DATA SHEET

FortiAuthenticator™

User Identity Management and Single Sign-On

FortiAuthenticator™ user identity management appliances strengthen enterprise security by simplifying and centralizing the management and storage of user identity information.

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.

FortiAuthenticator delivers transparent identification via a wide range of methods:

- Polling of 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 of RADIUS Accounting Start records.

FortiAuthenticator FSSO 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

Additional FortiAuthenticator Features

- Secure Two-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

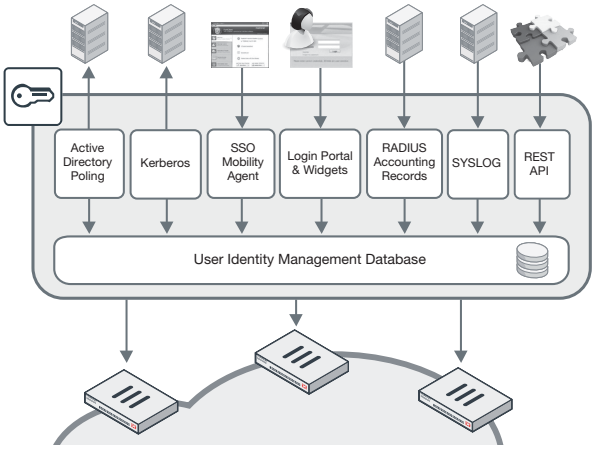
Highlights

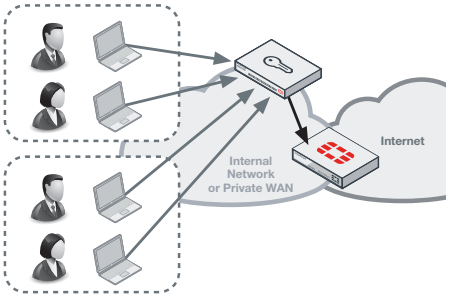
Key Features and Benefits

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 of 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.

FortiAuthenticator Single Sign-On User Identification Methods

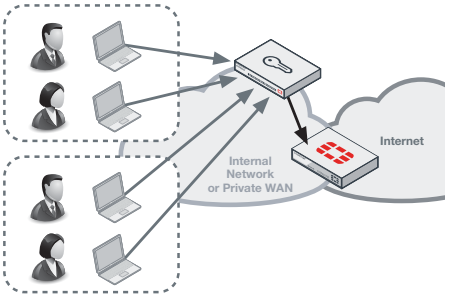
FortiAuthenticator can identify users through a varied range of methods and integrate with third-party LDAP or Active Directory systems to apply group or role data to the user and communicate with FortiGate for use in Identity-based policies. FortiAuthenticator is completely flexible and can utilize 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.





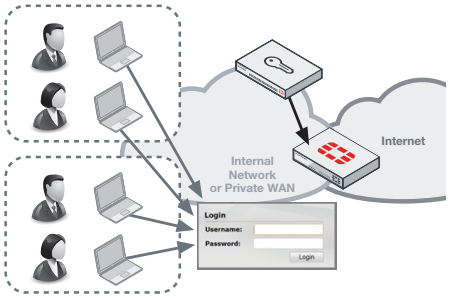
Active Directory Polling

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

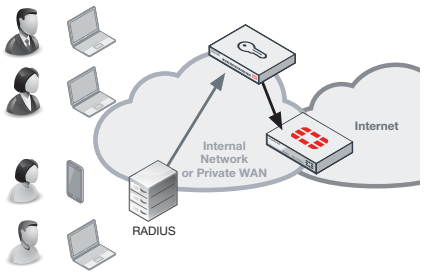
For complicated distributed domain architectures where the polling of domain controllers is not feasible or desired, an alternative is the FortiAuthenticator SSO Client. Distributed as part of FortiClient or as a standalone installation for Windows PCs, the client communicates login, IP stack changes (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 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 which automatically logs the users in through the use of browser cookies whenever they access the intranet homepage.

Highlights



RADIUS Accounting Login

In a network which 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 Two-factor Authentication

FortiAuthenticator extends two-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 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 supports the widest range of tokens possible to suit your user requirements. With the physical time-based FortiToken 200, FortiToken Mobile (for iOS and Android), e-mail and SMS tokens, FortiAuthenticator has token options for all users and scenarios. Two-factor 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.

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 preshared 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

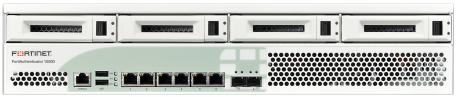
RADIUS and LDAP User Authentication	Local Authentication database with RADIUS and LDAP interfaces centralizes user management.
Wide Range of Strong Authentication Methods	Strong authentication provided by FortiAuthenticator via hardware tokens, e-mail, SMS, e-mail and digital certificates help to enhance password security and mitigate the risk of password disclosure, replay or brute forcing.
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.

Specifications

	FORTIAUTHENTICATOR 200E	FORTIAUTHENTICATOR 400E	FORTIAUTHENTICATOR 1000D
Hardware			
10/100/1000 Interfaces (Copper, RJ-45)	4	4	4
SFP Interfaces	0	0	2
Local Storage	1x 1 TB Hard Disk Drive	2x 1 TB Hard Disk Drive	2x 2 TB Hard Disk Drive
Power Supply	Single 250W Auto Ranging (100V–240V)	Dual (1+0) 300W Auto Ranging (100V–240V)	Dual (1+1) 300W Auto Ranging (100V–240V)
System Performance			
Total Users (Local + Remote)	500	2,000	10,000
FortiTokens	1,000	4,000	20,000
RADIUS Clients (NAS Devices)	166	666	3,333
User Groups	50	200	1,000
CA Certificates	10	10	50
User Certificates	2,500	10,000	50,000
Dimensions			
Height x Width x Length (inches)	1.75 x 17.05 x 13.86	1.73 x 17.24 x 16.38	3.50 x 17.24 x 14.49
Height x Width x Length (mm)	45 x 433 x 352	44 x 438 x 416	89 x 438 x 368
Weight	13.4 lbs (6.1 kg)	25.0 lbs (11.0 kg)	27.6 lbs (12.5 kg)
Environment			
Form Factor	Rack Mountable (1RU)	Rack Mountable (1RU)	Rack Mountable (2 RU)
Power Source	90–240V AC, 50–60 Hz	100–240V AC, 50–60 Hz	100–240V AC, 50–60 Hz
Maximum Current	4A / 110V, 2A / 220V	5A / 110V, 3A / 220V	5A /110V, 3A /220V
Power Consumption (Average)	60 W	102 W	115 W
Heat Dissipation	280 BTU/h	482 BTU/h	471 BTU/h
Operating Temperature	32–104°F (0–40°C)	32–104°F (0–40°C)	32–104°F (0–40°C)
Storage Temperature	-13–158°F (-25–70°C)	-13–167°F (-25–75°C)	-13–158°F (-25–70°C)
Humidity	5–95% non-condensing	5–95% non-condensing	5–95% 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)		
Management	CLI, Direct Console DB9 CLI, HTTPS	CLI, Direct Console DB9 CLI, HTTPS	CLI, Direct Console DB9 CLI, HTTPS
High Availability	Active-Passive HA and Config Sync HA	Active-Passive HA and Config Sync HA	Active-Passive HA and Config Sync HA
Compliance			
Safety	FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB	FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB	FCC Part 15 Class A, C-Tick, VCCI, CE, BSMI, KC, UL/cUL, CB, GOST

FortiAuthenticator 200E

FortiAuthenticator 400E



FortiAuthenticator 1000D

FortiAuthenticator 2000E

FortiAuthenticator 3000E

FortiAuthenticator
Virtual Appliance

Specifications

	FORTIAUTHENTICATOR 2000E	FORTIAUTHENTICATOR 3000E
Hardware		
10/100/1000 Interfaces (Copper, RJ-45)	4	4
SFP Interfaces	2	2
Local Storage	2x 2 TB SAS Drive	2x 2 TB SAS Drive
Power Supply	Dual (1+1) 740W Auto Ranging (100V–240V)	Dual (1+1) 1000W Auto Ranging (100V–240V)
System Performance		
Total Users (Local + Remote)	20,000	40,000
FortiTokens	40,000	80,000
RADIUS Clients (NAS Devices)	6,666	13,333
User Groups	2,000	4,000
CA Certificates	50	50
User Certificates	100,000	200,000
Dimensions		
Height x Width x Length (inches)	3.50 x 17.20 x 25.50	3.50 x 17.20 x 25.50
Height x Width x Length (mm)	89 x 437 x 647	89 x 437 x 647
Weight	32.0 lbs (14.5 kg)	40.0 lbs (18.6 kg)
Environment		
Form Factor	Rack Mountable (2 RU)	Rack Mountable (2 RU)
Power Source	100–240V AC, 50–60 Hz	100–240V AC, 50–60 Hz
Maximum Current	10A /110V, 4A /220V	10A /110V, 5A /220V
Power Consumption (Average)	189 W	347 W
Heat Dissipation	781 BTU/h	1325 BTU/h
Operating Temperature	41–95°F (5–35°C)	50–95°F (10–35°C)
Storage Temperature	-40–140°F (-40–60°C)	-40–158°F (-40–70°C)
Humidity	8–90% non-condensing	8–90% 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)	
Management	CLI, Direct Console DB9 CLI, HTTPS	CLI, Direct Console DB9 CLI, HTTPS
High Availability	Active-Passive HA and Config Sync HA	Active-Passive HA and Config Sync HA
Compliance		
Safety	FCC, ICES, CE, RCM, VCCI, BSMI, UL, CB	FCC Part 15 Class A, C-Tick, VCCI, CE, BSMI, KC, UL/cUL, CB, GOST

VIRTUAL APPLIANCES	FAC-VM BASE	FAC-VM-100-UG	FAC-VM-1000-UG	FAC-VM-10000-UG	FAC-VM-100000-UG
Capacity					
Local Users	100	+100	+1,000	+10,000	+100,000
Remote Users	100	+100	+1,000	+10,000	+100,000
FortiTokens	200	+200	+2,000	+20,000	+200,000
NAS Devices	33	+33	+333	+3,333	+33,333
User Groups	10	+10	+100	+1,000	+10,000
CA Certificates	5	+5	+50	+500	+500
User Certificates	100	+100	+1,000	+10,000	+100,000
Virtual Machine					
Hypervisors Supported	VMware ESXi / ESX 4 / 5 / 6, Microsoft Hyper-V Server 2010, 2012 R2, and 2016, KVM, Xen, Microsoft Azure, AWS				
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 200E	FAC-200E	4x GE RJ45 ports, 1x 1 TB HDD.
FortiAuthenticator 400E	FAC-400E	4x GE RJ45 ports, 2x 1 TB HDD.
FortiAuthenticator 1000D	FAC-1000D-E07S	4x GE RJ45 ports, 2x GE SFP, 2x 2 TB HDD.
FortiAuthenticator 2000E	FAC-2000E	4x GE RJ45 ports, 2x GE SFP, 2x 2 TB SAS Drive.
FortiAuthenticator 3000E	FAC-3000E	4x GE RJ45 ports, 2x GE SFP, 2x 2 TB SAS Drive.
FortiAuthenticator-VM License	FAC-VM-Base	Base FortiAuthenticator-VM with 100 user license. Unlimited vCPU.
	FAC-VM-100-UG	FortiAuthenticator-VM 100 user license upgrade.
	FAC-VM-1000-UG	FortiAuthenticator-VM 1,000 user license upgrade.
	FAC-VM-10000-UG	FortiAuthenticator-VM 10,000 user license upgrade.
	FAC-VM-100000-UG	FortiAuthenticator-VM 100,000 user license upgrade.
	FC1-10-0ACVM-248-02-12	1 Year 24x7 FortiCare Contract (1–500 users).
	FC2-10-0ACVM-248-02-12	1 Year 24x7 FortiCare Contract (1–1100 users).
	FC3-10-0ACVM-248-02-12	1 Year 24x7 FortiCare Contract (1–5100 users).
	FC4-10-0ACVM-248-02-12	1 Year 24x7 FortiCare Contract (1–10100 users).
	FC8-10-0ACVM-248-02-12	1 Year 24x7 FortiCare Contract (1–25100 users).
	FC5-10-0ACVM-248-02-12	1 Year 24x7 FortiCare Contract (1–50100 users).
	FC6-10-0ACVM-248-02-12	1 Year 24x7 FortiCare Contract (1–100100 users).
	FC9-10-0ACVM-248-02-12	1 Year 24x7 FortiCare Contract (1–500100 users).
	FC7-10-0ACVM-248-02-12	1 Year 24x7 FortiCare Contract (1–1M users).
Optional Accessories		
Power Supplies	SP-FAD700-PS	AC power supply for FAC-400E.
	SP-FXX1000D-PS	AC power supply for FAC-1000D.
	SP-FML2000E-PS	AC power supply for FAC-2000E.
	SP-FML3000E-PS	AC power supply for FAC-3000E.