FERTINET®

DATASHEET

# FortiAuthenticator™

## User Identity Management Appliance

FortiAuthenticator user identity management appliances strengthen enterprise security by simplifying and centralizing the management and storage of user identity information used for authentication. Designed as a central repository for user validation information, FortiAuthenticator enables multiple authentication technologies for controlling user access including two-factor authentication, identity verification and network access control.

FortiAuthenticator is available in a range of hardware appliances and in a VM format with stackable user licensing delivering the greatest flexibility possible.

### Stronger Security 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.

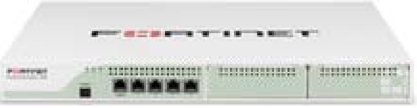
FortiAuthenticator supports the widest range of tokens possible to suit your user requirements. With the physical time based Fortitoken-200, FortiToken Mobile (for iOS and Android), e-mail and SMS tokens, FortiAuthenticator has a token options for all users. Two-factor authentication can be used to control access to applications such as FortiGate management, SSL and IPSEC VPN, Wireless Captive Portal login, third party networking equipment and web sites.

| Feature | Benefit |
|---|---|
| RADIUS and LDAP User Authentication | Local Authentication database with RADIUS and LDAP interfaces centralises 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 insecure passwords, something the user knows, with the need for a second factor based on something the user has i.e. a token or certificate. |
| Simplified User Management | FortiAuthenticator support user self registration and self password reset to minimise the impact on the user support requirements. |
| Integration with External LDAP Directories | Integration with existing directory simplifies deployment, speeds up installation times and reutilizes existing development. |
| Certificate Management | Simplified management of digital certificates allows for mutual authentication. |
| 802.1X Authentication | Deliver enterprise port access control to validate users connection to the LAN and Wireless LAN to prevent unauthorised access to the network. |
| On-board Fortinet Single Sign-On | Removes the need for installation of the Fortinet Single Sign-On software on a dedicated server.  Allows integration with RADIUS Accounting for carrier logins to trigger FSSO logins. |

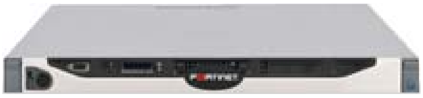
### FortiAuthenticator Features

- Strengthens enterprise security by simplifying and centralizing the management of user identity information
- Extends the scope of and enhances existing FortiToken deployments
- Increases confidence in user identity with Two-factor Authentication
- Supports a wide range of third-party solutions via RADIUS and LDAP integration
- Enables FortiGate identity-based policies through integration with Active Directory
- Provides users with transparent network authentication via Fortinet Single Sign-On
- Certificate Authority enables the signing, issuing and revoking of x.509 user certificates as a two-factor alternative

FortiAuthenticator-200D



FortiAuthenticator-400C



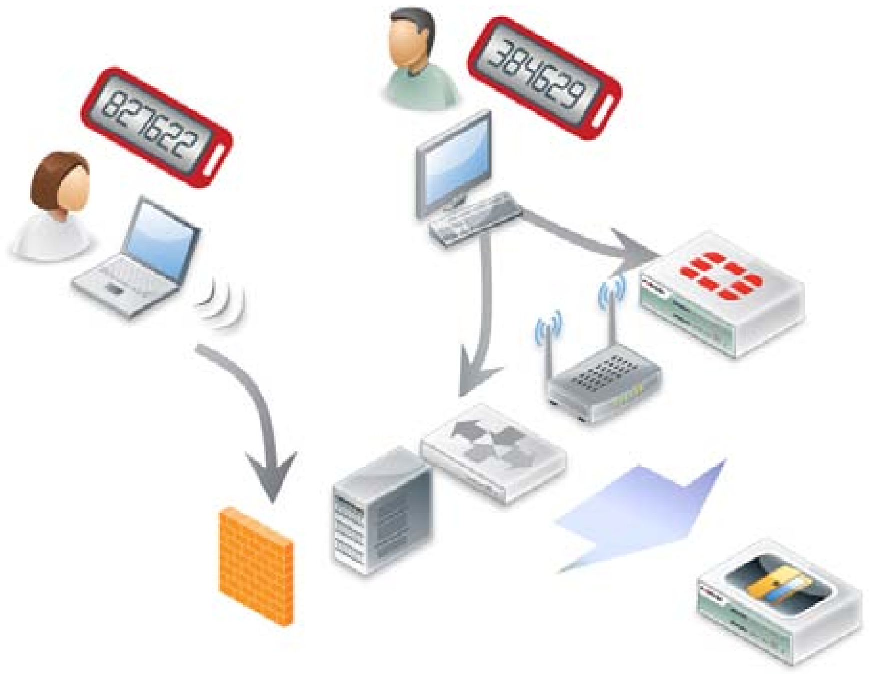
FortiAuthenticator-1000C

FortiAuthenticator-3000B

FortiAuthenticator Virtual Appliance

## Simpler Management and User Experience

By providing all services and storage of user identity information on a single device, the FortiAuthenticator appliance significantly lowers the cost of delivering secure user authentication. The FortiAuthenticator system can be deployed in minutes rather than hours and has been designed to simplify all steps of the user authentication life cycle; from integration with existing authentication databases to zero impact token initialization. Users can recover their own credentials through a self-service portal by answering pre-agreed questions and providing a token PIN, further reducing administrative burden. The FortiAuthenticator also allows users to self register their details such as e-mail address, phone number, mobile number and security questions for password recovery.  This enables FortiAuthenticator be used as a self-registration portal for wireless and guest networks or by a receptionist in a visitor environment.



## IEEE802.1X Port Access Control

The FortiAuthenticator supports, EAP-MD5, EAP-TTLS, EAP-TLS, EAP-GTC and PEAP protocols for authentication via 802.1X for Port Based Network Access Control.  This can be used by third party switches and wireless to authenticates devices (and their users) before allowing them onto the corporate network. FortiAuthenticator also supports fallback to MAC based authentication for non-interactive devices such as printers.

## FortiAuthenticator Certificate Authority

In addition to providing secure authentication via RADIUS enhanced with time based tokens, FortiAuthenticator supports certificate based two-factor authentication. Acting as a root or intermediary CA, FortiAuthenticator eases the typically painful process of signing, issuing and revoking client certificates for use in FortiGate VPN deployments with support for SCEP. When combined with FortiToken-300 for secure user certificate storage, FortiAuthenticator is the ideal strong authentication server solution, for all user and authentication types.

## Fortinet Single Sign On (FSSO)

Fortinet Single Sign On (FSSO) improves the user experience by reducing the number of authentications.  Transparent authentication can be provided in several ways:

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

Once detected, details of the logged in user are communicated to the FortiGate, together with group membership details to be used in dynamic, Identity Based Policies.

| Technical Specifications | FAC-VM Base | FAC-VM-100-UG | FAC-VM-1000-UG | FAC-VM-10000-UG | FAC-VM-100000-UG |
|---|---|---|---|---|---|
| **System Performance** | | | | | |
| 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 | 10 | +10 | +100 | +1,000 | +10,000 |
| 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 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 (Min/Max) | 60 GB / 2 TB | | | | |
| Virtual Machine Memory Required (Min/Max) | 512 MB / 4,096 MB | | | | |
| High Availability | Yes | | | | |

| Technical Specifications | FortiAuthenticator-200D | FortiAuthenticator-400C | FortiAuthenticator-1000C | FortiAuthenticator-3000B |
|---|---|---|---|---|
| **Hardware** | | | | |
| 10/100/1000 Interfaces (Copper, RJ-45) | 4 | 4 | 4 | 4 |
| Local Storage | 1 x 1 TB Hard Disk Drive | 1 x 1 TB Hard Disk Drive | 1 x 1 TB Hard Disk Drive | 1 x 1 TB Hard Disk Drive |
| Power Supply | Single 480W Auto Ranging (100V~240V) | | | Dual 480W Auto Ranging (100V~240V) |
| **System Performance** | | | | |
| Local Users | 500 | 2,000 | 10,000 | 20,000 |
| Remote Users | 500 | 2,000 | 10,000 | 20,000 |
| FortiTokens | 500 | 2,000 | 10,000 | 20,000 |
| Auth Clients (NAS Devices) | 50 | 200 | 1,000 | 2,000 |
| User Groups | 25 | 50 | 200 | 2,000 |
| CA Certificates | 2 | 10 | 50 | 250 |
| User Certificates | 500 | 2,000 | 10,000 | 200,000 |
| **Dimensions** | | | | |
| Height | 1.80 in (45 mm) | 1.70 in (44 mm) | 1.69 in (43 mm) | 3.50 in (89 mm) |
| Width | 17.1 in (433 mm) | 17.10 in (435 mm) | 17.09 in (434 mm) | 17.5 in (445 mm) |
| Length | 13.9 in (352 mm) | 14.3 in (364 mm) | 24.69 in (627 mm) | 27.5 in (698 mm) |
| Weight | 23 lb (10.43 kg) | 23 lb (10.43 kg) | 24.2 lb (11.0 kg) | 55.3 lb (25.1 kg) |
| **Environment** | | | | |
| Form Factor | Rack Mountable (1RU) | | | Rack Mountable (2RU) |
| Power Source | 100 - 240 VAC, 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) | 60W | 100 W | 189 W | 317 W |
| Heat Dissipation | 205 BTU/h | 411 BTU/h | 644 BTU/h | 1082 BTU/h |
| Operating Temperature | 32 – 104 deg F (0 – 40 deg C) | | 50 – 95 deg F (10 – 35 deg C) | |
| Storage Temperature | -13 – 158 deg F (-25 – 70 deg C) | | -40 – 149 deg F (-40 – 65 deg C) | |
| Humidity | Humidity 10 to 90% non-condensing | | Humidity 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 Compliance | 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 Compliance | CSA, C/US, CE, UL | | | |

## Ordering Information

| Product Description | SKU |
|---|---|
| FortiAuthenticator-200D 4 10/100/1000 ports, 2 USB ports, 1 TB HDD storage | FAC-200D |
| FortiAuthenticator-400C, 4 10/100/1000 ports, 2 USB ports, 1 TB HDD storage | FAC-400C |
| FortiAuthenticator-1000C, 4 10/100/1000 ports, 2 USB ports, 1 TB HDD storage | FAC-1000C-E07S |
| FortiAuthenticator-3000B, 4 10/100/1000 ports, 1 x 1TB HDD | FAC-3000B-EMS01 |
| Base FortiAuthenticator-VM with 100 user license. Unlimited vCPU | FAC-VM-Base |
| FortiAuthenticator-VM with 100 user license upgrade. | FAC-VM-100-UG |
| FortiAuthenticator-VM with 1000 user license upgrade | FAC-VM-1000-UG |
| FortiAuthenticator-VM with 10,000 user license upgrade | FAC-VM-10000-UG |
| FortiAuthenticator-VM with 100,000 user license upgrade | FAC-VM-100000-UG |
| 1 Year 24x7 FortiCare Contract (1 - 500 USERS) | FC1-10-0ACVM-248-02-12 |
| 1 Year 24x7 FortiCare Contract (1 - 1,100 USERS) | FC2-10-0ACVM-248-02-12 |
| 1 Year 24x7 FortiCare Contract (1 - 5,100 USERS) | FC3-10-0ACVM-248-02-12 |
| 1 Year 24x7 FortiCare Contract (1 - 10,100 USERS) | FC4-10-0ACVM-248-02-12 |
| 1 Year 24x7 FortiCare Contract (1 - 50,100 USERS) | FC5-10-0ACVM-248-02-12 |
| 1 Year 24x7 FortiCare Contract (1 - 100,100 USERS) | FC6-10-0ACVM-248-02-12 |

**GLOBAL HEADQUARTERS**

Fortinet Incorporated
1090 Kifer Road, Sunnyvale, CA 94086 USA
Tel +1.408.235.7700
Fax +1.408.235.7737
www.fortinet.com/sales

**EMEA SALES OFFICE – FRANCE**

Fortinet Incorporated
120 rue Albert Caquot
06560, Sophia Antipolis, France
Tel +33.4.8987.0510
Fax +33.4.8987.0501

**APAC SALES OFFICE – SINGAPORE**

Fortinet Incorporated
300 Beach Road 20-01
The Concourse, Singapore 199555
Tel +65-6513-3734
Fax +65-6295-0015

Performance metrics contained herein were attained in internal lab tests under ideal conditions, and performance 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 General Counsel, with a purchaser that expressly warrants that the identified product will perform according to the performance metrics herein. 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 guarantees. 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.