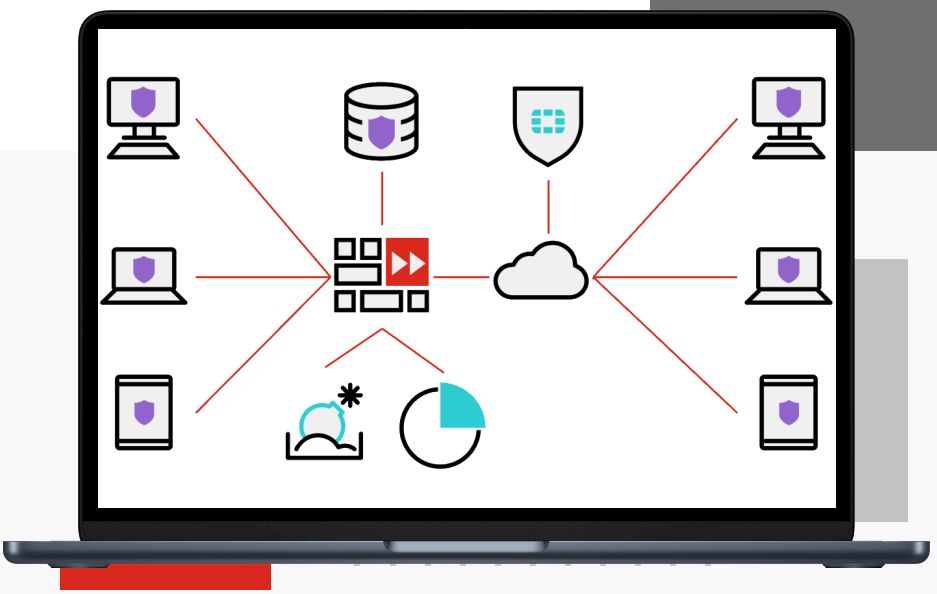
FortiClient



Highlights

- Security Fabric Agent
- VPN Agent
- ZTNA Agent
- Endpoint Protection (EPP)
- Sandboxing
- Vulnerability Assessment
- Centralized Management, Logging, Reporting
- FortiGate integrations
- Managed Services available
- On-premise and Cloud Management options

Endpoint Agent for Visibility and Control, Endpoint Protection, and Secure Remote Access using VPN and Zero Trust Technologies

FortiClient's Fortinet Security Fabric integration provides endpoint visibility through telemetry and ensures that all Security Fabric components – FortiGate, FortiAnalyzer, EMS, managed APs, managed Switches, and FortiSandbox – have a unified view of endpoints in order to provide tracking and awareness, compliance enforcement, and reporting. Traditional virtual private network (VPN) tunnels or new, automatic ZTNA tunnels provide secure remote connectivity. Provide security and protection for endpoints when local or remote.

Available in

Virtual

Hosted

Features

Unified Endpoint features including compliance, protection, and secure access into a single modular lightweight client. FortiClient is the agent for VPN, ZTNA, and Security Fabric telemetry and is incorporated into FortiSASE, FortiNAC, and FortiPAM.

Universal ZTNA, 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.

Simplified Management and Policy Enforcement with FortiClient EMS, FortiClient Cloud, and FortiGate.

Central Management Tools
Endpoint Management System- EMS

- Simple and user-friendly UI
- Remote FortiClient deployment
- ZTNA orchestration
- Real-time dashboard
- Software inventory management
- Active Directory (AD) integration
- Central quarantine management
- Automatic group assignment
- Dynamic access control
- Automatic email alerts
- Supports custom groups
- Remote triggers
- On-premise and cloud-based options

FortiGuard Security Services
www.fortiguard.com

FortiCare Worldwide 24/7 Support
support.fortinet.com

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. FortiOS and FortiAnalyzer leverage FortiClient endpoint telemetry intelligence to identify indicators of compromise. With the automation capability, administrators can investigate in 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 simplify the enforcement of enterprise security policies preventing endpoints from becoming easy attack targets.

Universal ZTNA

FortiClient Universal ZTNA works with FortiOS to enable secure granular access to applications no matter if the user is local or remote. Each session is initiated with an automatic, encrypted tunnel from FortiClient to the FortiOS ZTNA Application Gateway for user and device verification. If verified, access is granted for that session. You can also use multifactor authentication to provide an additional layer of security. With Universal ZTNA, organizations benefit from both a better remote access solution and a consistent policy for controlled access to applications irrespective of endpoint location.

Web Filtering and SaaS Control

FortiClient provides remote 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).

Vulnerability Assessment

FortiClient can reduce the attack surface by scanning endpoints for vulnerabilities and sharing that information for appropriate action. Any vulnerabilities can be leveraged by firewall policies, by ZTNA policies, or could result in quarantining of the endpoint.

Patch Policy Enforcement

Keeping endpoints up to date with the latest firmware can be difficult. FortiClient simplifies this by managing endpoint patching, even when the endpoints are not on the network.

Benefits continued

Malware and Exploit Prevention

By integrating with FortiClient Cloud Sandbox and leveraging FortiGuard global threat intelligence, FortiClient prevents advanced malware and vulnerabilities from being exploited. FortiClient integrates with FortiClient Cloud Sandbox to analyze all files downloaded to FortiClient endpoints in real time. Millions of FortiClient and FortiSandbox users worldwide share information about known and unknown malware with the cloud-based FortiGuard threat intelligence platform. FortiGuard automatically shares the intelligence with FortiClient endpoints to protect against emerging threats.

VPN

FortiClient provides flexible options for VPN connectivity. The split tunneling feature enables remote users on VPNs to access the Internet without their traffic having to pass through the corporate VPN headend, as in a typical VPN 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 the remote user experience with features such as autoconnect and always-on VPN, as well as dynamic VPN gate selection. You can also use multifactor authentication to provide an additional layer of security.

Ransomware Protection

Ransomware attacks have increased recently. In response, FortiClient has introduced new ransomware protection, with the ability to roll back changes made by malicious programs, putting the endpoint back to a preinfection state.

Flexible Licensing

The benefits of FortiClient are available through either the traditional device-based licensing or the new user-based FortiTrust licensing. Both options offer the same functionality and allow customers to decide how they want to subscribe to the benefits of FortiClient.

FortiClient Services

FortiClient Managed Services

FortiClient Managed Services include: cloud provisioning, onboarding, vulnerability monitoring, setup and integration.

To assist and offload busy IT teams, Fortinet is offering FortiClient Managed services to streamline the configuration, deployment, and monitoring of FortiClient agents. Services included with this offering include the following activities.

Initial FortiClient Cloud Provisioning

The managed services team works with customers to set up and configure their FortiClient Cloud environment for the following capabilities:

- Endpoint groups setup
- ZTNA
- VPN
- Endpoint security
- Vulnerability management
- Security profiles and policies configuration
- Endpoint posture check rules
- Custom FortiClient installer creation and ongoing installer updates

Endpoint Onboarding

The managed services team creates customer FortiClient installers for customer-specific use cases, sends invitation emails to users, and onboards them for FortiClient Cloud management and provisioning.

Security Fabric Setup and Integration

The managed services team integrates FortiClient Cloud with the Fortinet Security Fabric to support uses cases such as ZTNA, incidence response, and automation.

Endpoint Vulnerability Monitoring

The managed services team monitors customer endpoints to identify high risk endpoints and alert them of endpoints with critical and high vulnerabilities that would be easy targets for cyber attacks. The managed services team detects, reports, and guides customers to remediate those vulnerable endpoints.

Additional Services

Best Practice Service (BPS)

Access global knowledge of Fortinet customer best practices.

FortiClient Best Practices Service is an account-based annual subscription providing access to a specialized team that delivers remote guidance on deployment, upgrades, and operations. The service allows customers to share information about their deployment, user requirements, resources, and other related items. Based on the information provided, the BPS experts can provide recommended best practices, sample code, links to tools, and other materials or assistance to speed adoption and guide the customer towards best practice deployments. The team does not log into customer devices to make changes for them. This is a consulting and guidance service which may include sample configurations or playbooks. This is not an on-site professional services offer.

FortiClient Forensics Analysis Service

Extend your IT team with skilled FortiClient specialists.

FortiClient Forensic Service provides analysis to help endpoint customers respond to and recover from cyber incidents. For each engagement, forensic analysts from Fortinet's FortiGuard Labs will assist in the collection, examination, and presentation of digital evidence, including a final, detailed report. FortiClient subscriptions that include Forensic Services entitle the customer to call on these endpoint forensic experts whenever an event happens, offloading internal teams and accelerating investigations by analysts deeply familiar with the tools of endpoint security. Forensics Analysis Service is only available for cloud-hosted EMS deployments and is an annual subscription, not a per-incident license.

Fortinet CASB Service

Provide visibility, compliance, data security and threat protection.

To safely embrace the cloud, a Cloud Access Security Broker (CASB) can act as a gatekeeper by providing visibility, control, and protection to allow organizations to extend their security policies beyond their own infrastructure. CASB sits between cloud service users and secures SaaS cloud applications, monitors all activity, and enforces security policies. Fortinet's dual mode solution provides security, scalability, and performance using both Inline and API-based CASB protections to address all cloud security needs. A FortiClient license enables Inline CASB services on a FortiGate and provides a license for FortiCASB, Fortinet's API-based CASB service.

Feature Highlights

Central management tools provide the ability to centrally manage Windows, macOS, Linux, Chrome, iOS, and Android endpoints. FortiClient EMS provides on-premise management and FortiClient Cloud provides cloud-based management.

Central Management Tools

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 the central management tools so that you use the same organizational units from your AD server for simplified 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.

FortiSandbox integrations assist with configuration and suspicious file analysis. Sandbox settings are synchronized across managed endpoints, simplifying setup. A detailed analysis of FortiClient submitted files is available in the central management tools. Administrators can see all the behavior activity of a file, including graphic visualization of the full process tree.

FortiGate provides awareness and control over all your endpoints.

FortiGate Integrations

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	VPN / ZTNA	EPP / APT	Managed Services	Chromebook
Zero Trust Security	Windows, macOS, Linux	Windows, macOS, Linux	Windows, macOS, Linux	Chromebook
Zero Trust Agent with MFA	✓	✓	✓	
Security Posture Tagging Rules	✓	✓	✓	
Central Management via EMS or FortiClient Cloud	✓	✓	✓	✓
Dynamic Security Fabric Connector	✓	✓	✓	
Vulnerability Agent and Remediation	✓	✓	✓	
SSL VPN with MFA	✓	✓	✓	
IPSEC VPN with MFA	✓	✓	✓	
FortiGuard Web and Video Filtering	✓	✓	✓	✓
Cloud Access Security Broker (CASB)[1]	✓	✓	✓	
FortiPAM Support	✓	✓	✓	
Central Logging and Reporting[2]	✓	✓	✓	✓
Next Generation Endpoint Security				
Potentially Unwanted Applications		✓	✓	
AI powered NGAV		✓	✓	
Removable Media Control		✓	✓	
Automated Endpoint Quarantine		✓	✓	
Application Firewall[3]		✓	✓	
Software Inventory		✓	✓	
Ransomware Protection[4]		✓	✓	
FortiClient Cloud Sandbox (SaaS)[3]		✓	✓	
FortiSandbox Integration (PaaS/Public Cloud/On-premises)[3]	✓	✓	✓	
Managed FortiClient Service				
Endpoint Onboarding			✓	
Initial Provisioning			✓	
Security Fabric Setup/Integration			✓	
Vulnerability Monitoring			✓	
Endpoint Security Monitoring			✓	
Additional Services				
Best Practice Service (BPS) Consultation	Account add-on	Account add-on	N/A	Account add-on
24×7 Support	✓	✓	✓	✓
On-Premise/Air Gap Option	✓	✓		✓
FortiGuard Forensics Analysis Service Option	Account add-on	Account add-on	Account add-on	Account add-on

1. A license for Inline CASB and FortiCASB (API based) is included.
2. Requires FortiAnalyzer.
3. FortiClient (Linux) does not support Sandbox integration.
4. Only FortiClient (Windows) supports this feature.

CERTIFIED

Features Per Platform and Requirements

	WINDOWS	MACOS	ANDROID	IOS	CHROMEBOOK	LINUX
Zero Trust Security						
ZTNA Remote Access	✓	✓	✓	✓		✓
Endpoint Telemetry[1]	✓	✓	✓	✓	✓	✓
Web Filter[2]	✓	✓	✓	✓	✓	
Security Posture Tags for Compliance[1]	✓	✓	✓	✓		✓
Endpoint Audit and Remediation with Vulnerability Scanning	✓	✓				✓
IPSec VPN	✓	✓	✓			
SSL VPN[4]	✓	✓	✓	✓	✓	✓
Security Posture Tag Check before VPN	✓					
Windows AD SSO Agent	✓	✓				
FortiPAM Agent	✓					
Remote Logging and Reporting[3]	✓	✓		✓	✓	✓
Endpoint Security						
Antivirus	✓	✓				✓
Cloud-based Threat Detection	✓	✓				
Sandbox integration (on-premise)	✓	✓				
Sandbox integration (Saas/Paas)	✓	✓				
Automated Endpoint Quarantine	✓	✓				
AntiExploit	✓					
Application Firewall	✓	✓				
Potentially Unwanted Applications	✓	✓				
FortiClient Forensic Analysis	✓	✓				✓
Removable Media Control	✓	✓				✓

1. Requires EMS or FortiClient Cloud to centrally manage FortiClient.
2. Also compatible with Chrome OS.
3. Requires FortiAnalyzer.
4. Also compatible with Windows mobile.

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 11 (64-bit)
Microsoft Windows Server 2012 or later
macOS 10.14 or later
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 EMS
Supported Operating Systems
Microsoft Windows Server 2012 or later
Endpoint Requirement
FortiClient 6.4 or later, FortiClient for Windows and macOS X, 6.4 for iOS and Android
System Requirements
2.0 GHz 64-bit processor, six virtual CPUs, 8 GB RAM, 40 GB free hard disk, Gigabit (10/100/1000BaseT)
Ethernet adapter, Internet access

Order Information

You can order FortiClient based on the number of devices. The following table reflects the latest FortiClient device-based license packs.

EDITION	ZTNA	EPP/APT	MANAGED	CHROMEBOOK
SaaS (Cloud Hosted EMS)				
25-pack	FC1-10-EMS05-428-01-DD	FC1-10-EMS05-429-01-DD	FC1-10-EMS05-485-01-DD	FC1-10-EMS05-403-01-DD
500-pack	FC2-10-EMS05-428-01-DD	FC2-10-EMS05-429-01-DD	FC2-10-EMS05-485-01-DD	FC2-10-EMS05-403-01-DD
2000-pack	FC3-10-EMS05-428-01-DD	FC3-10-EMS05-429-01-DD	FC3-10-EMS05-485-01-DD	FC3-10-EMS05-403-01-DD
10 000 pack	FC4-10-EMS05-428-01-DD	FC4-10-EMS05-429-01-DD	FC4-10-EMS05-485-01-DD	FC4-10-EMS05-403-01-DD
On Premise				
25-pack	FC1-10-EMS04-428-01-DD	FC1-10-EMS04-429-01-DD		FC1-10-EMS04-403-01-DD
500-pack	FC2-10-EMS04-428-01-DD	FC2-10-EMS04-429-01-DD		FC2-10-EMS04-403-01-DD
2000-pack	FC3-10-EMS04-428-01-DD	FC3-10-EMS04-429-01-DD		FC3-10-EMS04-403-01-DD
10 000 pack	FC4-10-EMS04-428-01-DD	FC4-10-EMS04-429-01-DD		FC4-10-EMS04-403-01-DD
FortiCare Best Practices Consultation Service				
25-999 endpoints	FC1-10-FCBPS-310-02-DD			
1000-9999 endpoints	FC2-10-FCBPS-310-02-DD			
10 000+ endpoints	FC5-10-FCBPS-310-02-DD			
Training Services				
Classroom - virtual ILT	FT-FCT			
Lab access - standard NSE training lab environment	FT-FCT-LAB			
NSE5 exam voucher	NSE-EX-SPL5			

You can order FortiClient based on the number of users. The following table reflects the latest FortiTrust user-based license ranges.

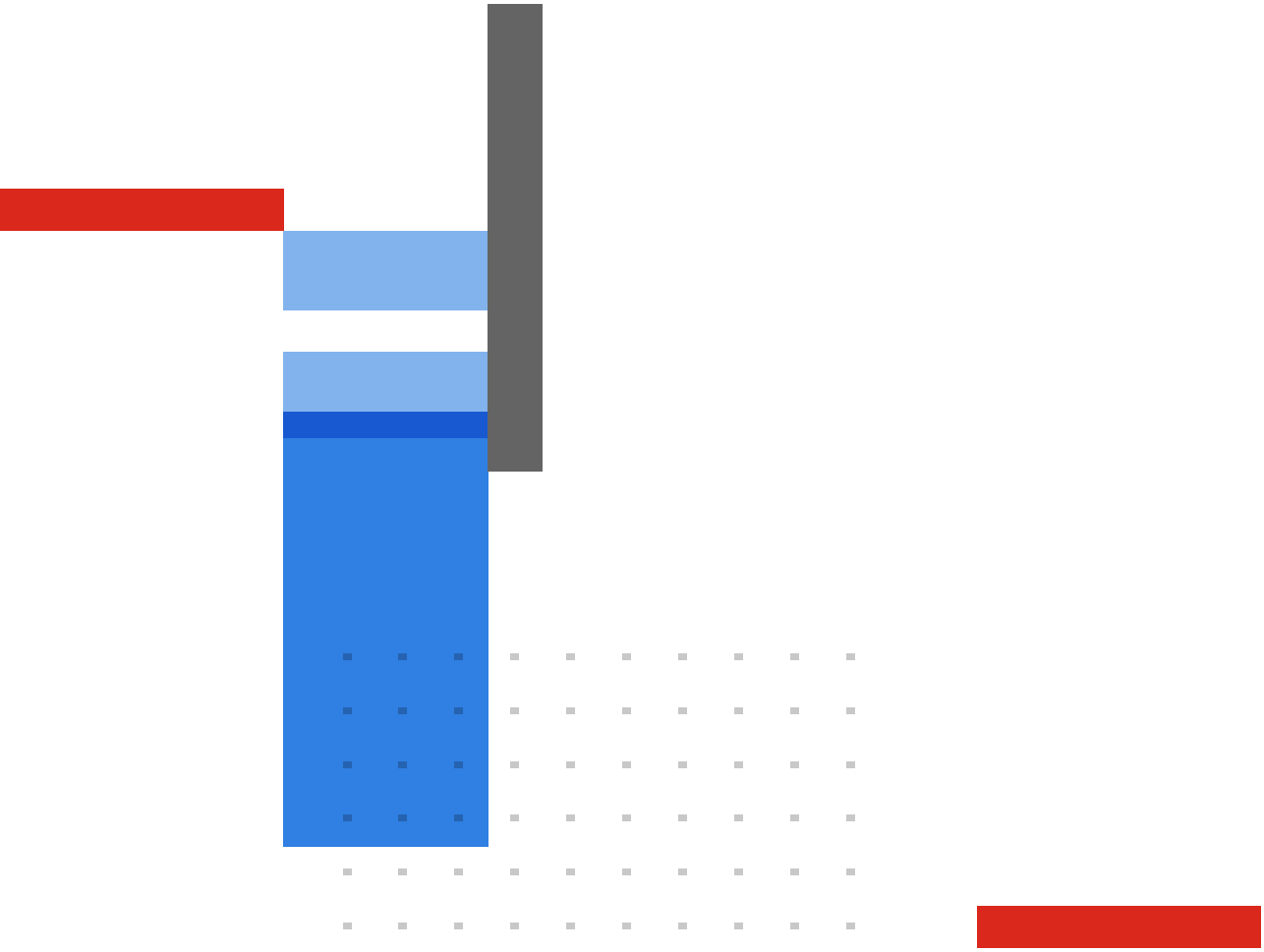
FORTITRUST USER-BASED LICENSE RANGES				
SOLUTION	**SKU LICENSE**	**VPN/ ZTNA**	**EPP/ APT**	**MANAGED**
Cloud-hosted EMS	100-499 users	FC2-10-EMS05-509-02-DD	FC2-10-EMS05-546-02-DD	FC2-10-EMS05-556-02-DD
	500-1999 users	FC3-10-EMS05-509-02-DD	FC3-10-EMS05-546-02-DD	FC3-10-EMS05-556-02-DD
	2000-9999 users	FC4-10-EMS05-509-02-DD	FC4-10-EMS05-546-02-DD	FC4-10-EMS05-556-02-DD
	10 000+ users	FC5-10-EMS05-509-02-DD	FC5-10-EMS05-546-02-DD	FC5-10-EMS05-556-02-DD

The following table reflects the latest licenses for the Forensic Analysis Service.

FORENSIC ANALYSIS SERVICE				
SOLUTION	**SKU LICENSE**	**VPN/ ZTNA**	**VPN/ ZTNA + EPP/ APT**	**MANAGED**
Device-based Licenses	25-pack	FC1-10-EMS05-537-01-DD	FC1-10-EMS05-538-01-DD	FC1-10-EMS05-539-01-DD
	500-pack	FC2-10-EMS05-537-01-DD	FC2-10-EMS05-538-01-DD	FC2-10-EMS05-539-01-DD
	2000-pack	FC3-10-EMS05-537-01-DD	FC3-10-EMS05-538-01-DD	FC3-10-EMS05-539-01-DD
	10 000-pack	FC4-10-EMS05-537-01-DD	FC4-10-EMS05-538-01-DD	FC4-10-EMS05-539-01-DD
FortiTrust (User-based Licenses)	100-499 users	FC2-10-EMS05-557-02-DD	FC2-10-EMS05-558-02-DD	FC2-10-EMS05-559-02-DD
	500-1999 users	FC3-10-EMS05-557-02-DD	FC3-10-EMS05-558-02-DD	FC3-10-EMS05-559-02-DD
	2000-9999 users	FC4-10-EMS05-557-02-DD	FC4-10-EMS05-558-02-DD	FC4-10-EMS05-559-02-DD
	10 000+ users	FC5-10-EMS05-557-02-DD	FC5-10-EMS05-558-02-DD	FC5-10-EMS05-559-02-DD

Fortinet Corporate Social Responsibility Policy

Fortinet is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet's products and services to engage in, or support in any way, violations or abuses of human rights, including those involving illegal censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the Fortinet EULA and report any suspected violations of the EULA via the procedures outlined in the Fortinet Whistleblower Policy.



www.fortinet.com

November 14, 2023

FCT-DAT-R38-20231114