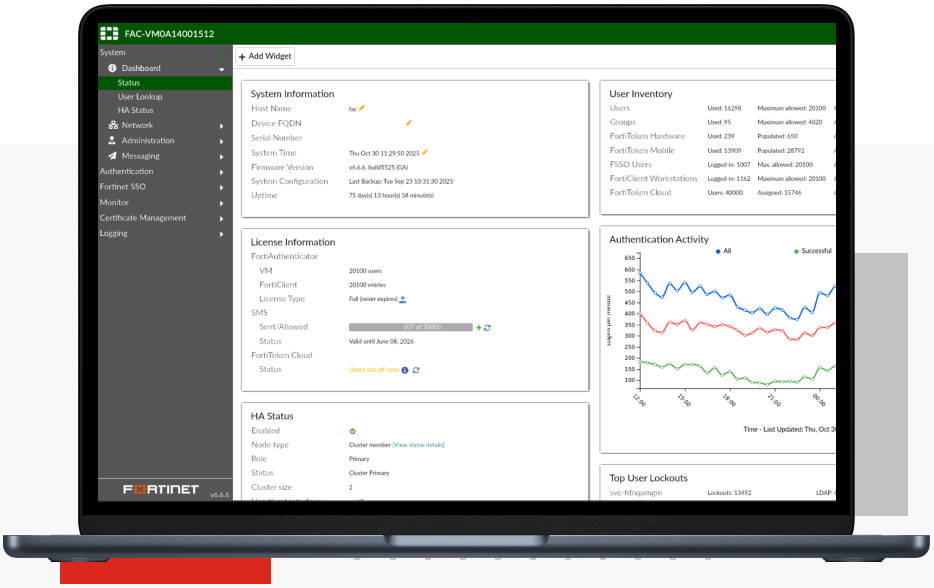
# FortiAuthenticator

## Identity and Access Management




### Highlights

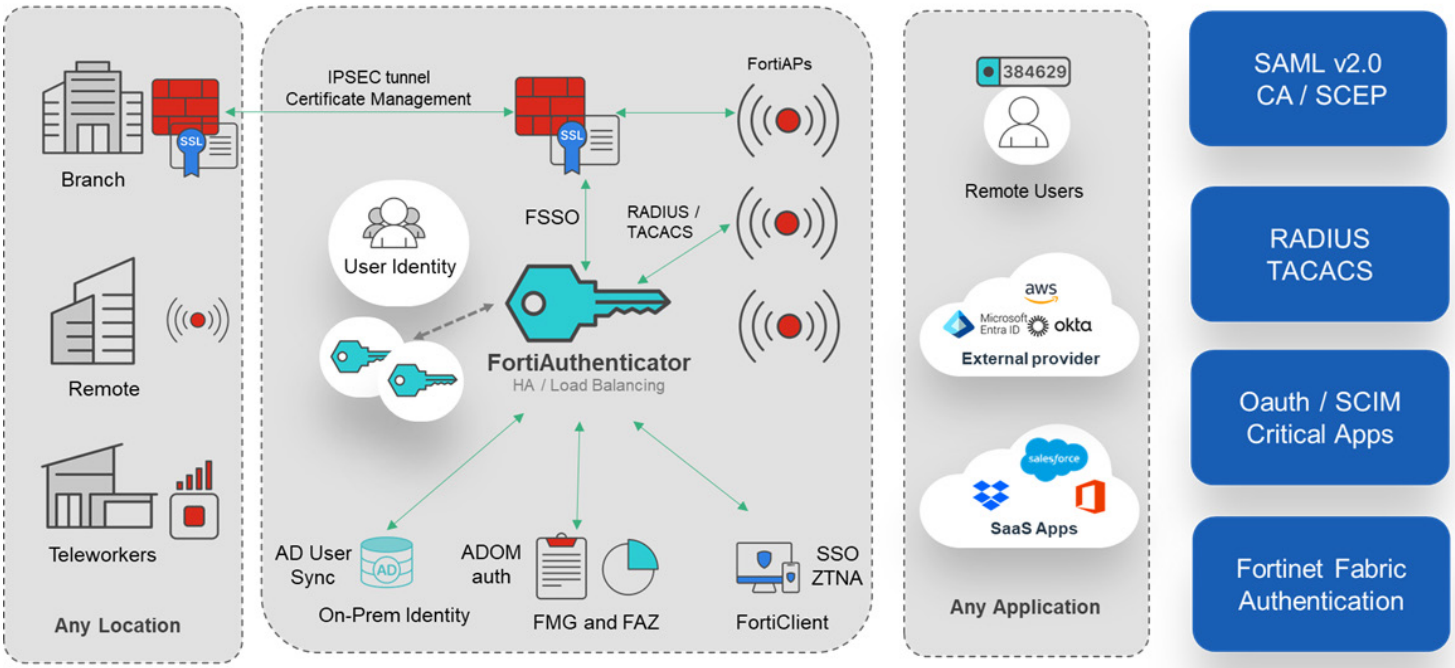
- Centralized user authentication and authorization
- Multi-factor authentication (MFA)
- Single Sign-On (SSO)
- FIDO passwordless registration and authentication
- Certificate management
- RADIUS, TACACS+, LDAP, SAML IdP and SP support
- Fortinet Single Sign-On (FSSO)
- Trusted Endpoint SSO

## 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.




## Features

**Strong User Identity with Multi-Factor Authentication (MFA)**

**Multi-Factor Authentication:** FortiToken Mobile, push authentication, hardware tokens, SMS/email OTP, client certificates, and FIDO2 password-less authentication.

**Adaptive Authentication:** Adjusts authentication requirements based on login context, including user, device, location, time, and source IP.

**Single Sign-On and Federation:** Supports SAML IdP, IdP proxy, SP- and IdP-initiated authentication, OIDC, and Fortinet Single Sign-On.

**Flexible Protocol Support:** Integrates through RADIUS, TACACS+, SAML, OIDC, LDAP, REST APIs, EAP, and 802.1X.

**Centralized AAA:** Provides authentication, authorization, accounting, policy enforcement, and granular administrative access control.

**Certificate Management:** Manages the X.509 certificate lifecycle, including issuance, import, renewal, revocation, SCEP, CMP, and certificate validation.

**Identity Synchronization:** Integrates with Active Directory, LDAP, cloud identity providers, and SCIM for automated provisioning and deprovisioning.

**User Self-Service:** Supports self-registration, guest onboarding, sponsor approval, password recovery, and token provisioning.

**Offline Authentication:** Enables FortiToken Mobile activation in air-gapped and isolated environments.

## Use-Case Examples

View all use-cases:

https://docs.fortinet.com/document/fortiauthenticator/8.0.0/examples/777493/fortiauthenticator-standalone-iam

**Standalone IAM Use Cases**

- Centralize identity and authentication services across on-premises, cloud, and hybrid environments.
- Protect VPNs, network devices, administrative portals, captive portals, SaaS applications, and custom web applications with MFA.
- Provide SAML and OIDC-based SSO for enterprise, cloud, mobile, and native applications.
- Deliver RADIUS and TACACS+ authentication for third-party firewalls, switches, wireless controllers, VPN appliances, and other infrastructure.
- Enforce 802.1X access control for wired, wireless, and VPN users using credentials, certificates, or both.
- Manage certificates for users, endpoints, VPNs, applications, and network devices.
- Automate user onboarding, provisioning, deprovisioning, password recovery, and guest access.
- Support certificate-based and offline authentication in regulated, operational technology, and air-gapped environments.

**Fortinet Security Fabric Use Cases**

- **FortiGate MFA:** Protect FortiGate administration, SSL VPN, IPsec VPN, captive portals, and ZTNA applications.
- **Identity-Aware Policies:** Share user, IP address, group, and login information with FortiGate for identity-based policy enforcement.
- **Fortinet Single Sign-On:** Collect identity through Active Directory polling, the SSO Mobility Agent, authentication portals, widgets, and RADIUS accounting.
- **FortiSwitch and FortiAP Access:** Provide RADIUS, 802.1X, certificate authentication, dynamic VLAN assignment, and identity-based wired and wireless access.
- **Trusted Endpoint SSO:** Combine FortiAuthenticator, FortiClient EMS, FortiClient, and FortiGate ZTNA to validate user identity and endpoint posture.
- **Security Fabric SSO:** Centralize SAML authentication and role-based access for FortiGate, FortiManager, FortiAnalyzer, FortiWeb, FortiSASE, and other supported products.
- **Certificate-Based Security:** Issue and manage certificates for FortiGate VPNs, administration, wireless access, endpoints, and device-to-device trust.
- **FortiManager Deployment:** Streamline certificate-based FortiGate and site-to-site VPN deployments.
- **Centralized Monitoring:** Send authentication and identity events to FortiAnalyzer for visibility, auditing, investigation, and compliance reporting.

| FORTIAUTHENTICATOR | | | |
|---|---|---|---|
| **Functional Area** | **Feature** | **Appliance and VM** | **FortiAuthenticator Cloud** |
| **RADIUS** | VPN Authentication | ✓ | ✓ |
| | Admin Authentication | ✓ | ✓ |
| | 802.1X | ✓ | ✓ |
| | Dynamic VLAN | ✓ | ✓ |
| | Change of Authorization | ✓ | ✓ |
| **TACACS+** | Admin Authentication | ✓ | — |
| | Command Authorization | ✓ | — |
| **FSSO** | FortiGate polling, Collector Agent support | ✓ | ✓ |
| | Syslog, RSSO, WSSO | ✓ | ✓ |
| | FortiClient SSO Mobility Agent[1] | ✓ | ✓ |
| **Single Sign-On** | SAML IdP, IdP Proxy | ✓ | ✓ |
| | SSLVPN | ✓ | ✓ |
| | Google, AWS, Azure and O365 integration | ✓ | ✓ |
| | OAuth2/OIDC Provider | ✓ | ✓ |
| | SCIM Provisioning (client and server) | ✓ | ✓ |
| **MFA** | FortiToken Mobile (FTM)[2] | ✓ | Add-on purchase |
| | FortiToken (FTK) | ✓ | Add-on purchase |
| | SMS[3] | Add-on purchase (or third party gateway) | Add-on purchase (or third party gateway) |
| | Email[3] | ✓ | ✓ |
| | FIDO Passwordless[4] | ✓ | ✓ |
| | Adaptive Authentication | ✓ | ✓ |
| | Windows Agent | ✓ | ✓ |
| | OWA Agent | ✓ | ✓ |
| **Portals** | Captive Portal | ✓ | ✓ |
| | Self-Registration and Guest | ✓ | ✓ |
| | Social Login | ✓ | ✓ |
| **PKI Certificate Management** | Server certificates | ✓ | ✓ |
| | User certificates | ✓ | ✓ |
| | VPNs, SCEP, ZTNA | ✓ | ✓ |
| | CMPv2 | ✓ | ✓ |
| **HA** | Active-Passive[5] | ✓ | — |
| | Load Balancing[5] | ✓ | — |

1 FortiClient SSO agent license purchased separately.

2 Software and hardware tokens are purchase separately.

3 FortiGuard SMS license needed (or use third party SMS gateway). If purchase FTM tokens, get 2 x No. of Tokens FortiGuard SMS credits (must be used within one year).

4 FIDO FTK400 tokens are purchased separately.

5 Separate license needed for each FortiAuthenticator VM.

Existing FortiAuthenticator Cloud customers are entitled to MFA from FortiIdentity Cloud until their subscription expires, then additional MFA purchases are required.

# Specifications

| FORTIAUTHENTICATOR MODEL NO. | FAC-300G | FAC-800G |
|---|---|---|
| **Hardware** | | |
| **10/100/1000 Interfaces (Copper, RJ-45)** | 4 | 4 |
| **SFP Interfaces** | 0 | 2 |
| **Local Storage** | 2 × 1TB SSD - RAID 1 | 2 × 2TB SSD - RAID 1 |
| **Trusted Platform Module (TPM)** | Yes | Yes |
| **Power Supply** | 450W Redundant Auto Ranging (100-240V), Ships with 1 PSU by default (0+1), additional PSU available, SKU SP-FAC300G-PS | Dual (1+1) 450W Redundant Auto Ranging (100-240V) |
| **System Capacity** (Based on the number of licensed users) | | |
| **Local + Remote Users (Base / Upper Limit)** | 1500 / 3500 | 8000 / 18 000 |
| **FortiTokens** | # of licensed users x2 | # of licensed users x2 |
| **Auth Clients (RADIUS and TACACS+)** | # of licensed users /3 | # of licensed users /3 |
| **User Groups** | # of licensed users /5 | # of licensed users /5 |
| **CA Certificates** | 10 | 50 |
| **User Certificates** | # of licensed users x5 | # of licensed users x5 |
| **Dimensions** | | |
| **Height x Width x Length (inches)** | 1.73 × 17.24 × 16.54 | 1.73 × 17.24 × 24 |
| **Height x Width x Length (mm)** | 44 × 438 × 420 | 44 × 438 × 610 |
| **Weight** | 12.7 lbs (5.75 kg) | 26.2 lbs (11.87 kg) |
| **Environment** | | |
| **Form Factor** | Rack Mountable (1RU) | Rack Mountable (1RU) |
| **Power Source** | 100-240 VAC, 50/60Hz 450W Redundant (1+0) | 100-240 VAC, 50/60Hz 450W Redundant (1+1) |
| **Maximum Current** | 6A Max. | 6A Max. |
| **Power Consumption (Average / Maximum)** | 101.5W/131.7W | 159.2W/175.4W |
| **Heat Dissipation** | 449.3 BTU/h | 598.1 BTU/h |
| **Forced Airflow** | Front to Back | Front to Back |
| **Noise Level** | | |
| **Operating Temperature** | 32°F to 104° F (0°C to 40° C) | 32°F to 104° F (0°C to 40° C) |
| **Storage Temperature** | -40°F to 158° F (-40°C to 70° C) | -40°F to 158° F (-40°C to 70° C) |
| **Humidity** | 5% to 95% relative humidity, non-operating, non-condensing 5% | 5% to 95% relative humidity, non-operating, non-condensing 5% |
| **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 |

For more hardware information please refer to quick start guide documentation
https://docs.fortinet.com/product/fortiauthenticator/hardware



FAC-300G

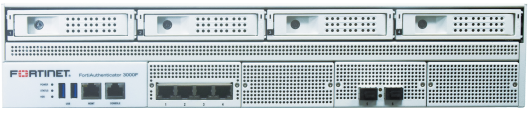


FAC-800G

# Specifications

| FORTIAUTHENTICATOR MODEL NO. | FAC-3000F | FAC-3000G (AVAILABLE Q1 2027) |
|---|---|---|
| **Hardware** | | |
| **10/100/1000 Interfaces (Copper, RJ-45)** | 4 | 4 |
| **SFP Interfaces** | 2 | 2 |
| **Local Storage** | 2× 2 TB SAS Drive - RAID 1 | 2 × 2TB SSD - RAID 1 |
| **Trusted Platform Module (TPM)** | Yes | Yes |
| **Power Supply** | Dual (1+1) 1000W Auto Ranging (100V–240V) | Dual (1+1) 850W Redundant Auto Ranging (100-240V) |
| **System Capacity** (Based on the number of licensed users) | | |
| **Local + Remote Users (Base / Upper Limit)** | 40 000 / 240 000 | 40 000 / 1 million |
| **FortiTokens** | # of licensed users x2 | # of licensed users x2 |
| **Auth Clients (RADIUS and TACACS+)** | # of licensed users /3 | # of licensed users /3 |
| **User Groups** | # of licensed users /5 | # of licensed users /5 |
| **CA Certificates** | 50 | 50 |
| **User Certificates** | # of licensed users x5 | # of licensed users x5 |
| **Dimensions** | | |
| **Height x Width x Length (inches)** | 3.46 × 17.24 × 23.66 | 3.46 × 17.24 × 23.66 |
| **Height x Width x Length (mm)** | 88 × 438 × 601 | 88 × 438 × 601 |
| **Weight** | 44 lbs (20 kg) | 42.3 lbs (19.2 kg) |
| **Environment** | | |
| **Form Factor** | Rack Mountable (2 RU) | Rack Mountable (2RU) |
| **Power Source** | 100–240V AC, 50–60 Hz | 100-240 VAC, 50/60Hz 850W Redundant (1+1) |
| **Maximum Current** | 100-127/200-240VAC, 50/60Hz, 10/5A | 70.8A Max. |
| **Power Consumption (Average / Maximum)** | 193.30 W / 236.28 W | 177W/210W |
| **Heat Dissipation** | 1325 BTU/h | 716.5 BTU/h |
| **Forced Airflow** | Front to back | Front to Back |
| **Noise Level** | 49.8 db | 49.8 dB |
| **Operating Temperature** | 32°–104°F (0°–40°C) | 32°F to 104° F (0°C to 40° C) |
| **Storage Temperature** | -40°–158°F (-40°–70°C) | -40°F to 158° F (-40°C to 70° C) |
| **Humidity** | 5%–90% non-condensing | 5% to 95% relative humidity, non-operating, non-condensing 5% |
| **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, BSMI, KC, UL/cUL, CB, GOST | |

For more hardware information please refer to quick start guide documentation
https://docs.fortinet.com/product/fortiauthenticator/hardware



FAC-3000F



FAC-3000G

# Subscription, Perpetual VM, and FortiAuthenticator Cloud

| VIRTUAL APPLIANCES | SUBSCRIPTION VM | FAC-VM BASE | FAC-VM-100-UG | FAC-VM-1000-UG | FAC-VM-10000-UG | FORTIAUTHENTICATOR CLOUD |
|---|---|---|---|---|---|---|
| **Capacity** | | | | | | |
| **Users (Local and Remote)** | per user | Up to 100 | 100+ | 1000+ | 10000+ | per user |
| **FortiTokens** | Users x2 | | | | | |
| **NAS Devices** | number of licensed users /3 | | | | | |
| **User Groups** | number of licensed users /5 | | | | | |
| **CA Certificates** | number of licensed users /10 | | | | | |
| **User Certificates** | number of licensed users x5 | | | | | |
| **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 | | | | | NA (hosted solution)<br>max vCPU support - depending on user licensed |
| **Minimum/Maximum Virtual CPUs Supported** | 8/64 | | | | | 64 |
| **Virtual NICs Required (Minimum / Maximum)** | 1 / 4 | | | | | 1 / 4 |
| **Virtual Machine Storage (Minimum / Maximum)** | 60 GB / 16 TB | | | | | 60 GB / 16 TB |
| **Virtual Machine Memory Required (Minimum / Maximum)** | 16 GB / 1 TB | | | | | Auto assign based on users |
| **High Availability Support** | Active-Passive HA and Config Sync HA | | | | | DR between Datacenters<br>(note AP, config sync like others) |

# Order Information

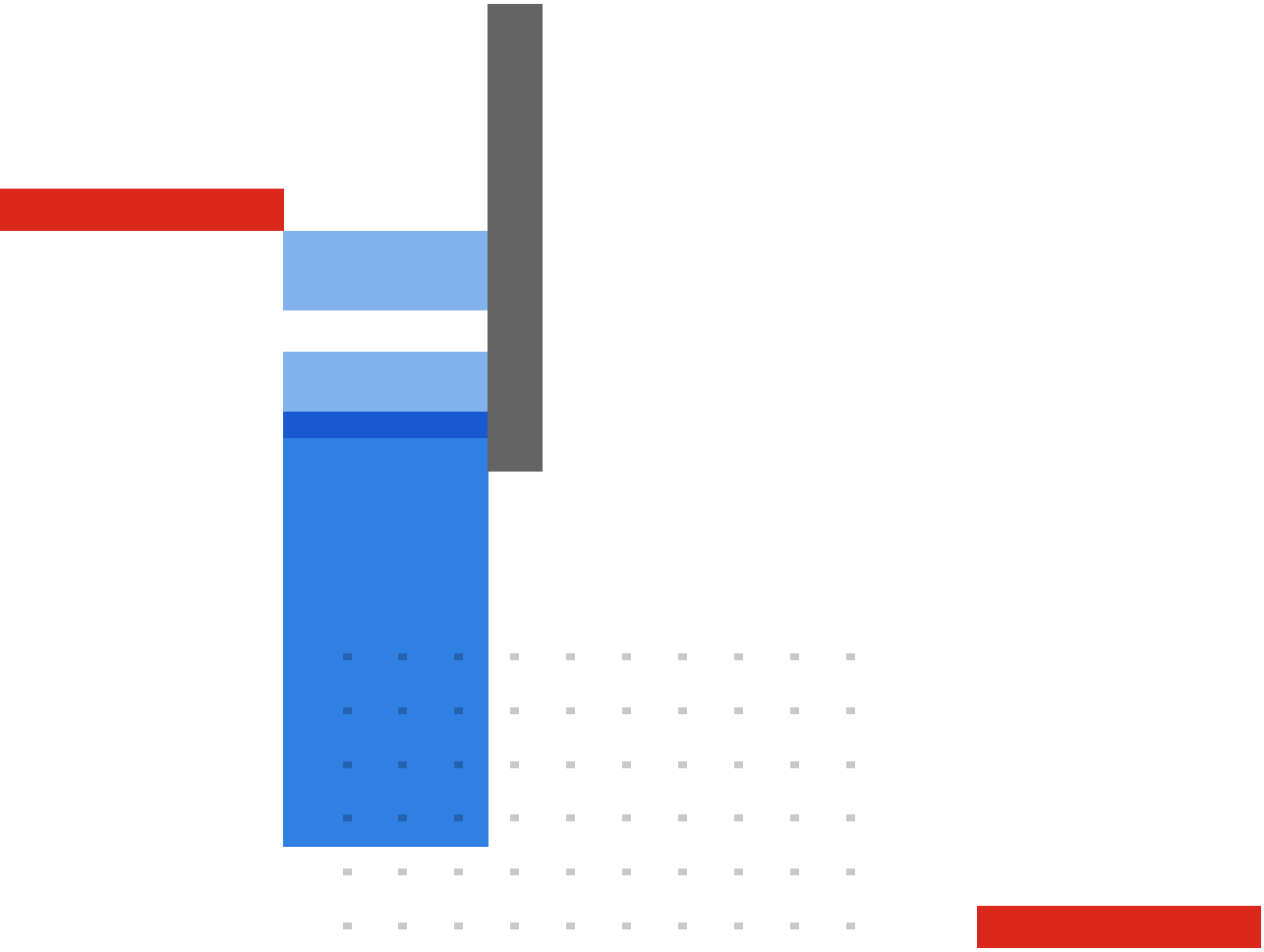
| PRODUCT | SKU | DESCRIPTION |
|---|---|---|
| **Hardware** | | |
| **FortiAuthenticator 300G** | FAC-300G | 4x GE RJ45 ports, 2× 1 TB HDD. Base License supports up to 1500 users. Expand user support to 3500 users by using FortiAuthenticator Hardware Upgrade License. |
| **FortiAuthenticator 800G** | FAC-800G | 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 3000G (Available Q1 2027)** | FAC-3000G | 4x GE RJ45 ports, 2× 10GE SPF, 2× 2TB SAS Drive. Base License supports up to 40 000 users. Expand user support to one million 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. |
| **Hardware Upgrade** | | |
| **Hardware Upgrade Licenses for hardware appliances** | FAC-HW-100UG | FortiAuthenticator 300G, 800G, 3000E, or 3000F/G, 100 user upgrade. |
| | FAC-HW-1000UG | FortiAuthenticator 300G, 800G, 3000E, or 3000F/G, 1000 user upgrade. |
| | FAC-HW-10KUG | FortiAuthenticator 800G, 3000E, or 3000F/G, 10 000 user upgrade. |
| | FAC-HW-100KUG | FortiAuthenticator 3000F/G, 100 000 user upgrade. |
| **FortiAuthenticator Carrier/Advance licence** | | |
| **FortiAuthenticator Carrier License** | FC-10-ACTCR-1343-02-DD | FortiAuthenticator Advance / Carrier License provides unlimited RADIUS and TACACs clients. Applicable to VM subscription and 3000F/G series hardware. |
| **Optional Accessories** | | |
| **Power Supplies** | SP-FAC300G-PS | Power Supply module for FAC-300G and FAC-800G. |
| **FortiAuthenticator VM (subscription and perpetual)** | | |
| **FortiAuthenticator-VM License (VM Subscription)** | FC1-10-ACVMS-1268-02-DD | FortiAuthenticator VM Subscription for 100-999 Users, with FortiCare Elite Support*. |
| | FC2-10-ACVMS-1268-02-DD | FortiAuthenticator VM Subscription for 1000-99 999 Users, with FortiCare Elite Support*. |
| | FC3-10-ACVMS-1268-02-DD | FortiAuthenticator VM Subscription for 100 000+ Users, with FortiCare Elite Support*. |
| **FortiAuthenticator-VM License (Perpetual)** | FAC-VM-Base | VM Base License supports 100 users. Expand user support to one 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 (1–1 M users). |
| **Fortinet Hosted Cloud Solution** | | |
| **FortiAuthenticator Cloud** | FC2-10-ACCLD-511-02-DD* | FortiAuthenticator-Cloud User Subscription including FortiCare Premium Support for 100-499 Users. |
| | FC3-10-ACCLD-511-02-DD* | FortiAuthenticator-Cloud User Subscription including FortiCare Premium Support for 500-1999 Users. |
| | FC4-10-ACCLD-511-02-DD* | FortiAuthenticator-Cloud User Subscription including FortiCare Premium Support for 2000-9999 Users. |
| | FC5-10-ACCLD-511-02-DD* | FortiAuthenticator-Cloud User Subscription including FortiCare Premium Support for 10 000+ Users. |
| **FortiAuthenticator Add-ons (applicable to both hardware, VM subscription, and perpetual and cloud)** | | |
| **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). |

The FortiAuthenticator ordering guide is available here:
https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/og-fortiauthenticator.pdf

For related ordering guides please visit: https://www.fortinet.com/resources/ordering-guides

### 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.



FORTINET

www.fortinet.com

Copyright © 2026 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., 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 SVP Legal and above, 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. 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.

October 21, 2026

FAC-DAT-R53-20261021