
 - Send usage statistics to Fortinet to improve product
- **XML Configuration**
 - Use XML editor to configure FortiClient settings

Manage Profiles > (Profile Name) > System Settings

The options in the **user identity settings** sections enables users to specify their identity in FortiClient using the following methods:

- Manually entering their details in FortiClient
- Logging in to a social media account, such as LinkedIn, Google, or Salesforce.

By default, FortiClient EMS obtains user details from the endpoint OS. If the user provides their details using one of the methods listed above, FortiClient EMS obtains the user-specified details instead. If this option is disabled, FortiClient EMS obtains and displays user details from the endpoint OS.

The **Zero Trust Network Access (ZTNA) Settings** section enables the ZTNA connection rules feature on FortiClient. This feature on FortiClient is required to manually add rules for ZTNA TCP forwarding access proxy connections.

The options in the **Other** section enable CA certificate installation on the client. You can add certificates on the **Manage CA Certificates** pane. It also enables the SSO mobility agent for FortiAuthenticator. To use this feature, you need to apply a FortiClient SSO mobility agent license to your FortiAuthenticator device. The default port is set to 8001. The FortiAuthenticator listens on a configurable TCP port. FortiClient connects to FortiAuthenticator using TLS/SSL with two-way certificate authentication. FortiClient sends a login packet to FortiAuthenticator, which replies with an acknowledgement packet. FortiClient to FortiAuthenticator communication requires the following:

1. The IP address must be unique in the entire network.
2. FortiAuthenticator must be accessible from clients in all locations.
3. FortiAuthenticator must be accessible by all FortiGate devices.

The option in the **iOS** section allows you to upload `.mobileconfig` file to distribute the configuration profile.

DO NOT REPRINT
© FORTINET

Settings—System

- The settings in the **System** window allow you to back up the FortiClient configuration

Settings > System

System

Restore a configuration

Backup Restore

Settings > System

System

Restore a configuration

File

C:\Users\Administrator\Desktop

☒ Include user settings

Password

Required

Re-enter Password

OK Cancel

Sample partial backup

```
<?xml version="1.0" encoding="UTF-8" ?>
<forticlient_configuration>
  <forticlient_version>6.0.3</forticlient_version>
  <version>6.0.3</version>
  <exported_by_version>6.0.3</exported_by_version>
  <date>2016-08-18 10:10:10</date>
  <partial_configuration>0</partial_configuration>
  <os_version>windows</os_version>
  <os_architecture>x64</os_architecture>
  <system>
    <ui>
      <disable_backup>0</disable_backup>
      <ads>1</ads>
    </ui>
  </system>
</forticlient_configuration>
```

There are additional settings available on the FortiClient system settings GUI, which include:

Backup: to back up the FortiClient configuration.

Restore: to restore the FortiClient configuration. Note that restore button is always grayed out because FortiClient is managed by FortiClient EMS.

Note that the FortiClient configuration file is an XML format configuration file. When performing a backup, you can select the file destination and save the file in an unencrypted (.conf) or encrypted format (.sconf). You can include or exclude comments in the XML configuration file.

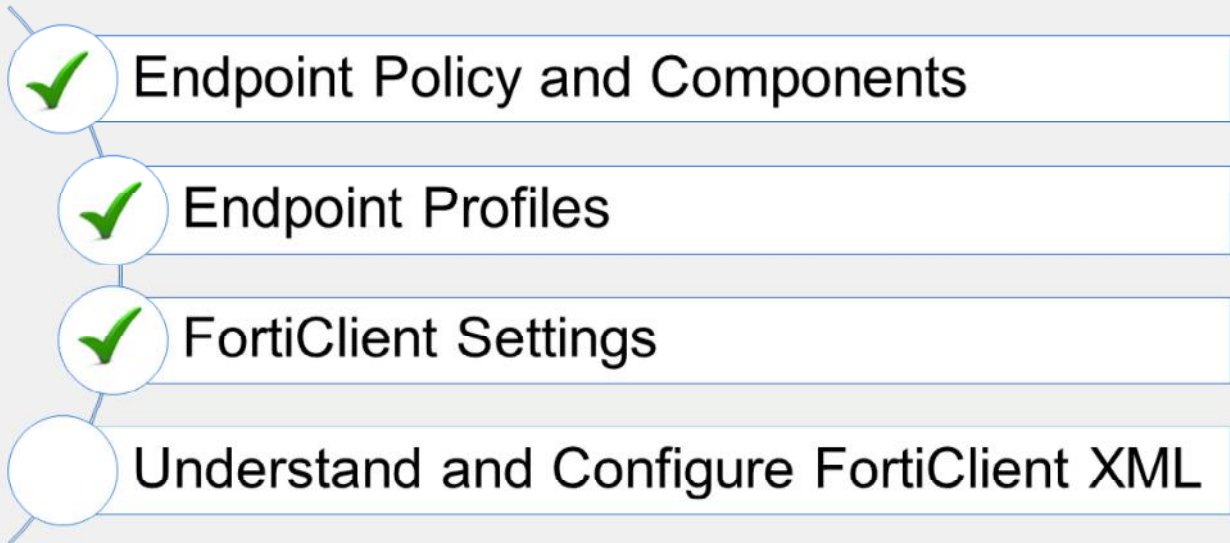
DO NOT REPRINT
© FORTINET

Knowledge Check

1. Which FortiClient setting does an administrator use to disallow users to disconnect a telemetry connection?
✓ A. Endpoint Control
B. UI
2. Which social media service can a user use to specify their identity?
A. Twitter
✓ B. LinkedIn

DO NOT REPRINT
© FORTINET

Lesson Progress



Fortinet
NSE Training Institute

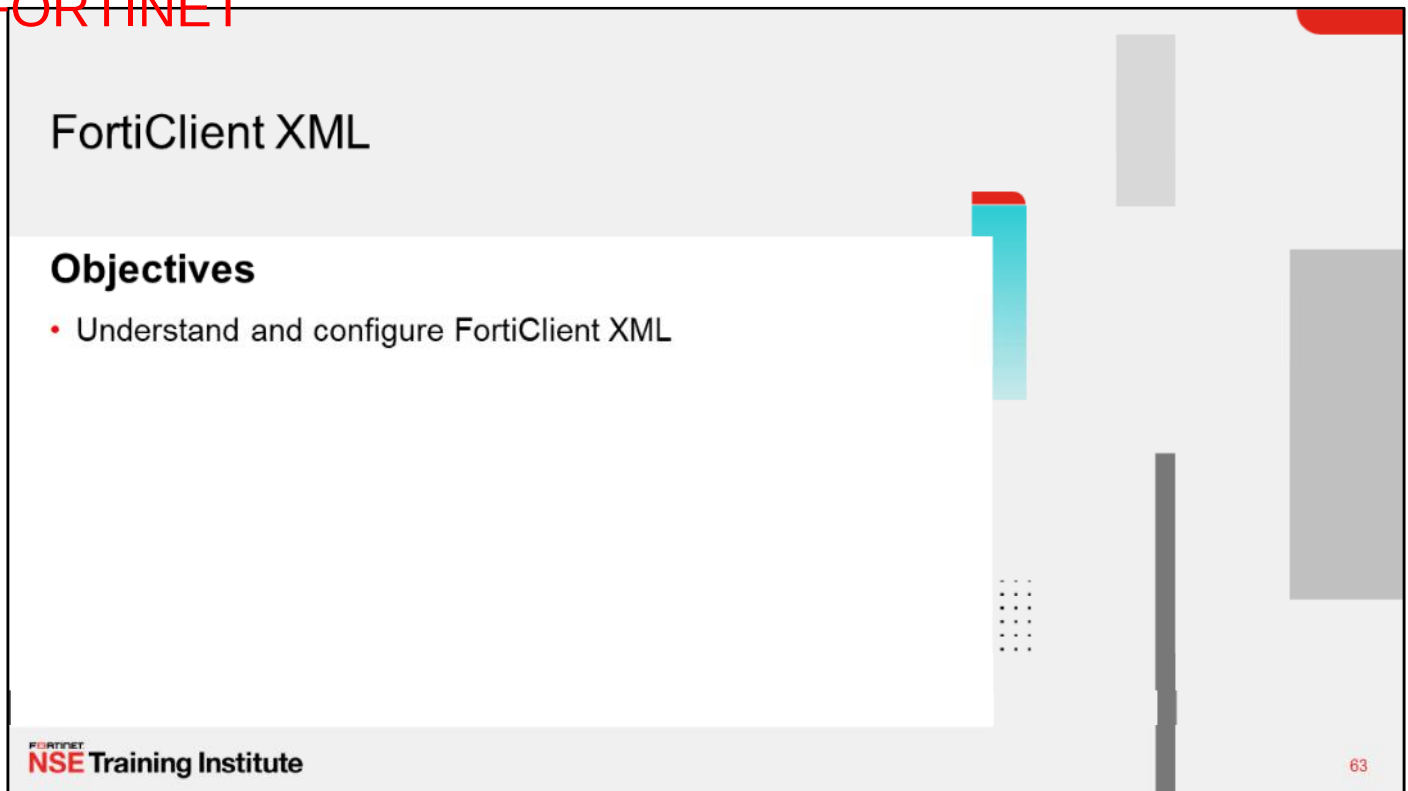
© Fortinet Inc. All Rights Reserved.

62

Good job! You now understand FortiClient settings

Now, you will learn how to configure FortiClient XML.

DO NOT REPRINT
© FORTINET



FortiClient XML

Objectives

- Understand and configure FortiClient XML

FORTINET
NSE Training Institute

63

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in configuring FortiClient XML, you will be able to configure FortiClient configuration in the XML editor.

DO NOT REPRINT
© FORTINET

FortiClient XML Configuration

- Extensible Markup Language (XML)
 - Set of rules in a format for encoding documents
 - Both human-readable and machine-readable
- Import and export FortiClient configurations through an XML file
- File extensions
 - .conf
 - .sconf Password is required
- Configuration file generated from:
 - FortiClient: **File > Settings > System**
 - FCConfig.exe: Command line program installed with FortiClient
- FortiClient EMS XML editor allows you to configure FortiClient settings in XML format

XML is a markup language that defines a set of rules for encoding documents in a format that is both human-readable and machine-readable.

FortiClient supports the import and export of its configuration in an XML file, and supports two file types, which are:

- **.conf**: a plain-text configuration file
- **.sconf**: a secure (encrypted) configuration file, which requires a password

You can generate and back up a configuration file (which is an XML file) on the **Settings** page of the FortiClient dashboard, or by using the command-line program `FCConfig.exe`, which is installed with FortiClient.

In the FortiClient EMS XML editor, you can configure FortiClient profile settings by using XML or a custom XML configuration file. The custom XML file must include all settings required by the endpoint at the time of deployment.

DO NOT REPRINT
© FORTINET

XML Configuration—File Section

- The XML configuration file contains:
 - Metadata
 - System settings
 - Endpoint control
 - VPN
 - Certificates
 - Antivirus
 - Single sign-on mobility agent
 - Web filtering
 - Application firewall
 - Vulnerability scan
- Boolean values
 - 0 means false (feature is disabled)
 - 1 means true (feature is enabled)

For the purpose of understanding the FortiClient XML configuration, the major section elements of the XML configuration are as follows:

- **Metadata:** facilitates the discovery of relevant information and is the basic data controlling the entire configuration file.
- **System settings:** are general settings that are not specific to any of the modules listed below (or affect more than one module).
- **Endpoint control:** includes settings related to controlling endpoints, such as enable enforcement, off-net update, skip confirmation, disable unregister, silent registration, and so on.
- **VPN:** includes settings related to global options that apply to both SSL VPN and IPsec VPN, and settings related to SSL VPN and IPsec VPN individually.

You can also configure XML for settings related to certificates, antivirus, single sign-on mobility agent, web filtering, application firewall, and vulnerability scan.

The XML configuration is controlled by two boolean values (usually denoted as true and false) that enable or disable a configuration setting—0 means false (feature is disabled), and 1 means true (feature is enabled).

Also in this lesson, you will learn how to enable and disable specific configuration settings.

XML Configuration—Metadata

- Configuration file is contained inside an XML tag
 - `<forticlient_configuration>`
- Standard XML start tag, which includes an XML version number and encoding
 - `<?xml version="1.0" encoding="utf-8"?>`
- Empty configuration will look like the following example:

```
<?xml version="1.0" encoding="UTF-8" ?>
<forticlient_configuration>
</forticlient_configuration>
```

Start of FortiClient
configuration

End of FortiClient
configuration

- Sample metadata

```
<?xml version="1.0" encoding="UTF-8" ?>
<forticlient_configuration generatedby="FCI-7.0.0.0029" policy="">
  <forticlient_version>7.0.0.29</forticlient_version>
  <version>7.0.0</version>
  <exported_by_version>7.0.0.0029</exported_by_version>
  <date>2021/06/21</date>
  <partial_configuration>0</partial_configuration>
  <os_version>windows</os_version>
  <os_architecture>x64</os_architecture>
```

FortiClient version

Date of configuration
generated

0→Config will be replaced
1→Config will be added

OS version – Windows
or Mac OS X

All of the XML tags and data in a configuration file are contained inside the XML tag `<forticlient_configuration>`. The first line of the configuration starts with a standard XML start tag `<?xml version="1.0" encoding="utf-8"?>`, which includes the XML version and encoding.

The XML configuration has elements (or nested child elements) that begin with a start tag and end with a matching end tag. An empty FortiClient configuration would look like the example shown on this slide.

If you export the configuration from FortiClient, it includes the FortiClient version, date of generation, and OS version (Windows or Mac OS X) from where the configuration was generated—either FortiGate or FortiClient FortiClient EMS.

`<partial_configuration>` is a line of metadata that controls whether the configuration is replaced or added in an import or restore. The value 0 replaces the configuration, and the value 1 appends the configuration to the existing configuration.

XML Configuration—Endpoint Control

- Endpoint control configuration is usually downloaded from FortiClient EMS
- Divided into two sections:
 - Endpoint control general attributes
 - Specific feature configurations

Endpoint control example

```
<forticlient_configuration>
<partial_configuration>1</partial_configuration>
<endpoint_control>
<enabled>1</enabled>
<disable_unregister>1</disable_unregister>
<silent_registration>1</silent_registration>
</endpoint_control>
<fortigates>
<addresses>192.168.1.99:9090</addresses>
</fortigates>
</forticlient_configuration>
```

Preventing a registered client from unregistering

Automatic registering

Registering to specified address—FortiClient EMS

The endpoint control configuration element controls settings related to controlling endpoints, such as disable unregister, silent registration, enable enforcement, off-net update, skip confirmation, which features to display on the FortiClient console, and so on.

You usually download the endpoint control configurations from FortiGate or FortiClient EMS, or you can build it using the instructions in the FortiClient XML configuration section in the *XML Reference Guide* available at <http://docs.fortinet.com>.

The endpoint control configurations are divided into two parts:

1. Endpoint control general attributes. These are contained in the <endpoint_control> XML tags.
2. Configuration details relating to specific FortiClient services, such as antivirus, web filtering, application firewall, vulnerability scanner, and so on. They are found in their respective configuration elements contained inside their XML tags. For example, the antivirus configuration is contained in the <antivirus> XML tags.

In the example shown on this slide, `silent_registration`, allows you to automatically register on FortiGate or FortiClient EMS without prompting the user to accept the registration. Silent registration is intended to be used with `disable_unregister`, which prevents a registered client from being able to unregister after successfully registering on a FortiGate or FortiClient EMS server.

The `addresses` XML setting defines that FortiClient will attempt to register on the first FortiGate or FortiClient EMS listed here. You can add multiple IP addresses delimited with a semicolon.

XML Design Considerations

- FortiClient configuration file is user editable
 - Uses XML format for easy parsing and validation
- Design considerations
 - Input validation
 - Handling of password fields
 - Segment of configuration file
 - Client certificate

Valid segment of configuration file

```
<?xml version="1.0" encoding="utf-8"?>
<forticlient_configuration>
  <system>
    <remote_logging>
      <log_upload_enabled>1</log_upload_enabled>
      <log_upload_server>10.0.1.210</log_upload_server>
    </remote_logging>
  </system>
</forticlient_configuration>
```

Invalid segment of configuration file

```
<?xml version="1.0" encoding="utf-8"?>
<forticlient_configuration>
  <remote_logging>
    <log_upload_enabled>1</log_upload_enabled>
    <log_upload_server>10.0.1.210</log_upload_server>
  </remote_logging>
</forticlient_configuration>
```

Does not follow syntax and hierarchy level
Missing <system> syntax and hierarchy level

The FortiClient configuration file is user editable and includes all client configurations. When building an XML configuration, you should adopt the following design considerations:

- Input validation:** The import function performs basic validation, and writes to a log when errors or warnings are found. The default values for omitted configurations are ignored, but for VPN they are defined in the configuration.
- Handling of password fields:** The password and username fields are encrypted (prefixed with "Enc") when a configuration is exported. However, the import function is able to take either the cleartext or encrypted format.
- Segment of configuration file:** The XML configuration allows you to import the segment (partial configuration) of a configuration file. However, the segment should follow the syntax and hierarchy defined in the *XML Reference Guide* available at <http://docs.fortinet.com>.

In the example, the invalid segment configuration file is missing the hierarchy and syntax for <system> level commands and is considered to be an invalid segment.

Client certificate: Client certificates are exported in an encrypted format in the configuration file.

DO NOT REPRINT
© FORTINET

Knowledge Check

1. In XML, which value controls feature configuration?
☐ A. Decimal value
☒ B. Boolean value

2. Which two parts make up the endpoint control configuration?
☒ A. Endpoint control general attributes and specific feature configurations
☐ B. Metadata and system settings

DO NOT REPRINT
© FORTINET

Lesson Progress

-  Endpoint Policy and Components
-  Endpoint Profiles
-  FortiClient Settings
-  Understand and Configure FortiClient XML

 **NSE Training Institute**

© Fortinet Inc. All Rights Reserved.

70

Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in this lesson.

DO NOT REPRINT
© FORTINET

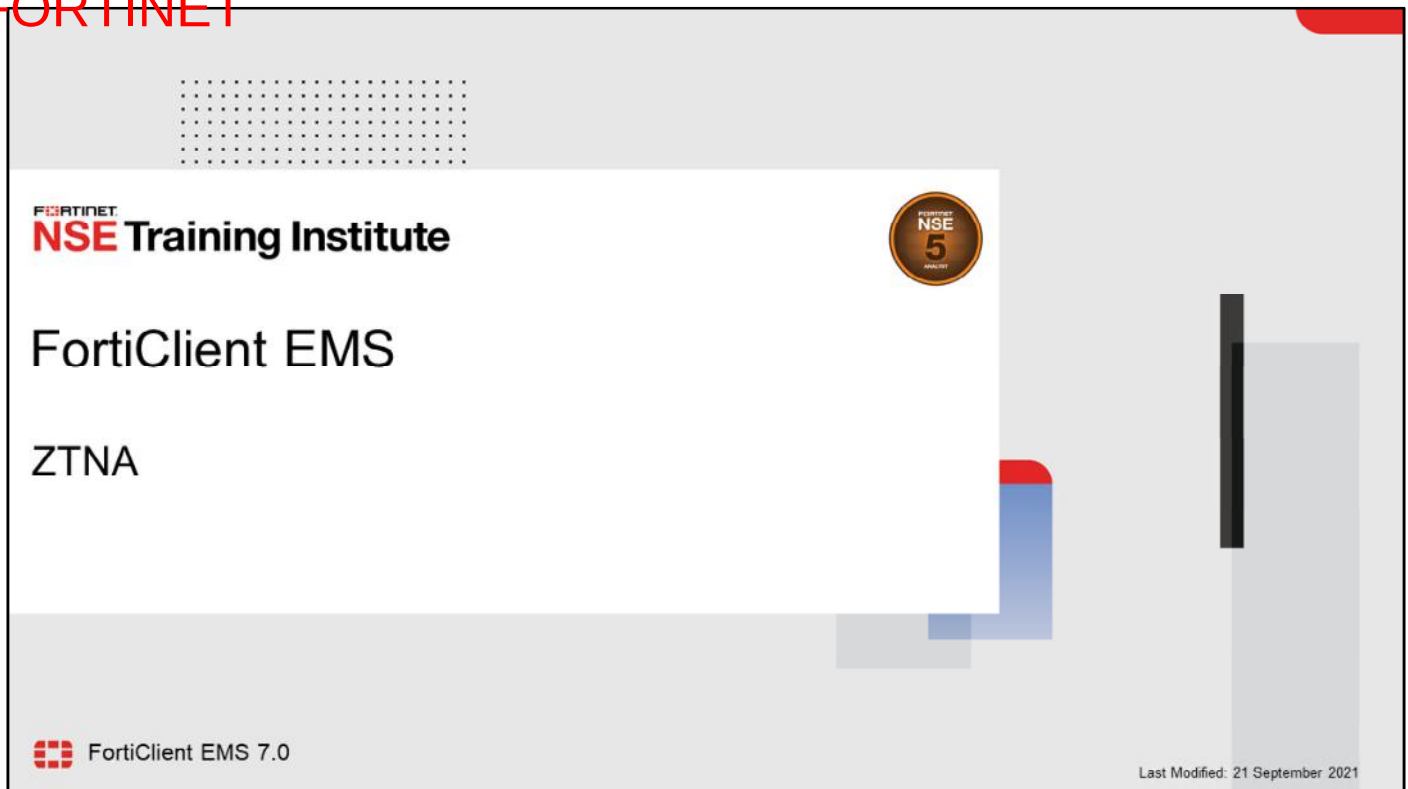
Review

- ✓ Understand endpoint policy
- ✓ Configure and edit endpoint policy
- ✓ Manage CA certificates
- ✓ Configure on-fabric detection rules
- ✓ Understand endpoint profiles
- ✓ Configure and edit endpoint profiles
- ✓ Configure endpoint profile references
- ✓ Configure FortiClient settings
- ✓ Understand and configure FortiClient XML

This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned how to use FortiClient EMS endpoint policy and components, profiles, profile references, and more. You also learned about FortiClient settings and XML configuration.

DO NOT REPRINT
© FORTINET

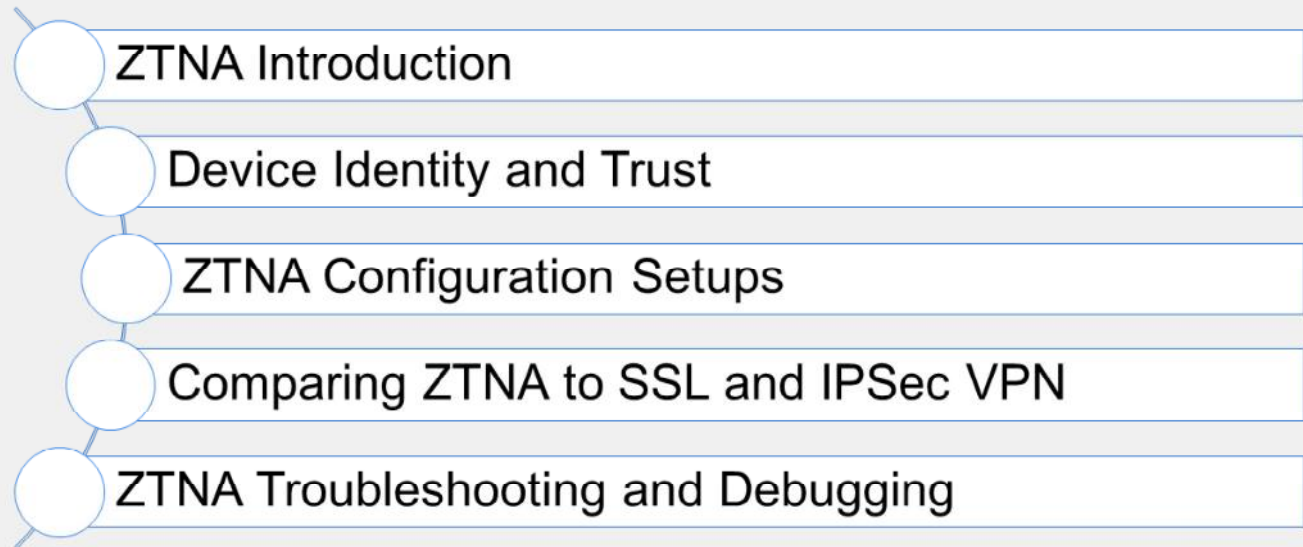


In this lesson, you will learn about zero trust network access (ZTNA).

By demonstrating competence in ZTNA, you will be able to understand key ZTNA concepts and how to configure ZTNA. You will also learn how to troubleshoot and debug ZTNA issues on the FortiGate and FortiClient EMS.

DO NOT REPRINT
© FORTINET

Lesson Overview

- 
- ZTNA Introduction
 - Device Identity and Trust
 - ZTNA Configuration Setups
 - Comparing ZTNA to SSL and IPSec VPN
 - ZTNA Troubleshooting and Debugging

In this lesson, you will learn about the topics shown on this slide.

DO NOT REPRINT
© FORTINET

ZTNA Introduction

Objectives

- Understand the benefits of using ZTNA
- Understand the fundamentals of ZTNA
- Understand ZTNA tagging rules
- Manage ZTNA tags on FortiClient EMS

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in understanding the benefits and basic configuration of ZTNA, you will be able to implement ZTNA in your environment.

What is ZTNA?

- Access control method that provides role-based application access
- ZTNA method uses:
 - Client device identification
 - Authentication
 - Zero-trust tags
- Provides flexibility to manage both on-fabric and off-fabric users
- ZTNA has two modes:
 - Full ZTNA
 - IP/MAC filtering

ZTNA is an access control method that uses client device identification, authentication, and zero trust tags to provide role-based application access. ZTNA gives administrators the flexibility to manage network access for on-fabric local users and off-fabric remote users. ZTNA grants access to applications only after device verification, authenticating the user's identity, authorizing the user, and then performing context-based posture checks using zero trust tags.

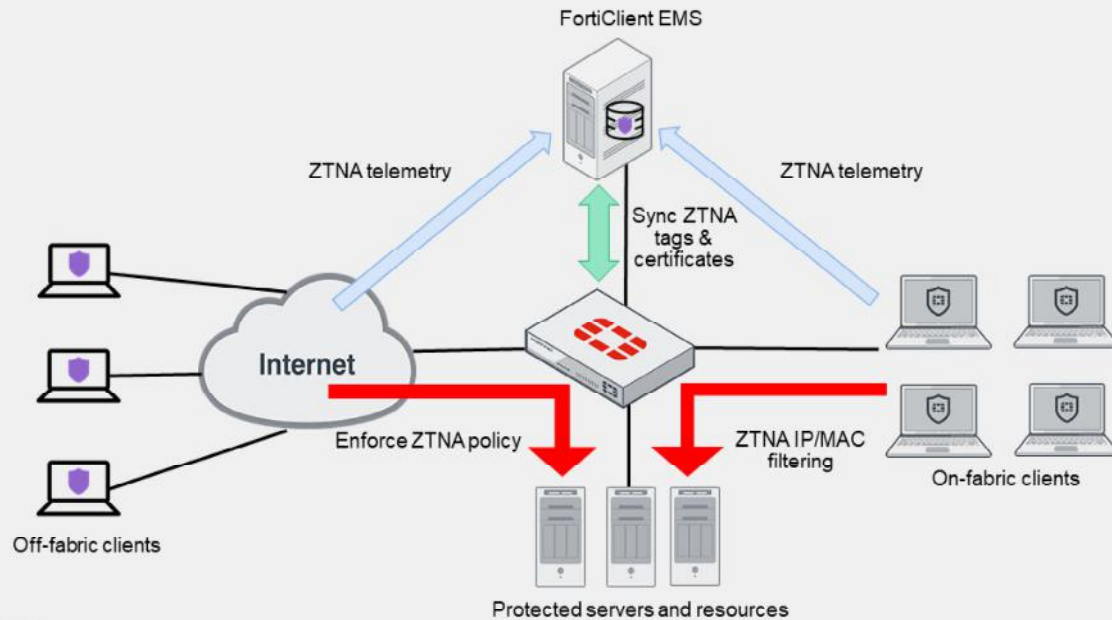
Traditionally, a user and a device have different sets of rules for on-fabric access and off-fabric VPN access to company resources. With a distributed workforce, and access that spans company networks, data centers, and the cloud, managing the rules can be complex. User experience is also affected when an organization needs multiple VPNs to access various resources.

ZTNA has two modes:

- Full ZTNA allows users to securely access resources through an SSL-encrypted access proxy. This simplifies remote access by eliminating the use of VPNs.
- IP/MAC filtering uses ZTNA tags to provide an additional factor for identification, and a security posture check to implement role-based zero-trust access.

DO NOT REPRINT
© FORTINET

ZTNA Workflow



Fortinet NSE Training Institute

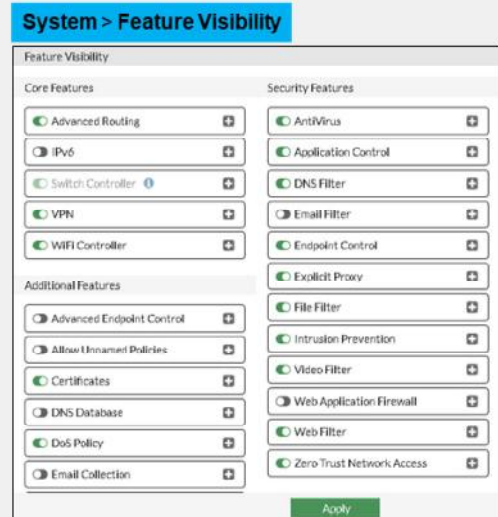
© Fortinet Inc. All Rights Reserved.

5

This slide demonstrates ZTNA telemetry, tags, and policy enforcement. You configure ZTNA tag conditions and policies on FortiClient EMS. FortiClient EMS shares the tag information with FortiGate through Security Fabric integration. FortiClient communicates directly with FortiClient EMS to continuously share device status information through ZTNA telemetry. FortiGate can then use ZTNA tags to enforce access control rules to incoming traffic through ZTNA access.

Basic ZTNA Configuration

- Configure ZTNA on FortiGate
- To enable ZTNA and Explicit Proxy on the GUI, **System > Feature Visibility**
- To deploy ZTNA, you need the following:
 - FortiClient endpoint
 - FortiClient EMS
 - FortiGate
 - FortiClient EMS connector
 - ZTNA server
 - ZTNA rule
 - Firewall policy for ZTNA
 - Authentication (optional)



To enable ZTNA on the GUI, you must enable the feature on FortiGate **System > Feature Visibility**, and then enable **Zero Trust Network Access**. You must also enable **Explicit Proxy** feature on the FortiGate **System > Feature Visibility**.

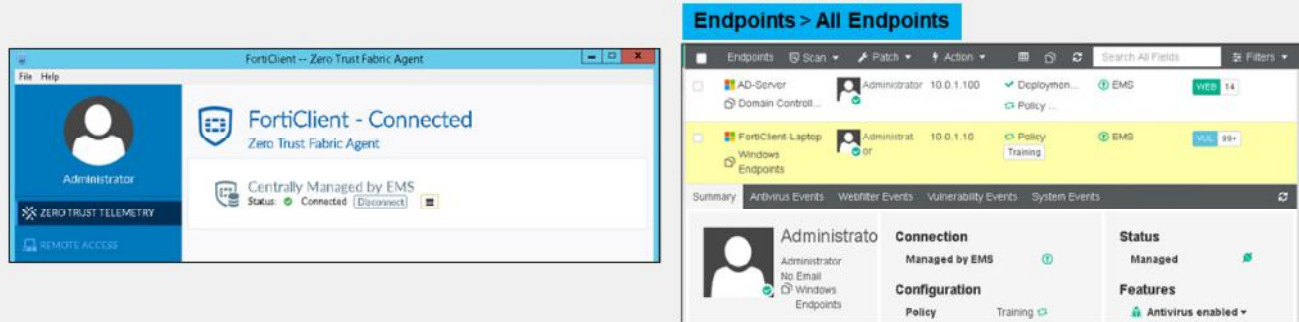
ZTNA configuration on the FortiGate requires the following configuration:

- FortiClient EMS adds a fabric connector in the security fabric. FortiGate maintains a continuous connection to the EMS server to synchronize endpoint device information, and also automatically synchronizes ZTNA tags. You can create groups and add tags to use in the ZTNA rules and firewall policies.
- The ZTNA server defines the access proxy VIP and the real servers that clients connect to. The firewall policy matches and redirects client requests to the access proxy VIP. You can also enable authentication.
- A ZTNA rule is a proxy policy used to enforce access control. You can define ZTNA tags or tag groups to enforce zero-trust role-based access. You can configure security profiles can be configured to protect this traffic.
- The firewall policy matches and redirects client requests to the access proxy VIP. You can define the source interface and addresses that can access the VIP can be defined. By default, the destination is any interface. UTM processing of the traffic happens at the ZTNA rule.

You can also configure authentication to the access proxy. ZTNA supports basic HTTP and SAML methods are supported.

FortiClient and FortiClient EMS Connectivity

- FortiClient endpoint must connect to FortiClient EMS
- Check connection status:
 - On **ZERO TRUST TELEMETRY** menu
 - On the FortiClient EMS GUI, **Endpoints > All Endpoints**

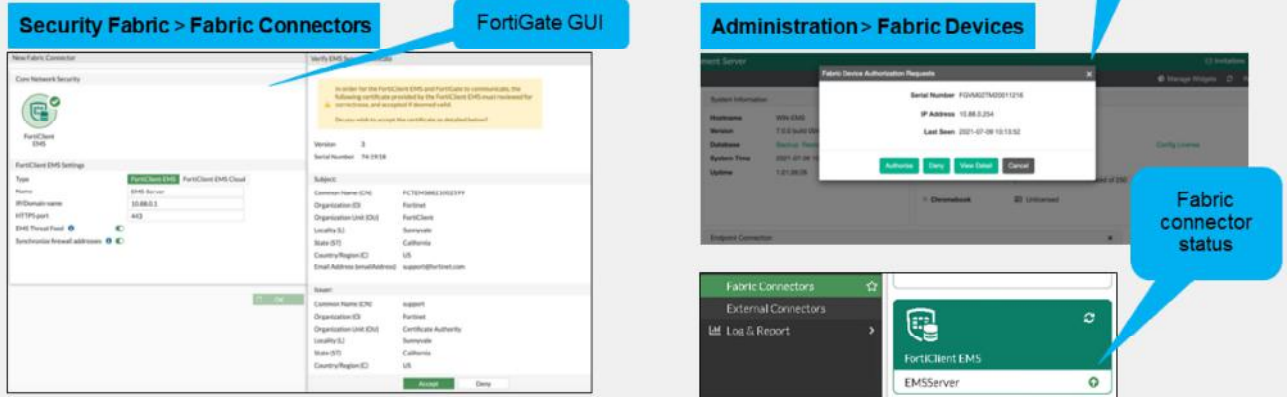


FortiClient must connect to FortiClient EMS. You can verify connection status on the FortiClient console in the **ZERO TRUST TELEMETRY** menu, or on FortiClient EMS by clicking **Endpoints > All Endpoints** page.

To provide connectivity to the remote FortiClient endpoints, you must allow access to port 8013 on the FortiClient EMS through the corporate firewall. On FortiGate, you can create a VIP and inbound policy to allow access to TCP port 8013 from the internet.

FortiGate and FortiClient EMS Connectivity

- FortiGate uses FortiClient EMS fabric connector to connect
- FortiGate must verify the FortiClient EMS server certificate
 - Need to install CA certificate on FortiGate, otherwise certificate is not trusted
- FortiClient EMS must authorize the FortiGate as fabric device



You can configure the on-premises FortiClient EMS connector on FortiGate by clicking **Security Fabric > Fabric Connectors**. After applying the FortiClient EMS settings, FortiGate must accept the FortiClient EMS server certificate. However, when you configure a new connection to FortiClient EMS server, the certificate might not be trusted. To resolve, you must manually export and install the certificate on FortiGate. The FortiClient EMS certificate that is used by default for the SDN connection is signed by the CA certificate that is saved on the Windows server when you first install FortiClient EMS. This certificate is stored in the **Trusted Root Certification Authorities** folder on the server. For more information about exporting and installing certificates on FortiGate, refer to the *FortiOS-7.0.1 Administration Guide*.

Next, you must authorize FortiGate on FortiClient EMS. If you log in to FortiClient EMS, a pop-up window opens, requesting you to authorize FortiGate. If you do not log in, you can click **Administration > Devices**, select the FortiGate device, and then authorize it. Note that the FortiClient EMS connector status appears down until you authorize FortiGate on FortiClient EMS.

FortiGate automatically synchronizes ZTNA tags after it connects to FortiClient EMS.

Zero-Trust Tagging Rules

- You can create, edit, and delete zero-trust tagging rules for Windows, macOS, Linux, iOS, and Android
- When using tagging rules with EMS and FortiClient
 - EMS sends zero-trust tagging rules to endpoints
 - FortiClient checks endpoints using the provided rules and sends the results to EMS
 - EMS dynamically groups endpoints together using the tag configured for each rule
 - You can view the dynamic endpoint groups in **Zero Trust Tags > Zero Trust Tag Monitor**

Zero Trust Tags > Zero Trust Tagging Rules

Zero Trust Tagging Rule Set

Name: Malicious-File-Detected

Tag Endpoint As: Malicious-File-Detected

Enabled: ☒

Comments: Optional

Rules: [Edit Logic](#) [Add Rule](#)

Type	Value
Windows (1)	
File	C:\virus.dll

[Save](#) [Cancel](#)

Zero Trust Tags > Zero Trust Tagging Monitor

Endpoint with Tag [Refresh](#)

Remote-Endpoints (1)

Endpoint	User	OS	IP	Tagged on
Remote-Client	Administrator	Microsoft Windows Ser...	10.0.2.20	2021-08-25 02:43:06

You can create, edit, and delete zero trust tagging rules for Windows, macOS, Linux, iOS, and Android endpoints. The following happens when using zero trust tagging rules with FortiClient EMS and FortiClient:

- FortiClient EMS sends zero trust tagging rules to endpoints through telemetry communication.
- FortiClient checks endpoints using the provided rules and sends the results to FortiClient EMS.
- FortiClient EMS receives the results from FortiClient.
- FortiClient EMS dynamically groups endpoints together using the tag configured for each rule. You can view the dynamic endpoint groups by clicking **Zero Trust Tags > Zero Trust Tag Monitor**.

Note that when the endpoint network changes or user login and logout events occur, FortiClient triggers an X-FFCK-TAG message to FortiClient EMS, even if there are no tag changes. After FortiClient EMS receives the tags, it processes them immediately, and updates the FortiOS tags within five seconds of the REST API response. For other tag changes, FortiClient sends the information to FortiClient EMS regularly.

Zero-Trust Tagging Rules (Contd)

- You click **Add** to add a new rule set
- In the rule set window, you can type a rule name, and select a new or existing tag and different rule types based on operating system
- You can configure multiple rules
- By default, an endpoint must satisfy all configured rules
- Use **Edit Logic** to apply the tag to endpoints that satisfy some, but not all, of the configured rules

Example to rule logic

Zero Trust Tags > Zero Trust Tagging Rules > +Add

Zero Trust Tagging Rule Set

Name: Required

Tag Endpoint As: Select or create a tag

Enabled: ☒

Comments: Optional

Rules Edit Logic + Add Rule

Type	Value
No Rules Found	

Save Cancel

Rules Default Logic + Add Rule

Type	Value
Windows (2)	
Antivirus Software	1. AV Software is installed and running
OS Version	2. Windows 7 3. Windows 10

Rule Logic (1 and 2) or 3 Reset

You can click **Add** to add a new rule on the **Zero Trust Tagging Rules** page. The rule set requires a name, tag, and rule types for different operating systems. The type of OS you select affects what rule types and related options are available. You can configure multiple rule types on the rule set.

By default, an endpoint must satisfy all configured rules to be eligible for the rule set. You may want to apply the tag to endpoints that satisfy some, but not all, of the configured rules. In this case, you can modify the rule set logic. In the example shown on this slide, an administrator wants to apply the same tag to endpoints that fulfill one of the following criteria:

- Running Windows 10
- Running Windows 7, and antivirus software is installed and running

With the default rule set logic, an endpoint would be eligible for the rule set if it is running Windows 7 or 10 and has antivirus software installed and running. To modify the rule set logic, click **Edit Logic** to numerical values to each rule. Enter **(1 and 2) or 3**, to indicate that endpoints that satisfy both the antivirus and Windows 7 rules (rules 1 and 2) or only the Windows 10 rule (rule 3) satisfy the rule set. To restore the default logic, you can click **Default Logic**.

You can use **and** and **or** to define the rule logic. You cannot use **not** when defining the rule logic. You can also use parentheses to group rules, as show on this slide.

Zero-Trust Tagging Rules (Contd)

- Import and export tagging rules as a JSON file

Zero Trust Tags > Zero Trust Tagging Rules

Zero Trust Tagging Rule Sets					Manage Tags	Import	Export	Add	Refresh
Name	Tag	Enabled	Comments						

- Use predefined rules for FortiGuard outbreak alert service by uploading signatures

Zero Trust Tags > Zero Trust Tagging Rules

FortiClient Endpoint Management Server

Dashboard

Endpoints

Deployment & Installers

Endpoint Policy & Components

Endpoint Profiles

Zero Trust Tags

Zero Trust Tagging Rules

Zero Trust Tag Monitor

Zero Trust Tagging Rule Sets

Name

Tag

Enabled

Comment

Chrome Running File_Linux

Chrome Running File_Linux

Managed by EMS

EMS_Managed_Endpoint_Windows

Firefox Running Process_Linux

Firefox Running Process_Linux

Firefox Running Process_Mac

Firefox Running Process_Mac

Skype Running File_Mac

Skype Running File_Mac

Skype Running File_Windows

Skype Running File_Windows

Skype Running Process_Windows

Skype Running Process_Windows

Import Signatures

Manage Tags

You can import and export a zero-trust tagging rule set as a JSON file. You can also use a zero-trust tagging rule as a predefined rule for FortiGuard outbreak alerts by uploading rule signatures.

The JSON file should contain an array of alert objects, each with a tag name and array of signatures. Each signature should have the following properties:

- OS (Windows, MacOS, Linux, iOS, Android)
- Type (file, registry, process)
- Content

If the import succeeds, FortiClient EMS displays a **FortiGuard outbreak alert signatures imported successfully** message. If the file is formatted incorrectly, FortiClient EMS shows an **Invalid JSON** error.

Zero-Trust Tagging Rules (Contd)

- **Manage Tags**

- Displays all configured tags and the rules that apply that tag to the endpoints
- Delete tags that do not have any rules attached



- **Zero Trust Tag Monitor**

- View all dynamic endpoint groups based on the tag configured for each rule



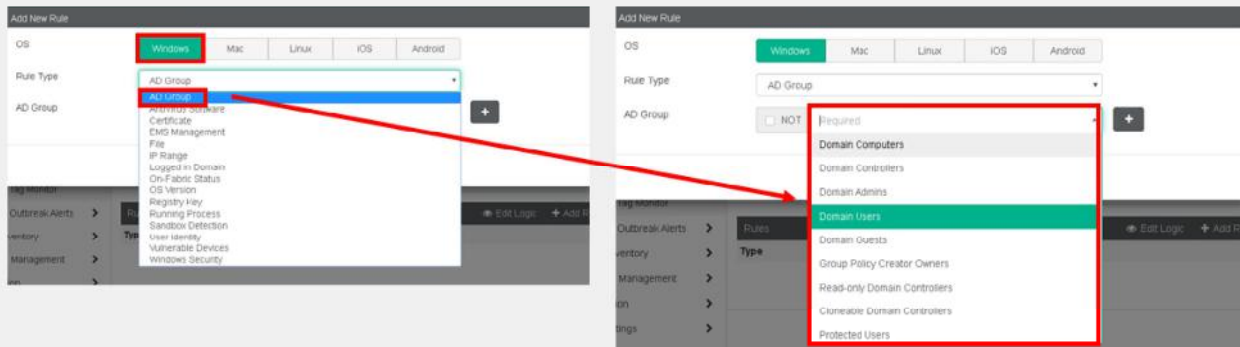
The **Manage Tags** window displays all configured tags and the rules that apply the tags to endpoints that satisfy the rule. You can delete tags that do not have any rules attached. In the example shown on this slide, you can delete the **Server 2012** rule because it does not have any rules attached.

You can view all dynamic endpoint groups in the **Zero Trust Tag Monitor** section. FortiClient EMS creates dynamic endpoint groups based on the tag configured for each rule.

The endpoint must satisfy all configured conditions to satisfy the rule. You can use the **NOT** operator as well. Note that not all the rule types support the **NOT** operator. For detailed information, refer to the *FortiOS 7.1 Administration Guide*.

Zero Trust Tagging Rules—Rule Types

- ZTNA tagging rule has different rules types that varies with OS you select



ZTNA tagging rule has different rule types which varies with OS you select. This slide shows the zero trust tagging rule types available for Windows OS. Each rule type gives options to select. For example if you select **AD Group** then you need to select the desired AD group from the available group on the domain server. To use this option, you must configure your domain under **Endpoints**. For all rule types, you can configure multiple conditions.

The endpoint must satisfy all configured conditions to satisfy the rule. You can use the **NOT** as well. Note that not all the rule types support **NOT** option. For detailed information about all the rules types and OS these are available for, refer to the *FortiOS-7.0-Administration Guide*.

DO NOT REPRINT
© FORTINET

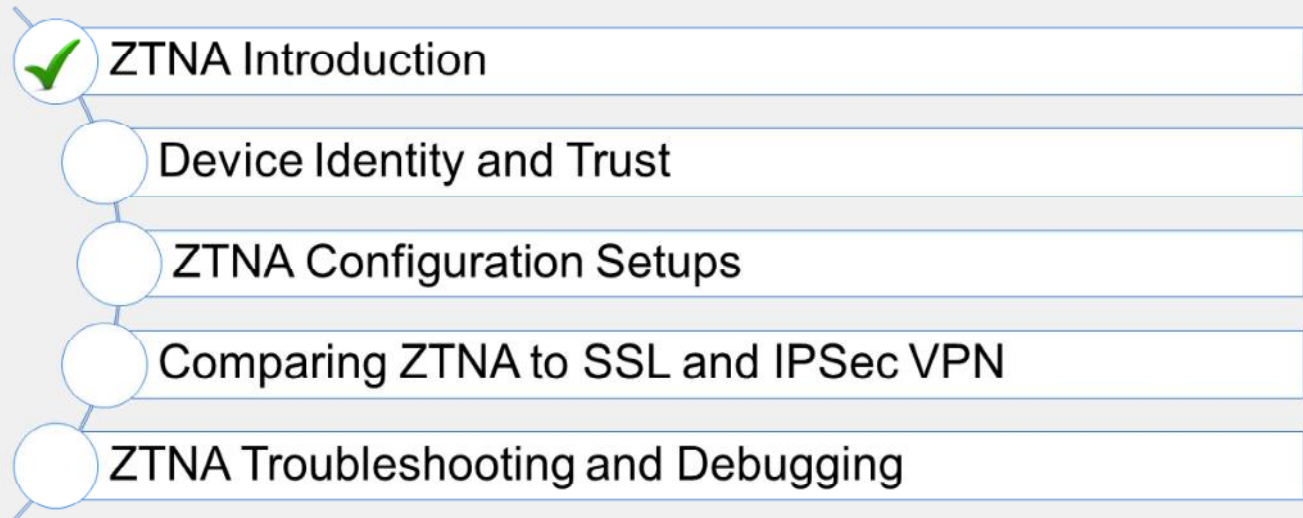
Knowledge Check

1. Which ZTNA mode provides secure access through access proxy?
 - A. ZTNA IP/MAC filtering
 - ✓ B. Full ZTNA

2. Which ZTNA configuration on FortiGate enforces access control?
 - A. ZTNA server
 - ✓ B. ZTNA rule

DO NOT REPRINT
© FORTINET

Lesson Progress



Good job! You now know about ZTNA and its basic configuration requirements.

Now, you will learn about device identity and trust among FortiClient, FortiClient EMS, and FortiGate.

Device Identity and Trust

Objectives

- Understand how to establish device identity and trust
- Understand SSL certificate-based authentication

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in device identity and trust, you will be able to understand device roles and how SSL certificate-based authentication works.

Device Roles

- Device identity and trust are integral to ZTNA
- Identity is established through client certificates
- Trust is established between:
 - FortiClient
 - Provides endpoint information (device information, logged on users, and security posture)
 - Obtains client certificate from FortiClient EMS
 - FortiClient EMS
 - Issues and signs the client certificate
 - Synchronizes certificate to FortiGate
 - Uses tagging rules to tag endpoints
 - FortiGate
 - Maintains continuous connection to FortiClient EMS to synchronize endpoint information
 - When device information changes, FortiClient EMS updates FortiGate
 - FortiGate WAD daemon uses this information when processing ZTNA traffic

Device identity and trust are integral to ZTNA. Device identity is established through client certificates, and trust is established among FortiClient, FortiClient EMS, and FortiGate devices. In ZTNA, devices perform specific roles.

FortiClient provides the following information to FortiClient EMS when it registers:

- Device information (network details, operating system, model, and so on)
- Logged in user information
- Security posture (On-fabric and Off-fabric, antivirus software, vulnerability status, and so on)

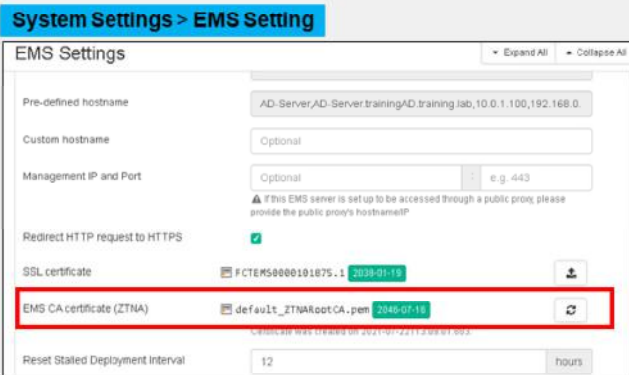
FortiClient also requests and obtains a client device certificate from the EMS ZTNA Certificate Authority (CA) on its first attempt to connect to the access proxy. The client uses this certificate to identify itself to FortiGate.

FortiClient EMS issues and signs the client certificate with the FortiClient UID, certificate serial number, and EMS serial number. FortiClient EMS then synchronizes the certificate with FortiGate. FortiClient EMS also shares its EMS ZTNA CA certificate with FortiGate, so that FortiGate can use it to authenticate the clients. FortiClient EMS uses zero-trust tagging rules to tag endpoints based on the information that it has on each endpoint. FortiClient EMS also shares the tags with FortiGate.

FortiGate maintains a continuous connection to FortiClient EMS to synchronize endpoint device information such as FortiClient UID, client certificate SN, FortiClient EMS SN, network details (IP and MAC address), and so on. When device information changes, such as when a client moves from on-fabric to off-fabric, or their security posture changes, FortiClient EMS updates the device information, and then updates the FortiGate.

FortiClient EMS Certificate Management

- FortiClient EMS has a default root CA certificate
- ZTNA CA uses root certificate to sign CSRs from the FortiClient endpoints
- You can revoke and update root CA
 - Force updates to the FortiGate and FortiClient endpoints by generating new certificates
- FortiClient EMS manages individual client certificates



FortiClient EMS has a **default_ZTNArootCA** certificate generated by default that the ZTNA CA uses to sign CSRs from the FortiClient endpoints. Clicking the refresh button revokes and updates the root CA, forcing updates to the FortiGate and FortiClient endpoints by generating new certificates for each client. FortiClient EMS can also manage individual client certificates. You can also revoke the certificate that is used by the endpoint when certificate private keys show signs of being compromised. Click **Endpoint > All Endpoints**, select the client, and then click **Action > Revoke Client Certificate**.

Do not confuse the FortiClient EMS CA certificate (ZTNA) with the SSL certificate. The latter is the server certificate that is used by FortiClient EMS for HTTPS access and fabric connectivity to the FortiClient EMS server.

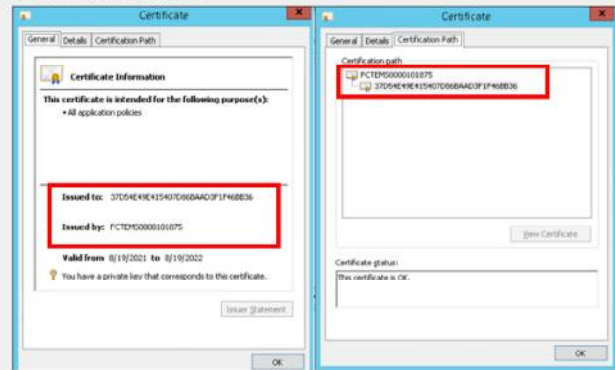
FortiClient EMS Certificate Management (Contd)

- On Windows endpoints, FortiClient automatically installs certificates in the certificate store
 - Certificate information, such as certificate UID and SN, should match the information on FortiClient EMS and FortiGate
 - Certificates > Personal > Certificates**
- You can verify by CLI command on the FortiGate
 - `diagnose endpoint record list <optional IP address>`

```

HQ-FortiGate # diagnose endpoint record list
Record #1:
  IP Address = 10.0.1.100
  MAC Address = 00:50:56:a1:1b:15
  MAC List = 00:50:56:a1:19:7a:00:50:56:a1:1b:15;
  VPN = root (0)
  EMS serial number: FCTEM00000101075
  Client cert SN: 37054E49E411407056BAAC0F1F46B36
  Public IP address: 206.47.132.124
  Quarantined: no
  Online status: online
  Registration status: registered
  On-net status: on-net
  Gateway interface: port3
  FortiClient version: 7.0.0
  AVDS version: 88.336
  FortiClient app signature version: 18.143
  FortiClient vulnerability scan engine version: 2.31
  FortiClient UID: 37054E49E411407056BAAC0F1F46B36
  Host Name: AD-Server
  OS Type: Win64
  OS Version: Microsoft Windows Server 2012 R2 Standard Edition, 6
  4-bit (build 9600)
  Host Description:
  Domain: trainingAD.training.lab
  Last Login User: Administrator
  Owner:
  Host Model: VMware Virtual Platform
  Host Manufacturer: VMware, Inc.

```



In Windows, FortiClient automatically installs certificates into the certificate store. The certificate information in the store, such as certificate UID and SN, should match the information on FortiClient EMS and FortiGate. To locate certificates on other operating systems, consult the vendor documentation.

You can use the CLI command `diagnose endpoint record list a` to verify the presence of matching endpoint record, and information such as the client UID, client certificate SN, and EMS certificate SN on the FortiGate. If any of the information is missing or incomplete, client certificate authentication might fail because FortiClient cannot locate the corresponding endpoint entry.

This slide shows that client certificate information is synchronized to the FortiGate.

SSL Certificate-Based Authentication

- An endpoint obtains a client certificate when it registers to FortiClient EMS
- FortiClient automatically submits CSR request
- FortiClient EMS signs and returns the client certificate
- Certificate is stored in OS certificate store
- By default:
 - Client certificate authentication is enabled on access proxy
 - Empty certificate response is set to block
 - Options can be configured on CLI only

```
config firewall access-proxy
    edit <name>
        set client-cert enable
        set empty-cert-action block
    end
```

- Currently, ZTNA supports the Microsoft Edge and Google Chrome browsers

Endpoint obtains a client certificate when it registers to FortiClient EMS. FortiClient automatically submits a CSR request and the FortiClient EMS signs and returns the client certificate. This certificate is stored in the operating system certificate store for subsequent connections. The endpoint information is synchronized between FortiGate and FortiClient EMS. When an endpoint disconnects or is unregistered from FortiClient EMS, its certificate is removed from the certificate store and revokes on FortiClient EMS. The endpoint obtains a certificate again when it reconnects to the FortiClient EMS.

By default, client certificate authentication is enabled on the access proxy, so when FortiGate receives the HTTPS request, the FortiGate WAD process challenges the client to identify itself with its certificate. The FortiGate makes a decision based on specific possibilities.

If the client responds with the correct certificate that the client UID and certificate SN can be extracted from:

- If the client UID and certificate SN match the record on FortiGate, the client is allowed to continue with the ZTNA proxy rule processing.
- If the client UID and certificate SN do not match the record on FortiGate, the client is blocked from further ZTNA proxy rule processing.

If the client cancels and responds with an empty client certificate, the client is allowed to continue with ZTNA proxy rule processing when you can `empty-cert-action` to `accept`. If `empty-cert-action` to `block`, FortiGate blocks the client from further ZTNA proxy rule processing.

DO NOT REPRINT
© FORTINET

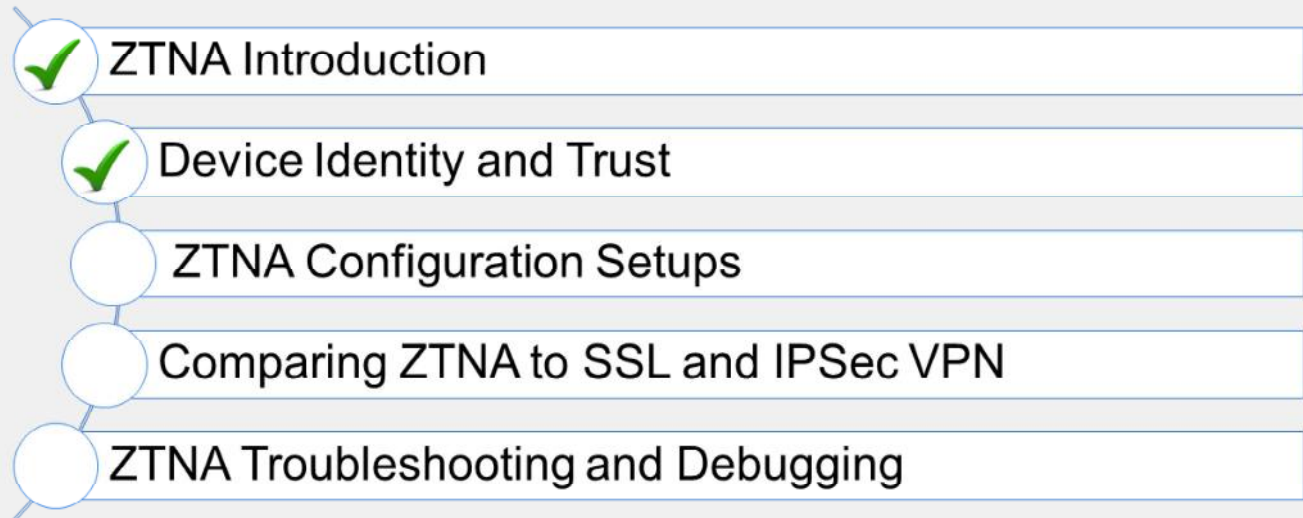
Knowledge Check

1. Which component issues and signs the client certificate?
☒ A. FortiClient EMS
☐ B. FortiClient

2. Which internet browser supports Fortinet ZTNA?
☐ A. Firefox
☒ B. Chrome

DO NOT REPRINT
© FORTINET

Lesson Progress



Good job! You now know about device identity, trust among FortiClient, FortiClient EMS, and FortiGate, and certificate-based authentication.

Now, you will learn about different ZTNA configuration setups.

DO NOT REPRINT
© FORTINET

ZTNA Configuration Setups

Objectives

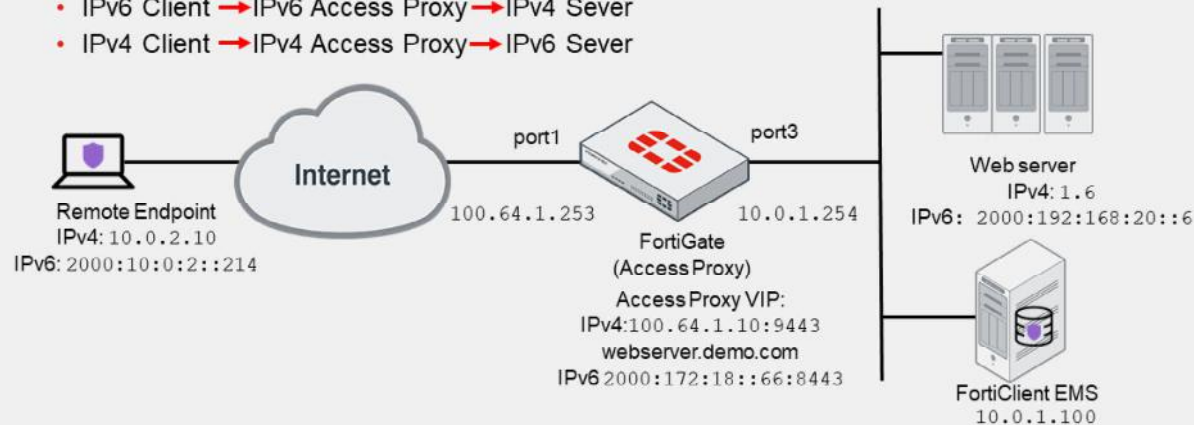
- Describe types of ZTNA configuration
- Configure ZTNA access on FortiOS

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in understanding ZTNA configuration setups, you will be able to implement the ZTNA configuration your environment requires.

ZTNA HTTPS Access Proxy

- HTTPS access proxy works as a reverse proxy
- Verifies user identity, device identity, and trust context before granting access
- Supports IPv6 scenarios:
 - IPv6 Client → IPv6 Access Proxy → IPv6 Server
 - IPv6 Client → IPv6 Access Proxy → IPv4 Server
 - IPv4 Client → IPv4 Access Proxy → IPv6 Server



Fortinet
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

24

The FortiGate HTTPS access proxy works as a reverse proxy for the HTTP server. When a client connects to a web page hosted by the protected server, the address resolves to the FortiGate access proxy VIP (192.186.2.86:8443), as shown on this slide. FortiGate proxies the connection and takes steps to authenticate the device. It prompts the user for the endpoint certificate on the browser, and verifies this against the ZTNA endpoint record that is synchronized from the FortiClient EMS.

This example shows access control that allows or denies traffic based on ZTNA tags. FortiGate allows the traffic when the FortiClient endpoint is tagged as **Low** risk, and denies the traffic when the endpoint is tagged with **Malicious-File-Detected**. This setup assumes that the FortiGate EMS fabric connector is already successfully connected and the tagging rule **Malicious-File-Detected** is configured, which you learned about in a previous section.

ZTNA also support IPv6. You can configure the following IPv6 scenarios:

- IPv6 Client — IPv6 Access Proxy — IPv6 Server
- IPv6 Client — IPv6 Access Proxy — IPv4 Server
- IPv4 Client — IPv4 Access Proxy — IPv6 Server

ZTNA HTTPS Access Proxy (Contd)

- ZTNA server:

Policy & Objects > ZTNA > ZTNA Servers

ZTNA Rules ZTNA Servers ZTNA Tags
+ Create New Edit Delete

Access Proxy VIP
IP address and port

Name: ZTNA-webserver
Comments:
Network:
Service: HTTPS
External interface: port1
External IP: 100.64.1.250
External port: 9443
Services and Servers
Default certificate: Fortinet_SSL
Service/server mapping
+ Create New Edit Delete
Service: URL
HTTPS: www.example2.com/map1

Virtual host matching rules

Service: HTTPS
Virtual Host: Any Host Specify
Match by: Substring Wildcard
Host: www.example2.com
Use certificate: Fortinet_CA_SSL
Match path by: Substring Wildcard Regular Expression
Path: /map1
Servers
+ Create New Edit Delete
IP: Port: Status:
10.0.1.250 443 Active

Real server
IP address and port

IP: 10.0.1.250
Port: 443
Status: Active Standby Disable

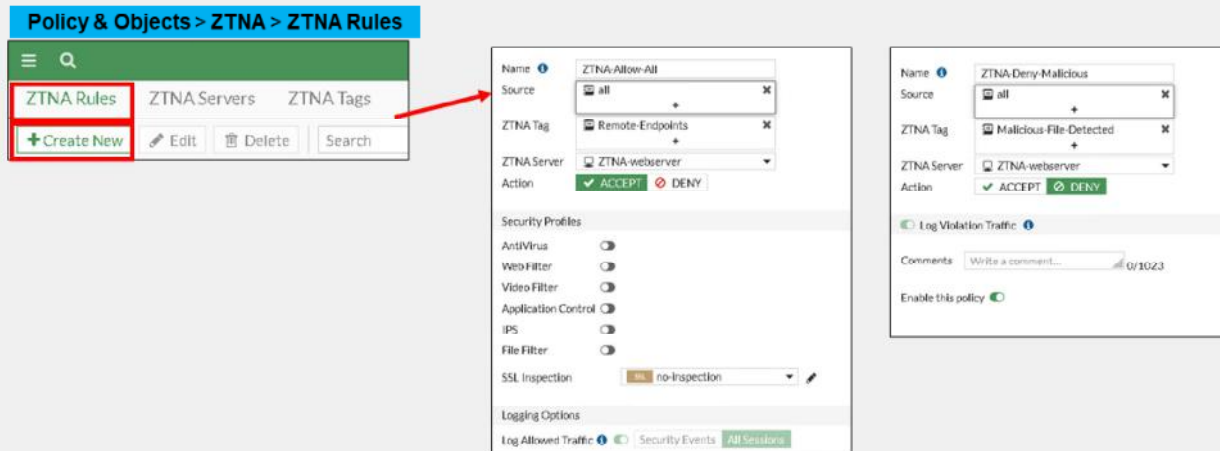
After you can FortiClient EMS as the fabric connector and you sync ZTNA tags with FortiGate, you must create a ZTNA server or access proxy. The access proxy VIP is the FortiGate ZTNA gateway that clients make HTTPS connections to. The service and server mappings define the virtual host matching rules and the real server mappings of the HTTPS requests.

The example on this slide shows access proxy VIP and the real server IP. The IP address 100.64.1.250 and port 9443 is an access proxy VIP that the client connects to, and then the request redirects the client to real server IP address 10.0.1.250 on port 443. In the **Service/server mapping** window, you can select **Any Host** so that any request that resolves to the access proxy VIP is mapped to the real servers. For example, if both `www.example1.com` and `www.example2.com` resolve to the VIP, then both requests are mapped to your real servers. The **Specify** option allows you to configure the name or IP address of the host that the request must match. For example, if you enter `www.example2.com` as the host, then only requests to `www.example2.com` match. The path can be matched by substring, wildcard, or regular expression. For example, if you specify the virtual host as `www.example2.com`, and the path substring is `map1` as shown on this slide, then `www.example2/map1` is matched.

The **Servers** table, allows you to configure the real server IP address, port number, and status. You can configure multiple servers and server mappings.

ZTNA HTTPS Access Proxy (Contd)

- ZTNA rule:



A ZTNA rule is a proxy policy used to enforce access control. You can define ZTNA tags or tag groups to enforce zero-trust role-based access. To create a rule, type a rule name, and add IP addresses and ZTNA tags or tag groups that are allowed or blocked access. You also select the ZTNA server as the destination. You can also apply security profiles to protect this traffic.

This slide shows two rules as an example. One is configured to allow endpoints that are tagged as **Remote-Endpoints**, and the other is configured to block endpoints that are tagged as **Malicious-File-Detected**.

ZTNA HTTPS Access Proxy (Contd)

- Firewall policy:
 - Redirects client requests to the access proxy
 - Select source interface and addresses that are allowed access to the VIP
 - UTM processing happens at the ZTNA rule

Policy & Objects > ZTNA > ZTNA Rules

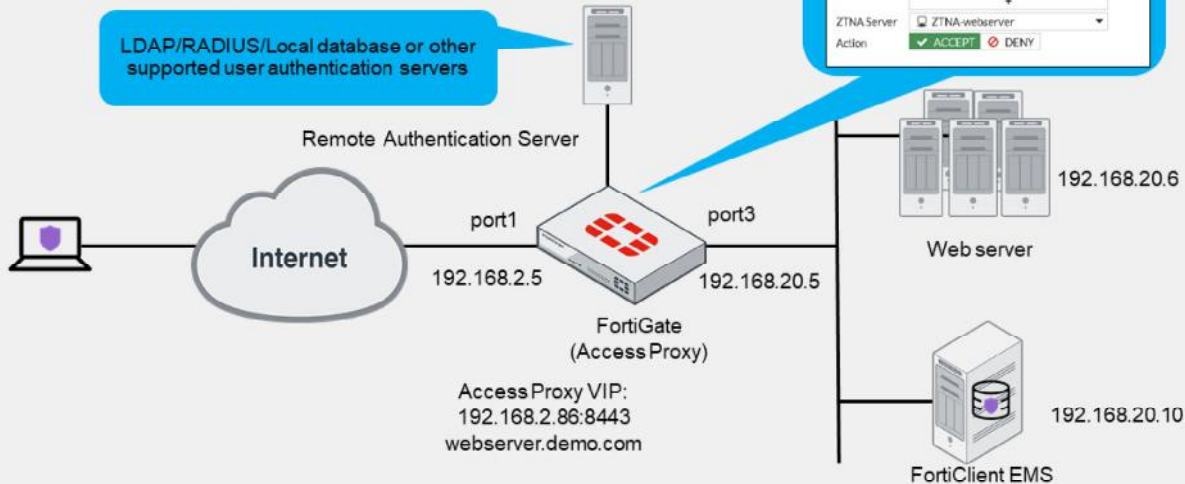
Name	ZTNA-WAN	
ZTNA	☒ Full ZTNA ☐ IP/MAC filtering	
Incoming Interface	port1	
Source	all	
ZTNA Server	ZTNA-webserver	
Schedule	always	
Service	ALL	
Action	☒ ACCEPT ☐ DENY	
Firewall / Network Options		
NAT	☐	
Logging Options		
Log Allowed Traffic	☒	
Comments	Write a comment... 0/1023	

The firewall policy matches and redirects client requests to the access proxy VIP. You can define source interface and addresses that are allowed access to the VIP. By default, the destination is any interface, so after a policy is configured for full ZTNA, the policy list is organized by sequence. The example on this slide is configured to allow **ALL** services from **all** IP addresses at **port1** as the incoming interface to **ZTNA-webserver** as the destination.

Note that UTM processing of the traffic happens at the ZTNA rule.

ZTNA HTTPS Access Proxy With Basic Authentication

- You can add authentication to the access proxy
- Requires authentication scheme and authentication rule
 - To authenticate proxy-based policies



Fortinet
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

28

You can add authentication to the access proxy, which requires you to configure an authentication scheme and authentication rule on the FortiGate CLI. You use authentication schemes and authentication rules to authenticate proxy-based policies, similar to configuring authentication for explicit and transparent proxy.

The authentication scheme defines the method of authentication that is applied. ZTNA supports basic HTTP and SAML methods. Each method has additional settings to define the data source. For example, with basic HTTP authentication, a user database can reference an LDAP server, RADIUS server, local database, or other supported authentication servers that the user is authenticated against.

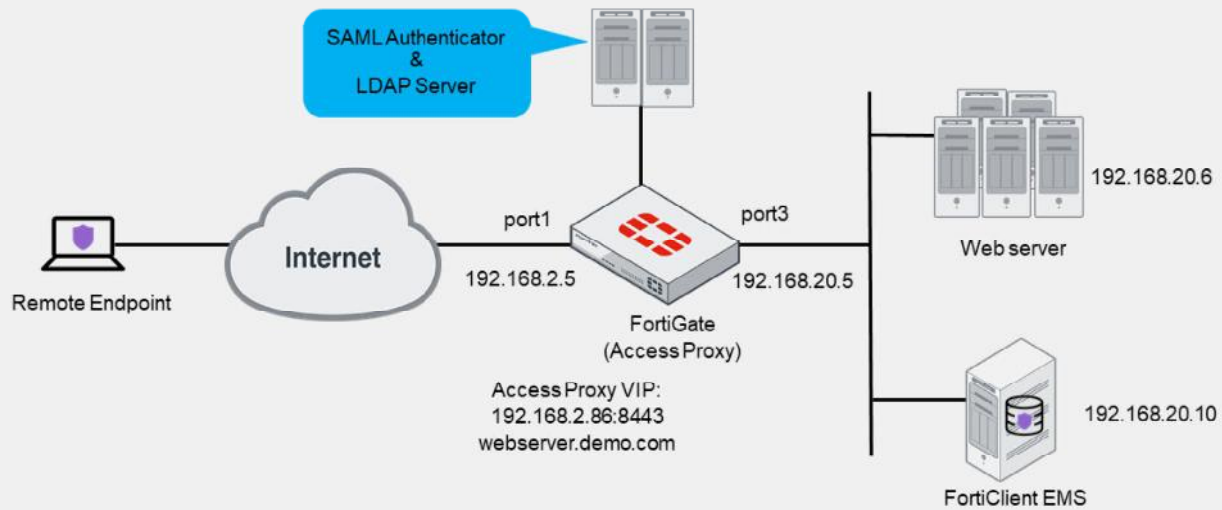
The authentication rule defines the proxy sources and destinations that require authentication, and which authentication scheme to apply. ZTNA supports the active authentication method. The active authentication method references a scheme where users are actively prompted for authentication, as they are with basic authentication. After the authentication rule triggers the method to authenticate the user, a successful authentication returns the groups that the user belongs to.

In the ZTNA rule and proxy policy, you can define a user or user group as the allowed source. Only users that match that user or group are allowed through the proxy policy. This slide shows the ZTNA rule example that user group **ZTNAaccess_group** was added to the authentication configuration after the authentication scheme and authentication rule were added to FortiGate.

DO NOT REPRINT
© FORTINET

ZTNA HTTPS Access Proxy With SAML Authentication

- SAML authentication



Fortinet
NSE Training Institute

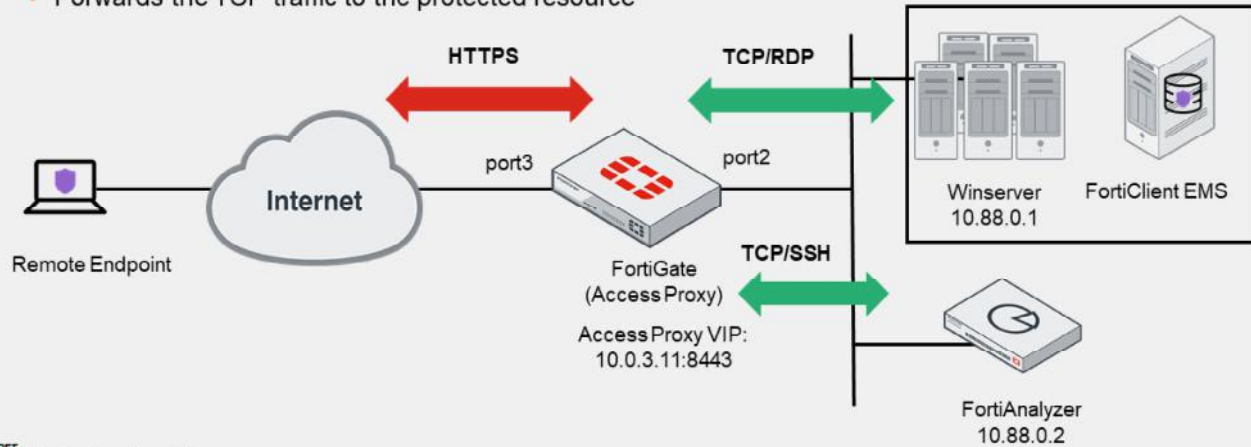
© Fortinet Inc. All Rights Reserved.

29

You can also apply the SAML authentication method to authenticate the client. The FortiGate acts as the SAML SP, and a SAML authenticator serves as the IdP. In addition to verifying the user and device identity with the client certificate, the user is also authorized, based on user credentials, to establish a trust context before granting access to the protected resource. For configuration details, refer to the *FortiOS 7.0.1 Administration Guide*.

ZTNA TCP Forwarding Access Proxy

- TCP forwarding access proxy demonstrates an HTTPS reverse proxy that forwards TCP traffic to the resource
- TCP forwarding access proxy:
 - Tunnels TCP traffic between the client and FortiGate over HTTPS
 - Forwards the TCP traffic to the protected resource



Fortinet
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

30

In the example shown on this slide, a TCP forwarding access proxy (TFAP) is configured to demonstrate an HTTPS reverse proxy that forwards TCP traffic to the designated resource. The access proxy tunnels TCP traffic between the client and FortiGate over HTTPS, and forwards the TCP traffic to the protected resource. It verifies user identity, device identity, and trust context, before granting access to the protected source.

RDP access is configured to Winserver, and SSH access to the FortiAnalyzer. The topology shown on this slide uses IP address 10.0.3.11 and port-8443 for the external access proxy VIP.

You can also add authentication and a security posture check for TCP Forwarding Access Proxy, which you learned about earlier in this lesson.

ZTNA TCP Forwarding Access Proxy (Contd)

- To configure access proxy VIP and server mappings from the FortiGate CLI

```

config firewall vip
    edit "ZTNA-tcp-server"
        set type access-proxy
        set extip 10.0.3.11
        set extintf "port3"
        set server-type https
        set extport 8443
        set ssl-certificate "Fortinet_SSL"
    next
end

config firewall access-proxy
    edit "ZTNA-tcp-server"
        set vip "ZTNA-tcp-server"
        set client-cert enable
        config api-gateway
            edit 1
                set service tcp-forwarding
                config realservers
                    edit 1
                        set address "FAZ"
                        set mappedport 22
                    next
                    edit 2
                        set address "winserver"
                        set mappedport 3389
                    end
                end
            end
        end
    end
end
  
```

Access Proxy VIP (points to the first configuration block)

Real server address and port mapping (points to the `edit 1` and `edit 2` sections in the second configuration block)

The topology shown on this slide uses IP address 10.0.3.11 and port-8443 for the external access proxy VIP. Currently, FortiOS 7.0.0 does not fully support TCP forwarding access proxy configurations done on the GUI. Therefore, you must configure the access proxy on the CLI. After you create the access proxy VIP, you can view it on the GUI but you cannot make changes to it on the GUI.

This slide shows how to configure the access proxy VIP and access proxy server mappings using the CLI. The RDP and SSH ports and real server IP addresses are already mapped. The mapped port restricts the mapping to the specified port or port range. If `mapped port` is not specified, then any port is matched. The mapped addresses must be address objects. Therefore, you can use the preexisting FortiAnalyzer and Winserver addresses. You must create an address object before configuring the proxy VIP.

ZTNA TCP Forwarding Access Proxy (Contd)

Policy & Objects > ZTNA > ZTNA Rules

New ZTNA Rule

Name: ZTNA-TCP

Source: all

ZTNA Tag: +

ZTNA Server: ZTNA-tcp-server

Action: ☒ ACCEPT ☐ DENY

Security Profiles

AntiVirus: ☐

Web Filter: ☐

Video Filter: ☐

Application Control: ☐

IPS: ☐

File Filter: ☐

SSL Inspection: no-inspection

Logging Options

Log Allowed Traffic: ☒ Security Events ☒ All Sessions

Comments: Write a comment... 0/1023

Enable this policy: ☒

OK Cancel

Policy & Objects > Firewall Policy

New Policy

Name: ZTNA-TCP

ZTNA: ☒ Full ZTNA (IP/MAC filtering)

Incoming Interface: WAN (port3)

Source: all

ZTNA Server: ZTNA-tcp-server

Schedule: always

Service: ALL

Action: ☒ ACCEPT ☐ DENY

Firewall / Network Options

NAT: ☐

Logging Options

Log Allowed Traffic: ☒

Generate Logs when Session Starts: ☐

Comments: Write a comment... 0/1023

Enable this policy: ☒

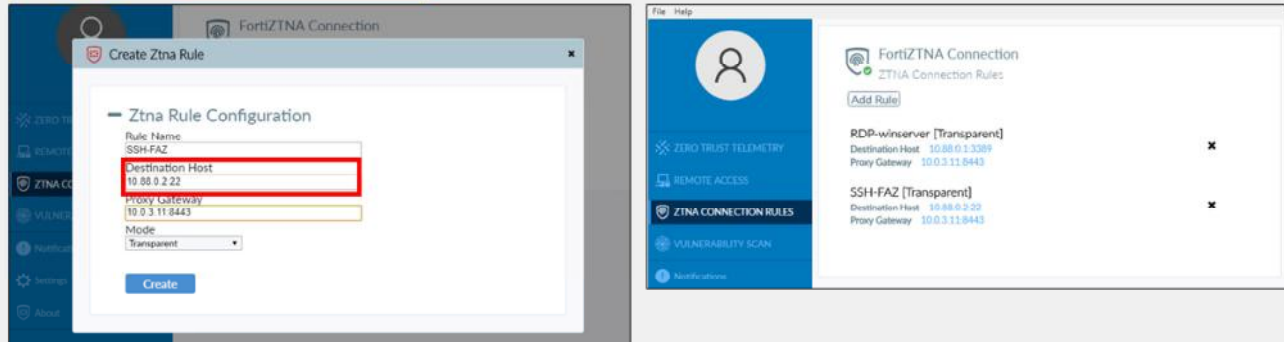
OK Cancel

Next, you configure a ZTNA rule for access control and a firewall policy for full ZTNA function. This slide shows the ZTNA rule and firewall policy for the example topology.

ZTNA TCP Forwarding Access Proxy (Contd)

- User must create a ZTNA rule on the FortiClient to connect

ZTNA CONNECTION RULES > Add Rule



- You can also configure ZTNA TCP forwarding access proxy without encryption
 - Improves performance by reducing encryption overhead of an already secure underlying protocol
 - Do not use for insecure protocols

Before connecting, users must create a ZTNA rule on FortiClient. Currently, ZTNA Connection Rule configuration from FortiClient EMS is not available in 7.0.0. You must configure them manually on FortiClient to connect.

Note that your **Destination Host** is the real internal IP address and port of the server. The RDP and SSH connections securely proxied through the gateway.

You can also configure a ZTNA TCP forwarding access proxy without encryption. The connection still begins with a TLS handshake. The client uses the HTTP 101 response to switch protocols and remove the HTTPS stack. Further end-to-end communication between the client and server are encapsulated in the specified TCP port, but not encrypted by the access proxy. This improves performance by reducing the overhead of encrypting an already secured underlying protocol, such as RDP, SSH, or FTPS. Users should still enable the encryption option for end-to-end protocols that are insecure. In a real-life application, you should use the encryption option for an insecure protocol such as Telnet.

ZTNA IP MAC Filtering

- When you enable ZTNA on FortiGate, the firewall policy provides two options:
 - Full ZTNA
 - IP/MAC filtering
- ZTNA IP/MAC filtering mode enhances security when endpoints are physically on the corporate network
 - Use ZTNA tags to control access
- Full ZTNA mode focuses on access for remote users

ZTNA IP/MAC filtering Firewall Policy

The screenshot shows the configuration for a firewall policy named 'Block-Malicious'. The 'ZTNA' section is enabled, and 'IP/MAC filtering' is selected. The 'ZTNA Tag' is set to 'Malicious-File-Detected'. The 'Incoming Interface' is 'LAN (port3)' and the 'Outgoing Interface' is 'port1'. The 'Source' is set to 'all' and the 'Destination' is set to 'all'. The 'Schedule' is 'always' and the 'Service' is 'ALL'. The 'Action' is set to 'DENY'. The 'Log Violation Traffic' checkbox is checked. The 'Comments' field is empty, and the '0/1023' character count is shown.

When you enable ZTNA on FortiGate, the firewall policy provides two options:

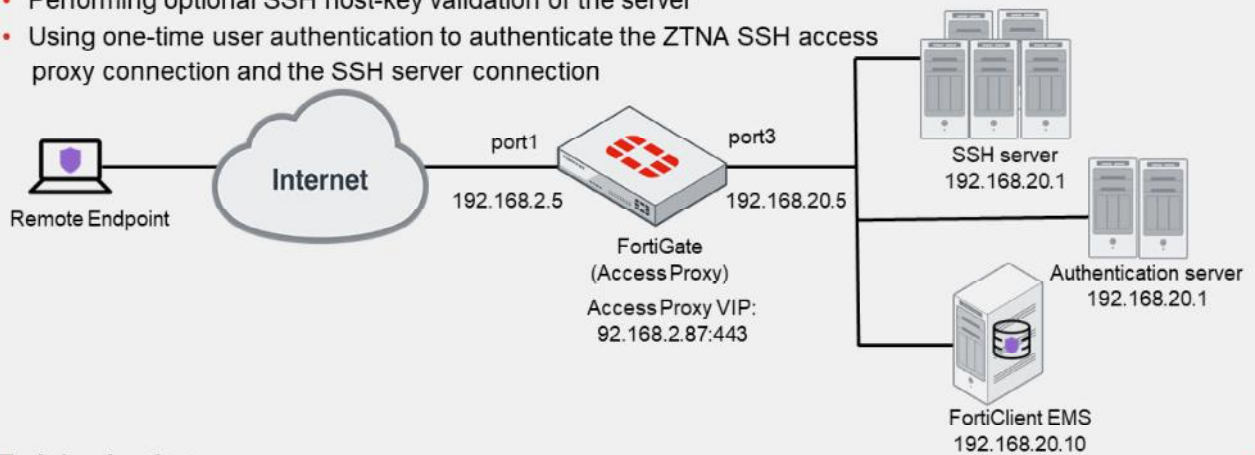
- Full ZTNA
- IP/MAC filtering

ZTNA IP/MAC filtering mode enhances security when endpoints are physically located on the corporate network, whereas full ZTNA mode focuses on access for remote users. ZTNA IP/MAC filtering mode uses ZTNA tags to control access between on-fabric devices and an internal web server or internet. This mode does not require the use of the access proxy, and uses only ZTNA tags for access control.

The example firewall policy on this slide uses the existing **Malicious-File-Detected** tag to control access. Traffic is denied to internet when the FortiClient endpoint is tagged with **Malicious-File-Detected**.

ZTNA SSH Access Proxy

- ZTNA supports SSH access proxy to provide seamless SSH connection
- Advantages over TCP forwarding access proxy:
 - Establishing device trust context with user identity and device identity checks
 - Applying SSH deep inspection to the traffic through the SSH related profile
 - Performing optional SSH host-key validation of the server
 - Using one-time user authentication to authenticate the ZTNA SSH access proxy connection and the SSH server connection



Fortinet
NSE Training Institute

© Fortinet Inc. All Rights Reserved.

35

You can configure ZTNA with an SSH access proxy to provide a seamless SSH connection to the server.

Advantages of using an SSH access proxy instead of a TCP forwarding access proxy include:

- Establishing device trust context with user identity and device identity checks
- Applying SSH deep inspection to the traffic through the SSH related profile
- Performing optional SSH host-key validation of the server
- Using one-time user authentication to authenticate the ZTNA SSH access proxy connection and the SSH server connection

To act as a reverse proxy for the SSH server, FortiGate must perform SSH host-key validation to verify the identity of the SSH server. FortiGate does this by storing the public key of the SSH server in its SSH host-key configurations. When endpoint makes a connection to the SSH server, if the public key matches one that is used by the server, then the connection is established. If there is no match, then the connection fails.

ZTNA SSH Access Proxy (Contd)

- One-time user authentication:
 1. The remote endpoint registers FortiClient EMS and receives the client certificate.
 2. The remote endpoint tries to connect to the SSH access proxy. It must use the same username that is later used for access proxy authentication.
 3. FortiGate challenges the endpoint with device identity validation.
 4. The remote endpoint provides the FortiClient EMS issued certificate for device identification.
 5. FortiGate challenges the endpoint with user authentication. For example, FortiGate could do this using basic or SAML authentication.
 6. The user enters their credentials on the remote endpoint.
 7. FortiGate authenticates the user and collects the username.
 8. Using the FortiGate CA or the customer CA certificate, FortiGate signs an SSH certificate and embeds the username in its principal.
 9. FortiGate attempts to connect to the SSH server using the certificate authentication.
 10. The SSH server verifies the authenticity of the certificate, and matches the username principal against its authorized_keys file.
 11. If the username matches a record in the file, then the SSH connection is established. If no match is found, then the SSH connection fails.

The SSH access proxy allows user authentication to occur between the client and the access proxy, while using the same user credentials to authenticate with the SSH server. The steps on this slide explains how this works.

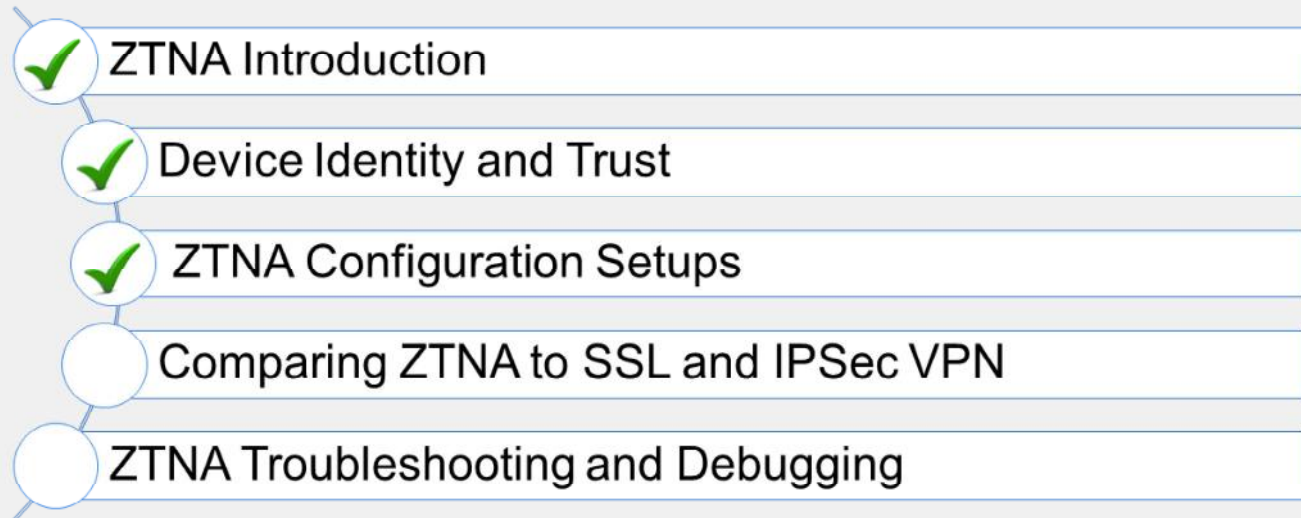
DO NOT REPRINT
© FORTINET

Knowledge Check

1. Which access proxy configuration forwards only TCP traffic?
☒ A. TCP forwarding access proxy
☐ B. HTTPS access proxy

2. Which access proxy configuration supports one-time user authentication?
☐ A. TCP forwarding access proxy
☒ B. SSH access proxy

Lesson Progress



Good job! You now know about different ZTNA configuration setups.

Now, you will compare ZTNA to SSL and IPsec VPN.

Comparing ZTNA to SSL and IPSec VPN

Objectives

- Understand the evolution of teleworker remote access with ZTNA

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in understanding the evolution of remote access with ZTNA, you will be able to migrate from VPN to ZTNA HTTPS access proxy.

Comparing SSL VPN, IPsec VPN, and ZTNA Access

	IPsec VPN	SSL VPN	ZTNA
Tunnel type:	IPsec tunnel only	Session-based OR tunnel	Session-based only
Configured between:	FortiClient and FortiGate FortiGate and FortiGate FortiGate and compatible third-party IPsec VPN gateway FortiGate and compatible third-party IPsec VPN clients	Browser and FortiGate FortiClient and FortiGate FortiGate (SSL Client) and FortiGate (SSL Server)	Browser and FortiGate FortiClient and FortiGate (TCP forwarding access)
Log in through:	IPsec client	HTTPS web page on FortiGate FortiClient FortiGate (SSL Client)	HTTPS hostname or IP and port number FortiClient (TCP forwarding access)

How are SSL VPN and ZTNA access different from IPsec VPNs?

SSL and TLS are commonly used to encapsulate and secure e-commerce and online banking on the internet (HTTP). SSL VPNs and ZTNA use a similar technique, and support non-HTTP protocol encapsulation as well. SSL resides higher up on the network stack than IP and, therefore, it usually requires more bits—more bandwidth—for SSL VPN headers. In comparison, IPsec uses some different methods to provide confidentiality and integrity. The primary protocol used in IPsec is ESP, which encapsulates and encrypts UDP, RDP, HTTP, or other protocols inside the IPsec tunnel.

IPsec is also an industry-standard protocol that can work with multiple vendors and supports peers that are devices and gateways—not just user clients with FortiGate only, like SSL VPN or ZTNA does.

The client software is also different. In an SSL VPN or ZTNA, your web browser might be the only client software you need. You can go to the FortiGate SSL VPN portal (an HTTPS web page) and then log in. Alternatively, you can install FortiClient or configure FortiGate as an SSL VPN client. In comparison, to use IPsec VPN, install special client software or have a local gateway, such as a desktop model FortiGate, to connect to the remote gateway. You might also need to configure firewalls between VPN peers to allow IPsec protocols.

Comparing SSL VPN, IPsec VPN, and ZTNA Access (Contd)

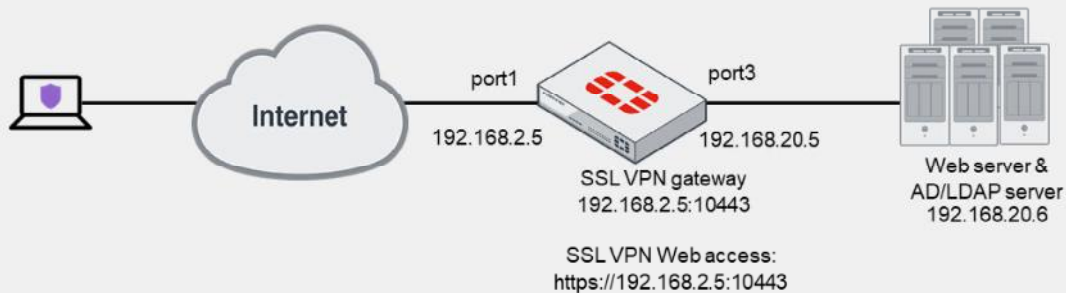
	IPsec VPN	SSL VPN	ZTNA
Category:	Industry standard	Vendor specific	Vendor specific
Configuration:	- Requires installation - Flexible setup - Mesh and star topologies - For clients or peer gateways - Performance based: IPsec encryption is faster in FortiOS	- Does not require installation - Simpler setup - Only client-to-FortiGate - No user-configured settings - Technical support less requested	- Does not require installation - Simpler setup - Only client-to-FortiGate - No user-configured settings - Technical support less requested
Better for:	Office-to-office traffic Data centers	Provides flexibility tunnel-mode or session-based access	Session-based access only

After you logged in, the SSL VPN connects your computer to your private network. No user-configured settings are required, and firewalls are typically configured to allow outgoing HTTP, so technical support calls are less likely. Simplicity makes ZTNA and SSL VPN ideal for non-technical users, or users who connect from public computers, such as those found in public libraries and internet cafés. ZTNA takes this a step further and makes it easier for administrators to perform device compliance checks and configuration. ZTNA also provides an additional authentication mechanism for access control without any interaction required from the end user.

In general, IPsec VPN is preferred when tunnels must be up continuously and interoperate with many types of devices, while SSL VPN is preferred when people travel and need to connect to the office.

Moving to ZTNA From SSL VPN

- You can migrate teleworking configurations that use SSL VPN tunnel or web portal mode access to ZTNA with HTTPS access proxy



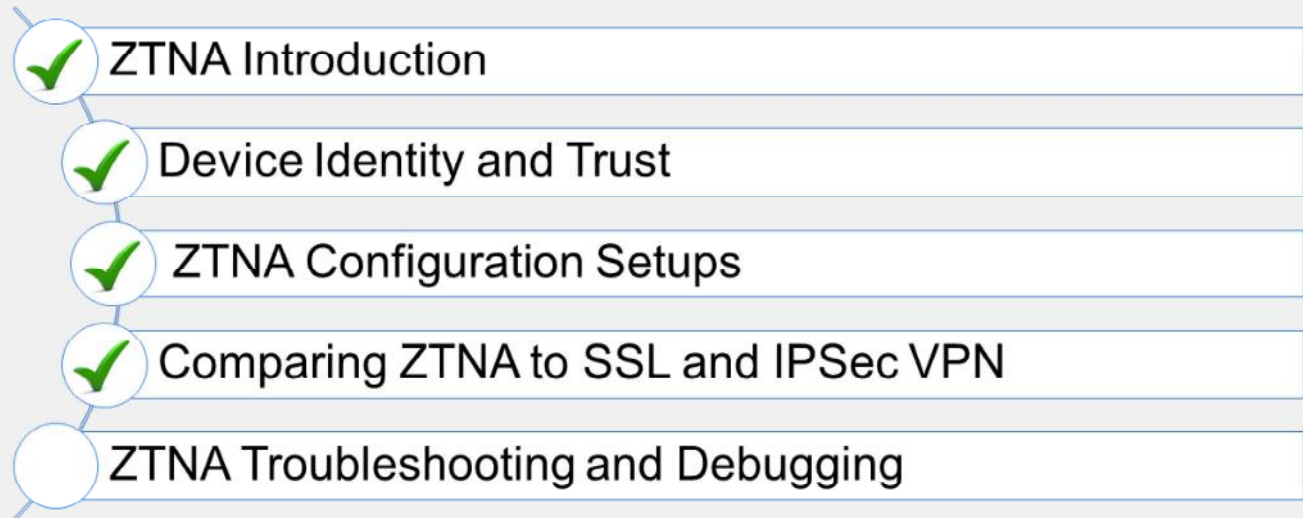
You can use ZTNA to replace VPN-based teleworking solutions. The example on this slide shows that you can migrate teleworking configurations that use SSL VPN tunnel or web portal mode access to ZTNA with HTTPS access proxy, and continue to use the same authentication server and groups to authenticate your remote users.

In addition, by integrating with FortiClient EMS, you can also ensure that FortiGate performs device identification is using client certificates, and checks the security posture before allowing the remote user into the website. This provides granular control over who can access the web resource using role-based access control. It also gives the user transparent access to the website using only their browser. You can even configure ZTNA IP/MAC filtering mode for on-fabric devices to provide similar access control while users are on the network.

Knowledge Check

1. Which remote access solution proxies HTTP and TCP over a secure HTTPS connection?
✓ A. ZTNA
B. IPSec
2. What does FortiClient EMS integration ensure?
✓ A. Device identification
B. User identification

Lesson Progress



Good job! You now understand the evolution of teleworker remote access with ZTNA

Now, you will learn how to troubleshoot and debug ZTNA configuration issues.

DO NOT REPRINT
© FORTINET

ZTNA Troubleshooting and Debugging

Objectives

- Troubleshoot and debug ZTNA issues

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in troubleshooting and debugging ZTNA issues, you will be able to solve ZTNA issues between FortiGate and FortiClient EMS.

ZTNA Troubleshooting and Debugging

- Use these CLI commands to troubleshoot ZTNA issues on FortiGate:

Command	Description
<code>diagnose endpoint fctems test connectivity <EMS name></code>	Verify FortiGate to FortiClient EMS connectivity
<code>execute fctems verify <EMS name></code>	Verify the FortiClient EMS certificate
<code>diagnose test application fcnacd 2</code>	Dump the EMS connectivity information
<code>diagnose debug app fcnacd -1</code> <code>diagnose debug enable</code>	Run real-time FortiClient NAC daemon debugs
<code>diagnose endpoint record list <ip></code>	Show the endpoint record list. Optionally, filter by the endpoint IP address
<code>diagnose endpoint wad-comm find-by uid <uid></code>	Query endpoints by client UID
<code>diagnose endpoint wad-comm find-by ip-vdom <ip> <vdom></code>	Query endpoints by the client IP-VDOM pair
<code>diagnose wad dev query-by uid <uid></code>	Query from WAD diagnose command by UID
<code>diagnose wad dev query-by ipv4 <ip></code>	Query from WAD diagnose command by IP address

The table on this slide shows the debug CLI commands that you can use to troubleshoot ZTNA on FortiGate.

ZTNA Troubleshooting and Debugging (Contd)

Command	Description
<code>diagnose firewall dynamic list</code>	List EMS ZTNA tags and all dynamic IP and MAC addresses
<code>diagnose test application fcnacd 7</code> <code>diagnose test application fcnacd 8</code>	Check the FortiClient NAC daemon ZTNA and route cache
<code>diagnose wad debug enable category all</code> <code>diagnose wad debug enable level verbose</code> <code>diagnose debug enable</code>	Run real-time WAD debugs
<code>diagnose debug reset</code>	Reset debugs when completed

- WAD daemon handles proxy
- FortiClient NAC daemon (fcnacd) handles connectivity between FortiGate and FortiClient EMS

This slide is the continuation of the CLI command table.

Note that the WAD daemon handles proxy-related processing, and the FortiClient NAC daemon (fcnacd) handles connectivity between FortiGate to FortiClient EMS. The next slides show the CLI command use and output.

ZTNA Troubleshooting and Debugging (Contd)

- To verify FortiGate to FortiClient EMS connectivity and EMS certificate:

```
# diagnose endpoint fctems test-connectivity WIN10-EMS
Connection test was successful:
```

Verifying connection
between FortiGate and
FortiClient EMS

```
# execute fctems verify WIN10-EMS
Server certificate already verified
```

Verifying FortiClient EMS
server certificate

```
# diagnose test application fcnacd 2
EMS context status:
FortiClient EMS number 1:
    name: WIN10-EMS confirmed: yes
    fetched-serial-number: FCTEMS0000109188
Websocket status: connected
```

Shows FortiClient EMS
connectivity information

- If `fcnacd` does not report correct status, run real-time debugs:

```
# diagnose debug application fcnacd -1
# diagnose debug enable
```

On this slide, the `diagnose endpoint fctems test-connectivity` command shows that the connection between FortiGate and FortiClient EMS is successful. The `execute fctems verify` command shows that the server certificate is verified with FortiGate, and the `diagnose test application fcnacd 2` command dumps the FortiClient EMS connectivity information.

If `fcnacd` does not report the correct status, run real-time `fcnacd` debugs by running the following CLI commands:

```
# diagnose debug application fcnacd -1
# diagnose debug enable
```

ZTNA Troubleshooting and Debugging (Contd)

- To verify information about an endpoint:

```
# diagnose endpoint record list 10.6.30.214
Record #1:
    IP Address = 10.6.30.214
    MAC Address = 00:0c:29:ba:1e:61
    MAC list = 00:0c:29:ba:1e:61;00:0c:29:ba:1e:6b;
    VDCM = root (0)
    EMS serial number: FCTEMS8821001322
    Client cert SN: 17FF6595600A1AF53B87627AB4EBEDD032593E64
    Quarantined: no
    Online status: online
    Registration status: registered
    On-net status: on-net
    Gateway Interface: port2
    FortiClient version: 7.0.0
    AVDB version: 84.778
    FortiClient app signature version: 18.43
    FortiClient vulnerability scan engine version: 2.30
    FortiClient UID: 5FCFA3ECDE4D478C911D9232EC9299FD
    Host Name: ADPC
    ...
    Number of Routes: (1)
        Gateway Route #0:
            - IP:10.1.100.214, MAC: 00:0c:29:ba:1e:6b,
            - Interface:port2, VFID:0, SN: FG5H1E5819902474
    Indirect: no
    online records: 1; offline records: 0; quarantined records: 0
```

The CLI command
output

On this slide, the `diagnose endpoint record list <IP address>` command shows the network, registration, client certificate, and device information. It also shows the vulnerability status and position relative to FortiGate. This command without an IP filter shows all the endpoint records that are connected to FortiClient EMS and synced with FortiGate.

ZTNA Troubleshooting and Debugging (Contd)

- To query endpoint information, including ZTNA tags, by UID or IP address:

```
# diagnose endpoint wad-comm find-by uid 5FCFA3ECDE4D478C911D9232EC9299FD
UID: 5FCFA3ECDE4D478C911D9232EC9299FD
status code:ok
Domain: qa.wangd.com
User: user1
Cert SN:17FF6595600A1AF53B87627AB4EBEDD032593E64
EMS SN: FCTEMS8821001322
Routes(1):
- route[0]: IP=10.1.100.214, VDom=root
Tags(3):
- tag[0]: name=ZT_OS_WIN
- tag[1]: name=all_registered_clients
- tag[2]: name=Medium

# diagnose endpoint wad-comm find-by ip-vdom 10.1.100.214 root
UID: 5FCFA3ECDE4D478C911D9232EC9299FD
status code:ok
Domain: qa.wangd.com
User: user1
Cert SN:17FF6595600A1AF53B87627AB4EBEDD032593E64
EMS SN: FCTEMS8821001322
Routes(1):
- route[0]: IP=10.1.100.214, VDom=root
Tags(3):
- tag[0]: name=ZT_OS_WIN
- tag[1]: name=all_registered_clients
- tag[2]: name=Medium
```

The CLI command
includes ZTNA tags

Use the `diagnose endpoint wad-comm find-by uid` or `ip-vdom` pair command is used to query endpoint information that includes ZTNA tags. The CLI output on this slide shows that specific endpoint has 3 ZTNA tags named `ZT_OS_WIN`, `all_registered_clients`, and `Medium`.

ZTNA Troubleshooting and Debugging (Contd)

- To query an endpoint information from WAD daemon by UID or IP address:

```
# diagnose wad dev query-by uid 5FCFA3ECDE4D478C911D9232EC9299FD
Attr of type=0, length=32, value(ascii)=5FCFA3ECDE4D478C911D9232EC9299FD
Attr of type=4, length=30, value(ascii)=MAC_FCTEMS8821001322_ZT_OS_WIN
Attr of type=4, length=26, value(ascii)=FCTEMS8821001322_ZT_OS_WIN
Attr of type=4, length=43, value(ascii)=MAC_FCTEMS8821001322_all_registered_clients
Attr of type=4, length=39, value(ascii)=FCTEMS8821001322_all_registered_clients
Attr of type=4, length=27, value(ascii)=MAC_FCTEMS8821001322_Medium
Attr of type=4, length=23, value(ascii)=FCTEMS8821001322_Medium
Attr of type=5, length=18, value(ascii)=FOSQA@qa.wangd.com
Attr of type=6, length=40, value(ascii)=17FF6595600A1AF53B87627AB4EBEDD032593E64

# diagnose wad dev query-by ipv4 10.1.100.214
Attr of type=0, length=32, value(ascii)=5FCFA3ECDE4D478C911D9232EC9299FD
Attr of type=4, length=30, value(ascii)=MAC_FCTEMS8821001322_ZT_OS_WIN
Attr of type=4, length=26, value(ascii)=FCTEMS8821001322_ZT_OS_WIN
Attr of type=4, length=43, value(ascii)=MAC_FCTEMS8821001322_all_registered_clients
Attr of type=4, length=39, value(ascii)=FCTEMS8821001322_all_registered_clients
Attr of type=4, length=27, value(ascii)=MAC_FCTEMS8821001322_Medium
Attr of type=4, length=23, value(ascii)=FCTEMS8821001322_Medium
Attr of type=5, length=18, value(ascii)=FOSQA@qa.wangd.com
Attr of type=6, length=40, value(ascii)=17FF6595600A1AF53B87627AB4EBEDD032593E64
```

Endpoint information
from WAD daemon

The `diagnose endpoint wad dev query-by uid` or `ipv4` command provides endpoint information from the FortiGate WAD daemon. The WAD daemon handles processing related to proxy (access proxy), which you learned about earlier.

ZTNA Troubleshooting and Debugging (Contd)

- To list all the dynamic ZTNA IP and MAC addresses learned from EMS:

```
# diagnose firewall dynamic list
List all dynamic addresses:
FCTEMS0000109188_all_registered_clients: ID(51)
  ADDR(172.17.194.209)
  ADDR(192.168.40.8)
...
FCTEMS0000109188_Low: ID(78)
  ADDR(172.17.194.209)
  ADDR(192.168.40.8)
...
FCTEMS0000109188_Malicious-File-Detected: ID(190)
  ADDR(172.17.194.209)
  ADDR(192.168.40.8)

MAC dynamic addresses in VDOM root(vfid: 0):

MAC_FCTEMS0000101875_Low(total-addr: 5): ID(377)
  MAC(00:50:56:A1:8A:21)
  MAC(00:50:56:A1:1B:15)

MAC_FCTEMS0000101875_all_registered_clients(total-addr: 5): ID(94)
  MAC(00:50:56:A1:8A:21)
  MAC(00:50:56:A1:1B:15)
```

Dynamic address and
MAC addresses

The `diagnose firewall dynamic list` command shows all the dynamic ZTNA IP and MAC addresses learned from EMS.

ZTNA Troubleshooting and Debugging (Contd)

- To check the FortiClient NAC daemon ZTNA and route cache:

```
# diagnose test application fcnacd 7
```

ZTNA Cache:

```
-uid 5FCFA3ECDE4D478C911D9232EC9299FD: { "tags": [ "ZT_OS_WIN",  
"all_registered_clients", "Medium" ], "domain": "qa.wangd.com", "user_name":  
"user1", "client_cert_sn": "17FF6595600A1AF53B87627AB4EBEDD032593E64", "owner":  
"FOSQA@qa.wangd.com", "gateway_route_list": [ { "gateway_info": { "fgt_sn":  
"FG5H1E5819902474", "interface": "port2", "vdom": "root" }, "route_info": [ {  
"ip": "10.1.100.214", "mac": "00-0c-29-ba-1e-6b", "route_type": "direct" } ] }  
], "ems_sn": "FCTEMS8821001322" }
```

Shows ZTNA cache

```
# diagnose test application fcnacd 8
```

IP-VfID Cache:

```
IP: 10.1.100.206, vfid: 0, uid: 3DED29B54386416E9888F2DCBD2B9D21  
IP: 10.1.100.214, vfid: 0, uid: 5FCFA3ECDE4D478C911D9232EC9299FD
```

Shows route cache

- Use the following commands to troubleshoot WAD with real-time debugs:

```
# diagnose wad debug enable category all  
# diagnose wad debug enable level verbose  
# diagnose debug enable
```

Use the `diagnose test application fcnacd 7` or `8` command shown on this slide to check endpoint ZTNA and route cache. The WAD commands on this slide is used to troubleshoot WAD with real-time debugs, to understand how the proxy handled a client request.

Note that you should always reset the debugs after using them by running, `diagnose debug reset` command.

ZTNA Logging Enhancements

- The ZTNA log subtype is added to UTM logs and a traffic log ID is added for ZTNA related traffic
- There are six events that generate logs:

Traffic log example of the empty certificate that is disallowed or block:

```
date=xxxx-xx-xx time=16:36:54 eventtime=1623281814371412983 tz="-0700" logid="0000000013" type="traffic"
subtype="forward" level="notice" vd="root" srcip=10.1.100.206 srcport=56494 srcintf="port2" srcintfrole="undefined"
dstip=172.18.62.112 dstport=443 dstintf="root" dstintfrole="undefined" srccountry="Reserved" dstcountry="Reserved"
sessionid=21453 proto=6 action="deny" policyid=5 policytype="policy" poluid="b4d4c466-8b64-51eb-2292-
5defbb0e34e5" policyname="ztna" service="HTTPS"trandisp="noop" duration=0 sentbyte=0 rcvdbyte=0 sentpkt=0
rcvdpkt=0 appcat="unscanned" utmaction="block" countztna=1 msg="Denied: empty client certificate"
utmref=65483-0
```

UTM log example of the empty certificate that is disallowed or block:

```
date=xxxx-xx-xx time=16:36:54 eventtime=1623281814371409480 tz="-0700" logid="2100060500" type="utm"
subtype="ztna" eventtype="ztna-clt-cert" level="warning" vd="root" msg="Client sends an empty certificate"
policyid=5 sessionid=21453 srcip=10.1.100.206 dstip=172.18.62.112 srcport=56494 dstport=443 srcintf="port2"
srcintfrole="undefined" dstintf="root" dstintfrole="undefined" proto=6 action="blocked" service="HTTPS" vip="zv2"
accessproxy="zs2"
```

The ZTNA log subtype is added to UTM logs, and a traffic log ID is added for ZTNA-related traffic. There are six events that generate logs in the subtype:

1. Received an empty client certificate
2. Received a client certificate that fails to validate
3. API gateway cannot be matched
4. None of the real servers can be reached
5. ZTNA rule (proxy policy) cannot be matched
6. HTTPS SNI virtual host does not match the HTTP host header

ZTNA-related traffic generates logs when you enable logging for allowed traffic in the policy. This slide shows the UTM and traffic logs that are generated when FortiGate connects to the ZTNA access proxy. The client did not send a client certificate to FortiGate for verification. FortiGate disallows and blocks the empty certificate.

ZTNA Logging Enhancements (Contd)

- Received client certificate that fails to validate:

Traffic log example of the client certificate that fails to validate:

```
date=xxxx-xx-xx time=15:06:47 eventtime=1623276407372012365 tz="-0700" logid="0000000013" type="traffic"
subtype="forward" level="notice" vd="root" srcip=10.1.100.206 srcport=55910 srcintf="port2" srcintfrole="undefined"
dstip=172.18.62.112 dstport=443 dstintf="root" dstintfrole="undefined" srccountry="Reserved" dstcountry="Reserved"
sessionid=16810 proto=6 action="deny" policyid=5 policytype="policy" poluid="b4d4c466-8b64-51eb-2292-5defbb0e34e5"
policyname="ztna" service="HTTPS"trandisp="noop" duration=0 sentbyte=0 rcvdbyte=0 sentpkt=0 rcvpkt=0
appcat="unscanned" utmaction="block" countztna=1 msg="Denied: client certificate authentication failed"
utmref=65491-0
```

UTM log example of the client certificate that fails to validate:

```
date=xxxx-xx-xx time=15:06:47 eventtime=1623276407372009447 tz="-0700" logid="2100060501" type="utm"
subtype="ztna" eventtype="ztna-clt-cert" level="warning" vd="root" msg="Client certificate has security problem"
policyid=5 sessionid=16810 srcip=10.1.100.206 dstip=172.18.62.112 srcport=55910 dstport=443 srcintf="port2"
srcintfrole="undefined" dstintf="root" dstintfrole="undefined" proto=6 action="blocked" service="HTTPS" vip="zv2"
accessproxy="zs2" desc="cert auth failed, cert-cn:qa.wangd.com, cert-issuer:qa.wangd.com, cert-status:failure "
```

This slide shows the UTM and traffic logs that are generated when FortiGate connects to the ZTNA access proxy. The client sends a client certificate to FortiGate for verification, but the certificate fails validation.

ZTNA Logging Enhancements (Contd)

- API gateway cannot be matched or real servers cannot be reached:

Traffic log example when API gateway or real server doesn't match:

```
date=xxxx-xx-xx time=15:15:39 eventtime=1623276939601851410 tz="-0700" logid="0000000013" type="traffic"
subtype="forward" level="notice" vd="root" srcip=10.1.100.206 srcport=55974 srcintf="port2" srcintfrole="undefined"
dstip=172.18.62.112 dstport=443 dstintf="root" dstintfrole="undefined" srccountry="Reserved" dstcountry="Reserved"
sessionid=17152 proto=6 action="deny" policyid=5 policytype="policy" poluid="b4d4c466-8b64-51eb-2292-5defbb0e34e5"
policyname="ztna" service="HTTPS"trandisp="noop" duration=0 sentbyte=0 rcvdbyte=0 sentpkt=0 rcvdpkt=0
appcat="unscanned" utmaction="block" countztna=2 msg="Denied: failed to match an API-gateway" utmref=65490-0
```

UTM log example when API gateway or real server doesn't match:

```
date=xxxx-xx-xx time=15:15:39 eventtime=1623276939601849940 tz="-0700" logid="2102060522" type="utm"
subtype="ztna" eventtype="ztna-error" level="warning" vd="root" msg="Unable to match an API-gateway" policyid=5
sessionid=17152 srcip=10.1.100.206 dstip=172.18.62.112 srcport=55974 dstport=443 srcintf="port2" srcintfrole="undefined"
dstintf="root" dstintfrole="undefined" proto=6 action="blocked" service="HTTPS" vip="zv2" accessproxy="zs2" desc="HTTP
url (https://qbcd.test.com/test123456) failed to match an API-gateway with
vhost(name/hostname:_def_virtual_host/_def_virtual_host)""
```

This slide shows the UTM and traffic logs that are generated when FortiGate connects to the ZTNA access proxy. The client tries to connect to an API gateway that does not match any virtual host, or the real server cannot be reached.

ZTNA Logging Enhancements (Contd)

- ZTNA rule (proxy policy) cannot be matched:

Traffic log example when unable to match ZTNA rule (proxy policy):

```
date=xxxx-xx-xx time=15:20:20 eventtime=1623277220133106783 tz="-0700" logid="0000000013" type="traffic"
subtype="forward" level="notice" vd="root" srcip=10.1.100.206 srcport=56010 srcintf="port2" srcintfrole="undefined"
dstip=172.18.62.112 dstport=443 dstintf="root" dstintfrole="undefined" srccountry="Reserved" dstcountry="Reserved"
sessionid=17456 proto=6 action="deny" policyid=0 policytype="proxy-policy" service="HTTPS"trandisp="noop" duration=0
sentbyte=0 rcvdbyte=0 sentpkt=0 rcvdpkt=0 appcat="unscanned" utmaction="block" countztna=2 msg="Denied: failed to
match a proxy-policy" utmref=65488-26
```

UTM log example when unable to match ZTNA rule (proxy policy):

```
date=xxxx-xx-xx time=15:20:20 eventtime=1623277220133105204 tz="-0700" logid="2101060510" type="utm"
subtype="ztna" eventtype="ztna-policy-match" level="warning" vd="root" msg="Connection is blocked due to unable
to match a proxy-policy" policyid=0 sessionid=17456 srcip=10.1.100.206 dstip=172.18.62.112 srcport=56010 dstport=443
srcintf="port2" srcintfrole="undefined" dstintf="root" dstintfrole="undefined" proto=6 action="blocked" service="HTTPS"
gatewayid=1 vip="zv2" accessproxy="zs2"
```

This slide shows the UTM and traffic logs that are generated when FortiGate connects to the ZTNA access proxy but is unable to match the ZTNA rule (proxy policy). For example, no ZTNA rule is matched for the ZTNA tag assigned to the endpoint.

ZTNA Logging Enhancements (Contd)

- HTTPS SNI virtual host does not match the HTTP host header:

Traffic log example when HTTPS SNI doesn't match HTTP host header:

```
date=xxxx-xx-xx time=15:15:39 eventtime=1623276939601851410 tz="-0700" logid="0000000013" type="traffic"
subtype="forward" level="notice" vd="root" srcip=10.1.100.206 srcport=55974 srcintf="port2" srcintfrole="undefined"
dstip=172.18.62.112 dstport=443 dstintf="root" dstintfrole="undefined" srccountry="Reserved" dstcountry="Reserved"
sessionid=17152 proto=6 action="deny" policyid=5 policytype="policy" poluid="b4d4c466-8b64-51eb-2292-5defbb0e34e5"
policyname="ztna" service="HTTPS"trandisp="noop" duration=0 sentbyte=0 rcvdbyte=0 sentpkt=0 rcvdpkt=0
appcat="unscanned" utmaction="block" countztna=2 msg="Denied: failed to match an API-gateway" utmref=65490-0
```

UTM log example when HTTPS SNI doesn't match HTTP host header:

```
date=xxxx-xx-xx time=15:24:25 eventtime=1623277465275003194 tz="-0700" logid="2102060522" type="utm"
subtype="ztna" eventtype="ztna-error" level="warning" vd="root" msg="Unable to match an API-gateway" policyid=5
sessionid=17614 srcip=10.1.100.206 dstip=172.18.62.112 srcport=56040 dstport=443 srcintf="port2" srcintfrole="undefined"
dstintf="root" dstintfrole="undefined" proto=6 action="blocked" service="HTTPS" vip="zv2" accessproxy="zs2" desc="HTTP
url (https://aq4.test.com/) failed to match an API-gateway with
vhost(name/hostname:_def_virtual_host/_def_virtual_host_)"
```

This slide shows the UTM and traffic logs that are generated when FortiGate connects to the ZTNA access proxy and the HTTPS SNI virtual host does not match the HTTP host header. The server name indication (SNI) or host name must match the *host* header field in the URL request.

Knowledge Check

1. Which CLI command shows the on-net and off-net status of an endpoint?
 - A. `diagnose endpoint wad-comm find-by`
 - ✓ B. `diagnose endpoint record list`

2. Which CLI command displays ZTNA IP and MAC addresses from EMS?
 - ✓ A. `diagnose firewall dynamic list`
 - B. `diagnose test application fcnacd 7`

Lesson Progress

-  ZTNA Introduction
-  Device Identity and Trust
-  ZTNA Configuration Setups
-  Comparing ZTNA to SSL and IPSec VPN
-  ZTNA Troubleshooting and Debugging

Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in this lesson.

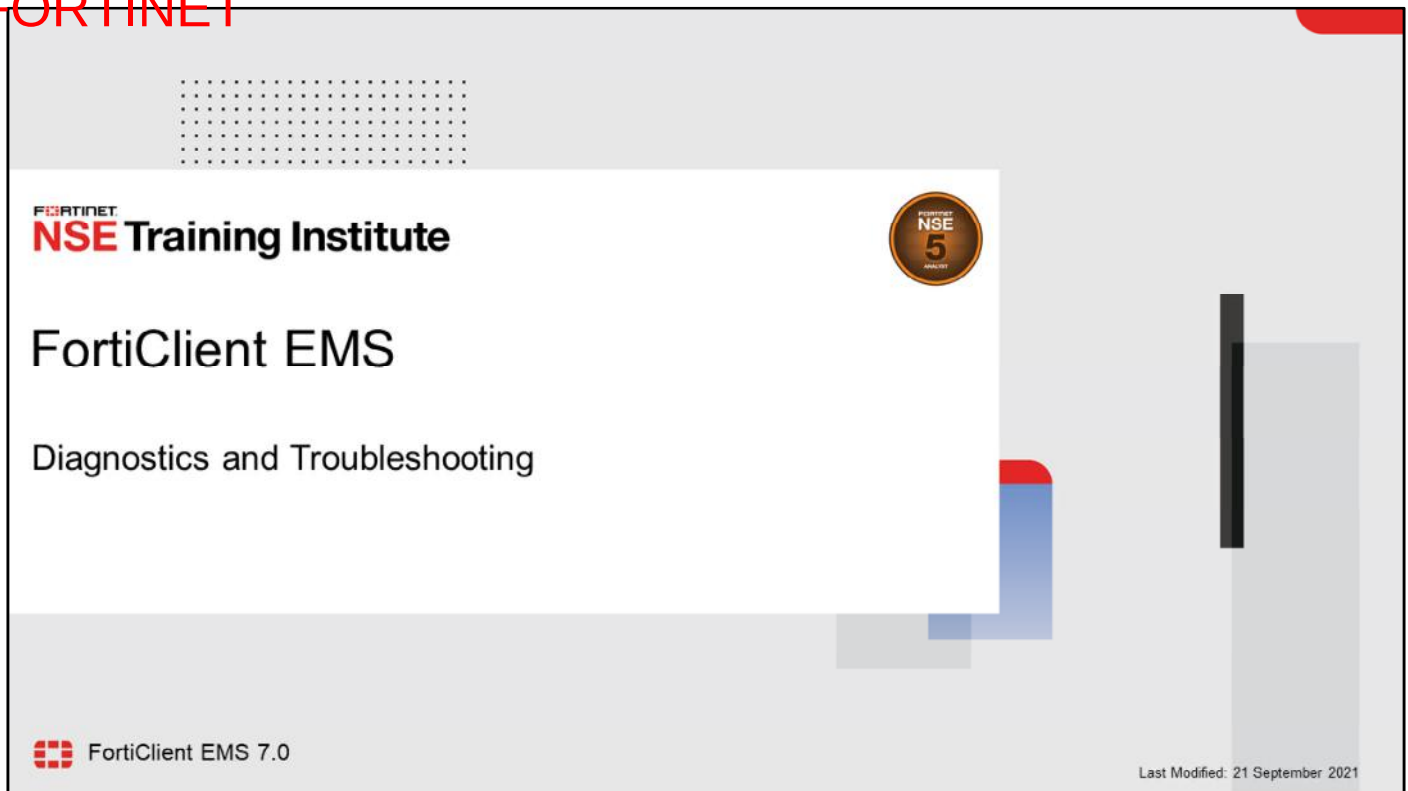
Review

- ✓ Understand the benefits of ZTNA
- ✓ Understand basic ZTNA configuration
- ✓ Understand ZTNA tagging rules
- ✓ Manage tags
- ✓ Understand how to establish device identity and trust
- ✓ Understand SSL certificate-based authentication
- ✓ Discuss ZTNA configuration setups
- ✓ Understand the evolution of teleworker remote access with ZTNA
- ✓ Troubleshoot and debug ZTNA issues

This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned about ZTNA key concepts and how to configure different configuration setups. You also learned about the evolution of teleworker remote access, and how to troubleshoot and debug ZTNA issues.

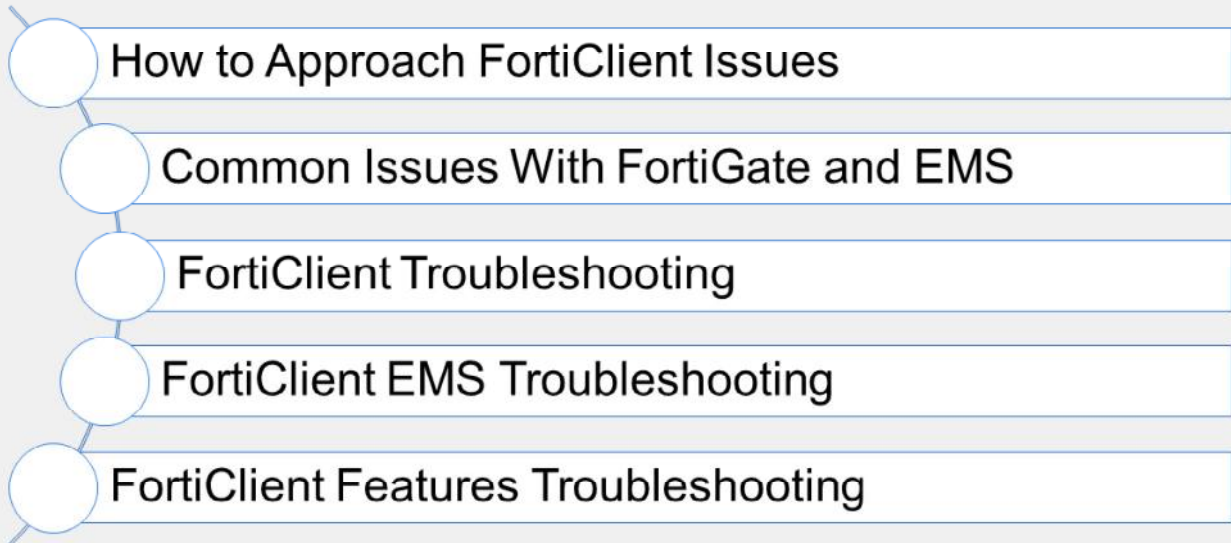
DO NOT REPRINT
© FORTINET



In this lesson, you will learn how to diagnose and troubleshoot FortiClient issues and FortiClient EMS issues.

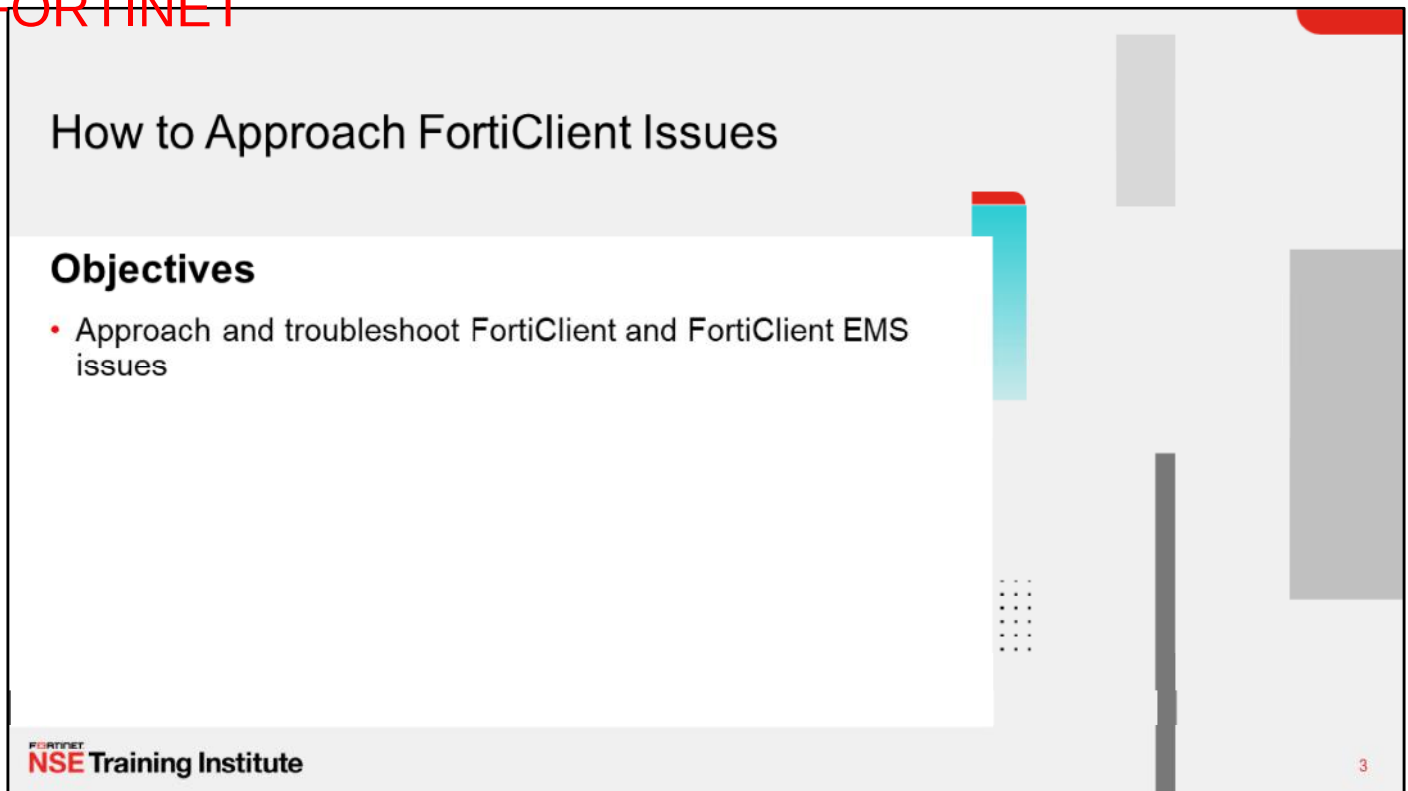
DO NOT REPRINT
© FORTINET

Lesson Overview



In this lesson, you will learn about the topics shown on this slide.

DO NOT REPRINT
© FORTINET



How to Approach FortiClient Issues

Objectives

- Approach and troubleshoot FortiClient and FortiClient EMS issues

FORTINET
NSE Training Institute

3

After completing this section, you should be able to achieve the objective shown on this slide.

By demonstrating competence in approaching and troubleshooting FortiClient issues, you will be able to solve FortiClient and FortiClient EMS issues.

DO NOT REPRINT
© FORTINET

Approaching FortiClient Issues—Methodology

- Gather information to dissect the problem
 - FortiClient version
 - Check minimum system requirements
 - Conflicting software—third-party antivirus software
 - New installation causing issues?
 - Did it ever work?
 - Existing installation—possible interference
 - Was it working fine before?
 - Any changes to workstation or mobile device?
 - Any changes to FortiClient configuration?
 - Network changes
 - Connecting location



Before you can resolve a FortiClient issue, you need to identify the issue by gathering information to pinpoint and define it.

For example, if the issue is *registering FortiClient to FortiGate or FortiClient EMS*, ask and answer the following questions: Has the registration process ever worked? Is the existing installation not working?

If the answer to these questions is yes, check for possible changes, such as changes to the device (OS updates, changes to administrator permissions), connection location (working from the office but not from home), and configuration and network changes.

Now you know the exact nature of the problem: *FortiClient is not registering from home*. The next step is to analyze the problem, which leads to possible opportunities to resolve the issue.

DO NOT REPRINT
© FORTINET

Approaching FortiClient Issues—Methodology (Contd)

- Analysis
 - Test on different workstation or mobile device
 - Other users having similar problems
 - Expected behaviour
 - Different behaviour
 - Reproducibility – always, random, unable to duplicate
- Possible solutions
 - List all possible options
 - Evaluate options in lab
 - Document
 - Implementation plan
 - Backup plan
- Implement and review the results
 - Monitoring and evaluation



The analysis phase requires testing, checking, and comparing with other users to determine if they are encountering similar issues.

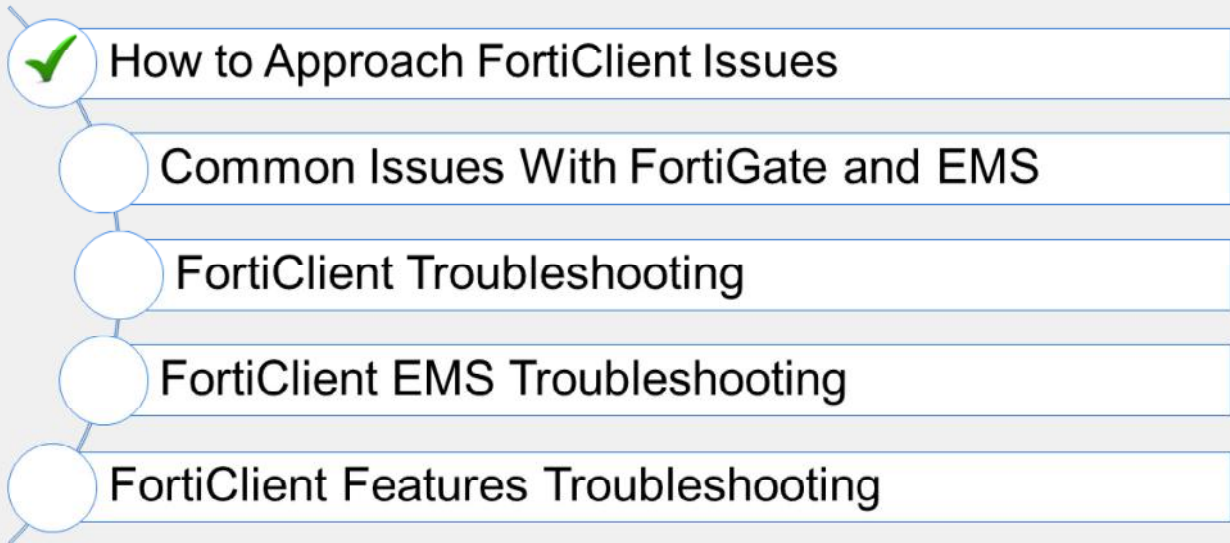
Once it is determined that other users are encountering similar problems, further dissect the issue. By comparing the expected results with your results. Find out if the issue is reproducible. These actions result in a list of possible solutions that you can evaluate in the lab.

Remember, there might be multiple ways to resolve an issue. You should always document each of possible solution. You should also create a backup plan before implementing a solution, in case you need to revert to a previous state.

Once you implement a solution, monitor and review the results.

DO NOT REPRINT
© FORTINET

Lesson Progress



Good job! You now understand how to approach FortiClient issues.

Now, you will learn about FortiClient EMS issues.

DO NOT REPRINT
© FORTINET

Common Issues With FortiGate and EMS

Objectives

- Understand the diagnostic steps to resolve issues between FortiClient, FortiClient EMS, and FortiGate

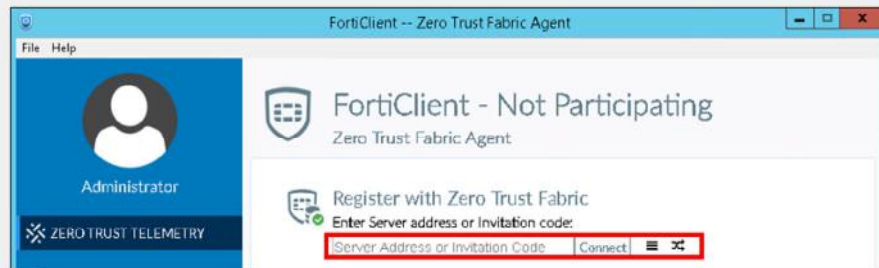
After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in taking diagnostic steps, you will be able to diagnose and resolve common issues between FortiClient, FortiClient EMS, and FortiGate.

DO NOT REPRINT
© FORTINET

FortiClient Registration

- FortiClient can use a Zero Trust Telemetry IP address to connect FortiClient Telemetry to EMS
- FortiClient automatically launches and connects telemetry to the EMS server after installation
- You can also manually enter the EMS IP address



FortiClient can use a Zero Trust Telemetry IP address to connect FortiClient Telemetry to FortiClient EMS. After FortiClient software installation completes on an endpoint, FortiClient automatically launches and connects telemetry to the FortiClient EMS server that created the installed deployment package. You can also manually enter the FortiClient EMS IP address.

Note that FortiClient uses the same process to connect telemetry to FortiClient EMS after the FortiClient endpoint restarts, rejoins the network, or encounters a network change.

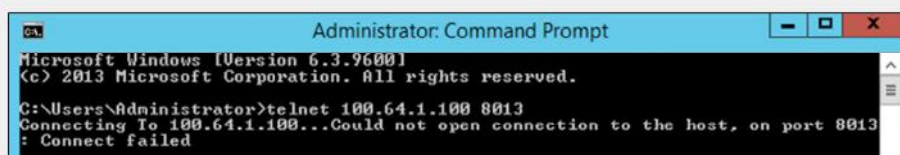
FortiClient and FortiClient EMS

- Verify services between FortiClient EMS and FortiClient on a domain

- Run `netstat -ano | find <port number>`
- RPC port: 135
- SMB port: 445

```
C:\Users>netstat -ano | find "135"
TCP    0.0.0.0:135      0.0.0.0:0        LISTENING       768
TCP    [::]:135        [::]:0           LISTENING       768
C:\Users>netstat -ano | find "445"
TCP    0.0.0.0:445     0.0.0.0:0        LISTENING        4
TCP    [::]:445       [::]:0           LISTENING        4
```

- To test connectivity
 - Run `telnet <FortiClient EMS IP> 8013`
 - If the command is successful, it returns blinking cursor
 - If the command is unsuccessful, it returns a warning that connect could not be open



```
Administrator: Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>telnet 100.64.1.100 8013
Connecting To 100.64.1.100...Could not open connection to the host, on port 8013
: Connect failed
```

If your FortiClient is installed on a domain-joined endpoint, you can use the following CLI command to verify the SMB and RPC services are bound to ports 445 and 135, respectively. Run CLI command `netstat -ano | find 135` or `445` on the endpoint to verify. The image on this slide shows that Windows is listing to port TCP 135 and 445. You can also use this command on the FortiClient EMS server.

To test the connectivity between FortiClient and FortiClient EMS, you can use the command prompt and the built-in Telnet application to verify this. Ensure that Telnet is enabled on your endpoint by going to **Control Panel > Turn Windows features on or off**, and ensuring that the **Telnet Client** checkbox is selected.

In the example on this slide, 100.64.1.100 is the FortiClient EMS server IP address, and 8013 is the port that is being checked. Run `telnet 100.64.1.100 8013`.

If the command is successful, the command prompt returns a blinking cursor. If the command is unsuccessful, the command prompt returns a warning that the connection could not be opened, as shown in this slide.

FortiClient and FortiClient EMS (Contd)

- Common issues
 - Unable to detect computers automatically
 - Unable to install, uninstall, or deploy changes
- Common causes
 - Computer browser services
 - Account permissions
 - Confirm required ports and Windows services are enabled
- Dashboard widgets
- Alerts and log messages
 - Common alerts
 - New version of FortiClient is available
 - FortiClient deployment failed
 - Failure to check for signature updates
 - Error encountered when downloading AD server entries
 - Error encountered when scanning for local computers



Multiple dependencies and various factors can be involved when troubleshooting FortiClient and FortiClient EMS issues. Common issues can be that FortiClient is unable to automatically detect any computer running Microsoft Windows, you are unable to install or uninstall FortiClient from the host machine, or you are unable to deploy changes using FortiClient EMS. You can resolve these issues by verifying the computer browser services, account permissions, and ports and services enabled for FortiClient EMS.

1. Computer browser services automatically detect Microsoft Windows computers within the same local network. Make sure computer browser services are running. For example, if the FortiClient EMS is installed on Windows 2012 R2, on which the computer browser service is disabled by default, FortiClient EMS will not detect computers on the same network, even if they are available.
2. Account permissions are required. Make sure the server and client have the correct account permissions to deploy the changes. For example, the administrator needs the correct permissions to create or deploy the changes on FortiClient EMS.
3. Confirm that the required ports and Windows services are enabled on EMS. FortiClient EMS uses many ports and services in order to communicate with clients and servers running associated applications. Make sure these ports and services are enabled for use for FortiClient EMS. On the client side, make sure **Task Scheduler** is set to **Automatic**, **Windows Installer** is set to **Manual**, and **Remote Registry** is set to **Automatic**.

FortiClient EMS has several dashboard widgets that provide information about managed clients and their current statuses. You can view alerts generated by FortiClient EMS by clicking the bell icon in the toolbar, which shows you generated alerts. An example of a common alert is “New version of FortiClient is available”. Note that configuration changes to FortiClient are always pushed by EMS. FortiClient sends telemetry data only for status updates.

FortiClient and EMS Issues—View Logs

- Logs messages
- Filter logs by date/time, level, source, and messages

Administration > Log Viewer

23/24/07	Info	Update Service	Generated AV whitelist signature info (sig count=0, version=1.00007)
23/24/07	Info	Update Service	EMS automatically disabled debug level logs after 30 minutes of logging at that le...
23/24/00	Debug	Update Service	checkFortiClientCorruptAssignmentsInstallers: 0 installer(s) need updating
23/22/57	Debug	Update Service	Rebuilt indexes
23/22/57	Debug	Update Service	Rebuilding indexes
23/03/03	Info	Console	admin created host verification policy: OS rule
23/02/51	Info	Console	admin created host verification tag: Windows Server
22/50/25	Info	Console	admin created Telemetry Gateway List: Corporate FortiGate
22/50/20	Info	Console	admin created Profile: Fortinet-Exam from UI
16/24/58	Info	Deployment Service	Host WIN-EHVKBEA3S71 entered deployment state 210 (install started)
16/24/55	Info	Deployment Service	Started FortiClient installation task on fortilab.net\WIN-EHVKBEA3S71...
16/24/55	Info	Deployment Service	Host WIN-EHVKBEA3S71 entered deployment state 120 (install task s...
16/24/55	Info	Deployment Service	Host WIN-EHVKBEA3S71 entered deployment state 80 (installer copi...
16/24/51	Info	Deployment Service	Deploying FortiClient to fortilab.net\WIN-EHVKBEA3S71 fortilab.net
16/24/51	Info	Deployment Service	There are 10 licenses available and 1 devices pending installation. Ser...
16/24/50	Info	Deployment Service	Host WIN-EHVKBEA3S71 entered deployment state 70 (Pending depl...
16/24/50	Info	Deployment Service	Host WIN-EHVKBEA3S71 entered deployment state 50 (Probed)
16/24/47	Info	Deployment Service	Host WIN-EHVKBEA3S71 entered deployment state 40 (Currently pro...

Engine/signature update

Console—profile creation

Deployment service

You can view the logs on FortiClient EMS using the **Log Viewer** page. You can filter logs by using various parameters, such as date/time, log level, source (such as **EMS Service**, **Update Service**, **AD Service**), and messages.

In the example shown on this slide, the logs provide detailed messages about the event occurred, which you can use to troubleshoot the issues with FortiClient and FortiClient EMS. You should change the log level to **Debug**.

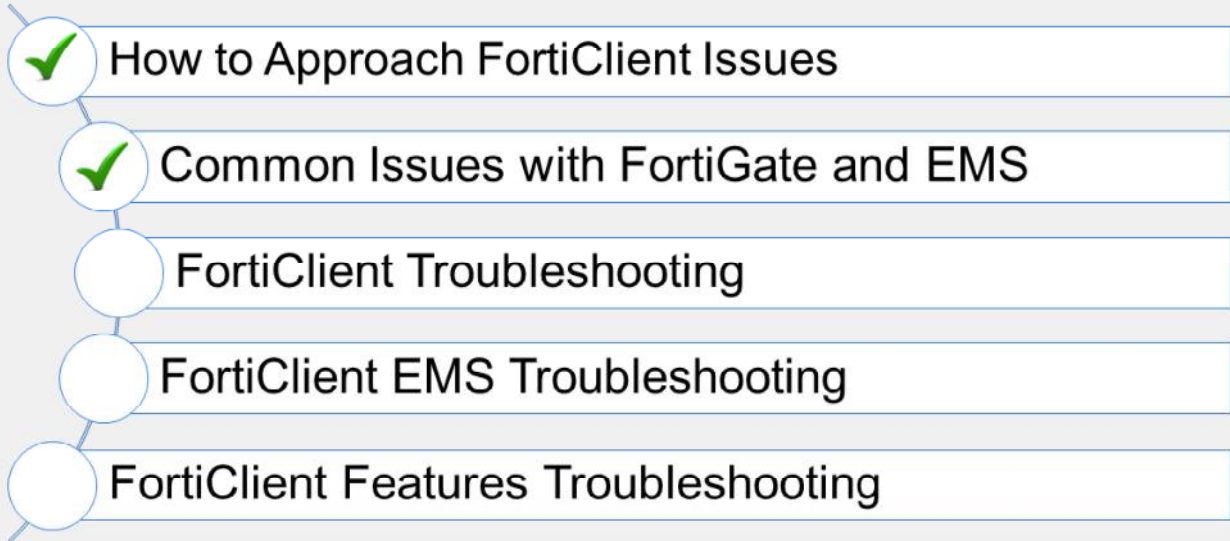
DO NOT REPRINT
© FORTINET

Knowledge Check

1. Which Fortinet device does FortiClient automatically connect to after installation?
☐ A. FortiGate
☒ B. FortiClient EMS
2. Which default port can you telnet to check connectivity between FortiClient and FortiClient EMS?
☐ A. 445
☒ B. 8013

DO NOT REPRINT
© FORTINET

Lesson Progress



Good job! You now understand the diagnostics steps involved in resolving common issues between FortiClient and FortiClient EMS.

Now, you will learn about FortiClient components and troubleshooting.

DO NOT REPRINT
© FORTINET

FortiClient Troubleshooting

Objectives

- Understand FortiClient components on Windows

FORTINET
NSE Training Institute

14

After completing this section, you should be able to achieve the objective shown on this slide.

By demonstrating competence in FortiClient components and troubleshooting, you will be able to resolve issues on the Windows operating systems.

DO NOT REPRINT
© FORTINET

Troubleshooting—Installation Directory

- Default FortiClient installation directory
 - Windows 32 bit – C:\Program Files(x86)\Fortinet\FortiClient
 - Windows 64 bit – C:\Program Files\Fortinet\FortiClient
- Created during installation time
- Removed during uninstall
- Protected by FortiShield
- Does not contain drivers (sys) files
 - With the exception of mdare driver
- Contains .EXE, .DLL, logs, signatures, quarantined files
 - Creates folders for logs, quarantine, and signatures (vir_sig)

When FortiClient is installed on Windows OS, by default it is installed in `Program Files(x86)` on Windows 32-bit OS, and `Program Files` on Windows 64-bit OS. The FortiClient directory is created only during installation and removed during uninstallation.

You can change the default installation directory while installing FortiClient. FortiClient is protected by FortiShield, which is digitally signed and prevents modification of the Windows registry. The FortiClient folder contains .EXE files, .DLL files, logs, signatures, quarantine files, and so on.

DO NOT REPRINT
© FORTINET

Troubleshooting—Installed FortiClient Files

- Some of the files installed in the FortiClient installation directory include:
 - `FortiClient.exe`: For FortiClient GUI (FortiClient console)
 - `fortifws.exe`: For FortiClient personal firewall service
 - `FortiWF.exe`: For FortiClient web filter service
 - `FortiTRAY.exe`: FortiClient system tray controller
 - `FortiESNAC.exe`: It handles the endpoint control
 - `fmon.exe`: FortiClient real-time file system monitor (real-time antivirus protection)
 - `submitv.exe`: FortiClient virus submit daemon (FortiClient virus feedback service)
 - `vpcd.exe`: FortiClient VPN policy retriever
 - `FortiSSLVPNdaemon.exe`: FortiClient SSL VPN daemon
 - `ipsec.exe`: FortiClient VPN service
 - `mdare.dll`: FortiClient malware detection and removal engine
 - `libav.dll`: FortinetAV engine library

When you install FortiClient, it installs a number of executables, DLL files, signatures, and so on. Refer to this slide for the list of FortiClient executable files and descriptions.

DO NOT REPRINT
© FORTINET

Troubleshooting—FortiClient Drivers

- Default FortiClient driver location
 - Windows 32-bit – C:\Windows\SysWoW64\Drivers
 - Windows 64-bit – C:\Windows\System32\Drivers
- FortiClient drivers
 - fortifw2.sys: FortiClient application firewall driver
 - fortiwf2.sys: FortiClient web filter driver
 - fortiloader.sys: FortiClient fortiloader driver
 - FortiShield.sys: FortiClient file system filter driver
 - fortips.sys: FortiClient IPsec driver
 - fortisniff2.sys: FortiClient IPS driver

When FortiClient is installed on Windows OS, it installs the necessary drivers on Windows 32-bit OS and Windows 64-bit OS. Refer to this slide for the list of FortiClient drivers and descriptions.

DO NOT REPRINT
© FORTINET

Troubleshooting—FortiClient Registry Keys

- HKLM\Software\Fortinet\FortiClient
 - Protected by FortiShield
- Cryptic
- Requires detailed knowledge
- Undocumented
- May or may not map to XML configuration
- No support on FortiClient GUI
- Intended for developers and corner cases

You can check the FortiClient registry keys at the location shown on this slide. The registry keys are protected by FortiShield.

Unlike XML, registry keys are cryptic and the user requires detailed knowledge to configure. The keys can't be documented in any format and so they are not supported on the FortiClient GUI. The keys are intended for use by developers.

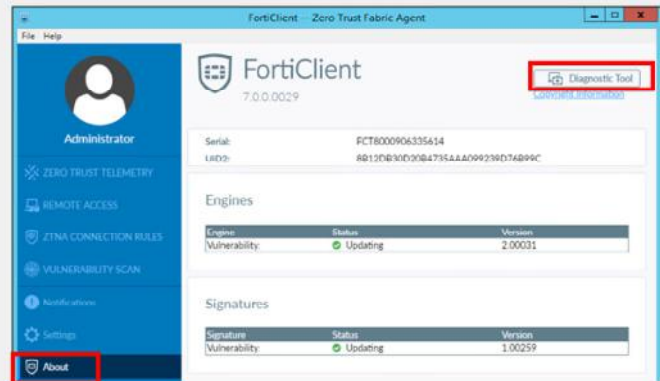
Note that, in some cases, Fortinet support can ask you to change the FortiClient registry or replace FortiClient files. To perform this task, you must stop FortiShield first:

- Disconnect FortiClient from FortiClient EMS.
- Shut down FortiClient.
- In an elevated command-line window, type `sc stop fortishield`.

DO NOT REPRINT
© FORTINET

Troubleshooting—Diagnostic Tool

- You can access the FortiClient Diagnostic Tool on the FortiClient console
 - Click **About**
- FortiClient Diagnostic Tool generates a debug report
- FortiClient Diagnostic Tool does not record sensitive information
- It contains the following information about the endpoint:
 - Windows operating system version
 - Windows software updates
 - Names and versions of installed software
 - Names and versions of installed drivers
 - FortiClient configuration
 - FortiClient logs



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

19

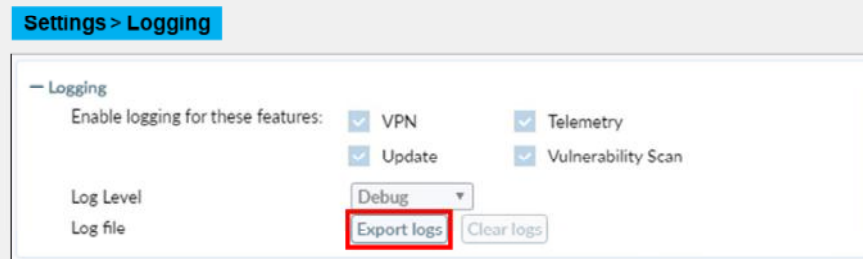
You can use the FortiClient Diagnostic Tool to generate a debug report, and then provide the debug report to the FortiClient team to help with troubleshooting. For example, if you are working with customer support on a problem, you can generate a debug report, and send the report to customer support to help with troubleshooting.

The FortiClient Diagnostic Tool does not record sensitive information. It contains information about the endpoint that are shown on this slide.

DO NOT REPRINT
© FORTINET

Troubleshooting—Logs

- You can export logs from FortiClient to review
- Change log level
 - To troubleshoot, you must change log level to **Debug**
- Default log level is **Information**



By default, the log level is set to **Information**, which provides enough related information to resolve common FortiClient issues. However, you can change the log level on FortiClient EMS, and then push the necessary configuration from the **System Settings** page to FortiClient.

There are various log levels on FortiClient, such as **Emergency**, **Alert**, **Information**, **Debug**, and so on. To get more detailed logs for debugging, change the log level to **Debug**.

Note that you can clear the checkboxes next to features to reduce log entries when troubleshooting a specific feature issue.

DO NOT REPRINT
© FORTINET

Troubleshooting—BSOD

- Provide a kernel memory dump file
 - Located in: C:\windows\MEMORY.dmp
 - Enabling a kernel-mode dump file
 - <http://msdn.microsoft.com/en-us/library/windows/hardware/ff542953>
- If interested in reading the dump file, use WinDbg
 - Analyzing a kernel-mode dump file with WinDbg
 - <http://msdn.microsoft.com/en-us/library/windows/hardware/ff538042>
- To download WinDbg installer
 - WDK and WinDbg downloads
 - <http://msdn.microsoft.com/en-us/windows/hardware/hh852365>
- Run and provide output of `FortiClient_Diagnostic_Tool.exe`
 - Collects system and FortiClient information for Fortinet support team
 - Useful when summarizing system

FortiClient can cause blue screen of death (BSOD) when it conflicts with third-party software. If this happens, provide a kernel memory dump. It is usually located in the Windows folder, as shown in this slide.

To configure the collection of dump files, refer to the Microsoft documents links that are shown on this slide.

Run and provide the output of `FortiClient_Diagnostic_Tool.exe`. You can download the tool from the Fortinet support website.

DO NOT REPRINT
© FORTINET

Knowledge Check

1. What protects FortiClient registry keys?
✓ A. FortiShield
B. FortiProxy
2. What is the default log level in FortiClient?
A. Warning
✓ B. Information

DO NOT REPRINT
© FORTINET

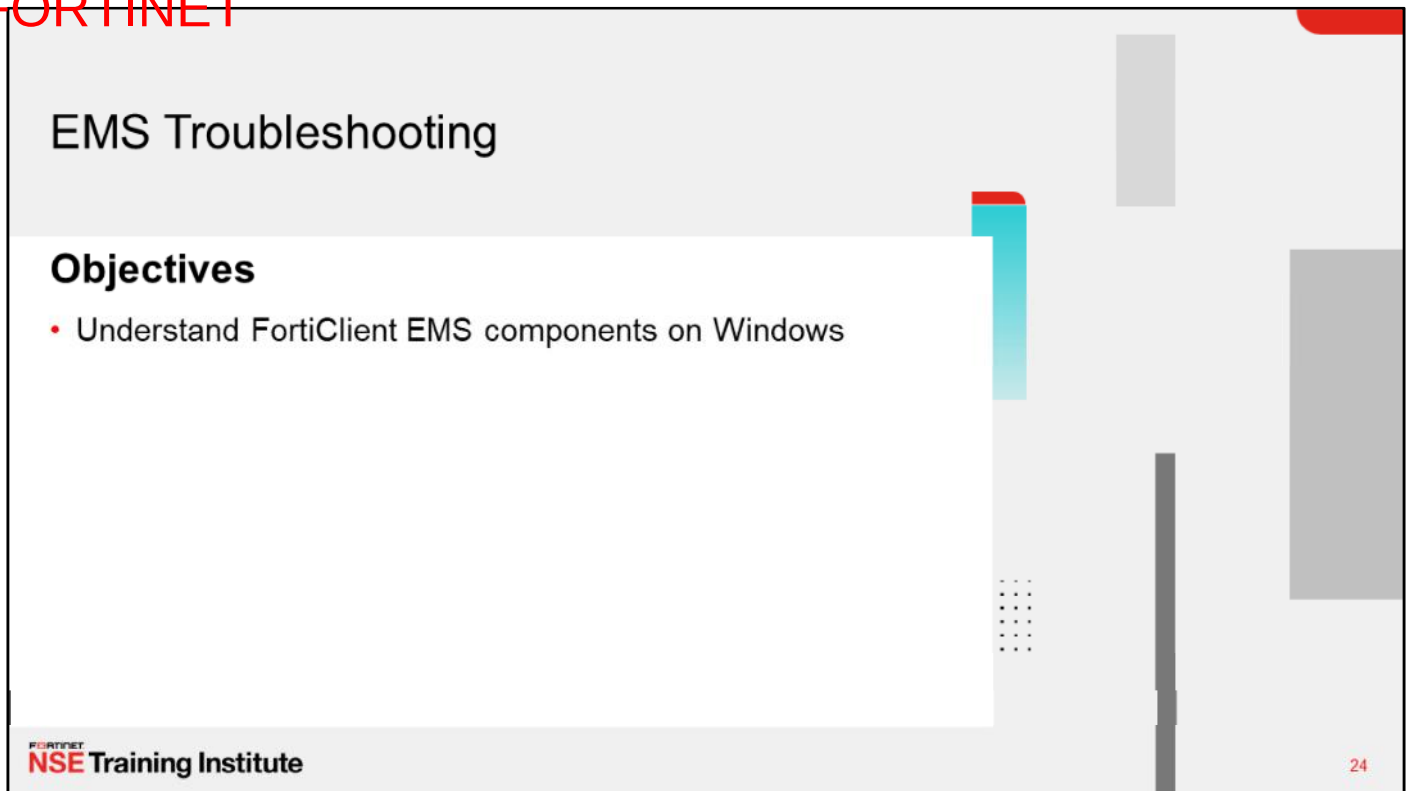
Lesson Progress

-  How to Approach FortiClient Issues
-  Common Issues With FortiGate and EMS
-  FortiClient Troubleshooting
-  FortiClient EMS Troubleshooting
-  FortiClient Features Troubleshooting

Good job! You now understand FortiClient components and troubleshooting on Windows operating systems.

Now, you will learn about FortiClient EMS troubleshooting.

DO NOT REPRINT
© FORTINET



EMS Troubleshooting

Objectives

- Understand FortiClient EMS components on Windows

FORTINET
NSE Training Institute

24

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in FortiClient EMS components and troubleshooting, you will be able to resolve EMS issues on Windows servers.

EMS Troubleshooting—Installation Directory

- Default FortiClient installation directory
 - Windows 64-bit – C:\Program Files (x86)\Fortinet\FortiClientEMS
- Created during installation time
- Removed during uninstallation
- FortiClientEMS installs SQL Server 2017 Express Edition on the server
 - Doesn't remove the SQL Server during uninstallation
 - Instance=FCEMS
 - Service=mssql\$FCEMS
- FortiClientEMS also installs Apache HTTP Server and Python

By default, FortiClient EMS is installed in Windows `Program Files (x86)` on the Windows 64-bit OS. The FortiClient EMS directory is created only during installation and is removed during uninstallation.

You can change the default installation directory while installing FortiClient EMS. FortiClient EMS installs SQL Server 2017 Express edition on the server. FortiClient EMS doesn't remove SQL Server during uninstallation. When managing more than 5000 endpoints, installing SQL Server Standard or Enterprise instead of SQL Server Express is recommended. Note that Microsoft SQL Server Express is free. All other editions require a license from Microsoft.

FortiClient EMS also installs Apache HTTP Server and Python.

DO NOT REPRINT
© FORTINET

EMS Troubleshooting—Installed Services

- List of services installed in FortiClient EMS installation directory:
 - FortiClient Enterprise Management Server: For client connectivity/endpoint control/registration
 - FcmDaemon.exe
 - FortiClient Enterprise Management Server Active Directory Service: For Active Directory groups
 - FcmAdDaemon.exe
 - FortiClient Enterprise Management Server Apache Service: For EMS web console
 - httpd.exe
 - FortiClient Enterprise Management Server: For Chromebooks management
 - FcmChromebookDaemon.exe
 - FortiClient Enterprise Management Server Update: To connect to FortiGuard for updates
 - FcmUpdateDaemon.exe
 - FortiClient Enterprise Management Server Deployment Service: For FortiClient deployment
 - FcmDeploy.exe
 - FortiClient Enterprise Management Server Monitor Service
 - FcmMonitor.exe
 - FA Scheduler: Keeps track of all the EMS services and starts them when stopped

When you install FortiClient EMS, it installs a number of executables, dll, signatures, and so on. Refer to this slide for the list of executable files and descriptions.

DO NOT REPRINT
© FORTINET

EMS Troubleshooting—GUI Issue Debugging

- Use **Chrome > More tools > Developer tools > Network** to see the active connections from the EMS
 - `C:\Program Files (x86)\Fortinet\FortiClientEMS\Apache24\logs`
- More verbose logging:
 - `/ProgramFiles/Fortinet/FortiClientEMS/Python/Scripts/FCM/FCM/Settings.py`
 - Change `DEBUG` from false to true
- Apache uses port 443 and 10443

You can debug GUI access issues either by using a web browser or enabling verbose logging for Python.

Make sure you turn off the debug after troubleshooting. You should not run the debug in a production environment. By default, Apache uses port 443 and 10443. You can use the `netstat` command to see if the default Apache ports are being used by another application.

DO NOT REPRINT
© FORTINET

EMS Troubleshooting—View Debug Logs

- You can check logs on FortiClient EMS GUI

Administration > Log Viewer

Date	Level	Source	Message
05:10:48	Debug	Console	[Host Tags: 690579198b841198db787e67f3d31e18] Request with SN [FGVM02TM19001113] succe...
05:10:48	Debug	Console	[Host Tags: 690579198b841198db787e67f3d31e18] Request made with params: {'sn_list': ['FGVM0...
05:10:46	Info	EMS Service	Tags cleared for endpoint FortiClient-Laptop
05:09:46	Debug	Console	[Host Tags: a5d19bc27fa14d31bbf3d471ad553a] Request with SN [FGVM02TM19001113] succe...
05:09:46	Debug	Console	[Host Tags: a5d19bc27fa14d31bbf3d471ad553a] Request made with params: {'sn_list': ['FGVM0...
05:08:46	Debug	Console	[Host Tags: 72ef1681fac47fa9a0f2322988f4f36] Request with SN [FGVM02TM19001113] succe...
05:08:46	Debug	Console	[Host Tags: 72ef1681fac47fa9a0f2322988f4f36] Request made with params: {'sn_list': ['FGVM02...
05:07:46	Debug	Console	[Host Tags: 42c35cd90f249fe998b7296c63644e] Request with SN [FGVM02TM19001113] succe...
05:07:46	Debug	Console	[Host Tags: 42c35cd90f249fe998b7296c63644e] Request made with params: {'sn_list': ['FGVM02...
05:07:22	Error	Update Service	Unable to connect to the update server
05:07:21	Debug	Update Service	Update result: A network error prevented updates from being downloaded.

- Change log level to **Debug**
- However this doesn't include FortiClient EMS installation logs
- For FortiClient EMS installation issues go to:
 - C:\Users\Administrator\AppData\Local\Temp\FortiClient_Enterprise
- SQL Server installation logs
 - %temp%\sql

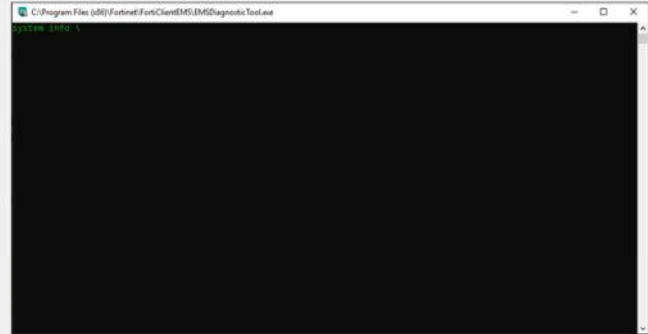
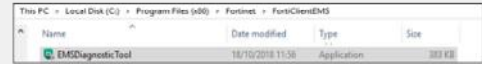
On FortiClient EMS, you can see the logs on the **Logs** page. To get more information, you should to change the log level to **Debug**. However this GUI log doesn't include FortiClient EMS and SQL installation logs. Installation logs are generally available in the temp folder.

Note that FortiClient EMS automatically reverts the log level from **Debug** to **Info** after 30 minutes to save resources on the server. The FortiClient EMS GUI displays logs only from the database; daemon debug logs are sent only to the file.

**DO NOT REPRINT
© FORTINET**

EMS Troubleshooting—Diagnostic Tool

- You can access the EMS Diagnostic Tool in:
 - C:\ProgramFile(x86)\Fortinet\FortiClientEMS
- FortiClient EMS Diagnostic Tool generates a debug report
- FortiClient Diagnostic Tool does not record sensitive information
- It contains the following information about the endpoint:
 - Windows operating system version
 - Server event logs
 - FortiClient EMS Apache configuration
 - FortiClient EMS Apache logs
 - FortiClient EMS logs
 - Names and versions of installed software
 - Names and versions of installed drivers
 - Python logs
 - Temp directory installation logs



You can use the FortiClient EMS Diagnostic Tool to generate a debug report, and then provide the debug report to the FortiClient team to help with troubleshooting. For example, if you are working with customer support on a problem, you can generate a debug report, and send the report to customer support to help with troubleshooting.

The FortiClient EMS Diagnostic Tool does not record sensitive information. It contains information about the server that is shown in this slide.

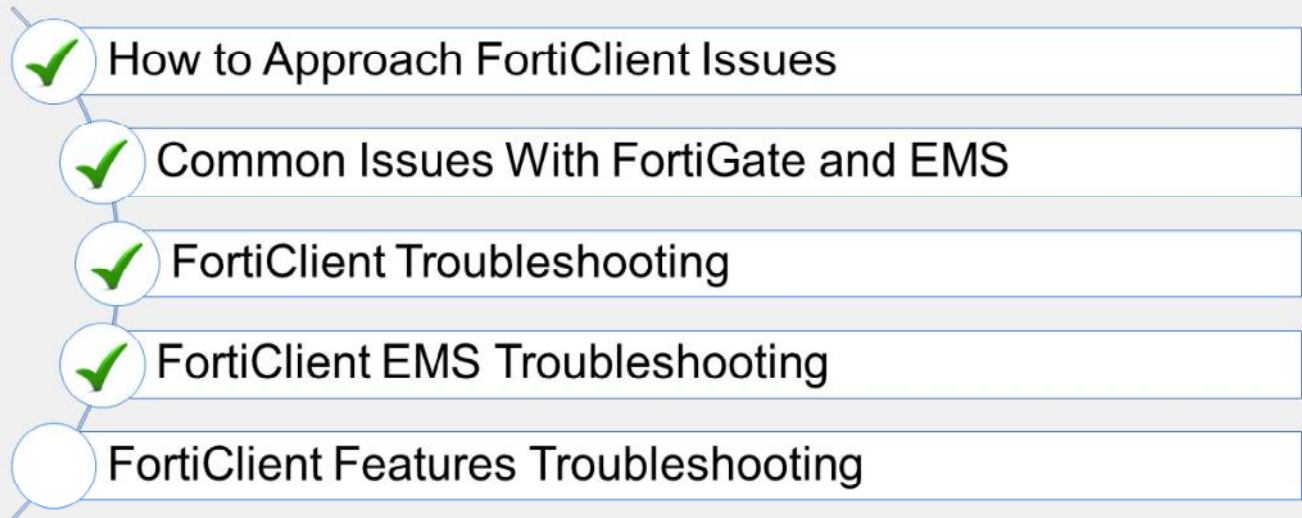
DO NOT REPRINT
© FORTINET

Knowledge Check

1. Which database is installed with the EMS installation?
☐ A. Oracle
☒ B. Microsoft SQL Server
2. Which process is responsible for the EMS web console?
☐ A. FcmDaemon.exe
☒ B. httpd.exe

DO NOT REPRINT
© FORTINET

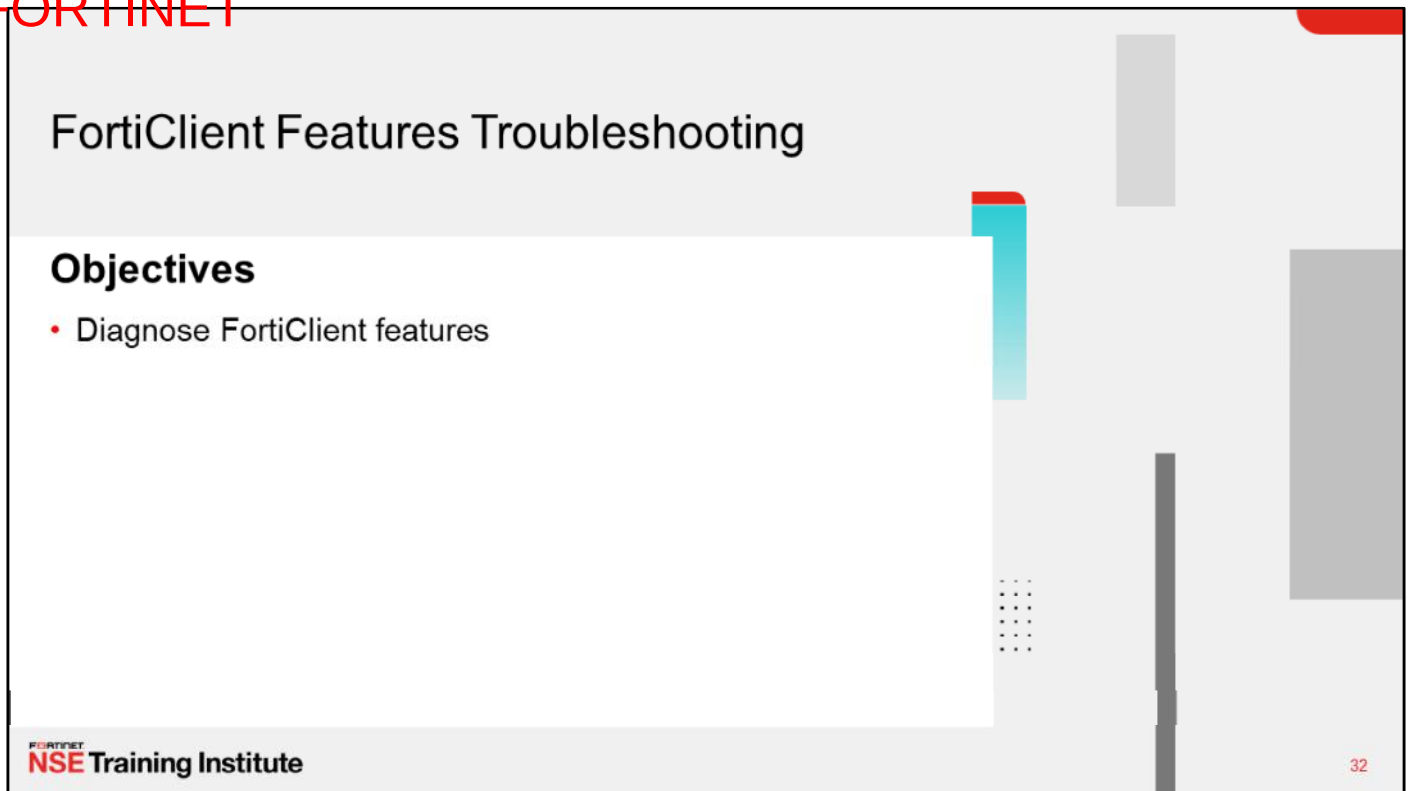
Lesson Progress



Good job! You now understand FortiClient EMS components and troubleshooting on Windows Servers systems.

Now, you will learn about diagnosing and troubleshooting FortiClient features.

DO NOT REPRINT
© FORTINET



FortiClient Features Troubleshooting

Objectives

- Diagnose FortiClient features

FORTINET
NSE Training Institute

32

After completing this section, you should be able to achieve the objective shown on this slide.

By demonstrating competence in diagnosing FortiClient features, you will be able to resolve issues related to individual features.

FortiClient Features—Updates

- Verify latest updates
 - Click **About**
 - In an elevated command line window run the following
 - `update_task.exe -s fd_01`
- Registry
 - FA_UPDATE
 - FA_Scheduler\00003
- Check XML configuration
 - `<forticlient_configuration> <system> <update>`
 - Check custom servers if defined
 - Backup server
 - Failover to FDN
 - Schedule update

Serial		
Serial	FCT90222076180	
UID2	C3B7338A6F24C584402D0B944540	
Engines		
Engine	Status	Version
Antivirus	Up To Date	6.100.12
Anti-Hacker	Up To Date	2.00062
Vulnerability	Up To Date	2.00028
Signatures		
Signature	Status	Version
AntiVirus	Up To Date	66.00659
AntiVirus-Extended	Up To Date	66.00659
AntiVirus-Extreme	Up To Date	66.00647
Vulnerability	Up To Date	1.00181
IDS Signatures	Up To Date	4.00421

```
<update>
  <use_custom_server>0</use_custom_server>
  <restrict_services_to_regions />
  <server />
  <port>80</port>
  <timeout>60</timeout>
  <failoverport />
  <fail_over_to_fdn>1</fail_over_to_fdn>
  <use_proxy_when_fail_over_to_fdn>1</use_proxy_when_fail_over_to_fdn>
  <auto_patch>0</auto_patch>
  <submit_virus_info_to_fds>1</submit_virus_info_to_fds>
  <submit_vuln_info_to_fds>1</submit_vuln_info_to_fds>
  <update_action>notify_only</update_action>
  <scheduled_update>
    <enabled>1</enabled>
    <type>interval</type>
    <daily_at>01:09</daily_at>
    <update_interval_in_hours>1</update_interval_in_hours>
  </scheduled_update>
</update>
```

The FortiClient console provides the latest information about engine and software statuses and versions used by FortiClient. To check the latest updates on FortiClient, click **About**.

By default, the value for `use_custom_server` element is 0, which means it is disabled, failover backup servers are not defined, and failover to public FDN is enabled. In this case, FortiClient will first attempt to connect to the public FortiClient server, `forticlient.fortinet.net` or `myforticlient.fortinet.net`, over TCP port 80 to download the list of secondary servers from which it will then download the signatures and packages for FortiClient.

If a string is specified in the `server` element and communication fails with that server, each of the servers specified in the `fail_over_servers` element are tried until one succeeds. If that also fails, then software updates will not be possible unless `fail_over_to_fdn` is set to 1. If communication fails with the server(s) specified in both `server` and `fail_over_servers` elements, `fail_over_to_fdn` specifies the next course of action.

You should leave the value of `fail_over_to_fdn` element to 1, which is the default value.

By default, scheduled updates are enabled at intervals that specify the frequency that FortiClient checks for updates. A network error will cause an update failure, and the temporary AV signatures keep growing. Run the `update_task` command manually.

FortiClient Features—Updates

- Signature update logs
 - Can be opened with any text editor

Settings > Logging > Export Logs

```

2017/08/08 6:33:25 AM Notice Update id=96650
avsig=28.00220 avsigetm=28.00105 avsigext=28.00083
avsigheu=28.00220 avsiglastupdate="2017-08-08 06:33:11-06"
ipssig=6.00699 irdbsig=2.00502

```

- Software update logs
 - Located in %temp% folder in Windows
 - C:\Users\\AppData\Local\Temp\

The signature update logs provide the date and time of the update, along with the version number of the signatures. You can request logs through FortiClient EMS or export logs using **Export logs** pane of FortiClient. Based on the logging level and log types enabled, it will export all types of logs.

The software update logs are located in the `temp` folder in Windows, which might be a hidden folder.

FortiClient Features—Antivirus

- Files and drivers:
 - fmon.exe, xmlav.dll, libav.dll, mdare.dll, mdare.sys
- vir_sig folder contains
 - Malware and antivirus signatures
 - Mdare_sig, vir_ext, vir_extreme, vir_heuristics, vir_high, vir_high
 - fdni.conf—list of FortiGuard servers
 - Block malicious websites
 - fortiwf.exe, fortiwf2.sys
 - Block known communication channels
 - fortifws.exe, fortisniff.sys, irdb.dat

```

SerialNumber=FPT-FCS-29500013|Address=208.91.112.135:443|FDNListener=208.91.112.135:8889|TimeZone=-5
SerialNumber=FPT-FCS-DELL0005|Address=208.91.112.132:443|FDNListener=208.91.112.132:8889|TimeZone=-5
SerialNumber=FPT-FCS-DELL0008|Address=208.91.112.133:443|FDNListener=208.91.112.133:8889|TimeZone=-5
SerialNumber=FPT-FCS-DELL0015|Address=208.91.112.136:443|FDNListener=208.91.112.136:8889|TimeZone=8

```

FortiClient requires a number of files and drivers in order to perform a real-time antivirus scan which includes EXE, DLL, SYS, and CONF files, and are located in the `Installation directory\Fortinet\FortiClient\` folder. The `vir_sig` folder contains malware and antivirus signatures along with the `fdni.conf` file, which contains a list of public FortiGuard servers that FortiClient contacts to get updates on the signatures and packages.

Antivirus—Real-Time Protection

- Check XML configuration
 - <forticlient_configuration> <antivirus> <real_time_protection>
- Fmon

```
<real_time_protection>
  <enabled>1</enabled>
  <use_extreme_db>0</use_extreme_db>
  <when>0</when>
  <ignore_system_when>2</ignore_system_when>
  <on_virus_found>5</on_virus_found>
  <cloud_based_detection>
    <on_virus_found>4</on_virus_found>
  </cloud_based_detection>
  <compressed_files>
    <scan>1</scan>
    <maxsize>10</maxsize>
  </compressed_files>
```

Compressed file size to scan in MB

```
<scan_file_types>
  <all_files>1</all_files>
  <file_types>
    <extensions>.386,.ACE,.ACM,.ACV,.ACK,.ADT,.APP,.ASD,.ASP,.ASX,.AVB,.AX,.A
    X2,.BAT,.BIN,.BTM,.CDR,.CFM,.CHM,.CLA,.CLASS,.CMD,.CND,.COM,.CPL,.CPT
    ,.CPV,.CSC,.CSH,.CSS,.DEV,.DLL,.DOC,.DOT,.DRV,.DVB,.DWS,.EML,.EXE,.FO
    N,.GMS,.GVV,.HLP,.HTA,.HTM,.HTML,.HTI,.HTW,.HTX,.HXS,.INF,.INI,.JPG,.
    JS,.JTD,.KSE,.LGP,.LIB,.INX,.MBS,.MHT,.MHTM,.MHTML,.MOD,.MPD,.MPP,.MP
    T,.MRC,.OCK,.PIF,.PL,.PLG,.PM,.PNF,.PNP,.POT,.PPA,.PPS,.PPT,.PRC,.PWZ
    ,.QLB,.QPM,.REG,.RTF,.SBE,.SCR,.SCI,.SH,.SHB,.SHS,.SHI,.SHML,.SHW,.S
    IS,.SML,.SWF,.SYS,.TDO,.TIB,.TSM,.TSP,.TT4,.VBA,.VBE,.VBS,.VEX,.VMI,.
    VSD,.VSS,.VST,.VWP,.VXD,.VXE,.VXE,.VXE,.VXE,.VXE,.VXE,.VXE,.VXE,.VXE,.
    VXF,.VXH,.XLS,.XML,.XTP</extensions>
    <include_files_with_no_extension></include_files_with_no_extension>
  </file_types>
</scan_file_types>
```

It is very important to check the XML configuration if the real-time antivirus protection is not functioning correctly. By default, when a virus is found, FortiClient blocks access to the file. There are five levels of `on_virus_found` XML configuration tags:

- 0: clean
- 1: ignore
- 2: repair
- 3: warning
- 4: quarantine
- 5: deny access

FortiClient also performs a scan on the compressed files and allows you to define the compressed file size to scan up to 65535MB. 0 means no limit. FortiClient performs a real-time scan on a wide range of extensions and allows you to modify the list of extensions to scan.

For example, if you set the value of the `on_virus_found` XML configuration tag to 1, it will ignore the virus file and the virus will not be caught. Another example is if you modify and remove a few extensions from the `extensions` XML configuration element and if the suspicious file extension is not listed in the `extensions` XML configuration element, it will not be caught.

Note that this partial XML configuration is for a real-time antivirus. For a complete list of available XML configuration elements, refer to the *FortiClient 7.0.0 XML Reference guide* available at Fortinet documentation site.

Antivirus—Real-Time Protection (Contd)

- FortiClient logs

- **Settings > Logging > Export logs**
- Installation directory\Fortinet\FortiClient\logs\realtime_scan.log

Exported logs

```

15 9:44:37 AM Notice AntiVirus id=96533 user= msg="User enabled Realtime AntiVirus protection"
15 9:44:49 AM Warning AntiVirus id=96530 user= action=quarantined checksum=0x31db28d1 filesize=184
msg="Found virus by AntiVirus realtime protection,
in filesystem" sigid=439072 virus=EICAR_TEST_FILE
file=C:\Users\S\AppData\Local\Temp\UI0JJnCn.zip.part

```

realtime_scan.log

```

File Edit Format View Help
realtime_scan - Notepad
Realtime scan result:
time: 09:44:39, Realtime Protection Started, AV_ENGINE:5.00220 MDARE_ENGINE:2.00060 AV_SIG:28.00336 AV_EXT_SIG:28.00226 MDARE_SIG:1.00000
time: 09:44:48, virus found: EICAR_TEST_FILE, action: Quarantined, C:\Users\S\AppData\Local\Temp\UI0JJnCn.zip.part

```

The antivirus logs provides the date and time of the real-time antivirus scan along with the action taken, virus, and location of the file. You can request logs from the endpoint through FortiClient EMS. If you need to export the logs to a local computer from FortiClient, select **Settings > Logging > Export Logs** option.

Based on the logging level and log types enabled, **Export Logs** will export all types of logs.

The `realtime_scan.log` located in Installation directory\Fortinet\FortiClient\logs\realtime_scan.log provides more detailed information about malware and antivirus engines and signatures used in the real-time antivirus scan, along with name of the virus file, action taken, and location of the file.

Debug: In an elevated command line window:

- Disable RTP on FortiClient.
- Change the FortiClient installation directory: `fmon.exe -s -fd_1`

Antivirus—Real-Time Protection (Contd)

- RTP for other security risks protection
 - Sandbox
 - `<use_sandbox_signatures>0</use_sandbox_signatures>`
 - Block malicious websites
 - `<forticlient_configuration><webfilter><block_malicious_websites>`
 - Block known attack communication channels
 - `<forticlient_configuration><firewall><candc_enabled>`
 - Email protection
 - `<forticlient_configuration><antivirus><email>`
 - Boolean value is used to enable or disable RTP features
 - `<block_malicious_websites>0</block_malicious_websites>`

```
<email>
  <smtp>1</smtp>
  <pop3>1</pop3>
  <outlook>1</outlook>
  <wormdetection>
    <enabled>0</enabled>
    <action>0</action>
  </wormdetection>
  <heuristic_scanning>
    <enabled>0</enabled>
    <action>0</action>
  </heuristic_scanning>
  <mime_scanning>
    <enabled>0</enabled>
  </mime_scanning>
</email>
```

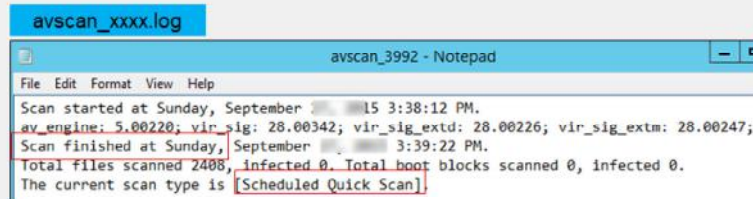
There are other security risks that are also handled by real-time protection. The sandbox signatures can also be used by FortiClient to identify the threat. The block access to malicious websites function blocks malicious websites. The web filter module must be installed before you can enable this protection.

FortiClient RTP also blocks known communication channels used by attackers. The application firewall module must be installed before you can enable this protection. An Email protection on FortiClient scans email for malicious files. It supports POP3 and SMTP.

You can use Boolean values in the EMS XML editor to enable or disable real-time protection features. The boolean value 0 for `<block_malicious_websites>` shown on this slide will disable blocking of malicious websites.

Antivirus—Schedule and Custom Scan

- Uses the same files and drivers as real-time antivirus scan
 - Uses `av_task.exe` instead of `fmon.exe`
 - `av_task.exe <options>`
 - `-q` - quick scan
 - `-f` - full system scan
 - `-d <dir>` - scan the specified directory
 - `-x` - use multiple `av_task.exe` instances for scanning
- Check XML configuration
- `<forticlient_configuration> <antivirus> <scheduled_scan>`
- `<forticlient_configuration> <antivirus> <on_demand_scanning>`
- FortiClient Logs



The scheduled and custom scan uses the same real-time antivirus files and drivers except it uses `av_task.exe` instead of `fmon.exe`. It uses `av_task.exe` with the option `-f` to perform a full system scan and `av_task.exe -d` to scan the specified directory.

The factory default behavior at the time of installation is to run a full system scan on the first day of the month at 18:30 hours. It also scans removable media. However, the default XML configuration file can be modified to change the default behavior. You can view and modify the factory default full-scan schedule under the full element of the XML file.

There is a priority parameter in the XML file as well. By default, the priority of the scan is set to normal and has three different levels—0 for normal priority, 1 for low priority, and 2 for high priority. The `on_demand_scanning` element defines how the antivirus scanner handles the scanning of files manually requested by the end user. The scheduled and on-demand scan logs are located in `Installationdirectory\Fortinet\FortiClient\logs\av_scanxxxx.log`.

DO NOT REPRINT
© FORTINET

FortiClient Features—Sandbox Detection

- Files and drivers
 - `fortiAptFilter.sys`
 - `fcaptmon.exe`
 - `vir_sandbox_sig`
- Registry
 - `FA_SANDBOX`
 - `FA_Scheduler/000022`
- XML
 - `<forticlient_configuration><sandboxing>`
- Maximum file size is 200MB
- Command-line: `Fcaptmon.exe -s fd_01`
- FortiSandbox cache improves performance
 - `Fcaptmon.apl`: cache file used by `fcaptmon.exe`
 - `Aptcache.dat`: cache file used by sandbox driver

FortiClient requires a number of files and drivers in order to perform file submission to FortiSandbox. The `vir_sanbox_sig` folder contains malware and antivirus software. The maximum file size you can submit from FortiClient to FortiSandbox is 200 MB.

Files can be submitted from the following sources:

- Removable media
- Mapped network drives
- Web downloads
- Email download

You can run a sandbox debug by entering the CLI command `Fcaptmon.exe -s fd_01` in an elevated command-line window.

FortiSandbox also caches files to improve performance.

FortiClient Features—Web Filter

- Files and drivers
 - fortiproxy.exe, fortiWF.exe, xmlwf.dll, fortiWF.sys
- Check XML configuration
 - <forticlient_configuration> <webfilter>

Settings > Logging > Export logs

```
<webfilter>
  <enable_filter>1</enable_filter>
  <enabled>1</enabled>
  <current_profile>0</current_profile>
  <max_violations>5000</max_violations>
  <max_violation_age>7</max_violation_age>
  <block_malicious_websites>1</block_malicious_websites>
  <browser_read_time_threshold>180</browser_read_time_threshold>
```

Web filtering
enabled by default

FortiGuard querying
service

- FortiClient logs
 - View recent violations on FortiClient GUI

FortiClient requires a number of files and drivers in order to perform web filtering. By default, web filtering and the FortiGuard querying service are enabled, and can store up to 5000 violations for a period of seven days. The default value for the `max_violations` element is set to 5000 and can be ranged from 250 to 5000, and the `max_violation_age` element is set to seven days and can be ranged from 1 to 90 days.

You can also configure safe search and the YouTube education filter under the `<safe_search>` and `<youtube_education_filter>` XML elements.

For a complete list of available XML configuration elements, refer to the *FortiClient 7.0.0 XML Reference guide* available at <http://docs.fortinet.com>.

Safe Search is a feature of Google search that acts as an automated filter of pornography and potentially offensive content. The upcoming release of FortiClient will include the ability to modify the host file to force all Google or YouTube traffic to connect to safe search websites, such as WackySafe, that only delivers safe search results. The drawback is that this will affect all Google services, such as search, YouTube, and so on.

Enabling the **Client Web Filtering When On-Net** option will keep using the FortiClient web filter even if it is behind FortiGate and on-net. When this is disabled, the FortiClient endpoint will be protected by the FortiGate web filter profile when on-net.

You can view the web filtering violation logs directly on the FortiClient GUI or export the logs from **Export Logs**.

FortiClient Features—Web Filter (Contd)

- FortiClient logs

Settings > Logging > Export logs

```

4:16:56 PM Notice WebFilter date=2008-08-07 time=16:16:55
logver=2 type=traffic level=info sessionid=34973356 hostname=WIN-8IBESU9FULP
uid=89054F3525124328A62F432C52F5562E devid=FC78003460228176
fgtserial=FGV0810000045784 regip=N/A srcname=firefox.exe srcproduct=Firefox
srcip=10.0.1.10 srcport=54346 direction=outbound destinationip=66.171.121.44
remotename=www.fortinet.com destinationport=80 user=Saurabh proto=6 rcvbyte=N/A
sentbyte=N/A utmaction=passthrough utmevent=webfilter threat="General Interest -
Business:Information Technology" vd-root fctver=5.0.0.0 os="Microsoft
Windows Server 2012 R2 Datacenter Edition, 64-bit (build 9600)"
usingpolicy="Training" service=http url=index.html userinitiated=0
browstime=N/A

4:40:12 PM Notice WebFilter date=2008-08-07 time=16:40:12
logver=2 type=traffic level=warning sessionid=34973356 hostname=WIN-8IBESU9FULP
uid=89054F3525124328A62F432C52F5562E devid=FC78003460228176 fgtserial=N/A
regip=N/A srcname=firefox.exe srcproduct=Firefox srcip=10.0.1.10 srcport=55672
direction=outbound destinationip=23.235.39.81 remotename=www.bbc.com
destinationport=80 user=Saurabh proto=6 rcvbyte=N/A sentbyte=N/A
utmaction=blocked utmevent=webfilter threat="General Interest - Personal:News
and Media" vd=N/A fctver=5.0.0.0 os="Microsoft Windows Server 2012 R2
Datacenter Edition, 64-bit (build 9600)" usingpolicy="" service=http url=/
userinitiated=1 browstime=N/A

```

- Webfilter cache file
 - urlcache.dat
- Debug CLI commands
 - fortiwmf.exe -s fd_01
 - fortiproxy.exe -s fd_01 -d 4

In the example shown on this slide, the first log entry is from a FortiClient. The FortiClient log show the FortiGate serial number along with the name of the FortiClient profile it is using, and other details such as utmaction, utmevent, and so on.

So, when diagnosing and troubleshooting web filtering issues, always pay attention to the logs because the URL or category might be blocked in the managed profile, but allowed in the URL list, and the results might be different than what you were expecting.

- The webfilter cache URL rating results in the urlcache.dat file. You can also run the CLI commands `fortiwmf.exe -s fd_01` and `fortiproxy.exe -s fd_01 -d 4` in elevated mode, to further troubleshoot webfilter issues.

The above commands provide debug level logs for web filter and FortiProxy processes.

DO NOT REPRINT
© FORTINET

FortiClient Features—IPsec VPN

- Files and drivers
 - ipsec.exe (IPsec daemon)
 - FCAuth.exe (involved in IPsec certificate)
 - Fortips.sys
 - FortiFilter.sys
 - ftnic.sys
- Registry
 - FA_IKE
 - IPsec
 - FA_VPN
 - FA_Scheduler\000002
- XML
 - <forticlient_configuration><vpn><options>
 - <forticlient_configuration><vpn><ipsecvpn>

FortiClient requires a number of files and drivers for IPsec VPN. The VPN-related information is contained inside the `VPN` XML tags. The `options` XML tag contains global options that apply to both SSL VPN and IPsec VPN, as shown in this slide.

The `ipsecvpn` XML tag contains configurations specifically related to IPsec VPN.

IPsec VPN has two subsections:

- Options: options related to the specific type of VPN
- Connections: user-defined connections

FortiClient Features—IPsec VPN (Contd)

- FortiClient logs
 - Change log level to **Debug**
 - Optionally, disable other types of logging

Settings > Logging > Export logs

```

2:51:25 PM Debug VPN ==
2:51:25 PM Debug VPN initiate new phase 1 negotiation: 172.26.33.156[500]<=>10.0.0.1[500]
2:51:25 PM Debug VPN begin Aggressive mode.
2:51:25 PM Debug VPN new cookie: e710f7549f544d54
2:51:25 PM Debug VPN use ID type of IPv4 address
2:51:25 PM Debug VPN compute DH's private.
2:51:25 PM Debug VPN 7466cad5 77673ec1 717f3443 c2909c48 f62f7209 95eef934 826ba073 1bf914fe
2:51:25 PM Debug VPN compute DH's public.
2:51:25 PM Debug VPN 81614101 8218c29b 5ab9ec58 138dd412 3d5abb34 23d69c9b b3117092 45575831
2:51:25 PM Debug VPN authmethod is p2f-shared key
2:51:25 PM Debug VPN add payload of len 96, next type 9
2:51:25 PM Debug VPN add payload of len 192, next type 10
2:51:25 PM Debug VPN add payload of len 16, next type 5
2:51:25 PM Debug VPN add payload of len 8, next type 13
2:51:25 PM Debug VPN add payload of len 16, next type 13
2:51:25 PM Debug VPN (repeated 3 times in last 0 sec) add payload of len 16, next type 13
2:51:25 PM Debug VPN add payload of len 8, next type 13
2:51:25 PM Debug VPN add payload of len 16, next type 13
2:51:25 PM Debug VPN (repeated 1 times in last 0 sec) add payload of len 16, next type 13
2:51:25 PM Debug VPN add payload of len 16, next type 0
2:51:25 PM Debug VPN 508 bytes from 172.26.33.156[500] to 10.0.0.1[500]
2:51:25 PM Debug VPN sockname 0.0.0.0[500]
2:51:25 PM Debug VPN send packet from 172.26.33.156[500]
2:51:25 PM Debug VPN send packet to 10.0.0.1[500]
2:51:25 PM Debug VPN 1 times of 508 bytes message will be sent to 10.0.0.1[500]
2:51:25 PM Debug VPN e710f754 9f544d54 00000000 00000000 01100400 00000000 000001fc 04000064
2:51:25 PM Debug VPN resend phase1 packet e710f7549f544d54:0000000000000000
2:51:25 PM Information VPN id=96566 msg="negotiation information, loc_ip=172.26.33.156 loc_por
2:51:27 PM Debug VPN CHKPHTHERE: no established ph1 handler found
2:51:27 PM Debug VPN (repeated 1 times in last 1 sec) CHKPHTHERE: no established ph1 handle

```

You can request VPN-related logs through FortiClient EMS or export logs using the **Export logs** pane of FortiClient. When troubleshooting VPN issues, as a best practice, change the log level to **Debug** and disable other types of logging to minimize the logs from other features.

The FortiClient-FortiGate dialup request is sent from FortiClient toward FortiGate. FortiClient-FortiGate negotiates using aggressive mode. In aggressive mode, the IKE SA contains almost everything, such as the encryption type, length, hash type, and Diffie-Hellman (DH) group. It contains fewer exchanges and packets and is faster than main mode.

FortiClient Features—IPsec VPN Debug

- Debug
 - Change log level on FortiClient
 - Enable IKE debug on FortiGate
 - `diag debug application ike -1`
 - `diag debug application fnbamd -1`
 - `diag debug enable -1`
- Capture network traffic on both FortiClient host and FortiGate
- You can also initiate IPsec on the CLI
 - `ipsec.exe [-d debuglevel] [-i sessionid] [-b] [-k] tunnel`
 - `ipsec.exe -U fortinet -P st70ngP@ssw07d prague_off`

You can run the real-time debug commands on FortiGate, which will show you similar information as on FortiClient.

As a best practice, run the debug commands on FortiGate to compare with the IPsec VPN logs on FortiClient.

Apart from the real-time debug command shown on this slide, you can also run the following commands on FortiGate to troubleshoot IPsec VPN issues:

- The `diagnose vpn ike config list` command checks the configuration as it is seen by IKE daemon on the FortiGate device
- To list IKE SA on FortiGate, run `diagnose vpn ike gateway list`.
- To list IPsec SA on FortiGate, run `diagnose vpn tunnel list`.
- To check the status of all tunnels (equivalent to the GUI VPN monitor) on FortiGate, run `get ipsec tunnel list`.
- To check routes on FortiGate that were installed by the IKE daemon (applicable only for dialup IPsec VPN), run `diagnose vpn ike routes list`.

DO NOT REPRINT
© FORTINET

FortiClient Features—SSL VPN

- Files and drivers
 - FortiSSLVPNdaemon.exe
 - ftsvnic.sys
- Registry
 - FA_SSLVPN
 - Sslvpn
 - FA_VPN
 - FA_Scheduler\000019
- XML
 - `<forticlient_configuration><vpn><sslvpn>`

FortiClient requires a number of files and drivers for SSL VPN.

The `sslvpn` XML tag contains configurations specifically related to SSL VPN.
SSL VPN has two subsections:

- Options: options related to the specific type of VPN
- Connections: user-defined connections

FortiClient Features—SSL VPN (Contd)

- FortiClient logs
 - Change log level to Debug
 - Optionally disable other types of logging

SSL VPN initiated

```

3:53:03 PM Debug VPN (repeated 162 times in last 324 sec) FortiSslvpn: CSslvpnBase::RefreshConnection() Called.
3:53:05 PM Debug VPN FortiSslvpn: proxy flag: 1 proxy: (null)
3:53:05 PM Debug VPN FortiSslvpn: CSslvpnBase::OnConnect(): Before check server TCP port. *****
3:53:05 PM Debug VPN FortiSslvpn: CSslvpnBase::InitFortiSslvpn() Called.
3:53:05 PM Debug VPN FortiSslvpn: CSslvpnBase::InitFortiSslvpn(): Daemon is running
3:53:05 PM Debug VPN FortiSslvpn: SslvpnAgent: before connect pipe
3:53:05 PM Debug VPN FortiSslvpn: SslvpnAgent: before create file
3:53:05 PM Debug VPN FortiSslvpn: SslvpnAgent: ActiveX connected to SslvpnDaemon
3:53:05 PM Debug VPN FortiSslvpn: CSslvpnBase::InitFortiSslvpn(): SslvpnAgent initialized successfully
3:53:05 PM Debug VPN FortiSslvpn: >>>>DoConnect(fr.Fortinet-ems.com:443) ...
3:53:05 PM Debug VPN FortiSslvpn:
3:53:05 PM Debug VPN FortiSslvpn: GetWebPage(): URL=/remote/info -->
3:53:05 PM Debug VPN FortiSslvpn: =====
3:53:05 PM Debug VPN FortiSslvpn: <?xml version='1.0' encoding='utf-8'?><info><api_enomethod='0' salt='51479555' remoteauthtimeout='30' f='f' /></info>
3:53:05 PM Debug VPN FortiSslvpn: =====
3:53:05 PM Debug VPN FortiSslvpn: GetWebPage(): bRC=1,CT=(text/xml; charset=utf-8)

```

VPN connected

```

3:53:27 PM Information VPN FortiSslvpn: 7624: fortissl connect: device=fvyn10
3:53:27 PM Information VPN FortiSslvpn: 13908: PreferDtlsTunnel=0
3:53:28 PM Debug VPN FortiSslvpn: <<<<DoConnect(): bRC=1, ErrorCode=0
3:53:28 PM Debug VPN FortiSslvpn: CSslvpnBase::OnConnect(): DoConnect()==TRUE *****
3:53:28 PM Debug VPN FortiSslvpn: CSslvpnBase::OnConnect(): SSL VPN Tunnel is Connected *****
3:53:28 PM Debug VPN FortiSslvpn: CSslvpnBase::RefreshConnection() Called.
3:53:31 PM Debug VPN (repeated 2 times in last 4 sec) FortiSslvpn: CSslvpnBase::RefreshConnection() Called.
3:53:34 PM Notice VPN date=2019-02-26 time=15:53:33 logver=1 type=traffic level=notice sessionid=l65643392 hostname= pcdomain
3:53:34 PM Information VPN id=96600 user=" " msg="SSLVPN tunnel status" vpnstate=connected vpntunnel="SSL - " vpntype="ssl"

```

You can request VPN-related logs through FortiClient EMS or export logs using **Export logs** pane of FortiClient. When troubleshooting VPN issues, as a best practice change the log level to **Debug** and disable other types of logging to minimize the logs from other features.

The FortiClient-FortiGate SSL VPN request is sent from FortiClient towards FortiGate. FortiClient-FortiGate checks the port number for the SSL VPN service and user credentials to allow access. The SSL debug logs show the initial connection request made by FortiClient to FortiGate. Then the SSL certificate negotiation takes place between FortiClient and FortiGate. The FortiClient side certificate information is located in the `Installation directory\Fortinet\FortiClient` folder.

DO NOT REPRINT
© FORTINET

FortiClient Features—SSL VPN Debug

- Debug
 - Change log level on FortiClient
 - Enable SSL VPN debug on FortiGate
 - `diag debug application sslvpn -l`
 - `diag debug application fndamd -l`
 - `diag debug enable -l`
- Capture network traffic on both FortiClient host and FortiGate
- You can also initiate SSL on the CLI
 - `FortiSSLVPNclient.exe /?`
 - `FortiSSLVPNclient.exe connect -h 172.17.61.48:443 -u test:111111 -c client_cert -i`
 - `FortiSSLVPNclient.exe disconnect`

You can run real-time debug commands on FortiGate, which will show you the information that is similar to the information shown on FortiClient.

As a best practice, run the debug commands on FortiGate to compare them with the SSL VPN logs on FortiClient.

DO NOT REPRINT
© FORTINET

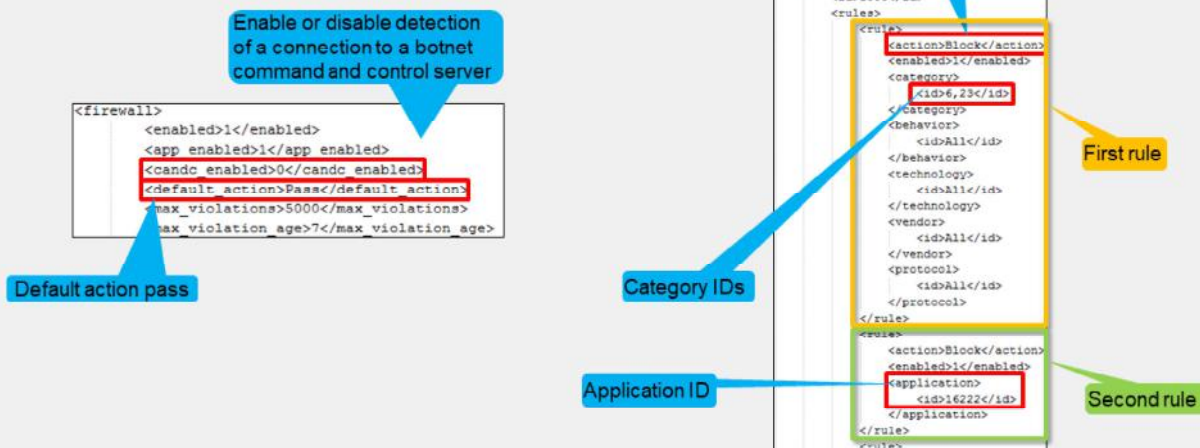
FortiClient Features—Application Firewall

- Configured on FortiGate or FortiClient EMS
- Files and drivers:
 - fcappdb.exe
 - fcappdb.db
 - xmlfw.dll
 - fortiws.exe
 - fortiapd.sys
 - fortifw2.sys
- vir_sig folder contains:
 - appsig.dat
 - ids.dat

An application firewall uses an IPS engine, so it matches the patterns in the entire byte stream of the packet and requires multiple files and drivers.

FortiClient Features—Application Firewall

- Check XML configuration
 - `<forticlient_configuration><vpn><firewall>`



The application firewall XML configuration elements can be grouped into two parts: general options and profiles. A general option applies to all firewall activities and a profile defines the applications and the actions that apply to the firewall activities.

You can enable the `candc_enabled` XML configuration element by setting the value equal to 1, to detect a connection to a botnet command and control server. The `default_action` XML configuration element value is set to `pass`, which enforces the action to pass on traffic that doesn't match any defined profiles. You can change the default action to `block`, `reset`, or `pass`. The `profiles` tag has a `rules` element. The `rules` element may have zero or more `rule` tags.

The following filter elements can be used to define applications in a `rule` tag:

- `category`
- `vendor`
- `behavior`
- `technology`
- `protocol`
- `application`
- `popularity`

If the `application` element is present, all other sibling elements (listed above) will be ignored. If it is not present, a given application must match all of the provided filters to trigger the rule.

In the example shown on this slide, in the first rule, categories 6 and 23 are blocked, which corresponds to Proxy and Social.Media respectively. In the second rule, application 16779 is blocked, which is Yahoo.Games. You can get the complete list of IDs corresponding to each category, behavior, and application on the FortiGate CLI.

DO NOT REPRINT
© FORTINET

FortiClient Features—Application Firewall (Contd)

- FortiClient logs
 - View recent violations on FortiClient GUI



Settings > Logging > Export logs

```
xx/xx/20xx 9:05:05 AM Notice Firewall date=20xx-xx-xx time=09:05:04 logver=2 type=traffic level=notice sessionid=34252360
hostname=Win-Internal uid=C7F30281D3E84F05A77E38AD62028B07 devid=FC78003611939390 fgtserial=FGVM010000042532 regip=N/A
srcname=firefox.exe srcproduct=Firefox srcip=10.0.1.10 srcport=62401 direction=outbound destinationip=199.59.148.82 remotename=N/A
destinationport=80 user=Administrator@TRAININGAD.TRAINING.LAB proto=6 rcvbyte=N/A sentbyte=N/A utmaction=blocked utmevent=appfirewall
threat=Twitter vd=root fctver=5.4.0.0780 os="Microsoft Windows Server 2012 R2 Standard Edition, 64-bit (build 9600)"
usingpolicy=default service=http

|
xx/xx/20xx 9:05:54 AM Notice Firewall date=20xx-xx-xx time=09:05:53 logver=2 type=traffic level=notice sessionid=34252360
hostname=Win-Internal uid=C7F30281D3E84F05A77E38AD62028B07 devid=FC78003611939390 fgtserial=FGVM010000042532 regip=N/A
srcname=firefox.exe srcproduct=Firefox srcip=10.0.1.10 srcport=62425 direction=outbound destinationip=104.25.62.28 remotename=N/A
destinationport=443 user=Administrator@TRAININGAD.TRAINING.LAB proto=6 rcvbyte=N/A sentbyte=N/A utmaction=blocked
utmevent=appfirewall threat=Proxy.Websites vd=root fctver=5.4.0.0780 os="Microsoft Windows Server 2012 R2 Standard Edition, 64-bit
(build 9600)" usingpolicy=default service=https

xx/xx/20xx 9:28:23 AM Notice Firewall date=20xx-xx-xx time=09:28:22 logver=2 type=traffic level=notice sessionid=26453064
hostname=Win-Internal uid=C7F30281D3E84F05A77E38AD62028B07 devid=FC78003611939390 fgtserial=FGVM010000042532 regip=N/A
srcname=firefox.exe srcproduct=Firefox srcip=10.0.1.10 srcport=62759 direction=outbound destinationip=208.71.44.31 remotename=N/A
destinationport=80 user=Administrator@TRAININGAD.TRAINING.LAB proto=6 rcvbyte=N/A sentbyte=N/A utmaction=blocked utmevent=appfirewall
threat=Yahoo.Games vd=root fctver=5.4.0.0780 os="Microsoft Windows Server 2012 R2 Standard Edition, 64-bit (build 9600)"
usingpolicy=default service=http
```

- Common issues
 - Traffic is blocked, applications crash or are not categorized correctly

You can view the application violation logs directly on the FortiClient GUI, request them through FortiClient EMS or export logs using the **Export logs** pane on FortiClient.

In the example shown on this slide, FortiClient blocks two categories (proxy and Social.Media) and the application Yahoo.Games, when FortiClient inspects the traffic passing through it and, based on the matching rule, takes action. In this example, FortiClient blocks Twitter, proxy websites, and Yahoo.Games, based on the defined rule.

Some common issues are blocked traffic, and applications that crash or are not categorized correctly. Try to disable FortiClient features one by one, to make sure the issue is caused by the application firewall.

FortiClient Features—Vulnerability Scan

- Files and drivers
 - VCM daemon: Fcvbltscan.exe
 - VCM engine: vcm2.exe
 - VCM signature: vcm.dat
- Registry
 - FA_VULN
 - FA_Schedule/000020
- Check XML configuration
 - <forticlient_configuration><vulnerability_scan>
- FortiClient logs
 - View vulnerabilities detected on FortiClient

```
<vulnerability_scan>
<enabled>1</enabled>
<scan_on_fgt_registration>0</scan_on_fgt_registration>
<scheduled_scans>
  <schedule>
    <enable_schedule>0</enable_schedule>
    <repeat>0</repeat>
    <type>24</type>
    <day>3</day>
    <time>19:30</time>
  </schedule>
</scheduled_scans>
</vulnerability_scan>
```

Settings > Logging > Export logs

```
xx/xx/20xx 10:07:25 AM Notice Vulnerability Scan id=96520 user=Administrator@TRAININGAD.TRAINING.LAB
msg="The vulnerability scan status has changed" status=started vulncat=N/A vulncvss=N/A vulnengine=N/A vulnid=N/A
vulnname=N/A vulnref=N/A vulnseverity=N/A

xx/xx/20xx 10:08:35 AM Notice Vulnerability Scan id=96521 user=Administrator@TRAININGAD.TRAINING.LAB
msg="A vulnerability scan result has been logged" status=failed vulncat=N/A vulncvss=N/A vulnengine=N/A vulnid=N/A
vulnname=MS.Windows.Enabled.Cached.Logon.Credential vulnref=msw.fortinet.com/ids/VID20762 vulnseverity=Medium
```

The FortiClient vulnerability scan module can check your workstation for known system vulnerabilities. It uses various files and drivers to perform a vulnerability scan. You can scan your workstation when registering on FortiGate, or on a scheduled basis. Or you can run an on-demand scan directly on the FortiClient GUI and view the vulnerabilities found on the FortiClient console.

You can view the recent vulnerabilities detected directly on the FortiClient GUI, or you can export logs through FortiClient EMS or use the **Export logs** option on the FortiClient settings.

The vulnerabilities logs shows the status (started, cancelled) and also shows the name of the vulnerabilities detected, the severity, the vulnerabilities engine, signatures used, and so on. It also provides a reference link, which provides the description, impact, and recommended actions for the vulnerability detected.

DO NOT REPRINT
© FORTINET

Vulnerability Scan—Debug

- Run debug from command line in elevated mode
 - Run VCM scan
 - `fcVlbtScan.exe -s fd_01 -d -n`
 - Run VCM patch
 - `fcVlbtScan.exe -s fd 01 -d -p path to install.json`
- Log file
 - `Forticlient_install_folder/logs/vcm/timestamp_folder`

You can run a vulnerability scan in debug mode on the command line in elevated mode. After running the commands shown on this slide, the log file will be available at the following location:

`Forticlient_install_folder/logs/vcm/timestamp_folder`

DO NOT REPRINT
© FORTINET

Knowledge Check

1. Which file is responsible for the FortiClient antivirus function?

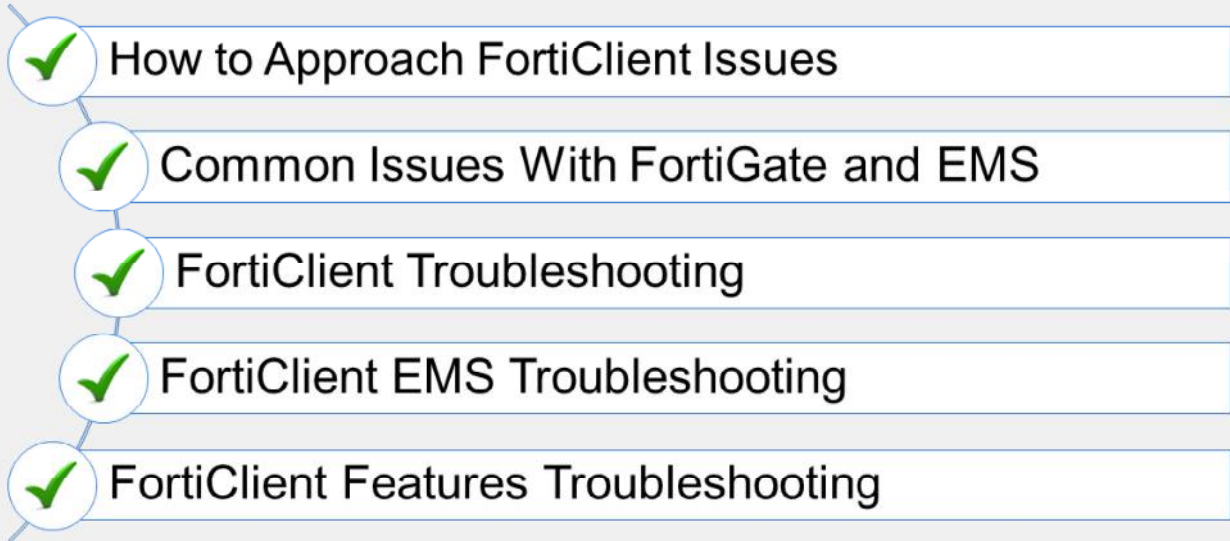
- ✓ A. fmon.exe
- B. fcappdb.exe

2. Which process is responsible for scheduled AV scans?

- A. fmon.exe
- ✓ B. av_task.exe

DO NOT REPRINT
© FORTINET

Lesson Progress



Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in this lesson.

DO NOT REPRINT
© FORTINET

Review

- ✓ Approach and troubleshoot FortiClient and FortiClient EMS issues
- ✓ Understand the diagnostic steps to troubleshoot issues between FortiClient, FortiClient EMS, and FortiGate
- ✓ Understand FortiClient components on Windows
- ✓ Understand FortiClient EMS components on Windows
- ✓ Diagnose FortiClient features

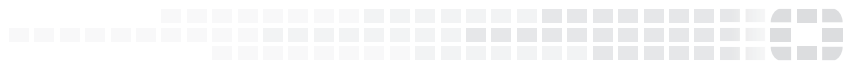
This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned how to approach FortiClient issues and common issues with FortiClient with FortiGate and EMS and how to diagnose and troubleshoot FortiClient features.

DO NOT REPRINT
© FORTINET



FORTINET®



No part of this publication may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from Fortinet Inc., as stipulated by the United States Copyright Act of 1976.

Copyright© 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.