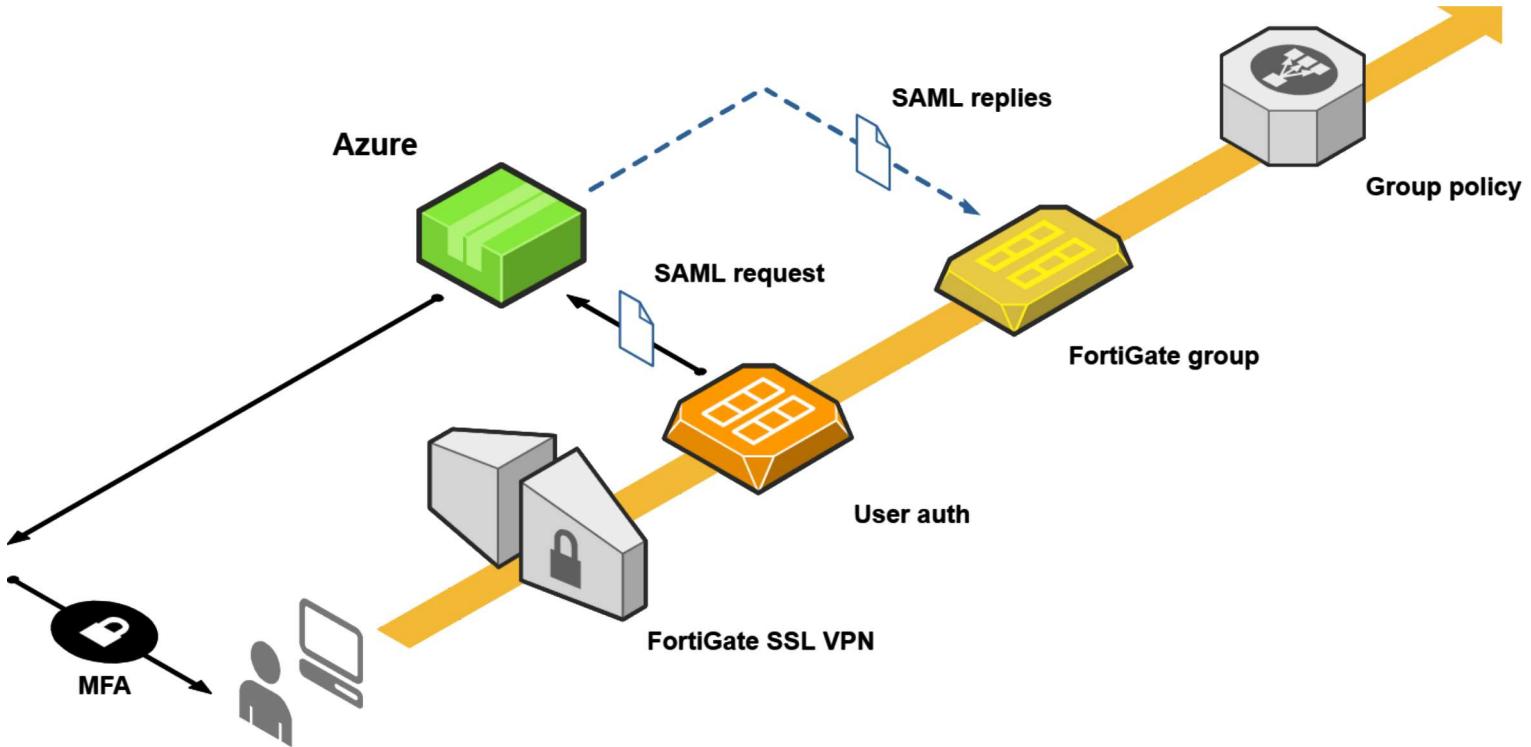


[en] Azure SAML authentication for FortiGate SSL VPN (with Azure MFA)

5 березня 2021 у розділі Технічні теми (<https://yura.stryi.com/category/tekhnichni-temi.html>) з тегами: Azure (<https://yura.stryi.com/tag/azure.html>), FortiGate (<https://yura.stryi.com/tag/fortigate.html>), MFA (<https://yura.stryi.com/tag/mfa.html>), VPN (<https://yura.stryi.com/tag/vpn.html>)

SAML authentication allows Fortigate to use Azure AD service directly as a source of users for SSL VPN and administrative logins.



In this article, I focus on **SSL VPN logins**, but very similarly the admin login can be done though. In FortiOS 6.4 administrative SSO login via SAML is now part of Security Fabric and can be configured from GUI.

The following setup was tested on FortiOS 6.2.7 and FortiOS 6.4.5 (with bugs described in debugging the section) on both physical FortiGate and virtual AWS appliance.

Table of contents:

- Azure setup
 - New Azure app
 - App settings
 - Basic SAML Configuration
 - User Attributes & Claims
 - Connection URLs
 - Azure certificate
 - Azure part
 - FortiGate part
 - Azure users and groups
 - Conditional access
- FortiGate setup

- SAML connection
- FortiGates groups connected to Azure
 - Azure part
 - FortiGate part
- FortiGate firewall policy
 - Very important — timeouts
 - FortiClient EMS setup
- FortiClient manual setup and run
- Troubleshooting and debugging
- References

Azure setup

New Azure app

Login into Azure Active Directory admin center at <https://aad.portal.azure.com> (<https://aad.portal.azure.com>).

Click **Enterprise applications** in the main menu and then **+New application**:

The screenshot shows the Azure Active Directory admin center interface. On the left, there's a sidebar with links: Dashboard, All services, FAVORITES (with Azure Active Directory, Users, and Enterprise applications), and Enterprise applications. The 'Enterprise applications' link is highlighted with a green arrow pointing to it. In the main content area, the title is 'Enterprise applications | All applications'. Below the title, there's a 'Try out the new Enterprise Apps search preview! Click to enable the preview' message. The 'Overview' section has two buttons: 'Overview' and 'Diagnose and solve problems'. The 'Manage' section has a 'All applications' button, which is also highlighted with a green arrow. At the top right, there are buttons for 'New application', 'Columns', 'Preview features', and a heart icon. Below the top right, there are filters for 'Application type' (set to 'Enterprise Applications') and 'Applications status' (set to 'Any'). A search bar at the bottom says 'First 50 shown, to search all of your applications, enter a display name c'.

Search for **FortiGate** and choose the corresponding result:

Azure Active Directory admin center

Dashboard > Enterprise applications > **Browse Azure AD Gallery (Preview)**

+ Create your own application | ⓘ Request new gallery app | ❤ Got feedback?

ⓘ Click here to switch back to the old app gallery experience. →

Search bar: FortiGate

Single Sign-on : All | User Account Management : All

Federated SSO | Provisioning

Showing 8 of 8 results

FortiGate SSL VPN | Fortinet

FortiSASE SIA | Fortinet Inc

Give it distinguish name and press **Create** at the bottom of the page:

FortiGate SSL VPN

X

Logo ⓘ

Name * ⓘ

Publisher ⓘ

Fortinet

Provisioning ⓘ

Automatic provisioning is not supported

Single Sign-On Mode ⓘ

SAML-based Sign-on
Linked Sign-on

URL ⓘ

<https://www.fortinet.com/>

App settings

Adding the new application will take a few seconds. You should be redirected to the app setting page. If not - go back to the **Enterprise applications** section and find the new app manually (by first letters of the name), open it by clicking:

[New application](#) | [Columns](#) | [Preview features](#) | [Got feedback?](#)

Try out the new Enterprise Apps search preview! Click to enable the preview. →

Application type	Applications status	Application visibility
Enterprise Applications	Any	Any

Test

Name: **Test FortiGate SSL VPN**

Homepage URL: <https://www.fortinet.com/>

In 2. Set up single sign on click Get Started:

Properties

Name ⓘ
Test FortiGate SSL VPN [Edit](#)

Application ID ⓘ
96e28e5e-b23f-4a72-bc29... [Edit](#)

Object ID ⓘ
fc8c8bc9-9c22-40b8-be4d... [Edit](#)

Getting Started



1. Assign users and groups

Provide specific users and groups access to the applications

[Assign users and groups](#)



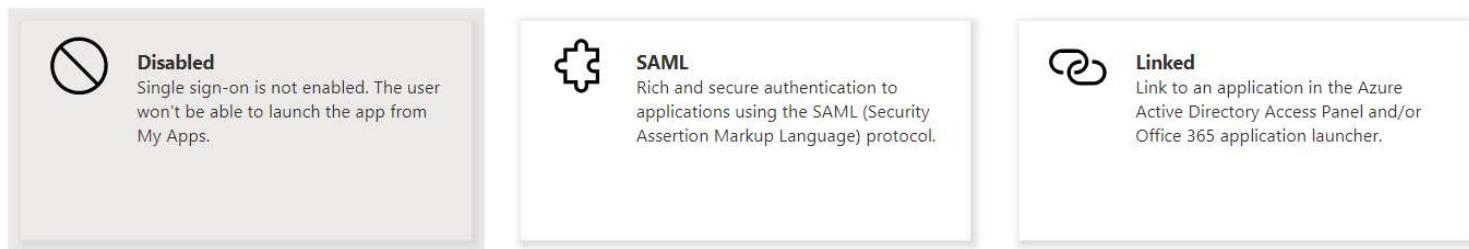
2. Set up single sign on

Enable users to sign into their application using their Azure AD credentials

[Get started](#)

and choose **SAML**:

Select a single sign-on method [Help me decide](#)



Basic SAML Configuration

Create SSL VPN portal base address. Check **IP-address** or FQDN of Fortigate interface used for incoming SSL VPN connection and available from the world (usually WAN). And SSL VPN TCP **port** (usually 10443). Also, note a **Server Certificate** name. You can see this data on **SSL-VPN Settings** page of the FortiGate:

No SSL-VPN policies exist. Click here to create a new SSL-VPN policy using these settings

Connection Settings ⓘ

Listen on Interface(s)

port1

Listen on Port

10443

Web mode access will be listening at <https://54.72.124.53:10443>

Redirect HTTP to SSL-VPN ⚡

Restrict Access

Allow access from any host Limit access to specific hosts

Idle Logout

Inactive For

300 Seconds

Server Certificate

self-sign

In my test case, the SSL VPN portal address base is <https://54.72.124.53:10443>. Use FQDN (<https://example-company.com:10443> (<https://example-site.com:10443>) if this domain points to the correct SSL VPN portal IP address).

Go back to Azure. In the App settings click **Edit** under section 1:

1

Basic SAML Configuration

 Edit

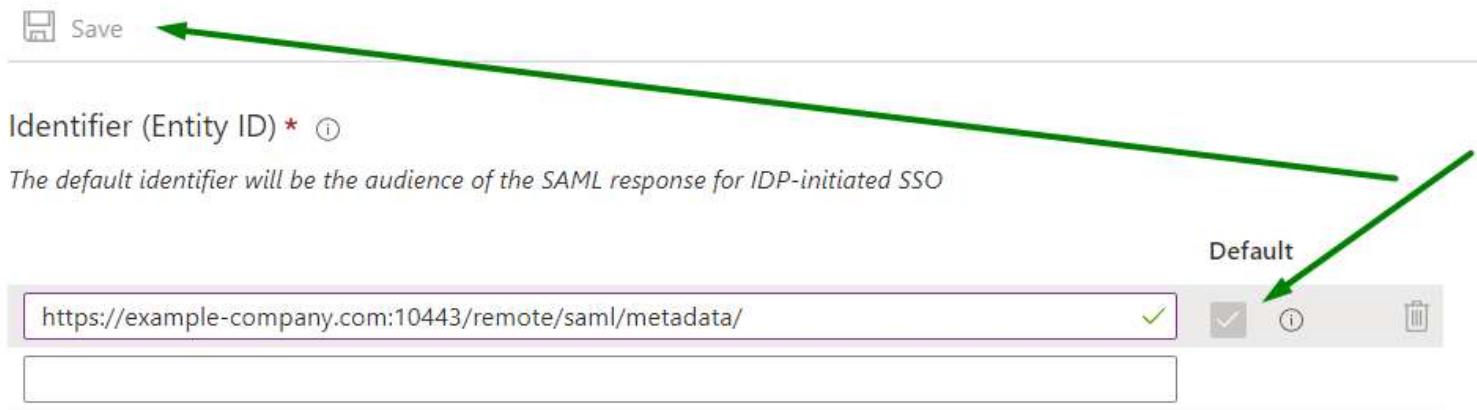
Identifier (Entity ID)	Required
Reply URL (Assertion Consumer Service URL)	Required
Sign on URL	Required
Relay State	<i>Optional</i>
Logout Url	<i>Optional</i>

Put the following

Parameter	Value
Identifier (Entity ID)	https://example-company.com:10443/remote/saml/metadata/
Reply URL	https://example-company.com:10443/remote/saml/login/
Sign on URL	https://example-company.com:10443/remote/login
Relay State	
Logout Url	https://example-company.com:10443/remote/saml/logout/

Make sure that value is set as **Default** were available:

Basic SAML Configuration



Identifier (Entity ID) * ⓘ

The default identifier will be the audience of the SAML response for IDP-initiated SSO

  ⓘ 

Finally, **Save**. When asked for a test — skip it by now.

User Attributes & Claims

Under section **2** click **Edit**:

2

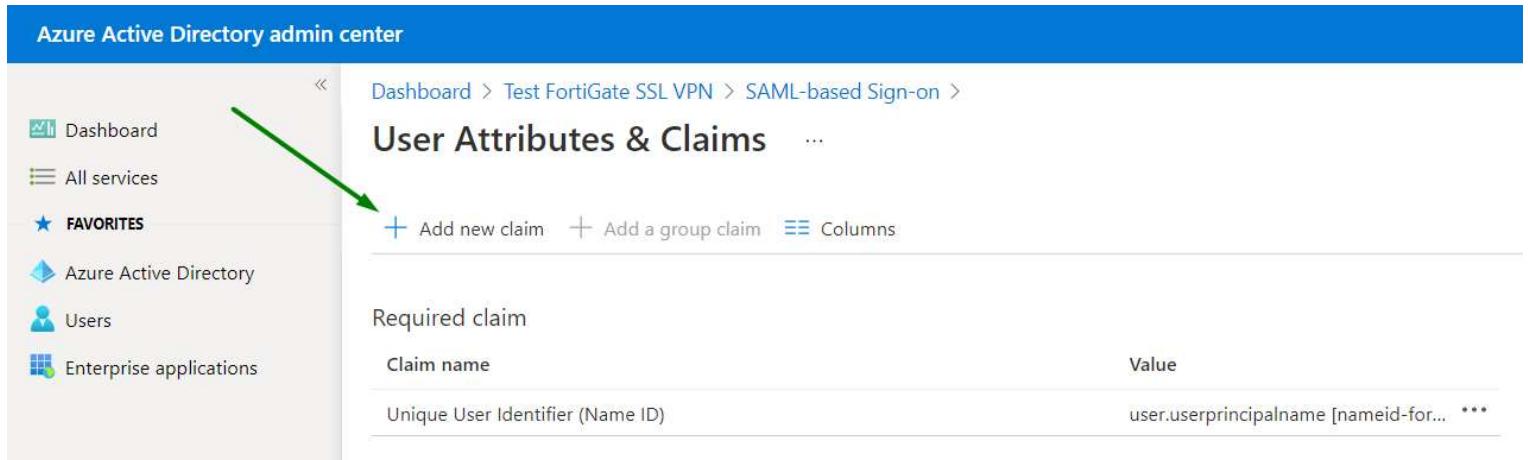
User Attributes & Claims

 Edit

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname
Group	user.groups

Click + Add new claim:

Azure Active Directory admin center



Dashboard > Test FortiGate SSL VPN > SAML-based Sign-on > User Attributes & Claims

+ Add new claim + Add a group claim Columns

Required claim

Claim name	Value
Unique User Identifier (Name ID)	user.userprincipalname [nameid-for... ***]

During one of the tests "Add new claim" was inactive. I found no reason for this — just re-created the Azure App.

Set the following (use autocompletion when possible):

Parameter	Value
Name	username
Source attribute	user.userprincipalname

Then Save:

Azure Active Directory admin center

Dashboard > Test FortiGate SSL VPN > SAML-based Sign-on > User Attributes & Claims > Manage claim

Save Discard changes

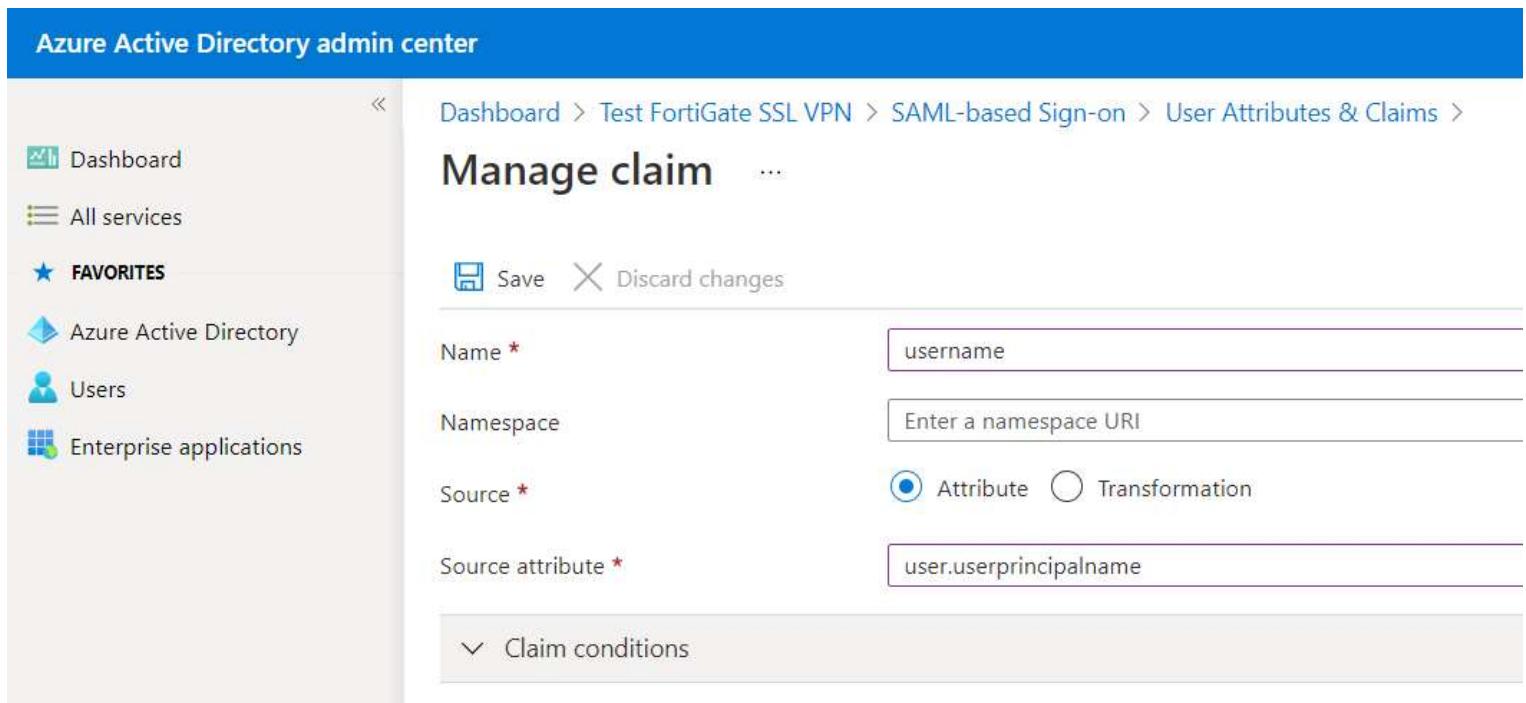
Name * username

Namespace Enter a namespace URI

Source * Attribute Transformation

Source attribute * user.userprincipalname

Claim conditions



We need to add another claim, this time a **Group claim**. But this option was always unavailable for me. We can edit existed group claim. I am still not sure about this part.

Click on **user.groups [SecurityGroup]** (do not use context menu ...). Enable **Customize the name of the group claim**. Set:

Parameter	Value
Name	group

Save and close setting:

User Attributes & Claims

Required claim

Claim name	Value
Unique User Identifier (Name ID)	user.userprincipalname [nameid-for...]

Additional claims

Claim name	Value
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	user.mail
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.givenname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	user.surname
username	user.userprincipalname

Group Claims

Manage the group claims used by Azure AD to populate SAML tokens issued to your app

Which groups associated with the user should be returned in the claim?

- None
- All groups
- Security groups
- Directory roles
- Groups assigned to the application

Source attribute *

Group ID

Advanced options

Customize the name of the group claim

Name (required)
group

Namespace (optional)

Emit groups as role claims ⓘ

Save

The final setting should look like this (check **username** and **group** parameters):

2 User Attributes & Claims

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
username	user.userprincipalname
group	user.groups
Unique User Identifier	user.userprincipalname

Edit

Connection URLs

From section 4 Set up Test FortiGate SSL VPN copy and save (we will use it later) content of

- Login URL
- Azure AD Identifier
- Logout URL

4

Set up Test FortiGate SSL VPN

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

Login URL

<https://login.microsoftonline.com/78831cc0-e027-4bb6-a21...> 

Azure AD Identifier

<https://sts.windows.net/78831cc0-e027-4bb6-a21...> 

Logout URL

<https://login.microsoftonline.com/78831cc0-e027-4bb6-a21...> 

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

Azure certificate

Azure part

From section 3 SAML Signing Certificate download file under **Certificate (Base64)**:

3

SAML Signing Certificate

 Edit

Status	Active
Thumbprint	7CD5665C3387AE99F2FEF3FAF6ECC7783A2B5C05
Expiration	3/2/2024, 5:20:34 PM
Notification Email	Yuriy.Smetana@example-company.com
App Federation Metadata Url	https://login.microsoftonline.com/78831cc0-e027-4bb6-a21... 
Certificate (Base64)	Download 
Certificate (Raw)	Download
Federation Metadata XML	Download

Save the file to the local computer.



This type of file can harm your computer. Do you want to keep Test FortiGate SSL....cer anyway?

[Keep](#)

[Discard](#)

If the certificate is wrong, most likely you will get this error later on:

```
saml_sp_login_resp [747]: Failed to process response message. ret=440(The profile cannot verify a signature on the message)
```

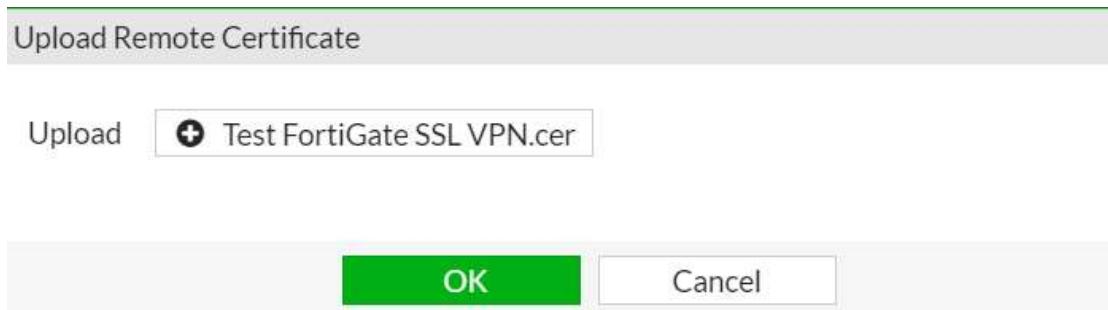
FortiGate part

In the FortiGate UI go to the **System → Certificates** section. Then do **Import → Remote Certificate**.

The screenshot shows the FortiGate VM64-AWS interface with the title bar "FortiGate VM64-AWS FTG-example". The left sidebar has a "System" section selected, indicated by a red circle with the number "1". The "Certificates" tab is also highlighted with a red circle and a star icon. The main content area shows a table of certificates. The "Import" dropdown menu is open, with "Remote Certificate" highlighted. The table includes columns for Name, Subject, and Details.

Name	Subject	Details
Local CA Certificate (2)		
Fortinet_CA_SSL	C = US, ST = California, L = Sunnyvale, O = Fortinet	
Fortinet_CA_Untrusted	C = US, ST = California, L = Sunnyvale, O = Fortinet	
Local Certificate (14)		
Fortinet_Factory	C = US, ST = California, L = Sunnyvale, O = Fortinet	
Fortinet_Factory_Backup	C = US, ST = California, L = Sunnyvale, O = Fortinet	
Fortinet_SSL	C = US, ST = California, L = Sunnyvale, O = Fortinet	
Fortinet_SSL_DSA1024	C = US, ST = California, L = Sunnyvale, O = Fortinet	
Fortinet_SSL_DSA2048	C = US, ST = California, L = Sunnyvale, O = Fortinet	
Fortinet_SSL_ECDSA256	C = US, ST = California, L = Sunnyvale, O = Fortinet	
Fortinet_SSL_ECDSA384	C = US, ST = California, L = Sunnyvale, O = Fortinet	

Click **+Upload**. Choose the Azure certificate (.cer file) which has just been downloaded and press **OK**:



The certificate will appear in **Remote Certificate** section with the name **REMOTE_CERT_n**:

The screenshot shows the "Remote Certificate" section with one entry. The entry shows the certificate name "REMOTE_Cert_1" and its subject "CN = accounts.accesscontrol.windows.net".

REMOTE_CERT_1	CN = accounts.accesscontrol.windows.net
---------------	---

Give it a reasonable name in CLI, if you want:

```
config vpn certificate remote
rename REMOTE_Cert_1 to Azure_SAML
end

show vpn certificate remote

FTG-example # show vpn certificate remote
config vpn certificate remote
edit "Azure_SAML"
set range global
next
end
```

The screenshot shows the FortiGate CLI interface. The command `show vpn certificate remote` is entered, followed by the configuration of a new certificate named "Azure_SAML". The configuration includes setting the range to "global" and saving the changes.

Azure users and groups

Not sure about this, but for test purposes add the user who can use our SAML SSL VPN login. In a real-life environment you would probably allow all users to use the app or use group-based assignment.

In the App settings open **Users and groups**, then **+ Add user/group**:

The screenshot shows the Azure Active Directory admin center. The user is on the 'Test FortiGate SSL VPN | Users and groups' page for an Enterprise Application. The 'Manage' section is selected. A green arrow points to the '+ Add user/group' button, which is located at the top right of the 'Manage' section. The 'Display Name' field is empty, and a message indicates that the application will appear on the Access Panel.

Click **None selected** first:

Azure Active Directory admin center

Dashboard > Test FortiGate SSL VPN >

Add Assignment

Symphony Solutions BV

Users and groups

None Selected 

Select a role

Default Access

Dashboard All services FAVORITES Azure Active Directory Users Enterprise applications

Search for the user, click it, click **Select**:

Users and groups

yuriy.smetana 

 Yuriy Smetana Yuriy.Smetana@example-company.com Selected
--

Selected items

 Yuriy Smetana Yuriy.Smetana@example-company.com	
--	---

Select 

And, finally, **Assign**:

The screenshot shows the 'Add Assignment' step in the Azure Active Directory admin center. A user named 'Symphony Solutions BV' has been selected. The 'Assign' button at the bottom left is highlighted with a green arrow. The interface includes sections for 'Users and groups', '1 user selected.', 'Select a role', and 'Default Access'.

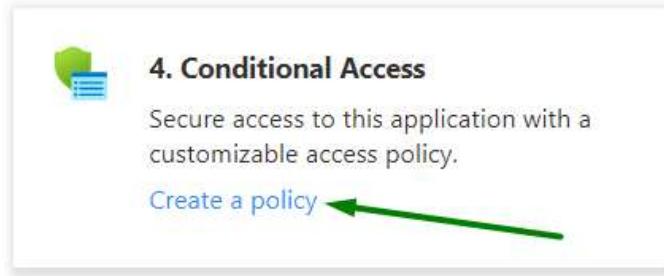
We have the first user now:

The screenshot shows the 'Test FortiGate SSL VPN | Users and groups' page in the Azure Active Directory admin center. The 'Users and groups' section is highlighted with a green arrow. A user named 'Yuriy Smetana' is listed with a checkbox next to it. Other options include 'Add user/group', 'Edit', and 'Remove'.

There are other user-related settings in **Properties** page of the App, but we do not use them at the moment.

Conditional access

From the main page of the App, in section **4. Conditional Access**, click **Create a policy**:



Then + New policy:

Azure Active Directory admin center

Dashboard > Test FortiGate SSL VPN

Test FortiGate SSL VPN | Conditional Access Enterprise Application

Overview Deployment Plan

Manage

What is conditional access?

Give it a name and under **Users and groups** select **All users**:

Dashboard > Test FortiGate SSL VPN >

New ...

Conditional access policy

Control user access based on conditional access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name *

Force MFA

Assignments

Users and groups ⓘ

All users

Cloud apps or actions ⓘ

1 app included

Conditions ⓘ

0 conditions selected

Access controls

Grant ⓘ

Control user access based on users and groups assignment for all users, specific groups of users, directory roles, or external guest users [Learn more](#)

Include

None

All users

Select users and groups

All guest and external users ⓘ

Directory roles ⓘ

Users and groups



⚠ Don't lock yourself out! This policy will affect all of your users. We recommend applying a policy to a small set of users first to verify it behaves as expected.

Under **Grant** section, enable **Require multi-factor authentication**, press **Select**, switch **Enable policy** to **On**, click **Create**.

Dashboard > Test FortiGate SSL VPN >

New

...

Conditional access policy

Control user access based on conditional access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name *

Force MFA



Assignments

Users and groups ⓘ

All users

Cloud apps or actions ⓘ

1 app included

Conditions ⓘ

0 conditions selected

Access controls

Grant ⓘ

0 controls selected

Session ⓘ

0 controls selected

Enable policy

Report-only

On

Off

Create

The result:

Grant

X

Control user access enforcement to block or grant access. [Learn more](#)

Block access

Grant access

Require multi-factor authentication ⓘ

Require device to be marked as compliant ⓘ

Require Hybrid Azure AD joined device ⓘ

Require approved client app ⓘ
See [list of approved client apps](#)

Require app protection policy ⓘ
See [list of policy protected client apps](#)

Require password change ⓘ

For multiple controls

Require all the selected controls

Require one of the selected controls

Select

The screenshot shows the Azure Active Directory admin center interface. On the left, there's a sidebar with links like Dashboard, All services, FAVORITES (with Azure Active Directory selected), Users, and Enterprise applications. The main area shows a 'Test FortiGate SSL VPN | Conditional Access' page for an 'Enterprise Application'. It has sections for Overview, Deployment Plan, Manage (Properties and Owners), and a search bar. At the bottom, there's a table with columns for Policy Name and Force MFA. A green arrow points to the 'Force MFA' column header.

FortiGate setup

Considering that the basic SSL VPN setup is already done.

We need to create FortiGate SAML connection server and local groups connected to the remote Azure groups via FortiGate SAML server.

SAML connection

To accomplish this step you will need:

- SSL VPN portal address and port (**example-company.com:10443**)
- SAML IdP URLs from **Azure app** (Connection URLs, **Step 4**)
- Local certificate name (e.g *Fortinet_Factory*)
- Remote certificate name (we renamed it to **Azure_SAML**)

In the FortiGate console:

```
config user saml
edit "azure-saml"
  set cert "Fortinet_Factory"
  set entity-id "https://example-company.com:10443/remote/saml/metadata/"
  set single-sign-on-url "https://example-company.com:10443/remote/saml/login/"
  set single-logout-url "https://example-company.com:10443/remote/saml/logout/"
  set idp-entity-id "https://sts.windows.net/YYY-e027-4bb6-a213-XXX/"
  set idp-single-sign-on-url "https://login.microsoftonline.com/YYY-e027-4bb6-a213-XXX/saml2"
  set idp-single-logout-url "https://login.microsoftonline.com/YYY-e027-4bb6-a213-XXX/saml2"
  set idp-cert "Azure_SAML"
  set user-name "username"
  set group-name "group"
next
end
```

Where:

set cert

Use local certificate name. Ideally, it should be your purchased SSL certificate for the domain you use for SSL VPN (i.e. example-company.com (<http://example-company.com>)). It also available on SSL-VPN settings page:

The screenshot shows the FortiGate VM64-AWS interface. The left sidebar is expanded to show the 'VPN' section, with 'SSL-VPN Settings' selected. The main panel displays 'SSL-VPN Settings' under 'Connection Settings'. It shows 'Listen on Interface(s)' set to 'port1' and 'Listen on Port' set to '10443'. A note indicates that 'Web mode access will be listening at <https://example-company.com:10443>'. Below this, 'Redirect HTTP to SSL-VPN' is enabled. Under 'Restrict Access', 'Allow access from any host' is selected. Other options like 'Idle Logout' and 'Inactive For' (set to 300 seconds) are also visible. A green arrow points to the 'Server Certificate' dropdown menu, which contains 'Fortinet_Factory'. The top navigation bar shows the device as 'FortiGate VM64-AWS FTG-example'.

set entity-id set single-sign-on-uri set single-logout-url

Just use it exactly as it is, but change `example-company.com:10443` for your own address and port. It corresponds to the addresses we set in Azure app settings in **Basic SAML Configuration**.

The screenshot shows the 'Basic SAML Configuration' blade in the Azure portal. It lists several configuration parameters with their values:

Setting	Value
Identifier (Entity ID)	https://example-company.com:10443/remote/saml/meta-data/
Reply URL (Assertion Consumer Service URL)	https://example-company.com:10443/remote/saml/login/
Sign on URL	https://example-company.com:10443/remote/login/
Relay State	Optional
Logout Url	https://example-company.com:10443/remote/saml/logout/

set idp-entity-id

Azure AD Identifier from Azure app settings 4 Set up Test FortiGate SSL VPN**4****Set up Test FortiGate SSL VPN**

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

Login URL<https://login.microsoftonline.com/78831cc0-e027-4bb6-a21...> **Azure AD Identifier**<https://sts.windows.net/78831cc0-e027-4bb6-a21...> **Logout URL**<https://login.microsoftonline.com/78831cc0-e027-4bb6-a21...> [View step-by-step instructions](#)

```
set idp-single-sign-on-url
```

Login URL from Azure app settings 4 Set up Test FortiGate SSL VPN**4****Set up Test FortiGate SSL VPN**

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

Login URL<https://login.microsoftonline.com/78831cc0-e027-4bb6-a21...> **Azure AD Identifier**<https://sts.windows.net/78831cc0-e027-4bb6-a21...> **Logout URL**<https://login.microsoftonline.com/78831cc0-e027-4bb6-a21...> [View step-by-step instructions](#)

```
set idp-single-logout-url
```

Logout URL from Azure app settings 4 Set up Test FortiGate SSL VPN**4****Set up Test FortiGate SSL VPN**

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

Login URL<https://login.microsoftonline.com/78831cc0-e027-4bb6-a21...> **Azure AD Identifier**<https://sts.windows.net/78831cc0-e027-4bb6-a21...> **Logout URL**<https://login.microsoftonline.com/78831cc0-e027-4bb6-a21...> [View step-by-step instructions](#)

```
set idp-cert
```

The one we downloaded from Azure app settings, imported into the Fortigate, and renamed for convenience.



FortiGates groups connected to Azure

Azure part

FortiGate will use the Azure group as an assignment to local groups. They will be used as user groups in firewall policies. We need to create one or use existed **Security** group. Find the Azure group ID first.

On the main page of the **Azure Active Directory admin center** click **Groups**:

The screenshot shows the Azure Active Directory admin center interface. On the left, there's a sidebar with links: Dashboard, All services, FAVORITES (with Azure Active Directory selected), Users, and Enterprise applications. The main content area shows the 'Example Company | Overview' page for Azure Active Directory. In the center, there's a navigation menu with links: Overview, Getting started, Preview hub, and Diagnose and solve problems. Below that is a 'Manage' section with 'Users' and 'Groups'. A green arrow points from the left sidebar towards the 'Groups' link in the 'Manage' section. To the right, there's a 'Tenant information' card and a search bar.

Search group by name. Click on the desired group name:

All groups

Deleted groups

Diagnose and solve problems

Settings

General

Expiration

Naming policy

Name	Object Id
TEST-SSLVPN-GENERAL-GROUP	c9f15d42-a79a-40f0-a2d
TEST-SSLVPN-IT-GROUP	b2fb854b-b782-4390-9d

Copy the Object ID of the group:

TEST-SSLVPN-GENERAL-GROUP

Group

Overview

Diagnose and solve problems

Manage

Properties

Members

Owners

Administrative units

Group memberships

Applications

Licenses

Azure role assignments

TEST-SSLVPN-GENERAL-GROUP

TE

Membership type	Assigned
Source	Cloud
Type	Security
Object Id	YYY-a79a-40f0-a2df-XXX
Creation date	2/23/2021, 4:49:32 PM

FortiGate part

Now, knowing Azure group ID link it with the FortiGate group:

```

config user group
edit "SAML_AZ_ALL"
    set member "azure-saml"
    config match
        edit 1
            set server-name "azure-saml"
            set group-name "YYY-a79a-40f0-a2df-XXX"
        next
    end
next
end

```

Where `set server-name` and `set server-name` are the SAML connection name we have just created in the FortiGate, and `set group-name` corresponds to group ID we have copied from Azure portal.

Check FortiGate groups info, the group should also be there:

The screenshot shows the FortiGate VM64-AWS interface with the title bar "FortiGate VM64-AWS FTG-example". The left sidebar menu includes: Dashboard, Security Fabric, Network, System (marked with a red circle containing the number 1), Policy & Objects, Security Profiles, VPN, User & Authentication (selected), and User Groups. The main content area has a toolbar with "Create New" (highlighted in green), Edit, Clone, and Delete buttons. Below the toolbar is a "Group Name" input field with "Guest-group" typed in. A list of user groups is shown: "SAML_AZ_ALL" (with a green arrow pointing to it) and "SSO_Guest_Users".

FortiGate firewall policy

The system needs the policy to allow users to connect via SSL VPN.

Remember — the first policy that matches some user's group will set this group as user default (main) and an appropriate VPN portal will be chosen based on this group.

The screenshot shows the FortiGate VM64-AWS interface. On the left, the navigation bar includes Dashboard, Security Fabric, Network, System (with a red notification badge), Policy & Objects (selected), Firewall Policy (highlighted in green), IPv4 DoS Policy, Addresses, Internet Service Database, Services, Schedules, Virtual IPs, IP Pools, and Protocol Options. Below these are Traffic Shapers and a section for recently modified objects.

The main panel displays a 'New Policy' configuration. The policy details are as follows:

- Name:** Test SAML users policy
- Incoming Interface:** SSL-VPN tunnel interface (ssl.root)
- Outgoing Interface:** port1
- Source:** SAML_AZ_ALL (highlighted with a green arrow)
- Destination:** gmail.com
- Schedule:** always
- Service:** ALL
- Action:** ACCEPT (selected)

At the bottom, the inspection mode is set to Flow-based.

The incoming interface should be **ssl.root**. Make sure to add **SAML** group as **Source**. Keep attention to NAT and other settings depending on your setup.

Very important — timeouts

In all my cases, it did not work until I tweaked some connection timeouts or you will get errors similar to:

```
Timeout for connection 0x7f1123ba2000.
Destroy sconn 0x7f1123ba2000, connSize=0. (root)
```

Set:

```
config system global
    set remoteauthtimeout 180
end
```

And, just to be sure:

```
config vpn ssl settings
    set login-timeout 180
end
```

FortiClient EMS setup

VPN connection can be added via EMS for all FortiClient that are connected to it. Edit endpoint profile in the EMS **Endpoint Profiles** → **Manage profiles**.

Add Tunnel in the **VPN Tunnels** section of **VPN** tab of the profile.

The screenshot shows the FortiClient Endpoint Management Server interface. The left sidebar has a tree view with 'Endpoint Profiles' selected, and 'Manage Profiles' is highlighted. The main area shows a profile named 'TEST-6-4-0'. Below it is a toolbar with icons for various management functions. A table titled 'VPN Tunnels' lists one entry: 'SAML Example' (Type: SSL, Remote Gateway: example-company.com). There are 'Save' and 'Discard Changes' buttons at the bottom.

Name	Type	Remote Gateway
SAML Example	SSL	example-company.com

Check the Fortigate **address** and SSL VPN **port** number:

Editing VPN Tunnel: SAML UA-LV X

i Changes to this VPN tunnel will not be saved until the profile is saved.

Basic Settings

Advanced Settings

On Connect Script
On Disconnect Script

Basic Settings

Name: SAML Example
Cannot contain the characters \"/&%<>.

Type: **SSL VPN** (IPsec VPN)

Remote Gateway: example-company.com - +

Port: 10443

Require Certificate
 Prompt for Username

Save Tunnel Cancel

Activate **Enable SAML Login** in Advanced Settings:

Editing VPN Tunnel: SAML UA-LV X

i Changes to this VPN tunnel will not be saved until the profile is saved.

Basic Settings

Advanced Settings (Selected)

On Connect Script
On Disconnect Script

Advanced Settings

Enable Single User Mode
 Enable Invalid Server Certificate Warning
 Save Username
 Allow Non-Administrators to Use Machine Certificates
 Enforce Acceptance of Disclaimer Message
 Enable SAML Login

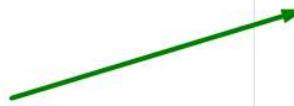
Redundant Sort Method

Server Ping Speed TCP Round Trip Time

The following features need to also be configured on FortiGate to be enabled.

Show "Remember Password" Option
 Show "Always Up" Option
 Show "Auto Connect" Option

Save Tunnel Cancel

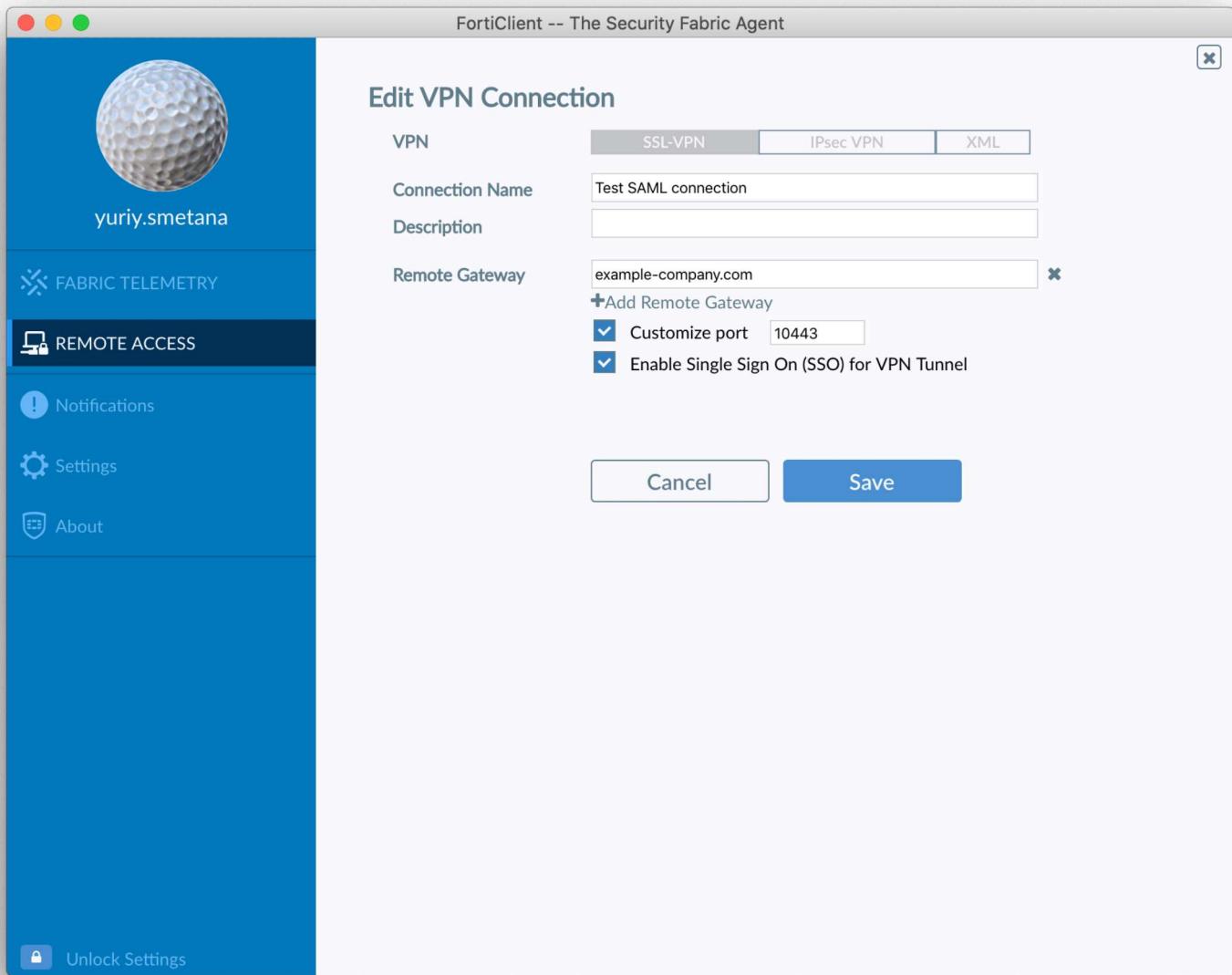


Wait till the FortiClients populated the settings.

FortiClient manual setup and run

SAML-based VPN connection available in FortiClient **6.4.0+**.

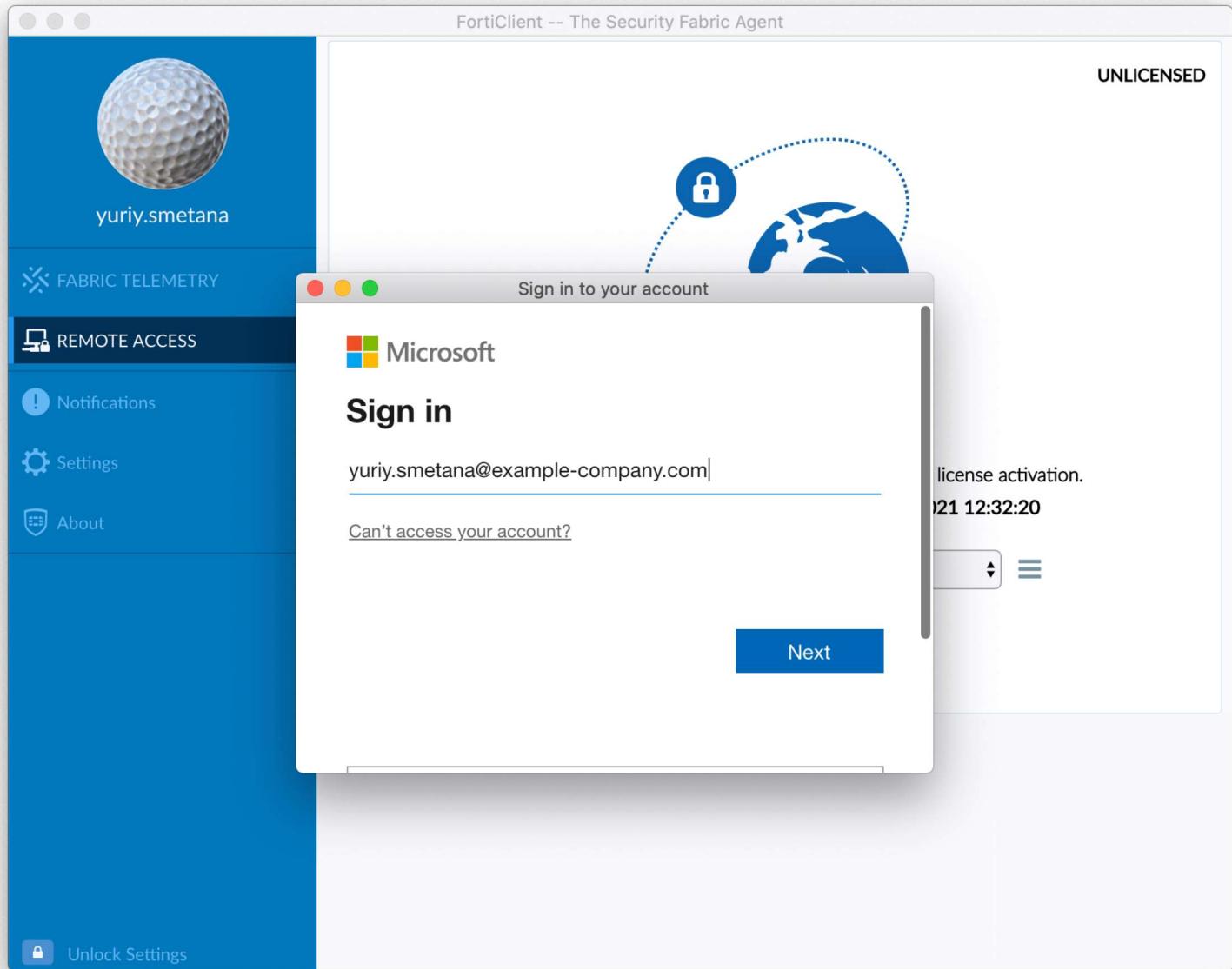
During the setup of SSL VPN connection manually enable **Single Sign On (SSO) for VPN Tunnel** and make sure that the Fortigate address and SSL VPN port number are correct:



You should see **SAML login** button when SSO-enabled connection is chosen:



Try to login and provide Azure user email and password:



If everything is fine — MFA request will be displayed:

Enter code

Please type in the code displayed on your authenticator app from your device

Code

Having trouble? [Sign in another way](#)

[More information](#)

If not — don't panic and please read the troubleshooting section below.

Troubleshooting and debugging

Current FortiOS 6.4.5 has a bug that causes the system to select an incorrect default user group and thus an incorrect VPN portal. FortiOS 6.2.7 has no such problem.

If login was successful, you can check logged in users via **SSL-VPN** users widget of FortiOS:

 SSL-VPN

Username	Last Login
Yuriy.Smetana@example-company.com	2021/03/06 10:33:06

and via **Firewall Users** widget to see user groups:

User Name	IP Address	User Group
 Yuriy.Smetana@example-company.com	172.20.0.1	 SAML_AZ_ALL

As well as from CLI with `get vpn ssl monitor`:

```
# get vpn ssl monitor
SSL VPN Login Users:
Index User Group Auth Type Timeout Auth-Timeout From HTTP in/out HTTPS in/out Two-factor Auth
0     Yuriy.Smetana@example-company.com SAML_AZ_ALL 256(1)          840    28369   153.53.53.53 0/0    0/0    0

SSL VPN sessions:
Index User Group Source IP Duration I/O Bytes Tunnel/Dest IP
0     Yuriy.Smetana@example-company.com SAML_AZ_ALL 193.53.53.53 424      42112/55944 172.20.0.1
```

If you can't login, or group is wrong — debugging can be really helpful. I personally discovered issues with timeouts, certificate problems as well as group assignment bug in FortiOS 6.4.5.

To troubleshoot SSL VPN SAML login issues use:

```
diag debug reset
diag debug console timestamp enable
diag debug app sslvpn -1
diag debug app samld -1
diag debug enable
```

Example of debug output:

```

FTG-example # 2021-03-03 17:26:44 [163:root:0]total sslvpn policy count: 2
2021-03-03 17:26:47 [163:root:37]allocSSLConn:298 sconn 0x7f11245ef900 (0:root)
2021-03-03 17:26:47 [163:root:37]client cert requirement: no
2021-03-03 17:26:47 [163:root:37]SSL state:SSLv3/TLS read client hello (153.53.53.53)
...
**** Auth Req URL ****
https://login.microsoftonline.com/YYY-e027-4bb6-a213-XXX/saml2?SAMLRequest=ZZZ
*****
__samld_sp_create_auth_req [394]:
**** SP Login Dump ****
2021-03-03 17:27:10 [163:root:39]Timeout for connection 0x7f11245ef900.
2021-03-03 17:27:10 [163:root:39]Destroy sconn 0x7f11245ef900, connSize=1. (root)
...
2021-03-03 17:27:21 [163:root:3b]req: /remote/saml/login/
__samld_sp_login_resp [733]:
Message Body
...xw0lJlc3BvbNlPg==

samld_send_common_reply [120]: Attr: 10, 50, 'username' 'Yuriy.Smetana@example-company.com'
samld_send_common_reply [120]: Attr: 10, 47, 'group' 'ZZZ-765c-4d61-9b26-ZZZ'
samld_send_common_reply [120]: Attr: 10, 47, 'group' 'MMM-a79a-40f0-a2df-MMM'
samld_send_common_reply [120]: Attr: 10, 47, 'group' 'KKK-b782-4390-9d22-KKK'
samld_send_common_reply [120]: Attr: 10, 47, 'group' 'LLL-d9ed-4e9a-8322-LLL'
samld_send_common_reply [120]: Attr: 10, 47, 'group' '000-c702-427c-a550-000'
samld_send_common_reply [120]: Attr: 10, 47, 'group' 'UUU-a05e-47b8-a884-UUU'
...
2021-03-03 17:27:23 [163:root:3b]stmt: username
2021-03-03 17:27:23 [163:root:3b]fsv_saml_login_response:437 Got saml username: Yuriy.Smetana@example-company.com.
2021-03-03 17:27:23 [163:root:3b]stmt: group
2021-03-03 17:27:23 [163:root:3b]fsv_saml_login_response:444 Got group username: ZZZ-765c-4d61-9b26-ZZZ.
2021-03-03 17:27:23 [163:root:3b]stmt: group
2021-03-03 17:27:23 [163:root:3b]fsv_saml_login_response:444 Got group username: MMM-a79a-40f0-a2df-MMM.
2021-03-03 17:27:23 [163:root:3b]stmt: group
2021-03-03 17:27:23 [163:root:3b]fsv_saml_login_response:444 Got group username: KKK-b782-4390-9d22-KKK.
2021-03-03 17:27:23 [163:root:3b]stmt: group
2021-03-03 17:27:23 [163:root:3b]fsv_saml_login_response:444 Got group username: LLL-d9ed-4e9a-8322-LLL.
2021-03-03 17:27:23 [163:root:3b]stmt: group
2021-03-03 17:27:23 [163:root:3b]fsv_saml_login_response:444 Got group username: 000-c702-427c-a550-000.
2021-03-03 17:27:23 [163:root:3b]stmt: group
2021-03-03 17:27:23 [163:root:3b]fsv_saml_login_response:444 Got group username: UUU-a05e-47b8-a884-UUU.
2021-03-03 17:27:23 [163:root:3b]sslvpn_auth_check_usrgroup:2603 forming user/group list from policy.
2021-03-03 17:27:23 [163:root:3b]sslvpn_auth_check_usrgroup:2641 got user (1) group (1:0).
2021-03-03 17:27:23 [163:root:3b]sslvpn_validate_user_group_list:1786 validating with SSL VPN authentication rules (0), realm ((none)).
2021-03-03 17:27:23 [163:root:3b]sslvpn_validate_user_group_list:2506 got user (1:0), group (1:0) peer group (0).
2021-03-03 17:27:23 [163:root:3b]sslvpn_update_user_group_list:1734 got user (1:0), group (1:0), peer group (0) after update.
2021-03-03 17:27:23 [163:root:3b]fsv_saml_auth_group:269 find a remote match group: MMM-a79a-40f0-a2df-MMM, portal: full-access, group: SAML_AZ_ALL.
2021-03-03 17:27:23 [163:root:3b]fsv_saml_auth_group:290 saml client cert: 0.
...
2021-03-03 17:27:23 [163:root:3b]User Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko)
o) FortiClient/6.0.0 Chrome/69.0.3497.128 Electron/4.2.9 Safari/537.36
2021-03-03 17:27:23 [163:root:3b]deconstruct_session_id:426 decode session id ok, user=[Yuriy.Smetana@example-company.com],group=[SAML_AZ_ALL],authserver=[azure-saml],portal=[full-access],host=[153.53.53.53],realm=[],idx=0,auth=256,sid=1b5fedc6,login=1614785243,access=1614785243,saml_logout_url=no

```

We can see:

- beginning of user connection (SSL state:SSLv3/TLS read client hello),

- if we have any connection with Azure, it responses
- certificate issue (described in the previous sections)
- any timeouts if happened (Timeout for connection 0x7f11245ef900)
- user name (samId_send_common_reply [120]: Attr: 10, 50, 'username' 'Yuriy.Smetana@example-company.com')
- list of user's Azure groups ID (samId_send_common_reply [120]: Attr: 10, 47, 'group')
(fsv_saml_auth_group:269 find a remote match group: MMM-a79a-40f0-a2df-MMM, portal: full-access, group: SAML_AZ_ALL.)
- very important — local group match and portal assignment
- client general info etc

References

The following resources were very helpful:

- <https://www.ultraviolet.network/post/fortigate-ssl-vpn-with-azure-mfa-using-saml> (<https://www.ultraviolet.network/post/fortigate-ssl-vpn-with-azure-mfa-using-saml>)
- <https://sites.google.com/frellsen.se/kimfrellsen/fortinet-ssl-vpn-with-okta-mfa-using-saml?authuser=0> (<https://sites.google.com/frellsen.se/kimfrellsen/fortinet-ssl-vpn-with-okta-mfa-using-saml?authuser=0>)
- <https://docs.microsoft.com/en-us/azure/active-directory/saas-apps/fortigate-ssl-vpn-tutorial> (<https://docs.microsoft.com/en-us/azure/active-directory/saas-apps/fortigate-ssl-vpn-tutorial>)

Less helpful official FortiNet docs (actually pretty bad):

- <https://docs.fortinet.com/document/fortigate/6.2.0/azure-cookbook/584456/configuring-saml-sso-login-for-ssl-vpn-web-mode-with-azure-ad-acting-as-saml-idp> (<https://docs.fortinet.com/document/fortigate/6.2.0/azure-cookbook/584456/configuring-saml-sso-login-for-ssl-vpn-web-mode-with-azure-ad-acting-as-saml-idp>)
- <https://docs.fortinet.com/document/fortigate/6.2.0/azure-cookbook/584456/configuring-saml-sso-login-for-ssl-vpn-web-mode-with-azure-ad-acting-as-saml-idp> (<https://docs.fortinet.com/document/fortigate/6.2.0/azure-cookbook/584456/configuring-saml-sso-login-for-ssl-vpn-web-mode-with-azure-ad-acting-as-saml-idp>)

Коментарі

Дивіться також:

Архів тем (<https://yura.stryi.com/archives.html>)

Теги (<https://yura.stryi.com/tags.html>)

RSS 

Розділи:

Технічні теми (<https://yura.stryi.com/category/tekhnichni-temi.html>)

Життєпис (<https://yura.stryi.com/category/zhittiepis.html>)

Життєпис, Технічні теми (<https://yura.stryi.com/category/zhittiepis-tekhnichni-temi.html>)

Соціальні мережі:

 Github (<https://github.com/YSmetana>)

 Bitbucket (<https://bitbucket.org/lufa/>)

Коментарі:

-  (https://disqus.com/by/disqus_HwMOUMo0DI/) guitman (https://disqus.com/by/disqus_HwMOUMo0DI/)

Thank you for this article. Does this also...

[en] Azure SAML authentification for FortiGate SSL VPN (with Azure MFA) (<http://yura.stryi.com/en/2021-03-05/fortigate-ssl-vpn-azure-mfa/>) · 6 days ago (<http://yura.stryi.com/en/2021-03-05/fortigate-ssl-vpn-azure-mfa/#comment-5580159914>)

-  (https://disqus.com/by/disqus_m9O6RoqWnT/) matjaz-m (https://disqus.com/by/disqus_m9O6RoqWnT/)

Hi Yura, this is a great article! Do you...

[en] Azure SAML authentification for FortiGate SSL VPN (with Azure MFA) (<http://yura.stryi.com/en/2021-03-05/fortigate-ssl-vpn-azure-mfa/>) · 1 month ago (<http://yura.stryi.com/en/2021-03-05/fortigate-ssl-vpn-azure-mfa/#comment-5551117554>)

-  (<https://disqus.com/by/adejauh/>) 'Ade Jauh' (<https://disqus.com/by/adejauh/>)

Hi

il try this, but error access denied

[en] Azure SAML authentification for FortiGate SSL VPN (with Azure MFA) (<http://yura.stryi.com/en/2021-03-05/fortigate-ssl-vpn-azure-mfa/>) · 2 months ago (<http://yura.stryi.com/en/2021-03-05/fortigate-ssl-vpn-azure-mfa/#comment-5482662615>)

Популярні статті:

Українська клавіатура для Андроїд (/2010-12-29/ukrainian-keyboard-android-gingerbread/)

3G на DIR-320 (/2010-02-12/dlink-dir-320-adu-500a-mts/)

Переваги дзеркального фотоапарата (/2007-08-02/dslr/)

Встановлення датчика температури (/2011-01-15/thermostat-auraton-2020-vaillant-turbotec-pro/)

Огляд Casio AWG-100-1A (/2010-12-13/casio-awg-100-1a/)

Фотогалерея (<https://picasaweb.google.com/103950464629760372334>)

Читаю:

Selyanchyn in Japan (<http://romanselyanchyn.blogspot.com>)

tivasyk@home (<http://www.tivasyk.info>)

Our world... (<http://kanfetas.blogspot.com>)

Яремин Блог (<http://yarema-blog.blogspot.com>)

Igor Melika (<http://igormelika.com.ua>)

 (<http://creativecommons.org/licenses/by/3.0/deed.uk>) «СЮМ», Юрій Сметана (<https://yura.stryi.com>), ліцензія ССА 3.0

Unported License (<http://creativecommons.org/licenses/by/3.0/deed.uk>). Працює на Pelican (<http://docs.getpelican.com>).

Шаблон від Bootstrap (<http://twitter.github.com/bootstrap/>).