SAML Interoperability Guide

FortiAuthenticator 8.0.0

FORTINET®

October 2, 2025
FortiAuthenticator 8.0.0 SAML Interoperability Guide
23-800-1084129-20251002

TABLE OF CONTENTS

Change Log

Date	Change Description
2025-10-02	Initial release.

About this Guide

The purpose of this guide is to aid in the configuration of Security Assertion Markup Language (SAML) authentication using FortiAuthenticator for Fortinet solutions.

Testing was performed with the following product versions:

- FortiAuthenticator 6.4.1
- FortiGate 7.0.2
- FortiManager 7.0.2
- FortiAnalyzer 7.0.2

FortiAuthenticator setup

This section includes configuration information for the FortiAuthenticator. Any deviations from this configuration will be detailed in the relevant section. For more information on the setup and configuration of the FortiAuthenticator, see the *FortiAuthenticator Administration Guide* on the Fortinet Docs Library.

This section includes the following information:

- Initial setup on page 6
- System settings on page 7
- Registering a token on page 7
- Creating a test user on page 8
- Configuring SAML settings on page 9

Initial setup

Upon initial deployment, the FortiAuthenticator is configured to the following default settings:

```
Port 1 IP: 192.168.1.99
Port 1 Netmask: 255.255.255.0
Default Gateway: 192.168.1.1
```

These settings can be modified by configuring a PC to an address on the same subnet and accessing the GUI via https://192.168.1.99/. Alternatively, you can configure these settings using the CLI.

To configure basic settings using the CLI:

1. Connect the management computer to the FortiAuthenticator using the supplied console cable.
2. Log in to the FortiAuthenticator unit using the default credentials below:
   ```
   Username: admin
   Password: <blank>
   ```
   You will be prompted to change and confirm your new password.
3. Configure the network settings as required, for example:
   ```
   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. This will give you access to the GUI through the specified IP address.

For more information on FortiAuthenticator initial setup, see the *FortiAuthenticator Administration Guide* in the Fortinet Document Library.

System settings

Once the initial setup of the FortiAuthenticator is complete, further configuration can be performed through the GUI.

DNS

To enable resolution of the FortiGuard network and other systems such as NTP servers, set your DNS to your local or ISP nameserver configuration via *Network > DNS*.

Configure the FQDN

You can configure the FQDN for the FortiAuthenticator from the *System Information* widget in *System > Dashboard*. Click the *edit* icon next to *Device FQDN* to open the *Edit Device FQDN* window, enter a name for *Fully qualified domain name*, and click *OK*.

Registering a token

Registering FortiToken

In order to test two-factor authentication, a token is required. The configuration instructions included in this guide use FortiToken.

For security reasons, a token can only be automatically registered from the FortiGuard network a single time. If you need to register it a subsequent time, please contact Fortinet support.

To register a FortiToken:

1. Go to *Authentication > User Management > FortiTokens*, and select *Create New*.
2. Select the *Token type* and enter the FortiToken *Serial number* or *Activation code*. Click *OK*.
   Once registered, tokens will be displayed with an *Available* status.

You can also deploy FortiToken Cloud to add multi-factor authentication (MFA) for users.

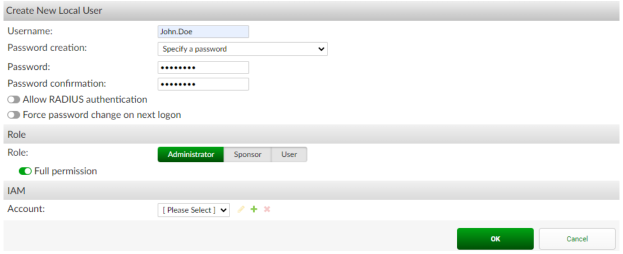
Creating a test user

Create a single test user with FortiToken Mobile two-factor authentication enabled.

If required, remote LDAP and RADIUS users can also be set up.
To configure remote RADIUS and LDAP users, see Remote users.

To create the user:

1. Go to *Authentication > User Management > Local Users*, and select *Create New*.
2. Enter a username and password for the local user.
3. Disable *Allow RADIUS authentication*.



Create New Local User

Username:	John.Doe
Password creation:	Specify a password
Password:	••••••••
Password confirmation:	••••••••

○ Allow RADIUS authentication
○ Force password change on next logon

Role

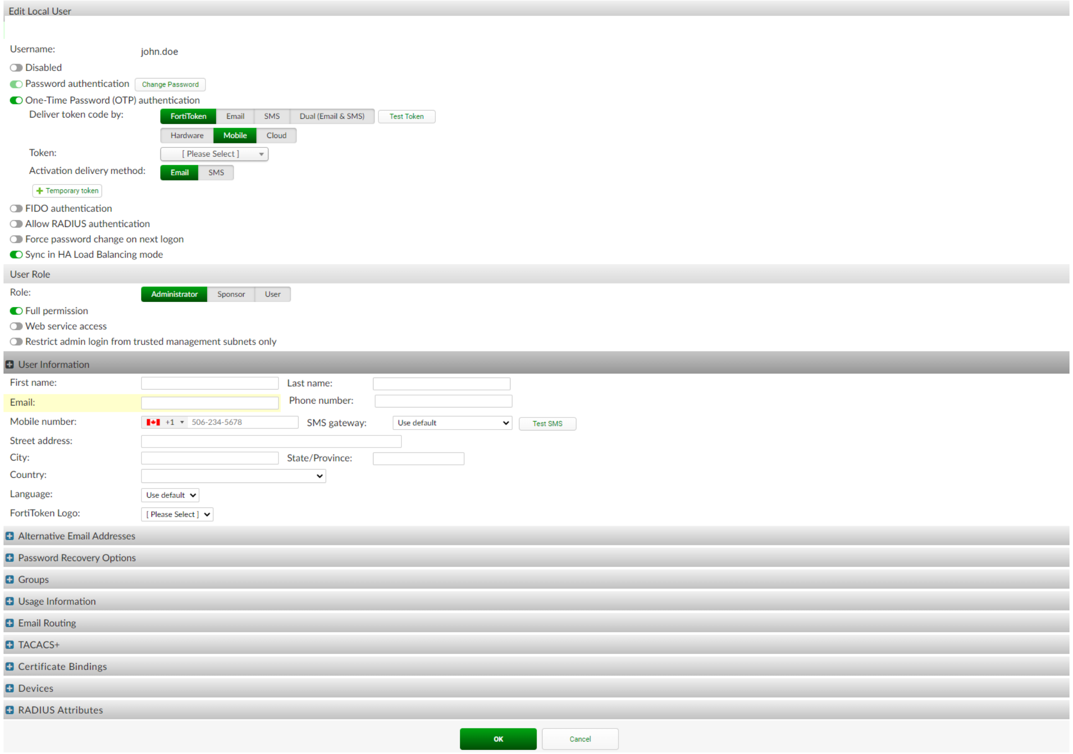
Role:	[✓ Administrator] Sponsor User

● Full permission

IAM

Account:	[Please Select]

4. Click *OK* and enter password to validate.
5. Enable *One-Time Password (OTP) authentication* and choose *Deliver token code by FortiToken Mobile*.
   Select FortiToken Mobile added earlier from the relevant dropdown menu.
6. Set the *Activation delivery method* to *Email*.
   This will automatically open the *User Information* section where you can enter the user email address in the field provided.
7. Click *OK* to save changes to the local user.
   The activation information is sent to the user via the email address provided in the *User Information* pane.



Edit Local User

Username: john.doe

○ Disabled

● Password authentication

● One-Time Password (OTP) authentication

Deliver token code by: [✓ FortiToken] Email SMS Dual (Email & SMS)

Hardware [✓ Mobile] Cloud

Token: [Please Select]

Activation delivery method: [✓ Email] SMS

○ FIDO authentication

○ Allow RADIUS authentication

○ Force password change on next logon

● Sync in HA Load Balancing mode

User Role

Role: [✓ Administrator] Sponsor User

● Full permission

○ Web service access

○ Restrict admin login from trusted management subnets only

User Information

First name:

Last name:

Email:

Phone number:

Mobile number: +1 506-234-5678

SMS gateway: Use default

Street address:

City:

State/Province:

Country:

Language: Use default

FortiToken Logo: [Please Select]

8. Open the email to complete the activation and install the token to the FortiToken Mobile app.

Configuring SAML settings

The following section includes information on how to configure the FortiAuthenticator as the SAML IdP. In addition to the IdP settings, SAML SP settings must be configured on the FortiAuthenticator for each SAML SP device.

This section includes the following instructions:

1. Configuring FortiAuthenticator IdP on page 10
2. Configuring SP settings on FortiAuthenticator on page 11

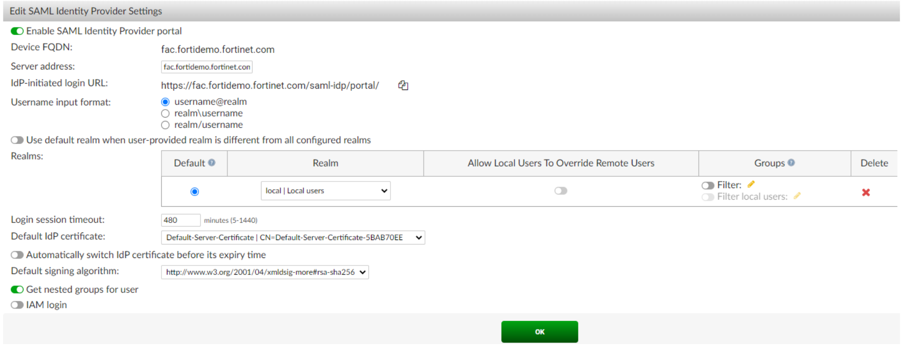
Configuring FortiAuthenticator IdP

To configure FortiAuthenticator IdP:

1. Go to *Authentication > SAML IdP > General*.
2. Enable *SAML Identity Provider portal*, and enter the following information:
    - **Server address**: Enter the device FQDN of the FortiAuthenticator IdP.

      > *Device FQDN* can be configured from the *System Information* widget in *System > Dashboard > Status*.
      >
      > See Configure the FQDN on page 7.

    - **Username input format**: Select the default username input format.
      The default is *username@realm*.
    - **Realms**: In the dropdown, select the local realm.
      Optionally, for group filtering, enable *Filter*, click the pen icon to edit, select groups from the *Available User Groups* search box, and click *OK*.
    - **Default IdP certificate**: Select a default certificate to use in your SAML configuration.
      The certificate is used in the https connection to the IdP portal.



Edit SAML Identity Provider Settings

● Enable SAML Identity Provider portal

Device FQDN: fac.fortidemo.fortinet.com

Server address: fac.fortidemo.fortinet.con

IdP-initiated login URL: https://fac.fortidemo.fortinet.com/saml-idp/portal/

Username input format:
● username@realm
○ realm\username
○ realm/username

○ Use default realm when user-provided realm is different from all configured realms

Realms:

Default	Realm	Allow Local Users To Override Remote Users	Groups	Delete
●	local | Local users	○	○ Filter: ○ Filter local users:	✖

Login session timeout: 480 minutes (5-1440)

Default IdP certificate: Default-Server-Certificate | CN=Default-Server-Certificate-5BAB70EE

○ Automatically switch IdP certificate before its expiry time

Default signing algorithm: http://www.w3.org/2001/04/xmldsig-more#rsa-sha256

● Get nested groups for user

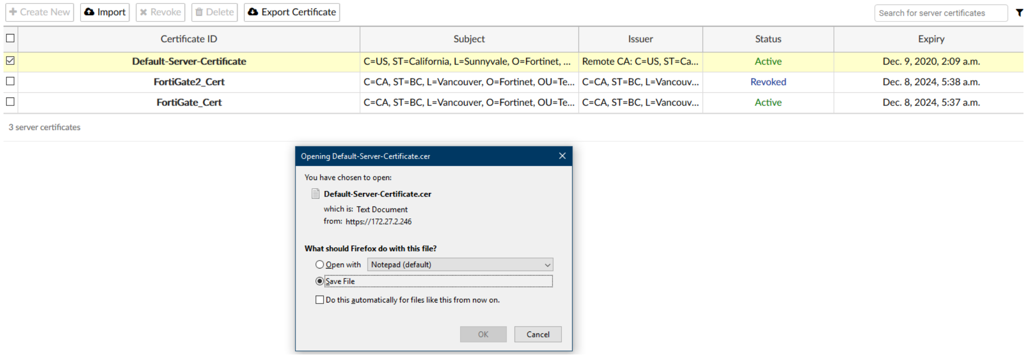
○ IAM login

3. Click *OK*.
   Once the IdP has been configured, you can proceed with setting up the service provider(s) of your choice.

In addition to configuring the SAML IdP settings, you will also need to select and export the default IdP certificate for use on the service providers.

To export the IdP certificate:

1. Go to *Certificate Management > End Entities > Local Services*.
2. Select the certificate used in the SAML IdP and click *Export Certificate*.



☐	Certificate ID	Subject	Issuer	Status	Expiry
☑	Default-Server-Certificate	C=US, ST=California, L=Sunnyvale, O=Fortinet, ...	Remote CA: C=US, ST=Ca...	Active	Dec. 9, 2020, 2:09 a.m.
☐	FortiGate2_Cert	C=CA, ST=BC, L=Vancouver, O=Fortinet, OU=Te...	C=CA, ST=BC, L=Vancouv...	Revoked	Dec. 8, 2024, 5:38 a.m.
☐	FortiGate_Cert	C=CA, ST=BC, L=Vancouver, O=Fortinet, OU=Te...	C=CA, ST=BC, L=Vancouv...	Active	Dec. 8, 2024, 5:37 a.m.

3 server certificates

Opening Default-Server-Certificate.cer

You have chosen to open:

Default-Server-Certificate.cer

which is: Text Document
from: https://172.27.2.246

What should Firefox do with this file?

○ Open with Notepad (default)
● Save File
☐ Do this automatically for files like this from now on.

Configuring SP settings on FortiAuthenticator

In order to complete the following configuration, you will need to configure the SAML settings on the SP device at the same time. This is because some fields including the SP entity ID, SP ACS URL, and SP SLS URL are only available when configuring the SAML settings on the SP device.

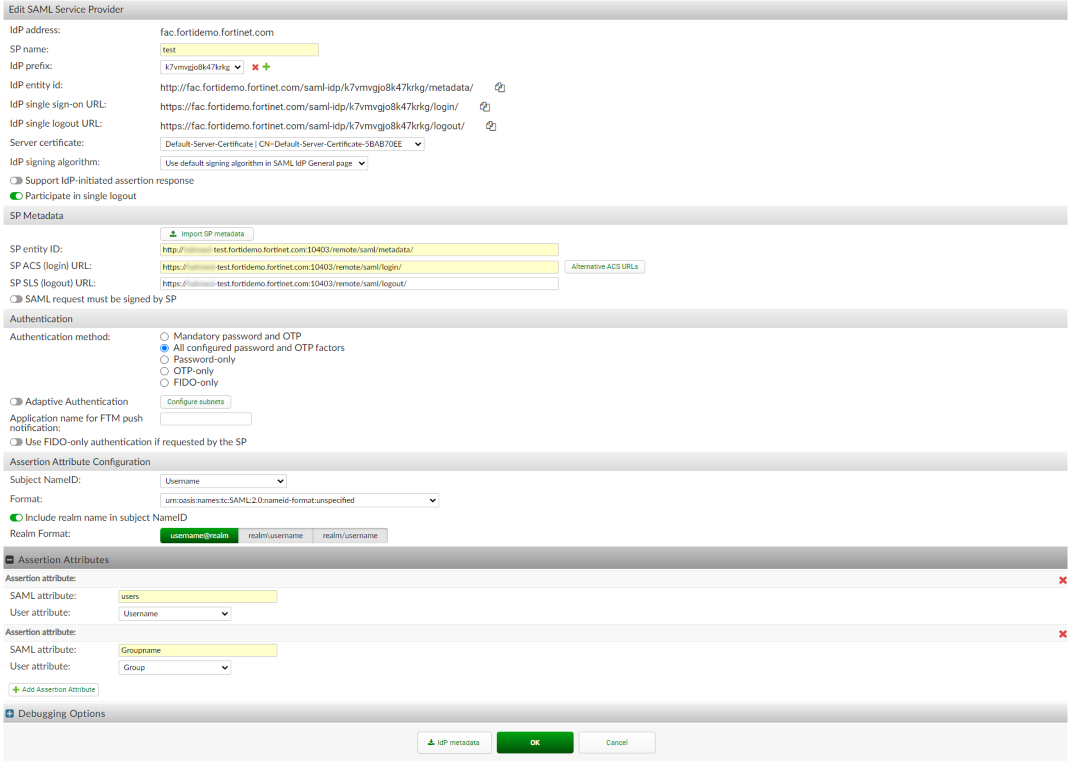
To configure service provider settings on the FortiAuthenticator:

1. Go to *Authentication > SAML IdP > Service Providers*, and click *Create New*.
2. Enter the following information:
    - **SP name**: Enter a name for the SP device.
    - **IDP prefix**: Select *+*, enter an IdP prefix in the *Create Alternate IdP Prefix* dialog or select *Generate prefix*, and click *OK*.
    - **Server certificate**: Select the same certificate as the default IdP certificate used in *Authentication > SAML IdP > General*. See Configuring FortiAuthenticator IdP on page 10.
    - Enable *Participate in single logout* to send logout requests to this SP when the user logs out from the IdP.
    - **Authentication method**: Select an authentication method.
3. Click *Save*.
4. The details for following settings are available when configuring the service provider device (e.g. a FortiAnalyzer or a FortiGate).
    - **SP entity ID**: Enter the SP entity ID.
    - **SP ACS (login) URL**: Enter the SP Assertion Consumer Service (ACS) login URL.
    - **SP SLS (logout) URL**: Enter the SP Single Logout Service (SLS) logout URL.

> ⚠ *SP entity ID*, *SP ACS (login) URL*, and *SP SLS (logout) URL* must match their respective configurations on the service provider device side, e.g., FortiGate, FortiManager, or a FortiAnalyzer.
>
> See Creating a new SAML user and server on page 14, FortiManager on page 18, and FortiAnalyzer on page 20.

5. Click *OK*.
6. Select and click *Edit* to edit the recently created SP.

7. In *Assertion Attribute Configuration*:
   a. Select *Username* from the *Subject NameID* dropdown.
   b. Select *urn:oasis:names:tc:SAML:2.0:nameid-format:unspecified* in *Format*.
8. In *Assertion Attributes*, select *Add Assertion Attribute*:
   a. Enter a name for the SAML attribute.
   b. Select *Username* from the *User attribute* dropdown.
   c. Select *Add Assertion Attribute* again and create a new SAML attribute with *User attribute* as *Group*.
9. Click *OK* to save changes.



Edit SAML Service Provider

IdP address: fac.fortidemo.fortinet.com
SP name: test
IdP prefix: k7vmvgjo8k47krkg
IdP entity id: http://fac.fortidemo.fortinet.com/saml-idp/k7vmvgjo8k47krkg/metadata/
IdP single sign-on URL: https://fac.fortidemo.fortinet.com/saml-idp/k7vmvgjo8k47krkg/login/
IdP single logout URL: https://fac.fortidemo.fortinet.com/saml-idp/k7vmvgjo8k47krkg/logout/
Server certificate: Default-Server-Certificate | CN=Default-Server-Certificate-5BAB70EE
IdP signing algorithm: Use default signing algorithm in SAML IdP General page
○ Support IdP-initiated assertion response
● Participate in single logout

SP Metadata

SP entity ID: http://[redacted]-test.fortidemo.fortinet.com:10403/remote/saml/metadata/
SP ACS (login) URL: https://[redacted]-test.fortidemo.fortinet.com:10403/remote/saml/login/
SP SLS (logout) URL: https://[redacted]-test.fortidemo.fortinet.com:10403/remote/saml/logout/
○ SAML request must be signed by SP

Authentication

Authentication method:
○ Mandatory password and OTP
● All configured password and OTP factors
○ Password-only
○ OTP-only
○ FIDO-only

○ Adaptive Authentication

Application name for FTM push notification:
○ Use FIDO-only authentication if requested by the SP

Assertion Attribute Configuration

Subject NameID: Username
Format: urn:oasis:names:tc:SAML:2.0:nameid-format:unspecified
● Include realm name in subject NameID
Realm Format: [✓ username@realm] realm\username realm/username

Assertion Attributes

Assertion attribute:
SAML attribute: users
User attribute: Username

Assertion attribute:
SAML attribute: Groupname
User attribute: Group

FortiGate

Before proceeding, ensure that system settings are up to date. See System settings on page 7.

FortiGate 7.0.2 was used to perform the testing.

The FortiGate appliance is the Gateway to your network, therefore, securing remote access, whether administrative access to the appliance itself or VPN access to the network behind it, is critical.

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, Salesforce, and FortiGate. FortiAuthenticator can be configured as an IdP, providing trust relationship authentication for unauthenticated users trying to access an SP.

One advantage of SAML authentication is that two-factor authentication can be provided by the SAML Identity Provider (IdP).

This chapter demonstrates configuring SAML SSO using a FortiGate as an SP and FortiAuthenticator as an IdP to allow users to log in through an SSL VPN portal.

See Configuring SAML SSO in the GUI.

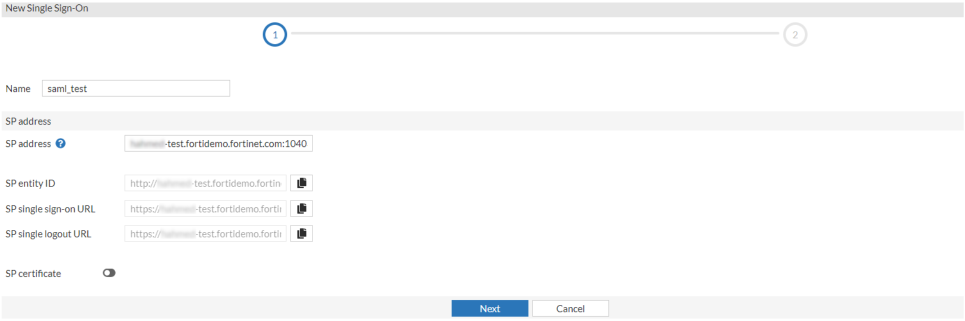
To configure SAML SSO using FortiAuthenticator:

1. Configuring FortiAuthenticator local users and registering a token:
    a. Registering a token on page 7
    b. Creating a test user on page 8
2. Configuring a SAML IdP and a service provider:
    a. Configuring FortiAuthenticator IdP on page 10
    b. Configuring SP settings on FortiAuthenticator on page 11
3. Configuring the FortiGate SAML related settings:
    a. Creating a new SAML user and server on page 14
4. Example: FortiGate SSL-VPN related settings:
    a. Adding SAML group to SSL VPN settings example on page 16
    b. Configuring a firewall policy to allow SSL VPN access example on page 17

Creating a new SAML user and server

To create a new SAML server from the GUI:

1. Go to *User & Authentication > Single Sign-On* and select *Create New*.
   The single-sign on wizard opens.
2. Enter a name for the SAML server.
   The other fields automatically populate based on the FortiGate's WAN IP and port.



Name: saml_test

SP address: [redacted]-test.fortidemo.fortinet.com:1040

SP entity ID: http://[redacted]-test.fortidemo.fortin

SP single sign-on URL: https://[redacted]-test.fortidemo.fortii

SP single logout URL: https://[redacted]-test.fortidemo.fortii

SP certificate: ○

Click the icon beside the *SP entity ID*, *SP single sign-on URL*, and *SP single logout URL* fields to copy the text.

SP entity ID, *SP single sign-on URL*, and *SP single logout URL* are then used when configuring SP settings on FortiAuthenticator.

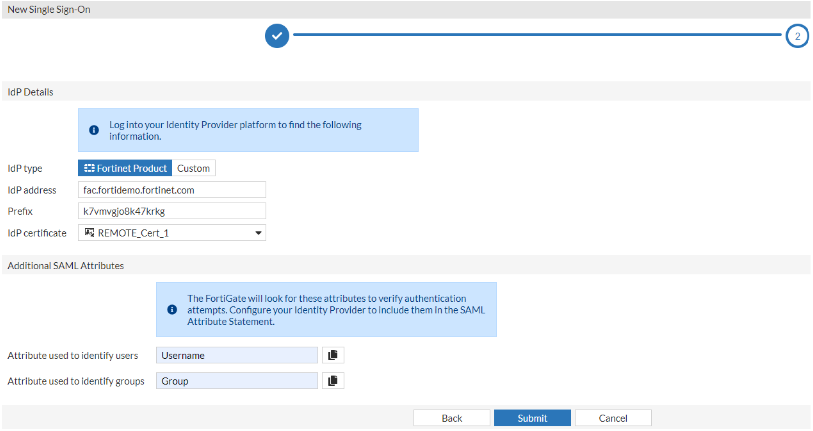
See Configuring SP settings on FortiAuthenticator on page 11.

3. Click *Next*.
4. In *IdP Details*:
   a. In *IdP address*, enter the IdP address from the FortiAuthenticator.
   b. In *Prefix*, enter the prefix from the FortiAuthenticator.
   c. In *IdP certificate*, select *REMOTE_Cert_1*.
5. In *Additional SAML Attributes*:
   a. In *Attribute used to identify users*, enter *Username*.
   b. In *Attribute used to identify groups*, enter *Group*.

In FortiAuthenticator IdP, SAML attributes are configured in the *Assertion Attributes* pane when configuring the SP settings.

See Configuring SP settings on FortiAuthenticator on page 11.

6. Click *Submit.*



New Single Sign-On

IdP Details

Log into your Identity Provider platform to find the following information.

IdP type: Fortinet Product | Custom

IdP address: fac.fortidemo.fortinet.com

Prefix: k7vmvgjo8k47krkg

IdP certificate: REMOTE_Cert_1

Additional SAML Attributes

The FortiGate will look for these attributes to verify authentication attempts. Configure your Identity Provider to include them in the SAML Attribute Statement.

Attribute used to identify users: Username

Attribute used to identify groups: Group

SAML related settings are available in the GUI for FortiOS 7.0.2 and above.
For FortiOS 7.0.1 and below, use the CLI commands to set up SAML related settings.

To create a new SAML user and server from the CLI:

1. Enter the following commands to create a SAML user object:

```
config user saml
  edit "saml_test"
     set cert "FortiDemo"
     set entity-id "http://[redacted]-test.fortidemo.fortinet.com:10403/remote/saml/metadata/"
     set single-sign-on-url "https://[redacted]-
           test.fortidemo.fortinet.com:10403/remote/saml/login/"
     set single-logout-url "https://[redacted]-
           test.fortidemo.fortinet.com:10403/remote/saml/logout/"
     set idp-entity-id "http://fac.fortidemo.fortinet.com/saml-
           idp/k7vmvgjo8k47krkg/metadata/"
     set idp-single-sign-on-url "https://fac.fortidemo.fortinet.com/saml-
           idp/k7vmvgjo8k47krkg/login/"
     set idp-single-logout-url "https://fac.fortidemo.fortinet.com/saml-
           idp/k7vmvgjo8k47krkg/logout/"
     set idp-cert "REMOTE_Cert_1"
     set user-name "Username"
     set group-name "Group"
     set digest-method sha1
  next
end
```

In the above CLI commands:

- The cert `FortiDemo` is a local certificate used to sign SAML messages exchanged between the client and the FortiGate SP. In this case, it is used to sign [redacted]`-test.fortidemo.fortinet.com`.
- The cert `REMOTE_Cert_1` is a remote certificate used to identify the IdP, which in this case is `fac.fortidemo.fortinet.com`.

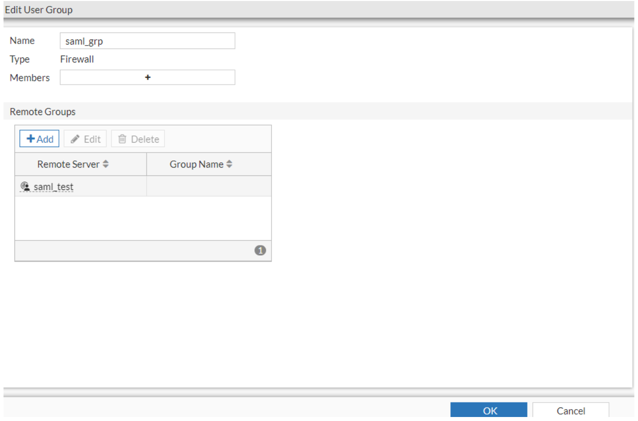
In the SP URL above:

- [redacted]`-test.fortidemo.fortinet.com`- FQDN that resolves to the FortiGate SP.
- `10403`- Port used to map FortiGate SAML SP service.

- `/remote/saml`- Custom user defined fields, typically to identify the service, i.e., remote access and SAML authentication.
- `metadata`, `/login`, and `/logout`- Standard convention used to identify the SP entity, login, and logout portal.

To create the SAML group:

1. Go to *User & Authentication >User Groups* and click *Create New*.
2. Enter a name for the group.
3. In Remote Groups, select *Add*, in the *Remote Server* dropdown, select *saml_test*, and click *OK*.
4. Click *OK*.



Edit User Group

Name: saml_grp
Type: Firewall
Members: +

Remote Groups

Remote Server	Group Name
saml_test	

To create the SAML group using the CLI:

1. Enter the following commands to add the SAML user object to a new user group:

```
config user group
  edit "saml_grp"
     set member "saml_test"
  next
end
```

The CLI commands above are based on their respective settings in the GUI.

Adding SAML group to SSL VPN settings EXAMPLE

To add the SAML group (saml_grp) created in To create the SAML group to SSL VPN settings, see *Add the SAML group in the SSL VPN settings* in Configuring SAML SSO in the GUI.

Configuring a firewall policy to allow SSL VPN access

EXAMPLE

To configure a firewall policy with the *Source* as the SAML group (saml_grp) created in To create the SAML group, see *Configure the firewall policy* in Configuring SAML SSO in the GUI.

This completes the authentication settings for FortiGate to provide SAML SSO.

See the following SAML related examples in the *FortiOS 7.0.2 Admin Guide*:

- Outbound firewall authentication for a SAML user
- SAML SP for VPN authentication

FortiManager

Before proceeding, ensure that you have configured SAML settings on the FortiAuthenticator. See Configuring SAML settings on page 9.

To configure FortiManager as a service provider:

1. Create a FortiManager administrator account.
2. Configure FortiManager as the SAML SP.
3. Review results.

Create a FortiManager administrator account

Create an administrator account on FortiManager that matches a user on the FortiAuthenticator.

To create an administrator account on FortiManager:

1. Go to *System Settings > Admin > Administrators*, and click *Create New*.
2. Configure the administrator account settings, and click *OK*.

Configure the FortiManager as an SP

To configure the FortiManager as a service provider:

1. Go to *System Settings > Admin > SAML SSO*.
2. In the *Single Sign-On Settings* window, Select *Service Provider (SP)* as the *Single Sign-On Mode*.
3. Enter the following information:
   - **Server Address**: Enter the IP address of the FortiManager.
   - **Default Login Page**: Select *Normal.*
   - **IdP Type**: Select *Fortinet*.
   - **IdP Address**: Enter the IP address of the IdP FortiAuthenticator.
   - **Prefix**: Enter the prefix that was created during SP configuration on FortiAuthenticator.
   - **IdP Certificate**: Import and select the certificate that was chosen during FortiAuthenticator setup.

4. Select *OK*.

The following settings are required for service provider configuration on FortiAuthenticator.

- *SP Entity ID*
- *SP ACS (Login) URL*
- *SP SLS (Logout) URL*

Results

When the administrator visits the SP IP address of FQDN, they will see an additional option on the login screen to sign in using SSO.

FortiAnalyzer

Before proceeding, ensure that you have configured SAML settings on the FortiAuthenticator. See Configuring SAML settings on page 9.

To configure FortiAnalyzer as a service provider:

1. Create a FortiAnalyzer administrator account.
2. Configure the FortiAnalyzer as a SAML SP.
3. Review results.

Create a FortiAnalyzer administrator account

Create an administrator account on FortiAnalyzer that matches a user on the FortiAuthenticator.

To create an administrator account on FortiAnalyzer:

1. Go to *System Settings > Admin > Administrators*, and click *Create New*.
2. Configure the administrator account settings, and click *OK*.

Configure the FortiAnalyzer as a SAML SP

In order to complete the following configuration, you will need to simultaneously configure the SAML SP settings on the FortiAuthenticator. This is because some fields required for configuring SP settings on the FortiAuthenticator are only available when configuring the SAML settings on the FortiAnalyzer.

See Configuring SP settings on FortiAuthenticator on page 11.

To configure the FortiAnalyzer as a service provider:

1. Go to *System Settings > Admin > SAML SSO*.
2. Select *Service Provider (SP)* as the *Single Sign-On Mode*.
3. Enter the following information:
   - **Server Address**: Enter the IP address of the FortiAnalyzer.
   - **Default Login Page**: Select *Normal*.
   - **IdP Type**: Select *Fortinet*.
   - **IdP Address**: Enter the IP address of the IdP FortiAuthenticator.
   - **Prefix**: Enter the prefix that was created during SP configuration on FortiAuthenticator.

- **IdP Certificate**: Import and select the certificate that was chosen during FortiAuthenticator setup.

4. Select *OK*.

Make note of the following settings, as they are required during SP configuration on FortiAuthenticator.

- *SP Entity ID*
- *SP ACS (Login) URL*
- *SP SLS (Logout) URL*

Results

When the administrator visits the SP IP address of FQDN, they will see an additional option on the login screen to sign in using SSO.

Third-party Service Provider

After completing FortiAuthenticator setup, please consult the vendor's documentation for information about configuring your third-party device as a SP.

Most third-party SP configurations require the following information:

- A public certificate from the IdP to validate signature.

  The signature is stored on the SP side and used when a SAML response arrives.

- The ACS URL from the SP where SAML responses are posted.
- The IdP Sign-in URL where SAML requests are posted.

FORTINET®

www.fortinet.com