FortiGate

FortiGate Next Generation Firewall utilizes purpose-built security processors and threat intelligence security services from FortiGuard labs to deliver top-rated protection and high performance, including encrypted traffic.

cchiriches
Staff

Created on 08-16-2019 05:50 AM
Article Id 194656

Technical Tip: Configuring SAML SSO login for FortiGate administrators with Azure AD acting as SAML IdP

Description

This article describes how to configure administrator login to FortiGate using the SAML standard for authentication and authorization.
SAML has been introduced as a new administrator authentication method in FortiOS 6.2. A FortiGate can act as an Identity Provider (IdP) for other FortiGates, or as a Service Provider (SP), utilizing other IdP.
This article provides an example for basic integration with Azure Active Directory (Azure AD) acting as the IdP.

Useful links.

Fortinet Documentation.

SAML overview and configuration (in the context of authentication between FortiGates in Security Fabric) version 6.2:
https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/288215/saml

SAML overview and configuration (in the context of authentication between FortiGates in Security Fabric) version 6.2.3:
https://docs.fortinet.com/document/fortigate/6.2.3/cookbook/288215/configuring-the-security-fabric-w...

SAML overview and configuration (in the context of authentication between FortiGates in Security Fabric) version 6.4.2:
https://docs.fortinet.com/document/fortigate/6.4.2/administration-guide/288215/configuring-the-secur...

External.
Microsoft documentation for setting up SAML non-gallery application: https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/configure-single-sign-on-non-gal...

Useful browser plugins for analyzing SAML communication:

Google Chrome.
SAML Chrome Panel: https://chrome.google.com/webstore/detail/saml-chrome-panel/paijfdbeoenhembfhkhllainmocckace

SAML Message Decoder: https://chrome.google.com/webstore/detail/saml-message-decoder/mpabchoaimgbdbbjjieoaeiibojelbhm

Mozilla Firefox.
SAML-tracer: https://addons.mozilla.org/en-US/firefox/addon/saml-tracer/

SAML Message Decoder: https://addons.mozilla.org/en-US/firefox/addon/saml-message-decoder-extension/

Solution

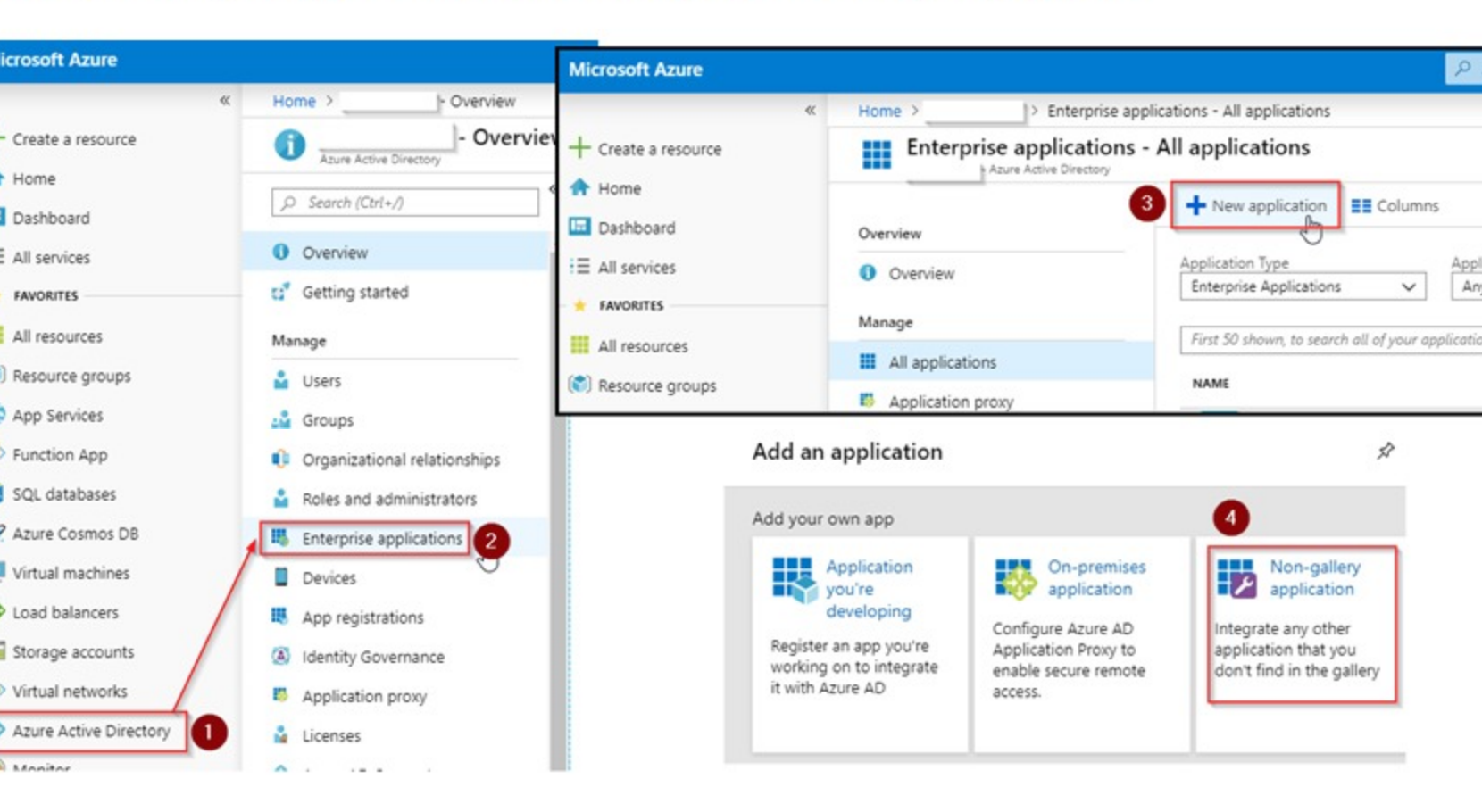
Below is a list of terms used in FortiGate GUI, and their equivalents in Azure, and the required SAML attributes.

FortiGate GUI	Azure
IdP entity ID	Azure AD Identifier
IdP single sign-on URL	Login URL
IdP single logout URL	Logout URL
SP entity ID	Identifier (Entity ID)
SP ACS (login) URL	Reply URL (Assertion Consumer Service URL)
SP SLS (logout) URL	Logout URL
SP portal URL	Sign on URL

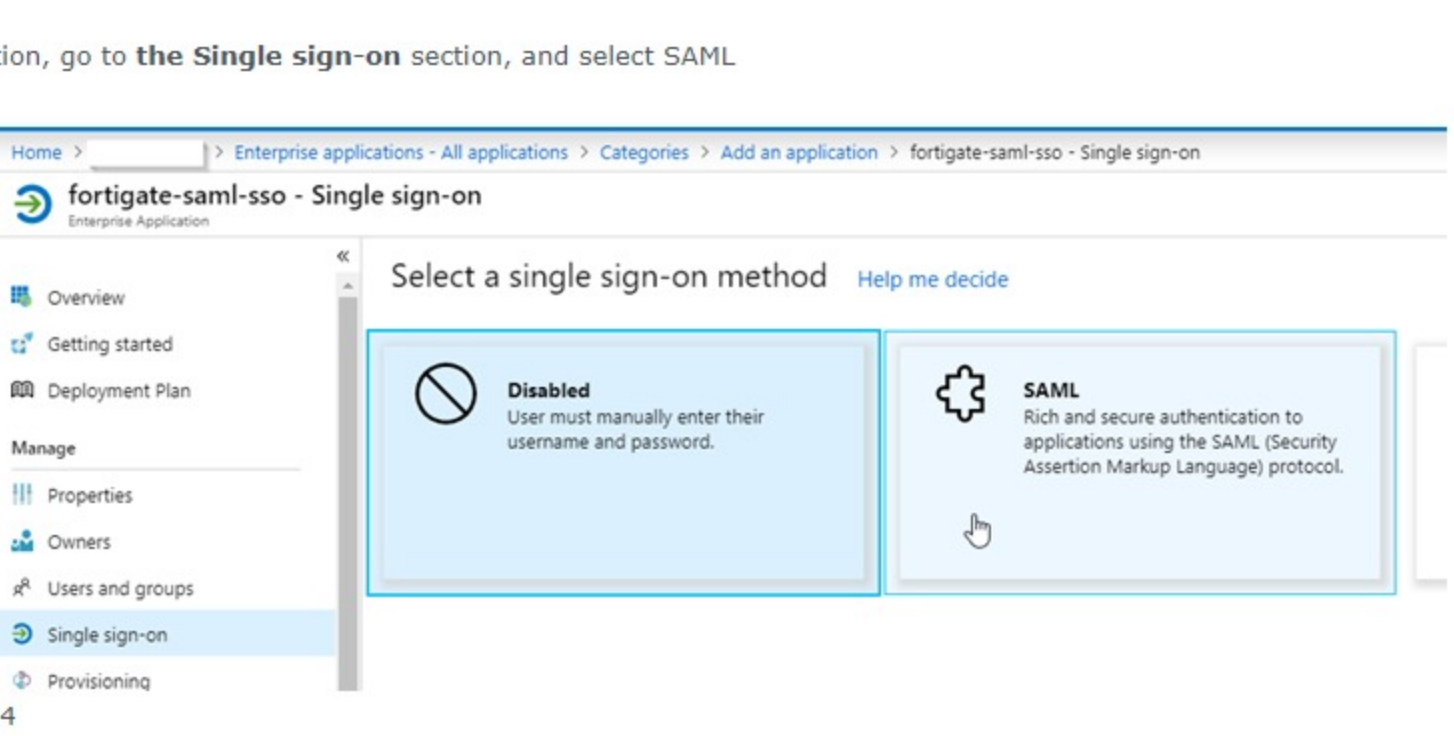
The only mandatory attribute required to be sent in the SAML response is "username", which is interpreted as the administrator's username/account name.

Step-by-step guide

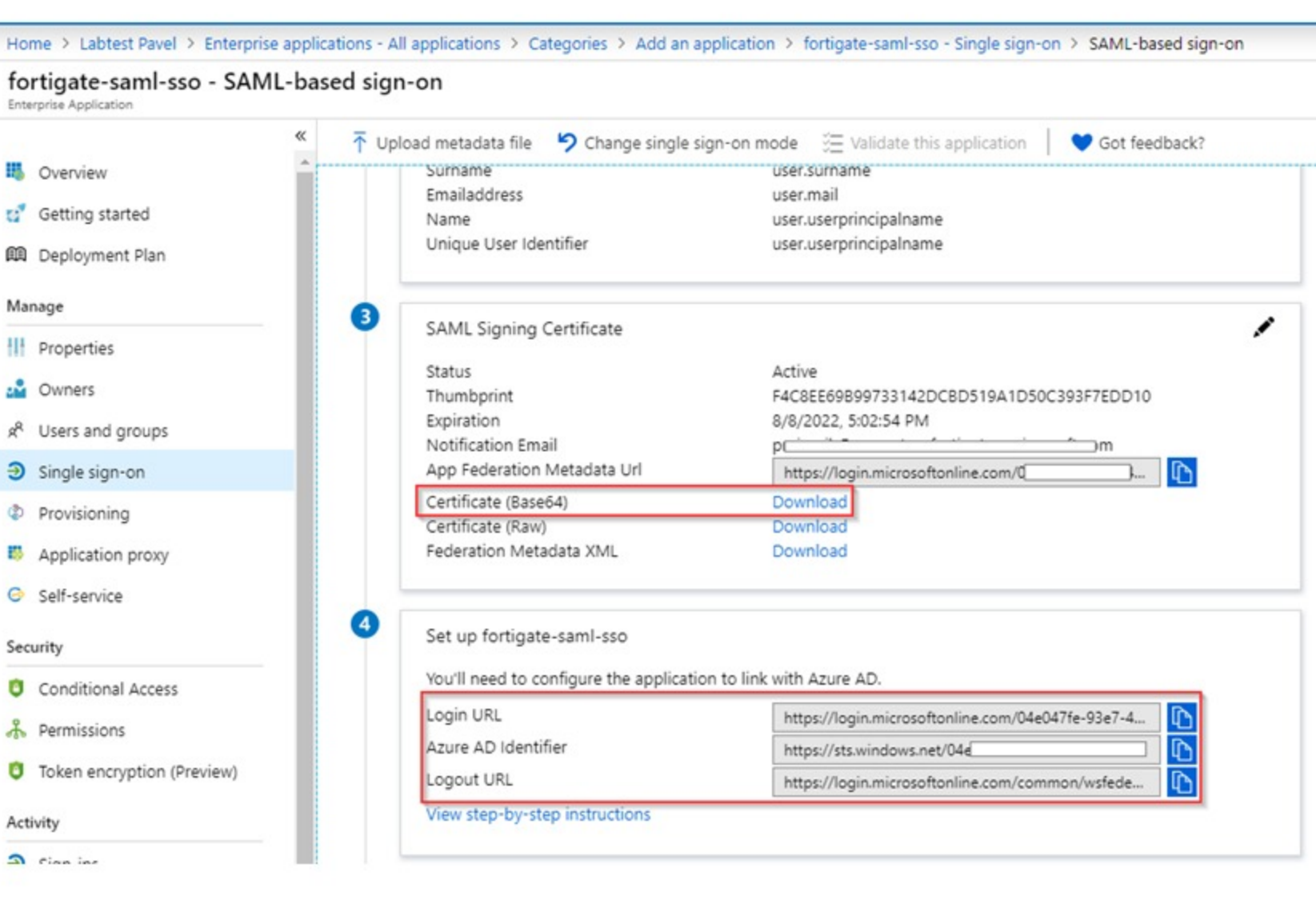
1) Create a new non-gallery Enterprise application in Azure AD
Go to Azure Active Directory -> Enterprise applications -> Create New Application -> Non-gallery application



2) In the newly created application, go to **the Single sign-on** section, and select SAML



3) Start with sections #3 and #4
In section #3, download the certificate.
In section #4 copy all three values (they will be used in step 5). Keep this page open, it is needed at later step to finish the configuration.



4) Switch to the FortiGate.
First step is to import the Azure AD SAML certificate from the previous step.

In GUI: **System -> Certificates -> Import -> Remote Certificate**
In CLI:

```
#config vpn certificate remote
```

OPTIONAL: The default name for an imported remote certificate is "REMOTE_Cert_<number>". To make it easier to distinguish from other certificates, it can be renamed in CLI.
Example: rename REMOTE_Cert_1 to Azure_SAML

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

5) FortiGate SAML configuration.

- GUI in version 6.2.
Go to **User & Device -> SAML SSO**

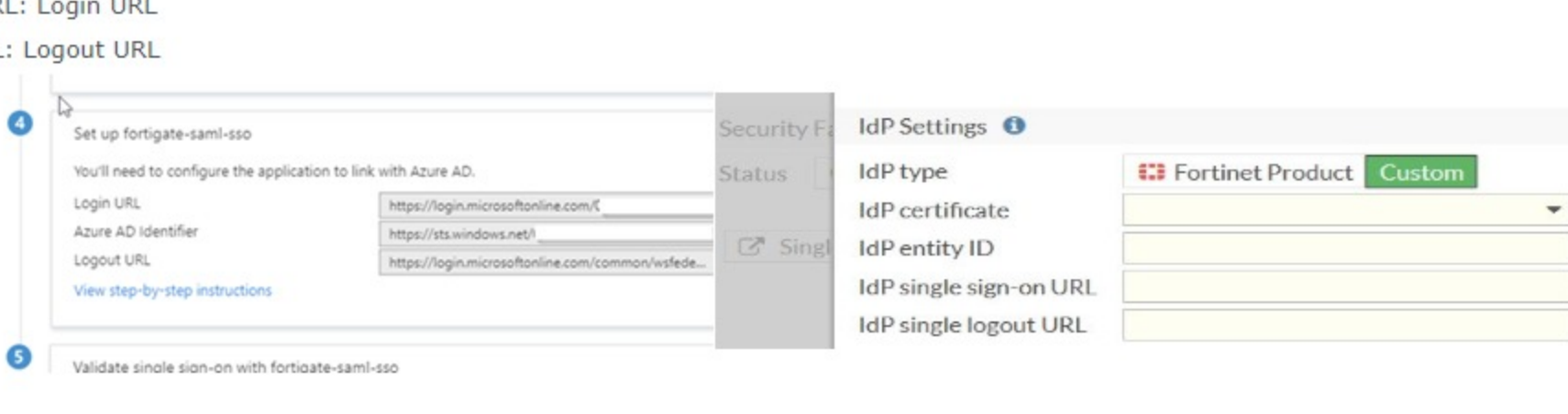
- GUI in version 6.2.3 and above.
Go to **Security Fabric -> Settings**
Enable FortiGate Telemetry, choose a Fabric name and an IP for FortiAnalyzer (can be an unused address)
Enable SAML Single Sign-On, Click on Advanced Options

- GUI in version 6.4 and above
Go to **Security Fabric -> Fabric Connectors -> Security Fabric Setup -> Single Sign-On Settings**
CLI:

```
#config system saml
```

Mode: Service Provider (SP)
SP address: This is the address that will be used to process the SAML login and as the SAML SP identity. FQDN or an IP address can be used.
Important Note: Since the redirects during SAML authentication flow will go through this address, make sure that the administrators attempting login are able to reach this address.
SP certificate: Leave disabled. Azure does not check this.
Default login page: "Normal" presents the standard login screen with an option to continue by SAML. "Single Sign-On" automatically redirects all GUI logins to SAML.
Recommended to leave at "Normal" at least for initial configuration and testing.
Default admin profile: This option controls which admin profile is assigned to newly created SAML SSO administrators.
Note: There is a special virtual profile available for selection called "admin_no_access". This profile blocks access into the FortiGate GUI until a different administrator assigns a real profile to this administrator. (useful for first-time logins, when you first want to decide what profile to assign to a new administrator before allowing them in)

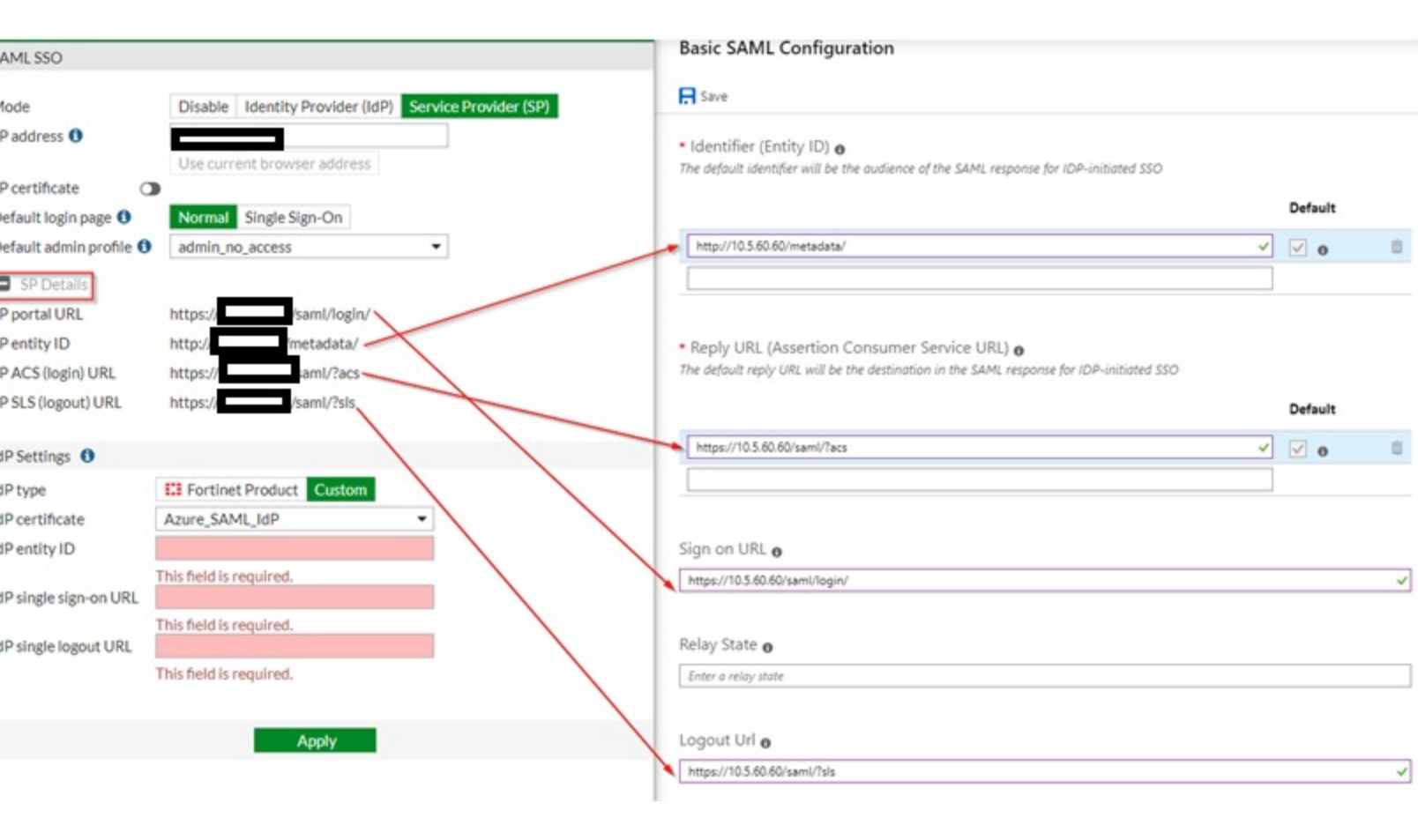
IdP settings
IdP type: Custom
IdP certificate: Select the certificate imported in step 4
The last three options should be filled with values saved in step 3.
IdP entity ID: Azure AD Identifier
IdP single sign-on URL: Login URL
Idp single logout URL: Logout URL



6) Click Apply to save the change.
Now expand the [+] SP details section to display the SP values that will be configured in Azure AD in the next step. These values contain the SP address set above, but they are only updated once click Apply to save the changes.

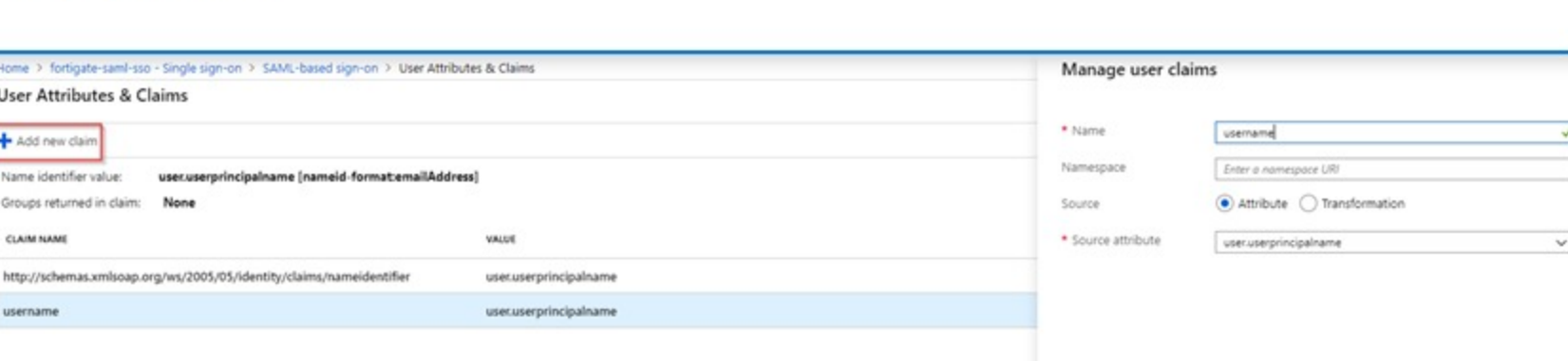
7) Go back to the SAML-based sign-on section in Azure.
Edit section #1 Basic SAML configuration.
Fill out the fields with the values from FortiGate SP in step 6 as follows:

Identifier (Entity ID): SP entity ID
Reply URL (Assertion Consumer Service URL): SP ACS (login) URL
Sign on URL: SP portal URL
Relay State: leave blank
Logout URL: SP SLS (logout) URL
Close this panel by clicking Save



8) Edit attributes sent by Azure
FortiGate expects to receive the username of the administrator in the "username" attribute. Azure AD does not send an attribute with this name by default.

Still in the Single Sign-on with SAML menu in Azure, edit the section #2 (User Attributes & Claims) and add a new claim:
Name: username
Namespace: leave blank
Source: Attribute
Source attribute: user.userprincipalname (The value of this attribute has to match the username the administrator will be using to log in)
Click the Save button to add this new claim.
The other unused claims can be deleted.
Select the close button in top right to return.



9) Access authorization
There are several options which control access to a SAML SP (FortiGate) on Azure side.
Switch to the Properties section of the SAML application in Azure.
"Enabled for users so sign-in": When set to "No", access is completely disabled for everyone.
"User assignment required": When set to "Yes", only users/groups configured in the section "Users and groups" are allowed access. When set to "No", any valid user from this directory is allowed to use this SAML SP and authenticate to FortiGate admin GUI.

10) Assigning admin profiles to SAML SSO administrators

Admin accounts can be manually created in GUI:
Go to System -> Administrators -> Create new -> SSO Admin
It's possible to set the username, admin profile to be assigned, and allowed VDOMs, if VDOMs are enabled on the unit.

CLI configuration example:

```
#config system sso-admin
edit "username@domain.com"
set accprofile "<admin_profile_name>"
set vdom "<VDOM-name>"
end
```

If a matching administrator account does not exist on the FortiGate yet, it will be automatically created, and assigned the default admin access profile as set in the SAML SSO configuration above (step 5).

Troubleshooting.

Useful debug commands
httpsd (general admin GUI debugging), samld (SAML-specific debugs)
Usage:

```
#diagnose debug application httpsd -1
#diagnose debug application samld -1
#optionally# diagnose debug console timestamp enable
#diagnose debug enable
```

In case of SSLVPN above debug would include the application SSL VPN.

Run tests now. When done, stop debugs and reset them with:

```
#diagnose debug disable
#diagnose debug reset
```

The SAML request message sent from the FortiGate SP to the Azure IdP is visible in the "**** Auth Req URL ****" section:

```
2019-08-14 10:04:49 [httpsd 8170 - 1565769889     info] ap_invoke_handler[569] -- new request (handler='saml-sp-login-handler', uri='/saml/login/', method='GET')
2019-08-14 10:04:49 [httpsd 8170 - 1565769889     info] ap_invoke_handler[573] -- User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
2019-08-14 10:04:49 [httpsd 8170 - 1565769889     info] ap_invoke_handler[576] -- Source: 10.5.63.254:58486 Destination: 10.5.60.60:443
__update_sp_sig_opt [251]: SP no sig is required.
__samld_sp_create_auth_req [381]:
**** Auth Req URL ****
https://login.microsoftonline.com/<tenant-ID>/saml2?SAMLRequest=<-###SAML-REQUEST-HERE-###>&RelayState=%2Fng
***********************
```

The SAMLRequest value contains the URL-encoded version of the request. If it is decodes, it will give the base64 encoded version of the request message, which can be further decoded and inflated to show the actual XML content of the request message.

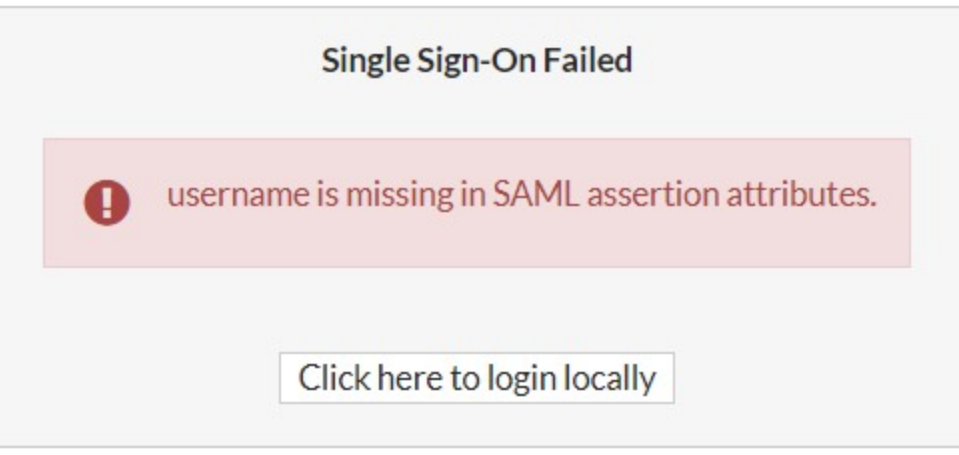
Similarly, the IdP response forwarded from the IdP back to the FortiGate SP is visible in the following section:

```
2019-08-14 10:05:06 [httpsd 8170 - 1565769906     info] ap_invoke_handler[569] -- new request (handler='saml-sp-handler', uri='/saml/', method='POST')
2019-08-14 10:05:06 [httpsd 8170 - 1565769906     info] ap_invoke_handler[573] -- User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
2019-08-14 10:05:06 [httpsd 8170 - 1565769906     info] ap_invoke_handler[576] -- Source: 10.5.63.254:58504 Destination: 10.5.60.60:443
__samld_sp_login_resp [723]:
Message Body
<###-base64-encoded-message-###>
```

This can also be base64-decoded and inflated to get the XML content of the SAML response.

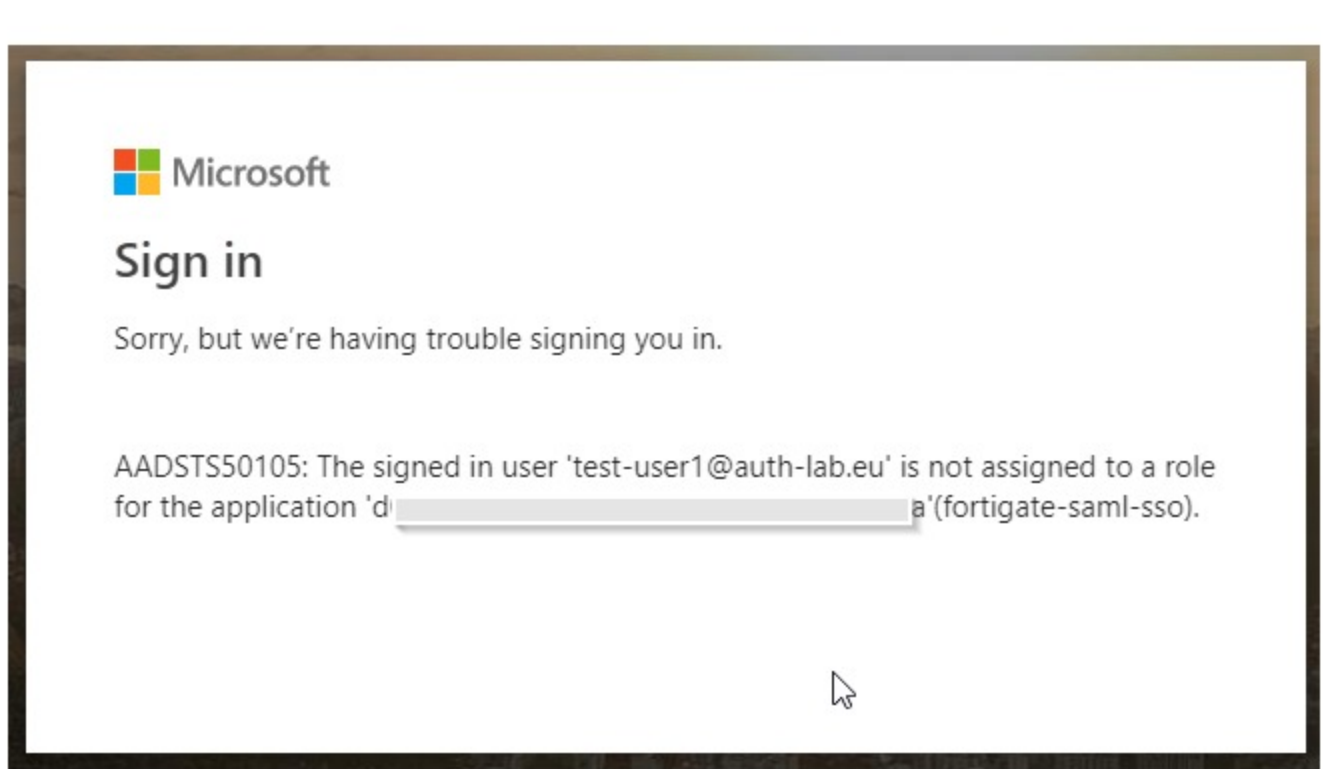
Error examples and possible remedies (non-exhaustive)

ERROR: "username is missing in SAML assertion attributes."



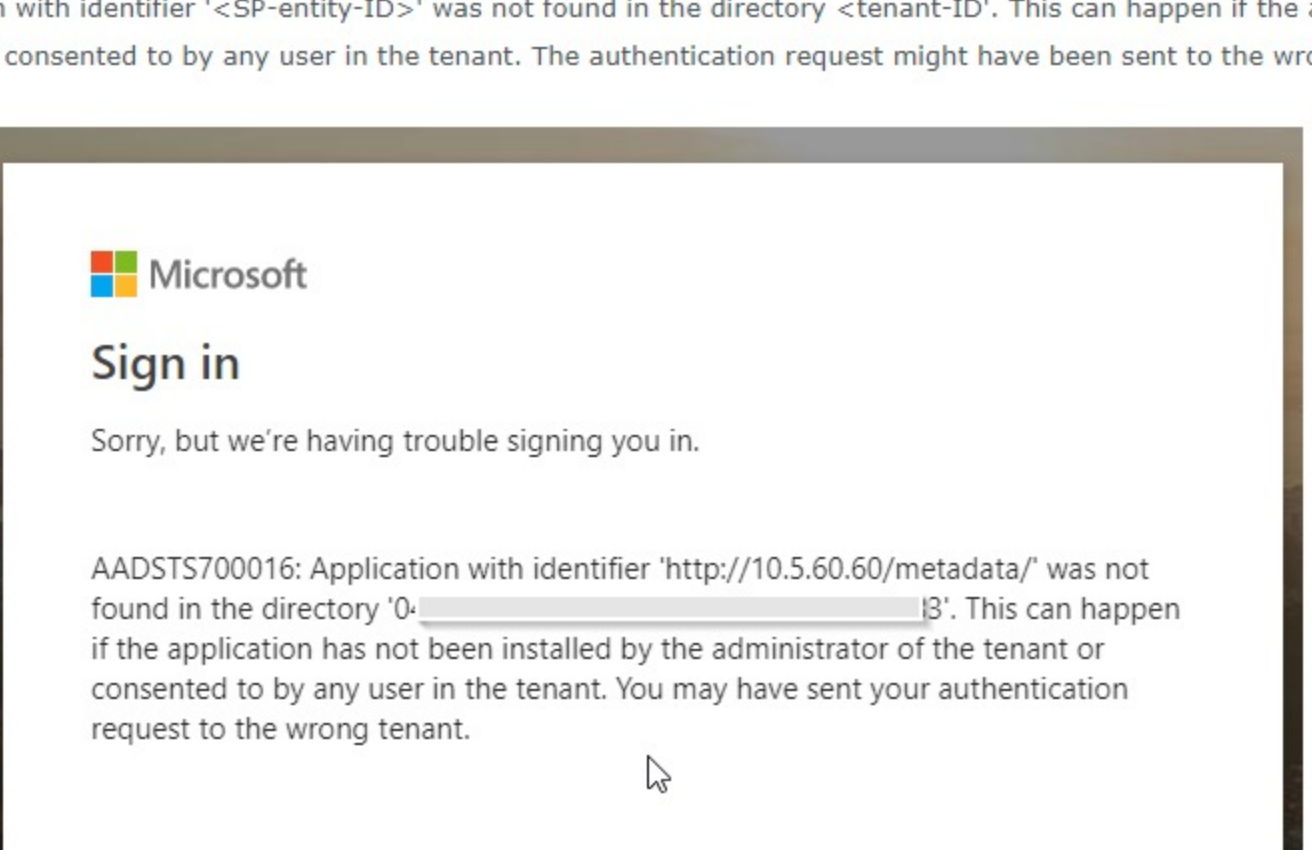
Fix: SAML assertion attributes are misconfigured and do not contain the "username" attribute/claim.
Refer to step 8 on how to add this in Azure AD.

ERROR: "AADSTS50105: The signed in user '<username>' is not assigned to a role for the application <application-ID>'(fortigate-saml-sso)."



Fix: The user was not given access to the FortiGate SAML SP in Azure.
Refer to step 9 to properly set up authorization for the user in Azure.

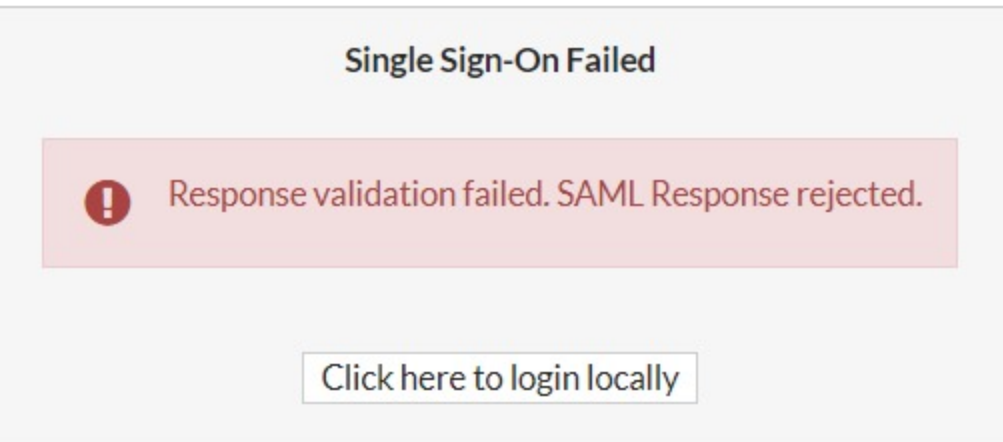
ERROR: "AADSTS700016: Application with identifier '<SP-entity-ID>' was not found in the directory <tenant-ID'. This can happen if the application has not been installed by the administrator of the tenant or consented to by any user in the tenant. The authentication request might have been sent to the wrong tenant."



Fix: Verify what is the currently configured SP entity ID on the FortiGate, and then make sure the exact same value is set in Azure (step 7).

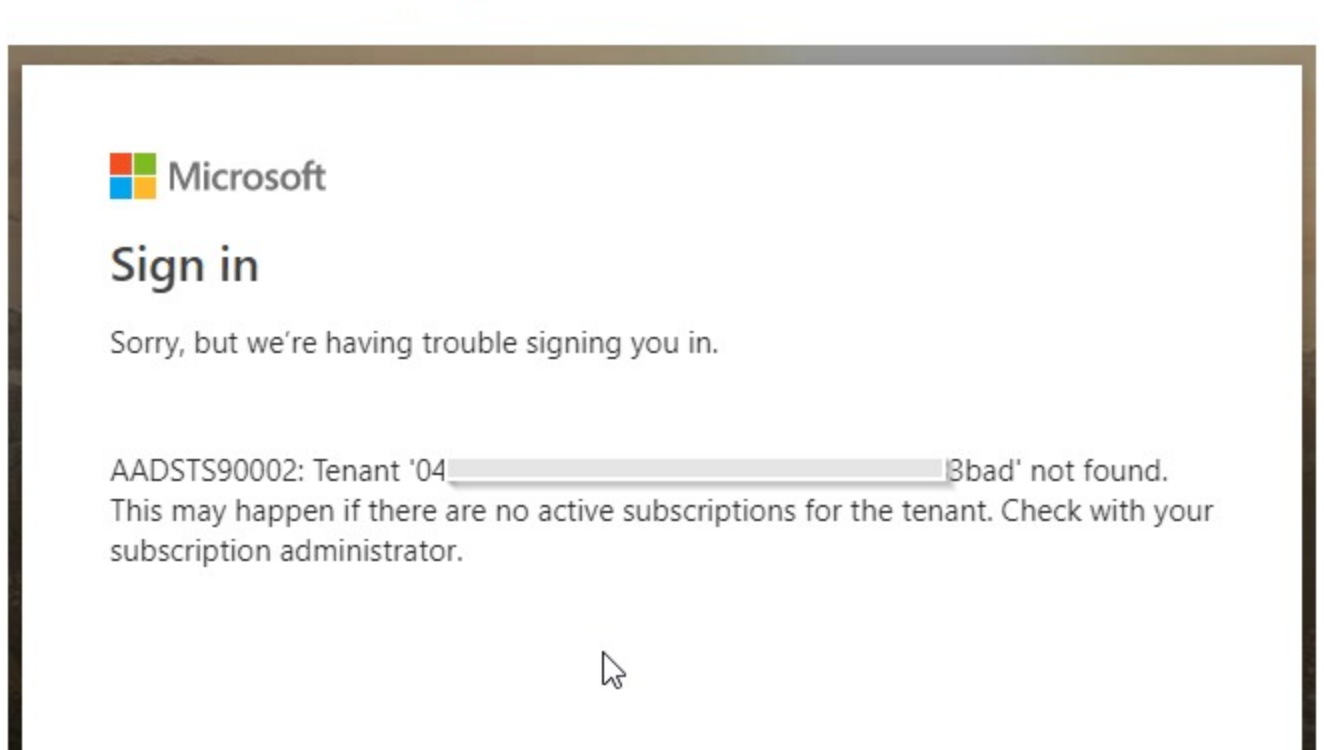
Error: After authentication succeeds with Azure IdP, the FortiGate page does not load, or "Error" is shown by FortiGate.
Fix: This may be a misconfigured Reply URL (Assertion Consumer Service URL) in Azure. Make sure this value matches the SP ACS (login) URL from FortiGate (step 7).

ERROR: "Response validation failed. SAML Response rejected."



Fix 1: This may be caused by selecting an incorrect IdP certificate in FortiGate configuration. Make sure it matches the certificate used by Azure (teps 3,4,7).
Fix 2: This may also be due to an incorrect IdP entity ID in FortiGate configuration. Make sure this matches the Azure AD Identifier (steps 3,5).

ERROR: "AADSTS90002: Tenant '<tenant-ID>' not found. This may happen if there are no active subscriptions for the tenant. Check with subscription administrator."



Fix: The tenant ID included in the IdP single sign-on URL configured on FortiGate is not correct. Make sure this value matches the Login URL from Azure (steps 3,5).

ERROR: Unable to log into FortiGate GUI because SAML SSO is the default login, and it is not functional.

Fix: If SAML login is the default method and fails before a user is redirected back to the FortiGate, an administrator may not be given a chance to perform a standard local logon.
To get around this, log in by manually opening the SP ACS (login) URL (https://<fortigate>/saml/?acs). Ignore the error displayed and proceed with "Click here to login locally". Afterward the default login page can be switched to "Normal" in GUI.

It's possible to make this change directly from SSH:

```
#config sytem saml
set default-login-page normal
end
```

From version 6.2.2 and above, refer to link in description.

FortiGate V6.2 FortiGate V6.4

137014 | 5 | Share | Submit Article Idea

Contributors

cchiriches