Getting Started

FortiAuthenticator 8.0.0

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO LIBRARY
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

April 29, 2026
FortiAuthenticator 8.0.0 Getting Started
23-800-1199086-20260429

TABLE OF CONTENTS

Change Log

Date	Change Description
2025-10-02	Initial release.
2025-10-07	Updated Licensing on page 7.
2026-04-29	Updated Getting started on page 5.

Getting started

The FortiAuthenticator device is an identity and access management solution that provides user identity services to Fortinet products and third-party devices.

It offers a range of features designed to secure your network infrastructure including authentication, MFA, IEEE 802.1X support, user authentication, and certificate management.

FortiAuthenticator is a critical system and should be isolated on a network interface separate from other hosts to enhance server-related firewall protection and prevent unauthorized access.

FortiAuthenticator can also replace the Fortinet Single Sign-On (FSSO) Agent on a Windows AD network.

Planning

Before deploying your standalone FortiAuthenticator, review the following key areas:

- Requirements on page 5
- Licensing on page 7
- Learning more on page 7

Requirements

Ensure the following prerequisites are met for a successful FortiAuthenticator setup:

Requirement	Description
Supported Environments	FortiAuthenticator 8.0 supports virtualization environments such as: VMware ESXi / ESX 6/7/8 Microsoft Hyper-V 2010, Hyper-V 2016, Hyper-V 2019, and Hyper-V 2022 Linux Kernel-based Virtual Machine (KVM) on Virtual Machine Manager and QEMU 2.5.0 Xen Virtual Machine (for Xen HVM) Nutanix AWS (Amazon Web Services) Microsoft Azure Oracle OCI

Requirement	Description
	Alibaba Cloud Saudi Cloud Computing Company (SCCC) and `alibabacloud.sa` domain (a standalone cloud backed by AliCloud) Proxmox
Browser Support	Microsoft Edge Mozilla Firefox Google Chrome For supported versions, see Web browser support in the latest *FortiAuthenticator Release Notes*.
VM Resources	Minimum 16 GB RAM required.
Administrative Access	You must have administrative access to both the GUI and/or CLI.
Initial System Configuration	Essential settings like system time, DNS settings, administrator password, and network interfaces must be configured. Network Time Protocol (NTP) is crucial for maintaining accurate and stable time, especially when using Time-based One-time Password (TOTP) for two-factor authentication
Third-Party Components	Any third-party software or servers intended for use with FortiAuthenticator should be configured according to their respective documentation.

Open Ports	Ensure that specific ports are open in security policies between the FortiAuthenticator and authentication clients, in addition to management protocols (`HTTP`, `HTTPS`, `SSH`, and `ping`):
	`UDP/161 (SNMP)`
	`UDP/1812 (RADIUS Auth)`
	`UDP/1813 (RADIUS Accounting)`
	`UDP/8002 (DC/TS Agent FSSO)`
	`TCP/389 (LDAP)`
	`TCP/636 (LDAPS)`
	`TCP/8000 (FortiGate FSSO)`
	`TCP/8001 (FortiClient Single Sign-On Mobility Agent FSSO)`
	`TCP/8002 (DC/TS Agent FSSO)`
	`TCP/8003 (Hierarchical FSSO)`
	`TCP/2560 (OCSP)`

Licensing

FortiAuthenticator-VM operates in evaluation mode until a license is applied, which limits the number of configurable users.

- A stackable license can be applied to increase user count and other associated metrics.
- For the license to be valid, one of the FortiAuthenticator interfaces must be set to the IP address specified in the license.
- Licenses for FortiAuthenticator-VM apply to:
  - The total number of local and remote user accounts configured.
  - The number of concurrent FSSO sessions.
  - Maximum limits on all other configuration objects are derived as a ratio to the maximum user count.
- SSO Mobility Agent (SSOMA) client limits are determined by the lowest of either "Maximum FortiClient SSO" or "Maximum users" from the onboard license.
- SSOMA, FTM (FortiToken Mobile), and SMS licenses are purchased separately and do not scale with the FortiAuthenticator user limit.

For High Availability (HA) clusters:

- Primary HA clusters require each FortiAuthenticator unit to have its own license of the same size (users and SSOMA clients).
- An HA load-balancer needs a user license size sufficient to replicate the configuration from the primary, though the SSOMA license size can differ based on which node SSOMA clients connect to.

FortiAuthenticator-VM accepts subscription based license.

See Subscription VM license in the latest *FortiAuthenticator Administration Guide*.

Learning more

- FortiAuthenticator documentation
- Fortinet Training and Certification
- FortiCloud
- 4-D resources

Activating

Activate FortiAuthenticator by completing the following

To activate your FortiAuthenticator device, you must register it with Fortinet and apply the license.

Creating a FortiCloud account

To create FortiCloud account:

1. Go to FortiCloud.
2. Click *Create Account* and follow instructions to create an account.

Registering your FortiAuthenticator license

After purchasing the FortiAuthenticator license, you will receive a registration code via email.

Before you begin configuring and customizing features, register your Fortinet product at the Fortinet Support website.

Product registration is necessary to access various Fortinet customer services, including firmware updates, technical support, FortiGuard Antivirus, and other FortiGuard services.

To register the FortiAuthenticator license:

1. While signed in to your FortiCloud account, go to *Services* > *Asset Management*, and click *Register Now*.
2. You should have received an email with your *Service Entitlement Summary* document.
   The document includes the *Contract Registration Code*.
3. In the *Registration Code* field, enter *Contract Registration Code* from the *Service Entitlement Summary* document.
4. Continue the remaining instructions to register FortiAuthenticator.
   For more information, see Registering assets in the latest *Asset Management Administration Guide*.
5. Upload the license key to your FortiAuthenticator-VM via the GUI by navigating to *System* > *Administration* > *Licensing*.
6. Select *Upload a file*, locate your license file, and click *Upload*.

Provisioning

For FortiAuthenticator installation instructions, see the latest FortiAuthenticator Private and Public Cloud docs.

Fortinet recommends not using the suspend feature of VMware; instead, shut down the virtual FortiAuthenticator system using the GUI or CLI, then shut down the virtual machine.

Provision your FortiAuthenticator

1. **Initial CLI Login and Configuration**:
   a. Access the CLI via console or SSH.
   b. At the FortiAuthenticator login prompt, enter admin and press Enter. By default, there is no password.
   c. You will be prompted to set and confirm a new administrator password.
   d. Configure `port1` IP address and default gateway:
   e. Substitute `<ip-address>/<netmask>` and `<ip-gateway>` with your desired values.
   f. You can now connect to the GUI at the IP address you set for `port1`.

   See *Initial setup* in the latest FortiAuthenticator Administration Guide.
2. **Essential GUI Configurations**:
   a. Go to *System > Network > DNS* and enter your internal network *Primary DNS server* and *Secondary DNS server* IP addresses.

   Note: This is essential for successful FSSO operation.

   See *DNS* in the latest FortiAuthenticator Administration Guide.
   b. Go to *System > Network > Static Routing* and create a default route (*Destination IP/Mask* `0.0.0.0/0`) to your network gateway on the interface that connects to the gateway.

   See *Static routing* in the latest FortiAuthenticator Administration Guide.
   c. Go to *System > Dashboard > Status*, find the *System Information* widget, select the pen icon in the *System Time* field, and select your *Time zone*.

   Either enable NTP or manually enter the date and time.

   Note: NTP is strongly recommended if you plan to use FortiToken devices for accurate time-based authentication.

   See *System information widget* in the latest FortiAuthenticator Administration Guide.
   d. If FortiAuthenticator is connected to additional subnets, configure additional interfaces as required in *System > Network > Interfaces*.

   See *Interfaces* in the latest FortiAuthenticator Administration Guide.
   e. Go to *Authentication > User Management* to configure an administrator user.
   f. Go to *System > Administration > Admin Profiles* to configure admin profiles.

   Admin profiles define who can access the device and with what privileges.

   See *Admin Profiles* in the latest FortiAuthenticator Administration Guide.
   g. Go to *Authentication > Remote Auth. Servers* to configure external RADIUS, LDAP, TACACS+, OAuth, or SAML servers as identity sources.

h. Go to the following in *Authentication* to configure authentication rules and flows:
   i. *RADIUS service > Policies*.
   ii. *TACACS+ Service > Policies*.
   iii. *OAuth Service > Policies*.
   iv. *SAML IdP > Service Providers*.
   v. *Portal > Policies* (captive and self-service policies).
   See *Authentication* in the latest FortiAuthenticator Administration Guide.
i. Review and adjust system access settings in *System > Administration > System Access*.
   See *System access* in the latest FortiAuthenticator Administration Guide.

What's next

After completing the initial setup and provisioning, you can monitor the FortiAuthenticator status and confirm its version.

The *Dashboard* displays widgets that provide performance and status information about your FortiAuthenticator.

See *Dashboard* in the latest FortiAuthenticator Administration Guide.

Confirm your FortiAuthenticator release version

To confirm the FortiAuthenticator release version:

1. Log in to the FortiAuthenticator GUI.
2. Go to *System > Dashboard > Status*.
3. In the *System Information* widget, the *Firmware Version* field shows the version and build number of the installed FortiAuthenticator.
   Always check the *FortiAuthenticator Release Notes* on the Fortinet Docs Library for details on new features, resolved, and known issues.

www.fortinet.com