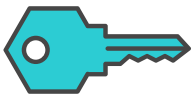
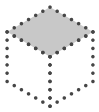


FortiAuthenticator

Available in

Hardware Appliance



Virtual Machine

BYOL using public cloud providers

FortiAuthenticator Cloud

FortiAuthenticator provides key services for creating effective security policies by ensuring that only authorized individuals can access sensitive networks and data. It helps transparently identify network users and enforce identity-driven policies within a Fortinet-enabled enterprise network. FortiAuthenticator offers seamless, secure multi-factor/OTP and FIDO passwordless authentication for various access protocols across an organization. It is available as a hardware appliance, a virtual machine for private and public cloud deployments, or as FortiAuthenticator-Cloud, which is part of a SaaS-based cloud service.

Key features and capabilities of FortiAuthenticator include:

- **Authentication**: RADIUS authentication (including 802.1x, Dynamic VLAN, Change of Authorization), TACACS+ (Admin Authentication, Command Authorization), FSSO (Agent, Polling, Syslog, RSSO, WSSO, SSO Mobility Agent).
- **Single Sign-On (SSO)**: SAML IdP, IdP Proxy, SSLVPN, integration with Google, AWS, Azure, and O365, OAuth2/OIDC Provider, and SCIM Provisioning.
- **Multi-Factor Authentication (MFA)**: Supports FortiToken Mobile (FTM), FortiToken (FTK), FortiToken Cloud (FTC), SMS and Email OTP, FIDO Passwordless, and Adaptive Authentication.
- **Portals**: Captive Portal, Self-Registration and Guest portals, and Social Login.
- **PKI Certificate Management**: Manages Server certificates, User certificates, VPNs, SCEP, ZTNA, and CMPv2.
- **High Availability (HA)**: Active Passive HA is supported for Appliance and VM deployments.
- **Load Balancing**: Supported for Appliance and VM deployments.

FUNCTIONAL AREA	FEATURE	FORTIAUTHENTICATOR APPLIANCE AND VM	FORTIAUTHENTICATOR CLOUD
RADIUS	VPN Authentication	✓	✓
	Admin Authentication	✓	✓
	802.1X	✓	✓
	Dynamic VLAN	✓	✓
	Change of Authorization	✓	✓
TACACS+	Admin Authentication	✓	N/A
	Command Authorization	✓	N/A
FSSO	FortiGate polling, Collector Agent support	✓	✓
	Syslog, RSSO, WSSO, etc	✓	✓
	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 3rd party gateway)	Add-on purchase (or 3rd 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]	✓	N/A
	Load Balancing[5]	✓	N/A

1 FortiClient SSO agent license purchased separately. See section “Other FortiAuthenticator Add-Ons” on page 5

2 Software and hardware tokens are purchased 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.

License Order Information

FORTIAUTHENTICATOR HARDWARE (F-SERIES MODELS)		
PRODUCT	**SKU**	**DESCRIPTION**
BASE USER LICENSE		
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 HARDWARE (G-SERIES MODELS)		
PRODUCT	**SKU**	**DESCRIPTION**
BASE USER LICENSE		
FortiAuthenticator 300G	FAC-300G	4x GE RJ45 ports, 2× 1 TB SSD. 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 SSD. Base license supports up to 8000 users. Expand user support to 18 000 users by using FortiAuthenticator Hardware Upgrade License.
FortiAuthenticator 3000G	FAC-3000G	4x GE RJ45 ports, 2x SFP, 2× 2TB SSD. Base License supports up to 40 000 users. Expand user support to 1 million users by using FortiAuthenticator Hardware Upgrade License.

USER UPGRADE LICENSE		
PRODUCT	**SKU**	**DESCRIPTION**
Hardware Upgrade licenses for FAC-300F/G, FAC-800F/G, and FAC-3000F/G	FAC-HW-100UG	FortiAuthenticator 300F/G, 800F/G, 3000E, or 3000F/G, 100 user upgrade.
	FAC-HW-1000UG	FortiAuthenticator 300F/G, 800F/G, 3000E, or 3000F/G, 1000 user upgrade.
	FAC-HW-10KUG	FortiAuthenticator 800F/G, 3000E, or 3000F/G, 10 000 user upgrade.
	FAC-HW-100KUG	FortiAuthenticator 3000F/G, 100 000 user upgrade.

User upgrade licenses are stackable. For example:
FAC-300F supporting 1500 users in base license and upgrading with 2 × 100UG to support total of 1500 + 200 users = 1700 users in total

Base and Upper Limit for HW Models

For hardware model please find the base and upper limit for number of users supported.

FAC H/W MODEL	BASE LICENSE USER LIMIT	UPGRADE UPPER LIMIT
300F/G	1500	3500
800F/G	8000	18000
3000F/G	40000	240000 (3000F), 1M (3000G)

FortiAuthenticator Carrier/Advance License

SHORT DESCRIPTION	SKU	DESCRIPTION
FortiAuthenticator Carrier License	FC-10-ACTCR-1343-02-DD	FortiAuthenticator Advance / Carrier License - applicable to FAC VMS and FAC-3000F/G only. Providing unlimited RADIUS and TACACs clients.

FORTIAUTHENTICATOR VIRTUAL MACHINE		
PRODUCT	**SKU**	**DESCRIPTION**
SUBSCRIPTION (PER USER LICENSE)		
FortiAuthenticator - VM Subscription (Available in v8.0 FortiAuthenticator)	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*
PERPETUAL WITH USER UPGRADES		
FortiAuthenticator-VM Perpetual	FAC-VM-Base	VM Base License supports 100 users. Exapnd 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.
SUPPORT CONTRACTS		
FortiAuthenticator-VM Perpetual	FC1-10-0ACVM-248-02-DD**	1 Year 24×7 FortiCare Contract (1-500 users).
	FC2-10-0ACVM-248-02-DD**	1 Year 24×7 FortiCare Contract (1-1100 users).
	FC3-10-0ACVM-248-02-DD**	1 Year 24×7 FortiCare Contract (1-5100 users).
	FC4-10-0ACVM-248-02-DD**	1 Year 24×7 FortiCare Contract (1-10 100 users).
	FC8-10-0ACVM-248-02-DD**	1 Year 24×7 FortiCare Contract (1-25 100 users).
	FC5-10-0ACVM-248-02-DD**	1 Year 24×7 FortiCare Contract (1-50 100 users).
	FC6-10-0ACVM-248-02-DD**	1 Year 24×7 FortiCare Contract (1-100 100 users).
	FC9-10-0ACVM-248-02-DD**	1 Year 24×7 FortiCare Contract (1-500 100 users).
	FC7-10-0ACVM-248-02-DD**	1 Year 24×7 FortiCare Contract (1-1M users).
	FCA-10-0ACVM-248-02-DD**	FortiCare Premium Support (1mil+ users).

*FortiCare Elite provides better response time. Please refer to https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-forticare-services.pdf

**DD specifies the number of years e.g. 1, 3 or 5 years of support

For new orders, FAC-VM user licenses are stackable but support contracts are not. For existing users and support upgrade, please request a co-term quotation to your Fortinet authorized partner.

FAC-VM HA nodes require separate licensing.

FORTIAUTHENTICATOR CLOUD		
PRODUCT	**SKU**	**DESCRIPTION**
SUBSCRIPTION (PER USER LICENSE)		
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 500-1,999 Users.
	FC4-10-ACCLD-511-02-DD	FortiAuthenticator-Cloud User Subscription including FortiCare Premium Support for 2,000-9,999 Users.
	FC5-10-ACCLD-511-02-DD	FortiAuthenticator-Cloud User Subscription including FortiCare Premium Support for 10,000+ Users.

*DD specifies the number of years e.g. 1, 3 or 5 years of support

Other FortiAuthenticator Add-Ons

FortiClient SSO mobility agent license enables FortiClient Single-Sign-On (SSO) to communicate to FortiAuthenticator on username/IP changes, so that they can be used in FortiGate user group based policy if required. These SKUs are applicable to both hardware, subscription and perpetual VM offerings.

FORTICLIENT SSO MOBILITY AGENT		
PRODUCT	**SKU**	**DESCRIPTION**
FortiClient SSO License for FortiAuthenticator	FCC-FAC2K-LIC	FortiAuthenticator FortiClient SSO Mobility License for 2000 FortiClient connections (does not include FortiClient Endpoint Control License for FortiGate)
	FCC-FAC10K-LIC	FortiAuthenticator FortiClient SSO Mobility License for 10 000 FortiClient connections (does not include FortiClient Endpoint Control License for FortiGate)
	FCC-FACUNL-LIC	FortiAuthenticator FortiClient SSO Mobility License for unlimited FortiClient connections (does not include FortiClient Endpoint Control License for FortiGate)

Stackable license. FAC HA nodes require separate licensing.

For additional FortiTokens (hardware, FIDO, or FortiToken Mobile) and FortiSMS add-ons to FortiAuthenticator or FortiAuthenticator Cloud please refer to FortiToken order guide here: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/og-fortitoken.pdf

FORTIGUARD SMS		
PRODUCT	**SKU**	**DESCRIPTION**
FortiSMS	SMS-ELIC-100	License for 100 SMS text messages.

License is stackable. Customer has option to use a third-party SMS gateway (Bring Your Own SMS). SMS SKUs for FortiIdentity Cloud cannot be applied to FortiAuthenticator SMS. FAC HA nodes require separate licensing.

Maximum Values in Relation to License

There are different object limits within FortiAuthenticator. The limits (max values) are derived from the total user license count. As a general rule of thumb, the maximum values, such as User Groups, will be a factor of the total user license limit. For example, 100 user licenses will provide 20 User Groups (100/5 = 20 user groups). Please consider carefully the use cases for license purchase.

For the full limit table, see the FortiAuthenticator Release Notes.

MAXIMUM VALUES FOR	VM	300F/G	800F/G	3000F/G
Users (local and remote)	100 (up to 1 million+ w/ upgrade license)	1500 (up to 3500 w/ upgrade license)	8000 (up to 18,000 w/ upgrade license)	40,000 (up to 240k(F), 1M(G) w/ upgrade license)
FortiTokens (Hardware & soft tokens sold separately)	# of licensed users x2			
User Groups	#of licensed users /5			
SSO Users	# of licensed users			
Guest Users	# of licensed users			
Social Users	# of licensed users			
Device (MAC-based Auth.)	# of licensed users x5			
Auth Clients (RADIUS and TACACS+)	# of licensed users /3			
Remote LDAP Servers	#of licensed users /25			
Remote RADIUS Servers	# of licensed users /25			
Remote SAML Servers	# of licensed users /25			
Remote OAuth Servers	# of licensed users /25			
User Certificates	# of licensed users x 5			
Server Certificates	# of licensed users /10			
TACACS+ Services	# of licensed users /10			
TACACS+ Service Attribute-value Pairs	# of services x 255			

Sample Bill of Materials (BOM)

BOM Example 1 — Small Office MFA + LDAP

Example organization size

- Employees: ~750
- Users in FortiAuthenticator: ~750
- Endpoints: ~1,500 to 2,000 (include BYOD)

Use case

- Small organization requiring centralized authentication services
- 1 year term
- RADIUS authentication for VPN and Wi-Fi access
- Basic multi-factor authentication (MFA) deployment across users
- Hardware tokens required for higher-risk roles (administrators, executives, privileged users)
- FortiToken Mobile used for the majority of users for cost-effective MFA
- High availability preferred since authentication services are 24×7 and critical to business operations

Bill of Materials – If physical appliance option is preferred

ITEM	SKU	QUANTITY	DESCRIPTION	WHY IS IT REQUIRED?
FortiAuthenticator Appliance	FAC-300F	1	FortiAuthenticator 300F appliance, up to 1,500 users	Serves as the central authentication platform for the organization. Provides identity services, LDAP directory integration, RADIUS authentication for VPN and Wi-Fi, and MFA enforcement. Sized to support the current ~750 users while allowing headroom for growth.
FortiAuthenticator Appliance (Secondary for HA)	FAC-300F	1	Second appliance for HA	Authentication is a critical service required for VPN access, Wi-Fi connectivity, and system logins. A secondary appliance enables high availability so authentication services remain operational during maintenance, hardware failure, or upgrades affecting the primary appliance.
FortiCare Premium Support	FC1-10-AC8HF-247-03-12	1	3 year FortiCare support for FAC-300F	Provides firmware updates, security patches, and 24×7 technical support. Ensures the authentication infrastructure remains secure, supported, and operational throughout the deployment lifecycle.
FortiToken Hardware Tokens	FortiToken-200B	1	500 pack hardware OTP tokens	Provides physical one-time-password MFA tokens for higher-risk users such as administrators, executives, or users without mobile devices. Hardware tokens provide a strong MFA method independent of smartphones.
FortiToken Mobile Software Tokens	FTM-ELIC-100 FTM-ELIC-200	1 1	300 FortiToken Software Tokens for FortiToken mobile	Enables mobile-based MFA using the FortiToken Mobile app. This is the primary MFA method for most users and provides a cost-effective, scalable authentication option without requiring dedicated hardware tokens.
SMS Credits	SMS-ELIC-100	1	100 SMS OTP credits	Provides a backup MFA mechanism in the event a user cannot access their FortiToken hardware or mobile token. SMS OTP allows administrators to temporarily authenticate users to maintain productivity.
FortiClient SSO Mobility	FCC-FAC2K-LIC	1	2,000 endpoint SSO license	Enables transparent Single Sign-On and roaming user-to-IP mapping between endpoints and FortiGate. This allows user identity to persist as users move across networks (Wi-Fi, LAN, VPN), enabling identity-based policies and seamless authentication without repeated login prompts.

Bill of Materials – If VM option is preferred

ITEM	SKU	QUANTITY	DESCRIPTION	WHY IS IT REQUIRED?
FortiAuthenticator VM License	FAC-VM-1000	1000	FortiAuthenticator VM license supporting up to 1,000 users	Provides the FortiAuthenticator platform as a virtual machine instead of dedicated hardware. Delivers the same authentication services including LDAP directory integration, RADIUS authentication for VPN and Wi-Fi, and MFA enforcement while allowing deployment on existing virtualization infrastructure such as VMware, Hyper-V, or cloud environments. Sized to support ~750 users with growth headroom.
FortiAuthenticator VM License (Secondary for HA)	FAC-VM-1000	1000	Secondary FortiAuthenticator VM license for HA deployment	Enables high availability for authentication services. Since authentication is required for VPN access, Wi-Fi connectivity, and user logins, a secondary VM ensures continuous operation during maintenance, outages, or host failures.
FortiCare Premium Support	FC1-10-FACVM-247-03-12	1	3 year FortiCare support for FortiAuthenticator VM	Provides firmware updates, security patches, and 24×7 technical support. Ensures the authentication infrastructure remains supported and secure throughout the deployment lifecycle.
FortiToken Hardware Tokens	FortiToken-200B	1	500 pack hardware OTP tokens	Provides physical MFA tokens for higher-risk users such as administrators, executives, or users without smartphones. Hardware tokens provide a secure authentication method independent of mobile devices.
FortiToken Mobile Software Tokens	FTM-ELIC-100 FTM-ELIC-200	1 1	300 FortiToken Mobile software tokens	Enables mobile-based MFA using the FortiToken Mobile application. This provides scalable and cost-effective MFA for most users without requiring dedicated hardware tokens.
SMS Credits	SMS-ELIC-100	1	100 SMS OTP credits	Provides a fallback authentication mechanism in cases where users cannot access their hardware or mobile token. Allows administrators to provide temporary authentication access to maintain productivity.
FortiClient SSO Mobility	FCC-FAC2K-LIC	1	2,000 endpoint SSO license	Enables transparent Single Sign-On and roaming-aware user-to-IP mapping between endpoints and FortiGate. This allows identity-based security policies and seamless authentication as users move between Wi-Fi, LAN, and VPN networks.

Bill of Materials – If FAC Cloud option is preferred

ITEM	SKU	QUANTITY	DESCRIPTION	WHY IS IT REQUIRED?
FortiAuthenticator Cloud Subscription	FC2-10-ACCLD-511-02-12	1000	FortiAuthenticator Cloud subscription supporting up to 1,000 users	Provides the FortiAuthenticator identity and authentication platform as a fully managed cloud service. Enables LDAP directory integration, RADIUS authentication for VPN and Wi-Fi, and MFA enforcement without requiring on-premises infrastructure. Sized to support ~750 users with headroom for growth.
FortiAuthenticator Cloud HA / Service Redundancy	Included	1000	Built-in high availability and redundancy within the Fortinet cloud platform	FortiAuthenticator Cloud includes built-in service redundancy and availability managed by Fortinet. This ensures authentication services remain operational without requiring customers to deploy and maintain secondary infrastructure.
FortiCare Premium Support	Included	1	Support and maintenance included with the cloud subscription	Provides firmware updates, security patches, and 24×7 technical support. Ensures the authentication infrastructure remains supported and secure throughout the deployment lifecycle.
FortiToken Hardware Tokens	FortiToken-200B	1	500 pack hardware OTP tokens	Provides physical MFA tokens for higher-risk users such as administrators, executives, or users without smartphones. Hardware tokens provide a secure authentication method independent of mobile devices.
FortiToken Mobile Software Tokens	FTM-ELIC-100 FTM-ELIC-200	1 1	300 FortiToken Mobile software tokens	Enables mobile-based MFA using the FortiToken Mobile application. This provides scalable and cost-effective MFA for most users without requiring dedicated hardware tokens.
SMS Credits	SMS-ELIC-100	1	100 SMS OTP credits	Provides a fallback authentication mechanism in cases where users cannot access their hardware or mobile token. Allows administrators to provide temporary authentication access to maintain productivity.
FortiClient SSO Mobility	FCC-FAC2K-LIC	1	2,000 endpoint SSO license	Enables transparent Single Sign-On and roaming-aware user-to-IP mapping between endpoints and FortiGate. This allows identity-based security policies and seamless authentication as users move between Wi-Fi, LAN, and VPN networks.

BOM Example 2 — Mid-Sized Organization VM Subscription with HA

Example organization size

- Employees: ~6,000
- Users in FortiAuthenticator: ~6,100
- Endpoints: ~9,000 to 12,000
- Budget: Opex model preferred (renewing every year)

Use case

- Mid-sized enterprise requiring a virtual IAM platform for 1 year with:
- High availability for VPN (with SMS authentication with VPN)
- Wi-Fi RADIUS with Cisco APs,
- SAML authentication with public cloud

Bill of Materials

ITEM	SKU	QUANTITY	DESCRIPTION	WHY IS IT REQUIRED?
FortiAuthenticator VM Subscription	FC2-10-ACVMS-1268-02-12	6000	FortiAuthenticator VM subscription supporting the required user capacity	Provides the virtual FortiAuthenticator identity and authentication platform. Delivers centralized authentication services including RADIUS for VPN and Wi-Fi, LDAP directory integration, SAML identity provider functionality for public cloud applications, and MFA enforcement. Sized to support the organization's user base.
FortiAuthenticator VM Subscription (Secondary HA)	FC1-10-ACVMS-1268-02-12	6000	Second VM license for HA node	Provides a secondary FortiAuthenticator instance for high availability. Since authentication services are required for VPN connectivity and enterprise Wi-Fi access, a secondary node ensures service continuity during maintenance, upgrades, or infrastructure failure.
FortiToken Mobile Software Tokens	FTM-ELIC-5000 FTM-ELIC-2000 FTM-ELIC-200	1 1 1	7200 FortiToken Software Tokens for FortiToken mobile	Provides mobile-based MFA for VPN access, SAML authentication to cloud services, and other protected resources. Software tokens allow users to authenticate securely through the FortiToken Mobile application without requiring hardware token distribution.
SMS Credits	SMS-ELIC-100	3	300 SMS credits total, to serve as a backup to FortiToken Mobile	Provides a fallback authentication method when users cannot access their mobile token (for example lost device or application unavailable). SMS OTP allows administrators to maintain access continuity for VPN and remote access users.

BOM Example 3 — Cloud-First IAM

Example organization size

- Employees: ~3,500
- Users in FortiAuthenticator Cloud: ~3,500
- Endpoints: ~5,000 to 7,000

Use case

- Organization preferring SaaS-delivered identity services with no on-premises infrastructure.
- 1 year commitment
- Do not have own DC, so prefer Fortinet hosted cloud solution

Bill of Materials

ITEM	SKU	QUANTITY	DESCRIPTION	WHY IS IT REQUIRED?
FortiAuthenticator Cloud Subscription	FC4-10-ACCLD-511-02-12	3500	Cloud IAM subscription 2,000–9,999 users	Provides the FortiAuthenticator identity and authentication platform as a fully managed SaaS service hosted by Fortinet. Delivers centralized authentication, MFA enforcement, and integration with VPN, Wi-Fi RADIUS, and SAML-based authentication for cloud applications without requiring the organization to deploy or manage on-premises infrastructure.
FortiToken Mobile Software Tokens	FTM-ELIC-2000	2	4000 Mobile MFA tokens covering all users	Enables mobile-based MFA using the FortiToken Mobile application. Provides strong second-factor authentication for VPN access, cloud application authentication, and other protected services. Mobile tokens eliminate the need to distribute and manage hardware tokens while supporting the entire user population.
FortiClient SSO Mobility	FCC-FAC10K-LIC	Optional	10,000 endpoint SSO license	Enables endpoint-based identity awareness and transparent Single Sign-On between endpoints and FortiGate. This allows the security infrastructure to maintain continuous user-to-device mappings, enabling identity-based policies and seamless access as users move between networks. This is optional if device-aware identity tracking is required.

BOM Example 4 — Mid-Size Enterprise MFA + SSO (VM vs Hardware + HA Options)

Example organization size

- Employees: ~5,700
- Users in FortiAuthenticator: ~5,700
- Endpoints: ~8,000 to 10,000

Use case

- Mid-sized enterprise requiring centralized authentication and MFA for 1 year
- ~50% of users (2,850) require FortiToken Mobile MFA
- Full deployment of FortiClient SSO Mobility across all users/devices
- Customer evaluating both VM and Hardware deployment models
- High availability required (Active/Passive or Active/Active)
- Licensing must support HA regardless of deployment model

Bill of Materials — VM Subscription (Standalone + w/HA Additions)

ITEM	SKU	QUANTITY	DESCRIPTION	WHY IS IT REQUIRED?
FortiAuthenticator VM Subscription	FC2-10-ACVMS-1268-02-12	6000	VM subscription supporting required user capacity	Provides the FortiAuthenticator platform as a subscription-based virtual appliance. Delivers centralized authentication, LDAP integration, RADIUS for VPN/Wi-Fi, SAML for cloud apps, and MFA enforcement without requiring hardware. Sized for ~5,700 users with growth headroom.
FortiToken Mobile Software Tokens	FTM-ELIC-2000	1	2,000 mobile MFA tokens	Provides MFA coverage for the majority of users using FortiToken Mobile.
FortiToken Mobile Software Tokens	FTM-ELIC-1000	1	1,000 mobile MFA tokens	Completes MFA coverage (~3,000 total) with additional headroom in a cost-effective manner.
FortiClient SSO Mobility	FCC-FAC10K-LIC	1	10,000 endpoint SSO license	Enables endpoint-based identity awareness and seamless SSO across all users and devices.
HA Add-On: FortiAuthenticator VM Subscription	FC2-10-ACVMS-1268-02-12	+6000	Additional VM subscription for HA node	Required to deploy a second FortiAuthenticator VM instance for high availability. Subscription licensing must match the primary node to support full user capacity.
HA Add-On: FortiClient SSO Mobility	FCC-FAC10K-LIC	+1	Additional SSO license for HA node	Required per node to maintain SSO and identity mapping across the HA cluster.

Bill of Materials — Hardware (Standalone + w/HA Additions)

ITEM	SKU	QUANTITY	DESCRIPTION	WHY IS IT REQUIRED?
FortiAuthenticator Appliance	FAC-800F	1	Appliance supporting up to 8,000 users	Provides a dedicated hardware platform for centralized authentication, MFA, LDAP, RADIUS, and SAML services sized for the organization.
FortiToken Mobile Software Tokens	FTM-ELIC-2000	1	2,000 mobile MFA tokens	Provides MFA coverage for the majority of users.
FortiToken Mobile Software Tokens	FTM-ELIC-1000	1	1,000 mobile MFA tokens	Completes MFA coverage with additional headroom.
FortiClient SSO Mobility	FCC-FAC10K-LIC	1	10,000 endpoint SSO license	Enables user-to-device mapping and seamless SSO across the environment.
FortiCare Premium Support	FC-10-AC8HF-247-02	1	Support for FAC-800F	Ensures ongoing support, updates, and maintenance for the hardware appliance.
HA Add-On: FortiAuthenticator Appliance	FAC-800F	+1	Second appliance for HA	Required to enable high availability for authentication services.
HA Add-On: FortiClient SSO Mobility	FCC-FAC10K-LIC	+1	Additional SSO license for HA node	Required per appliance in HA to maintain identity awareness and SSO.
HA Add-On: FortiCare Premium Support	FC-10-AC8HF-247-02	+1	Support for HA appliance	Each appliance in the HA cluster requires its own support contract.

Fortinet Training and Certification

FCP – FortiAuthenticator Administrator Training and Certification

Learn how to use FortiAuthenticator for secure authentication and identity management, configure and deploy FortiAuthenticator, use FortiAuthenticator for certificate management and two-factor authentication, authenticate users using LDAP and RADIUS servers, and explore SAML SSO options on FortiAuthenticator.

Course Details

For prerequisites, agenda topics, and learning objectives, visit:
https://training.fortinet.com/local/staticpage/view.php?page=library_fortiauthenticator-administrator

Training Offering

For training SKUs, purchasing, and delivery options, visit:
https://training.fortinet.com/local/staticpage/view.php?page=purchasing_process

Frequently Asked Questions

Is it possible to purchase a license for 3000 users and split it between two FortiAuthenticators with 1500 users each?

No. The FAC user licenses are tied to their respective FortiAuthenticators; such a configuration is not possible.

Do I need an additional FTM license for an FAC HA node (either Active Passive or Active-Active Load Balancing)?

No. The FTM license is replicated across all HA nodes.

FAC-OG-R20-20260505