FortiClient

Secure remote access with visibility and controls for Zero Trust Network Access (ZTNA)

FortiClient’s Security Fabric Integration provides endpoint visibility through telemetry and ensures that all fabric components – FortiGate, FortiAnalyzer, EMS, Managed AP, Managed Switches, and Sandbox – have a unified view of endpoints in order to provide tracking and awareness, compliance enforcement, and reporting. Fortinet extends ZTNA control to end-user devices both on- and off-network operation through FortiClient. Easy to use Secure Remote Access and Mobility via SSL and IPsec VPN. FortiClient connects every endpoint to form a cohesive security fabric.

Key Advantages

- **Unified endpoint** features including compliance, protection, and secure access into a single, modular lightweight client.
- **End-to-end threat visibility** and control by natively integrating endpoint into the Security Fabric architecture.
- **Advanced threat protection** against exploits and advanced malware, powered by FortiGuard along with FortiSandbox integration.
- **Integrated vulnerability shielding** and patch management to harden all endpoints.
- **Simplified management and policy enforcement** with Enterprise Management Server (EMS) and FortiGate, respectively.

EMS for Central Management

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

FortiGuard Security Services
www.fortiguard.com

FortiCare Worldwide
24/7 support
support.fortinet.com
FortiClient Benefits

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

Web Filtering and SAAS Control
FortiClient provides off network web filtering, delivering web security and content filtering. The web application firewall provides botnet protection and granular application traffic control including web-based applications and software as a service (Saas).

Zero Trust Network Access
Fortinet extends ZTNA control to end-user devices both on- and off-network operation through FortiClient. With FortiClient endpoint telemetry and risk assessment, Admin gain the critical endpoint visibility and can set conditional-access policies to control access from the endpoints. For example, limit a vulnerable endpoint from accessing critical areas of the network or even block VPN connection.

Secure Remote Access
To enable secure remote access, FortiClient provides flexible options for VPN connectivity. It supports both secure sockets layer (SSL) and Internet Protocol security (IPsec) VPNs. A split tunneling feature enables remote users on SSL VPNs to access the internet without their traffic having to pass through the corporate VPN headend, as in a typical SSL tunnel. This feature reduces latency, which improves user experience. At the same time, FortiClient includes protections to ensure that internet-based transactions cannot backflow into the VPN connection and jeopardize the corporate network.

In addition to simple remote connectivity, FortiClient simplifies remote user experience with features such as auto-connect and always-on VPN, as well as Dynamic VPN Gate Selection. Two-Factor authentication can also be used to provide an additional layer of security.

Endpoint Hygiene
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.

Malware and Exploit Prevention
By integrating with FortiSandbox Cloud and leveraging FortiGuard Global Threat Intelligence, FortiClient prevents advanced malware and vulnerabilities from being exploited. FortiClient integrates with FortiSandbox Cloud to 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 threat intelligence platform. FortiGuard automatically shares the intelligence with FortiClient endpoints to protect against emerging threats.
**Feature Highlights**

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

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

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

**Real-time Endpoint Status** always provides current information on endpoint activity & security events.

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

**Centralized FortiClient Deployment & Provisioning** allows administrators to remotely deploy endpoint software and perform controlled upgrades. Makes deploying FortiClient configuration to thousands of clients an effortless task with a click of a button.

Sandbox settings are automatically synchronized with EMS and detailed analysis of FortiClient submitted files for behavior based detection is accessible in EMS. Administrators can see all behavior activity of a file including graphic visualization of full process tree.

**FortiGate provides 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. Telemetry also ensures that all fabric components have a unified view of the endpoints.

**Dynamic Access Control for Compliance Enforcement** requires EMS to create virtual groups based on endpoint security posture. These virtual groups are then retrieved by FortiGate and used in firewall policy for dynamic access control. Dynamic groups help automate & simplify compliance to security policies.

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

**Automated Response** helps detect and isolate suspicious or compromised endpoints without manual intervention.

**Application-based Split Tunnel** supports source application-based split tunnel, where you can specify application traffic to exclude from the VPN tunnel, such as high bandwidth apps.

**Web Filtering with Keyword Search / YouTube Filters** blocks web pages containing words or patterns that you specify as well as limit users’ access by blocking or only allowing specified YouTube channels.

---

<table>
<thead>
<tr>
<th>SECURITY FABRIC AGENT</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Provisioning</strong></td>
</tr>
<tr>
<td>Centralized Client Provisioning</td>
</tr>
<tr>
<td>Client Software Updates</td>
</tr>
<tr>
<td>Windows AD Integration</td>
</tr>
<tr>
<td>FortiTelemetry Gateway IP List</td>
</tr>
<tr>
<td>Software Inventory</td>
</tr>
<tr>
<td>Automatic Group Assignment</td>
</tr>
<tr>
<td><strong>Compliance Enforcement and Security Fabric Integration</strong></td>
</tr>
<tr>
<td>Fortinet Security Fabric Integration</td>
</tr>
<tr>
<td>Security Posture Check</td>
</tr>
<tr>
<td>Vulnerability Compliance Check</td>
</tr>
<tr>
<td>Dynamic Access Control</td>
</tr>
<tr>
<td>Authorized Device Detection</td>
</tr>
<tr>
<td>Automated Endpoint Quarantine</td>
</tr>
<tr>
<td><strong>Remote Control</strong></td>
</tr>
<tr>
<td>On-demand Antivirus Scan</td>
</tr>
<tr>
<td>On-demand Vulnerability Scan</td>
</tr>
<tr>
<td>Host Quarantine</td>
</tr>
<tr>
<td><strong>Telemetry and Monitoring</strong></td>
</tr>
<tr>
<td>Client Information (client version, OS IP/MAC address, office assigned, user avatar)</td>
</tr>
<tr>
<td>Client Status</td>
</tr>
<tr>
<td>Reporting (to FortiAnalyzer)</td>
</tr>
</tbody>
</table>

PLUS - Add Sandbox Cloud Subscription for Proactive Advanced Threat Detection as well as other upcoming add-ons in the future.
Security Fabric Components

Endpoint Telemetry
Compliance Enforcement using Dynamic Access Control
Endpoint Audit and Remediation with Vulnerability Scanning
Automated Endpoint Guarantee
Host Security and VPN Components

Antivirus
Cloud-based Threat Detection
Anti-Exploit
Sandbox Detection (on-prem)
Sandbox Cloud Detection
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

Order Information

<table>
<thead>
<tr>
<th>Product</th>
<th>SKU</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FortiClient Security Fabric Agent</td>
<td>FC1-15-EMS01-299-02-DD</td>
<td>Security Fabric Agent with EPP license subscription for 25 endpoints. Includes Fabric Agent, Anti-Malware, Remote Access, Web Filter, Vulnerability Scan, Software Inventory, Application Firewall, SSOMA, Threat Outbreak Detection, Sandbox Agent with Cloud Sandbox subscription, Central Management and 24x7 Support</td>
</tr>
<tr>
<td>FortiClient Chromebook for 25 Clients</td>
<td>FC1-15-EMS01-403-02-DD</td>
<td>FortiClient Chromebook license subscription for 25 Chrome OS users. Includes Web Filter, Central Management and 24x7 Support</td>
</tr>
</tbody>
</table>