Administration Guide

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

February 2, 2026
FortiAuthenticator 8.0.0 Administration Guide
23-800-1084116-20260202

TABLE OF CONTENTS

Change Log

Date	Change Description
2025-10-02	Initial release.
2025-10-20	Updated FortiGuard on page 64.
2025-10-27	Updated FortiAuthenticator 8.0.0 on page 10 and General on page 200.
2025-11-06	Updated Remote user sync rules- SCIM on page 120.
2025-11-21	Updated Windows AD connection troubleshooting on page 337.
2025-11-25	Updated Windows AD connection troubleshooting on page 337.
2025-11-26	Updated Windows event log sources on page 280.
2025-11-27	Updated Creating a portal rule on page 170.
2025-12-22	Updated Service providers on page 137.
2026-01-06	Added video to What's new in FortiAuthenticator on page 10.
2026-01-13	Updated Licensing on page 61.
2026-01-22	Updated FortiClient SSO Mobility Agent on page 275.
2026-02-02	Updated • Guest Portals (beta) on page 161 • FortiAuthenticator 8.0.0 on page 10 • Subscription VM license on page 63

What's new in FortiAuthenticator

This section provides a summary of the new features and enhancements in FortiAuthenticator:

Always review the *FortiAuthenticator Release Notes* on the Fortinet Docs Library prior to upgrading your device.

FortiAuthenticator 8.0.0

The following list contains new and expanded features added in FortiAuthenticator 8.0.0.

Allow multiple user certificate and key export

The **Certificate Expiry** tab in **Certificate Management > Policies** has been renamed to **General**.

A new **Delete user certificate's private key once downloaded** option is available in the **General** tab that controls if a user certificate private key is deleted after being downloaded from the admin UI.

See General on page 288.

SCEP with Microsoft InTune and EAP-TLS with Entra ID users/groups

FortiAuthenticator offers the following new settings to support integration with MS InTune client certificates distribution and EAP-TLS RADIUS authentication with Entra ID users/groups:

- A new **InTune** option in **Challenge Password > Password generation** when creating/editing a certificate enrollment request in **Certificate Management > SCEP > Enrollment Requests**.

  See Enrollment requests on page 309.
- The **Azure AD tenant ID** field is no more dependent on the **Include for SSO** option when creating/editing a remote OAuth server in **Authentication > Remote Auth. Servers > OAuth**.

  See OAUTH on page 185.
- A new **Certificate Bindings** pane available that allows you to configure certificate bindings when creating/editing a remote SAML user in **Authentication > User Management > Remote Users**.

  See Remote users on page 107.
- A new **RADIUS Attributes** pane available that allows you to configure RADIUS attributes when creating/editing a SAML user group in **Authentication > User Management > User Groups**.

  See User groups on page 126.

- The **Realms** table can now include SAML realms and remote SAML group filters when configuring a RADIUS policy in **Authentication > RADIUS Service > Policies**.

  See Policies on page 192.

FIDO authentication for IdP initiated SAML

The general SAML IdP settings page in **Authentication > SAML IdP > General** now offers the ability to specify the required authentication method for IdP initiated logins in the new **IdP Initiated Login** pane.

See General on page 227.

REST API enhancements for local users management

A new `users` field in the `/localusers/` endpoint that displays the list of users.

The following new allowed methods available for the `/localusers/` endpoint:

Method	Endpoint	Description
`POST`	`/api/v1/localusers/`	Create multiple new local users
`DELETE`	`/api/v1/localusers/`	Delete multiple local users

The following new allowed filtering available for the `/localusers/` endpoint:

- `custom1`
- `custom2`
- `custom3`

The following new allowed filtering available for the `/csv/localusers/` endpoint:

- `username`
- `abridged`
- `custom1`
- `custom2`
- `custom3`

See the latest *FortiAuthenticator REST API Guide*.

REST API enhancements: Track end-user operations

A new `X-Request-ID` header for request tracking and correlation across distributed systems to trace logs and debug issues.

HTTP Header	Type	Required	Other Restrictions
X-Request-ID	string	No	ASCII alphanumeric, dash (-), and underscore (_) only. Maximum length = 64 characters.

The X-Request-ID header is supported for all the read/write operations (GET, POST, PUT, PATCH, DELETE) for the following endpoints:

- /localusers/
- /ldapusers/
- /iamaccounts/
- /iamusers/
- /fortitokens/
- /usergroups/
- /localgroup-memberships/

Usage Example

cURL Example

```
curl -k -X GET \
 https://[FAC_IP]/api/v1/localusers/ \
 -H 'Content-Type: application/json' \
 -H 'X-Request-ID: request_12345' \
 -u "admin:[api_key]"
```

Sample Response

```
{
  "meta": {
  "request_id": "request_12345"
},
"objects": [
  {
    "username": "john.doe",
    "email": "john.doe@example.com"
  }
 ]
}
```

See the latest *FortiAuthenticator REST API Guide*.

In the FortiAuthenticator 8.0.0 GUI, a new *Request ID* column in *Logging > Log Access > Logs*.

It contains the value of the X-Request-ID header in the logs associated with the REST API operations for the supported endpoints.

See Log access on page 319.

Support for subscription VM license

FortiAuthenticator-VM now accepts subscription based licenses.

The following new CLI commands have been introduced:

- `get system license-info`: Displays the license information
- `diagnose system updated status`: Displays license information fetched from FDN
- `diagnose system updated info`: Displays the updated runtime information
- `diagnose debug application updated <level>`: Set debug level for updated

Once the license expires, all the authentication stops.
The administrator can still access the GUI for configuration and troubleshooting.

The subscription license requires FortiAuthenticator version 8.0.0 or above.

See Subscription VM license on page 63.

Override option in A/P HA

A new **Priority override** option when editing high availability settings in **System > Administration > High Availability**.

The **Priority override** option allows you to select from the following:

- **Favor healthy high priority node**: If the low priority node is active, failover to the high priority node whenever it becomes available.
- **Minimize HA failovers**: If the low priority node is active, do not failover to the high priority node until the low priority node becomes unavailable.

See High availability on page 51.

SmartConnect/EAP-TLS: Enforce client certificate install on unique endpoint

In FortiAuthenticator 8.0.0, when configuring a Smart Connect profile for EAP-TLS connections with the **Authentication** as **WPA2 Enterprise** in **Authentication > Portals > Smart Connect Profiles**, a new **Client certificate CN** dropdown indicates which user account attribute to use as the CN value in the client certificate (previously, hardcoded to `username`).

The **Client certificate CN** dropdown also offers a new **MAC Device** option.

Similarly, when configuring a Smart Connect profile with the **Connect type** as **Certificate**, the **Client certificate CN** dropdown is available.

See Smart Connect profiles on page 158.

When configuring an EAP-TLS RADIUS policy in **Authentication > RADIUS Service > Policies**, a new **Verify MAC address in CN of client certificate** (default = disabled) setting under **Device authorization** in the **Authentication factors** tab is available.

When enabled, the endpoint MAC address sent by the RADIUS client must match the `CN` in the subject field of the client certificate.

See Policies on page 192.

When configuring a portal in **Authentication > Portals > Portals**, **Device Tracking and Management** has been replaced with a new **Devices** option that includes the following:

- **Tracking and Management**
- **Tracking-only**
- **Management-only**

When device tracking is used, the end-user with successful log in to the captive portal with a new MAC device is asked to register the device (when under the maximum number of allowed MAC devices).

When device management is used and the end-user successfully logs in to the captive portal with a new MAC device in excess of the maximum number of devices per user, the end-user is asked if they will replace an existing device.

When device management is disabled and the end-user successfully logs in to the captive portal with a new MAC device, the access is denied since an existing device cannot be replaced.

See Portals on page 144.

In the post login portal:

- The **Devices** menu is only visible when device management is enabled.
- If `"Client certificate CN"=="MAC Device"`, the end-user is given a dropdown to select which device to use.
- If no MAC devices have been registered to the logged-in user account, e.g., device tracking is disabled, the Smart Connect menu shows an error message.

SAML IdP: Custom multi-value SAML attributes

FortiAuthenticator 8.0.0 now supports custom SAML assertion attributes in the SAML response sent to SPs.

A new **SAML Assertion Attributes** pane available when configuring a user group in **Authentication > User Management > User Groups**.

See User groups on page 126.

The following events are now logged:

- System logs: Add/edit/delete custom SAML assertion attributes in user groups.
- GUI debug logs: Information about the user groups used to build the list of custom SAML assertion attributes for the SAML response.

See Logging on page 319.

SAML IdP: Per SAML SP authorization

The remote LDAP group filters now offer a new **Subtype** setting (previously labeled **User retrieval**) in **Authentication > User Management > User Groups**.

The **Subtype** setting offers the following three options:

- **LDAP directory group**: Maps to a group object at the specified Distinguished Name in the remote LDAP directory.
- **List of users**
- **LDAP filter (advanced)** (default): Queries the remote LDAP server with a custom filter that returns the list of member users.

Selecting **Set Group Filter** imports the **Distinguished name** of the selected LDAP group only.

See User groups on page 126.

A new tooltip is available when the **User attribute** is **Group** while adding an **Assertion attribute**.

See Service providers on page 230.

A new SAML IdP replacement message for SP authorization failure (**SAML IdP Unauthorized SP Page**).

See Replacement messages on page 237.

The **Filter By Group** column has been renamed to **Global Authorization** in **Authentication > SAML IdP > User Sources**.

See User sources on page 236.

The IdP initiated portal now hides any SP for which the logged in user is unauthorized based on the SP group filters.

The following events are now logged:

- Add/edit/delete SP group filter.
- SP access is denied due to failed SP group filter authorization.

See Logging on page 319.

FortiAuthenticator- FortiGuest integration

Starting FortiAuthenticator 8.0.0, FortiGuest features are available from within FortiAuthenticator.

A new **Guest Portals (beta)** menu available in **Authentication** that offers FortiGuest configuration in FortiAuthenticator.

The following three tabs are available in **Guest Portals (beta)**:

- **Portals**: Allow administrators to create their portal pages and host them on FortiAuthenticator.
- **Portals Rules**: Create a set of rules to allow user access to different portals that have been created.
- **Guest Themes**: Create guest portal themes as per your business requirement.

Note: This is a beta feature.

Limitations:

- Only supports login for local users
- Configuration backup/restore does not preserve all the customizations
- HA A-P and HA A-A are not supported

- Only administrators with full permissions can access the configuration

See Guest Portals (beta) on page 161.

Legacy self-service portal retired

Starting FortiAuthenticator 8.0.0, the **Legacy Self-service Portal** available in **Authentication** has been removed.

The administrator must now log in with their username only, i.e., `username + realm` is no longer accepted.

Also, the previously available **Legacy Self-Service Portal Settings** pane in **System > Administration > System Access** has been removed.

See System access on page 48.

New CLI command for EAP

Starting FortiAuthenticator 8.0.0, a new `diagnose authentication radius-eap-ecdh-curve` CLI command has been added.

Use the CLI command to override the default `ECDH_CURVE` for EAP.

default = `secp521r1:secp384r1:prime256v1`

See Extensible Authentication Protocol on page 242.

New CRL check mode for remote LDAP servers

Starting FortiAuthenticator 8.0.0, a new **CRL Check Mode** setting is available in the **Secure Connection** pane when configuring a remote LDAP server in **Authentication > Remote Auth. Servers > LDAP**.

See LDAP on page 176.

New Exclude Windows AD computer accounts from SSO option in FSSO

Starting FortiAuthenticator 8.0.0, a new **Exclude Windows AD computer accounts from SSO** option is available in **Fortinet SSO > Settings > Methods**.

When **Exclude Windows AD computer accounts from SSO** is enabled, FortiAuthenticator does an AD lookup to determine whether an account ending with `$` is a computer or a user, and excludes it from FSSO if it is a computer.

See Methods on page 250.

New debug log categories for Web Server

In FortiAuthenticator 8.0.0, the following new debug categories are now available for **Web Server**:

- **SAML**
- **Generic API**

See Debug logs on page 328.

New OTP-Only Push notification setting in User Account Policies

Starting FortiAuthenticator 8.0.0, a new **OTP-Only Push notification mode** setting is available when configuring user account policies in **Authentication > User Account Policies > General**.

See General on page 82.

RADSec support enhancements

FortiAuthenticator RADIUS server can now process RADIUS accounting requests being sent over RADSec from RADIUS clients.

Furthermore, the RADIUS server now verifies that RADSec clients provide a certificate issued by one of the configured **Local CAs** or **Trusted CAs** under **Certificate Management > Certificate Authorities** during their TLS connection handshake.

See RADSEC support on page 200.

Introduction

The FortiAuthenticator device is an identity and access management solution. Identity and access management solutions are an important part of an enterprise network, providing access to protected network assets and tracking user activities to comply with security policies.

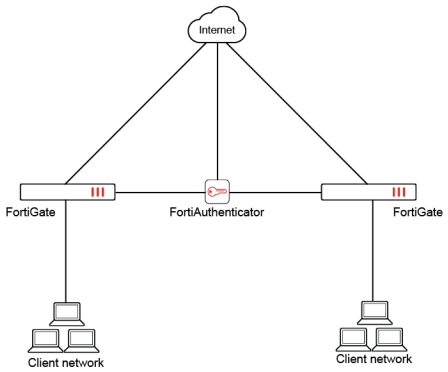
FortiAuthenticator provides user identity services to the Fortinet product range, as well as third-party devices.

FortiAuthenticator delivers multiple features including:

- **Authentication**: FortiAuthenticator includes Remote Authentication Dial In User Service (RADIUS), Terminal Access Controller Access-Control System Plus (TACACS+), and Lightweight Directory Access Protocol (LDAP) server authentication methods, and Security Assertion Markup Language (SAML), which is used for exchanging authentication and authorization data between an Identity Provider (IdP) and a Service Provider (SP).
- **Two-Factor Authentication**: FortiAuthenticator can act as a two-factor authentication server with support for one-time passwords (OTP) using FortiToken Hardware, FortiToken Mobile, Short Message Service (SMS), or email. FortiAuthenticator two-factor authentication is compatible with any system which supports RADIUS.
- **IEEE802.1X Support**: FortiAuthenticator supports 802.1X for use in FortiGate Wireless and Wired networks.
- **User Identification**: FortiAuthenticator can identify users through multiple data sources, including Active Directory (AD), desktop client, guest portal logon, RADIUS accounting, Kerberos, and a Representational State Transfer (REST) API. It can then communicate this information to FortiGate or FortiMail units for use in identity based policies.
- **Certificate Management**: FortiAuthenticator can create and sign digital certificates for use, for example, in FortiGate VPNs and with the FortiToken 300 USB certificate store.
- **Integration**: FortiAuthenticator can integrate with third-party RADIUS, LDAP, and SAML authentication systems, allowing you to reuse existing information sources. The REST API can also be used to integrate with external provisioning systems.

FortiAuthenticator is a critical system, and should be isolated on a network interface that is separated from other hosts to facilitate server-related firewall protection. Be sure to take steps to prevent unauthorized access to the FortiAuthenticator.

FortiAuthenticator on a multiple FortiGate unit network



The FortiAuthenticator series of identity and access management appliances complement the FortiToken range of two-factor authentication tokens for secure remote access. FortiAuthenticator allows you to extend the support for FortiTokens across your enterprise by enabling authentication with multiple FortiGate appliances and third-party devices. FortiAuthenticator and FortiToken deliver cost effective, scalable, secure authentication to your entire network infrastructure.

The FortiAuthenticator device provides an easy-to-configure remote authentication option for FortiGate users. Additionally, it can replace the Fortinet Single Sign-On (FSSO) Agent on a Windows AD network.

For more information about FortiTokens, see the FortiToken information page on the Fortinet web site.

Before you begin

Before you begin using this guide, please ensure that:

- You have administrative access to the GUI and/or CLI.
  For details of how to accomplish this, see the QuickStart Guide provided with your product, or online at https://docs.fortinet.com/product/fortiauthenticator/hardware.
- FortiAuthenticator is integrated into your network.
- The operation mode has been configured.
- The system time, DNS settings, administrator password, and network interfaces have been configured.

  Network Time Protocol (NTP) is critical for maintaining accurate and stable time, and is required when using the Time-based One-time Password (TOTP) method for two-factor authentication.

  For more information, see Configuring the system date, time, and time zone on page 36.

- Any third-party software or servers have been configured using their documentation.

While using the instructions in this guide, note that administrators are assumed to have all permissions, unless otherwise specified.

Some restrictions will apply to administrators with limited permissions.

How this guide is organized

This FortiAuthenticator Administration Guide contains the following sections:

Setup	The initial setup for standalone and HA cluster FortiAuthenticator configurations.
System	The options available in the **System** menu tree, including network configuration, administration settings, and messaging settings.

Authentication	Configure built-in and remote authentication servers and manage users and user groups.
Port-based network access control (PNAC)	Configure FortiAuthenticator for IEEE 802.1X Extensible Authentication Protocol (EAP) authentication methods, Bring Your Own Device (BYOD), and MAC-based device authentication.
Fortinet Single Sign-On (FSSO)	Use FortiAuthenticator in a single sign-on (SSO) environment.
RADIUS Single Sign-On (RSSO)	Use FortiAuthenticator RADIUS accounting proxy.
Monitoring	Monitor SSO and authentication information.
Certificate management	Manage X.509 certificates and how to set up FortiAuthenticator to act as a certificate authority (CA).
Logging on page 319	View the logs on your FortiAuthenticator unit.
Troubleshooting	Suggestions to resolve common problems.
LDAP filter syntax	Basic filter syntax that is used to select users and groups in LDAP User Import, Dynamic LDAP Groups, and Remote User Sync Rules.

Registering your Fortinet product

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

Many Fortinet customer services such as firmware updates, technical support, FortiGuard Antivirus, and other FortiGuard services require product registration.

Setup

For information about installing FortiAuthenticator and accessing the CLI or GUI, refer to the Quick Start Guide provided with your unit.

This chapter provides basic setup information for getting started with your FortiAuthenticator device. For more detailed information about specific system options, see System on page 33.

Initial setup

The following section provides information about setting up the virtual machine (VM) version of FortiAuthenticator on VMware. For setup instructions for other environments, see the Fortinet Document Library.

The following virtualization environments are supported by FortiAuthenticator 8.0.0:

- VMware ESXi 6/7/8
- Microsoft Hyper-V 2010, 2016, 2019, and 2022
- KVM (Kernel-based Virtual Machine)
- Xen Virtual Machine (for Xen HVM)
- Nutanix
- Amazon Web Services (AWS)
- Microsoft Azure
- Oracle Cloud Infrastructure (OCI)
- Alibaba Cloud
- SCCC (Saudi Cloud Computing Company)
- Proxmox

FortiAuthenticator-VM setup on VMware

Before using FortiAuthenticator-VM, you need to install the VMware application to host the FortiAuthenticator-VM device.

The installation instructions for FortiAuthenticator-VM assume you are familiar with VMware products and terminology.

System requirements

FortiAuthenticator-VM is compatible with Hyper-V Windows Server 2010, 2016, 2019, and 2022.

For information on the FortiAuthenticator-VM system requirements, see the FortiAuthenticator datasheet.

FortiAuthenticator-VM has kernel support for more than 4 GB of RAM in VM images. However, this support also depends on the VM player version. For more information, see http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1014006

The default **Hardware Version** is 4 in order to support the widest base of VM players. However you can modify the VM Hardware Version by editing the following line in the `FortiAuthenticator-VM.vmx` file:

```
virtualHW.version = "4"
```

FortiAuthenticator-VM image installation and initial setup

The following procedure describes setup on VMware Fusion.

To set up the FortiAuthenticator-VM image:

1. Download the VM image zip file to the local computer where VMware is installed.
2. Extract the files from the zip file into a folder.
3. In your VMware software, go to **File > Open**.
4. Navigate to the expanded VM image folder, select the **FortiAuthenticator-VM.vmx** file, and select **Open**.
   VMware will install and start FortiAuthenticator-VM.
   This process can take a minute or two to complete.
5. At the FortiAuthenticator login prompt, enter `admin` and press **Enter**.
   By default, there is no password, however, a password must be set before you can proceed.
   Enter and confirm the new administrator password.
6. At the CLI prompt enter the following commands:

```
config system interface
 edit port1
  set ip <ip-address>/<netmask>
  set allowaccess https-gui https-api ssh
 next
end
config router static
 edit 0
  set device port1
  set dst  0.0.0.0/0
  set gateway <ip-gateway>
 next
end
```

   Substitute your own desired FortiAuthenticator IP address and default gateway.
   You can now connect to the GUI at the IP address you set for `port1`.

Suspending the FortiAuthenticator-VM can have unintended consequences. Fortinet recommends that you do not use the suspend feature of VMware. Instead, shut down the virtual FortiAuthenticator system using the GUI or CLI, and then shut down the virtual machine using the VMware console.

Administrative access

Administrative access is enabled by default on `port 1`.

Using the GUI, you can enable administrative access on other ports if necessary.

To add administrative access to an interface:

1. Go to **System > Network > Interfaces** and select the interface you need to add administrative access to. See Network on page 41 for more information.
2. Under **Access Rights**, for **Admin access**, select the types of access to allow.
3. Select **OK**.

GUI access

To use the GUI, point your browser to the IP address of port 1 (`192.168.1.99` by default).

For example, enter the following in the URL box:

```
https://192.168.1.99
```

Enter `admin` as the **User Name** and leave the **Password** field blank.

HTTP access is not enabled by default.

To enable access, use the `set ha-mgmt-access` command in the CLI (see CLI commands on page 28), or enable HTTP access on the interface in the GUI (see Network on page 41).

For security reasons, the host or domain names that the GUI responds to are restricted. The list of trusted hosts is automatically generated from the following:

- Configured hostname.
- Configured DNS domain name.
- Network interface IP addresses that have HTTP or HTTPS enabled.
- HA management IP addresses.

Additional IP addresses and host or domain names that the GUI responded to can be defined in the **GUI Access** settings.

See System access on page 48 for more information.

SSH

SSH provides secure access to the CLI. Connect to the port1 interface IP address (`192.168.1.99` by default).

Specify the user name `admin` or SSH will attempt to log on with your user name.

For example:

```
$ ssh admin@192.168.1.99
```

By default there is no password.

When you are finished, use the `exit` command to end the session.

After three failed login attempts, the interface/connection will reset, and that SSH timeout is set to 60 seconds following an incomplete login or broken session.

Adding FortiAuthenticator to your network

Before setting up FortiAuthenticator, there are some requirements for your network:

- You must have security policies that allow traffic between the client network and the subnet of the FortiAuthenticator.
- You must ensure that the following ports are open in the security policies between the FortiAuthenticator and authentication clients, in addition to management protocols such as HTTP, HTTPS, SSH, ping, and other protocols you may choose to allow:
  - `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/2560` (OCSP)
  - `TCP/8001` (FortiClient Single Sign-On Mobility Agent FSSO)
  - `TCP/8002` (DC/TS Agent FSSO)
  - `TCP/8003` (Hierarchical FSSO)

To setup FortiAuthenticator on your network:

1. Log in to the GUI with the username `admin` and no password.
2. Go to **System > Network > DNS**.
   Enter your internal network primary and secondary name server IP addresses.
   This is essential for successful FSSO operation.
   See DNS on page 44 for more information.
3. Go to **System > Network > Static Routing** and create a default route (IP/Mask `0.0.0.0/0`) to your network gateway on the interface that connects to the gateway.
   See Static routing on page 45 for more information.
4. Go to **System > Dashboard > Status**.
5. In the **System Information** widget select **Change** in the **System Time** field, and select your **Time zone** from the list.
6. Either enable the NTP or manually enter the date and time.
   See Configuring the system date, time, and time zone on page 36 for more information.
   Enter a new time and date by either typing it manually, selecting **Today** or **Now**, or select the calendar or clock icons.

If you plan to use FortiToken devices, Fortinet strongly recommends using NTP. FortiToken Time based authentication tokens are dependent on an accurate system clock.

7. Select **OK**.
8. If the FortiAuthenticator is connected to additional subnets, configure additional FortiAuthenticator interfaces as required.
   See Network on page 41 for more information.

Maintenance

System maintenance tasks include:

- Backing up the configuration on page 25
- Upgrading the firmware on page 25
- Licensing on page 26
- Swapping hard disks on page 26
- Platform migration on page 27

Backing up the configuration

You can back up the configuration of FortiAuthenticator to your local computer.

See Backing up and restoring the configuration on page 37 for more information.

Automatic system configuration backup can also be configured.

See Configuring auto-backup on page 57 for information.

Upgrading the firmware

Periodically, Fortinet issues firmware upgrades that fix known issues, add new features and functionality, and generally improve your FortiAuthenticator experience.

See Firmware upgrade on page 57 for more information.

Before proceeding to upgrade your system, Fortinet recommends you back up your configuration.

Follow the procedure detailed in Backing up and restoring the configuration on page 37.

To upgrade the firmware, you must first register your FortiAuthenticator with Fortinet.

See Registering your Fortinet product on page 20 for more information.

To upgrade FortiAuthenticator firmware from the GUI:

1. Download the latest firmware to your local computer from the Fortinet Support website.
2. Go to **System > Administration > Firmware Upgrade**.
3. Select **Upload a file** and locate the firmware image on your local computer.
4. Select **Upload**.
   The firmware image uploads from your local computer to the FortiAuthenticator device, which will then reboot.
   For a short period of time during this reboot, the FortiAuthenticator device is offline and unavailable for authentication.

To upgrade FortiAuthenticator firmware using the CLI:

1. Copy the latest firmware image file to the root directory of the FTP/TFTP server.
2. Log into the CLI.
3. Enter the following command to copy the firmware image from the FTP/TFTP server to FortiAuthenticator:
   For ftp servers:

   ```
   execute restore image ftp <filename> <ftp_ipv4>
   ```

   For tftp servers:

   ```
   execute restore image tftp <filename> <tftp_ipv4>
   ```

   Where is the `<filename>` is the name of the firmware image file and `<ftp_ipv4>` or `<tftp_ipv4>` is the IP address of the FTP/TFTP server.
4. Type y.
   FortiAuthenticator uploads the firmware image file, upgrades to the new firmware version, and restarts.

Licensing

FortiAuthenticator-VM works in evaluation mode until it is licensed. The license is valid only if one of the FortiAuthenticator interfaces is set to the IP address specified in the license. See Licensing on page 61 for more information.

To license FortiAuthenticator:

1. Go to **System > Administration > Licensing**.
2. Select **Upload a file** and locate on your local computer the license file you received from Fortinet.
3. Select **Upload**.

Swapping hard disks

If a hard disk on a FortiAuthenticator unit fails, it must be replaced. On FortiAuthenticator devices that support hardware RAID, the hard disk can be replaced while the unit is still running - know as hot swapping. On FortiAuthenticator units with software RAID, the device must be shutdown prior to exchanging the hard disk.

To identify the failed hard disk, go to **System > Dashboard > Status** and view the **Disk Monitor** widget. When a hard disk fails, the RAID status shows as **Degraded** and the RAID status icon displays a warning indication in yellow. In the RAID graphic, the failed hard disk disappears from the RAID array or displays with a blue question mark symbol.

When replacing a hard disk, you need to first verify that the new disk is the same size as those supplied by Fortinet and has at least the same capacity as the old one in the FortiAuthenticator unit. Installing a smaller hard disk will affect the RAID setup and may cause data loss. Due to possible differences in sector layout between disks, the only way to guarantee that two disks have the same size is to use the same brand and model.

The size provided by the hard drive manufacturer for a given disk model is only an approximation. The exact size is determined by the number of sectors present on the disk.

Electrostatic discharge (ESD) can damage FortiAuthenticator equipment.

Only perform the procedures described in this document from an ESD workstation.

If no such station is available, you can provide some ESD protection by wearing an anti-static wrist or ankle strap and attaching it to an ESD connector or to a metal part of a FortiAuthenticator chassis.

To hot swap a hard disk on a device that supports hardware RAID:

1. Remove the faulty hard disk.
2. Install a new disk in the same slot from which the failed disk was removed.
   The **Disk Monitor** widget updates.
   In the RAID graphic, a blue question mark symbol appears in the representative slot where the new hard disk is installed.
   If the blue question mark symbol does not appear shortly after the new disk is installed, in the widget, click **Refresh** to refresh the RAID status.
3. In the RAID graphic, click the blue question mark symbol.
   The hard disk re-synchronization/rebuild process is initialized.
   This process can take over an hour to complete, depending on the size of the hard disk.
   The RAID status changes to display the progress of the RAID re-synchronization/rebuild.
   After the re-synchronization/rebuild process is complete, the RAID status changes to OK and the RAID status icon displays a green checkmark.

In FortiAuthenticator 300F, use `execute factory-reset-skip-raid` CLI command to skip RAID creation during factory reset.

Platform migration

Follow the steps below when changing FortiAuthenticator to a different platform type, for example a new hardware platform, a VM using a different hypervisor, or when moving from hardware to VM or from VM to hardware.

To migrate FortiAuthenticator platforms:

1. The configuration file will need to be converted by Fortinet.
   - Save the configuration file of the existing FortiAuthenticator.
     See Backing up and restoring the configuration on page 37.
   - Contact Fortinet support to open a case requesting a configuration conversion.
     Provide the configuration file as well as the target platform.
2. The following licenses must be transferred to the new hardware: FTM, SSOMA, SMS.
   - In same case, specify the license numbers as well as the serial number of the new FortiAuthenticator.

Following this process, provisioned software tokens remain on the new system after conversion and end users do not have to replace the token on their mobile application.

CLI commands

The FortiAuthenticator has CLI commands that are accessed using SSH or through the CLI console if a FortiAuthenticator is installed on a FortiHypervisor. The commands can be used to initially configure the unit, perform a factory reset, or reset the values if the GUI is not accessible.

All FortiAuthenticator CLI commands fall under the following initial setup commands:

- `config router static`
- `config system dns`
- `config system global`
- `config system ha`
- `config system interface`

The FortiAuthenticator-VM's console allows scrolling up and down through the CLI output by using `Shift+PageUp` and `Shift+PageDown`.

Like FortiOS, the `?` key can be used to display all possible options available to you, depending upon where you are hierarchically-situated.

Note that `get`, `execute`, and `diagnose` commands are also available.

Command	Description
`?`	Display list of valid CLI commands.

Command	Description
`exit`	Terminate the CLI session.
`show`	Display bootstrap configuration.
`set port1-ip <IP/netmask>`	Enter the IPv4 address and netmask for the port1 interface. Netmask is expected in the /xx format, for example `192.168.0.1/24`. After this port is configured, you can use the GUI to configure the remaining ports.
`set default-gw <IP>`	Enter the IPv4 address of the default gateway for this interface. This is the default route for this interface.
`set date <YYYY-MM-DD>`	Enter the current date. Valid format is four digit year, two digit month, and two digit day. For example: `set date 2014-08-12` sets the date to August 12, 2014.
`set time <HH:MM:SS>`	Enter the current time. Valid format is two digits each for hours, minutes, and seconds. 24-hour clock is used. For example 15:10:00 is 3:10pm.
`set tz <timezone_index>`	Enter the current time zone using the time zone index. To see a list of index numbers and their corresponding time zones, enter `set tz ?`.
`set ha-mode {enable | disable}`	Enable or disable (default) HA mode.
`set ha-port <interface>`	Select a network interface to use for communication between the two cluster members. This interface must not already have an IP address assigned and it cannot be used for authentication services. Both units must use the same interface for HA communication.
`set ns-gw <gateway>`	Set a default gateway for the HA management interface.
`set ha-priority {high | low}`	Set to `low` on one unit and `high` on the other. Normally, the unit with High priority is the primary unit.
`set ha-password <password>`	Set the HA password.
`set ha-mgmt-ip <IP/netmask>`	Enter the IP address, with netmask, that this unit uses for HA related communication with the other FortiAuthenticator unit (e.g. `1.2.3.4/24`. The two units must have different addresses. Usually, you should assign addresses on the same private subnet.

Command	Description
`set ha-mgmt-access {ssh | https | http}`	Select the types of administrative access to allow.
`set ha-dbg-level <level>`	Enter the level for HA service debug logs. Range: -4 (fatal) to 4 (debug high). Default: -2 (warn).
`unset <setting>`	Restore default value. For each `set` command listed above, there is an `unset` command, for example `unset port1-ip`.
`raid-add-disk <slot>`	Add a disk to a degraded RAID array.
`ha-rebuild`	Rebuild the configuration database from scratch using the HA peer's configuration.
`restore-admin`	Restore factory reset's admin access settings to the port1 network interface.
`reboot`	Perform a hard restart of FortiAuthenticator. All sessions are terminated. The unit goes offline and a delay occurs while it restarts.
`factory-reset`	Enter this command to reset the FortiAuthenticator settings to factory default settings. This includes clearing the user database. This procedure deletes all changes that you have made to the FortiAuthenticator configuration and reverts the system to its original configuration, including resetting interface addresses. **Note**: When `factory-reset` is used, all the logs are deleted.
`shutdown`	Turn off the FortiAuthenticator.
`status`	Display basic system status information including firmware version, build number, serial number of the unit, and system time.
`hardware-info`	Display general hardware status information.
`disk-attributes`	Display system disk attributes.
`disk-errors`	Display any system disk errors.
`disk-health`	Display disk health information.
`disk-info`	Display disk hardware status information.

Command	Description
`raid-hwinfo`	Display RAID hardware status information.
`nslookup`	Basic tool for DNS debugging.
`dig`	Advanced DNS debugging.
`ping`	Test network connectivity to another network host.
`tcpdump`	Examine local network traffic.
`tcpdumpfile`	Same as `tcpdump`, but the output is written to a downloadable file that can be downloaded in the debug logs. Debug logs can be accessed via your web browser by navigating to: `https://<FortiAuthenticator-IP-Address>/debug` For more information, see Debug logs on page 328.
`traceroute`	Examine the route taken to another network host.

Troubleshooting

Troubleshooting includes useful tips and commands to help deal with issues that may occur. For additional help, contact customer support.

See Troubleshooting on page 327 for more information.

If you have issues when attempting authentication on a FortiGate unit using the FortiAuthenticator, there are some FortiAuthenticator and FortiGate settings to check.

In addition to these settings you can use log entries, monitors, and debugging information to determine more knowledge about your authentication problems. For help with FortiAuthenticator logging, see Logging on page 319.

FortiAuthenticator settings

When checking FortiAuthenticator settings, you should ensure that:

- There is an authentication client entry for the FortiGate unit (see RADIUS service on page 189).
- The user trying to authenticate has a valid active account that is not disabled, and that the username and password are entered correctly.
- The user account allows RADIUS authentication if RADIUS is enabled on the FortiGate unit.
- The FortiGate unit can communicate with FortiAuthenticator, on the required ports:
- RADIUS Authentication: `UDP/1812`
- LDAP: `TCP/389`
- The user account exists either:

    - as a local user on the FortiAuthenticator (if using RADIUS authentication),
    - in the local LDAP directory (if using local LDAP authentication),
    - and/or in the remote LDAP directory (if using RADIUS authentication with remote LDAP password validation).
- The user is a member in the expected user groups and these user groups are allowed to communicate on the authentication client (e.g. the FortiGate).
- If authentication fails with the log error "bad password", try resetting the password. If this fails, verify that the pre-shared secret is identical on both FortiAuthenticator and the authentication client.

If FortiToken authentication is failing, try the following:

- Verify that the token is correctly synchronized.
- Remove the token from the user authentication configuration and verify authentication works when the token is not present.
- Attempt to log into the FortiAuthenticator with the user credentials.

These steps enable the administrator to identify whether the problem is with the FortiGate unit, the credentials, or the FortiToken.

FortiGate settings

When checking FortiGate authentication settings, you should ensure that:

- The user has membership in the required user groups and identity-based security policies.
- There is a valid entry for the FortiAuthenticator device as a remote RADIUS or LDAP server.
- The user is configured either explicitly or as a wildcard user.

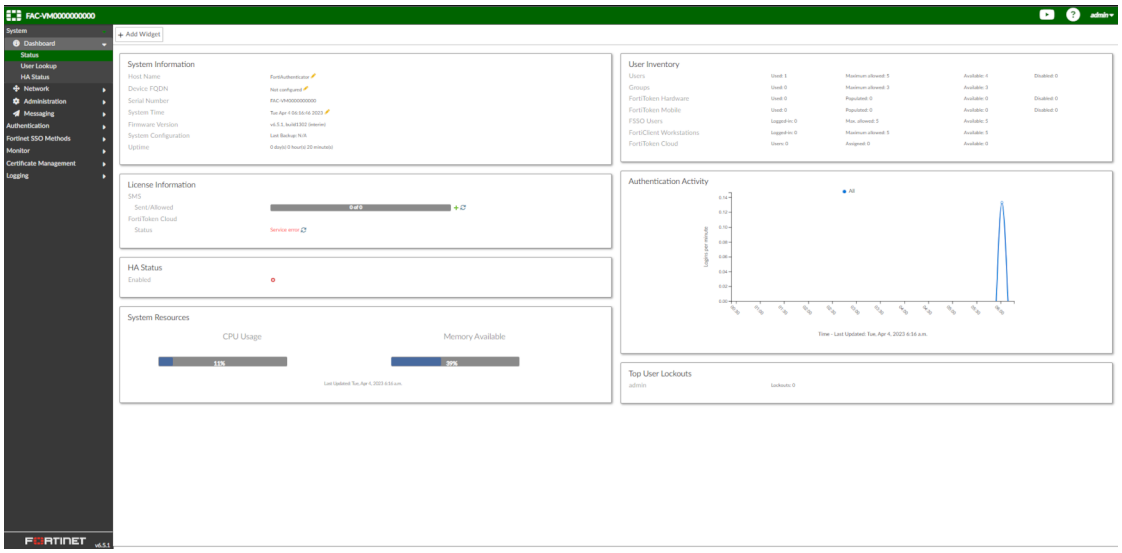
System

The **System** tab enables you to manage and configure the basic system options for FortiAuthenticator.

This includes the basic network settings to connect the device to the corporate network, the configuration of administrators and their access privileges, managing and updating firmware for the device, and managing messaging servers and services.

Dashboard

The **Dashboard** page displays widgets that provide performance and status information, allowing you to configure some basic system settings. These widgets appear on a single dashboard.



The following widgets are available:

System Information	Displays basic information about the FortiAuthenticator system including host name, device FQDN name, serial number, system time, firmware version, architecture, system configuration, current administrator, and up time. From this widget you can manually update the FortiAuthenticator firmware to a different release. For more information, see System information widget on page 35.
System Resources	Displays the usage status of the CPU and memory. For more information, see System resources widget on page 38.

Authentication Activity	Displays a customizable graph of the number of logins to the device. For more information, see Authentication activity widget on page 38.
User Inventory	Displays the numbers of users, groups, FortiTokens, FSSO users, FortiClient, and FortiToken Cloud users currently used or logged in, as well as the maximum allowed number, the number still available, and the number that are disabled. For more information, see User inventory widget on page 39.
HA Status	Displays whether or not HA is enabled.
License Information	Displays the device's license information, as well as SMS information. For more information, see License information widget on page 39.
Disk Monitor	Displays if RAID is enabled, and the current disk usage in GB. For more information, see Disk monitor widget on page 39.
Top User Lockouts	Displays the top user lockouts. For more information, see Top user lockouts widget on page 40.
Power Supply Monitor	Displays the status of power supply units connected to FortiAuthenticator. Available for select FortiAuthenticator hardware devices. For more information, see Power supply monitor widget on page 41

Customizing the dashboard

The FortiAuthenticator system settings dashboard is customizable. You can select which widgets to display, where they are located on the page, and whether they are minimized or maximized.

To move a widget

Position your mouse cursor on the widget's title bar, then click and drag the widget to its new location.

To add a widget

In the dashboard toolbar, select **Add Widget**, then select the widget you want to show. Multiple widgets of the same type can be added. To hide a widget, in its title bar, select the **Hide** icon.

To see the available options for a widget

Position your mouse cursor over the icons in the widget's title bar. Options include show/hide the widget, edit the widget, refresh the widget content, and close the widget.

The following table lists the widget options.

Show/Hide arrow	Display or minimize the widget.

Widget Title	The name of the widget.
Edit	Select to change settings for the widget. This option appears only in certain widgets.
Refresh	Select to update the displayed information.
Remove	Select to remove the widget from the dashboard. You are prompted to confirm the action. To add the widget, select **Widget** in the toolbar and then select the name of the widget you want to show.

To change the widget title

Widget titles can be customized by selecting the edit button in the title bar and entering a new title in the widget settings dialog box. Some widgets have more options in their respective settings dialog box.

To reset a widget title to its default name, simply leave the **Custom widget title** field blank.

The widget refresh interval can also be manually adjusted from this dialog box.

System information widget

The system dashboard includes a **System Information** widget, which displays the current status of FortiAuthenticator and enables you to configure basic system settings.

The following information is available on this widget:

Host Name	The identifying name assigned to this FortiAuthenticator unit. For more information, see Changing the host name on page 36.
Device FQDN	The FQDN domain name. For more information, see Changing the FQDN domain name on page 36.
Serial Number	The serial number of FortiAuthenticator. The serial number is unique to FortiAuthenticator and does not change with firmware upgrades. The serial number is used for identification when connecting to the FortiGuard server.
System Time	The current date, time, and time zone on the FortiAuthenticator internal clock or NTP servers. For more information, see Configuring the system date, time, and time zone on page 36.
Firmware Version	The version and build number of the firmware installed on FortiAuthenticator. To update the firmware, you must download the latest version from the Customer Service & Support portal at https://support.fortinet.com. Select **Upgrade** and select the firmware image to load from your management computer.
System Configuration	The date of the last system configuration backup. Select **Backup/Restore** to backup or restore the system configuration. For more information, see Backing up and restoring the configuration on page 37.

Uptime	The duration of time FortiAuthenticator has been running since it was last started or restarted.

Changing the host name

The **System Information** widget will display the full host name.

To change the host name:

1. Go to **System > Dashboard > Status**.
2. In the **System Information** widget, select the edit icon in the **Host Name** field. The **Edit Host Name** page opens.
3. In the **Host name** field, type a new host name.

The host name may be up to 35 characters in length. It may include US-ASCII letters, numbers, hyphens, and underscores. Spaces and special characters are not allowed.

4. Select **Save** to save the setting.

Changing the FQDN domain name

To change the FQDN domain name:

1. Go to **System > Dashboard > Status**.
2. In the **System Information** widget, select the edit icon in the **Device FQDN** field. The **Edit Device FQDN** page opens.
3. Type a domain name in the field.
   The FQDN domain name identifies the exact location of this server in the DNS hierarchy.
4. Select **Save** to save the setting.

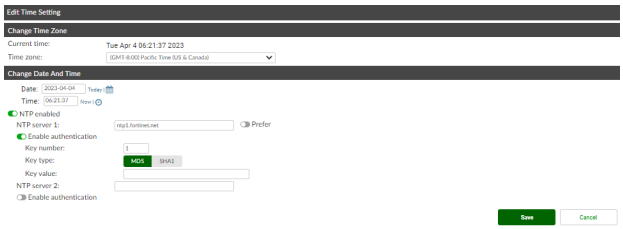
Configuring the system date, time, and time zone

You can either manually set the FortiAuthenticator system date and time, or configure the FortiAuthenticator unit to automatically keep its system time correct by synchronizing with an NTP server.

For many features to work the FortiAuthenticator system time must be accurate. Synchronization with a NTP server is highly recommended.

To configure the date and time:

1. Go to **System > Dashboard > Status**.
2. In the **System Information** widget, select the edit icon in the **System Time** field. The **Edit Time Setting** dialog box appears.



3. Configure the following settings to either manually configure the system time, or to automatically synchronize the FortiAuthenticator unit's clock with a NTP server:

Change Time Zone	
Time zone	Select a timezone from the dropdown menu.
Change Date and Time	
Set date/time	Select **Today** or the calendar icon to specify the date, and **Now** or the clock icon to specify the time.
NTP enabled	Enable this option to set an NTP server. Note that, if you configure both NTP servers, you can select **Prefer** to make **NTP server 1** the preferred server. The **NTP server 1** is set to **ntp1.fortinet.net** by default. In addition, you can select **Enable authentication** for each NTP server configured and enter a key number, type, and the key value.

4. Select **Save** to apply your changes.

Backing up and restoring the configuration

Fortinet recommends that you back up your FortiAuthenticator configuration to your management computer on a regular basis to ensure that, should the system fail, you can quickly get the system back to its original state with minimal effect to the network. You should also perform a back up after making any changes to the FortiAuthenticator configuration.

The backup file is encrypted to prevent tampering. This configuration file includes both the CLI and GUI configurations of FortiAuthenticator, including users, user groups, FortiToken device list, authentication client list, LDAP directory tree, FSSO settings, remote LDAP, and certificates.

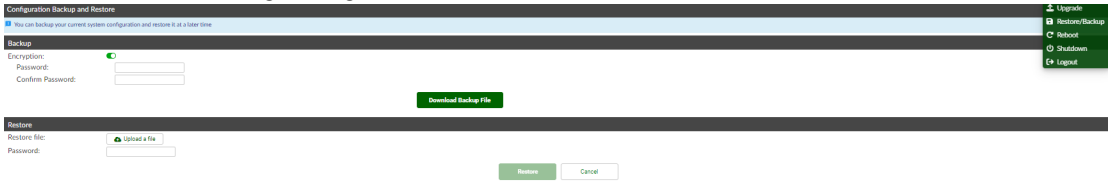
The date and time that the FortiAuthenticator was last backed up is displayed in the System Information widget.

You can perform backups manually. Fortinet recommends backing up all configuration settings from your FortiAuthenticator unit before upgrading the FortiAuthenticator firmware.

Your FortiAuthenticator configuration can also be restored from a backup file on your management computer.

To backup or restore the FortiAuthenticator configuration:

1. In the user dropdown menu, select **Restore/Backup**. The **Configuration Backup and Restore** page opens.
2. Select from the following settings:



Backup	Enable **Encryption** to use a dynamic encryption key, and specify the encryption password. By default, **Encryption** is disabled. Select **Download backup file** to save a backup file onto the management computer.
Restore	Select **Upload a file** to find the backup file on your management computer, enter the encryption password in **Password**, then select **Restore** to restore the selected backup configuration to the device. By default, decryption is disabled. You are prompted to confirm the restore action, and FortiAuthenticator will reboot.

3. Select **Cancel** to return to the dashboard page.

When you restore the configuration from a backup file, any information changed since the backup will be lost. Any active sessions will be ended and must be restarted. You will have to log back in when the system reboots.

Restoring a configuration is only possible from a backup file made on the same model running the same version of the operating system.

If you are restoring a configuration on the primary device in an HA cluster, shutdown the secondary device until the primary device is back online to ensure that the configuration synchronization occurs correctly.

When someone restores a configuration backup, the automated SCIM task could result in severely undesirable side effects if allowed to run.

For example, restoring an old configuration backup into a lab environment with access to the public internet could come in conflict with the SCIM replication of the production environment.

For this reason, SCIM syncing to any configured SP is disabled after a configuration restore.

A warning message is displayed when you login after a configuration restore if SCIM has been disabled.

To reactivate the SCIM service, go to **Authentication > User Account Policies > General** and enable **Re-activate SCIM (client)**.

See General on page 82.

System resources widget

The **System Resources** widget on the dashboard displays the usage status of the CPU and memory as a percentage.

Authentication activity widget

The **Authentication Activity** widget displays a line graph of the number of logins versus time.

This graph in the **Authentication Activity** widget is designed to measure average authentication rates in systems with steadily high volumes of authentication attempts. The statistics at every time scale (i.e. 6 hours, 24 hours, 3 days, etc.) are accumulated into 48-time segments representing each point on the graph.

For example, for the "Last 6 hours", each point on the graph represents the rate for the preceding 450 secs (i.e. 6 hours * 3600 sec/hr/48).

To adjust the data displayed in the graph, select the edit button to open the **Authentication Activity Widget Settings** dialog box.

The following settings are available:

Custom widget title	Enter a custom widget title for the widget, or leave it blank to keep the default title.
Refresh interval	Enter a custom refresh interval for the widget (in seconds), or leave it as the default time of 300 seconds (or five minutes).
Time period	Select a time period for the graph to cover from the dropdown menu: **Last 6 hours**, **Last 24 hours**, **Last 3 days**, **Last 7 days**, or **Last 30 days**.
Activity Type	Select the activity type to display in the graph: **All login attempts**, **Successful login attempts**, or **Failed login attempts**.

User inventory widget

The **User Inventory** widget displays the numbers of users, groups, FortiTokens, FSSO users, FortiClient, and FortiToken Cloud users currently used or logged in, as well as the maximum allowed number, the number still available, and the number that are disabled.

The FSSO user quota limit is per FSSO user, not per FSSO session.

License information widget

The **License Information** widget displays the device's license information, as well as SMS information. You can also add a license and more SMS messages.

To upload a new license file, select **Upload** in the **License Type** field, then browse to the license file on the management computer.

To add more SMS messages, select **Add Messages** from either the **Sent/Allowed** field or the **Status** field. In the **Add Messages** dialog box, enter the certificate number for the messages and then select **OK** to add the messages. You can also **Refresh Messages**.

Disk monitor widget

The **Disk Monitor** widget displays the RAID status, and the current disk usage in GB. If RAID is enabled, the RAID status is visible and the RAID graphic displays the position and status of each disk in the RAID array.

Top user lockouts widget

The **Top User Lockouts** widget displays the users who are locked out the most. For more information on user lockouts and for instruction on adjusting user lockout settings, see Lockouts on page 85.

To change the number of user lockouts displayed in the widget, select the edit icon and change the number in the **Number of lockouts** field (set to five by default).

User lookup

You can search for users to easily manage and monitor the ongoing activity of a specific user. Selecting a user from the search results presents a consolidated view of the user's information and recent activities, as well as shortcuts to manage that user.

To search for users, go to **System > Dashboard > User Lookup**. From the search results, click the username to see user details.

The following information and options are available:

User Info		
	Username	The user accounts' username.
	Full name	The user accounts' first name and last name.
	Email	The user account's email address.
	User Type	The user account type, either **Local**, **LDAP/<server name>**, or **RADIUS/<server name>**.
	Account status	The status of the user account, either **Enabled**, **Disabled**, or **Locked until <date/time>**. The following account management shortcuts are available depending on the account status: **Disable**: Select to disable the account of a user that is enabled. **Re-enable**: Select to enable the account of a user that is disabled. **Unlock**: Select to unlock the account of a user that has been locked.
	Token	The token that is assigned to the user account. Select **Edit** to manage the token assigned to the account. See Configuring One-Time Password (OTP) authentication on page 101.
RADIUS-based Usage		The user accounts' cumulative RADIUS-based usage statistics. See Authentication on page 282 for more information.
Active RADIUS Sessions		The user accounts' active RADIUS accounting sessions. See Authentication on page 282 for more information.
Recent Activity		The 20 most recent system logs containing the selected username in the log's User and/or Short message fields. For more information about system logs, see Log access on page 319.

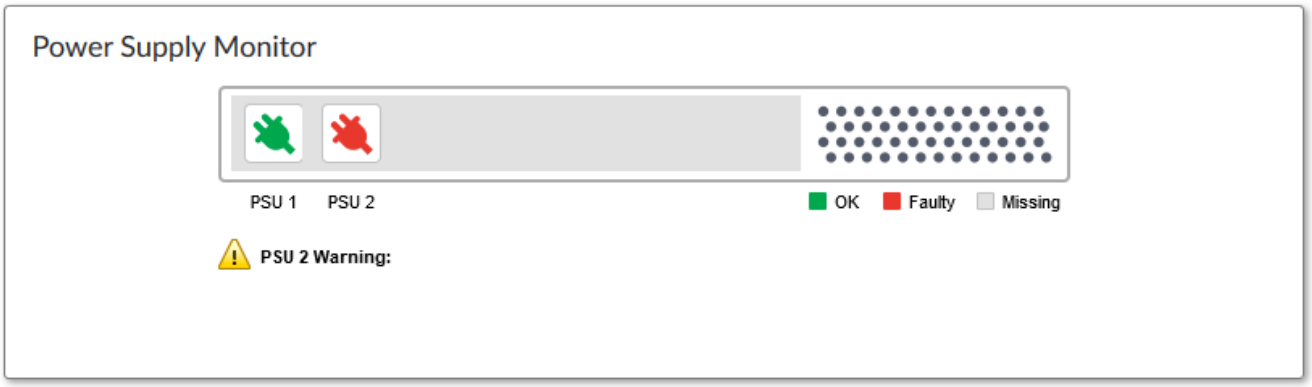
Refresh	Select to refresh the Recent Activity list.
View All	Select to view all logs containing the selected username. See Log access on page 319 for more information.

Power supply monitor widget

The **Power Supply Monitor** displays the status of the power supply units (PSU) connected to the FortiAuthenticator. The widget is only available FortiAuthenticator 400E and 3000E hardware devices.

Each PSU is displayed as a color-coded icon to indicate their current status:

- **Green**: PSU is OK.
- **Red**: PSU is faulty.
- **Gray**: PSU is missing/disconnected.



A warning message is displayed in the widget when a faulty PSU is detected. You can additionally configure SNMP traps to send alerts for PSU failure. See SNMP on page 58

Network

The **Network** tree menu allows you to configure device interfaces, DNS configuration, static routing, zero trust tunnels, and packet capturing.

Interfaces

To view the interface list, go to **System > Network > Interfaces**.

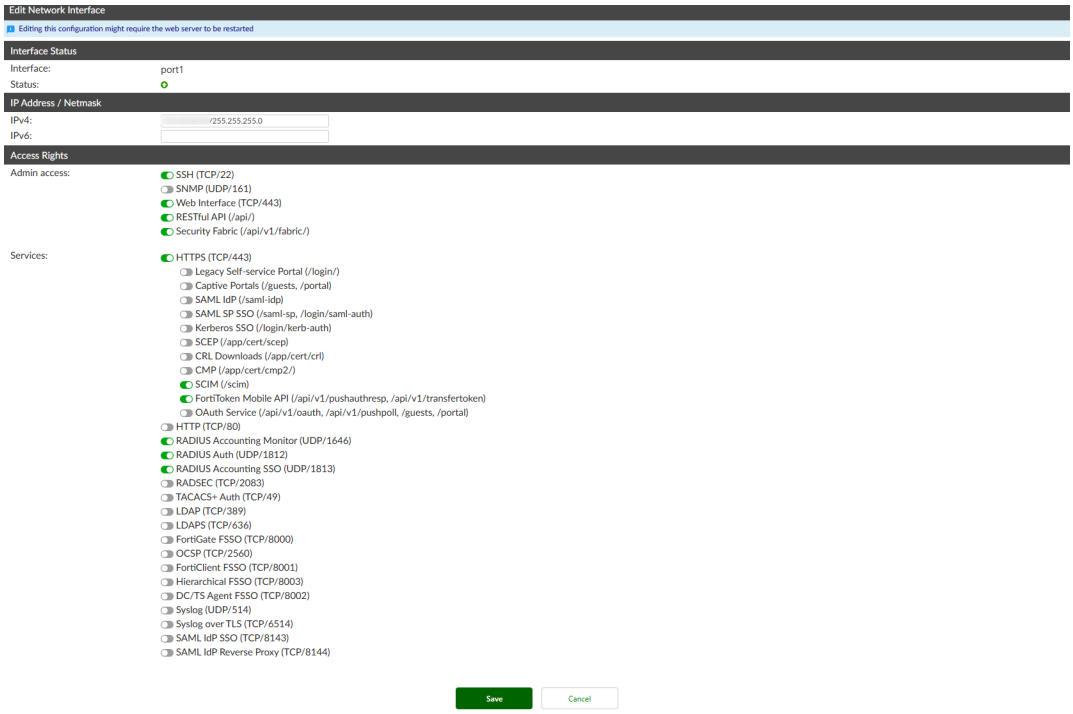
The following information is shown:

Edit	Select to edit the selected interface.

Search	Enter a search term in the search text box then select **Search** to search the interface list.
Interface	The names of the physical interfaces on your FortiAuthenticator unit. The name, including number, of a physical interface depends on the model.
IPv4	The IPv4 address of the interface.
IPv6	The IPv6 address of the interface, if applicable.
Link status	The link status of the interface.

To edit an interface:

1. In the interfaces list, select the interface you need to edit and select the **Edit** button, or select the interface name. The **Edit Network Interface** window opens.



2. Edit the following settings as required.

Interface	The interface name is displayed.
Status	The interface's current link status is displayed.
IP Address / Netmask	
IPv4	Enter the IPv4 address and netmask associated with this interface.
IPv6	Enter the IPv6 address associated with this interface.

	FortiAuthenticator only offers limited support for IPv6.
	FortiAuthenticator does not support incoming communication over IPv6 for most features.
	IPv6 support is available only for the following features:
	• Admin GUI access over IPv6.
	• **FSSO**:
	  • Extract end-user IPv6 addresses from Syslog messages (received over IPv4).
	  • Extract end-user IPv6 addresses from RADIUS accounting messages (received over IPv4).
	  • Extract end-user IPv6 addresses from Windows event logs polling.
	  • Create active end-user sessions for IPv6 addresses and send them to FortiGates.

Access Rights	
Admin access	Select the allowed administrative service protocols from: **SSH (TCP/22)**, **SNMP (UDP/161)**, **Web Interface (TCP/443)**, **RESTful API (/api/)**, and **Security Fabric (/api/v1/fabric/)**. By default, only **SSH (TCP/22)**, **Web Interface (TCP/443)**, and **RESTful API (/api/)** are enabled on `port1`.
Services	Enable the services that you want FortiAuthenticator to act as a server for: • **HTTPS (TCP/443)** • **HTTP (TCP/80)** • **RADIUS Accounting Monitor (UDP/1646)** • **RADIUS Auth (UDP/1812)** • **RADIUS Accounting SSO (UDP/1813)** • **RADSEC (TCP/2083)** • **TACACS+ Auth (TCP/49)** • **LDAP (TCP/389)** • **LDAPS (TCP/636)** • **FortiGate FSSO (TCP/8000)** • **OCSP (TCP/2560)** • **FortiClient FSSO (TCP/8001)** • **Hierarchical FSSO (TCP/8003)** • **DC/TS Agent FSSO (TCP/8002)** • **Syslog (UDP/514)** • **Syslog over TLS (TCP/6514)** • **SAML IdP SSO (TCP/8143)** • **SAML IdP Reverse Proxy**: Enable/disable the IdP reverse proxy port on the selected network interface.

When HTTPS is enabled, you can also specify access for the following services:

- **Legacy Self-service Portal (/login/)**
- **Captive Portals (/guests, /portal)**
- **SAML IdP (/saml-idp)**
- **SAML SP SSO (/saml-sp, /login/saml-auth)**
- **Kerberos SSO (/login/kerb-auth)**
- **SCEP (/app/cert/scep)**
- **CRL Downloads (/app/cert/crl)**
- **CMP (/app/cert/cmp2/)**
- **SCIM (/scim)**
- **FortiToken Mobile API (/api/v1/pushauthresp, /api/v1/transfertoken)**
- **OAuth Service (/api/v1/oauth, /api/v1/pushpoll, /guests, /portal)**

When HTTP is enabled, you can also specify access for the following services:

- **SCEP (/app/cert/scep)**
- **CRL Downloads (/app/cert/crl)**
- **CMP (/app/cert/cmp2/)**
- **SAML IdP metadata (/saml-idp)**
- **Kerberos SSO (/login/kerb-auth)**

Note that **Syslog (UDP/514)** is only available if **Syslog SSO** has been enabled. See Methods on page 250 for more information.

A disabled service will not answer queries as it is not active. Enabling the service but leaving it unconfigured will make the service respond to queries, even with incorrect responses. This will use resources and may cause a potential attack.

3. Select **Save** to apply the edits to the network interface.

DNS

To configure DNS settings:

1. Go to **System > Network > DNS**.

2. The following settings can be configured:

Primary DNS server	The IP address of the primary DNS server.
Secondary DNS server	The IP address of the secondary DNS server.

Enable DNS cache	Enable to cache the responses to DNS queries.
DNS cache maximum TTL	When DNS cache is enabled, configure the length of time (30 - 600) in seconds responses to DNS queries are cached. If the configured value is larger than the time to live (TTL) value specified in the DNS record, the DNS TTL value is used. The default is set to 0, which uses the TTL value specified in the DNS record.

3. To apply changes, select **Save**.

Static routing

To view the list of static routes, go to **System > Network > Static Routing**. Routes can be created, edited, and deleted as required. Use the checkboxes to select the static route entries you want to either **Delete** or **Edit**.

The following information is shown:

Create New	Select to create a new static route.
Delete	Select to delete the selected static route.
Edit	Select to edit the selected static route.
IP/Mask	The destination IP address and netmask for this route.
Gateway	The IP address of the next hop router to which this route directs traffic.
Device	The device or interface associated with this route.

To create a new static route:

1. In the static route list, select **Create New**. The **Create New Static Route** window opens.
2. Edit the following settings as required.

Destination IP/Mask	Enter the destination IP address and netmask for this route.
Network interface	Select the network interface that connects to the gateway.
Gateway	Enter the IP address of the next hop router to which this route directs traffic.
Comment	Optionally, enter a comment about the route.

3. Select **Save** to create the new static route.

Zero trust tunnels

To view the list of zero trust tunnels, go to **System > Network > Zero Trust Tunnels**. Zero trust tunnels can be created, edited, and deleted as required.

The following information is shown:

Create New	Select to create a new zero trust tunnel.
Delete	Select to delete the selected zero trust tunnel.
Edit	Select to edit the selected zero trust tunnel.
Reset table column widths	Select the reset icon to reset the table column widths to default.

To create a new zero trust tunnel:

1. In the zero trust tunnel list, select **Create New**.
   The **Create New Zero Trust Tunnel** window opens.
2. Edit the following settings as required.

Name	The name of the zero trust tunnel.
URL	The IP/FQDN and port number for the ZTNA server, e.g., `https://fac.school.net:8443/`.
Client certificate	From the dropdown, select a certificate that is used to authenticate to the ZTNA server. See Local CAs on page 299.

3. Select **Save** to create the new zero trust tunnel.

See Configuring a zero trust tunnel example on page 46.

Configuring a zero trust tunnel EXAMPLE

For information on Zero Trust Network Access (ZTNA), see Zero Trust Network Access introduction in the *FortiOS Admin Guide*.

This example shows zero trust tunnel-related configuration for FortiAuthenticator.

For detailed zero trust tunnel configuration, including setting up a remote zero trust server, see the *Setting up a zero trust tunnel* recipe in the *FortiAuthenticator Cookbook* on the Fortinet Docs Library.

Configuring a zero trust tunnel on FortiAuthenticator

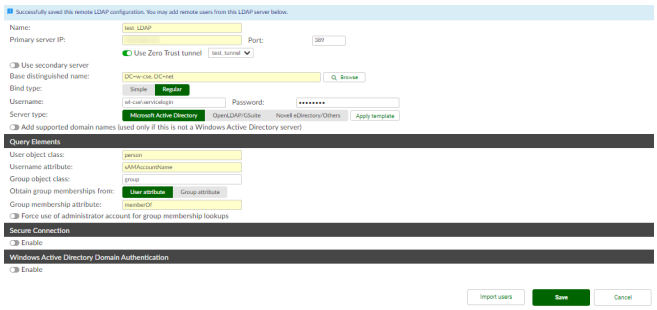
To configure a zero trust tunnel:

1. Go to **System > Network > Zero Trust Tunnels**.
2. Select **Create New**.
   The **Create New Zero Trust Tunnel** window opens.
3. In **Name**, enter a name for the zero trust tunnel.
4. In **URL**, enter a URL specifying the IP/FQDN and port for the ZTNA server, e.g., `https://fac.school.net:8443/`.
5. In the **Client certificate** dropdown, select a certificate. This certificate is used to authenticate to the ZTNA server.
6. Click **Save**.

Configuring an LDAP server with zero trust tunnel enabled on FortiAuthenticator

To configure an LDAP server:

1. Go to **Authentication > Remote Auth. Servers > LDAP**, and select **Create New**.
2. In **Create New LDAP server**:
   a. In **Name**, enter a name.
   b. Enable **Use Zero Trust tunnel** and from the dropdown select a zero trust tunnel.
   c. In **Primary Server IP**, enter the IP address/FQDN of the LDAP server.
   d. In **Port**, enter the port number of the LDAP server.
   e. In **Base distinguished name**, enter a base distinguished name.
   f. In **Bind Type**, select **Regular**.
   Enter the username and password for the LDAP server administrator account.
3. Click **Save**.



Packet capture

Packets can be captured on configured interfaces by going to **System > Network > Packet Capture**.

The following information is available:

Edit	Select to edit the packet sniffer on the selected interface.
Interface	The name of the configured interface for which packets can be captured. For information on configuring an interface, see Interfaces on page 41.
Maximum packets to capture	The maximum number of packets that can be captured on a sniffer.
Status	The status of the packet capture process. Allows you to start and stop the capturing process, and download the most recently captured packets.

To start capturing packets on an interface, select the **Start capturing** button in the **Status** column for that interface. The **Status** changes to **Capturing**, and the **Stop capturing** and download buttons become available.

To download captured packets:

1. Select the download button for the interface whose captured packets you are downloading.
   If no packets have been captured for that interface, select the **Start capturing** button.
2. When prompted, save the packet file (**sniffer_[interface].pcap**) to your management computer.
   The file can then be opened using packet analyzer software.

To edit a packet sniffer:

1. Select the interface whose packet capture settings you need to configure by either selecting the configured interface name from the interface list, or selecting the checkbox in the interface row and selecting **Edit** from the toolbar.
   The **Edit Packet Sniffer** page opens.
2. Configure the following options:

interface	The interface name (non-changeable).
Max packets to capture	Enter the maximum number of packets to capture, between 1-10000. The default is 500 packets.
Include IPv6 packets	Select to include IPv6 packets when capturing packets.
Include non-IP packets	Select to include non-IP packets when capturing packets.

3. Select **Save** to apply your changes.

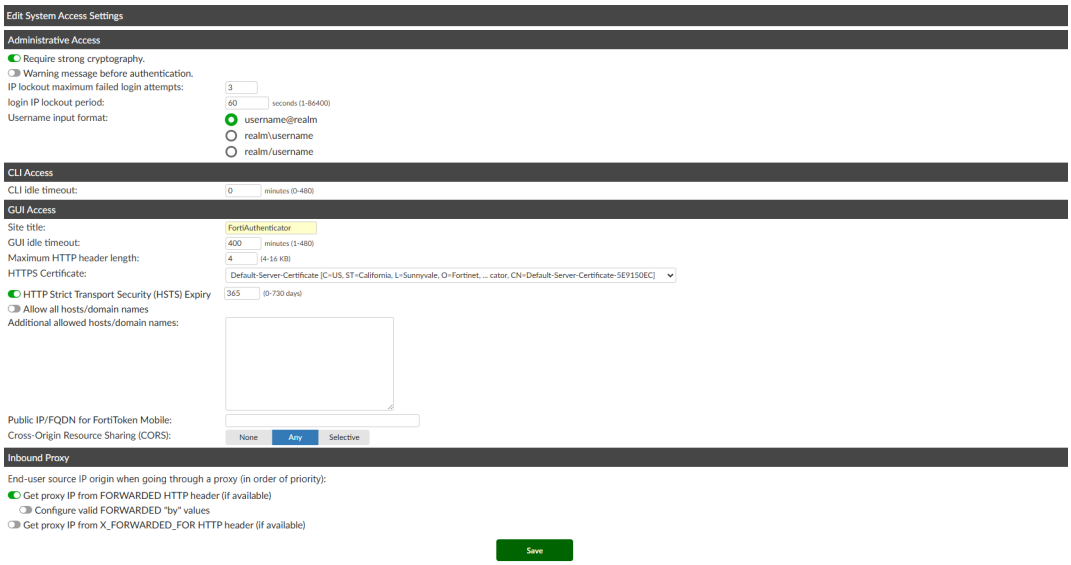
Administration

Configure administrative settings for the FortiAuthenticator device.

System access

To adjust system access settings:

1. Go to **System > Administration > System Access**.
   The **Edit System Access Settings** page will open.



2. The following settings are available:

Administrative Access	
Require strong cryptography	Enable this option to restrict administrative access using stronger cryptographic algorithms. FortiAuthenticator supports the following cryptographic protocols: • TLS 1.2: `AES128/256 GCM/CBC`, `SHA256/384`, `DHE2048`, and `ECDHx25519`. • TLS 1.3: `AES128/256 GCM`, `SHA256/384`, and `ECDHx25519`.
Warning message before authentication	Pre-authentication warning messages can be found under **Authentication > Portals > Replacement Messages**.
IP lockout maximum failed login attempts	Enter the maximum number of administrator login attempts after which the source IP address is blocked from gaining administrative access for the configured **Administrator login lockout period** (default = 3). **Note**: The failed login attempts are counted by the source IP address.
Login IP lockout period	Enter the period of time for which the administrator logins from the locked source IP address are blocked, in seconds (1 - 86400 or one minute to a day, default = 60).
Username input format	The separator used for administrator login and fabric: • **username@realm** (default) • **realm\username** • **realm/username**
CLI Access	
CLI idle timeout	Enter the amount of time before the CLI times out due to inactivity, from 0 to 480 minutes (maximum of eight hours).

GUI Access	
Site title	Specify the string to display as the page title in web browsers. The following variables are available for the construction of the string: • **{{:hostname}}**: Host name • **{{:fqdn}}**: Device FQDN The default is set to FortiAuthenticator.
GUI idle timeout	Enter the amount of time before the GUI times out due to inactivity, from 1 to 480 minutes (maximum of eight hours).
Maximum HTTP header length	Enter the maximum HTTP header length, from 4 to 16 KB.
HTTPS Certificate	Select an HTTPS certificate from the dropdown menu.
HTTP Strict Transport Security (HSTS) Expiry	Enable or disable HSTS enforcement, to avoid SSL sniffing attacks, and set an expiry from 0 to 730 days (where 0 means no expiry, maximum of two years). The default is set to 180.
Allow all hosts/domain names	Enable to allow all the hosts/domain names.
Additional allowed hosts/domain names	Specify any additional hosts that this site can serve, separated by commas or line breaks. This option is only available when **Allow all hosts/domain** names is disabled.
Public IP/FQDN for FortiToken Mobile	Enter the IP, or FQDN, of the FortiAuthenticator for external access. The mobile device running the FortiToken Mobile app requires access to the FortiAuthenticator interface for push to operate. Enter the IPs/FQDNs in the following format: `ip_addr[:port]` or `FQDN[:port]`
Cross-Origin Resource Sharing (CORS)	A website should use CORS (Cross-Origin Resource Sharing) to enable secure and controlled access to its resources from different origins, enhancing functionality and security by allowing or blocking requests from specific domains, while mitigating risks from cross-site scripting (XSS) attacks. From the following options specify how to handle Cross-Origin Resource Sharing (CORS): • **None**: No cross-origin allowed. • **Any**: All cross-origins allowed (default). • **Selective**: Specify a list of allowed cross-origin URIs. **Note**: When an HTTP request contains the Origin header, FortiAuthenticator works in accordance with the configured administrative option and the CORS specification.
Inbound Proxy	

	End-user source IP origin when going through a proxy (in order of priority)		
	Get proxy IP from FORWARDED HTTP header (if available)	Enable to get the proxy IP address from the FORWARDED HTTP header when available.	
		Configure valid FORWARDED "by" values	Enable to specify a list of valid "by" identifiers for the FORWARDED header, separated by a comma or a new line. This determines the client IP address used while logging in and can be used to determine if a proxy IP address is trusted in some security features (e.g. trusted subnets for SAML IdP and admin GUI access and user portal adaptive authentication, etc). **Note:** This option provides a way to select the correct source IP address in case of a chain of inbound proxy. It also provides additional protection against spoofing.
	Get proxy IP from X_FORWARDED_FOR HTTP header (if available)	Enable to get the proxy IP address from the X-FORWARDED_FOR HTTP (non-standard equivalent of FORWARDED+ "for") header when available. **Note:** When **Get proxy IP from FORWARDED HTTP header (if available)** and **Get proxy IP from X_FORWARDED_FOR HTTP header (if available)** options are enabled, FortiAuthenticator looks for a matching "FORWARDED" header and only uses the "X_FORWARDED_FOR" header if a valid "FORWARDED" header is not present.	

3. Select **Save** to apply any changes.
   See Certificate management on page 287 for more information about certificates.

The administrator must log in with their username only, i.e., `username + realm` is no longer accepted.

High availability

Multiple FortiAuthenticator units can operate as a high availability (HA) cluster to provide even higher reliability.

There are three HA roles:

1. Cluster member
2. Standalone primary
3. Load-balancer

The FortiAuthenticator can operate in two separate HA modes:

1. **Cluster:** Active-passive clustered fail-over mode where all of the configuration is synchronized between the devices.
2. **Load-balancing:** Active-active HA method in which one device acts as the standalone primary with up to ten additional, geographically separated load-balancers. The load can be distributed across the devices using round-robin DNS, Auth/NAS client load distribution, or external load balancing devices. Load-balancing mode is intended

for two-factor authentication deployments, as only a subset of the configuration is synchronized between the devices.

Both HA modes can be combined with an HA cluster acting as a standalone primary for geographically distributed load-balancers.

If an HA cluster is configured on an interface (such as port 2) and then disabled, it will not be possible to re-enable HA.

This is because, when disabled, the interface's IP address is reconfigured to the interface to allow the administrator to access the newly standalone device. To ensure the port is available for use again in a HA cluster, the IP address must be manually removed.

AES encryption is used in load-balancing (active-active) and cluster (active-passive) modes.

Cluster member role

In the cluster member role, one unit is active and the other is on standby. If the active unit fails, the standby unit becomes active. The cluster is configured as a single authentication server on your FortiGate units.

Authentication requests made during failover from one unit to another are lost, but subsequent requests are completed normally. Depending on the state of the primary cluster when the failover occurs, the failover process may take between 30 to 180 seconds to complete.

Cluster mode uses Ethernet broadcasts through UDP/720 as part of its primary/secondary election mechanism and for ongoing communication. Layer 2 connectivity is required between the two devices in an HA cluster, preferably via a crossover cable, as some network devices might block such Ethernet broadcasts.

Layer 2 connectivity (broadcast packets) is mandatory for discovering the other node in an HA-A-P cluster.

To configure FortiAuthenticator HA:

1. On each unit, go to **System > Administration > High Availability**.
2. Enter the following information:

Enable HA	Enable HA.
Role	Select **Cluster member**. For more information about the other options, see Standalone Primary and Load Balancer role below.
Maintenance Mode	Enable to put the FortiAuthenticator unit of an HA cluster into maintenance mode to remove it from the cluster. Upon entering maintenance mode, if the FortiAuthenticator unit is the active member, it relinquishes the active role and assumes a standby role. While in maintenance mode, the FortiAuthenticator will continue to monitor the status of its HA pair and announce its presence.

	When set to **Enabled with synchronization**, the FortiAuthenticator continues to keep its configuration synchronized with the active member. When set to **Enabled without synchronization**, the FortiAuthenticator stops synchronizing its configuration with the active member.
Interface	Select a network interface to use for communication between the cluster members. This interface must not already have a IP address assigned and it cannot be used for authentication services. Both units must use the same interface for HA communication.
Cluster member IP address	Enter the IP address this unit uses for HA-related communication with the other FortiAuthenticator unit. The units must have different addresses. Usually, you should assign addresses on the same private subnet.
HA admin access	Select the types of administrative access to allow from: **SSH**, **HTTPS**, **GUI**, **REST API**, **Fabric**, **HTTP**, and **SNMP**.
Priority	Set to **Low** on one unit and **High** on the other. Normally, the unit with **High** priority is the active member.
Priority override	Select from the following two options: • **Favor healthy high priority node**: If the low priority node is active, failover to the high priority node whenever it becomes available. • **Minimize HA failovers**: If the low priority node is active, do not failover to the high priority node until the low priority node becomes unavailable.
Password	Enter a string to use as a shared key for IPsec encryption. This must be the same on both units.
Load Balancers	Add the other load-balancing cluster members by entering their IP addresses.
Monitored interfaces	Enable the interfaces you want to monitor. When specifying one or more monitored interfaces, FortiAuthenticator considers their Ethernet link status in the decision algorithm to determine the active/passive role of each FortiAuthenticator node in a primary cluster. The number of monitored interfaces with link status "up" takes precedence over the priority setting to decide which FortiAuthenticator node assumes the active role.
Monitored interfaces stability period	Define the stability period for the monitored interfaces in seconds, between 0-3600 (or one hour). The default is set to `30`.
Default Gateway	Select from the following two options: • **Use Static Routing table** • **Override Static Routing default gateway for HA management interface (this cluster member only; not replicated)**: In **Node-Specific Default Gateway**, enter the default gateway for the current node. **Note**: The **Default Gateway** setting is required if the HA management port has a different default gateway than the one specified in the static routes. Typically, this is done on the low priority primary node if not colocated with the high priority node.

Heartbeat interval	Number of milliseconds between each HA heartbeats sent to the other primary cluster member. The default value is 1000 milliseconds.
Heartbeat lost threshold	Number of consecutive heartbeats from the other primary cluster member that must be missed before declaring it out-of-service. The standby unit uses this measure to trigger a failover. The default value is 6.

The Priority setting is a static value. It allows the administrator to specify which unit to elect as the active member when both units are working equally well (i.e. in a failover situation, the "high priority" setting will not be transferred to the new active member).

- If both units are healthy, the one with high priority will be elected as the active member.
- If the high priority active member goes down, the low priority unit becomes the active member.
- When the low priority member is active and the high priority member comes back online, the high priority member assigns the standby role and syncs from the low priority active member. If the high priority member is synced and remains stable for around five minutes, it takes over and becomes the active member again.
- When the low priority member is active because of an issue with a monitored interface on the high priority member and the high priority member has remained synced with the low priority member, then if the monitored interface status comes back to normal and remains so for the configured monitored interface stability period, the high priority member takes over and becomes the active member again.

3. Select **OK** to apply the settings.

When one unit has become the active member, reconnect to the GUI and complete your configuration. The configuration will automatically be copied to the standby member.

Standalone Primary and Load Balancer role

The load-balancing HA method enables active-active HA across geographically separated locations and Layer 3 networks.

Only the following authentication related features can be synchronized:

- *Users, Groups, FortiTokens, Certificates, MAC devices* (always enabled and read-only)
- *Realms*
- *Remote Auth. Servers*
- *Trusted Subnets*

Trusted Subnets controls the synchronization of trusted subnets and adaptive MFA rules.

- *SAML IdP*
- *RADIUS Service*

- *OAuth Service*
- *TACACS+ Service*
- *Replacement Messages (SAML IdP & OAuth service only)*

  Note: Replacement messages for SAML IdP or OAuth can only be activated when SAML IdP or the OAuth service is enabled.

Other features, such as FSSO cannot be synchronized between devices.

The current synchronization status of the standalone primary to load-balancers can be viewed at **Dashboard > HA Status**.

The standalone primary is the primary system where users, groups, and tokens are configured. Load-balancers are synchronized to the standalone primary device.

To improve the resilience of the primary system, an active-passive cluster with up to ten load-balancing devices can be configured.

To configure load-balancing HA:

1. On each unit, go to **System > Administration > High Availability**.
2. Enter the following information:

Enable HA	Enable HA.
Role	Select **Standalone Primary** on the primary device, and **Load Balancer** on the load-balancing device(s).
Load Balancing primary IP address	On the load-balancing device(s), enter the management IP of the Primary member unit.
Password	Enter a string to use as a shared key for IPsec encryption. This must be the same on both units.
Load Balancers	On the standalone primary unit, enter IP address or IP addresses of the load-balancing devices. Up to ten can be added.
Synced settings (load-balancing)	On the standalone primary unit, choose groups of items which you would like to synchronize over to the LB node.

3. Select **Save** to apply the settings.

Administrative access to the HA cluster

Administrative access is available through any of the network interfaces using their assigned IP addresses or through the HA interface using the **Cluster member IP address**, assigned on the **System > Administration > High Availability** page. In all cases, administrative access is available only if it is enabled on the interface.

Administrative access through any of the network interface IP addresses connects only to the active cluster member. The only administrative access to the standby cluster member is through the HA interface using the standby member's **Cluster member IP address**.

Configuration changes made on the active member are automatically pushed to the standby member. The standby member does not permit configuration changes, but you might want to access the unit to change HA settings, or for firmware upgrades, shutdown, reboot, or troubleshooting.

FortiAuthenticator VMs used in a HA cluster each require a license. Each license is tied to a specific IP address. In an HA cluster, all interface IP addresses are the same on the units, expect for the HA interface.

Request each license backed on either the unique IP address of the unit's HA interface or the IP address of a non-HA interface which is the same on both units.

If you disable and then re-enable HA operation, the interface that was assigned to HA communication will not be available for HA use. You must first go to **System > Network > Interfaces** and delete the IP address from that interface.

Restoring the configuration

When restoring a configuration to an HA active cluster member, the active member reboots and in the interim the standby member is promoted to the role of active member. When the previous active member returns to service, it becomes a standby member and the existing active member overwrites its configuration, defeating the configuration restore. To avoid this, use the following process when restoring a configuration:

1. Shutdown the standby unit.
2. Restore the configuration on the active member.
3. Wait until the active member is back online.
4. Turn on standby member – it will synchronize to the restored configuration after booting up.

Firmware upgrade

For a stable HA configuration, all units in an HA cluster must be running the same firmware version, and have the same sized license for HA devices.

When upgrading the firmware on FortiAuthenticator devices in an HA cluster, you can perform a coordinated upgrade of both cluster members. During the coordinated upgrade, the cluster upgrades the standby device and then the active device to run the new firmware image. The firmware upgrade takes place without interrupting communication through the cluster. This firmware upgrade method can only be initiated from the active member of the cluster.

The following sequence describes the steps the cluster goes through during a coordinated firmware upgrade.

1. The administrator initiates the firmware upgrade from the active member.
2. The firmware image transfers to the standby member.
3. The firmware upgrades on the standby member.
4. The standby member reboots and synchronizes with the active member.
5. The firmware upgrade begins on the active member. The standby member becomes the new active cluster member.
6. The former active member reboots and synchronizes with the new active member.
7. The former active member becomes the active device, and the former standby member becomes the standby device.

If you want to perform the firmware upgrade on each FortiAuthenticator cluster member individually, specific steps must be taken to ensure that the upgrade is successful:

1. Start the firmware upgrade on the active member. See Upgrading the firmware on page 25.
   The device reboots. While the active member device is rebooting, the standby member becomes the active member.
2. Start the firmware upgrade on the new active member (former standby device).
   The device reboots. After both devices have rebooted, the original active member becomes the active device, while the standby member returns to being the standby device.

If a situation arises where both devices are claiming to be the active cluster member due to a firmware mismatch, and the HA port of the device that is intended to be the standby member cannot be accessed (such as when a crossover cable is used), use the following steps:

1. Shutdown the active cluster member to which you have access, or, if physical access to the unit is not available to turn it back on, reboot the device. See System information widget.
   Note that, if rebooting the device, **Step 2** below must be completed before the device finishes rebooting, which can be as short as 30 seconds.
2. With the previously inaccessible device now accessible, upgrade its firmware to the required version so that both devices have the same version.
   The device reboots.
3. If you shutdown the device in **Step 1**, power it back on.
   After both devices are back online, they assume the HA roles dictated by their respective HA priorities.

Firmware upgrade

The FortiAuthenticator firmware can be upgraded from **System > Administration > Firmware**, the CLI via FTP/TFTP, or through the **System Information** widget on the dashboard (see System information widget on page 35).

For instructions on upgrading the device's firmware, see Upgrading the firmware on page 25.

Upgrade history

The upgrade history of the device is shown under the **Upgrade History** heading in the **Firmware Upgrade or Downgrade** pane. It displays the version that was upgraded to, the time and date that the upgrade took place, and the user that performed the upgrade. This information can be useful when receiving support to identify incorrect upgrade paths that can cause stability issues.

Always review all sections in the FortiAuthenticator Release Notes prior to upgrading your device.

Configuring auto-backup

You can configure the FortiAuthenticator to automatically perform configuration back ups to an FTP or SFTP server.

Even though the backup file is encrypted to prevent tampering, access to the FTP server should be restricted. This configuration file backup includes both the CLI and GUI configurations of FortiAuthenticator. The backed-up information includes users, user groups, FortiToken device list, authentication client list, LDAP directory tree, FSSO settings, remote LDAP and RADIUS, and certificates.

To configure automatic backups, go to **System > Administration > Config Auto-backup**.

Enter the following information, and then select **Save** to apply the settings:

Enable configuration auto-backup		Enable the configuration of automatic configuration backups.
	Frequency	Select the automatic backup frequency: **Hourly**, **Daily**, **Weekly**, or **Monthly**.
	Backup time	Entire a time, select **Now**, or select the clock icon to set the scheduled time for backups to occur. Note that this options is not available when the frequency is set to hourly.
	FTP directory	Enter the FTP directory where the backup configuration files are saved to.
	FTP server	Select the FTP server to which the backup configuration files are saved to. See FTP servers on page 66 for information on adding FTP servers.
	Secondary FTP server	Select a secondary FTP server.
	Encryption	Enable and enter a password to encrypt the backup file.

SNMP

Simple Network Management Protocol (SNMP) enables you to monitor hardware on your network. You can configure the hardware, such as the FortiAuthenticator SNMP agent, to report system information and send traps (alarms or event messages) to SNMP managers. An SNMP manager, or host, is typically a computer running an application that can read the incoming trap and event messages from the agent, and send out SNMP queries to the SNMP agents.

By using an SNMP manager, you can access SNMP traps and data from any FortiAuthenticator interface configured for SNMP management access. Part of configuring an SNMP manager is listing it as a host in a community on the FortiAuthenticator device it will be monitoring. Otherwise, the SNMP monitor will not receive any traps from that device, or be able to query that device.

The FortiAuthenticator SNMP implementation is read-only. SNMP v1, v2c, and v3 compliant SNMP managers have read-only access to system information through queries and can receive trap messages from FortiAuthenticator.

To monitor FortiAuthenticator system information and receive FortiAuthenticator traps, your SNMP manager needs the Fortinet and FortiAuthenticator Management Information Base (MIB) files. A MIB is a text file that lists the SNMP data objects that apply to the monitored device. These MIBs provide information that the SNMP manager needs to interpret the SNMP trap, event, and query messages sent by FortiAuthenticator SNMP agent.

The Fortinet implementation of SNMP includes support for most of RFC 2665 (Ethernet-like MIB) and most of RFC 1213 (MIB II). RFC support for SNMP v3 includes Architecture for SNMP Frameworks (RFC 3411), and partial support of User-based Security Model (RFC 3414).

SNMP traps alert you to important events that occur, such as overuse of memory or a high rate of authentication failures.

SNMP fields contain information about FortiAuthenticator, such as CPU usage percentage or the number of sessions. This information is useful for monitoring the condition of the unit on an ongoing basis and to provide more information when a trap occurs.

Configuring SNMP

Before a remote SNMP manager can connect to the Fortinet agent, you must configure one or more interfaces to accept SNMP connections by going to **System > Network > Interfaces**. Edit the interface, and under **Admin access**, enable **SNMP**. See Network on page 41.

You can also set the thresholds that trigger various SNMP traps. Note that a setting of zero disables the trap.

To configure SNMP settings:

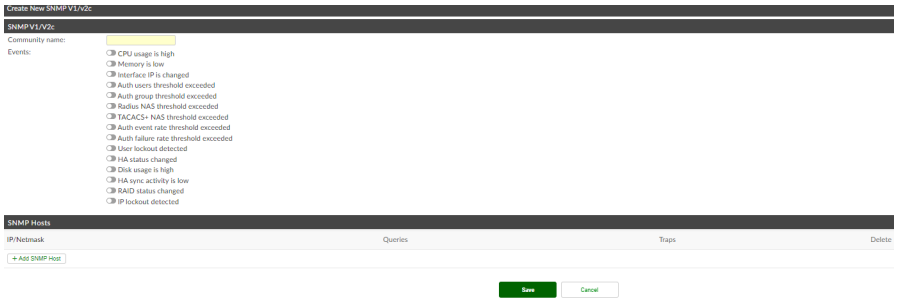
1. Go to **System > Administration > SNMP** and select the **Settings** icon.
2. Enter the following information:

SNMP Contact	Enter the contact information for the person responsible for this FortiAuthenticator unit.
SNMP Description	Enter descriptive information about FortiAuthenticator.
SNMP Location	Enter the physical location of FortiAuthenticator.
User Table Nearly Full Trap Threshold	The user table is nearly full. The threshold is a percentage of the maximum permitted number of users.
User Group Table Nearly Full Trap Threshold	The user group table is nearly full. The threshold is a percentage of the maximum permitted number of user groups.
RADIUS Authentication Client Table Nearly Full Trap Threshold	The RADIUS authenticated client table is nearly full. The threshold is a percentage of the maximum permitted number of RADIUS clients.
TACACS+ Authentication Client Table Nearly Full Trap Threshold (%)	The TACACS+ authentication client table is nearly full. The threshold is a percentage of the maximum permitted number of TACACS+ clients.
Authentication Event Rate Over Limit Trap Threshold	High authentication load. The threshold is the number of authentication events over a five minute period.
Authentication Failure Rate Over Limit Trap Threshold	High rate of authentication failure. The threshold is the number of authentication failures over a five minute period.
CPU Utilization Trap Threshold (%)	High load on CPU. The default is set to 90%.
Disk Utilization Trap Threshold (%)	Disk usage is high. The default is set to 80%.
Memory Utilization Trap Threshold (%)	Too much memory used. The default is set to 90%.

3. Select **Save** to apply the changes.

To create a new SNMP community:

1. Go to **System > Administration > SNMP.**
2. Select **Create New** under **SNMP v1/v2c**. The **Create New SNMP V1/v2c** window opens.



3. Enter the following information in the **SNMPv1/v2c** section:

Community name	The name of the SNMP community.
Events	Select the events for which traps are enabled. Options include: • CPU usage is high • Memory is low • Interface IP is changed • Auth users threshold exceeded • Auth group threshold exceeded • Radius NAS threshold exceeded • TACACS+ NAS threshold exceeded • Auth event rate threshold exceeded • Auth failure rate threshold exceeded • User lockout detected • HA status is changed • Power Supply Unit failure The Power Supply Unit failure event is available with hardware units that support the Power Supply Monitor widget. See Power supply monitor widget on page 41. • Disk usage is high • HA sync activity is low • RAID status changed

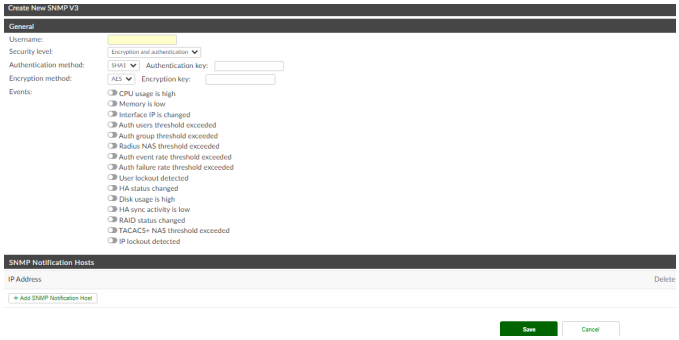
4. In **SNMP Hosts**, select **Add another SNMP Host** and enter the following information:

IP/Netmask	Enter the IP address and netmask of the host.
Queries	Select if this host uses queries.
Traps	Select if this host uses traps.
Delete	Select to delete the host.

5. Select **Save** to create the new SNMP community.

To create a new SNMP user:

1. Go to **System > Administration > SNMP**.
2. Select **Create New** under **SNMP v3**. The **Create New SNMP V3** window opens.



3. Enter the following information in the **General** section:

Username	The name of the SNMP user.
Security level	Select the security level from the dropdown menu: • **None**: No authentication or encryption. • **Authentication only**: Select the **Authentication method** then enter the authentication key in the **Authentication key** field. • **Encryption and authentication**: Select the **Authentication method**, enter the authentication key in the **Authentication key** field, then select the **Encryption method** and enter the encryption key in the **Encryption key** field. This option is set by default.
Events	Select the events for which traps are enabled. See Events on page 60.

4. In **SNMP Notification Hosts**, select **Add another SNMP Notification Host** and enter the following information:

IP/Netmask	Enter the IP address and netmask of the notification host.
Delete	Select to delete the notification host.

5. Select **Save** to create the new SNMP V3 user.

To download MIB files:

1. Go to **System > Administration > SNMP** and select **Settings**.
2. Under **FortiAuthenticator SNMP MIB**, select the MIB file you need to download, options include the FortiAuthenticator MIB and Fortinet Core MIB files.

Licensing

FortiAuthenticator-VM supports two licensing models:

- **Perpetual**

  A one-time purchase license that does not expire. It is based on the VM and allows stacking user capacity starting from 100 users (`FAC-VM-Base`).

  Additional user capacity can be added by stacking licenses.

Support services such as firmware updates and technical support are purchased separately.

Use Case: Ideal for organizations that prefer a capital expenditure (CapEx) model with fixed, long-term licensing and no recurring subscription fees.

- **Subscription license**

  A term-based license billed per user and includes support services as part of the subscription.

  Subscription licenses require connectivity to FortiGuard for entitlement validation.

  If the subscription expires, authentication services stop, but the administrator can still access the GUI for troubleshooting.

  In HA environments, both active and passive units require separate subscription licenses, and mixing perpetual and subscription licenses is not supported.

  See Subscription VM license on page 63.

  Use Case: Best for organizations that prefer an operational expenditure (OpEx) model with bundled support and the flexibility to scale per user.

For detailed ordering information, see the FortiAuthenticator Ordering Guide.

FortiAuthenticator-VM works in evaluation mode until it is licensed. In evaluation mode, only a limited number of users can be configured on the system. To expand this capability, a stackable license can be applied to the system to increase both the user count, and all other metrics associated with the user count.

When a license is purchased, a registration code is provided. Go to support.fortinet.com and register your device by entering the registration code. You are asked for the IP address of your FortiAuthenticator device, and are then provided with a license key.

Ensure that the IP address specified while registering your unit is configured on one of the device's network interfaces, then upload the license key to your FortiAuthenticator-VM.

The **License Information** widget shows the current state of the device license.

See License information widget on page 39.

To license FortiAuthenticator:

1. Register your device at the Fortinet Support website.
2. Ensure that one of your device's network interfaces is configured to the IP address specified during registration.
3. Go to **System > Administration > Licensing**.
4. Select **Upload a File** and locate the license file you received from Fortinet.
5. Select **Upload**.

FortiAuthenticator licenses

FortiAuthenticator licenses include the following components:

- Maximum number of users (FortiAuthenticator-VM models only).
- Maximum number of SSO Mobility Agent clients (all models).
- Expiry date (trial licenses only; full licenses are perpetual).

FortiAuthenticator-VM licenses with user limits:

FortiAuthenticator-VM licenses include a user limit which applies to:

- The number of user accounts configured on the FortiAuthenticator (local and remote users combined).

- The number of concurrent FSSO sessions.
- The maximum limits on all other configuration objects are derived as a ratio to the maximum number of users.

SSO Mobility Agent (SSOMA) client limits:

The SSOMA client component is only required for scenarios where you are doing FSSO with SSOMA clients. It determines how many SSOMA clients can concurrently have active FSSO sessions on the FortiAuthenticator.

The FortiAuthenticator sets the maximum number of SSOMA clients to the lowest of these values from its onboard license:

- Maximum FortiClient SSO
- Maximum users

SSOMA, FTM, and SMS licenses are purchased separately, and these limits do not scale with the FortiAuthenticator license user limit.

Licensing FortiAuthenticator HA units

Primary HA cluster: Each FortiAuthenticator unit is required to have its own license. Both units must have the same license size (users and SSOMA clients).

HA load-balancer: The HA load-balancer needs to have a user license size big enough to be able to replicate the configuration from the primary. While this means a load-balancer could have a smaller license than the primary, administrators must be careful to not undersize load-balancer licenses. The size of the SSOMA license can be different from the primary, depending on which FortiAuthenticator node the SSOMA clients will be connecting to.

Subscription VM license

The subscription license requires FortiAuthenticator version 8.0.0 or above.

Using the following, the administrator can install the subscription VM license:

1. Ensure that FortiAuthenticator can reach `TCP/443` to FQDN `update.fortiguard.net`.
2. Obtain the subscription VM license file from FortiCloud.
3. Go to **System > Administration > Licensing** to upload the subscription VM license file to FortiAuthenticator. To upload a license to FortiAuthenticator, see Licensing on page 61.

   FortiAuthenticator reboots.

   FortiAuthenticator retrieves the subscription VM license entitlements from https://update.fortiguard.net:443.

If a subscription VM license expires, in the FortiAuthenticator:

1. The user license limit is lowered to the unlicensed VM limits.
2. Authentication services are halted.

3. The administrator can still access the administrator UI.

Once the license expires, all the authentication stops.
The administrator can still access the GUI for configuration and troubleshooting.

When FortiAuthenticator is a member of a redundant HA pair:

1. The administrator must install separate subscription VM license file for the active and passive FortiAuthenticator devices.

Mixing perpetual and subscription VM licenses within a redundant HA pair is not supported.

2. The active FortiAuthenticator device retrieves the subscription VM license entitlements from https://update.fortiguard.net:443 for itself and the passive FortiAuthenticator device.
3. If subscription VM license entitlements are different between the active and passive FortiAuthenticator devices, the lower of the two is used.

If you have purchased an add-on SSOMA license for the subscription VM, that entitlement is included within the subscription VM license file.

CLI commands

CLI command	Description
`get system license-info`	Displays the license information.
`diagnose system updated status`	Displays license information fetched from FDN.
`diagnose system updated info`	Displays the updated runtime information.
`diagnose debug application updated <level>`	Set debug level for updated.

FortiGuard

To view and configure FortiGuard connections, go to **System > Administration > FortiGuard**.

The FortiGuard Distribution Network (FDN) page provides information and configuration settings for FortiGuard subscription services.

Communication to FortiCloud services for FortiTokens (FTK, FTM, FTC) management is done over a secure TLS tunnel.
FortiAuthenticator prevents man-in-the-middle attack by verifying that the FortiCloud server certificates are valid and issued by the Fortinet Certificate Authority (CA).
The Fortinet CA is private and safeguarded through highly secure internal controls.

For more information about FortiGuard services, see the FortiGuard web page.

Configure the following settings, then select **Save** to apply them:

FortiGuard Subscription Services		
	Messaging Service	The data to which the messaging service license is valid.
	SMS messages	The total number of allowed SMS messages, and the number of messages that have been used.
FortiGuard Proxy Server		
	Enable FortiGuard proxy server	If enabled, communication with FortiGuard servers will go through this proxy server. Enter the proxy server's address, port, and optionally specify a **Username** and **Password** for user authentication.
FortiToken Hardware Provisioning		
	Server address **Server port**	The server address (set to **update.fortiguard.net** by default) and server port (set to **443** by default).
FortiToken Mobile Provisioning		
	Server address **Server port**	The server address (set to **fortitokenmobile.fortinet.com** by default) and server port (set to **443** by default).
	FTM trial license activation	Option to disable the FortiAuthenticator device's free trial FortiToken Mobile licenses.
FortiGuard Messaging Service		
	Server address **Server port**	The server address (set to **msgctrl1.fortinet.com** by default) and server port (set to **443** by default).

FTM Push credentials for Apple and Google can be updated via FortiGuard without admin user intervention.

FortiGuard cannot send messages longer than 269 characters.

FortiNACs

To view a list of the configured FortiNAC servers, go to **System > Administration > FortiNACs**.

The following information is shown:

Create New	Select to configure a new FortiNAC server (this is the only option available if no FortiNAC servers are configured).
Delete	Select to delete the selected FortiNAC server(s).
Edit	Select to edit the selected FortiNAC server.
Name	The name of the FortiNAC server.

To create a new FortiNAC server:

1. Select **Create New**.
   The **Create New FortiNAC** window opens.
2. Enter the following information:

Name	Enter a name for the FortiNAC server.
IP/FQDN	Enter the IP address or Fully Qualified Domain Name (FQDN) of the FortiNAC server.
Port	Enter the port number.
Password	Enter the FortiNAC server password.

3. Select **Save** to create the new FortiNAC server.

FTP servers

To view a list of the configured FTP servers, go to **System > Administration > FTP Servers**.

The following information is shown:

Create New	Select to create a new FTP server (this is the only option available if no FTP servers are configured).
Delete	Select to delete the selected FTP server(s).
Edit	Select to edit the selected FTP server.
Name	The name of the FTP server.
Server name/IP	The server name or IP address, and port number.

To create a new FTP server:

1. Select **Create New**. The **Create New FTP Server** window will open.
2. Enter the following information:

Name	Enter a name for the FTP server.
Connection type	Select the connection type, either **FTP** or **SFTP**.
Server name/IP	Enter the server name or IP address.
Port	Enter the port number.
Anonymous	Select to make the server anonymous.
Username	Enter the server username (if **Anonymous** is not selected).
Password	Enter the server password (if **Anonymous** is not selected).

3. Select **Save** to create the new FTP server.

Admin profiles

Similar to FortiOS, FortiAuthenticator can incorporate the use of admin profiles. Each administrator can be granted either full permissions or a customized admin profile. Profiles are defined as aggregates of read-only or read/write permission sets. A built-in read-only admin profile is available. The most commonly used permission sets are pre-defined, but custom permission sets can also be created.

To create a new admin profile, go to **System > Administration > Admin Profiles > Create New**. You can give the admin profile a **Name**, a **Description**, and configure the **Permission sets** you want for that particular admin profile.

An administrator is now allowed to edit a guest user account if its admin profile has **Read & Write** access for **Can change guest user**, **Can change password of guest user**, and/or **Can change custom fields of guest user**.

Go to **Authentication > User Management > Local Users**, and select the admin profile to an administrator. You can assign more than one admin profile to each administrator.

NetHSMs

NetHSMs can be configured on the FortiAuthenticator for the purpose of storing the private keys of Local CAs or issuing user and local service certificates with local CAs that have their private keys stored on the HSM.

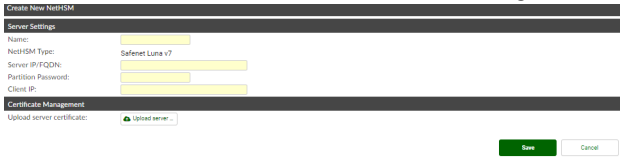
Supported HSM servers currently include *Safenet Luna v7*.

Configuring an HSM server on FortiAuthenticator

Before creating the HSM server on FortiAuthenticator, you must first configure your HSM with an SSH administrator account and key partition.

To configure a new HSM server:

1. Go to **System > Administration > NetHSMs**, and click **Create New**.
2. In the **Create New HSM Server** window, configure the HSM server settings.



Name	The name of the HSM server. This name is for FortiAuthenticator reference purposes only and does not need to match any configuration on the HSM.
HSM Server Type	The HSM type. **Safenet Luna v7** is currently the only supported HSM type.
Server IP/FQDN	The address of the HSM.
Partition Password	The password for the key partition on the HSM.
Client IP	The address of the FortiAuthenticator interface that the HSM can see. For example, if the FortiAuthenticator is behind a NAT device, this should be the NAT'ed address.
Upload server certificate	Upload the server certificate downloaded from your HSM.

3. Click **OK** to complete setup.
You can edit an existing HSM server to download the HSM client certificate, as well as view the server and client Network Trust Link (NTL) certificate fingerprints.

Authorizing FortiAuthenticator as an HSM client

Once your HSM server has been configured, you can authorize FortiAuthenticator as a client on your HSM.

To authorize FortiAuthenticator as a Safenet Luna client:

1. Edit the previously configured HSM server on FortiAuthenticator, and click **Download client certificate**.
Make sure the downloaded certificate uses the **`<FAC IP>.pem`** naming convention. For example: `172.16.68.47.pem`.
2. Upload the client certificate to the Safenet Luna HSM using SCP transfer.
```
scp [certificate filename] admin@[HSM address]:
```
3. Use SSH to connect to the HSM, then register your FortiAuthenticator, and associate it with a partition.
```
ssh -1 admin [HSM address]
client register -c [client name] -ip [client address]
client assignpartition -c [client name] -p [partition name]
```
4. Confirm the status. For example:
```
client show -c my_fac
   ClientID: my_fac
   IPAddress: 172.16.68.47
   Partitions: my_partition
```

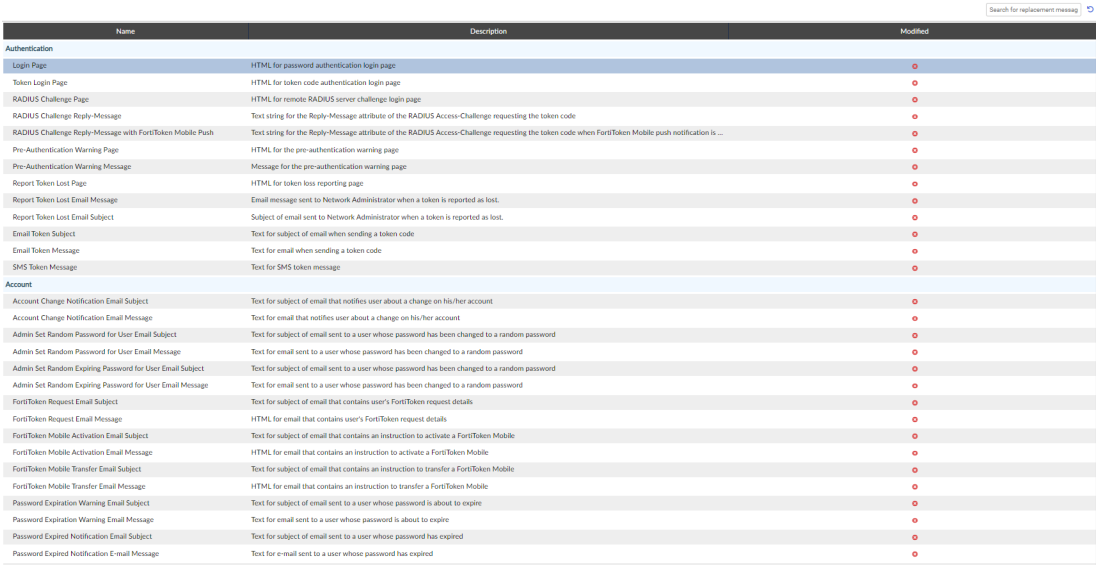
Configuring or importing an HSM CA certificate

After the HSM server has been configured and FortiAuthenticator is authorized as an HSM client, local CA certificates using the HSM can be created or imported at **Certificate Management > Certificate Authorities > Local CAs**. See Local CAs on page 299.

Replacement messages

The replacement messages list lets you view and customize replacement messages.

Go to **System > Administration > Replacement Messages** to view the replacement message list.



Name	Description	Modified
Authentication		
Login Page	HTML for password authentication login page	
Token Login Page	HTML for token code authentication login page	
RADIUS Challenge Page	HTML for remote RADIUS server challenge login page	
RADIUS Challenge Reply-Message	Text string for the Reply-Message attribute of the RADIUS Access-Challenge requesting the token code	
RADIUS Challenge Reply-Message with FortiToken Mobile Push	Text string for the Reply-Message attribute of the RADIUS Access-Challenge requesting the token code when FortiToken Mobile push notification is ...	
Pre-Authentication Warning Page	HTML for the pre-authentication warning page	
Pre-Authentication Warning Message	Message for the pre-authentication warning page	
Report Token Lost Page	HTML for token loss reporting page	
Report Token Lost Email Message	Email message sent to Network Administrator when a token is reported as lost.	
Report Token Lost Email Subject	Subject of email sent to Network Administrator when a token is reported as lost.	
Email Token Subject	Text for subject of email when sending a token code	
Email Token Message	Text for email when sending a token code	
SMS Token Message	Text for SMS token message	
Account		
Account Change Notification Email Subject	Text for subject of email that notifies user about a change on his/her account	
Account Change Notification Email Message	Text for email that notifies user about a change on his/her account	
Admin Set Random Password for User Email Subject	Text for subject of email sent to a user whose password has been changed to a random password	
Admin Set Random Password for User Email Message	Text for email sent to a user whose password has been changed to a random password	
Admin Set Random Expiring Password for User Email Subject	Text for subject of email sent to a user whose password has been changed to a random password	
Admin Set Random Expiring Password for User Email Message	Text for email sent to a user whose password has been changed to a random password	
FortiToken Request Email Subject	Text for subject of email that contains user's FortiToken request details	
FortiToken Request Email Message	HTML for email that contains user's FortiToken request details	
FortiToken Mobile Activation Email Subject	Text for subject of email that contains an instruction to activate a FortiToken Mobile	
FortiToken Mobile Activation Email Message	HTML for email that contains an instruction to activate a FortiToken Mobile	
FortiToken Mobile Transfer Email Subject	Text for subject of email that contains an instruction to transfer a FortiToken Mobile	
FortiToken Mobile Transfer Email Message	HTML for email that contains an instruction to transfer a FortiToken Mobile	
Password Expiration Warning Email Subject	Text for subject of email sent to a user whose password is about to expire	
Password Expiration Warning Email Message	Text for email sent to a user whose password is about to expire	
Password Expired Notification Email Subject	Text for subject of email sent to a user whose password has expired	
Password Expired Notification E-mail Message	Text for e-mail sent to a user whose password has expired	

The replacement messages are divided into seven categories: **Authentication**, **Account**, **Device Certificate Enrollment**, **Password Reset**, **User Registration**, **SAML SP (FSSO)**, and **System**.

To view and customize SAML IdP replacement messages, go to **Authentication > SAML IdP > Replacement Messages**.

The two pre-authentication replacement messages under **Authentication** are only available after pre-authentication has been enabled under **System > Administration > System Access**.

Selecting a specific message will display the text and HTML or plain text of the message in the content pane.

Selecting **Toggle Tag List** will display a table of the tags used for that message atop the message's HTML or plain text box.

To edit a replacement message:

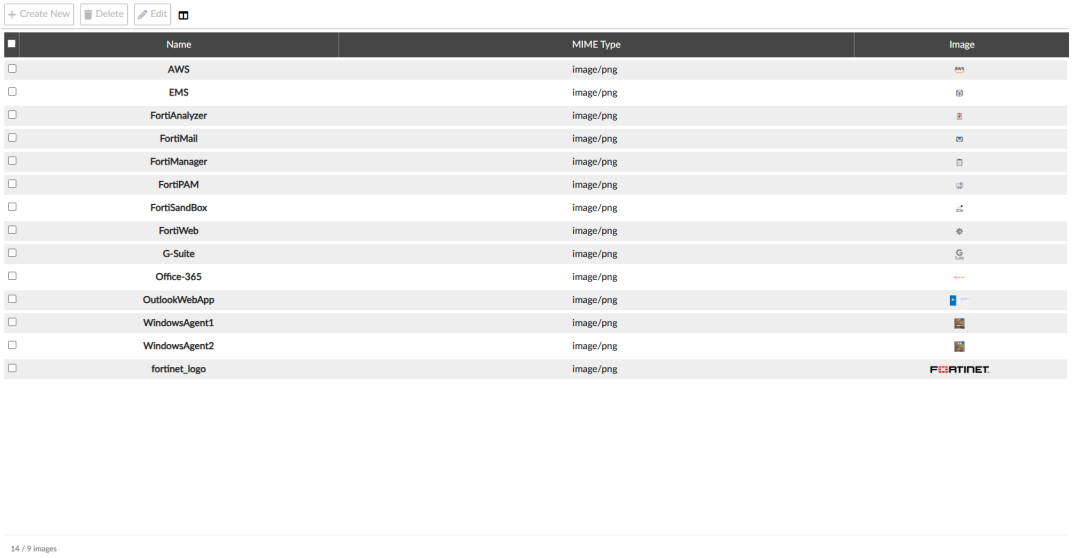
1. Select a message in the replacement message list.
2. Edit the plain text or HTML code in the lower right pane, or select **Detach** to edit the message in a new browser window.

3. When you are finished editing the message, select **Save** to save your changes.
4. If you have made an error when editing the message, select **Restore Default** to restore the message to its default value.

Images

Images can be managed by going to **Images** in **Administration**.

Images can also be added, deleted, and edited.



The following default images are available:

- **AWS**
- **EMS**
- **FortiAnalyzer**
- **FortiMail**
- **FortiManager**
- **FortiPAM**
- **FortiSandBox**
- **FortiWeb**
- **G-Suite**
- **Office-365**
- **OutlookWebApp**
- **WindowsAgent1**
- **WindowsAgent2**
- **fortinet_logo**

To add an image:

1. In **Images**, select **Create New** to open the **Create New Image** window.
2. In the **Name** field, enter a name for the image.

3. Select **Image File**, find the `GIF`, `JPEG`, or `PNG` image file that you want to add, and then select **Upload a file**.
   Note: The maximum image size is 1000 kB.
4. Select **Save**.
   To insert the image into a replacement message, add the following HTML code:

```
<img src={{:image/<image_name>}}>
```

   Where `<image_name>` is the name entered for the image.
   For example, the HTML code for an image named `Acme_logo` is:

```
<img src={{:image/Acme_logo}}>
```

To delete an image:

1. In **Images**, select an image, then select **Delete**.
2. Select **Yes, I'm sure** in the confirmation window to delete the image.

Default images cannot be deleted.

To edit an image:

1. In **Images**, select an image, then select **Edit**.
2. In the **Edit Image** window, edit the image name and file as required.
3. Select **Save** to apply your changes.

Messaging

FortiAuthenticator sends email for several purposes, such as password reset requests, new user approvals, user self-registration, and two-factor authentication.

By default, FortiAuthenticator uses its built-in Simple Mail Transfer Protocol (SMTP) server.

This is provided for convenience, but is not necessarily optimal for production environments.

Fortinet recommends that you configure the unit to use a reliable external mail relay.

There are two distinct email services:

1. **Administrators:** Password reset, new user approval, two-factor authentication, etc.
2. **Users:** Password reset, self-registration, two-factor authentication, etc.

If you plan to send SMS messages to users, you must configure the SMS gateways that you will use.

Ask your SMS provider for information about using its gateway.

The FortiAuthenticator SMS gateway configuration differs according to the protocol your SMS provider uses.

SMTP servers

To view a list of the SMTP servers, go to **System > Messaging > SMTP Servers**.

Although FortiAuthenticator can be configured to send emails from the built-in mail server (localhost), this is not recommended.

Anti-spam methods such as IP lookup, DKIM, and SPF can block mail from such ad-hoc mail servers.

It is highly recommended that email is relayed from an official mail server for your domain.

The following information is shown:

Create New	Select to create a new SMTP server.
Delete	Select to delete the selected SMTP server or servers.
Set as Default	Set the selected SMTP server as the default SMTP server.
Reset table column widths	Select the reset icon to reset the table column widths to default.
Name	The name of the SMTP server.
Server	The server name and port number.
Default	Shows a green circle with a check mark for the default SMTP server. To change the default server, select the server you would like to use as the default, then select **Set as Default** in the toolbar.

To add an external SMTP server:

1. Go to **System > Messaging > SMTP Servers** and select **Create New**.
   The **Create New SMTP Server** window opens.

2. Enter the following information:

Name	Enter a name to identify this mail server on FortiAuthenticator.
Server name/IP	Enter the IP address or Fully Qualified Domain Name (FQDN) of the mail server.
Port	The default port 25. Change it if your SMTP server uses a different port.
SMTP connection timeout value in second	Enter the SMTP connection timeout value, in seconds (default = 5).
Sender name (optional)	Optionally, enter the name that will appear when sending an email from FortiAuthenticator.

Sender email address		In the From field, enter the email address that will appear when sending an email from FortiAuthenticator.
Connection Security and Authentication		Customize the secure connection and authentication for a user.
	Secure connection	For a secure connection to the mail server, select **STARTTLS** from the dropdown menu.
	Enable authentication	Enable if the email server requires you to authenticate when sending email. Enter the **Account username** and **Password** if required.

3. Optionally, select **Test Connection** to send a test email message.
   Specify a recipient and select **Send**.
   Confirm that the recipient received the message.

   The recipient email system might treat the test email message as spam.

4. Select **Save** to create the new SMTP server.

For troubleshooting tips, see Troubleshooting SMTP server tests on page 332.

Email services

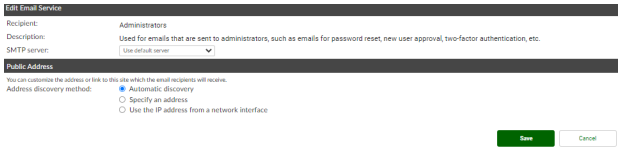
To view a list of the email services, go to **System > Messaging > Email Services**.

The following information is shown:

Save	Select to save any changes made to the email services.
Edit	Select to edit the selected email service.
Reset table column widths	Select the reset icon to reset the table column widths to default.
Recipient	The name of the email recipient.
SMTP server	The SMTP server associated with the recipient. The server can be selected from the dropdown.

To configure email services:

1. Go to **System > Messaging > Email Services** and select the recipient you need to edit (the user email service is shown below).
   The **Edit Email Service** window opens.



2. Configure the following:

SMTP server	Select the SMTP server from the dropdown menu.
Public Address	Customize the address or link for the email.
Address discovery method	Select the address discovery method: • **Automatic discovery**: Use device FQDN if configured, or automatically obtain address from the browser, or an active network interface. • **Specify an address**: Manually enter the address and port number. • **Use the IP address from a network interface**: Select a specific network interface from the dropdown menu.
Address	Enter the recipient IP address or FQDN. Only available if **Address discovery method** is set to **Specify an address**.
Port	Enter the recipient port number (set to 80 by default). Only available if **Address discovery method** is set to **Specify an address**.
Network interface	Select a configured network interface from the dropdown menu. This option is only available when the **Address discovery method** is set to **Use the IP address from a network interface**.

3. Select **Save** to apply your changes.

SMS gateways

To view a list of the configured SMS gateways, go to **System > Messaging > SMS Gateways**.

The following information is shown:

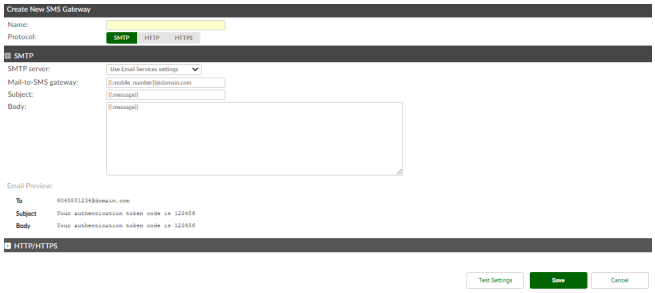
Create New	Select to create a new SMS gateway.
Delete	Select to delete the selected SMS gateway or gateways.
Set as Default	Set the selected SMS gateway as the default SMS gateway.
Reset table column widths	Select the reset icon to reset the table column widths to default.
Name	The name of the SMS gateway.
Protocol	The protocol used by the gateway.
SMTP Server	The SMTP server associated with the gateway.
API URL	The gateway API URL, if it has one.
Default	Shows a green circle with a check mark for the default SMS gateway. To change the default gateway, select the gateway you would like to use as the default, then select **Set as Default** in the toolbar.

You can also configure the message that you will send to users. You can use the following tags for user-specific information:

Tag	Information
{{:country_code}}	Telephone country code, e.g., 01 for North America.
{{:mobile_number}}	User's mobile phone number.
{{:message}}	"Your authentication token code is" and the code.
{{:null}}	Empty string or null value.

To create a new SMTP SMS gateway:

1. Go to **System > Messaging > SMS Gateways** and select **Create New**.
   The **Create New SMS Gateway** window opens.



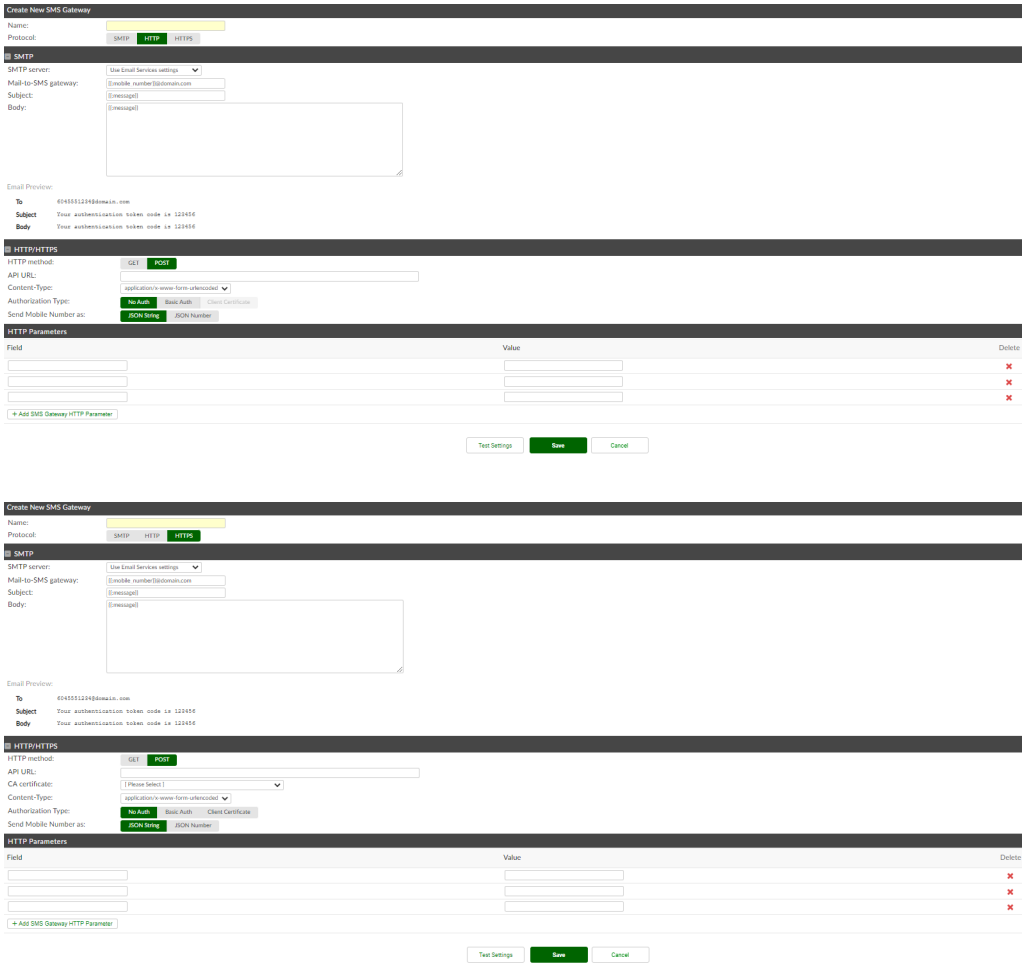
2. Enter the following information:

Name		Enter a name for the new gateway.
Protocol		Select **SMTP**.
SMTP server		Select the SMTP server you use to contact the SMS gateway. The SMTP server must already be configured, see SMTP servers on page 72.
Mail-to-SMS gateway		Change `domain.com` to the SMS provider's domain name. The default entry `{{:mobile_number}}@domain.com` assumes that the address is the user's mobile number followed by **@** and the domain name. In the **Email Preview** section, check the **To** field to ensure that the format of the address matches the information from your provider.
Subject		The subject for the email.
Body		The email message.
Email Preview		View a preview of the email message.
	To	Format of the email address, as determined by the **Mail-to-SMS gateway** field.
	Subject	Optionally, enter a subject for the message.
	Body	Optionally, enter body text for the message.

3. Optionally, select **Test Settings** to send a test SMS message to the user.
4. Select **Save** to create a new SMTP SMS gateway.

To create a new HTTP or HTTPS SMS gateway:

1. Go to **System > Messaging > SMS Gateways** and select **Create New**.
   The **Create New SMS Gateway** window opens.



2. Expand the **HTTP/HTTPS** section, then enter the following information:

HTTP/HTTPS	
HTTP method	Select the method to use, either **GET** or **POST**.
API URL	Enter the gateway URL, omitting the protocol prefix `http://` or `https://`. Also omit the parameter string that begins with `?`.
CA certificate	Select CA certificate that validates this SMS provider from the dropdown menu.
Content-Type	Select a content type from the dropdown menu.
Authorization Type	Enter the **Username** and **Password** for **Basic Auth**. For **Client Certificate**, use the dropdown to select a client certificate.
Send Mobile Number as	Select the format to use, either **JSON String** or **JSON Number**. This option is only available when the **Content-Type** is **application/json**.

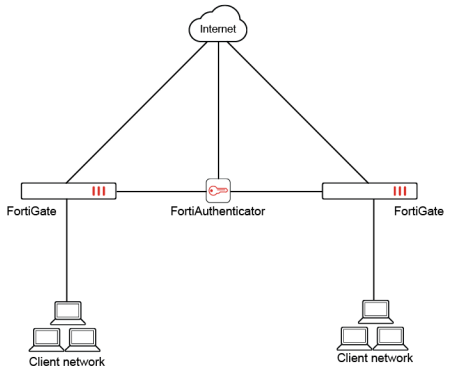
HTTP Parameters	
Field	Enter the parameter names that the SMS provider's URL requires, such as `user` and `password`.
Value	Enter the values or tags corresponding to the fields.
Delete	Delete the field and its value.

3. If you need more parameter entries, select **Add another SMS Gateway HTTP Parameter.**
4. Optionally, select **Test Settings** to send a test SMS message to the user.
5. Select **Save** to create a new HTTP or HTTPS SMS gateway.

Authentication

FortiAuthenticator provides an easy to configure authentication server for your users. Multiple FortiGate units can use a single FortiAuthenticator unit for remote authentication and FortiToken device management.

FortiAuthenticator in a multiple FortiGate unit network



What to configure

You need to decide which elements of the FortiAuthenticator configuration you need:

- Determine the type of authentication you will use: password-based or token-based.
  Optionally, you can enable both types. This is called two-factor authentication.
- Determine the type of authentication server you will use: RADIUS, TACACS+, built-in LDAP, or Remote LDAP.
  You will need to use at least one of these server types.
- Determine which FortiGate units or third-party devices will use the FortiAuthenticator.
  The FortiAuthenticator must be configured on each FortiGate unit as an authentication server, either RADIUS or LDAP.
  For RADIUS authentication, each FortiGate or third-party device must be configured on the FortiAuthenticator as an authentication client.

Password-based authentication

User accounts can be created on the FortiAuthenticator device in multiple ways:

- Administrator creates a user and specifies their username and password.
- Administrator creates a username and a random password is automatically emailed to the user.
- Users are created by importing either a CSV file or from an external LDAP server.

Users can self-register for password-based authentication.

This reduces the workload for the system administrator.

Users can choose their own passwords or have a randomly generated password provided in the browser or sent to them via email or SMS.

Self-registration can be instant, or it can require administrator approval.

See Self-service portal policies on page 154.

Once created, users are automatically part of the RADIUS Authentication system and can be authenticated remotely.

See User management on page 94 for more information about user accounts.

Two-factor authentication

Two-factor authentication increases security by requiring multiple pieces of information on top of the username and password.

There are generally two factors:

- Something the user knows, usually a password,
- Something the user has, such as a FortiToken device.

Requiring the two factors increases the difficulty for an unauthorized person to impersonate a legitimate user.

To enable two-factor authentication, configure both password-based and token-based authentication in the user's account.

FortiAuthenticator token-based authentication requires the user to enter a numeric token, or one-time password (OTP), at login.

Two types of numerical tokens are supported:

- **Time-based (TOTP):** The token passcode is generated using a combination of the time and a secret key which is known only by the token and the FortiAuthenticator device.
  The token password changes at regular time intervals, and FortiAuthenticator is able to validate the entered passcode using the time and the secret seed information for that token.
  Passcodes can only be used a single time (one time passcodes) to prevent replay attacks. Fortinet has the following time based tokens:
  - FortiToken hardware
  - FortiToken Mobile, running on a compatible smartphone

For more information about TOTP, see RFC 6238.

- **Event-based or HMAC-based (HOTP):** The token passcode is generated using an event trigger and a secret key. Event tokens are supported using a valid email account and a mobile phone number with SMS service.
  FortiToken devices, FortiToken Mobile apps, email addresses, and phone numbers must be configured in the user's account.
  For more information about HOTP, see RFC 4226.
  Only the administrator can configure token-based authentication.
  See Configuring One-Time Password (OTP) authentication on page 101.

Two-factor token and password concatenation

Concatenated passwords and one-time password (OTP) codes can be provided by the client in the password field so that there is no second step to enter an OTP code.

This is supported by all authentication methods on the FortiAuthenticator that also support password-only authentication.

See Authentication methods.

One-time activation protection for FortiToken on-boarding

One-time activation minimizes the risk of a bad actor stealing a token provisioned to an end-user.

FortiToken Mobile software tokens

End-users receive an activation code as text and QR code to install the FortiToken Mobile token in the FortiToken Mobile application. The activation code is used to request a token seed for a previously provisioned token and does not contain the token seed. The activation window, during which the activation code is valid, is configurable. When the end-user activates the token, the FortiToken Mobile application sends a unique device fingerprint (device Id) to the FortiGuard FortiToken Mobile server. This device Id binds the token to the device by serving as a critical material to encrypt the token seed. Therefore, only that device can decrypt the seed after it is installed. This prevents a “backup and restore” or cloning attack on the token seed.

Further, the FortiGuard FortiToken Mobile server will only honor a successive activation request if the device Id matches the one sent in the original activation request and is within the activation window. This guarantees that the FortiToken Mobile activation codes cannot be reused, and tokens cannot be stolen if the activation code is somehow leaked after the token is installed. Suppose an attacker intercepts the activation code and tries to activate the token before the intended user can. In that case, the intended user will know since they cannot activate that token on their mobile device and will report the issue.

FortiToken Hardware tokens

Standard FTK200B tokens are activated from the server device console or GUI by requesting the token seed from the secure FortiGuard FTK Activation Service. FortiGuard records the identity of the device from which token activation request originated. Thereafter, requests to activate the same token, as identified by the token Serial Number, will only be allowed from the server device on which it was originally activated.

Authentication servers

FortiAuthenticator has built-in RADIUS and LDAP servers. It also supports the use of remote RADIUS and LDAP (which can include Windows AD servers).

The built-in servers are best used where there is no existing authentication infrastructure, or when a separate set of credentials is required. You build a user account database on FortiAuthenticator. The database can include additional user information such as street addresses and phone numbers that cannot be stored in a FortiGate unit’s user

authentication database. To authenticate, either LDAP or RADIUS can be used. The remote LDAP option adds your FortiGate units to an existing LDAP structure. Optionally, you can add two-factor authentication to remote LDAP.

RADIUS

If you use RADIUS, you must enable RADIUS in each user account.

FortiGate units must be registered as RADIUS authentication clients under **Authentication > RADIUS Service > Clients**.

See RADIUS service on page 189.

On each FortiGate unit that will use the RADIUS protocol, FortiAuthenticator must be configured as a RADIUS server under **User & Device > RADIUS Servers**.

Built-in LDAP

If you use built-in LDAP, you will need to configure the LDAP directory tree. You add users from the user database to the appropriate nodes in the LDAP hierarchy.

See Creating the directory tree on page 215.

On each FortiGate unit that will use LDAP protocol, FortiAuthenticator must be configured as an LDAP server under **User & Device > LDAP Servers**.

Remote LDAP

Remote LDAP is used when an existing LDAP directory exists and should be used for authentication. User information can be selectively synchronized with FortiAuthenticator, but the user credentials (passwords) remain on, and are validated against the LDAP directory.

To utilize remote LDAP, the authentication client (such as a FortiGate device) must connect to the FortiAuthenticator device using RADIUS to authenticate the user information (see **User & Device > RADIUS Servers**).

The password is then proxied to the LDAP server for validation, while any associated token passcode is validated locally.

Authentication methods

RADIUS and TACACS+ with PAP, user portals, SAML IdP, and REST API:

- End-user password provided to FortiAuthenticator as cleartext.
- Any type of user account (i.e. local or remote) can authenticate.

RADIUS with CHAP/MSCHAPv2:

- End-user password provided to FortiAuthenticator as a hash digest.
- Only local user accounts with passwords stored using reversible cryptography can authenticate.
  See Local user account password storage on page 107

Machine authentication

Machine (or computer) authentication is a feature of the Windows supplicant that allows a Windows machine to authenticate to a network via 802.1X prior to user authentication.

Machine authentication is performed by the computer itself, which sends its computer object credentials before the Windows logon screen appears. User authentication is performed after the user logs in to Windows.

Based on the computer credentials provided during machine authentication, limited access to the network can be granted. For example, access can be granted to just the Active Directory server to enable user authentication.

Following machine authentication, user authentication can take place to authenticate that the user is also valid, and to then grant further access to the network.

Machine authentication commonly occurs on boot up or log out, and not, for example, when a device awakens from hibernation. Because of this, the FortiAuthenticator caches authenticated devices based on their MAC addresses for a configurable period (see User account policies on page 82).

For more information on cached users, see Windows device logins on page 284.

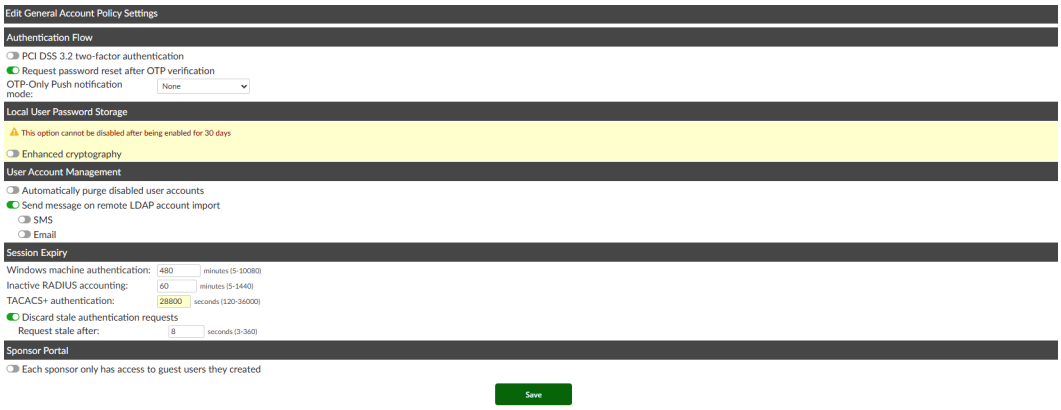
To configure machine authentication, see RADIUS service on page 189.

User account policies

General policies for user accounts include lockout settings, password policies, custom user fields, tokens, trusted subnets, and adaptive MFA rules.

General

To configure general account policy settings, go to **Authentication > User Account Policies > General**.



Configure the following settings:

Authentication Flow

	PCI DSS 3.2 two-factor authentication	Enable to always collect all authentication factors before indicating a success or failure.
	Request password reset after OTP verification	Enable if password reset is required, a change password request is sent once the OTP is verified.
	OTP-Only Push notification mode	Select from the following three options: • **None**: Do not support push notification for OTP-only users (default). • **Normal**: Do push notification for OTP-only users when a push trigger is received and the user account supports push notifications. If the user account does not support push notifications, the authentication request is rejected. • **Forticlient-compatible**: Do push notification for OTP-only users when a push trigger is received and the user account supports push notifications. If the user account does not support push notifications, the authentication request is ignored, which will allow the end-user to manually enter their username and OTP into the FortiClient and get verified through a new authentication request.
Local User Password Storage		
	Enhanced cryptography	When disabled, FortiAuthenticator uses AES256 encryption for local user passwords. When enabled, local user passwords are hashed using bcrypt. With enhanced cryptography, cleartext passwords can no longer be recovered, and authentication requests requiring cleartext passwords for validation will fail. Enhanced cryptography can be disabled within 30 days of being enabled. After 30 days it cannot be disabled. FortiAuthenticator sends an email reminder to the administrator before the end of the 30-day period. Local admin passwords are always hashed using bcrypt. This option cannot be disabled after being enabled for 30 days.
User Account Management		
	Automatically purge disabled user accounts	Enable to automatically purge disabled user accounts. Select the frequency of the purge in the **Frequency** field: **Hourly**, **Daily**, **Weekly**, or **Monthly**. Enter the time of the purge in the **Time** field: **Now** to set the time to the current time, or select the clock icon to choose a time: **Now**, **Midnight**, **6 a.m.**, **Noon**, or **6 p.m**.
	Purge users that are disabled due to the following reasons	Set the reason for purging disabled users: • **Manually disabled** • **Login inactivity** • **Too many login attempts**

		• **Account expired** • **Password expired** • **FTM activation expired** • **Manually disabled by user** • **Usage limit exceeded** • **Not Activated**
	Send message on remote LDAP account import	Enable to send message to the user account when a remote LDAP account is imported. **Note**: When enabled, you can select **Email** and/or **SMS**.
Session Expiry		
	Windows machine authentication	Enter a time after which the login sessions timeout for Windows machine authentication using 802.1.X, from 5 to 10080 minutes (or five minutes to seven days). The default is set to 480 minutes.
	Inactive RADIUS accounting	Enter a time after which RADIUS accounting sessions timeout, from 5 to 1440 minutes (or five minutes to one day). The default is set to 60 minutes.
	TACACS+ authentication	The maximum time duration (in seconds) for which an authenticated TACACS+ user is authorized to issue commands, from 120 to 36000 seconds. The default is set to 28800 seconds.
	Discard stale RADIUS authentication requests	Enable to select a time after which RADIUS authentication requests are considered stale and are discarded, from 3 - 360 seconds (or six minutes). The default is set to 8 seconds.
Sponsor Portal		
	Each sponsor only has access to guest users they created	Enable to allow sponsors to view only those guest users created by the sponsor. **Note**: This option is disabled by default.

PCI DSS 3.2 two-factor authentication

The login flows for RADIUS authentication, SAML IdP, guest portals, and GUI login all meet PCI DSS 3.2 standards regarding multi-factor authentication.

In the case where the **Bypass FortiToken authentication when user is from a trusted subnet** option is enabled (under **Authentication > SAML IdP > Service Providers**), *and* the user is logging in from a trusted subnet, the login flow reverts to password-only regardless of the PCI mode.

The GUI login page is hard-coded to **Apply two-factor authentication if available (authenticate any user)**, so it behaves the same as the guest portal.

All failed authentications will return the same generic message, so as not to reveal any clue to an attacker about which piece of information was valid or invalid:

```
Please enter correct credentials. Note that the password is case-sensitive.
```

Remote login to the CLI, i.e., SSH, also complies with the new PCI requirements.

Guest portal exception

There is one exception for guest portals. When a user has exceeded their time and/or data usage limit, the FortiAuthenticator shows the "Usage exceeded" replacement message.

The best behavior would be to only show the replacement message if the credentials are valid.

However, this would require a major change in the internal flow of the current authentication implementation.

Instead, the FortiAuthenticator only requires that the account name be valid (not the credentials).

The downside is that it opens the door for leaking valid account names. Nonetheless, it is deemed acceptable because:

1. Account name leakage prevention is not a PCI requirement (just a best practice).
2. Leaked account names are not usable because they are disabled (due to exceeded usage).
3. Disabled accounts cannot be leveraged to brute-force credentials (in the hope of using them if an account gets re-enabled/usage extended).

Lockouts

For various security reasons, you may want to lock a user's account. For example, repeated unsuccessful attempts to log in might indicate an attempt at unauthorized access.

Information on locked-out users can be viewed in the **Top User Lockouts** widget, see Top user lockouts widget on page 40.

Currently locked-out users can be viewed in **Monitor > Authentication > Locked-out Users**.

To configure the user lockout policy:

1. Go to **Authentication > User Account Policies > Lockouts**.
2. Configure the following settings, then select **Save** to apply any changes:

User account lockout policy	Enable user account lockout for failed login attempts and enter the maximum number of allowed failed attempts in the **Maximum failed login attempts** field. **Note**: The lockout policy applies to user accounts with the **User** role only and not administrator accounts.
Specify lockout period	Enable and specify the length of the lockout period in **User account lockout period**, from 60 to 86400 seconds (or one minute to one day). After the lockout period expires, the **Maximum failed login attempts** number applies again. When disabled, locked out users are permanently disabled until an administrator manually re-enables them.

Inactive user lockout		Select to enable disabling a local user account if there is no login activity for a given number of days. Inactive user lockout applies to local users only. In the **Lock out inactive users after** field, enter the number of days, from 1 to 1825 (or one day to five years), after which a local user is locked out.
IP lockout policy		Enable to block login attempts by source IP addresses after repeated failed attempts.
	Maximum failed login attempts	Enter the maximum number of login attempts after which the source IP address is blocked from gaining access for the configured **IP Lockout period** (default = 3). **Note**: The failed login attempts are counted by the source IP address.
	Specify IP lockout period	Enable to specify the IP address lockout period. When disabled, locked out IP addresses are permanently disabled until an administrator manually re-enables them.
	IP Lockout period	Enter the period of time for which the logins from the locked source IP address are blocked, in seconds (60 - 86400 or one minute to a day, default = 60).
	Captcha on SAML IdP login	Enable to use CAPTCHA on the SAML IdP login and set the number of failed login attempts in **Display captcha after** from the same source IP address, after which CAPTCHA challenge must be completed to log in (default = 0). **Note**: Set to `0` to require users to complete the CAPTCHA challenge on every login.  The value entered in **Display captcha after** must be smaller than the one in **Maximum failed login attempts**.
IP Address/Mask		When handling a failed authentication attempt, the IP lockout mechanism ignores that attempt if it originated from an exempt IP address/subnet. Select **Add IP Lockout Exemption** to specify a list of IPv4 addresses/subnets that are exempt from the IP lockout policy. **Note**: IPv6 addresses are not supported by IP lockout policy.

Passwords

Multiple password policies can be created and implemented for different groups, as opposed to enforcing a global password policy.

When a user is a member of multiple user groups, FortiAuthenticator applies the strictest password policy settings. For example, if two password policies have different password expiry periods, FortiAuthenticator applies the shortest expiry period.

For load-balancing HA (A-A), new password policy settings in user groups must be manually duplicated on the backup unit(s).

You can enforce a minimum length and complexity for user passwords, and can force users to change their passwords periodically.

For information on setting a user's password, and password recovery options, see Editing a user on page 99.

Go to **Authentication > User Account Policies > Passwords** and select **Create New** to configure a password policy.

To set password complexity requirements:

1. Under **User Password Complexity**, enter the minimum password length in the **Minimum length** field.

   The default length is 8. The minimum length is 0, which means that there is no minimum length but the password cannot be empty.

   Administrator passwords can be up to 64 characters in length.

2. Optionally, select **Check for password complexity** and then configure the following password requirements as needed:
   - **Minimum upper-case letters**
   - **Minimum lower-case letters**
   - **Minimum numeric characters**
   - **Minimum non-alphanumeric characters**
     You can also enable **Use non-alphanumeric characters in random passwords** and enter the characters in the field provided.
   - Enable **Enforce password not equal to username** to ensure that the password can never be same as the username.
3. Select **Save** to apply the password length and complexity settings.

To set a password change policy:

1. Under **User Password Change Policy**, optionally select **Enable password expiry**, then set the **Maximum password age**. When enabled, users are required to change their passwords after a period of time. Users are notified by email when their password is expiring. Accounts with expired passwords are disabled. The default maximum password age is 90 days. The minimum value allowed is 14 days.

   You can also set the password renewal reminder intervals in the **Send password renewal reminder on** field available, separating each entry by a comma. The default is every 14, 7, 3, and 1 days.

2. Optionally, select **Enforce password history** to prevent users from creating a new password that is the same as their current password or recently used passwords. Then, enter the **Number of passwords to remember**. FortiAuthenticator remembers up to 24 previously used passwords. New passwords must not match any of the remembered passwords.
   For example, if three passwords are remembered (set by default), users cannot reuse any of their three previous passwords.
3. Optionally, select **Enable random password expiry** to force randomly generated passwords to expire. Then, enter the number of hours after which a randomly generated password will expire in the **Random passwords expire after** field.
   The default randomly generated password expiry age is 72 hours (or three days). The value can be set from 1 to 168 hours (or seven days).
   You can also set the number of hours users have to set a new password upon receiving a new password email link. The default is 24 hours. The value can be set from 1 to 168 hours (or seven days).
4. Select **Save** to create the password policy.

Custom user fields

You can configure custom fields to include in the user information of local and remote users.

To edit custom fields, go to **Authentication > User Account Policies > Custom User Fields**. A maximum of three custom fields can be added.

When configuring a SAML SP, SAML user attributes in the **Assertion Attributes** pane include the custom user fields set here. See Service providers on page 230.

When configuring an OAuth relying party, user attributes in the **Claims** pane include the custom user fields set here, provided the grant type is set to either **Authorization code** or **Authorization code with PKCE**. See Relying Party on page 219.

When configuring a SCIM service provider, user attributes in the **User Attributes Mapping** pane include the custom user fields set here. See Service providers on page 137.

Tokens

To configure token policy settings, go to **Authentication > User Account Policies > Tokens**.

Configure the following settings:

FIDO		
	user verification	Select from the following options to determine which type of user verification to instruct the end user's browser to use when registering/authenticating with FIDO: • **preferred**: The client can choose to enforce biometrics verification (default). • **required**: The client must enforce biometrics verification. • **discouraged**: The client is encouraged to not use biometrics verification.
FortiTokens		
	TOTP authentication window size	Configure the length of time, plus or minus the current time, that a FortiToken code is deemed valid, from 1 - 60 minutes. The default is set to 1 minute.
	HOTP authentication window size	Configure the count, or number of times, that the FortiToken passcode is deemed valid, from 1 - 100 counts. The default is set to 3 counts.
	TOTP sync window size	Configure the period of time in which the entry of an invalid token can trigger a synchronization, from 5 - 480 minutes. The default is set to 60 minutes. If the token is incorrect according to the FortiToken valid window, but exists in the sync window, synchronization will be initiated.
	HOTP sync window size	Configure the count, or number of times, that the entry of an invalid token can trigger a synchronization, from 5 - 500 counts. The default is set to 100 counts. If the token is incorrect according to the FortiToken valid window, but exists in the sync window, synchronization will be initiated.

	Use geolocation in FortiToken Mobile push notifications	Enable or disable geolocation lookup for the user IP address (if possible).
FortiToken Mobile Provisioning		
	Activation timeout	The activation timeout, a maximum of 30 days.
	Token size	The token size, either **6** (set by default) or **8**.
	Token algorithm	Time-based One-time Password (**TOTP**, set by default) or Hash-based One-time Password (**HOTP**) algorithm.
	Time step	The time step, either **60** (set by default) or **30**.
	Require PIN	Select whether or not to require a PIN, or to enforce a mandatory PIN. When set to **Required** (set by default), the user has the option to set a PIN, but doesn't have to set one. However, a user must set a PIN when set to **Enforced**, which cannot be deleted.
	PIN Length	The PIN length, either **8**, **6**, or **4** (set by default).

	Provision mode	Set the method of FortiToken Mobile token provisioning:
		• **Online**: Provision FortiToken Mobile token by connecting to the FortiCloud server.
		  • **Enable token transfer feature**: Enable to let users securely transfer FortiToken Mobile tokens from one mobile device to another. See Transferring FortiToken Mobile tokens from old to new devices on page 91 below.
		  • **Seed encryption passphrase**: Passphrase to derive a seed encryption key from, for seed returned when provisioning a FortiToken Mobile via web service (REST API).
		• **Offline**: Air-gapped FortiAuthenticator devices can provision FortiToken Mobile tokens without connecting to the FortiCloud server.
		  FortiToken Mobile license activation requires a temporary online connection to *fortitokenmobile.fortinet.com*.
		Offline token provisioning can be done by scanning QR code or manually entering an activation code obtained within the FortiAuthenticator administrator GUI or using the self-service portal.
		  FortToken Mobile token transfer (**Enable token transfer feature**) and push features are unavailable when operating in the FortiToken Mobile offline mode.

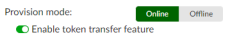
		FortiAuthenticator rejects setting the **Provision mode** to **Offline** if : • An existing remote user synchronization rule is configured with FortiToken Mobile in the OTP method assignment priority, i.e., the **FortiToken Mobile (assign an available token)** option is enabled in **Synchronization Attributes** in **Authentication > User Management > Remote User Sync Rules**. • An existing user portal has **Allow users to reconfigure their FortiToken Mobile** option enabled (when **FortiToken Revocation** is enabled) in the **Pre-Login Services** pane in **Authentication > Portals > Portals**.
FortiAuthenticator Agent Offline FortiToken Support		
	Enable offline support	Configure to allow the Windows Agent to cache future-dated tokens when the client's PC is offline. Enable this option to set the following: • **Shared secret:** Set the shared secret used in offline support. • **TOTP cache size:** Period of time after last login to pre-cache offline TOTP tokens, from 1 - 200 days. The default is set to 7 days. • **HOTP cache size:** Period of time after last login to pre-cache offline HOTP tokens, from 1 - 4000 counts. The default is set to 10 counts.
	Enable emergency codes	Enable to allow the Windows Agent to use emergency codes. The emergency code helps users with 2FA who may find themselves without access to FortiToken, SMS, or email. **Note:** This option is disabled by default.
		Emergency codes valid for — Configure the number of days for which an emergency code is valid, from 1 - 30. The default is set to 7.
Email/SMS		
	Token timeout	Set a time after which a token code sent via email or SMS will be marked as expired, from 10 - 3600 seconds (or one hour). The default is set to 60 seconds.

Transferring FortiToken Mobile tokens from old to new devices

Changing devices requires the user to install new tokens on their new device because the unique device ID is used to form the seed decryption key.

If you wipe data from your device, or upgrade your device, you will need to re-provision your accounts.

The option to **Enable token transfer feature** is available under **Authentication > User Account Policies > Tokens** when the **Provision mode** is **Online**.



If it is not enabled, FortiAuthenticator blocks all requests to **Transfer Activation Code** (see below).

The process for transferring a token to a new device is as follows:

1. The end user selects a new FortiToken Mobile menu option: **Initiate Token Transfer**.
2. FortiToken Mobile requests a new "Token Transfer Request" service from FortiCare, and includes the token data.
3. FortiCare stores the token data and creates a **Transfer Activation Code**.
4. FortiCare signals back to FortiToken Mobile on the old device that "Transfer Initialization" is complete.
5. On the old device, FortiToken Mobile sends a request to FortiAuthenticator for the **Transfer Activation Code**.
6. FortiAuthenticator retrieves the **Transfer Activation Code** from FortiCare and signals back to FortiToken Mobile (on the old device) that the **Transfer Activation Code** request was successful.
7. FortiAuthenticator sends either an email or SMS to the end user with the transfer code (as a QR code in the case of email).
8. On the new device, the end user selects the FortiToken Mobile menu option **Complete Token Transfer** and enters the transfer code (or scans the QR code).
9. FortiToken Mobile receives the token data from FortiCare and installs the token(s) on the new device.

All tokens are removed on the old device after the transfer is complete.

Trusted subnets

To configure trusted subnets, go to **Authentication > User Account Policies > Trusted Subnets**.

The following options are available:

Create New	Select to configure a new trusted subnet.
Delete	Select to delete the selected subnets.
Edit	Select to edit the selected trusted subnet.
Search	Using the search bar, look up a trusted subnet.
Reset table column widths	Select the reset icon to reset the table column widths to default.
Name	The name of the trusted subnet.
Trusted Subnet	The IP address of the subnet.

To configure the trusted subnets:

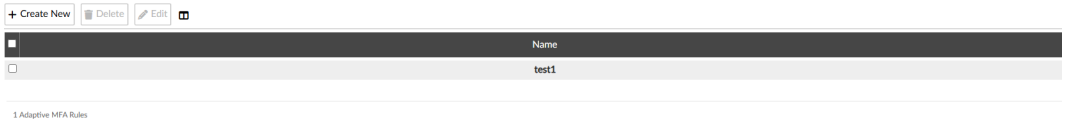
1. Go to **Authentication > User Account Policies > Trusted Subnets**.
2. Configure the following settings, then select **Save** to apply any changes:

Name	The name of the trusted subnets.
Address	Select from the following two options:

	• **Subnet** • **Range**
Trusted subnet	Enter a subnet or a range of IP addresses. **Note**: You can enter either an IPv4 or an IPv6 address.

Adaptive MFA rules

The **Adaptive MFA rules** displays a list of adaptive MFA rules.



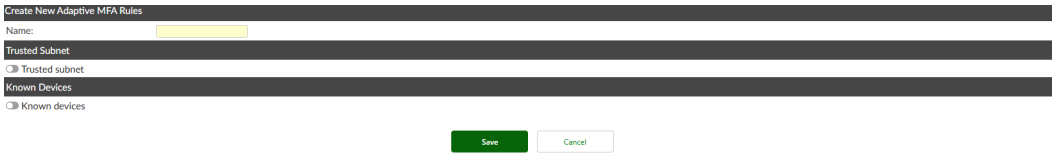
Certain users can bypass the OTP verification, so long as they belong to a trusted subnet or they are a known device.

The following options are available in the **Adaptive MFA Rules** tab:

Create New	Select to create an adaptive MFA rule.
Delete	Select to delete the selected adaptive MFA rules.
Edit	Select to edit the selected adaptive MFA rule.
Reset table column widths	Select the reset icon to reset the table column widths to default.

To configure adaptive MFA Rules:

1. Go to **Authentication > User Account Policies > Adaptive MFA Rules**.
2. Select **Create New**.
   The **Create New Adaptive MFA Rules** window opens.



3. Enter the following information:

Name	The name of the adaptive MFA rule.
Trusted Subnet	
Trusted subnet	Enable to bypass OTP validation if the end user is on a trusted subnet and select from the following two options: • **All trusted subnets**: Add all the available trusted subnets. • **Specify trusted subnets**: Specify the trusted subnets. Choose from a list of available trusted subnets. **Note**: Trusted subnets can be configured in **Authentication > User Account Policies > Trusted Subnets**.

Known Devices	
Known devices	Enable to bypass OTP validation if the end-user is a known device.
Validate OTP again after	Enter the time after which OTP is required, in minutes/hours/days (default = 5 hours).
FortiTokens	Select how to send the OTP: • **FortiTokens** • **Email** • **SMS**

4. Click **Save**.

User management

The FortiAuthenticator user database has the benefit of being able to associate extensive information with each user, as you would expect of RADIUS and LDAP servers. This information includes whether the user is an administrator, uses RADIUS authentication, or uses two-factor authentication, and includes personal information such as full name, address, password recovery options, and the groups that the user belongs to.

The RADIUS server on FortiAuthenticator is configured using default settings. For a user to authenticate using RADIUS, the option **Allow RADIUS Authentication** must be selected for that user's entry, and the FortiGate unit must be added to the authentication client list. See RADIUS service on page 189.

Administrators

Administrator accounts on FortiAuthenticator are standard user accounts that are flagged as administrators. Both local users and remote LDAP users can be administrators.

Once flagged as an administrator, a user account's administrator privileges can be set to either full access or customized to select their administrator rights for different parts of FortiAuthenticator.

The subnets from which administrators are able to log in can be restricted by entering the IP addresses and netmasks of trusted management subnets.

There are log events for administrator configuration activities. Administrators can also be configured to authenticate to the local system using two-factor authentication.

An account marked as an administrator can be used for RADIUS authentication if **Allow RADIUS Authentication** is selected. See RADIUS service on page 189. These administrator accounts only support Password Authentication Protocol (PAP).

Administrator accounts can be synced from the primary standalone device to load-balancer in an HA load-balancing configuration when **Sync in HA Load Balancing mode** is enabled.

See Configuring a user as an administrator on page 104 for more information.

The administrator must log in with their username only, i.e., `username + realm` is no longer accepted.

Whenever an admin attempts to add, edit, or delete an admin account in FortiAuthenticator, a dialog is displayed requesting the password for the currently logged in administrator before settings can be saved.

Groups for administrators

Local and remote user accounts with administrator or sponsor roles can be entered into groups. This provides the following benefits:

- Group filtering of administrators.
- A single account for individuals needing both administrator and user roles.
- Inclusion of RADIUS attributes from groups in RADIUS Access-Accept responses.

Local users

Local user accounts can be created, imported, exported, edited, and deleted as needed. Expired local user accounts can be purged manually or automatically (see User account policies on page 82).

To manage local user accounts, go to **Authentication > User Management > Local Users**.

The local user account list shows the following information:

Create New	Select to create a new user.
Import	Select to import local user accounts from a CSV file or FortiGate configuration file. If using a CSV file, it must have one record per line, with the following format: username (30 characters max), display name (64 characters max), first name (30 characters max), last name (30 characters max), email (75 characters max), alternate emails (75 characters max; semicolon separated if multiple alternate emails), phone number (25 characters max), mobile number (25 characters max), street address, city, state/province, zip/postal code (16 characters max), country, company (64 characters max), department (64 characters max), title (64 characters max), birthdate, custom1, custom2, custom3, password (optional, 128 characters max), otp, otp-only, groups (semicolon separated if multiple groups). If the optional password is left out of the import file, the user is emailed temporary login credentials and requested to configure a new password. Note that even if an optional field is empty, it still must be defined with a comma. Multiple groups can be separated by a semi-colon, e.g., g1;g2;g3.

	 Custom field must be predefined in **User Account Policies**. See Custom user fields on page 88.
	 A valid (configured) FortiToken serial number must be provided to disable password authentication and use FortiToken-based authentication only.
	 Click the **Export** option on the top to download a sample CSV file. Fill in the file and use it to import users.
	Import error handling: If any error is detected (e.g., duplicate user, invalid field, etc.), none of the local user accounts from the CSV file are created. For FortiAuthenticator to successfully add the imported local users from a CSV file to the specified groups: • All the specified local groups must already exist on the FortiAuthenticator. • If a line is missing the group field (e.g., CSV export from a previous FortiAuthenticator version), FortiAuthenticator assumes no group membership.
	 Use # at the start of a row if you want to comment out the row. For example, in the sample CSV file that you can download by clicking **Export** on the top, the first row is commented out as it starts with #.
	When importing local users from a CSV file, click **+** to expand **Advanced options**. In **Advanced options**, you can select the action to take for existing accounts missing from the CSV file: • **Keep user accounts** • **Disable user accounts** • **Delete user accounts**
Export	Select to export the user account list to a CSV file.
Delete	Select to delete the selected user account or accounts.
Edit	Select to edit the selected user account.
Disabled Users	• **Re-enable:** This allows the administrator to re-enable disabled accounts. Expired users accounts can only be re-enabled individually. • **Purge Disabled:** This offers the option to choose which type of disabled users to purge. • **Manually disabled**

	• **Login inactivity** • **Too many login attempts** • **Account expired** • **Password expired** • **FTM activation expired** • **Manually disabled by user** • **Usage limit exceeded** • **Not Activated** **Note**: All users matching the type(s) selection are deleted.
Search	Enter a search term in the search field, then select **Search** to search the user account list.
User	The user accounts' usernames.
First name	The user accounts' first names, if included.
Last name	The user accounts' last names, if included.
Email address	The user accounts' email addresses, if included.
Admin	If the user account is set as an administrator, a green circle with a check mark is shown.
Status	If the user account is enabled, a green circle with a check mark is shown.
Token	The token that is assigned to that user account. Select the token name to edit the FortiToken, see FortiToken device maintenance on page 142.
Token requested	The status of the user's token request.
Groups	The group or groups to which the user account belongs.
Authentication Methods	The authentication method used for the user account.
Expiration	The date and time that the user account expires, if an expiration date and time have been set for the account.

Adding a user

When creating a user account, there are three ways to handle the password:

1. The administrator assigns a password immediately and communicates it to the user.
2. FortiAuthenticator creates a random password and automatically emails it to the new user.
3. No password is assigned because only One-Time Password (OTP) authentication will be used.

To add a new user:

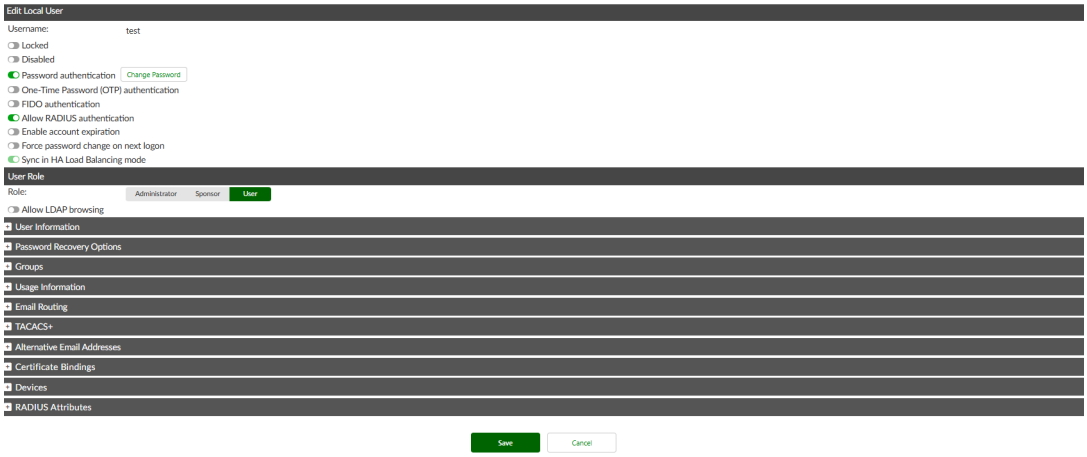
1. In the local users list, select **Create New**. The **Create New Local User** window opens.
2. Enter the following information:

Username	Enter a username for the user.
Password creation	Select one of the options from the dropdown menu: • **Specify a password**: Manually enter a password in the **Password** field, then reenter the password in the **Password confirmation** field. • **Set and email a random password**: Enter an email address to which to send the password in the **Email address** field, then reenter the email address in the **Confirm email address** field. • **No password, FortiToken authentication only**: After you select **OK**, you will need to associate a FortiToken device with this user. See FortiToken physical device and FortiToken Mobile on page 140.
Allow RADIUS authentication	For a user to authenticate using RADIUS, this must be enabled.
Force password change on next logon	Enable or disable the option for users to change their local password on FortiAuthenticator at first logon. This feature prevents administrators from having to call or email the franchisee to deliver user credentials, which is not a secure method of delivery and adds additional time to the onboarding process.
Role	Select whether the new account is for an **Administrator**, **Sponsor**, or regular **User**. Administrators can either have full permissions or have specific administrator profiles applied. Regular users can have their account expiration settings configured. When creating a new administrator account, you are prompted to enter the password of the currently logged in administrator before changes can be saved.
Enable account expiration	Select to enable user account expiration, either after a specific amount of time has elapsed, or on a specific date.
Expire after	Select when the account will expire: • **Set length of time**: Enter the number of hours, days, months, or years until the account expires. • **Set an expire date**: Enter the date on which the account will expire, either by manually typing it in, or by selecting the calendar icon and selecting a date.
IAM	Add this local user to an IAM account.

3. Select **Save** to create the new user. You are redirected to the **Change local user** window to continue the user configuration in greater detail.
   If the password creation method was set to **No password, FortiToken authentication only**, you are required to associate a FortiToken with the user before the user can be enabled.

Editing a user

User accounts can be edited at any time. To edit a user, go to the user account list, select a user to edit, and select **Edit** from the toolbar. Conversely, select the username in the user list.



The following information can be viewed or configured:

Username	The username cannot be changed.
Locked	Enabling **Locked** gives the administrator the ability to lock user accounts independent of the **Disabled** option. When **Locked** is enabled, FortiAuthenticator rejects all authentication attempts for the user.
Disabled	Select to disable the user account. When **Disabled** is enabled, FortiAuthenticator rejects all authentication attempts for the user.
Password authentication	Select to enable password authentication. The user's password can be changed by selecting **Change Password**.
One-Time Password (OTP) authentication	Select to enable FortiToken-based authentication. See Configuring One-Time Password (OTP) authentication on page 101.
FIDO authentication	Select to enable FIDO authentication. This is disabled by default for new user accounts.
Register FIDO key	Select to open the **Add new Fido Key** dialog, enter the **FIDO key name**, and click **OK** to register a FIDO key for the user. **Note**: Use the **Delete all FIDO keys** button to delete all the registered FIDO keys.
Allow RADIUS authentication	Select to allow RADIUS authentication. This applies only to regular users.
Enable account expiration	Select to enable account expiration and specify the account's expiration. See Enable account expiration on page 98.

Force password change on next logon	Require the user to change their password on their next logon. Once changed, this setting will be automatically disabled again.
Sync in HA Load Balancing mode	Select to sync the administrator across load-balanced FortiAuthenticator devices from the primary standalone device to load-balancers.
User Role	Configure the user's role.
Role	Select **Administrator**, **Sponsor**, or **User**. If setting a user as an administrator, see Configuring a user as an administrator on page 104.
Allow LDAP browsing	Select to allow LDAP browsing. When the option is enabled and the user account is added into the directory tree of the FortiAuthenticator LDAP Service (under **Authentication > LDAP Service > Directory Tree**), the user account will be able to perform LDAP searches within the directory tree after having done a successful LDAP bind.
Full permission	Enable to grant this administrator full permission, or enter an Admin profile in the field provided. This applies only to administrators.
Web service access	Enable to allow this administrator to access the web services either through a REST API or using a client application. This applies only to administrators. After enabling **Web service access** and saving your changes, the User API Access Key window is displayed allowing you to view, copy, and/or email the API access key.
Restrict admin login from trusted management subnets only	Enable and enter trusted IP addresses and netmasks for restricted administrator login access. This applies only to administrators.
User Information	Enter user information, such as their address and phone number. See Adding user information on page 104.
Password Recovery Options	Configure password recovery options for the user. See Configuring password recovery options on page 105
Groups	Assign the user to one or more groups. See Local users on page 95.
Usage Information	View the user's usage information: • Bytes in/out • Total bytes • Time used • Reset the usage statistics by selecting **Reset Usage** • Display historical data usage by selecting **Usage History**

	When allocated usage is reached, the user account is locked and needs to be unlocked manually by an admin or via API. Upon unlock, usage data is reset.
Email Routing	Enter a mail host and routing address into their respective fields to configure email routing for the user.
TACACS+	Add a TACACS+ authorization rule. See Assigning authorization rules on page 212.
Alternative email addresses	Add alternate email addresses for the user. In LDAP, alternative email addresses are defined by the `rfc822MailMember` attribute.
Certificate Bindings	Add, edit, or removed certificate bindings for the user account. See Configuring certificate bindings on page 107. Select the certificate name to view the certificate, or select the **Revoke Certificate** button to revoke the certificate. For administrator and sponsor user roles, this field is available only when **Sync in HA Load Balancing** mode is enabled.
Devices	Add devices, based on MAC address, for the user account.
RADIUS Attributes	Add RADIUS attributes. See RADIUS attributes on page 137. For administrator and sponsor user roles, this field is available only when **Sync in HA Load Balancing** mode is enabled.

Select **Save** when you have finished editing the user's information and settings.

Configuring One-Time Password (OTP) authentication

One-Time Password (OTP) authentication requires either a FortiToken device or a mobile device with the FortiToken Mobile app installed, or a device with either email or SMS capability.

FortiToken and FortiToken Mobile tokens must first be registered under **Authentication > User Management > FortiTokens**. For more information, see FortiTokens on page 132.

To configure an account for One-Time Password (OTP) authentication:

1. To view the One-Time Password (OTP) authentication options, edit a user and select **One-Time Password (OTP) authentication**.
2. Specify the source of tokens; **FortiAuthenticator** or **FortiToken Cloud**:
   a. When **FortiAuthenticator** is selected, select a token delivery method:
      i. **FortiToken**, then select the type of FortiToken used from the available options.
         i. **Hardware**, then select the FortiToken device serial number from the **Token** dropdown menu.
         ii. **Mobile**, then select the FortiToken Mobile device serial number from **Token** dropdown menu, and select an **Activation delivery method** from **Email**, **SMS**, or **Scan QR code**.

When editing a local/remote user with the **Provision mode** set to **Offline** in Tokens on page 88:

- The edit user page only offers the **Scan QR code Activation delivery method** for **FortiToken Mobile** (no **Email** or **SMS** options) as the **Deliver token code by** option.

The device must be known to FortiAuthenticator. See FortiToken physical device and FortiToken Mobile on page 140.

Optionally, select **Temporary token** to receive a temporary token code via email or SMS.

The **Temporary token** option is meant as a backup token delivery method when FortiToken Hardware/Mobile are the primary delivery methods.

When emergency codes are enabled in Tokens on page 88, you can view emergency codes from within the user account by clicking **Display Emergency Code** if FortiToken is provisioned for the account.

If the Temporary token is enabled with **Email** or **SMS**, the user configured for 2FA receives an OTP via email or SMS when attempting a 2FA login. This helps the user access the network with a temporary OTP in case they do not have access to their phone or a hardware token.

The temporary token based authentication is automatically disabled the next time the end-user does a successful login using their FTK/FTM.

      ii. **Email**, then enter the user's email address in the **User Information** section.
      iii. **SMS**, then enter the user's mobile number in the **User Information** section.
      iv. **Dual (Email & SMS)**, then enter the user's email address and mobile number in the **User Information** section.
      v. Select **Test Token** to validate the token passcode. The **Test Email Token** or **Test SMS Token** window opens (depending on your selection).
         - For email and SMS tokens, confirm that the contact information is correct, select **Next**, then enter the token code received via email or SMS.
         - Select **Back** to return to edit the contact information, select **Verify** to verify the token passcode, or select **Resend Code** if a new code is required.
         - For FortiToken, enter the token code in the **Token code** field, then select **Verify** to verify the token passcode.

b. When **FortiToken Cloud** is selected, select a token delivery method:

i. **Default**, the user is assigned the default token code delivery option configured on the FortiToken Cloud side.

If the default is FortiToken Mobile, the activation code delivery method is also the default configured on the FortiToken Cloud side.

If the default provisioning is successful, FortiAuthenticator tells the FortiAuthenticator administrator about the result of the provisioning and logs it:

- `FortiToken Cloud provisioned with FortiToken Hardware <serial number>`.
- `FortiToken Cloud provisioned with FortiToken Mobile. The user was notified by <email/SMS>`.
- `FortiToken Cloud provisioned with email OTP`.
- `FortiToken Cloud provisioned with SMS OTP`.

FortiAuthenticator informs the FortiAuthenticator admin if there is a missing user account field, e.g., email address.

ii. **FortiToken**, then select the type of FortiToken used from the available options.

i. **Hardware**, then FortiToken Cloud randomly assigns an FTK from its pool of available FTKs.

If the provisioning is successful, FortiAuthenticator tells the FortiAuthenticator administrator about the result of the provisioning and logs it as `FortiToken Cloud provisioned with FortiToken Hardware <serial number>`.

FortiAuthenticator informs the administrator in case of a provisioning error.

ii. **Mobile**, then FortiToken Cloud randomly assigns an FortiToken Mobile token from its pool of available FortiToken Mobile tokens. Select an **Activation delivery method** from **Default**, **Email**, and **SMS**.

If the provisioning is successful, FortiAuthenticator tells the FortiAuthenticator administrator about the result of the provisioning and logs it as `FortiToken Cloud provisioned with FortiToken Mobile. The user was notified by <email/SMS>`.

FortiAuthenticator informs the administrator in case of a provisioning error.

iii. **Email**, then enter the user's email address in the **User Information** section.

If the provisioning is successful, FortiAuthenticator tells the FortiAuthenticator administrator about the result of the provisioning and logs it as `FortiToken Cloud provisioned with email OTP`.

FortiAuthenticator informs the administrator in case of a provisioning error.

iv. **SMS**, then enter the user's mobile number in the **User Information** section.

If the provisioning is successful, FortiAuthenticator tells the FortiAuthenticator administrator about the result of the provisioning and logs it as `FortiToken Cloud provisioned with SMS OTP`.

FortiAuthenticator informs the administrator in case of a provisioning error.

3. Click **Save**.
   Since a user's FortiToken Cloud token code delivery method can be changed at any point from the FortiToken Cloud portal, FortiAuthenticator does not save the FortiToken Cloud token code delivery method in its config database. Instead, FortiAuthenticator queries FortiToken Cloud API whenever the FortiAuthenticator administrator requests to see the FortiToken Cloud token code delivery method.

When editing a user account with FortiToken Cloud OTP enabled, FortiAuthenticator does not automatically show token code delivery options. Select **Show delivery options** to see the token delivery options in the same format as when first enabling FortiToken Cloud OTP.

If the administrator changes the token code delivery option, FortiToken Cloud is updated with the new token code delivery method.

By default, token code verification must be completed within 60 seconds after the token code is sent by email or SMS. To change this timeout, go to **Authentication > User Account Polices > Tokens** and modify the **Email/SMS Token timeout** field. For more information, see Lockouts on page 85.

Configuring a user as an administrator

For more information, see Administrators on page 94.

To set a user as an administrator:

1. Edit a user and set **Role** to **Administrator** under the **User Role** section.
2. Enable **Full permission** to give the administrator full administrative privileges, or enter **Admin profiles** to customize the administrator's permissions.
3. Optionally, enable **Web service access** to allow the administrator to access the web services via a REST API or FortiAuthenticator Agent for Microsoft Windows.
4. Select **Restrict admin login from trusted management subnets only**, then enter the IP addresses and netmasks of trusted management subnets in the table, to restrict the subnets from which an administrator can log in.
5. Select **Sync in HA Load Balancing mode** to allow the administrator to be synced from the primary standalone device to load balancers in an HA load balancing configuration.
6. Select **Save** to save your changes.
   A dialog appears requesting the password for the currently logged in admin account. Enter your password and click **Verify**.

Adding user information

Some user information can be required depending on how the user is configured. For example, if the user is using One-Time Password (OTP) authentication by SMS, a mobile number and SMS gateway must be configured before the user can be enabled.

The following user information can be entered:

Display name

First name	**Last name**
Email	**Phone number**
Mobile number	**SMS gateway**: select from the dropdown menu. Select **Test SMS** to send a test message.
Street address	
City	**State/Province**
Postal Code	
Country: Select from the dropdown menu.	
Company	
Department	
Title	
Birthdate: Select the calendar icon and then use the dropdowns to select a date.	
Language: Select a specific language from the dropdown menu, or use the default language.	
FortiToken Logo: Select a FortiToken Mobile logo from the dropdown menu. See FortiTokens on page 132.	

When editing a local/remote user with the **Provision mode** set to **Offline** in Tokens on page 88, you are not required to add an **Email**.

Configuring password recovery options

To replace a lost or forgotten password, FortiAuthenticator can send the user a password recovery link by email or in a browser in response to a pre-arranged security question. The user must then set a new password.

You can also configure password recovery using SMS or FortiToken.

To configure password recovery by email:

1. Edit a user and ensure that the user has an email address entered. See Adding user information on page 104.
2. Under **Password Recovery Options** section, enable **Email recovery**.
   In the event that additional email addresses have been configured under **Alternative Email Addresses**, an email is sent to all configured email addresses.
3. Select **Save** to apply the changes.

To configure password recovery by SMS:

1. Edit a user and ensure that the user has a phone number entered. See Adding user information on page 104.
2. Under **Password Recovery Options** section, enable **SMS recovery**.
3. Select **Save** to apply the changes.

To configure password recovery by FortiToken:

1. Edit a user and ensure that the user has an associated FortiToken. See Configuring One-Time Password (OTP) authentication on page 101.
2. Under **Password Recovery Options** section, enable **FortiToken recovery**.
3. Select **Save** to apply the changes.

To configure password recovery by security question:

1. Edit a user and, under **Password Recovery Options**, enable **Security question**, and select **Edit**.
2. Enter the administrator password and click **Verify**.
3. Choose one of the questions from the dropdown menu, or select **Write my own question** and enter a question in the **Custom question** field.
4. Enter the answer for the question in the **Answer** field.
5. Select **Save** to create the security question.
6. Select **Save** again to apply the changes to the user account.

How the user can configure password recovery by security question:

1. Log in to the user account.
2. Select **Edit Profile** at the top left of the page.
3. Under **Password Recovery Options**, select **Security Question**, and select **Edit**.
4. Choose one of the questions in the list, or select **Write my own question** and enter a question in the **Custom question** field.
5. Enter the answer for your question.
6. Select **Save**.

How the user can configure password recovery by email:

1. Log in to the user account.
2. Select **Edit Profile** at the top left of the page.
3. Under **Password Recovery Options**, select **Email recovery**.
4. Optionally, select **Alternative email addresses** and enter additional email addresses for this user.
5. Select **Save**.

How the user recovers from a lost password:

1. Browse to the IP address of the FortiAuthenticator.
   Security policies must be in place on the FortiGate unit to establish these sessions.
2. At the login screen, select **Forgot password?**.
3. Select to recover your password either by **Username** or **Email**.
4. Enter either your username or email address as selected in the previous step, and select **Next**.
   This information is used to select the user account. If your information does not match a user account, password recovery cannot be completed.
5. Do one of the following:
   - If an email address was entered, check your email, open the email and select the password recovery link.
   - If a username was entered, answer the security question and select **Next**.
6. On the **Reset Password** page, enter and confirm a new password and select **Next**.

The user can now authenticate using the new password.

Active Directory users password reset

To allow Active Directory (AD) users to reset their password from the main login page, follow the same workflow for resetting a local user's password described above.

The **Password Recovery Options** setting is included in the remote LDAP users configuration page.

This feature is available for both self-service and guest portals.

Configuring certificate bindings

To use a local certificate as part of authenticating a user, you need to:

- Create a user certificate for the user (see To create a new certificate: on page 289 for more information).
- Create a binding to that certificate in the user's account.

To create a binding to a certificate in a user's account:

1. Edit a user and expand the **Certificate Bindings** section.
2. Select **Add Certificate Binding**.
3. Select either a local CA or a trusted CA from the **Issuer** dropdown.
4. Enter the **Common Name** on the certificate. For example, if the certificate says `CN=rgreen` then enter `rgreen`.
5. Select **Save** to add the new binding.

Local user account password storage

FortiAuthenticator protects local user account passwords in its storage using cryptography:

- Password storage for local user accounts with the "sponsor" or "administrator" role always uses irreversible cryptography (i.e. bcrypt hash).
- Password storage for local user accounts with the "user" role depends on the **Enhanced cryptography for storage of local user passwords** option under **Authentication > User Account Policies > General**:
  - If enabled, irreversible cryptography (i.e. bcrypt hash) is used.
  - If disabled, reversible cryptography (i.e. AES256) is used.

Remote users

Remote LDAP users must be imported into the FortiAuthenticator user database from LDAP servers. For more information, see LDAP on page 176.

Note that you will only be able to import a maximum of five remote users if you have an unlicensed version of FortiAuthenticator-VM.

A FortiToken device already allocated to a local account cannot be allocated to an LDAP user as well; it must be a different FortiToken device.

Remote RADIUS users can be created, migrated to LDAP users, edited, and deleted.

LDAP users

When an LDAP user is successfully authenticated, subsequent authentication requests from the same user within a 2 minute window succeed without the need to check the remote LDAP server.

The LDAP user accounts list shows the following information:

Import	Select to import remote LDAP user accounts. See Import remote LDAP users.
Export Users	Select to export the user accounts list to a CSV file.
Delete	Select to delete the selected user account or accounts.
Re-enable	This allows the administrator to re-enable disabled accounts. Expired users accounts can only be re-enabled individually.
Search	Enter a search term in the search field, then select **Search** to search the LDAP user accounts list.

To import remote LDAP users:

1. Go to **Authentication > User Management > Remote Users**, ensure that **LDAP users** is selected, and select **Import**.
2. Select a server from the **Remote LDAP server** dropdown menu, then select **Import users** or **Import users by group membership**, and select **Import**.

   An LDAP server must already be configured to select it in the dropdown menu. For information on adding a remote LDAP server, see Remote authentication servers on page 176.

   The **Import Remote LDAP Users** or **Import Remote LDAP Users by Group Memberships** window opens in a new browser window.
3. Optionally, enter a **Filter** string to reduce the number of entries returned, and then select **Apply**, or select **Clear** to clear the filters.

   Please note that the **Member attribute** field is only available if you select to **Import users by group membership**. Use this field to specify the filter by which users will be shown. In the example, the default attribute (**member**) will only show users that are members of groups (users must be part of member attribute of the groups).
4. The default configuration imports the attributes commonly associated with Microsoft Active Directory LDAP implementations. Select **User Attributes** to edit the remote LDAP user mapping attributes.
   Selecting the field **FirstName**, for example, presents a list of detected attributes that can be selected. This list is not exhaustive as additional, non-displayed attributes may be available for import. Consult your LDAP administrator for a full list of available attributes.

5. Select the entries you want to import.
6. Optionally, select a logo from the **FortiToken Logo** dropdown menu to associate the imported users with the specified logo. This logo is displayed beside the one-time password in FortiToken. See FortiTokens on page 132 for more information.
7. Optionally, select an IAM account from the **IAM Account** dropdown to associate the imported users with.
8. Select **OK**.
   The amount of time required to import the remote users will vary depending on the number of users to import.

When a remote LDAP user is imported, FortiAuthenticator saves the DN. When it is time to authenticate, FortiAuthenticator uses the DN to perform the LDAP bind directly instead of searching the username in the directory first.

When the `diagnose authentication radius-force-ldap-user-lookup {enable | disable}` CLI command is enabled, FortiAuthenticator ignores the DN and searches the LDAP directory for the username before performing the LDAP bind.

There is no equivalent GUI option for the CLI command.

To add two-factor authentication to a remote LDAP user:

1. Edit the remote user, select **One-Time Password (OTP) authentication**, and follow the same steps as when editing a local user (Editing a user on page 99).
2. Configure the **User Role**, **User Information**, **RADIUS Attributes**, and **Certificate Bindings** for the user as needed.
3. Select **Save** to apply the changes.

RADIUS users

To view remote RADIUS users, go to **Authentication > User Management > Remote Users** and select **RADIUS users** in the toolbar. See RADIUS on page 183 for more information about remote RADIUS servers.

The following options are available (when remote RADIUS users are available to edit):

Create New	Select to create a new remote RADIUS user.
Import	Select to import remote RADIUS user accounts from a CSV file. The **Import RADIUS Users** page has the same options as the **Import Local Users** page except that you cannot change the **File type**. See Import on page 95 in Local users on page 95.
Export	Select to export the remote RADIUS user accounts list to a CSV file.
Delete	Select to delete the selected user or users.
Edit	Select to edit the selected user.

Re-enable	Select to re-enable the status of a user that has been disabled.
Migrate	Select to migrate the selected user or users. See To migrate RADIUS users to LDAP users: on page 112.
Token	Select to either **Enforce** or **Bypass** One-Time Password (OTP) authentication for the selected user(s).
Search	Search the remote RADIUS users list.
Username	The remote user's name.
Remote RADIUS server	The remote RADIUS server where the user resides.
Admin	Displays whether or not the user is configured as an administrator.
Status	Displays whether or not the user is enabled or disabled.
Token	The FortiToken used by the user, if applicable.
Token Requested	Displays whether or not a FortiToken has been requested for the user.
Enforce token-based authentication	Displays whether or not token-based authentication is enforced.

To create a new remote RADIUS user:

1. From the remote users list, select **RADIUS users** and select **Create New**.
2. Enter the following information:

Remote RADIUS	Select the remote RADIUS server on which the user will be created from. For more information on remote RADIUS servers, see RADIUS on page 183.
Username	Enter a username.
Locked	Enabling **Locked** gives the administrator the ability to lock user accounts independent of the **Disabled** option. When **Locked** is enabled, FortiAuthenticator rejects all authentication attempts for the user.
Disabled	Select to disable the user account. When **Disabled** is enabled, FortiAuthenticator rejects all authentication attempts for the user.
Enforce token-based authentication if configured below	Select to enforce token-based authentication, if you are configuring token-based authentication.
One-Time Password (OTP) authentication	Select to configure One-Time Password (OTP) authentication. See Configuring One-Time Password (OTP) authentication on page 101.

FIDO authentication	Select to enable FIDO authentication. This is disabled by default for new user accounts.
Register FIDO key	Select to open the **Add new Fido Key** dialog, enter the **FIDO key name**, and click **OK** to register a FIDO key for the user. **Note**: Use the **Delete all FIDO keys** button to delete all the registered FIDO keys.
Allow RADIUS authentication	Enable or disable RADIUS authentication.
Sync in HA Load Balancing mode	Select to sync the administrator across load-balanced FortiAuthenticator devices from the primary standalone device to load-balancers.
User Role	Configure a remote user's role. Select whether the remote user is either an **Administrator** (along with related permissions), **Sponsor**, or a regular **User**.
Role	Select **Administrator**, **Sponsor**, or **User**.
Full Permission	Enable to grant this administrator full permission, or enter an Admin profile in the field provided. This applies only to administrators.
Use backup password	Enable to set up a backup password to be used when the remote server is unreachable. This applies to administrator and sponsors only.
Restrict admin login from trusted management subnets only	Enable and enter trusted IP addresses and netmasks for restricted administrator login access. This applies to administrator and sponsors only.
User Information	Enter user information as needed. The following options are available: • **Display name** • **Email** • **Company** • **Department** • **Title** • **Birthdate** • **Mobile number** and **SMS gateway** • **Language** • **FortiToken Logo** - see FortiTokens on page 132.  When editing a remote user with the **Provision mode** set to **Offline** in Tokens on page 88, you are not required to add an **Email**.
TACACS+	Add a TACACS+ authorization rule. See Assigning authorization rules on page 212.
Usage Information	View the user's usage information: • Bytes in/out • Total bytes • Time used

	• Reset the usage statistics by selecting **Reset Usage** • Display historical data usage by selecting **Usage History** When allocated usage is reached, the user account is locked and needs to be unlocked manually by an admin or via API. Upon unlock, usage data is reset.
Certificate Bindings	Add, edit, or removed certificate bindings for the user account. See Configuring certificate bindings on page 107. Select the certificate name to view the certificate, or select the **Revoke Certificate** button to revoke the certificate. For administrator and sponsor user roles, this field is available only when **Sync in HA Load Balancing** mode is enabled.
Devices	Add devices, based on MAC address, for the user account.

3. Select **Save** to create the new remote RADIUS user.

To migrate RADIUS users to LDAP users:

1. From the remote RADIUS users list (see Learned RADIUS users on page 284), select the user or users you need to migrate, then select **Migrate** from the toolbar.
2. Select an LDAP server from the dropdown menu and select **Next**.
3. Enter the distinguished names for the users to migrate, or browse the LDAP tree (see Directory tree overview on page 214) to find the users.
4. Select **Migrate** to migrate the user or users.

SAML users

To view remote SAML users, go to **Authentication > User Management > Remote Users** and select **SAML users**.

The SAML user accounts list shows the following information:

Create New	Select to create a new remote SAML user.
Import	Select the file type to import remote SAML users from. See Import remote SAML users.
Export	Select to export the remote SAML user accounts list to a CSV file.
Delete	Select to delete the selected user or users.
Edit	Select to edit the selected user.
Search	Search the remote SAML users list.

To create a new remote SAML user:

1. From the remote users list, select **SAML users** and select **Create New**.
   The **Create New Remote SAML User** window appears.
2. Enter the following information:

Remote SAML	Select the remote SAML server on which the user will be created from. For more information on remote SAML servers, see SAML on page 186.
Username	Enter a username.
Locked	Enabling **Locked** gives the administrator the ability to lock user accounts independent of the **Disabled** option. When **Locked** is enabled, FortiAuthenticator rejects all authentication attempts for the user.
Disabled	Select to disable the user account. When **Disabled** is enabled, FortiAuthenticator rejects all authentication attempts for the user.
One-Time Password (OTP) authentication	Select to configure One-Time Password (OTP) authentication. See Configuring One-Time Password (OTP) authentication on page 101.
User Information	Enter user information as needed. The following options are available: • **Display name** • **First name** • **Last name** • **Email** • **Mobile number** and **SMS gateway** • **Company** • **Department** • **Title** • **Birthdate** • **Language** • **FortiToken Logo** - see FortiTokens on page 132.  When editing a remote user with the **Provision mode** set to **Offline** in Tokens on page 88, you are not required to add an **Email**.
Certificate Bindings	Add, edit, or removed certificate bindings for the user account. See Configuring certificate bindings on page 107.

3. Select **Save** to create the new remote SAML user.

To import remote SAML users:

1. From the remote users list, select **SAML**, and select **Import**.
   The **Import remote SAML Users window** opens.

2. Select the following:

File type	Select the file type to import remote SAML users from: • **SAML Server** • **CSV**
Remote SAML server	Select the remote SAML server on which the users will be imported from.  Only servers with cloud group membership can import users. **Note**: The option is only available when the **File type** is **SAML Server**. For more information on remote SAML servers, see SAML on page 186.
Group	Select the SAML server group to import users from. **Note**: The option is only available when a remote SAML server is selected.
SAML user file (.csv)	Select **Upload a file**, locate the CSV file on your computer, and click **Open**. **Note**: The option is only available when the **File type** is **CSV**.
Advanced options	
Action to take for existing accounts missing from the CSV file	You can select the action to take for existing accounts missing from the CSV file: • **Keep user accounts** • **Disable user accounts** • **Delete user accounts** **Note**: The option is only available when the **File type** is **CSV**.

3. Select **Import** to import the remote SAML users.

To export a SAML users list:

1. From the remote users list, select **SAML**, and select **Export**.
   A `samlusers.csv` file is downloaded on your management computer.

TACACS+ users

To view remote TACACS+ users, go to **Authentication > User Management > Remote Users** and select TACACS+ users in the toolbar. See TACACS+ on page 184 for more information about the remote TACACS+ servers.

The following options are available (when remote TACACS+ users are available to edit):

Create New	Select to create a new remote TACACS+ user.

Delete	Select to delete the selected user or users.
Re-Enable	Select to re-enable the status of a user that has been disabled.
Search	Search the remote TACACS+ users list.
Username	The remote user's name.
Remote TACACS+ Server	The remote TACACS+ server where the user resides.
Admin	Displays whether or not the user is configured as an administrator.
Status	Displays whether or not the user is enabled or disabled.

To create a new remote TACACS+ user:

1. From the remote users list, select **TACACS+** and select **Create New**.
   The **Create New Remote TACACS+ User** window opens.
2. Enter the following information:

Remote TACACS+ Server	Select the remote TACACS+ server on which the user will be created from. For more information on remote TACACS+ servers, see TACACS+ on page 184.
Username	Enter a username.
Disabled	Select to disable the user account. When **Disabled** is enabled, FortiAuthenticator rejects all authentication attempts for the user.
Sync in HA Load Balancing mode	Select to sync the administrator across load-balanced FortiAuthenticator devices from the primary standalone device to load-balancers.
User Role Configure a remote user's role.	

Role	Only **Administrator** role (along with related permissions) is available.
Full Permission	Enable to grant this administrator full permission, or enter an Admin profile in the field provided. This applies only to administrators.
Use backup password	Enable to set up a backup password to be used when the remote server is unreachable. Enter the backup password and enter again to confirm. This applies to administrators.
Restrict admin login from trusted management subnets only	Enable and enter trusted IP addresses and netmasks for restricted administrator login access. This applies to administrators.

3. Click **Save** to create the new remote TACACS+ user.

Remote user sync rules

Synchronization rules can be created to control how and when remote LDAP and SAML users are synchronized.

In case of SCIM user synchronization rule, user changes are pushed by the remote user source acting as the SCIM client to FortiAuthenticator as the SCIM server.

To view a list of the remote user synchronization rules, go to **Authentication > User Management > Remote User Sync Rules**.

Synchronization rules only set the 2FA settings when a user account is newly imported to FortiAuthenticator because enabling 2FA or changing the 2FA method for a user account already imported can render previously working user accounts unable to authenticate to various services.

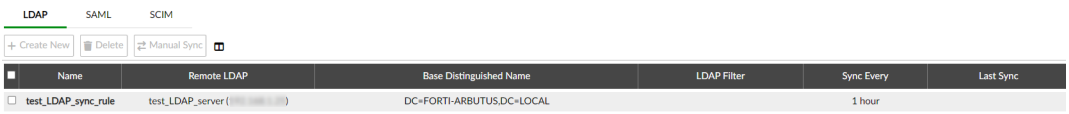
See:

- Remote user sync rules- LDAP on page 116
- Remote user sync rules- SAML on page 119
- Remote user sync rules- SCIM on page 120

Remote user sync rules- LDAP

The remote LDAP user synchronization rules only work with remote LDAP servers for which the group memberships can be retrieved from a user object's attribute.

For example, you must activate the `memberof` overlay if using the synchronization rules with an OpenLDAP server.



The LDAP user synchronization rule list shows the following options:

Create New	Select to create new remote LDAP user synchronization rule.
Delete	Select to delete the selected remote LDAP user synchronization rules.
Manual Sync	Select to manually sync the selected remote LDAP user synchronization rule.

To create a new remote LDAP user synchronization rule:

1. From the **Remote User Sync Rules** page, select **LDAP**, and select **Create New**.
2. Configure the following settings:

Name	Enter a name for the synchronization rule.
Remote LDAP	Select a remote LDAP server from the dropdown menu. To configure a remote LDAP server, see LDAP on page 176.

Base distinguished name	Base DN of the remote LDAP server that automatically populates when a remote LDAP server is selected above.
LDAP filter	Optionally, enter an LDAP filter. Select **Set Group Filter** to set the LDAP filter. This opens the **Set Group Filter** window where you can select one or more groups within the tree to build the LDAP filter string. Click **Use Filter** to confirm the selection.  Once the groups have been selected, the LDAP filter string is set to the proper syntax that filters the selected groups.  The `objectClass` and the `memberOf` portion must be set according to the **User object class** and the **Group membership attribute** setting of the remote LDAP server configuration respectively. See LDAP on page 176. If the LDAP filter is already configured with a non-empty value, selecting **Set Group Filter** attempts to interpret the LDAP filter value to preselect the already configured groups in the LDAP tree. However, if the LDAP filter value does not match the string generated by **Set Group Filter**, the existing filter is ignored, and **Set Group Filter** opens with no preselected groups. Clicking **Use Filter** overwrites the previous LDAP filter. Select **Test Filter** to test that the filter functions as expected. FortiAuthenticator shows an LDAP tree with all the users that match the current remote LDAP server setting (i.e., the users that the sync rule syncs when it runs).
OTP method assignment priority	Select the required authentication synchronization priorities. Drag the priorities up and down in the list change the priority order.  When editing/creating a remote user synchronization rule with **Provision mode** set to **Offline** in Tokens on page 88, **FortiToken Mobile (assign an available token)** cannot be enabled.
FIDO authentication	Select to enable FIDO authentication for synced user accounts. This is disabled by default for new user accounts.
Sync as	Select to synchronize as a remote LDAP user, remote RADIUS user, or a local user.  In the **Synchronization Attributes** pane, selecting **Local User** for **Sync as** results in FortiAuthenticator generating a unique random password for each user imported from AD/LDAP, and emailing the password to the user.

User Role for new user imports	Select the user role to assign to remote users. Users assigned the role of Administrator are granted full permissions.
Remote RADIUS	Specify a remote RADIUS server to associate the imported users with. This dropdown allows you to select from a list of RADIUS servers. Select the pen icon to edit the selected RADIUS server, **+** to create a new RADIUS server, or **x** to delete the selected RADIUS server. This setting is available only when **Remote RADIUS User** is selected as the **Sync as** option. See RADIUS on page 183.
Sync every	Select the amount of time between synchronizations.
Group to associate users with	Optionally, select a group from the dropdown menu with which to associate the users with, or select **Create New** to create a new user group. See User groups on page 126. When **Sync as** is set to **Remote RADIUS User**, this option contains a list of remote RADIUS user groups to choose from.
FortiToken Logo	Optionally, select a logo from the **FortiToken Logo** dropdown menu to associate the imported users with the specified logo. This logo is displayed beside the one-time password in FortiToken. See FortiTokens on page 132 for more information.
Certificate binding CA	Select CA certificates from the **Certificate binding CA** dropdown for users who use remote user sync rules. When the **Certificate binding common name** field is populated (under **LDAP User Mapping Attributes**) this field must also be specified.
Sync users to IAM Account	Select an IAM account to synchronize the remote users with.
Password recovery by email	When enabled, FortiAuthenticator will enable the email password recovery setting for new and existing remote LDAP users if they also have a valid email address. A password reset link is sent to the email address. When disabled (default), the email password recovery setting will not be available to new or existing remote LDAP users.
Password recovery by SMS	When enabled, FortiAuthenticator will enable the SMS password recovery setting for new and existing remote LDAP users if they provided a phone number. A verification code is sent to the mobile number. When disabled (default), the SMS password recovery setting will not be available to new or existing remote LDAP users.
Password recovery by FortiToken	When enabled, FortiAuthenticator will enable the FortiToken password recovery setting for new and existing remote LDAP users if they have a FortiToken. The password is recovered by using an MFA token device. When disabled (default), the FortiToken password recovery setting will not be available to new or existing remote LDAP users.

Do not delete synced users when they are no longer found on the remote server	Select to ensure that synchronized users are not deleted when they are no longer found on the remote server. This option is only available when **Proceed with rule even when response empty** is disabled.
Proceed with rule even when response empty	Select to enforce the synchronization rule even when the LDAP response is empty. Use this option to delete all users from a FortiAuthenticator group when synchronization rule returns an empty response. This option is only available when **Do not delete synced users when they are no longer found on the remote server** is disabled. **Warning**: This option should be used with caution. An error from the administrator (e.g. a typo when changing the LDAP query) could cause the deletion of all existing synchronized users, requiring the administrator to reprovision any assigned FortiTokens.
LDAP User Mapping Attributes	Optionally, edit the remote LDAP user mapping attributes.
Debugging Settings	Optionally, log synchronization details, including LDAP query results. These log files can be downloaded under **Debug Report > LDAP Sync**. In addition, select whether to delete synchronized users when they are no longer found on the remote server.
Preview Mapping	Select to preview the LDAP user sync mappings in a new window.
Show Sync Fields	Select to view the user fields that will be synchronized.

3. Select **Save** to create the new LDAP synchronization rule.

Remote user sync rules- SAML

The SAML user synchronization rule list shows the following options:

Create New	Select to create new remote SAML user synchronization rule.
Delete	Select to delete the selected remote SAML user synchronization rules.
Manual Sync	Select to manually sync the selected remote SAML user synchronization rule.

To create a new remote SAML user synchronization rule:

1. From the **Remote User Sync Rules** page, select **SAML**, select **Create New**.
2. Configure the following settings:

Name	Enter a name for the synchronization rule.
Remote SAML server	Select a remote SAML server from the dropdown menu. To configure a remote SAML server, see SAML on page 186.

SAML group	Select a group from the SAML server. SAML groups are retrieved dynamically from the server.
Token-based authentication sync priorities	Select the required authentication synchronization priorities. Drag the priorities up and down in the list change the priority order. When editing/creating a remote user synchronization rule with **Provision mode** set to **Offline** in Tokens on page 88, **FortiToken Mobile (assign an available token)** cannot be enabled.
Sync every	Select the amount of time between synchronizations.
Group to associate users with	Optionally, select a group from the dropdown menu with which to associate the users with. See User groups on page 126.
FortiToken Logo	Optionally, select a logo from the **FortiToken Logo** dropdown menu to associate the imported users with the specified logo. This logo is displayed beside the one-time password in FortiToken. See FortiTokens on page 132 for more information.
Do not delete synced users when they are no longer found on the remote server	Select to ensure that synchronized users are not deleted when they are no longer found on the remote server. This option is only available when **Proceed with rule even when response empty** is disabled.
SAML User Mapping Attributes	Optionally, edit the remote SAML user mapping attributes.

3. Select **Save** to create the new SAML synchronization rule.

Remote user sync rules- SCIM

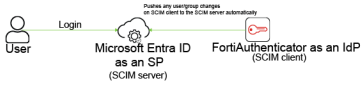
SCIM

System for Cross-domain Identity Management (SCIM) is an open standard for automating user identity information exchange between an identity provider (IdP) and a service provider (SP) requiring user identity information, e.g., enterprise SaaS applications.

SCIM makes user data more secure and simplifies the user experience by automating the user identity provisioning and management process.

SCIM is a REST and JSON based protocol that defines a client and a server role.

The following is an example of SCIM implementation with Microsoft Entra ID as the SP and FortiAuthenticator as the IdP:



When changes to identities are made in the IdP, including creating, updating, and deleting, they are automatically synced to the SP according to the SCIM protocol.

The IdP can read identities from the SP to add to its directory and detect inconsistencies in the SP that potentially create security vulnerabilities. This provides a seamless access to applications for which end users are assigned, with up-to-date profiles and permissions.

In the SCIM context, the SCIM SP is the SCIM client and the SCIM server is the SCIM relying party. This is not to be confused with the SAML SP and the OIDC relying party.

The SCIM server role is needed to allow automated provisioning from an external IdP, e.g., Microsoft Entra ID to FortiAuthenticator acting as the IdP proxy.

Prerequisites

In general, the following are necessary to configure SCIM:

- SCIM client account with appropriate level of permissions and complimentary SCIM capabilities.
- FortiAuthenticator administrator with **Administrator** role is required to generate an API key.

Considerations

- The SCIM client is where the identities are sourced and serves as the primary for user attributes. Once the identity is added to FortiAuthenticator, you can manage access and authentication and extend the identity to all the downstream SAML SPs federated and OIDC rely parties (RP) to FortiAuthenticator as the IdP and OIDC provider, respectively.
- When a user is created on the SCIM client, the user has the option to be added as a user to FortiAuthenticator as a user with a pending password status (the user must establish and maintain a password within FortiAuthenticator), thereby becoming a local user in FortiAuthenticator.
- The other option is for the user created in FortiAuthenticator to keep its password on the SCIM client, i.e., the upstream IdP, and add the user to FortiAuthenticator as a remote user.
- The generic SCIM integration uses SCIM version 2.0.
- The FortiAuthenticator SCIM API is based on the version 2.0 of the SCIM Standard.

See How to integrate a generic SCIM client with FortiAuthenticator SCIM server on page 123.

SCIM vs the FortiAuthenticator legacy remote synchronization rule

In the FortiAuthenticator legacy remote sync rule, FortiAuthenticator pulls the user changes by querying the remote user source whereas in the case of SCIM, the user changes are pushed by the remote user source acting as the SCIM client to FortiAuthenticator as the SCIM server.

In addition to the user account information, SCIM protocol allows pushing the user groups to FortiAuthenticator.

The SCIM user synchronization rule list shows the following options:

Create New	Select to create new remote SCIM user synchronization rule.
Delete	Select to delete the selected remote SCIM user synchronization rules.

To create a new remote SCIM user synchronization rule:

1. From the **Remote User Sync Rules** page, select **SCIM**, select **Create New**.
2. Configure the following settings:

Name	Enter a name for the SCIM synchronization rule.
URL	The SCIM base URL for FortiAuthenticator. (`https://[FQDN]/scim/v2/`)
OTP method assignment priority	Select the required authentication synchronization priorities: • **FortiToken Cloud - Default** • **FortiToken Cloud - FortiToken Mobile** • **FortiToken Cloud - FortiToken Hardware** • **FortiToken Cloud - Email** • **FortiToken Cloud - SMS** • **Email** • **SMS** • **Dual (Email and SMS)** • **None (users are synced explicitly with no token based authentication)**  Drag the priorities up and down in the list change the priority order.
FIDO authentication	Select to enable FIDO authentication for synced user accounts. This is disabled by default for new user accounts.
Sync as	Select to synchronize as a remote SAML user, remote LDAP user, or a remote RADIUS user.
User role for new user imports	Select the user role to assign to remote users. Users assigned the role of Administrator are granted full permissions.
FortiToken Logo	Optionally, select a logo from the **FortiToken Logo** dropdown menu to associate the imported users with the specified logo. This logo is displayed beside the one-time password in FortiToken. See FortiTokens on page 132 for more information.
Certificate binding CA	Select CA certificates from the **Certificate binding CA** dropdown for users who use remote user sync rules. When the **Certificate binding common name** field is populated (under **SCIM User Mapping Attributes**) this field must also be specified.
Email password recovery	When enabled, FortiAuthenticator will enable the email password recovery setting for new and existing remote users if they also have a valid email address. When disabled (default), the email password recovery setting will not be available to new or existing remote users.
SCIM User Mapping Attributes	Optionally, edit the SCIM user mapping attributes.

SCIM Group Mapping Attributes		
	Group display name	The SCIM group display name attribute, e.g., `displayName`.
	Group members	The SCIM group member attribute, e.g., `members`.

3. Select **Save** to create the new SCIM user synchronization rule.
4. After creating the SCIM user sync rule, the **SCIM Secret Token** window opens:
   The secret token is used to authorize the SCIM integration between the client and the server.
   You can share the randomly generated secret token (API access key).
   Note: The secret token is associated with an administrator account. You must use an administrator account with appropriate role.
   a. A new secret token is generated.
   b. Enable **Send Email** and enter the email address to send the SCIM secret token.

You can view secret token by clicking the eye icon.

Select the copy icon () to copy the secret token.
You can then save it on your management computer.

   c. Click **OK**.

The SCIM secret token is no more visible once you close the **SCIM Secret Token** window.

Only when editing a remote SCIM user sync rule, **SCIM Secret Token** window can be accessed by selecting **Change Secret Token**.

How to integrate a generic SCIM client with FortiAuthenticator SCIM server

The following describes how to integrate a generic SCIM client with the FortiAuthenticator SCIM server:

1. Log in to FortiAuthenticator.
2. Get an API key.
   Alternatively, use OAuth 2.0.
3. Copy the API key and paste it in the appropriate field on the SCIM SP, i.e., the SCIM client.
4. Log in to the SCIM SP administrator account.
   Note that every SCIM SP has a different way of accessing application integrations.
5. Create a custom application for FortiAuthenticator in the SCIM SP.

6. Each SCIM SP has different questions for the application. However, all SCIM SPs require a Tenant URL and a FortiAuthenticator API key (**Secret Token**):
   a. **Tenant URL**: The **URL** field when creating or editing a remote SCIM user sync rule.
   b. **API key**: The **Secret Token** when creating or editing a remote SCIM user sync rule. The secret token is used to authorize the SCIM integration between the client and the server.
      Note: The secret token is associated with an administrator account. You must use an administrator account with appropriate role.
7. The SCIM client indicates that FortiAuthenticator was created successfully.
8. The SCIM client application gallery confirms the newly created application.
   All the other settings to integrate with FortiAuthenticator should be set, including attribute mappings.
9. The SCIM client is now visible in FortiAuthenticator.
10. You can now configure attribute mappings on FortiAuthenticator.
    See Creating a new remote SCIM user synchronization rule.

Guest users

Guest user accounts can be created as needed. Guest users are similar to local users, only they are created with a restricted set of attributes.

To manage guest user accounts, go to **Authentication > User Management > Guest Users**.

Users can be authenticated against local or remote user databases with single sign-on using client certificates or SSO (Kerberos/SAML).

Common use cases might include:

- Hotel receptionists creating room accounts
- Office staff creating visitor accounts

Newly created account information can be sent to users via email, SMS, or printed out individually.

Each guest user account counts as one user towards the user license limit.

To create a new guest user/multiple guest users:

1. Go to **Authentication > User Management > Guest Users** and select **Create New**.
2. Enter the following information:

The "Sponsor" role for local and remote users is equivalent to an administrator with Read-Write permissions to the **Guest Users** sub-menu only.

General		
	Creation Mode	There are three guest user creation methods: • **Express**: Quickly create guest user accounts without the need to enter

		any user information. Guest accounts generated this way only have four attributes: **Sponsor**, **Username** (eight random lowercase letters–must be unique from any other existing user account), **Password**, and **Expiry**. • **From CSV file**: Create guest user accounts using information from a CSV file in the following format: **<first name>, <last name>, <email>, <mobile>, <group>**. • **Manual Input**: Create guest user accounts by manually entering the user attributes for each guest user.
	Expiry date	Set the date that the guest user account(s) will expire.
	Expiry time	Set the time that the guest user account(s) will expire. The time can either be manually entered, or defined from four options: **Now**, **Midnight**, **6 a.m.**, or **Noon**.
Express		The following is only available when **Creation Mode** is set to **Express**.
	Number of new guest users	Number of new guest users to add, up to a maximum of 1000.
	Sponsor	When an admin creates a guest user account, the admin selects the sponsor from the dropdown. Sponsors do not have this capability. This option is only available when the admin creates a guest user account. When a sponsor creates a guest user account, the guest user is automatically assigned to the sponsor creating it.
	Groups	Choose user groups from the list available to assign the new guest users.
CSV Import		The following is only available when **Creation Mode** is set to **From CSV file**.
	CSV file	Choose a CSV file to import the user attributes.
Guest Basic Information		The following is only available when **Creation Mode** is set to **Manual Input**.
	Add Guest User	Manually enter guest user information, including their **First name**, **Last name**, **Email address**, **Mobile number**, **Groups**, and **Actions**. Choose user groups from the list available to assign the new guest users.

3. Click **Save**.
The **Export Guest User** window opens with the following options:

Print	Print the guest user information.
Email	Select to open the **Send Guest User Credential Via Email** window, enter the Email, and select **Send**.
Export	Select to export the guest user information as a CSV file.

SMS	Select the SMS icon to open the **Send Guest User Credential Via SMS** window, enter the mobile phone number, and select **Send**.

4. Click **Save** to add the guest user.

When editing a guest user:

- The password is obfuscated by default.
  Upon clicking the eye ( ) icon, the current password is displayed.
  Reclicking the eye icon obfuscates the password again.
- Clicking the **Set a random password** ( ) icon sets a random password.
- Click the **Change password** ( ) icon to manually change the password.
  Note: The password must be at least 8 and at most 64 characters in length.

User groups

Users can be assigned to groups during user account configuration (see Editing a user on page 99), or by editing the groups to add users to it.

To view the user groups list, go to **Authentication > User Management > User Groups**.

User groups can be created for MAC devices. However, MAC devices will only be available to add in a MAC user group after devices have been created or imported.
See MAC devices for more information.

The user groups list shows the following information:

Create New	Select to create user groups.
Import	Select to import user groups from a CSV file. See Importing user groups on page 129.
Export	Select to export the user group list to a CSV file.
Delete	Select to delete the selected user groups.
Edit	Select to edit the selected user groups.
Search	Enter a search term in the search field, then select **Search** to search the user group list.

To create a new user group:

1. Go to **Authentication > User Management > User Groups** and select **Create New**.
2. Enter the following information:

Name	Enter a name for the group.
Type	Select the type of group:

	• **Local** (default) • **Remote LDAP** • **Remote RADIUS** • **Remote SAML** • **MAC**
Subtype	Select from the following three options: • **LDAP directory group**: Maps to a group object at the specified Distinguished Name in the remote LDAP directory. • **List of users** • **LDAP filter (advanced)** (default): Queries the remote LDAP server with a custom filter that returns the list of member users. This option is only available if **Type** is **Remote LDAP**.
Visible to Sponsors	Enable to make the user group visible to sponsors in the Sponsor Portal. This option is only available if **Type** is **Local**.
Users	Select users from the search box. This option is only available if **Type** is **Local**.
Password policy	Select a password policy from the dropdown. A default password policy is already selected, see Passwords on page 86. This option is only available if **Type** is **Local**.
Usage Profile	Enable to determine user time and data usage on a granular level. Select a usage profile from the dropdown. At least one usage profile must already be configured, see Usage profile on page 129. This option is only available if **Type** is **Local**, **Remote LDAP**, or **Remote RADIUS**.
Remote LDAP	Select a remote LDAP server from the dropdown menu. At least one remote LDAP server must already be configured, see Remote authentication servers on page 176. This option is only available if **Type** is **Remote LDAP**.
Remote RADIUS	Select a remote RADIUS server from the dropdown menu. At least one remote RADIUS server must already be configured, see Remote authentication servers on page 176. This option is only available if **Type** is **Remote RADIUS**.
LDAP filter	Enter an **LDAP filter**. Optionally, select **Test filter** to ensure that the filter works as expected. Selecting **Set Group Filter** imports the **Distinguished name** of the selected LDAP group only. Select **Set Group Filter** to set the LDAP filter. This opens the **Set Group Filter** window where you can select one or more groups within the tree to build the LDAP filter string. Click **Use Filter** to confirm the selection.

	 Once the groups have been selected, the LDAP filter string is set to the proper syntax that filters the selected groups.  The `objectClass` and the `memberOf` portion must be set according to the **User object class** and the **Group membership attribute** setting of the remote LDAP server configuration respectively. See LDAP on page 176. If the LDAP filter is already configured with a non-empty value, selecting **Set Group Filter** attempts to interpret the LDAP filter value to preselect the already configured groups in the LDAP tree. However, if the LDAP filter value does not match the string generated by **Set Group Filter**, the existing filter is ignored, and **Set Group Filter** opens with no preselected groups. Clicking **Use Filter** overwrites the previous LDAP filter. Select **Test Filter** to test that the filter functions as expected. FortiAuthenticator shows an LDAP tree with all the users that match the current remote LDAP server setting (i.e., the users that the sync rule syncs when it runs). This option is only available if **Type** is **Remote LDAP** and **Subtype** is set to **LDAP filter (advanced)**.
LDAP users	Select remote LDAP users from the **LDAP users** search box. This option is only available if **Type** is **Remote LDAP** and **Subtype** is set to **List of users**.
RADIUS users	Select remote RADIUS users from the **RADIUS users** search box. This option is only available if **Type** is **Remote RADIUS**.
Remote saml	Select a remote SAML server from the dropdown menu. At least one remote SAML server must already be configured, see Remote authentication servers on page 176. This option is only available if **Type** is **Remote SAML**.
SAML users	Select remote SAML users from the **SAML users** search box. This option is only available if **Type** is **Remote SAML**.
MAC devices	Select from **Available MAC Devices** and move them to the **Chosen MAC Devices** box to add them to the group. This option is only available if **Type** is **MAC**.
TACACS+ authorization rule	Select a TACACS+ authorization rule to apply to the user group.
Include for FSSO	Enable to specify if the remote LDAP group is included for FSSO. The option is disabled by default. The option is only available when the **Type** is **Remote LDAP** and **Subtype** is **List of Users**.

RADIUS Attributes	See RADIUS attributes on page 137.
SAML Assertion Attributes	Select **Add SAML Assertion Attribute** and enter the **Attribute name** and the **Attribute value**. To add additional SAML assertion attributes, select **Add SAML Assertion Attribute**.

3. Select **Save** to create the new group.

To edit a user group:

1. In the user group list, select the group that you need to edit.
2. Edit the settings as required. The settings are the same as when creating a new group.
3. Select **Save** to apply your changes.

User groups for MAC-based RADIUS authentication

Once created, MAC user groups can then be used under the MAC-based authentication section of RADIUS clients, under **Authentication > RADIUS Service > Clients**. See RADIUS service for more information.

Importing user groups

To import user groups:

1. From the user group list, select **Import**.
   The **Import FAC groups** page opens.
2. Select the following:

FAC group file (.csv)	Select **Upload a file**, locate the CSV file on your computer, and click **Open**.	
Advanced options		
	Action to take for existing groups missing from the CSV file	You can select the action to take for existing groups missing from the CSV file: • **Keep groups** • **Delete groups**

3. Select **Import** to import user groups.

Usage profile

Usage profiles can be created to determine user time and data usage on a granular level.

To view the usage profile list, go to **Authentication > User Management > Usage Profile**.

To create a new usage profile:

1. Go to **Authentication > User Management > Usage Profile** and select **Create New**.
2. Enter the following information:

Name		Enter a name for the profile.
Description		Optionally, enter information about the usage profile.
Time Usage		Select how time usage is determined.
	Time limit	For this profile, the user's time limit will be either unlimited or measured from the moment their account was created, from when they first logged on, or how much time they have used. When the method has been chosen, enter the time period, in either **minutes**, **hours**, **days**, **weeks**, or **months**. The default is set to seven days.
Data Usage		Select how data usage is determined.
	Data limit	For this profile, the user's data limit will either be **Unlimited**, restricted to the cumulative amount of data they have used, or restricted to the amount of data used per time interval. When **Cumulative data used** is selected, enter the data amount in either **KB**, **MB**, **GB**, or **TB**. **Note**: The default is set to 1 GB. When **Data used per time interval** is selected, enter the data amount in either **KB**, **MB**, **GB**, or **TB**. From the time period dropdown, select from the following: • **daily** • **weekly** • **monthly** **Note**: The default is set to 1 GB daily.
Time Schedule		Select the timezone the usage profile should follow.
	Timezone	Timezone the usage profile should follow. The default is set to (GMT) UTC - No Daylight Savings.
Devices		Limit number of concurrent MAC devices per user.
	Maximum devices per user	Enter the maximum number of different MAC device addresses allowed concurrently for every user in the active RADIUS accounting sessions. By default, the **Max. devices per user** is set to `0`. When set to `0`, MAC devices control is disabled, i.e., there is no limit on the number of concurrent MAC devices per user.

3. Select **Save** to add the new usage profile.

Realms

Realms allow multiple domains to authenticate to a single FortiAuthenticator unit. LDAP, RADIUS, and SAML remote servers are supported. Each RADIUS realm is associated with a name, such as a domain or company name, that is used during the login process to indicate the remote (or local) authentication server on which the user resides.

For example, the username of the user **PJFry**, belonging to the company **P_Express**, would become any of the following, depending on the selected format:

- **PJFry@P_Express**
- **P_Express\PJFry**
- **P_Express/PJFry**

The FortiAuthenticator uses the specified realm to identify the back-end RADIUS, LDAP, or SAML authentication server (s) used to authenticate the user.

Acceptable realms can be configured on a per RADIUS server client basis.

See Realms on page 131.

The administrator must log in with their username only, i.e., `username + realm` is no longer accepted.

To manage realms, go to **Authentication > User Management > Realms**.

The following options are available:

Create New	Select to create a new realm.
Delete	Select to delete the selected realm or realms.
Edit	Select to edit the selected realm.
Name	The names of the realms.
User Source	The source of the users in the realms.
Chained token authentication with remote RADIUS server	Available when **User source** is set to an LDAP server. Enable from the dropdown menu to chain token authentication with a RADIUS server.
Restrict authentication to imported user account only	Available when **User source** is set as LDAP, RADIUS, or SAML servers. Enable to only allow remote authentications for imported remote user accounts.

To create a new realm:

1. From the realms list, select **Create New**.
2. Enter a **Name** for the realm.

The realm name may only contain letters, numbers, periods, hyphens, and underscores. It cannot start or end with a special character.

3. Select the **User source** for the realm from the dropdown menu.
   The options include **Local users**, or from specific RADIUS, LDAP, or SAML servers.
4. Enable **Chained token authentication with remote RADIUS server**.
   Note: The option is only available when selecting a remote LDAP server as the **User source**.
   Chained authentication provides the ability to chain two different authentication methods together so that, for example, a two-factor authentication RSA solution can validate passcodes via RADIUS.
5. Enable **Restrict authentication to imported user account only**.
   Notes:
   - The option is only available when selecting a remote LDAP, RADIUS, or SAML servers as the **User Source**.
   - The option provides the ability to only allow remote authentications for imported remote user accounts.
6. Select **Save** to create the new realm.

FortiTokens

Go to **Authentication > User Management > FortiTokens** to view a list of configured FortiTokens. From here, FortiTokens can be added, imported, exported, edited, deleted, and activated.

There is a delay of 5 to 10 minutes before a freshly assigned FortiToken is activated on a mobile device and when it can deliver PUSH notifications.

The delay is expected, even when all the components needed for FortiToken Mobile PUSH are configured correctly.

It applies after FortiToken Mobile activation is finished on a mobile device and before the authentication request/attempt.

Once the token is activated on a mobile device in the FortiToken Mobile application, it can be used immediately for authentication.

- However, a PUSH notification might not be delivered at all if that authentication attempt happens within a period of up to 5 to 10 minutes after token activation.
- If everything is configured correctly, any authentication attempted past 10 minutes after activation is expected to receive a PUSH notification.

When the FortiToken Mobile is firstly provisioned, push notification may not be available for up to 300 seconds (5 minutes) or after the manual token authentication.

See FortiToken physical device and FortiToken Mobile on page 140 for more detailed information.

The following information is shown on the **FortiTokens** tab:

Create New	Create a new FortiToken.
Import	Import a list of FortiTokens from a serial number CSV file, a seed CSV file, or from a FortiGate configuration.
Export FTK Hardware	Export the FortiToken list.
Refresh FTM	Refresh the **Status** of a FortiToken Mobile token.
Delete	Delete the selected FortiToken(s).
Edit	Edit the selected FortiToken. **Note:** When editing a FortiToken, you can now see the last used date and time.
Activate	Activate the selected FortiToken(s).
Unlock	Unlock the selected FortiToken(s).
Search	Search the FortiToken list.
Serial number	The FortiToken's serial number.
Token type	The FortiToken type, either **FortiToken Hardware** or **FortiToken Mobile**.
Status	Whether or not the FortiToken is activated.
Comment	Comments about the token.
User	The user to whom the FortiToken applies.
Algorithm	The FortiToken's encryption.
Size	The size of the token.
Drift/Counter	The time difference between the FortiAuthenticator and the FortiToken.
Timestep	The FortiToken timestep.
FTM license	The FortiToken Mobile license applied to the FortiToken.
Platform	The FortiToken's platform.
Last used	The last used date and time for the FortiToken.

Logos

FortiToken can include an organization's logo. Logos can be associated with local and remote users.

When a user provisions FortiToken Mobile on their device, the organization's logo is automatically pushed to the device, rebranding the user interface of the FortiToken Mobile application.

Logos can be created, edited, and deleted as needed. Logos are applied to users from the various user management pages. See Local users on page 95, Remote users on page 107, and Remote user sync rules on page 116 for more information.

To manage FortiToken's logos, go to **Authentication > User Management > FortiTokens > Logos**.

The following information is shown on the **Logos** tab:

Create New	Create a new logo.
Delete	Delete the selected logo(s).
Edit	Edit the selected logo.

To create a new logo:

1. From the **Logos** tab, click **Create New**.
2. Enter a **Name** for the organization.
3. Upload a logo file on your computer. The image can be a maximum of 320x320 pixels, and must be 24-bit PNG file.
4. Select **Save** to create the new logo.

MAC devices

Non-802.1X compliant devices can be identified and accepted onto the network using MAC address authentication. See Non-compliant devices on page 244 for more information.

Go to **Authentication > User Management > MAC Devices** to view a list of configured MAC devices. From here, MAC devices can be created, imported, exported, edited, and deleted.

The following information is shown:

Create New	Create a new MAC-based authentication devices.
Import	Import a list of MAC devices from a CSV file. See Importing MAC devices from a CSV file on page 135.
Export	Export a list of MAC devices to a CSV file.
Delete	Delete the selected MAC device(s).
Edit	Edit the selected MAC device.
Search	Enter a search term in the search field, then select **Search** to search the MAC devices list.

Once created/imported, MAC devices can be added to MAC user groups. See User groups for more information.

Importing MAC devices from a CSV file

To import MAC devices from a CSV file:

1. From the MAC devices list in **Authentication > User Management > MAC Devices**, select **Import**.
   The **Import MAC Devices** window opens.

2. Select **Upload a file**, locate the MAC devices CSV file on your management computer, and select **Open**.
3. Optionally, from the **Add MAC device(s) to group** dropdown, select a MAC devices user group where the imported MAC devices are added to.
4. Click **Save**.

Device tracking

When enabled, this feature allows end users to self-register their devices, and to have those devices tracked, based on the device MAC address.

An unregistered device is granted restricted network access, and is redirected to the FortiAuthenticator guest portal. The user enters valid credentials, then the FortiAuthenticator detects the unregistered device and offers the user an option to register it. If the user registers the device, it becomes part of their authorized device group and the user is granted network access on that device (if the user does not register the device, they are redirected to the guest portal login page).

To link a device **to** a user configuration, create a new MAC-based authenticaation device entry under **Authentication > User Management > MAC Devices**, and enable **This device belongs to a user**. Similarly, it is possible to link a device *from* a user configuration. In either case, names and MAC addresses must be unique.

To fully benefit from this feature, you must use a FortiAuthenticator in conjunction with a FortiGate running FortiOS 6.0+.

Identity and Account Management (IAM)

Previously, each FortiCloud customer account had one set of usernames (email addresses) and passwords. All devices were registered under one account, making it difficult to implement *Roles* in FortiCloud. To solve this, FortiAuthenticator allows you to configure IAM users and accounts. Each IAM user is unique to an IAM account, whereas each IAM account is unique to the FortiAuthenticator instance or cluster. For more information on IAM users, see *IAM user* in the *Identity & Access Management 23.1.a Administration Guide*.

To view IAM users and accounts, go to **Authentication > User Management > IAM**, and toggle between **Users** or **Accounts**.

The IAM users and accounts list shows the following information:

Create New	Select to create an IAM account or user.
Delete	Select to delete the selected IAM accounts or users.
Import	Select to import IAM users. In the **Import IAM Users** window, enter information as shown in To create an IAM user.
Edit	Select to edit the selected IAM account. In the **Edit IAM Account** window, enter information as shown in To create an IAM account.

To create an IAM account:

1. Go to **Authentication > User Management > IAM**.
2. Select **Accounts**, and then select **Create New**.
3. Enter the following information:

Account Name	Enter the account name. The name must be unique among all the IAM accounts.
Alias	Enter alias. This must be unique among all the IAM accounts.

4. Click **Save**.

To create an IAM user:

1. Go to **Authentication > User Management > IAM**.
2. Select **Users**, and then select **Create New**.
3. Enter the following information:

Username	Enter the account name. The name must be unique within the selected IAM account.
Administrator	Enable to give this user administrator privileges. An administrator can manage users within the same account.
Account	From the dropdown, select the account to add this user to. Use the pen icon to edit the selected account, **+** to create a new IAM account, and **x** to delete the selected IAM account.
User Type	Select the user account type, either **Local** or **Remote LDAP**.
Local User	From the dropdown, select the local user. This option is only available when the **User Type** is **Local**.
Remote LDAP server	From the dropdown, select the Remote LDAP server. This option is only available when the **User Type** is **Remote LDAP**.
LDAP User	From the dropdown, select the LDAP user. This option is only available when the **User Type** is **Remote LDAP**.

4. Click **Save**.

RADIUS attributes

Some services can receive information about an authenticated user through RADIUS vendor-specific attributes. FortiAuthenticator user groups and user accounts can include RADIUS attributes for Fortinet and other vendors.

Attributes in user accounts can specify user-related information. For example, the **Default** attribute **Framed-IP-Address** specifies the VPN tunnel IP address sent to the user by the Fortinet SSL VPN.

Attributes in user groups can specify more general information, applicable to the whole group. For example, specifying third-party vendor attributes to a switch could enable administrative level login to all members of the **Network_Admins** group, or authorize the user to the correct privilege level on the system.

To add RADIUS attributes to a user or group:

1. Go to **Authentication > User Management > Local Users** and select a user account to edit, or go to **Authentication > User Management > User Groups** and select a group to edit.
2. In the **RADIUS Attributes** section, select **Add RADIUS Attribute**.
3. Select the appropriate **Vendor** and **Attribute ID**.
4. Set the RADIUS attribute **Value Type** to a **Static** or a **Dynamic** value.
   Note: The **Value Type** option depends on the **Vendor** and **Attribute ID** selection.
   The following restrictions apply to the new **Dynamic** option:
   - When the user group is local or remote RADIUS groups, the **Dynamic** option is only available if the RADIUS attribute type is **String**.
   - When the user group is remote LDAP, the **Dynamic** option only available if RADIUS attribute type is **String** or **IP**.
   - When the user group is remote SAML or MAC groups, the **Dynamic** option is not available.
5. When **Static** is selected, enter attribute's value in the **Value** field.
   When **Dynamic** is selected, select an option from the **User attribute** dropdown.
   The user attribute provides value(s) for the RADIUS attribute.
6. Select **Save** to add the new attribute to the user or group.
7. Repeat the above steps to add additional attributes as needed.

SCIM

System for Cross-domain Identity Management (SCIM) is an open standard for automating user identity information exchange between an identity provider (IdP) and a service provider (SP).

In **Authentication > SCIM > Service Provider**, you can create and edit SCIM service providers. See Service providers on page 137.

Service providers

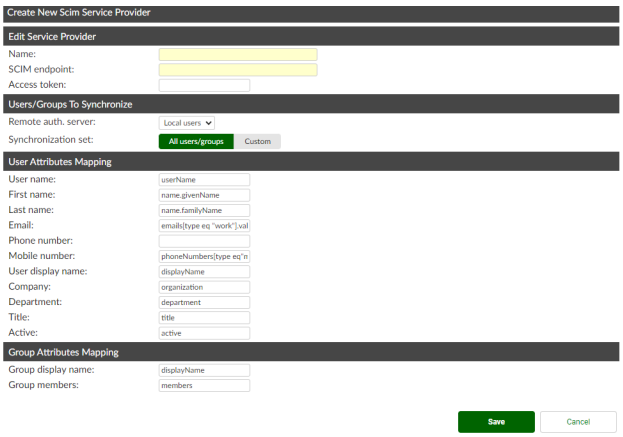
Service providers (SP) can be managed from **Authentication > SCIM > Service Provider**.

For the connection to the SCIM server to succeed, the SCIM server CA certificate must be imported into FortiAuthenticator in the **Trusted CAs**.

See Trusted CAs on page 307.

To configure SCIM service provider settings:

1. In **Authentication > SCIM > Service Provider**, select **Create New**.
   The **Create New Scim Service Provider** window opens.



2. Enter the following information:

Edit Service Provider		
	Name	Enter the name for the SCIM SP.
	SCIM endpoint	Enter the SCIM SP IP address.
	Access token	Enter the SCIM SP access token.
Users/Groups To Synchronize		
	Remote auth. server	From the dropdown, select a remote authentication server (LDAP, RADIUS, or SAML) or select local users.
	Synchronization set	Select from the following two options to synchronize users/groups: • **All users/groups** (default) • **Custom**: Select user groups from **Available Groups** list and move them to the **Chosen Groups** list. Only the selected user groups and the members of those user groups are synced.

For remote LDAP servers, only groups with the list of users are included. These are groups without LDAP filter.

User Attributes Mapping

User name	Enter the user name. Set to **userName** by default.
First name	Enter the attribute that specifies the user's first name. Set to **name.givenName** by default.
Last name	Enter the attribute that specifies the user's last name. Set to **name.familyName** by default.
Email	Enter the attribute that specifies the user's email address. Set to **emails[type eq "work"].value** by default.
Phone number	Enter the attribute that specifies the user's phone number.
Mobile number	Enter the attribute that specifies the user's mobile number. Set to **phoneNumbers[type eq"mobile"].value** by default.
User display name	Enter the attribute that specifies the user's display name. Set to **displayName** by default.
Company	Enter the attribute that specifies the user's company. Set to **organization** by default.
Department	Enter the attribute that specifies the user's department. Set to **department** by default.
Title	Enter the attribute that specifies the title. Set to **title** by default.
Active	Enter the attribute that specifies the user status. Set to **active** by default.

Custom fields configured in **Authentication > User Account Policies > Custom User Fields** are available here.

Group Attributes Mapping

Group display name	Enter the attribute that specifies the group's display name. Set to **displayName** by default.
Group members	Enter the attribute that specifies group's members. Set to **members** by default.

3. Click **Save**.

FortiToken physical device and FortiToken Mobile

A FortiToken device is a disconnected one-time password (OTP) generator. It is a small physical device with a button that when pressed displays a six digit token passcode. FortiToken Mobile is an application for mobile devices that performs the same one-time password function as a FortiToken device.

Each FortiAuthenticator unit or VM is supplied with two trial FortiToken Mobile tokens. To obtain the free FortiToken Mobile tokens (if they have not been created dynamically on install), select **Get FortiToken Mobile trial tokens** when adding a FortiToken Mobile token. This may be required if, for example, you are upgrading an unlicensed FortiAuthenticator unit to a licensed one, as the old tokens associated with the unlicensed serial number will not be compatible with the new, licensed serial number. The tokens will still work, but they cannot be reassigned to a new user. In this case, you must delete the old tokens, and then generate new ones.

Time-based token passcodes require that FortiAuthenticator clock is accurate. If possible, configure the system time to synchronize with an NTP server.

To perform token-based authentication, the user must enter the token passcode. If the user's username and password are also required, this is called two-factor authentication. The displayed code changes every 60 seconds.

FortiAuthenticator supports FortiToken OTP push notifications, or FTMv4 push notifications. Using FTMv4, when required to authenticate themselves, FortiToken Mobile users don't have to look-up a code in FortiToken and enter the code into their browser. Instead FortiToken Mobile is queried and the user just responds to accept the connection and the session is authenticated.

To migrate FortiToken Mobile tokens from FortiAuthenticator to FortiToken Cloud, see *Migrate FTM tokens from FortiAuthenticator* in the latest *FortiToken Cloud Admin Guide*.

FortiAuthenticator and FortiTokens

With FortiOS, FortiToken identifiers must be entered into the FortiGate unit, which then contacts FortiGuard servers to verify the information before activating them.

FortiAuthenticator on the other hand acts as a repository for all FortiToken devices used on your network. It is a single point of registration and synchronization for easier installation and maintenance.

To register FortiTokens, you must have a valid FortiGuard connection; otherwise, any FortiTokens you enter will have an **Inactive** status. However, after the FortiTokens are registered, the connection to FortiGuard is no longer essential.

For activating physical FortiTokens in an air-gapped environment, you can request a seed file from the Fortinet Customer Service and upload it locally without needing FortiGuard or Internet access.

If a token authentication fails, check that the system time on FortiAuthenticator is correct and re-synchronize the FortiToken.

To add FortiTokens manually:

1. Go to **Authentication > User Management > FortiTokens** and select **Create New**.
2. Select the **Token type**, either **FortiToken Hardware** or **FortiToken Mobile**.
3. If **FortiToken Hardware** is selected, enter one or more token serial numbers in the **Serial numbers** field.
   You can also import multiple tokens by selecting **Import Multiple**, or by selecting **Add all FortiTokens from the same Purchase Order** and entering a single token's serial number; all tokens associated with that purchase order will then be imported.
4. If **FortiToken Mobile**, enter the **Activation codes** in the field provided, or select **Get FortiToken Mobile free trial tokens** to use temporary tokens.
5. Select **Save** to add the FortiToken(s).

To import FortiTokens from a CSV file:

1. From the FortiToken list, select **Import**.
2. Do one of the following:
   - Select **Serial number file** to load a CSV file that contains token serial numbers. FortiToken devices have a serial number barcode on them used to create the import file.
   - Select **Seed file** to load a CSV file that contains the token serial numbers, encrypted seeds, and IV values.
3. Select **Upload a file**, find the configuration file, and select **Open**.
4. Select **Save** to import the FortiTokens.

To import FortiTokens from a FortiGate unit:

1. Export the FortiGate unit configuration to a file.
2. From the FortiToken list, select **Import**.
3. Select **FortiGate configuration file**.
4. For **Data to import**, select **Import FortiToken Hardware only**, **Import FortiToken Hardware and only their associated users**, or **Import all FortiToken Hardware and users**.
5. Select **Upload a file**, find the configuration file, and select **Open**.
6. If the file is encrypted, enter the **Password** in the field provided.
7. Select **Save** to import the FortiTokens.

To export FortiTokens:

1. From the FortiToken list, select **Export FTK Hardware**.
2. Save the file to your computer.

Monitoring FortiTokens

To monitor the total number of FortiToken devices registered on FortiAuthenticator, as well as the number of disabled FortiTokens, go to **System > Dashboard > Status** and view the **User Inventory** widget.

You can also view the list of FortiTokens, their status, token clock drift, and which user they are assigned to from the FortiToken list found at **Authentication > User Management > FortiTokens**.

FortiToken device maintenance

Go to **Authentication > User Management > FortiTokens**, then select the FortiToken you need to perform maintenance and select **Edit**. The following actions can be performed:

- Comments can be added for FortiToken.
- The device can be locked if it has been reported lost or stolen.
  A reason for locking the device must be entered, and a temporary SMS token can be provided.
- The device can be unlocked if it is recovered.
- The device can be synchronized.
  Synchronize the FortiAuthenticator and the FortiToken device when the device clock has drifted. This ensures that the device provides the token code that FortiAuthenticator expects, as the codes are time-based. Fortinet recommends synchronizing all new FortiTokens.
- The device history can be viewed, showing all commands applied to this FortiToken.

FortiToken Mobile licenses

FortiToken Mobile licenses are purchased for a specified number of FortiToken Mobile tokens. Activating a FortiToken Mobile license imports the FTM tokens to FortiAuthenticator. During activation, Fortinet links the FTM license and corresponding FTM token's serial numbers with the FortiAuthenticator serial number. After activation on the FortiAuthenticator, no other FortiAuthenticator or other Fortinet products are permitted to re-use the same FTM license, however, there is no limit to how many times an FTM license can be re-activated on the same FortiAuthenticator (for example after a factory reset).

When an FTM license is activated in FortiAuthenticator, the customer is automatically credited with SMS messages = 2x No. Of Tokens. This allows the customer to use SMS to send token activation codes to end-users. The unused SMS credits expire one year from activation.

When more than one FortiAuthenticators are deployed in the environment, FortiToken Mobile licenses cannot be split up among these FortiAuthenticators. All FTM tokens associated with one license must be registered to the same FortiAuthenticator per FortiOS device (FTK hard tokens, however, can be split up).

You must contact Fortinet Support to transfer a FortiToken Mobile license to a new FortiAuthenticator unit (for example for RMA or migration to a new FortiAuthenticator unit).

For information on registering FortiToken Mobile tokens, see the FortiToken Comprehensive Guide.

Portals

The following section describes how to configure captive or self-service portals on a per customer or per AP/controller basis.

Portals can permit certain pre-login and post-login services for users, including password reset and token registration abilities.

Policies and access points are used to determine access to the portal.

Social pinholes and replacement messages can be configured to further customize portals.

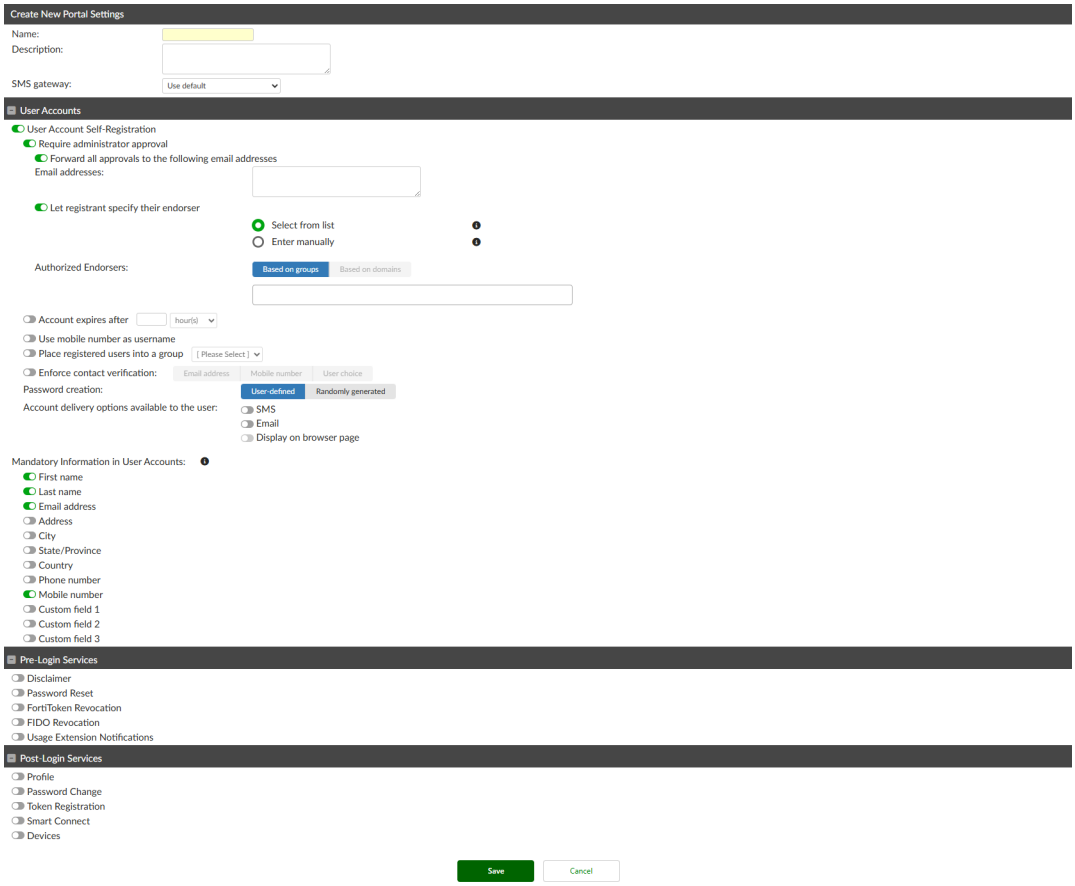
Beginning in 6.1.0, portal authentication logic is determined by policies, configured in **Authentication > Portals > Policies**.

When upgrading from a version prior to 6.1.0, existing guest portal configurations are migrated into portals, policies, and access points with corresponding settings.

Portals

To create a portal:

1. Go to **Authentication > Portals > Portals**, and select **Create New**.



2. Enter the following information:

Name	Enter the name of the portal.
Description	Optionally, enter a description of the portal.
SMS gateway	From the dropdown, select an SMS gateway for self-registered users.
User Accounts	
User Account Self-Registration	Enable to provide a link on the login page for new users to create an account.
Require administrator approval	Enable to require administrator approval to register an account. Select from the following two options: • **Forward all approvals to the following email**

		addresses: Enable and then specify administrator email addresses where the registration approval link for new users is sent.
		Note: Email addresses must be separated by commas or entered in a new line.
		• **Let registrant specify their endorser**: Enable and then specify the approver groups. Users within these groups can approve registering new accounts:
		  • **Select from list**: The registrant select their endorser from a list of the group members.
		  • **Enter manually**: The registrant provides the email address of the endorser. Only the email addresses of the authorized endorsers are accepted.
		Note: Ensure that users in the approver groups have email addresses set up.
		• **Authorized Endorsers**:
		  • When **Let registrant specify their endorser** is set to **Select from the list**, specify one or more groups.
		  • When **Let registrant specify their endorser** is set to **Enter manually**:
		  • Specify one or more groups.
		OR
		  • Specify the email address domains.
		Note: The **Authorized Endorsers** option is only available when **Let registrant specify their endorser** is enabled.

	Account expires after	Enable/disable account expiration. If enabled, enter the number of hours, days, months, or years the account remains expired from the dropdown.
	Use mobile number as username	Determine whether to require the user's mobile number as their username.
	Place registered users into a group	Determine whether to place registered users into a group from the dropdown.

	Enforce contact verification	Enable/disable whether to enforce contact verification. If enabled, select whether to verify the user's email address or mobile number, or allow the user to decide between email address or mobile number.
	New user is automatically logged-in after successful contact verification	Enable to allow newly registered users to access the guest network without having to enter their credentials. Disable to require users to enter their credentials to access the guest network after successful registration. This option is enabled by default. **Note**: The option is only available when **Enforce contact verification** is enabled.
	Password creation	Determine whether the user's password is user-defined or randomly generated.
	Account delivery options available to the user	Determine whether the user's account information is sent to them by SMS, email, or displayed on the browser page. If more than one option is selected, the self-registering user decides which account delivery method to use. **Note**: If **Require administrator approval** is enabled, **Display on browser page** is disabled.
Mandatory Information in User Accounts		Configure the available fields required by the user to enter: • **First name** • **Last name** • **Email address** • **Address** • **City** • **State/Province** • **Country** • **Phone number** • **Mobile number** • **Custom field 1** • **Custom field 2** • **Custom field 3** **Note**: **First name**, **Last name**, **Email address**, and **Mobile number** are enabled by default.
Pre-login Services		Configure various pre-login services to permit to users.
Disclaimer		Enable or disable the appearance of a disclaimer to the end-user that must be accepted before proceeding to the login page.

		To configure the disclaimer, edit the **Login Disclaimer Page** replacement message under **Authentication > Portals > Replacement Messages**.
	Password Reset	Enable or disable pre-login password reset link.
	Verification Methods	Specify the acceptable methods to confirm a user's identity before allowing them to reset their password: • **Email** (default) • **SMS** • **Token device** • **Security question**

	FortiToken Revocation	Select to revoke tokens based on various conditions:
		• **Allow users to report a lost token to the Administrator at this email address**
		• **Allow users to temporarily use SMS token authentication if a mobile number was pre-configured**
		• **Allow users to temporarily use email token authentication if an email was pre-configured**
		• **Allow users to reconfigure their FortiToken Mobile**:
		  • **Authorized delivery options**: Ability to control the available delivery methods for FortiToken Mobile reprovisioning using:
		  • **Email**
		  • **SMS**
		  When editing/creating a portal with **Provision mode** set to **Offline** in Tokens on page 88, **Allow users to reconfigure their FortiToken Mobile** (when **FortiToken Revocation** is enabled) cannot be enabled.
		• **Allow users to reconfigure their FortiToken Cloud**

	FIDO Revocation	Select to revoke FIDO: • **Temporary credential delivery options**: You can select either SMS and/or Email.  The end-user must authenticate using an OTP via Email and/or SMS before completing the FIDO operation. One or both of Email/SMS must be selected. • **Allow user to revoke all FIDO keys**: Enable to allow the end-user to revoke all FIDO keys at once. • **Allow users to re-register their FIDO token**: Enable to allow end-users to re-register a FIDO token if their FIDO keys have been revoked.
	Usage Extension Notifications	Allow users who exceeded their time and/or data usage to request an extension via an email notification.
Post-login Services		Configure various post-login services to permit to users.

Profile	Select to determine whether authenticated users can view/edit their account information.
Password Change	Select to determine whether local and/or remote users have the ability to change their passwords after they log in.
Token Registration	Select to configure FortiToken Mobile self-provisioning privileges, including: • **Allow FortiToken Hardware self-provisioning** • **Allow FortiToken Mobile self-provisioning** • **Allow FortiToken Cloud self-provisioning** • **Allow FIDO token registration**: End-user may register new FIDO authenticators up to a maximum of 5 per account. • **Allow FIDO token revocation**: End-user may revoke any of the FIDO authenticators previously registered under their account. • **Allow Email self-provisioning** • **Allow SMS self-provisioning** • **Allow user to request a token from Administrator at this email address** • **Restrict token self-provisioning to members of specific group**
Smart Connect	Select to assign a Smart Connect profile. See Smart Connect Profiles for more information.
Devices	Select to require users to register their devices after they log in. Select from the following: • **Tracking and Management** • **Tracking-only** (default): The end-user with successful log in to the captive portal with a new MAC device is asked to register the device (when under the maximum number of allowed MAC devices). • **Management-only**: The end-user successfully logs in to the captive portal with a new MAC device in excess of the maximum number of devices per user, the end-user is asked if they will replace an existing device. **Note**: When device management is disabled and the end-user successfully logs in to the captive portal with a new MAC device, the access is denied since an existing device cannot be replaced. In the post login portal: • The **Devices** menu is only visible when device management is enabled. • If `"Client certificate CN"=="MAC Device"`, the end-user is given a dropdown to select which device to use. • If no MAC devices have been registered to the logged-in user account, e.g., device tracking is disabled, the Smart Connect menu shows an error message.
Maximum number of devices	Enter the maximum number of devices that can be registered (default =3).

	Place registered devices into this group	Enable to place registered devices into a specific MAC device user group. **Note**: The option is disabled by default.
	Remove MAC devices after	Enable and enter the number of days after which MAC devices expire (default = 7, 1 - 365). **Note**: The option is disabled by default.

3. Select **Save** to create the new portal.

Token self-revocation

Token self-provisioning is offered as a pre-login service for guest portals.

When the token self-revocation feature is enabled (**Authentication > Self-service Portal > Token self-provisioning**), the guest portal's token verification page will have an additional **Lost my token** link. Clicking this link provides access to the token self-revocation service page that includes the following options:

- **Re-provision my FortiToken Mobile**
- **Switch to email token authentication**
- **Disable my account**

Post-login device tracking

When the post-login service option **Devices** is enabled, the administrator must specify into which device group to put the self-registered devices, as well as specify the **Maximum number of devices per user** (up to 20; 3 by default). When enabled, users have access to a post-login interface where they can add/edit/delete their list of devices. If enabled but the device is **not** registered, the FortiAuthenticator presents a device registration page after account credential validation.

If the user reaches their device limit, they must select an existing device to replace. If the MAC address is currently associated with a different user, it is re-assigned to this newly logged-in user with the following warning message:

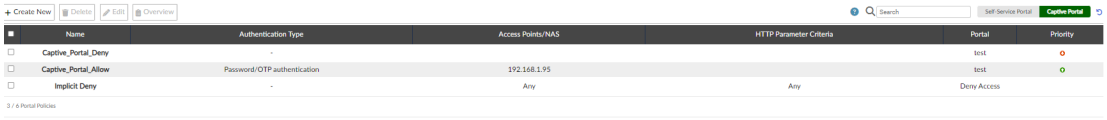
"Your device had previously been registered by another user. Ownership has now been changed to your account."

Policies

Portal policy configuration is available in **Authentication > Portals > Policies**.

To determine policy priority, FortiAuthenticator attempts to match the portal access request to each policy, starting with the top policy in the list, and moves down until a match is found. Policy priority can be re-arranged by selecting the up and down icons next to each policy in the list.

You can change between **Captive portals** and **Self-service portals** views using the toggle in the top-right corner of the GUI.



For more information on the captive portal workflow, click the **help** icon in the top-right corner of the GUI, and select an access point/NAS.

Captive portal policies

There are two types of captive portal policies:

- **Allow captive portal access**: Presents a captive portal login page when end-users' HTTP requests contain parameters or values that meet the pre-defined criteria.
- **Deny captive portal access:** Blocks end-users from accessing a captive portal login page if their HTTP request contains parameters or values that meet the pre-defined criteria.

To configure an allow access captive portal policy:

1. Go to **Authentication > Portals > Policies**, click **Captive portals** and **Create New**.
   The **Captive Portal Policy Creation Wizard** is launched.
2. Enter the following information:

Policy type	Specify the name and type of the portal policy.
Name	Enter a name for the policy.
Description	Optionally, enter a description of the policy.
Type	Select **Allow captive portal access** and choose a portal.
Portal selection criteria	Specify the necessary criteria for presenting this captive portal to an end user.
Portal Rule Conditions	Redirects to this captive portal must contain parameters that meet all of the criteria included here. For example, a condition to restrict the portal to users from subnet `192.168.1.0/24` would be: • **HTTP parameter** = `userip` • **Operator** = `[ip]in_range` • **Value** = `192.168.1.0/24`
Authorized clients	
Access points	Select the access points used to access the captive portal.
RADIUS clients	Select the RADIUS clients to associate with this portal policy.
Authentication type	Specify the type of end-user authentication used by the portal.
Authentication type	Select either Password/OTP or MAC authentication. • **Password/OTP Authentication**: Selected by default, this option requires authentication with user account credentials (local or remote)

	or with social site credentials: • **Local/remote user**: Credentials are verified against one of the local or remote user accounts. • **Social users**: Authentication with social site credentials (OAUTH), phone number, or email. Successful authentication creates a social user account containing details about the third-party account. • **MAC Authorization**: The access point/NAS can attempt a MAC authentication bypass (MAB) prior to redirecting to the captive portal. If the MAB is successful, the access point/NAS provides network access without redirecting to the captive portal. • **No authentication**: End-user does not require any credentials. If **Disclaimer** is enabled in the **Pre-Login Services** pane in **Authentication > Portals > Portals**, the end-user is required to accept the disclaimer to trigger the follow up API call to the access points, e.g., FortiGate, FortiAP, or CiscoWLC. After the access point API has been called, the end-user is redirected to the website they were originally trying to reach. If the end-user declines the disclaimer, the end-user is prevented from leaving the captive portal and is sent to the **Disclaimer Denied Page** replacement message. Once the disclaimer is accepted or the disclaimer option was disabled, the follow up API call still requires FortiAuthenticator to provide login credentials input. The login credential is included in the RADIUS authentication request sent by the access point.  Since the end-user does not identify themselves for **No authentication**, **Account Registration**, **Pre-login Services**, and **Post-login Services** from Portals on page 144 are ignored. Only **Disclaimer** in **Pre-login Services** applies.
Identity sources	Specify the identity sources against which to authenticate end users.
Social Users	Enable authorized redirects to social platforms and specify if phone or email verification is required. This setting is only available for **Password/OTP Authentication** when **Social Users** is enabled in **Authentication type**.
Username format	Select one of the following three username input formats: • **username@realm** • **realm\username** • **realm/username** This setting is only available for **Password/OTP Authentication**.

	Use default realm when user-provided realm is different from all configured realms	When enabled, FortiAuthenticator selects the default realm for authentication when the user-specified realm is different from all configured realms.
	Realms	Add realms to which the client will be associated. • Select a realm from the dropdown menu in the **Realm** column. • Select whether or not to allow local users to override remote users for the selected realm. • Select whether or not to use Windows AD domain authentication. • Edit the group filter as needed to filter users based on the groups they are in. • If necessary, add more realms to the list. • Select the realm that will be the default realm for this client. This setting is only available for **Password/OTP Authentication**.
Authentication factors		Specify which authentication factors to verify.
	Authentication type	Select one of the following: • **Mandatory password and OTP**: Two-factor authentication is required for every user. • **All configured password and OTP factors**: Two-factor authentication is required if it is enabled on the user's account, otherwise, allow one-factor authentication. • **Password-only**: Authenticate users through password verification only. User accounts for which password authentication is disabled cannot be authenticated. • **OTP-only**: Authenticate users through token verification only. User accounts for which token authentication is disabled cannot be authenticated. This setting is only available for **Password/OTP Authentication**.
	User IP address parameter	Select the user IP address parameter. Use *userip* for FortiGate/FortiWiFi.
	Adaptive Authentication	Enable this option if you would like to have certain users bypass OTP validation, so long as they belong to a trusted subnet. Select **All trusted subnets** to add all the available trusted subnets. You can specify the trusted subnets by selecting **Specify trusted subnets** and clicking the pen icon. This opens a window where you can choose from a list of available trusted subnets.  **Adaptive Authentication** is available only for the following authentication types: • **Mandatory password and OTP** • **All configured password and OTP factors**

	FIDO authentication (effective once a token has been registered)	Enable or disable FIDO authentication.	
		Options	Select from the following two options: • **FIDO token only**: Log in with FIDO token only (without password). • **Password and FIDO token**: Log in with the password and the FIDO token.
		Allow two-factor authentication (password and OTP) if all FIDO keys have been revoked for the user account	Enable to allow two-factor authentication (password and OTP) if all FIDO keys have been revoked for the user account.
	MAC address parameter	Select the MAC address parameter. Use *usermac* for FortiGate/FortiWiFi, *station_mac* for WortiWLC, or *client_mac* for Cisco WLC.	
	Restrict access based on end-user MAC address	Select the authorized MAC device groups. Authorized groups must be first created under **Authentication > User Management > User Groups**, where the **Type** is **MAC**.	
	Advanced Options		
		Allow FortiToken Mobile push notifications	Toggle on/off FTM Push notifications for RADIUS users. This setting is only controlled here on a per RADIUS client basis, not for specific users. This setting is only available for **Password/OTP Authentication**.
		Application name for FTM push notification	Enter the client application name. This field is displayed on the FortiToken app. When creating a new policy or upgrading to FortiAuthenticator 8.0, the policy name is the default client application name.
		Resolve user geolocation from their IP address	Enable to resolve the user geolocation from their IP address (if possible).
		Reject usernames containing uppercase letters	Enable this setting to reject usernames that contain uppercase letters. This setting is only available for **Password/OTP Authentication**.
RADIUS response	Specify the content of the RADIUS authentication response based on the outcome of the authentication.		

3. Click **Save and exit**.

To configure a deny access captive portal policy:

1. Go to **Authentication > Portals > Policies**, click **Captive portals** and **Create New**.
   The **Captive Portal Policy Creation Wizard** is launched.
2. Enter the following information:

Policy type	Specify the name and type of the portal policy.
Name	Enter a name for the policy.
Description	Optionally, enter a description of the policy.
Type	Select **Deny captive portal access**.
Portal selection criteria	Specify the necessary criteria for denying captive portal access to an end-user.
Portal Rule Conditions	Redirects to this captive portal must contain parameters that meet all of the criteria included here. For example, a condition to restrict the portal to users from subnet `192.168.1.0/24` would be: • **HTTP parameter** = `userip` • **Operator** = `[ip]in_range` • **Value** = `192.168.1.0/24`
Access points	Select the portal access points. End-users must be redirected to the captive portal from one of these access points/NAS.
Browser response	The FortiAuthenticator presents an error message to end-users' browsers when captive portal access is denied. You can customize the browser response error message at **Authentication > Self-service Portal > Replacement Message > System > 403 Forbidden.**

3. Click **Save and exit**.

Self-service portal policies

Self-service portals are accessed directly and allow local and remote users to self-manage their account.

To configure a self-service portal policy:

1. Go to **Authentication > Portals > Policies**, click **Self-service portals** and **Create New**.
   The **Self-Service Portal Policy Creation Wizard** is launched.
2. Enter the following information:

Policy type	Specify the name and type of the portal policy.
Name	Enter a name for the policy.
Description	Optionally, enter a description of the policy.
Portal	**Allow self-service portal access** is enabled by default. Select a portal.

Identity sources	Specify the identity sources against which to authenticate the end-users.
Username format	Select one of the following three username input formats: • **username@realm** • **realm\username** • **realm/username**
Use default realm when user-provided realm is different from all configured realms	When enabled, FortiAuthenticator selects the default realm for authentication when the user-specified realm is different from all configured realms.
Realms	Add realms to which the client will be associated. • Select a realm from the dropdown menu in the **Realm** column. • Select whether or not to allow local users to override remote users for the selected realm. • Select whether or not to use Windows AD domain authentication. • Edit the group filter as needed to filter users based on the groups they are in. • If necessary, add more realms to the list. • Select the realm that will be the default realm for this client.
Authentication factors	Specify which authentication factors to verify.
Authentication type	Select one of the following: • **Mandatory password and OTP**: Two-factor authentication is required for every user. • **All configured password and OTP factors**: Two-factor authentication is required if it is enabled on the user's account, otherwise, allow one-factor authentication. • **Password-only**: Authenticate users through password verification only. User accounts for which password authentication is disabled cannot be authenticated. • **OTP-only**: Authenticate users through token verification only. User accounts for which token authentication is disabled cannot be authenticated.
Adaptive Authentication	Enable this option if you would like to have certain users bypass OTP validation, so long as they belong to a trusted subnet. Select **All trusted subnets** to add all the available trusted subnets. You can specify the trusted subnets by selecting **Specify trusted subnets** and clicking the pen icon. This opens a window where you can choose from a list of available trusted subnets.  **Adaptive Authentication** is available only for the following authentication types: • **Mandatory password and OTP** • **All configured password and OTP factors**

	FIDO authentication (effective once a token has been registered)	Enable or disable FIDO authentication.	
		Options:	Select from the following two options: • **FIDO token only**: Log in with FIDO token only (without password). • **Password and FIDO token**: Log in with the password and the FIDO token.
		Allow two-factor authentication (password and OTP) if all FIDO keys have been revoked for the user account	Enable to allow two-factor authentication (password and OTP) if all FIDO keys have been revoked for the user account.
	Advanced Options		
		Allow FortiToken Mobile push notifications	Toggle to enable or disable FortiToken Mobile push notifications for RADIUS users.
		Application name for FTM push notification	Enter the client application name. This field is displayed on the FortiToken app. When creating a new policy or upgrading to FortiAuthenticator 8.0, the policy name is the default client application name.
		Resolve user geolocation from their IP address	Enable to resolve the user geolocation from their IP address (if possible).
		Reject usernames containing uppercase letters	Enable this setting to reject usernames that contain uppercase letters.

3. Click **Save and exit**.

Access points

An access point is the address that an end-user must be redirected from in order to access the configured portal.

To create an access point:

1. Go to **Authentication > Portals > Access Points**, and select **Create New**.
2. Enter the following information.

Name	Enter a name for the access point.
Client address	Provide the client IPv4/IPv6 address. Client addresses can be in the format of **IP/Hostname**, **Subnet**, or **Range**.

3. Click **Save**.

Access points must be configured based on whether the access point address identifier in the redirection URL to the captive portal contains an IP address or an FQDN (e.g. FortiGate uses `apip =< IP` or `FQDN >`).

If access point address identifier contains an IP address, set **Client address** to one of the following:

- IP/FQDN with AP's single IP address value
- Subnet or Range containing AP's IP address

If access point address identifier contains an FQDN, set **Client address** to one of the following:

- IP/FQDN with AP's FQDN value
- If FQDN can be resolved to an IP address via DNS, Subnet or Range containing resolved IP address

FortiWLC Pinholes

Portal pinhole configuration is available under **Authentication > Portals > FortiWLC Pinholes**.

Pinhole values can be added to the default list, separated by comma or a new line.

The default pinholes are:

- www.google.com
- accounts.google.com
- ssl.gstatic.com
- fonts.gstatic.com
- www.gstatic.com
- accounts.youtube.com
- www.facebook.com
- static.xx.fbcdn.net

Replacement messages

Portal replacement message mappings are available under **Authentication > Portals > Replacement Messages**.

The replacement messages are split into four categories: **Authentication**, **Password Reset**, **User Registration**, and **Post-Login**.

Selecting a specific message will display the text and HTML or plain text of the message in the content pane.

Selecting **Toggle Tag List** will display a table of the tags used for that message above the message's HTML or plain text box.

To edit a replacement message:

1. Select a message in the replacement message list.
2. Edit the plain text or HTML code in the lower right pane, or select **Detach** to edit the message in a new browser window.
3. When you are finished editing the message, select **Save** to save your changes.

4. If you have made an error when editing the message, select **Restore Default** to restore the message to its default value.

To insert an image into a replacement message:

1. Add the following HTML code to a replacement message:
   `<img src={{:image/<image_name>}}>`
   Where `<image_name>` is the name entered for the image. For example, the HTML code for an image named Acme_logo is `<img src={{:image/Acme_logo}}>`
2. Select **Save**.

Smart Connect profiles

Smart Connect profiles are available under **Authentication > Portals > Smart Connect Profiles**.

This feature provides the ability to set up network settings (such as WiFi configuration) on an endpoint by downloading a script or an executable (depending on the endpoint's OS) from the FortiAuthenticator portal.

FortiAuthenticator supports Smart Connect profiles for Windows, macOS, iOS, Android, and Chromebooks.

When configured, the Smart Connect feature will show up as a new button on the portal's post-login main page:

When clicking on the Smart Connect button, the user is given the option to download a self-install file for the OS type of their choice, including iOS/MacOS, Windows, and Android. A device ID can also be entered, however, this is only available if the Smart Connect profile uses EAP-TLS. If entered, the ID is used to generate the end-user certificate.

To configure a Smart Connect profile:

1. Select **Create New** to start the profile configuration wizard.
2. Enter a **Name**.
3. In **Connect type**, either select **Wireless** or **Certificate** (for certificates-only installs), and select **Next**.
4. When the **Connect type** is **Wireless**:
   a. Enter an **SSID**, and select the **Auth method** to use: **WPA2 Personal** or **WPA2 Enterprise**.
   You can optionally enable or disable **Hidden SSID** to show or hide the SSID. When finished, select **Next**.
   b. When the **Auth method** is **WPA2 Personal**, enter a **Pre-shared Key**, then select **Next**.
   When the **Auth method** is **WPA2 Enterprise**, enter the following information, then select **Next**:

EAP Type	Select an EAP type: • **TLS** (default) • **TTLS**

	• **PEAP**
Client Certificate CN	From the following, select the user account attribute to use as the CN value in the client certificate (previously, hardcoded to `Username`): • `Username` (default) • `MAC Device` • `First name` • `Last name` • `Email` • `Display name` • `Company` • `Department` • `Title`
Signing CA	From the dropdown, select a local CA certificate to sign certificates for EAP/TLS connection. **Note**: The option is only available when the **EAP Type** is **TLS**.
Anonymous Identity	Select either **Anonymous** or **Username**. If **Username** is selected, select a format from **Username Format**.  Do not send username over unencrypted communication. **Note**: The option is not available when **EAP Type** is **TLS**.
Username Format	Select from the following formats: • **username** • **username@realm** • **realm\username** • **realm/username**
Phase 2 Authentication	From the following options, select an authentication protocol: • **PAP** • **CHAP** • **MSCHAP** • **MSCHAPv2** (default) **Note**: The option is only available when the **EAP Type** is **TTLS**.
Include user credentials in configuration file	Enable to include username/password in configuration files/executables that users can download. **Notes**: • The option is enabled by default. • The option is only available when the **EAP Type** is **TTLS** or **PEAP**.

c. In the **CA Installation Settings** window:
   i. In **Install local CA certificates**, from the list of available local CA certificates, select CA certificates and move them to the **Chosen Install Local CA Certificates** list.

The selected CA certificates are installed on the client devices.

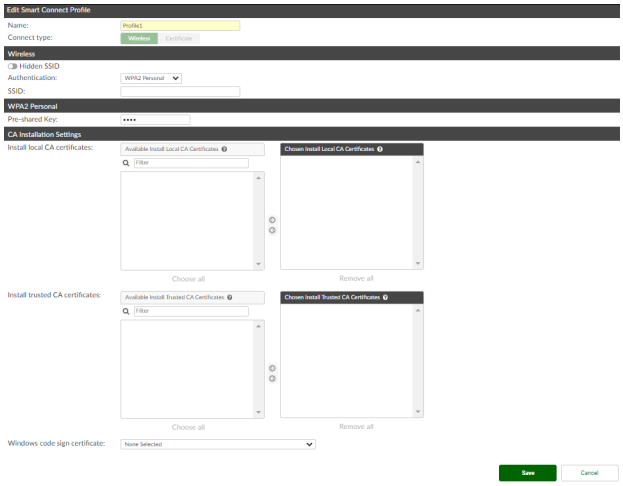
ii. In **Install trusted CA certificates**, from the list of trusted CA certificates, select trusted CA certificates and move them to the **Chosen Install Trusted CA Certificates** list.

iii. From the **Windows code sign certificate** dropdown, select a certificate or select the default `Default-Server-Certificate`.

Note: The option is only available when editing a Smart Connect profile.

d. Click **Save**.

e. You can edit the profile to review and change any of the previously set options, and define additional settings, as shown below:



f. Click **Save** to apply your options and finish the configuration.

When created, a Smart Connect profile can be associated with a guest portal and be available as a post-login service (see **Post-login Services** under Portals).

5. When the **Connect type** is **Certificate**:

a. In the **Client Certificate CN** dropdown, from the following, select the user account attribute to use as the CN value in the client certificate (previously, hardcoded to `Username`):

- `Username` (default)
- `MAC Device`
- `First name`
- `Last name`
- `Email`
- `Display name`
- `Company`
- `Department`
- `Title`

b. In the **Signing CA** dropdown, select the local CA certificate to sign the client certificates issued by the Smart Connect profile, and select **Next**.

c. In the **CA Installation Settings** window:

i. In **Install local CA certificates**, from the list of available local CA certificates, select CA certificates and move them to the **Chosen Install Local CA Certificates** list.

The selected CA certificates are installed on the client devices.

ii. In **Install trusted CA certificates**, from the list of trusted CA certificates, select trusted CA certificates and move them to the **Chosen Install Trusted CA Certificates** list.

iii. From the **Windows code sign certificate** dropdown, select a certificate or select the default `Default-Server-Certificate`.
Note: The option is only available when editing a Smart Connect profile.

d. Click **Save**.

Smart Connect for Windows

The Smart Connect for Windows feature provides an executable file that adds specific network settings to an end-user's Windows device. The Smart Connect profile settings are the same as the ones implemented for iOS and macOS. The main difference is in how the downloaded executable file is built and packaged, so that it installs seamlessly on Windows devices.

Self-service URL

When using the device tracking feature, users are no longer redirected by the FortiGate after initial device registration. Instead, the FortiAuthenticator provides a specific URL for each guest portal, as derived from the guest portal name (under **Authentication > Portals > Portals**).

When the end user navigates to the self-service URL, they must provide valid credentials to get network access, but the login does not trigger the call to the FortiGate device's API.

Note that special characters must be encoded in the self-service URL.

Firmware upgrade

When upgrading from a previous release, as a result of the device tracking feature, the following occurs:

- MAB **Unauthorized devices** are set to **Deny access** by default for existing RADIUS clients.
- MAB **Blocked groups** are set to **empty** by default for existing RADIUS clients.
- Device tracking and device management are disabled by default for existing guest portals.
- Existing replacement messages are left unchanged for existing guest portals.
- New (default) replacement messages are added to existing guest portals.

Guest Portals (beta)

Portals are used to allow administrators to create their own portal pages and host them on the FortiAuthenticator.

These are created by administrators and can be fully customized and used to provide the following.

- Customized authentication pages: Allow portal pages to be located on the FortiAuthenticator instead of on each captive portal device, providing a centralized location for configuration and display.

The following tabs are available in **Guest Portals (beta)**:

- Portals on page 162
- Portal rules on page 169
- Guest themes on page 171

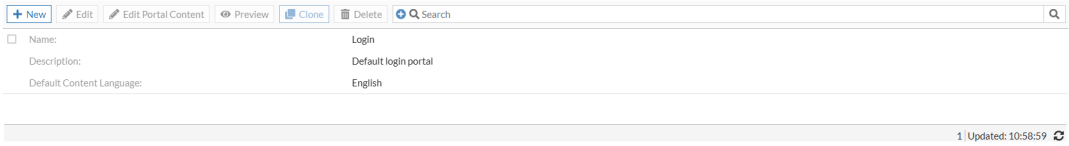
Note: This is a beta feature.

Limitation:

- Only supports login for local users
- Configuration backup/restore does not preserve all the customizations
- HA A-P and HA A-A are not supported
- Only administrators with full permissions can access the configuration

Portals

Go to **Authentication > Guest Portals (beta) > Portals** to see the list of guest portals.



The following settings are available in the **Portals** tab:

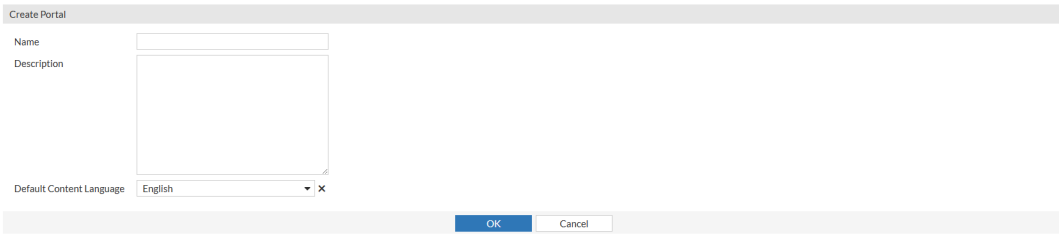
New	Select to create a new portal. See Creating a guest portal on page 162.
Edit	Select to edit the selected portal.
Edit Portal Content	Select to edit the selected portal content.
Preview	Select to preview the selected guest portal in a new tab.
Clone	Select to clone the selected portal.
Delete	Select to delete the selected portals.
Search	Enter a search term in the search field, then select **Search** to search the portals list.

Creating a guest portal

Follow these steps to create a guest portal in FortiAuthenticator.

To create a guest portal

1. Go to **Authentication > Guest Portals (beta) > Portals**, and select **New**.
   The **Create Portal** window opens.



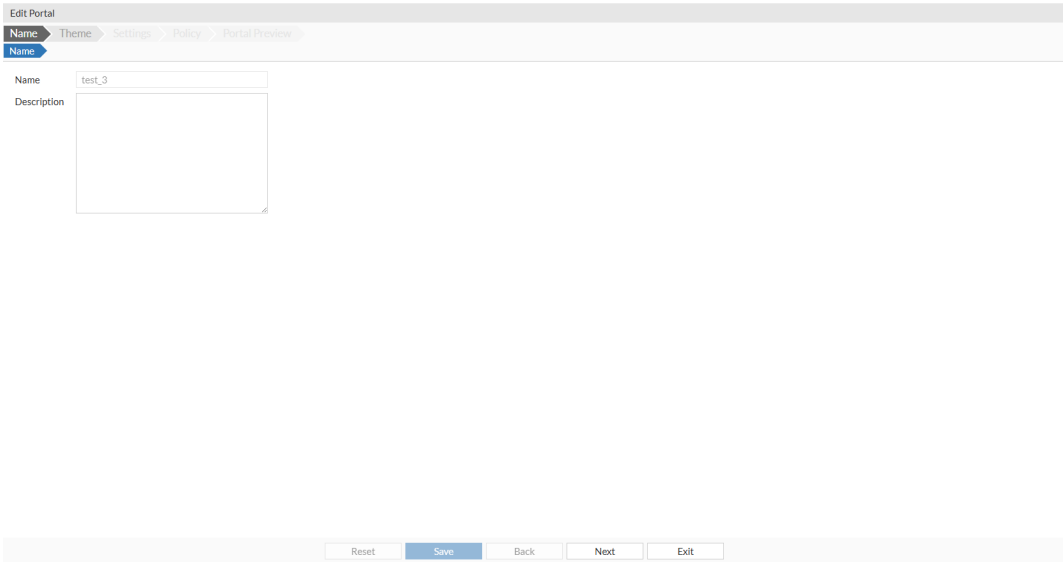
2. Enter a name and description.

The name you enter is included in the portal URL and is visible to portal users.

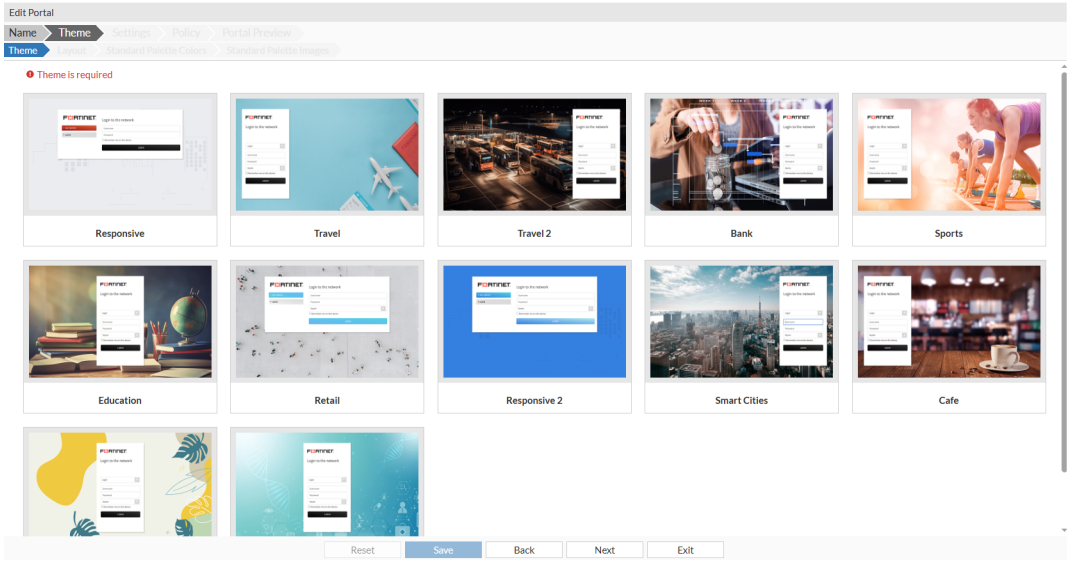
3. From the dropdown, select the **Default Content Language**, and click **OK**.

This is the default portal language unless it is manually changed.

The **Edit Portal** wizard opens.



4. Optionally, enter a description for the portal.
Click **Next**.
The **Theme** tab opens.



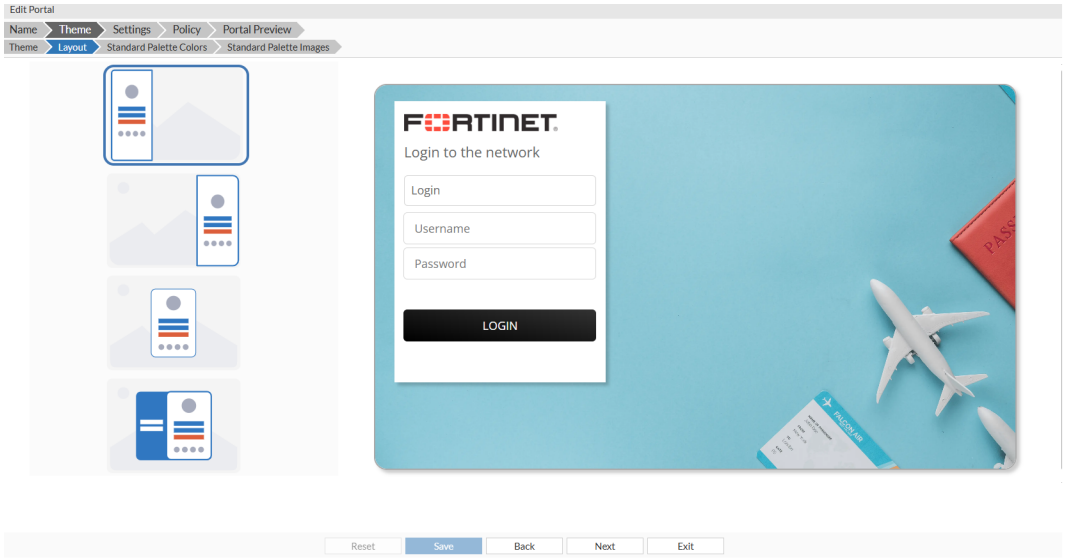
5. Select a predefined portal theme, multiple default themes are available for the guest portal based on your enterprise requirements.

   You can also upload new customized themes in **Guest Themes**.

   Click **Next**.

   See Guest themes on page 171.

6. In the **Layout** tab, define the layout type for visual representation of the portal page.

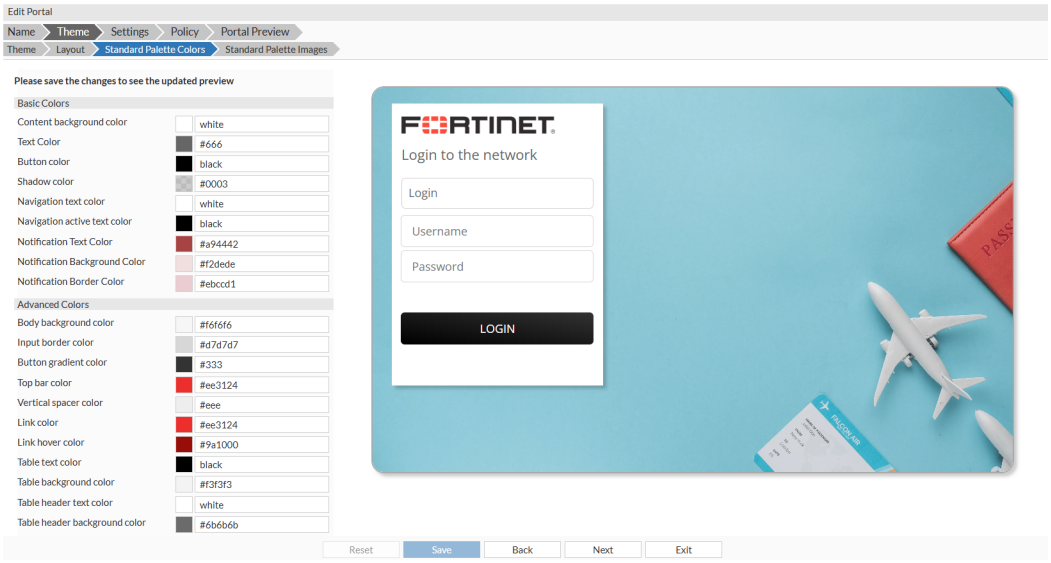


   Select the layout in the **Layout** tab, the available options allow you to align the content in the center, right, or left side of the portal page.

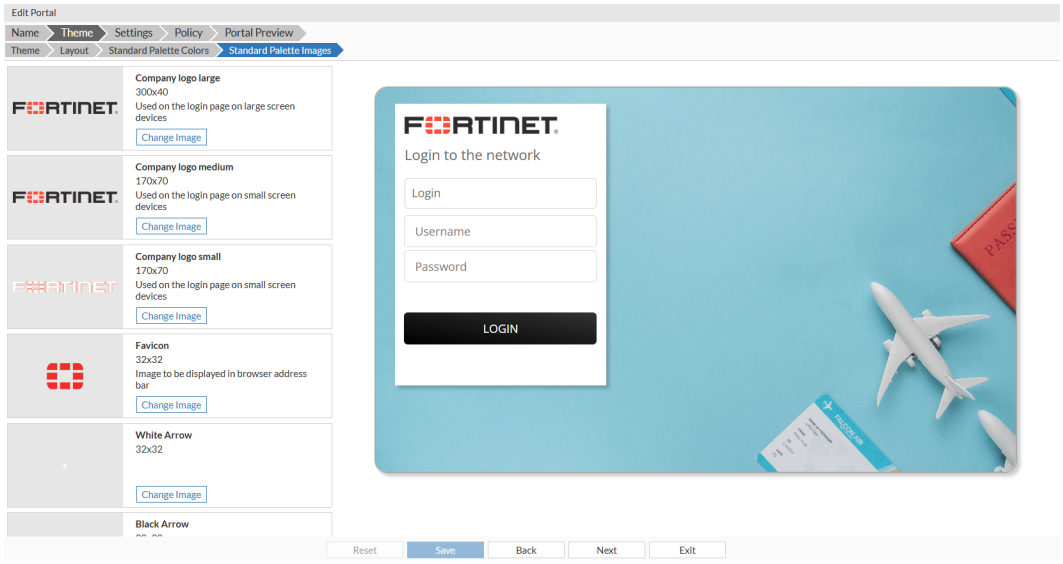
   Click **Next**.

   Note: The background image of the pages does not change as per the defined layout, it is just the position of the content that is changed as depicted in the following image.

7. In the **Standard Palette Colors** tab, select a color scheme for your portal theme, and click **Next**.



8. In the **Standard Palette Images** tab, select a corporate logo image for the device accessing the guest portal.



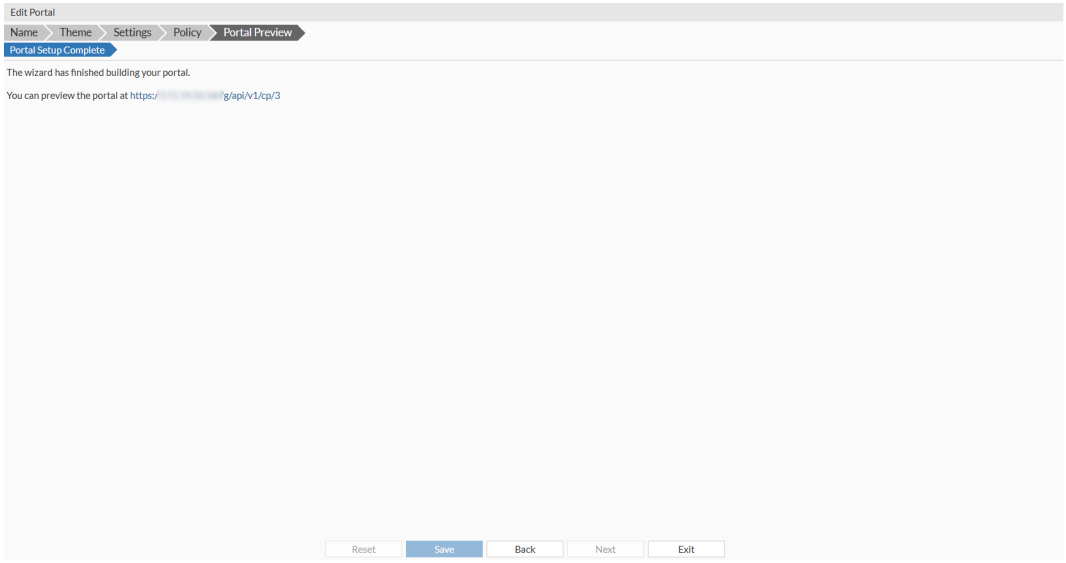
Click **Change Image** to upload display images of your choice.

You can preview the portal page with the selected **Layout, Standard Palette Colors**, and **Standard Palette Images**, in the live preview component/pane.

Click **Next**.

9. Configure Settings on page 166 and Policy on page 167 to complete creating the guest portal.

10. In the **Portal Preview** tab, the following message is displayed.



11. Click the URL to preview the portal in a new tab.

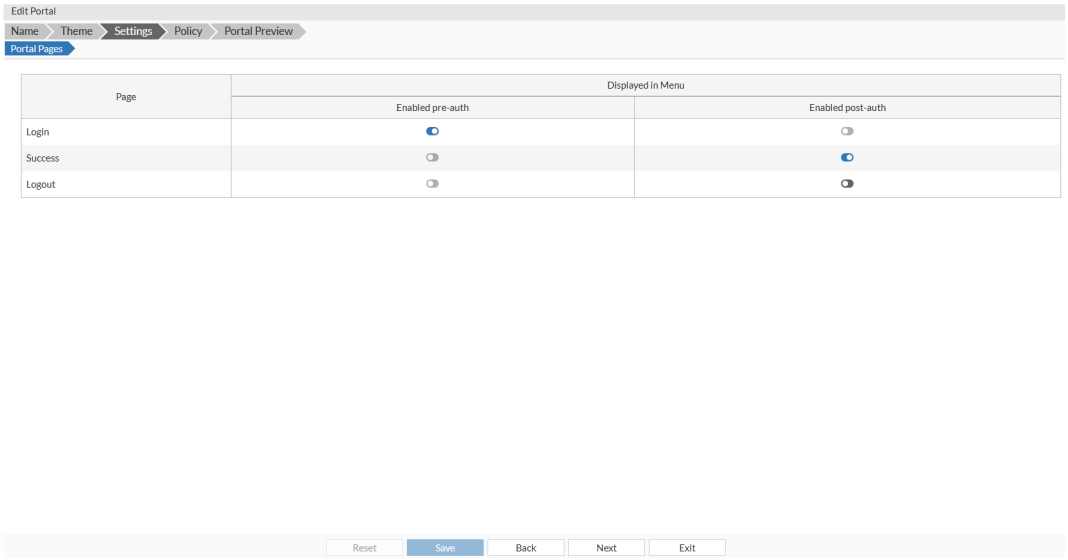
Settings

You are required to configure and apply multiple general and specific settings to the guest portal across various tabs displayed on this page.

Portal pages

You can add or remove features to the guest portal by modifying the selection of pages that should be available to users. In each case, enable pre-authentication to make the feature available before authentication and enable post-authentication to make the feature available after authentication.

If you do not enable either of the options, then the feature is disabled.



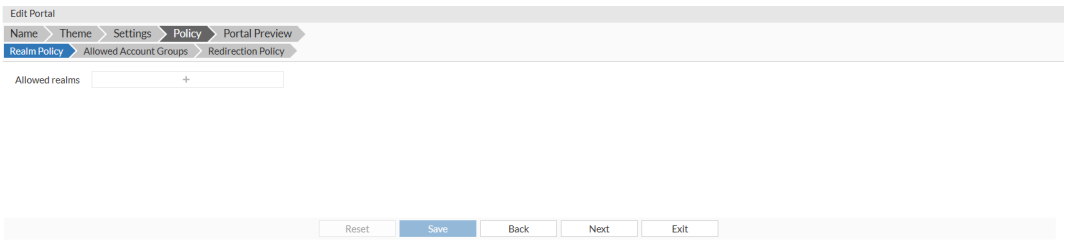
The following options can be enabled for the guest portal:

- **Login**: Display a screen that will allow a user to log in.
- **Success**: Display a screen that shows successful authentication.
- **Logout**: Display a logout button.

Policy

You can define various policies for users to access and use the guest portal:

Realm policy



This policy selects the realms to use for authentication in the login page.

The realms are used to authenticate users against different external servers.

- **Allowed realms**: Select and add the realms for authentication.

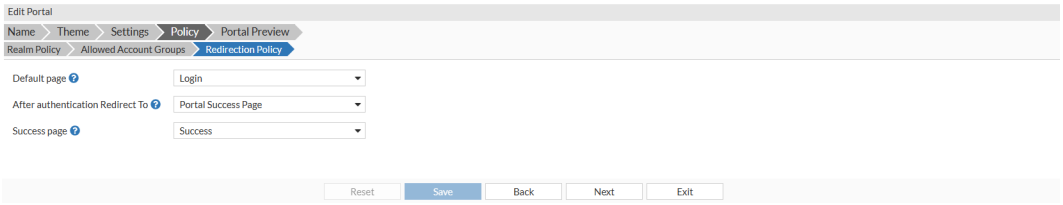
> Realm selection is disabled for this beta feature.
> **Allowed realms** always defaults to the local realm.

Allowed account groups

Select the preconfigured account groups.

Note: **Allowed account groups** can only be set to **Allow all account groups** for this beta feature.

Redirection policy



Configure this policy to redirect the users are they login into the guest portal.

- **Default page**: The portal page that the guests are redirected to after they login into the network for the first time.
- **After authentication Redirect To**: The configured portal page where the user is redirected to after successful portal authentication.
- **Success page**: The configured portal page that the returning users are taken to after successful authentication.

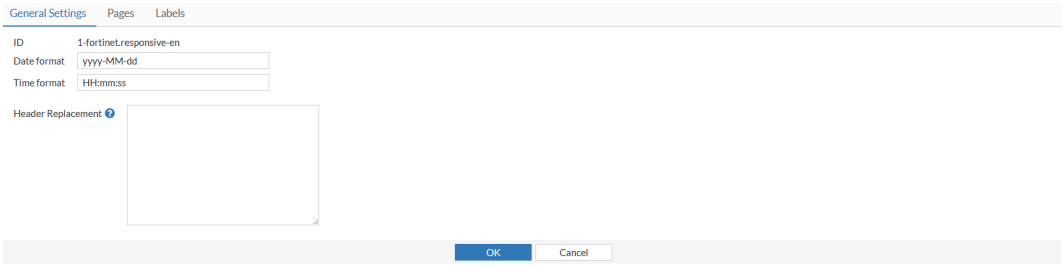
Configuring restriction information

FortiAuthenticator supports a secondary landing page for captive portals.

The page provides users with more specific information when they exceed usage limits or experience access restrictions.

To customize the secondary portal:

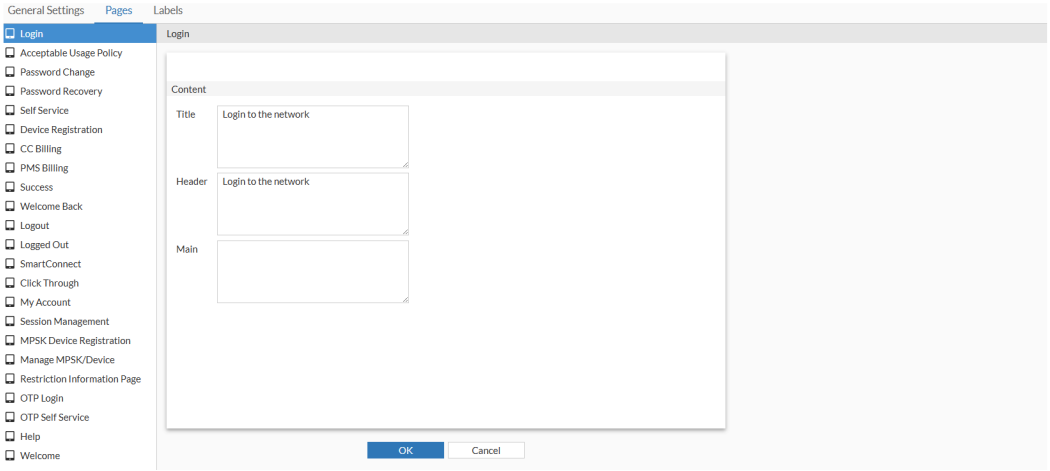
1. Go to **Authentication > Guest Portals (beta) > Portals**.
2. Select a portal from the list, and select **Edit Portal Content**.
3. Select the language of the portal, and click **Edit**.
   The **General Settings** tab opens.



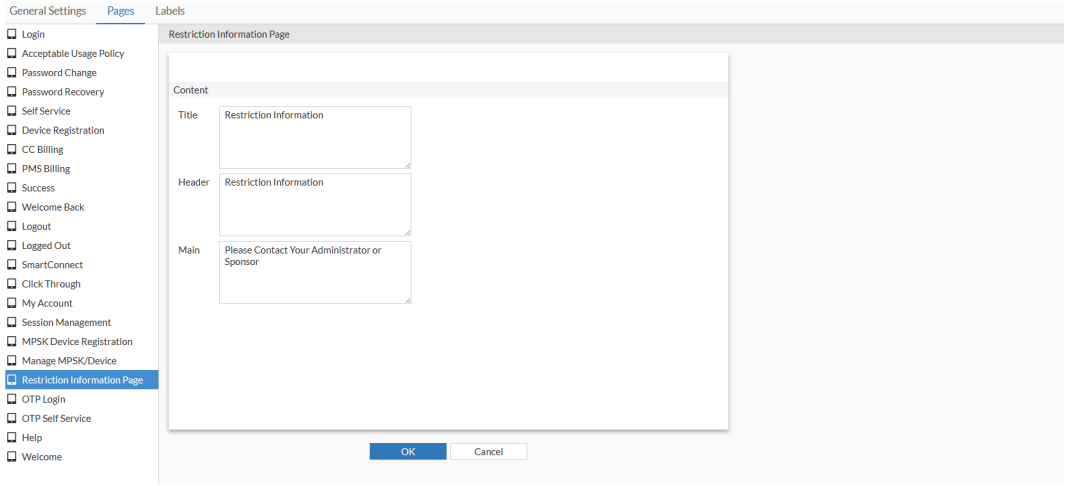
4. Enter the following information:

ID	The ID for the portal.
Date format	The date format (default = `yyyy-MM-dd`).
Time format	The time format (default = `HH:mm:ss`).
Header Replacement	Enter a valid header. An invalid header breaks guest portal rendering.

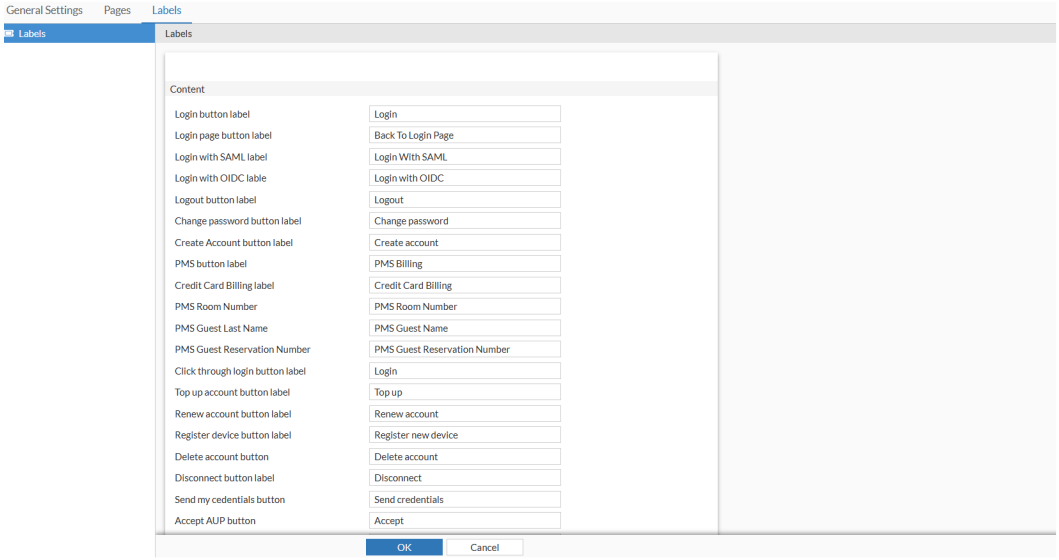
5. Switch to the **Pages** tab to customize the title and header content:



a. In the **Pages** tab, click **Restriction information Page** to edit **Title**, **Header**, and **Main**.



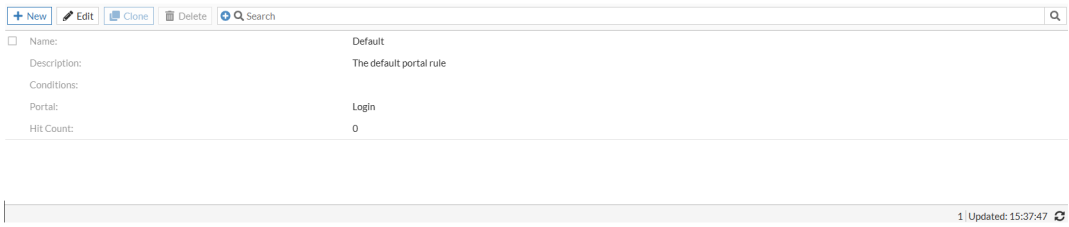
6. Switch to the **Labels** tab to customize the names of the GUI components on the guest portal.



7. Click **OK**.

Portal rules

The FortiAuthenticator can be used to create a set of rules to allow user access to different portals that have been created.



The following settings are available in the **Portal Rules** tab:

New	Select to create a new portal rule. See Creating a portal rule on page 170.
Edit	Select to edit the selected portal rule.
Clone	Select to clone the selected portal rules.
Delete	Select to delete the selected portal rules.
Search	Enter a search term in the search field, then select **Search** to search the portal rules list.

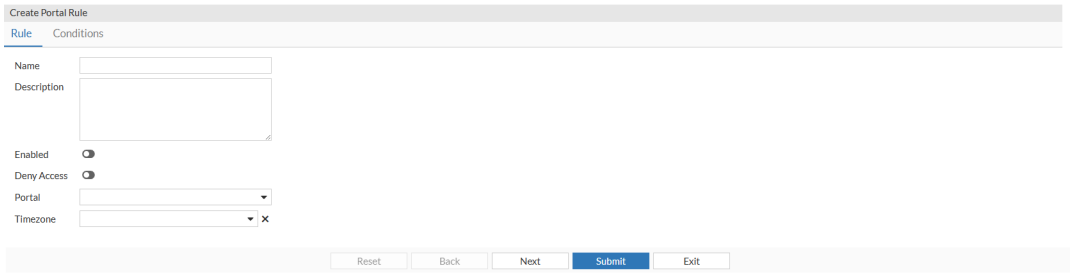
Each rule that is created is subject to certain conditions that you can create.

If a rule is matched, the user is allowed or denied access to the portal and no other rules are checked. If no rule matches then the default rule is applied.

Creating a portal rule

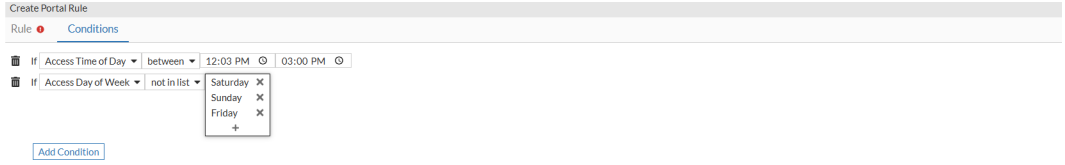
To create a portal rule:

1. Go to **Authentication > Guest Portals (beta) > Portal Rules**, and select **New**.
   The **Create Portal Rule** window opens.



2. Enter the **Name** of the rule.
3. Optionally, enter a description.
4. Select **Enabled** and then select one of the portals you have created, or the default portal from the **Portal** dropdown menu to direct the user to the relevant portal.
5. Enable **Deny Access** if you do not wish to redirect the user to the guest portal.
6. From the dropdown, select the applicable **Timezone**.
7. Switch to the **Conditions** tab and create the conditions applicable to your portal rules.
8. Click **Add Condition** to create new conditions, and click **Submit**.
   From the provided drop down lists, create a set of rules that apply to your portal.

   In this example, the user is redirected to the portal **Login** (specified in the previous step) on a given day of the week (except Saturday, Sunday, and Friday) between 12:30 PM and 3:00 PM.



Notes:

- Configure the following URL in the SSID for captive portal re-direction.

  ```
  {FortiAuthenticator_IP or FQDN}/fg/api/v1/cp/portal/fortigate
  ```

  To redirect to the success page, the post login URL is:

  ```
  {FortiAuthenticator_IP or FQDN}/fg/api/v1/cp/success
  ```

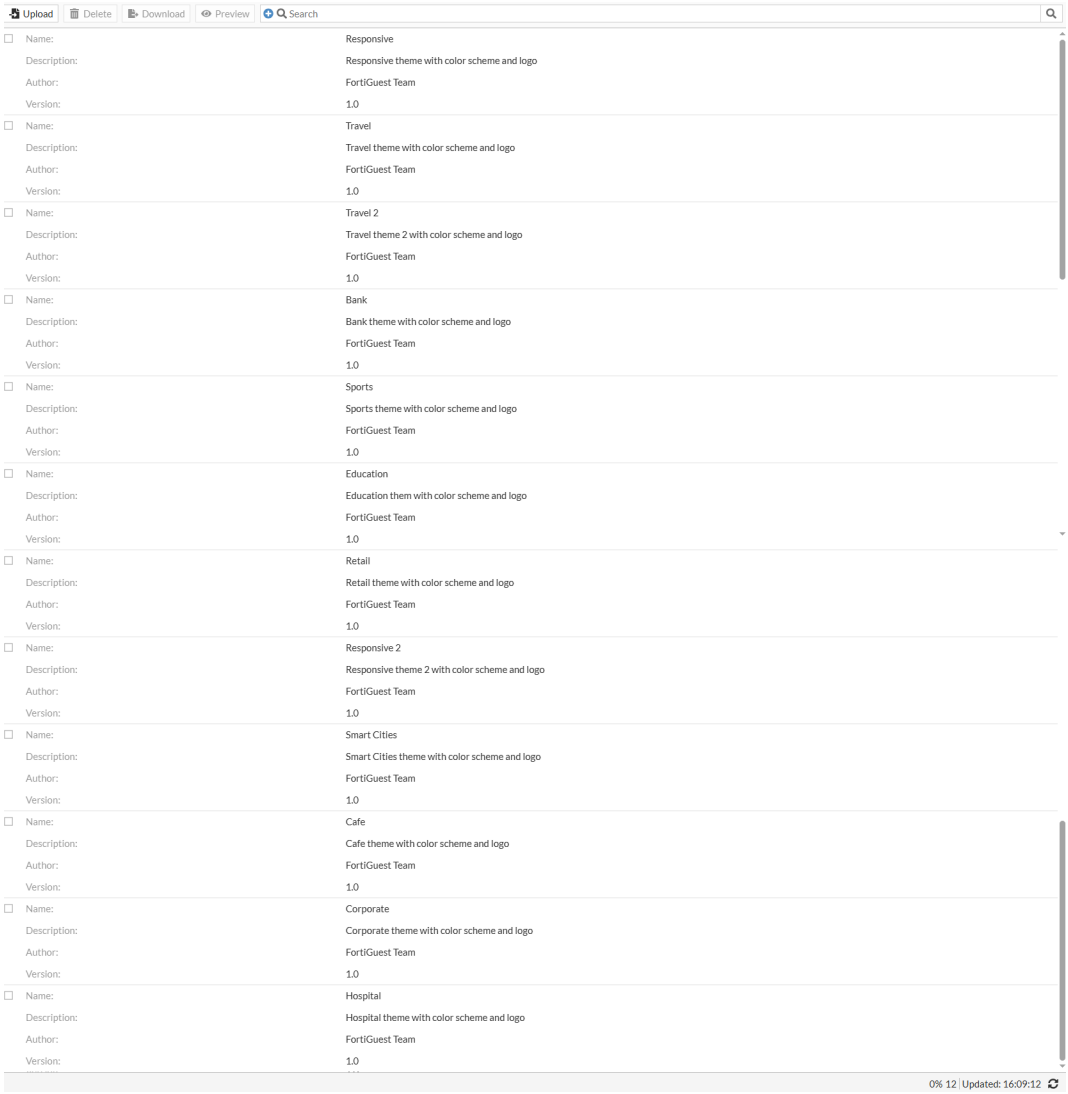
- Add the following FQDNs in the allowed list in FortiGate, for captive portal login with Google Chrome (Windows).
  - Google Chrome: IP subnet `13.107.4.52 255.255.255.255`
  - `Fonts.gstatic.com FQDN`
  - `ssl.gstatic.com`
- RADIUS clients with a generic type cannot be added to any group.
- A RADIUS client cannot belong to multiple groups.

Guest themes

You can create guest portal themes as per your business requirement.

FortiAuthenticator provides a default theme that you can download, customize and upload it.

Ensure that you comply with Rules on page 175, to successfully upload guest themes.



The following options are available in the **Guest Themes** tab:

Upload	Select to upload a guest theme from the management computer.
Delete	Select to delete the selected guest themes.
Download	Select to download the selected guest themes.
Preview	Select to preview the selected guest portal.
Search	Enter a search term in the search field, then select **Search** to search the guest themes list.

1. Go to **Authentication > Guest Portals (beta) > Guest Themes**.
2. Select the default theme (or any existing theme), and click **Download**.
3. Unzip the downloaded file view the folder structure of the theme.
4. Update the following files and folders and upload on the page.
   a. theme.css on page 173
   b. theme.json on page 173

c. images on page 175
d. html on page 175

`theme.css`

This file is in the `css` directory of the theme structure and contain all the styles that are applied to the several HTML pages that make up the portal site.

`theme.json`

The `theme.json` file lists all resources used by the theme as well as defining the default values for several elements.

You can update the following elements.

- id on page 173
- public_name on page 173
- author on page 173
- mandatory_pages on page 173
- optional_pages on page 174
- Layout on page 175
- images on page 175
- standard_palettes on page 175

`id`

This is a mandatory element, it should only contain letters, digits and the underscore symbol, theme IDs are unique so if there is already a theme with this ID installed on FortiAuthenticator, then you cannot install this theme.

`public_name`

This is an optional element, it should contain the name displayed on the administration interface when referring to the theme, this element does not have the restrictions that apply to the ID element. If the `public_name` element is not present, the theme's internal name is displayed.

`author`

This attribute is used by the theme author to place his name and/or contact details.

`mandatory_pages`

In this element, you can list the HTML templates for every kind of page the portal uses as well as declaring what content areas each page has and what should be it's default value.

```
"login": {
"menu_item_weight": 1,
"label": "Login",
"components": [
{
"label": "Title",
"tag": "%TITLE%",
"content": "Login to the network"
},
{
"label": "Header",
"tag": "%HEADER%",
"content": "Login to the network"
},
```

```
{
"label": "Main",
"tag": "%MAIN%"
}
]
}
```

This example specifies the HTML template for the login page in the `html` folder. The `login.html` file uses the following components.

```
<h2 id="pageTilte">%HEADER%</h2>
<div class="feedbackContent">%FEEDBACK_AREA</div>
<div class="mainContent">%MAIN%</div>
<div class="widgetContainer">%LOGIN_WIDGET%</div>
<div id="loginNavigation" class="col-md-4 hidden-sm hidden-xs"> %NAVIGATION_MENU% </div>
```

The placeholder variables for the several components defined in `theme.json` are placed amongst the markup, when the portal pages are generated the placeholders are replaced with the content associated with them. The content of these placeholders is built dynamically by FortiAuthenticator depending on what options are selected during the portal setup. When creating your own themes you should make sure that these placeholders are in your template files otherwise the portal might not work as expected.

`optional_pages`

This section allows you to specify any optional pages you want to make available to portals using your theme. The default theme defines several optional pages, to add more you can copy one of the existing definitions and edit it as appropriate.

```
"menu_item_weight": 1000,
"lablel" : "Welcome",
"id": "welcome",
"description": "Welcome page, can be used as alternative landing page to portal"
"components": [
{
"label": "Title",
"tag": "%TITLE%",
"content": "Welcome"
},
{
"label": "Header",
"tag": "%HEADER%",
"content": "Welcome"
},
{
"label"; "Header",
"tag": "%HEADER%",
"content": "Welcome"
},
{
"label": "Main",
"tag": "%MAIN%",
"content":"Welcome"
```

```
}
]
```

`Layout`

The element layout is present in `theme.json` with the supported values of `one_panel_center`, `one_panel_right`, `one_panel_left`, and `two_panel`.

```
"layout": "two_panel"
```

`images`

This element of the file is used to list all image files that are referenced by the HTML and CSS for the theme.

You can modify the default images by replacing them with your own `file_name`.

```
{
"label": "Company logo large",
"description": "Used on the login page on large screen devices",
"tag": "%IMG_LOGO%", "file_name": "Logo.png",
"dimensions": "300x40"
}
```

`standard_palettes`

These elements contain a list of all customizable colors used in the theme.

The default theme already has a set of color palettes defined, to add a new one, you can edit as follows.

```
{
"tag": "%CL_BODY_BACKGROUND%",
"label": "Body background color",
"value": "#f6f6f6"
}
```

This snippet specifies the label and value for the color, this information is displayed on the portal setup page so the administrator knows where and what for the color is used for. The tag specifies what placeholder variable is used in HTML and CSS template files to refer to this color, the value element specifies the color hex value.

`images`

This folder contains all images used in your guest theme. Add all the images that you want to use in this folder.

`html`

This folder contains all the HTML files that are a part of the guest portal. You can edit all these files as per your requirement and portal design.

Rules

To successfully enable the upload of guest themes, ensure that the following rules are complied with.

Rule	Acceptable values
HTML elements	`html, body, nav, a, abbr, acronym, address, area, b, big, blockquote, br, button, caption, center, cite, code, col, colgroup, dd, del, dfn, dir, div, dl, dt, em, font, h1, h2, h3, h4, h5, h6, hr, i, img, ins, kbd, label, legend, li, map, menu, ol, p, pre, q, s, samp, small, span, strike, strong, sub, sup, table, tbody, td, tfoot, th, thead, tr, tt, u, ul, var`
HTML attributes	`abbr, accept, accept-charset, accesskey, action, align, alt, axis, border, cellpadding, cellspacing, char, charoff, charset, checked, cite, clear, cols, colspan, color, compact, coords, datetime, dir, enctype, for, headers, height, href, hreflang, hspace, id, ismap, label, lang, longdesc, maxlength, method, multiple, name, nohref, noshade, nowrap, prompt, rel, rev, rows, rowspan, rules, scope, shape, size, span, src, start, summary, tabindex, target, title, type, usemap, valign, value, vspace, width, class, role, data-toggle, data-target, style`
HTTP schemes	`http, https, lml`

Remote authentication servers

If you already have LDAP, RADIUS, SAML, OAuth, and TACACS+ servers configured on your network, FortiAuthenticator can connect to them for remote authentication, much like FortiOS remote authentication.

General

Go to **Authentication > Remote Auth. Servers > General** to edit general settings for remote LDAP and RADIUS authentication servers.

Remote LDAP	Enter the number of seconds between 1-3600 (or one second to one hour) for the LDAP server response and status cache timeouts.
Remote RADIUS	Select whether the remote RADIUS server requires case sensitive usernames.

Click **Save** to save your changes.

LDAP

If you have existing LDAP servers, you may choose to continue using them with FortiAuthenticator by configuring them as remote LDAP servers.

When entering the remote LDAP server information, if any information is missing or in the wrong format, error messages will highlight the problem for you.

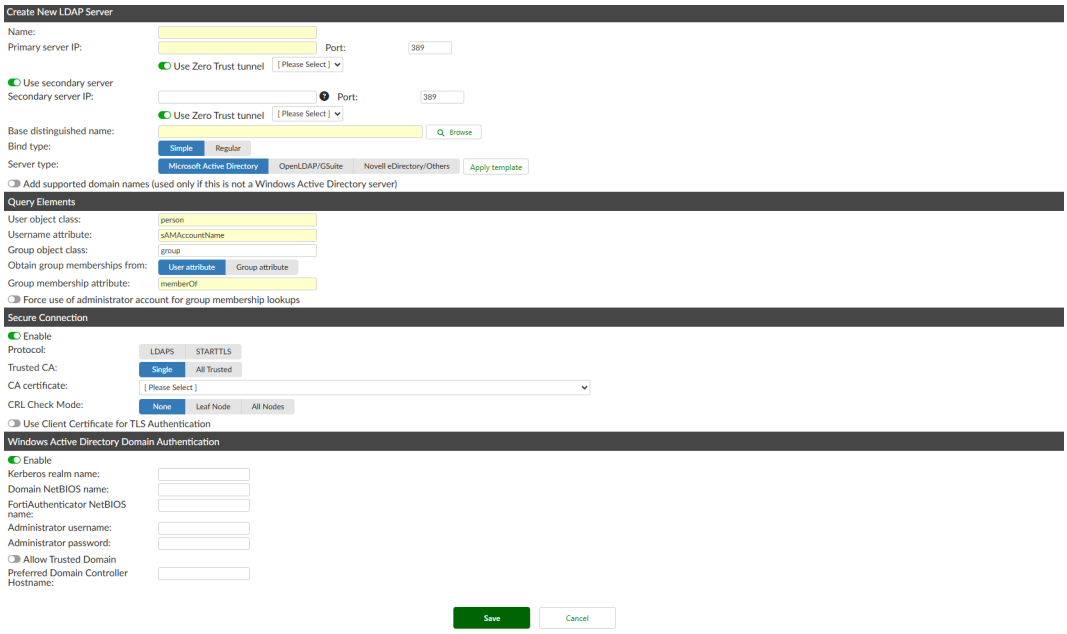
FortiAuthenticator supports multiple Windows AD server forests, with a maximum of 99 remote LDAP servers with Windows AD enabled.

To view all information about your multiple servers, go to **Monitor > Authentication > Windows AD**.

FortiAuthenticator LDAP server does not support Password+OTP concatenation for FortiToken Cloud-issued FortiToken Mobile tokens.

To add a remote LDAP server entry:

1. Go to **Authentication > Remote Auth. Servers > LDAP** and select **Create New**. The **Create New LDAP Server** window opens.



2. Enter the following information.

Name	Enter the name for the remote LDAP server on FortiAuthenticator.
Primary server name/IP	Enter the IP address or FQDN for this remote server. Enter the IP address only when **Use Zero Trust tunnel** is enabled.
Port	Enter the port number.
Use Zero Trust tunnel	Enable to use a zero trust tunnel. From the dropdown, select a zero trust tunnel.

Use secondary server	Select to use a secondary server. The secondary server name/IP and port must be entered.  **Limitations of the secondary LDAP server** • The secondary LDAP server is only used for user authentication. • The secondary LDAP server cannot be used for domain joining, i.e., domain joining may fail when the primary server is unavailable. • The secondary LDAP server cannot be used for FSSO related activities, e.g., group lookup. See AD server authentication on page 182.
Secondary server name/IP	Enter the IP address or FQDN for the secondary remote server. Enter the IP address only when **Use Zero Trust tunnel** is enabled. This option is only available when **Use secondary server** is selected.  The secondary IP address/FQDN is used exclusively as redundancy for the queries to the LDAP protocol. It is not used as redundancy for Windows AD authentication (NTLM). The NTLM authentication redundancy can be accomplished by using FQDN for the primary and multiple AD server IP addresses registered to that FQDN in the DNS infrastructure.
Secondary port	Enter the port number for the secondary server. This option is only available when **Use secondary server** is selected.
Use Zero Trust tunnel	Enable to use a zero trust tunnel for the secondary server. From the dropdown, select a zero trust tunnel. This option is only available when **Use secondary server** is selected. **Note:** FortiAuthenticator uses the zero trust tunnel associated with the secondary server only when it is unable to reach the primary server (zero trust enabled).
Base distinguished name	Enter the base distinguished name for the server using the correct X.500 or LDAP format. The maximum length of the DN is 512 characters. You can also select the browse button to view and select the DN on the LDAP server.
Bind Type	The Bind Type determines how the authentication information is sent to the server. Select the bind type required by the remote LDAP server. • **Simple**: bind using the user's password which is sent to the server in plaintext without a search. • **Regular**: bind using the user's DN and password and then search. If the user records fall under one directory, you can use **Simple** bind type. But **Regular** is required to allow a search for a user across multiple domains.

Server type	Select a LDAP server type and click **Apply template** to populate the **Query Elements** fields with the selected template: **Microsoft Active Directory**, **OpenLDAP**, or **Novell eDirectory**
Add supported domain names (used only if this is not a Windows Active Directory server)	Select to enter multiple domain names for remote LDAP server configurations. The FortiAuthenticator can then identify the domain that users on the LDAP server belong to.

3. If you want to want to import a specific LDAP system's template, under **Query Elements**, enter the following:

User object class	The type of object class to search for a user name search. The default is **person**.
Username attribute	The LDAP attribute that contains the user name. The default is **sAMAccountName**.
Group object class	The type of object class to search for a group name search. The default is **group**.
Obtain group memberships from	The LDAP attribute (either user or group) used to obtain group membership. The default is **User attribute**.
Group membership attribute	Used as the attribute to search for membership of users or groups in other groups.
Force use of administrator account for group membership lookups	Enabling this feature prevents non-admin users from searching their own attributes even after successful binding. This feature has been implemented to enhance Oracle-based ODSEE LDAP support.

4. If you want to have a secure connection between FortiAuthenticator and the remote LDAP server, under **Secure Connection**, select **Enable**, then enter the following:

Protocol	Select **LDAPS** or **STARTLS** as the LDAP server requires.
Trusted CA	Select **Single** or **All Trusted CA**: • **Single**: only one specific CA is trusted. • **All Trusted**: allow all configured trusted CAs (local and trusted).
CA Certificate	Select the CA certificate that verifies the server certificate from the dropdown menu.
CRL Check Mode	Select from the following three options: • **None** (default): Does not check CRL(s). • **Leaf Node**: Only checks the CRL, if any, for issuing CA of remote LDAP server certificate. • **All Nodes**: Checks all the CRLs of CAs in the chain. **Note**: When selected, FortiAuthenticator must be configured with a CRL for every CA in the chain and the remote LDAP server must provide the full certificate chain during the TLS handshake.
Use Client Certificate for TLS Authentication	Enable to select a client certificate to use to authenticate a TLS connection with the secure remote LDAP server.

5. If you want to authenticate users using MSCHAP2 PEAP in an Active Directory environment, enable **Windows Active Directory Domain Authentication**, then enter the required Windows AD Domain Controller information.

Kerberos realm name	Enter the domain's DNS name in uppercase letters.
Domain NetBIOS name	Enter the domain's DNS prefix in uppercase letters.
FortiAuthenticator NetBIOS name	Enter the NetBIOS name that identifies FortiAuthenticator as a domain member.
Administrator username	Enter the name of the user account that's used to associate FortiAuthenticator with the domain. This user must have at least domain user privileges. To configure an Active Directory user with the minimum privileges needed to join an AD domain, see Configure minimum privilege Windows AD user account on page 181.
Administrator password	Enter the administrator account's password.
Allow Trusted Domain	Enable to allow trusted domain.
Preferred Domain Controller Hostname	Enter the preferred domain controller hostname.

When you are finished here, go to **Authentication > RADIUS Service > Clients** to choose whether authentication is available for all Windows AD users or only for Windows AD users who belong to particular user groups that you select. See RADIUS service on page 189 for more information.

6. If you want to import remote LDAP users, under **Remote LDAP Users**, select either **Import users** or **Import users by group memberships** and click **Go**. A separate window opens where you may specify the LDAP server, apply filters, and attributes. Select **User attributes** to edit the following LDAP user mapping attributes:

Username	Enter the remote LDAP user's name.
First name	Enter the attribute that specifies the user's first name. Set to **givenName** by default.
Last name	Enter the attribute that specifies the user's last name. Set to **sn** by default.
Email	Enter the attribute that specifies the user's email address. Set to **mail** by default.
Phone	Enter the attribute that specifies the user's number. Set to **telephoneNumber** by default.
Mobile number	Enter the attribute that specifies the user's mobile number. Set to **mobile** by default.
FTK-200 serial number	Enter the remote LDAP user's FortiToken serial number.
Certificate binding common name	Enter the remote LDAP user's certificate-binding CN. When this field is populated, the **Certificate binding CA** must also be specified.
Certificate binding CA	Local or trusted CAs to apply for the remote LDAP user. Must be specified if the **Certificate binding common name** is populated.
Display name	Enter the attribute that specifies the user's display name. Set to displayName by default.

Company	Enter the attribute that specifies the user's company. Set to company by default.
Department	Enter the attribute that specifies the user's department. Set to department by default.
Title	Enter the attribute that specifies the title. Set to title by default.

7. Select **Save** to apply your changes.
   You can now add remote LDAP users, as described in Remote users on page 107.

Configure minimum privilege Windows AD user account

To respect the principle of least privilege, a domain administrator account should not be used to associate FortiAuthenticator with a Windows AD domain. Instead, a non-administrator account can be configured with the minimum privileges necessary to successfully join a Windows AD domain. To do this, create a user account in the applicable hierarchy of your Active Directory, then delegate the ability to manage computer objects to the user account.

1. In the Active Directory, create a user account with the following options selected:
   - **User cannot change password**
   - **Password never expires**
2. In **Active Directory Users and Computers**, right-click the container under which you want the computers added, then click **Delegate Control**.
   The Delegation of Control Wizard opens.
3. Click **Next**.
4. Click **Add**, then enter the user account created in step 1.
5. Click **Next**.
6. Select **Create custom task to delegate**, then click **Next**.
7. Select **Only the following objects in the folder**, and then select **Computer objects**.
8. Select **Create selected objects in this folder**, then click **Next**.
9. Under **Permissions**, select **Create All Child Objects**, **Write All Properties**, and **Change password**.
10. Click **Next**, then click **Finish**.

Remote LDAP password change

The current password has to be provided to change a password when an account joins the domain.

Windows AD users can conveniently change their passwords without provision changes being made to the network by a Windows AD system administrator. There are three ways FortiAuthenticator supports a password change: RADIUS login, GUI user login, and GUI user portal.

RADIUS login:

For the method to work, all of the following conditions must be met:

- FortiAuthenticator has joined the Windows AD domain.
- RADIUS client has been configured to "Use Windows AD domain authentication".

- RADIUS authentication request uses MS-CHAPv2.
- RADIUS client must also support MS-CHAPv2 password change.

A "change password" response is produced that FortiAuthenticator will recognize, which allows cooperation between the NAS and the Windows AD server that will result in a password change.

GUI user login:

For this method to work, **one** of the following conditions must be met:

- FortiAuthenticator has joined the Windows AD domain
- Secure LDAP is enabled and the LDAP admin (i.e. regular bind) has the permissions to reset user passwords

You must log in via the GUI portal. FortiAuthenticator will validate the user password against a Windows AD server. The Windows AD server returns with a change password response. If that happens, the user is prompted to enter a new password.

GUI user portal:

For this method to work, **one** of the following conditions must be met:

- FortiAuthenticator has joined the Windows AD domain.
- Secure LDAP is enabled.

After successfully logging into the GUI, the user has access to the user portal. If desired, the user can change their password in the user portal.

Remote LDAP password reset

Password reset, i.e., setting a new password without providing the old password, is only allowed over LDAPS and only if the LDAP admin, i.e., regular bind, has permission to reset the user passwords.

AD server authentication

FortiAuthenticator can use two modes of authentication to the AD server depending on how FortiAuthenticator is configured:

1. LDAP based authentication (LDAP bind)
2. Windows AD authentication (NTLM- FortiAuthenticator must join the domain)

In the case of 1:

- The secondary IP address/FQDN is used if FortiAuthenticator fails to connect to the primary server.
- If using an FQDN for the primary or secondary server, you can decide to do load-balancing/failover to multiple LDAP servers at the DNS level.

In the case of 2:

- The secondary IP address/FQDN is never used.
- If load-balancing/failover is required, it must be done at the DNS level.

RADIUS

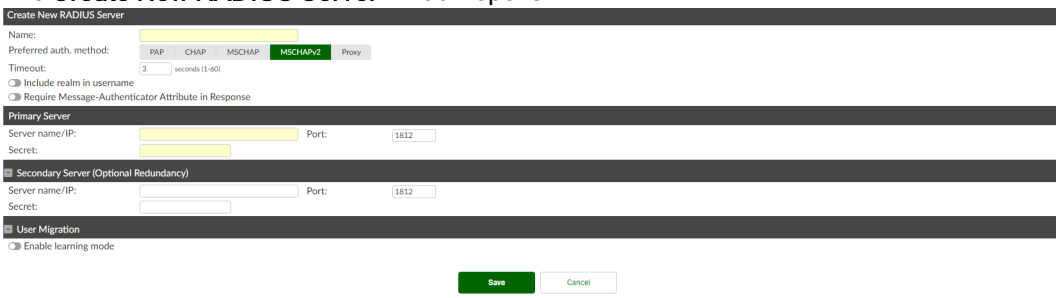
If you have existing RADIUS servers, you may choose to continue using them with FortiAuthenticator by configuring them as remote RADIUS servers. This feature can also be used to migrate away from third-party two-factor authentication platforms.

When entering the remote RADIUS server information, if any information is missing or in the wrong format, error messages will highlight the problem for you.

FortiAuthenticator RADIUS server does not support Password+OTP concatenation for FortiToken Cloud-issued FortiToken Mobile tokens.

To add a remote RADIUS server entry:

1. Go to **Authentication > Remote Auth. Servers > RADIUS** and select **Create New**.
   The **Create New RADIUS Server** window opens.



2. Enter the following information, then select **Save** to add the RADIUS server.

Name	Enter the name for the remote RADIUS server on FortiAuthenticator.
Preferred auth. method	Select from either **MSCHAPv2** (by default), **MSCHAP**, **CHAP**, **PAP**, or **Proxy**. **Note**: The **Proxy** option allows FortiAuthenticator to proxy RADIUS authentication sessions without changing the authentication method, meaning FortiAuthenticator passes the authentication credentials sent by the RADIUS client through to the remote RADIUS server unchanged.
Timeout	Enter a timeout in seconds between 1-60 seconds (3 by default). Note that a high timeout may impact the processing rate of authentication requests if the remote RADIUS server becomes unresponsive.
Include realm in username	Enable for eduroam services. When enabled, the username string sent to the remote RADIUS server is the same as the username string received from the RADIUS client. FortiAuthenticator can now keep the realm portion of the username before proxying.

	This allows FortiAuthenticator to route the RADIUS authentication requests through a hierarchy of RADIUS authentication proxy servers. **Note**: The option is disabled by default.
Require Message-Authenticator Attribute in Response	When FortiAuthenticator is the RADIUS client, FortiAuthenticator always includes the message authenticator attribute when sending the RADIUS authentication requests. When the option is enabled, FortiAuthenticator only accepts the responses that include the message authenticator attribute that was sent.
Primary Server	Enter the server name or IP address, port, and secret in the fields provided to configure the primary server.
Secondary Server (Optional Redundancy)	Optionally, add redundancy by configuring a secondary server.
User Migration	Select **Enable learning mode** to record and learn users that authenticate against this RADIUS server. This option should be enabled if you need to migrate users from the server to the FortiAuthenticator.

TACACS+

FortiAuthenticator can be configured to connect to remote TACACS+ servers.

FortiAuthenticator TACACS+ server does not support Password+OTP concatenation for FortiToken Cloud-issued FortiToken Mobile tokens.

To add a remote TACACS+ server:

1. Go to **Authentication > Remote Auth. Servers > TACACS+** and select **Create New**.
   The **Create New TACACS+ Server** window opens.
2. Enter the following information:

Name	The name of the remote TACACS+ server.
Preferred auth. method	Select either **ASCII** or **PAP**.
Timeout	Enter a timeout in seconds between 1-60 seconds (3 by default).  A high timeout may impact the processing rate of authentication requests if the remote TACACS+ server becomes unresponsive.
IP address/FQDN	The IP address or FQDN with the port number (default = 49) of the TACACS+ server.
Secret	The TACACS+ server passphrase.

Secondary Server (Optional Redundancy)	
Server name/IP	The IP address or FQDN with the port number (default = 49) of the secondary TACACS+ server.
Secret	The secondary TACACS+ server passphrase.

3. Click **Save** to add the remote TACACS+ server.

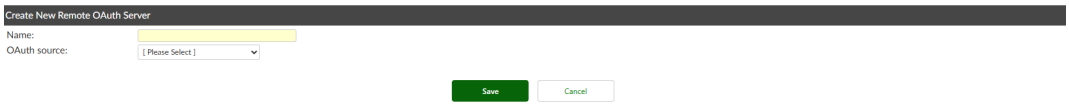
OAUTH

FortiAuthenticator can be configured to connect to remote OAuth servers to dynamically look up group memberships from third-party SAML identify providers, such as G Suite and Azure, for SAML SP FSSO.

FortiAuthenticator OAuth server does not support Password+OTP concatenation for FortiToken Cloud-issued FortiToken Mobile tokens.

To add a remote OAuth Server:

1. Go to **Authentication > Remote Auth. Servers > OAUTH** and select **Create New**.
The **Create New Remote OAuth Server** window appears.



2. Enter the following information:

Name	Enter the name for the remote OAuth server on FortiAuthenticator.
OAuth source	Select an OAuth source: **Social Authentication** • **Facebook** • **Google** • **LinkedIn** • **Twitter** • **WeChat** For **Facebook**, **Google**, **LinkedIn**, **Twitter**, and **WeChat** enter the **Key** and **Secret** for the selected OAuth source. **SAML Authentication** • **Azure Directory** • **Google Workspace Directory** For **Azure Directory**: • Enter the **Client ID** and **Client Key** for the Azure Directory. • Enable **Include for FSSO** and enter the **Azure AD tenant ID**.

	For **Google Workspace Directory**, enter the **Google workspace admin** and select and upload the **Service account key file (.json)** from the management computer.
Key	Enter the OAuth application key for the selected OAuth source. This option is only available when **Facebook**, **Google**, **LinkedIn**, **Twitter**, or **WeChat** is selected as an OAuth source.
Secret	Enter the OAuth application secret for the selected OAuth source. This option is only available when **Facebook**, **Google**, **LinkedIn**, **Twitter**, or **WeChat** is selected as an OAuth source.
Client ID	Enter the application ID for the Azure Directory application, obtained from the Azure portal. This option is only available when **Azure Directory** is selected as an OAuth source.
Client Key	Enter the key for the Azure Directory application, obtained from the Azure portal. This option is only available when **Azure Directory** is selected as an OAuth source.
Azure AD tenant ID	Enter the Microsoft Entra ID (formerly Azure AD) tenant ID. This option is only available when **Azure Directory** is selected as an OAuth source. **Note**: The field is required for SCEP integration with MS InTune.
Include for SSO	Enable to include the OAuth server for SSO. This option is only available when **Azure Directory** is selected as the OAuth source. **Note**: The option is disabled by default. For information on configuring SSOMA with AD, see Configuring SSOMA with AD in the latest *EMS Administration Guide*.
Google workspace admin	Enter the Google Workspace admin username for the G Suite Directory application. This option is only available when **Google Workspace Directory** is selected as an OAuth source.
Service account key file (.json)	Select and upload the service account key file for the Google Workspace Directory application, obtained from the Google developers portal. This option is only available when **Google Workspace Directory** is selected as an OAuth source.

3. Select **Save** to add the remote OAuth server.

SAML

FortiAuthenticator SAML server does not support Password+OTP concatenation for FortiToken Cloud-issued FortiToken Mobile tokens.

To add a remote SAML Server:

1. Go to **Authentication > Remote Auth. Servers > SAML** and select **Create New**.
   The **Create New Remote SAML Server** window appears.
2. Enter the following information:

Name	Enter a name for the remote SAML server.
Description	Enter a description for the remote SAML server.
Device FQDN	The FQDN of the configured device from the system dashboard.
Type	Select **FSSO** or **Proxy** as the remote SAML server type.
URL Nomenclature	Select the method to determine the URL path of the SAML service provider. • **Individualize**:Enable to include the name of the SAML service provider in the URL path. • **Legacy**: Enable to set the URL to a predetermined URL path. Note that Legacy can only be enabled for an existing configured SAML identity providers.
Portal URL	The SAML service provider login URL.
Entity ID	The SAML service provider Entity ID.
ACS (login) URL	The SAML service provider Assertion Consumer Service (ACS) login URL.
Import IDP metadata/certificate	Select to import the SAML IdP metadata or certificate file.
IDP entity ID	Also known as the entity descriptor. Enter the unique name of the SAML identity provider, typically an absolute URL: `https://idp_name.example.edu/idp`
IDP single sign-on URL	Enter the identity provider portal URL you want to use for SSO.

IDP certificate fingerprint	Enter the fingerprint of the certificate file. To calculate the fingerprint, you can use OpenSSL.
	Use the following OpenSSL command:
	`$ openssl x509 -noout -fingerprint -in "server.crt"`
	Example result, showing the fingerprint:
	`SHA1 Fingerprint=AF:E7:1C:28:EF:74:0B:C8:74:25:BE:13:A2:26:3D:37:97:1D:A1:F9`

Fingerprint algorithm	The SAML portal by default uses SHA-256. **Note**: SHA-1 has been deprecated.

	 A warning is displayed if SHA-1 is detected upon upgrade.
Certificate issuer	Displays the certificate issuer.
Certificate subject	Displays the certificate subject.
Validity period	Displays the certificate validity period.
Authentication context	Select the authentication context value for the "RequestedAuthnContext" assertion. • **Default**: The default value uses "PasswordProtectedTransport" authentication, which indicates that the IdP requires users to be authenticated using a password-based method. • **MFA**: Enforces MFA on the remote SAML IdP server.  When selected, FortiAuthenticator indicates in the SAML authentication requests to the remote SAML IdP server that MFA is required.  When MFA enforcement is enabled, and a non-MFA authentication context is included in the IdP response, the authentication fails with `Error 401 Unauthorized`. • **None**: Omits the "RequestedAuthnContext" assertion when an alternative to password-based authentication is used. **Attempt token-based authentication locally if external IdP does password-only authentication**: Enable to attempt token-based authentication locally if external IdP does password-only authentication. **Note**: The option is only available when the **Type** is **Proxy** and **Authentication context** is **MFA**.
Send username in this parameter	Specify the parameter name in which the remote IdP receives the username so as to prefill the username login field (default = username).
Strip realm from username before sending	Enable to strip realm from the username before sending. The option is enabled by default.
Enable IdP-initiated assertion response	Allows IdP to send an assertion response to the SP without a prior request from the SP. Enabling this setting allows the SP to participate in IdP initiated login.
Send AuthnRequest with HTTP-POST binding	If enabled, HTTP-POST binding is used for authentication requests. Otherwise, HTTP-Redirect binding is used by default.

Sign SAML requests with a local certificate		Select to choose a local SAML certificate.
Single Logout		
	Enable SAML single logout	Select to enable **SLS (logout) URL** and set **IDP single logout URL**.
Username		
	Obtain username from	Select the method to extract usernames: • **Subject NameID SAML assertion**: Enable to obtain usernames from the subject NameID assertion returned by the SAML IdP. • **Text SAML assertion**: Enable and enter the text-based SAML assertion that usernames are obtained from. For example: `email`
Group Membership		
	Obtain group membership from	Most SAML IdP services will return the username in the Subject NameID assertion, however not all IdP services are consistent. FSSO requires group membership of each user with an active SSO session while different SAML IDP services require different methods of retrieving the group information. Before now, group information could only be obtained from very specific (hardcoded) SAML assertions. You can choose to configure SAML assertions used in group membership retrieval, retrieve group membership from an LDAP service, or retrieve group membership from an OAuth server. Select the method to extract usernames: • **SAML assertions**: Enable and choose whether usernames are pulled in from boolean assertions or text-based attributes. • **LDAP lookup**: Enable and select the LDAP server to obtain group memberships. • **Cloud**: Enable and select the OAuth server and group field to obtain group memberships.
	Implicit group membership	Select to choose a local group the retrieved SAML users are placed into.

3. Select **Save** to add the remote SAML server.

RADIUS service

The FortiAuthenticator RADIUS AAA (authentication, authorization, and account) server is already configured and running with default values. Each user account on FortiAuthenticator has an option to allow authentication using the RADIUS database.

Before FortiAuthenticator will accept RADIUS authentication requests from a device, it must be registered as a authentication client on FortiAuthenticator, and it must be assigned a RADIUS policy.

When changes are made to RADIUS authentication clients and policies, log messages are generated to confirm the admin configuration change, and to state that the RADIUS server was restarted to apply the change.

FortiAuthenticator allows both RADIUS and remote authentication for RADIUS configurations. If you want to use a remote server, you must configure it first. See Remote authentication servers on page 176. You can configure the built-in LDAP server before or after creating client entries, see LDAP service on page 213.

For VM appliances, the ratio for RADIUS clients is "number of max users / 3".

The number of RADIUS policies is "number of max users".

See the **Maximum values** table included in the latest FortiAuthenticator Release Notes for more details.

Beginning in 6.1.0, RADIUS authentication logic is determined by policies, created in **Authentication > RADIUS Service > Policies**.

When upgrading from a version prior to 6.1.0, existing RADIUS client configurations are migrated into clients and policies with corresponding settings.

RADIUS related services must be enabled on the interface being used in **System > Network > Interfaces**.

Clients

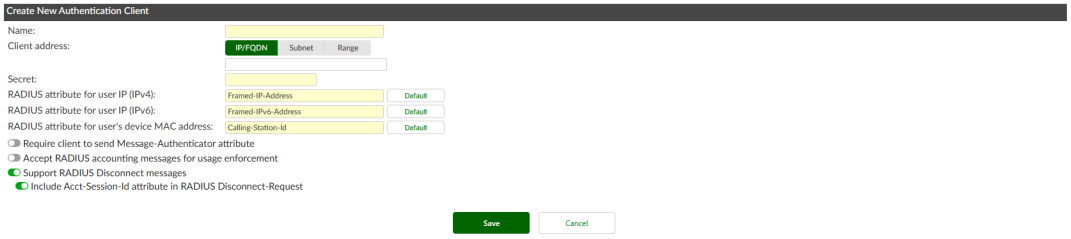
You must configure each device requesting authorization from the RADIUS server as a FortiAuthenticator RADIUS client.

RADIUS accounting clients can be managed from **Authentication > RADIUS Service > Clients**.

Configured clients are assigned to one or more RADIUS policies that determine the authentication logic.

To configure a RADIUS client:

1. Go to **Authentication > RADIUS Service > Clients**, and click **Create New** to add a new RADIUS client. The **Create New Authentication Client** window opens.



2. Provide the following information to configure the client:

Subnets and IP ranges can be defined in the **Client address** field. All authentication clients within a defined subnet/IP range will share the same configuration and shared secret. For example, 192.168.0.0/24 would allow all 255 IP addresses to authenticate. This saves time because it only uses a single client entry in the license table.

Name	A name to identify the authentication client.
Client address	The **IP/Hostname**, **Subnet**, or **Range** of the client.
Secret	The RADIUS passphrase shared with the client.
RADIUS attribute for user IP (IPv4)	Enter the radius attribute for the user IPv4 address. **Framed-IP-Address** is the default RADIUS attribute.
RADIUS attribute for user IP (IPv6)	Enter the radius attribute for the user IPv6 address. **Note**: **Framed-IPv6-Address** is the default RADIUS attribute.
RADIUS attribute for user's device MAC address	Enter the can RADIUS attribute for the user MAC IP address. **Note**: **Calling-Station-Id** is the default RADIUS attribute.
Require client to send Message-Authenticator attribute	When FortiAuthenticator is the RADIUS server and the option is enabled, the RADIUS client must include the message authenticator attribute in the RADIUS authentication requests. Otherwise, FortiAuthenticator discards the RADIUS authentication requests.
Accept RADIUS account messages for usage enforcement	Allows FortiAuthenticator to accept RADIUS accounting messages for usage enforcement.  In order to accept account messages for enforcement, the client address must be set as an **IP/Hostname**. **Subnet** and **Range** client address types are not supported.
Support RADIUS Disconnect messages	Allows FortiAuthenticator to support RADIUS Disconnect messages.  In order to support RADIUS disconnect messages, the client address must be set as an **IP/Hostname**. **Subnet** and **Range** client address types are not supported.
Include Acct-Session-Id attribute in RADIUS Disconnect-Request	Enable to include the account session ID attribute in the RADIUS Disconnect messages. **Note**: The option is only available when **Support RADIUS Disconnect messages** is enabled.

3. Select **Save** to add the new RADIUS client.

If authentication fails, check that the authentication client is configured and that its IP address is correctly specified. Common causes of problems are:

- RADIUS packets sent from an unexpected interface, or IP address.
- NAT performed between the authentication client and FortiAuthenticator.

To import RADIUS clients:

1. Go to **Authentication > RADIUS Service > Clients**, and click **Import**.
   The **Import RADIUS Clients** window opens.
2. Click **Upload a file** and choose the file location of the CSV file containing your RADIUS client list.
   Each line of the CSV file must contain values in the following format:
   - **Name**: String (the same character restrictions as in the GUI).
   - **Address**: IP address, subnet, or IP range.
   - **Secret**: String (the same character restrictions as in the GUI).
   - **RADIUS attribute for user IP (IPv4)**: String (the same character restrictions as in the GUI).
   - **RADIUS attribute for user IP (IPv6)**: String (the same character restrictions as in the GUI).
   - **RADIUS attribute for user's device MAC address**: String (the same character restrictions as in the GUI).
   - **Accept RADIUS accounting messages for usage enforcement**: Boolean ('t' or 'f').
   - **Support RADIUS Disconnect messages**: Boolean ('t' or 'f').
   - **Policy**: Name of a RADIUS policy (optional).
     For example:
   - **Unique IP and policy**: `myclient,1.2.3.4,secret123,f,f,mypolicy`
   - **Subnet and no policy**: `myclients,1.2.4.0/24,secret123,t,t,`
   - **IP range and policy**: `myotherclients,1.2.5.10-1.2.5.19,secret123,t,f,mypolicy`
3. Click **Save**.

Policies

RADIUS policy configuration is available in **Authentication > RADIUS Service > Policies**.

FortiAuthenticator RADIUS authentication requires that RADIUS clients are assigned one or more policies. Policies can be created for Password/OTP, MAC authentication bypass (MAB), and EAP-TLS authentication.

To distinguish authentication requirements for clients, RADIUS attributes can be added to policies to indicate the type of service the user has requested or the type of service that is provided. Each policy can contain up to two RADIUS attributes.

When FortiAuthenticator receives a RADIUS authentication request, it first has to determine which policy it will use to process the request.

The selected policy will match the following characteristics of the RADIUS authentication request:

1. RADIUS client corresponding to the source IP address of the request must be included in the policy.*
2. If policy is configured with RADIUS attribute criteria, it must match with the RADIUS attributes in the request.
3. Authentication type in the request must match the authentication type of the policy (MAB, EAP-TLS, password/OTP).

If FortiAuthenticator does not find a policy that meets all three conditions, it automatically returns an authentication failure response.

If the request matches more than one policy, FortiAuthenticator selects the policy closest to the top of the list.

Policy priority can be reordered by selecting the up and down icons next to each policy in the list.

To configure a RADIUS policy:

1. Go to **Authentication > RADIUS Service > Policies**, and click **Create New** to add a new RADIUS policy. The **RADIUS Policy Creation Wizard** is launched.
2. Configure the RADIUS policy:

Displayed configuration settings vary depending on the *Authentication type* selected. The list below contains all possible settings, but only settings that are applicable to your configuration are shown in the GUI.

RADIUS clients	The policy name, description, and clients.
Policy name	Enter a name to identify the RADIUS policy.
Description	Optionally, provide a description of the policy.
RADIUS clients	Choose the clients to which this policy applies. For more information, see Clients on page 190.
RADIUS attribute criteria	The attributes that must be present in the RADIUS authentication request in order to be processed by this policy.
RADIUS authentication request must contain specific attributes	When enabled, RADIUS authentication requests must contain specific attributes from the FortiAuthenticator's list of vendors, viewable at **Authentication > RADIUS Service > Dictionaries**.
Authentication type	The type of end-user authentication used by this policy.
Password/OTP authentication	Configure password or one-time password authentication on selected realms. When **Accept EAP** is enabled, password/OTP authentication can be configured to accept EAP, including **PEAP**, **EAP-TTLS**, **EAP-GTC**, and **EAP-MSCHAPv2**.  EAP settings are only relevant for the EAP sessions terminated by FortiAuthenticator and not for the EAP sessions proxied to the remote RADIUS servers.

	MAC authentication bypass (MAB)	Configure MAC authentication bypass (MAB) for certain devices, provided their MAC addresses appear in the User-Name, User-Password, and Calling-Station-ID attributes.
	Client Certificates (EAP-TLS)	Configure client certificates (EAP-TLS) to verify the certificate provided by the end-user. A certificate is deemed valid if **ALL** of the following conditions match the certificate binding settings of one of the configured local or remote users: • End-user certificate "Subject" has a CN value AND that value matches the "Common name" certificate binding setting of one of the configured local or remote users. • End-user certificate "Issuer" matches the "CA" certificate binding setting of that same configured user account. • End-user certificate is properly signed. • End-user certificate is **NOT** expired. For example, if an end-user provides a certificate with the following fields: • Subject: `CN=SAM, OU=Sales, DC=Company, DC=com` • Issuer: `CN=MyCA, OU=IT, DC=Company, DC=com` • Properly signed and not expired. This certificate would be deemed valid if it matches a configured user account with the following certificate binding settings: • Common name: `Sam` • CA: `CN=MyCA, OU=IT, DC=Company, DC=com`
Identity source		The identity sources against which to authenticate end-users. Identity source settings vary depending on the authentication type selected.
	Authentication mode	Select from the following two options: • **Certificate bindings:** Legacy mode that uses certificate bindings. • **Trusted CA(s):** Accepts all the valid client certificates signed by one of the trusted CAs. This allows FortiAuthenticator to successfully authenticate any endpoint presenting a valid client certificate signed by one of the trusted CA certificates. When the **Authentication mode** is set as **Trusted CA(s)**, the RADIUS daemon ignores any configured certificate bindings and only verifies that the client certificate is: • Signed by one of the trusted CAs • Not expired • Not revoked (if CRL is configured) **Note**: This option is only available when the **Authentication type** is **Client Certificates (EAP-TLS)**.
	Eduroam	Enable to force settings to the values required in an eduroam environment.

	Note: The option is only available when the **Authentication mode** is **Certificate bindings**.
Username format	Select one of the following three username input formats: • **username@realm** • **realm\username** • **realm/username** These settings are only displayed for **Password/OTP** and **EAP-TLS** authentication. **Note**: The option is only available when the **Authentication mode** is **Certificate bindings**.
Use default realm when user-provided realm is different from all configured realms	When enabled, FortiAuthenticator selects the default realm for authentication when the user-specified realm is different from all configured realms. **Note**: The option is only available when the **Authentication mode** is **Certificate bindings**.
Realms	Add realms to which the client will be associated. • Select a realm from the dropdown menu in the **Realm** column. • Select whether or not to allow local users to override remote users for the selected realm. • Select whether or not to use Windows AD domain authentication. See Windows AD domain authentication on page 199. For RADIUS policies with **Use Windows AD Domain Authentication** enabled, Windows Server 2008 is not supported. • Edit the group filter as needed to filter users based on the groups they are in. • If necessary, add more realms to the list. • Select the realm that will be the default realm for this client. These settings are only displayed for **Password/OTP** and **EAP-TLS** authentication. When editing group filters for remote RADIUS realms, you can enable **Allow remote LDAP groups** to allow the selection of remote LDAP groups. **Note**: The option is only available when the **Authentication mode** is **Certificate bindings**. The **Realms** table can now include SAML realms and remote SAML group filters.
Require Call-Check attribute for MAC-based authentication	Optionally, you can require the Call-Check attribute for MAC-based authentication. **Notes**: • The option is disabled by default.

		• The option is only displayed when the **Authentication type** is **MAC authentication bypass (MAB)**.
	Authorized groups	From the dropdown, select authorized MAC devices groups. If a MAC device is a member of one of the authorized MAC groups, FortiAuthenticator accepts MAB authentication requests for the device. **Note**: The option is only displayed when the **Authentication type** is **MAC authentication bypass (MAB)**.
	Blocked groups	From the dropdown, select blocked MAC devices groups. If a MAC device is a member of one of the blocked MAC groups, FortiAuthenticator rejects the MAB authetication requests for the device. **Note**: The option is only displayed when the **Authentication type** is **MAC authentication bypass (MAB)**.
	Local CA certificates	From the dropdown, select local CA certificates. **Note**: The option is only available when the **Authentication mode** is **Trusted CA(s)**.
	Trusted CA certificates	From the dropdown, select trusted CA certificates. **Note**: The option is only available when the **Authentication mode** is **Trusted CA(s)**.
Authentication factors		The authentication factors to verify. Authentication factor settings are only displayed for **Password/OTP** and **EAP-TLS** authentication types.
	Authentication Methods	Select one of the following: • **Mandatory password and OTP**: Two-factor authentication is required for every user. • **All configured password and OTP factors**: Two-factor authentication is required if it is enabled on the user's account, otherwise, allow one-factor authentication. • **Password-only**: Authenticate users through password verification only. User accounts for which password authentication is disabled cannot be authenticated. • **OTP-only**: Authenticate users through token verification only. User accounts for which token authentication is disabled cannot be authenticated.
	Adaptive Authentication	Enable this option if you would like to have certain users bypass the OTP validation, so long as they belong to a trusted subnet. Select **All trusted subnets** to add all the available trusted subnets. You can specify the trusted subnets by selecting **Specify trusted subnets** and clicking the pen icon. This opens a window where you can choose from a list of available trusted subnets.

Adaptive Authentication is available only for the following authentication types:

- **Mandatory password and OTP**
- **All configured password and OTP factors**

Device authorization	When the **Authentication type** is **Password/OTP authentication**, and: • **Verify MAC address in CN of client certificate** is enabled, the endpoint MAC address sent by the RADIUS client must match the `CN` in the subject field of the client certificate (default = disabled). • **Verify MAC address in authentication requests** is enabled, you can add MAC devices groups to the **Authorized groups** field. Only the MAC devices that are members of at least one of the MAC devices groups are authorized to proceed with authentication. If the MAC device is a member of an authorized MAC devices group, FortiAuthenticator validates the authentication request. If the MAC device is not a member of an authorized MAC devices group, FortiAuthenticator rejects the request.
Advanced Options	
Allow FortiToken Mobile push notifications	Enable this setting to allow FortiToken Mobile push notifications for RADIUS users. This setting is controlled on a per RADIUS client basis, not for specific users. **Trigger push without RADIUS challenge (warning: NOT recommended if using with FortiGate RADIUS clients)**: When enabled, FortiAuthenticator triggers the FortiToken Mobile push notification once the password is verified without requiring the end-user to respond "push" to a RADIUS challenge. **Limitations**: • Entering OTP manually is only possible by concatenating the password and OTP in the initial credential submissions. • Suppose the end-user forgets to

		concatenate the OTP in the original credentials submission, or the push notification does not reach the FortiToken Mobile. In that case, the end-user must wait 30 seconds to up to a few minutes before receiving the authentication failure message. **Note**: The option is disabled by default.
	Application name for FTM push notification	Enter the client application name. This field is displayed on the FortiToken app. When creating a new policy or upgrading to FortiAuthenticator 8.0, the policy name is the default client application name.
	Resolve user geolocation from their IP address	Enable to resolve the user geolocation from their IP address (if possible).
	Reject usernames containing uppercase letters	Enable this setting to reject usernames that contain uppercase letters.
	Allow OTP for EAP-MSCHAPv2 Authentication with Forticlient	Enable this setting to allow OTP for EAP-MSCHAPv2 authentication with FortiClient. **Note**: The option is only available when the **Authentication type** is **Password/OTP authentication** with **Accept EAP > EAP-MSCHAPv2** enabled.
RADIUS response	The content of the RADIUS authentication response based on the outcome of the authentication. When the **AD Computer Authentication Result** is successful and the user is not authenticated yet, you can select between the following RADIUS attribute response options: • **Return User Group Attributes**: Returns RADIUS attributes configured in the user groups that the computer is a member of. • **Return Additional Attributes**.	

By default, **Return User Group Attributes** is disabled and **Return Additional Attributes** is available.

If **Return User Group Attributes** is enabled then **Return Additional Attributes** becomes unavailable.

For EAP-TLS RADIUS policies with **Authentication mode** set as **Trusted CA(s)**, since FortiAuthenticator does not match the authenticating endpoints with a user account, FortiAuthenticator cannot use RADIUS attributes specified in user accounts or user groups to return in the RADIUS **Accept-Accept** response. The EAP-TLS RADIUS policy allows specifying a set of RADIUS attributes to be included in all **Accept-Accept** responses.

When the **Authentication mode** is **Trusted CA(s)**, the **RADIUS response** tab includes a new **Additional Attributes** pane. In the **Additional Attributes** pane, you can add RADIUS attributes to be included with the **Accept-Accept** response.

The **Additional Attributes** pane is similar to the **Additional Attributes For MAC Authentication Bypass** pane available in the **RADIUS response** tab when the **Authentication type** is **MAC authentication bypass (MAB)**.

For **Authentication type** set as **MAC authentication bypass (MAB)** and given that the MAC device is not a member of either the **Authorized groups** or **Blocked groups** set up in the **Identity sources** tab, FortiAuthenticator accepts or rejects the MAB authentication requests depending on the response that you have set up for **Unauthorized** setting in the **RADIUS response** tab.

The following two options are available:

- **Access-Accept**
- **Access-Reject**

3. Select **Save** to add the new RADIUS policy.

Windows AD domain authentication

Windows AD domain authentication can be enabled to allow for PEAP-MSCHAPv2 (802.1x) over RADIUS.

When enabled, authentication is performed using NTLM once the FortiAuthenticator has joined the AD domain, replacing the default LDAP authentication process. The ports used with Windows AD domain authentication are TCP/88, 135, 139, and 445.

When determining which LDAP server to authenticate users against, the domain provides a list of domain controllers, and FortiAuthenticator cycles round-robin through them when joining the domain instead of using the primary/secondary IP/FQDN from the remote LDAP server settings. Enabling **Preferred Domain Controller Hostname** will limit the round-robin activity to the DCs specified by this setting.

* If some RADIUS clients are configured with overlapping IP addresses, subnets and/or ranges, FortiAuthenticator selects the RADIUS client with the narrowest IP address, subnet or range containing the source IP address of the request.

General

FortiAuthenticator supports RADSEC and several IEEE 802.1X Extensible Authentication Protocol (EAP) methods, configurable from **Authentication > RADIUS Service > General**. For more information about EAP, see Extensible Authentication Protocol on page 242.

You can specify the following certificate information:

Max Fragment Size for EAP-TLS	The RADIUS server is configured with a maximum fragment size. Enter the maximum fragment size for EAP-TLS (default = 1024). The setting allows the administrator to adjust the RADIUS server maximum fragment size. **Note**: The Framed-MTU size in EAP-TLS is negotiated between the server and the client.
Server Settings	
EAP Server Certificate	Specify the server certificate to be used with Extensible Authentication Protocol (EAP) methods.
RADSEC Server Certificate	Specify the server certificate to be used with RADSEC RADIUS requests.
EAP-TLS Authentication	
Local CAs	Specify the local CA.
Trusted CAs	Specify trusted CAs.

FortiAuthenticator does not support wildcard certificates for EAP server.

RADSEC support

When using RADSEC, the certificate used to encrypt the TLS traffic between FortiAuthenticator and the RADSEC client must be configured in the **Radsec Server Certificate** field. Certificates can be created locally or imported to FortiAuthenticator.

When a RADSEC client connects to FortiAuthenticator through TLS on the specified port, they must provide a valid client certificate signed by one of the configured Local or Trusted CAs. After being decrypted out the TLS tunnel, the RADIUS authentication/accounting requests are handled by the FortiAuthenticator RADIUS daemon like standard RADIUS requests via UDP. The maximum number of simultaneous RADSEC clients supported is **500**.

The default RADSEC port is **2083** and can be configured in **Authentication > RADIUS Service > Services**.

See Services on page 201

Services

You can optionally change the RADIUS authentication, accounting SSO, and accounting monitor ports under **Authentication > RADIUS Service > Services**.

By default, the ports are set to:

- **RADIUS authentication port**: 1812
- **RADIUS accounting SSO port**: 1813
- **RADIUS accounting monitor port**: 1646
- **RADSEC port**: 2083

When upgrading from a firmware version prior to 5.0, and the **Enable RADIUS Accounting SSO clients** option is enabled under **Fortinet SSO Methods > SSO > General**, both the SSO accounting port and the usage monitoring accounting port should remain at their default values (1813 and 1646 respectively) in order to avoid service disruption.

Custom dictionaries

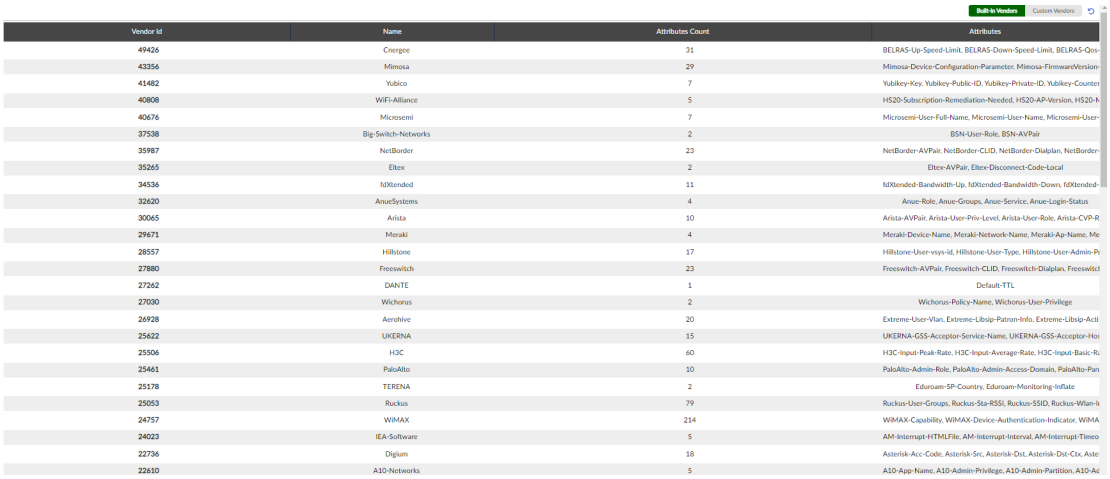
The custom dictionary list enables you to view built-in vendors and their RADIUS attributes, and create new customized entries.

Go to **Authentication > RADIUS Service > Dictionaries** to view the list.

Some services can receive information about an authenticated user through RADIUS vendor-specific attributes. FortiAuthenticator user groups and user accounts can include RADIUS attributes for Fortinet and other vendors.

Attributes in user accounts can specify user-related information. For example, the **Default** attribute **Framed-IP-Address** specifies the VPN tunnel IP address sent to the user by the Fortinet SSL VPN.

Attributes in user groups can specify more general information, applicable to the whole group. For example, specifying third-party vendor attributes to a switch could enable administrative level login to all members of the **Network_Admins** group, or authorize the user to the correct privilege level on the system.



To create a new custom RADIUS attribute vendor, open the **Custom Vendors** view and select **Create New** where you are prompted to upload a RADIUS dictionary file.

To add RADIUS attributes to a user or group:

1. Go to **Authentication > User Management > Local Users** and select a user account to edit, or go to **Authentication > User Management > User Groups** and select a group to edit.
2. In the **RADIUS Attributes** section, select **Add RADIUS Attribute**.
3. Select the appropriate **Vendor** and **Attribute ID**, then enter the attribute's value in the **Value** field.
4. Select **Save** to add the new attribute to the user or group.
5. Repeat the above steps to add additional attributes as needed.

Accounting proxy

The FortiAuthenticator receives RADIUS accounting packets from a carrier RADIUS server, transforms them, and forwards them to multiple FortiGate or FortiMail devices for use in RADIUS Single Sign-On (RSSO). This differs from the packet use of RADIUS accounting (RADIUS accounting on page 262).

The accounting proxy needs to know:

- the rule sets to define or derive the RADIUS attributes that the FortiGate unit requires,
- the source of the RADIUS accounting records (i.e. the RADIUS server),
- and the destination(s) of the accounting records (i.e. the FortiGate units using this information for RSSO authentication).

General

General RADIUS accounting proxy settings can be configured by going to **Authentication > RADIUS Service > Accounting Proxy** and select **General**.

The following settings are available:

Log level	Select **Error**, **Warning**, **Info**, or **Debug** as the minimum event severity level to log from the dropdown menu. The default is **Error**.
Group cache lifetime	Enter the amount of time after which user group memberships will expire in the cache, from 1-10080 minutes (maximum of one week). The default is **480**.
Number of proxy retries	Enter the number of times to retry proxy requests if they timeout, from 0-3 retries, where 0 disables retries. The default is **3**.
Proxy retry timeout	Enter the retry timeout period of a proxy request, from 1-10 seconds. The default is **5**.
Statistics update period	Enter the time between statistics updates to the seconds debug log, from 1-3600 seconds (maximum of one hour). The default is **5**.

Select **Save** to apply your changes.

Rule sets

A rule set can contain multiple rules. Each rule can do one of the following:

- Add an attribute with a fixed value.
- Add an attribute retrieved from a user's record on an LDAP server.
- Rename an attribute to make it acceptable to the accounting proxy destination.

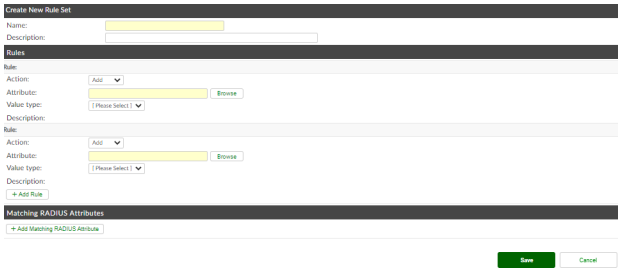
FortiAuthenticator can store up to 25 rule sets. You can provide both a name and description to rule sets to help identify each rule set and their purpose.

Rules access RADIUS attributes of which there are both standard attributes and vendor-specific attributes (VSAs). To select a standard attribute, select the default vendor. See RADIUS attributes on page 137.

To view the accounting proxy rule set list, go to **Authentication > RADIUS Service > Accounting Proxy** and select **Rule Sets**.

To add RADIUS accounting proxy rule sets:

1. From the rule set list, select **Create New**. The **Create New Rule Set** window opens.



2. Enter the following information:

Name	Enter a name to use when selecting this rule set for an accounting proxy destination.
Description	Optionally, enter a brief description of the rule's purpose.
Rules	Enter one or more rules.
Action	The action for each rule can be either **Add** or **Modify**. • **Add**: Add either a static value or a value derived from an LDAP server. • **Modify**: Rename an attribute.
Attribute	Select **Browse** and choose the appropriate **Vendor** and **Attribute ID** in the **Select a RADIUS Attribute** dialog box. If the field is empty, no filtering is applied.
Attribute 2	If **Action** is set to **Modify**, a second attribute may be selected. The first

		attribute is renamed to the second attribute.
	Value type	If the action is set to **Add**, select a value type from the dropdown menu. • **Static value**: Adds the attribute in the **Attribute** field containing the static value in the **Value** field. • **Group names**: Adds attribute in the **Attribute** field containing "Group names" from the group membership of the **Username Attribute** on the remote LDAP server.
	Value	If the action is set to **Add** and **Value Type** is set to **Static value**, enter the static value.
	Username attribute	If the action is set to **Add,** and **Value Type** is not set to **Static value**, specify an attribute that provides the user's name, or select **Browse** and choose the appropriate Vendor and Attribute ID in the **Select a RADIUS Attribute** dialog box.
	Remote LDAP	If the attribute addition requires an LDAP server, select one from the dropdown menu. See LDAP on page 176 for information on remote LDAP servers.
	Description	A brief description of the rule is provided.
	Add Rule	Select to add another rule to the rule set.
Matching RADIUS Attributes		Controls which RADIUS accounting requests are proxied. Select to add a RADIUS attribute.
	Not	Enable to filter out non-proxied users. **Note**: The option is disabled by default.
	Vendor	From the dropdown, select a vendor.
	Attribute ID	From the dropdown, select an attribute ID.
	Value	Enter the attribute value.
	Allow substring match	Enable to allow substring match. **Note**: The option is disabled by default and only available for some attribute IDs.
	Type	Displays the attribute type. **Note**: The option is noneditable.
	Add Matching RADIUS Attributes	Select to add another RADIUS attribute to the rule set.

3. Select **Save** to create the new rule set.

Example rule set

The incoming accounting packets contain the following fields:

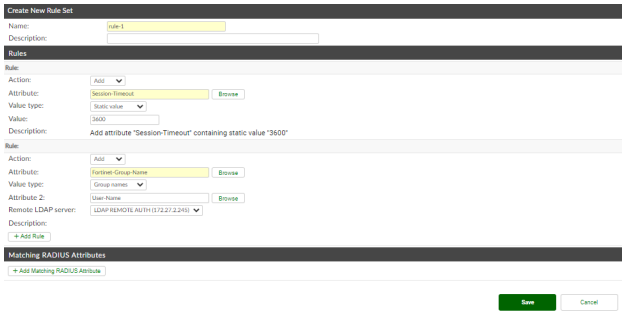
- User-Name
- NAS-IP-Address

- Fortinet-Client-IP-Address

The outgoing accounting packets need to have these fields:

- User-Name
- NAS-IP-Address
- Fortinet-Client-IP-Address
- Session-Timeout: Value is always 3600
- Fortinet-Group-Name: Value is obtained from user's group membership on remote LDAP

The rule set needs two rules to add Session-Timeout and Fortinet-Group-Name. The following image provides an example:



Sources

The RADIUS accounting proxy sources list can be viewed in **Authentication > RADIUS Service > Accounting Proxy** and select **Proxy Sources**. Sources can be added, edited, and deleted as needed. A maximum of 500 proxy sources can be configured.

To add a RADIUS accounting proxy source:

1. From the source list, select **Create New**. The **Create New RADIUS Accounting Proxy Source** window opens.
2. Enter the following information:

Name	Enter the name of the RADIUS server. This is used in FortiAuthenticator configurations.
Source name/IP	Enter the FQDN or IP address of the server.
Secret	Enter the pre-shared secret required to access the server.
Description	Optionally, enter a description of the source.

3. Select **Save** to add the RADIUS accounting proxy source.

Destinations

The destination of the RADIUS accounting records is the FortiGate unit that will use the records to identify users. When defining the destination, you also specify the source of the records (a RADIUS client already defined as a source) and the rule set to apply to the records.

To view the RADIUS accounting proxy destinations list, go to **Authentication > RADIUS Service > Accounting Proxy** and select **Destinations**. A maximum of 500 proxy destinations can be configured.

To add a RADIUS accounting proxy destinations:

1. From the destinations list, select **Create New**. The **Create New RADIUS Accounting Proxy Destination** window opens.
2. Enter the following information:

Name	Enter a name to identify the destination device in your configuration.
Destination name/IP	Enter The FQDN or IP address of the FortiGate that will receive the RADIUS accounting records.
Secret	Enter the pre-shared key of the destination.
Source	Select a RADIUS client defined as a source from the dropdown menu. See Sources on page 205.
Rule set	Select an appropriate rule set from the dropdown menu or select **Create New** to create a new rule set.

3. Select **Save** to add the RADIUS accounting proxy destination.

TACACS+ service

Before FortiAuthenticator can accept TACACS+ authentication requests from a client, the device must be registered on FortiAuthenticator, and it must be assigned to a policy. TACACS+ authorization can be specified by creating authorization rules that can be applied to users and user groups in FortiAuthenticator.

The TACACS+ service can be enabled or disabled on each FortiAuthenticator network interface individually. Before you configure the TACACS+ service for use, confirm that it is enabled on the desired FortiAuthenticator network interface(s).

TACACS+ logs are viewable from the debug logs page.

To view the logs, go to (`https://<FAC IP>/debug/`), and select **TACACS+** from the **Service** dropdown.

TACACS+ authentication on FortiAuthenticator does not currently support challenge/response, which means:

- Two-factor authentication is only supported by appending the token to the password during login. For example, where the password is `Fortinet` and the token PIN is `123456`, the password entered by the user will be `Fortinet123456`.
- Having end-users change their password during login is not supported.

Creating policies

TACACS+ policy configuration is available under **Authentication > TACACS+ Service > Policies**.

FortiAuthenticator TACACS+ authentication requires that a TACACS+ client is assigned one or more policies. Policies determine the authentication method, identity source, and TACACS+ response for the clients assigned to the policy.

To create a TACACS+ policy:

1. Go to **Authentication > TACACS+ Service > Policies**, and click **Create New**.
   The **Create New TACACS+ Policy** Wizard opens.
2. Enter the following information:

TACACS+ clients		Specify the policy name and description. Specify all clients that this policy will accept TACACS+ requests from.
	Policy name	Enter a name for the policy.
	Description	Optionally, enter a description of the policy.
	TACACS+ clients	Lists the available TACACS+ clients. Select the client(s) to which this policy applies by using the arrows to move clients into the **Chosen TACACS+ Clients** box. For more information about creating TACACS+ clients, see Adding clients on page 208.
Identity source		Specify the identity sources against which to authenticate end-users.
	Username format	Select one of the following three username input formats: • **username@realm** • **realm\username** • **realm/username**
	Use default realm when user-provided realm is different from all configured realms	When enabled, FortiAuthenticator selects the default realm for authentication when the user-specified realm is different from all configured realms.
	Realms	Add the realms to which the client(s) will be associated. • Select a realm from the dropdown menu in the **Realm** column. • Select whether or not to allow local users to override remote users for the selected realm. • Select whether or not to use Windows AD domain authentication. • Edit the group filter as needed to filter users based on the groups they are in. • If necessary, add more realms to the list. • Select the realm that will be the default realm for this client.

Authentication factors	Specify which authentication factors to verify.
Authentication method	Select one of the following: • **Mandatory password and OTP**: Two-factor authentication is required for every user. • **All configured password and OTP factors**: Two-factor authentication is required if it is enabled on the user's account, otherwise, allow one-factor authentication. • **Password-only**: Authenticate users through password verification only. If password authentication is disabled on the user account, the account cannot be authenticated. • **OTP-only**: Authenticate users through token verification only. If token-based authentication is disabled on the user account, the account cannot be authenticated.
Adaptive Authentication	Enable this option if you would like to have certain users bypass OTP validation, so long as they belong to a trusted subnet. Select **All trusted subnets** to add all the available trusted subnets. You can specify the trusted subnets by selecting **Specify trusted subnets** and clicking the pen icon. This opens a window where you can choose from a list of available trusted subnets. **Adaptive Authentication** is available only for the following authentication types: • **Mandatory password and OTP** • **All configured password and OTP factors**
TACACS+ response	TACACS+ authentication response based on the outcome of the authentication.

3. Click **Save** to save the policy.

Adding clients

TACACS+ clients can be managed from **Authentication > TACACS+ Service > Clients**.

Clients can be added, imported, deleted, and edited as needed.

TACACS+ clients must use single-connection mode when using FortiAuthenticator for TACACS+ AAA.

Once created, clients can be assigned to a TACACS+ policy. See Creating policies on page 207.

To configure a TACACS+ client:

1. Go to **Authentication > TACACS+ Service > Clients**, and click **Create New** to add a new TACACS+ client. The **Create New TACACS+ Client** window opens.

2. Enter the following information:

Name	Input a name to identify the TACACS+ client.
Client address	Choose to specify the client address as an IP address or Subnet.
IP Address/Subnet	Enter the IP address or subnet of the client.  Subnets of up to 8 bits of network prefix (`/8`) are supported.
Secret	Enter the TACACS+ passphrase that is shared with the client.

3. Select **Save** to add the new TACACS+ client.

If authentication fails, check that the authentication client is configured and that its IP address is correctly specified. Common causes of authentication problems are:

- TACACS+ packets sent from an unexpected interface, or IP address.
- NAT performed between the authentication client and FortiAuthenticator.

TACACS+ on FortiAuthenticator supports the ASCII and PAP authentication types. Other authentication types supported by the TACACS+ protocol (CHAP and MSCHAPv2) will be denied.

When configuring TACACS+ settings on a client, for example FortiGate, the ASCII authentication type must be selected.

To import TACACS+ clients:

1. Go to **Authentication > TACACS+ Service > Clients**, and click **Import**.
   The **Import TACACS+ Clients** window opens.
2. Click **Upload a file** and choose the file location of the CSV file containing your TACACS+ client list.
   Each line of the CSV file must contain values in the following format:
   - **Name**: String.
   - **Address**: IP address or subnet.
   - **Secret**: String.
   - **Policy**: Name of a TACACS+ policy (optional).

   For example:
   - **Unique IP and policy**: `myclient,1.2.3.4,secret123,mypolicy`
   - **Subnet and no policy**: `myclients,1.2.3.0/24,secret123,`
3. Click **Import**.

Creating authorization rules

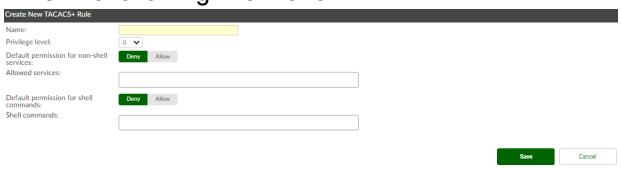
TACACS+ authorization can be managed from **Authentication > TACACS+ Service > Authorization**. In the TACACS+ **Authorization** menu, you can configure **Rules**, non-shell **Services**, and **Shell Commands**. Authorization rules can be specified within user groups or on individual user accounts. See Assigning authorization rules on page 212.

After successful authentication, FortiAuthenticator creates an authorization session for the user that lasts 28,800 seconds (8 hours). Any changes made to authorization rule configurations during that time will not apply to the user until the 8 hour session has expired.

To configure the maximum time duration (in seconds) for which an authenticated TACACS+ user is authorized to issue commands, go to **Authentication > User Account Policies > General**, and enter a value between 120 - 36,000 for **Session duration of authenticated TACACS+ user**.

To create an authorization rule:

1. Go to **Authentication > TACACS+ Service > Authorization**, select **Rules**, and click **Create New**. The **Create New TACACS+ Rule** window opens.
2. Enter the following information:



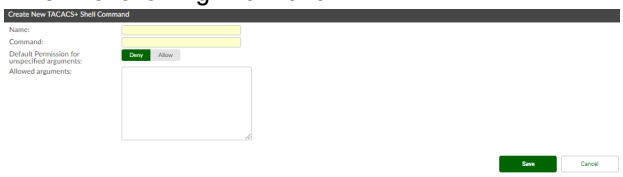
Name	Enter a name for the authorization rule.
Privilege level	Determines the access level users have before they are required to enter an enable password. The privilege level can be set in the range of 0 and 15. Currently, escalation/elevation of privileges using the enable mode is not supported.
Default permission for non-shell services	Set the permissions for non-shell services. Non-shell services cannot be specified and are only supported as **Allow** all or **Deny** all.
Allowed services	Specify the list of allowed services. See Services.
Default permission for shell commands	Set the permissions for shell commands not explicitly specified under **Allowed shell commands**.
Shell commands	Select the configured shell commands to include in this authorization rule.

3. Click **Save** to save the authorization rule.

To create a shell command:

1. Go to **Authentication > TACACS+ Service > Authorization**, select **Shell commands**, and click **Create New**. The **Create New TACACS+ Shell Command** window opens.

2. Enter the following information:



Name	Enter a name for the shell command.
Command	Enter the shell command.
Default permission for unspecified arguments	Set the permission for command arguments not explicitly specified under **Allowed/Denied arguments**.
Allowed arguments/Denied arguments	Specify all sets of arguments to be allowed or denied. One set of arguments can be provided per line, and curly braces are not permitted.

3. Select **Save** to save the shell command.

To create a non-shell service:

1. Go to **Authentication > TACACS+ Service > Authorization**, select **Services**, and click **Create New**. The **Edit TACACS+ Service** window opens.
2. Enter the following information:

Name	Enter a name for the non-shell service.
Service	Enter the service. The service string can only contain ASCII characters in the 0x20-0x7E range, except '@' and '/'.
Default permission for attributes	**Allow**: Attributes *not* listed in this service are *allowed*. These attributes are copied unchanged from the authorization request into the authorization response. **Deny**: Attributes *not* listed in this service are *denied*. If the TACACS+ client marked the denied attribute as mandatory, the authorization response is fail. If marked as optional, the attribute is removed from the authorization response.
Tacacs Service Attribute-Value Pairs	Select **Add Tacacs Service Attribute-value Pair**, enter an attribute and value, and select if the attribute-value pair is mandatory or optional. Repeat the above to add additional attributes as needed.

3. Click **Save** to save the non-shell service.
4. Once the non-shell service has been created, you can then edit it to add, edit, or remove attribute-value pairs. To create a new attribute-value pair, click **Add Tacacs Service Attribute-Value Pairs** in the **Tacacs Service Attribute-Value Pairs** pane and configure the following information:

Attribute-value Pairs	Specify the attribute, value, and restriction for this service. The available options for the restriction setting include:

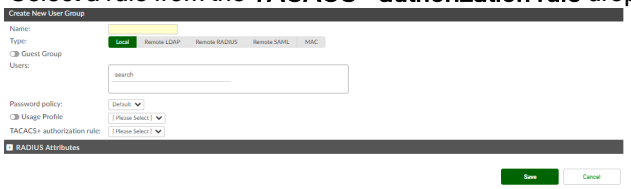
- **Mandatory**: Requires that the receiving side understands the attribute and will act on it. If the client receives a mandatory argument that it cannot oblige or does not understand, it must consider the authorization to have failed.
- **Optional**: May be disregarded by the client.

Assigning authorization rules

Authorization rules can be specified within user groups or on individual user accounts. If the user is member of multiple groups, the FortiAuthenticator arbitrarily chooses one of the TACACS+ authorization rules from one of the groups. When a TACACS+ authorization rule is specified on a user's account, it will override rules from any group for which the user is a member.

To configure TACACS+ authorization rules in user groups:

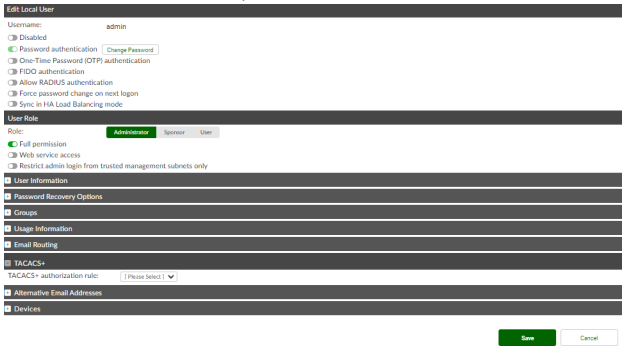
1. Go to **Authentication > User Management > User Groups**.
2. Create a new user group or edit an existing one.
3. Select a rule from the **TACACS+ authorization rule** dropdown



4. Click **Save**.

To configure TACACS+ authorization rules on individual users:

1. Go to **Authentication > User Management > Local Users**.
2. Create a new user or edit an existing one.
3. Under the **TACACS+**, select a rule from the **TACACS+ authorization rule** dropdown.



4. Click **Save**.

LDAP service

LDAP is an Internet protocol used to maintain authentication data that may include departments, people, groups of people, passwords, email addresses, and printers. LDAP consists of a data-representation scheme, a set of defined operations, and a request/response network.

In the LDAP protocol there are a number of operations a client can request such as search, compare, and add or delete an entry. Binding is the operation where the LDAP server authenticates the user. If the user is successfully authenticated, binding allows the user access to the LDAP server based on the user's permissions.

rfc822MailMember attribute

For users, the `rfc822MailMember` attribute lists the alternative email addresses configured for the local user.
For user groups, the `rfc822MailMember` attribute records the values of all unique email addresses (not including alternative email addresses) associated with users belonging to that group. In Windows AD, this is mapped by the `memberOf` attribute.
Email addresses and alternative email addresses can be configured for the local user settings in *Authentication > User Management > Local Users*.

General

To configure general LDAP service settings, go to **Authentication > LDAP Service > General**.

LDAP Server Settings	
LDAP server certificate	Select the certificate that the LDAP server will present from the dropdown menu.
LDAP User Auto Provisioning	
Auto provision users into LDAP from following sources	Enable **Auto provision users into LDAP from following sources** and specify how users can be automatically provisioned into LDAP using the following options: • **GUI (Manually created local users)** • **GUI (Imported local users)** • **Self-registration** • **API** **Note**: The API option also includes local users imported through the REST API CSV import.
Provision users into the following container	From the dropdown, select a container where the users are provisioned.

Auto provision local groups from following sources	Enable **Auto provision local groups from following sources** and specify how local groups can be automatically provisioned from the following sources: • **GUI (Imported local users)** • **API (Imported local users)** **Note**: These are new groups created when importing local users using a CSV file.
Provision users into the following container	From the dropdown, select a container where the users are provisioned.

Select **Save** to apply any changes that you have made.

Directory tree overview

The LDAP tree defines the hierarchical organization of user account entries in the LDAP database. The FortiGate unit requesting authentication must be configured to address its request to the right part of the hierarchy.

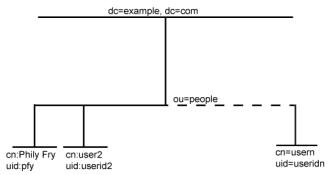
An LDAP server's hierarchy often reflects the hierarchy of the organization it serves. The root represents the organization itself, usually defined as Domain Component (DC), a DNS domain, such as `example.com` (as the name contains a dot, it is written as two parts separated by a comma: `dc=example,dc=com`). Additional levels of hierarchy can be added as needed; these include:

- Country (c)
- User Group (cn)
- Local User (uid)
- Organization (o)
- Organizational Unit (ou)

The user account entries relevant to user authentication will have element names such as UID or CN; the user's name. They can each be placed at their appropriate place in the hierarchy.

Complex LDAP hierarchies are more common in large organizations where users in different locations and departments have different access rights. For basic authenticated access to your office network or the Internet, a much simpler LDAP hierarchy is adequate.

The following is a simple example of an LDAP hierarchy in which the all user account entries reside at the OU level, just below DC.



When requesting authentication, an LDAP client, such as a FortiGate unit, must specify the part of the hierarchy where the user account record can be found. This is called the distinguished name (DN). In the above example, DN is `ou=People,dc=example,dc=com`.

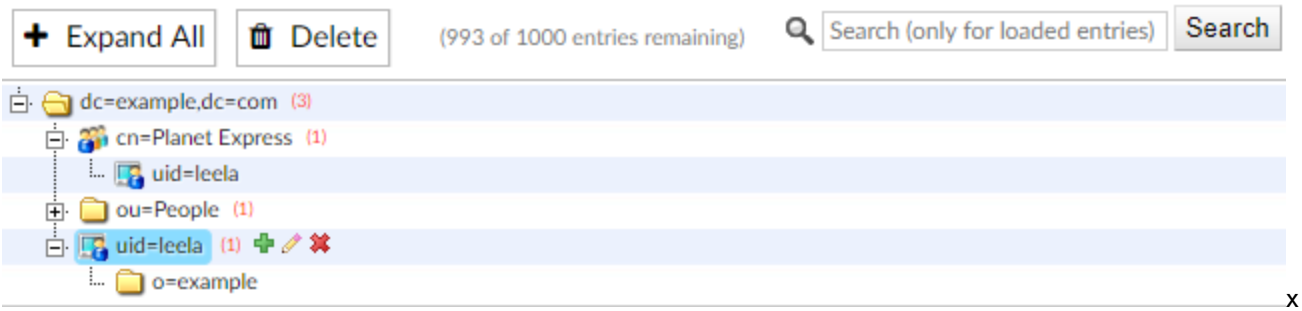
The authentication request must also specify the particular user account entry. Although this is often called the common name (CN), the identifier you use is not necessarily CN. On a computer network, it is appropriate to use UID, the person's user ID, as that is the information that they will provide at logon.

Creating the directory tree

The following sections provide a brief explanation of each part of the LDAP attribute directory, what is commonly used for representation, and how to configure it on FortiAuthenticator.

When an object name includes a space, as in **Test Users**, you have to enclose the text with double-quotes. For example:

`cn="TesTUsers",cn=Builtin,dc=get,dc=local`.



Editing the root node

The root node is the top level of the LDAP directory. There can be only one. All groups, OUs, and users branch off from the root node. Choose a DN that makes sense for your organization's root node.

There are three common forms of DN entries:

The most common consists of one or more DC elements making up the DN. Each part of the domain has its own DC entry. This comes directly from the DNS entry for the organization. For example, for example.com, the DN entry is `"dc=example,dc=com"`.

Another popular method is to use the company's Internet presence as the DN. This method uses the domain name as the DN. For example, for example.com, the DN entry would be `"o=example.com"`.

An older method is to use the company name with a country entry. For example, for Example Inc. operating in the United States, the DN would be `o="Example, Inc.",c=US`. This makes less sense for international companies.

When you configure FortiGate units to use FortiAuthenticator as an LDAP server, you will specify the distinguished name that you created here. This identifies the correct LDAP structure to reference.

To rename the root node:

1. Go to **Authentication > LDAP Service > Directory Tree**.
2. Select `dc=example,dc=com` to edit the entry.

3. In the **Distinguished Name (DN)** field, enter a new name (e.g. "`dc=fortinet,dc=com`").
4. Select **Save** to apply your changes.

If your domain name has multiple parts to it, such as shiny.widgets.example.com, each part of the domain should be entered as part of the DN, for example:

`dc=shiny,dc=widgets,dc=example,dc=com`

Adding nodes to the LDAP directory tree

You can add a subordinate node at any level in the hierarchy as required.

To add a node to the tree:

1. From the LDAP directory tree, select the green plus symbol next to the DN entry where you want to add the node. The **Create New LDAP Entry** window opens.
2. In the **Class** field, select the identifier to use.
   For example, to add the ou=People node from the earlier example, select Organizational Unit (ou).
3. Select the required value from the dropdown menu, or select **Create New** to create a new entry of the selected class.
4. Select **Save** to add the node.

Nodes can be edited after creation by selecting the edit, or pencil, icon next to the node name.

Adding user accounts to the LDAP tree

You must add user account entries at the appropriate place in the LDAP tree. These users must already be defined in the FortiAuthenticator user database. See Adding a user on page 97.

To add a user account to the tree:

1. From the LDAP directory tree, expand nodes as needed to find the required node, then select the node's green plus symbol.
   In the earlier example, you would do this on the `ou=People` node.
2. In the **Class** field, select **User (uid)**.
   The list of available users is displayed. You can choose to display them alphabetically by either user group or user.
3. Select the required users in the **Available Users** box and move them to the **Chosen Users** box. If you want to add all local users, select **Choose all** below the users box.
4. Select **Save** to add the user account to the tree.
   You can verify your users were added by expanding the node to see their UIDs listed below it.

Moving LDAP branches in the directory tree

At times you may want to rearrange the hierarchy of the LDAP structure. For example a department may be moved from one country to another.

While it is easy to move a branch in the LDAP tree, all systems that use this information will need to be updated to the new structure or they will not be able to authenticate users.

To move an LDAP branch:

1. From the LDAP directory tree, select **Expand All** and find the branch that you want to move.
2. Click and drag the branch from its current location to its new location
   When the branch is hovered above a valid location, an arrow appears to the left of the current branch to indicate where the new branch will be inserted. It will be inserted below the entry with the arrow.

Removing entries from the directory tree

Adding entries to the directory tree involves placing the attribute at the proper place. However, when removing entries it is possible to remove multiple branches at one time.

Take care not to remove more branches than you intend. Remember that all systems using this information will need to be updated to the new structure or they will not be able to authenticate users.

To remove an entry from the LDAP directory tree:

1. From the LDAP directory tree, select **Expand All** and find the branch that you want to remove.
2. Select the red X to the right of the entry name.
   You are prompted to confirm your deletion. Part of the prompt displays the message of all the entries that will be removed with this deletion. Ensure this is the level that you intend to delete.
3. Select **Yes, I'm sure** to delete the entry.
   If the deletion was successful there is a green check next to the successful message above the LDAP directory and the entry is removed from the tree.

Configuring a FortiGate unit for FortiAuthenticator LDAP

When you have defined the FortiAuthenticator LDAP tree, you can configure FortiGate units to access the FortiAuthenticator as an LDAP server and authenticate users.

To configure the FortiGate unit for LDAP authentication:

1. On the FortiGate unit, go to **User & Device > LDAP Servers** and select **Create New**.
2. Enter the following information:

Name	Enter a name to identify the FortiAuthenticator LDAP server on the FortiGate unit.
Server IP/Name	Enter the IP address FQDN of FortiAuthenticator.

Server Port	Leave at default (389).
Common Name Identifier	Enter `uid`, the user ID.
Distinguished Name	Enter the LDAP node where the user account entries can be found. For example, `ou=People,dc=example,dc=com`
Bind Type	The FortiGate unit can be configured to use one of three types of binding: • **Simple**: Bind using a simple password authentication without a search. • **Anonymous**: Bind using anonymous user search. • **Regular**: Bind using username/password and then search. You can use simple authentication if the user records all fall under one distinguished name (DN). If the users are under more than one DN, use the anonymous or regular type, which can search the entire LDAP database for the required username. If your LDAP server requires authentication to perform searches, use the regular type and provide the **Username** and **Password**.
Secure Connection	If you select **Secure Connection**, you must select LDAPS or STARTTLS protocol and the CA security certificate that verifies the FortiAuthenticator device's identity. If you select LDAPS protocol, the Server Port will change to 636.

3. Optionally, use the **Test Connectivity** and **Test User Credentials** features. Select **OK** to apply your settings.
4. Add the LDAP server to a user group. Specify that user group in identity-based security policies where you require authentication.

OAuth Service

FortiAuthenticator can act as an authorization server to issue and manage OAuth access tokens via a set of REST API endpoints. An OAuth client is issued an OAuth access token by FortiAuthenticator after successfully providing its login credentials. The OAuth client can then use this access token as proof of authorization to access a third-party service. The third-party service may contact FortiAuthenticator to validate any given OAuth access token.

To enable OAuth service access, enable the **OAuth Service (/api/v1/oauth, /api/v1/pushpoll, /guests, /portal)** service available when you enable **HTTPS (TCP/443)** on the applicable network interface(s) under **System > Network > Interfaces**. See Interfaces on page 41.

You can use OpenID Connect (OIDC) by configuring an authentication policy, authorization code, and OIDC claim(s) for participating clients. See Relying Party on page 219.

OIDC only works with remote users if their account has been imported to the FortiAuthenticator configuration.

General

To configure general OAuth settings, go to **Authentication > OAuth Service > General**.

User Login session lifetime	Determines the length of the user login session, in minutes (1 - 1440, default = 5).
Authorization code expiry	Determines the length of the authorization code expiration, in seconds (1 - 56000, default = 60).
Auto-generated client secret length	Determines the length of the generated client secret for confidential OAuth applications (16 - 256, default = 128).
JWT private key	Select the local certificate used to sign the JSON Web Token (JWT).
Restrict number of authentication requests to	Enter the maximum number of REST API requests sent (1 - 2880, default = 360) during a time period. The time period can be set in the **For duration** field, in minutes (1 - 480, default = 60).

Select **Save** to apply the changes you have made.

Relying Party

OAuth relying parties (RP), otherwise known as clients, can be managed from **Authentication > OAuth Service > Relying Party**. They correspond to the OAuth clients that have been issued credentials for requesting OAuth tokens from the FortiAuthenticator.

OpenID Connect (OIDC) authentication can be enabled for the relying party by configuring an authorization code, policy, redirect URI, and claim(s).

To configure an OAuth application:

1. From the OAuth relying party list, select **Create New** to add a new relying party.
   The **Create New Relying Party** window opens.
2. Enter the following information:

Name	Enter a name for the client.
Policy	Select a policy. OAuth policies are configured in **Authentication > OAuth Service > Policies**. See Policies on page 223.
Access token expiry	Enter a length of time for which OAuth access tokens issued by this application are valid. **Note**: The default is set to 36000 seconds (10 hours). **Note**: Access tokens will not expire if the value is set to `0`.
Refresh token expiry	The amount of time in days/weeks/months the refresh token issued is valid upon authorization (default = 1 day). **Note**: The refresh token never expires if the expiry period is configured as `0`.

	Note: FortiAuthenticator does not issue a new OAuth token using an expired refresh token.
Client type	Select the client type for the client: • **Confidential**: The relying party must provide a valid client ID, user credentials, and the client secret to obtain an OAuth token. • **Public**: The relying party must provide a valid client ID and user credential to obtain an OAuth token. Clients are not required to provide a client secret in requests to the OAuth application.

Authorization grant types	Select the authorization grant type:
	• **Password-based**: Authentication and authorization is API-based.
	• **Authorization code**: Authentication and authorization is initiated by the relying party, but the end-user provides their credentials through their browser on the FortiAuthenticator login portal.
	Selecting this setting allows for the configuration of OpenID Connect claims.
	This option is only available when the **Client type** is **Confidential**.
	• **Authorization code with PKCE**: When this grant type is selected, FortiAuthenticator applies the following modifications to the standard **Authorization code** grant type:
	  • The `client_secret` field is ignored in requests to the `/oauth/authorize/` endpoint.
	  • New `code_challenge_method` and `code_challenge` fields are required in requests to the `/oauth/authorize/` endpoint.
	  • A new `code_verifier` field is required in the requests to the `/oauth/token/` endpoint.
	  • FortiAuthenticator rejects requests to the `/oauth/token/` endpoint if the SHA256 digest for `code_verifier` does not match the `code_challenge` provided when the `code` was issued by the `/oauth/authorize/`endpoint.
	The option is only available when the **Client type** is **Public**.

Client ID	Enter a client ID. A generated value is provided by default.
Client secret	Enter a client secret. A generated value is provided by default. You can configure the length of the automatically generated value under **Authentication > OAuth Service > General**. This field is only available when the **Client type** is **Confidential**.
Authorized Successful Callback URLs	Enter the allowed uniform resource identifier (URI) for authorized successful callback that the OAuth service is authorized to redirect end-users to after authentication. Multiple entries can be separated by spaces. The field is only available when the **Authorization grant types** is **Authorization code** or **Authorization code with PKCE**. **Note**: Redirecting to `https` URL(s) is strongly recommended.

Authorized Logout Callback URLs	Enter the allowed uniform resource identifier (URI) for authorized logout callback that the OAuth service is authorized to redirect end-users to after authentication. Multiple entries can be separated by spaces. The field is only available when the **Authorization grant types** is **Authorization code** or **Authorization code with PKCE**. **Note**: Redirecting to `https` URL(s) is strongly recommended.
Relying Party Scopes	Add scopes for the relying party. See Scopes on page 222.
Claims	Add claims for the relying party. See Claims on page 221. This field is only available when the **Authorization grant type** is **Authorization code** or **Authorization code with PKCE**.

3. Select **Save** to create the new relying party.

Claims

You can configure relying parties to return claims about the authenticated end-user. Claims can be configured for relying parties using OIDC where the **Authorization grant type** is **Authorization code**.

To configure claims:

1. Create or edit an Oauth relying party with **Authorization grant types** set to **Authorization code**.
2. Under **Claims**, click **Add Claim**.
3. Configure the claim:

Scope	Select the claim scope.
Name	Enter the claim name.
User attribute	Select the user attribute from the following list: • **Username** • **First name** • **Last name** • **Email** • **Group** • **IAM account name** • **IAM account alias** • **IAM username**  Custom fields configured in **Authentication > User Account Policies > Custom User Fields** are available here.

4. Click **Save** to save the relying party or click **Add Claim** to create another claim before saving your changes.

Scopes

Scopes in **Authentication > OAuth Service** lists scopes authorized for relying parties.

A scope is a string with the following characteristics:

- 1 to 64 ASCII characters in length
- Case-sensitive
- Allowed characters are all printable ASCII characters (`0x21` to `0x7E`), except the double-quotes " (`0x22`) and the backslash \ (`0x5C`).

There are two types of scopes:

- **Default**: Scope is always assigned to the OAuth session, even if the relying party does not request it.
- **Optional**: Scope is only assigned to the OAuth session if the relying party explicitly requests it.

When forming a list of more than one scope, each scope is separated by a whitespace, e.g., `"read write"`.

A default `openid` scope is available.

To configure a scope:

1. From the Scopes list, select **Create New** to create a new OAuth scope.
   The **Create New OAuth Scope** window opens.
2. Enter the following information:

Name	The name of the scope. **Note**: The name appears in the `scope` parameter of the API endpoints.
Description	A string value.

3. Click **Save**.

To add a scope to a relying party:

1. When editing a relying party, select **Add Relying Party Scope** in the **Relying Party Scopes** pane.
2. From the **Scope** dropdown, select a scope.
3. In **Scope Type**, select either **Optional** or **Default**.

The default `openid` scope is already added and can be removed by clicking **x**.

The scopes included in the default and optional lists must be mutually exclusive, i.e., the same scope must not appear in both default and optional lists.

4. Click **Save** to save the relying party or click **Add Relying Party Scope** to create another scope before saving your changes.

Policies

OAuth policy configuration is available under **Authentication > OAuth > Policies**.

You can configure policies to be used in OAuth and OpenID Connect authentication to relying parties when the authorization grant type is **Authorization code**. See Relying Party on page 219.

To configure an OAuth policy:

1. Go to **Authentication > OAuth Service > Policies**, and click **Create New**.
   The OAuth Service wizard opens.
2. Configure the OAuth policy:
3.

Policy type	Select the name and login portal.
Name	Enter a name for the policy.
Description	Optionally, provide a description of the policy.
Portal	Select the portal to use with the policy. See Portals on page 143.
Identity sources	Select the identity sources.
Username format	Select one of the following three username input formats: • **username@realm** • **realm\username** • **realm/username**
Use default realm when user-provided realm is different from all configured realms	When enabled, FortiAuthenticator selects the default realm for authentication when the user-specified realm is different from all configured realms.
IAM login	Enable to allow IAM login. When IAM login is enabled: • The OAuth login page (**Login Page** replacement message) now offers **Sign-in as IAM user** link. • If the end-user clicks **Sign-in as IAM user**, the end-user is presented with an **OAuth IAM Login** form where they enter their credentials using the IAM account name/alias and the IAM username. The **OAuth IAM Login Page** is a new customizable replacement message. **Note**: The option is disabled by default.

	Realms	Add realms to which the client will be associated. • Select a realm from the dropdown menu in the **Realm** column. • Select whether or not to allow local users to override remote users for the selected realm. • Edit the group filter as needed to filter users based on the groups they are in. • If necessary, add more realms to the list. • Select the realm that will be the default realm for this client.
Authentication Factors		Select the authentication factors.
	Authentication Methods	Select one of the following: • **Mandatory password and OTP**: Two-factor authentication is required for every user. • **All configured password and OTP factors**: Two-factor authentication is required if it is enabled on the user's account, otherwise, allow one-factor authentication. • **Password-only**: Authenticate users through password verification only. User accounts for which password authentication is disabled cannot be authenticated. • **OTP-only**: Authenticate users through token verification only. User accounts for which token authentication is disabled cannot be authenticated.
	Adaptive MFA	Certain users can bypass the OTP verification, so long as they belong to a trusted subnet or they are a known device. See Adaptive MFA on page 233. This option is only available for **Mandatory password and OTP** and **All configured password and OTP factors** authentication methods.
	FIDO authentication (effective once a token has been registered)	Enable or disable FIDO authentication.
	Options	Select from the following two options: • **FIDO token only**: Log in with FIDO token only (without password). • **Password and FIDO token**: Log in with the password and the FIDO token.
	Allow two-factor authentication (password and OTP) if all FIDO keys have been revoked for the user account	Enable to allow two-factor authentication (password and OTP) if all FIDO keys have been revoked for the user account.

	Skip authorization consent form	Enable to skip the authorization consent form.	
	Advanced options		
		Allow FortiToken Mobile push notifications	Toggle to enable or disable FortiToken Mobile push notifications for RADIUS users.
		Application name for FTM push notification	Enter the client application name. This field is displayed on the FortiToken app. When creating a new policy or upgrading to FortiAuthenticator 6.4, the policy name is the default client application name.
		Resolve user geolocation from their IP address	Enable to resolve the user geolocation from their IP address (if possible).
		Reject usernames containing uppercase letters	Enable this setting to reject usernames that contain uppercase letters.

4. Select **Save and exit** to create the new policy.

Portals

The following section describes how to configure OAuth portals.

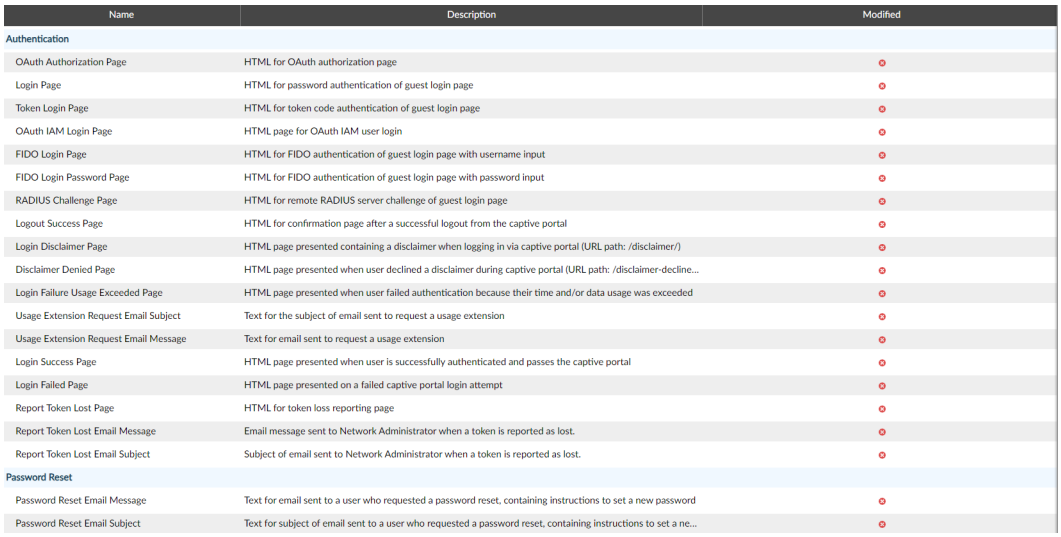
Portals can permit certain pre-login and post-login services for users, including password reset and token registration abilities.

Configuring an OAuth portal is same as configuring configure captive or self-service portals. See Portals on page 144.

Replacement messages

The replacement messages list lets you view and customize OAuth replacement messages.

To view the OAuth replacement message list, go to **Authentication > OAuth Service > Replacement Messages**.



Name	Description	Modified
Authentication		
OAuth Authorization Page	HTML for OAuth authorization page	
Login Page	HTML for password authentication of guest login page	
Token Login Page	HTML for token code authentication of guest login page	
OAuth IAM Login Page	HTML page for OAuth IAM user login	
FIDO Login Page	HTML for FIDO authentication of guest login page with username input	
FIDO Login Password Page	HTML for FIDO authentication of guest login page with password input	
RADIUS Challenge Page	HTML for remote RADIUS server challenge of guest login page	
Logout Success Page	HTML for confirmation page after a successful logout from the captive portal	
Login Disclaimer Page	HTML page presented containing a disclaimer when logging in via captive portal (URL path: /disclaimer/)	
Disclaimer Denied Page	HTML page presented when user declined a disclaimer during captive portal (URL path: /disclaimer-decline...	
Login Failure Usage Exceeded Page	HTML page presented when user failed authentication because their time and/or data usage was exceeded	
Usage Extension Request Email Subject	Text for the subject of email sent to request a usage extension	
Usage Extension Request Email Message	Text for email sent to request a usage extension	
Login Success Page	HTML page presented when user is successfully authenticated and passes the captive portal	
Login Failed Page	HTML page presented on a failed captive portal login attempt	
Report Token Lost Page	HTML for token loss reporting page	
Report Token Lost Email Message	Email message sent to Network Administrator when a token is reported as lost.	
Report Token Lost Email Subject	Subject of email sent to Network Administrator when a token is reported as lost.	
Password Reset		
Password Reset Email Message	Text for email sent to a user who requested a password reset, containing instructions to set a new password	
Password Reset Email Subject	Text for subject of email sent to a user who requested a password reset, containing instructions to set a ne...	

For more information about customizing replacement messages, see Replacement messages on page 69.

SAML IdP

Security Assertion Markup Language (SAML) is used for exchanging authentication and authorization data between an identity provider (IdP) and a service provider (SP), such as Google Apps, Office 365, and Salesforce. The FortiAuthenticator can be configured as an IdP, providing trust relationship authentication for unauthenticated users trying to access an SP.

Realms can be selectively enabled while configuring the FortiAuthenticator as the IdP. When more than one realm is selected, a default realm can be chosen. New realms can be configured at **Authentication > User Management > Realms**.

SAML authentication on FortiAuthenticator can be set up in an SP-initiated or IdP-initiated configuration.

SAML SP-initiated authentication works as follows:

1. A user attempts to access an SP, for example Google, using a browser.
2. The SPs web server requests the SAML assertions for its service from the browser.
3. Two possibilities:
   - The user's browser already has valid SAML assertions, so it sends them to the SPs web server. The web server uses them to grant or deny access to the service. SAML authentication stops here.
   - The user's browser doesn't have valid SAML assertions, so the SPs web server redirects the browser to the SAML IdP.
4. Two possibilities:
   - The user's browser is already authenticated with the IdP, go to **step 5**.
   - The user's browser is not yet authenticated with the IdP, so the IdP requests and validates the user's credentials. If successful, go to **step 5**. Otherwise, access is denied.
5. IdP provides SAML assertions for the SPs and redirects the user's browser back to the SPs web server. Go back to **step 2**.

SAML IdP-initiated authentication works as follows:

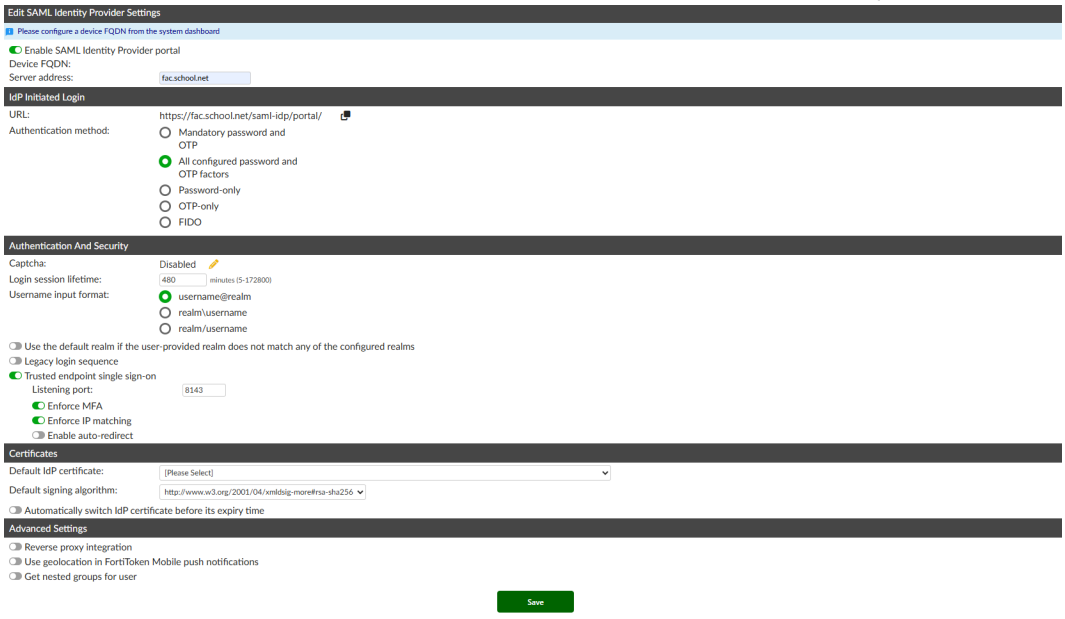
1. A user attempts to access the IdP login portal, resulting in one of two possibilities:
   - The user's browser is already authenticated by the IdP. Proceed to **step 2**.
   - The user's browser is not yet authenticated by the IdP, so the IdP requests and validates the user's credentials. If successful, go to **step 2**. Otherwise, access is denied.
2. The user is presented with an IdP portal landing page that includes a list of the SPs participating in IdP-initiated login. The user selects an SP.
3. IdP generates the SAML assertions for the browser and sends it to the SP.
4. The SP receives the assertions and authenticates the user, resulting in one of two possibilities:
   - The user is authorized, and the SP provides the requested resource to the user.
   - The user is not authorized, and access to the SP is denied.

When FIDO authentication is required, the end-user starts the login process on a username-only (**Login Fido Page** replacement message) login page same as for self-service portal, then proceeds through the subsequent authentication steps (FIDO/password validation) depending on the configuration.

General

To configure general SAML IdP portal settings:

1. Go to **Authentication > SAML IdP > General**, and select **Enable SAML Identity Provider portal**.



2. Configure the following settings:

Device FQDN	To configure this setting, you must enter a **Device FQDN** in the **System Information** widget in the **Dashboard**.

Server address	Enter the IP address or FQDN of the FortiAuthenticator device.
URL	The URL used to access the IdP portal in an IdP-initiated login scenario. SPs configured in FortiAuthenticator must have the option **Support IdP-initiated assertion response** enabled in order to be listed in the portal.

Authentication method	Select one of the following:
	• **Mandatory password and OTP**: Two-factor authentication is required for every user.
	• **All configured password and OTP factors**: Two-factor authentication is required if it is enabled on the user's account, otherwise, allow one-factor authentication (default).
	• **Password-only**: Authenticate users through password verification only. If password authentication is disabled on the user account, the account cannot be authenticated.
	• **OTP-only**: Authenticate users through token verification only. If token-based authentication is disabled on the user account, the account cannot be authenticated.
	• **FIDO**: Authenticate users through FIDO.
	  • **FIDO-only**: Log in with FIDO token only (without password).
	  • **Password and FIDO**: Log in with the password and the FIDO token.
	  • **Allow two-factor authentication (password and OTP) if all FIDO keys have been revoked for the user account**: Enable to allow two-factor authentication (password and OTP) if all FIDO keys have been revoked for the user account.
	  Note: FIDO is unavailable for a user account when:
	  • FIDO is disabled.
	  • FIDO is enabled, but no FIDO key was registered.
	  • FIDO is enabled, but all the FIDO keys were revoked.

Captcha	The state of the optional IP lockout CAPTCHA settings. **Note**: The option is read-only.  Select the pen icon to edit the IP lockout CAPTCHA settings in Lockouts on page 85.
Login session timeout	Set the user's login session timeout limit between 5 - 172800 minutes (120 days). The default is 480 minutes (eight hours).
Username input format	Select one of the following three username input formats: • **username@realm** • **realm\username** • **realm/username**

Use default realm when user-provided realm is different from all configured realms	When enabled, FortiAuthenticator selects the default realm for authentication when the user-specified realm is different from all configured realms.	
Legacy login sequence	When enabled, the legacy sequence requests username and password on the same form. When disabled, only the username is requested on the first form. The option is disabled by default.  When doing IdP proxy to multiple remote SAML IdP servers, keep this option disabled.	
	IAM login	Enable to allow IAM login. Note: The option is now only available when **Legacy login sequence** is enabled.
Trusted endpoint single sign-on	When enabled, SSOMA endpoints can log in without reentering username and password. The username login page includes a **Trusted Endpoint Single Sign-On** button that allows single sign-on for trusted endpoints. The legacy login page does not offer the **Trusted Endpoint Single Sign-On** button. The option is disabled by default. **Note**: **Trusted endpoint single sign-on** and **Legacy login sequence** options are mutually exclusive.	
	Listening port	Trusted endpoints TLS-connect to this TCP port to present their client certificate to the FortiAuthenticator (default = 8143).
	Enforce MFA	When enabled, FortiAuthenticator enforces token-based settings configured for the SP during trusted endpoint single sign-on. When disabled, token-based verification is bypassed for trusted endpoints. **Note**: The option is only available when **Trusted endpoint single sign-on** is enabled.
	Enforce IP matching	When enabled, the source IP address of the endpoint connecting to the listening port must match one of the IP addresses reported by the SSOMA to do a successful trusted endpoint authentication. For example, if the endpoint is on a private network and its connection to the FortiAuthenticator is being NAT'ed, this option should be disabled.
	Enable auto-redirect	When enabled, you are automatically redirected to use the trusted endpoint single sign-on (SSO) on the default login page.

Default IdP certificate	Select a default certificate the IdP uses to sign SAML assertions from the dropdown menu.	
Default signing algorithm	Select a default signing algorithm from the dropdown.	
Automatically switch IdP certificate before its expiry time	Enable and select a **New default IdP certificate** from the dropdown.	
	Switch at	Enter a date (YYYY-MM-DD) and time when the new default IdP certificate applies. Alternatively, use the calendar icon to select a date. For changing time, select the clock icon and choose a time from the list.  Select **Today** to switch to today's date or select **Now** to switch to the time now.
Reverse proxy integration	When enabled, SAML authentication response is redirected to the **Reverse proxy URL** instead of the **SP ACS (login) URL** when the authentication request is received at the reverse proxy **Listening Port**.	
	Listening port	Enter the reverse proxy listening port (default = TCP/8144).
	Reverse proxy URL	Enter the reverse proxy URL.
Use geolocation in FortiToken Mobile push notifications	Enable to use geolocation in FortiToken Mobile push notifications.	
Get nested groups for user	Enable to get nested groups for Windows AD users.	

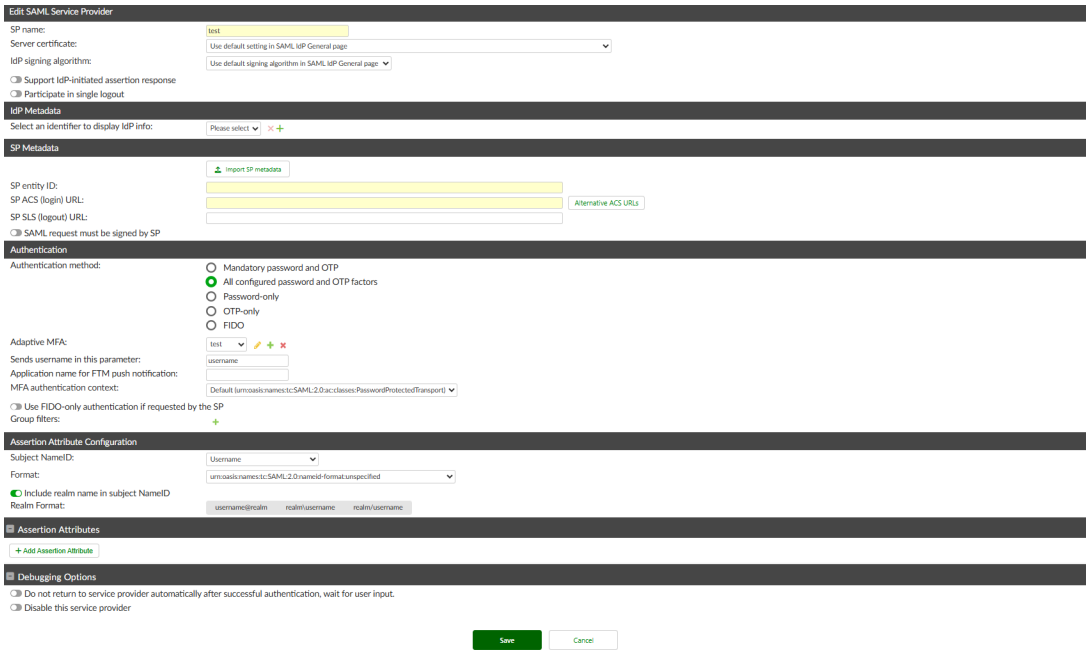
3. Select **Save** to apply any changes that you have made.

Service providers

Service providers (SP) can be managed from **Authentication > SAML IdP > Service Providers**.

To configure SAML service provider settings:

1. Select **Create New**.



2. Enter the following information:

IdP address	To configure the IdP address (and IdP settings below), you must have already configured the server's address under **Authentication > SAML IdP > General**.
SP name	Enter a name for the SP.
Server certificate	Select a server certificate to use for the SP. If a certificate is not selected, the specified default IdP certificate is used.
IdP signing algorithm	Select an IdP signing algorithm from the dropdown.
Support IdP-initiated assertion response	Allows the IdP to send an assertion response to the SP without a prior request from the SP. Enabling this setting allows the SP to participate in IdP initiated login, and causes the SP to appear in the IdP login portal.
Relay state	Allows SP to redirect user to the provided URL after a successful assertion response.
Icon	From the dropdown, select an icon to use. Select the pen icon to edit the current icon or select **+** to create a new icon.
Participate in single logout	Enable or disable participation in single logout for the SAML IdP service.
IdP Metadata	
Select an identifier to display IdP info:	Select a prefix for the IdP that is appended to the end of the IdP URLs.

		Select **+** to create an alternate IdP prefix. Alternatively, you can select **Random** in the **Create Alternate IdP Prefix** dialog to generate a random 16 digit alphanumeric string. Select **x** to remove the IdP prefix. **Note**: Multiple endpoints can be generated for each SAML service provider using the identifiers.
	IdP entity id	The IdP's entity ID, for example: `http://www.example.com/saml-idp/xxx/metadata/`
	IdP single sign-on URL	The IdP's login URL, for example: `http://www.example.com/saml-idp/xxx/login/`
	IdP single logout URL	The IdP's logout URL, for example: `http://www.example.com/saml-idp/xxx/logout/`
	IdP metadata	Select **IdP metadata** to download the IdP metadata to your management computer.
SP Metadata		SP Metadata fields are only available once the SAML Service Provider settings has been saved.
	Import SP metadata	Select **Import SP metadata** to import the SP metadata from your management computer and click **Save**.
	SP entity id	Enter the SP's entity ID.
	SP ACS (login) URL	Enter the SP's Assertion Consumer Service (ACS) login URL. Click **Alternative ACS URLs** to configure up to three additional ACS (login) and SLS (logout) URLs.
	SP SLS (logout) URL	Enter the SP's Single Logout Service (SLS) logout URL.
	SAML request must be signed by SP	Enable this option and import the SP certificate for authentication request signing by the SP.
	Certificate type	• **SP certificate**: The SP request is signed by the specified certificate. • **Direct CA certificate**: The SP request must contain the SP certificate fingerprint that was used to sign the request, and the certificate fingerprint must be issued by the CA specified in the configuration.
	Certificate fingerprint	The primary certificate for verifying the SP request signature
	Fingerprint algorithm	Displays the detected fingerprint algorithm of the certificate fingerprint or alternative certificate fingerprint. **Note**: SHA-1 has been deprecated.  A warning is displayed if SHA-1 is detected upon upgrade.

	Certificate issuer	Displays the certificate issuer.
	Certificate subject	Displays the certificate subject.
	Validity period	Displays the certificate validity period.
	Use ACS URL from SP authentication request (override ACS URLs configured above)	When enabled, indicates that the ACS URL must be included within the SP request, and that the FortiAuthenticator must use it instead of the pre-configured ACS URL.
Authentication		

	Authentication method	Select one of the following:
		• **Mandatory password and OTP**
		• **All configured password and OTP factors**
		• **Password-only**
		• **OTP-only**
		• **FIDO-only**:
		  • **FIDO-only**: Log in with FIDO token only (without password).
		  • **Password and FIDO**: Log in with the password and the FIDO token.
		  • **Allow two-factor authentication (password and OTP) if all FIDO keys have been revoked for the user account**: Enable to allow two-factor authentication (password and OTP) if all FIDO keys have been revoked for the user account.

	Adaptive MFA	Certain users can bypass the OTP verification, so long as they belong to a trusted subnet or they are a known device: 1. Select **+** to add an adaptive MFA rule. The **Create New Adaptive MFA Rules window** opens. 2. In the **Trusted Subnet** pane, enable **Trusted subnet** to bypass OTP validation if the end-user is on a trusted subnet: **Note**: Trusted subnets can be configured in **Authentication > User Account Policies > Trusted Subnets**. a. Select **All trusted subnets** to add all the available trusted subnets. OR b. Select **Specify trusted subnets** to specify the trusted subnets. Choose from a list of available trusted subnets. 3. In the **Known Devices** pane, enable **known devices** to bypass OTP validation if the end-user is a known device. a. In **Validate OTP again after**, enter the time after which OTP is required, in minutes/hours/days (default = 5 hours). b. Select how to send the OTP (**FortiTokens**/**Email**/**SMS**). 4. Click **Save**.

	 This option is only available for **Mandatory password and OTP** and **All configured password and OTP factors** authentication methods.
Sends username in this parameter	Specify the parameter name that the SP uses to prefill the username login field (default = username).
Application name for FTM push notification	Enter the client application name. This field is displayed on the FortiToken app. When creating a new SP or upgrading to FortiAuthenticator 8.0, the SP name is the default client application name.
Use FIDO-only authentication if requested by the SP	Enable to use FIDO-only authentication if requested by the SP. This option is not available for **FIDO-only** authentication method.
Group filters	Select **+** to add a group filter. See User sources on page 236.
Assertion Attribute Configuration	
Subject NameID	Select the user attribute that serves as SAML assertion subject NameID. Select from either **Username**, **Email**, **Remote LDAP user DN**, **Remote LDAP user objectGUID**, **Remote LDAP user mS-DS ConsistencyGuid**, **Remote LDAP Custom attribute**, **Remote SAML Subject NameID**, or **Remote SAML Custom assertion**. If the attribute selected is not available for a user, **Username** is used by default.
Format	Select from **Unspecified**, **Transient**, or **Persistent**.
Include realm name in subject NameID	When enabled, you can select the username/realm format to include in subject NameID.
Assertion Attributes	
SAML Attribute	Enter a name for the **SAML attribute**. Select **Add Assertion Attribute** to add the attribute. The following user attributes are available when creating a new assertion attribute: FortiAuthenticator: • **Username** • **First Name** • **Last Name** • **Email** • **Group** **Note**: The attribute contains the list of group names that the logged in user is a

"member of" from the set of groups configured in **Authentication > User Management > User Groups**.

The list of groups is reduced based on how the global and SP group filters were configured for the SAML IdP services:

- Global and SP disabled: All groups the logged-in user is a member of, except LDAP groups of **LDAP filter** subtype.
- Group enabled and SP disabled: All groups the logged in user is a member of within the global group filter.
- Global disabled and SP disabled: All groups the logged in user is a member of within the SP group filter.
- Global and SP enabled: All groups the logged in user is a member of within the union of the global and SP group filters.

- **IAM account name**
- **IAM account alias**
- **IAM username**

Remote LDAP server:

- **DN**
- **sAMAccountName**
- **userPrincipalName**
- **displayName**
- **objectGUID**
- **mS-DS-ConsistencyGuid**
- **LDAP group membership**
- **LDAP custom attribute (ASCII/UTF8)**
- **LDAP custom attribute (BASE64)**

Remote RADIUS server:

- **RADIUS attribute**

When **RADIUS attribute** is selected as the **User attribute**, the following additional settings are available in the **Create New Assertion Attribute** dialog:

- **Vendor**: The RADIUS vendor name.
- **Attribute ID**: The attribute within the vendor's RADIUS dictionary.

Remote SAML server:

- **SAML username**
- **SAML group membership**
- **SAML assertion**

Other:

- **Authentication status**
- **Realm** (returns the realm that the end user was authenticated against)
- **IdP session identifier**

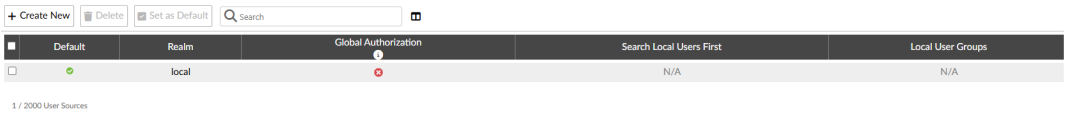
Custom fields configured in **Authentication > User Account Policies > Custom User Fields** are available here.

Debugging Options	
Do not return to service provider automatically after successful authentication, wait for user input	Enable this option to let users choose where to navigate to after they are authenticated.
Disable this service provider	Disables the SP.

3. Select **Save**.

User sources

Go to **Authentication > SAML IdP > User Sources** to see the list of user sources for the SAML service.



The maximum number of allowed realms is equal to the maximum number of realms in the legacy self-service portal plus the realms in SAML IdP.

A maximum of 400 realms can be added.

The following options are available:

Create New	Select to create a new realm. See Creating a user source on page 237.
Delete	Select to delete the selected realms.
Set as Default	Select to set the selected realm as the default user source.
Search	Enter a search term in the search field, then select **Search** to search the user sources list.
Reset table column widths	Select the reset icon to reset the table column widths to default.

The **Global Authorization** column displays global group filters only.

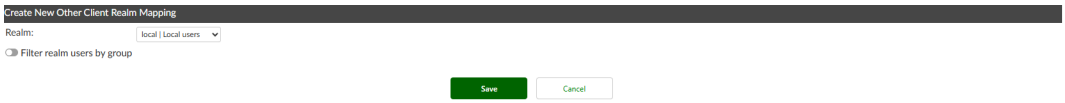
Only users authorized by the group filters are able to obtain a SAML IdP session.

Omit group filters to authorize all the realm users.

Creating a user source

To create a user source:

1. Go to **Authentication > SAML IdP > User Sources**.
2. Select **Create New**.
   The **Create New Other Client Realm Mapping** window opens.



3. Enter the following information:

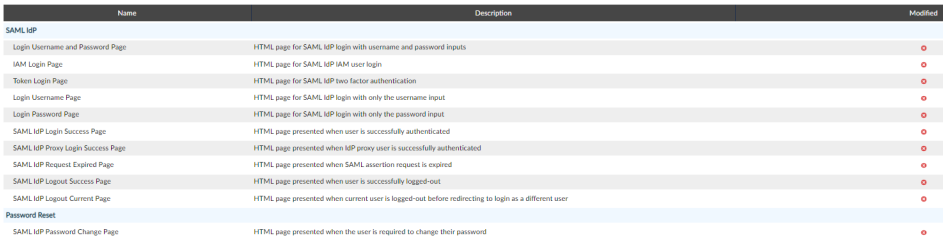
Realm	From the dropdown, select a realm source.
Filter realm users by group	Enable to filter realm users by user groups.
	To select user groups, from the **Available User Groups** table, move the user groups to the **Chosen User Groups** list.

4. Click **Save**.

Replacement messages

The replacement messages list lets you view and customize SAML IdP replacement messages and manage images.

To view the SAML replacement message list, go to **Authentication > SAML IdP > Replacement Messages**.



For more information about customizing replacement messages, see Replacement messages on page 69.

FortiAuthenticator agents

FortiAuthenticator provides multiple agents for use in two-factor authentication:

- FortiAuthenticator Agent for Microsoft Windows
- FortiAuthenticator Agent for Outlook Web Access

For information on installing the agents, see the latest Install Guides for FortiAuthenticator Agent for Microsoft Windows and FortiAuthenticator Agent for Microsoft OWA.

FortiAuthenticator Agent for Microsoft Windows and FortiAuthenticator Agent for Microsoft OWA download files are now available in the `FortiAuthenticator_and_FortiTrustID_Agents` folder in **Support > Firmware Download** within the FortiCare portal.

FortiAuthenticator Agent for Microsoft Windows

FortiAuthenticator Agent for Microsoft Windows is a credential provider plug-in that enhances the Windows login process with a one time password, validated by FortiAuthenticator.

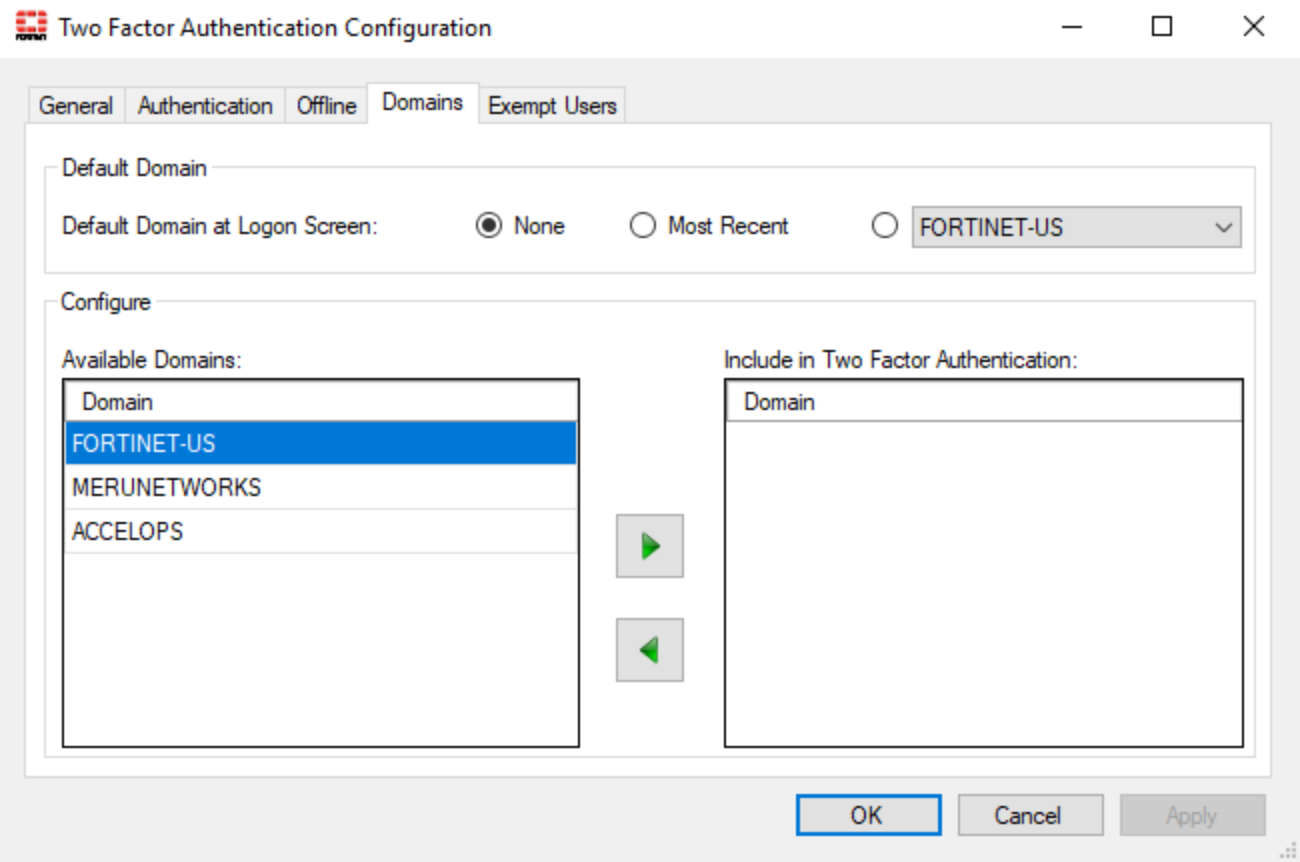
Key features

- **2FA**
  Adds an extra layer of security by requiring users to authenticate using two different factors, typically a password and a secondary token, such as a mobile application, hardware token, or SMS-based code.
- **Integration with FortiAuthenticator**
  Works in conjunction with FortiAuthenticator, Fortinet's centralized authentication management solution, providing a robust and scalable authentication framework for the organization.
- **Integration with Active Directory**
  It integrates seamlessly with Microsoft Active Directory, leveraging existing user accounts and groups for authentication.
- **Event logging and reporting**
  It provides detailed logs and reports on authentication events, helping administrators monitor and audit access activities.
- **Compliance**
  By implementing strong authentication mechanisms, it helps organizations comply with various regulatory requirements and security standards.

Configurable default domain

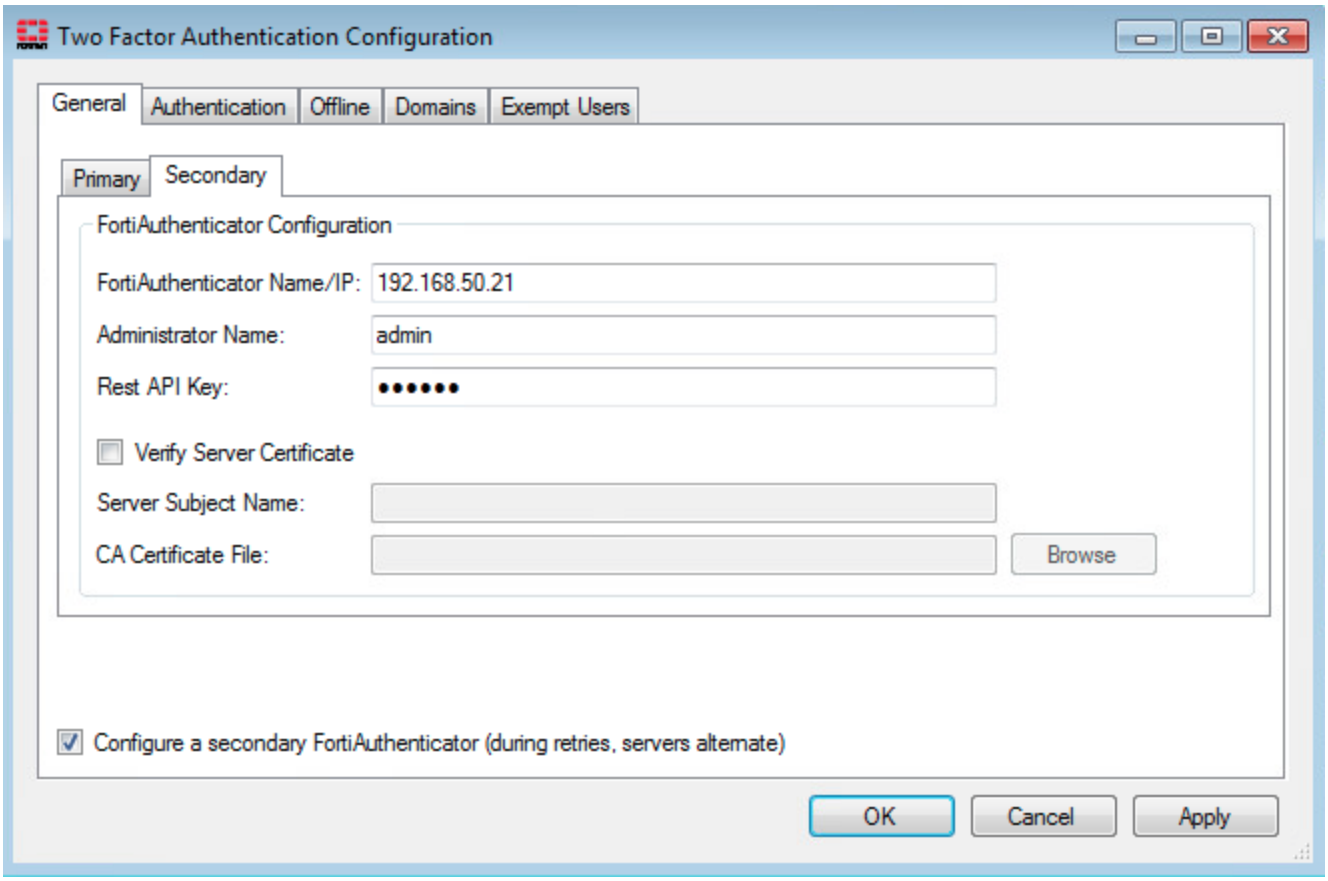
When configuring two-factor authentication in the FortiAuthenticator Agent for Microsoft Windows, you can select a **Default Domain at Logon Screen**. The options are **None**, **Most Recent**, and a populated list of available domains (also configurable).

This is particularly useful for environments that have a single domain (where previously, the user had to manually pick a domain from a dropdown every single login, even in single-domain environments).



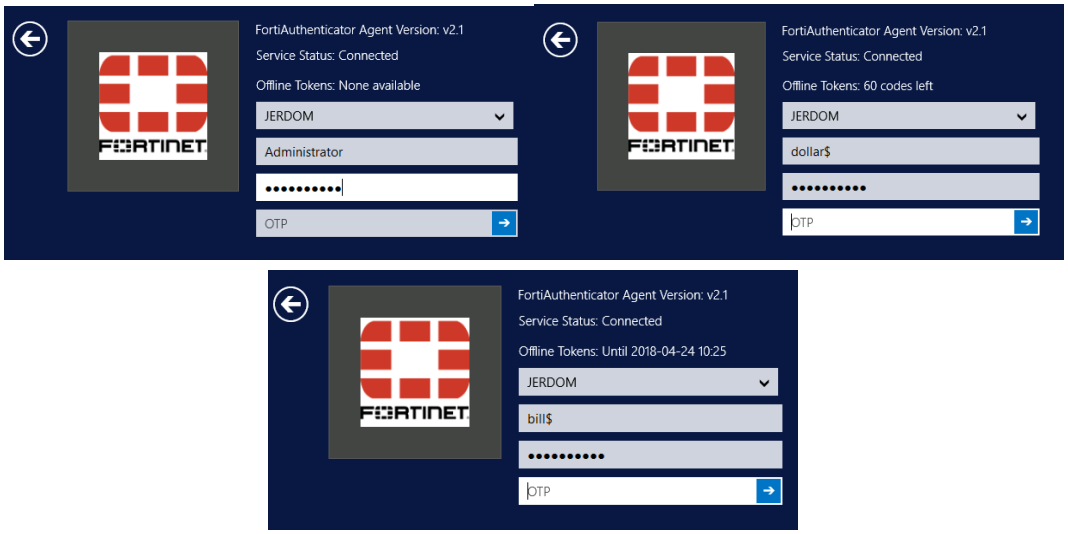
Load-balancing HA configurations

Customers with a load-balancing HA configuration can configure the FortiAuthenticator Agent for Microsoft Windows to try to reach the secondary FortiAuthenticator if the primary is unreachable, with retries occurring in the same order (in round-robin fashion).



Offline token validation at login

You can view the time remaining for offline token validation when logging in using the FortiAuthenticator Agent for Microsoft Windows.



For all tokens, FortiAuthenticator downloads enough offline tokens for the configured cache size plus the authentication window size (so if the HOTP cache = 50 and the HOTP window = 10, you initially have 60 tokens remaining; when tokens are displayed but not submitted to FortiAuthenticator, this ends up as fewer than 60 authentication attempts).

TLS 1.2 support

All network communications take place over TLS 1.2. As a result, the minimum required version of the .NET Framework is 4.6.0. The FortiAuthenticator Agent for Microsoft Windows installer will offer to install TLS 1.2 when it is necessary.

FortiAuthenticator Agent for Outlook Web Access

FortiAuthenticator Agent for Outlook Web Access is a plug-in that enhances the Web login process with a one time password, validated by FortiAuthenticator.

Key features

- **2FA**
  Adds an extra layer of security by requiring users to authenticate using two different factors, typically a password and a secondary token, such as a mobile app, hardware token, or SMS-based code.
- **Seamless integration**
  Integrates directly with Microsoft OWA, allowing organizations to enhance security without significant changes to their existing email infrastructure.
- **Integration with FortiAuthenticator**
  Works in conjunction with FortiAuthenticator to support various Fortinet authentication solutions, including FortiToken, providing a robust and scalable authentication framework for the organization.
- **Improved security**
  Protects against unauthorized access to email accounts, reducing the risk of email-based attacks and data breaches.
- **User-friendly experience**
  Maintains a straightforward login process for users, ensuring that the additional security measures do not hinder productivity.
- **Centralized management**
  Provides centralized management of authentication policies, with configurations required on both FortiAuthenticator (for users and tokens) and the OWA Agent on the Exchange server, making it easier for administrators to enforce security policies across the organization.
- **Enhanced compliance**
  Helps organizations meet regulatory requirements for data protection by implementing strong authentication mechanisms.

Port-based network access control

Port-based network access control (PNAC), or 802.1X authentication requires a client, an authenticator, and an authentication server (such as a FortiAuthenticator device).

The client is a device that wants to connect to the network. The authenticator is simply a network device, such as a wireless access point or switch. The authentication server is usually a host that supports the RADIUS and EAP protocols.

The client is not allowed access to the network until the client's identity has been validated and authorized. Using 802.1X authentication, the client provides credentials to the authenticator, which the authenticator forwards to the authentication server for verification. If the authentication server determines that the credentials are valid, the client device is allowed access to the network.

FortiAuthenticator supports several IEEE 802.1X EAP methods.

Extensible Authentication Protocol

FortiAuthenticator supports several IEEE 802.1X Extensible Authentication Protocol (EAP) methods. These include authentication methods most commonly used in WiFi networks.

EAP is defined in RFC 3748 and updated in RFC 5247. EAP does not include security for the conversation between the client and the authentication server, so it is usually used within a secure tunnel technology such as TLS, TTLS, or MS-CHAP.

FortiAuthenticator supports the following EAP methods:

Method	Server Auth	Client Auth	Encryption	Native OS Support
PEAP (MSCHAPv2)	Yes	Yes	Yes	Windows XP, Vista, 7, 8, 10, 11
EAP-TTLS	Yes	No	Yes	Windows Vista, 7, 8, 10, 11
EAP-TLS	Yes	Yes	Yes	Windows (XP, 7, 8, 10, 11), Mac OS X, iOS, Linux, Android
EAP-GTC	Yes	Yes	Yes	None (external supplicant required)
EAP-MSCHAPv2	Yes	Yes	Yes	Windows Vista, 7, 8, 10, 11

In addition to providing a channel for user authentication, EAP methods also provide certificate-based authentication of the server computer. EAP-TLS provides mutual authentication: the client and server authenticate each other using certificates. This is essential for authentication onto an enterprise network in a BYOD environment.

For successful EAP-TLS authentication, the user's certificate must be bound to their account in **Authentication > User Management > Local Users** (see Local users on page 95) and the relevant RADIUS client in **Authentication > RADIUS**

Service > Clients (see RADIUS service on page 189) must permit that user to authenticate. By default, all local users can authenticate, but it is possible to limit authentication to specified user groups.

FortiAuthenticator and EAP

FortiAuthenticator delivers all of the authentication features required for a successful EAP-TLS deployment, including:

- **Certificate Management**: Create and revoke certificates as a CA. See Certificate management on page 287.
- **Simple Certificate Enrollment Protocol (SCEP) Server**: Exchange a certificate signing request (CSR) and the resulting signed certificate, simplifying the process of obtaining a device certificate.

CLI

Use `diagnose authentication radius-eap-ecdh-curve` to override the default `ECDH_CURVE` for EAP (default = `secp521r1:secp384r1:prime256v1`).

FortiAuthenticator unit configuration

To configure FortiAuthenticator, you need to:

1. Create a CA certificate for FortiAuthenticator. See Certificate authorities on page 299.
   Optionally, you can skip this step and use an external CA certificate instead. Go to **Certificate Management > Certificate Authorities > Trusted CAs** to import CA certificates. See Trusted CAs on page 307.
2. Create a server certificate for FortiAuthenticator, using the CA certificate you created or imported in the preceding step. See End entities on page 288.
3. If you configure EAP-TTLS authentication, go to **Authentication > RADIUS Service > EAP** and configure the certificates for EAP. See Configuring certificates for EAP on page 243.
4. If SCEP will be used:
   - Configure an SMTP server for sending SCEP notifications. Then configure the email service for the administrator to use the SMTP server that you created. See Email services on page 73.
   - Go to **Certificate Management > SCEP > General**, select **Enable SCEP**, select the CA certificate that you created or imported in Step 1 in the **Default CA** field, and select **OK**. See SCEP on page 307.
5. Go to **Authentication > Remote Auth. Servers > LDAP** and add the remote LDAP server that contains your user database. See LDAP on page 176.
6. Import users from the remote LDAP server. You can choose which specific users are permitted to authenticate. See Remote users on page 107.
7. Go to **Authentication > RADIUS Service > Clients** to add the FortiGate wireless controller as an authentication client. Be sure to select the type of EAP authentication you intend to use. See RADIUS service on page 189.

Configuring certificates for EAP

FortiAuthenticator can authenticate itself to clients with a CA certificate.

1. Go to **Certificate Management > Certificate Authorities > Trusted CAs** to import the certificate you will use. See Trusted CAs on page 307.

2. Go to **Authentication > RADIUS Service > EAP**.
3. Select the EAP server certificate from the **EAP Server Certificate** dropdown menu.
4. Select the trusted CAs and local CAs to use for EAP authentication from their requisite lists.
5. Select **OK** to apply the settings.

Configuring switches and wireless controllers to use 802.1X authentication

The 802.1X configuration is largely vendor dependent. The key requirements are:

- **RADIUS server IP**: This is the IP address of the FortiAuthenticator.
- **Key**: The pre-shared secret configured in the FortiAuthenticator authentication client settings.
- **Authentication port**: By default, FortiAuthenticator listens for authentication requests on port 1812.

Non-compliant devices

802.1X methods require interactive entry of user credentials to prove a user's identity before allowing them access to the network. This is not possible for non-interactive devices, such as printers. MAC Authentication Bypass (MAB) is supported to identify and accept non-802.1X compliant devices onto the network using their MAC address as authentication.

This feature is only for 802.1X MAB. FortiGate captive portal MAC authentication is supported by configuring the MAC address as a standard user, with the MAC address as both the username and password, and not by entering it in the **MAC Devices** section.

Multiple MAC devices can be imported in bulk from a CSV file. The first column of the CSV file contains the device names (maximum of 50 characters), and the second column contains the corresponding MAC addresses (`0123456789AB` or `01:23:45:67:89:AB`).

When creating a new MAC-based authentication device, MAC addresses can be defined using wildcard capability to identify and accept all devices from a specific vendor. The first three bytes of a MAC address identify the vendor of the device. Define MAC devices using only the top three bytes to include all devices from a specific vendor. The following wildcard input formats are valid:

- 112233
- 11:22:33
- 112233xxxxxx
- 11:22:33:xx:xx:xx

To configure MAC-based authentication for a device:

1. Go to **Authentication > User Management > MAC Devices**.
   The MAC device list is displayed.
2. If you are adding a new device, select **Create New** to open the **Create New MAC-based Authentication Device** window.
   If you are editing an already existing device, select the device from the device list.

3. Enter the device name in the **Name** field.
4. Enter the device's MAC address in the **MAC address** field. Alternatively, enter a wildcard MAC address to represent all MAC devices from a specific vendor.
5. Optionally, enter a description about the device.
6. Optionally, enable **This device belongs to a user**. In **User Type**, select one of **Local**, **Remote LDAP**, or **Remote RADIUS** user types, and then select the user from the **Owner** dropdown.
7. Select **Save** to apply your changes.

To import MAC devices:

1. In the MAC device list, select **Import**.
2. Select **Upload a file** to locate the CSV file on your computer.
3. If you intend to add the MAC device to a group, from the **Add MAC device(s) to group** dropdown, select a group.
4. Select **Save** to import the list.
   The import will fail if the maximum number of MAC devices has already been reached, or if any of the information contained within the file does not conform, for example if the device name too long, or there is an incorrectly formatted MAC address.

Fortinet Single Sign-On

Fortinet Single Sign-On (FSSO) is a set of methods to transparently authenticate users to FortiGate devices. This means that FortiAuthenticator is trusting the implicit authentication of a different system, and using that to identify the user. FortiAuthenticator takes this framework and enhances it with several authentication methods:

- Users can authenticate through a web portal and a set of embeddable widgets.
- Users with FortiClient Endpoint Security installed can be automatically authenticated through the FortiClient SSO Mobility Agent.
- Users authenticating against Active Directory can be automatically authenticated.
- RADIUS Accounting packets can be used to trigger an FSSO authentication.
- Users can be identified through the FortiAuthenticator API. This is useful for integration with third-party systems.

This section describes FSSO only. FSSO authentication methods do not require accounting proxy configuration.

FortiAuthenticator must be configured to collect the relevant user logon data. After this basic configuration is complete, the various methods of collecting the log in information can be set up as needed.

A maximum of 3500 FortiGate devices can connect to the FortiAuthenticator. This value is hardcoded for all FortiAuthenticator models and is independent of the user license limit.

Domain controller polling

When FortiAuthenticator runs for the first time, it will poll the domain controller (DC) logs backwards until either the end of the log file or the logon timeout setting, whichever is reached first.

When FortiAuthenticator is rebooted, the memory cache is written to the disk, then re-read at startup, retaining the previous state. Windows DC polling restarts on boot, then searches backwards in the DC log files until it reaches either the log that matches the last known serial number found in the login cache file, the log that is older than the last recorded read time, or the end of the log file, whichever is reached first.

The currently logged in FSSO users list is cached in memory and periodically written to disk. In an active-passive HA cluster, this file is synchronized to the standby member.

Windows management instrumentation polling

FortiAuthenticator supports Windows Management Instrumentation (WMI) polling to detect workstation log off. This validates the currently logged on user for an IP address that has been discovered by the DC polling detection method.

Remote WMI access requires that the related ports are opened in the Windows firewall, and access to a domain account that belongs to the domain admin group.

To open ports in the Windows firewall in Windows 7, run `gpedit.msc`, go to **Computer configuration > Administrative Templates > Network > Network Connections > Windows Firewall > Domain Profile**, go to **Allow remote admin exception**, then enable **remote admin exception** and, if necessary, configure an IP subnet/range.

Settings

FortiAuthenticator units listen for requests from authentication clients and can poll Windows AD servers.

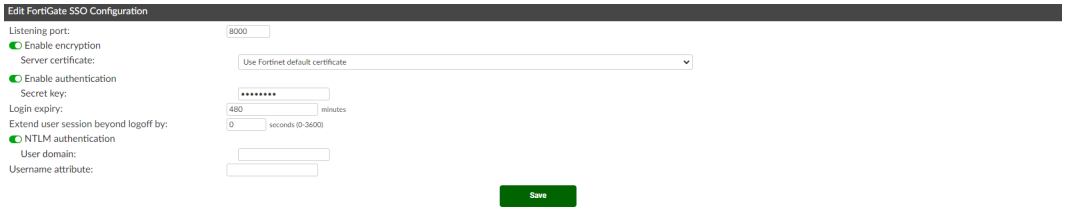
Go to **Fortinet SSO > Settings** to access the following FSSO settings tabs:

- FortiGate on page 247
- Methods on page 250
- User group membership on page 253
- Tiered architecture on page 255
- Log config on page 256

FortiGate

To configure FortiGate SSO settings:

1. Go to **Fortinet SSO > Settings > FortiGate**.
   The **Edit FortiGate SSO Configuration** window opens.



2. Configure the following settings:

Listening port	Leave at 8000 unless your network requires you to change this. Ensure this port is allowed through the firewall.
Enable encryption	Enable/disable encryption, then from the dropdown, select a server certificate. See End entities on page 288. **Note**: When enabled, FortiGates connect over TLS, and FortiAuthenticator uses Fortinet CA-signed certificate as the TLS server certificate. Depending on whether **Require strong cryptography** is enabled in System access on page 48, the following TLS cipher suites are accepted by FortiAuthenticator when FortiGate/FortiAuthenticator FSSO communication is encrypted. When **Require strong cryptography** is disabled:

- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES256-GCM-SHA384
- DHE-RSA-AES128-GCM-SHA256
- DHE-DSS-AES128-GCM-SHA256
- kEDH+AESGCM
- ECDHE-RSA-AES128-SHA256
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-RSA-AES128-SHA
- ECDHE-ECDSA-AES128-SHA
- ECDHE-RSA-AES256-SHA384
- ECDHE-ECDSA-AES256-SHA384
- ECDHE-RSA-AES256-SHA
- ECDHE-ECDSA-AES256-SHA
- DHE-RSA-AES128-SHA256
- DHE-RSA-AES128-SHA
- DHE-DSS-AES128-SHA256
- DHE-RSA-AES256-SHA256
- DHE-DSS-AES256-SHA
- DHE-RSA-AES256-SHA
- AES128-GCM-SHA256
- AES256-GCM-SHA384
- AES128-SHA256
- AES128-SHA
- AES256-SHA256
- AES128-SHA
- AES256-SHA
- AES CAMELLIA
- !DES-CBC3-SHA
- !aNULL
- !eNULL
- !EXPORT
- !DES
- !RC4
- !MD5
- !aECDH
- !EDH-DSS-DES-CBC3-SHA
- !EDH-RSA-DES-CBC3-SHA
- !KRB5-DES-CBC3-SHA

When **Require strong cryptography** is enabled:

- TLS-AES-128-GCM-SHA256

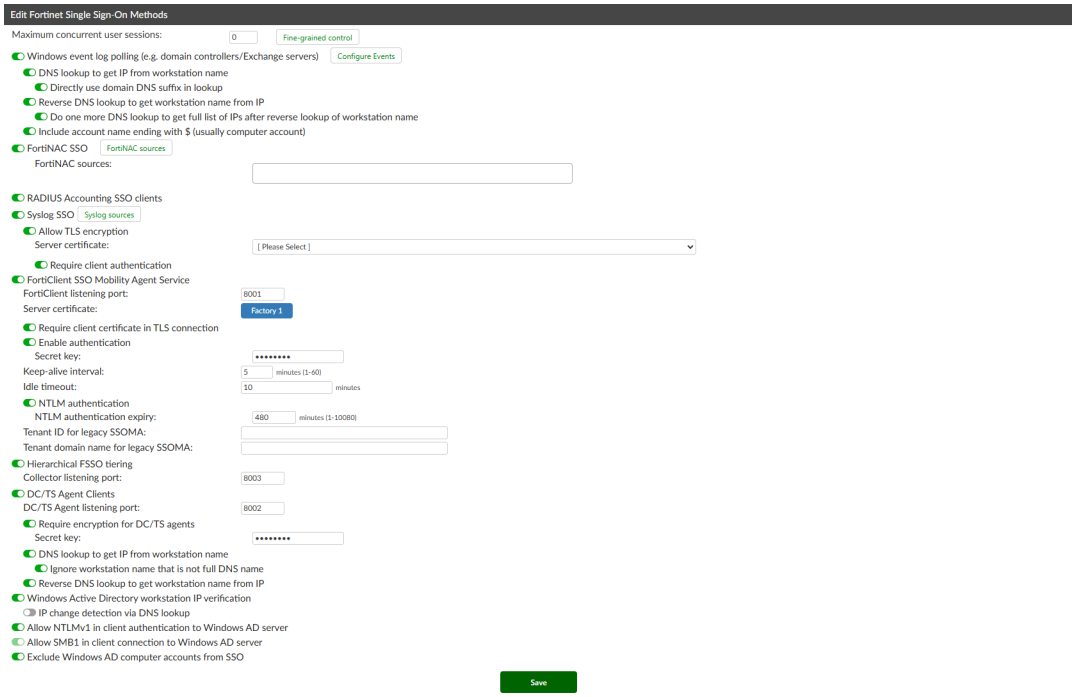
	• TLS-AES-256-GCM-SHA384 • TLS-CHACHA20-POLY1305-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-ECDSA-CHACHA20-POLY1305 • ECDHE-RSA-CHACHA20-POLY1305 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-RSA-AES256-SHA384 • ECDHE-RSA-AES128-SHA256 • DHE-RSA-AES128-GCM-SHA256 • DHE-RSA-AES256-SHA256 • DHE-RSA-AES128-SHA256 • ECDHE-RSA-AES256-SHA • ECDHE-RSA-AES128-SHA • AES256-GCM-SHA384 • PSK • DHE-RSA-AES128-SHA • !aNULL • !eNULL • !EXPORT • !DES • !RC4 • !MD5 • !aECDH • !EDH-DSS-DES-CBC3-SHA
Enable authentication	Select to enable authentication, then enter a secret key, or password, in the **Secret key** field.
Login expiry	The length of time, in minutes, that users can remain logged in before the system logs them off automatically. The default is 480 minutes (8 hours).
Extend user session beyond logoff by	The length of time, in seconds, that a user session is extended after the user logs off, from 0 (default) to 3600 seconds.
NTLM authentication	Select to enable NTLM authentication, then enter the NETBIOS or DNS name of the domain that the login user belongs to in the **User domain** field.
Username attribute	The username attribute expected by FortiGate for the remote LDAP user, e.g., **userPrincipalName** or **sAMAccountName**, regardless of the username used during login.

3. Click **Save**.

Methods

To configure FSSO methods:

1. Go to **Fortinet SSO > Settings > Methods**.
   The **Edit Fortinet Single Sign-On Methods** window opens.



2. Configure the following settings:

Maximum concurrent user sessions		Enter the maximum number of concurrent FSSO login sessions a user is allowed to have. Use **0** for unlimited. Select **Fine-grained control** to configure the maximum number of concurrent sessions for each user or group. See Fine-grained controls on page 271.
Windows event log polling (e.g. domain controllers/Exchange servers)		Select to enable Windows AD polling. This includes polling logon events from devices using Kerberos authentication or from Mac OS X systems. Select **Configure Events** to select the Windows security event IDs to use in event log polling. Select from event IDs 528, 540, 672, 673, 674, 680, 4624, 4768, 4769, 4770, and 4776.
	DNS lookup to get IP from workstation name	Select to use DNS lookup to get IP address information when an event contains only the workstation name. This option is enabled by default.
	Directly use domain DNS suffix in lookup	Select to use the domain DNS suffix when doing a DNS lookup. This option is disabled by default.
	Reverse DNS	Select to enable reverse DNS lookup. Reverse DNS lookup is used when

	lookup to get workstation name from IP	an event contains only an IP address and no workstation name. This option is enabled by default.
	Do one more DNS lookup to get full list of IPs after reverse lookup of workstation name	Reverse DNS lookup is used when an event contains only an IP address and no workstation name. After the workstation name is determined, it is used in the DNS lookup again to get more complete IP address information. This is useful in environments where workstations have multiple network interfaces. This option is disabled by default.
	Include account name ending with $ (usually computer account)	Accounts that end in "$" used to exclusively denote computer accounts with no actual user, but in some cases, valid accounts imported from dated systems can feature them. This option is disabled by default.
FortiNAC SSO		Select to enable the retrieval of SSO sessions from FortiNAC sources. Select **FortiNAC sources** to choose one or more configured FortiNAC sources to use as SSO sources. Select **Configure FortiNACs** to configure FortiNAC sources (under **System > Administration > FortiNACs**). For more information, see FortiNACs on page 65.
Radius Accounting SSO clients		Select to enable the detection of users sign-ons and sign-offs from incoming RADIUS accounting (Start, Stop, and Interim-Update) records.
Syslog SSO		Select to enable Syslog SSO, and configure syslog sources.
	Allow TLS encryption	Enable to allow TLS encryption.
	Server Certificate	From the dropdown, select one of the configured local server certificates.
	Require client authentication	Enable to require that the client certificate must be signed by one of the configured local or trusted CA certificates.
FortiClient SSO Mobility Agent Service		Select to enable single sign-on (SSO) by clients running FortiClient Endpoint Security. For more information, see FortiClient SSO Mobility Agent on page 275.
	FortiClient listening port	Enter the FortiClient listening port number.
	Server certificate	Choose which SSOMA server certificate to use, i.e, **Factory 1** (CA1) or **Factory 2** (CA2-signed) to ensure cross compatibility with all SSOMA versions. The FSSO daemon (`fsae`) uses the certificate specified in this new setting as the SSOMA server certificate.
	Require client certificate in TLS connection	Enable to require client certificate in TLS connection. This option is disabled by default.
	Enable authentication	Select to enable authentication, then enter a secret key, or password, in the **Secret key** field.

	Keep-alive interval	Enter the duration between keep-alive transmissions, from 1 to 60 minutes. Default is 5 minutes.
	Idle timeout	Enter an amount of time in minutes after which to logoff a user if their status is not updated. The value cannot be lower than the **Keep-alive interval** value.
	NTLM authentication	Select to enable the NT LAN Manager (NTLM) to allow logon of users who are connected to a domain that does not have the FSSO DC Agent installed. Disable NTLM authentication only if your network does not support NTLM authentication for security or other reasons. Enter an amount of time after which NTLM authentication expires in the **NTLM authentication expiry** field, from 1 to 10080 minutes (7 days).
	Tenant ID for legacy SSOMA	Optionally, enter the default Microsoft Entra ID (formerly Azure AD) tenant ID for legacy SSOMA.
	Tenant domain name for legacy SSOMA	Enter the tenant domain name for legacy SSOMA.
Hierarchical FSSO tiering		Select to enable hierarchical FSSO tiering. Enter the collector listening port in the **Collector listening port** field.
DC/TS Agent Clients		Select to enable clients using DC or TS Agent. Enter the TCP or UDP port in the **DC/TS Agent listening port** field. Default is 8002.
	Require encryption for DC/TS agents	Select to require authentication, then enter a secret key, or password, in the **Secret key** field. **Note**: If this option is enabled, the TCP port is used and the UDP port is disabled. Otherwise, the UDP port is used and the TCP port is disabled.
	DNS lookup to get IP from workstation name	Select to use DNS lookup to get IP address information when a client contains only the workstation name. This option is enabled by default. FortiAuthenticator attempts to obtain the workstation IP address using DNS lookup if the logon request contains only the workstation name. If the initial lookup fails, FortiAuthenticator will retry every 10 seconds for the following 5 minutes.
	Ignore workstation name that is not full DNS name	Select if the DNS server does not support a workstation name that is not a full DNS name, otherwise service delay may occur. This option is enabled by default.
	Reverse DNS lookup to get workstation name from IP	Select to enable reverse DNS lookup. Reverse DNS lookup is used when a client contains only an IP address and no workstation name. This option is enabled by default.
Windows Active Directory workstation IP verification		Select to enable workstation IP verification with Windows Active Directory. If enabled, select **IP change detection via DNS lookup** to detect IP changes via DNS lookup.

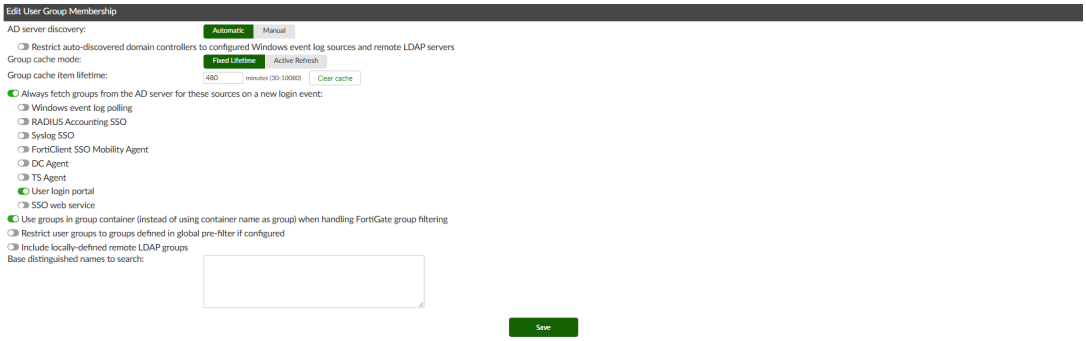
	Use changed IP even when workstation cannot be probed	Enable to use changes IP address even when the workstation cannot be probed.
Allow NTLMv1 in client authentication to Windows AD server	Optionally, enable NTLMv1.	
Allow SMB1 in client connection to Windows AD server	Optionally, enable SMB1.	
Exclude Windows AD computer accounts from SSO	When enabled, FortiAuthenticator does an AD lookup to determine whether an account ending with $ is a computer or a user, and excludes it from FSSO if it is a computer.	

3. Click **Save**.

User group membership

To configure user group membership settings:

1. Go to **Fortinet SSO > Settings > User Group Membership**.
   The **Edit User Group Membership** window opens.



2. Configure the following settings:

AD server discovery	Select from the following two options: • **Automatic** (default): The legacy discovery mechanism where FortiAuthenticator consults the global catalog to get a list of all domains and their AD servers. • **Manual**: The discovery mode is disabled. Instead, the AD servers list for group lookups must be explicitly configured.

	Restrict auto-discovered domain controllers to configured Windows event log sources and remote LDAP servers	Select to enable restricting automatically discovered domain controllers to already configured domain controllers only (disabled by default). See Windows event log on page 261. **Note**: The option is only available when **AD server discovery** is **Automatic**.
	AD servers	Specify the AD servers that can be used for group lookups. **Note**: The option is only available when **AD server discovery** is **Manual**.
Group cache mode		Select the group cache mode: • **Fixed Lifetime**: Items have an expiry time after which the are removed and re-queried on the next logon. • **Active Refresh**: Items are periodically updated for all currently logged on users.
	Group cache item lifetime	Enter the amount of time in minutes between 30-10080 (maximum of one week) after which items will expire. Additionally, you can **Clear cache**. **Note**: The option is only available when **Group cache mode** is **Fixed Lifetime**.
	Group cache update period for active logons	The amount of time between 30-10080 minutes (maximum of one week) after which items will update for active logins Additionally, you can manually **Update cache**. **Note**: The option is only available when **Group cache mode** is **Active Refresh**.
Always fetch groups from the AD server for these sources on a new login event		Select to prevent using cached groups and to always load groups from server for the following SSO sources: • **Windows event log polling** • **RADIUS Accounting SSO** • **Syslog SSO** • **FortiClient SSO Mobility Agent** • **DC Agent** • **TS Agent** • **User login portal** • **SSO web service**
Use groups in group container (instead of using container name as group) when handling FortiGate group filtering		Select to use groups in group container instead of using container name as the group when handling FortiGate group filtering. This option is enabled by default.
Restrict user groups to groups defined in global pre-filter if configured		Enable/disable the feature wherein the group memberships in the FSSO sessions should be restricted to the subset of groups specified in the FSSO global pre-filter.

Include locally-defined remote LDAP groups	Enable/disable the feature wherein you can specify whether to include FortiAuthenticator LDAP groups (remote LDAP user groups with **User retrieval** set to **Set a list of imported remote LDAP users** in **Authentication > User Management > User Groups**) for FSSO. The option is disabled by default.
Base distinguished names to search	Enter the base distinguished names to search for nesting of users or groups into cross domain and domain local groups.

3. Click **Save**.

Tiered architecture

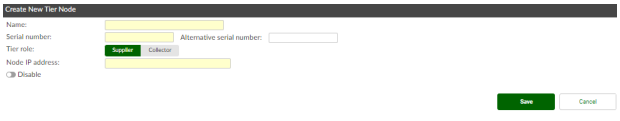
Tier nodes can be managed by going to **Fortinet SSO > Settings > Tiered Architecture**. A maximum of five tier nodes can be configured.

The following options are available:

Create New	Select to create a new tier node.
Delete	Select to delete the selected node or nodes.
Edit	Select to edit the selected node.
Search	Enter a search term to search the tier node list.
Name	The node name.
Tier Role	The node's tier role, either **Collector** or **Supplier**.
Address	The IP address of the node.
Port	The collector port number. Only applicable if **Tier Role** is **Collector**.
Serial Number	The serial number or numbers.
Enabled	If the node is enabled, a green circle with a check mark is shown. A node can be disabled without losing any of its settings.

To add a new tier node:

1. From the tier node list, select **Create New**. The **Create New Tier Node** window opens.



2. Enter the following information:

Name	Enter a name to identify the node.
Serial number	Enter the device serial number.
Alternative serial number	Optionally, enter a second, or alternate, serial number for an HA cluster member.
Tier role	Select the tier node role, either **Supplier** or **Collector**.
Node IP address	Enter the IP address for the supplier or collector.
Collector Port	Enter the collector port number. Default is 8003. This is only available when **Tier role** is set to **Collector**.
Disable	Disable the node without losing any of its settings.

3. Select **Save** to create the new tier node.

Log config

To configure log settings:

1. Go to **Fortinet SSO > Settings > Log Config**.
The **Edit SSO Log Configuration** window opens.

2. Configure the following settings:

Log level	Select one of **Error**, **Warning**, **Info**, or **Debug** as the minimum severity level of events to log.
Enable SSO log filtering	Select to enable SSO log filtering and enter keywords in the **Keywords** field.

3. Click **Save**.

Methods

Go to **Fortinet SSO > Methods** to access the following FSSO methods tabs:

- Web services on page 257
- SAML authentication on page 259
- Windows event log on page 261
- RADIUS accounting on page 262
- Syslog on page 263

Web services

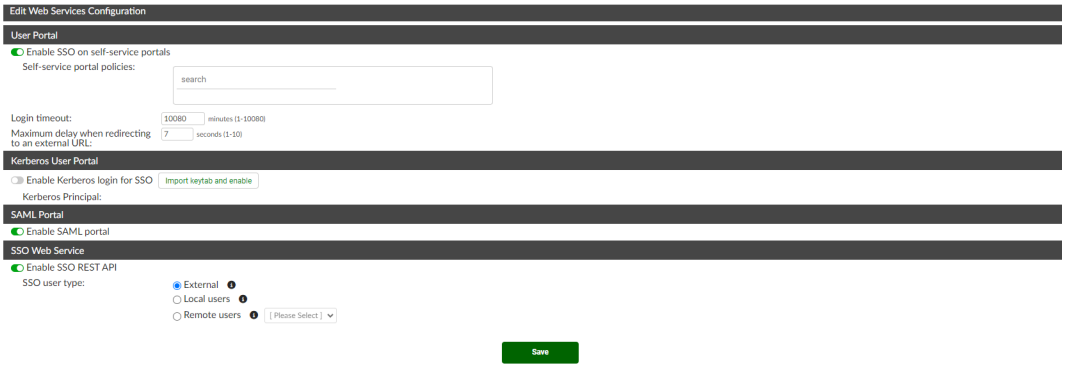
The SSO portal supports a logon widget that you can embed in any web page. Typically, an organization would embed the widget on its home page.

The SSO portal sets a cookie on the user's browser. When the user browses to a page containing the login widget, FortiAuthenticator recognizes the user and updates its database if the user's IP address has changed. The user will not need to re-authenticate until the login timeout expires, which can be up to 30 days. To log out of FSSO immediately, the user can select the **Logout** button in the widget.

The SSO portal supports multiple authentication methods including manual authentication, embeddable widgets, and Kerberos authentication.

To configure FSSO web services configurations:

1. Go to **Fortinet SSO > Methods > Web Services**.
   The **Edit Web Services Configurations** window opens.



2. Configure the following settings:

User Portal		
	Enable SSO on self-service portal policies	Select to use self-service portals as SSO login portal.
	Self-service portal policies	Select self-service portal policies from the **Self-service portal policies** search box.
	Login timeout	Set the maximum number of minutes a user is allowed to stay logged in before they are automatically logged out from SSO, between 1-10080 (maximum of one week, set by default).
	Maximum delay when redirecting to an external URL	Set the delay in seconds that occurs when redirecting to an external URL, between 1-10 seconds, with a default of 7 seconds.
Kerberos User Portal		

	Enable Kerberos login for SSO	Select **Enable Kerberos login for SSO** to enable Kerberos log in for SSO. Select **Import keytab and enable** to open the **Import Keytab** window where you can import a keytab from your computer. A keytab must be imported to enable Kerberos log in for SSO. See Kerberos on page 258 for more information.
	Kerberos Principal	View the Kerberos principal.
SAML Portal		
	Enable SAML portal	Select **Enable SAML portal** to enable SAML Portal log in for SSO.
SSO Web Service		
	Enable SSO REST API	Select **Enable SAML portal** to enable SAML Portal log in for SSO.
	SSO user type	Specify the type of user that the client will provide: • **External**: Users not defined on FortiAuthenticator. User groups are retrieved from the source. • **Local users**: Users defined on FortiAuthenticator as local users. Users groups are retrieved from the local groups. • **Remote users**: Users defined on a remote LDAP server. User groups are retrieved form the remote LDAP server. From the dropdown, select a remote LDAP server.

3. Click **Save**.

Kerberos

Kerberos authentication allows the FortiAuthenticator to identify connecting users through a Kerberos exchange after a redirect from a FortiGate device.

A keytab file that describes your Kerberos infrastructure is required. To generate this file, you can use a ktpass utility. The following code can be used in a batch file to simplify the keytab file creation:

```
set OUTFILE=FortiAuthenticator.keytab
set USERNAME=FortiAuthenticator@corp.example.com

set PRINC=HTTP/FortiAuthenticator.corp.example.com@CORP.EXAMPLE.COM
set CRYPTO=all

set PASSWD=Pa$$p0rt
set PTYPE=KRB5_NT_PRINCIPAL

ktpass -out %OUTFILE% -pass %PASSWD% -mapuser %USERNAME% -princ %PRINC% -crypto %CRYPTO% -ptype
      %PTYPE%
```

The FortiGate device can be configured to redirect unauthenticated users to the FortiAuthenticator, however the Kerberos authentication URL is different than the standard login URL. The Custom Message HTML for the Login Page HTML Redirect for Kerberos is as follows:

```
<!DOCTYPE HTML>
<html lang="en-US">
   <head>
      <meta charset="UTF-8">
      <meta http-equiv="refresh" content="1;url=http://<FortiAuthenticator-fqdn>/login/kerb-
            auth?user_continue_url=%%PROTURI%%">
      <script type="text/javascript">
         window.location.href = http://<FortiAuthenticator-fqdn>/login/kerb-auth?user_continue_
               url=%%PROTURI%%
      </script>
      <title>
         Page Redirection
      </title>
   </head>
   <body>
      If you are not redirected automatically, click on the link
      <a href='http://<FortiAuthenticator-fqdn>/login/kerb-auth?user_continue_url=%%PROTURI%%'>
      http://<FortiAuthenticator-fqdn>/login/kerb-auth?user_continue_url= %%PROTURI%%
      </a>
   </body>
</html>
```

SAML authentication

Security Assertion Markup Language (SAML) is an XML standard that allows for maintaining a single repository for authentication amongst internal and/or external systems.

The FortiAuthenticator can act as a Service Provider (SP) to request user identity information from a third-party Identity Provider (IDP). This information can then be used to sign the user on transparently based on what information the IDP sends.

Multiple SAML SP portals can be created on the FortiAuthenticator, with each portal configured to a different SAML IDP.

In this scenario:

1. A user attempts to connect to the Internet via FortiGate.
2. The user is not authenticated in FSSO so gets redirected to FortiAuthenticator.
3. FortiAuthenticator (a service provider) checks with the existing third-party IDP to get the user identity.
4. FortiAuthenticator pushes identity and group information into FSSO.

5. FortiAuthenticator redirects the user to the original URL.
6. FortiGate sees the user in FSSO and allows the user to pass.

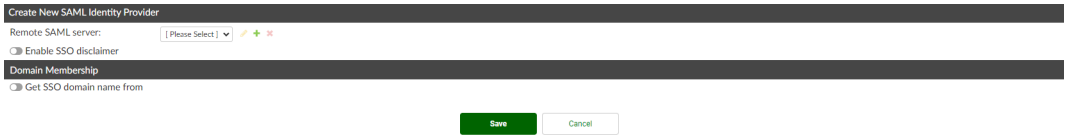
To configure a SAML SP portal, go to **Fortinet SSO > Methods > SAML Authentication**.

The following options are available:

Create New	Configure a new SAML SP portal.
Delete	Delete the selected SAML SP portals.
Edit	Edit the selected SAML SP portal.

To configure a new SAML SP portal:

1. From **Fortinet SSO > Methods > SAML Authentication**, select **Create New**.
   The **Create New SAML Identity Provider** window opens.



2. Configure the following settings:

Remote SAML server	Select a configured remote SAML server, or select **+** to configure a new remote SAML server. See SAML on page 186 for more information.
Enable SSO disclaimer	Select to require a SAML SP SSO end-user to agree to a disclaimer before they are redirected to the SAML IDP for authentication. The Login Disclaimer Page and Disclaimer Denied Page can be customized. See Replacement messages on page 69 for more information.
Domain Membership	
Get SSO domain name from	Select the method that determines the domain name: • **SAML assertion attribute**: Enable and enter the SAML assertion attribute that domain names are obtained from. • **Username prefix/suffix**: Enable to obtain the domain name specified in the username. For example: `user@domain`, `domain\user`, `domain/user` • **Explicitly set to**: Enable and enter the domain name to assign to the user.

3. Select **Save** to create the new SAML SP portal.

Windows event log

FortiAuthenticator must be configured to communicate with the domain controller if Active Directory (AD) will be used to ascertain group information.

A domain controller entry can be disabled without deleting its configuration. This can be useful when performing testing and troubleshooting, or when moving controllers within your network.

In order to properly discover the available domains and domain controllers, the DNS settings must specify a DNS server that can provide the IP addresses of the domain controllers. See DNS on page 44.

To add a domain controller:

1. Go to **Fortinet SSO > Methods > Windows Event Log**.
2. Select **Create New** to open the **Create New Windows Event Log Source** window.

3. Enter the following information:

NetBIOS name	Name of the domain controller as it appears in NetBIOS.
Display name	Unique name to easily identify this domain controller.
IP	Network IP address of the controller.
Account	Account name used to access logon events. The user must have read access to the logs using the built in AD security group "Event Log Readers."
Password	Password for the above account.
Server type	Select either **Domain controller** or **Exchange server** as the server type.
Disable	Disable the domain controller without losing any of its settings.
Priority	Define multiple domain controllers for the same domain. Each can be designated as **Primary** or **Secondary**. The **Primary** unit is accessed first.
Enable secure connection	Enable a secure connection over either **LDAPS** or **STARTTLS** with a **CA certificate**.

4. Select **Save**.
By default, FortiAuthenticator uses auto-discovery of Domain Controllers. If you want to restrict operation to the configured domain controllers only, go to **Fortinet SSO > Settings > Methods** and enable **Restrict auto-discovered domain controllers to configured Windows event log sources and remote LDAP servers**.
See Methods on page 250.

RADIUS accounting

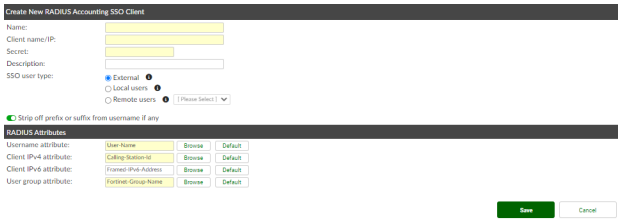
If required, SSO can be based on RADIUS accounting records. The FortiAuthenticator receives RADIUS accounting packets from a carrier RADIUS server or network device, such as a wireless controller, collects additional group information, and then inserts it into FSSO for use by multiple FortiGate devices for identity based policies.

The FortiAuthenticator must be configured as a RADIUS accounting client to the RADIUS server.

To view the RADIUS accounting SSO client list, go to **Fortinet SSO > Methods > RADIUS Accounting**.

To configure and enable a RADIUS accounting client:

1. From the RADIUS accounting SSO client list, select **Create New**. The **Create New RADIUS Accounting SSO Client** window opens.



2. Enter the following information:

Name	Enter a name in the **Name** field to identify the RADIUS accounting client on the FortiAuthenticator.
Client name/IP	Enter the RADIUS accounting client's FQDN or IP address.
Secret	Enter the RADIUS accounting client's pre-shared key.
Description	Optionally, enter a description of the client.
SSO user type	Specify the type of user that the client will provide: • **External**: Users not defined on FortiAuthenticator. User groups are retrieved from the source. • **Local users**: Users defined on FortiAuthenticator as local users. Users groups are retrieved from the local groups. • **Remote users**: Users defined on a remote LDAP server. User groups are retrieved form the remote LDAP server.  From the dropdown, select a remote LDAP server.
Strip off prefix or suffix from username if any	Enable to strip prefixes and suffixes from the SSO usernames.
RADIUS Attributes	If required, customize the username, client IP, and user group RADIUS attributes to match the ones used in the incoming RADIUS accounting records. See RADIUS attributes on page 137.

3. Select **Save** to apply the changes.

4. Enable RADIUS accounting SSO clients by going to **Fortinet SSO > Settings > Methods** and selecting **RADIUS Accounting SSO clients**. See Methods on page 250.

Syslog

The FortiAuthenticator can parse username and IP address information from a syslog feed from a third-party device, and inject this information into FSSO so it can be used in FortiGate identity based policies.

Syslog objects include sources and matching rules. Sources identify the entities sending the syslog messages, and matching rules extract the events from the syslog messages. Messages coming from non-configured sources will be dropped.

Injection of IPv6 addresses using Syslog-to-FSSO and API-to-FSSO is supported. IPv6 addresses are accepted by the backend parsing engine.

To configure syslog objects, go to **Fortinet SSO > Methods > Syslog**.

From the top, you can select from the following tabs:

- **Syslog Sources**
- **Matching Rules**

Syslog SSO must be enabled to configure syslog objects. Go to **Fortinet SSO > Settings > Methods** to enable **Syslog SSO**. See Methods on page 250.

The following options and information are available:

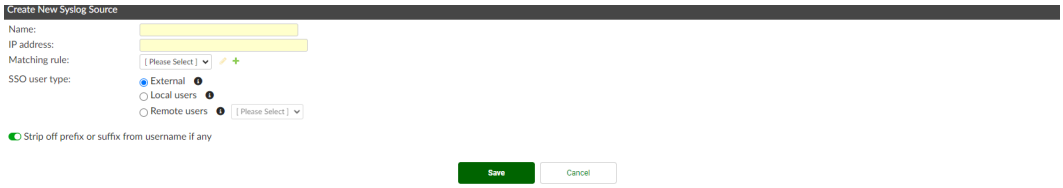
Create New	Create a new syslog source or matching rule.
Delete	Select to delete the selected object or objects.
Edit	Select to edit the selected object.
Reset column width	Select to reset the column widths to default.
Name	The name of the source.
IP Address	The IP address of the source.
Matching Rule	The matching rule for the source.
Syslog Matching Rule	The syslog matching rule.

Syslog sources

Each syslog source must be defined for the syslog daemon to accept traffic. Each source must also be configured with a matching rule (either pre-defined or custom built; see below), and syslog service must be enabled on the network interface(s) that will listen to remote syslog traffic.

To add a new syslog source:

1. Go to **Fortinet SSO > Methods > Syslog** and select **Syslog Sources** from the top.
2. Select **Create New**.
   The **Create New Syslog Source** window ones.



3. Enter the following information:

Name	Enter a name for the source.
IP address	Enter the IP address of the source.
TLS encryption	Enable to specify if TLS encryption is required. **Note**: This option is only available when **Allow TLS encryption** in **Syslog SSO** is enabled in **Fortinet SSO > Settings > Methods**. See Methods on page 250.
Matching rule	Select the requisite matching rule from the dropdown menu. A matching must already be created for the source.
SSO user type	Select the SSO user type: • **External**: Users are not defined on the FortiAuthenticator and user groups come from the source. • **Local users**: Users are defined on the FortiAuthenticator as local users, and user groups are retrieved from the local groups. Any group from the syslog messages are ignored. • **Remote users**: Users are defined on a remote LDAP server and user groups are retrieved from the LDAP server. Any group from the syslog messages are ignored.
Strip off prefix or suffix from username if any	Enable to strip prefixes and suffixes from the SSO usernames.
Use a different attribute when searching user in the remote LDAP server (other than the username attribute in the remote LDAP server config)	Enable and in **Remote LDAP user attribute**, enter a remote LDAP user attribute to use when searching a user in the remote LDAP server. **Note**: The option is only available when **SSO user type** is set to **Remote users**.

Use prefix or suffix in username as domain (other than the remote LDAP server domain)	Enable to use prefix or suffix in username as the domain. Once enabled, in **Default domain if not specified**, enter a default domain. **Note**: The option is only available when **SSO user type** is set to **Remote users**.

4. Select **Save** to add the source.

Matching rules

A matching rule is a query, or policy, that is applied to a syslog message in order to determine required information, such as the username and IP address. Rules are required for every syslog source.

Predefined rules are available for FortiNAC appliances, and Aruba and Cisco wireless controllers (see Predefined rules on page 265). For other systems, custom policies can be created to parse message files in various formats.

Predefined rules

Predefined matching rules are included for FortiNAC appliances, and Aruba and Cisco ACS or ISE wireless controllers.

Each field containing a variable (e.g. Client IPv4 and Client IPv6 fields) needs one or more characters after the {{:variable}} to let FortiAuthenticator know where to stop the parsing. Any combination of characters will work. The examples below use ",".

FortiNAC

Trigger	`FSSO`
Auth Type Indicators	**Logon:**`login` **Logoff:**`logout`
Username field	`username={{:username}},`
Client IPv4 field	`IP={{:client_ip}},`
Client IPv6 field	e.g. `Framed-IPv6-Address={{:client_ipv6}},`
Group field	`tags="{{:group}}"`
Group list separator	SSO syslog feed can parse multiple groups if the names are separated by a plus (**+**) symbol or a comma (**,**).

Aruba

Trigger	None; any logs are accepted.
Auth Type Indicators	**Logon:**`User Authentication Successful` (exact match required; no delimiter or value)
Username field	`username={{:username}},`
Client IPv4 field	`IP={{:client_ip}},`
Client IPv6 field	e.g. `Framed-IPv6-Address={{:client_ipv6}},`
Group field	`AAA profile={{:group}}`
Group list separator	SSO syslog feed can parse multiple groups if the names are separated by a plus (**+**) symbol or a comma (**,**).

Cisco

Trigger	`NOTICE Radius-Accounting`
Auth Type Indicators	**Logon:**`Acct-Status-Type=Start` **Update:**`Acct-Status-Type=Interim` **Logoff:**`Acct-Status-Type=Stop`
Username field	`User-Name={{:username}},`
Client IPv4 field	`Framed-IP-Address={{:client_ip}},`
Client IPv6 field	e.g. `Framed-IPv6-Address={{:client_ipv6}},`
Group field	e.g. `profile={{:group}}`
Group list separator	SSO syslog feed can parse multiple groups if the names are separated by a plus (**+**) symbol or a comma (**,**).

To create a new matching rule:

1. Go to **Fortinet SSO > Methods > Syslog** and select **Matching Rules** from the top.
2. Select **Create New**.
   The **Create New Syslog Matching Rule** page opens.
3. Enter the following information:

Name	Enter a name for the source.
Description	Optionally enter a description of the rule.

Mode	Select from the following two options: • **Key-value pairs**: parses syslog messages with key/value pairs. • **List of values**: parses syslog messages with a list of values.
Fields to Extract	Configure the fields to extract from the message.
Field separator	The field separator (default = ,). **Note**: The option is only available when the **Mode** is **List of values**.
Trigger	Optionally, enter a string that must be present in all syslog messages. This will act as a pre-filter (default = `NOTICE Radius-Accounting`). **Note**: The option is only available when the **Mode** is **Key-value pairs**.
Field position	Enter the position of the trigger field (default = 4). **Note**: The option is only available when the **Mode** is **List of values**.
Field value	Enter the value for the trigger field, e.g., USERID. **Note**: The option is only available when the **Mode** is **List of values**.
Auth Type Indicators	Enter strings to differentiate between the types of user activities: **Logon** (default = `Acct-Status-Type=Start`), **Update** (default = `Acct-Status-Type=Interim`) (optional), and **Logoff** (default = `Acct-Status-Type=Stop`) (optional). **Note**: The option is only available when the **Mode** is **Key-value pairs**.
Logon field position	Enter the **Logon** field position (default = 5). **Note**: The option is only available when the **Mode** is **List of values**.
Logon field value	Enter the **Logon** field value, e.g., login. **Note**: The option is only available when the **Mode** is **List of values**.
Update field position	Enter the **Update** field position (default = 0). **Note**: The option is only available when the **Mode** is **List of values**.
Update field value	Enter the **Update** field value. **Note**: The option is only available when the **Mode** is **List of values**.
Logoff field position	Enter the **Logoff** field position (default = 0). **Note**: The option is only available when the **Mode** is **List of values**.
Logoff field value	Enter the **Logoff** field value.

	Note: The option is only available when the **Mode** is **List of values**.
Username field	Define the semantics of the username field. For example: `User-Name={{:username}}`, where `{{:username}}` indicates where the username is extracted from. **Note**: The option is only available when the **Mode** is **Key-value pairs**.
Username field position	Enter the username field position (default = 10). **Note**: The option is only available when the **Mode** is **List of values**.
Client IPv4 field	Define the semantics of the client IPv4 address (default = `Framed-IP-Address={{:client_ip}},`). **Note**: The option is only available when the **Mode** is **Key-value pairs**.
Client IPv4 field position	Enter the client IPv4 field position (default = 9). **Note**: The option is only available when the **Mode** is **List of values**.
Client IPv6 field	Define the semantics of the client IPv6 address (default = `Framed-IPv6-Address={{:client_ipv6}},`). **Note**: The option is only available when the **Mode** is **Key-value pairs**.
Client IPv6 field position	Enter the client IPv6 field position (default = 0). **Note**: The option is only available when the **Mode** is **List of values**.
Group field	Optionally, define the semantics of the group. The group may not always be included in the syslog message, and may need to be retrieved from a remote LDAP server, e.g., `profile = {{:group}}`. **Note**: The option is only available when the **Mode** is **Key-value pairs**.
Group field position	Enter the group field position (default = 0). **Note**: The option is only available when the **Mode** is **List of values**.
Group list separator	Specify the separator (default = ,).
Test Rule	Paste a sample log message into the text box, then select **Test** to test that the desired fields are correctly extracted.

4. Select **Save** to add the new matching rule.

Filtering

Go to **Fortinet SSO > Filtering** to access the following FSSO filtering tabs:

SSO users

To manage SSO users, go to **Fortinet SSO > Filtering > SSO Users**.

The following options are available:

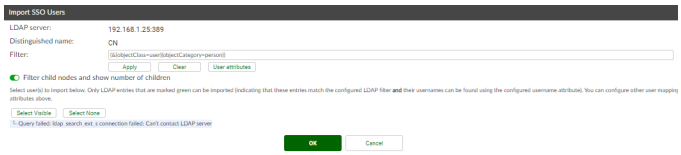
Create New	Select to create a new user. In the **Create New SSO User** window: 1. Enter a name for the user. 2. Select **Save**.
Import	Import SSO users from a remote LDAP server.
Delete	Delete the selected users.
Edit	Edit the selected user.
Name	The SSO user name.
Created/Imported	Displays whether or not the user was created or imported.

To import SSO users:

1. In the **SSO Users** list, select **Import**.
   - In the **Import SSO Users** window, select whether to import the **DN** or **Username**, and select a remote LDAP server from the **Remote LDAP Server** dropdown menu, then select **Import**.

An LDAP server must already be configured to select it in the dropdown menu. See LDAP service on page 213 for more information on adding a remote LDAP server.

The **Import SSO Users** window opens in a new browser window.



The **Distinguished name** field is automatically filled when you select a remote LDAP server from the **Remote LDAP Server** dropdown.

2. Optionally, enter a **Filter** string to reduce the number of entries returned, and then select **Apply**, or select **Clear** to clear the filters.
   For example, `uid=j*` returns only user IDs beginning with "j".
3. The default configuration imports the attributes commonly associated with Microsoft Active Directory LDAP implementations. Select **User attributes** to edit the remote LDAP user mapping attributes.
   Selecting the field, **FirstName** for example, presents a list of attributes which have been detected and can be selected. This list is not exhaustive; other non-displayed attributes may be available for import. Consult your LDAP administrator for a list of available attributes.
4. Select the entries you want to import.
5. Click **OK**.
6. Click **Save**.

SSO groups

To manage SSO groups, go to **Fortinet SSO > Filtering > SSO Groups**.

The following options are available:

Create New	Select to create a new group. In the **Create New SSO Group** window: 1. Enter a name for the SSO group. 2. In **Azure UUID**, enter the Azure Universally Unique Identifier (UUID). 3. Select **Save**.
Import	Import SSO groups from a remote LDAP server.
Delete	Delete the selected groups.
Edit	Edit the selected group.
Name	The SSO group name.
Created/Imported	Displays whether or not the user group was created or imported.

FortiAuthenticator SSO user groups cannot be used directly in a security policy on a FortiGate device.

An FSSO user group must be created on the FortiGate unit, then the FortiAuthenticator SSO groups must be added to it.

FortiGate FSSO user groups are available for selection in identity-based security policies.

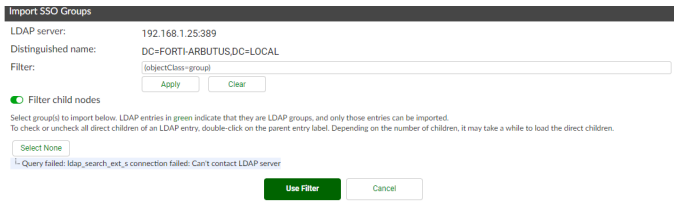
To import SSO groups:

1. In the **SSO Groups** list, select **Import**.
   - In the **Import SSO Groups** window, select a remote LDAP server from the **Remote LDAP Server** dropdown menu and select **Import**. Alternatively, select **Azure ADFS** and specify the **Graph API Service Root**, **Client ID**, and **Client key**.

   To be able to select a remote SAML server, you must enable SAML portal service.

   An LDAP server must already be configured to select it in the dropdown menu. See LDAP service on page 213 for more information on adding a remote LDAP server.

   The **Import SSO Groups** window opens in a new browser window.



   The **Distinguished name** field is automatically filled when you select a remote LDAP server from the **Remote LDAP Server** dropdown.

2. Optionally, enter a **Filter** string to reduce the number of entries returned, and then select **Apply**, or select **Clear** to clear the filters.
   For example, `uid=j*` returns only user IDs beginning with “j”.
3. The default configuration imports the attributes commonly associated with Microsoft Active Directory LDAP implementations. Select **User attributes** to edit the remote LDAP user mapping attributes.
   Selecting the field, **FirstName** for example, presents a list of attributes which have been detected and can be selected. This list is not exhaustive; other non-displayed attributes may be available for import. Consult your LDAP administrator for a list of available attributes.
4. Select the entries you want to import.
5. Click **OK**.
6. Click **Save**.

Fine-grained controls

The **Fine-grained Controls** menu provides options to include or exclude a user or group from SSO, and set the maximum number of concurrent sessions that a user or group can have.

To adjust the controls, go to **Fortinet SSO > Filtering > Fine-grained Controls**.

The following options are available:

Clear Configuration	Clear the SSO configuration for the selected users or groups.
Include in SSO	Select a user or users, then select **Include in SSO** to include the selected users in SSO.
SSO Type	Select the SSO type to view from the dropdown menu. The options are: **Local Users**, **Local Groups**, **SSO Users**, and **SSO Groups**.
SSO Name	The users' or groups' names. Select the column title to sort the list by this column.
Maximum Concurrent Sessions	The maximum concurrent sessions allowed for the user or group. This number cannot be greater than five.
Excluded from SSO	If the user or group is excluded from SSO, a red circle with a line is displayed.

To edit an SSO user or group:

1. In the **Fine-grained Controls** window, click the SSO user or group to edit.
   The **Edit SSO Fine-grained Control Item** window opens.
2. Enter the maximum number of concurrent SSO logon sessions per user that the user or group is allowed to have. Enter `0` for unlimited. The value must be less than or equal to five.
3. Select **Save** to apply the changes.

Domain groupings

Domain groupings enable you to identify and group together SSO sessions from domains belonging to a specific FortiGate or virtual domain (VDOM). This is useful in environments where the networks behind each FortiGate or VDOM have their own set of users and IP subnets. Domain groupings allow the FortiAuthenticator to return only the SSO sessions belonging to users from a specific FortiGate or VDOM.

To manage domain groupings, go to **Fortinet SSO > Filtering > Domain Groupings**.

The following options are available:

Create New	Configure a new domain grouping.
Delete	Delete the selected domain groupings.
Edit	Edit the selected domain grouping.
Name	The name of the domain grouping.
Description	A description of the domain grouping.
Domains	A list of domains that belong to the domain grouping.

Logins from domains that do not belong to any other configured domain grouping are assigned to the Default domain grouping.

To create a new domain grouping:

1. From the Domain Groupings list, select **Create New**.
   The **Create New Domain Grouping** window opens.
2. Enter the following information:

Name	Enter a name for the domain grouping.
Description	Optionally, enter a description for the domain grouping.
Domain list	Enter the domains that belong to the domain grouping, separated with commas or line breaks. **Note**: A domain can only belong to one domain grouping.

3. Select **Save** to create the new domain grouping.
   After domain groupings are defined, the SSO sessions list displays the corresponding domain grouping of each SSO session. See SSO on page 279 for more information.

FortiGate

If you are providing FSSO to only certain groups on a remote LDAP server, you can filter the polling information so that it includes only those groups, or organizational units (OU).

To view a list of the FortiGate group filters, go to **Fortinet SSO > Filtering > FortiGate**.

To create a new filter:

1. From the FortiGate filters select **Create New**.
   The **Create New FortiGate Filter** window opens.
2. Enter the following information:

Name	Enter a name in the **Name** field to identify the filter.
FortiGate name/IP	Enter the FortiGate unit's FQDN or IP address.
Description	Optionally, enter a description of the filter.
IP Filtering	Select to enable IP filtering for this service and from the dropdown, select IP filtering rules. **Note**: If you have not yet configured IP filtering rules, you can create them in **Fortinet SSO > Filtering > IP Rules** (see IP rules on page 274 for more information).
Domain Grouping Filtering	Select to enable forwarding FSSO information for users from only the selected domain groupings. See Domain groupings on page 272 for more information.
Fortinet Single Sign-On (FSSO)	Select to enable forwarding FSSO information for users from only the specific subset of users, groups, or containers. Select from the following options: • **Add Filtering Object**: Enter the name and select an object type from the following:

- **Group:** Specifies the DN of a group. All users who are members of that group must be included in SSO.
- **Group container:** Specifies the DN of an LDAP container, e.g. OU. All users who are members of a group under that container or one of its sub-containers must be included in SSO.
- **User:** Specifies the DN of a user. This user must be included in SSO.
- **User container:** Specifies the DN of an LDAP container, e.g. OU. All users who are under that container or one of its sub-containers must be included in SSO.
- **User and group container:** Specifies the DN of an LDAP container, e.g. OU. It is the union of the user and the group containers.

- **Import from LDAP server**:
  In the **Import Remote LDAP Objects** window:
  a. Enable **Exclude users** to exclude users from the FortiGate filter.
  b. From the **Remote LDAP server** dropdown, select an LDAP server.
  c. Click **OK**.
- **Select from SSO users/groups**:
  In **Select SSO Objects**:
  a. From **SSO Groups**, select groups from the **Available Groups** list and move them to the **Chosen Groups** list.
  b. From **SSO Users**, select groups and move them to the **Chosen Users** list.
  c. From **Remote LDAP Groups**, select FortiAuthenticator LDAP groups from the **Available Groups** list and move them to the **Chosen Groups** list.
  d. Click **Save**.
- **Import from Azure AD**:
  In **Select Azure Groups**:
  a. From the **OAuth server** dropdown, select an OAuth server.
  b. From **Azure Groups**, select groups from the **Available Azure Groups** list and move them to the **Chosen Azure Groups** list.
  c. Click **Save**.
  This allows you to import native Microsoft Entra ID (formerly Azure AD) groups.

3. Select **Save** to create the new FortiGate group filter.

IP rules

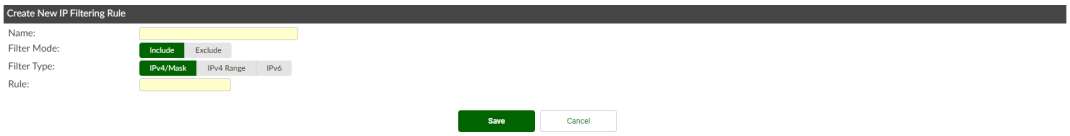
The user logon information sent to FortiGate units can be restricted to specific IP addresses or address ranges. If no filters are defined, information is sent for all addresses.

When created, IP filtering rules must be assigned to FortiGate filters under **Fortinet SSO > Filtering > FortiGate** (see FortiGate on page 273 for more information).

To view the list of the IP filtering rules, go to **Fortinet SSO > Filtering > IP Rules**.

To create new IP filtering rules:

1. From the IP filtering rules list, select **Create New**.
   The **Create New IP Filtering Rule** window opens.



2. Enter the following information:

Name	Enter a name for the rule.
Filter Mode	Either **Include** or **Exclude** the defined IPs in SSO.
Filter Type	Select whether the rule will specify an IPv4 address and netmask, an IPv6 address range, or an IPv6 address.
Rule	Enter either an IP address and netmask or an IP address range (depending on the selected filter type). For example: • IPv4 address/mask: `10.0.0.1/255.255.255.0` • IP range: `10.0.0.1/10.0.0.99` • IPv6: `2001:db8:1ced:f00d::/128`

3. Select **Save** to create the new IP filtering rule.

FortiClient SSO Mobility Agent

The FortiClient SSO Mobility Agent is a feature of FortiClient Endpoint Security. The agent automatically provides user name and IP address information to FortiAuthenticator for transparent authentication. IP address changes are automatically sent to the FortiAuthenticator. When the user logs off or otherwise disconnects from the network, FortiAuthenticator is aware of this and deauthenticates the user.

The FortiClient SSO Mobility Agent Service must be enabled in **Fortinet SSO > Settings > Methods**.

See FortiClient SSO Mobility Agent Service on page 251.

Setup of the FortiClient SSO Mobility Agent uses standard Msiexec installation switches as well as FortiClient SSO switches, including **SSOSERVER**, **SSOPORT**, and **SSOPSK**. For example: `FortiClientSSO.msi /qn /i SSOSERVER="1.2.3.4" SSOPORT="8001" SSOPSK="pre_shared_key"`.

SSOSERVER="1.2.3.4", **SSOPORT="8001"**, and **SSOPSK="pre_shared_key"** are the only switches that the installer supports for SSO.

For additional Msiexec installation switches, see Microsoft's documentation on command-line options.

For information on configuring FortiClient, see the FortiClient Administration Guide for your device.

Fake client protection

Some attacks are based on a user authenticating to an unauthorized AD server in order to spoof a legitimate user logon through the FortiClient SSO Mobility Agent. You can prevent this type of attack by enabling **NTLM authentication** (see FortiGate on page 247).

FortiAuthenticator will initiate NTLM authentication with the client, proxying the communications only to the legitimate AD servers it is configured to use.

If NTLM is enabled, FortiAuthenticator requires NTLM authentication when:

- The user logs on to a workstation for the first time,
- The user logs off and then logs on again,
- The workstation IP address changes,
- The workstation user changes,
- And NTLM authentication expires (user configurable).

FortiClient SSO Mobility Agent deployment support

Standalone (Windows Only)

The FortiClient SSO Mobility Agent can be installed outside of FortiClient using `FortiClientSSOSetup_XXX.zip`.

`FortiClientSSOSetup_XXX.zip` can be packaged with `FortiClientSSOConfigurationTool` for deployment.

Note: This is only possible when no other FortiClient instances are present on the machine.

FortiClient (MacOS and Windows)

In this case, the SSOMA feature can be configured from FortiClient EMS.

See Configuring SSOMA with AD in the latest EMS Administration Guide.

Multiple FortiAuthenticator

To provide redundancy, each agent can update multiple FortiAuthenticator instances at the same time.

To do so, multiple destinations need to be configured within the agent (either IP address or FQDN) separated with ";".

They all have to share the same PSK:

`FAC1;FAC2;FAC3;FAC4`

or

`FAC1:PORT1;FAC2:PORT2;FAC3`

Troubleshooting the standalone agent

The standalone agent does not provide GUI, so to change the log level, change the following registry keys:

```
\Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Fortinet\FortiClient\FA_SSOMA
logenenabled=1
loglevel=7 (debug)
```

Once the issue is replicated, you can export the logs:

```
"C:\Program Files\Fortinet\FortiClient\FCDBLog.exe” -f PATH_TO_FILE
```

RADIUS Single Sign-On

A FortiGate or FortiMail unit can transparently identify users who have already authenticated on an external RADIUS server by parsing RADIUS accounting records. However, this approach has potential difficulties:

- The RADIUS server is business-critical IT infrastructure, limiting the changes that can be made to the server configuration.
- In some cases, the server can send accounting records only to a single endpoint. Some network topologies may require multiple endpoints.

The FortiAuthenticator RADIUS accounting proxy overcomes these limitations by proxying the RADIUS accounting records, modifying them, and replicating them to the multiple subscribing endpoints as needed. See Accounting proxy on page 202.

Starting FortiAuthenticator 6.5.0, the accounting proxy settings are now available in the RADIUS service on page 189.

Monitoring

The **Monitor** menu tree provides options for monitoring SSO and authentication activity.

For more information, see SSO on page 279 and Authentication on page 282.

SSO

FortiAuthenticator can monitor the units that make up FSSO. This is useful to ensure there is a connection to the different components when troubleshooting.

Domains

To monitor SSO domains, go to **Monitor > SSO > Domains**. Select **Refresh** to refresh the domain list. Select **Expand All** to expand all of the listed domains, or **Collapse All** to collapse the view.

All configured domain controllers appear in the domain list. Each domain controller is displayed in:

- green if the last connection attempt was successful.
- gray if no recent connection information is available.
- red if the last connection attempt failed.

Hold the pointer over a domain controller to view the status of the last LDAP query, how long ago it was, and the LDAP query's response time in milliseconds (ms). This response time will show a warning icon if the highest recent response time is above 500 ms.

In addition, you can click on the domain controller entry to view statistics for the 100-most recent LDAP queries. The listed response times are color coordinated as follows: green for less than 500 ms, orange for between 500 and 1000 ms, and red for more than, or equal to, 1000 ms.

SSO sessions

To monitor SSO sessions, go to **Monitor > SSO > SSO Sessions**. Users can be manually logged off of if required.

The following information is available:

Refresh	Refresh the SSO sessions list.
Logoff All	Log off all of the connected users.
Logoff Selected	Log off only the selected users.

Search	Enter a search term in the search field, then select **Search** to search the SSO sessions list.
Filter	Filter the SSO session list by the source of the connection and/or by Domain Group. To view SSO sessions not associated with any configured domain grouping, select **Default**.
Logon Time	When the session was started.
Update Time	When the session was last updated.
Workstation	The workstation that the user is using.
IP address	The IP address of the workstation.
Domain Grouping	The domain group to which the domain belongs.
Domain	The domain to which the user belongs.
Username	The username of the user.
Source	The source of the connection.
Group	The group to which the user belongs.

Windows event log sources

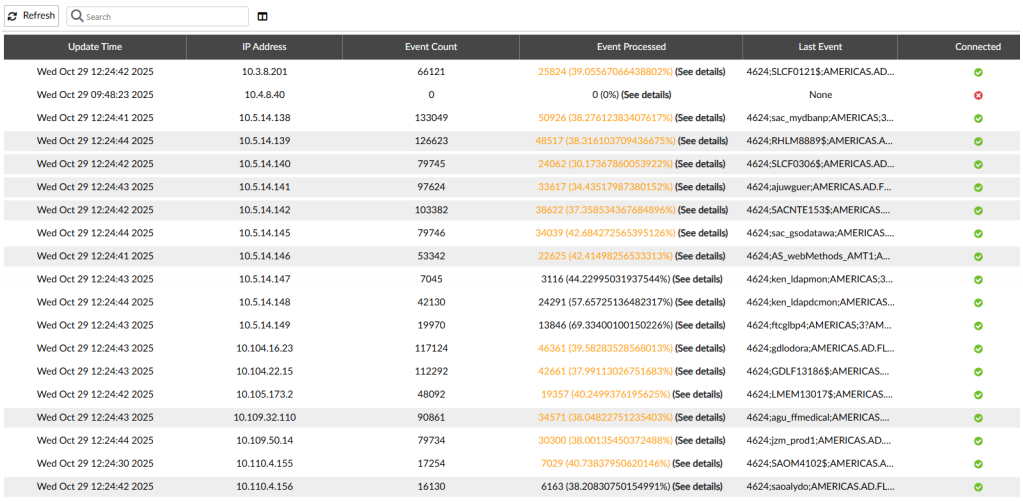
Windows event log sources can be viewed by going to **Monitor > SSO > Windows Event Log Sources**.

The sources list can be refreshed by selecting **Refresh**, and searched using the search field.

The list shows the total number of events, as well as the most recent event.

Color coding for events

When there are `10000` or more unprocessed FSSO events with a processing ratio below `50 %`, the **Event Processed** column entry is highlighted in orange.


Refresh Search

Update Time	IP Address	Event Count	Event Processed	Last Event	Connected
Wed Oct 29 12:24:42 2025	10.3.8.201	66121	25824 (39.0556706643880 2%) (See details)	4624;SLCF0121$;AMERICAS.AD...	✓
Wed Oct 29 09:48:23 2025	10.4.8.40	0	0 (0%) (See details)	None	✗
Wed Oct 29 12:24:41 2025	10.5.14.138	133049	50926 (38.2761238340761 7%) (See details)	4624;sac_mydbanp;AMERICAS;3...	✓
Wed Oct 29 12:24:44 2025	10.5.14.139	126623	48517 (38.3161037094366 75%) (See details)	4624;RHLM8889$;AMERICAS.A...	✓
Wed Oct 29 12:24:42 2025	10.5.14.140	79745	24062 (30.1736786005392 2%) (See details)	4624;SLCF0306$;AMERICAS.AD...	✓
Wed Oct 29 12:24:43 2025	10.5.14.141	97624	33617 (34.4351798738015 2%) (See details)	4624;ajuwguer;AMERICAS.AD.F...	✓
Wed Oct 29 12:24:42 2025	10.5.14.142	103382	38622 (37.3585343676848 96%) (See details)	4624;SACNTE153$;AMERICAS....	✓
Wed Oct 29 12:24:44 2025	10.5.14.145	79746	34039 (42.6842725653951 26%) (See details)	4624;sac_gsodatawa;AMERICAS....	✓
Wed Oct 29 12:24:41 2025	10.5.14.146	53342	22625 (42.4149825653331 3%) (See details)	4624;AS_webMethods_AMT1;A...	✓
Wed Oct 29 12:24:43 2025	10.5.14.147	7045	3116 (44.229950319375 44%) (See details)	4624;ken_ldapmon;AMERICAS;3...	✓
Wed Oct 29 12:24:44 2025	10.5.14.148	42130	24291 (57.657251364823 17%) (See details)	4624;ken_ldapdcmon;AMERICAS...	✓
Wed Oct 29 12:24:43 2025	10.5.14.149	19970	13846 (69.334001001502 26%) (See details)	4624;ftcglbp4;AMERICAS;3?AM...	✓
Wed Oct 29 12:24:43 2025	10.104.16.23	117124	46361 (39.5828352856801 3%) (See details)	4624;gdllodora;AMERICAS.AD.FL...	✓
Wed Oct 29 12:24:43 2025	10.104.22.15	112292	42661 (37.9911302675168 3%) (See details)	4624;GDLF13186$;AMERICAS....	✓
Wed Oct 29 12:24:42 2025	10.105.173.2	48092	19357 (40.2499376195625 %) (See details)	4624;LMEM13017$;AMERICAS....	✓
Wed Oct 29 12:24:43 2025	10.109.32.110	90861	34571 (38.0482275123540 3%) (See details)	4624;agu_ffmedical;AMERICAS....	✓
Wed Oct 29 12:24:44 2025	10.109.50.14	79734	30300 (38.0013545037248 8%) (See details)	4624;jzm_prod1;AMERICAS.AD....	✓
Wed Oct 29 12:24:30 2025	10.110.4.155	17254	7029 (40.7383795062014 6%) (See details)	4624;SAOM4102$;AMERICAS.A...	✓
Wed Oct 29 12:24:42 2025	10.110.4.156	16130	6163 (38.2083075015499 1%) (See details)	4624;saoalydo;AMERICAS.AD.FL....	✓

When there are `10000` or more unprocessed FSSO events with a processing ratio below `20 %`, the **Event Processed** column entry is highlighted in red.

FortiGates

FortiGate units that are registered with FortiAuthenticator can be viewed at **Monitor > SSO > FortiGates**.

The list can be refreshed by selecting **Refresh** and searched using the search field. The list shows the connection time of each device, as well as its IP address and serial number.

User authentication events are logged in the FortiGate event log. See the FortiGate Handbook for more information.

DC/TS agents

Domain controller (DC) agents and terminal server (TS) agents that are registered with FortiAuthenticator can be viewed at **Monitor > SSO > DC/TS Agents**.

The list can be refreshed by selecting **Refresh** and searched using the search field.

The list shows the server name of each agent, as well as its IP address, its agent type, last connection time, connection status, and the number of logged-on users.

When FortiAuthenticator communicates with TS/DC agents:

- There is no limit for UDP connections.
- A maximum of 2048 concurrent TCP/TLS connections are allowed.

For TCP/TLS connections, TS/DC agent connects, provides FSSO session information, and disconnects after 30 seconds if there is no new FSSO session to report.

NTLM statistics

Dumped NTLM statistics can be viewed at **Monitor > SSO > NTLM Statistics**.

The statistics can be refreshed and cleared by selecting **Refresh** and **Clear** respectively.

Authentication

Locked-out source IP addresses, locked out/inactive users, RADIUS sessions, the Windows AD server and device login sessions, learned RADIUS users, SAML IdP sessions, and OAuth sessions can be monitored under **Monitor > Authentication**.

Locked-out IP addresses

To view the locked-out source IP addresses, go to **Monitor > Authentication > Locked-out IP Addresses**.

The source IP address and the remaining lockout period in seconds are displayed for every locked-out source.

To unlock a source IP address from the list, select the IP address and select **Unlock**. The list can be refreshed by selecting **Refresh**, and searched using the search field.

For more information on locked-out source IP addresses, see **Maximum failed administrator login attempts** and **Administrator login lockout period** options in System access on page 48 and **IP Lockout Policy Settings** pane in Lockouts on page 85.

Locked-out users

To view the locked-out users, go to **Monitor > Authentication > Locked-out Users**.

To unlock a user from the list, select the user and select **Unlock**. The list can be refreshed by selecting **Refresh**, and searched using the search field.

The list shows the username, server, the reason the user was locked out, and when their lock-out expires.

For more information on locked-out users, see Top user lockouts widget on page 40, Lockouts on page 85, and User management on page 94.

RADIUS sessions

You can monitor RADIUS activity and log out users.

To view currently active RADIUS accounting sessions, go to **Monitor > Authentication > RADIUS Sessions**.

The page shows the user's name, type, IP address, MAC address, and RADIUS client, duration, and data usage columns. More specifically, Accounting-Start Interim-Update packets are received. A user session is removed from this

table after the Accounting-Stop packet is received, or the session doesn't receive any RADIUS accounting packets before the timeout period expires.

To log out a user as an admin, select the user from the table and select **Logoff**.

There are two pages to view: **Active** and **Cumulative**. Select **Cumulative** to view statistics for user who have a time and/or data usage limit. This information may be accumulated through a succession of RADIUS accounting sessions. A user's stats are removed when explicitly deleted by the administrator (by selecting the user and selecting **Delete**), or when the user's account itself is deleted.

Select **Clear** to clear the cumulative RADIUS accounting sessions in the **Cumulative** tab.

While administrators can log out users, they can also reset a user's time and/or data usage using **Reset Usage**.

For more information on user time and data usage limits, see Usage profile on page 129.

RADIUS accounting sessions can be configured to timeout after a specific time period has been reached. To do so, see General.

RADIUS accounting features

FortiAuthenticator offers three separate RADIUS accounting features:

1. RADIUS accounting proxy: As the name implies, this feature relays, i.e., proxies RADIUS accounting messages between external RADIUS accounting clients and servers. Depending on its configuration, FortiAuthenticator may add/delete/modify the attributes of the RADIUS accounting requests it proxies.
2. RADIUS accounting for FSSO: FortiAuthenticator uses the RADIUS session information from the RADIUS accounting requests to detect end-user logins, logouts, and IP address updates to create/update/delete FSSO sessions.
3. RADIUS accounting for usage profile: FortiAuthenticator uses the RADIUS session information from the RADIUS accounting requests to track and restrict end-users' time and/or data usage.

Features 1 and 2 process the RADIUS accounting messages received on the UDP port specified by the **Accounting SSO port** option in **Authentication > RADIUS Service > Services**.

Feature 3 processes the RADIUS accounting messages received on the UDP port specified by the **Accounting monitor port** option in **Authentication > RADIUS Service > Services**.

Windows AD

FortiAuthenticator supports multiple Windows AD server forests, as shown below. A maximum of 20 remote LDAP servers with Windows AD enabled can be configured at once. In addition, you can see when the server was last updated, and an option to reset the connection for individual servers.

To view Windows AD server information, go to **Monitor > Authentication > Windows AD**.

To refresh the connection, select **Refresh** in the toolbar. The server name, IP address, authentication realm, agent, and connection are shown.

Windows device logins

To view the Windows device logins, go to **Monitor > Authentication > Windows Device Logins**.

To refresh the list, select **Refresh** in the toolbar. See Machine authentication on page 82 for more information.

Learned RADIUS users

Learned RADIUS users are users that have been learned by the FortiAuthenticator after they have authenticated against a remote RADIUS server.

For information on enabling learning RADIUS users, see RADIUS on page 183.

SAML IdP sessions

This page monitors active sessions of SAML IdP logged-in users. The monitoring page displays a list of all the active sessions in a table format with each row containing the key information of the session.

To view currently active SAML sessions, go to **Monitor > Authentication > SAML IdP Sessions**.

The page shows the user's name, type, IP address, MAC address, authentication time, and validity period.

You can search for active SAML IdP sessions by username or IP address in the search field.

The following options are available for each SAML IdP session:

Logoff All	Log out all sessions after confirmation. Always enabled.
Logoff Selected	Log out selected sessions after confirmation. Only enabled when some sessions are selected.

Selecting an active session opens the **SAML IdP session Details**. Session details include the following information:

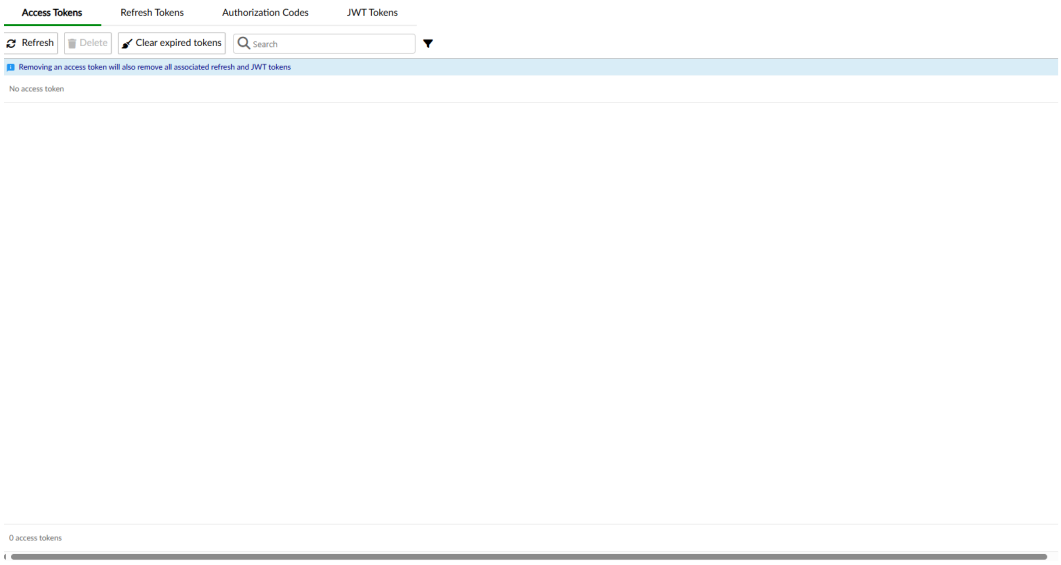
User Info	
Username	The username of the user.
User type	The user type (local or remote).
User IP	The user's IP address.
Session valid	The session validity period (start and end time).
Authentication factor	The authentication factors used (password, token, etc.).
User Attributes	Lists the user attributes and their values associated with this session.
Service Providers	

Name	The name of the service provider.
Time of Request	The time the SAML request was made.
Certificate Subject	Identifies the certificate subject of the SAML request.

OAuth sessions

This page monitors active OAuth tokens. The monitoring page displays a list of all the active OAuth tokens in a table format.

To view currently active OAuth tokens, go to **Monitor > Authentication > OAuth Sessions**.



The following tabs are displayed:

- **Access Tokens**: Displays access tokens.
- **Refresh Tokens**: Displays refresh tokens linked to every access token.
- **Authorization Codes**: Displays authorization grants associated with the issued tokens.
- **JWT Tokens**: Displays JWT tokens associated with the issued tokens.

The following options are available:

Refresh	Select to refresh the page.
Delete	Select to delete the selected tokens.
Clear expired tokens	Select to delete the expired OAuth tokens from the list.
Clear expired and revoked tokens	Select to delete the revoked and expired OAuth tokens from the list.
Search	Enter a search term in the search field, then select **Search** to search the tokens list.
Filter	Filter the tokens by the grant type or the status.

By Grant Type

- **All**
- **Password-based**
- **Authorization code**
- **Authorization code with PKCE**

By Status

- **All**
- **Expired**
- **Active**

Note: Not all options are available in every tab.

Certificate management

This section describes managing certificates with the FortiAuthenticator device.

FortiAuthenticator can act as a CA for the creation and signing of X.509 certificates, such as server certificates for HTTPS and SSH, and client certificates for HTTPS, SSL, and IPsec VPN.

The FortiAuthenticator unit has several roles that involve certificates:

Certificate authority	The administrator generates CA certificates that can validate the user certificates generated on this FortiAuthenticator. The administrator can import other authorities' CA certificates and Certificate Revocation Lists (CRLs), as well as generate, sign, and revoke user certificates. See End entities on page 288 for more information.
SCEP server	A SCEP client can retrieve any of the local CA certificates (Local CAs on page 299), and can have its own user certificate signed by the FortiAuthenticator device's CA.
CMP server	CMPv2 is a Certificate Management Protocol designed by Safenet for the secure signing of digital certificates and complete certificate life cycle management.
Remote LDAP authentication	Acting as an LDAP client, FortiAuthenticator can authenticate users against an external LDAP server. It verifies the identity of the external LDAP server by using a trusted CA certificate. See Trusted CAs on page 307 for more information.
EAP authentication	FortiAuthenticator can check that the client's certificate is signed by one of the configured authorized CA certificates (see Certificate authorities on page 299). The client certificate must also match one of the user certificates (see End entities on page 288).

Any changes made to certificates generate log entries that can be viewed under **Logging > Log Access > Logs**.

See Logging on page 319.

Policies

The policies section includes global configuration settings which are applied across all CAs and end-entity certificates created on FortiAuthenticator.

General

Certificate expiration settings can be configured under **Certificate Management > Policies > General**.

When **Delete user certificate's private key once downloaded** is enabled, the user certificate private keys generated by FortiAuthenticator are deleted after they are downloaded for distribution to the endpoint.

This is a secure configuration when the certificate/key distribution model does not require redownloading the private keys after the initial distribution.

Note: The **Delete user certificate's private key once downloaded** is enabled by default.

The **Delete user certificate's private key once downloaded** setting affects whether the private key in the **Users** tab (downloaded using **Export Key Cert**) in **Certificate Management > End Entities** is deleted.

See End entities on page 288.

Enable **Warn when a certificate is about to expire** to configure the following:

Send a warning email	Enter the number of days before the certificate expires that the email will be sent (0 - 365, default = 7).
Administrator's email	Enter the email address to which the expiry warning message are sent to.

Select **Save** to apply any configuration changes.

End entities

User and server certificates are required for mutual authentication on many HTTPS, SSL, and IPsec VPN network resources. You can create a user certificate on the FortiAuthenticator device, or import and sign a CSR. User certificates, client certificates, or local computer certificates are all the same type of certificate.

To view the user certificate list, go to **Certificate Management > End Entities > Users**.

To view the server certificate list, go to **Certificate Management > End Entities > Local Services**.

The following information is available:

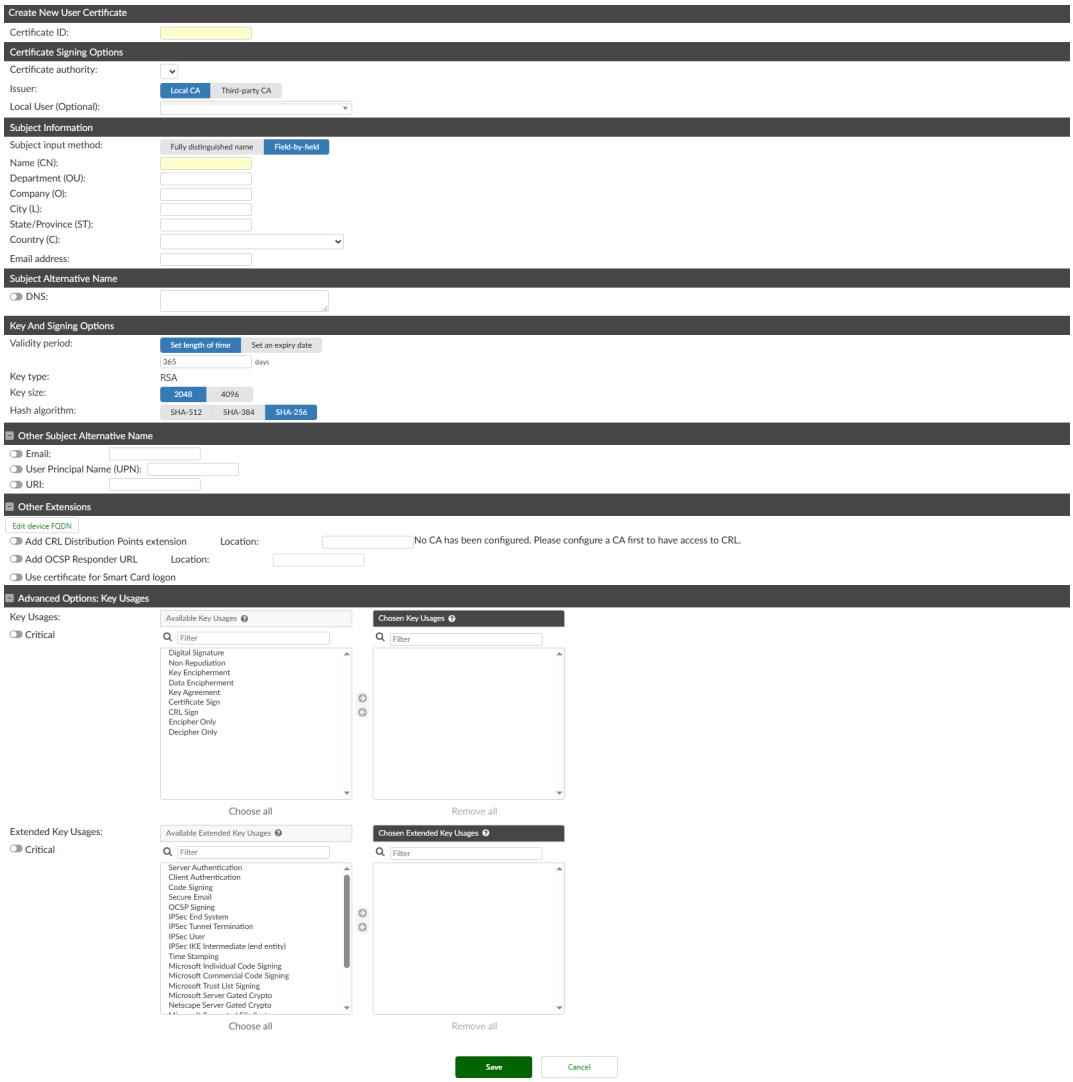
Create New	Create a new certificate.

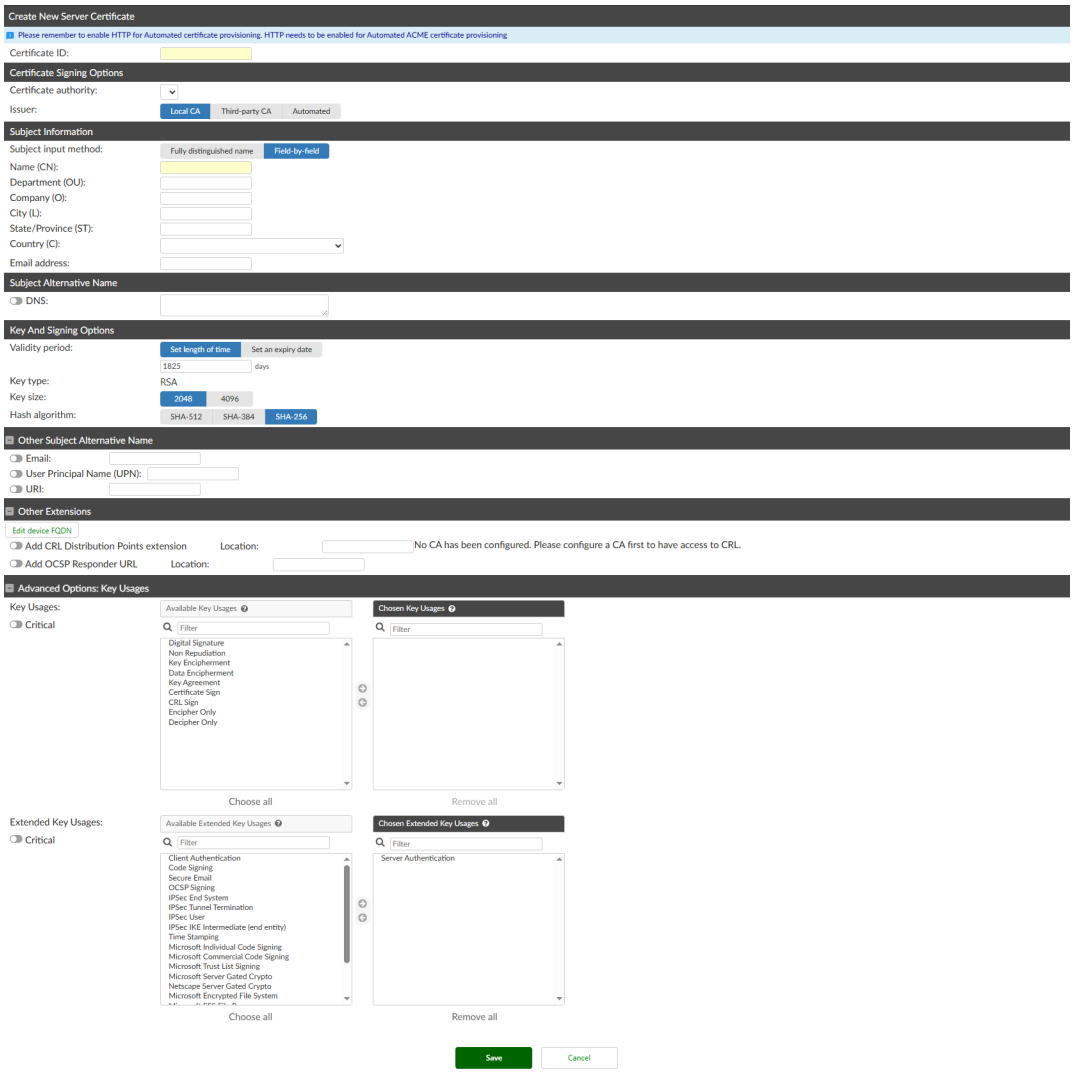
Import	Select to import a certificate signed by a third-party CA for a previously generated CSR (see To import a local user certificate: on page 296 and To import a server certificate: on page 296) or to import a CSR to sign (see To import a CSR to sign: on page 296).
Revoke	Revoke the selected certificate. See To revoke a certificate: on page 298.
Delete	Delete the selected certificate.
Export Certificate	Save the selected certificate to your computer.
Export Key and Cert	Export the PKCS#12. This is only available for user certificates. See **Delete user certificate's private key once downloaded** in Policies on page 287.
Search	Enter a search term in the search field, then press Enter to search the certificate list.
Filter	Select to filter the displayed certificates by status. The available selections are: **Active and Pending**, **Pending**, **Pending**, **Expired**, **Revoked**, **Active**, and **All**. By default, only valid (active and pending) certificates are shown.
Certificate ID	The certificate ID.
Subject	The certificate subject.
Issuer	The issuer of the certificate.
Status	The status of the certificate.
Expiry	The expiration date of the certificate.

Certificates can be created, imported, exported, revoked, and deleted as required. CSRs can be imported to sign, and the certificate detail information can also be viewed, see To view certificate details: on page 298.

To create a new certificate:

1. To create a new user certificate, go to **Certificate Management > End Entities > Users**. To create a new server certificate, go to **Certificate Management > End Entities > Local Services**.
2. Select **Create New** to open the **Create New User Certificate** or **Create New Server Certificate** window.


Create New User Certificate
Certificate ID:
Certificate Signing Options
Certificate authority:
Issuer:
Local CA
Third-party CA
Local User (Optional):
Subject Information
Subject input method:
Fully distinguished name
Field-by-field
Name (CN):
Department (OU):
Company (O):
City (L):
State/Province (ST):
Country (C):
Email address:
Subject Alternative Name
DNS:
Key And Signing Options
Validity period:
Set length of time
Set an expiry date
365
days
Key type:
RSA
Key size:
2048
4096
Hash algorithm:
SHA-512
SHA-384
SHA-256
Other Subject Alternative Name
Email:
User Principal Name (UPN):
URI:
Other Extensions
Edit device FQDN
Add CRL Distribution Points extension
Location:
No CA has been configured. Please configure a CA first to have access to CRL.
Add OCSP Responder URL
Location:
Use certificate for Smart Card logon
Advanced Options: Key Usages
Key Usages:
Critical
Available Key Usages
Chosen Key Usages
Filter
Digital Signature
Non Repudiation
Key Encipherment
Data Encipherment
Key Agreement
Certificate Sign
CRL Sign
Encipher Only
Decipher Only
Choose all
Remove all
Extended Key Usages:
Critical
Available Extended Key Usages
Chosen Extended Key Usages
Server Authentication
Client Authentication
Code Signing
Secure Email
OCSP Signing
IPSec End System
IPSec Tunnel Termination
IPSec User
IPSec IKE Intermediate (end entity)
Time Stamping
Microsoft Individual Code Signing
Microsoft Commercial Code Signing
Microsoft Trust List Signing
Microsoft Server Gated Crypto
Netscape Server Gated Crypto
Choose all
Remove all
Save
Cancel



3. Configure the following settings:

Certificate ID	Enter a unique ID for the certificate.
Certificate Signing Options	
Certificate authority	If **Local CA** is selected as the issuer, select one of the available CAs configured on FortiAuthenticator from the dropdown menu. The CA must be valid and current. If it is not you will have to create or import a CA certificate before continuing. See Certificate authorities on page 299.
Issuer	Select the issuer of the certificate, either **Local CA** or **Third-party CA**. Selecting **Third-party CA** generates a CSR that is to be signed by a third-party CA. **Note**: When creating a server certificate, an additional **Automated** option is also available. Selecting **Automated** allows you to automatically create a certificate using the ACME protocol with Let's Encrypt service.

	Acme service URL	The ACME service URL. **Note**: The option is only available when the **Issuer** is **Automated**.
		Create Account — Select **Create Account** after filling in the **ACME service URL**, the ACME account information persists on FortiAuthenticator upon successful account creation. **Note**: • Once the server certificate is created, the ACME server endpoint is disabled and grayed out. The **Create Account** option changes to **Change Account**. • Clicking **Change Account** deletes the existing account information from the FortiAuthenticator.
		ACME account email — Optionally, set the account email by clicking the edit icon for the field.
	Local User (Optional)	If **Local CA** is selected as the issuer, you may select a local user from the dropdown menu to whom the certificate will apply. **Note**: The option is only available when creating a new user certificate.
Subject Information		
	Subject input method	Select the subject input method, either **Fully distinguished name** or **Field-by-field**.
	Subject DN	If the subject input method is **Fully distinguished name**, enter the full distinguished name of the subject. There should be no spaces between attributes. Valid DN attributes are `DC, C, ST, L, O, OU, CN, and emailAddress`. They are case-sensitive.
	Name (CN)	If the subject input method is **Field-by-field**, enter the subject name in the **Name (CN)** field, and optionally fill-in the following fields: • **Department (OU)** • **Company (O)** • **City (L)** • **State/Province (ST)** • **Country (C)** (select from dropdown menu) • **Email address** **Note**: When creating a server certificate, if the **Issuer** is **Automated**, then only **Name(CN)** and **Email address** options are available.
	Subject Alternative Name	Subject alternative names (SAN) allow you to protect multiple host names with a single SSL certificate. SAN is part of the X.509 certificate standard.

	For example, SANs are used to protect multiple domain names such as `www.example.com` and `www.example.net`, in contrast to wildcard certificates that only protect all first-level subdomains on one domain, such as `*.example.com`. **Note**: The options in the pane are not available when creating a server certificate if the **Issuer** is **Automated**.
	DNS — Enter the DNS used to validate and sign the imported CSR.  You can specify multiple SAN DNS entries by separating them with commas and adding the `DNS:` prefix to the following entries, e.g., `san1.com, DNS:san2.com, DNS:san3.com`.
Key and Signing Options	
Validity period	Select the amount of time before this certificate expires. This validity period option is only available when **Issuer** is set to **Local CA**. Select **Set length of time** to enter a specific number of days, or select **Set an expiry date** to enter the specific date on which the certificate expires. **Note**: The option is not available when creating a server certificate if the **Issuer** is **Automated**.
Key type	The key type is set to **RSA**.
Key size	Select the key size, in bits: • **2048** (default) • **4096** **Note**: Only **4096** bits are available when creating a server certificate if the **Issuer** is **Automated**.
Hash algorithm	Select the hash algorithm: • **SHA-512** • **SHA-384** • **SHA-256** (default) **Note**: Only **SHA-256** and **SHA-512** are available when creating a server certificate if the **Issuer** is **Automated**.
Other Subject Alternative Name	
Email	Enter the email address of a user to map to this certificate.
User Principal Name (UPN)	Enter the UPN used to find the user's account in Microsoft Active Directory. This will map the certificate to this specific user. The UPN is unique for the Windows Server domain. This is a form of one-to-one mapping.

URI	Enter the URI used to validate certificates.
Other Extensions	
Edit device FQDN	Select to edit the device FQDN.
Add CRL Distribution Points extension (Location: Device FQDN has not been configured)	Select to add CRL distribution points extension to the certificate. A DNS domain name must be configured. If it has not been, select **Edit DNS name** to configure one. See DNS on page 44. **Note:** After a certificate is issued with this extension, the server must be able to handle the CRL request at the specified location.
Add OCSP Responder URL (Location: Device FQDN has not been configured)	Enable Online Certificate Status Protocol (OCSP) to obtain the revocation status of a certificate.
Use certificate for Smart Card logon	Select to use the certificate for smart card logon. Enabling this setting will automatically enable **Add CRL Distribution Points extension**. **Note**: The option is only available when creating a user certificate.
Advanced Options: Key Usages	Some certificates require the explicit presence of key usage attributes before the certificate can be accepted for use. **Note**: The options in the pane are not available when creating a server certificate if the **Issuer** is **Automated**.
Digital Signature	A high-integrity signature that assures the recipient that a message was not altered in transit
Non Repudiation	An authentication that is deemed as genuine with high assurance.
Key Encipherment	Uses the public key to encrypt private or secret keys.
Data Encipherment	Uses the public key to encrypt data.
Key Agreement	An interactive method for multiple parties to establish a cryptographic key, based on prior knowledge of a password.
Certificate Sign	A message from an applicant to a certificate authority in order to apply for a digital identity certificate.
CRL Sign	A Certificate Revocation List (CRL) Sign states a validity period for an issued certificate.
Encipher Only	Information is converted into code only.
Decipher Only	Code is converted into information only.

Advanced Options: Extended Key Usages	Some certificates require the explicit presence of **extended** key usage attributes before the certificate can be accepted for use. **Note**: The options in the pane are not available when creating a server certificate if the **Issuer** is **Automated**.
Server Authentication	Authentication will only be granted when the user submits their credentials to the server.
Client Authentication	Authentication is granted to the server by exchanging a client certificate.
Code Signing	Used to confirm the software author, and guarantees that the code has not been altered or corrupted through use of a cryptographic hash.
Secure Email	A secure email sent over SSL encryption.
OCSP Signing	Online Certificate Status Protocol (OCSP) Signing sends a request to the server for certificate status information. The server will send back a response of "current", "expired", or "unknown". OCSP permits a grace period to users or are expired, allowing them a limited time period to renew. This is typically used over CRL.
IPSec End System	
IPSec Tunnel Termination	IPsec Security Associations (SAs) are terminated through deletion or by timing out
IPSec User	
IPSec IKE Intermediate (end entity)	An intermediate certificate is a subordinate certificate issued by a trusted root specifically to issue end-entity certificates. The result is a certificate chain that begins at the trusted root CA, through the intermediate CA (or CAs) and ending with the SSL certificate issued to you.
Time Stamping	
Microsoft Individual Code Signing	User submits information that is compared to an independent consumer database to validate their credentials.
Microsoft Commercial Code Signing	User submits information that proves their identity as corporate representatives.
Microsoft Trust List Signing	Uses a certificate trust list (CTL), a list of hashes of certificates. The list is comprised of pre-authenticated items that were approved by a trusted signing entity.
Microsoft Server Gated Crypto	A defunct mechanism that stepped up 40-bit and 50-bit to 128-bit cipher suites with SSL.
Netscape Server Gated Crypto	A defunct mechanism that stepped up 40-bit and 50-bit to 128-bit cipher suites with SSL.
Microsoft Encrypted File	The Encrypted File System (EFS) enables files to be transparently

System	encrypted to protect confidential data.
Microsoft EFS File Recovery	The certificate is granted on the condition it has an EFS file recovery agent prepared.
Smart Card Logon	The certificate is granted on the condition that the user logs on to the network with a smart card.
EAP over PPP	Extensible Authentication Protocol (EAP) will operate within a Point-to-Point Protocol (PPP) framework.
EAP over LAN	EAP will operate within a Local Area Network (LAN) framework.
KDC Authentication	An authentication server forwards usernames to a key distribution center (KDC), which issues an encrypted, time-stamped ticket back to the user.

4. Select **Save** to create the new certificate.

To import a local user certificate:

FortiAuthenticator can import certificates signed with RSA or Elliptic Curve.

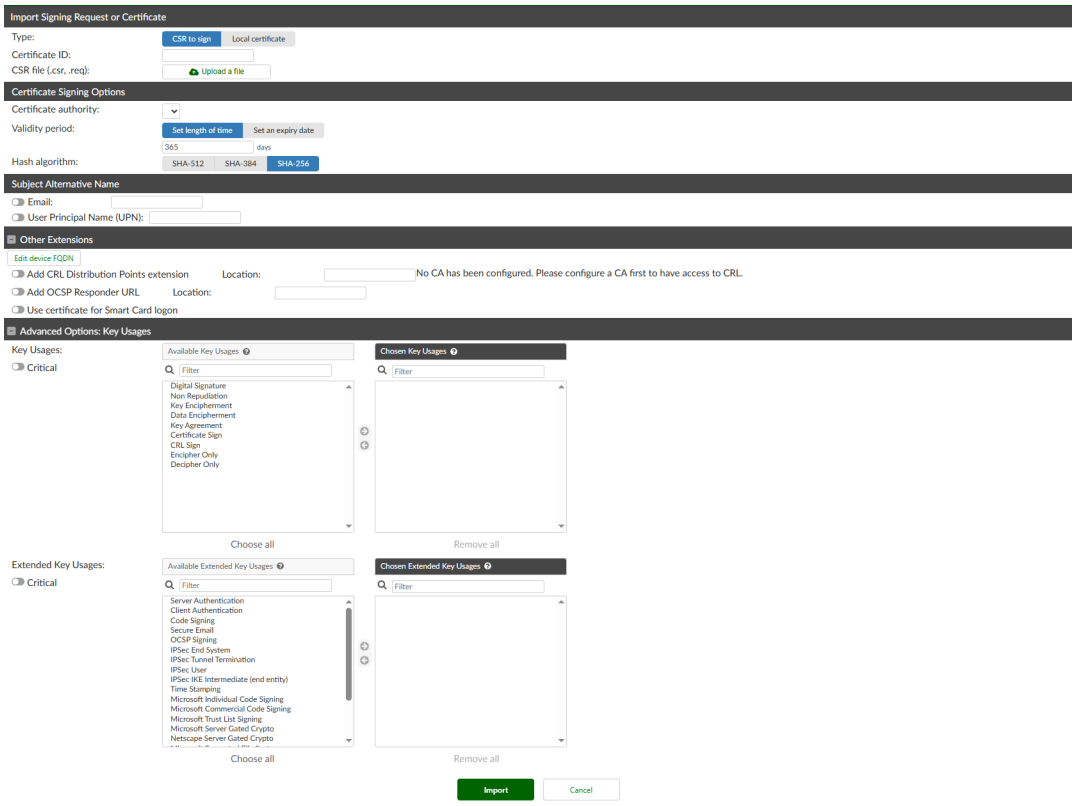
1. Go to **Certificate Management > End Entities > Users** and select **Import**.
2. For **Type**, select **Local certificate**.
3. Select **Upload a file** to locate the certificate file on your computer.
4. Select **Import** to import the certificate.

To import a server certificate:

1. Go to **Certificate Management > End Entities > Local Services** and select **Import**.
2. Select **Upload a file** to locate the certificate file on your computer.
3. Select **Save** to import the certificate.

To import a CSR to sign:

1. Go to **Certificate Management > End Entities > Users** and select **Import**.
2. For **Type**, select **CSR to sign**.



3. Configure the following settings:

Certificate ID	Enter a unique ID for the certificate.
CSR file (.csr, .req)	Select **Upload a File** then locate the CSR file on your computer.
Certificate Signing Options	
Certificate authority	Select one of the available CAs configured on the FortiAuthenticator from the dropdown menu. The CA must be valid and current. If it is not you will have to create or import a CA certificate before continuing. See Certificate authorities on page 299.
Validity period	Select the amount of time before this certificate expires. Select **Set length of time** to enter a specific number of days, or select **Set an expiry date** and enter the specific date on which the certificate expires
Hash algorithm	Select the hash algorithm: • **SHA-512** • **SHA-384** • **SHA-256** (default)
Subject Alternative Name	
Email	Enter the email address of a user to map to this certificate.
User Principal	Enter the UPN used to find the user's account in Microsoft Active Directory.

	Name (UPN)	This will map the certificate to this specific user. The UPN is unique the Windows Server domain. This is a form of one-to-one mapping.
Other Extensions		
	Edit device FQDN	Select to edit the device FQDN. Enter a new FQDN and select **Save**.
	Add CRL Distribution Points extension (Location: Device FQDN has not been configured)	Select to add CRL distribution points extension to the certificate. A DNS domain name must be configured. If it has not been, select **Edit DNS name** to configure one. See DNS on page 44. **Note:** After a certificate is issued with this extension, the server must be able to handle the CRL request at the specified location.
	Add OCSP Responder URL (Location: Device FQDN has not been configured)	Enable Online Certificate Status Protocol (OCSP) to obtain the revocation status of a certificate.
	Use certificate for Smart Card logon	Select to use the certificate for smart card logon. Enabling this setting will automatically enable **Add CRL Distribution Points extension**.
Advanced Options: Key Usages and Extended Key Usages		Some certificates require the explicit presence of key usage attributes before the certificate can be accepted for use. Same settings available as when creating a new user certificate (see above).

4. Select **Import** to import the CSR.

To revoke a certificate:

1. Go to **Certificate Management > End Entities > Users** or to **Certificate Management > End Entities > Local Services**.
2. Select the certificate you want to revoke and select **Revoke**.
3. Select a reason for revoking the certificate from the **Reason code** dropdown menu. The reasons available are:
   - **Unspecified**
   - **Key has been compromised**
   - **CA has been compromised**
   - **Changes in affiliation**
   - **Superseded**
   - **Operation ceased**
   - **On Hold**

   Some of these reasons are security related (such as a compromised key or CA), while others are more business related. A **Change in affiliation** could be an employee leaving the company, while **Operation ceased** could be a project that was canceled.
4. Select **OK** to revoke the certificate.

To view certificate details:

From the certificate list, select a certificate ID to open the **Certificate Detail Information** window.

Select **Edit** next to the **Certificate ID** field to change the certificate ID.

If any of this information is out of date or incorrect, you will not be able to use this certificate.

If this is the case, delete the certificate and re-enter the information in a new certificate, see To create a new certificate: on page 289.

Select **Close** to return to the certificate list.

Certificate authorities

A certificate authority (CA) is used to sign other server and client certificates. Different CAs can be used for different domains or certificates. For example, if your organization is international you may have a CA for each country, or smaller organizations might have a different CA for each department. The benefits of multiple CAs include redundancy, in case there are problems with one of the well-known trusted authorities.

After you have created a CA certificate, you can export it to your local computer.

Local CAs

The FortiAuthenticator device can act as a self-signed, or local, CA.

To view the certificate information, go to **Certificate Management > Certificate Authorities > Local CAs**.

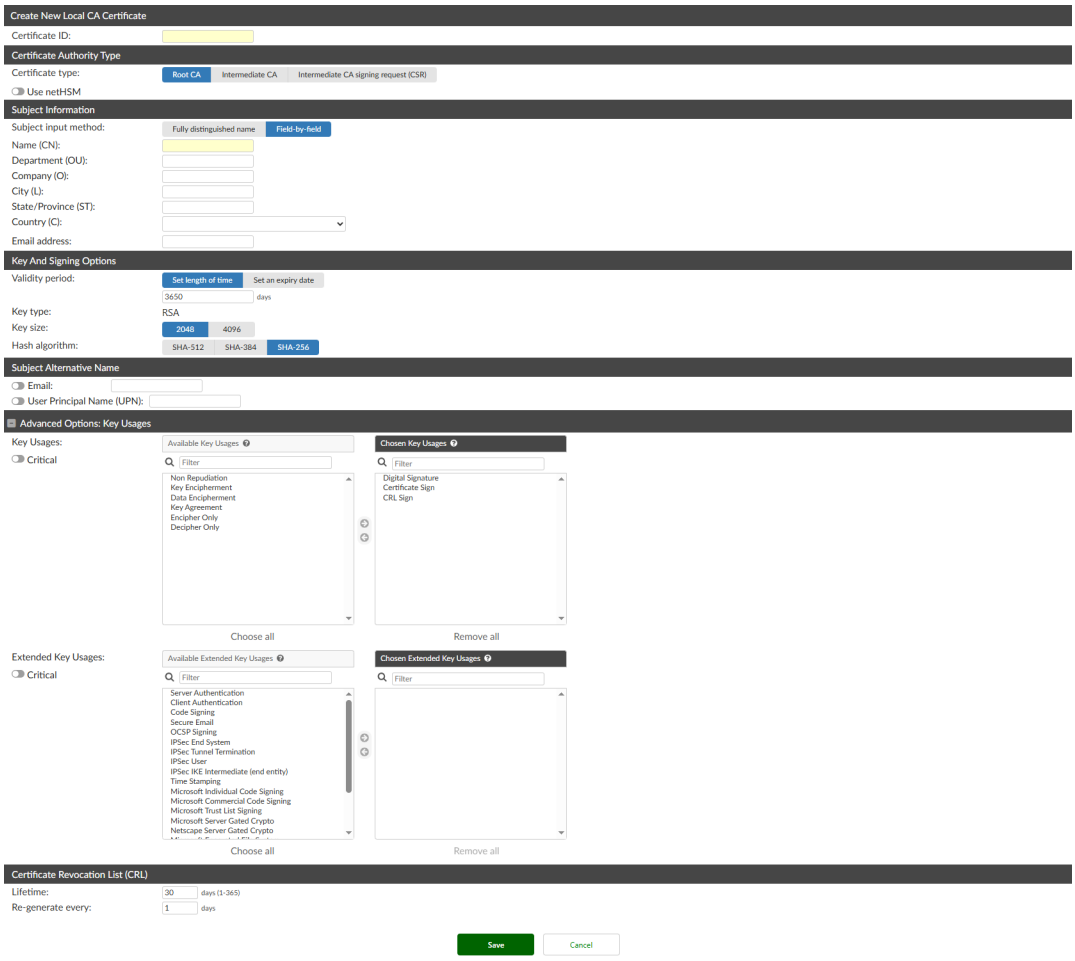
The following information in shown:

Create New	Create a new CA certificate.
Import	Import a CA certificate. See Importing CA certificates and signing requests on page 303.
Revoke	Revoke the selected CA certificate.
Delete	Delete the selected CA certificate.
Export Certificate	Save the selected CA certificate to your computer.
Export Key and Cert	Save the selected intermediate CA certificate and private key to your computer.
Search	Enter a search term in the search field, then press **Enter** to search the CA certificate list. The search will return certificates that match either the subject or issuer.
Filter	Select to filter the displayed CAs by status. The available selections are: **All**, **Pending**, **Expired**, **Revoked**, and **Active**.

Certificate ID	The CA certificate ID.
Subject	The CA certificate subject.
Issuer	The issuer of the CA certificate.
Status	The status of the CA certificate.
CA Type	The CA type of the CA certificate.

To create a CA certificate:

1. From the local CA certificate list, select **Create New**.
   The **Create New Local CA Certificate** window opens.



2. Enter the following information:

Certificate ID	Enter a unique ID for the CA certificate.
Certificate Authority Type	

	Certificate type	Select one of the following options: • **Root CA certificate**: A self-signed CA certificate. • **Intermediate CA certificate**: A CA certificate that refers to a different root CA as the authority. • **Intermediate CA certificate signing request (CSR)**
	Certificate authority	Select one of the available CAs from the dropdown menu. This field is only available when the certificate type is **Intermediate CA certificate**.
	Use netHSM	Select one of the available NetHSMs from the dropdown menu. See NetHSMs on page 67. This field is only available when the certificate type is **Root CA**.
Subject Information		
	Subject input method	Select the subject input method, either **Fully distinguished name** or **Field-by-field**.
	Subject DN	If the subject input method is **Fully distinguished name**, enter the full distinguished name of the subject. There should be no spaces between attributes. Valid DN attributes are `DC, C, ST, L, O, OU, CN,` and `emailAddress`. They are case-sensitive.
	Name (CN)	If the subject input method is **Field-by-field**, enter the subject name in the **Name (CN)** field, and optionally enter the following fields: • **Department (OU)** • **Company (O)** • **City (L)** • **State/Province (ST)** • **Country (C)** (select from dropdown menu) • **Email address**
Key and Signing Options		
	Validity period	Select the amount of time before this certificate expires. Select **Set length of time** to enter a specific number of days, or select **Set an expiry date** and enter the specific date on which the certificate expires. This option is not available when the certificate type is set to **Intermediate CA certificate signing request (CSR)**.
	Key type	The key type is set to **RSA**.
	Key size	Select the key size, in bits: • **2048** (default) • **4096**
	Hash algorithm	Select the hash algorithm: • **SHA-512** • **SHA-284** • **SHA-256** (default)

Subject Alternative Name		SANs allow you to protect multiple host names with a single SSL certificate. SAN is part of the X.509 certificate standard. This section is not available when the certificate type is **Intermediate CA certificate signing request (CSR)**.
	Email	Enter the email address of a user to map to this certificate.
	User Principal Name (UPN)	Enter the UPN used to find the user's account in Microsoft Active Directory. This will map the certificate to this specific user. The UPN is unique for the Windows Server domain. This is a form of one-to-one mapping.
Advanced Options: Key Usages		Some certificates require the explicit presence of extended key usage attributes before the certificate can be accepted for use. For detailed information about these attributes, see End entities on page 288.
	Key Usages	• **Digital Signature** • **Non Repudiation** • **Key Encipherment** • **Data Encipherment** • **Key Agreement** • **Certificate Sign** • **CRL Sign** • **Encipher Only** • **Decipher Only**
	Extended Key Usages	• **Server Authentication** • **Client Authentication** • **Code Signing** • **Secure Email** • **OCSP Signing** • **IPSec End System** • **IPSec Tunnel Termination** • **IPSec User** • **IPSec IKE Intermediate (end entity)** • **Time Stamping** • **Microsoft Individual Code Signing** • **Microsoft Commercial Code Signing** • **Microsoft Trust List Signing** • **Microsoft Server Gated Crypto** • **Netscape Server Gated Crypto** • **Microsoft Encrypted File System** • **Microsoft EFS File Recovery** • **Smart Card Logon** • **EAP over PPP** • **EAP over LAN** • **KDC Authentication**
Other Extensions		Specify an OCSP and/or CRL distribution URL.

		Other Extensions options are only available for **Intermediate CA certificates**.
	Edit device FQDN	Select to edit the device FQDN. Enter a new FQDN and select **Save**.
	Add CRL Distribution Points extension	Select to add a CRL Distribution Points extension to the certificate. Once a certificate is issued with this extension, the server must be able to handle the CRL request at the specified location. A fully qualified domain name (FQDN) must be configured. The FQDN can be added or configured by clicking **Edit device FQDN**.
	Add OCSP Responder URL	Select to add an Online Certificate Status Protocol (OCSP) responder URL to obtain the revocation status of a certificate. A fully qualified domain name (FQDN) must be configured. The FQDN can be added or configured by clicking **Edit device FQDN**.
Certificate Revocation List (CRL)		Determine the certificate's lifetime before the CA certificate is revoked.
	Lifetime	Enter the lifetime of the certificate in days, between 1 - 365 (maximum of one year). The default is **30**.
	Re-generate every	Enter how often the certificate will regenerate.

3. Select **Save** to create the new CA certificate.

Importing CA certificates and signing requests

Five options are available when importing a certificate or signing request: **PKCS12 Certificate**, **Certificate and Private Key**, **CSR to sign**, **Local certificate**, and **NetHSM certificate**.

To import a PKCS12 certificate:

1. From the local CA certificate list, select **Import**.
   The **Import Signing Request or Local CA Certificate** window opens.
2. Select **PKCS12 Certificate** in the type field.
3. Enter the following:

Certificate ID	Enter a unique ID for the certificate.
PKCS12 certificate file (.p12)	Select **Upload a file** to locate the certificate file on your computer.
Passphrase	Enter the certificate passphrase.

4. Select **Import** to import the certificate.

To import a certificate with a private key:

1. From the local CA certificate list, select **Import**.
   The **Import Signing Request or Local CA Certificate** window opens.
2. Select **Certificate and Private Key** in the type field.

3. Enter the following:

Certificate ID	Enter a unique ID for the certificate.
Certificate file (.cer)	Select **Upload a file** to locate the certificate file on your computer.
Private key file	Select **Upload a file** to locate the private key file on your computer.
Passphrase	Enter the certificate passphrase.

4. Select **Save** to import the certificate.

To import a CSR to sign:

1. From the local CA certificate list, select **Import**.
   The **Import Signing Request or Local CA Certificate** window opens.
2. Select **CSR to sign** in the type field.
3. Enter the following:

Certificate ID	Enter a unique ID for the certificate.
CSR file (.csr, .req)	Select **Upload a file** to locate the CSR file on your computer.
Certificate Signing Options	
Certificate authority	Select one of the available CAs from the dropdown menu.
Validity period	Select the amount of time before this certificate expires. Select **Set length of time** to enter a specific number of days, or select **Set an expiry date** and enter the specific date on which the certificate expires.
Hash algorithm	Select the hash algorithm: • **SHA-512** • **SHA-384** • **SHA-256** (default)
Subject Alternative Name	SANs allow you to protect multiple host names with a single SSL certificate. SAN is part of the X.509 certificate standard.
Email	Enter the email address of a user to map to this certificate.
User Principal Name (UPN)	Enter the UPN used to find the user's account in Microsoft Active Directory. This will map the certificate to this specific user. The UPN is unique for the Windows Server domain. This is a form of one-to-one mapping.
Advanced Options: Key Usages	Some certificates require the explicit presence of extended key usage attributes before the certificate can be accepted for use. For detailed information about these attributes, see End entities on page 288.

4. Select **Import** to import the CSR.

To import a local CA certificate:

1. From the local CA certificate list, select **Import**.
   The **Import Signing Request or Local CA Certificate** window opens.
2. Select **Local certificate** in the type field.
3. Select **Upload a file** to locate the certificate file on your computer.
4. Select **Import** to import the local CA certificate.

To import a NetHSM certificate:

1. From the local CA certificate list, select **Import**.
   The **Import Signing Request or Local CA Certificate** window opens.
2. Select **NetHSM certificate** in the type field.
3. Select **Upload a file** to locate the certificate file on your computer.
4. Select the previously configured NetHSM.
   See NetHSMs on page 67.
5. Select **Import** to import the local CA certificate.

Certificate revocations lists

A certificate revocation list (CRL) is a file that contains a list of revoked certificates, their serial numbers, and their revocation dates. The file also contains the name of the issuer of the CRL, the effective date, and the next update date. By default, the shortest validity period of a CRL is one hour.

Some potential reasons certificates can be revoked include:

- A CA server was hacked and its certificates are no longer trusted.
- A single certificate was compromised and is no longer trusted.
- A certificate has expired and cannot be used past its lifetime.

Go to **Certificate Management > Certificate Authorities > CRLs** to view the CRL list.

The following information is shown:

Import	Import a CRL.
Automatic Downloads	Select to view automatically downloaded CRLs. Select **View CRLs** to switch back to the regular CRL view.
Export	Save the selected CRL to your computer.
Delete	Select to delete the selected CRLs. **Note**: Only imported CRLs can be deleted (Local CAs CRLs cannot be deleted).
CA Type	The CA type of CRL.
Issuer name	The name of the issuer of the CRL.

Subject	The CRL subject.
Revoked Certificates	The number of revoked certificates in the CRL.

To import a CRL:

1. Download the most recent CRL from a CDP. One or more CDPs are usually listed in a certificate under the **Details** tab.
2. From the CRL list, select **Import**.
3. Select **Upload a file** to locate the file on your computer, then select **Import** to import the list.

Before importing a CRL file, make sure that either a local CA certificate or a trusted CA certificate for this CRL has first been imported.

When successful, the CRL is displayed in the CRL list on the FortiAuthenticator.

You can select it to see the details (see To view certificate details: on page 298).

Locally created CRLs

When you import a CRL, it is from another authority. If you are creating your own CA certificates, you can also create your own CRL to accompany them.

As a CA, you sign user certificates. If for any reason you need to revoke one of those certificates, it will go on a local CRL. When this happens you must export the CRL to all your certificate users so they are aware of the revoked certificate.

To create a local CRL:

1. Create a local CA certificate. See Local CAs on page 299.
2. Create one or more user certificates. See End entities on page 288.
3. Go to **Certificate Management > End Entities > Users**, select one or more certificates, and select **Revoke**. See To revoke a certificate: on page 298.

   The selected certificates are removed from the user certificate list and a CRL is created with those certificates as entries in the list. If there is already a CRL for the CA that signed the user certificates, the certificates is added to the current CRL.

If later one or more CAs are deleted, their corresponding CRLs will also be deleted, along with any user certificates that they signed.

Configuring OCSP

FortiAuthenticator also supports Online Certificate Status Protocol (OCSP), defined in RFC 2560. To use OCSP, configure the FortiGate unit to use TCP port 2560 on the FortiAuthenticator IP address.

For example, enter the following to configure OCSP on the FortiGate **CLI Console**, where the URL is the IP address of the FortiAuthenticator:

```
config vpn certificate ocsp-server
 edit FortiAuthenticator_ocsp
  set cert "REMOTE_Cert_1"
  set url "http://172.20.120.16:2560"
 next
end
```

Trusted CAs

Trusted CA certificates can be used to validate certificates signed by an external CA.

To view the trusted CA certificate list, go to **Certificate Management > Certificate Authorities > Trusted CAs**.

The certificate ID, subject, issuer, and status are shown.

Certificates can be imported, exported, deleted, and searched.

FortiAuthenticator does not have preinstalled 3rd party trusted CA certificates.

To import a trusted CA certificate:

1. From the trusted CA certificate list, select **Import**.
2. Enter a certificate ID in the **Certificate ID** field.
3. Select **Upload a file** to locate the certificate file on your computer, and select **Import** to import the list.
   When successful, the trusted CA certificate is displayed in the list on the FortiAuthenticator device.
   You can select it to see the details (see To view certificate details: on page 298).

To extract a trusted CA certificate with chain from a server:

1. From the trusted CA certificate list, select **Learn Certificate**.
2. Enter host name/ IP address in the **Host name/IP** field, the port number in the **Port** field, and click **Learn**.
3. Under **Import**, enable the toggle to select the CA certificates to import, enter their certificate IDs, and click **Import**.
   When successful, the trusted CA certificates are displayed on the FortiAuthenticator device.
   You can select it to see the details (see To view certificate details: on page 298).

SCEP

FortiAuthenticator contains a Simple Certificate Enrollment Protocol (SCEP) server that can sign user CSRs, and distribute CRLs and CA certificates. To use SCEP, you must:

- Enable HTTP administrative access on the interface(s) connected to the Internet.
  See Network on page 41.

The recommended configuration for SCEP interfaces includes:

- One dedicated interface for system administration which includes enforced IP address restriction on admin access.
- One dedicated interface for service provisioning.
- One dedicated interface for the HA heartbeat when configured in an HA cluster.

- Add a local certificate authority (root or intermediate).
  See Certificate authorities on page 299.
- Select the local signing CA to use for SCEP.
  See Default CA on page 308.

Users can request a user certificate through online SCEP, found at:

```
http://<FortiAuthenticator-IP-Address>/app/cert/scep
```

General

As an administrator, you can allow FortiAuthenticator to either automatically sign the user's certificate or alert you about the request for a signature.

To enable SCEP and configure general settings:

1. Go to **Certificate Management > SCEP > General**, and select **Enable SCEP**.
2. Configure the following settings:

Default CA	From the dropdown, select the default local CA used to issue certificates via SCEP.
Default enrollment password	Enter the default enrollment password that is used when not setting a random password. **Note**: You can still choose between the default password or a randomly generated password when creating a new enrollment request.
Enrollment method	Select the enrollment method: • **Automatic**: The certificate is pre-approved by the administrator. The administrator enters the certificate information on FortiAuthenticator and gives the user a challenger password to use when submitting their request. • **Manual and Automatic**: The user submits the CSR, the request shows up as pending on FortiAuthenticator unit, then the administrator manually approves the pending request. Optionally, enter an email address to be informed of pending approval notifications.

Revoke the old certificate on renewal	Enable to revoke the old certificate after it is renewed.

3. Select **Save** to apply any changes you have made.

Enrollment requests

To view and manage certificate enrollment requests, go to **Certificate Management > SCEP > Enrollment Requests**.

Before you can create or configure certificate enrollment requests, SCEP must be enabled, and HTTP access must be enabled on the network interface(s) that will serve SCEP clients (under **System > Network > Interfaces**).

The following information is available:

Create New	Create a new certificate enrollment request.
Delete	Delete the selected certificate enrollment request.
Approve or Reject	Approve or reject the selected certificate enrollment request.
Delete & Revoke Certificate	Delete the selected SCEP enrollment requests and revoke all the corresponding active user certificates.  This option is available only if the **Automatic request type** for the selected request is **Regular**.
Search	Search for SCEP enrollment requests with subject fields matching the input text string.
Method	The enrollment method used.
Status	The status of the enrollment: **Pending**, **Approved**, or **Rejected**.
Wildcard	If it is a wildcard request, a green circle with a check mark is shown.
Issuer	The issuer of the certificate. Hover over the truncated value to see the full issuer name.
Subject	The certificate subject. Hover over the truncated value to see the full subject name.
Renewable Before Expiry (days)	The number of days before the certificate enrollment request expires that it can be renewed.

Updated at	The date and time that the enrollment request was last updated.

To view the enrollment request details:

1. From the enrollment request list, select a request by clicking within its row.
2. Select **Cancel** to return to the enrollment request window.

To create a new certificate enrollment request:

1. From the certificate enrollment requests list, select **Create New**.

2. Enter the following information:

Automatic request type	Select the automatic request type, either **Regular** or **Wildcard**.
Certificate Authority	Select one of the available local CAs configured on FortiAuthenticator from the dropdown menu.

	The CA must be valid and current. If it is not you will have to create or import a CA certificate before continuing. See Certificate authorities on page 299.
Subject Information	
Subject input method	Select the subject input method, either **Fully distinguished name** or **Field-by-field**.
Subject DN	If the subject input method is **Fully distinguished name**, enter the full distinguished name of the subject. There should be no spaces between attributes. Valid DN attributes are `DC, C, ST, L, O, OU, CN`, and `emailAddress`. They are case-sensitive.
Name (CN)	If the subject input method is **Field-by-field**, enter the subject name in the **Name (CN)** field (if the **Automatic request type** is set to **Regular**), and optionally enter the following fields: • **Department (OU)** • **Company (O)** • **City (L)** • **State/Province (ST)** • **Country (C)** (select from dropdown menu) • **Email address**
Certificate Signing Options	
Validity period	Select the amount of time before this certificate expires. Select **Set length of time** to enter a specific number of days (default = 365), or select **Set an expiry date** and enter the specific date on which the certificate expires.
Hash algorithm	Select the hash algorithm: • **SHA-512** • **SHA-384** • **SHA-256** (default)
Challenge Password	
Password generation	Select to set a random password, use the default enrollment password (see Enrollment requests on page 309), or select **InTune**. Select from the following three options: • **Random** • **Default**: Use the default enrollment password (see Enrollment requests on page 309). • **InTune**: Select an OAuth server from the dropdown to be used to communicate to the Microsoft Graph API. **Note**: The dropdown only includes remote OAuth servers with type as **Azure Directory** and a non-empty **Tenant ID**.
Challenge password distribution	Select the challenge password distribution method. This option is only available if **Password creation** is set to **Set a random password**.

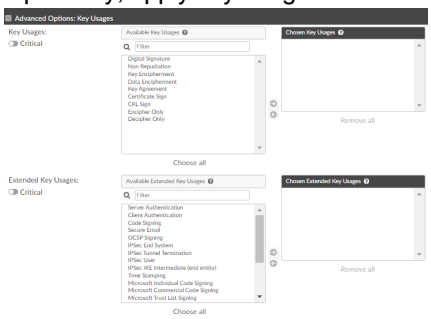
	• **Display**: Display the password on the screen. • **SMS**: Send the password to a mobile phone. Enter the phone number in the **Mobile number** field and select an SMS gateway from the dropdown menu. • **Email**: Send the password to the email address entered in the email field.

Renewal	To allow renewals, select **Allow renewal**, then enter the number of days before the certificate expires (default = 7).
	When renewal is enabled, you can optionally either allow or reject SCEP renewal requests for expired and revoked certificates (as burst renewal requests from FortiGate devices could exhaust the FortiAuthenticator and create duplicate certificates), and either allow or reject SCEP renewal requests signed using the old private key.
	When an SCEP enrollment request is configured to accept certificate renewals with **Verify renewal request signature using the old private key** enabled:
	• If the certificate renewal request contains a password, FortiAuthenticator verifies that (in addition to renewal time window and the certificate status settings):
	  • The private key of the previous certificate signs the request.
	  • The request password matches the configured challenge password for the renewed certificate.
	• If the certificate renewal request does not contain a password, FortiAuthenticator verifies that (in addition to renewal time window and the certificate status settings) the previous certificate's private key signs the request.

Subject Alternative Name	SANs allow you to protect multiple host names with a single SSL certificate. SAN is part of the X.509 certificate standard.
Email	Enter the email address of a user to map to this certificate.  You can use `{{:cn}}` tag as a placeholder for the value of the certificate CN from the subject field in the **Email** field, e.g., `{{:cn}}@domain.org`.
User Principal Name (UPN)	Enter the UPN used to find the user's account in Microsoft Active Directory. This will map the certificate to this specific user. The UPN is unique for the Windows Server domain. This is a form of one-to-one mapping.  You can use `{{:cn}}` tag as a placeholder for the value of the certificate CN from the subject field in the **User Principal Name (UPN)** field, e.g., `{{:cn}}@domain.org`.
Other Extensions	Includes optional settings for SCEP enrollment requests.
Edit device FQDN	Select to edit the device FQDN.

	Enter a new FQDN and select **Save**.
Add CRL Distribution Points extension	Select to add a CRL Distribution Points extension. A fully qualified domain name (FQDN) must be configured. The FQDN can be added or configured by clicking **Edit device FQDN**.
Add OCSP Responder URL	Select to add an Online Certificate Status Protocol (OCSP) responder URL to obtain the revocation status of a certificate. A fully qualified domain name (FQDN) must be configured. The FQDN can be added or configured by clicking **Edit device FQDN**.

3. Optionally, apply key usage attributes.



Advanced Options: Key Usages	
Key Usages	Key usage attributes identify the purpose(s) of a certificate's key. Some applications require the explicit presence of attributes before the certificate will be accepted for use. When an entity contains multiple certificates or keys, key usage attributes can also be used to identify which is the correct certificate or key to use. When the **Critical** option is enabled, the certificate can only be used for the purposes indicated by the selected attributes, and attempting to use the certificate for other purposes results in a CA policy violation. For detailed information about key usage attributes, see End entities on page 288.
Extended Key Usages	Extended Key Usages provides an extended list of selectable attributes. The **Critical** option can also be applied to extended key usage attributes. When the **Critical** option is applied to both key usage and extended key usage attributes, only certificates that are consistent with both fields are accepted. For detailed information about extended key usage attributes, see End entities on page 288

4. Select **Save** to create the new certificate enrollment request.
When created, the request will have a **Status** of **Pending**.
A code is displayed which must be provided to the client as a challenge password for the automatic certificate enrollment process.

CMP

CMPv2 is a Certificate Management Protocol designed by Safenet for the secure signing of digital certificates and complete certificate life cycle management.

When enabled, the CMP server is available via HTTP.

The CMP URL is:

```
http://<FAC IP/FQDN>/app/cert/cmp2/
```

The section contains the following topics:

General

To enable CMP and configure general settings:

1. Go to **Certificate Management > CMP > General**, and select **Enable CMPv2**.
2. Configure the following settings:

Server certificate	From the dropdown, select the default server certificate used to prove the server identity to the client. To create a server certificate, see End entities on page 288.
Default enrollment password	Enter a default password if you do not want randomly generated passwords for enrollment requests. **Note**: You can still choose between the default password and a random password when creating a new enrollment request.

3. Select **Save** to apply any changes you have made.

Enrollment requests

To view and manage certificate enrollment requests, go to **Certificate Management > CMP > Enrollment Requests**.

Before you can create or configure certificate enrollment requests, CMP must be enabled, and HTTP access must be enabled on the network interface(s) that will serve CMP clients in **System > Network > Interfaces**.

The following information is available:

Create New	Create a new certificate enrollment request.

Delete	Delete the selected certificate enrollment request.
Search	Search for CMP enrollment requests with subject fields matching the input text string.
Filter	Select and then choose a status filter to apply.
Refresh	To refresh the contents, click the refresh icon.
Method	The enrollment method used.
Status	The status of the enrollment: **Pending**, **Approved**, or **Rejected**.
Type	The request type: **User** or **Device**. **Note**: Auto-generated enrollments are displayed as **Device** type.
Subject	The certificate subject. Hover over the truncated value to see the full subject name.
Renewable Before Expiry (Days)	The number of days before the certificate enrollment request expires that it can be renewed.
Updated At	The date and time that the enrollment request was last updated.

To view the enrollment request details:

1. From the enrollment request list, select a request by clicking within its row.
2. Select **Cancel** to return to the enrollment request window.

To create a new certificate enrollment request:

1. From the certificate enrollment requests list, select **Create New**.
2. Enter the following information:

Request type	Select the request type, either **Regular** or **Device (3GPP)**.	
Profile name (enrollment id)	The name for the enrollment request.	
Certificate authority	Select one of the available local CAs configured on FortiAuthenticator from the dropdown menu. The CA must be valid and current. If it is not you will have to create or import a CA certificate before continuing. See Certificate authorities on page 299.	
Subject Information		
	Subject input method	Select the subject input method, either **Fully distinguished name** or **Field-by-field**.
	Subject DN	If the subject input method is **Fully distinguished name**, enter the full distinguished name of the subject. There should be no spaces between attributes.

		Valid DN attributes are `DC, C, ST, L, O, OU, CN`, and `emailAddress`. They are case-sensitive.
	Name (CN)	If the subject input method is **Field-by-field**, enter the subject name in the **Name (CN)** field (if the **Request type** is set to **Regular**), and optionally enter the following fields: • **Department (OU)** • **Company (O)** • **City (L)** • **State/Province (ST)** • **Country (C)** (select from dropdown menu) • **Email address** **Note**: **Name (CN)** option is not available when the **Request type** is **Device (3GPP)**.
Certificate Signing Options		
	Validity period	Select the amount of time before this certificate expires. Select **Set length of time** to enter a specific number of days (default = 365), or select **Set an expiry date** and enter the specific date on which the certificate expires.
	Hash algorithm	Select the hash algorithm: • **SHA-512** • **SHA-384** • **SHA-256** (default)
Device Authorization **Note**: The pane is only available when the **Request type** is **Device (3GPP)**.		
	Device vendor CA certificate	From the dropdown select the device vendor CA certificate.
	Restrict enrollment by serial number	Enable to restrict enrollment by serial number and enter the authorized serial number for the device. Select **+** to open a text box that allows entering multiple serial numbers. **Note**: You can enter multiple serial numbers provided that they are either comma-separated or entered in a new line.
Challenge Password **Note**: The pane is only available when the **Request type** is **Regular**.		

	Password creation	Select to either set a random password, or use the default enrollment password. **Note**: If **Default** is selected then the password created in General on page 314 is used.
	Challenge password distribution	Select the challenge password distribution method. This option is only available if **Password creation** is set to **Random**. • **Display**: Display the password on the screen. • **SMS**: Send the password to a mobile phone. Enter the phone number in the **Mobile number** field and select an SMS gateway from the dropdown menu. • **Email**: Send the password to the email address entered in the email field.
Renewal	To allow renewals, select **Allow renewal**, then enter the number of days before the certificate expires (default = 7). When renewal is enabled, you can optionally either allow or reject CMP renewal requests for expired and revoked certificates (as burst renewal requests from FortiGate devices could exhaust the FortiAuthenticator and create duplicate certificates), and either allow or reject CMP renewal requests signed using the old private key.	
Subject Alternative Name	SANs allow you to protect multiple host names with a single SSL certificate. SAN is part of the X.509 certificate standard. In **Subject Alternative Name**, DNS name is included (along with `e-mail+UPN`). **Note**: The section is only available when the **Request type** is **Regular**.	
	Email	Enable and enter the email address of a user to map to this certificate.
	User Principal Name (UPN)	Enable and enter the UPN used to find the user's account in Microsoft Active Directory. This will map the certificate to this specific user. The UPN is unique for the Windows Server domain. This is a form of one-to-one mapping.
Other Extensions	Includes optional settings for CMP enrollment requests.	
	Edit device FQDN	Select to edit the device FQDN. Enter a new FQDN and select **Save**.
	Add CRL Distribution Points extension	Select to add a CRL Distribution Points extension. A fully qualified domain name (FQDN) must be configured.

	The FQDN can be added or configured by clicking **Edit device FQDN**.
Add OCSP Responder URL	Select to add an Online Certificate Status Protocol (OCSP) responder URL to obtain the revocation status of a certificate. A fully qualified domain name (FQDN) must be configured. The FQDN can be added or configured by clicking **Edit device FQDN**.

3. Optionally, apply key usage attributes.

Advanced Options: Key Usages	
Key Usages	Key usage attributes identify the purpose(s) of a certificate's key. Some applications require the explicit presence of attributes before the certificate will be accepted for use. When an entity contains multiple certificates or keys, key usage attributes can also be used to identify which is the correct certificate or key to use. When the **Critical** option is enabled, the certificate can only be used for the purposes indicated by the selected attributes, and attempting to use the certificate for other purposes results in a CA policy violation. For detailed information about key usage attributes, see End entities on page 288.
Extended Key Usages	Extended Key Usages provides an extended list of selectable attributes. The **Critical** option can also be applied to extended key usage attributes. When the **Critical** option is applied to both key usage and extended key usage attributes, only certificates that are consistent with both fields are accepted. For detailed information about extended key usage attributes, see End entities on page 288

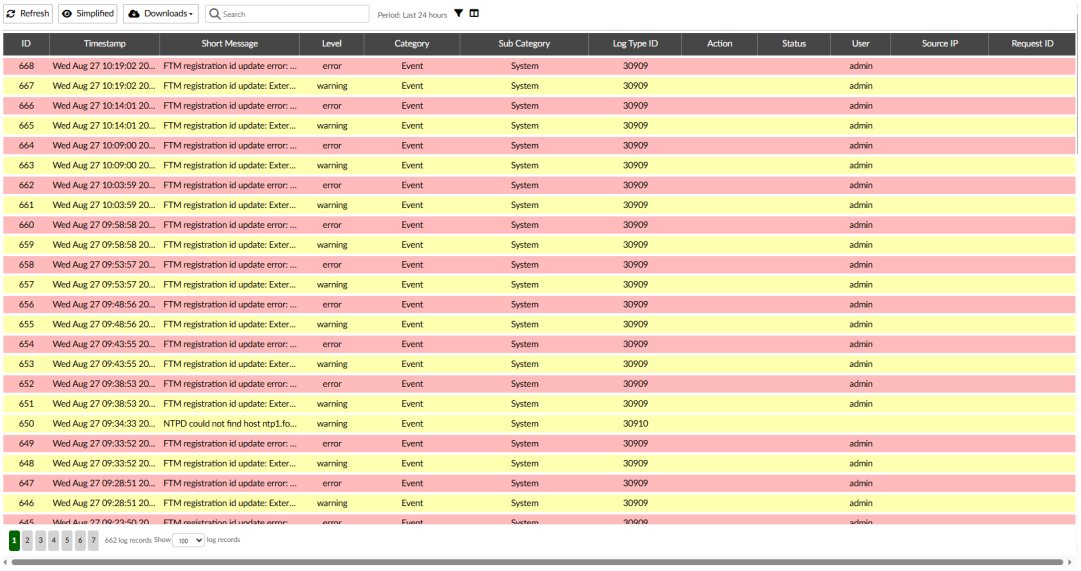
4. Select **Save** to create the new certificate enrollment request.
   When created, the request will have a **Status** of **Pending**.
   A code is displayed which must be provided to the client as a challenge password for the automatic certificate enrollment process.

Logging

Accounting is an important part of FortiAuthenticator. The **Logging** menu tree provides a record of the events that have taken place on FortiAuthenticator.

Log access

To view the log events table, go to **Logging > Log Access > Logs**.



The following options and information are available:

Refresh	Refresh the log list.
Simplified/ Full View	Simplified or full log view.
Downloads	Using **Raw Log** from the dropdown, export the FortiAuthenticator log to your computer as a text file named **fac.log**. You can also download a full debug report for one of the following from the dropdown: • **Summary** • **Authentication** • **Database** • **GUI** • **FastAPI** • **LDAP Sync**

	• **Accounting** • **Authorization** • **SSO** • **System** • **WAD Services** • **REST API**
Search by substring (e.g. username)	Enter a search term in the search field to search the log message list. The search string must appear in the Message portion of the log entry to result in a match. To prevent each term in a phrase from matching separately, multiple keywords must be in quotes and be an exact match. After the search is complete the number of positive matches is displayed next to the Search button, with the total number of log entries in brackets following. Select the total number of log entries to return to the full list. Subsequent searches will search all the log entries, and not just the previous search's results.  Use the search bar to retrieve log records containing the specified substring (case-insensitive) in one of the following columns: • Short Message • Category • Sub Category • Log Type ID • User • Source IP
Time period	Select the filter icon and filter the log events table by selecting from the following available time periods: • **Last hour** • **Last 8 hours** • **Last 24 hours** • **Last 7 days** • **Last month** • **Last 3 months** • **Last year** • **All**
Reset table column widths	Select the reset icon to reset the table column widths to default.
ID	The log message's ID.
Timestamp	The time the message was received.
Short Message	The log message itself, sometimes slightly shortened.

Level	The log severity level: • **Emergency**: The system has become unstable. • **Alert**: Immediate action is required. • **Critical**: Functionality is affected. • **Error**: An erroneous condition exists, and functionality is probably affected. • **Warning**: Functionality could be affected. • **Notification**: Information about normal events. • **Information**: General information about system operations. • **Debug**: Detailed information useful for debugging purposes.
Category	The log category, which is always **Event**. See Log access on page 319.
Sub Category	The log subcategory. See Log access on page 319.
Log Type ID	The log type ID.
Action	The action which created the log message, if applicable.
Status	The status of the action that created the log message, if applicable.
User	The user to whom the log message pertains.
Source IP	The source IP address of the relevant device if an authentication action fails.
Request ID	Displays the value of the `X-Request-ID` header in the logs associated with the REST API operations for the supported endpoints.

To view log details:

From the log list, select the log whose details you need to view by clicking anywhere within the log's row. The **Log Details** pane will open on the right side of the window.

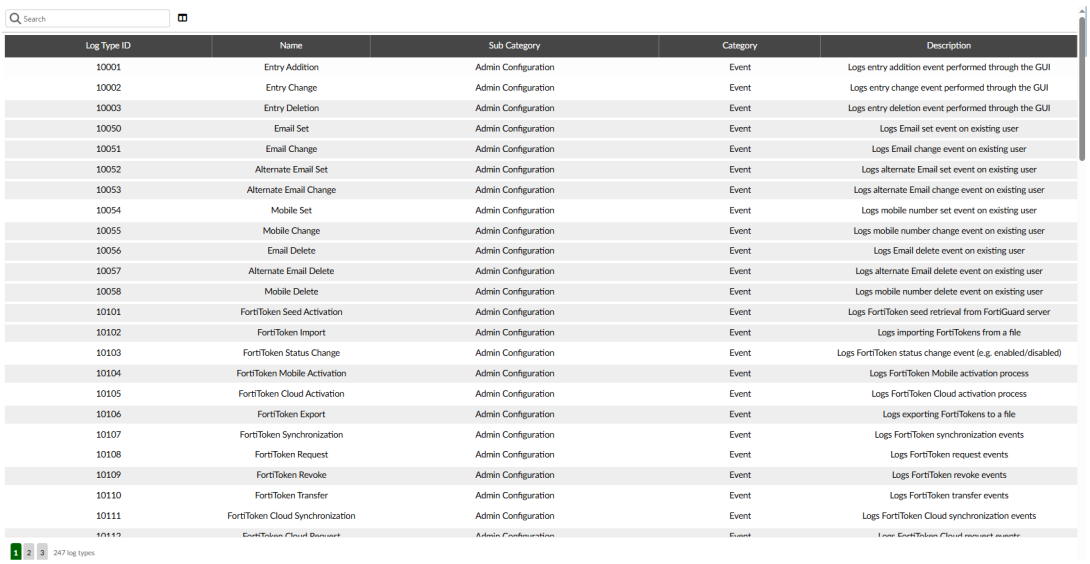
After viewing the log details, select the close icon in the top right corner of the pane to close the details pane.

Sort the log messages

The log message table can be sorted by any column. To sort the log entries by a particular column, select the title for that column. The log entries will now be displayed based on data in that column in ascending order. Select the column heading again to sort the entries in descending order. Ascending or descending is displayed with an arrow next to the column title, an up arrow for ascending and down arrow for descending.

Log types

To view the log types, go to **Logging > Log Access > Log Types**.



Log Type ID	Name	Sub Category	Category	Description
10001	Entry Addition	Admin Configuration	Event	Logs entry addition event performed through the GUI
10002	Entry Change	Admin Configuration	Event	Logs entry change event performed through the GUI
10003	Entry Deletion	Admin Configuration	Event	Logs entry deletion event performed through the GUI
10050	Email Set	Admin Configuration	Event	Logs Email set event on existing user
10051	Email Change	Admin Configuration	Event	Logs Email change event on existing user
10052	Alternate Email Set	Admin Configuration	Event	Logs alternate Email set event on existing user
10053	Alternate Email Change	Admin Configuration	Event	Logs alternate Email change event on existing user
10054	Mobile Set	Admin Configuration	Event	Logs mobile number set event on existing user
10055	Mobile Change	Admin Configuration	Event	Logs mobile number change event on existing user
10056	Email Delete	Admin Configuration	Event	Logs Email delete event on existing user
10057	Alternate Email Delete	Admin Configuration	Event	Logs alternate Email delete event on existing user
10058	Mobile Delete	Admin Configuration	Event	Logs mobile number delete event on existing user
10101	FortiToken Seed Activation	Admin Configuration	Event	Logs FortiToken seed retrieval from FortiGuard server
10102	FortiToken Import	Admin Configuration	Event	Logs importing FortiTokens from a file
10103	FortiToken Status Change	Admin Configuration	Event	Logs FortiToken status change event (e.g. enabled/disabled)
10104	FortiToken Mobile Activation	Admin Configuration	Event	Logs FortiToken Mobile activation process
10105	FortiToken Cloud Activation	Admin Configuration	Event	Logs FortiToken Cloud activation process
10106	FortiToken Export	Admin Configuration	Event	Logs exporting FortiTokens to a file
10107	FortiToken Synchronization	Admin Configuration	Event	Logs FortiToken synchronization events
10108	FortiToken Request	Admin Configuration	Event	Logs FortiToken request events
10109	FortiToken Revoke	Admin Configuration	Event	Logs FortiToken revoke events
10110	FortiToken Transfer	Admin Configuration	Event	Logs FortiToken transfer events
10111	FortiToken Cloud Synchronization	Admin Configuration	Event	Logs FortiToken Cloud synchronization events

The following options and information are available:

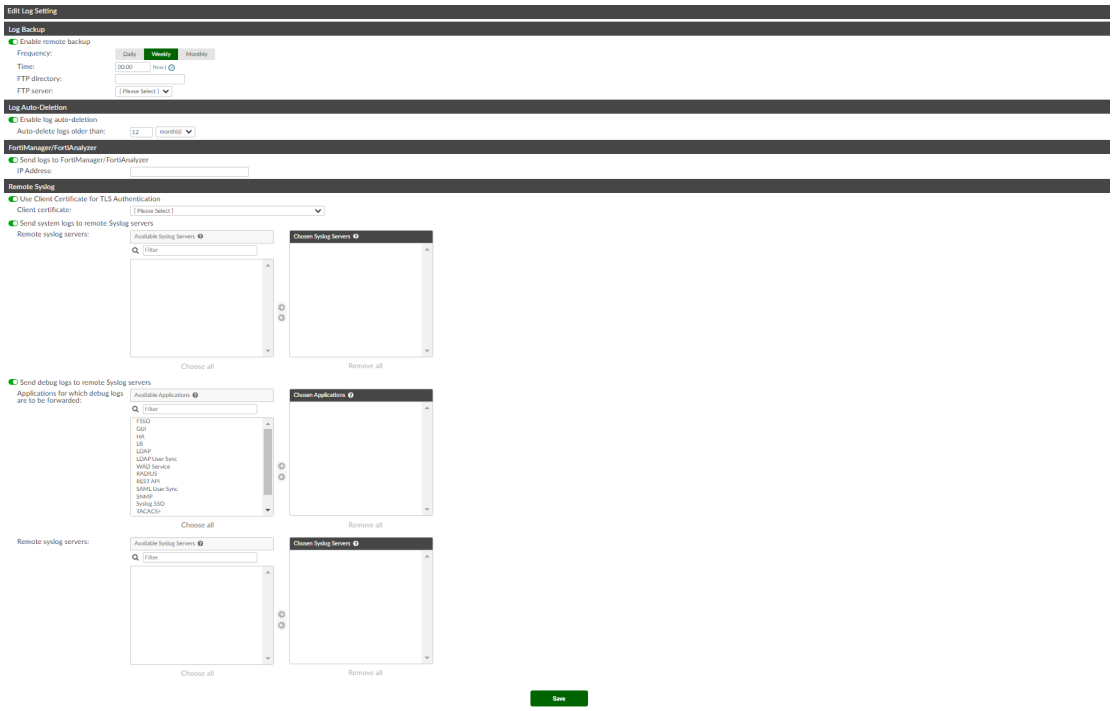
Search	Enter a search term in the search field to search the log types list.
Reset table column widths	Select the reset icon to reset the table column widths to default.
Log Type ID	The log type ID.
Name	The name of the log type.
Sub Category	The subcategory of the log type.
Category	The category of the log type.
Description	The log type description.

Log configuration

Logs can be remotely backed up to an FTP server, automatically deleted, and sent to a remote syslog server in lieu of storing them locally.

Log settings

To configure log backups, automatic deletion, and remote storage, go to **Logging > Log Config > Log Settings**.



To configure log backups:

1. Under **Log Backup**, select **Enable remote backup**.
2. Set the **Frequency** to either **Daily**, **Weekly**, or **Monthly**.
3. Configure the time of day that the backup will occur in one of the following ways:
   - Enter a time in the **Time** field.
   - Select **Now** to enter the current time.
   - Select the clock icon and choose a time from the pop-up menu: **Now**, **Midnight**, **6 a.m.**, **Noon**, or **6 p.m**.
4. In **FTP directory**, enter the FTP directory for a folder on a remote computer.
5. Select an FTP server from the **FTP server** dropdown menu. For information on configuring an FTP server, see FTP servers on page 66.
6. Select **Save** to save your settings.

To configure automatic log deletion:

1. Under **Log Auto-Deletion**, select **Enable log auto-deletion**.
2. Use the **Auto-delete logs older than** field and dropdown menu to specify the number of either **day(s)**, **week(s)**, or **month(s)** after which a log will be deleted. By default, the logs are automatically deleted after 12 months.
3. Select **Save** to save your settings.

To configure logging to a FortiManager/FortiAnalyzer unit:

1. Under **FortiManager/FortiAnalyzer**, select **Send logs to FortiManager/FortiAnalyzer**.
2. Enter the Internet-facing IP address of the FortiManager or FortiAnalyzer unit.
3. Select **Save** to save your settings.

To configure logging to a remote syslog server:

To use a client certificate for TLS authentication, enable **Use Client Certificate for TLS Authentication** and select a client certificate from the **Client certificate** dropdown.

1. Under **Remote Syslog**, select **Send system logs to remote Syslog servers**.
2. Move the remote syslog servers to which the logs will be sent from the **Available Syslog Servers** box to the **Chosen Syslog Servers** box.
   For information on adding syslog servers, see Syslog servers on page 324.
3. Select **Save** to save your settings.

To send debug logs to a remote syslog server:

1. Under **Remote Syslog**, select **Send debug logs to remote Syslog servers**.
2. Move the available applications for which debug logs are to be forwarded from the **Available Applications** box to the **Chosen Applications** box.
3. Move the remote syslog servers to which the debug logs will be sent from the **Available Syslog Servers** box to the **Chosen Syslog Servers** box.
4. Select **Save** to save your settings.

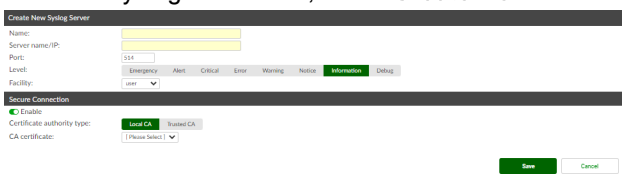
Syslog servers

Syslog servers can be used to store remote logs. To view the syslog server list, go to **Logging > Log Config > Syslog Servers**. A maximum of 20 syslog servers can be configured.

Create New	Add a new syslog server.
Delete	Delete the selected syslog server or servers.
Edit	Edit the selected syslog server.
Name	The syslog server name on FortiAuthenticator.
Server name/IP	The server name or IP address, and port number.

To add a syslog server:

1. From the syslog servers list, select **Create New**.



2. Enter the following information:

Name	Enter a name for the syslog server on FortiAuthenticator.
Server name/IP	Enter the syslog server name or IP address.
Port	Enter the syslog server port number. The default port is 514.
Level	Select a log level to store on the remote server from the dropdown menu. See Level on page 321.
Facility	Select a facility from the dropdown menu.
Secure Connection	
Enable	Enable to send syslog messages over TLS. This option is disabled by default.
Certificate authority type	Select either the **Local CA** or the **Trusted CA**.
CA certificate	From the dropdown, select a local CA certificate used to verify the syslog server certificate. This option is only available when the **Certificate authority type** is **Local CA**.
Trusted certificate	From the dropdown, select a trusted certificate used to verify the syslog server certificate. This option is only available when the **Certificate authority type** is **Trusted CA**.

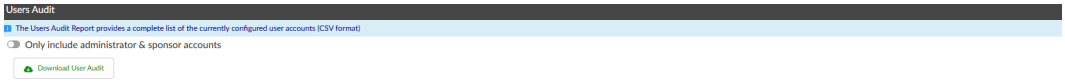
3. Select **Save** to add the syslog server.

Audit reports

User audit reports can be generated in order to comply with audit requirements. These reports include various attributes for all users configured on the FortiAuthenticator.

Users audit

To generate and download user audit reports, go to **Logging > Audit Reports > Users Audit** and select **Download User Audit**. A CSV format file will be saved to the computer.



Enable **Only include administrator & sponsor accounts** to include administrator and sponsor accounts in the user audit report.

Note: The **Only include administrator & sponsor accounts** option is disabled by default.

The following attributes are included in the `.CSV` file:

username	Username.
user type	Set to either **local**, **ldap**, or **radius**.
remote server name	Set to either **ldap** or **radius**, or empty for local.
first name	User's first name.
last name	User's last name.
email address	User's email address.
active	Set to either **t** for true/enabled or **f** for false/disabled.
role	Set to either **user**, **sponsor**, or **administrator**.
admin profile	One of the following: • Set to **full** if role is set to **administrator** with full permissions. • Set to their admin profile names separated by "/" for multiple profiles (e.g. **logging/saml**) if **role** is set to **administrator** without full permissions. • Empty is role is set to either **user** or **sponsor**.
lb synced	Load-balancing status.
trusted subnets	List of trusted subnets. **Note**: Values in the column can be a comma-separated list.
created	Date and time of account creation.
last used	Date and time of last login.
password auth	Password authentication status.
token type	Type of token-based authentication.
token info	Token information.

Troubleshooting

This chapter provides suggestions to resolve common problems encountered while configuring and using your FortiAuthenticator device, as well as information on viewing debug logs.

For more support, visit the Fortinet Support website.

Before starting, please ensure that your FortiAuthenticator device is plugged in to an appropriate, and functional, power source.

Troubleshooting

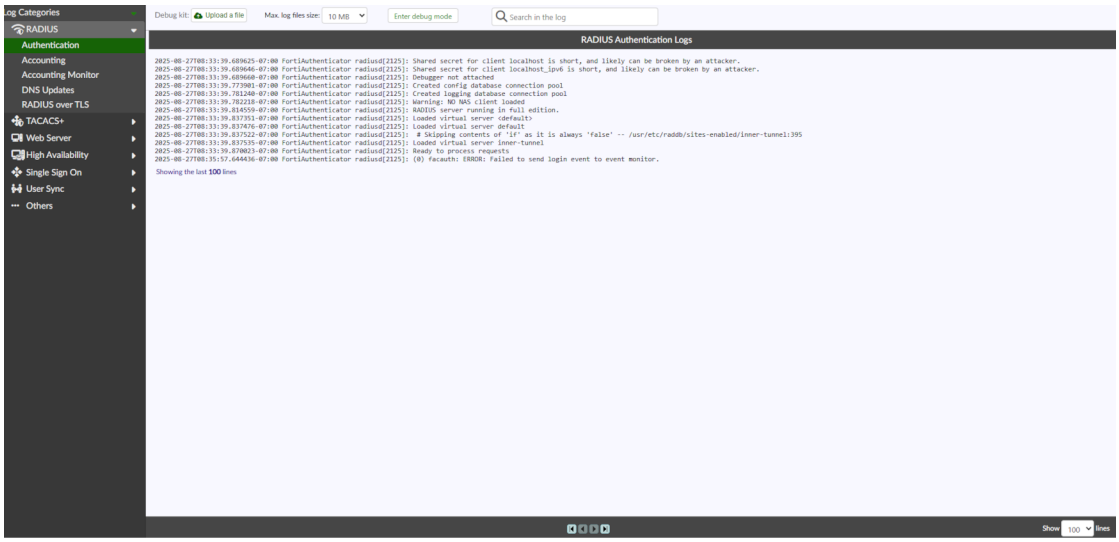
The following table describes some of the basic issues that can occur while using your FortiAuthenticator device, and suggestions on how to solve said issues.

Problem	Suggestions
All user log in attempts fail, there is no response from the FortiAuthenticator device, and there are no entries in the system log.	• Check that the authentication client has been correctly configured. See Adding FortiAuthenticator to your network on page 24. • If the authentication client is not configured, all requests are silently dropped. • Verify that traffic is reaching the FortiAuthenticator device. • Check to see if there is an intervening firewall blocking 1812/UDP RADIUS authentication traffic, if the routing correct, if the authentication client is configured with the correct IP address for FortiAuthenticator, etc.
All user log in attempts fail with the message **RADIUS ACCESS-REJECT**, and **invalid password** shown in the logs.	• Verify that the authentication client secrets are identical to those on FortiAuthenticator.
Generally, user log in attempts are successful, however an individual user authentication attempt fails with **invalid password** shown in the logs.	• Reset the user's password and try again. See Editing a user on page 99. • Have the user privately show their password to the administrator to check for unexpected characters (possibly due to keyboard regionalization issues).
Generally, user log in attempts are successful, however an individual user authentication attempt fails with **invalid token** shown in the logs.	• Verify that the user is not trying to use a previously used PIN. Tokens are one time passwords, so you cannot log in twice with the same PIN. • Verify that the time and timezone on FortiAuthenticator are correct and, preferably, synchronized using NTP. See Configuring the system date, time, and time zone on page 36.

Problem	Suggestions
	• Verify that the token is correctly synchronized with FortiAuthenticator, and verify the drift by synchronizing the token. • Verify the user is using the token assigned to them (validate the serial number against FortiAuthenticator configuration). See User management on page 94. • If the user is using an email or SMS token, verify it is being used within the valid timeout period. See Lockouts on page 85.

Debug logs

Extended debug logs can be accessed by using your web browser to browse to `https://<FortiAuthenticator-IP-Address>/debug`.



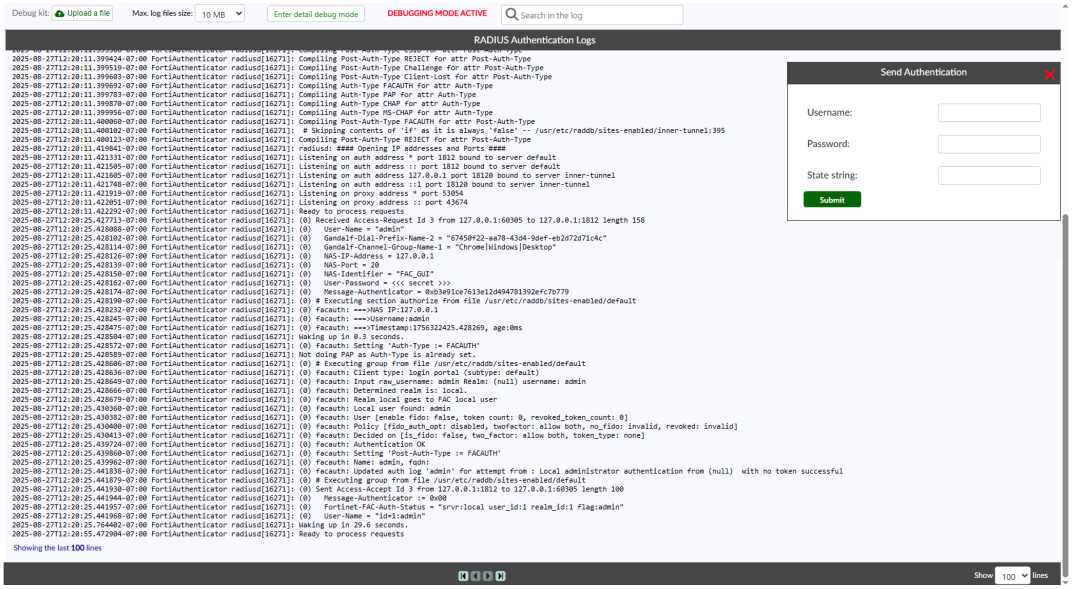
Log Categories	From the tree menu select a log type: • **RADIUS**: Authentication, Accounting, Accounting Monitor, DNS Updates, and RADIUS over TLS. • **TACACS+**: General, Authentication, Accounting, and Authorization. • **Web Server**: Apache, WAD, FastAPI, SAML, and Generic API. See FastAPI debug mode on page 331. • **High Availability**: Slony, Load Balancing, and Load Balancing HA Sync. • **Single Sign On**: FSSO Agent, FSSO Agent Filtered, and Domain Manager, and Syslog SSO. • **User Sync**: LDAP and SAML. • **Other**: GUI, REST API, LDAP, SCEP/CMP, Windows AD Monitor, SNMP, Disk Monitor, Hardware Monitor, Kernel, Updated, Config Monitor, and Database

	Monitor. **Note:** The **CLI Packet Capture (tcpdumpfile)** log category is only available when the `tcpdumpfile` command has been entered using SSH or through the CLI Console if a FortiAuthenticator is installed on a FortiHypervisor. For more information, see CLI commands on page 28.
Debug Kit	Select **Upload a file** to upload a debug kit from your computer. **Note**: The option is only available for some log types.
Max. log files size	From the dropdown, select the maximum log file size: • **200 KB** • **1 MB** • **10 MB** • **50 MB** • **100 MB** • **250 MB** • **500 MB** You can select up to a maximum of 500 MB. This gives you access to an extended history of debug files. **Note**: The option is only available for some log types.
Log level	From the dropdown, select the log severity level.
Enter debug mode	If **HA** or **RADIUS Authentication** is selected from the log category, the option to enter the debug mode is available. See RADIUS debugging on page 329.
Enter detail debugging mode	You can enter detailed debugging mode if **RADIUS Authentication** is selected from the log category. See RADIUS debugging on page 329.
Search	Enter a search term in the search field, then select **Search** to search the debug logs.
Page navigation	Use the **First Page**, **Previous Page**, **Next Page**, and **Last Page** icons to navigated through the logs.
Show	Select the number of lines to show per page from the dropdown menu. The options are: **100** (default), **250**, and **500**.

RADIUS debugging

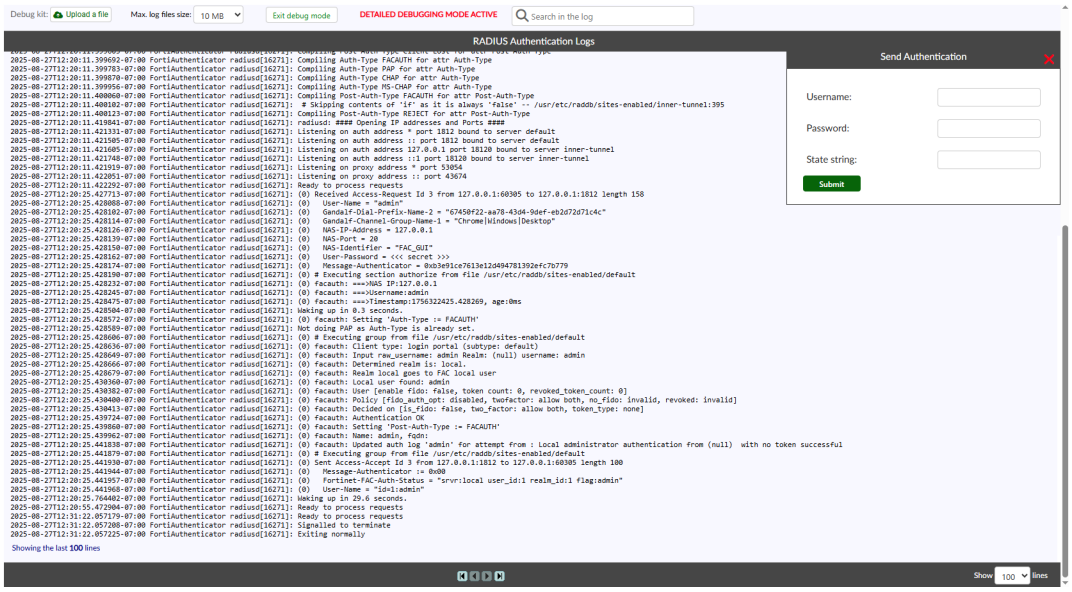
RADIUS authentication debugging mode can be accessed to debug RADIUS authentication issues.

From the **Log Categories** menu, select **RADIUS Authentication** and select **Enter debug mode** from the toolbar.



Enter the username and password and select **Submit** to test the RADIUS authentication and view the authentication response and returned attributes.

Select **Enter detail debug mode** to enter the detailed debug mode.



Enter the username and password and select **Submit** to test the RADIUS authentication and view the authentication response and returned attributes.

Select **Exit debug mode** to deactivate the debugging mode.

The following table lists the related CLI commands and GUI elements for RADIUS debugging:

CLI command	Description	GUI
`debug radius 0`	Put the RADIUS service into normal running mode (only error and system info debug logs).	**Exit debug mode**
`debug radius 1`	Put the RADIUS service into debug mode. **Note**: `debug radius 1` is the normal running mode in 6.4.x and below.	**Enter debug mode**
`debug radius 2`	`Put the RADIUS service into detailed debug mode.` **Note**: `debug radius 2 is the debug mode in 6.4.x and below.`	**Enter detail debug mode**

After a reboot, the RADIUS service will automatically be in the normal running mode (equivalent to `debug radius 0`).

TCP stack hardening

Configure the number of TCP SYNACK retries for the Linux kernel by accessing:

`https://<FortiAuthenticator-IP-Address>/debug/tcp_tuning`

Enter the number of retries between 1 - 255 (default = 3) and then select **Save**.

FastAPI debug mode

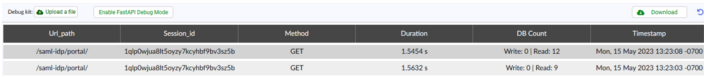
When **FastAPI** is selected in **Log Categories > Web Server**, **Enable FastAPI Debug Mode** button is available. Clicking **Enable FastAPI Debug Mode** allows you to record the activity according to the selected options:

Max request amount	The maximum number of requests: • **50** (default) • **100** • **150** • **200** • **250**
Debug run time	The debug run time: • **1 Minutes** (default)

- **10 Minutes**
- **1 Hour**
- **2 Hours**
- **4 Hours**
- **6 Hours**
- **1 Day**

For example, if the **Max request amount** is set to **50** and the **Debug run time** is **1 Minutes**, the FortiAuthenticator profiler tool saves the 50 slowest HTTP requests within the next 1 minute.

High level details of the slowest HTTP requests are displayed in the **Log Categories > Web Server > FastAPI** page.



Once the **Debug run time** has elapsed, click **Download** to download a report generated by the profiler tool with additional information.

Troubleshooting SMTP server tests

The following table describes some of the causes behind SMTP test failure and suggestions on how to solve the causes.

Cause	Further diagnostics	Troubleshooting tips
Unable to resolve SMTP server's FQDN.		Verify that the **Server name/IP** and DNS server settings are set correctly.
SMTP server did not respond.	Retry with other standard SMTP ports (25, 587, or 2525).	If there is no response from any port: • Verify that your network settings (interface subnet and static routes) are set properly. If there is a response from a different port: • SMTP server may be using port X.
SMTP server's certificate is signed by a non-trusted certificate.		Import the SMTP server's CA as a trusted CA.
SMTP server requires a secure connection.		Enable **STARTTLS** for **Secure connection**.
SMTP server requires authentication.		Enable **Enable authentication** and specify the credentials.
Invalid authentication credentials.		Verify that you configured the proper credentials.

Cause	Further diagnostics	Troubleshooting tips
SMTP server is unable to reverse resolve the FortiAuthenticator's IP (i.e. no DNS entry) to identify as a valid sender.		Update your DNS records.
SMTP server AUTH option must be set to "PLAIN".		Change your SMTP server authentication options.

PEAP troubleshooting

The topic describes common FortiAuthenticator 802.1x PEAP authentication issues and ways to troubleshoot them.

Issue: No mutually acceptable types found

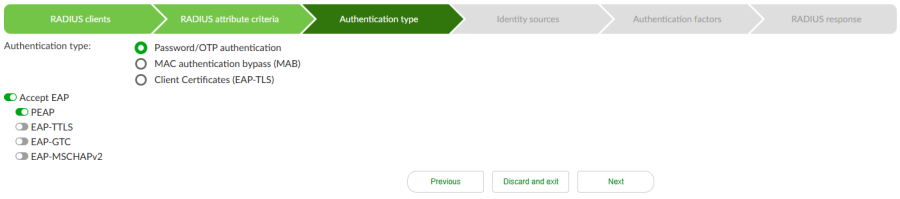
For PEAP authentication, FortiAuthenticator must accept the incoming EAP requests.

If FortiAuthenticator is not configured to accept the incoming EAP requests, the following error is returned:
`FortiAuthenticator radiusd[9216]: (9) eap: ERROR: No mutually acceptable types found`

Resolution

If the error is observed in the debug RADIUS log, ensure that the RADIUS policy configured to serve the 802.1x authentication requests accepts EAP requests with PEAP enabled.

See Policies on page 192.



Also, ensure that **Use Windows AD domain authentication** is enabled in the **Identity sources** tab in the RADIUS policy.

Issue: `NULL password is not allowed`

Resolution

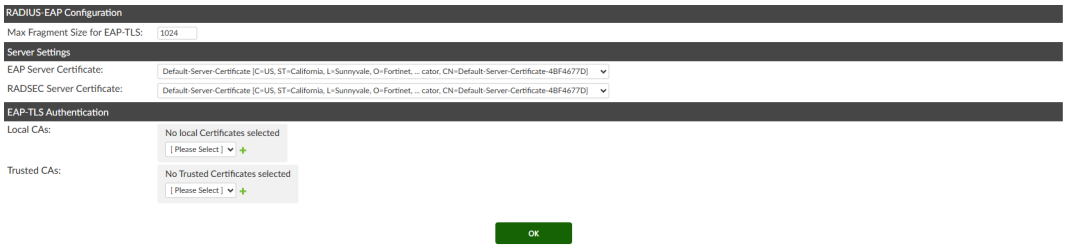
In the RADIUS log, if `NULL password is not allowed error` is displayed, ensure that **Use Windows AD domain authentication** is enabled in the **Identity sources** tab for the RADIUS policy.

See Policies on page 192.

PEAP requires MSCHAPv2 authentication method to be enabled in the RADIUS policy. MSCHAPv2 authentication is controlled by the **Use Windows AD domain authentication** setting.

Issue: Failed TLS handshake

FortiAuthenticator, as an 802.1x server, presents an EAP server certificate to a client.



See General on page 200.

If FortiAuthenticator EAP certificate is not trusted by the client, similar TLS errors appear in the RADIUS debug log:

```
FortiAuthenticator radiusd[1607]: (120) eap_peap: ERROR: (TLS) Alert write:fatal:bad record mac
FortiAuthenticator radiusd[1607]: (120) eap_peap: ERROR: (TLS) Failed reading from OpenSSL:
error:0A000119:SSL routines::decryption failed or bad record mac
FortiAuthenticator radiusd[1607]: (120) eap_peap: ERROR: (TLS) System call (I/O) error (-1)
FortiAuthenticator radiusd[1607]: (120) eap_peap: ERROR: (TLS) EAP Receive handshake failed during
operation
FortiAuthenticator radiusd[1607]: (120) eap_peap: ERROR: [eaptls process] = fail
```

Resolution

Windows wireless profile

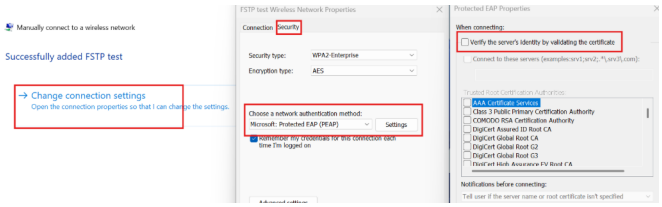
Windows may be configured to either validate or ignore untrusted EAP certificate. Commonly, this is done using the wireless network profiles pushed via GPO on an enterprise network.

For testing, a wireless profile can be created manually on the Windows endpoint which is helpful in verifying if FortiAuthenticator EAP server certificate is the root cause for TLS issues.

To manually configure a Windows wireless profile:

1. In the **Control Panel**, go to **Network and Internet > Network and Sharing Center**.
2. Select **Set up a new connection or network**.
   The **Set Up a Connection or Network** window opens.
3. Select **Manually connect to a wireless network** and click **Next**.
   The **Manually connect to a wireless network** window opens.
4. Match the name to a configured SSID.
5. From the **Security type** dropdown, select **WPA2-Enterprise**, and click **Next**.
   The network is successfully added.

6. Click **Change connection settings**.
   The **Network Properties** window opens.
7. Switch to the **Security** tab.
8. In **Choose a network authentication** method dropdown, select **Microsoft: Protected EAP (PEAP)**.
9. Ensure that **Remember my credentials for this connection each time I'm logged on** is selected.
10. Select **Settings**.
    The **Protected EAP Properties** window opens.
11. Clear **Verify server's identity by validating the certificate**, and click **OK**.
12. Click **OK**.
13. Click **Close**.



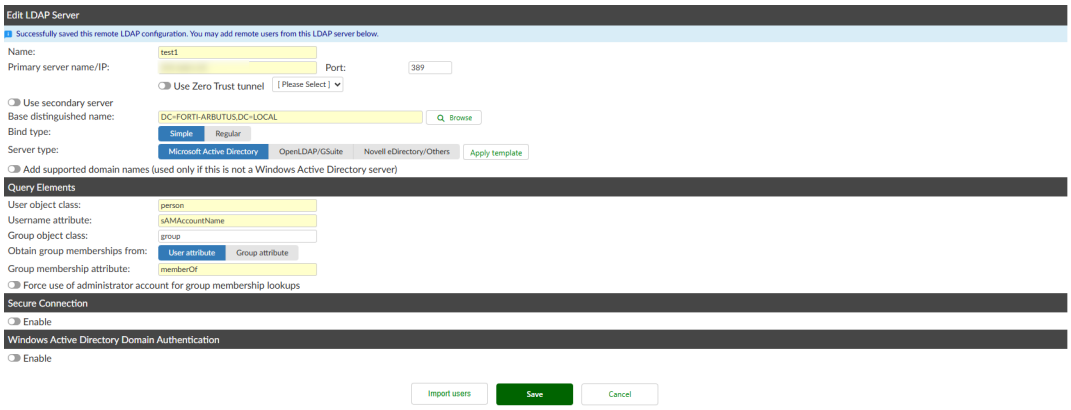
This ensures that the Windows endpoint does not validate FortiAuthenticator EAP certificate.

If TLS errors are no longer observed, validate FortiAuthenticator EAP certificate details and ensure that this is trusted by endpoints.

MSCHAPv2

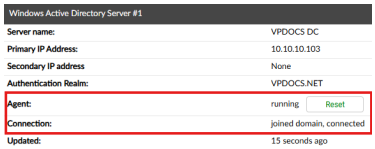
MSCHAPv2 authentication is controlled by the **Use Windows AD domain authentication** setting within individual RADIUS policies.

The setting directly relates to **Windows Active Directory Domain Authentication** setting when creating/editing an LDAP server in **Authentication > Remote Auth. Servers > LDAP**.



The status of the AD connection can be verified from **Monitor > Authentication > Windows AD**.

The following is an example of healthy status:



Issue: Reading winbind reply failed

(0xc0000001) error code indicates that a connection to AD is failing.

```
FortiAuthenticator radiusd[21452]: (5) mschap: ERROR: Program returned code (1)
and output 'Reading winbind reply failed! (0xc0000001)'
FortiAuthenticator radiusd[21452]: (5) mschap: Authentication failed
FortiAuthenticator radiusd[21452]: (5) facauth: Module-Failure-Message:
mschap: Program returned code (1) and output 'Reading winbind reply failed! (0xc0000001)'
FortiAuthenticator radiusd[21452]: (5) facauth: MS-CHAP-Error: CE=691 R=1
C=bd20eae31c9e2ec1f95e4b8ed604866f V=3 M=Authentication failed
```

Note: The error is observed when MSCHAPv2 is enabled in a RADIUS policy.

See Windows AD connection troubleshooting on page 337.

Issue: The attempted logon is invalid

(0xc000006d) error is related to an AD connection status as well.

Ensure that the FortiAuthenticator AD connection status is **running** and **joined domain**, **connected**.

See Windows AD connection troubleshooting on page 337.

```
FortiAuthenticator radiusd[11990]: (87) mschap: ERROR: MS-CHAP2-Response is incorrect
FortiAuthenticator radiusd[11990]: (87) facauth: Module-Failure-Message:
mschap: Program returned code (1) and output 'The attempted logon is invalid.
This is either due to a bad username or authentication information. (0xc000006d)
```

For more information on the error codes, see the table in 4776(S, F): The computer attempted to validate the credentials for an account.

0xc000006d error may indicate a generic logon failure.

A potential cause:

- An invalid username and/or password was used.

Issue: No logon servers are currently available

Check the connection to the AD server.

```
2025-03-05T11:29:28.995739-08:00 FortiAuthenticator radiusd[1499]: (3) facauth: ERROR: Program
returned code (1) and output 'NT_STATUS_NO_LOGON_SERVERS:
No logon servers are currently available to service the logon request. (0xc000005e)'
```

See Windows AD connection troubleshooting on page 337.

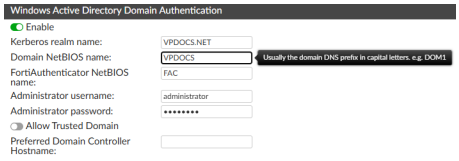
Windows AD connection troubleshooting

The topic provides a checklist to troubleshoot Windows AD connection issues on FortiAuthenticator.

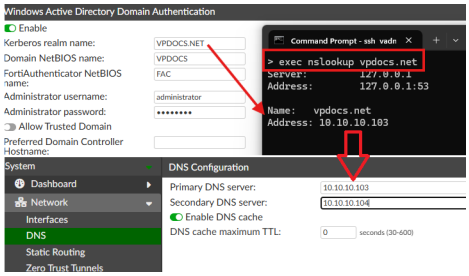
Checklist

Ensure that the AD connection is established and is stable:

1. Verify the **Windows Active Directory Domain Authentication** settings are filled in correctly when creating/editing an LDAP server in **Authentication > Remote Auth. Servers > LDAP**.

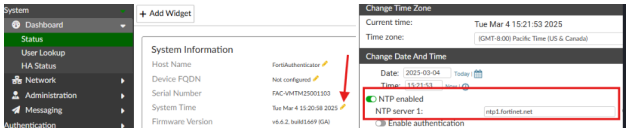


2. Ensure that FortiAuthenticator resolves AD domain names.
Set FortiAuthenticator DNS server to one of the domain controllers or domain controller FortiAuthenticator is connecting to.



Though recommended, new FortiAuthenticator versions do not depend on setting the DNS to one of the domain controllers.

3. Check the NTP source to ensure that the time is synchronized between the domain controller and FortiAuthenticator.



4. Ensure that the account specified in **Administrator username** in **Windows Active Directory Domain Authentication** has sufficient permission to join FortiAuthenticator to a domain.

To rule out account permissions issue, always use the domain administrator account.

See Configure minimum privilege Windows AD user account on page 181.

Common issues

When troubleshooting AD connection issues, look into the raw log (**Logging > Log Access > Logs**) and the **Windows AD Monitor** debug log available in the **Other** category when you go to the extended debug logs in `https://<FortiAuthenticator-IP-Address>/debug`.

Issue: DNS related

If the FortiAuthenticator is not configured with a DNS server that resolves the DNS names of the domain it is joining, this may result in connection failure.

```
FortiAuthenticator netadsjoin[srvid:1]: DNS update failed: NT_STATUS_INVALID_PARAMETER
FortiAuthenticator netadsjoin[srvid:1]: No DNS domain configured for . Unable to perform DNS
Update
```

Issue: Invalid domain

When the administrator account username/password is invalid, FortiAuthenticator presents the following error:

```
FortiAuthenticator winad_mon[1510]: Failed to join Windows AD network: VPDOCS.NET
```

```
FortiAuthenticator netadsjoin[srvid:1]: Failed to join domain: failed to lookup DC info for domain
'VPDOCS.NET' over rpc: The attempted logon is invalid. This is either due to bad username or
authentication information.
```

Ensure that the credentials are correct.

Issue: Time drift

When the time between FortiAuthenticator and DC is misaligned, user authentication carried over Kerberos may fail, resulting in an error similar to the one below.


```
FortiAuthenticator winad_mon[1510]: Wbinfo ping failed for LDAP 1, rc 110
FortiAuthenticator winad_mon[1510]: Rejoin request for LDAP 1. Reason:  winbind error [0], radius
error [0], ping auth error [1]
FortiAuthenticator winad_mon[1510]:  * try ads join for server 1
FortiAuthenticator netadsjoin[srvid:1]: gse_get_client_auth_token: gss_init_sec_context failed
with [ Miscellaneous failure (see text): FAST fast response is missing FX-FAST (ldap/vp-
dc.vpdocs.net@VPDOCS.NET)](2529639059)
FortiAuthenticator netadsjoin[srvid:1]: ads_sasl_spnego_bind: kinit succeeded but SPNEGO bind with
Kerberos failed for ldap/vp-dc.vpdocs.net - user[administrator], realm[VPDOCS.NET]: The attempted
logon is invalid. This is either due to a bad username or authentication information.
FortiAuthenticator netadsjoin[srvid:1]: gse_get_client_auth_token: gss_init_sec_context failed
with [ Miscellaneous failure (see text): FAST fast response is missing FX-FAST (cifs/vp-
dc.vpdocs.net@VPDOCS.NET)](2529639059)
```

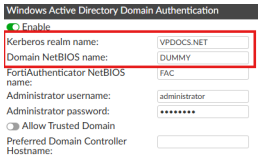
Check the NTP settings on FortiAuthenticator. See step 3 in the Checklist on page 337.

Note: Windows AD debug logs may directly specify a time drift error which is more descriptive than in the log above.

Issue: Invalid configuration

When **Windows Active Directory Domain Authentication** is invalid, FortiAuthenticator notifies about this in the debug log.

This is related to the **Kerberos realm name** field when creating/editing an LDAP server in **Authentication > Remote Auth. Servers > LDAP**.



Always double-check the **Kerberos realm name** and the **Domain NetBIOS name** fields.

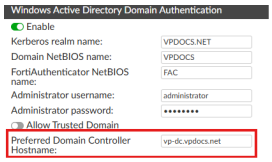
Every individual domain join connection (within one FortiAuthenticator or across many FortiAuthenticator devices) must use a unique **Domain NetBIOS name**.

Issue: Preferred domain controller hostname

With multiple domain controllers in an AD environment, FortiAuthenticator may have issues joining a domain.

If FortiAuthenticator fails to join to AD with multiple DCs and items in the Checklist on page 337 are checked, add one of the domain controller hostname in the **Preferred Domain Controller Hostname** field.

For reliability, add the hostname of a configured LDAP server.



LDAP filter syntax

This chapter outlines some basic filter syntax that is used to select users and groups in LDAP User Import, Dynamic LDAP Groups, and Remote User Sync Rules.

Filters are constructed using logical operators:

=	Equal to
~=	Approximately equal to
<=	Lexicographically less than or equal to
>=	Lexicographically greater than or equal to
&	AND
|	OR
!	NOT

Filters can consist of multiple elements, such as `(&(filter1)(filter2))`.

More information about the query syntax of AD filters, see the following web sites:

- Search Filter Syntax
- Active Directory: LDAP Syntax Filters

Examples

The following examples are for a Windows 2008 AD server with the domain **corp.example.com**, default domain administrators and users, and an additional group called FW_Admins:

- Users (CN) = atano, pjfry, tleela, tbother
- FW_Admins (Security Group) = atano, tbother

An unfiltered browse will return all results from the query, including system and computer accounts. To prevent this and only return user accounts, apply the filter `(objectClass=person)` or `(objectCategory=user)`.

Even if unfiltered, only user accounts are imported, so this is only required to clean up the results that are displayed in the GUI.

To filter and return only members of the security group: `(&(objectCategory=user)(memberOf=CN=FW_Admin,DC=corp,DC=example,DC=com))`.

It is not possible to use the filter to limit results to CNs or OUs. To achieve this, you must change the Base DN in the LDAP Server configuration. For example, to return only users from the CompanyA OU, create an LDAP Server entry with the following Base DN: `OU=CompanyA,DC=corp,DC=example,DC=com`.

Caveats

Users do not always have a **memberOf** property for their primary group, this means that querying system groups, such as Domain Users, may return zero results. This can be confusing as these are often the first queries tried, and can lead the user to think the filter syntax is incorrect.

For example: `(memberOf=CN=Domain Users,CN=Domain Admins,DC=corp,DC=example,DC=com)` will return no valid results.

To return all users in such a group, the filter can be made against the ID value of the Primary Group. So, for Domain Users (Group ID = 513), the filter would be: `(primaryGroupId=513)`.

www.fortinet.com