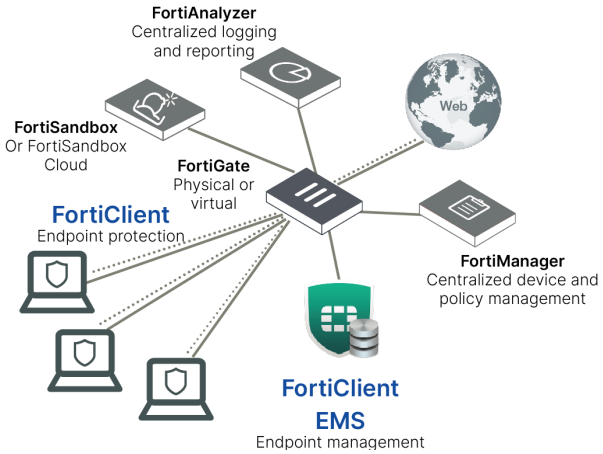
DATA SHEET

# FortiClient 7.0

## Visibility and Controls for Zero Trust Network Access (ZTNA) and Secure Access Service Edge (SASE)




FortiClient's 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. SASE cloud-based firewall protection is available on premium edition. Provide security and protection for endpoints when off the network.

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

**Zero Trust Applied**, with automatic, encrypted tunnels for controlled, validated, per-session access to applications.

**Advanced Threat Protection** against exploits and advanced malware, powered by FortiGuard along with FortiSandbox integration.

**Cloud-based Endpoint Security** from FortiSASE SIA services adds another layer of FortiOS-powered security.

**Simplified Management and Policy Enforcement** with Endpoint Management Server (EMS) and FortiGate, respectively.

## EMS for Central Management

- Simple and 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

# BENEFITS

## Security Fabric Integration

FortiClient integrates the endpoints into Fortiner's Security Fabric for early detection and prevention of advanced threats. This integreation 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 and 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

FortiClient ZTNA works with FortiOS to enable secure, granular access to applications no matter if the user is on-net or off-net. 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.

### 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.

### Virtual Private Network (VPN)

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.

### Enable SASE Secure Internet Access (SIA)

FortiSASE SIA™ is a Security-as-a-Service deployed via FortiClient SASE edition. 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-Net 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.

For more information on FortiSASE go to https://www.fortinet.com/products/sase.

# 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 licence management to improve security hygiene. You can use inventory information to detect and remove unnecessary or outdated applications that might have vulnerabilities to reduce your attack surface.

**Windows AD Integration** helps sync 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 and security events.

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

**Centralized FortiClient Deployment and Provisioning** that 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 and 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.

# BUNDLES

| FORTICLIENT EDITION | ZTNA | EPP / APT | SASE SIA | CHROMEBOOK |
|---|---|---|---|---|
| **Zero Trust Security** | **Windows, Mac, Linux** | **Windows, Mac, Linux** | **Windows, Mac, Linux** | **Chromebook** |
| **Zero Trust Agent with MFA** | ✓ | ✓ | ✓ | |
| **Central Management via EMS** | ✓ | ✓ | ✓ | ✓ |
| **Central Logging & Reporting** | ✓ | ✓ | ✓ | ✓ |
| **Dynamic Security Fabric Connector** | ✓ | ✓ | ✓ | |
| **Vulnerability Agent & Remediation** | ✓ | ✓ | ✓ | |
| **SSL VPN with MFA** | ✓ | ✓ | ✓ | |
| **IPSEC VPN with MFA** | ✓ | ✓ | ✓ | |
| **FortiGuard Web Filtering** | ✓ | ✓ | ✓ | ✓ |
| **USB Device Control** | ✓ | ✓ | ✓ | |
| **Next Generation Endpoint Security** | | | | |
| **AI powered NGAV** | | ✓ | ✓ | |
| **FortiClient Cloud Sandbox**[1] | | ✓ | ✓ | |
| **Automated Endpoint Quarantine** | | ✓ | ✓ | |
| **Application Firewall**[1] | | ✓ | ✓ | |
| **Application Inventory** | | ✓ | ✓ | |
| **Ransomware Protection**[2] | | ✓ | ✓ | |
| **Cloud Based Endpoint Security** | | | | |
| **SSL Inspection** | | | ✓ | |
| **Inline AV & Anti-Malware** | | | ✓ | |
| **Intrusion Prevention (IPS)** | | | ✓ | |
| **FortiGuard Web Filtering** | | | ✓ | |
| **DNS Security** | | | ✓ | |
| **Data Leak Prevention** | | | ✓ | |
| **Additional Services** | | | | |
| **Cloud Hosted EMS** | | Add-on | | |
| **24×7 Support** | | Included | | |
| **FortiCare BPS** | | Included first year | | |

1. FortiClient (Linux) does not support this feature.
2. Only FortiClient (Windows) supports this feature.


# FEATURES PER PLATFORM AND REQUIREMENTS

| | WINDOWS | MACOS | ANDROID | IOS | CHROMEBOOK | LINUX |
|---|---|---|---|---|---|---|
| **Security Fabric Components** | | | | | | |
| Endpoint Telemetry[1] | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Compliance Enforcement Using Dynamic Access Control[1] | ✓ | ✓ | ✓ | ✓ | | ✓ |
| Endpoint Audit and Remediation with Vulnerability Scanning | ✓ | ✓ | | | | ✓ |
| Automated Endpoint Quarantine | ✓ | ✓ | | | | |
| **Host Security and VPN Components** | | | | | | |
| Antivirus | ✓ | ✓ | | | | ✓ |
| Cloud-based Threat Detection | ✓ | ✓ | | | | |
| AntiExploit | ✓ | | | | | |
| Sandbox Detection (On-premise) | ✓ | ✓ | | | | ✓[5] |
| Sandbox Cloud Detection | ✓ | ✓ | | | | |
| Web Filter[2] | ✓ | ✓ | ✓ | ✓ | ✓ | |
| Application Firewall | ✓ | ✓ | | | | |
| IPsec VPN | ✓ | ✓ | ✓ | | | |
| SSL VPN[3] | ✓ | ✓ | ✓ | ✓ | | ✓ |
| **Other** | | | | | | |
| Remote Logging and Reporting[4] | ✓ | ✓ | | ✓ | ✓ | ✓ |
| Windows AD SSO Agent | ✓ | ✓ | | | | |
| USB Device Control | ✓ | ✓ | | | | ✓ |

**PLUS - Add Sandbox Cloud susbcription for Proactive Advanced Threat Detection.**

1. Requires FortiClient to be managed by EMS.
2. Also compatible in Chrome OS.
3. Also compatible in Windows mobile.
4. Requires FortiAnalyzer.
5. No file submission.

The above list is based on the latest OS for each platform.

| FORTICLIENT |
|---|
| **Supported Operating Systems*** |
| Microsoft Windows 7 (32-bit and 64-bit) |
| Microsoft Windows 8, 8.1 (32-bit and 64-bit) |
| Microsoft Windows 10 (32-bit and 64-bit) |
| Microsoft Windows Server 2008 or later |
| macOS 11+, 10.15, 10.14 |
| iOS 9.0 or later |
| Android 5.0 or later |
| Linux Ubuntu 16.04 and later, Red Hat 7.4 and later, CentOS 7.4 and later with KDE or GNOME |
| **Authentication Options** |
| RADIUS, LDAP, local database, xAuth, TACACS+, digital certificate (X509 format), FortiToken |
| **Connection Options** |
| Autoconnect VPN before Windows logon |
| IKE mode configuration for FortiClient IPsec VPN tunnel |

* FortiClient 6.2.0 does not support Windows XP or Vista.

| FORTICLIENT EMS |
|---|
| **Supported Operating Systems** |
| Microsoft Windows Server 2012 or later |
| **Endpoint Requirement** |
| FortiClient 6.0 or later, FortiClient for Windows and macOS X, 6.0 for iOS and Android |
| **System Requirements** |
| 2.0 GHz 64-bit processor, four virtual CPUs, 4 GB RAM, 40 GB free hard disk, Gigabit (10/100/1000BaseT) |
| Ethernet adapter, Internet access |

# ORDER INFORMATION

| EDITION | ZTNA | EPP/APT | SASE/SIA | CHROMEBOOK |
|---|---|---|---|---|
| **PaaS (Cloud Hosted EMS)** | | | | |
| **25-pack (add)** | FC1-10-EMS05-370-01-DD | FC1-10-EMS05-371-01-DD | FC1-10-EMS05-372-01-DD | FC1-10-EMS05-373-01-DD |
| **500-pack (add)** | FC2-10-EMS05-370-01-DD | FC2-10-EMS05-371-01-DD | FC2-10-EMS05-372-01-DD | FC2-10-EMS05-373-01-DD |
| **2000-pack (add)** | FC3-10-EMS05-370-01-DD | FC3-10-EMS05-371-01-DD | FC3-10-EMS05-372-01-DD | FC3-10-EMS05-373-01-DD |
| **10,000 pack (add)** | FC4-10-EMS05-370-01-DD | FC4-10-EMS05-371-01-DD | FC4-10-EMS05-372-01-DD | FC4-10-EMS05-373-01-DD |
| **25-pack (renew)** | FC1-10-EMS05-428-02-DD | FC1-10-EMS05-429-02-DD | FC1-10-EMS05-434-02-DD | FC1-10-EMS05-403-02-DD |
| **500-pack (renew)** | FC2-10-EMS05-428-02-DD | FC2-10-EMS05-429-02-DD | FC2-10-EMS05-434-02-DD | FC2-10-EMS05-403-02-DD |
| **2000-pack (renew)** | FC3-10-EMS05-428-02-DD | FC3-10-EMS05-429-02-DD | FC3-10-EMS05-434-02-DD | FC3-10-EMS05-403-02-DD |
| **10,000-pack (renew)** | FC4-10-EMS05-428-02-DD | FC4-10-EMS05-429-02-DD | FC4-10-EMS05-434-02-DD | FC4-10-EMS05-403-02-DD |
| **On Premise** | | | | |
| **25-pack (add)** | FC1-10-EMS04-370-01-DD | FC1-10-EMS04-371-01-DD | Not Applicable | FC1-10-EMS04-373-01-DD |
| **500-pack (add)** | FC2-10-EMS04-370-01-DD | FC2-10-EMS04-371-01-DD | Not Applicable | FC2-10-EMS04-373-01-DD |
| **2000-pack (add)** | FC3-10-EMS04-370-01-DD | FC3-10-EMS04-371-01-DD | Not Applicable | FC3-10-EMS04-373-01-DD |
| **10,000 pack (add)** | FC4-10-EMS04-370-01-DD | FC4-10-EMS04-371-01-DD | Not Applicable | FC4-10-EMS04-373-01-DD |
| **25-pack (renew)** | FC1-10-EMS04-428-02-DD | FC1-10-EMS04-429-02-DD | Not Applicable | FC1-10-EMS04-403-02-DD |
| **500-pack (renew)** | FC2-10-EMS04-428-02-DD | FC2-10-EMS04-429-02-DD | Not Applicable | FC2-10-EMS04-403-02-DD |
| **2000-pack (renew)** | FC3-10-EMS04-428-02-DD | FC3-10-EMS04-429-02-DD | Not Applicable | FC3-10-EMS04-403-02-DD |
| **10,000-pack (renew)** | FC4-10-EMS04-428-02-DD | FC4-10-EMS04-429-02-DD | Not Applicable | FC4-10-EMS04-403-02-DD |
| **Professional Services** | | | | |
| **Professional Services (4hr)** | | FP-10-FTEMS-000-00-00 | | |

FORTINET®

www.fortinet.com



FST-PROD-DS-XXX
FCT-DAT-R25-202103