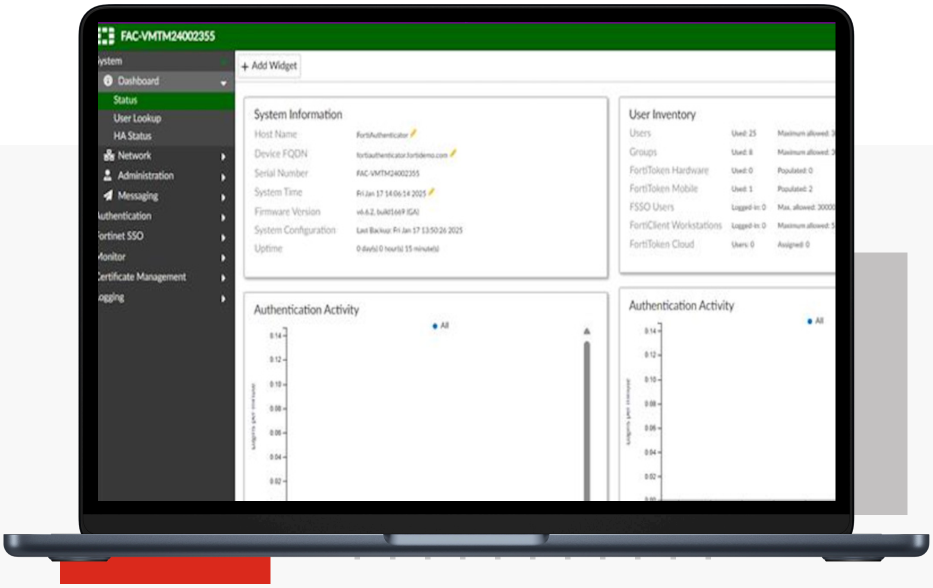
Britannic

FORTINET

Data Sheet

FortiAuthenticator™

Identity and Access Management



System Information

Host Name	FortiAuthenticator
Device FQDN	fortiauthenticator.fortidemo.com
Serial Number	FAC-VMTM24002355
System Time	Fri Jan 17 14:06:14 2025
Firmware Version	v6.6.2, build1669 (GA)
System Configuration	Last Backup: Fri Jan 17 13:50:26 2025
Uptime	0 day(s) 0 hour(s) 15 minute(s)

User Inventory

Users	Used: 25	Maximum allowed: 3
Groups	Used: 8	Maximum allowed: 3
FortiToken Hardware	Used: 0	Populated: 0
FortiToken Mobile	Used: 1	Populated: 2
FSSO Users	Logged in: 0	Max. allowed: 30000
FortiClient Workstations	Logged in: 0	Maximum allowed: 5
FortiToken Cloud	Users: 0	Assigned: 0

Highlights

- Centralized user authentication and authorization
- Multi-factor authentication (MFA)
- Single Sign-On (SSO)
- FIDO passwordless registration and authentication
- Certificate management
- RADIUS, TACACS+, LDAP, SAML IdP and SP support
- Fortinet Single Sign-On (FSSO)
- Trusted Endpoint SSO

Centralized Identity and Access Management Solution

Network and Internet access is key for almost every role within the enterprise; however, this requirement must be balanced with the risk that it brings. The key objective of every enterprise is to provide secure but controlled network access enabling the right person the right access at the right time, without compromising on security.

FortiAuthenticator is a scalable Identity and Access Management (IAM) solution that enhances security and simplifies authentication for enterprises. Available as a physical or virtual appliance for private and public cloud deployments, it provides robust services such as RADIUSTACACS+ service, Multi-Factor Authentication (MFA), Passwordless Authentication, Adaptive Authentication (AA), Single Sign-On (SSO), Identity Provider (IdP), and IdP Proxy, System for Cross Identity Management (SCIM), Fortinet Single Sign-On (FSSO), and Certificate Authority.

FortiAuthenticator integrates seamlessly with remote on-prem and cloud directories, applications, and Fortinet's Security Fabric. This entegration ensures secure and streamlined access to business resources and internal and external SaaS applications (e.g., Microsoft 365). Supporting legacy and modern authentication protocols, including FIDO passkeys, FortiAuthenticator employs context-aware, adaptive authentication to grant, challenge, or deny access based on login criteria. Acting as a gatekeeper, it identifies users, queries third-party access permissions, and communicates identity-based policies to FortiGate devices, securing enterprise networks with precision and ease.

Available in:

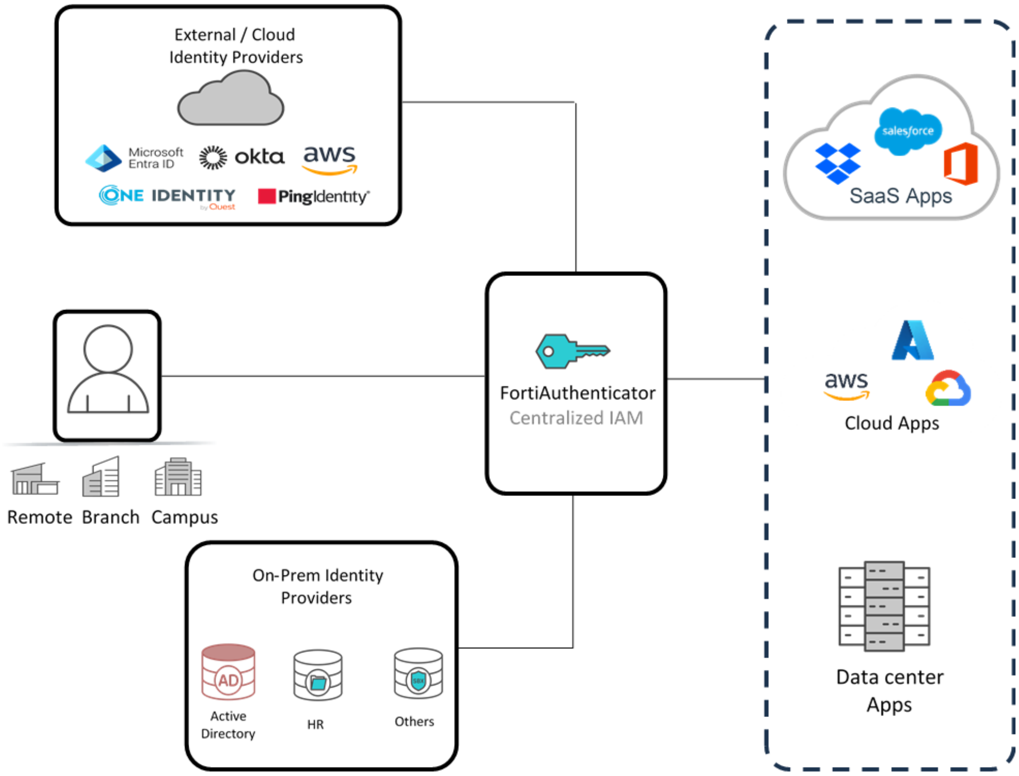
Appliance

Virtual Machine

Hosted

Cloud

Solution Deployment



Features

Centralized Authentication

FortiAuthenticator streamlines and secures user authentication by acting as a standalone IdP or integrating with both on-premises and cloud identity providers, offering seamless access to systems and applications for users, regardless of location. It supports a wide range of multi-factor authentication (MFA) methods, including FortiToken, SMS and email OTP, and FIDO2 for passwordless authentication, delivering a consistent, secure, and unified authentication experience. By centralizing authentication, FortiAuthenticator enhances security across the organization, improves operational efficiency, and reduces the complexity associated with managing multiple disparate authentication systems.

FortiAuthenticator integrates seamlessly with multiple Fortinet products and services, providing identity management and strong authentication across Fortinet's Security Fabric. Additionally, it functions as a fully standalone authentication solution for third-party environments, supporting RADIUS and LDAP authentication and SAML and OAuth/OIDC SSO. This flexibility allows organizations to implement FortiAuthenticator in both Fortinet-centric and heterogeneous IT infrastructures with ease.

Strong User Identity with Multi-Factor Authentication (MFA)

FortiAuthenticator enhances user security by enforcing robust multi-factor authentication (MFA) to secure access to critical resources. It supports a diverse range of MFA methods, including FortiToken Mobile and hardware tokens, SMS and email OTP, client certificate-based authentication, and FIDO2 for passwordless authentication, ensuring flexible and secure user verification across all scenarios.

By combining user identity information with authentication data from FortiToken or FIDO2 services, FortiAuthenticator ensures only authorized individuals gain access, reducing the risk of unauthorized access and data breaches. This added layer of security also helps organizations comply with government and business privacy regulations.

With the industry's widest range of MFA options, FortiAuthenticator accommodates diverse user needs, offering time-based physical tokens, mobile apps (iOS, Android, Windows), and modern passwordless methods like FIDO2. Its capabilities extend to controlling access for FortiGate management, SSL/IPsec VPNs, wireless captive portals, third-party RADIUS-compliant networking equipment, and SAML service providers.

FortiAuthenticator also features a REST API for adding MFA to custom web-based applications, enabling seamless integration into existing workflows. To simplify local user management, it includes self-registration and password recovery capabilities, ensuring a streamlined and user-friendly experience.

Features

Certificate Management

FortiAuthenticator serves as a robust Certificate Authority (CA), enabling administrators to create, import, and manage X.509 certificates, including server certificates for HTTPS and SSH, and client certificates for HTTPS, SSL, and IPsec VPNs. It supports the full certificate lifecycle, including generation, signing, and revocation, and offers streamlined management of Certificate Revocation Lists (CRLs).

To ensure secure and automated certificate operations, FortiAuthenticator supports SCEP and CMP protocols, simplifying certificate deployment and renewal processes. It integrates seamlessly with remote LDAP servers, verifying identities using trusted CA certificates, and supports EAP authentication by validating client certificates against authorized CA certificates and user records.

In environments with site-to-site VPNs, where pre-shared keys can pose a security risk, FortiAuthenticator enhances security by enabling certificate-based VPNs. Its integration with FortiManager automates bulk certificate deployment and simplifies certificate management, removing the complexity traditionally associated with these solutions. Certificates are securely delivered via the SCEP protocol, making it easier to implement and manage certificate-secured VPNs within FortiGate environments.

For client-based VPNs, FortiAuthenticator supports the FortiToken 300 USB Certificate Store, a secure, PIN-protected hardware solution that enhances client VPN security. This USB-based certificate store is fully compatible with FortiClient, ensuring an additional layer of protection for client VPN connections.

Adaptive Authentication

FortiAuthenticator provides advanced adaptive authentication capabilities by analyzing contextual factors during login, such as user location, device type, time of day, behavior patterns, and IP address. Based on this context and predefined policies, it dynamically adjusts authentication requirements, such as enforcing MFA, bypassing MFA, or blocking access entirely. This approach ensures secure, context-aware access control, allowing organizations to apply stricter security measures or deny access based on risk. These adaptive features enable organizations to strengthen security while maintaining a seamless user experience.

Protocol Support for Flexible Integration

FortiAuthenticator is designed for interoperability, supporting a wide range of protocols including RADIUS, SAML, OIDC, LDAP, and TACACS+. This extensive protocol compatibility ensures seamless integration with diverse systems, allowing organizations to leverage existing infrastructure while enhancing security and scalability.

Features

802.1X Authentication

FortiAuthenticator supports 802.1X authentication, a foundational protocol for enterprise network access control. Acting as a RADIUS server, it provides authentication, authorization, and accounting (AAA) services for devices connecting to wired, wireless, or VPN networks. By validating user credentials, device certificates, or both, FortiAuthenticator ensures that only authorized users and devices gain access, effectively preventing unauthorized network access.

FortiAuthenticator integrates seamlessly with existing identity stores such as Active Directory, LDAP, and PKI systems, and supports advanced protocols like EAP-TLS for certificate-based authentication. These capabilities enable enterprises to enforce Zero Trust principles, ensure compliance with security policies, and safeguard sensitive resources against unauthorized access.

With FortiAuthenticator, organizations can achieve secure port-level access control for LAN and WLAN environments, offering robust protection for enterprise networks while supporting scalable and flexible deployment options.

TACACS+ and RADIUS Authentication

Serving as a centralized Authentication, Authorization, and Accounting (AAA) server, FortiAuthenticator supports both TACACS+ and RADIUS protocols. This approach enables secure network access control by authenticating users and devices, enforcing access policies, and providing granular control over network commands and configurations.

Single Sign-On (SSO)

FortiAuthenticator can function as a SAML Identity Provider (IdP) or as an IdP proxy, allowing it to federate user and group information from remote IdPs to service providers (SPs) (including FortiGate). It supports both SP-initiated and IdP-initiated login flows, ensuring compatibility with a wide range of systems. Additionally, FortiAuthenticator can serve as an OIDC Provider, making it ideal for scenarios involving mobile and native applications.

Trusted Endpoint SSO

FortiAuthenticator's Trusted Endpoint SSO feature enhances seamless and secure user authentication by leveraging FortiClient EMS and ZTNA. Once users log in to their endpoint devices, their credentials are securely cached by FortiAuthenticator, allowing for transparent authentication to service providers without requiring repeated logins.

This feature integrates device security posture checks from FortiClient EMS, ensuring only trusted and compliant endpoints are granted access. It enhances user experience, reduces friction during authentication, and enforces Zero Trust principles by validating both user identity and device trustworthiness. This feature makes Trusted Endpoint SSO a valuable differentiator for organizations prioritizing secure, user-friendly access.

Features

Fortinet Single Sign-On (FSSO)

Fortinet Single Sign-On (FSSO) is a proprietary feature that enables seamless and transparent user authentication for FortiGate firewalls. By collecting user, IP, and group information from external identity sources such as Active Directory or LDAP, FSSO allows FortiGate devices to enforce identity-based policies for network access control. FortiAuthenticator serves as a central collector for user authentication events, channeling login and logout status from various sources and ensuring accurate identity tracking across Fortinet deployments.

FortiAuthenticator's FSSO capability ensures consistent and centralized user identity management for FortiGate deployments. By supporting multiple authentication methods and integrating with diverse directory systems, it provides flexibility for complex network environments. This approach not only enhances security by enabling identity-based policies but also improves the user experience with transparent authentication processes.

Key Features of FortiAuthenticator FSSO Integration:

1. **Active Directory Polling:** FortiAuthenticator detects user logins by regularly polling Active Directory domain controllers. Once a login is identified, it collects the username, IP address, and group details, storing them in the FortiAuthenticator User Identity Management Database. These details can then be shared with multiple FortiGate devices to enforce identity-based policies.
2. **FortiAuthenticator SSO Mobility Agent**: For distributed or complex domain environments where polling domain controllers is impractical, the FortiAuthenticator SSO Mobility Agent provides an alternative. Distributed via FortiClient or as a standalone application, it communicates login events, IP changes (e.g., between wired and wireless networks), and logout events to FortiAuthenticator, ensuring real-time user tracking without relying on polling.
3. **Explicit Authentication Portal and Widgets**: For systems that do not support AD polling or where an SSO client is not feasible, FortiAuthenticator offers a user authentication portal. Users can manually log in to gain network access, and to streamline repeated logins, organizations can deploy widgets on their intranet. These widgets leverage browser cookies to automatically log in users when they access the intranet homepage.
4. **RADIUS Accounting Integration**: In networks utilizing RADIUS authentication (e.g., for wireless or VPN access), RADIUS Accounting can serve as a user identification method. FortiAuthenticator uses this information to detect logins, associate IP and group details with users, and eliminate the need for redundant authentication tiers.

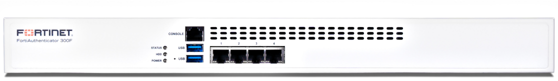
Features

System for Cross-domain Identity Management (SCIM)

FortiAuthenticator supports SCIM, an open standard for automating the exchange of user identity information between identity providers and service providers. This method facilitates seamless synchronization of user data, streamlining provisioning and deprovisioning processes, and reducing administrative overhead.

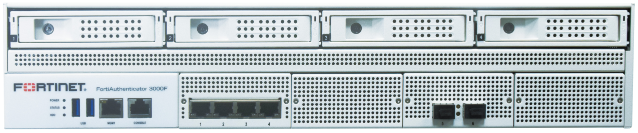
Offline Token Provisioning for Air-Gapped Environments

FortiAuthenticator ensures secure authentication even in air-gapped environments by supporting offline token provisioning. Administrators can activate FortiToken Mobile tokens without internet connectivity through QR codes or manual activation codes. This feature is particularly valuable for operational technology (OT) networks and other isolated environments where internet access is restricted, providing robust authentication while maintaining strict network isolation and security.



FortiAuthenticator 300F

FortiAuthenticator 800F



FortiAuthenticator 3000F

Specifications

FORTIAUTHENTICATOR MODEL NO.	FAC-300F	FAC-800F	FAC-3000F
Hardware			
10/100/1000 Interfaces (Copper, RJ-45)	4	4	4
SFP Interfaces	0	2	2
Local Storage	2× 1TB Hard Disk Drive - RAID 1	2× 2 TB Hard Disk Drive - RAID 1	2× 2 TB SAS Drive - RAID 1
Trusted Platform Module (TPM)	Yes	Yes	Yes
Power Supply	300W Redundant Auto Ranging (100V-240V), Optional Dual (1+1)	Dual (1+1) 300W Redundant Auto Ranging (100V–240V)	Dual (1+1) 1000W Auto Ranging (100V–240V)
System Capacity			
Local + Remote Users (Base / Upper Limit)	1500 / 3500	8000 / 18 000	40 000 / 240 000
FortiTokens	3000	16 000	480 000
RADIUS Clients (NAS Devices) (Base / Upper Limit)	500 / 1166	2666 / 6000	13 333 / 80 000
User Groups	150	800	24 000
CA Certificates	10	50	300
User Certificates	7500	40 000	1 200 000
Dimensions			
Height x Width x Length (inches)	1.75 × 17.0 × 15.04	1.75 × 17.0 × 27.61	3.46 × 17.24 × 23.66
Height x Width x Length (mm)	44 × 438 × 422	44 × 438 × 701.2	88 × 438 × 601
Weight	18.0 lbs (8.2 kg)	33.0 lbs (15.0 kg)	44 lbs (20 kg)
Environment			
Form Factor	Rack Mountable (1RU)	Rack Mountable (1RU)	Rack Mountable (2 RU)
Power Source	100-240 VAC, 50/60 Hz 300W Redundant (1+0)	100–240V AC, 50/60 Hz	100–240V AC, 50–60 Hz
Maximum Current	5A /100V, 2.5A /240V	5A /100V, 2.5A /240V	100-127/200-240VAC, 50/60Hz, 10/5A
Power Consumption (Average / Maximum)	82.35 W / 131.23 W	154 W / 196.04 W	193.30 W / 236.28 W
Heat Dissipation	482 BTU/h	703 BTU/h	1325 BTU/h
Forced Airflow	Front to back	Front to back	Front to back
Noise Level			49.8 db
Operating Temperature	32°–104°F (0°–40°C)	32°–104°F (0°–40°C)	32°–104°F (0°–40°C)
Storage Temperature	-4°–158°F (-20°–70°C)	-4°–158°F (-20°–70°C)	-40°–158°F (-40°–70°C)
Humidity	5%–90% non-condensing	5%–95% non-condensing	5%–90% non-condensing
System			
Standards Supported	10/100/1000 Base-TX (GE), IP, Telnet, HTTP 1.0/1.1, SSL, RS232, NTP Client (RFC1305), RADIUS (RFC2865), LDAP (RFC4510), x.509 (RFC5280), Certificate Revocation (RFC3280), PKCS#12 Certificate Import, PKCS#10 CSR Import (RFC2986), Online Certificate Status Protocol (RFC 2560), EAP-TLS (RFC2716), Simple Certificate Enrollment Protocol (SCEP), oAuth, OIDC, and SAML2.0		
Management	CLI, Direct Console DB9 CLI, HTTPS		
High Availability	Active-Passive HA and Config Sync HA		
Compliance			
Safety	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB	FCC Part 15 Class A, RCM, VCCI, CE, BSMI, KC, UL/cUL, CB, GOST	FCC Part 15 Class A, RCM, VCCI, CE, BSMI, KC, UL/cUL, CB, GOST

Specifications

VIRTUAL APPLIANCES	FAC-VM BASE	FAC-VM-100-UG	FAC-VM-1000-UG	FAC-VM-10000-UG
Capacity				
Users (Local and Remote)	100	+100	+1000	+10 000
FortiTokens	200	+200	+2000	+20 000
NAS Devices	33	+33	+333	+3333
User Groups	10	+10	+100	+1000
CA Certificates	5	+5	+50	+500
User Certificates	500	+500	+5000	+50 000
Virtual Machine				
Hypervisors Supported	VMware ESXi/ ESX 6/ 7/ 8, Microsoft Hyper-V Server 2010, 2012 R2, 2016, and 2019, KVM, Xen, Microsoft Azure, AWS, Nutanix AHV (Acropolis Hypervisor), Oracle OCI, Alibaba Cloud			
Maximum Virtual CPUs Supported	64			
Virtual NICs Required (Minimum / Maximum)	1 / 4			
Virtual Machine Storage (Minimum / Maximum)	60 GB / 16 TB			
Virtual Machine Memory Required (Minimum / Maximum)	2 GB / 1 TB			
High Availability Support	Active-Passive HA and Config Sync HA			

Order Information

Product	SKU	Description
FortiAuthenticator 300F	FAC-300F	4x GE RJ45 ports, 2× 1 TB HDD. Base License supports up to 1500 users. Expand user support to 3500 users by using FortiAuthenticator Hardware Upgrade License.
FortiAuthenticator 800F	FAC-800F	4x GE RJ45 ports, 2x GE SFP, 2× 2 TB HDD. Base License supports up to 8000 users. Expand user support to 18 000 users by using FortiAuthenticator Hardware Upgrade License.
FortiAuthenticator 3000F	FAC-3000F	4x GE RJ45 ports, 2× 10GE SPF, 2× 2TB SAS Drive. Base License supports up to 40 000 users. Expand user support to 240 000 users by using FortiAuthenticator Hardware Upgrade License
FortiAuthenticator-VM License	FAC-VM-Base	VM Base License supports 100 users. Expand user support to 1 million plus users by using FortiAuthenticator VM Upgrade License.
	FAC-VM-100-UG	FortiAuthenticator-VM 100 user license upgrade.
	FAC-VM-1000-UG	FortiAuthenticator-VM 1000 user license upgrade.
	FAC-VM-10000-UG	FortiAuthenticator-VM 10 000 user license upgrade.
	FC1-10-0ACVM-248-02-12	1 Year 24×7 FortiCare Contract (1–500 users).
	FC2-10-0ACVM-248-02-12	1 Year 24×7 FortiCare Contract (1–1100 users).
	FC3-10-0ACVM-248-02-12	1 Year 24×7 FortiCare Contract (1–5100 users).
	FC4-10-0ACVM-248-02-12	1 Year 24×7 FortiCare Contract (1–10 100 users).
	FC8-10-0ACVM-248-02-12	1 Year 24×7 FortiCare Contract (1–25 100 users).
	FC5-10-0ACVM-248-02-12	1 Year 24×7 FortiCare Contract (1–50 100 users).
	FC6-10-0ACVM-248-02-12	1 Year 24×7 FortiCare Contract (1–100 100 users).
	FC9-10-0ACVM-248-02-12	1 Year 24×7 FortiCare Contract (1–500 100 users).
	FC7-10-0ACVM-248-02-12	1 Year 24×7 FortiCare Contract (1–1M users).
FortiClient SSO License for FortiAuthenticator	FCC-FAC2K-LIC	FortiAuthenticator FortiClient SSO Mobility Agent License for 2000 FortiClient connections (does not include FortiClient Endpoint Control License for FortiGate).
	FCC-FAC10K-LIC	FortiAuthenticator FortiClient SSO Mobility Agent License for 10 000 FortiClient connections (does not include FortiClient Endpoint Control License for FortiGate).
	FCC-FACUNL-LIC	FortiAuthenticator FortiClient SSO Mobility Agent License for unlimited FortiClient connections(does not include FortiClient Endpoint Control License for FortiGate).
Hardware Upgrade Licenses for FAC-300F, FAC-800F, and FAC-3000F	FAC-HW-100UG	FortiAuthenticator 300F, 800F, 3000E, or 3000F, 100 user upgrade.
	FAC-HW-1000UG	FortiAuthenticator 300F, 800F, 3000E, or 3000F, 1000 user upgrade.
	FAC-HW-10KUG	FortiAuthenticator 800F, 3000E, or 3000F, 10 000 user upgrade.
	FAC-HW-100KUG	FortiAuthenticator 3000F, 100 000 user upgrade.
Optional Accessories		
Power Supplies	SP-FML900F-PS	AC power supply for FAC-300F.
	SP-FML900F-PS	AC power supply for FAC-800F.

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.

February 3, 2025