

Azure AD SSO integration with FortiGate SSL VPN

Prerequisites

To get started, you need the following items:

- An Azure AD subscription. If you don't have a subscription, you can get a [free account](#).
- A FortiGate SSL VPN with single sign-on (SSO) enabled.

Add FortiGate SSL VPN from the gallery

To configure the integration of FortiGate SSL VPN into Azure AD, you need to add FortiGate SSL VPN from the gallery to your list of managed SaaS apps:

1. Sign in to the Azure portal with a work or school account or with a personal Microsoft account.
2. In the left pane, select Azure Active Directory.
3. Go to Enterprise applications and then select All Applications.
4. To add an application, select New application.
5. In the Add from the gallery section, enter FortiGate SSL VPN in the search box.
6. Select FortiGate SSL VPN in the results panel and then add the app. Wait a few seconds while the app is added to your tenant.

Configure Azure AD SSO

Follow these steps to enable Azure AD SSO in the Azure portal:

1. In the Azure portal, on the FortiGate SSL VPN application integration page, in the Manage section, select single sign-on.
2. On the Select a single sign-on method page, select SAML.

3. On the Set up Single Sign-On with SAML page, select the Edit button for Basic SAML Configuration to edit the settings:

Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. [Learn more.](#)

Read the [configuration guide](#) for help integrating azure-fgt-sslvpn.

1

Basic SAML Configuration

 Edit

Identifier (Entity ID)	Required
Reply URL (Assertion Consumer Service URL)	Required
Sign on URL	Required
Relay State (Optional)	<i>Optional</i>
Logout Url (Optional)	<i>Optional</i>

4. On the Set up Single Sign-On with SAML page, enter the following values:
 - a. In the Identifier box, enter a URL in the pattern `https://<FortiGate IP or FQDN address>:<Custom SSL VPN port>/remote/saml/metadata`.
 - b. In the Reply URL box, enter a URL in the pattern `https://<FortiGate IP or FQDN address>:<Custom SSL VPN port>/remote/saml/login`.
 - c. In the Sign on URL box, enter a URL in the pattern `https://<FortiGate IP or FQDN address>:<Custom SSL VPN port>/remote/saml/login`.
 - d. In the Logout URL box, enter a URL in the pattern `https://<FortiGate IP or FQDN address>:<Custom SSL VPN port><FQDN>/remote/saml/logout`.

1

Basic SAML Configuration


 Edit

Identifier (Entity ID)	<code>https://vpn.██████████.com:10443/remote/saml/metadata</code>
Reply URL (Assertion Consumer Service URL)	<code>https://vpn.██████████.com:10443/remote/saml/login</code>
Sign on URL	<code>https://vpn.██████████.com:10443/remote/saml/login</code>
Relay State (Optional)	<i>Optional</i>
Logout Url (Optional)	<code>https://vpn.██████████.com:10443/remote/saml/logout</code>

5. The FortiGate SSL VPN application expects SAML assertions in a specific format, which requires you to add custom attribute mappings to the configuration. The

following screenshot shows the list of default attributes.

2

Attributes & Claims		 Edit
givenname	user.givenname	
surname	user.surname	
emailaddress	user.mail	
name	user.userprincipalname	
Unique User Identifier	user.userprincipalname	
Group	user.groups	

6. The claims required by FortiGate SSL VPN are shown in the following table. The names of these claims must match the names used in the Perform FortiGate command-line configuration section of this tutorial. Names are case-sensitive.

Name	Source attribute
username	user.userprincipalname
group	user.groups

To create these additional claims:


- Next to User Attributes & Claims, select Edit.
 - Select Add new claim.
 - For Name, enter username.
 - For Source attribute, select user.userprincipalname.
 - Select Save.
- Select Add a group claim.
 - Select All groups.
 - Under Advanced options, select the Customize the name of the group claim check box.
 - For Name, enter group.
 - Select Save.


2

Attributes & Claims		 Edit
givenname	user.givenname	
surname	user.surname	
emailaddress	user.mail	
name	user.userprincipalname	
username	user.userprincipalname	
group	user.groups	
Unique User Identifier	user.userprincipalname	

7. On the Set up Single Sign-On with SAML page, in the SAML Signing Certificate section, select the Download link next to Certificate (Base64) to download the certificate and save it on your computer:

3

SAML Signing Certificate  Edit




Status	Active
Thumbprint	<Thumbprintvalue >
Expiration	<Expiration >
Notification Email	<Email address>
App Federation Metadata Url	<input type="text" value="<App Federation Metadata Url>"/> 
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

8. In the Set up FortiGate SSL VPN section, copy the appropriate URL or URLs, based on your requirements:

4

Set up <App name>

You'll need to configure the application to link with Azure AD.

Login URL	<input type="text" value="https://login.microsoftonline.com/0a..."/> 
Azure AD Identifier	<input type="text" value="https://sts.windows.net/0ac53016-30..."/> 
Logout URL	<input type="text" value="https://login.microsoftonline.com/co..."/> 

[View step-by-step instructions](#)

Create an Azure AD test user

In this section, you'll create a test user named Maruf in the Azure portal.

1. In the left pane of the Azure portal, select Azure Active Directory. Select Users, and then select All users.
2. Select New user at the top of the screen.
3. In the User properties, complete these steps:
 - a. In the Name box, enter Maruf.
 - b. In the User name box, enter <username>@<companydomain>.<extension>. For example, `Maruf@contoso.com`.
 - c. Select Show password, and then write down the value that's displayed in the Password box.

- d. Select Create.

Grant access to the test user

In this section, you'll enable Maruf to use Azure single sign-on by granting that user access to FortiGate SSL VPN.

1. In the Azure portal, select Enterprise applications, and then select All applications.
2. In the applications list, select FortiGate SSL VPN.
3. On the app's overview page, in the Manage section, select Users and groups.
4. Select Add user, then select Users and groups in the Add Assignment dialog.
5. In the Users and groups dialog box, select Maruf in the Users list, and then click the Select button at the bottom of the screen.
6. If you're expecting any role value in the SAML assertion, in the Select Role dialog box, select the appropriate role for the user from the list. Click the Select button at the bottom of the screen.
7. In the Add Assignment dialog box, select Assign.

Create a security group for the test user

In this section, you'll create a security group in Azure Active Directory for the test user. FortiGate will use this security group to grant the user network access via the VPN.

1. In the left pane of the Azure portal, select Azure Active Directory. Then select Groups.
2. Select New group at the top of the screen.
3. In the New Group properties, complete these steps:
 - a. In the Group type list, select Security.
 - b. In the Group name box, enter FortiGateAccess.
 - c. In the Group description box, enter Group for granting FortiGate VPN access.
 - d. For the Azure AD roles can be assigned to the group (Preview) settings, select No.
 - e. In the Membership type box, select Assigned.
 - f. Under Members, select No members selected.

- g. In the Users and groups dialog box, select Maruf from the Users list, and then click the Select button at the bottom of the screen.
- h. Select Create.
4. After you're back in the Groups section in Azure Active Directory, find the FortiGate Access group and note the Object Id. You'll need it later.

Configure FortiGate SSL VPN SSO

Upload the Base64 SAML Certificate to the FortiGate appliance

After you completed the SAML configuration of the FortiGate app in your tenant, you downloaded the Base64-encoded SAML certificate. You need to upload this certificate to the FortiGate appliance:

1. Sign in to the management portal of your FortiGate appliance.
2. In the left pane, select System.
3. Under System, select Certificates.
4. Select Import > Remote Certificate.
5. Browse to the certificate downloaded from the FortiGate app deployment in the Azure tenant, select it, and then select OK.

After the certificate is uploaded, take note of its name under System > Certificates > Remote Certificate. By default, it will be named REMOTE_Cert_N, where N is an integer value.

Feature Visibility	
Certificates	☆
Security Fabric	1 >
Log & Report	>
Remote CA Certificate 4	
Fortinet_CA	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certi...
Fortinet_CA_Backup	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certi...
Fortinet_Sub_CA	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certi...
Fortinet_Wifi_CA	C = US, O = DigiCert Inc, CN = DigiCert TLS RSA SHA256 2020...
Remote Certificate 1	
REMOTE_Cert_1	CN = Microsoft Azure Federated SSO Certificate

Complete FortiGate command-line configuration

Although you can configure SSO from the GUI since FortiOS 7.0, the CLI configurations apply to all versions and are therefore shown here.

To complete these steps, you'll need the values you recorded earlier:

1. Establish an SSH session to your FortiGate appliance, and sign in with a FortiGate Administrator account.
2. Run these commands and substitute the `<values>` with the information that you collected previously:

```
config user saml
  edit azure
    set cert <FortiGate VPN Server Certificate Name>
    set entity-id < Identifier (Entity ID)Entity ID>
    set single-sign-on-url < Reply URL Reply URL>
    set single-logout-url <Logout URL>
    set idp-entity-id <Azure AD Identifier>
    set idp-single-sign-on-url <Azure Login URL>
    set idp-single-logout-url <Azure Logout URL>
    set idp-cert <Base64 SAML Certificate Name>
    set user-name username
    set group-name group
  next
end
```

```
config user saml
edit azure
set cert Fortinet_Factory
set entity-id https://[redacted]data.com:10443/remote/saml/metadata
set single-sign-on-url https://[redacted]data.com:10443/remote/saml/login
set single-logout-url https://[redacted]data.com:10443/remote/saml/logout
set idp-entity-id https://sts.windows.net/9ea04a[redacted]e24913/
set idp-single-sign-on-url https://login.microsoftonline.com/9ea04a[redacted]24913/saml2
set idp-single-logout-url https://login.microsoftonline.com/9ea04a[redacted]913/saml2
set idp-cert REMOTE_Cert_2
set user-name username
set group-name group
next
end
```

Configure FortiGate for group matching

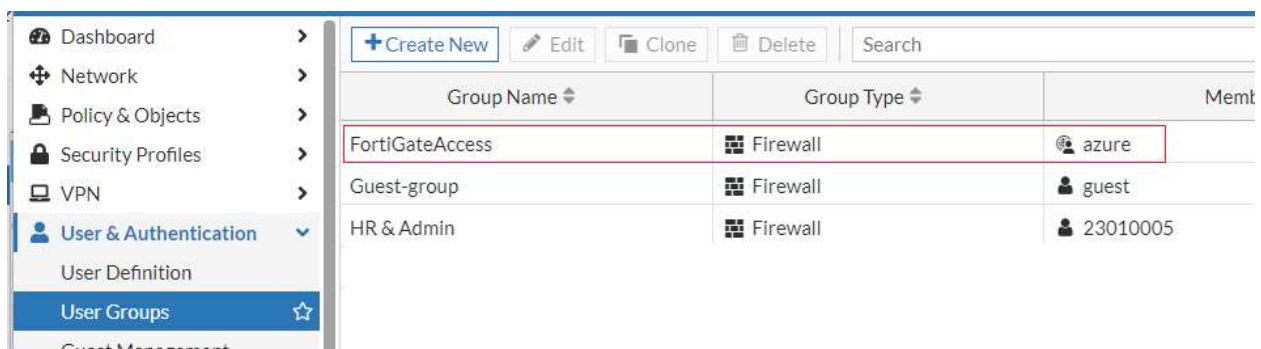
In this section, you'll configure FortiGate to recognize the Object ID of the security group that includes the test user.

To complete these steps, you'll need the Object ID of the FortiGateAccess security group that you created earlier in this tutorial.

1. Establish an SSH session to your FortiGate appliance, and sign in with a FortiGate Administrator account.
2. Run these commands:

```
config user group
  edit FortiGateAccess
    set member azure
    config match
      edit 1
        set server-name azure
        set group-name <Object Id>
      next
    end
  next
end
```

```
config user group
edit FortiGateAccess
set member azure
config match
edit 1
set server-name azure
set group-name b62a1ec0-1c93-4de9-ac46-2c3b04457b1c
next
end
next
end
```



Group Name	Group Type	Members
FortiGateAccess	Firewall	azure
Guest-group	Firewall	guest
HR & Admin	Firewall	23010005

Configure the remote authentication timeout value as needed:

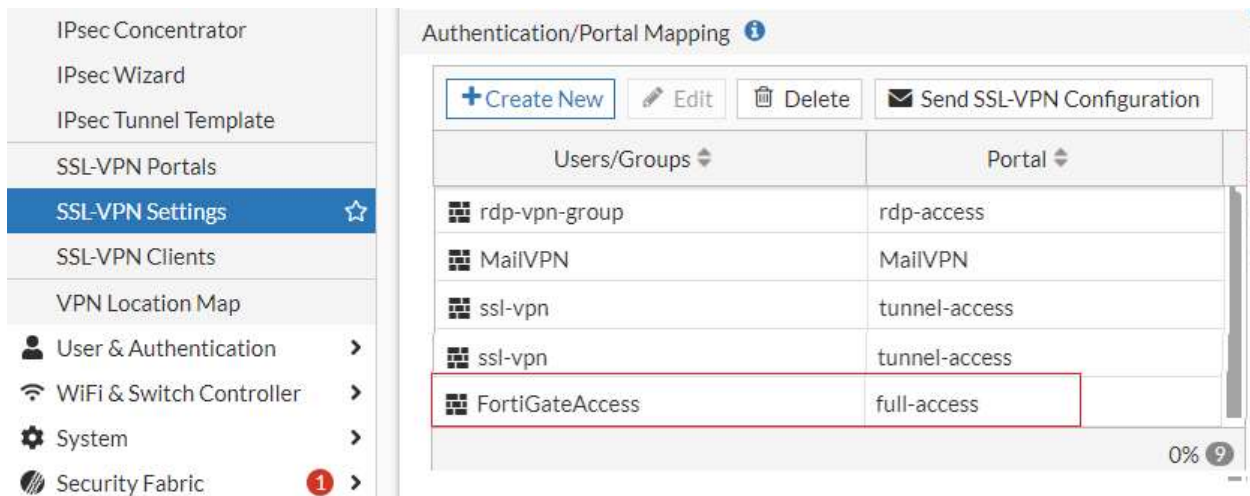
```
config system global
  set remoteauthtimeout 60
```


end

Create a FortiGate VPN Portals and Firewall Policy

To configure SSL VPN settings:

1. Go to *VPN > SSL VPN Settings*. Enable SSL VPN.
2. Configure *Listen on Interface(s)*.
3. Configure the *Listen on Port*. This port should be the port used in the SP URLs in the SAML configurations.
4. Select a server certificate. Fortinet_Factory is used by default. This certificate should match the SP certificate used in the SAML configurations.
5. Under *Authentication/Portal Mapping*, click *Create New*.
6. Set *Users/Groups* to the user group that you defined earlier. In this example, it is FortiGateAccess.
7. Set *Portal* to the desired SSL VPN portal.
8. Click *OK*.
9. Click *Apply*.



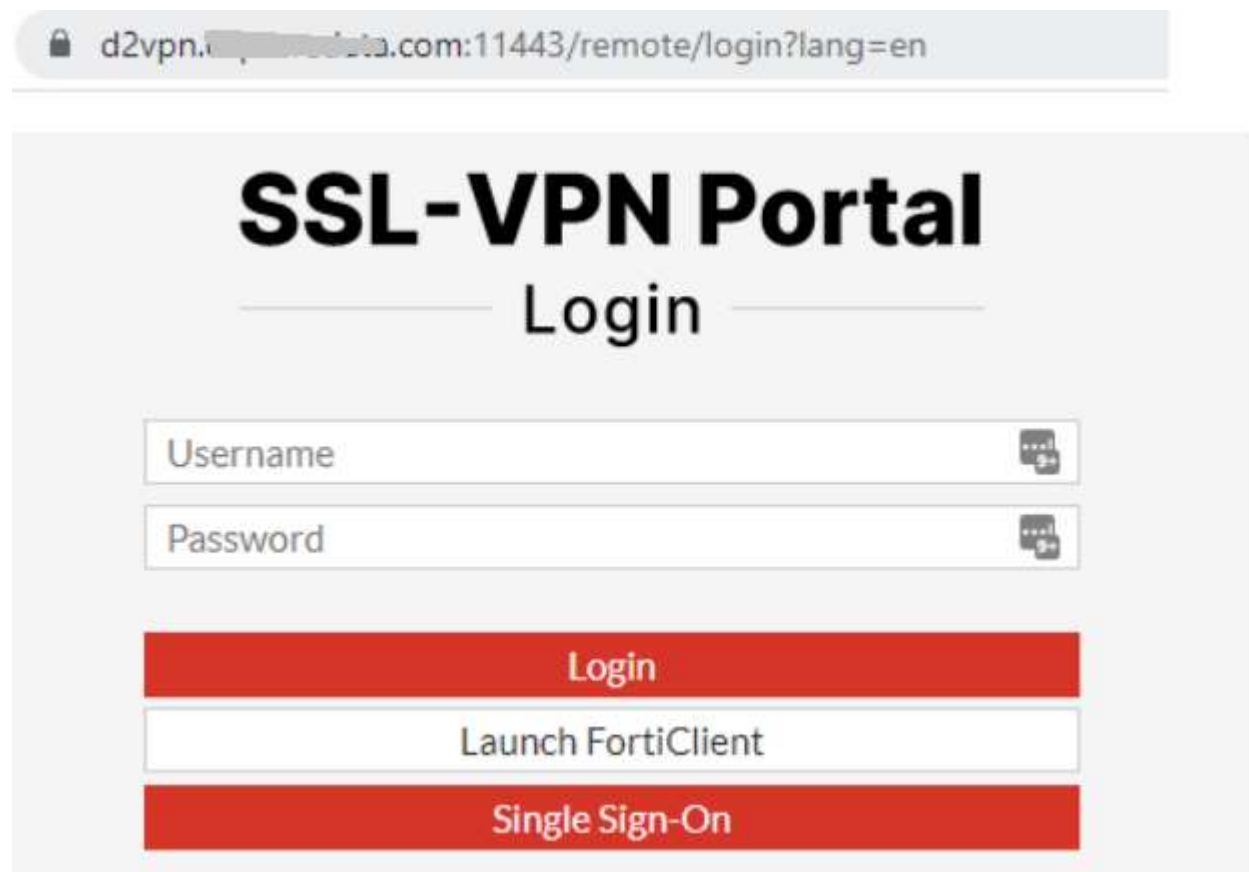
To configure a firewall policy:

1. Go to *Policy & Objects > Firewall Policy*. Click *Create new* to create a new SSL VPN firewall policy.
2. Select the incoming and outgoing interfaces. The incoming interface is the SSL VPN tunnel interface (ssl.root).
3. For *Source*, select the SSL VPN tunnel address group and FortiGateAccess user group.

4. Configure other settings as desired.
5. Click *OK*.

To connect in web mode:


1. Go to *https://<FortiGate FQDN / IP address>:10443* in a browser.
2. Click *Single Sign-On*. The browser redirects to the Azure login portal.
3. Sign in with your Azure account and password. Once logged in, the browser redirects to the SSL VPN portal.




d2vpn.11443.com:11443/remote/login?lang=en

SSL-VPN Portal

Login

Username 

Password 

Login

Launch FortiClient

Single Sign-On

To connect in tunnel mode with FortiClient:

1. In FortiClient, go to *Remote Access*.
2. Add a new connection:
 - a. Enter the desired connection name and description.
 - b. Set the remote gateway to the FortiGate's fully qualified domain name or IP address.
 - c. Enable *Customize port*, then specify the SSL VPN port.
 - d. Select *Enable Single Sign On (SSO) for VPN Tunnel*.

- e. (Optional) Enable *Use external browser as user-agent for saml user authentication* if you want users to use their browser session for login.
 - f. Click **Save**.
3. Click **SAML Login**. FortiClient redirects the user to the Azure login portal.
4. Sign in with your Azure account and password. Once logged in, the browser redirects to the SSL VPN portal.

Edit VPN Connection

VPN SSL-VPN IPsec VPN XML

Connection Name

Description

Remote Gateway ✕

[+Add Remote Gateway](#)

☒ Customize port

☒ Enable Single Sign On (SSO) for VPN Tunnel

☐ Use external browser as user-agent for saml user authentication

☐ Enable auto-login with Azure Active Directory

After provide Azure User credentials successfully connected to VPN



VPN Name **vpn-sso**
IP Address 10.212.134.100
Username Maruf.Hasan@corp-**ltd.com**
Duration 00:00:36
Bytes Received 0 KB
Bytes Sent 33.68 KB

Disconnect