FortiClient

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

Security Fabric Integration

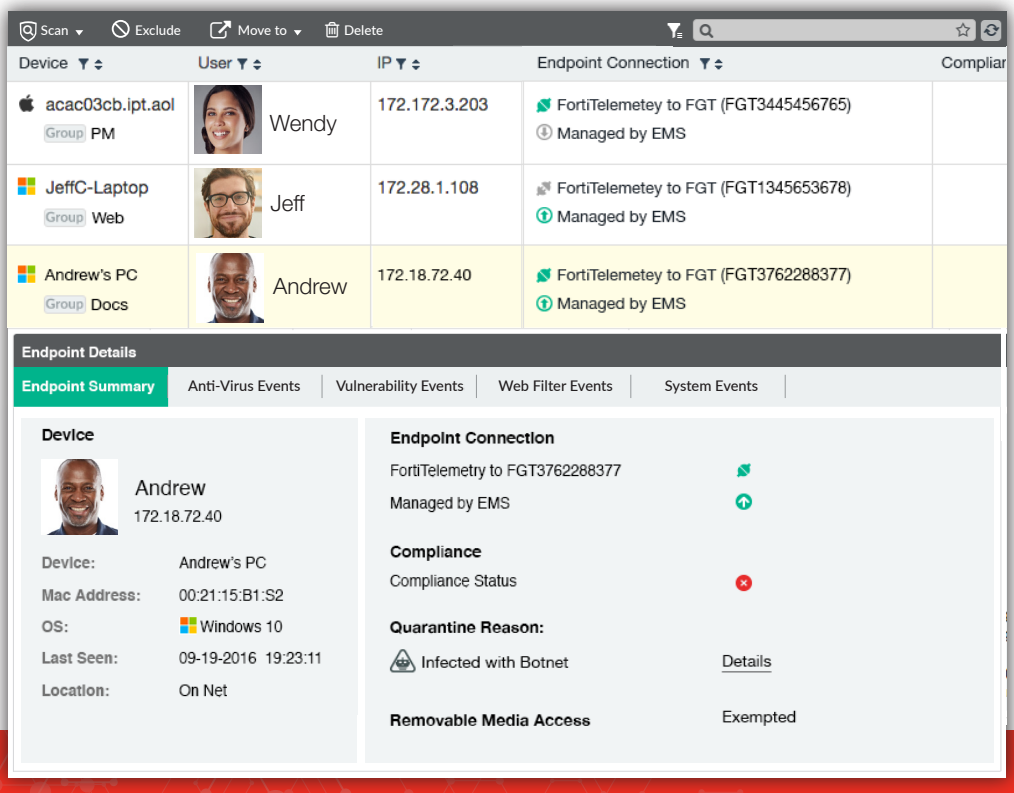
Provides endpoint awareness, compliance and enforcement by sharing endpoint telemetry.

Advanced Threat Protection

Automates prevention of known and unknown threats through built-in host-based security stack and integration with FortiSandbox.

Secure Remote Access & Mobility

Easy-to-use secure remote access via SSL and IPsec VPN.



EMS for Central Management

- Simple & User Friendly UI
- Remote FortiClient Deployment
- Realtime Dashboard
- Active Directory Integration
- Automatic Email Alerts
- Supports Custom Groups
- Remote Triggers

FortiClient connects every endpoint to form a cohesive security fabric

Advanced Threat Protection

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

Security Fabric Integration

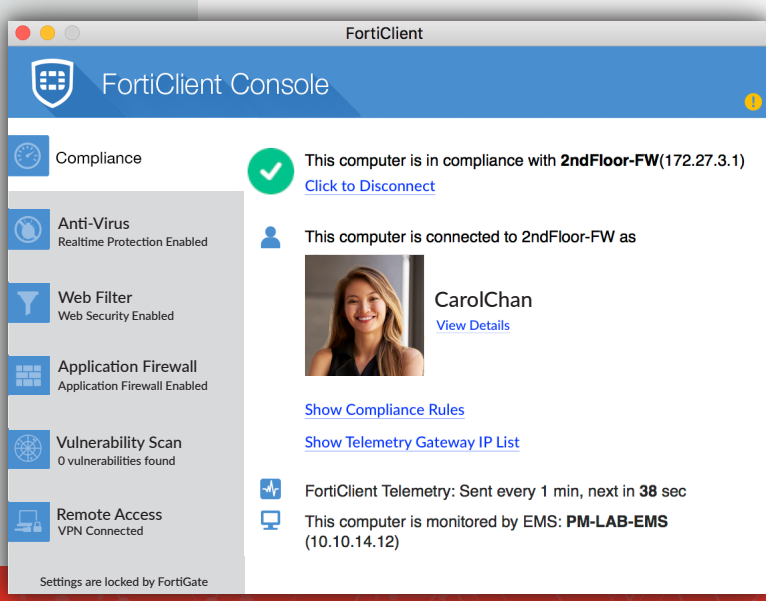
As a key piece of the Fortinet Security Fabric, FortiClient integrates the endpoints into the fabric for early detection and prevention of advanced threats. Security events including zero-day malware, botnet detections, and vulnerabilities are reported in real-time. The deep real-time visibility into the network allows administrators to investigate and remotely quarantine compromised endpoints. Our endpoint compliance & vulnerability detection features enables simplified enforcement of enterprise security policies protecting endpoints from becoming easy targets.

Secure Remote Access & Mobility

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

Anti-Exploit adds another layer of protection.
It protects against zero-day attacks that target applications that have undiscovered or unpatched vulnerabilities without relying on signatures like traditional anti-virus.

- **Protects against zero-day** attacks targeting undiscovered or unpatched application vulnerabilities
- **Protects against various memory techniques** used in an exploit
- **Shields web browsers,** Java/Flash plug-ins, Microsoft Office applications, and PDF Reader
- **Detects and Blocks** the use of exploit kits
- **Signature-less** solution

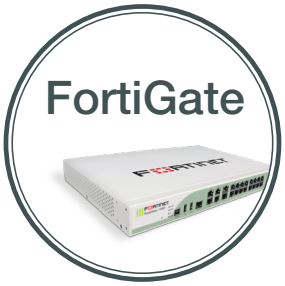


Key Features

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

- **Remote FortiClient Deployment** that allows administrators to remotely deploy endpoint software and perform controlled upgrades.
- **Centralized Client Provisioning** makes depoying FortiClient configuration to thousands of clients an effortless task with a click of a button.
- **Windows AD Integration** helps sync organisations AD structure into EMS so same OUs can be used for endpoint management.
- **Realtime Endpoint Status** always provides current information on endpoint activity & security events.
- **Vulnerablity Dashboard** helps manage organizations attack surface. All vulnerable endpoints are easily identified for administrative action.
- **Email Alerts** helps notify administrators of any critical events so they can be attended on priority.

FortiGate provide awareness and control over all your endpoints



- **Telemetry** provides real-time endpoint visibility (including user avatar) on FortiGate console so administrators can get a comprehensive view of the whole network.
- **Compliance Enforcement** can be used to enforce organisations security policies. Only authorized and compliant endpoints with no security risks are granted access.
- **Endpoint Quarantine** helps to quickly disconnect a compromised endpoint from the network and stop it from infection other assets.

FortiClient EMS and FortiGate Endpoint Licenses

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

PLUS - STARTING FCT 5.6 THE FORTICLIENT CUSTOM INSTALLER TOOL IS AVAILABLE FOR FREE ON FNDN.
REBRANDING TOOL REQUIRES AN FNDN SUBSCRIPTION

Compatibility

	WINDOWS	MAC OS X	ANDROID	iOS	ChromeBook	Linux
SECURITY FABRIC COMPONENTS						
Endpoint Telemetry[1]	✓	✓	✓	✓	✓	
Compliance Enforcement[1]	✓	✓	✓	✓		
Endpoint Audit and Remediation with Vulnerability Scanning[1]	✓	✓				
HOST SECURITY AND VPN COMPONENTS						
Antivirus	✓	✓				
Anti-Exploit	✓					
Sandbox Detection	✓					
Web Filtering[2]	✓	✓	✓	✓	✓	
Application Firewall[1]	✓	✓				
IPSec VPN	✓	✓	✓	✓		
SSL VPN[3]	✓	✓	✓	✓		✓
OTHERS						
Remote Logging and Reporting[4]	✓	✓		✓	✓	
Windows AD SSO Agent	✓	✓				

PLUS - **ADVANCED THREAT PROTECTION COMPONENTS FOR WINDOWS:** File Analysis with FortiSandbox and Host Quarantine Enforcement[1]

[1] Requires FortiClient to be managed by EMS [2] Also compatible in Chrome OS [3] Also compatible in Windows Mobile. The list above is based on the latest OS for each platform.
[4] Requires FortiAnalyzer

Order Information

PRODUCT	SKU	DESCRIPTION
Enterprise Management Server Endpoint License for 100 clients	FC1-15-EMS01-158-02-DD	FortiClient Enterprise Management Server License subscription for 100 clients. Includes 24x7 support.
FortiClient Chromebook Enterprise Management Server License for 100 users	FC1-15-EMS02-158-02-DD	Chromebook Enterprise Management Server License subscription for 100 ChromeOS users. Includes 24x7 support
FortiClient Telemetry License for 100 Clients	FC1-10-C1100-151-02-DD	Endpoint Telemetry & Compliance License subscription for 100 clients. Includes 24x7 support. Note1: Compatible with FortiOS 5.6 and above only; Note2: Refer to the FortiOS admin guide for specific platform restrictions and maximum license limit.

FortiGuard Security Services
www.fortiguard.com

FortiCare Worldwide 24/7 support
support.fortinet.com

Specifications

FORTICLIENT

Operating System Supported:
Microsoft Windows 10, 8.1, 7, Windows Server 2008 R2 and Windows Server 2012, 2012 R2, 2016
Mac OS X v10.12, v10.11, v10.10, v10.9, v10.8
iOS 5.1 or later (iPhone, iPad, iPod Touch)
Android OS 4.4.4 or later (phone and tablet)

Authentication Options
RADIUS, LDAP, Local Database, xAuth, TACACS+, Digital Certificate (X509 format), FortiToken

Connection Options
Auto Connect VPN before Windows logon, IKE Mode config for FortiClient VPN IPsec tunnel

Note: All specifcations are based on FortiClient 5.6.

FORTICLIENT EMS

Operating System Supported
Microsoft Windows Server 2016, 2012, 2012 R2, 2008 R2

Endpoint Requirement
FortiClient version 5.6 or newer, FortiClient for Microsoft Windows and Mac OS X, 5.4 for iOS and Android

System Requirements
2.0 GHz 64-bit processor, dual core (or two virtual CPUs), 4 GB RAM, 20 GB free hard disk, Gigabit (10/100/1000BaseT) Ethernet adapter Internet access

CERTIFIED

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
Valbonne 06560
Alpes-Maritimes, France
Tel: +33.4.8987.0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6395.2788

LATIN AMERICA SALES OFFICE
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
United States
Tel: +1.954.368.9990

FST-PROD-DS-FCT

FCT-DAT-R17-201712