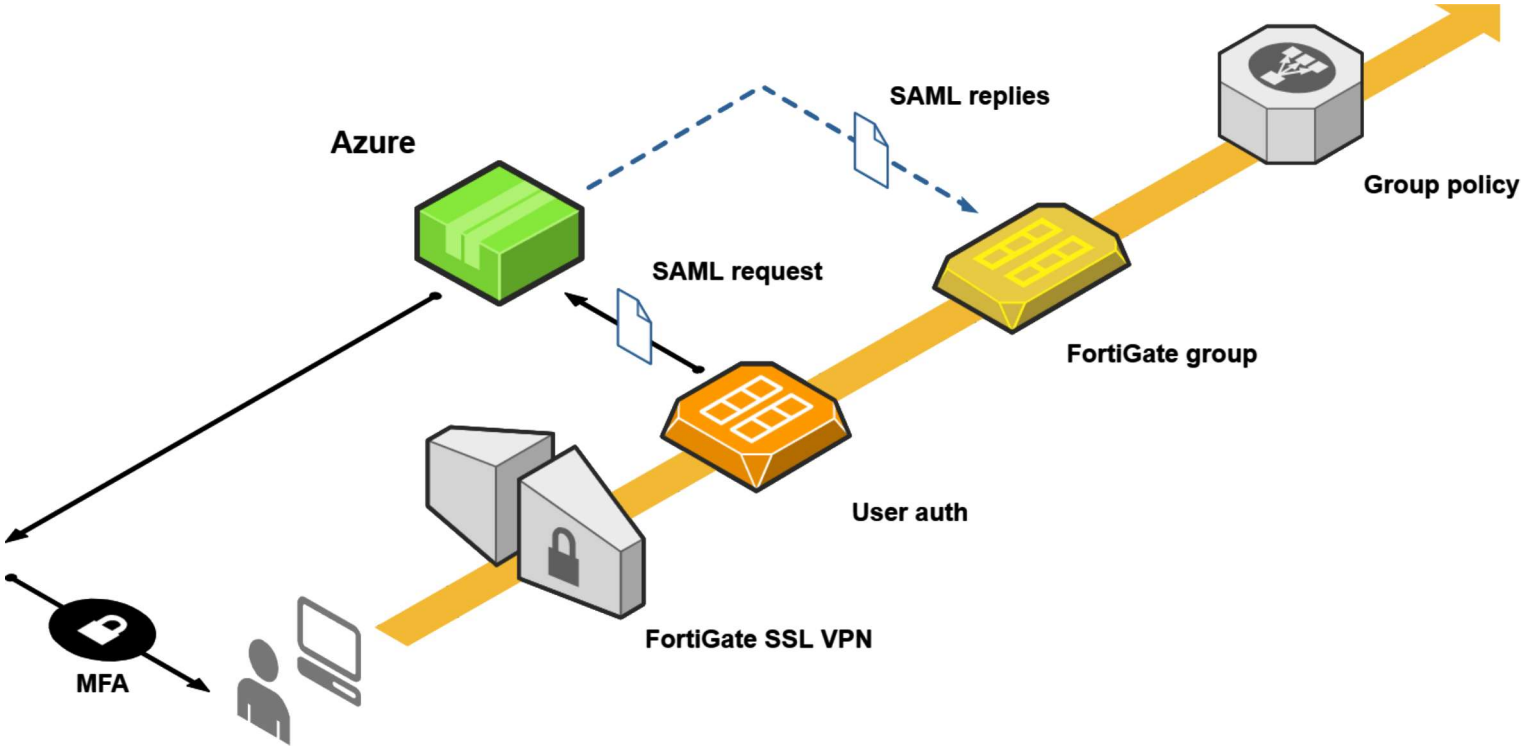
[en] Azure SAML authentification for FortiGate SSL VPN (with Azure MFA)

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 authentification 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 applience.

Table of contents:

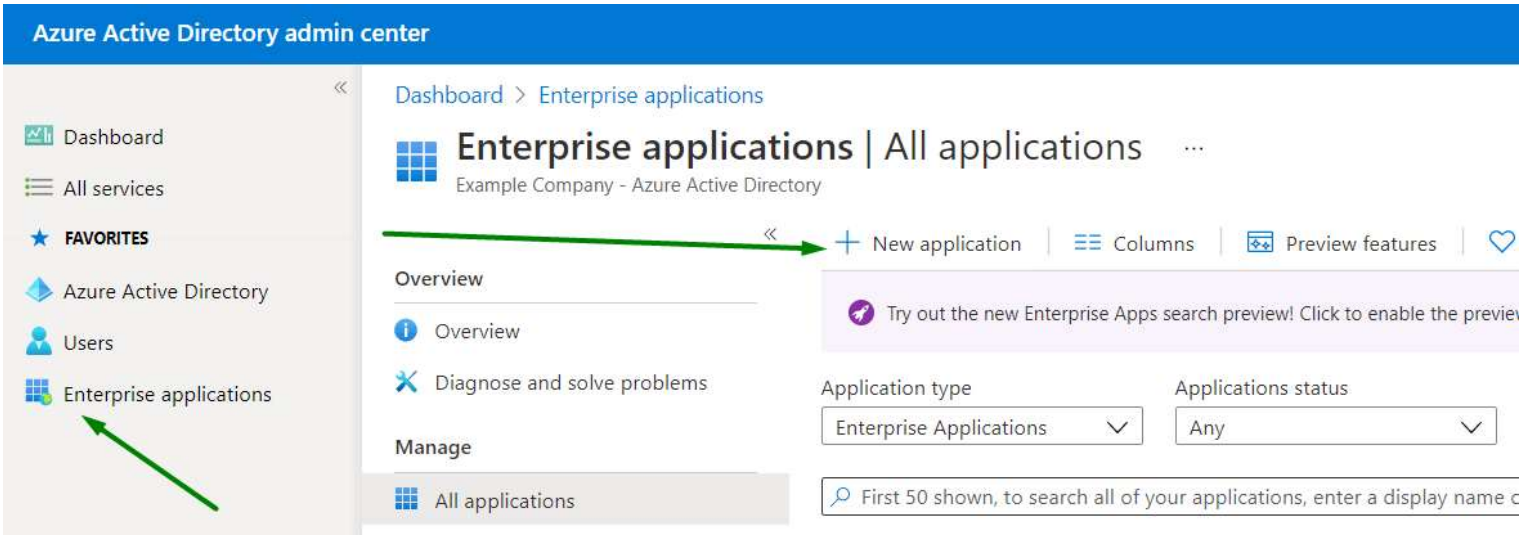
    - SAML connection
    - FortiGates groups connected to Azure
        - Azure part
        - FortiGate part
    - FortiGate firewall policy
    - Very important — timeouts
    - FortiClient EMS setup
- FortiClient manual setup and run
- Troubleshooting and debugging
- References

Azure setup

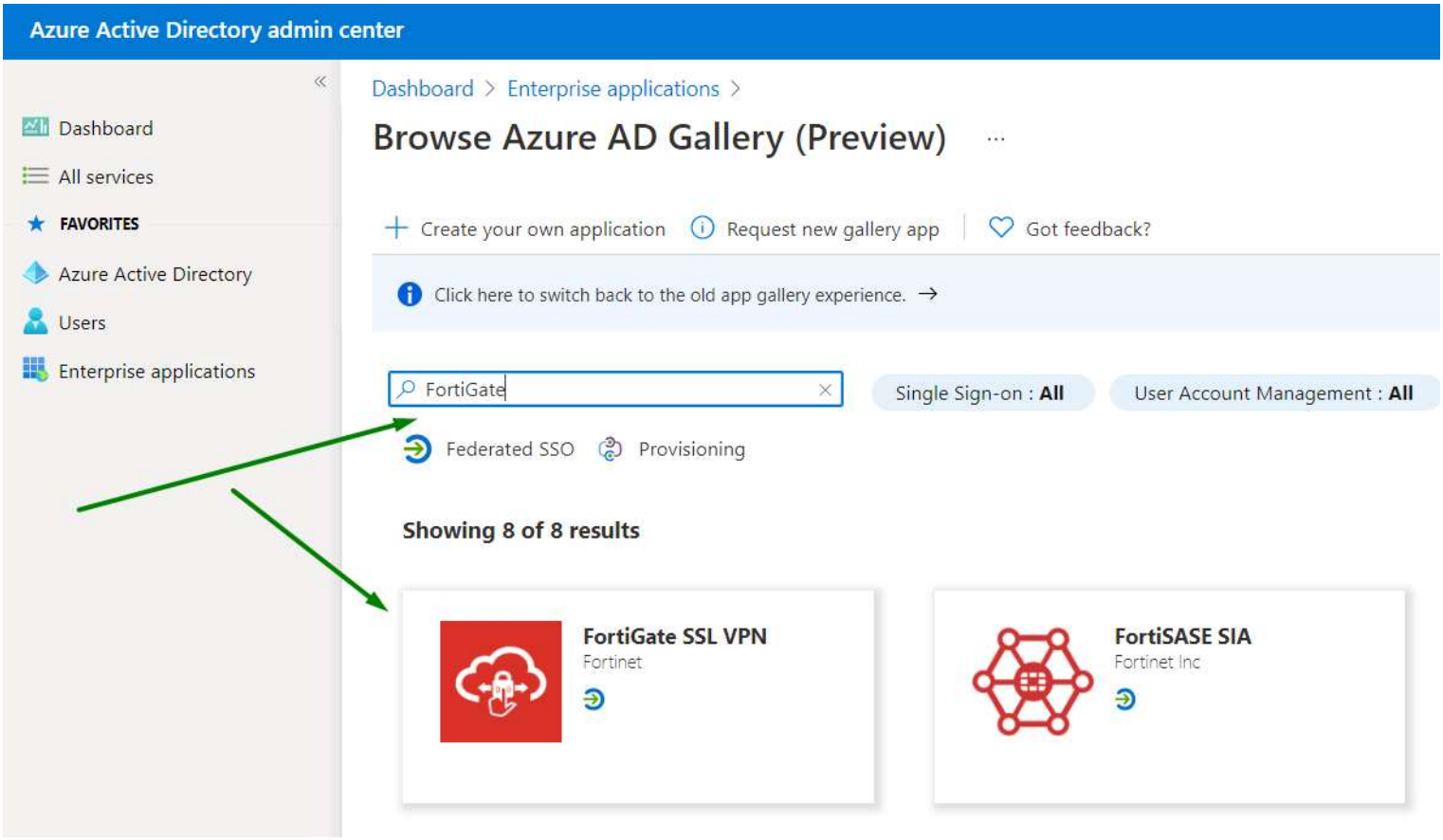
New Azure app

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

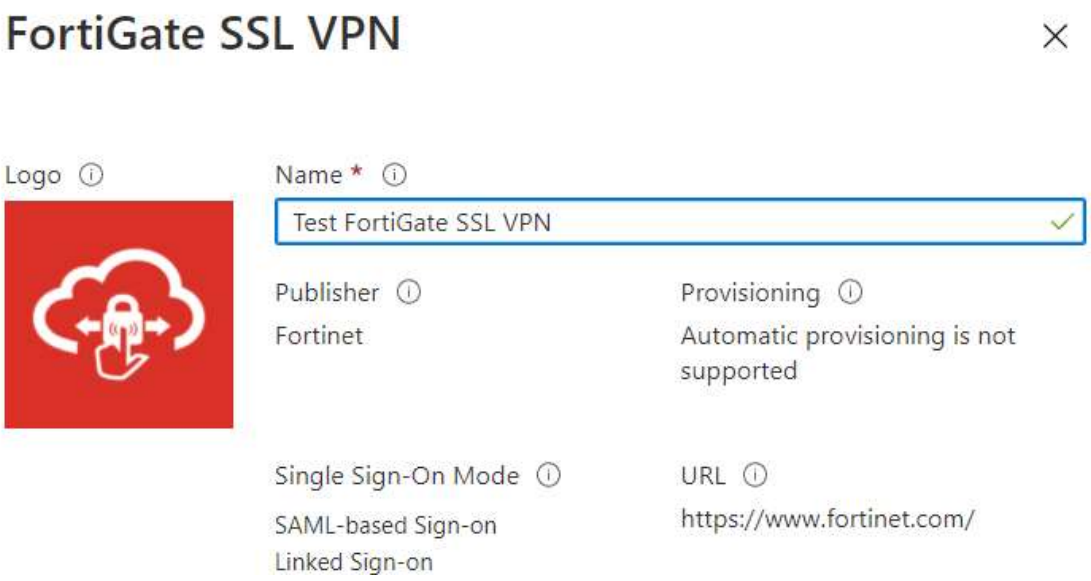
Click **Enterprise applications** in the main menu and then **+New application**:



Search for `FortiGate` and choose the corresponding result:

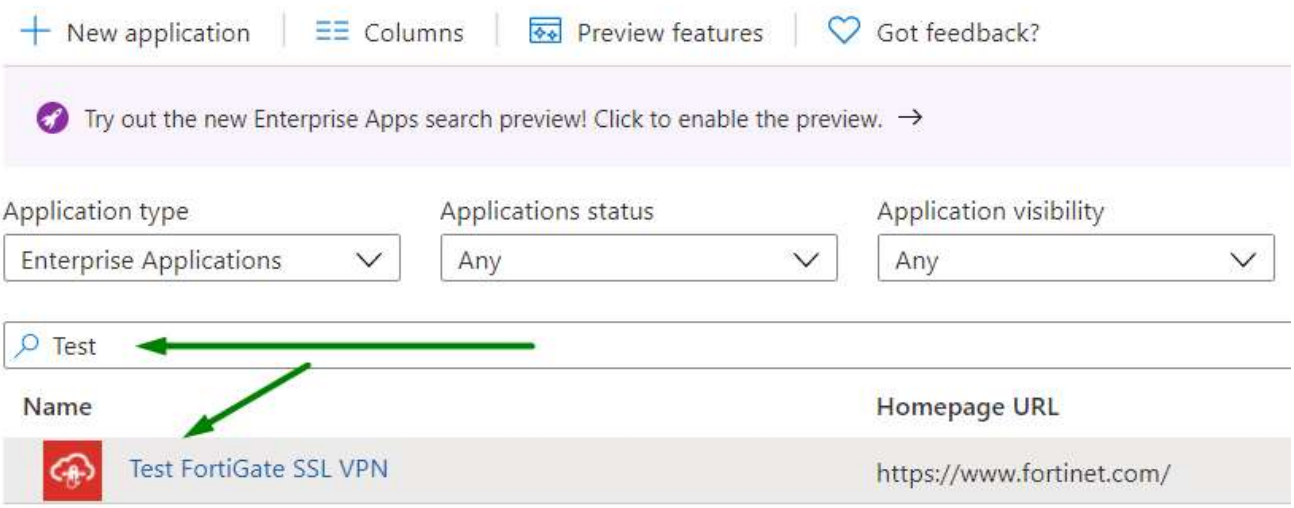


Give it distinguish name and press **Create** at the bottom of the page:

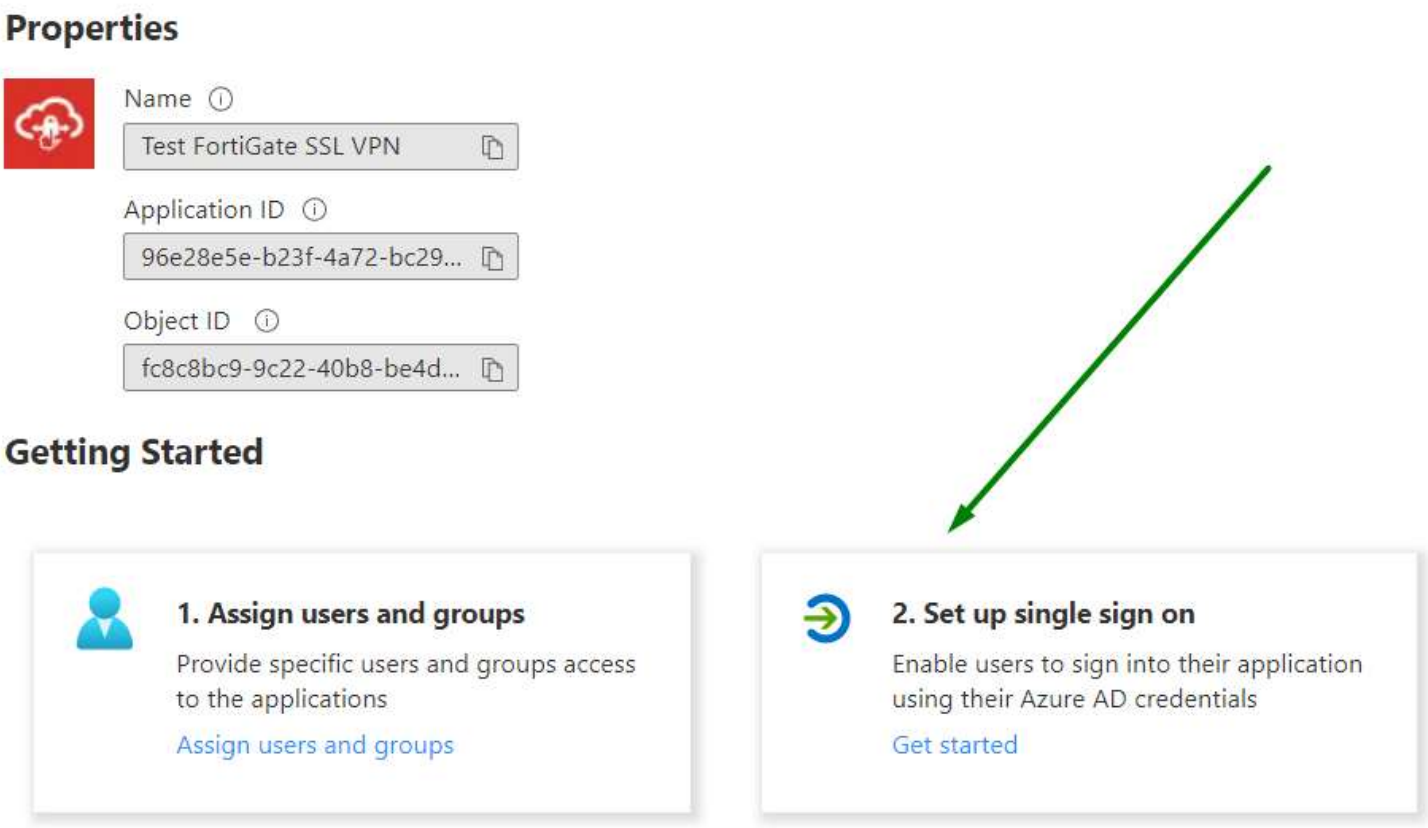


App settings

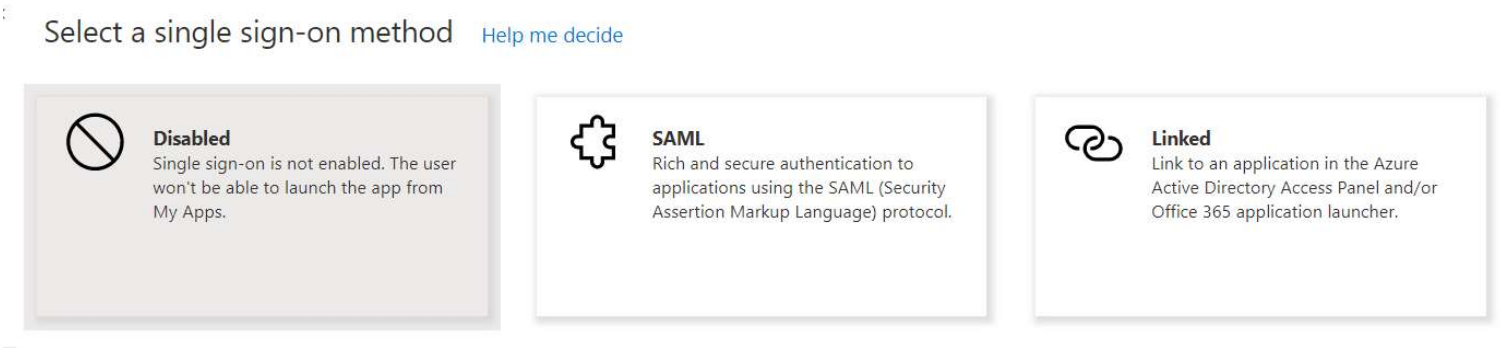
Adding the new application will take a few seconds. You should be redirected to the app setting page. If not - go back to the **Enterprise applications** section and find the new app manually (by first letters of the name), open it by clicking:



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

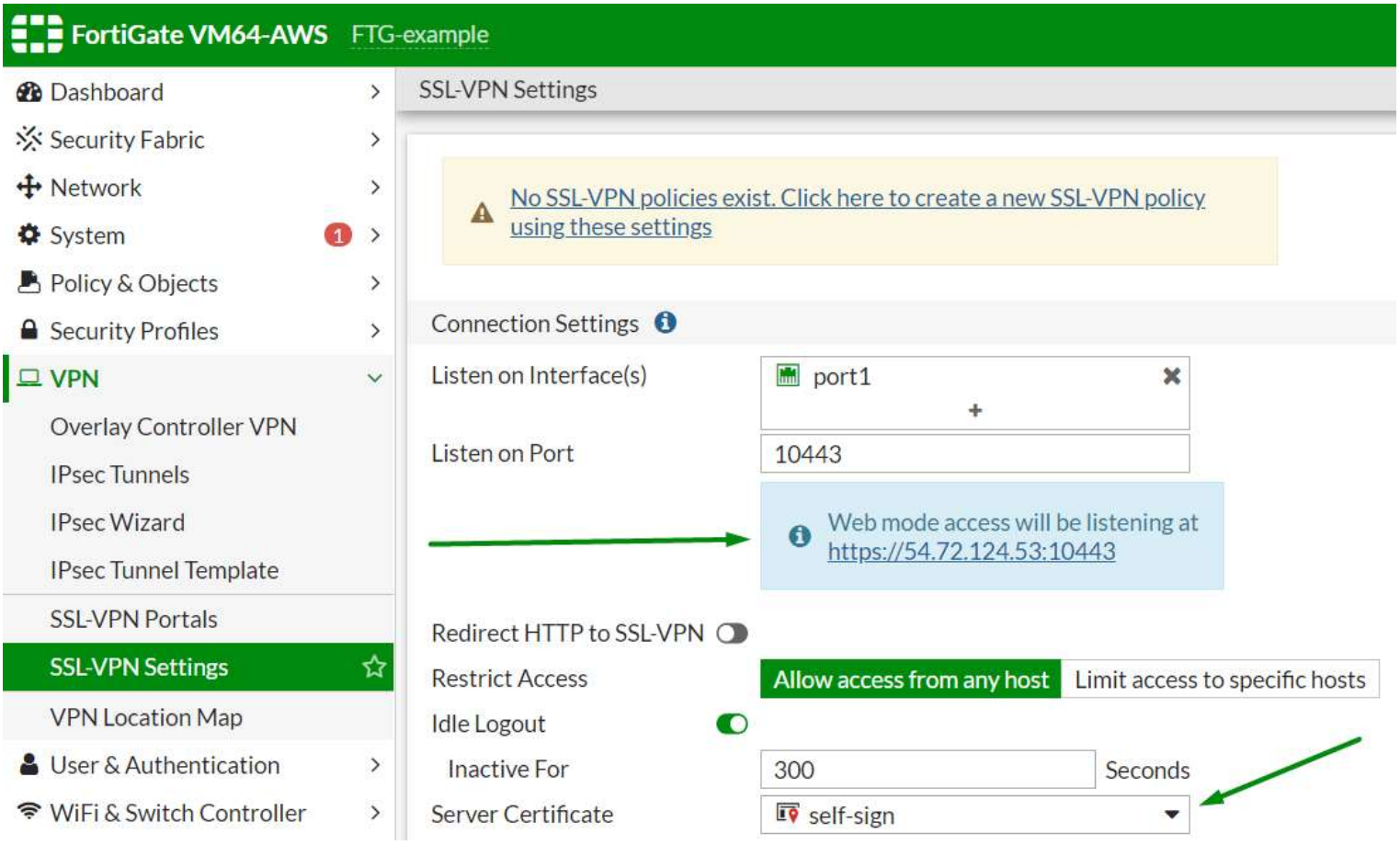


and choose **SAML**:



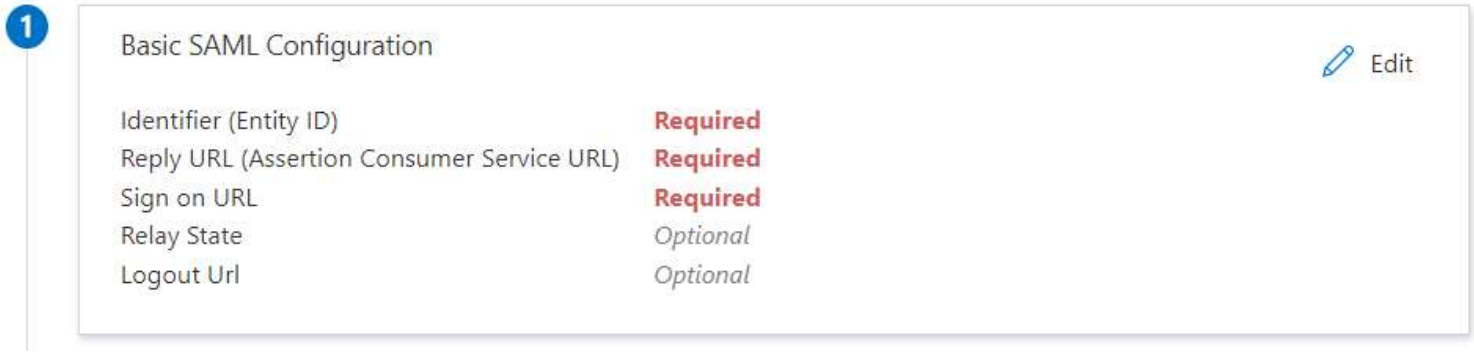
Basic SAML Configuration

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:



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).

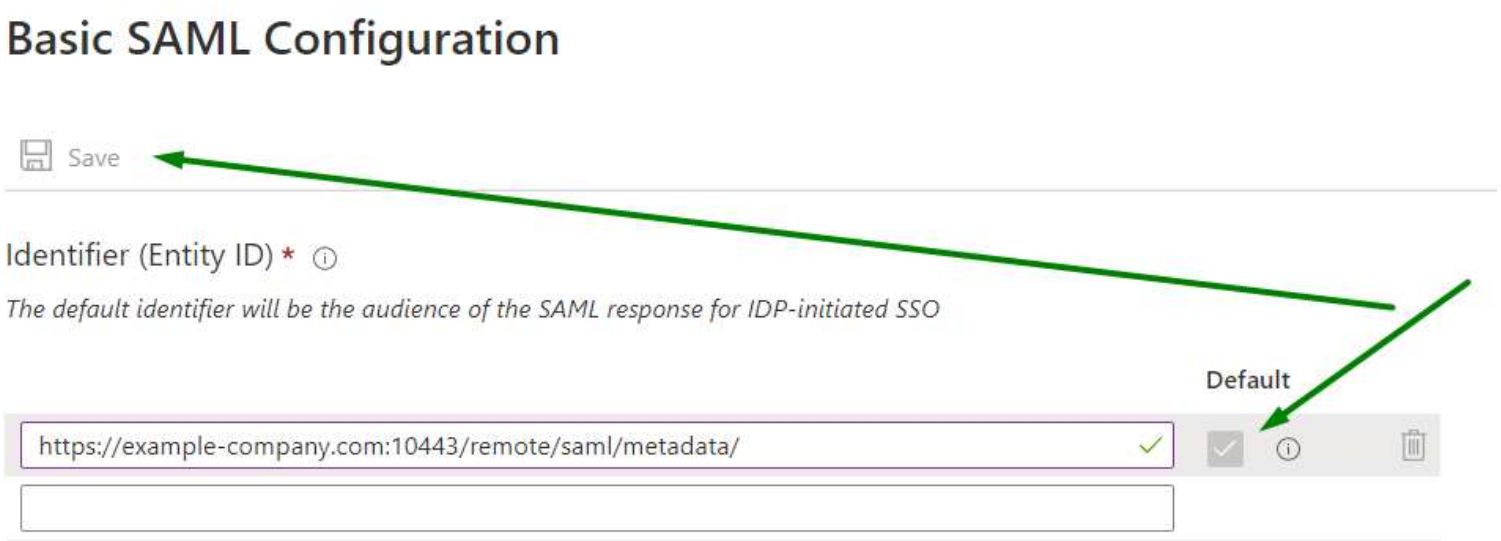
Go back to Azure. In the App settings click **Edit** under section **1**:



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/

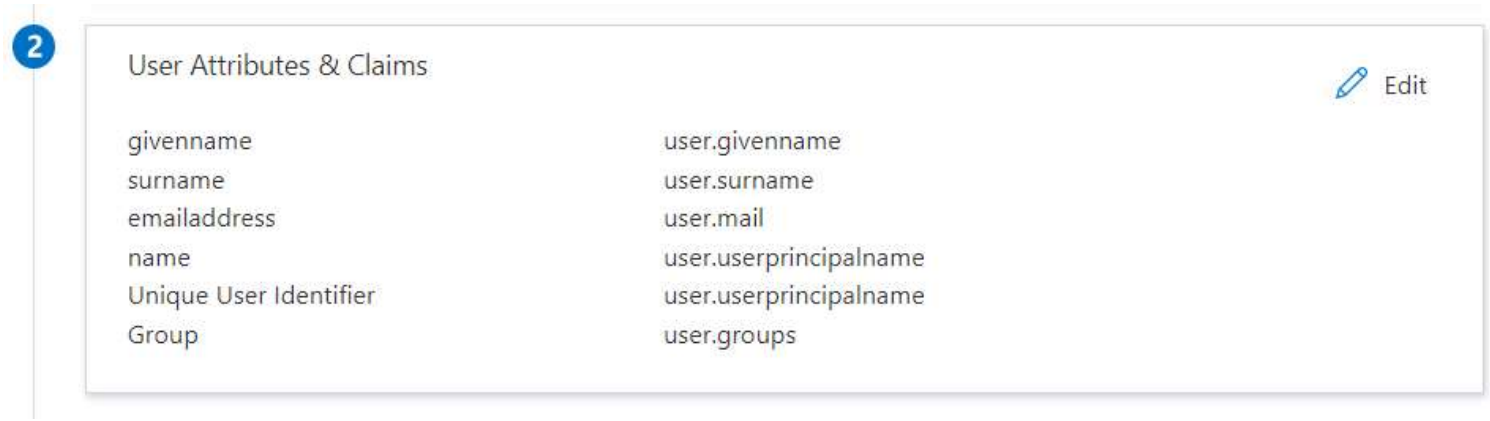
Make sure that value is set as **Default** were available:



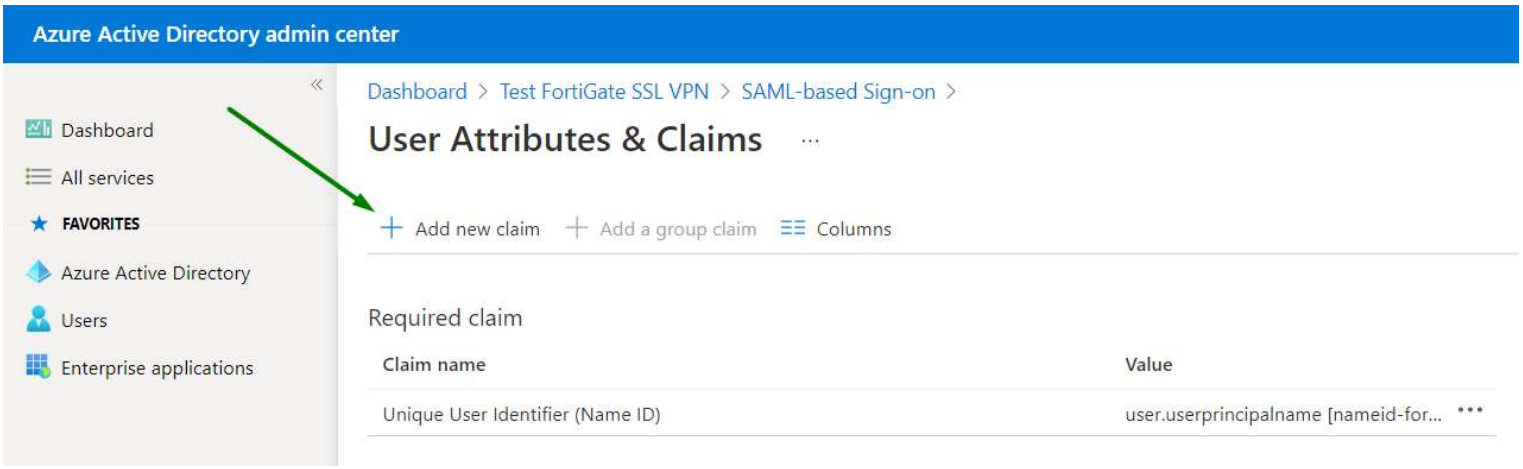
Finally, **Save**. When asked for a test — skip it by now.

User Attributes & Claims

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



Click **+ Add new claim**:

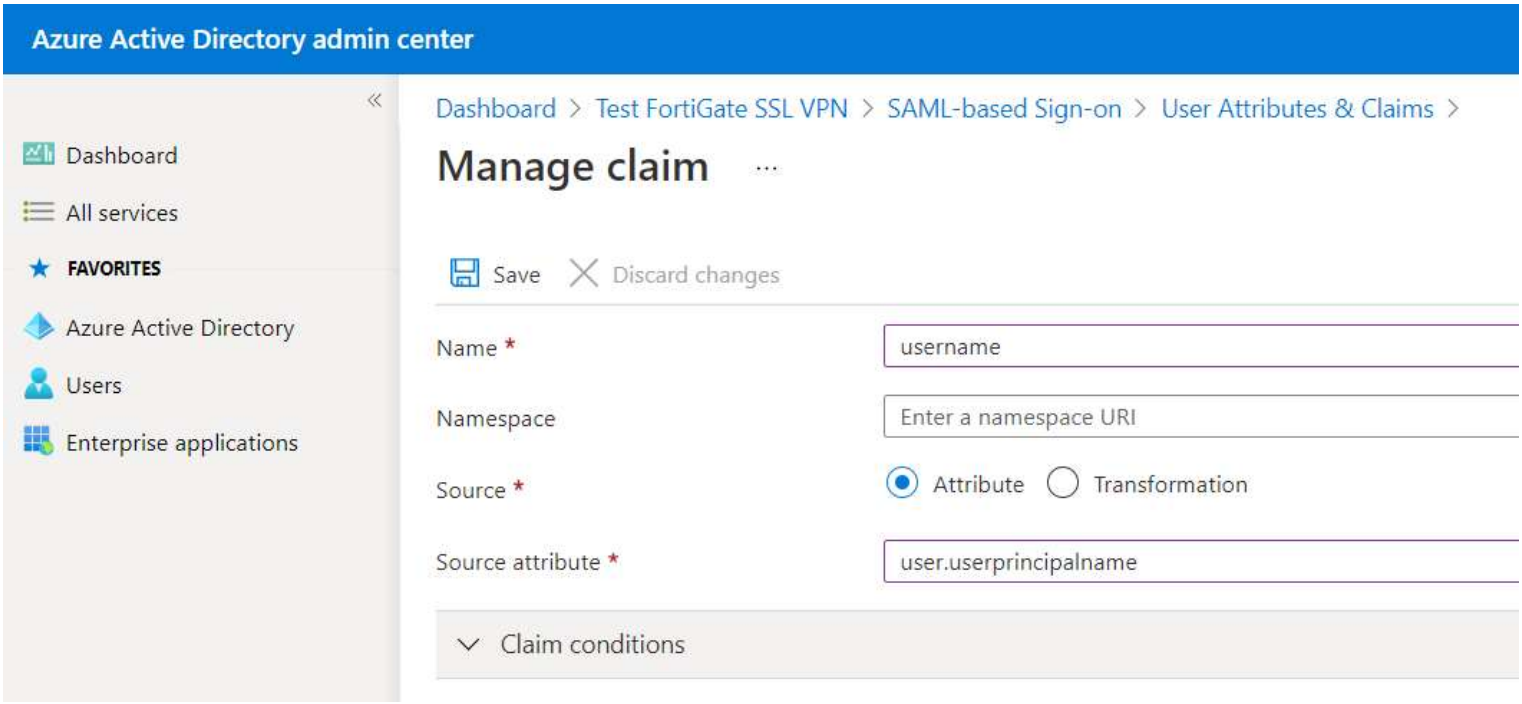


During one of the tests "Add new claim" was inactive. I found no reason for this — just re-created the Azure App.

Set the following (use autocompletion when possible):

Parameter	Value
Name	username
Source attrribute	user.userprincipalname

Then Save:

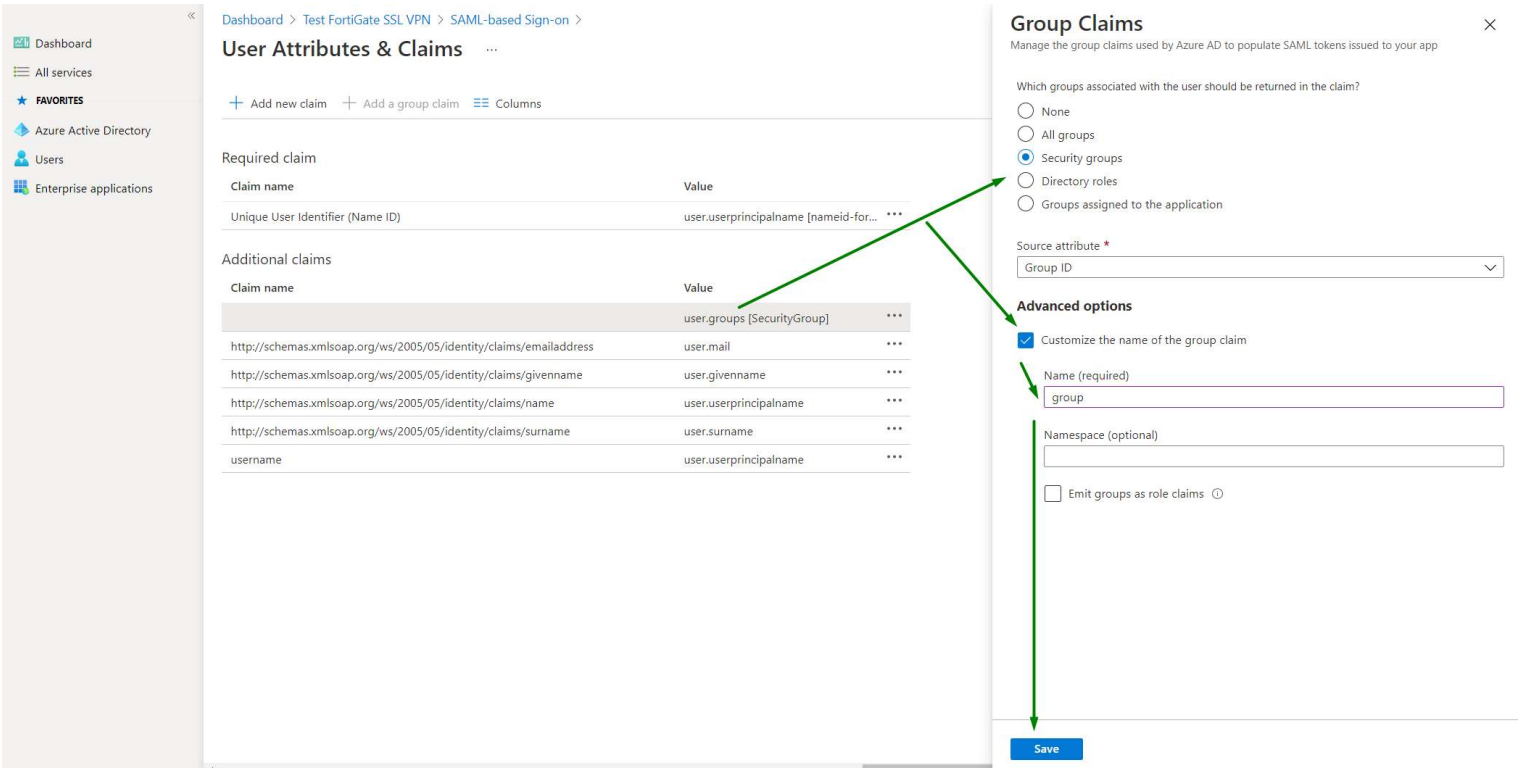


We need to add another claim, this time a **Group claim**. But this option was always unavailable for me. We can edit existed group claim. I am still not sure about this part.

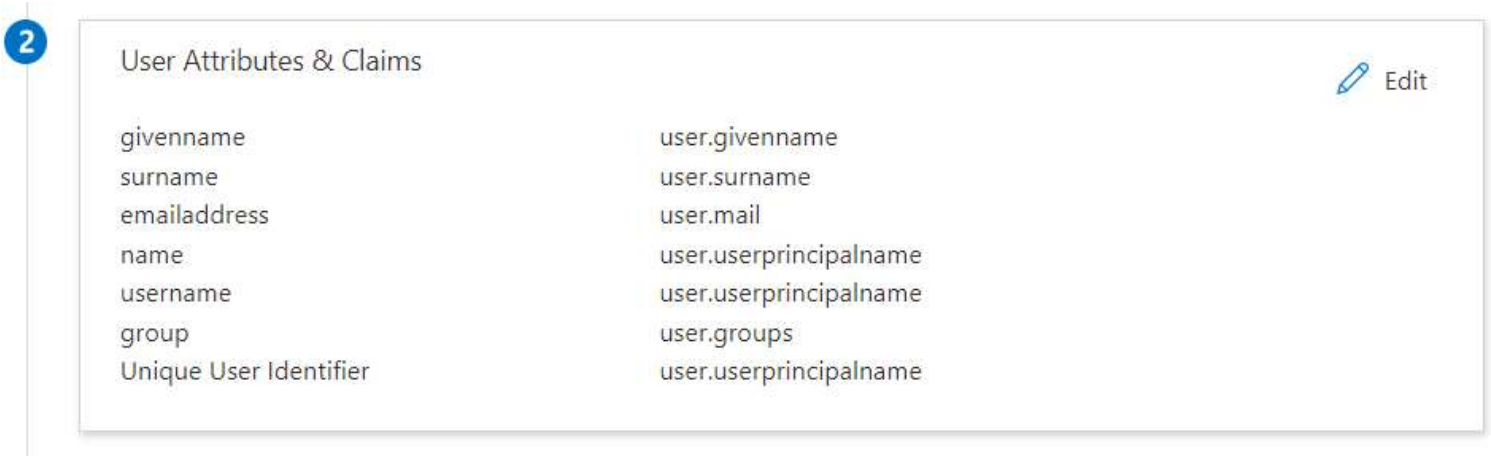
Click on **user.groups [SecurityGroup]** (do not use context menu •••). Enable **Customize the name of the group claim**. Set:

Parameter	Value
Name	group

Save and close setting:



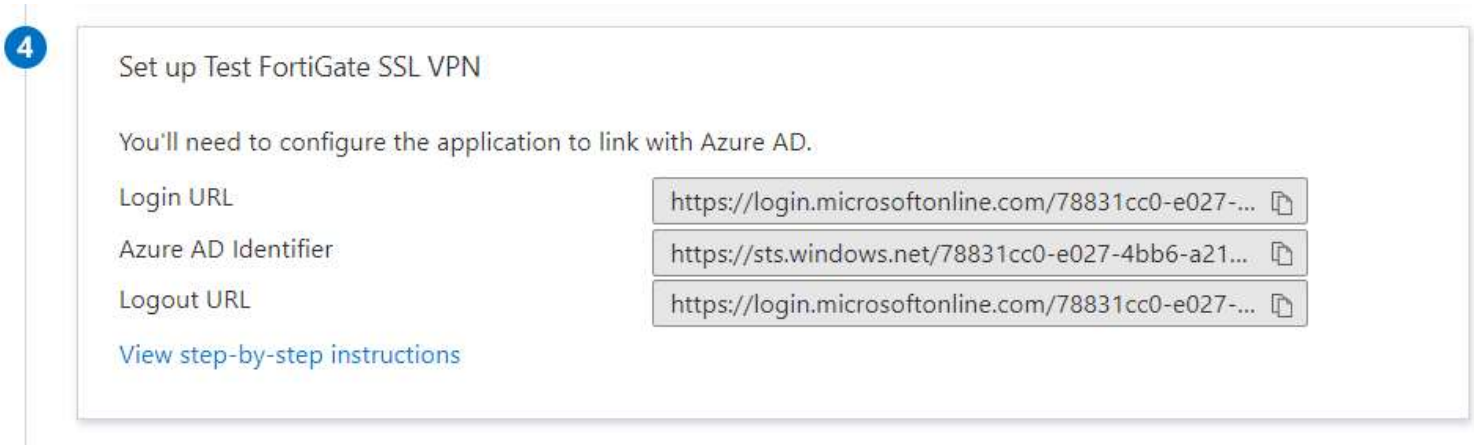
The final setting should look like this (check **username** and **group** parameters):



Connection URLs

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

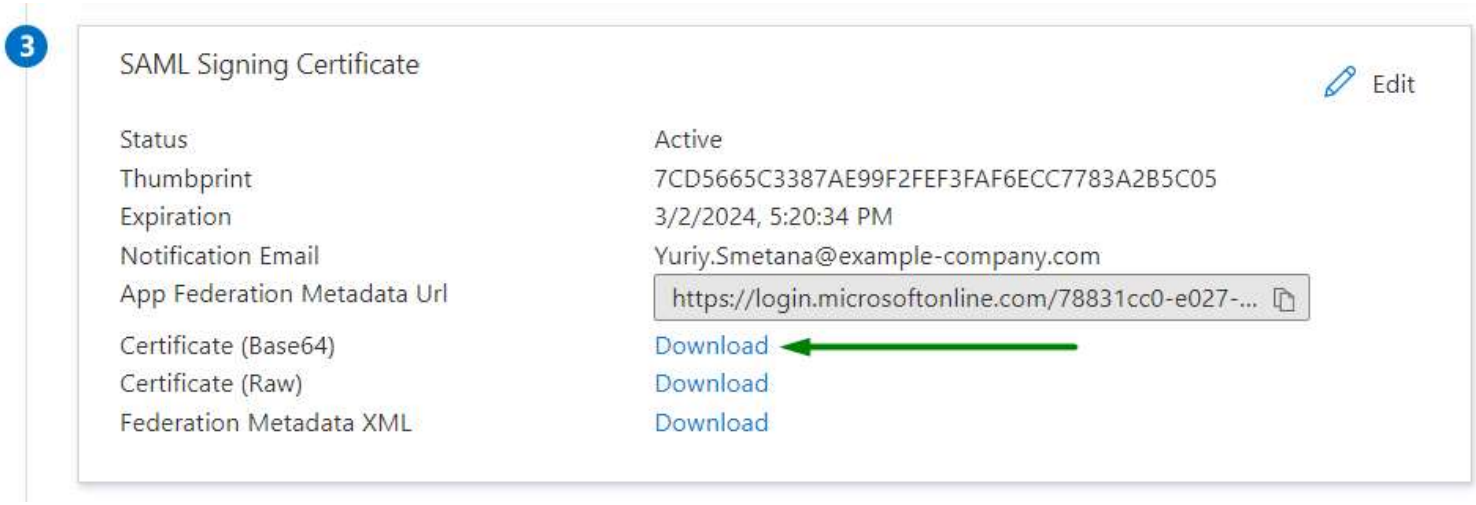
- Login URL
- Azure AD Identifier
- Logout URL



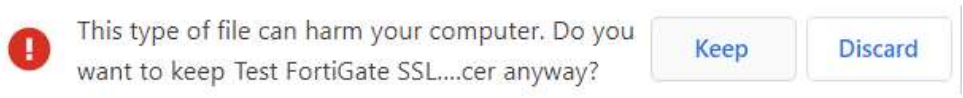
Azure certificate

Azure part

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



Save the file to the local computer.

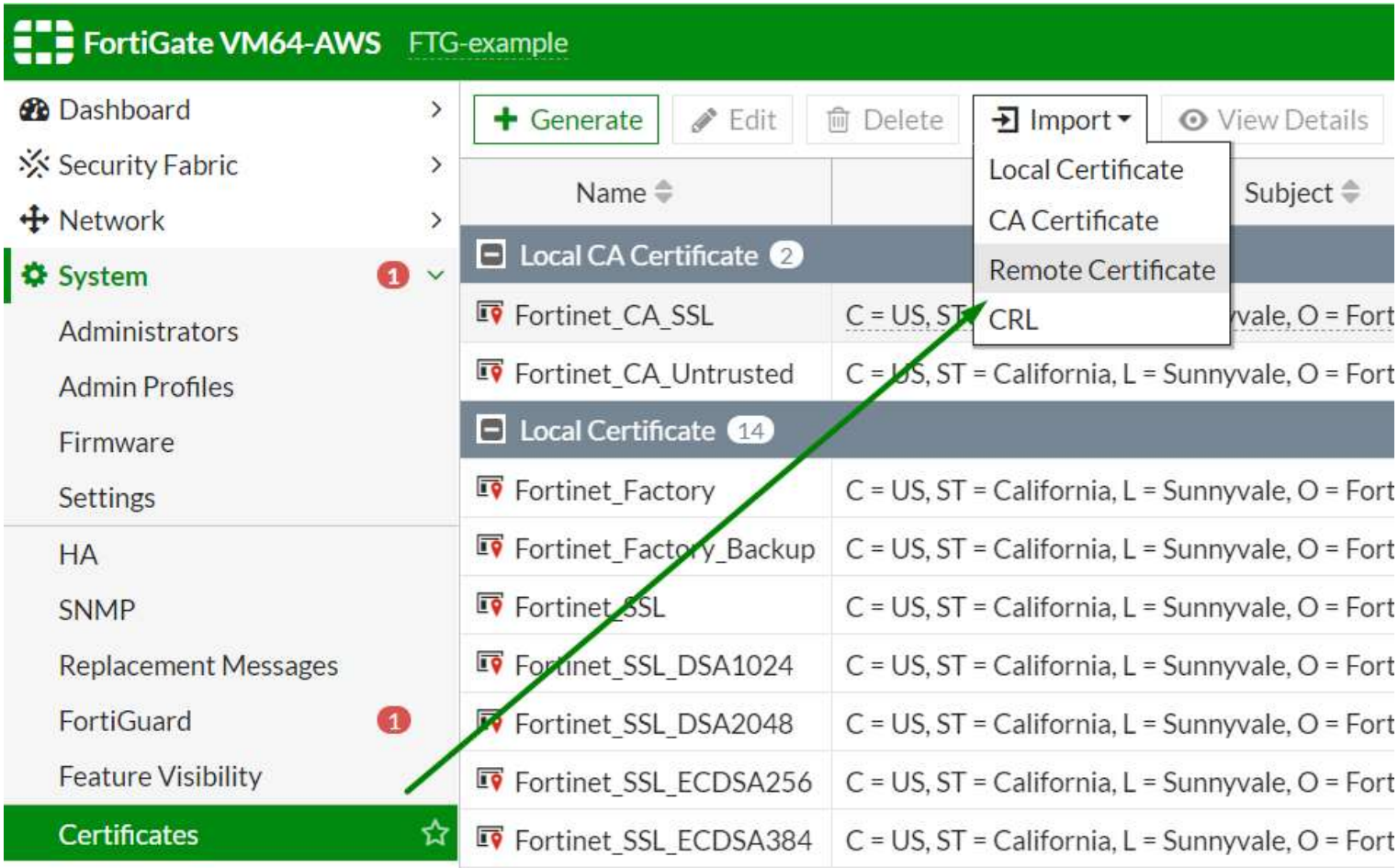


If the certificate is wrong, most likely you will get this error later on:

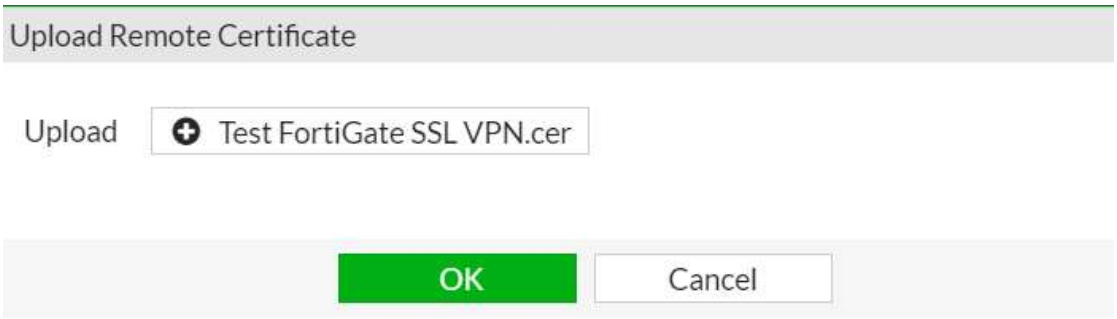
```
samld_sp_login_resp [747]: Failed to process response message. ret=440(The profile cannot verify a signature on the message)
```

FortiGate part

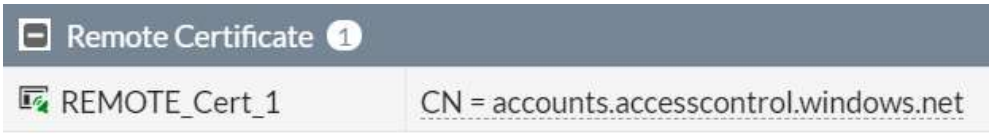
In the FortiGate UI go to the **System → Certificates** section. Then do **Import → Remote Certificate**.



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**:



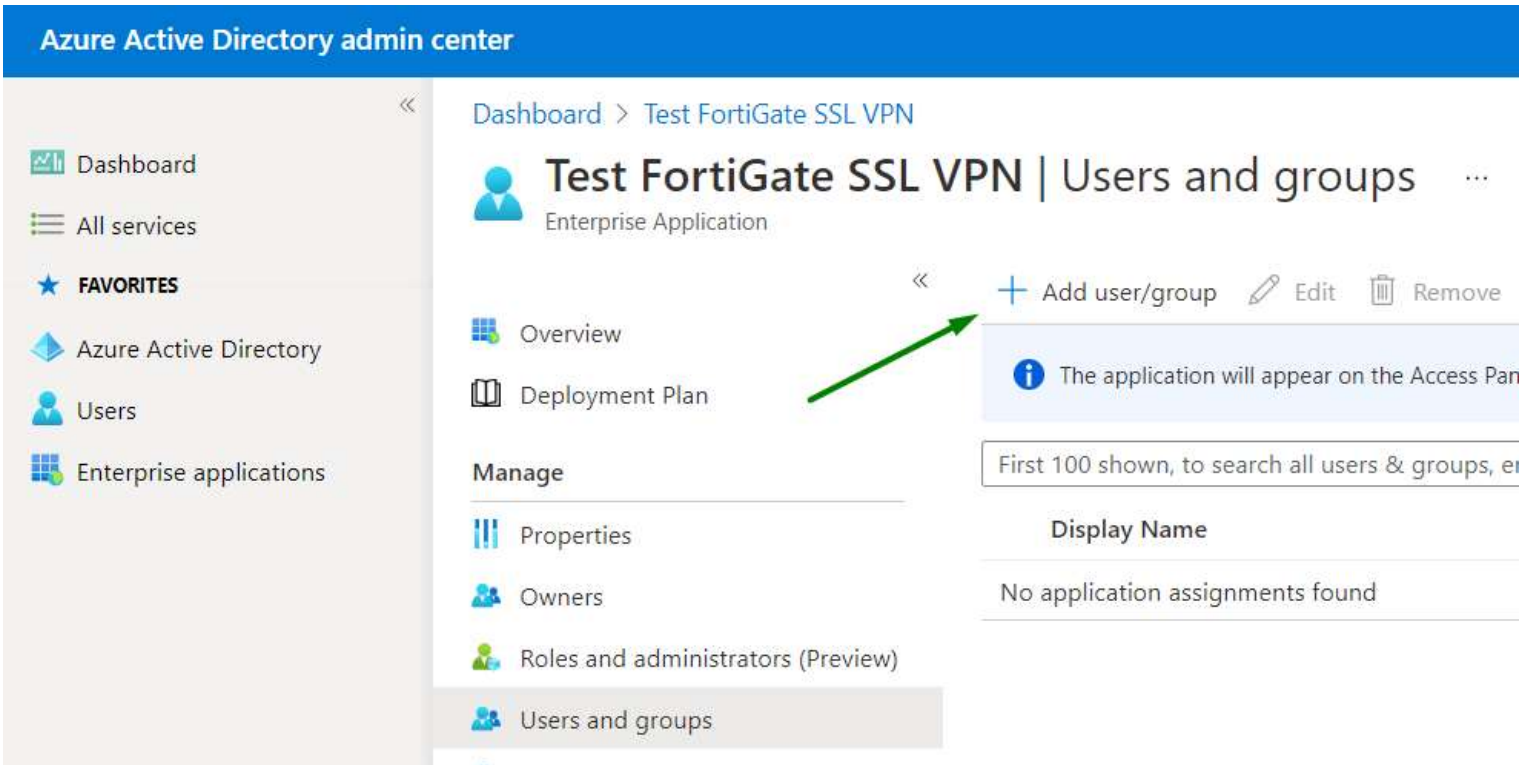
Give it a reasonable name in CLI, if you want:

```
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
```

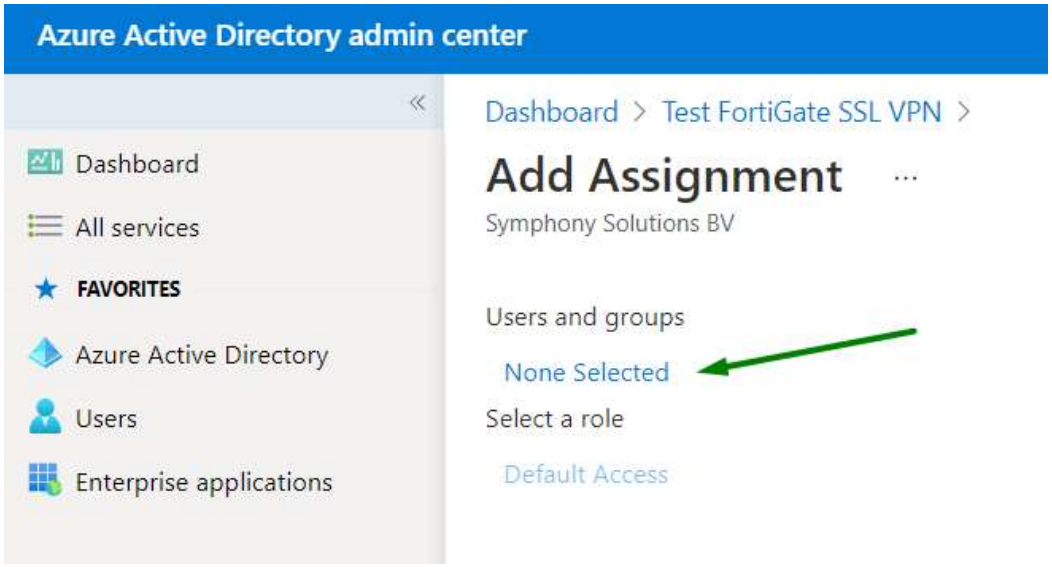
Azure users and groups

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.

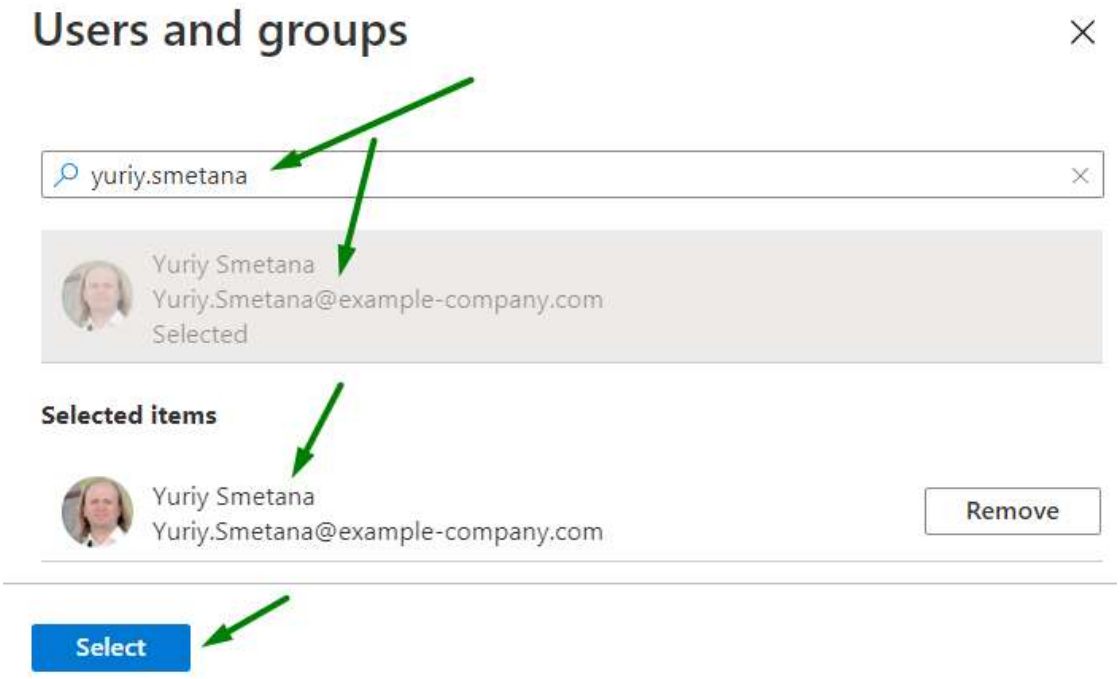
In the App settings open **Users and groups**, then **+ Add user/group**:



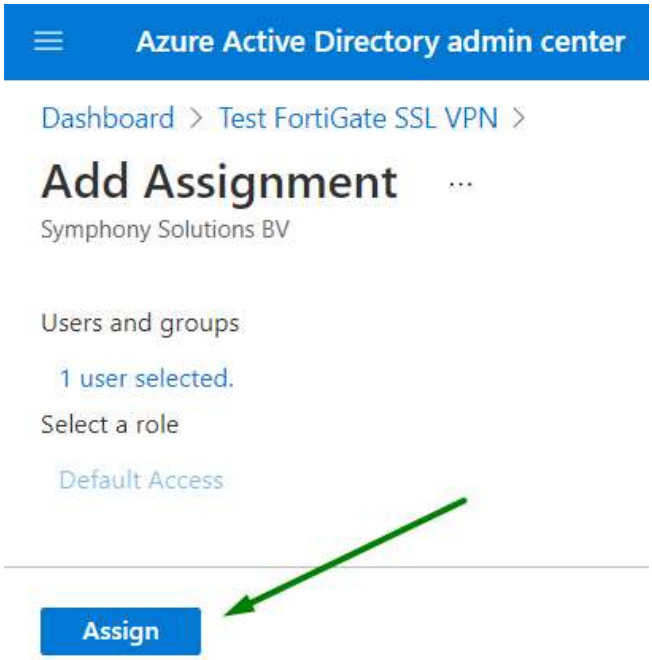
Click **None selected** first:



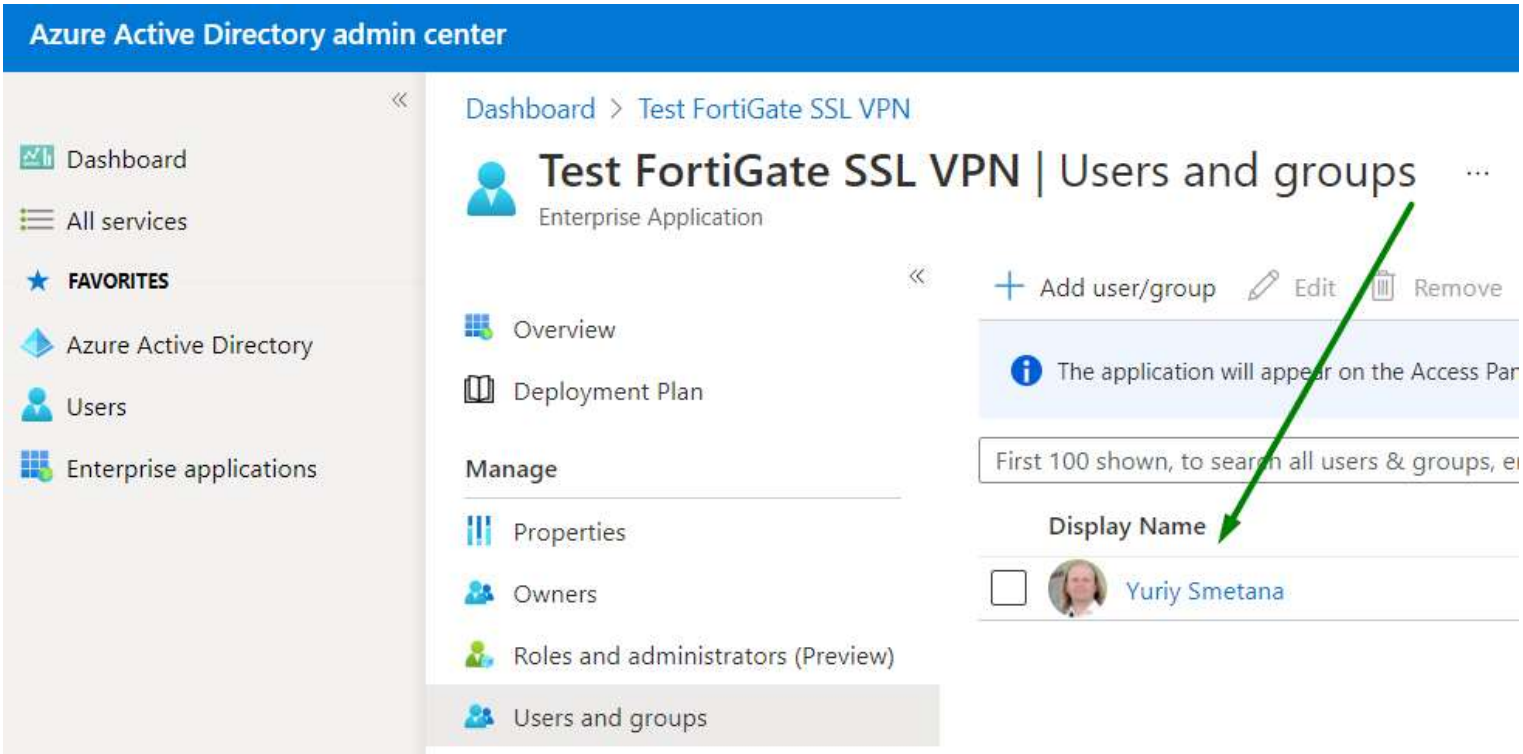
Search for the user, click it, click **Select**:



And, finally, **Assign**:



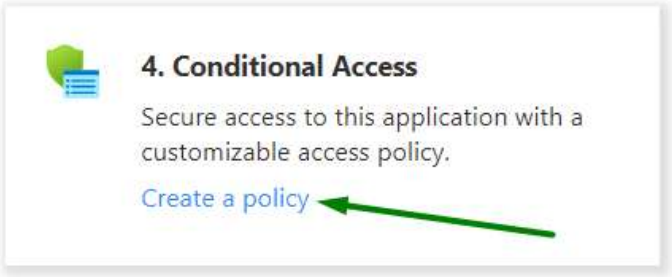
We have the first user now:



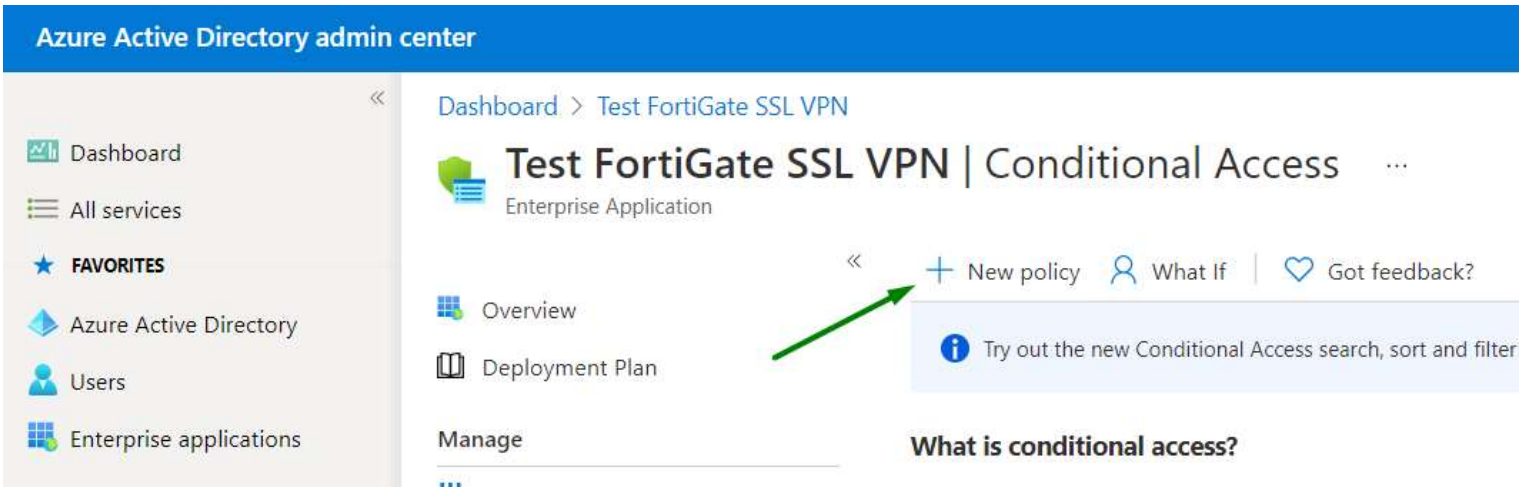
There are other user-related settings in **Properties** page of the App, but we do not use them at the moment.

Conditional access

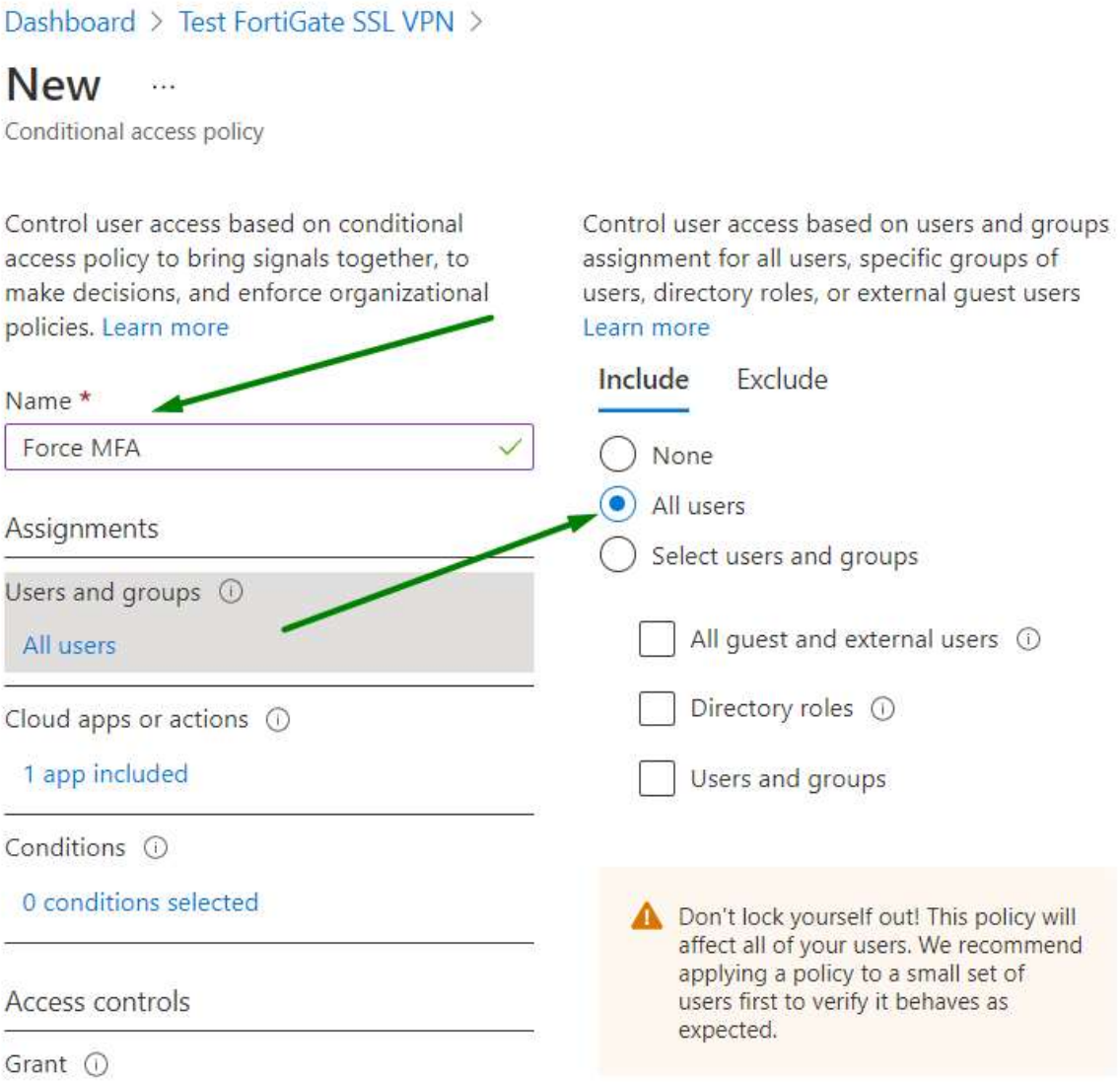
From the main page of the App, in section **4. Conditional Access,** click **Create a policy**:



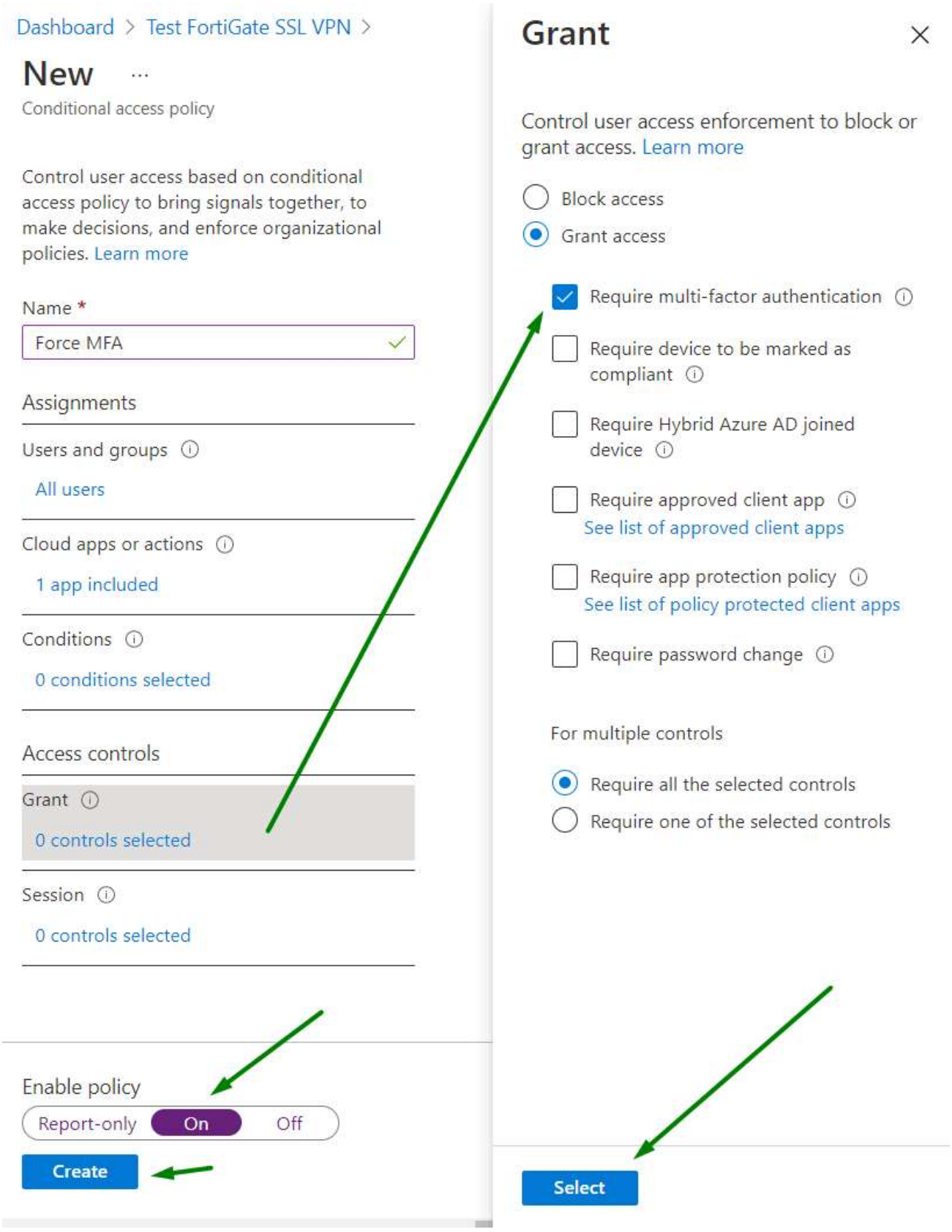
Then **+ New policy**:



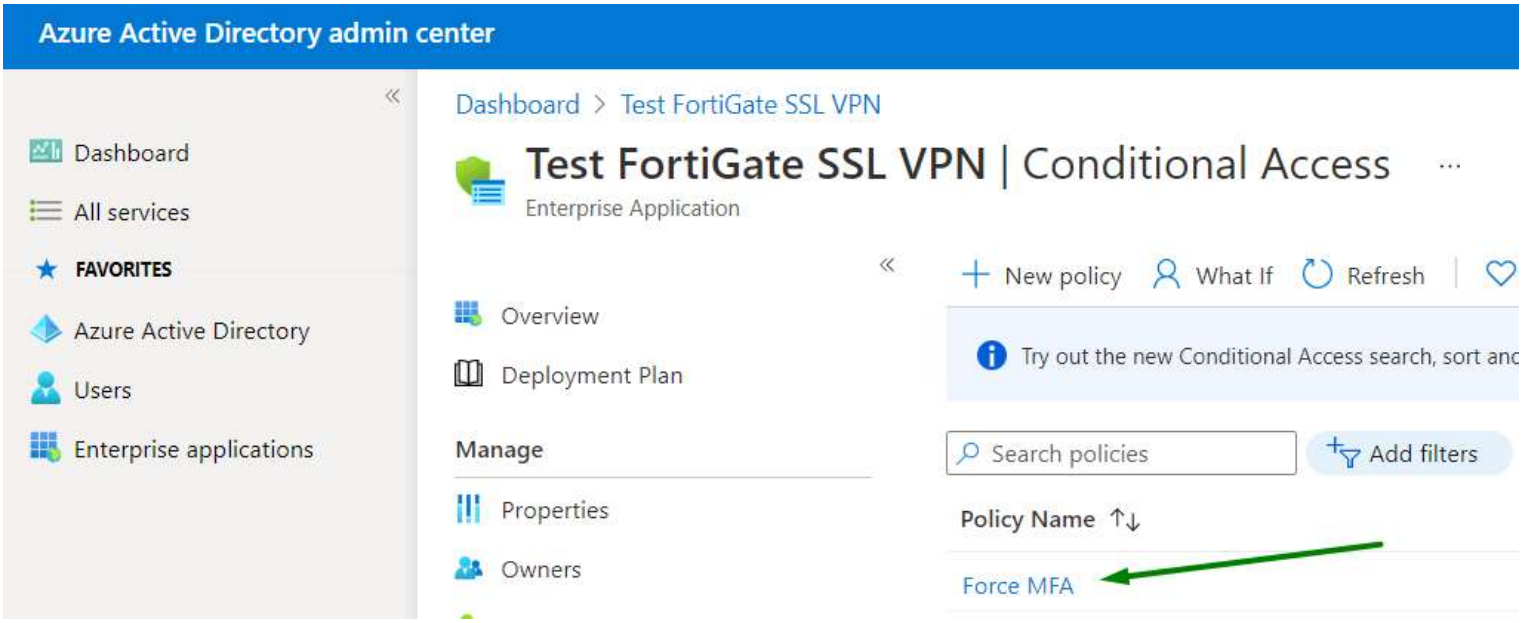
Give it a name and under **Users and groups** select **All users**:



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
Grant
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 result:



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.q *Fortinet_Factory*)
- Remote certificate name (we renamed it to **Azure_SAML**)

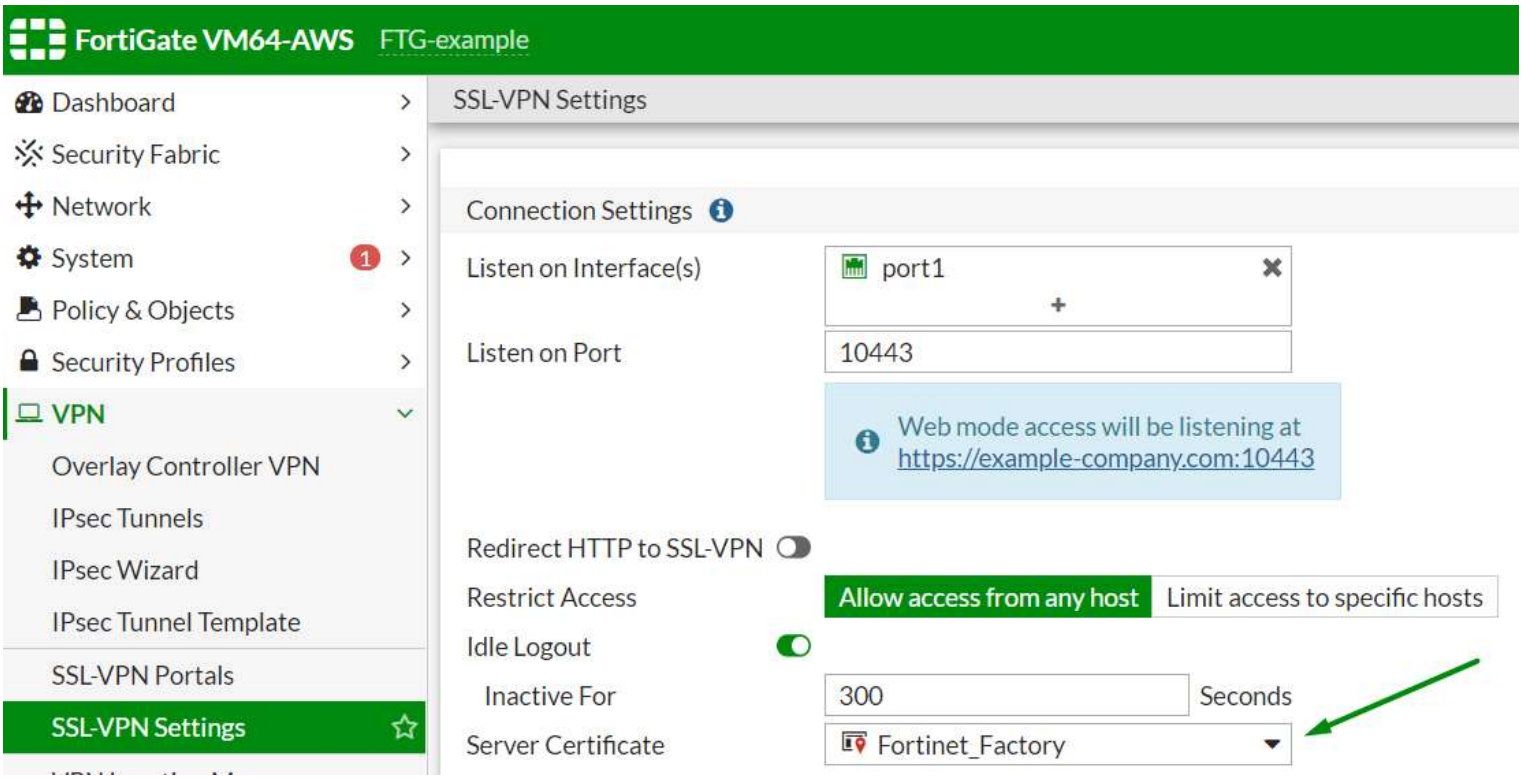
In the FortiGate console:

```
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:

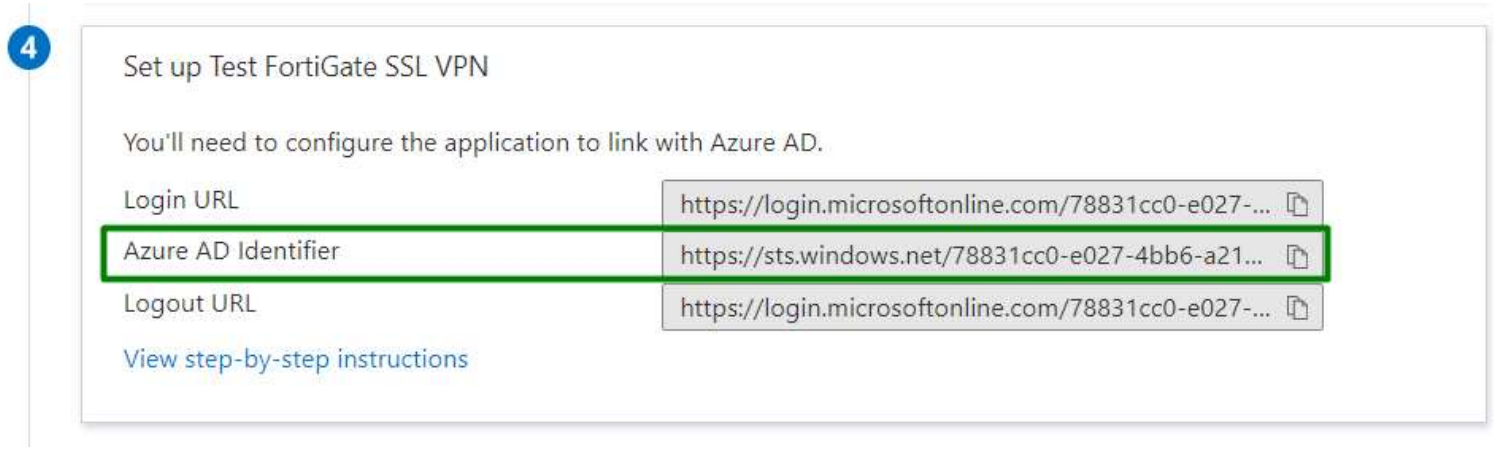


`set entity-id set single-sign-on-ur set single-logout-url`

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**.

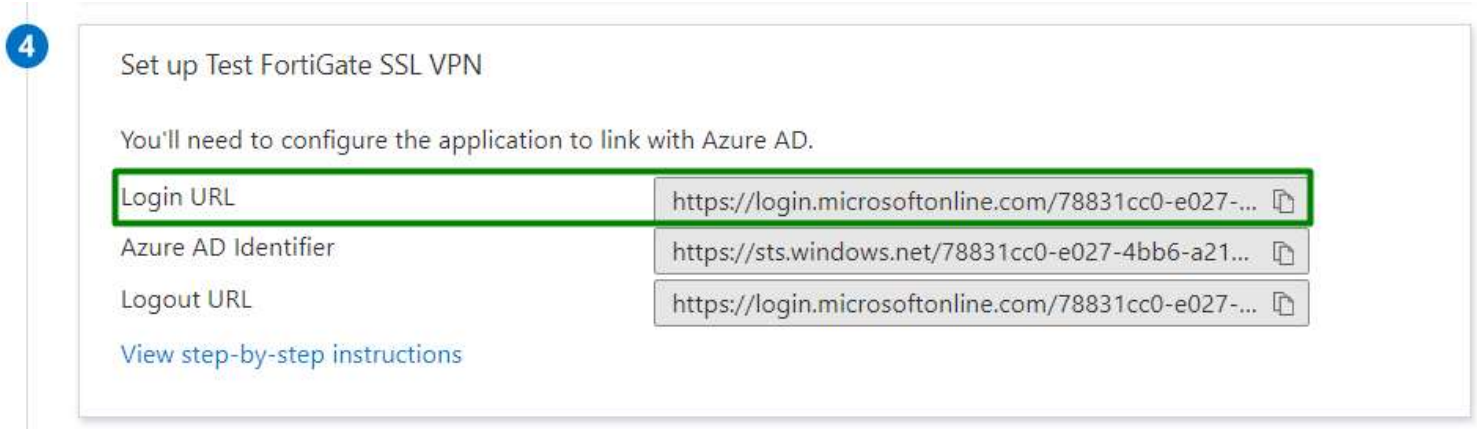
`set idp-entity-id`

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



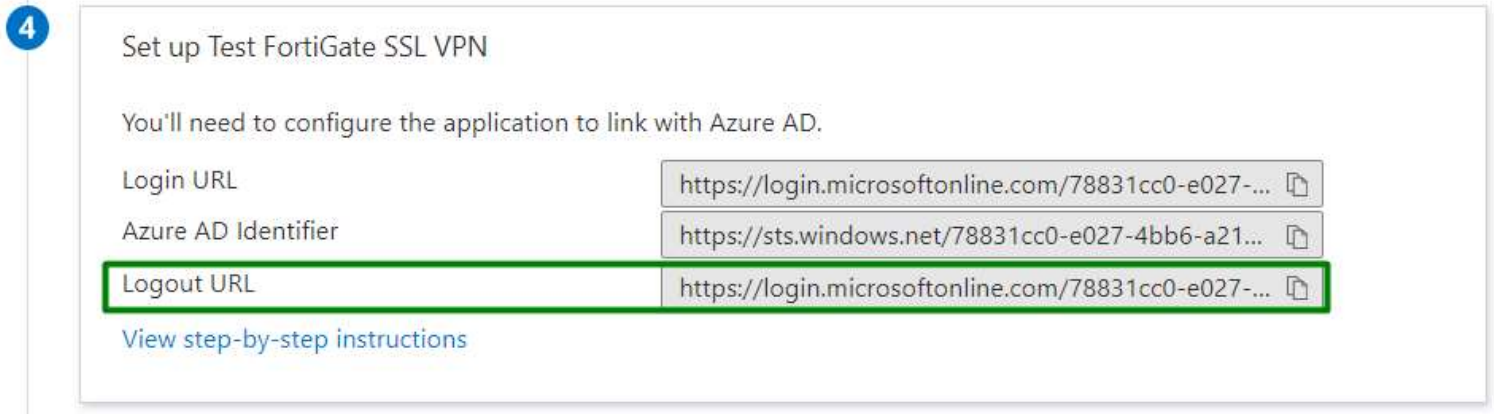

```
set idp-single-sign-on-url
```

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




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

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



```
set idp-cert
```

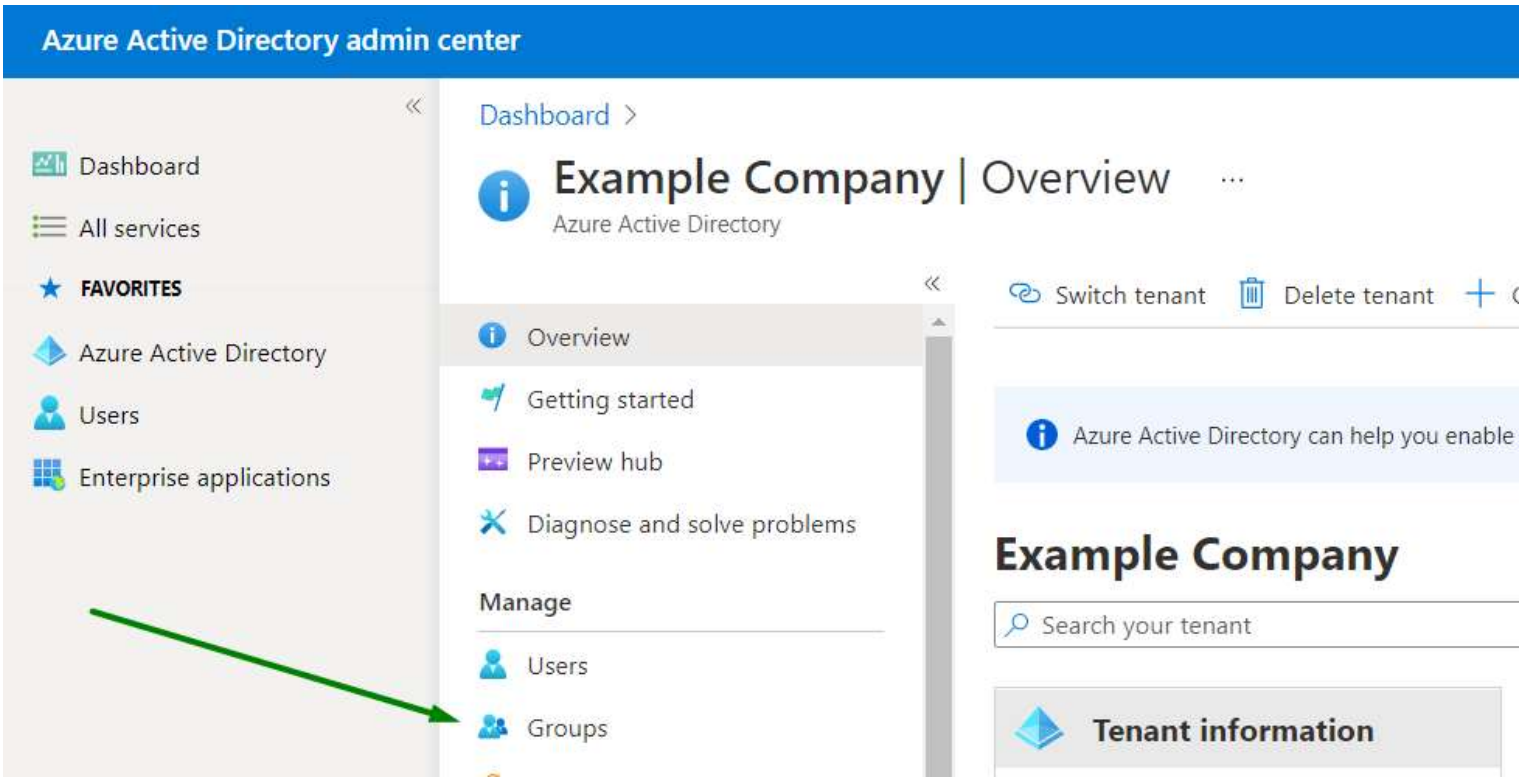
The one we downloaded from Azure app settings, imported into the Fortigate, and renamed for convenience.

FortiGates groups connected to Azure

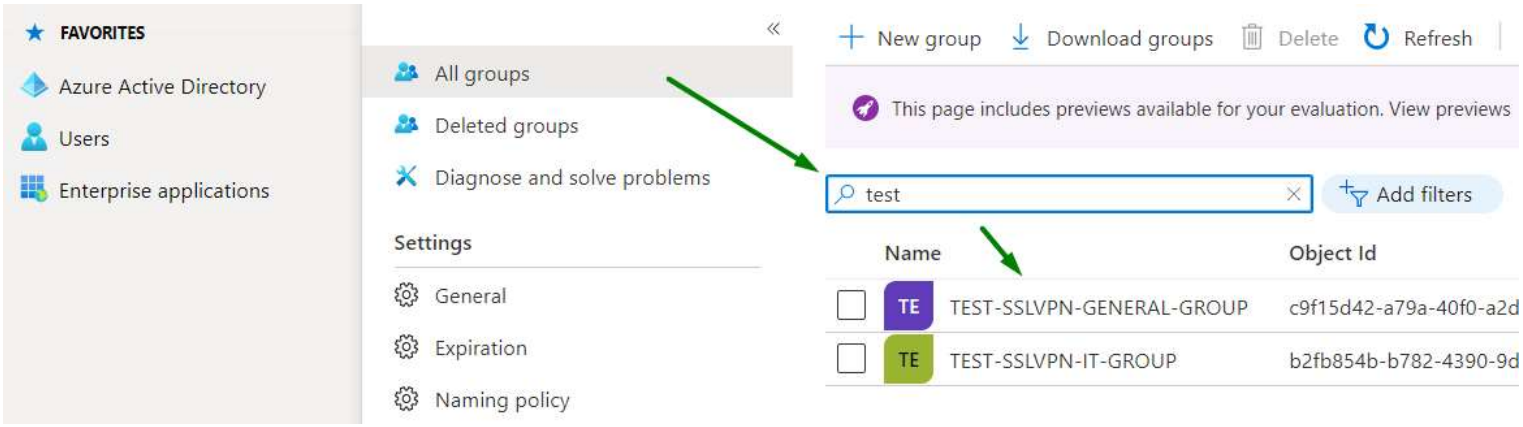
Azure part

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.

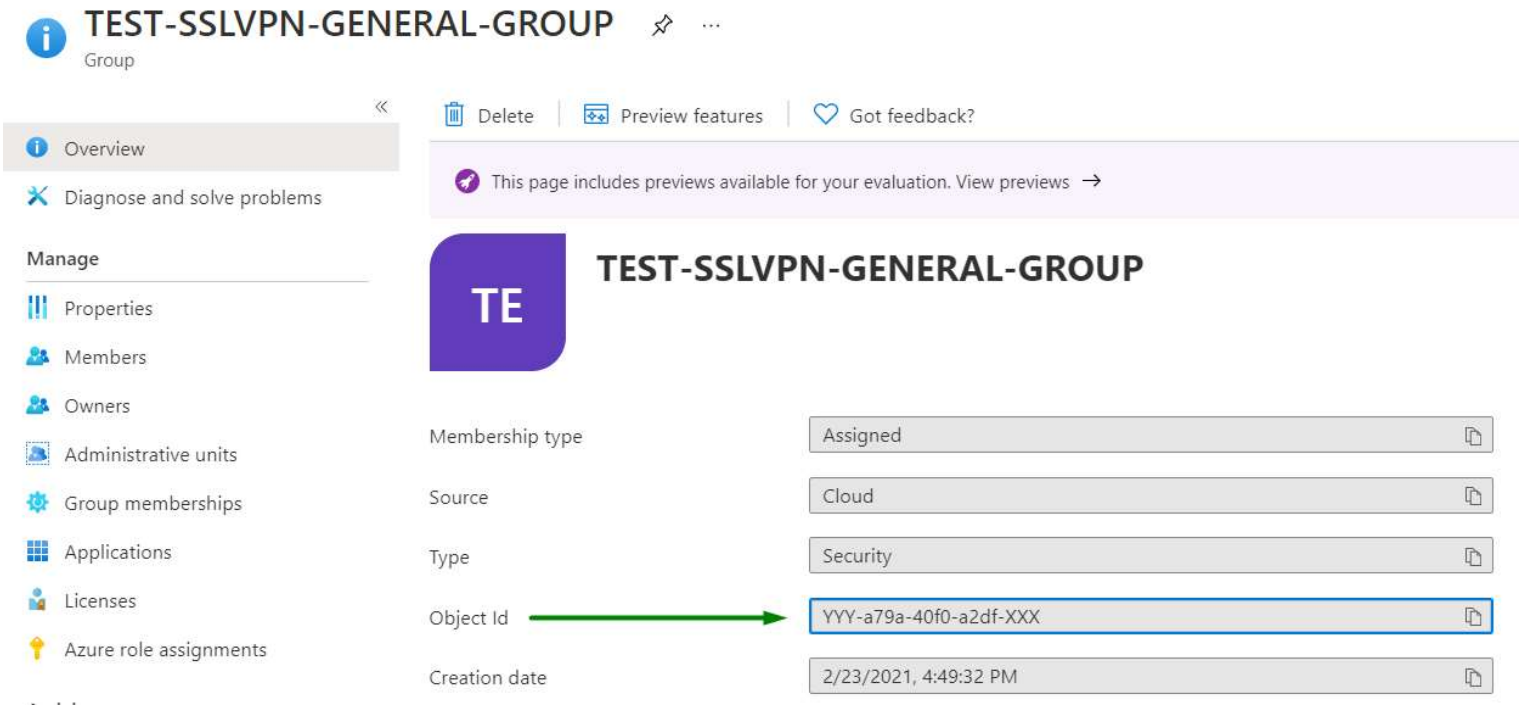
On the main page of the **Azure Active Directory admin center** click **Groups**:



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



Copy the Object ID of the group:



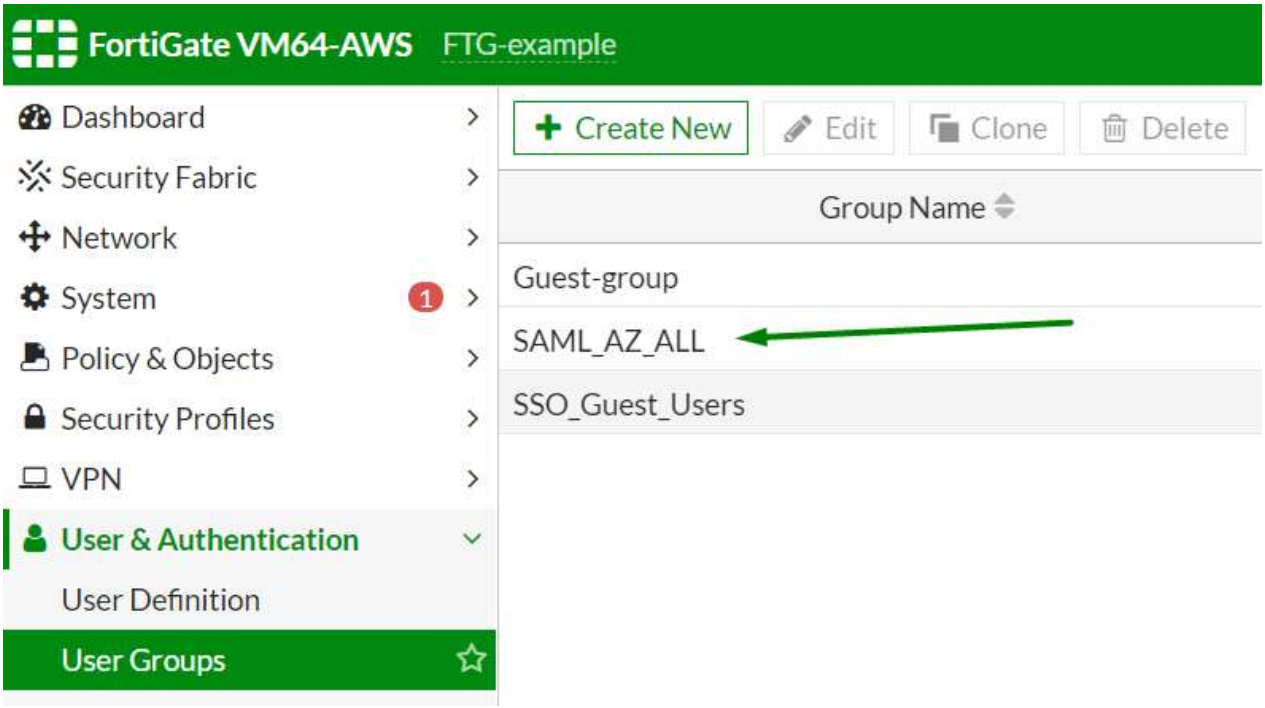
FortiGate part

Now, knowing Azure group ID link iot 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.

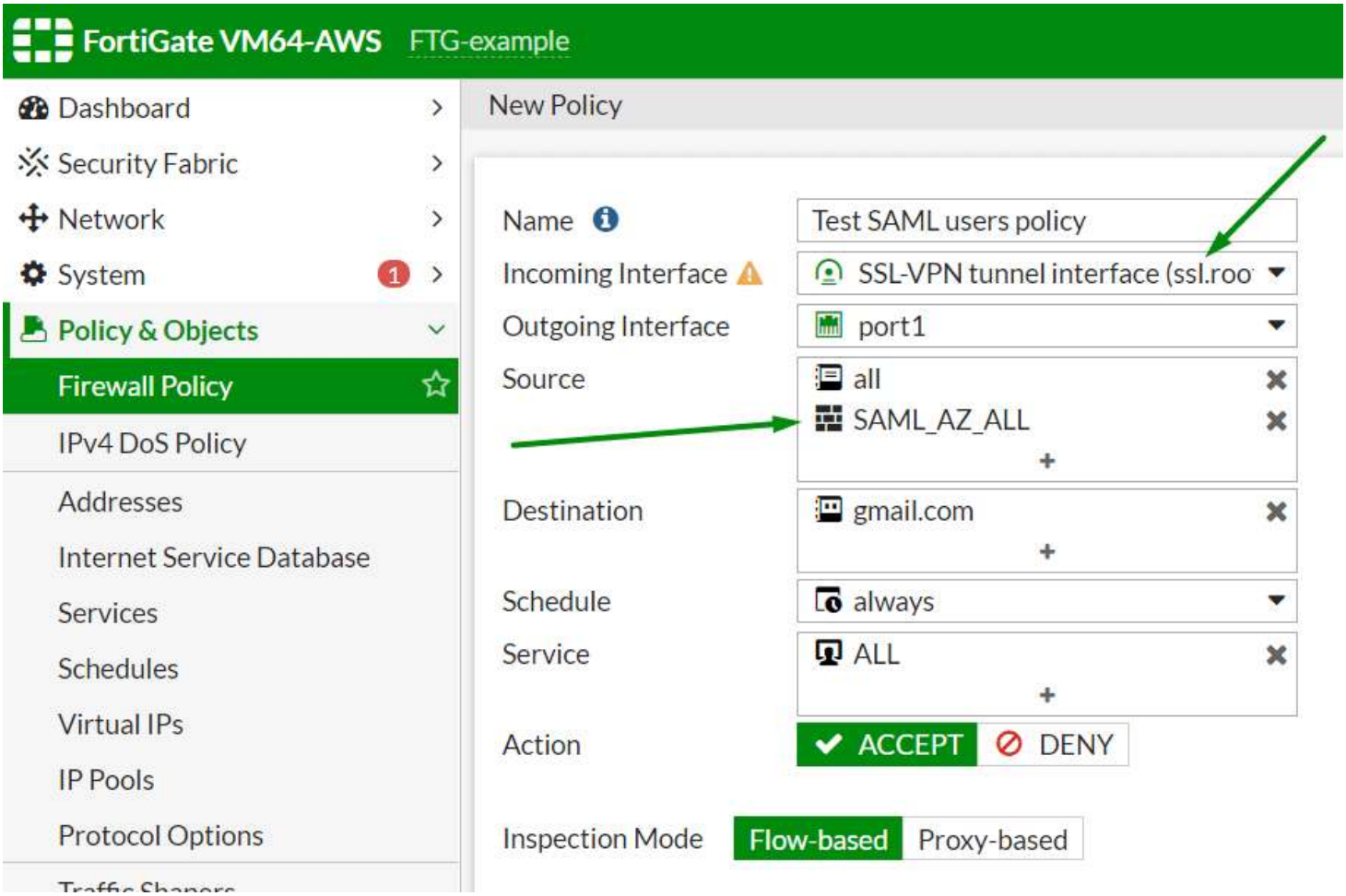
Check FortiGate groups info, the group should also be there:



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 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
```

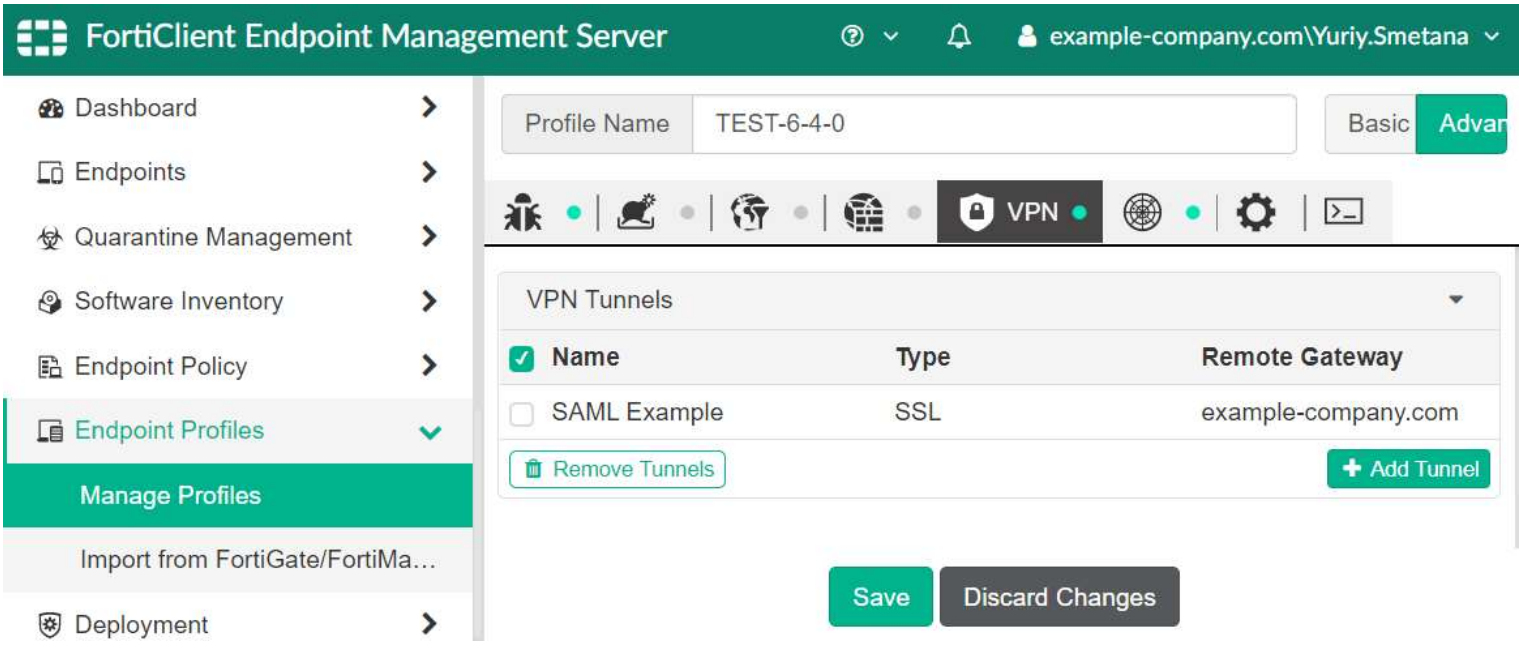
And, just to be sure:

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

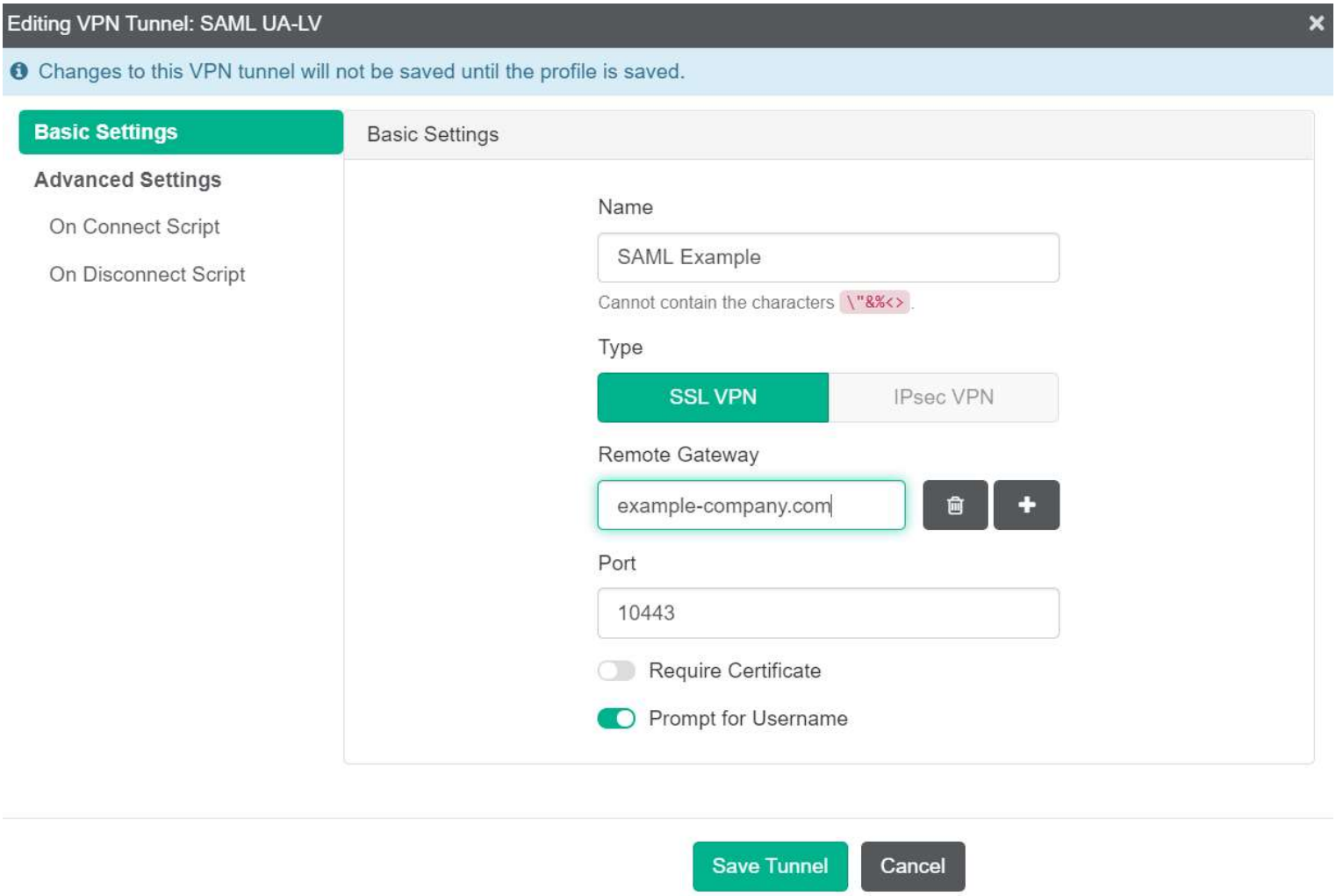
FortiClient EMS setup

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**.

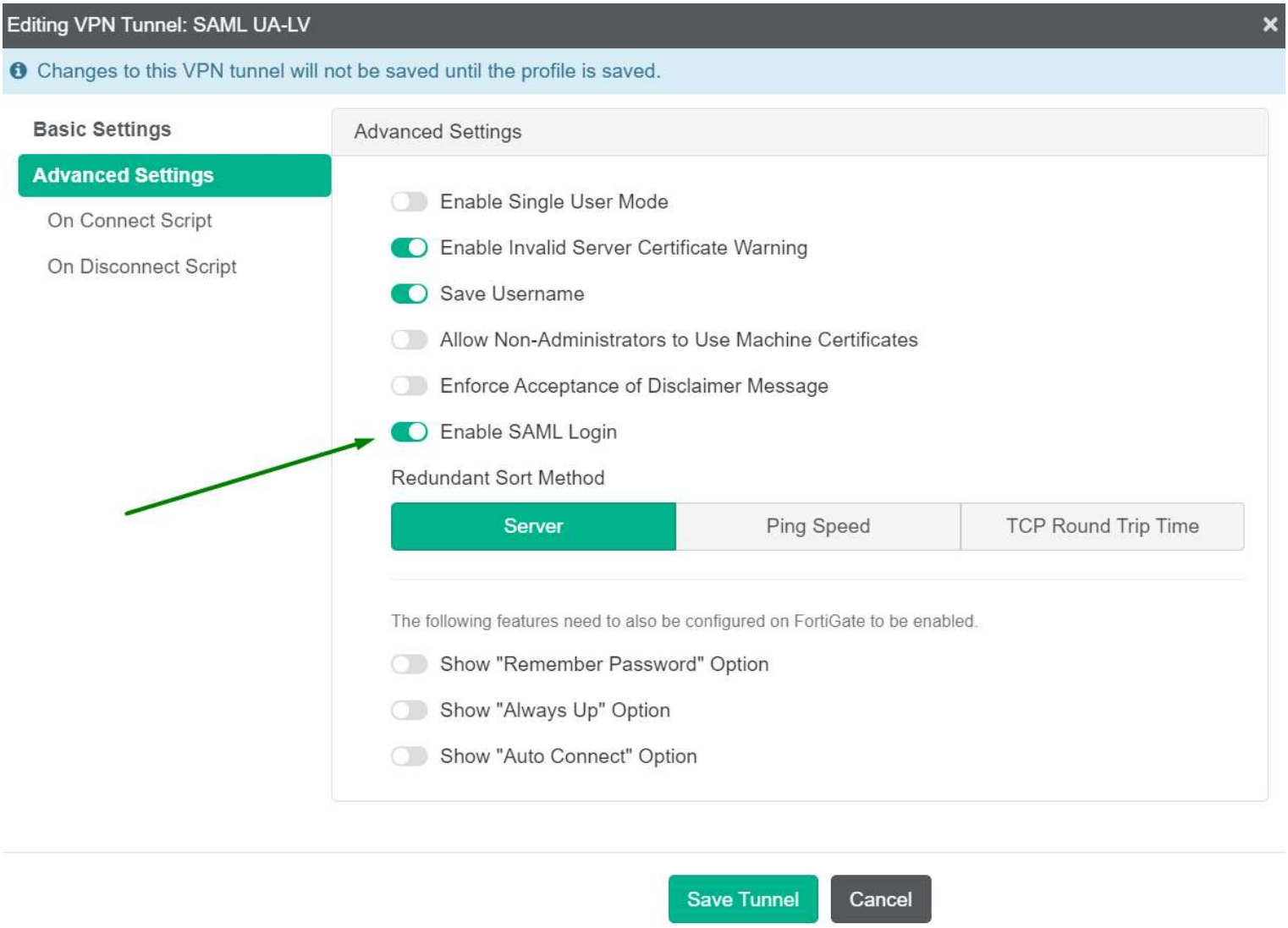
Add Tunnel in the **VPN Tunnels** section of **VPN** tab of the profile.



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



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

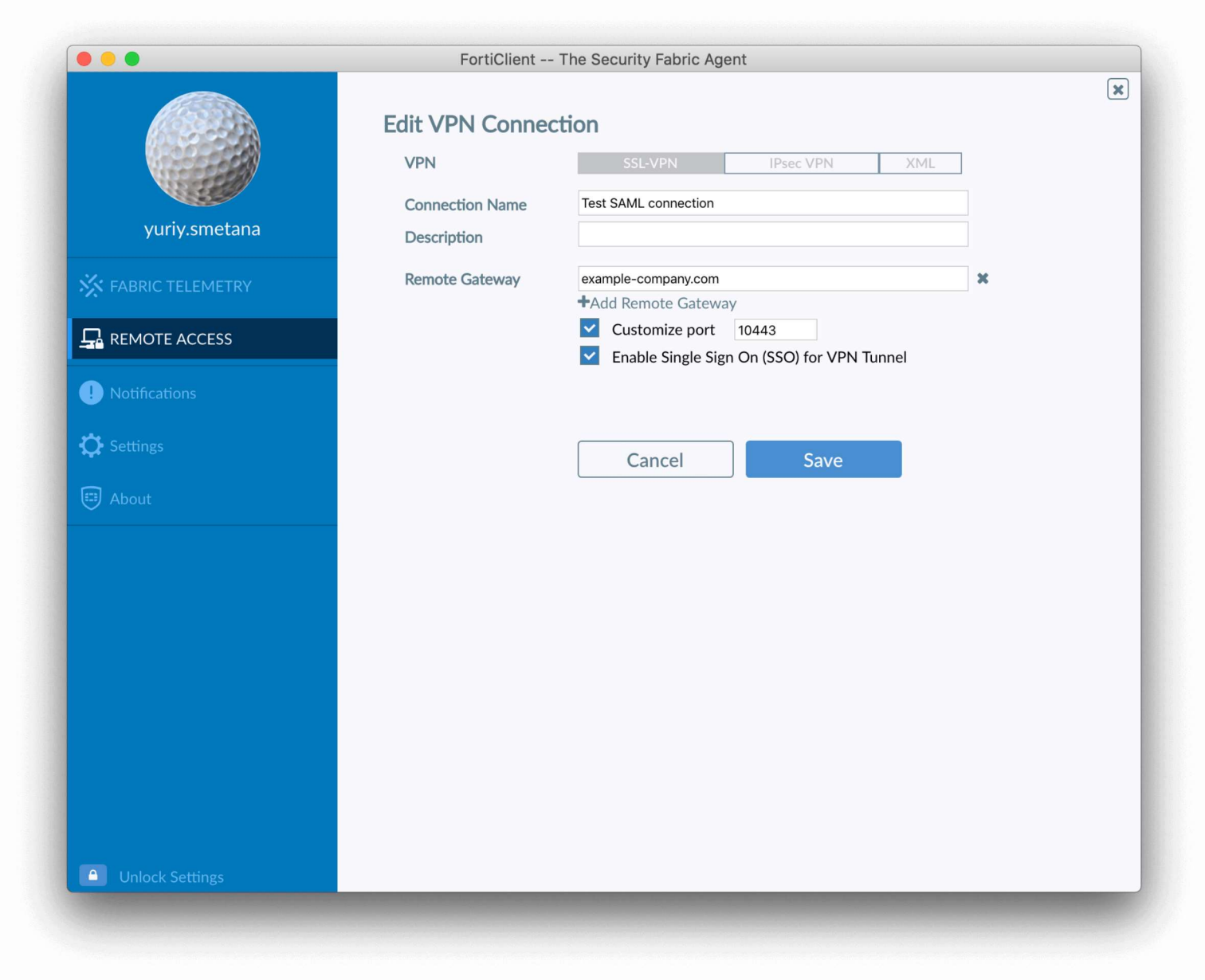


Wait till the FortiClients populated the settings.

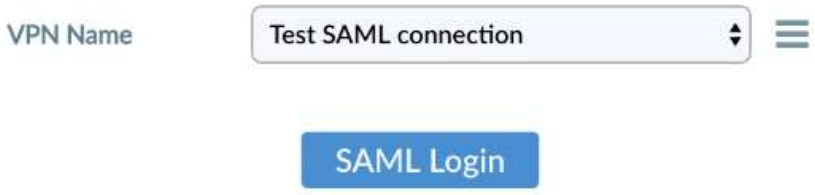
FortiClient manual setup and run

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

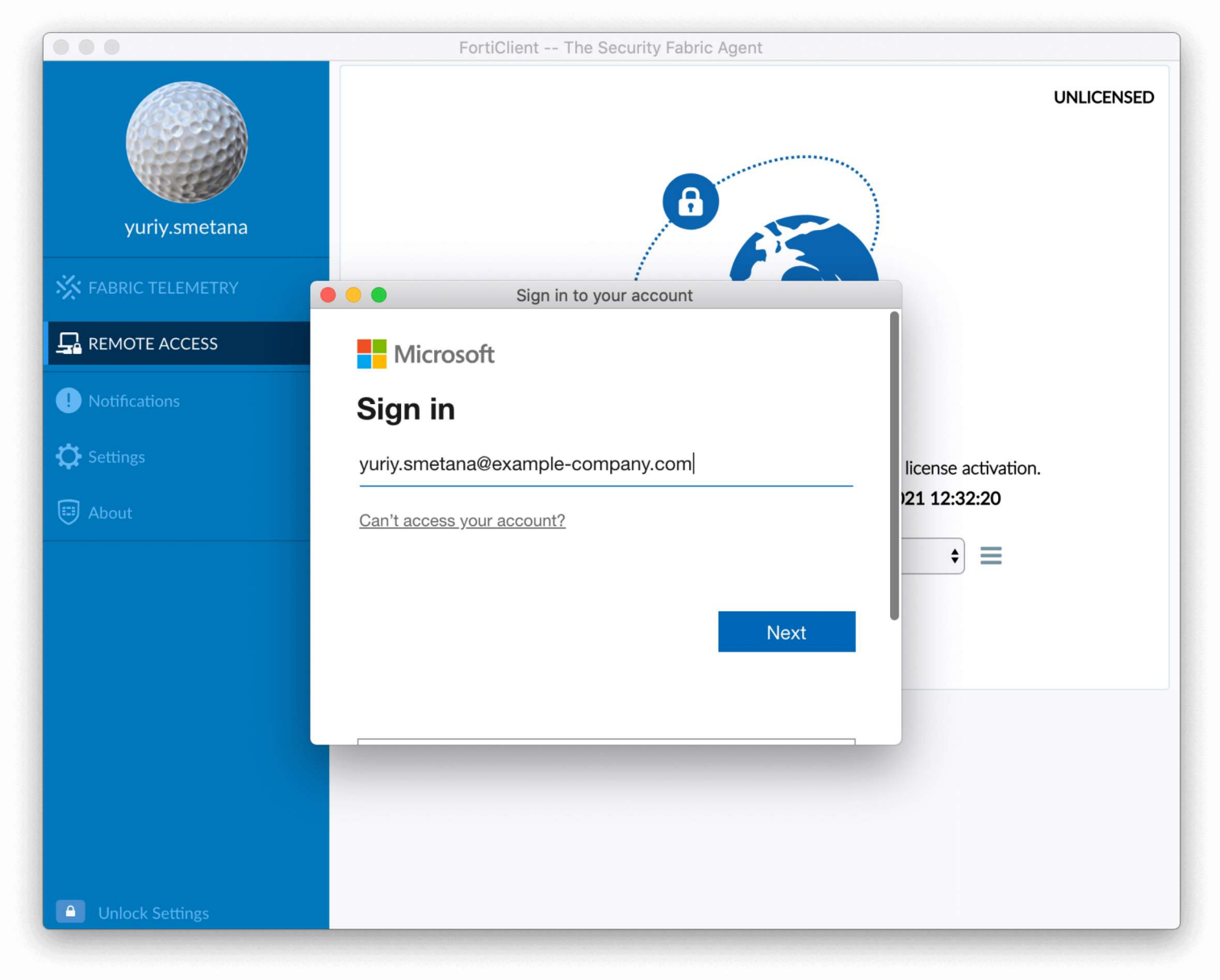
During the setup of SSL VPN connection manually enable **Single Sign On (SSO) for VPN Tunnel** and make sure that the Fortigate address and SSL VPN port number are correct:



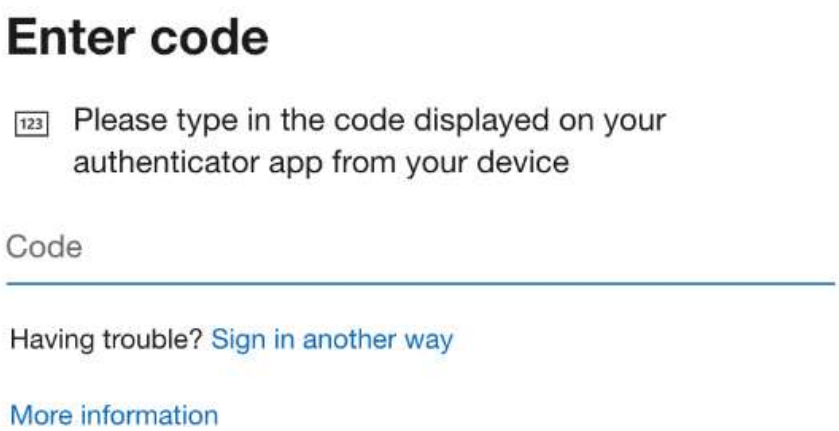
You should see **SAML login** button when SSO-enabled connection is chosen:



Try to login and provide Azure user email and password:



If everything is fine — MFA request will be displayed:



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 successfull, you can check logged in users wia **SSL-VPN** users widget of FortiOS:

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

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
...xwOlJlc3BvbnNlPg==
..
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' 'OOO-c702-427c-a550-OOO'
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: OOO-c702-427c-a550-OOO.
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 ((nu
ll)).
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, g
roup: 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 Geck
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=16147852
43,access=1614785243,saml_logout_url=no
```

We can see:

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

- 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 (`samld_send_common_reply [120]: Attr: 10, 50, 'username' 'Yuriy.Smetana@example-company.com'`)
- list of user's Azure groups ID (`samld_send_common_reply [120]: Attr: 10, 47, 'group'`)
- very important — local group match and portal assigment
  (`fsv_saml_auth_group:269 find a remote match group: MMM-a79a-40f0-a2df-MMM, portal: full-access, group: SAML_AZ_ALL.`)
- 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 фотоапарату (/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)
Ігор Меліка (http://igormelika.com.ua)