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

---

**FortiClient Console**
- Compliance
  - This computer is in compliance with 2ndFloor-FW (172.27.3.1)
- Anti-Virus
  - Realtime Protection Enabled
- Web Filter
  - Web Security Enabled
- Application Firewall
  - Application Firewall Enabled
- Vulnerability Scan
  - 0 vulnerabilities found
- Remote Access
  - VPN Connected
- CarolChan
  - View Details
  - Show Compliance Rules
  - Show Telemetry Gateway IP List
  - FortiClient Telemetry: Sent every 1 min, next in 38 sec
  - This computer is monitored by EWS: PM-LAB-EMS (10.10.10.12)

Settings are locked by FortiGate.
**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 deploying 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.
- **Vulnerability Dashboard** helps manage organisations 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.

---

**FortiClient EMS and FortiGate Endpoint Licenses**

<table>
<thead>
<tr>
<th>Feature</th>
<th>EMS License</th>
<th>FortiGate License</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PROVISIONING</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Centralized Client Provisioning</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Client Software Updates</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Windows AD Integration</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>FortiTelemetry Gateway IP List</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td><strong>COMPLIANCE ENFORCEMENT AND SECURITY FABRIC INTEGRATION</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fortinet Security Fabric Integration</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Security Posture Check</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Vulnerability Compliance Check</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Minimum System Compliance</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Authorized Device Detection</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td><strong>REMOTE CONTROL</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>On-demand Antivirus Scan</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>On-demand Vulnerability Scan</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Host Quarantine</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td><strong>TELEMETRY AND MONITORING</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Client Information (client version, OS IP/MAC address, profile assigned, user avatar)</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Client Status</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Reporting</td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>

**FortiGate**

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**

<table>
<thead>
<tr>
<th>Feature</th>
<th>EMS License</th>
<th>FortiGate License</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PROVISIONING</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Centralized Client Provisioning</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Client Software Updates</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Windows AD Integration</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>FortiTelemetry Gateway IP List</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td><strong>COMPLIANCE ENFORCEMENT AND SECURITY FABRIC INTEGRATION</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fortinet Security Fabric Integration</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Security Posture Check</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Vulnerability Compliance Check</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Minimum System Compliance</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Authorized Device Detection</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td><strong>REMOTE CONTROL</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>On-demand Antivirus Scan</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>On-demand Vulnerability Scan</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Host Quarantine</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td><strong>TELEMETRY AND MONITORING</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Client Information (client version, OS IP/MAC address, profile assigned, user avatar)</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Client Status</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Reporting</td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>

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

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-C1-100-151-02-DD Endpoint Telemetry & Compliance License subscription for 100 clients. Includes 24x7 support.

Note 1: Requires FortiGate Endpoint License. 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

FORTICLIENT

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

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

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

Note: All specifications are based on FortiClient 5.6.

Specifications

HOST SECURITY AND VPN COMPONENTS

Antivirus Anti-Exploit
Sandbox Detection Web Filtering
Application Firewall
IPSec VPN SSL VPN

OTHERS
Remote Logging and Reporting
Windows AD SSO Agent

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

Copyright© 2017 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.