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

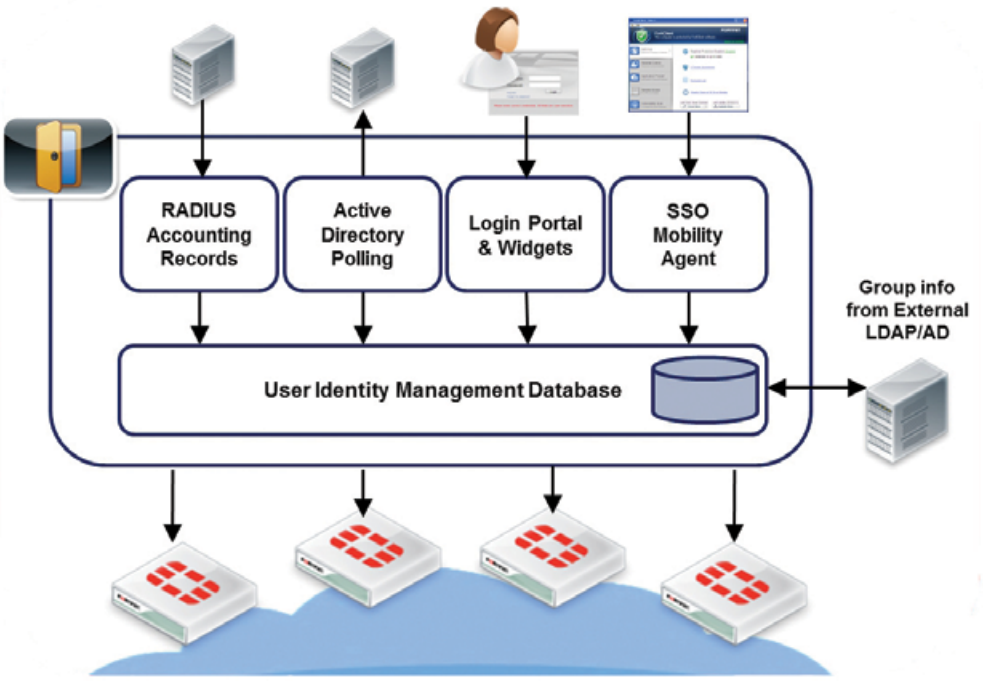
Key Features & Benefits

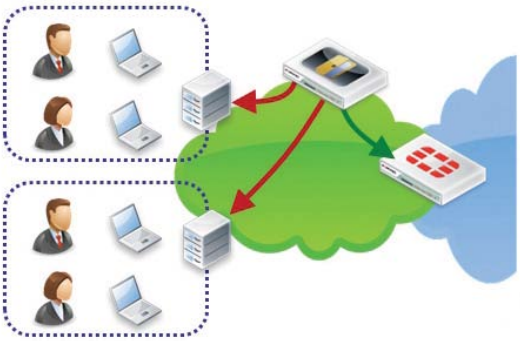
FSSO Transparent User Identification	Zero impact for enterprise users.
Integration with LDAP and AD for group membership	Utilizes existing systems for network authorization information, reducing deployment times and streamlining management processes. Integration with existing procedures for user management.
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.

HIGHLIGHTS

FortiAuthenticator Single Sign-On User Identification Methods

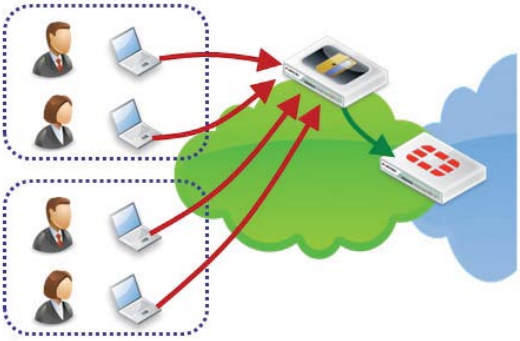
FortiAuthenticator can identify users through a varied range of methods and integrate with third party LDAP or Active Directory systems to apply group or role data to the user and communicate with FortiGate for use in Identity based policies. FortiAuthenticator is completely flexible and can utilize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





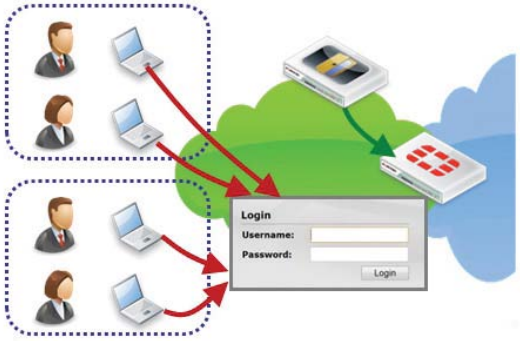
Active Directory Polling

User authentication into 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

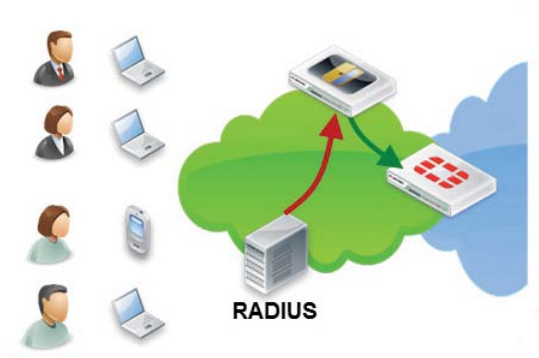
For complicated distributed domain architectures where polling of domain controllers is not feasible or desired, an alternative is the FortiAuthenticator SSO Client. Distributed as part of FortiClient or as a standalone installation for Windows PCs, the client communicates login, IP stack changes (Wired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



FortiAuthenticator Portal and Widgets

For systems which 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 a 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, 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 FortiToken300 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 & 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-200D	FORTIAUTHENTICATOR-400C	FORTIAUTHENTICATOR-1000C	FORTIAUTHENTICATOR-3000D
Hardware				
10/100/1000 Interfaces (Copper, RJ-45)	4	4	4	4
Local Storage	1x 1 TB Hard Disk Drive	1x 1 TB Hard Disk Drive	1x 1 TB Hard Disk Drive	2x 2 TB Hard Disk Drive
Power Supply	Single 480W Auto Ranging (100V–240V)	Single 480W Auto Ranging (100V–240V)	Single 480W Auto Ranging (100V–240V)	Dual 480W Auto Ranging (100V–240V)
System Performance				
Local Users	500	2,000	10,000	40,000
Remote Users	500	2,000	10,000	40,000
FortiTokens	500	2,000	10,000	40,000
Auth Clients (NAS Devices)	50	200	1,000	4,000
User Groups	25	50	200	2,000
CA Certificates	2	10	50	250
User Certificates	500	2,000	10,000	20,000
Dimensions				
Height x Width x Length (in)	1.8 x 17.1 x 13.9 in	1.7 x 17.1 x 14.3 in	1.7 x 17.1 x 24.7 in	3.5 x 17.5 x 27.5 in
Height x Width x Length (mm)	45 x 433 x 352 mm	44 x 435 x 364 mm	43 x 434 x 627 mm	89 x 445 x 698 mm
Weight	23 lbs (10.43 kg)	23 lbs (10.43 kg)	24.2 lbs (11.0 kg)	55.3 lbs (25.1 kg)
Environment				
Form Factor	Rack Mountable (1RU)	Rack Mountable (1RU)	Rack Mountable (1RU)	Rack Mountable (2RU)
Power Source	100–240V AC, 50–60 Hz	100–240V AC, 50–60 Hz	100–240V AC, 50–60 Hz	100–240V AC, 50–60 Hz
Current (Max)	1.00A / 110V, 0.50A / 220V	4.00A / 110V, 2.00A / 220V	3.50A / 110V, 1.75A / 220V	9.4A / 110V, 4.7A / 220V
Power Consumption (AVG)	60 W	100 W	189 W	317 W
Heat Dissipation	205 BTU/h	411 BTU/h	644 BTU/h	1082 BTU/h
Operating Temperature	32–104°F (0–40°C)	32–104°F (0–40°C)	50–95°F (10–35°C)	50–95°F (10–35°C)
Storage Temperature	-13–158°F (-25–70°C)	-13–158°F (-25–70°C)	-40–149°F (-40–65°C)	-40–149°F (-40–65°C)
Humidity	10 to 90% non-condensing	10 to 90% non-condensing	20 to 80% non-condensing	20 to 80% non-condensing
System				
Standards Supported	10/100/1000 Base-TX (GbE), 1000, 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			
Compliance				
Regulatory	IEC 60950-1, CSA 60950-1, EN 60950-1, ICES-003, EN 55024, CISPR 22, AS/NZS 3548, FCC, 47FR part 15 Class A, VCCI-A			
Safety	CSA, C/US, CE, UL			

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	+1000	+10000	+100000
Remote Users	100	+100	+1000	+10000	+100000
FortiTokens	200	+200	+2000	+20000	+200000
NAS Devices	10	+10	+100	+1000	+10000
User Groups	10	+10	+100	+1000	+10000
CA Certificates	5	+5	+50	+500	+500
User Certificates	100	+100	+1000	+10000	+100000
Virtual Machine					
Hypervisors Supported	VMware ESXi / ESX 3.5 / 4.0 / 4.1 / 5.0				
Virtual Machine Form Factor	Open Virtualization Format (OVF)				
Max Virtual CPUs Supported	Unlimited				
Virtual NICs Required (Min/Max)	1 / 4				
Virtual Machine Storage Required	60 GB / 2 TB				
Virtual Machine Memory Required (Min/Max)	512 MB / 4,096 MB				
High Availability Support	Yes				

FortiAuthenticator-200D

FortiAuthenticator-400C

FortiAuthenticator-1000C

FortiAuthenticator-3000D

FortiAuthenticator Virtual Appliance

ORDERING INFORMATION

SKU	Description
FAC-200D	FortiAuthenticator-200D, 4 10/100/1000 ports, 1x 1 TB HDD
FAC-400C	FortiAuthenticator-400C, 4 10/100/1000 ports, 1x 1 TB HDD
FAC-1000C-E07S	FortiAuthenticator-1000C, 4 10/100/1000 ports, 1x 1 TB HDD
FAC-3000D	FortiAuthenticator-3000D, 4 10/100/1000 ports, 2x 2 TB HDD
FAC-VM-Base	Base FortiAuthenticator-VM with 100 user license. Unlimited vCPU
FAC-VM-100-UG	FortiAuthenticator-VM with 100 user license upgrade
FAC-VM-1000-UG	FortiAuthenticator-VM with 1000 user license upgrade
FAC-VM-10000-UG	FortiAuthenticator-VM with 10,000 user license upgrade
FAC-VM-100000-UG	FortiAuthenticator-VM with 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)
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)

GLOBAL HEADQUARTERS
Fortinet Inc.
1090 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
Fax: +1.408.235.7737

EMEA SALES OFFICE
120 rue Albert Caquot
06560, Sophia Antipolis,
France
Tel: +33.4.8987.0510
Fax: +33.4.8987.0501

APAC SALES OFFICE
300 Beach Road #20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730
Fax: +65.6223.6784

LATIN AMERICA SALES OFFICE
Prol. Paseo de la Reforma 115 Int. 702
Col. Lomas de Santa Fe,
C.P. 01219
Del. Alvaro Obregón
México D.F.
Tel: 011-52-(55) 5524-8480