

Merhaba Microsoft Azure authentication ile Fortigate SSL vpn bağlantısı kurmak için öncelikle bir alan adınızın olması ve bu alan adınızda vpn bağlantısında kullanılan wan bacağının ip adresini gösteren bir host A kaydı olması gerekiyor.

Ayrıca bu alan adınız için ücretli yada ücretsiz (lets encrypt) ssl sertifikanızın olması gerekli. Self sign sertifika maalesef azure tarafından güvenilmediği için olmuyor. Ben fortigate içerisinden oluşturulup kullanılabilen lets-encrypt ile ilerledim.

	Name	Subject	Comments	
Network	Fortinet_Factory	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN ...	This certificate is embedded in the hardware at the factory and is unique...	Fortinet
Policy & Objects	Fortinet_Factory_Backup	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN ...	This certificate is embedded in the hardware at the factory and is unique...	Fortinet
Security Profiles	Fortinet_GUI_Server	C = US, ST = California, L = Sunnyvale, O = Fortinet Ltd., OU = FortiGate, ...	This is the default CA certificate the SSL Inspection will use when genera...	Fortinet
VPN	Fortinet_SSL	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN ...	This certificate is embedded in the hardware at the factory and is unique...	Fortinet
User & Authentication	Fortinet_SSL_DSA1024	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN ...	This certificate is embedded in the hardware at the factory and is unique...	Fortinet
WiFi & Switch Controller	Fortinet_SSL_DSA2048	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN ...	This certificate is embedded in the hardware at the factory and is unique...	Fortinet
System	Fortinet_SSL_ECDSA256	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN ...	This certificate is embedded in the hardware at the factory and is unique...	Fortinet
Administrators	Fortinet_SSL_ECDSA384	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN ...	This certificate is embedded in the hardware at the factory and is unique...	Fortinet
Admin Profiles	Fortinet_SSL_ECDSA521	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN ...	This certificate is embedded in the hardware at the factory and is unique...	Fortinet
Fabric Management	Fortinet_SSL_ED448	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN ...	This certificate is embedded in the hardware at the factory and is unique...	Fortinet
Settings	Fortinet_SSL_ED25519	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN ...	This certificate is embedded in the hardware at the factory and is unique...	Fortinet
HA	Fortinet_SSL_RSA1024	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN ...	This certificate is embedded in the hardware at the factory and is unique...	Fortinet
SNMP	Fortinet_SSL_RSA2048	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN ...	This certificate is embedded in the hardware at the factory and is unique...	Fortinet
Replacement Messages	Fortinet_SSL_RSA4096	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN ...	This certificate is embedded in the hardware at the factory and is unique...	Fortinet
FortiGuard	Fortinet_Wifi	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN ...	This certificate is embedded in the hardware at the factory and is unique...	Fortinet
Feature Visibility	azurevpn	CN = vpn., r.com	Renewed with ACME on Tue Jan 3 14:22:36 2023 (UTC)	Let's Encrypt
Certificates	Remote CA Certificate			
Security Fabric	ACME_CA_Cert_1	C = US, O = Let's Encrypt, CN = R3		Internet Security
Log & Report	Fortinet_CA	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Aut...		Fortinet
	Fortinet_CA_Backup	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Aut...		Fortinet
	Fortinet_Sub_CA	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Aut...		Fortinet
	Fortinet_Wifi_CA	C = US, O = DigiCert Inc, CN = DigiCert TLS RSA SHA256 2020 CA1		DigiCert Inc

İlk önce Azure tarafında yapmamız gereken işleri halledelim.

Portal.azure.com adresine hesabınız ile login olduktan sonra arama kısmına **enterprise** yazarak **Enterprise applications** u bulup açıyoruz.

The screenshot shows the Microsoft Azure portal search results for the term "enterprise". The search bar at the top contains the word "enterprise". Below the search bar, there are tabs for "All", "Services (3)", "Resources", "Resource Groups", "Marketplace (20)", and "Documentation (29)". The "Services (3)" tab is selected, and it shows a list of services. The first service listed is "Enterprise applications", which is highlighted with a red arrow. Below the "Enterprise applications" service, there are sections for "Marketplace" and "Documentation". The "Marketplace" section lists various products like "VIDIZMO EnterpriseTube Premium - PAYG", "HPE OneView for Azure Log Analytics (v1.4.0)", "HPE StoreOnce VSA 4.3.2", and "VIDIZMO EnterpriseTube Standard - PAYG". The "Documentation" section lists various articles like "What is Windows 365 Enterprise? | Microsoft Learn", "Enterprise app management - Windows Client Management", "Getting Started with Windows IoT Enterprise | Microsoft Learn", and "Enterprise-grade edge in Azure Static Web Apps | Microsoft Learn". At the bottom of the search results, there is a section for "Azure Active Directory" which lists "EnterpriseAgentPlatform", "Office 365 Enterprise Insights", and "Office Enterprise Protection Service".

Ardından New applications a tıklıyoruz.

Microsoft Azure Search resources, services, and docs (G+/J)

Home > Enterprise applications

## Enterprise applications | All applications

- Azure Active Directory

Overview

View, filter, and search applications in your organization that are set up to use your Azure AD tenant as their Identity Provider.

The list of applications that are maintained by your organization are in [application registrations](#).

Search by application name or object ID

Application type == Enterprise Applications

Application ID starts with

Add filters

19 applications found

Browse Azure AD Gallery kısmında fortigate için arama yapıyoruz ve Fortigate SSL VPN seçip sağda açılan pencereden Create tıklayarak uygulamamızı oluşturuyoruz.

Microsoft Azure Search resources, services, and docs (G+/J)

Home > Enterprise applications | All applications

## Browse Azure AD Gallery

Create your own application

Got feedback?

The Azure AD App Gallery is a catalog of thousands of apps that make it easy to deploy and configure single sign-on (SSO) and automation templates to connect your users more securely to their apps. Browse or create your own application here. If you are wanting to publish and use, you can file a request using the process described in [this article](#).

fortigate

Federated SSO

Provisioning

Showing 8 of 8 results

**FortiGate SSL VPN**  
Fortinet

**FortiSASE**  
Fortinet Inc

**LogicGate**  
LogicGate

**FortiWeb Web Application Firewall**  
Fortinet

### FortiGate SSL VPN

Got feedback?

Logo

Name \*

FortiGate SSL VPN

Publisher

Fortinet

Provisioning

Automatic provisioning is not supported

Single Sign-On Mode

SAML-based Sign-on

Linked Sign-on

URL

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

[Read our step-by-step FortiGate SSL VPN integration tutorial](#)

The application uses Azure AD as the SAML IdP to authenticate users to the FortiGate SSL VPN via a web browser. It also authenticates users via the FortiClient application in SSL VPN tunnel mode.

Create

Set up single sign on tıklıyoruz.

Microsoft Azure Search resources, services, and docs (G+)

Home > Enterprise applications | All applications > Browse Azure AD Gallery >

## FortiGate SSL VPN | Overview

Enterprise Application

- Overview
- Deployment Plan
- Diagnose and solve problems
- Manage
  - Properties
  - Owners
  - Roles and administrators
  - Users and groups
  - Single sign-on
  - Provisioning
  - Self-service
  - Custom security attributes (preview)
- Security
  - Conditional Access
  - Permissions
  - Token encryption
- Activity
  - Sign-in logs
  - Usage & insights
  - Audit logs
  - Provisioning logs
  - Access reviews
- Troubleshooting & Support

### Properties

**Name** FortiGate SSL VPN

**Application ID** 68dcafe2-ec7a-414a-9f6e-1...

**Object ID** fe641867-5cef-4b94-82cd-e...

### 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](#)
- 3. Provision User Accounts**  
You'll need to create user accounts in the application  
[Learn more](#)
- 4. Conditional Access**  
Secure access to this application with a customizable access policy.  
[Create a policy](#)
- 5. Self service**  
Enable users to request access to the application using their Azure AD credentials  
[Get started](#)

Ardından SAML tıklıyoruz.

Microsoft Azure Search resources, services, and docs (G+)

Home > Enterprise applications | All applications > Browse Azure AD Gallery > FortiGate SSL VPN

## FortiGate SSL VPN | Single sign-on

Enterprise Application

- Overview
- Deployment Plan
- Diagnose and solve problems
- Manage
  - Properties
  - Owners
  - Roles and administrators
  - Users and groups
  - Single sign-on
  - Provisioning
  - Self-service
  - Custom security attributes (preview)

Single sign-on (SSO) adds security and convenience when users sign on to applications in Azure Active Directory by enabling a user in your organization to sign in to every application they use with only one account. Once the user logs into an application, that credential is used for all the other applications they need access to. [Learn more](#).

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

**Disabled**  
Single sign-on is not enabled. The user won't be able to launch the app from My Apps.

**SAML**  
Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

**Linked**  
Link to an application in My Apps and/or Office 365 application launcher.

Bu ekranda işaretli 4 alana pattern olarak belirtildiği gibi dolduracağız. **FORTIGATE-FQDN.com** olarak belirtilen yer, giriş kısmında da açıkladığım gibi fortigate wan bacağını işaret eden alan adınız olacak. Örneğin **azurevpn.gokhanunal.com**. Alan adınızın dns yönetiminde azurevpn host A kaydı için dış ip adresimizi yazıyoruz. Ayrıca eğer 443 portundan farklı bir vpn portu kullanıyorsak onu yazmalıyız. Örnekler aşağıdaki gibi.

**Identifier** <https://azurevpn.gokhanunal.com:19443/remote/saml/metadata>

**Reply URL** <https://azurevpn.gokhanunal.com:19443/remote/saml/login>

**Sign on URL** <https://azurevpn.gokhanunal.com:19443/remote/saml/login>

**Log out URL** <https://azurevpn.gokhanunal.com:19443/remote/saml/logout>

**Bu linkleri daha sonra fortigate cli ile kullanacağız.**

**Microsoft Azure** Search resources, services, and docs (G+)

Home > Enterprise applications | All applications > Browse Azure AD Gallery > FortiGate SSL VPN >

**FortiGate SSL VPN | SAML-based Sign-on** Enterprise Application

Overview Deployment Plan Diagnose and solve problems Manage Properties Owners Roles and administrators Users and groups Single sign-on Provisioning Self-service Custom security attributes (preview) Security Conditional Access Permissions Token encryption Activity Sign-in logs Usage & insights Audit logs Provisioning logs Access reviews Troubleshooting & Support

Set up Single Sign-On with SAML

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

Read the [configuration guide](#) for help integrating FortiGate SSL VPN.

1 Basic SAML Configuration [Edit](#)

Identifier (Entity ID) \* [Add identifier](#)  
The unique ID that identifies your application to Azure Active Directory. This value must be unique across all applications in your Azure Active Directory tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.  
Patterns: [https://<FORTIGATE-FQDN>/remote/saml/metadata](#)

Reply URL (Assertion Consumer Service URL) \* [Add reply URL](#)  
The reply URL is where the application expects to receive the authentication token. This is also referred to as the 'Assertion Consumer Service' (ACS) in SAML.  
Patterns: [https://<FORTIGATE-FQDN>/remote/saml/login](#)

Sign on URL \*  
Sign on URL is used if you would like to perform service provider-initiated single sign-on. This value is the sign-in page URL for your application. This field is unnecessary if you want to perform identity provider-initiated single sign-on.  
Enter a sign on URL  
Please enter a valid URL starting with "https://". If your URL has query parameters, ensure that there is a slash preceding the question mark (i.e. /?).  
This field is required  
Patterns: [https://<FORTIGATE-FQDN>/remote/saml/login](#)

Relay State (Optional) [Add relay state](#)  
The Relay State instructs the application where to redirect users after authentication is completed, and the value is typically a URL or URL path that takes users to a specific location within the application.  
Enter a relay state

Logout Url (Optional)  
This URL is used to send the SAML logout response back to the application.  
Enter a logout URL

2 Attributes & Claims [Edit](#)

Fill out required fields in Step 1

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

3 SAML Certificates [Edit](#)

Token signing certificate

Status	Active
Thumbprint	F8A23743D9CD4786D1A1FC66799A17A9B1D919EC
Expiration	10/2/2027, 9:06:49 PM
Notification Email	
App Federation Metadata Url	<a href="https://login.microsoftonline.com/cb243bf0-2036-...">https://login.microsoftonline.com/cb243bf0-2036-...</a>
Certificate (Base64)	<a href="#">Download</a>
Certificate (Raw)	<a href="#">Download</a>

İlgili alanları doldurduktan sonra **Save** ile kaydediyoruz.

**Microsoft Azure** Search resources, services, and docs (G+)

Home > Enterprise applications | All applications > Browse Azure AD Gallery > FortiGate SSL VPN >

**FortiGate SSL VPN | SAML-based Sign-on** Enterprise Application

Overview Deployment Plan Diagnose and solve problems Manage Properties Owners Roles and administrators Users and groups Single sign-on Provisioning Self-service Custom security attributes (preview) Security Conditional Access Permissions Token encryption Activity Sign-in logs Usage & insights Audit logs Provisioning logs Access reviews Troubleshooting & Support

Set up Single Sign-On with SAML

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

Read the [configuration guide](#) for help integrating FortiGate SSL VPN.

1 Basic SAML Configuration [Edit](#)

Identifier (Entity ID) \* [Add identifier](#)  
The unique ID that identifies your application to Azure Active Directory. This value must be unique across all applications in your Azure Active Directory tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.  
Patterns: [https://<FORTIGATE-FQDN>/remote/saml/metadata](#)

Reply URL (Assertion Consumer Service URL) \* [Add reply URL](#)  
The reply URL is where the application expects to receive the authentication token. This is also referred to as the 'Assertion Consumer Service' (ACS) in SAML.  
Patterns: [https://<FORTIGATE-FQDN>/remote/saml/login](#)

Sign on URL \*  
Sign on URL is used if you would like to perform service provider-initiated single sign-on. This value is the sign-in page URL for your application. This field is unnecessary if you want to perform identity provider-initiated single sign-on.  
Enter a sign on URL  
Please enter a valid URL starting with "https://". If your URL has query parameters, ensure that there is a slash preceding the question mark (i.e. /?).  
This field is required  
Patterns: [https://<FORTIGATE-FQDN>/remote/saml/login](#)

Relay State (Optional) [Add relay state](#)  
The Relay State instructs the application where to redirect users after authentication is completed, and the value is typically a URL or URL path that takes users to a specific location within the application.  
Enter a relay state

Logout Url (Optional)  
This URL is used to send the SAML logout response back to the application.  
Enter a logout URL

2 Attributes & Claims [Edit](#)

Fill out required fields in Step 1

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

3 SAML Certificates [Edit](#)

Token signing certificate

Status	Active
Thumbprint	F8A23743D9CD4786D1A1FC66799A17A9B1D919EC
Expiration	10/2/2027, 9:06:49 PM
Notification Email	
App Federation Metadata Url	<a href="https://login.microsoftonline.com/cb243bf0-2036-...">https://login.microsoftonline.com/cb243bf0-2036-...</a>
Certificate (Base64)	<a href="#">Download</a>
Certificate (Raw)	<a href="#">Download</a>

1 nolu kısmı doldurduk. İşaretli alan son şekli. Şimdi 2 nolu kısımda **Edit** e tıklıyoruz.

Microsoft Azure

Home > Enterprise applications | All applications > Browse Azure AD Gallery > FortiGate SSL VPN

### FortiGate SSL VPN | SAML-based Sign-on

Enterprise Application

Overview  
Deployment Plan  
Diagnose and solve problems

Manage

- Properties
- Owners
- Roles and administrators
- Users and groups
- Single sign-on**
- Provisioning
- Self-service
- Custom security attributes (preview)

Security

- Conditional Access
- Permissions
- Token encryption

Activity

- Sign-in logs
- Usage & insights
- Audit logs
- Provisioning logs
- Access reviews

Troubleshooting & Support

Upload metadata file | Change single sign-on mode | Test this application | Got feedback?

#### Set up Single Sign-On with SAML

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

Read the [configuration guide](#) for help integrating FortiGate SSL VPN.

- Basic SAML Configuration** [Edit](#)

Identifier (Entity ID)	https://ata	19443/remote/saml/metadata
Reply URL (Assertion Consumer Service URL)	https://	19443/remote/saml/login
Sign on URL	https://	19443/remote/saml/login
Relay State (Optional)	Optional	
Logout Url (Optional)	https://	19443/remote/saml/logout
- Attributes & Claims** [Edit](#)

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname
Group	user.groups
- SAML Certificates** [Edit](#)

Token signing certificate	Active
Status	6077670FF2957D5C69F105FBC947614E1F7B9F8F
Thumbprint	1/3/2026, 3:14:23 PM
Expiration	
Notification Email	
App Federation Metadata Url	<a href="https://login.microsoftonline.com/cb243bf0-2036-...">https://login.microsoftonline.com/cb243bf0-2036-...</a>
Certificate (Base64)	<a href="#">Download</a>
Certificate (Raw)	<a href="#">Download</a>

Manage claim penceresinde **Name** olarak **username** yazıyoruz, **Source attribute** olarak **user.userprincipalname** seçiyoruz.

**Save** ile kaydediyoruz.

Microsoft Azure

Home > Enterprise applications | All applications > FortiGate SSL VPN | SAML-based Sign-on > SAML-based Sign-on > Attributes & Claims

### Manage claim

Save | Discard changes | Got feedback?

Name \*

Namespace

Choose name format (Preview)

Source \* ☒ Attribute ☐ Transformation

Source attribute \*

Claim conditions

Advanced SAML claims options

Username claim oluřtu. Sonrasında **Add a group claim** e tıklıyoruz.

Microsoft Azure

Search resources, services, and docs (G+/)

Home > Enterprise applications | All applications > FortiGate SSL VPN | SAML-based Sign-on > SAML-based Sign-on >

## Attributes & Claims

+ Add new claim + Add a group claim Columns Got feedback?

Required claim

Claim name	Type	Value
Unique User Identifier (Name ID)	SAML	user.userprincipalname [...]

Additional claims

Claim name	Type	Value
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailadd...	SAML	user.mail [...]
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	SAML	user.givenname [...]
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SAML	user.userprincipalname [...]
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	SAML	user.surname [...]
username	SAML	user.userprincipalname [...]

Advanced settings (Preview)

**Group claims** penceresinde **All groups** seçip, **Advanced options** u genişletiyoruz. **Customize the name of group claim** işaretleyip **Name** alanına **group** yazıyoruz ve **Save** ile kaydediyoruz.

Microsoft Azure

Search resources, services, and docs (G+/)

Home > Enterprise applications | All applications > FortiGate SSL VPN | SAML-based Sign-on > SAML-based Sign-on >

## Attributes & Claims

+ Add new claim + Add a group claim Columns Got feedback?

Required claim

Claim name	Type	Value
Unique User Identifier (Name ID)	SAML	user.userprincipalname [...]

Additional claims

Claim name	Type	Value
http://schemas.microsoft.com/ws/2008/06/identity/claims/groups	SAML	user.groups [SecurityGro...]
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailadd...	SAML	user.mail [...]
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	SAML	user.givenname [...]
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SAML	user.userprincipalname [...]
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	SAML	user.surname [...]
username	SAML	user.userprincipalname [...]

Advanced settings (Preview)

**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?

☒ All groups

☐ None

☐ Security groups

☐ Directory roles

☐ Groups assigned to the application

Source attribute \*

Group ID

☐ Emit group name for cloud-only groups (Preview)

Advanced options

☐ Filter groups

Attribute to match

Match with

String

☒ Customize the name of the group claim

Name (required)

group

Namespace (optional)

Save

Attributes & Claim son durum ařağıdaki gibi olacak.

Microsoft Azure

Search resources, services, and docs (G+)

[Home](#) > [Enterprise applications | All applications](#) > [FortiGate SSL VPN | SAML-based Sign-on](#) > [SAML-based Sign-on](#) >

## Attributes & Claims

[+ Add new claim](#) [+ Add a group claim](#) [Columns](#) [Got feedback?](#)

Required claim

Claim name	Type	Value
Unique User Identifier (Name ID)	SAML	user.userprincipalname [...]

Additional claims

Claim name	Type	Value
group	SAML	user.groups
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailadd...	SAML	user.mail
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	SAML	user.givenname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SAML	user.userprincipalname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	SAML	user.surname
username	SAML	user.userprincipalname

Advanced settings (Preview)

Sonrasında pencerenin sağındaki X ile bu alanı kapatıyoruz. **SAML & based Sign-on** ekranına geri geldik. **Certificate (Base64)** yanındaki **download** a tıklayarak sertifikayı indiriyoruz.

Microsoft Azure

Search resources, services, and docs (G+)

[Home](#) > [Enterprise applications | All applications](#) > [FortiGate SSL VPN](#) >

## FortiGate SSL VPN | SAML-based Sign-on

Enterprise Application

Overview

Deployment Plan

Diagnose and solve problems

Manage

Properties

Owners

Roles and administrators

Users and groups

Single sign-on

Provisioning

Self-service

Custom security attributes (preview)

Security

Conditional Access

Permissions

Token encryption

Activity

Sign-in logs

Usage & insights

Audit logs

Provisioning logs

Access reviews

Upload metadata file

Change single sign-on mode

Test this application

Got feedback?

### Set up Single Sign-On with SAML

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

Read the [configuration guide](#) for help integrating FortiGate SSL VPN.

1

Basic SAML Configuration

Edit

Identifier (Entity ID)	https://ata	:om:19443/remote/saml/metadata
Reply URL (Assertion Consumer Service URL)	https://	:om:19443/remote/saml/login
Sign on URL	https://	:om:19443/remote/saml/login
Relay State (Optional)	Optional	
Logout Url (Optional)	https://	:om:19443/remote/saml/logout

2

Attributes & Claims

Edit

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

3

SAML Certificates

Edit

Token signing certificate

Status

Thumbprint

Expiration

Notification Email

App Federation Metadata Url

Certificate (Base64)

Certificate (Raw)

Active

6077670FF2957D5C69F105FBC947614E1F7B9F8F

1/3/2026, 3:14:23 PM

https://login.microsoftonline.com/cb243bf0-2036-...

Download

Download



Şimdi 3 nolu kısma geldi buradaki sertifikayı fortigate üzerine import edeceğiz. **System->Certificate** menüsüne geliyoruz. **Create/Import** a tıklıyoruz.

Menüden **Remote Certificate** seçiyoruz. İndirdiğimiz sertifikayı seçip ekliyoruz.

Eğer Certificates görünmüyorsa System->Feature Visibility menüsünden açmanız gerekir.

The screenshot shows the FortiGate web interface. On the left, the 'System' menu is expanded, and 'Certificates' is highlighted with a red star. In the main area, the 'Create/Import' button is highlighted with a red arrow. Below it, the 'Remote Certificate' option is also highlighted with a red arrow. The table below shows a list of certificates, including 'Fortinet\_Factory\_Backup', 'Fortinet\_GUI\_Server', 'Fortinet\_SSL', 'Fortinet\_SSL\_DSA1024', 'Fortinet\_SSL\_DSA2048', 'Fortinet\_SSL\_ECDSA256', 'Fortinet\_SSL\_ECDSA384', 'Fortinet\_SSL\_ECDSA521', 'Fortinet\_SSL\_ED448', 'Fortinet\_SSL\_ED25519', 'Fortinet\_SSL\_RSA1024', 'Fortinet\_SSL\_RSA2048', 'Fortinet\_SSL\_RSA4096', and 'Fortinet\_Wifi'. The 'Remote CA Certificate' section is also visible, showing 'Fortinet\_CA'.

Name	Subject	Comments
Fortinet_Factory_Backup	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN = Fortinet_Factory_Backup	This certificate is embedded in the hardware at the factory and is unique
Fortinet_GUI_Server	C = US, ST = California, L = Sunnyvale, O = Fortinet Ltd., OU = FortiGate, CN = Fortinet_GUI_Server	This is the default CA certificate the SSL Inspection will use when generating certificates
Fortinet_SSL	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN = Fortinet	This certificate is embedded in the hardware at the factory and is unique
Fortinet_SSL_DSA1024	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN = Fortinet	This certificate is embedded in the hardware at the factory and is unique
Fortinet_SSL_DSA2048	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN = Fortinet	This certificate is embedded in the hardware at the factory and is unique
Fortinet_SSL_ECDSA256	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN = Fortinet	This certificate is embedded in the hardware at the factory and is unique
Fortinet_SSL_ECDSA384	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN = Fortinet	This certificate is embedded in the hardware at the factory and is unique
Fortinet_SSL_ECDSA521	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN = Fortinet	This certificate is embedded in the hardware at the factory and is unique
Fortinet_SSL_ED448	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN = Fortinet	This certificate is embedded in the hardware at the factory and is unique
Fortinet_SSL_ED25519	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN = Fortinet	This certificate is embedded in the hardware at the factory and is unique
Fortinet_SSL_RSA1024	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN = Fortinet	This certificate is embedded in the hardware at the factory and is unique
Fortinet_SSL_RSA2048	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN = Fortinet	This certificate is embedded in the hardware at the factory and is unique
Fortinet_SSL_RSA4096	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN = Fortinet	This certificate is embedded in the hardware at the factory and is unique
Fortinet_Wifi	C = US, ST = California, L = Sunnyvale, O = "Fortinet, Inc.", CN = auth-cert...	This certificate is embedded in the firmware and is the same on every unit

Sertifikayı import ettik. Buradaki **REMOTE\_Cert\_1** ismi önemli bunu da not edelim.

The screenshot shows the FortiGate web interface. On the left, the 'System' menu is expanded, and 'Certificates' is highlighted with a red star. In the main area, the 'Remote Certificate' option is highlighted with a red arrow. The table below shows a list of certificates, including 'Fortinet\_CA', 'Fortinet\_CA\_Backup', 'Fortinet\_Sub\_CA', 'Fortinet\_Wifi\_CA', and 'REMOTE\_Cert\_1'. The 'REMOTE\_Cert\_1' certificate is highlighted with a red box.

Name	Subject	Comments	Issuer	Expires	Status
Fortinet_CA	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN = Fortinet_CA	This certificate is embedded in the hardware at the factory and is unique	Fortinet	2038/01/1...	Valid
Fortinet_CA_Backup	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN = Fortinet_CA_Backup	This certificate is embedded in the hardware at the factory and is unique	Fortinet	2038/01/2...	Valid
Fortinet_Sub_CA	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN = Fortinet_Sub_CA	This certificate is embedded in the hardware at the factory and is unique	Fortinet	2038/01/2...	Valid
Fortinet_Wifi_CA	C = US, O = DigiCert Inc, CN = DigiCert TLS RSA S...	This certificate is embedded in the hardware at the factory and is unique	DigiCert I...	2030/09/2...	Valid
REMOTE_Cert_1	CN = Microsoft Azure Federated SSO Certificate		Microsoft ...	2026/01/0...	Valid



4 nolu kısımdaki 3 adet link bizim için önemli.

Microsoft Azure

Search resources, services, and docs (G+ /)

Home > Enterprise applications | All applications > FortiGate SSL VPN >

## FortiGate SSL VPN | SAML-based Sign-on

Enterprise Application

Overview  
Deployment Plan  
Diagnose and solve problems

Manage

- Properties
- Owners
- Roles and administrators
- Users and groups
- Single sign-on
- Provisioning
- Self-service
- Custom security attributes (preview)

Security

- Conditional Access
- Permissions
- Token encryption

Activity

- Sign-in logs
- Usage & insights
- Audit logs
- Provisioning logs

Upload metadata file | Change single sign-on mode | Test this application | Got feedback?

Token signing certificate

Status	Active	Edit
Thumbprint	6077670FF2957D5C69F105FBC947614E1F7B9F8F	
Expiration	1/3/2026, 3:14:23 PM	
Notification Email		
App Federation Metadata Url	<a href="https://login.microsoftonline.com/cb243bf0-2036-...">https://login.microsoftonline.com/cb243bf0-2036-...</a>	
Certificate (Base64)	<a href="#">Download</a>	
Certificate (Raw)	<a href="#">Download</a>	
Federation Metadata XML	<a href="#">Download</a>	

Verification certificates (optional) (Preview)

Required	No	Edit
Active	0	
Expired	0	

4 Set up FortiGate SSL VPN

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

Login URL	<a href="https://login.microsoftonline.com/cb243bf0-2036-...">https://login.microsoftonline.com/cb243bf0-2036-...</a>
Azure AD Identifier	<a href="https://sts.windows.net/cb243bf0-2036-4d3a-b86-...">https://sts.windows.net/cb243bf0-2036-4d3a-b86-...</a>
Logout URL	<a href="https://login.microsoftonline.com/cb243bf0-2036-...">https://login.microsoftonline.com/cb243bf0-2036-...</a>

5 Test single sign-on with FortiGate SSL VPN

Test to see if single sign-on is working. Users will need to be added to Users and groups before they can sign in.

[Test](#)

Bu işaretli alanların yanındaki ikona tıklayıp bir not defterine ekleyelim. Fortigate de cli ile gireceğimiz komutlar şu şekilde olacak.

```
config user saml
edit Azure-SSL-SAML
set cert azurevpn
set entity-id https://. :19443/remote/saml/metadata
set single-sign-on-url https://. :19443/remote/saml/login
set single-logout-url https://. :19443/remote/saml/logout
set idp-entity-id https://sts.windows.net/cb243bf0-2036-4d3a-b863-c9e37f25ed38/
set idp-single-sign-on-url https://login.microsoftonline.com/cb243bf0-2036-4d3a-b863-c9e37f25ed38/saml2
set idp-single-logout-url https://login.microsoftonline.com/cb243bf0-2036-4d3a-b863-c9e37f25ed38/saml2
set idp-cert REMOTE_Cert_1
set user-name username
set group-name group
next
end

config user group
edit AzureAD-VPN
set member Azure-SSL-SAML
config match
edit 1
set server-name Azure-SSL-SAML
set group-name 79aaf40b-db9b-441e-b885-5c301c531779
next
end
next
end
```

Editleyebilmeniz için aşağıya kodları ekliyorum.

```
config user saml
edit Azure-SSL-SAML
set cert azurevpn
set entity-id https://azurevpn.gokhanunal.com:19443/remote/saml/metadata
set single-sign-on-url https://azurevpn.gokhanunal.com:19443/remote/saml/login
set single-logout-url https://azurevpn.gokhanunal.com:19443/remote/saml/logout
set idp-entity-id https://sts.windows.net/cb243bf0-2036-4d3a-b863-c9e37f25ed38/
set idp-single-sign-on-url https://login.microsoftonline.com/cb243bf0-2036-4d3a-b863-c9e37f25ed38/saml2
set idp-single-logout-url https://login.microsoftonline.com/cb243bf0-2036-4d3a-b863-c9e37f25ed38/saml2
set idp-cert REMOTE_Cert_1
set user-name username
set group-name group
next
end
```

Kırmızı alanlar değiştirilecek yerler.

**azurevpn** : ücretli yada ücretsiz olarak fortigate içine eklediğimiz sertifika adı.

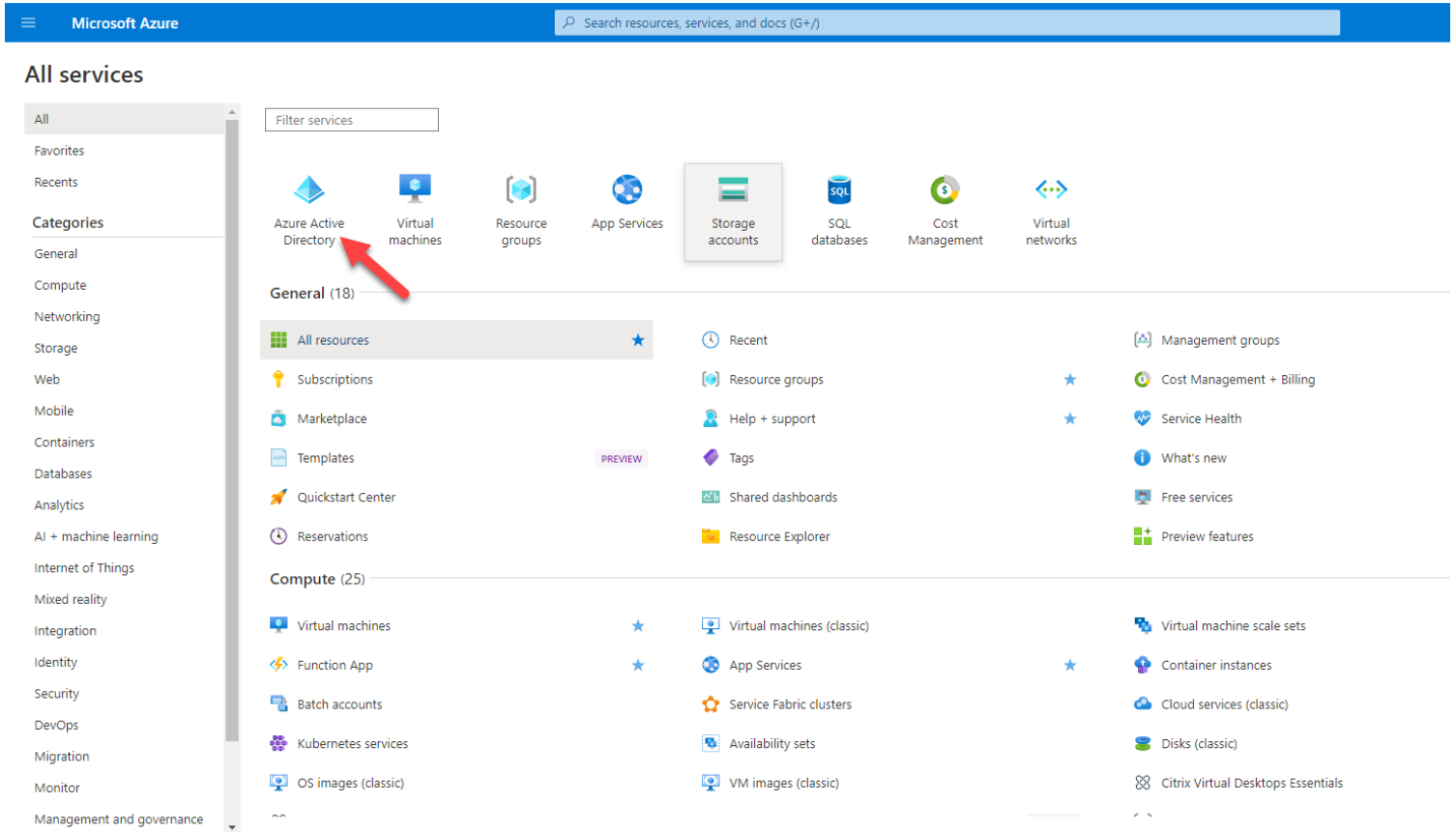
**set entity-id ,set single-sign-on-url ,set single-logout-url** : Azure Basic SAML Configuration kısmında girdiğimiz linkler.

**set idp-entity-id, set idp-single-sign-on-url, set idp-single-logout-url** : 4 nolu bölümdeki kopyaladığımız linkler.

**REMOTE\_Cert\_1**: Azure dan indirip fortigate içine import ettiğimiz sertifikanın görünen adı.

**username, group** : Attributes & Claim kısmında verdiğimiz adlar.

Şimdi Azure Active Directory açıyoruz.



**New Group** a tıklayıp Azure Authentication için bir grup oluşturuyoruz.

Microsoft Azure

Search resources, services, and docs (G+/)

All services >

Groups | All groups

- Azure Active Directory

All groups

Deleted groups

Diagnose and solve problems

Settings

General

Expiration

Naming policy

New group

Download groups

Refresh

Manage view

Delete

Got feedback?

Dynamic group memberships have not been updated due to system delays. We're working to resolve the issue.

Search

Add filter

Search mode

Contains

42 groups found

Name

Object Id

Group type

**Group type** olarak **Security** seçiyoruz ve **Group name** kısmına grup adını yazıp **Create** tıklıyoruz.

Microsoft Azure

Search resources, services, and docs (G+/)

All services > Groups | All groups >

New Group

Got feedback?

Group type \*

Security

Group name \*

AzureAD-VPN

Group description

Enter a description for the group

Azure AD roles can be assigned to the group

Yes

No

Membership type \*

Assigned

Owners

No owners selected

Members

No members selected

Create

Grup oluřtu. Grup adına tıklayıp detaylarını aıyoruz.

Microsoft Azure

Search resources, services, and docs (G+/)

All services > Groups | All groups

r - Azure Active Directory

Dynamic group memberships have not been updated due to system delays. We're working to resolve the issue.

Search

Search mode Contains

43 groups found

Name	Object Id	Group type	Membership type	Email	Source
AzureAD-VPN	79aaf40b-db9b-441e-b885-5c301c531779	Security	Assigned		Cloud

Object ID bizim iin nemli bunu da komut satırında kullanacaėız. O yzden kaydediyoruz.

Microsoft Azure

Search resources, services, and docs (G+/)

All services > Groups | All groups

AzureAD-VPN

Group

Overview

Diagnose and solve problems

Manage

Properties

Members

Owners

Roles and administrators

Administrative units

Group memberships

Applications

Licenses

Azure role assignments

Activity

Access reviews

Audit logs

Bulk operation results

Troubleshooting + Support

New support request

AzureAD-VPN

Membership type Assigned

Source Cloud

Type Security

Object Id 79aaf40b-db9b-441e-b885-5c301c531779

Created at 1/3/2023, 4:39:37 PM

Direct members

0 Total 0 User(s) 0 Group(s) 0 Device(s) 0 Other(s)

Group memberships 0 Owners 0 Total members 0

Tekrar Enterprise applications a gelip Fortigate SSL VPN açıyoruz. Users and groups tıklıyoruz.

Microsoft Azure

Home > Enterprise applications | All applications > FortiGate SSL VPN | Overview

FortiGate SSL VPN | Overview

Overview

Deployment Plan

Diagnose and solve problems

Manage

Properties

Owners

Roles and administrators

Users and groups

Single sign-on

Provisioning

Self-service

Custom security attributes (preview)

Security

Conditional Access

Permissions

Token encryption

Activity

Properties

Name

FortiGate SSL VPN

Application ID

68dcafe2-ec7a-414a-9f6e-1...

Object ID

fe641867-5cef-4b94-82cd-e...

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

3. Provision User Account

You'll need to create user accounts for the application

Learn more

5. Self service

Enable users to request access to the application using their Azure AD credentials

Get started

Add Assignment penceresinde Users and groups altındaki None Selected e tıklıyoruz. Sağda açılan kısımdan oluşturduğumuz grubu seçiyoruz.

Microsoft Azure

Home > Enterprise applications | All applications > FortiGate SSL VPN | Users and groups > Add Assignment

Add Assignment

Users and groups

None Selected

Select a role

Default Access

Users and groups

Search

AZ AzureAD-VPN Selected

Selected items

AZ AzureAD-VPN Remove

Assign tıklayarak grubu tanımlıyoruz.

Microsoft Azure

Home > Enterprise applications | All applications > FortiGate SSL VPN | Users and groups > Add Assignment

Add Assignment

When you assign a group to an application, only users directly in the group will have access. The assignment does not cascade to nested groups.

Users and groups

1 group selected.

Select a role

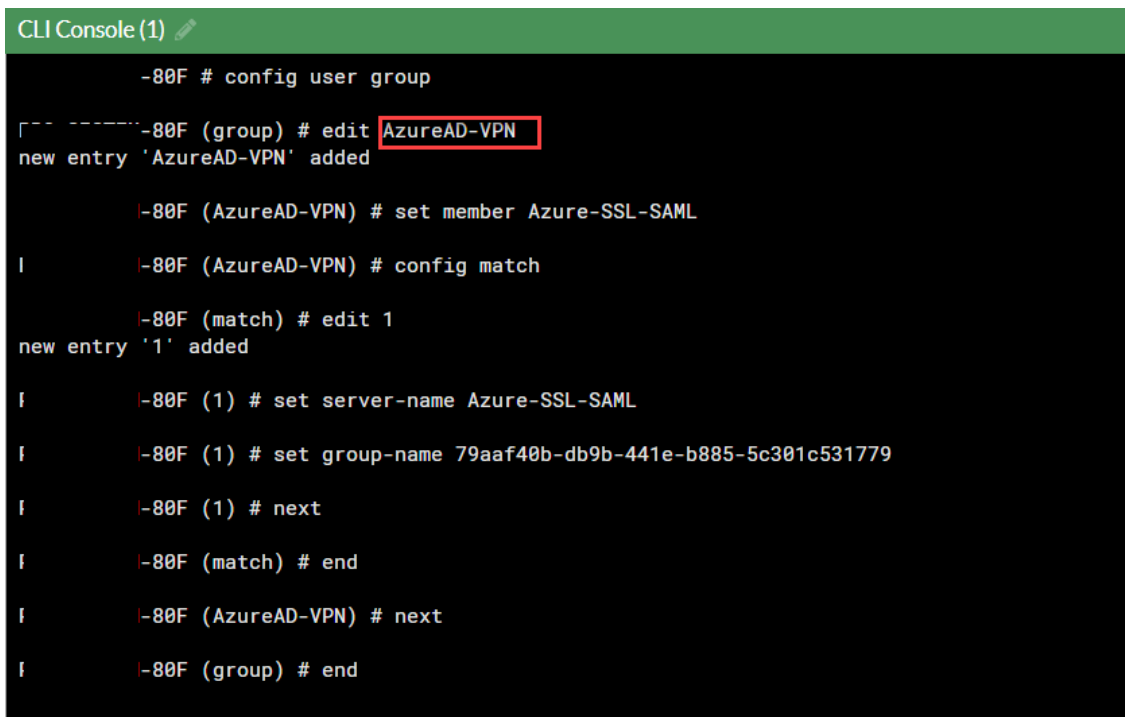
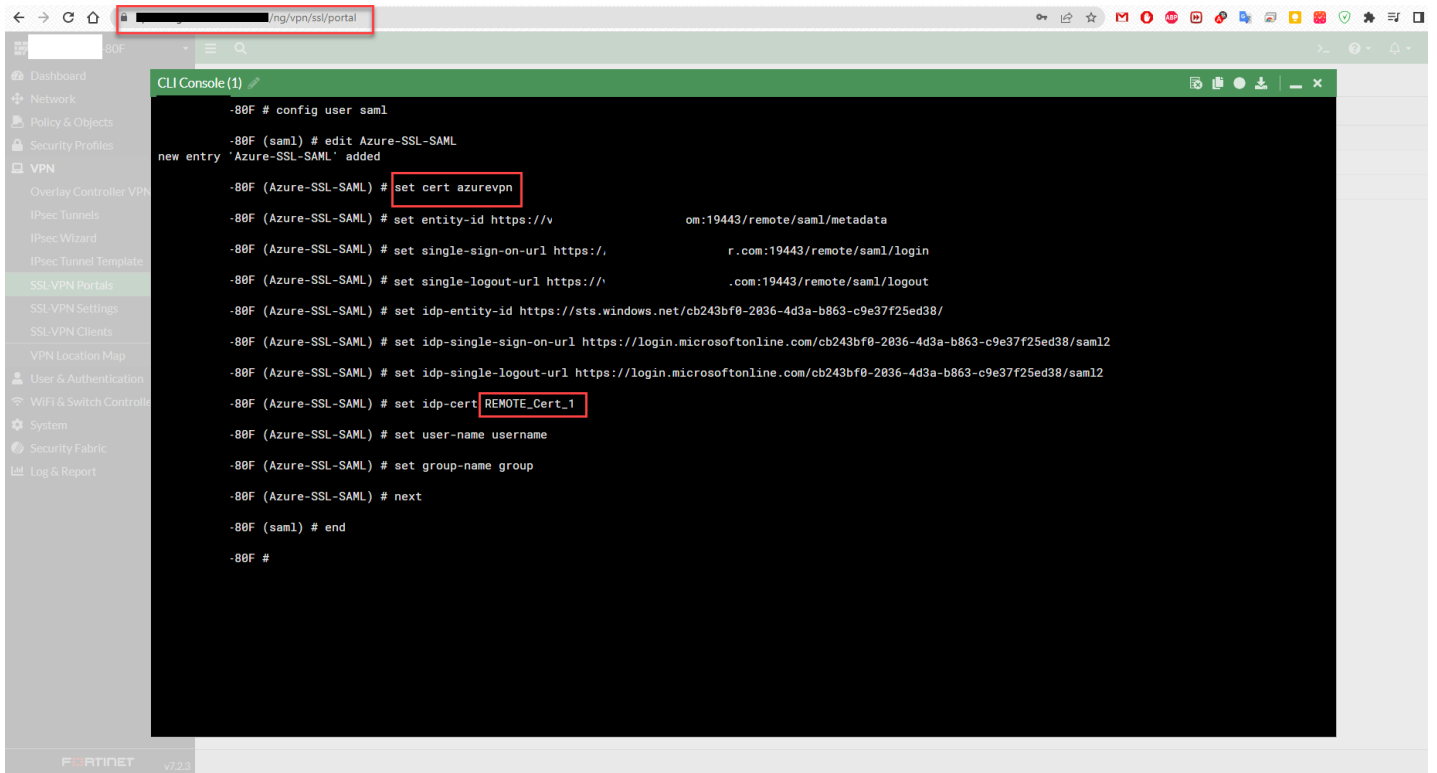
Default Access

Assign

2. komut kısmımız da aşağıdaki gibi kırmızı alan daha önce kopyaladığımız grup id.

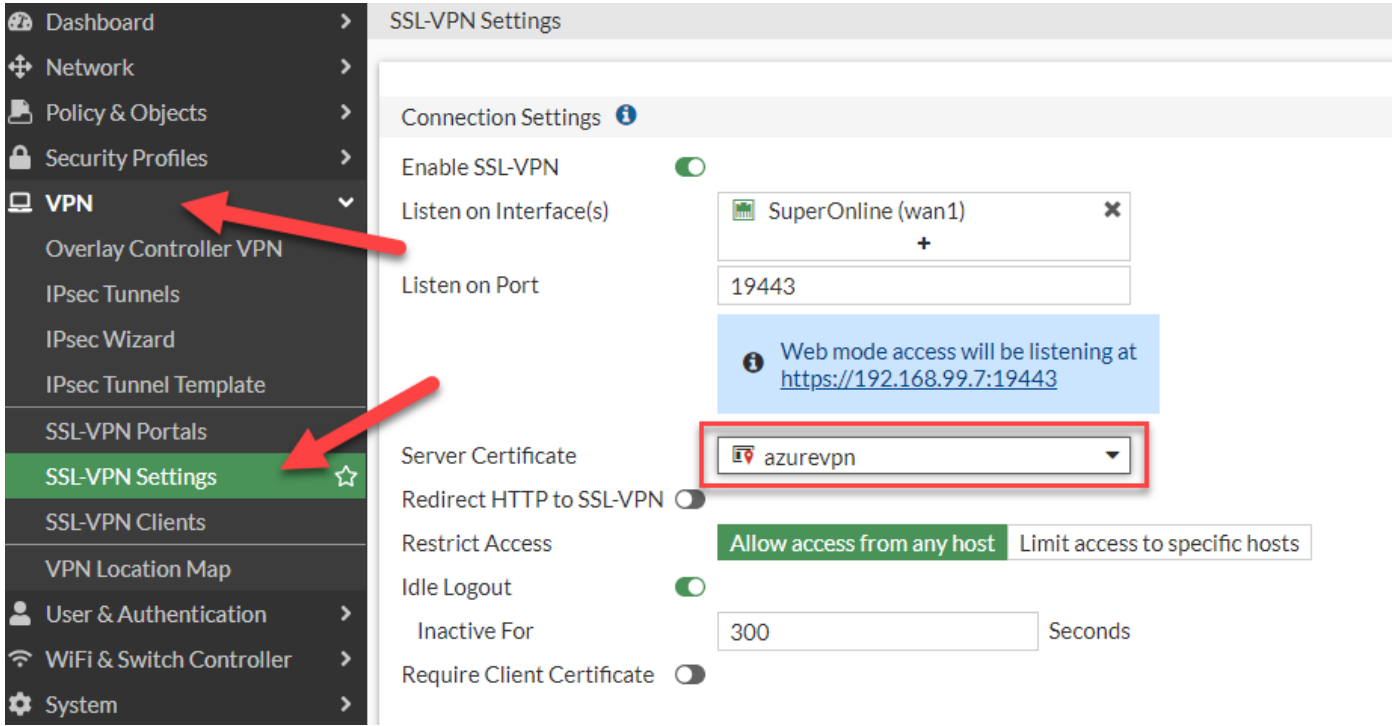
```
config user group
edit AzureAD-VPN
set member Azure-SSL-SAML
config match
edit 1
set server-name Azure-SSL-SAML
set group-name 79aaf40b-db9b-441e-b885-5c301c531779
next
end
next
end
```

Şimdi komutlarımızı fortigate cli üzerinden gireceğiz. Sertifikasını oluşturduğumuz alan adımız veya ip adresimiz ile firewall a giriş yapıp cli açıyoruz ve komutlarımızı giriyoruz.

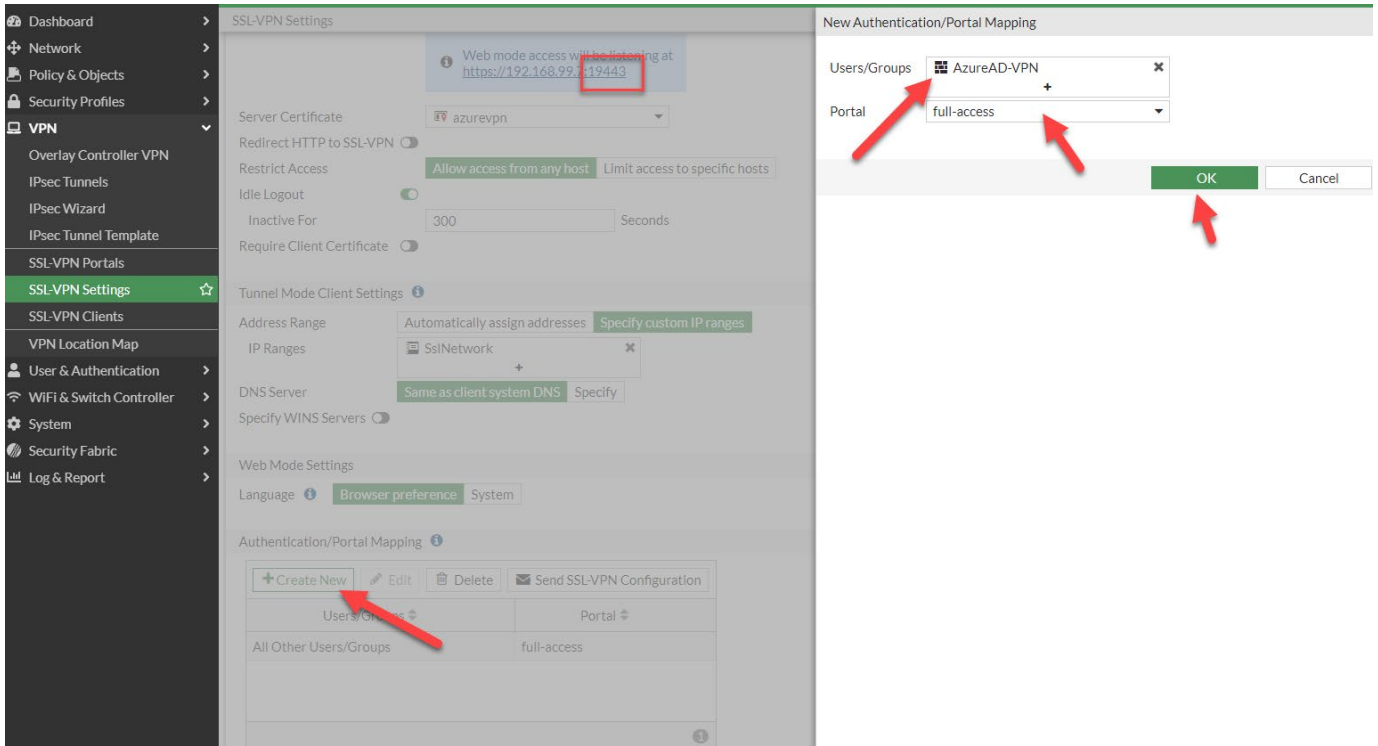




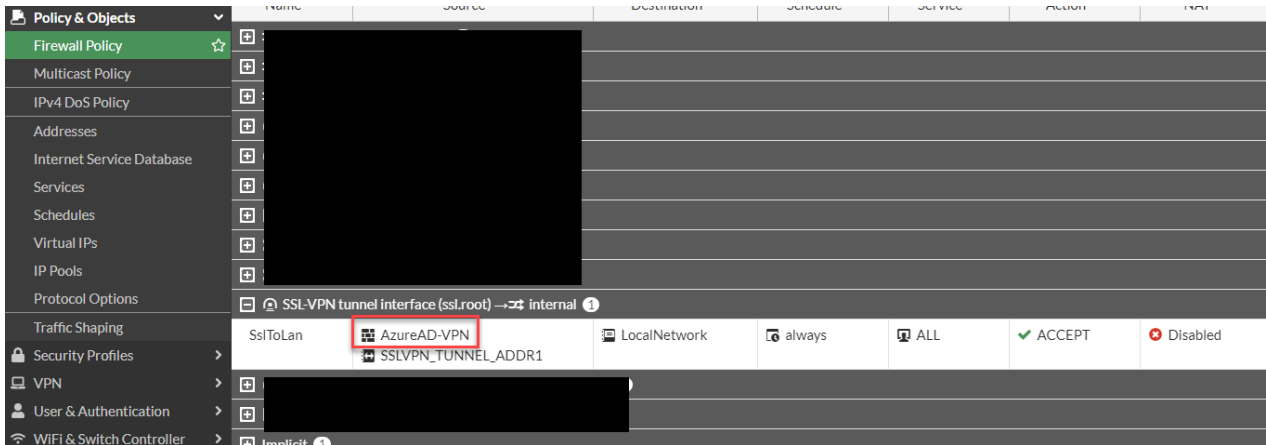
Sonrasında SSL-VPN Settings e gelip sertifikamızı seçiyoruz.



Ardından **Authentication/Portal Mapping** kısmında **Create New** diyerek grubumuzu seçiyoruz.

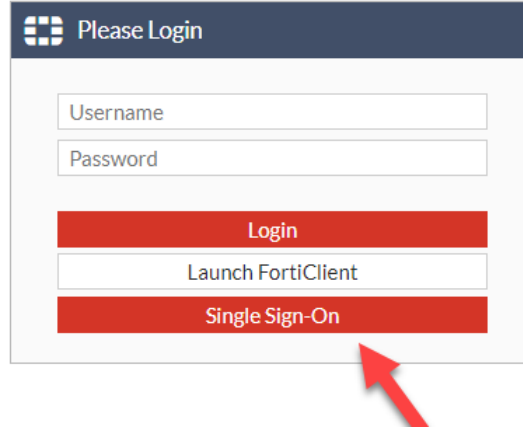
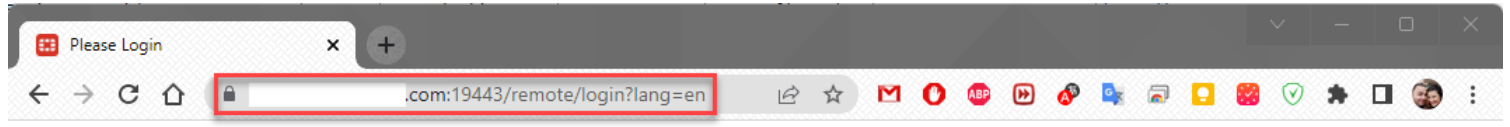


Son olarak firewall policy de grubu ekleyerek işlemi tamamlıyoruz.

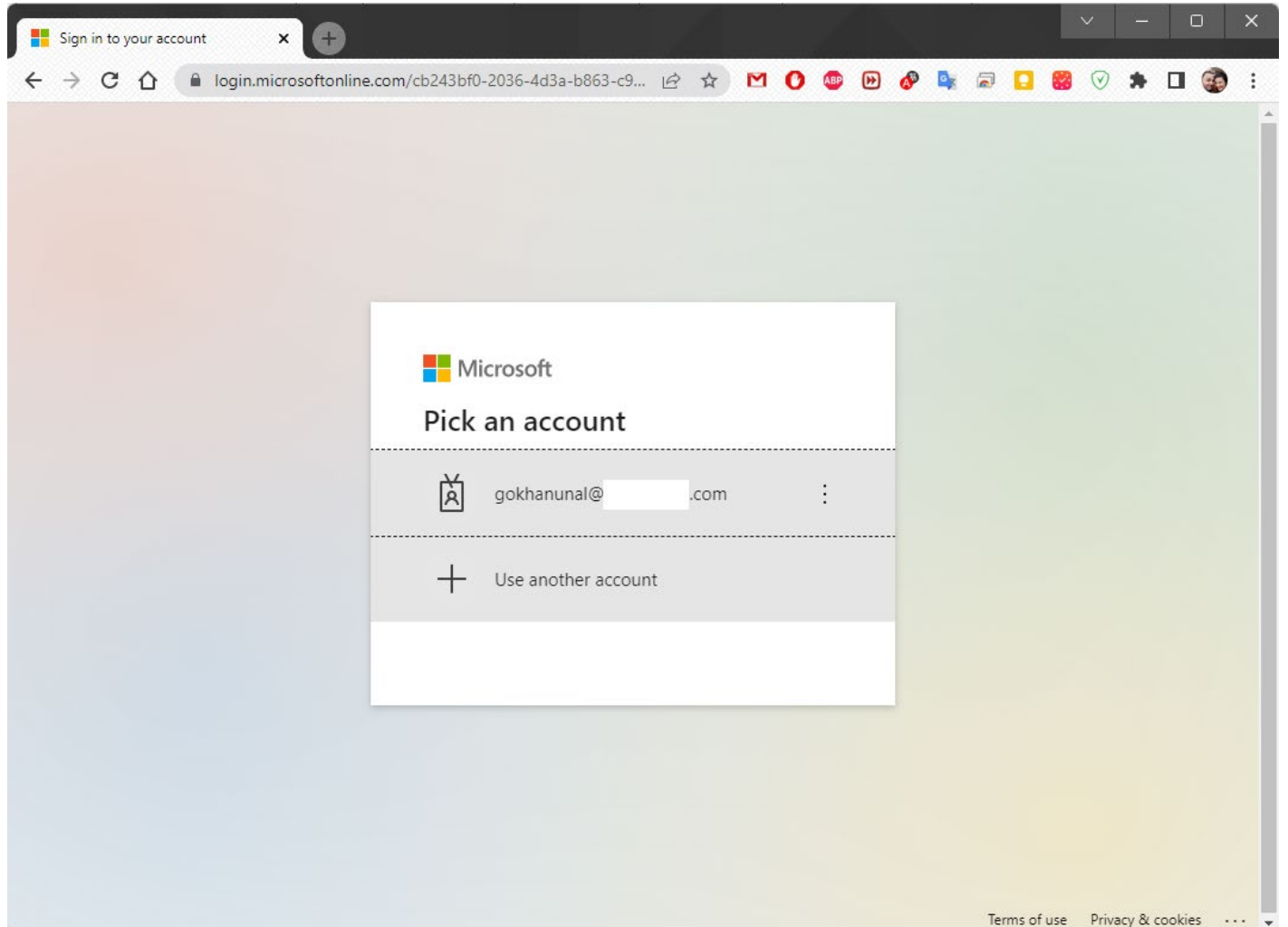


Şimdi test işlemine başlayalım.

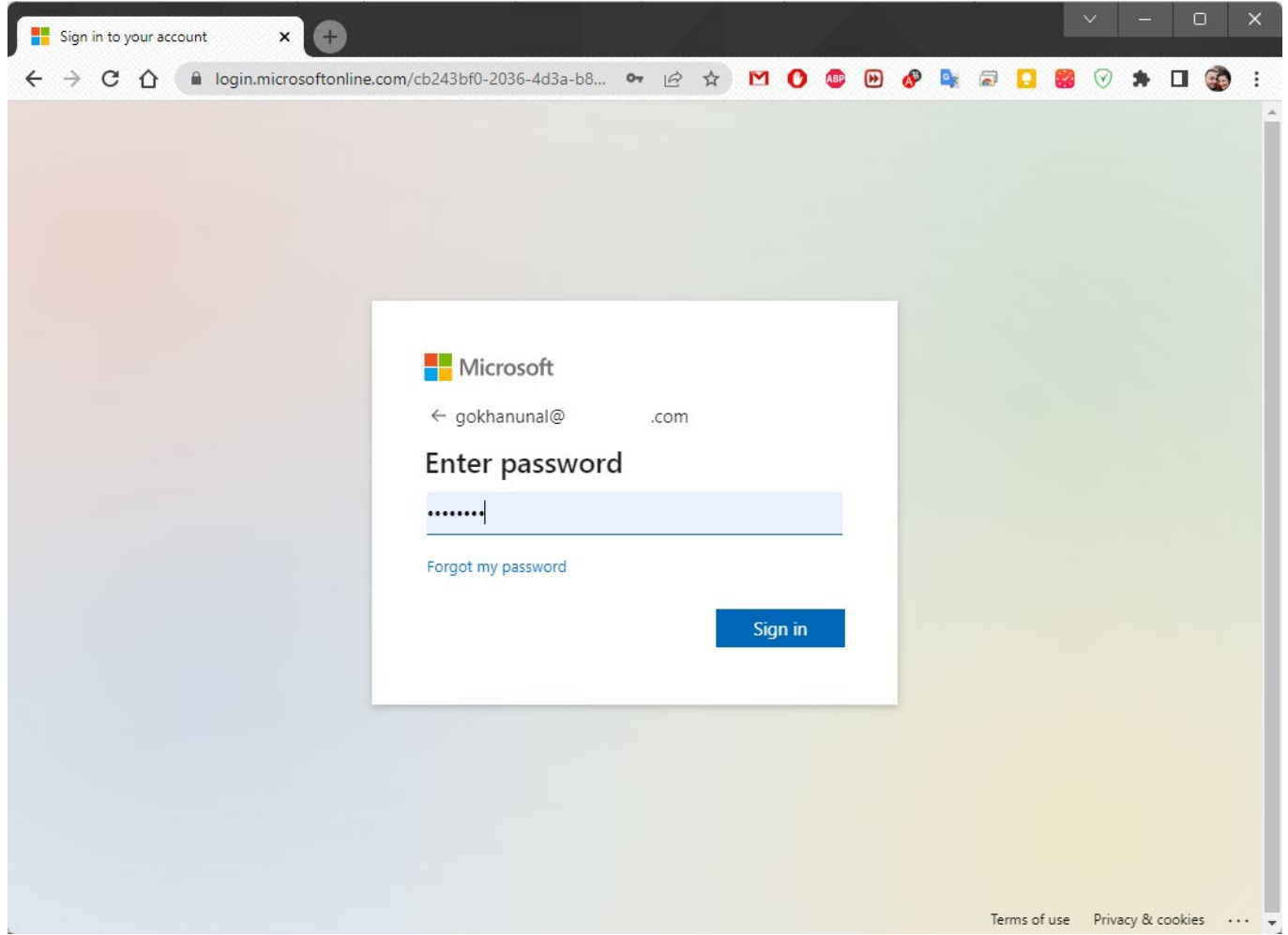
https://Alan adımız:19443 ile aşağıdaki login ekranına geliyoruz.



Beni Microsoft login ekranına yönlendiriyor. Kullanıcı adımızı giriyoruz.



Şifremi giriyorum.



Sign in to your account

login.microsoftonline.com/cb243bf0-2036-4d3a-b8...

Microsoft

← gokhanunal@ .com

Enter password

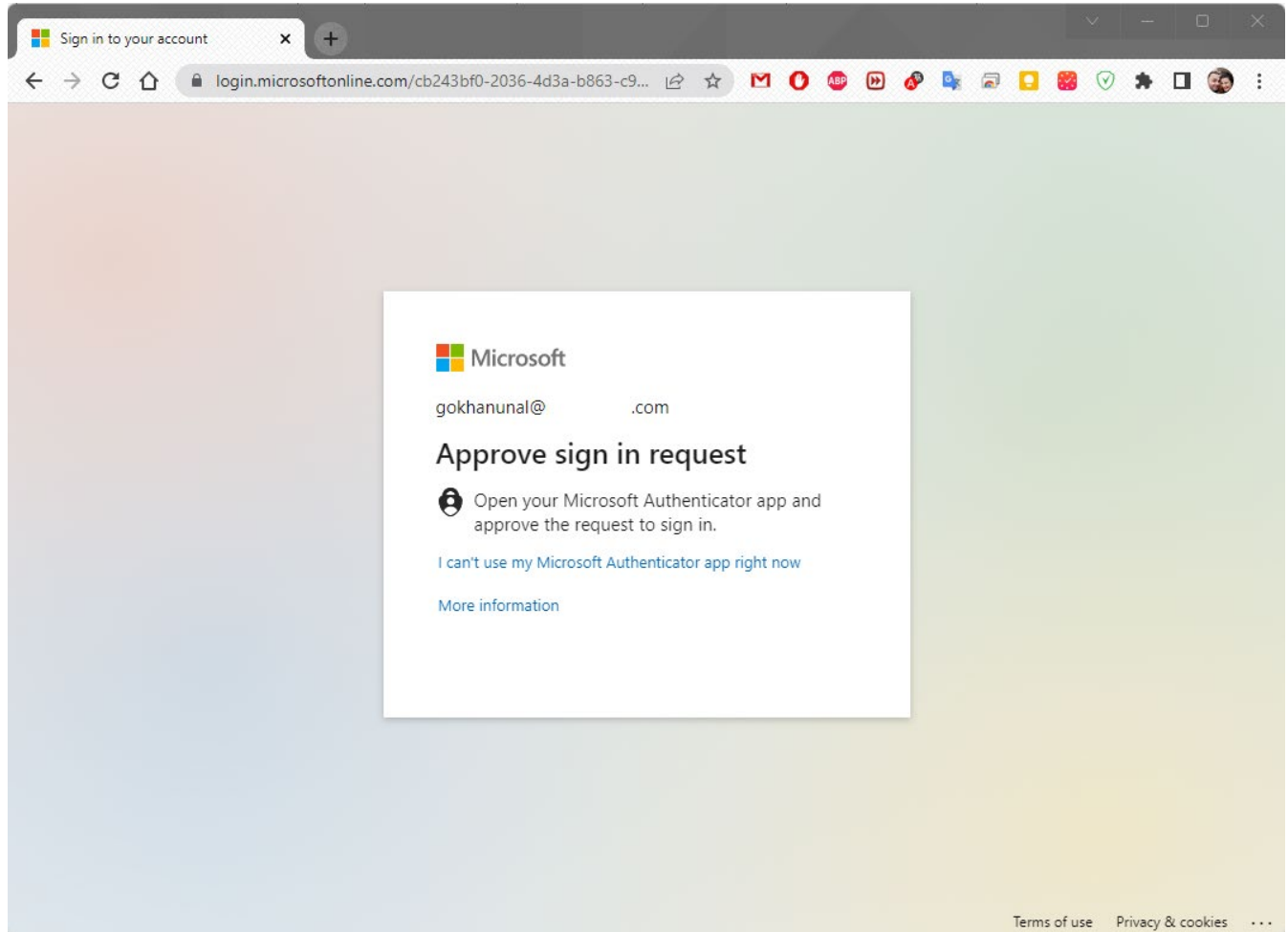
.....

[Forgot my password](#)

[Sign in](#)

[Terms of use](#) [Privacy & cookies](#) ...

Telefonumda Microsoft Authenticator ile izin vermemi bekliyor.



Sign in to your account

login.microsoftonline.com/cb243bf0-2036-4d3a-b863-c9...

Microsoft

gokhanunal@ .com

Approve sign in request

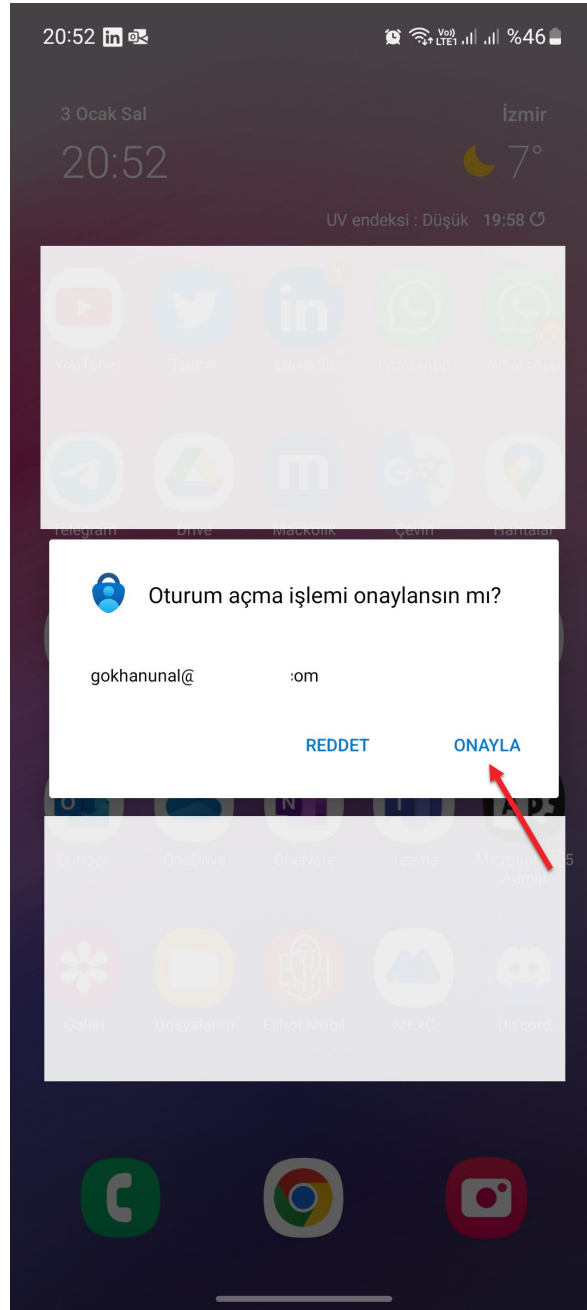
Open your Microsoft Authenticator app and approve the request to sign in.

[I can't use my Microsoft Authenticator app right now](#)

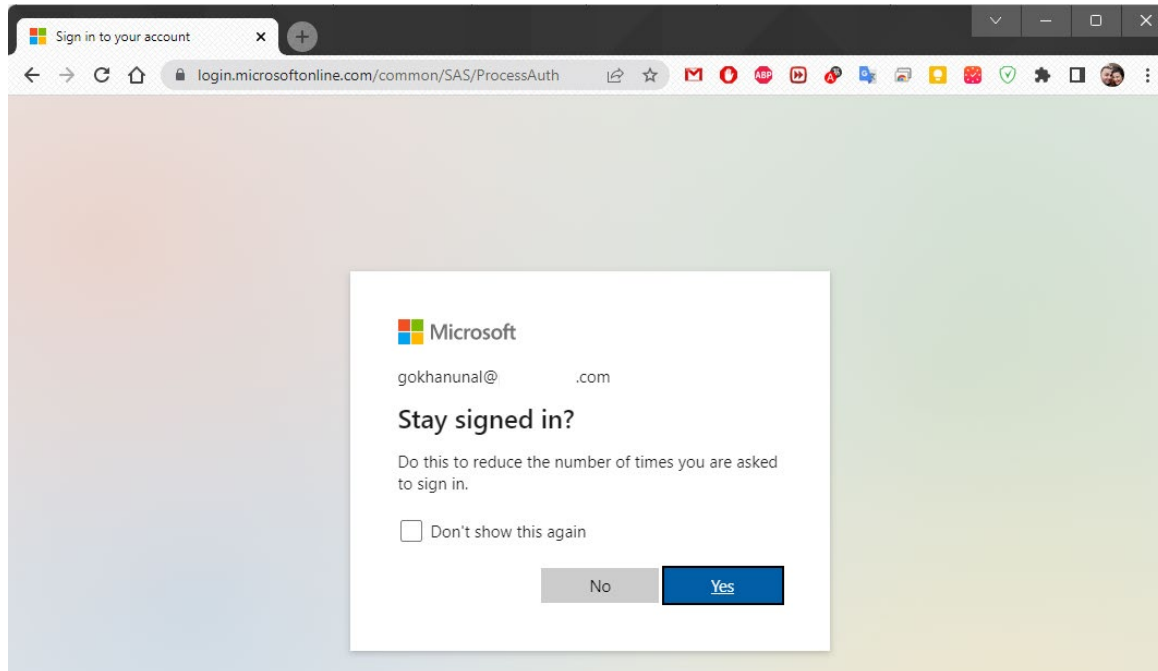
[More information](#)

[Terms of use](#) [Privacy & cookies](#) ...

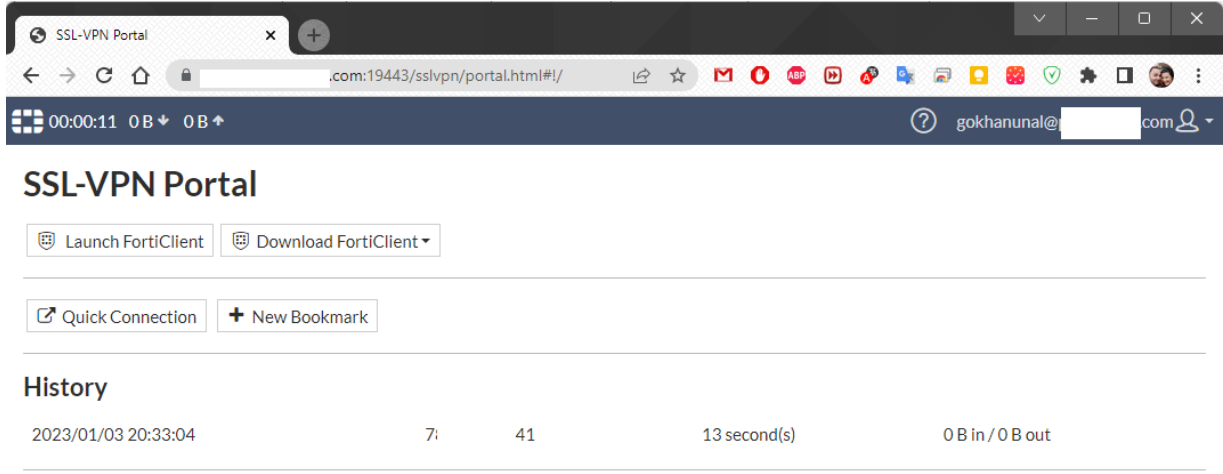
Telefonumda onay veriyorum.



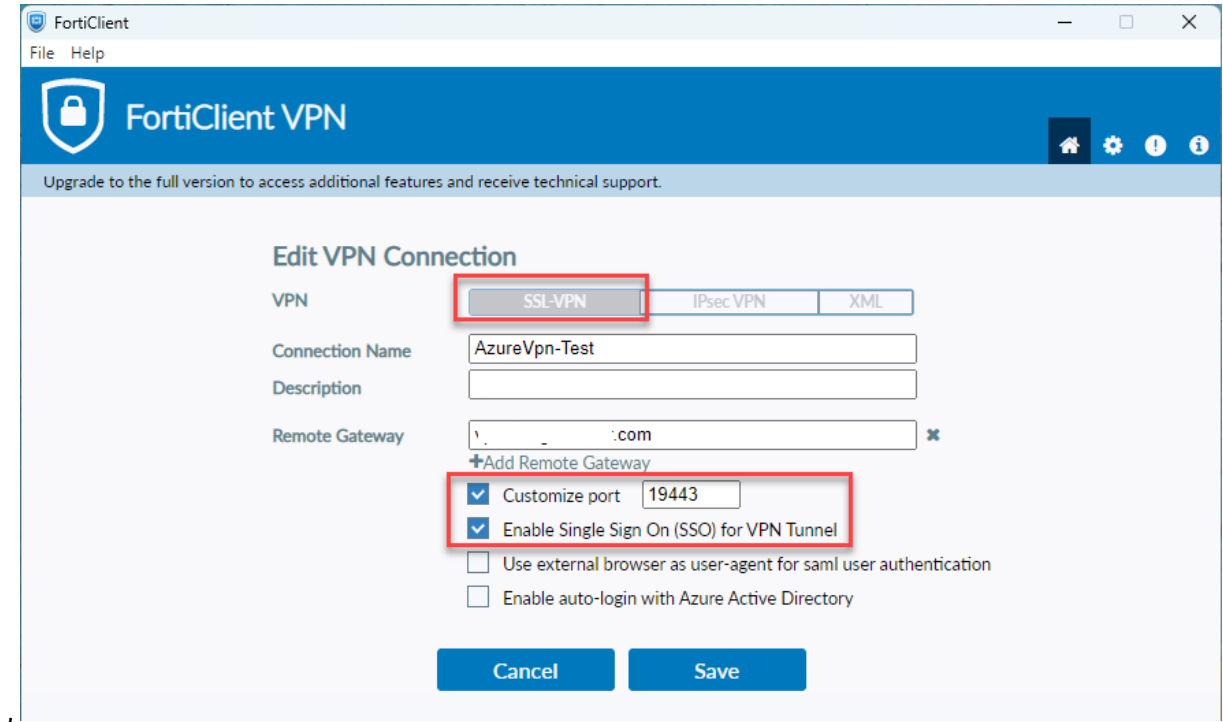
Oturum açık kalsın mı diye soruyor. Evet diyorum.



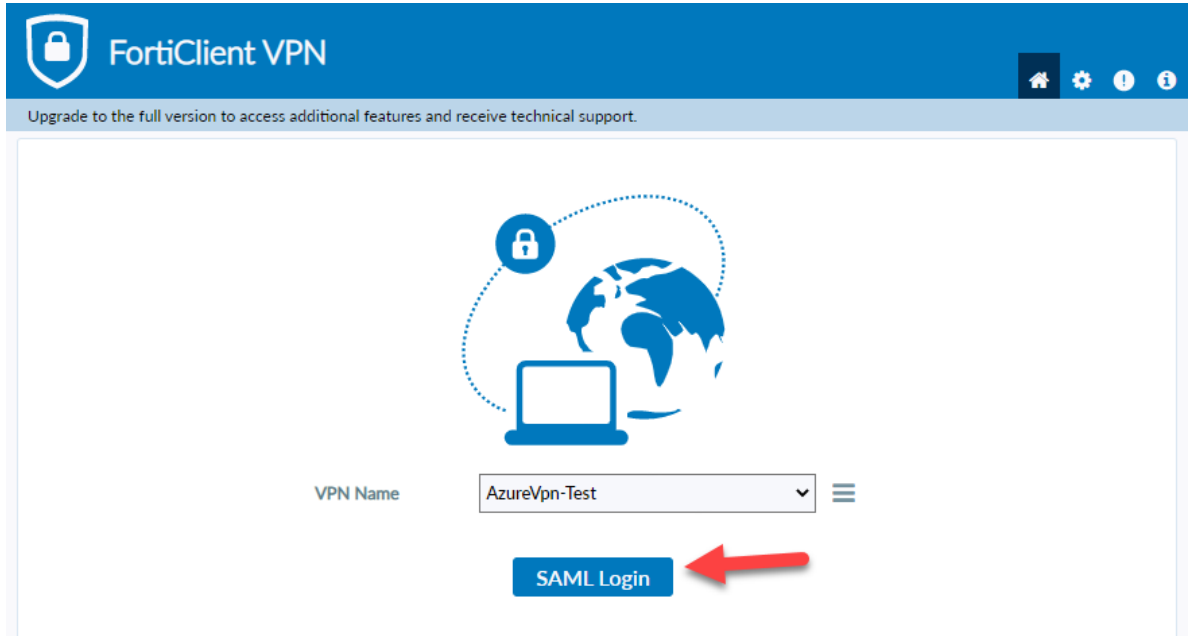
SSL-VPN bağlantımız gerçekleşti.



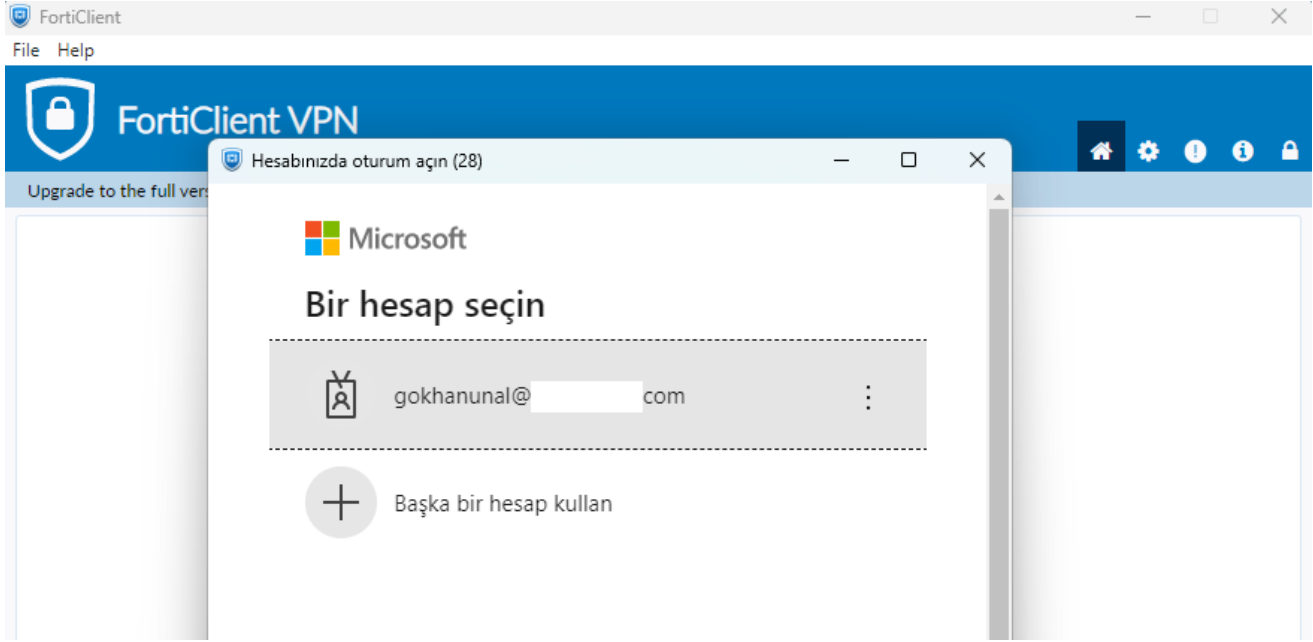
Şimdi FortiClient ile bağlantı sağlayalım. **Remote gateway** satırına sertifika aldığımız alan adımızı, **customize port** kısmına belirlediğimiz portu yazıyoruz. **Enable Single Sign On (SSO) for VPN Tunnel** işaretleyip **Save** diyoruz.



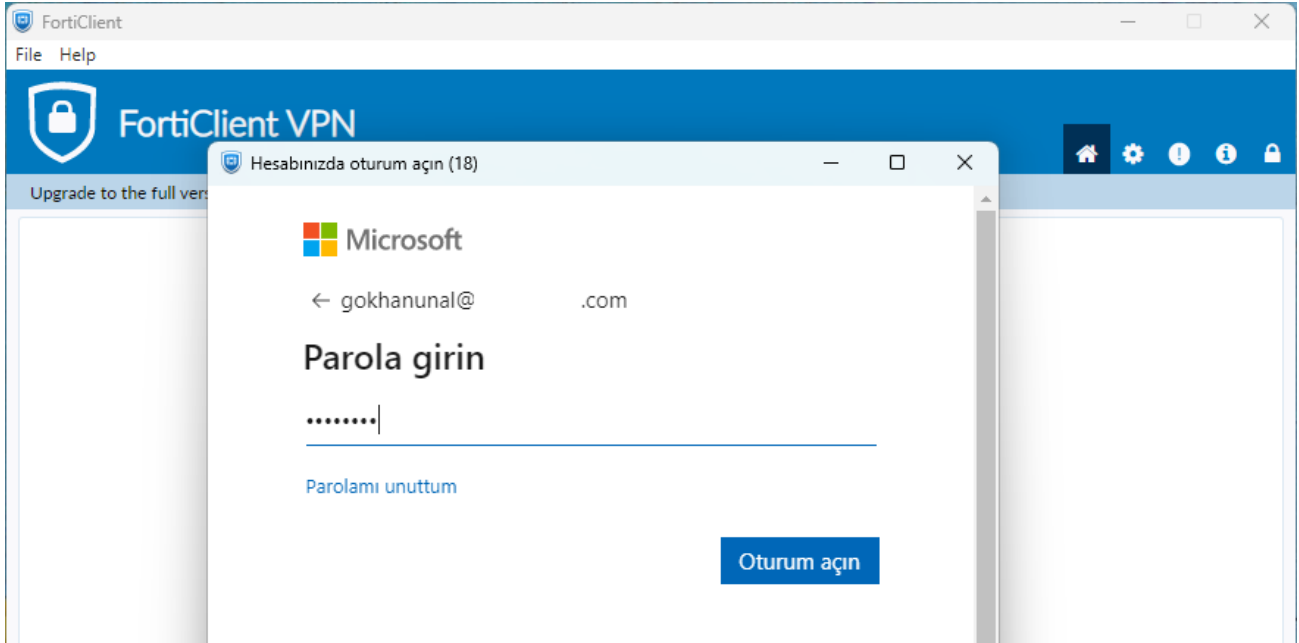
**SAML Login** e tıklıyoruz.



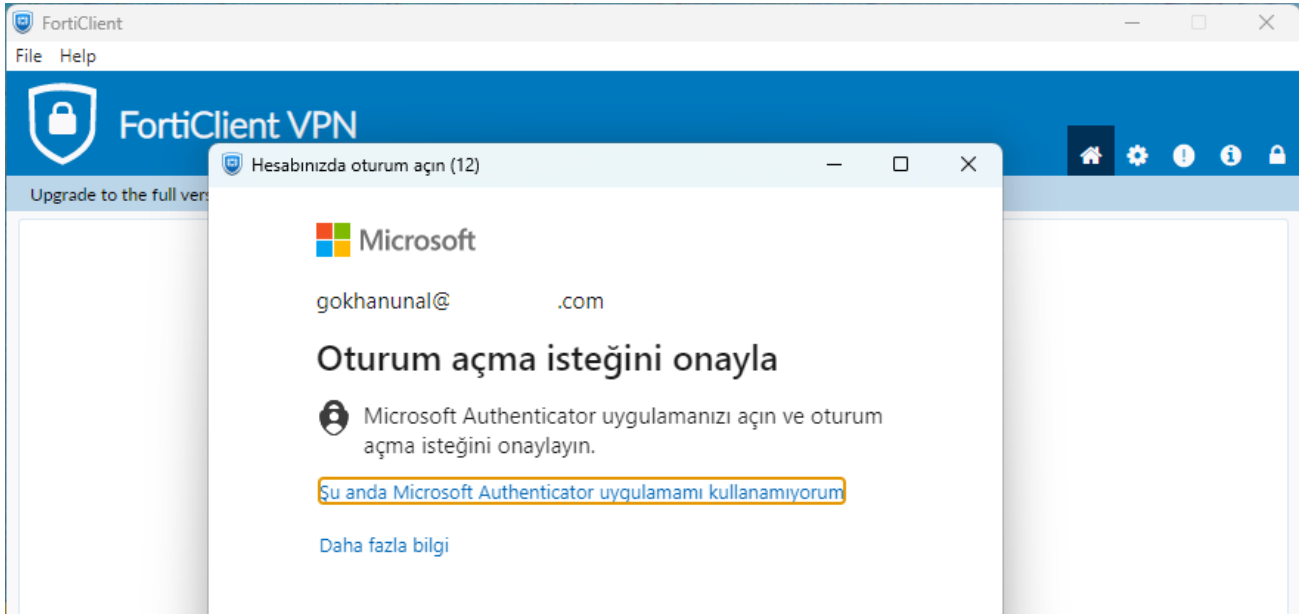
Kullanıcı adımızı giriyoruz/seiyoruz.



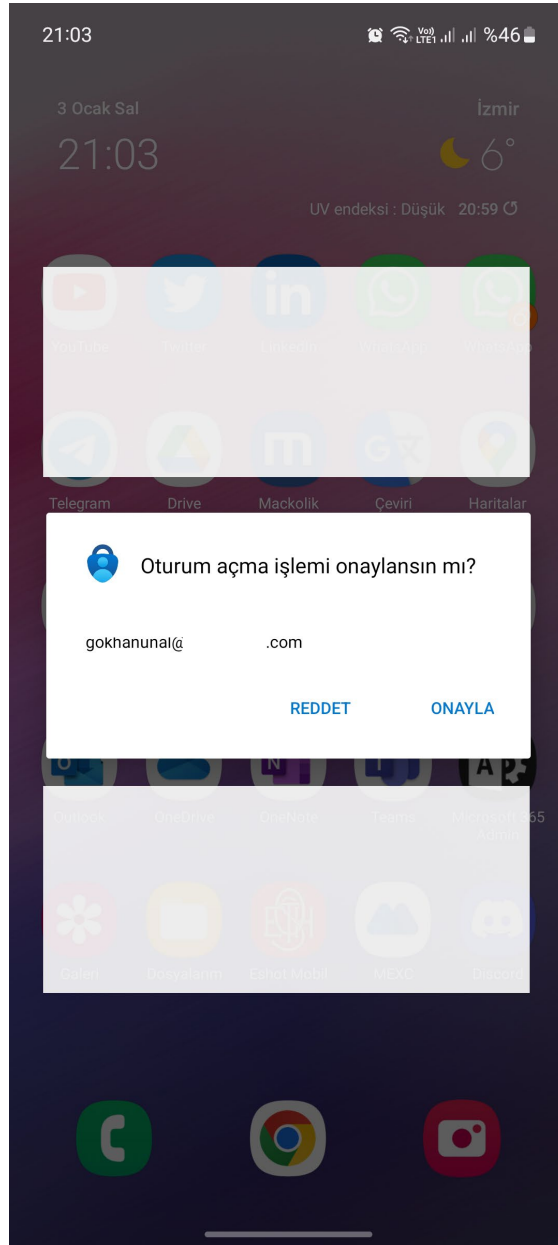
Parolamızı giriyoruz.



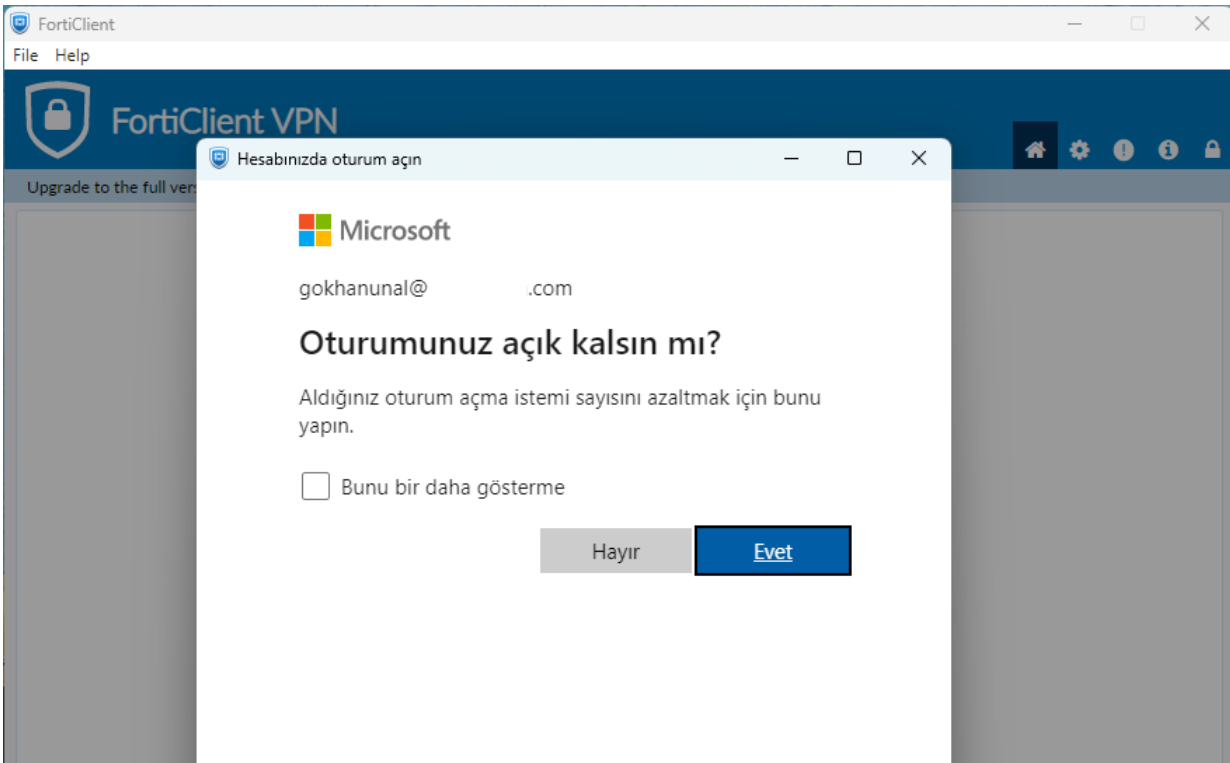
Telefonumuza oturum açma isteęi geliyor.



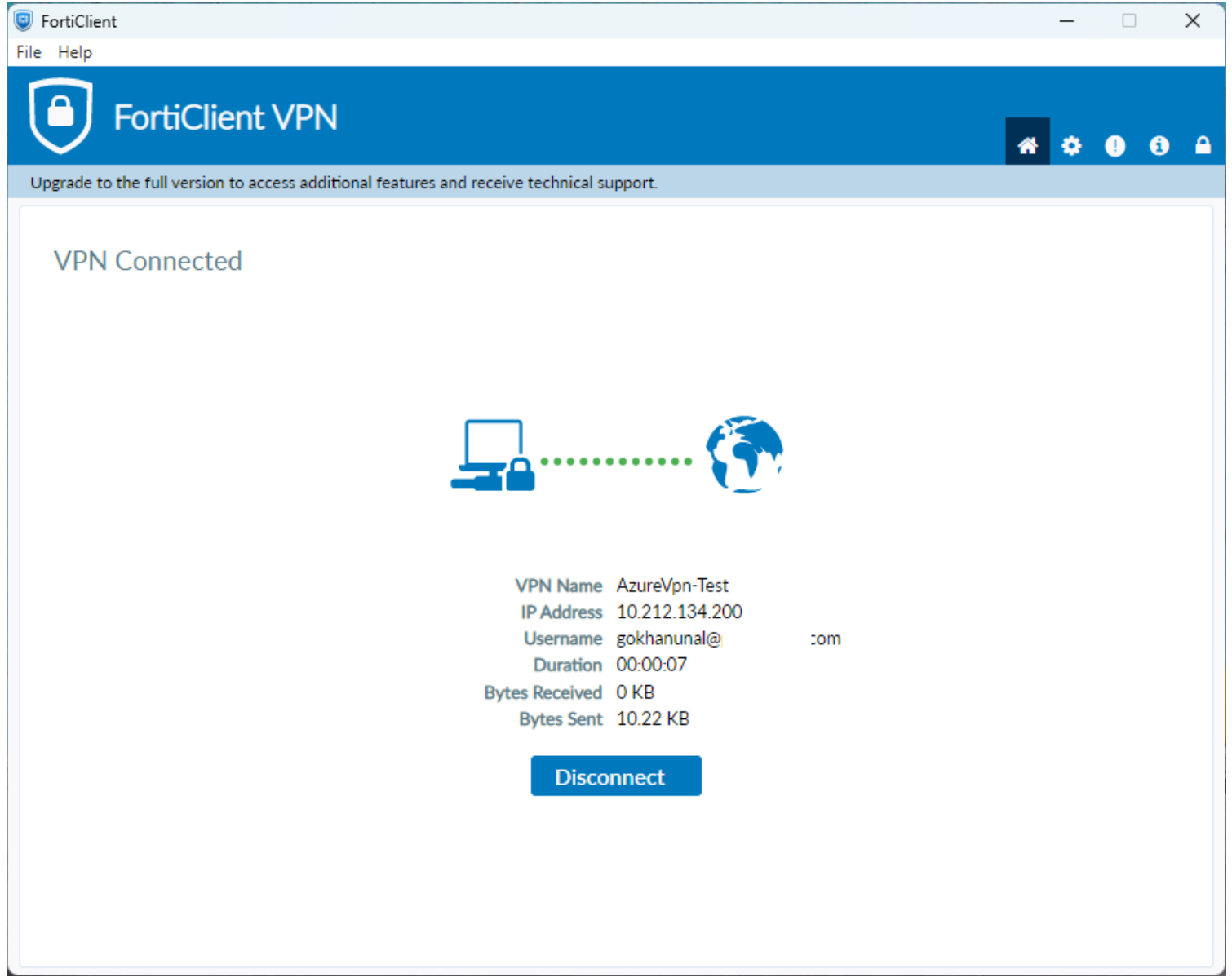




Oturum açık kalsın mı diye soruyor. Evet diyoruz.



Vpn bağlantımız başarıyla gerçekleşiyor.



Başka bir makalede görüşmek üzere.