Two-factor authentication for WatchGuard Access Portal

logintc.com/docs/connectors/watchguard-access-portal

Overview

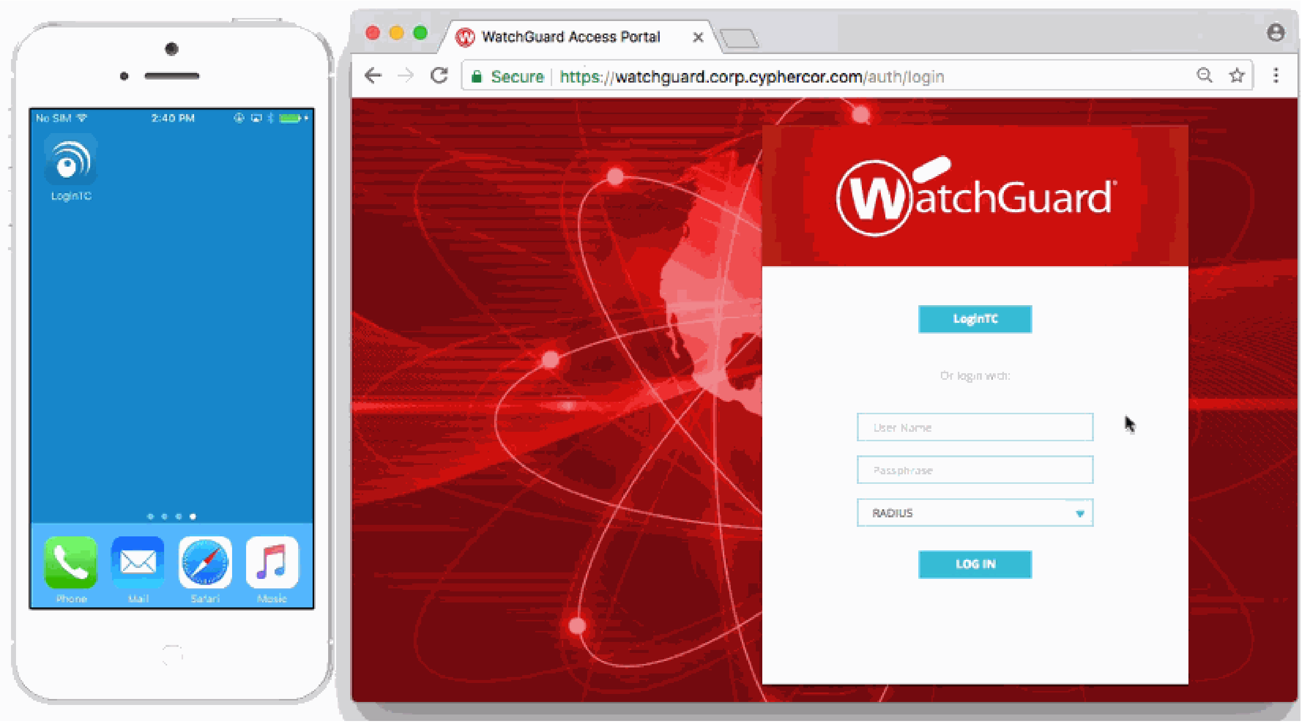
LoginTC protects access to your WatchGuard Access Portal using SAML SSO. The LoginTC AD FS Connector protects access to your Microsoft Active Directory Federation Services (AD FS) by adding a second factor LoginTC challenge to existing username and password authentication. The LoginTC AD FS Connector provides a LoginTC multi-factor authentication (MFA) method to your AD FS deployment, used by your WatchGuard Access Portal.

Subscription Requirement

Your organization requires the **Business** or **Enterprise** plan to use the LoginTC AD FS Connector. See the Pricing page for more information about subscription options.

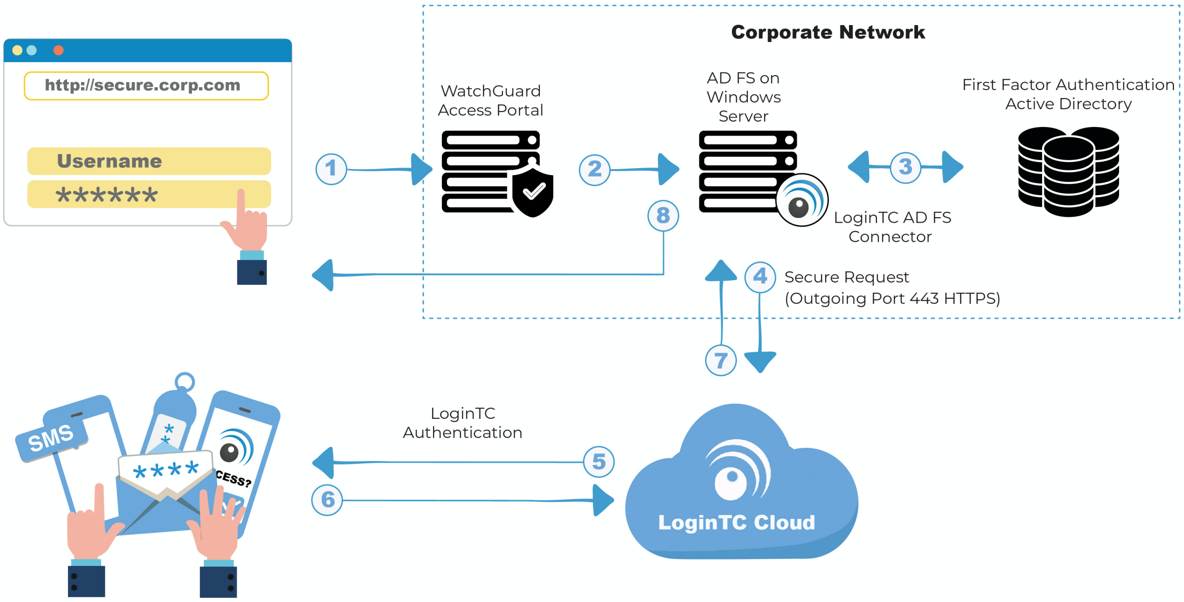
User Experience

After clicking on `LoginTC` from the WatchGuard Access Portal and entering the username and password into the AD FS login page, the user is shown a selection of second factor options. The user clicks a button to receive a LoginTC push notification, authenticates and is logged in.



- LoginTC Push
- OTP

Architecture



Authentication Flow

1. A user attempts access to WatchGuard Access Portal with username / password
2. A SAML request is made to AD FS
3. The username / password is verified against an existing first factor directory (i.e. Active Directory)
4. The request is trapped by LoginTC AD FS Connector and an authentication request is made to LoginTC Cloud Services
5. Secure push notification request sent to the user's mobile or desktop device
6. User response (approval or denial of request) sent to LoginTC Cloud Services
7. The LoginTC AD FS Connector validates the user response
8. User is granted access to WatchGuard Access Portal

Prerequisites

Before proceeding, please ensure you have the following:

- WatchGuard appliance with Access Portal support
- WatchGuard Fireware 12.1.1
- LoginTC Admin Panel account
- Active Directory Federation Services (AD FS) Host, Microsoft Windows Server 2016 (or Windows Server 2012)
- WatchGuard Access Portal configured with federation to your on-premise AD FS

WatchGuard Resources:

Working WatchGuard Access Portal Federation Deployment

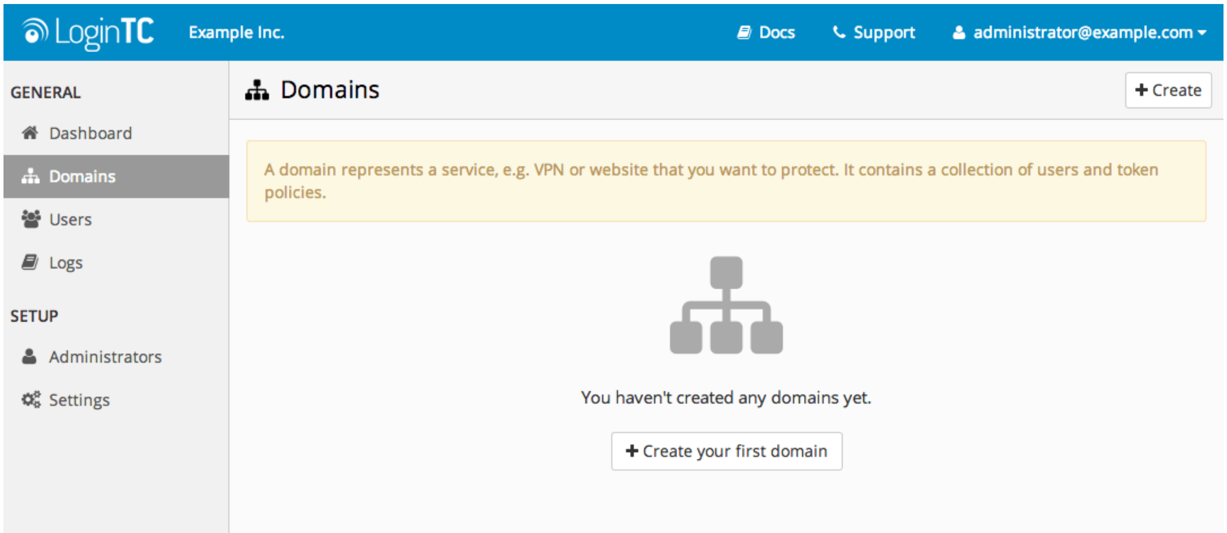
It is strongly recommended that you have a working WatchGuard Access Portal with federation against your on-premise AD FS prior to adding LoginTC multi-factor authentication.

LoginTC Domain Creation

Create a LoginTC domain in LoginTC Admin Panel. The domain represents a service (e.g. your corporate AD FS) that you want to protect with LoginTC. It will contain token policies and the users that access your service.

If you have already created a LoginTC domain for your AD FS deployment, then you may skip this section and proceed to Installation.

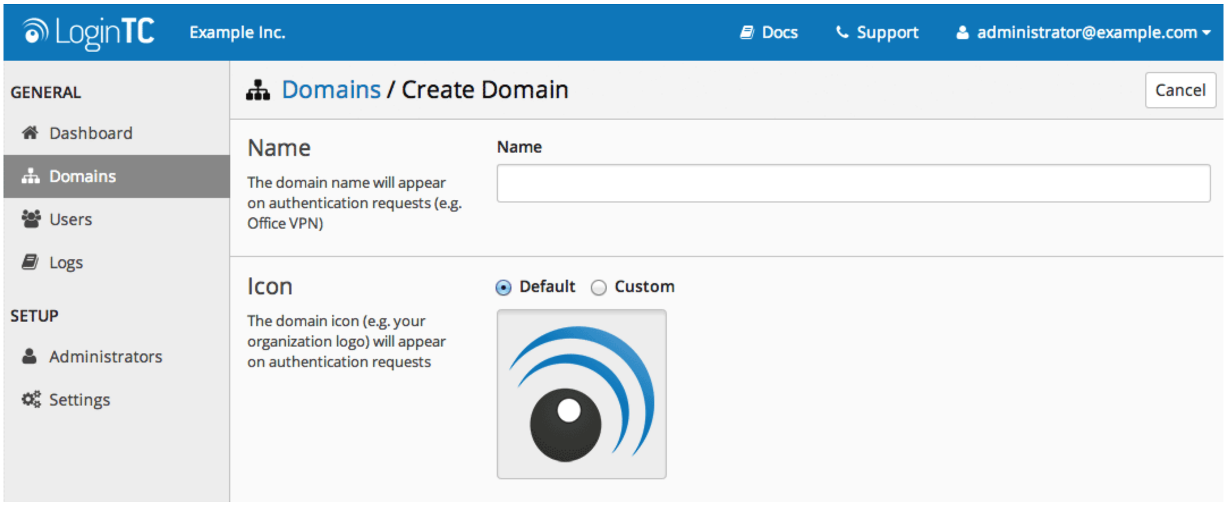
1. Log in to LoginTC Admin
2. Click **Domains**:
3. Click **Create Domain**:



A domain represents a service, e.g. VPN or website that you want to protect. It contains a collection of users and token policies.

You haven't created any domains yet.

4. Enter a name and optionally pick an icon



Name

The domain name will appear on authentication requests (e.g. Office VPN)

Name

Icon

The domain icon (e.g. your organization logo) will appear on authentication requests

● Default ○ Custom

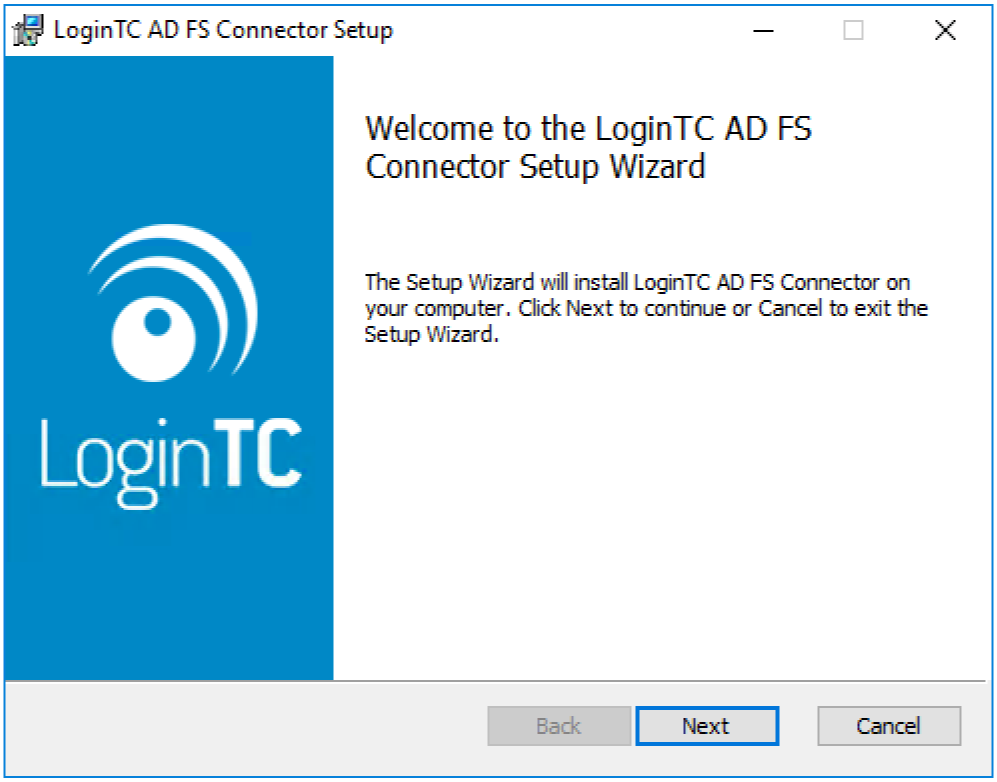
5. Scroll down and click **Create**

Use Default Domain Settings

Domain settings can be modified at any time by navigating to **Domains > Your Domain > Settings**.

Installation

1. Download the latest version of the LoginTC AD FS Connector
2. Run the installer file as a privileged administrator user on the Windows Server with the AD FS role. Also ensure that the AD FS service is running prior to installing.
3. Press **Next**

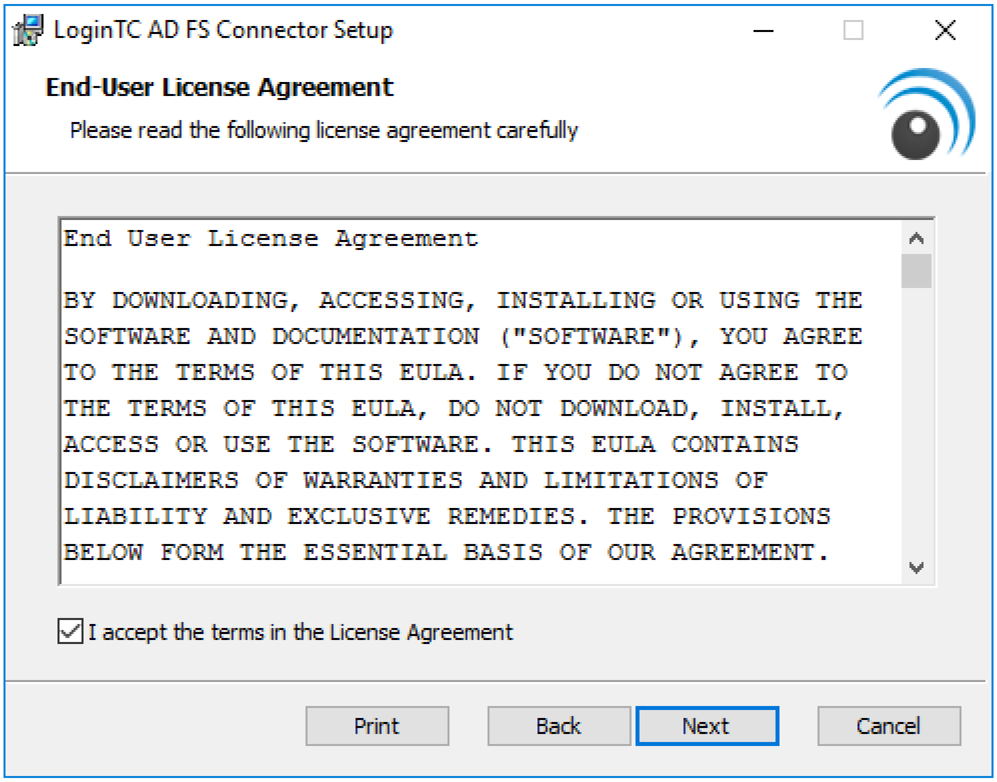


LoginTC AD FS Connector Setup

Welcome to the LoginTC AD FS Connector Setup Wizard

The Setup Wizard will install LoginTC AD FS Connector on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

4. Read the License Agreement and press **Next** if you accept the terms.



LoginTC AD FS Connector Setup

End-User License Agreement

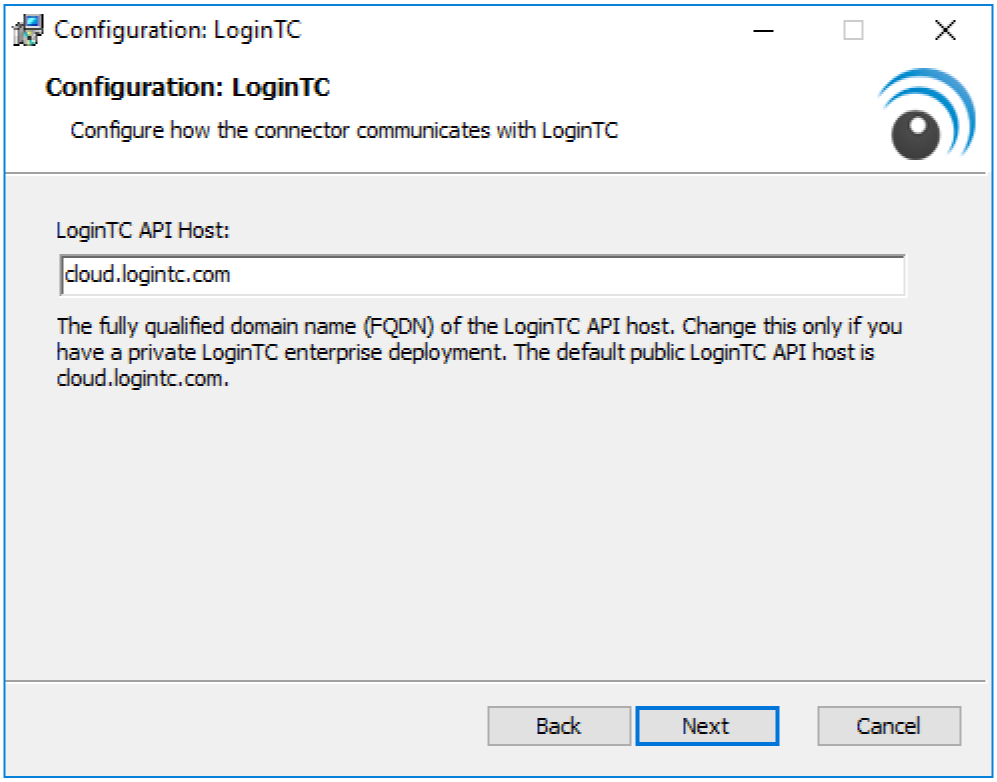
Please read the following license agreement carefully

```
End User License Agreement

BY DOWNLOADING, ACCESSING, INSTALLING OR USING THE
SOFTWARE AND DOCUMENTATION ("SOFTWARE"), YOU AGREE
TO THE TERMS OF THIS EULA. IF YOU DO NOT AGREE TO
THE TERMS OF THIS EULA, DO NOT DOWNLOAD, INSTALL,
ACCESS OR USE THE SOFTWARE. THIS EULA CONTAINS
DISCLAIMERS OF WARRANTIES AND LIMITATIONS OF
LIABILITY AND EXCLUSIVE REMEDIES. THE PROVISIONS
BELOW FORM THE ESSENTIAL BASIS OF OUR AGREEMENT.
```

☑ I accept the terms in the License Agreement

5. Change the **LoginTC API Host** only if you have a private enterprise LoginTC deployment. Press **Next**:



Configuration: LoginTC

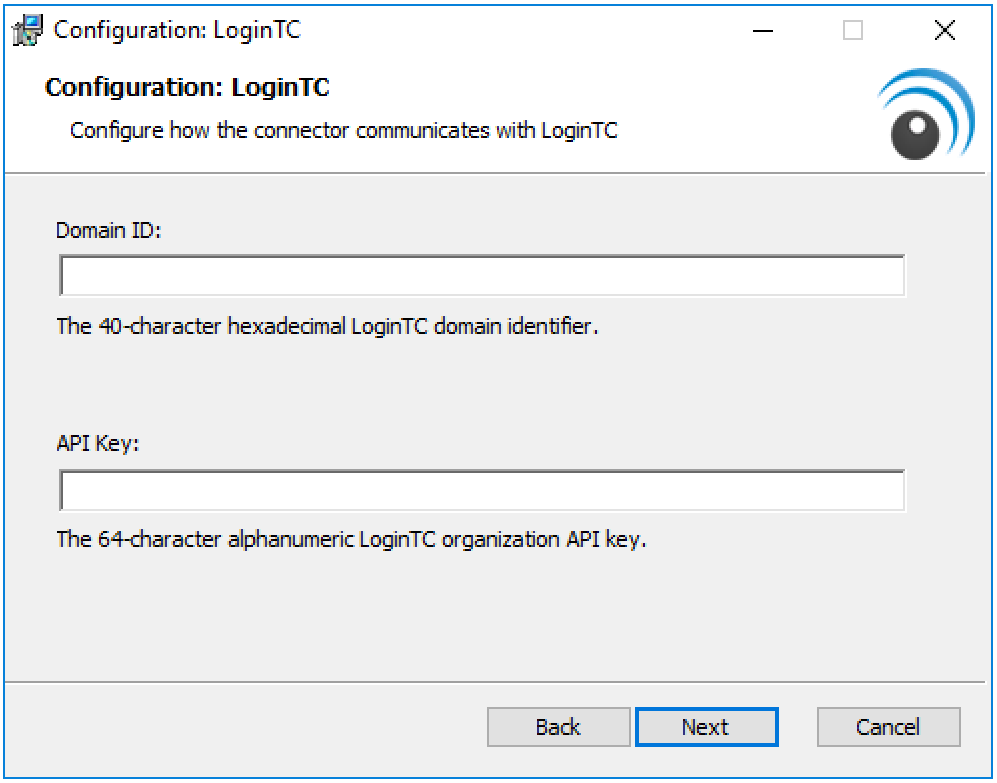
Configuration: LoginTC

Configure how the connector communicates with LoginTC

LoginTC API Host: cloud.logintc.com

The fully qualified domain name (FQDN) of the LoginTC API host. Change this only if you have a private LoginTC enterprise deployment. The default public LoginTC API host is cloud.logintc.com.

6. Enter your LoginTC **Domain ID** and **Organization API Key**. These values are found on your LoginTC Admin Panel. Press **Next**



Configuration: LoginTC

Configuration: LoginTC

Configure how the connector communicates with LoginTC

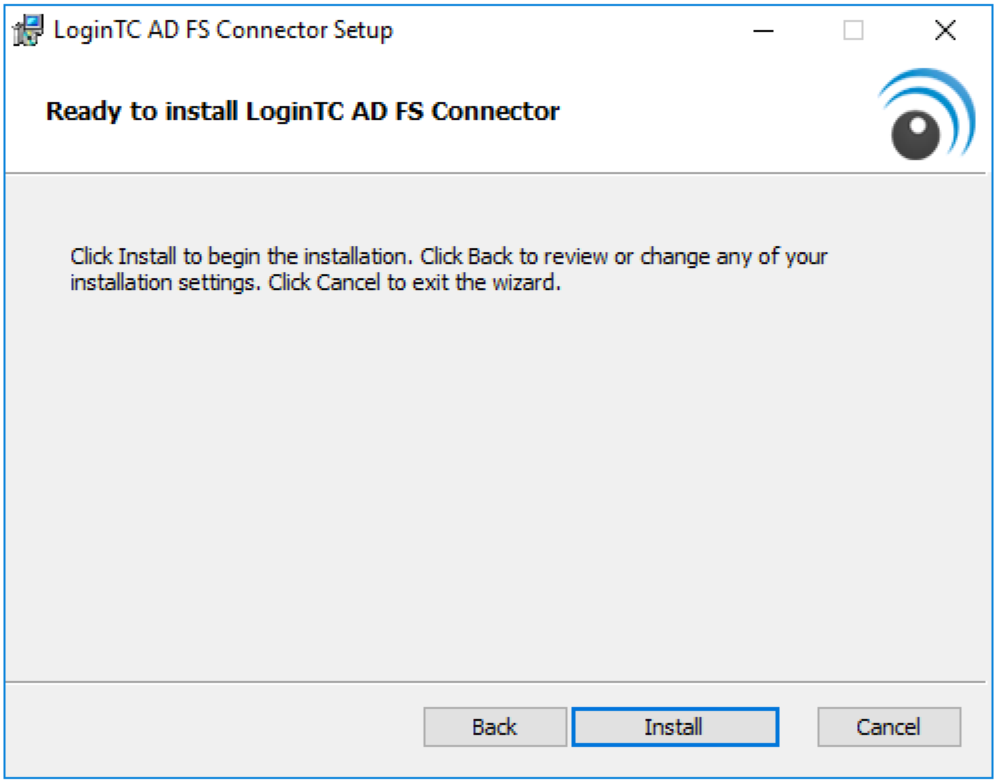
Domain ID:

The 40-character hexadecimal LoginTC domain identifier.

API Key:

The 64-character alphanumeric LoginTC organization API key.

7. Press **Install**. Note that the AD FS service will be restarted during installation and may be temporarily unavailable to your users.



LoginTC AD FS Connector Setup

Ready to install LoginTC AD FS Connector

Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

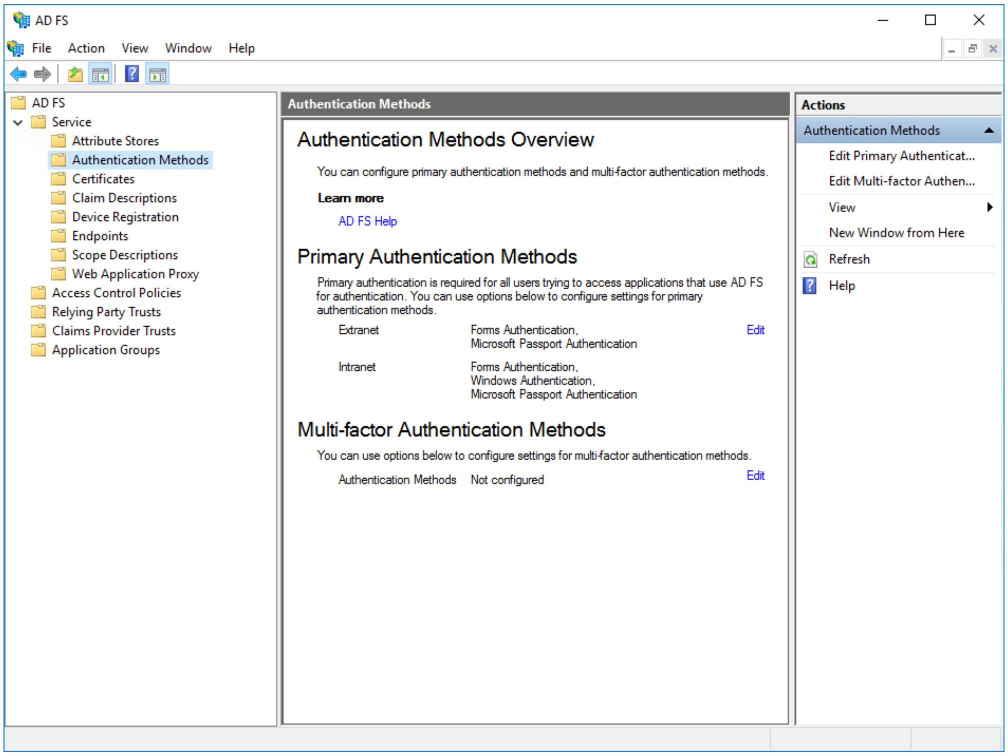
AD FS LoginTC MFA Configuration

Windows Server 2016 (AD FS version 4.0)

The instructions below are for AD FS (version 4.0) running on Windows Server 2016. If you have AD FS (3.0) running on Windows Server 2012 R2, see AD FS Configuration in Two-factor authentication for AD FS on Windows Server 2012 R2.

To configure your AD FS to use the LoginTC MFA method:

1. Open the **AD FS Management** console.
2. Click on the **Services > Authentication Policies** directory in the left side menu.



Authentication Methods Overview

You can configure primary authentication methods and multi-factor authentication methods.

Learn more

AD FS Help

Primary Authentication Methods

Primary authentication is required for all users trying to access applications that use AD FS for authentication. You can use options below to configure settings for primary authentication methods.

Extranet	Forms Authentication, Microsoft Passport Authentication	Edit
Intranet	Forms Authentication, Windows Authentication, Microsoft Passport Authentication	

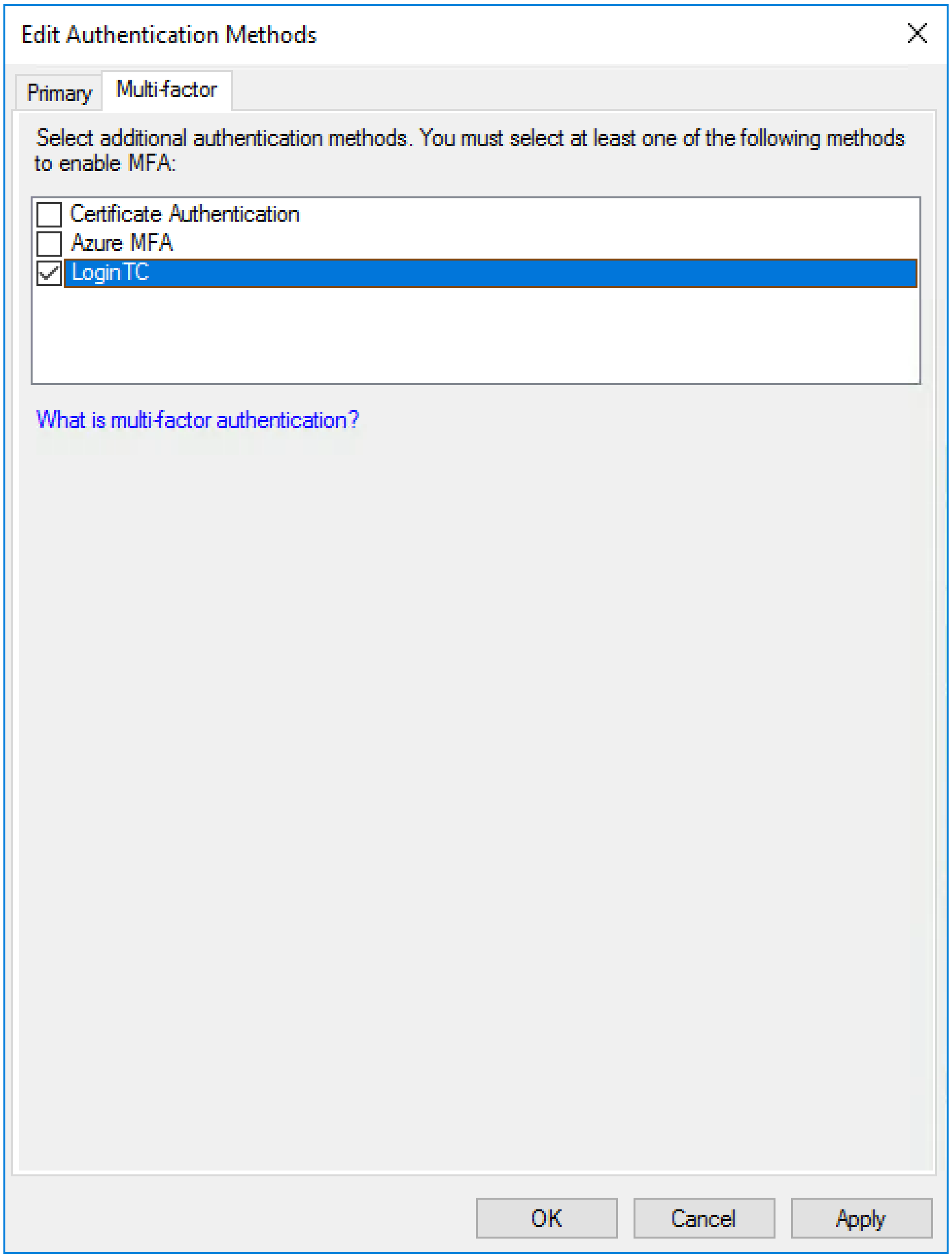
Multi-factor Authentication Methods

You can use options below to configure settings for multi-factor authentication methods.

Authentication Methods	Not configured	Edit

3. Click on **Edit Global Multi-factor Authentication…**

4. Check **LoginTC** in the list of MFA methods.



Edit Authentication Methods

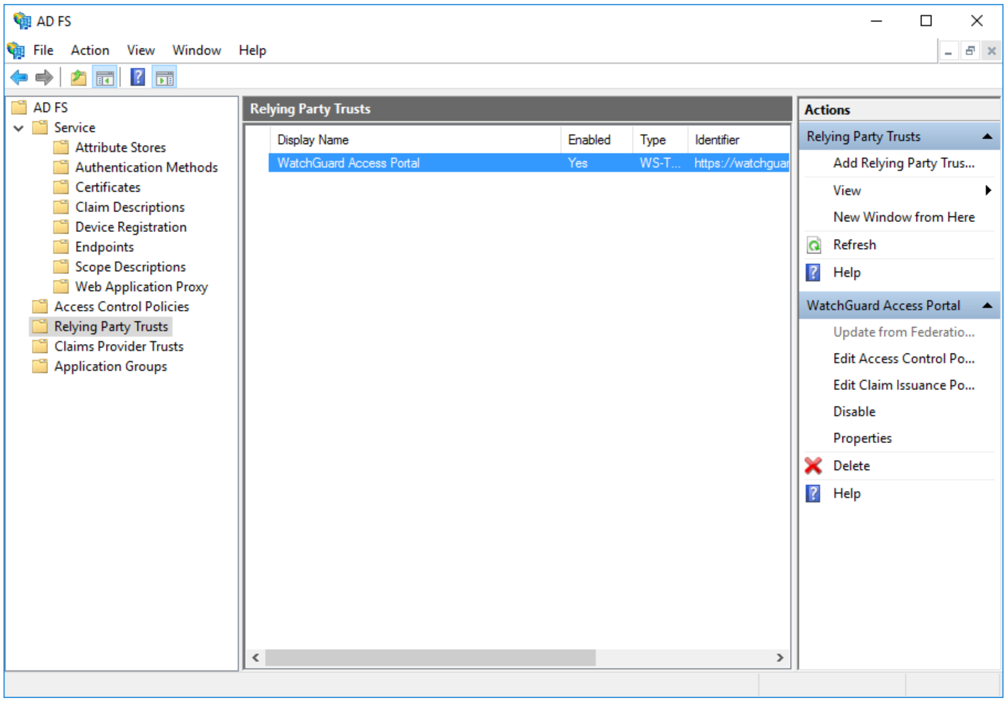
Select additional authentication methods. You must select at least one of the following methods to enable MFA:

☐ Certificate Authentication
☐ Azure MFA
☑ LoginTC

5. Press **Apply** then **Ok**
6. Click on **Relying Party Trusts** in the left side menu
7. Select the Relying Party you wish to add LoginTC MFA to

   Don’t have a Relying Party for WatchGuard Access Portal setup yet?
   For instructions on configuring a Relying Party for Access Portal see sections WatchGuard Access Portal Configuration and AD FS Relying Party.

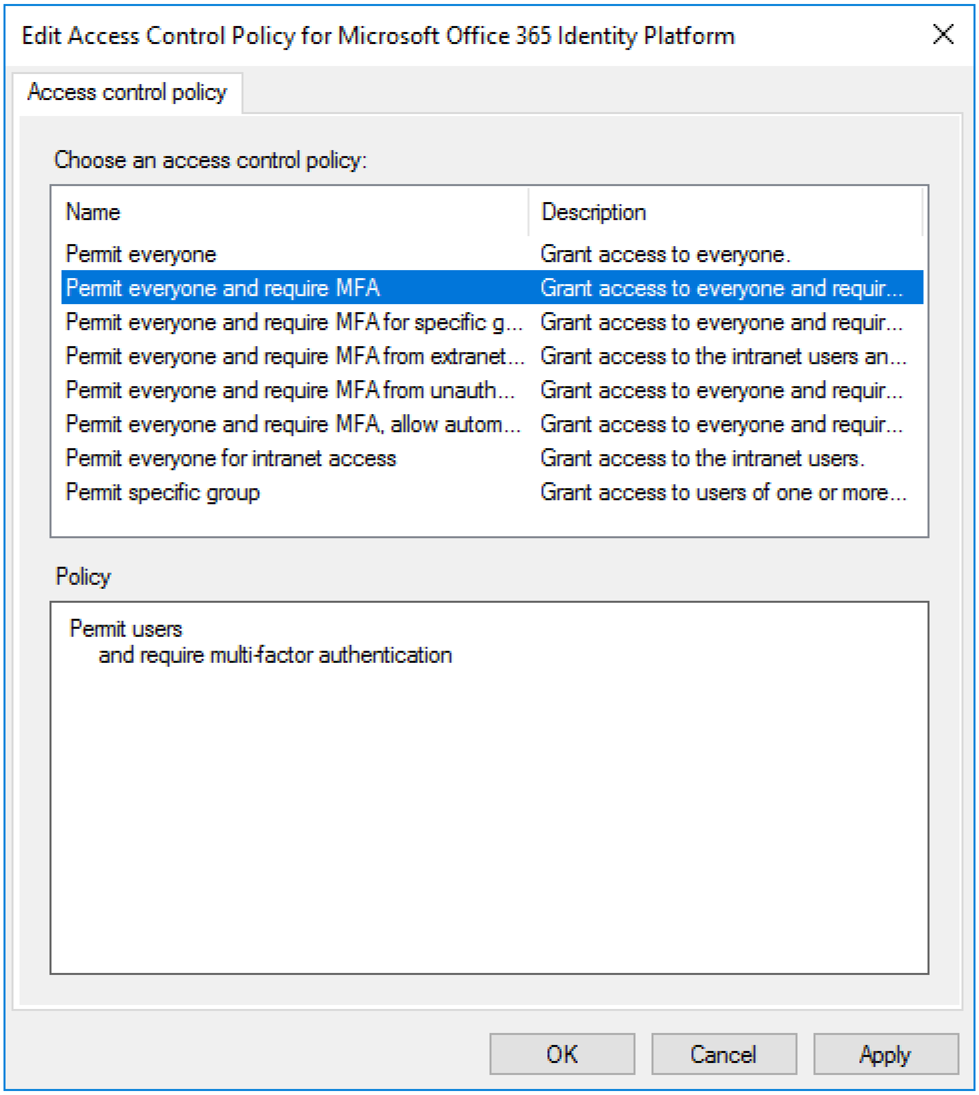
8. Click on **Edit Access Control Policy…** under Actions in the right sidebar



Display Name	Enabled	Type	Identifier
WatchGuard Access Portal	Yes	WS-T...	https://watchguar

9. Select an access control policy that uses MFA (e.g. **Permit everyone and require MFA**)

10. Press **Apply** and **OK**



Edit Access Control Policy for Microsoft Office 365 Identity Platform

Access control policy

Choose an access control policy:

Name	Description
Permit everyone	Grant access to everyone.
Permit everyone and require MFA	Grant access to everyone and requir...
Permit everyone and require MFA for specific g...	Grant access to everyone and requir...
Permit everyone and require MFA from extranet...	Grant access to the intranet users an...
Permit everyone and require MFA from unauth...	Grant access to everyone and requir...
Permit everyone and require MFA, allow autom...	Grant access to everyone and requir...
Permit everyone for intranet access	Grant access to the intranet users.
Permit specific group	Grant access to users of one or more...

Policy

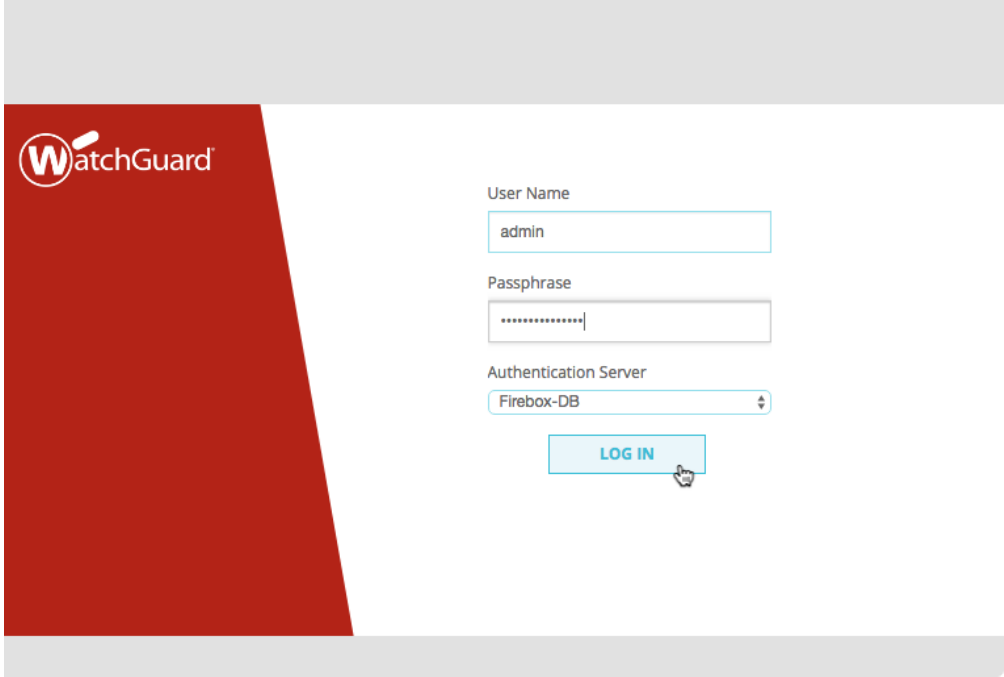
Permit users
and require multi-factor authentication

Your AD FS login will now present the user with a secondary LoginTC authentication page.

Configuration for WatchGuard Access Portal 2FA

Configure WatchGuard Access Portal for SAML Single Sign-On (SSO):

1. Log in to your WatchGuard Fireware Web UI:

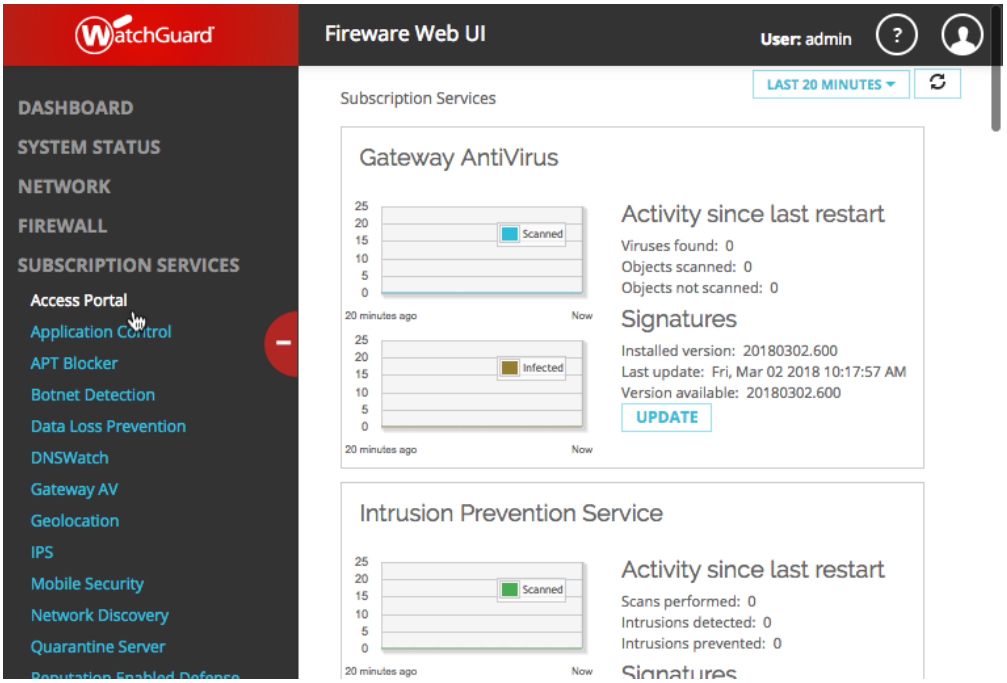


User Name: admin

Passphrase: •••••••••••••••

Authentication Server: Firebox-DB

2. Under **Subscription Services** click **Access Portal**:



Gateway AntiVirus

Activity since last restart

Viruses found: 0
Objects scanned: 0
Objects not scanned: 0

Signatures

Installed version: 20180302.600
Last update: Fri, Mar 02 2018 10:17:57 AM
Version available: 20180302.600

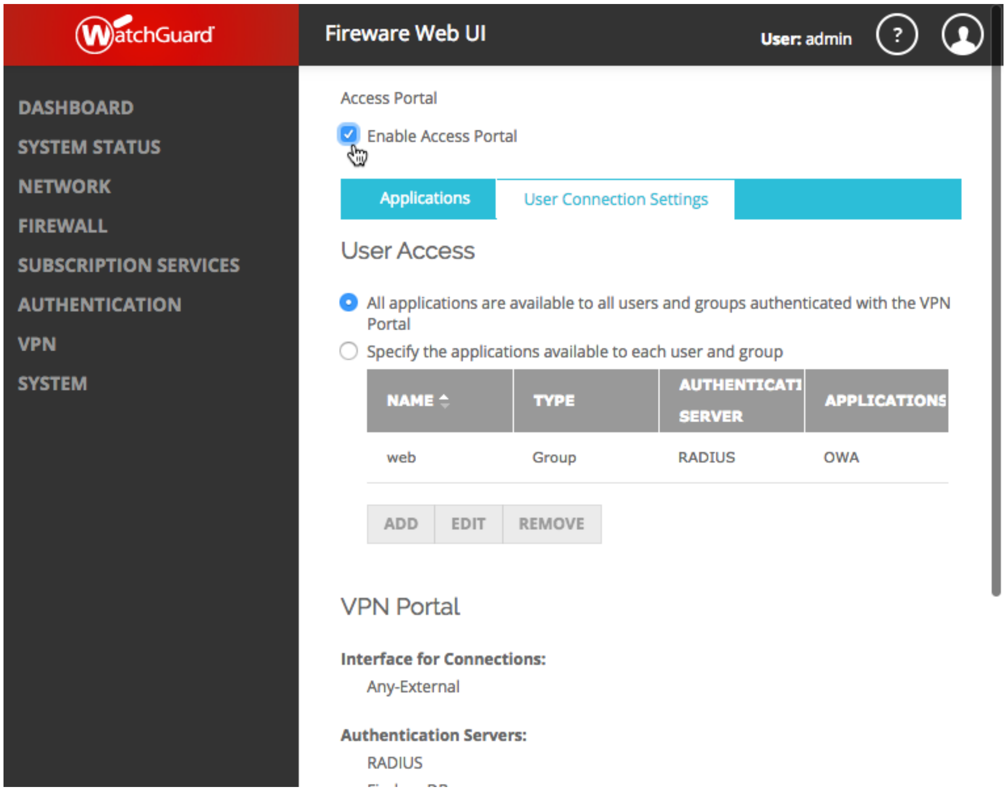
Intrusion Prevention Service

Activity since last restart

Scans performed: 0
Intrusions detected: 0
Intrusions prevented: 0

Signatures

3. Click **Enable Access Portal**:



Access Portal

☑ Enable Access Portal

User Access

● All applications are available to all users and groups authenticated with the VPN Portal

○ Specify the applications available to each user and group

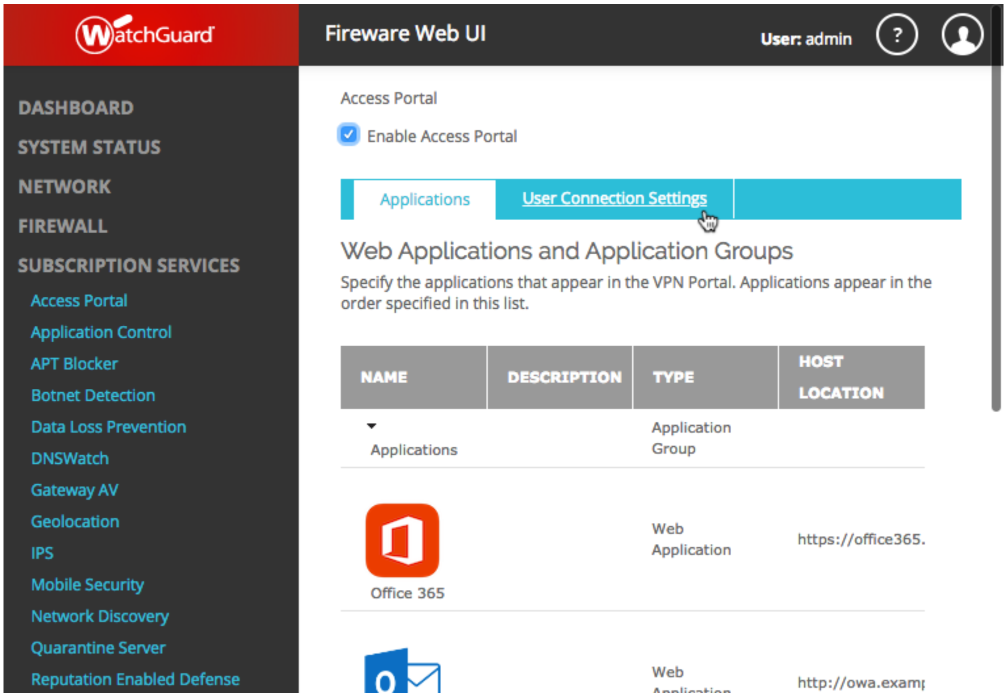
NAME	TYPE	AUTHENTICATI SERVER	APPLICATIONS
web	Group	RADIUS	OWA

VPN Portal

Interface for Connections:
Any-External

Authentication Servers:
RADIUS

4. Click on the **User Connection Settings** tab:



Access Portal

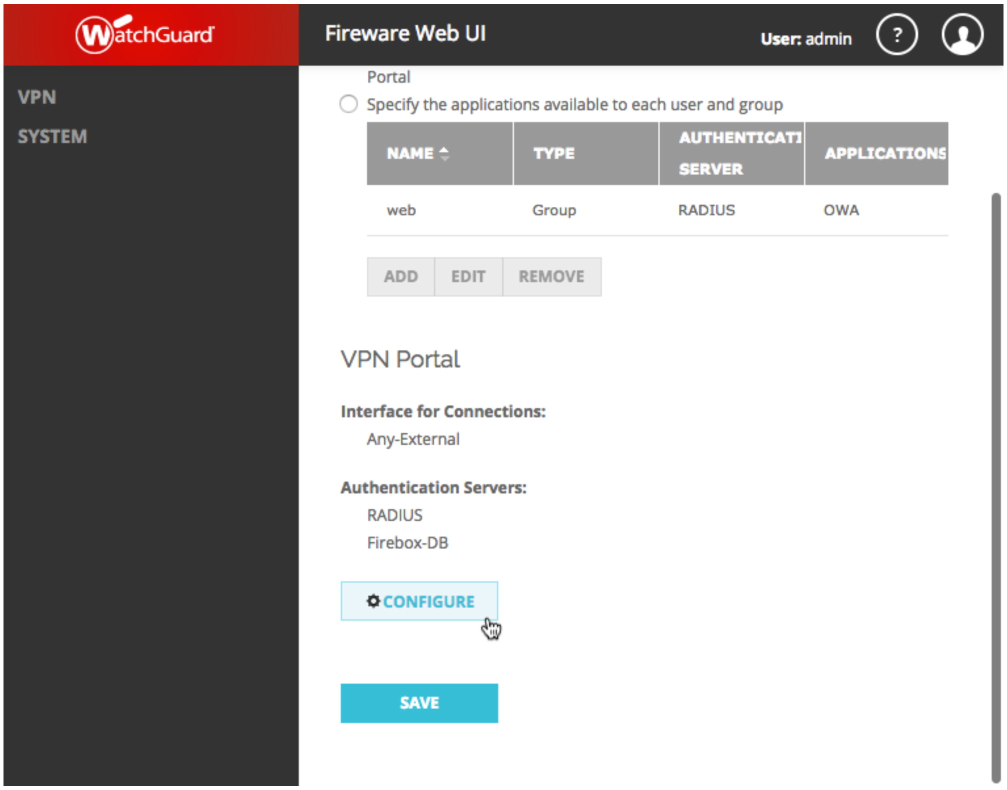
☑ Enable Access Portal

Web Applications and Application Groups

Specify the applications that appear in the VPN Portal. Applications appear in the order specified in this list.

NAME	DESCRIPTION	TYPE	HOST LOCATION
Applications		Application Group	
Office 365		Web Application	https://office365.
		Web	http://owa.examp

5. Scroll down and click **Configure**:



Portal

○ Specify the applications available to each user and group

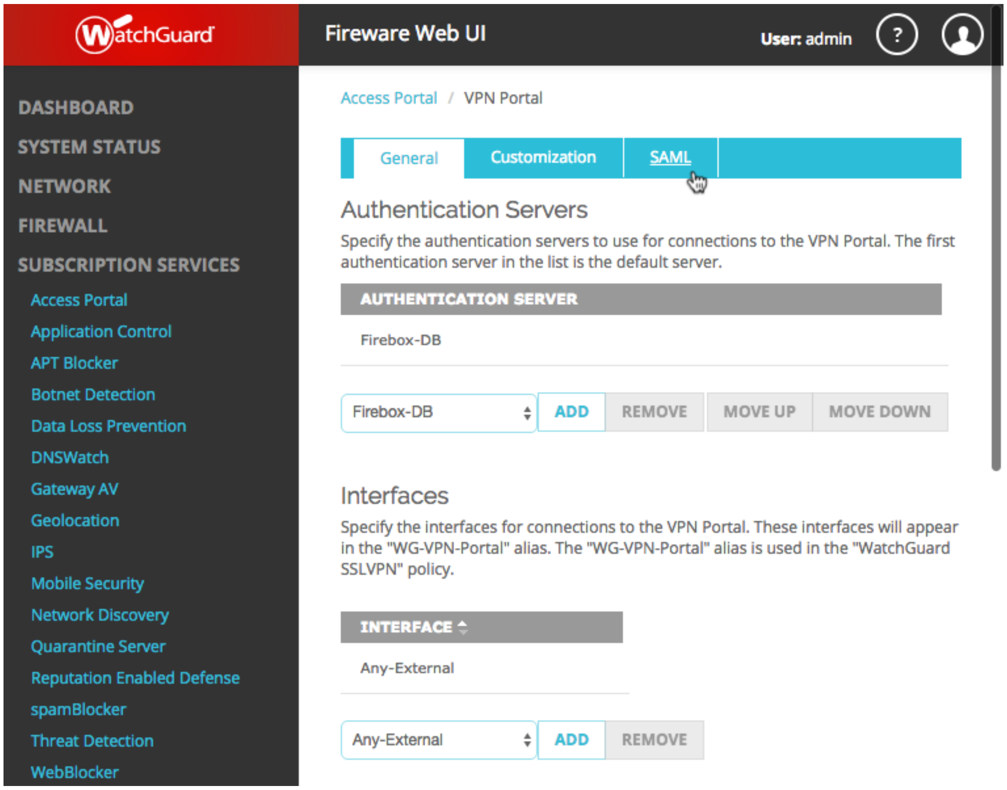
NAME	TYPE	AUTHENTICATI SERVER	APPLICATIONS
web	Group	RADIUS	OWA

VPN Portal

Interface for Connections:
Any-External

Authentication Servers:
RADIUS
Firebox-DB

6. Click on the **SAML** tab:



Access Portal / VPN Portal

Authentication Servers

Specify the authentication servers to use for connections to the VPN Portal. The first authentication server in the list is the default server.

AUTHENTICATION SERVER
Firebox-DB

Firebox-DB

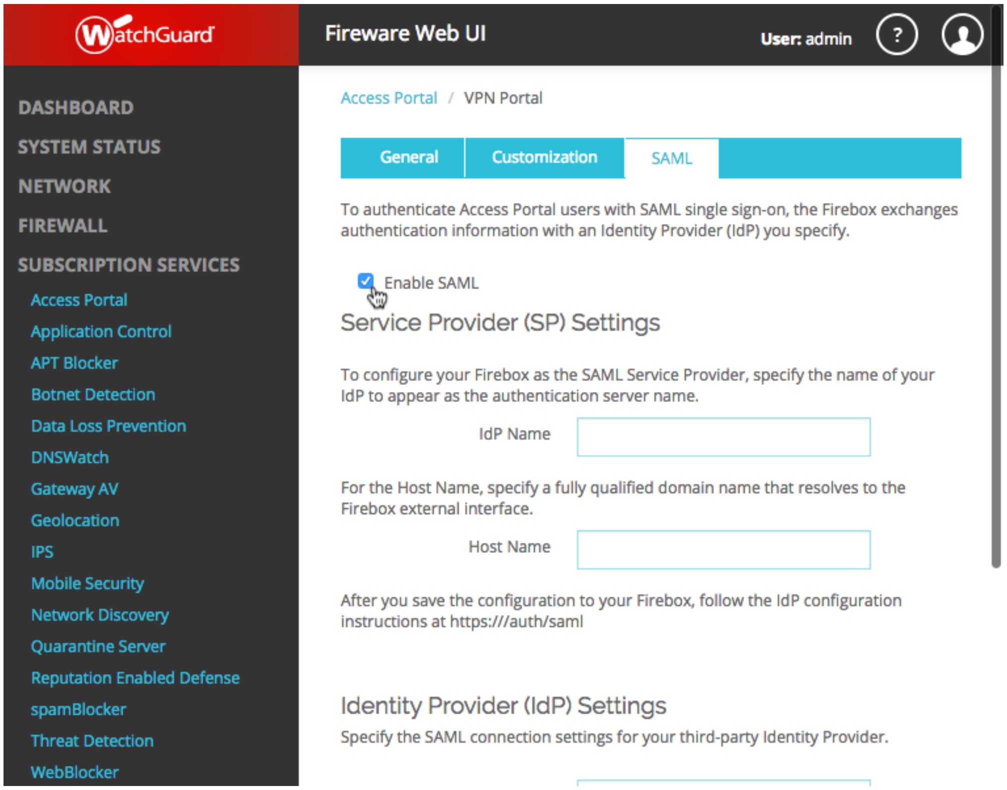
Interfaces

Specify the interfaces for connections to the VPN Portal. These interfaces will appear in the "WG-VPN-Portal" alias. The "WG-VPN-Portal" alias is used in the "WatchGuard SSLVPN" policy.

INTERFACE
Any-External

Any-External

7. Click **Enable SAML**:



To authenticate Access Portal users with SAML single sign-on, the Firebox exchanges authentication information with an Identity Provider (IdP) you specify.

☑ Enable SAML

Service Provider (SP) Settings

To configure your Firebox as the SAML Service Provider, specify the name of your IdP to appear as the authentication server name.

IdP Name

For the Host Name, specify a fully qualified domain name that resolves to the Firebox external interface.

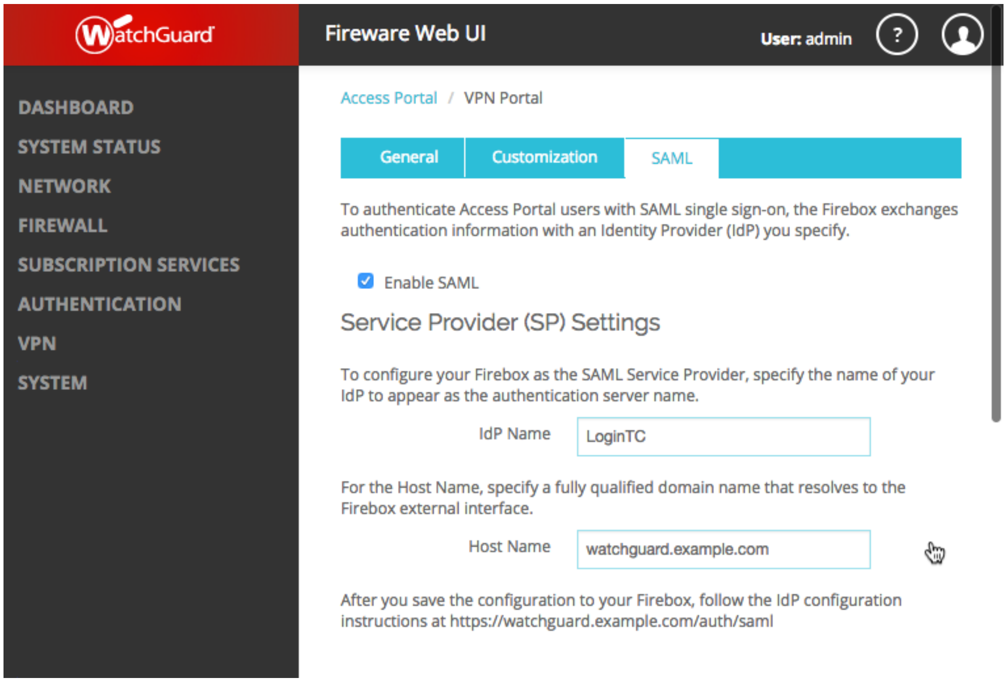
Host Name

After you save the configuration to your Firebox, follow the IdP configuration instructions at https:///auth/saml

Identity Provider (IdP) Settings

Specify the SAML connection settings for your third-party Identity Provider.

8. Complete the Service Provider (SP) Settings configuration:



To authenticate Access Portal users with SAML single sign-on, the Firebox exchanges authentication information with an Identity Provider (IdP) you specify.

☑ Enable SAML

Service Provider (SP) Settings

To configure your Firebox as the SAML Service Provider, specify the name of your IdP to appear as the authentication server name.

IdP Name: LoginTC

For the Host Name, specify a fully qualified domain name that resolves to the Firebox external interface.

Host Name: watchguard.example.com

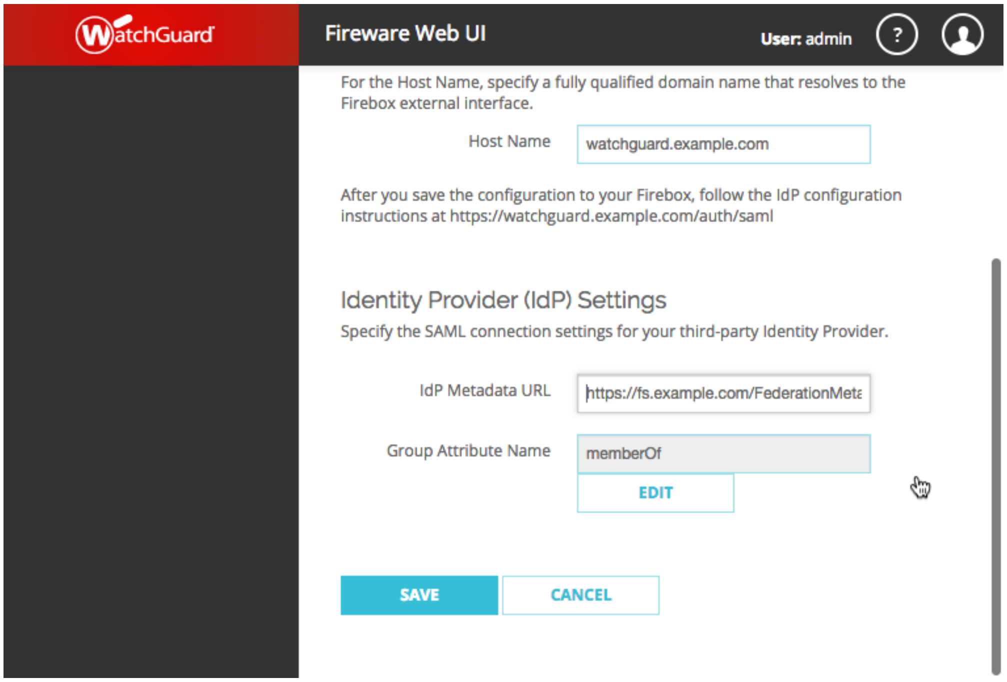
After you save the configuration to your Firebox, follow the IdP configuration instructions at https://watchguard.example.com/auth/saml

Service Provider (SP) Settings:

Property	Explanation	Example

Property	Explanation	Example
`IdP Name`	Name to appear as the authentication server name	LoginTC
`Host Name`	A fully qualified domain name that resolves to the Firebox external interface	watchguard.example.com

8. (Continued) Complete the Service Provider (SP) Settings configuration:



For the Host Name, specify a fully qualified domain name that resolves to the Firebox external interface.

Host Name: watchguard.example.com

After you save the configuration to your Firebox, follow the IdP configuration instructions at https://watchguard.example.com/auth/saml

Identity Provider (IdP) Settings

Specify the SAML connection settings for your third-party Identity Provider.

IdP Metadata URL: https://fs.example.com/FederationMeta

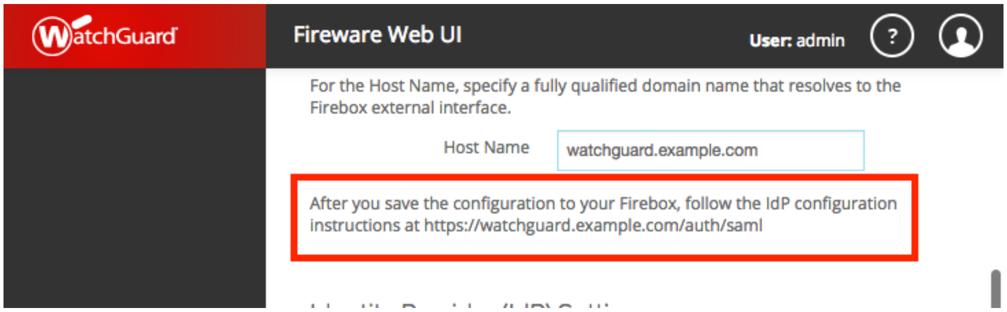
Group Attribute Name: memberOf

Identity Provider (IdP) Settings

Property	Explanation	Example
`IdP Metadata URL`	AD FS Federation Metadata URL	https://fs.example.com/FederationMetadata/2007-06/FederationMetadata.xml
`Group Attribute Name`	The name of the attribute returning group claims	memberOf

9. Click **SAVE**

10. Navigate to **SAML 2.0 Configuration for WatchGuard Access Portal** page (i.e. https://watchguard.example.com/auth.saml):

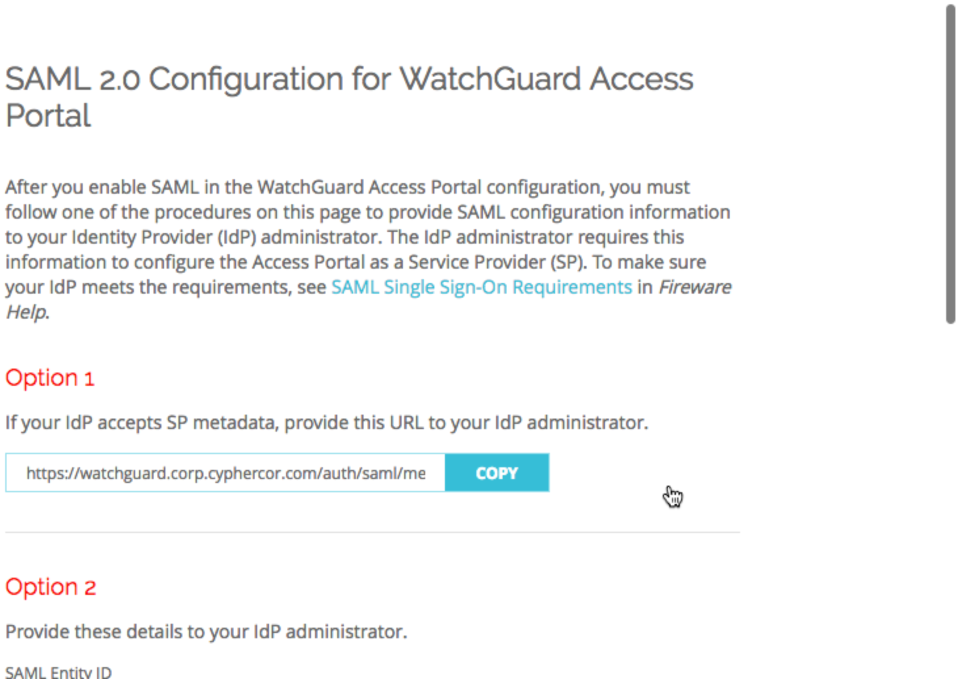


For the Host Name, specify a fully qualified domain name that resolves to the Firebox external interface.

Host Name: watchguard.example.com

After you save the configuration to your Firebox, follow the IdP configuration instructions at https://watchguard.example.com/auth/saml

11. Copy the SP metadata URL found under **Option 1** and paste in your browser. Save the file as `metadata.xml`.



SAML 2.0 Configuration for WatchGuard Access Portal

After you enable SAML in the WatchGuard Access Portal configuration, you must follow one of the procedures on this page to provide SAML configuration information to your Identity Provider (IdP) administrator. The IdP administrator requires this information to configure the Access Portal as a Service Provider (SP). To make sure your IdP meets the requirements, see SAML Single Sign-On Requirements in *Fireware Help*.

Option 1

If your IdP accepts SP metadata, provide this URL to your IdP administrator.

https://watchguard.corp.cyphercor.com/auth/saml/me

Option 2

Provide these details to your IdP administrator.

SAML Entity ID

WatchGuard SAML Configuration

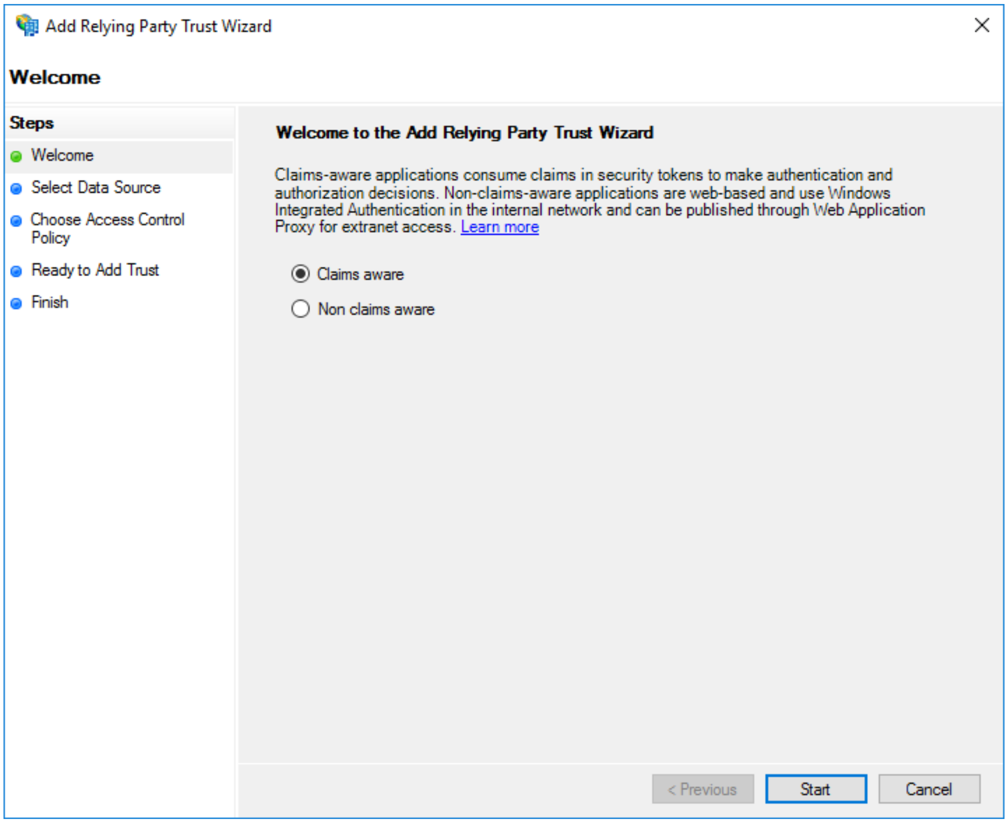
WatchGuard Access Portal is now configured to use your AD FS server to perform authentication. In the next section the `metadata.xml` file will be used to configure AD FS to properly authenticate WatchGuard Access Portal requests.

AD FS Relying Party

To configure a WatchGuard Access Portal Relying Party in AD FS:

1. Open the **AD FS Management** console.
2. Click on **Relying Party Trusts** in the left side menu
3. Click on **Add Relying Party Trust…**

4. Select **Claims Aware**



Add Relying Party Trust Wizard

Welcome

Welcome to the Add Relying Party Trust Wizard

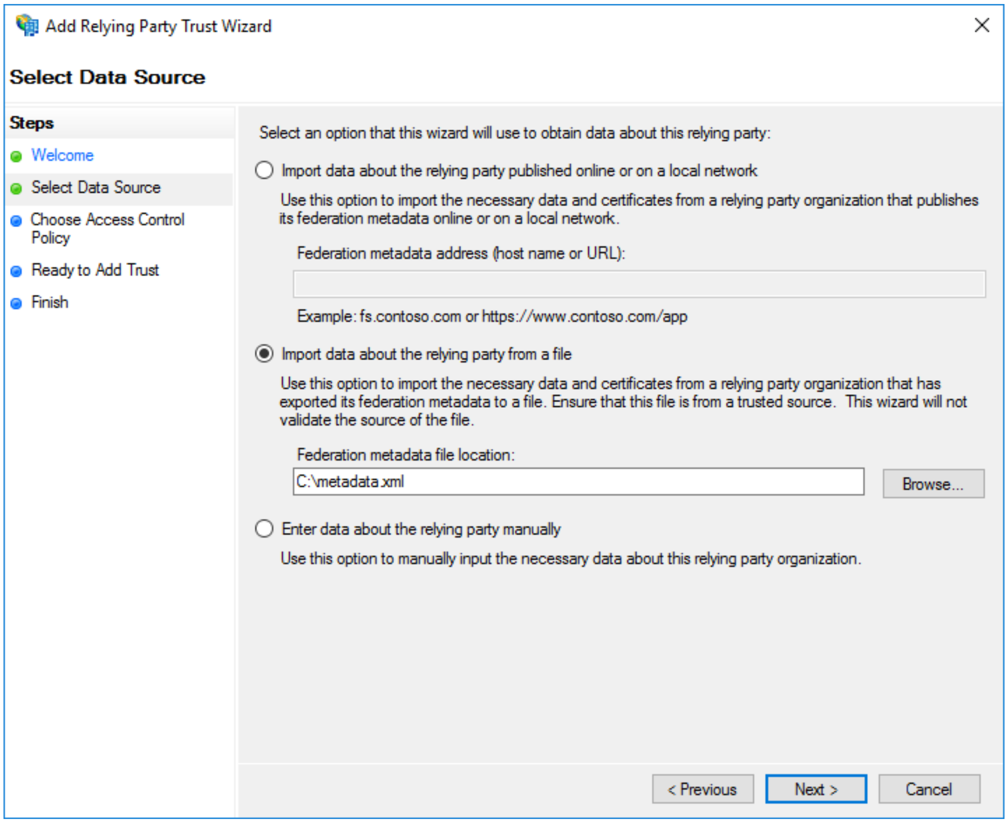
Claims-aware applications consume claims in security tokens to make authentication and authorization decisions. Non-claims-aware applications are web-based and use Windows Integrated Authentication in the internal network and can be published through Web Application Proxy for extranet access. Learn more

● Claims aware

○ Non claims aware

5. Click **Start**

6. Select **Import data about the relying party from a file** and then browse the where `metadata.xml` from the final section of WatchGuard Access Portal Configuration is saved.



Add Relying Party Trust Wizard

Select Data Source

Steps
- Welcome
- Select Data Source
- Choose Access Control Policy
- Ready to Add Trust
- Finish

Select an option that this wizard will use to obtain data about this relying party:

○ Import data about the relying party published online or on a local network

Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.

Federation metadata address (host name or URL):

Example: fs.contoso.com or https://www.contoso.com/app

● Import data about the relying party from a file

Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.

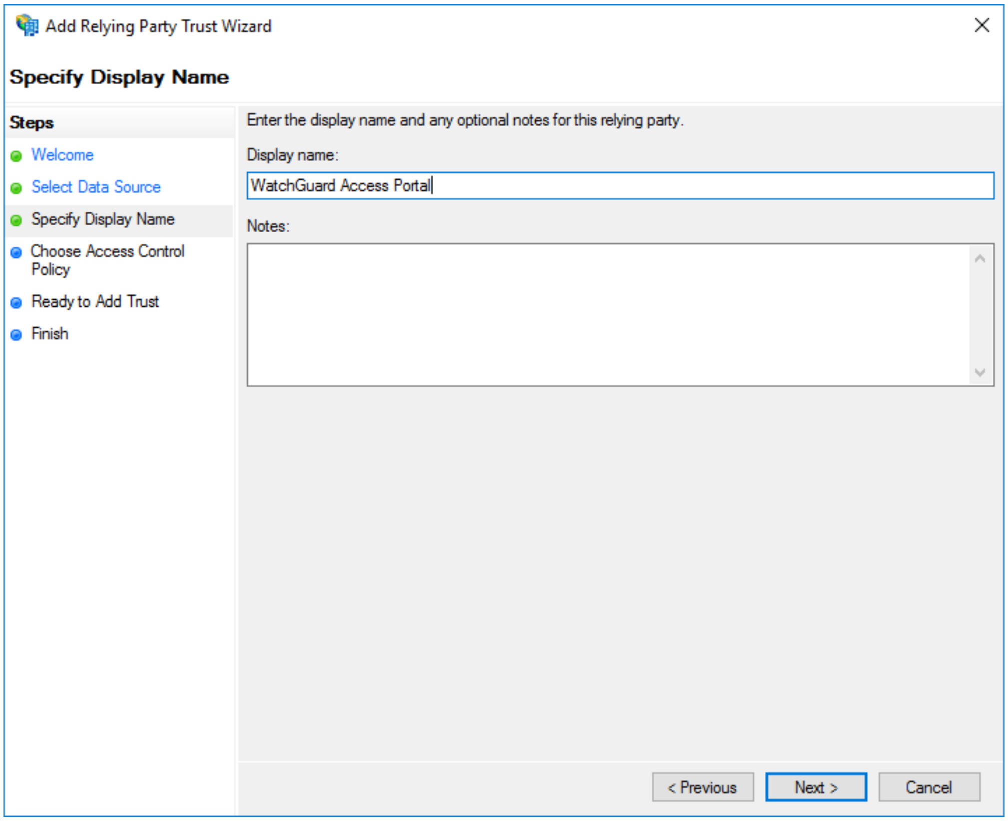
Federation metadata file location: C:\metadata.xml

○ Enter data about the relying party manually

Use this option to manually input the necessary data about this relying party organization.

7. Click **Next**

8. Enter a **Display name** (for example: `WatchGuard Access Portal`):



Add Relying Party Trust Wizard

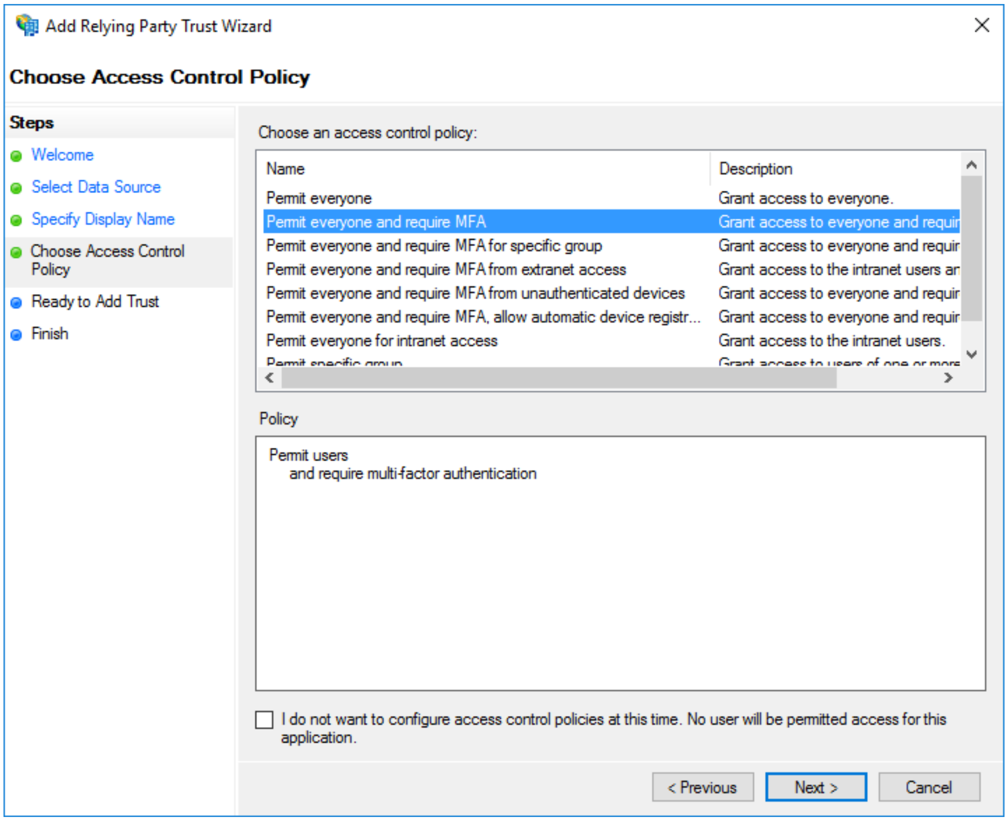
Specify Display Name

Enter the display name and any optional notes for this relying party.

Display name: WatchGuard Access Portal

Notes:

9. Click **Next**
10. Under **Choose an access control policy** select **Permit everyone and require MFA**



Add Relying Party Trust Wizard

Choose Access Control Policy

Choose an access control policy:

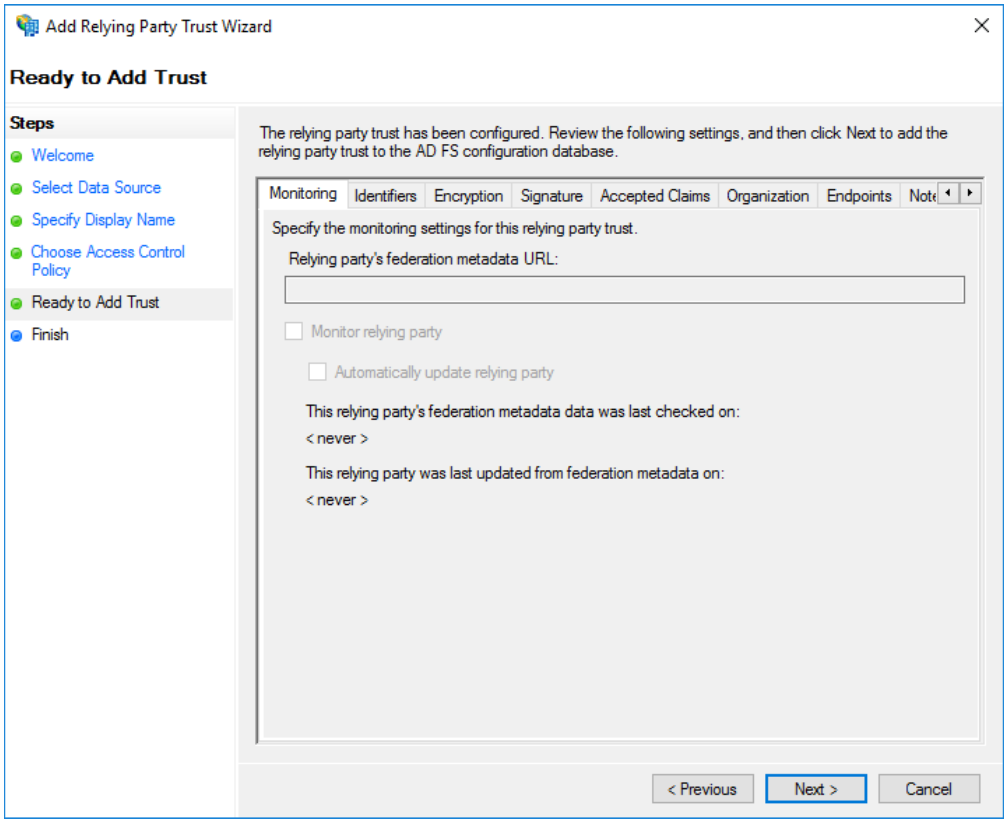
Name	Description
Permit everyone	Grant access to everyone.
Permit everyone and require MFA	Grant access to everyone and requir
Permit everyone and require MFA for specific group	Grant access to everyone and requir
Permit everyone and require MFA from extranet access	Grant access to the intranet users ar
Permit everyone and require MFA from unauthenticated devices	Grant access to everyone and requir
Permit everyone and require MFA, allow automatic device registr...	Grant access to everyone and requir
Permit everyone for intranet access	Grant access to the intranet users.
Permit specific group	Grant access to users of one or more

Policy

Permit users
and require multi-factor authentication

☐ I do not want to configure access control policies at this time. No user will be permitted access for this application.

11. Click **Next**



Add Relying Party Trust Wizard

Ready to Add Trust

The relying party trust has been configured. Review the following settings, and then click Next to add the relying party trust to the AD FS configuration database.

Specify the monitoring settings for this relying party trust.

Relying party's federation metadata URL:

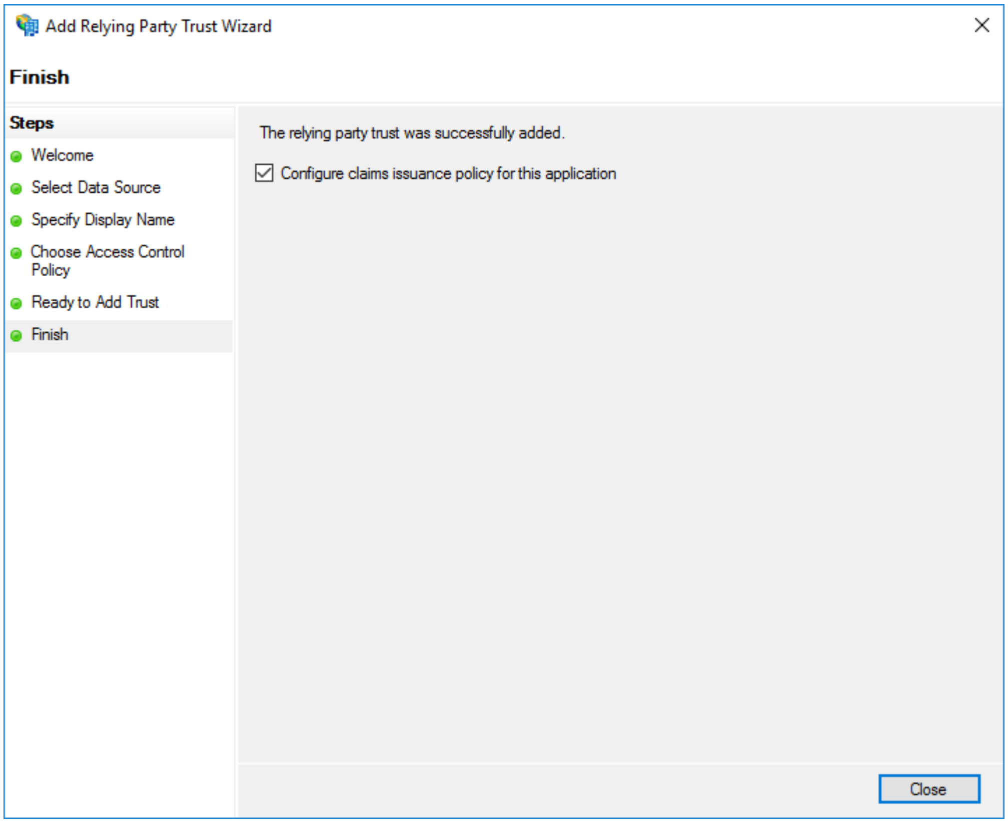
□ Monitor relying party

□ Automatically update relying party

This relying party's federation metadata data was last checked on:
< never >

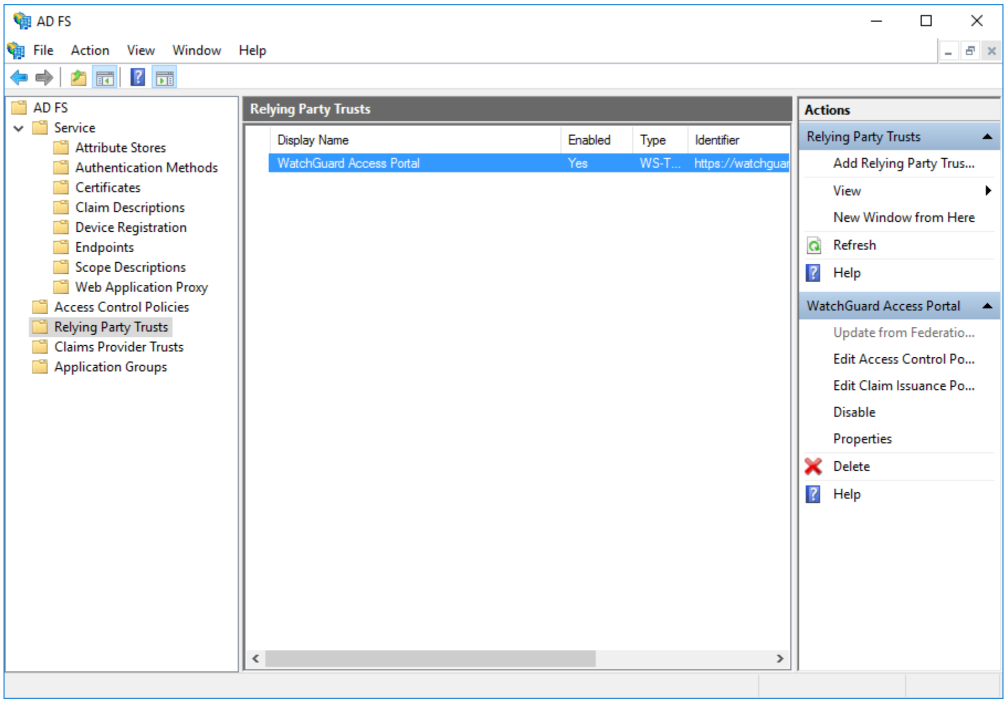
This relying party was last updated from federation metadata on:
< never >

12. Click **Close**



The relying party trust was successfully added.

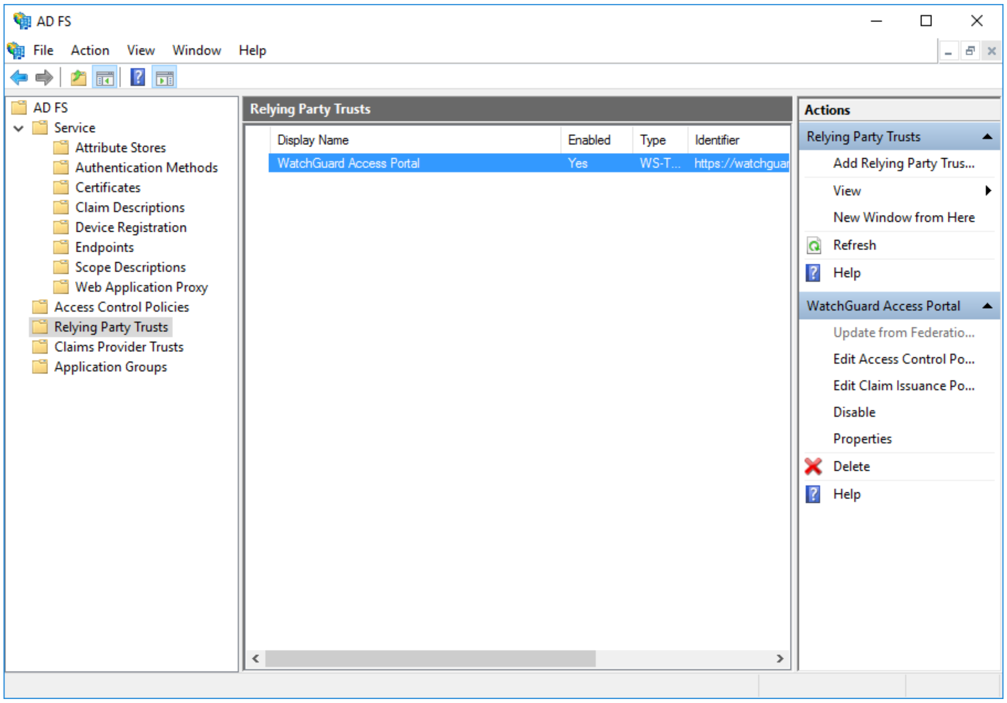
☑ Configure claims issuance policy for this application



Display Name	Enabled	Type	Identifier
WatchGuard Access Portal	Yes	WS-T...	https://watchguar

13. Select the Relying Party just created

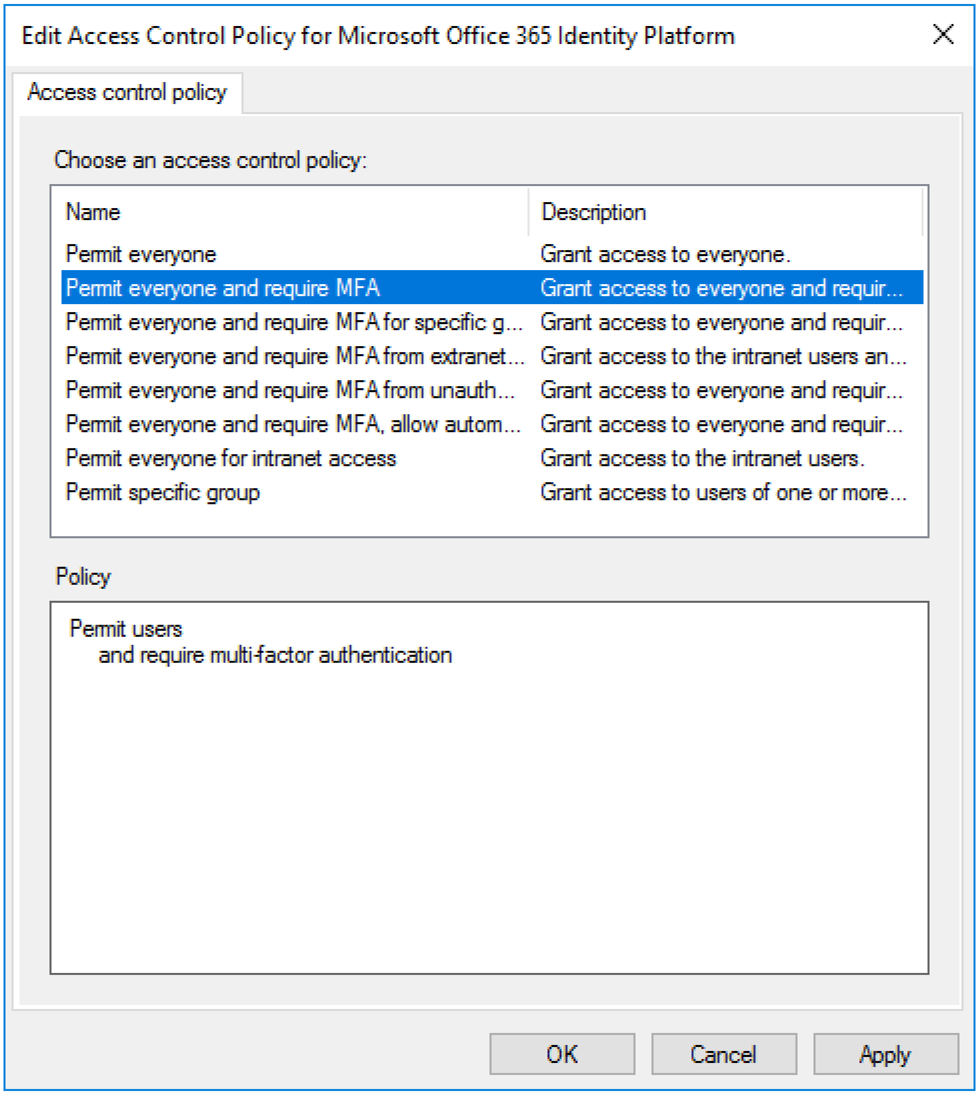
14. Click on **Edit Access Control Policy…** under Actions in the right sidebar



Display Name	Enabled	Type	Identifier
WatchGuard Access Portal	Yes	WS-T...	https://watchguar

15. Select an access control policy that uses MFA (e.g. **Permit everyone and require MFA**)

16. Press **Apply** and **OK**


Edit Access Control Policy for Microsoft Office 365 Identity Platform
Access control policy
OK
Cancel
Apply

Choose an access control policy:

Name	Description
Permit everyone	Grant access to everyone.
Permit everyone and require MFA	Grant access to everyone and requir...
Permit everyone and require MFA for specific g...	Grant access to everyone and requir...
Permit everyone and require MFA from extranet...	Grant access to the intranet users an...
Permit everyone and require MFA from unauth...	Grant access to everyone and requir...
Permit everyone and require MFA, allow autom...	Grant access to everyone and requir...
Permit everyone for intranet access	Grant access to the intranet users.
Permit specific group	Grant access to users of one or more...

Policy

Permit users
  and require multi-factor authentication

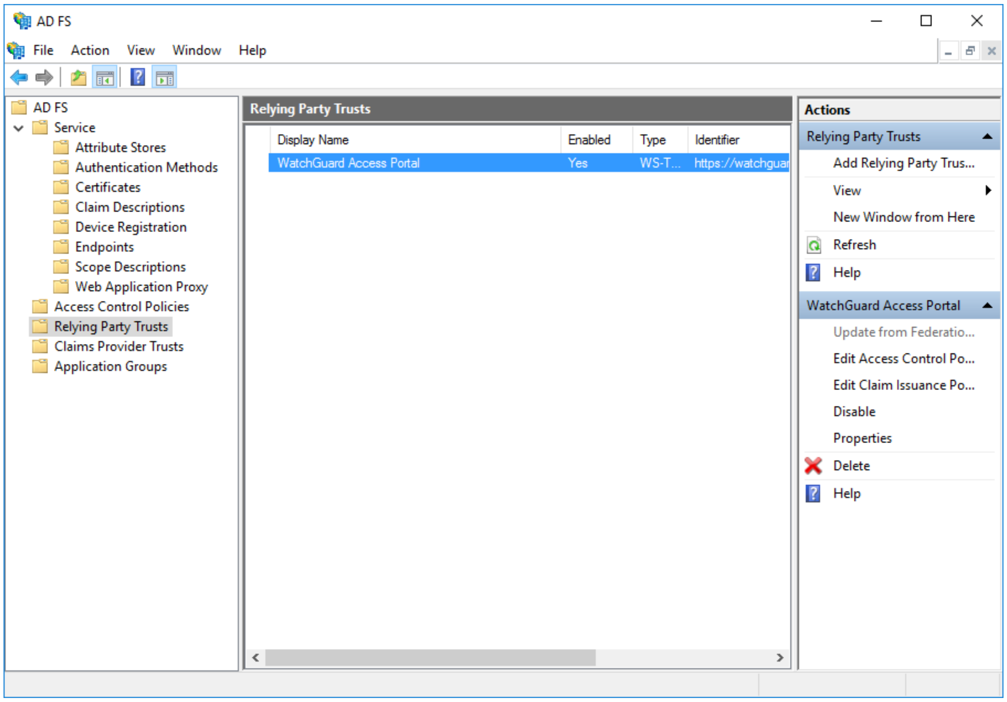
Next you will need to configured the AD FS Claims for your WatchGuard Access Portal Relying Party.

AD FS Claims

WatchGuard Access Portal requires the following claims to be configured:

Claim 1: LDAP Attribute for SAM-Account-Name

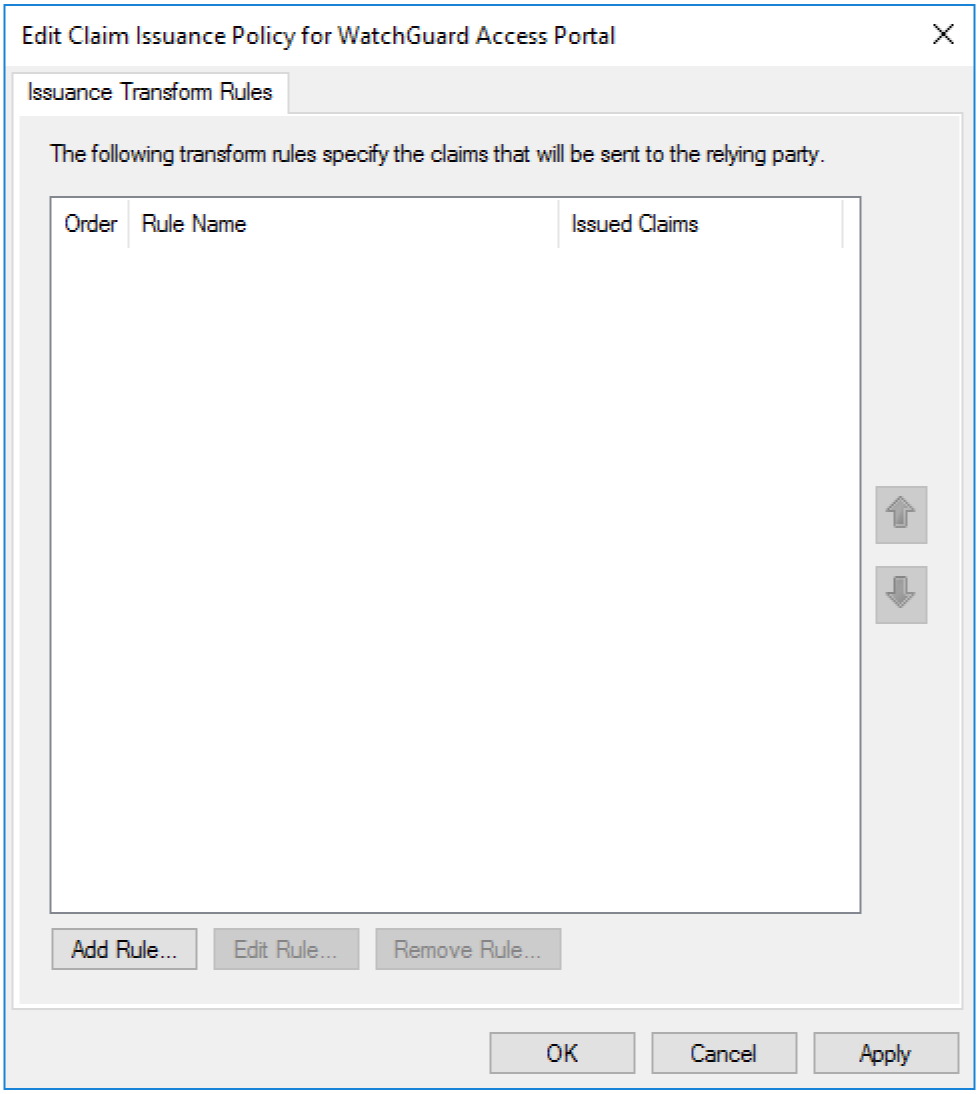
1. Click on **Relying Party Trusts** in the left side menu



Display Name	Enabled	Type	Identifier
WatchGuard Access Portal	Yes	WS-T...	https://watchguar

2. Select the WatchGuard Access Portal Relying Party

3. Click on **Edit Claims Issuance Policy…** under Actions in the right sidebar



Edit Claim Issuance Policy for WatchGuard Access Portal

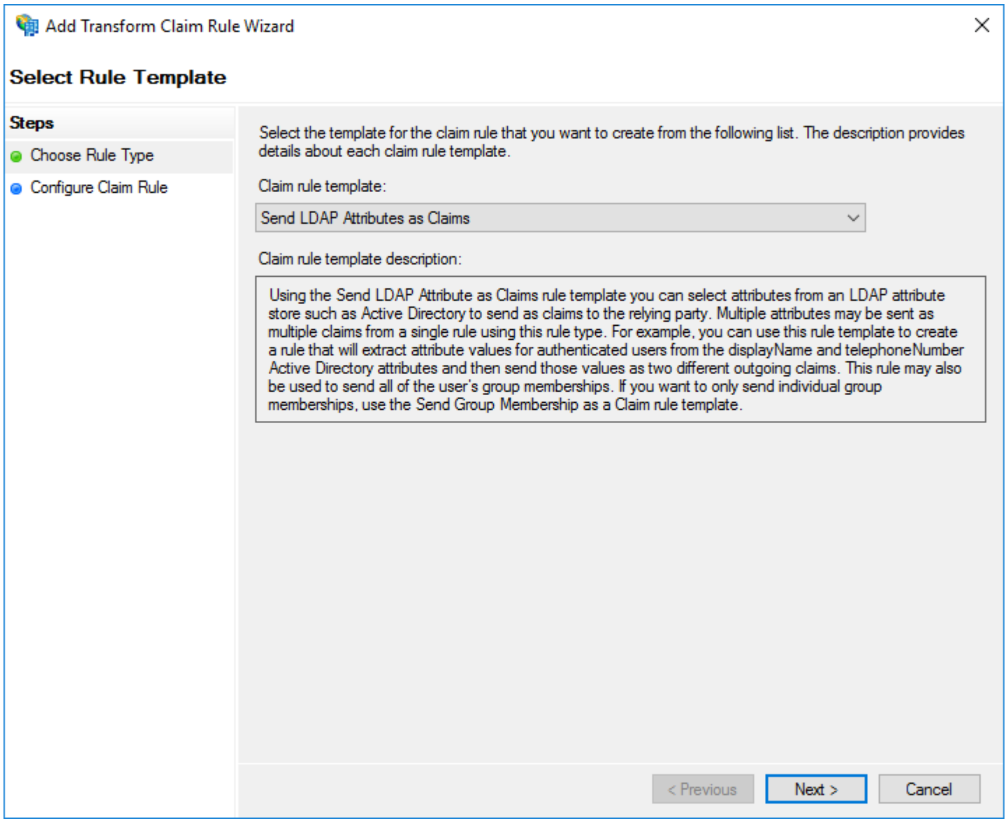
Issuance Transform Rules

The following transform rules specify the claims that will be sent to the relying party.

Order	Rule Name	Issued Claims

4. Click **Add Rule**

5. Select **Send LDAP Attributes as Claims** and click **Next**



Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

Claim rule template:

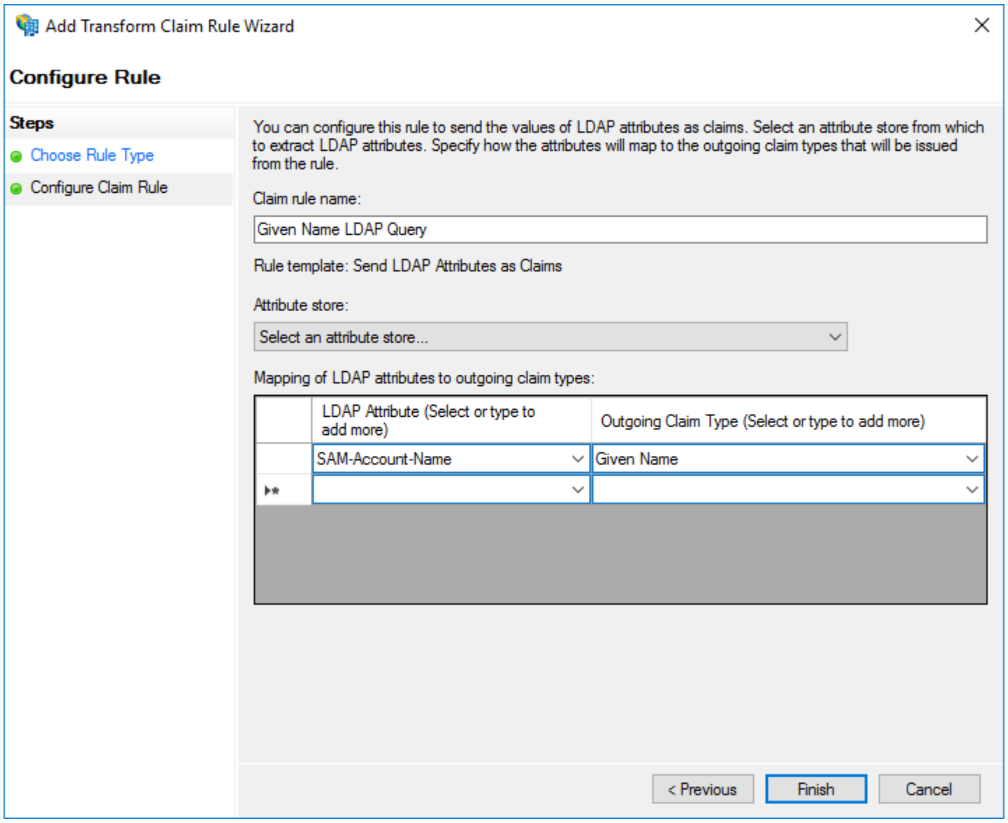
Send LDAP Attributes as Claims

Claim rule template description:

Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute store such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to create a rule that will extract attribute values for authenticated users from the displayName and telephoneNumber Active Directory attributes and then send those values as two different outgoing claims. This rule may also be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template.

6. Enter a **Claim rule name** (for example, `Given Name LDAP Query`)
7. Under **LDAP Attribute** enter **SAM-Account-Name**

8. Under **Outgoing Claim Type** enter **Given Name**



You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:

Given Name LDAP Query

Rule template: Send LDAP Attributes as Claims

Attribute store:

Select an attribute store...

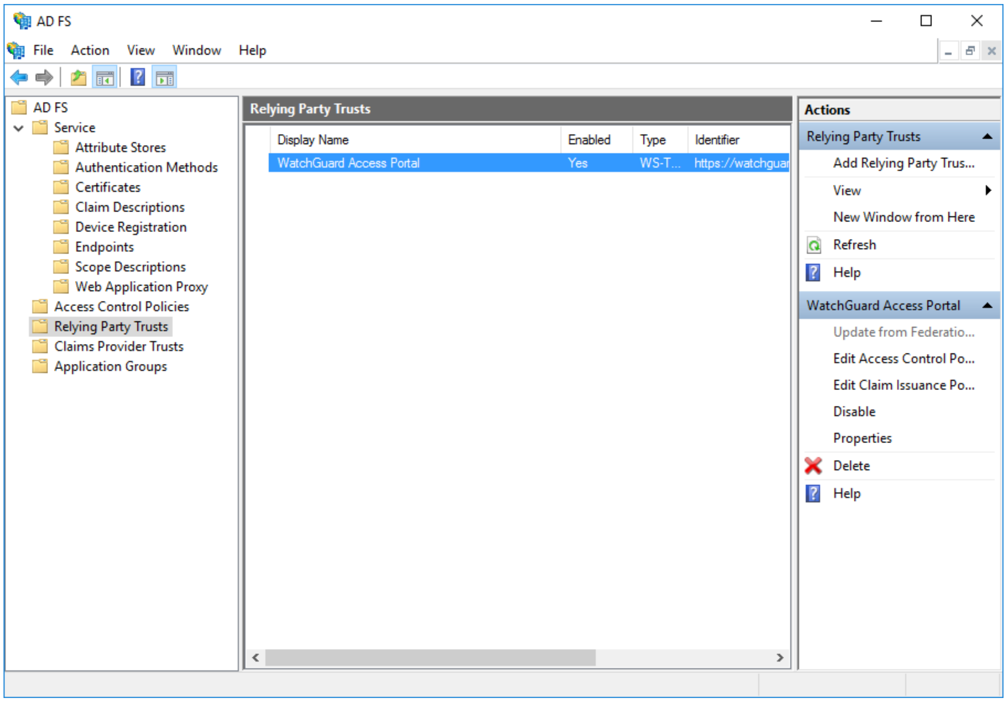
Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
	SAM-Account-Name	Given Name
▶*		

9. Click **Finish**

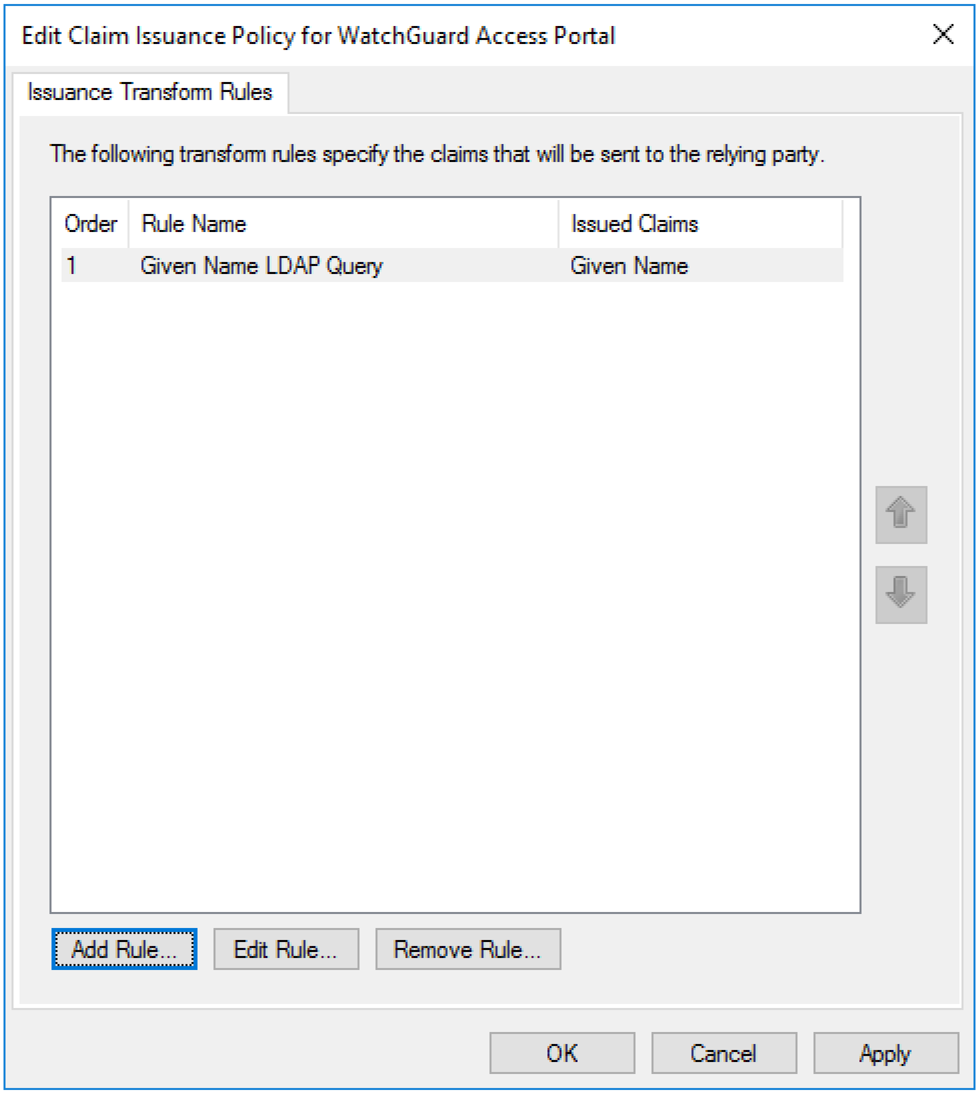
Claim 2: Transform Given Name to Name ID

1. Click on **Relying Party Trusts** in the left side menu



Display Name	Enabled	Type	Identifier
WatchGuard Access Portal	Yes	WS-T...	https://watchguar

2. Select the WatchGuard Access Portal Relying Party
3. Click on **Edit Claims Issuance Policy…** under Actions in the right sidebar



Edit Claim Issuance Policy for WatchGuard Access Portal

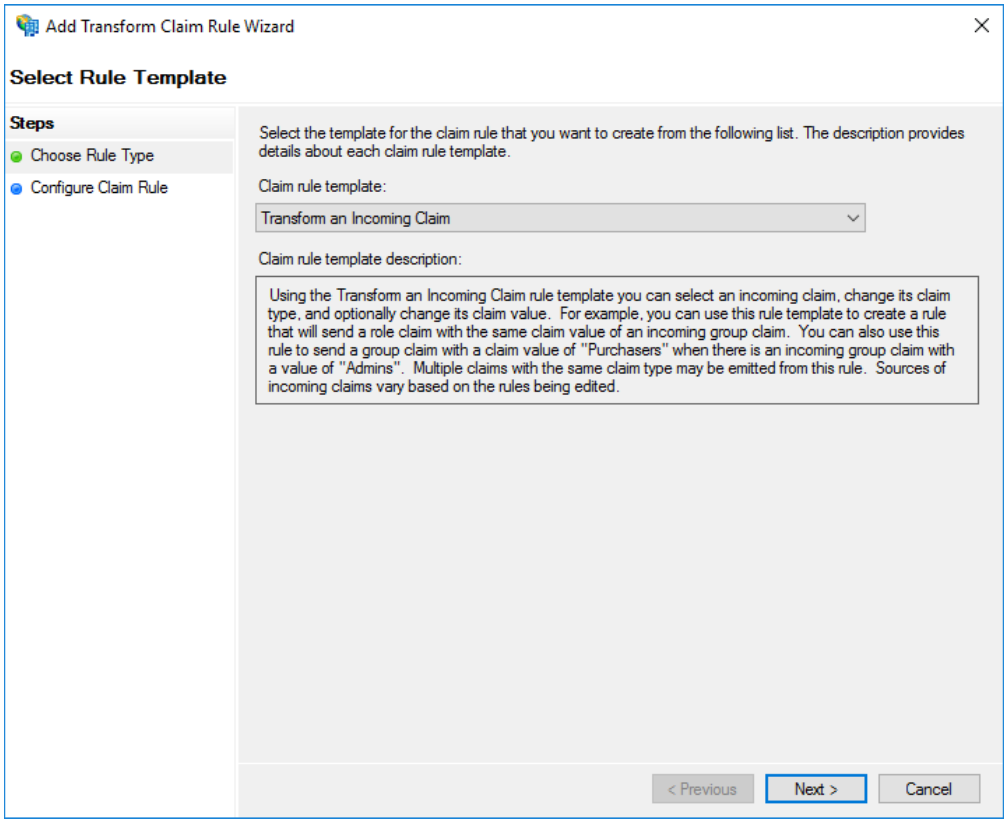
Issuance Transform Rules

The following transform rules specify the claims that will be sent to the relying party.

Order	Rule Name	Issued Claims
1	Given Name LDAP Query	Given Name

4. Click **Add Rule**

5. Select **Transform an Incoming Claim** and click **Next**



Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

Claim rule template:

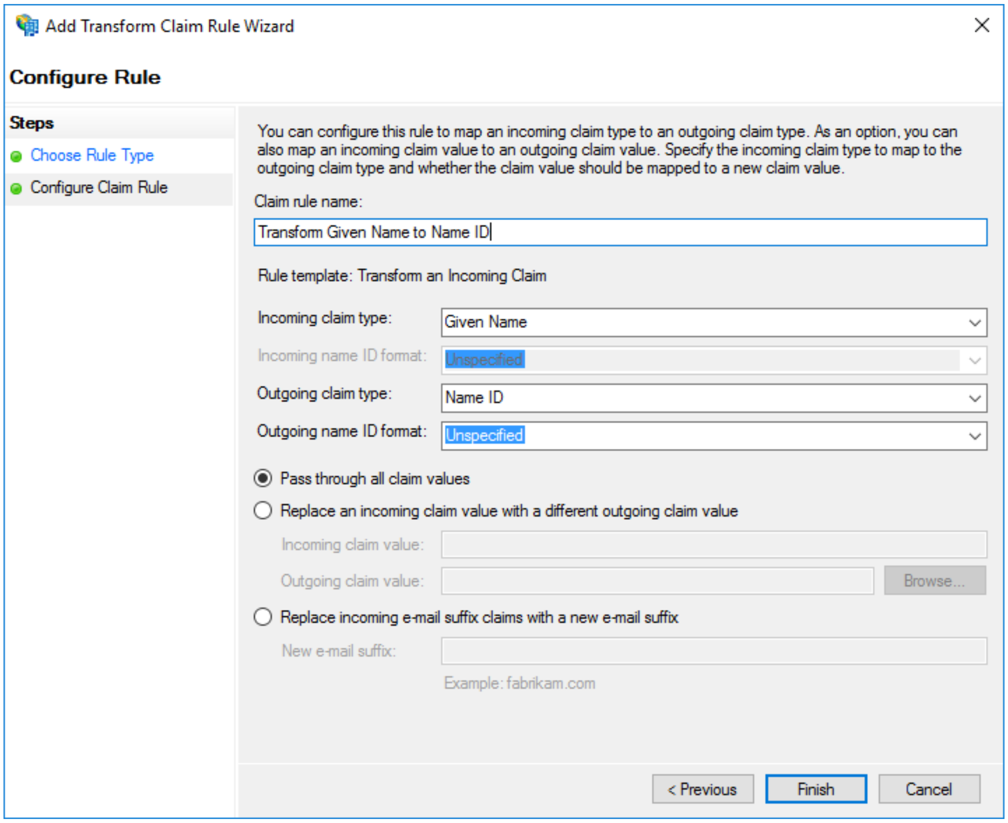
Transform an Incoming Claim

Claim rule template description:

Using the Transform an Incoming Claim rule template you can select an incoming claim, change its claim type, and optionally change its claim value. For example, you can use this rule template to create a rule that will send a role claim with the same claim value of an incoming group claim. You can also use this rule to send a group claim with a claim value of "Purchasers" when there is an incoming group claim with a value of "Admins". Multiple claims with the same claim type may be emitted from this rule. Sources of incoming claims vary based on the rules being edited.

6. Enter a **Claim rule name** (for example, `Transform Given Name to Name ID`)
7. Under **Incoming claim type** enter **Given Name**
8. Under **Outgoing claim Type** enter **Name ID**

9. Select **Pass through all claim values**



Add Transform Claim Rule Wizard

Configure Rule

You can configure this rule to map an incoming claim type to an outgoing claim type. As an option, you can also map an incoming claim value to an outgoing claim value. Specify the incoming claim type to map to the outgoing claim type and whether the claim value should be mapped to a new claim value.

Claim rule name:
Transform Given Name to Name ID

Rule template: Transform an Incoming Claim

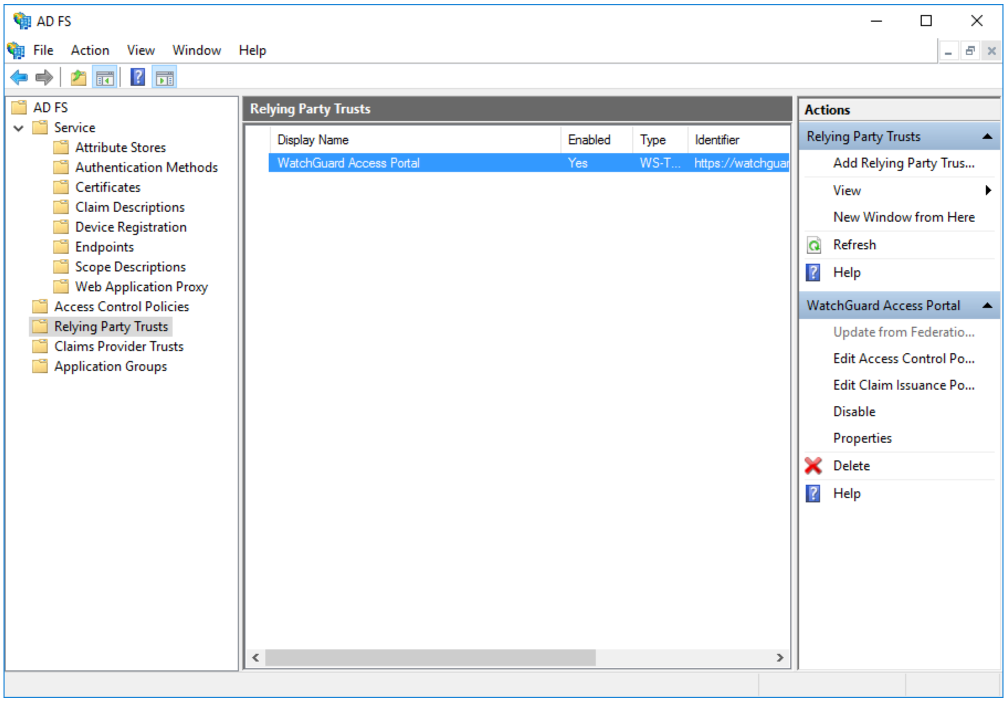
Incoming claim type: Given Name
Incoming name ID format: Unspecified
Outgoing claim type: Name ID
Outgoing name ID format: Unspecified

● Pass through all claim values
○ Replace an incoming claim value with a different outgoing claim value
Incoming claim value:
Outgoing claim value:
○ Replace incoming e-mail suffix claims with a new e-mail suffix
New e-mail suffix:
Example: fabrikam.com

10. Click **Finish**

Claim 3: Group Membership Claim

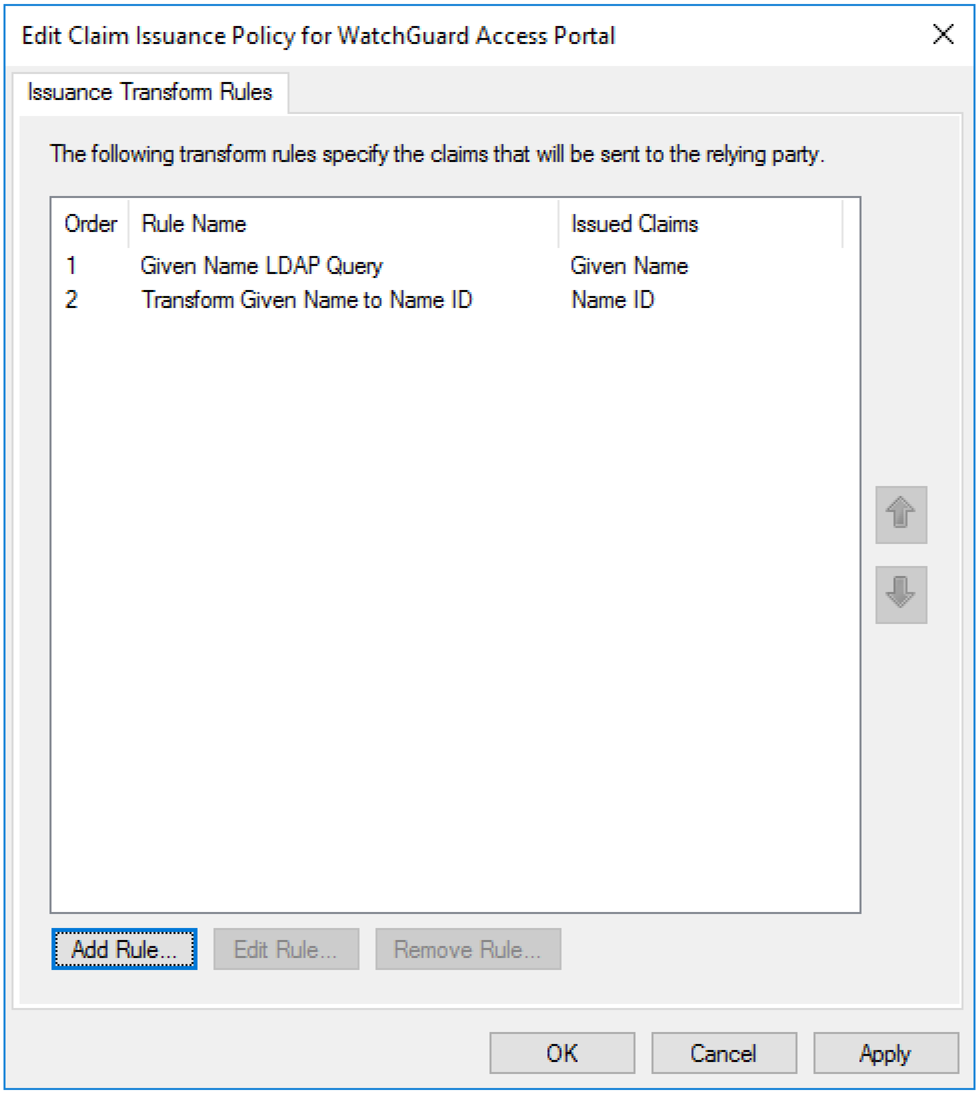
1. Click on **Relying Party Trusts** in the left side menu



Relying Party Trusts

Display Name	Enabled	Type	Identifier
WatchGuard Access Portal	Yes	WS-T...	https://watchguar

2. Select the WatchGuard Access Portal Relying Party
3. Click on **Edit Claims Issuance Policy…** under Actions in the right sidebar



Edit Claim Issuance Policy for WatchGuard Access Portal

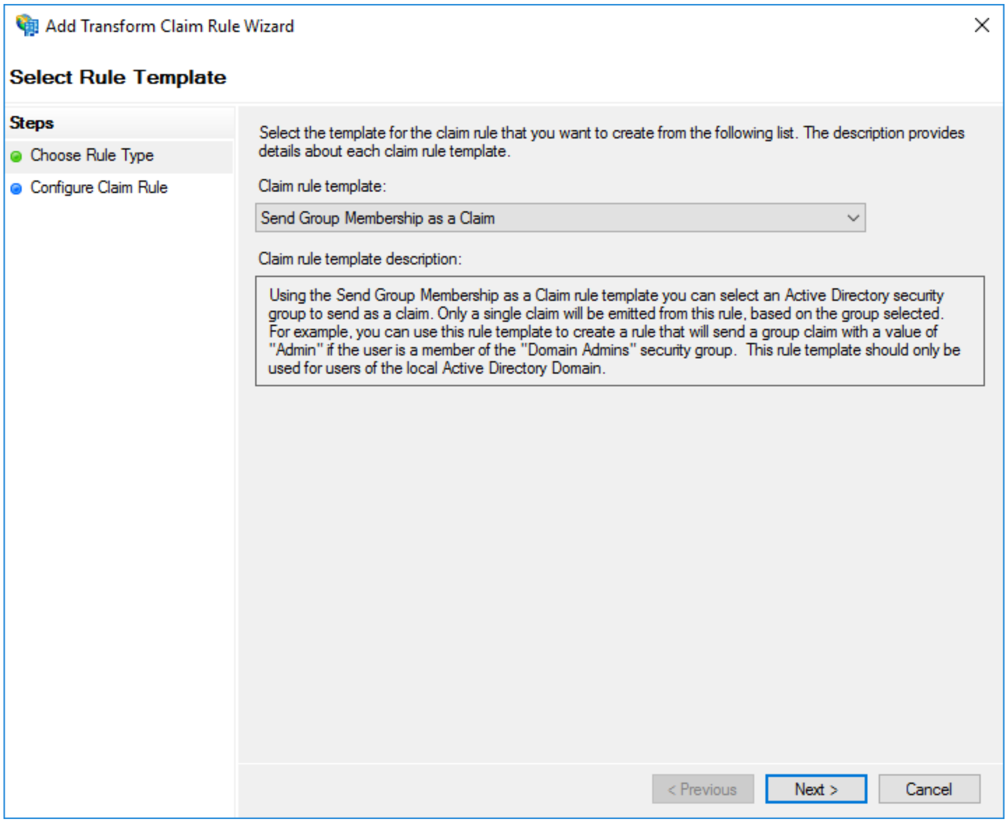
Issuance Transform Rules

The following transform rules specify the claims that will be sent to the relying party.

Order	Rule Name	Issued Claims
1	Given Name LDAP Query	Given Name
2	Transform Given Name to Name ID	Name ID

4. Click **Add Rule**

5. Select **Send Group Membership as a Claim**



Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

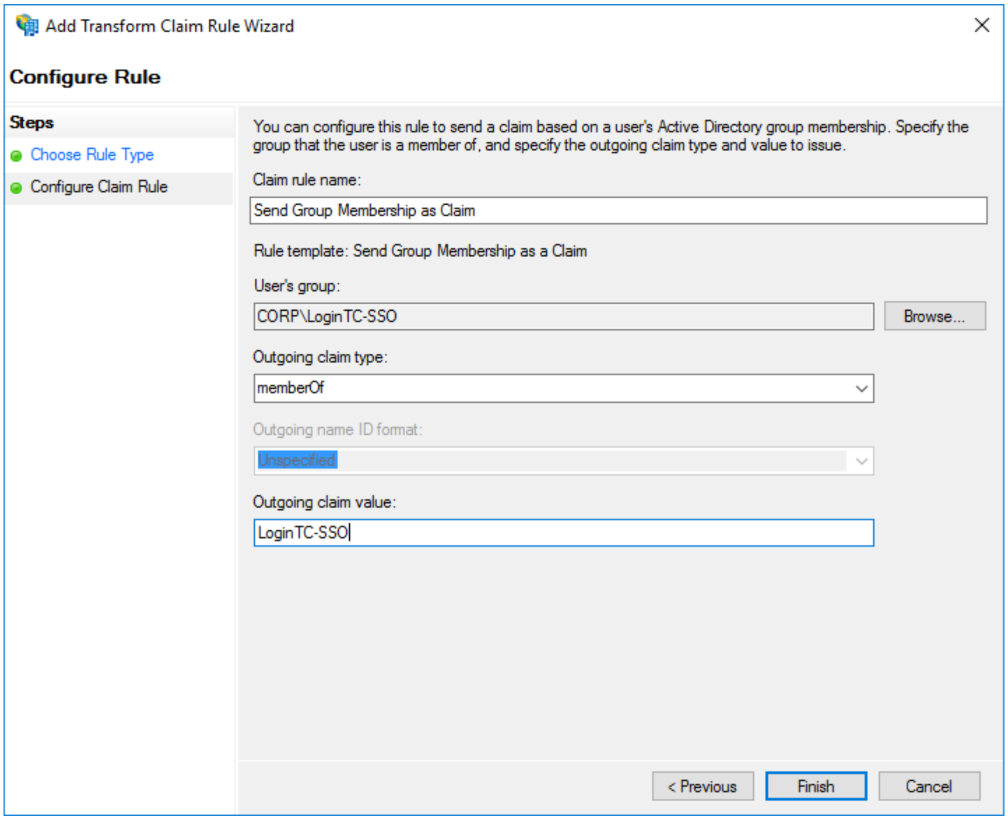
Claim rule template: Send Group Membership as a Claim

Claim rule template description:

Using the Send Group Membership as a Claim rule template you can select an Active Directory security group to send as a claim. Only a single claim will be emitted from this rule, based on the group selected. For example, you can use this rule template to create a rule that will send a group claim with a value of "Admin" if the user is a member of the "Domain Admins" security group. This rule template should only be used for users of the local Active Directory Domain.

6. Enter a **Claim rule name** (for example, `Send Group Membership as Claim`)
7. Under **User's group** click **Browse** and select the group configured for WatchGuard Access Portal
8. Under **Outgoing claim type** enter **memberOf**

9. Under **Outgoing claim value** enter the name of the group. This should match exactly the name configured in the WatchGuard Access Portal



Add Transform Claim Rule Wizard

Configure Rule

You can configure this rule to send a claim based on a user's Active Directory group membership. Specify the group that the user is a member of, and specify the outgoing claim type and value to issue.

Claim rule name: Send Group Membership as Claim

Rule template: Send Group Membership as a Claim

User's group: CORP\LoginTC-SSO

Outgoing claim type: memberOf

Outgoing name ID format: Unspecified

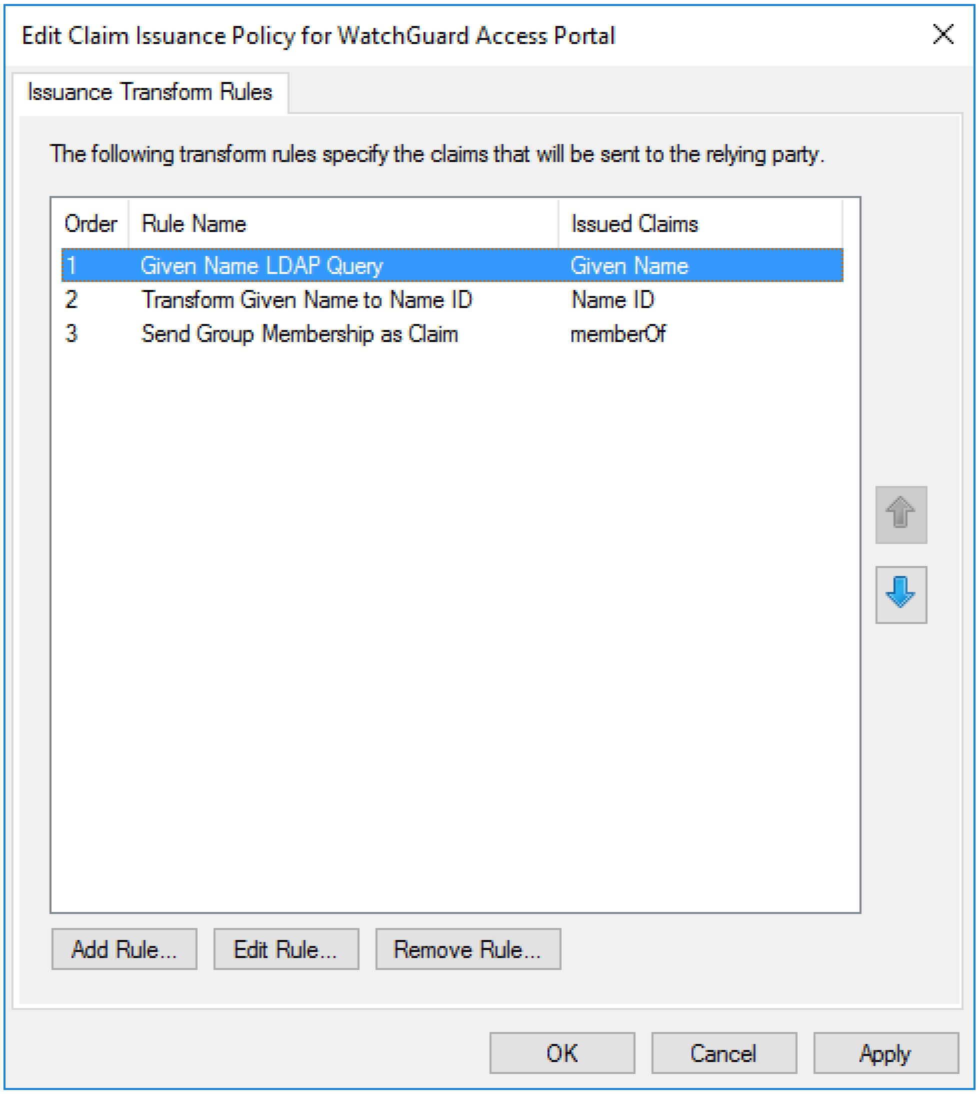
Outgoing claim value: LoginTC-SSO

10. Click **Finish**

Additional AD FS Groups

If your WatchGuard Access Portal is configured with multiple groups, subsequent groups can be added as claims following the same procedure listed above

With these claims configured you are now ready to test logging into the WatchGuard Access Portal using LoginTC and AD FS.



Edit Claim Issuance Policy for WatchGuard Access Portal

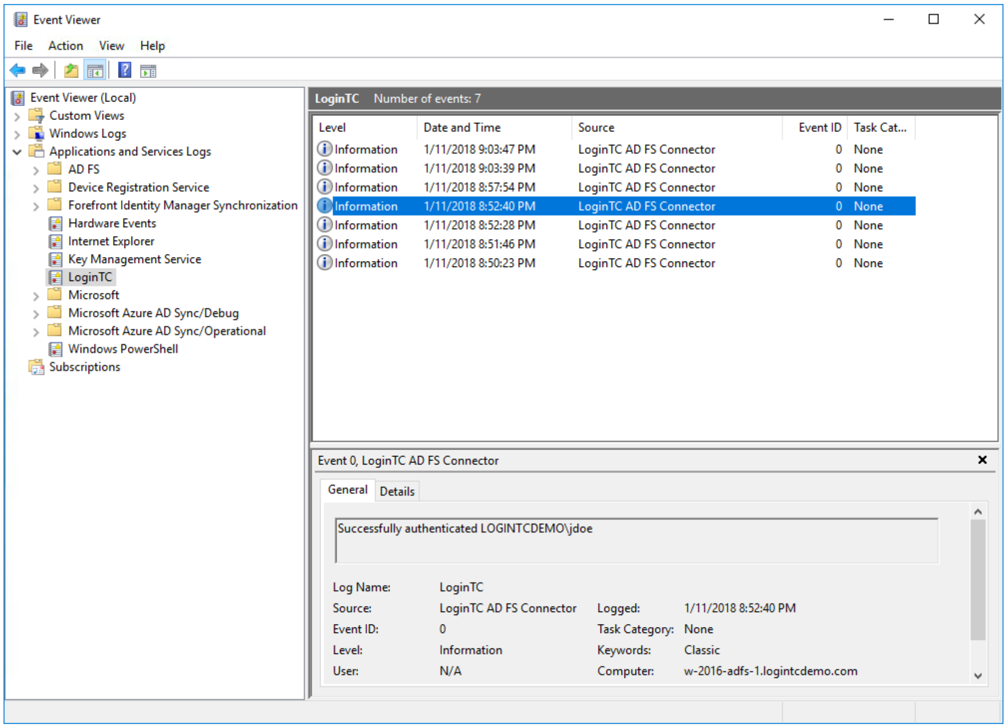
Issuance Transform Rules

The following transform rules specify the claims that will be sent to the relying party.

Order	Rule Name	Issued Claims
1	Given Name LDAP Query	Given Name
2	Transform Given Name to Name ID	Name ID
3	Send Group Membership as Claim	memberOf

Logging

The LoginTC AD FS Connector logs events to the Microsoft Event Viewer under **Applications and Service Logs** → **LoginTC**. In some cases, it may be helpful to also look at the general AD FS logs under **Custom Views** → **ServerRoles** → **Active Directory Federation Services**.



LoginTC Number of events: 7

Level	Date and Time	Source	Event ID	Task Cat...
Information	1/11/2018 9:03:47 PM	LoginTC AD FS Connector	0	None
Information	1/11/2018 9:03:39 PM	LoginTC AD FS Connector	0	None
Information	1/11/2018 8:57:54 PM	LoginTC AD FS Connector	0	None
Information	1/11/2018 8:52:40 PM	LoginTC AD FS Connector	0	None
Information	1/11/2018 8:52:28 PM	LoginTC AD FS Connector	0	None
Information	1/11/2018 8:51:46 PM	LoginTC AD FS Connector	0	None
Information	1/11/2018 8:50:23 PM	LoginTC AD FS Connector	0	None

Event 0, LoginTC AD FS Connector

Successfully authenticated LOGINTCDEMO\jdoe

Log Name:	LoginTC		
Source:	LoginTC AD FS Connector	Logged:	1/11/2018 8:52:40 PM
Event ID:	0	Task Category:	None
Level:	Information	Keywords:	Classic
User:	N/A	Computer:	w-2016-adfs-1.logintcdemo.com

Uninstallation

To uninstall the LoginTC AD FS Connector, simply navigate to the **Add or remove programs** in the Windows **Control Panel**, find LoginTC AD FS Connector in the list and follow the prompts.

Prior to Uninstalling

Prior to uninstalling the LoginTC AD FS Connector, ensure that the LoginTC MFA method is not being used in any of your AD FS authentication policies. The uninstallation will fail if the LoginTC MFA method is being used in any of your AD FS authentication policies.

Troubleshooting

Email Support

For any additional help please email support@cyphercor.com. Expect a speedy reply.