FortiAuthenticator™

Identity and Access Management

Highlights

FortiAuthenticator delivers transparent identification via wide range of methods

- Polling an Active Directory Domain Controller
- Integration with FortiAuthenticator Single Sign-On Mobility Agent which detects login, IP address changes, and logout
- FSSO Portal-based authentication with tracking widgets to reduce the need for repeated authentications
- Monitoring RADIUS Accounting Start records

Enterprise Network Identity Policy

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.

Fortinet Single Sign-On is the method of providing secure identity and role-based access to the Fortinet connected network. Through integration with existing Active Directory or LDAP authentication systems, it enables enterprise user identity-based security without impeding the user or generating work for network administrators.

FortiAuthenticator builds on the foundations of Fortinet Single Sign-on, adding a greater range of user identification methods and greater scalability. FortiAuthenticator is the gatekeeper of authorization into the Fortinet secured enterprise network identifying users, querying access permissions from third party systems, and communicating this information to FortiGate devices for use in Identity-Based Policies.

Available in:

Appliance

Virtual Machine

Hosted

Cloud

Features

- Enables identity and role-based security policies in the Fortinet secured enterprise network without the need for additional authentication through integration with Active Directory
- Strengthens enterprise security by simplifying and centralizing the management of user identity information
- Secure Multi-factor/OTP Authentication with full support for FortiToken
- RADIUS and LDAP Authentication
- Certificate management for enterprise VPN deployment
- IEEE802.1X support for wired and wireless network security
- SAML SP/IdP Web SSO
- OpenID Connect SSO
- FIDO2 Features
  Also known as Passwordless authentication, FIDO2 is another Strong Authentication technique allowing use of strong single factor (passwordless), two-factor, and multi-factor authentication for added protection

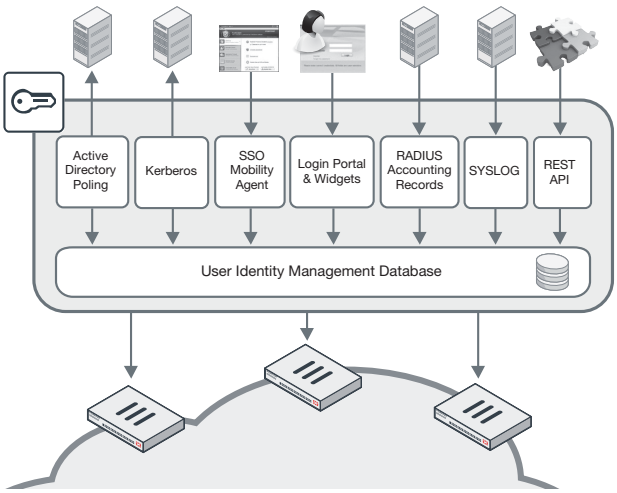
Key Features and Benefits

FSSO Transparent User Identification	Zero impact for enterprise users
Integration with LDAP and AD for group membership	Utilizes existing systems for network authorization information, reducing deployment times and streamlining management processes. Integration with existing procedures for user management
Wide range of user identification methods	Flexible user identification methods for integration with the most diverse enterprise environments
Enablement of identity and role-based security	Allows security administrator to give users access to the relevant network and application resources appropriate to their role, while retaining control and minimizing risk

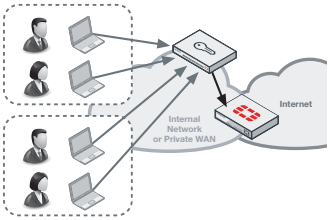
Features

FortiAuthenticator Single Sign-On User Identification Methods

FortiAuthenticator can identify users through a varied range of methods and integrate with third party LDAP or Active Directory systems to apply group or role data to the user and communicate with FortiGate for use in Identity-based policies. FortiAuthenticator is completely flexible and can utilize these methods in combination. For example, in a large enterprise, AD polling or FortiAuthenticator SSO Mobility Agent may be chosen as the primary method for transparent authentication with fallback to the portal for non-domain systems or guest users.

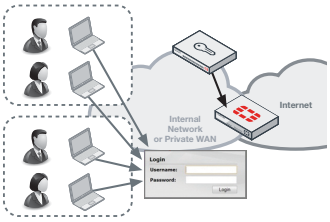


Active Directory Polling



User authentication into an active directory is detected by regularly polling domain controllers. When a user login is detected, the username, IP, and group details are entered into the FortiAuthenticator User Identity Management Database and according to the local policy, can be shared with multiple FortiGate devices.

FortiAuthenticator SSO Mobility Agent

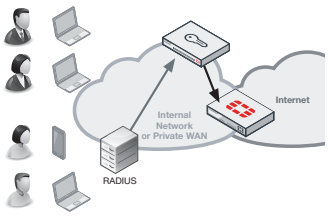


For complicated distributed domain architectures where the polling of domain controllers is not feasible or desired, an alternative is the FortiAuthenticator SSO Client. Distributed as part of FortiClient or as a standalone installation for Windows PCs, the client communicates login, IP stack changes (Wired > Wireless, wireless network roaming), and logout events to the FortiAuthenticator, removing the need for polling methods.

FortiAuthenticator Portal and Widgets

For systems that do not support AD polling or where a client is not feasible, FortiAuthenticator provides an explicit authentication portal. This portal allows the users to manually authenticate to the FortiAuthenticator and subsequently into the network. To minimize the impact of repeated logins required for manual authentication, a set of widgets is provided for embedding into an organization's intranet that automatically logs the users in with browser cookies whenever they access the intranet homepage.

Highlights



RADIUS Accounting Login

In a network that utilizes RADIUS authentication (e.g. wireless or VPN authentication), RADIUS Accounting can be used as a user identification method. This information is used to trigger user login and to provide IP and group information, removing the need for a second tier of authentication.

Additional Functionality

Strong User Identity with Multi-factor Authentication

FortiAuthenticator extends multi-factor authentication capability to multiple FortiGate appliances and to third party solutions that support RADIUS or LDAP authentication. User identity information from FortiAuthenticator combined with authentication information from FortiToken, and/or FIDO2 authentication service ensures that only authorized individuals are granted access to your organization's sensitive information. This additional layer of security greatly reduces the possibility of data leaks while helping companies meet audit requirements associated with government and business privacy regulations.

FortiAuthenticator offers the widest range of multi-factor authentication possible including FIDO2 passwordless authentication service to suit your user requirements. With the physical time-based FortiToken 200, FortiToken Mobile (for iOS, Android, and Windows), e-mail/SMS OTP as well as FIDO2, FortiAuthenticator has strong authentication options for all users and scenarios.

Multifactor authentication can be used to control access to applications such as FortiGate management, SSL and IPsec VPN, Wireless Captive Portal login and third party, RADIUS compliant networking equipment and SAML Service Providers. FortiAuthenticator also offers a REST API that can be used to add MFA to any web-based application.

To streamline local user management, FortiAuthenticator includes user self-registration and password recovery features.

Enterprise Certificate-based VPNs

Site-to-site VPNs often provide access direct to the heart of the enterprise network from many remote locations. Often these VPNs are secured simply by a pre-shared key, which, if compromised, could give access to the whole network. FortiOS support certificate-based VPNs; however, the use of certificate secured VPNs has been limited, primarily due to the overhead and complexity introduced by certificate management. FortiAuthenticator removes this overhead involved by streamlining the bulk deployment of certificates for VPN use in a FortiGate environment by cooperating with FortiManager for the configuration and automating the secure certificate delivery via the SCEP protocol.

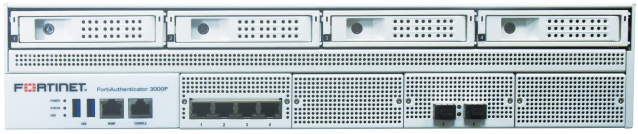
For client-based certificate VPNs, certificates can be created and stored on the FortiToken 300 USB Certificate store. This secure, pin protected certificate store is compatible with FortiClient and can be used to enhance the security of client VPN connections in conjunction with FortiAuthenticator

Additional Features and Benefits

RADIUS and LDAP User Authentication	Local Authentication database with RADIUS and LDAP interfaces centralizes user management
Wide Range of Strong Authentication Methods	Strong authentication provided by FortiAuthenticator via software and hardware One Time Password (OTP) tokens, e-mail and SMS OTP, digital certificates, and FIDO keys helps to ensure password security and mitigate the risk of password disclosure, MITM, phishing, replay, or brute force attacks
User Self-registration and Password Recovery	Reduces the need for administrator intervention by allowing the user to perform their own registration and resolve their own password issues, which also improves user satisfaction
Integration with Active Directory and LDAP	Integration with existing directory simplifies deployment, speeds up installation times, and reutilizes existing development
Certificate Management	Streamlined certificate management enables rapid, cost-effective deployment of certificate-based authentication methods such as VPN
802.1X Authentication	Deliver enterprise port access control to validate users connection to the LAN and Wireless LAN to prevent unauthorized access to the network

FortiAuthenticator 300F

FortiAuthenticator 800F



FortiAuthenticator 3000F

Specifications

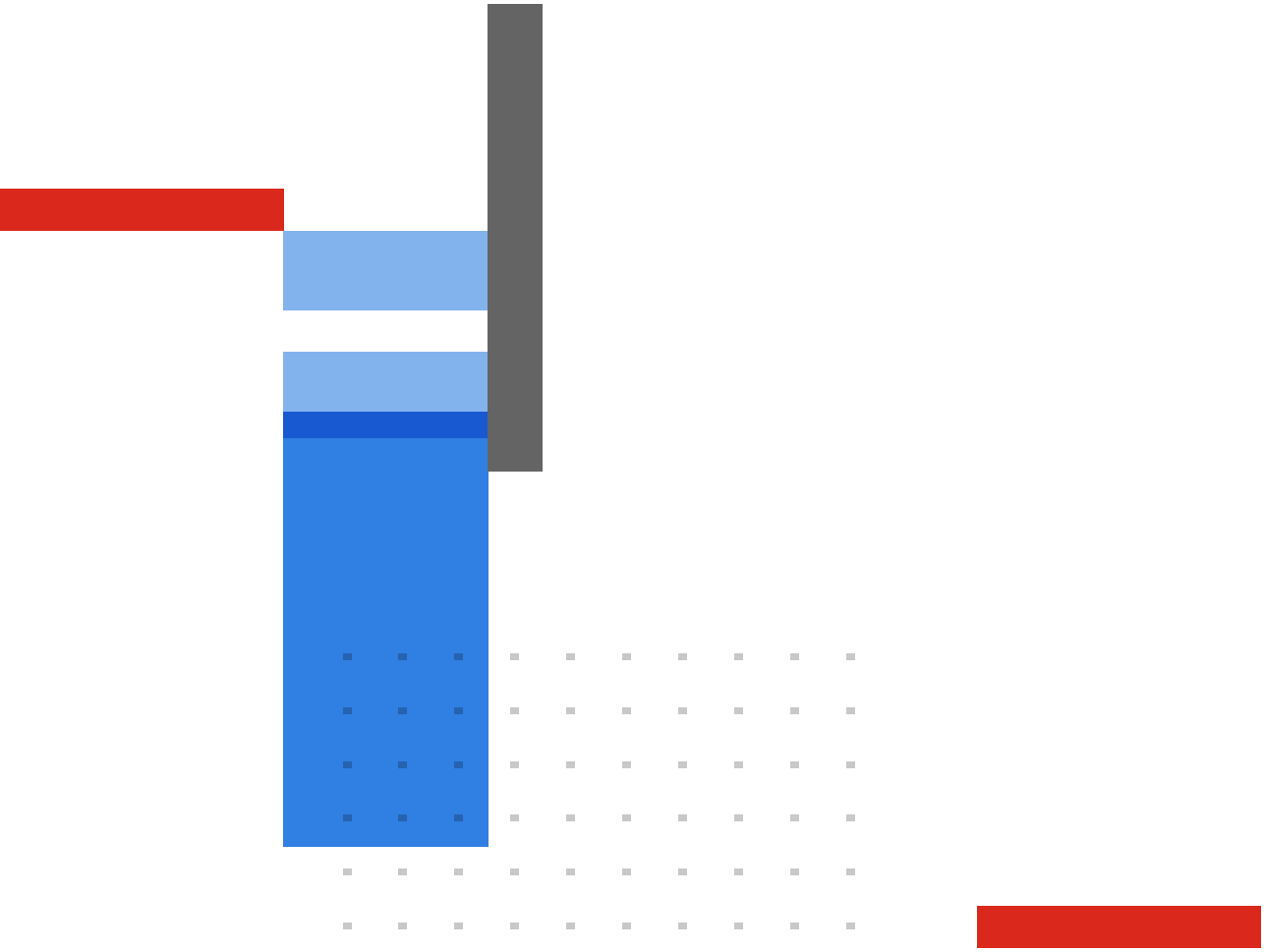
FORTIAUTHENTICATOR MODEL NO.	FAC-300F	FAC-800F	FAC-3000F
Hardware			
10/100/1000 Interfaces (Copper, RJ-45)	4	4	4
SFP Interfaces	0	2	2
Local Storage	2× 1TB Hard Disk Drive - RAID 1	2× 2 TB Hard Disk Drive - RAID 1	2× 2 TB SAS Drive - RAID 1
Trusted Platform Module (TPM)	Yes	Yes	Yes
Power Supply	300W 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)	500	2666	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.



www.fortinet.com

November 29, 2023

FAC-DAT-R41-20231129