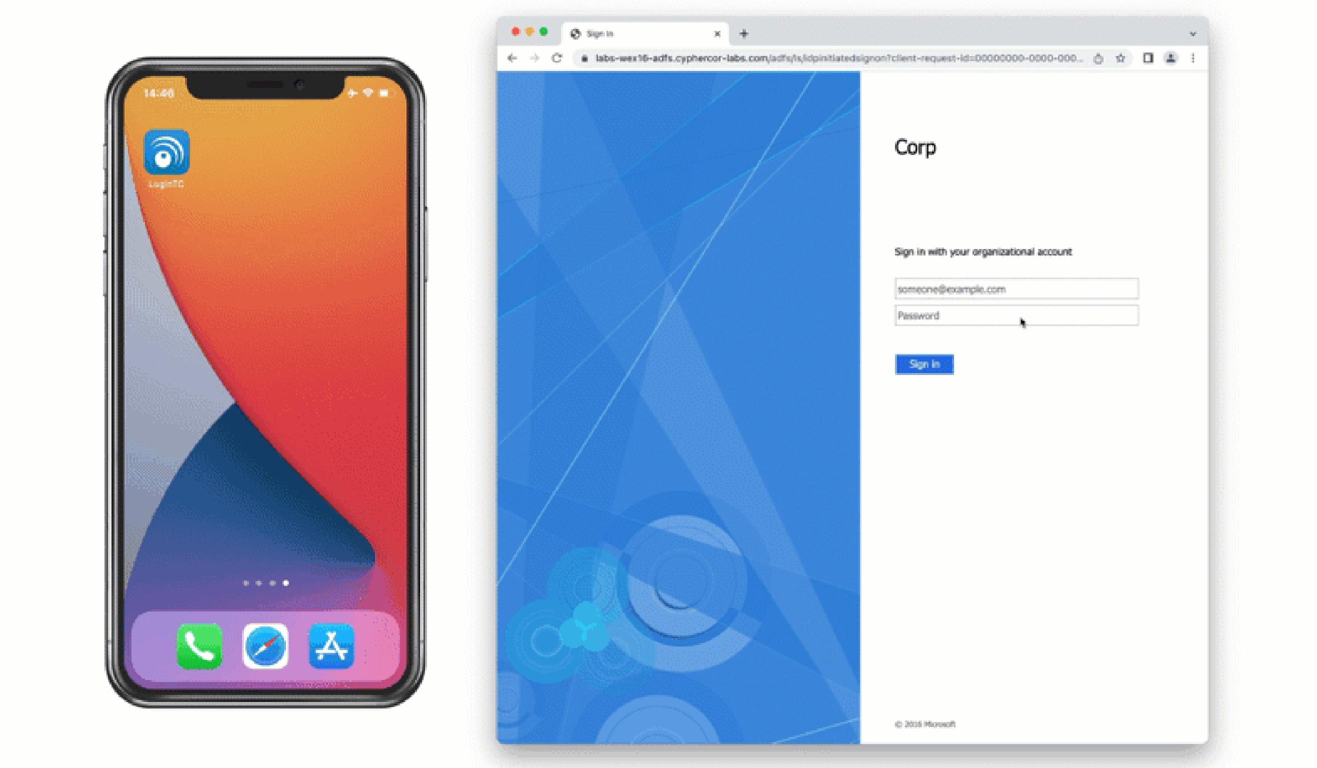
2FA for AD FS on Windows Server 2016, 2019 and 2022

logintc.com/docs/connectors/adfs



14:46
LoginTC
Sign In
labs-wex16-adfs.cyphercor-labs.com/adfs/ls/idpinitiatedsignon?client-request-id=00000000-0000-000...

Corp

Sign in with your organizational account

someone@example.com

Password

Windows Server 2016, 2019 and 2022

This guide is for installing the LoginTC AD FS Connector on **Windows Server 2016, 2019 and 2022**. For AD FS on Windows Server 2012 R2, see Two factor authentication for Active Directory Federation Services (AD FS) on Windows Server 2012 R2.

Overview

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.

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.

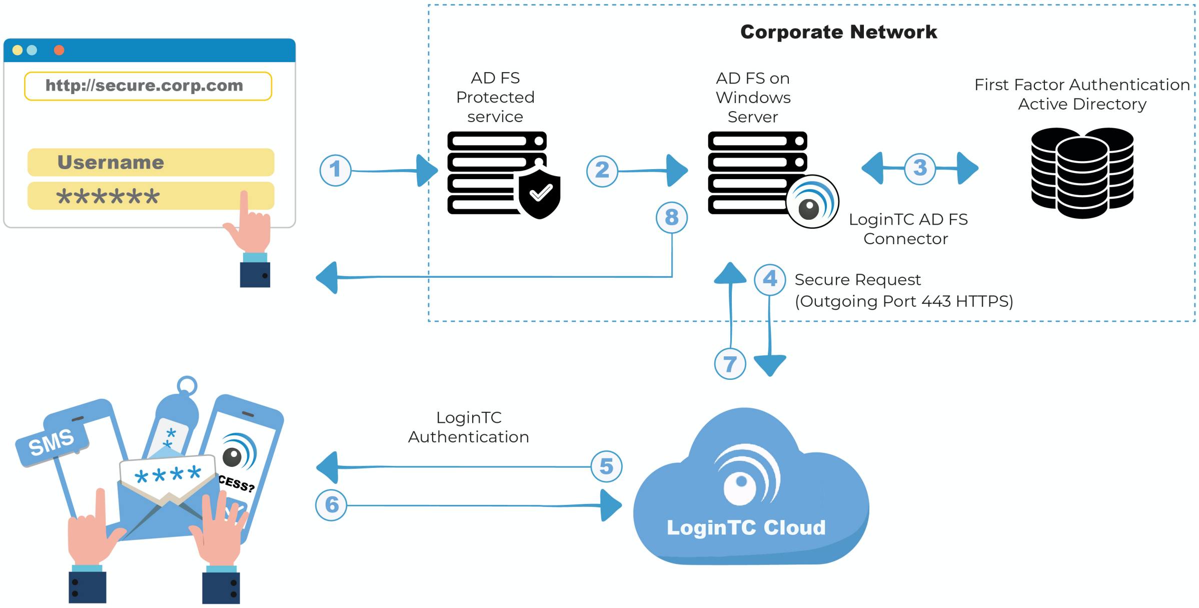
User Experience

After entering the username and password into the AD FS login, 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.

Video Instructions

Watch Video At: https://youtu.be/LljAHJc9ap8

Architecture



Authentication Flow

1. A user attempts access to AD FS protected service 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 AD FS protected service

Prerequisites

Before proceeding, please ensure you have the following:

- LoginTC Admin Panel account
- Microsoft Windows Server 2016, Windows Server 2019 or Windows Server 2022
- Active Directory Federation Services (AD FS) role

Working AD FS Deployment

It is strongly recommended that you have a working and tested AD FS deployment with at least one service prior to adding LoginTC authentication.

Create Application

Start by creating a LoginTC Application for your deployment. An Application represents a service (e.g. An application is a service (e.g., VPN or web application) that you want to protect. e) that you want to protect with LoginTC.

Create a LoginTC Application in LoginTC Admin Panel, follow Create Application Steps.

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

Normalize Usernames

Usernames in ADFS are typically in the form "CORP\john.doe", while in the LoginTC Admin Panel it is generally more convenient to simply use "john.doe".

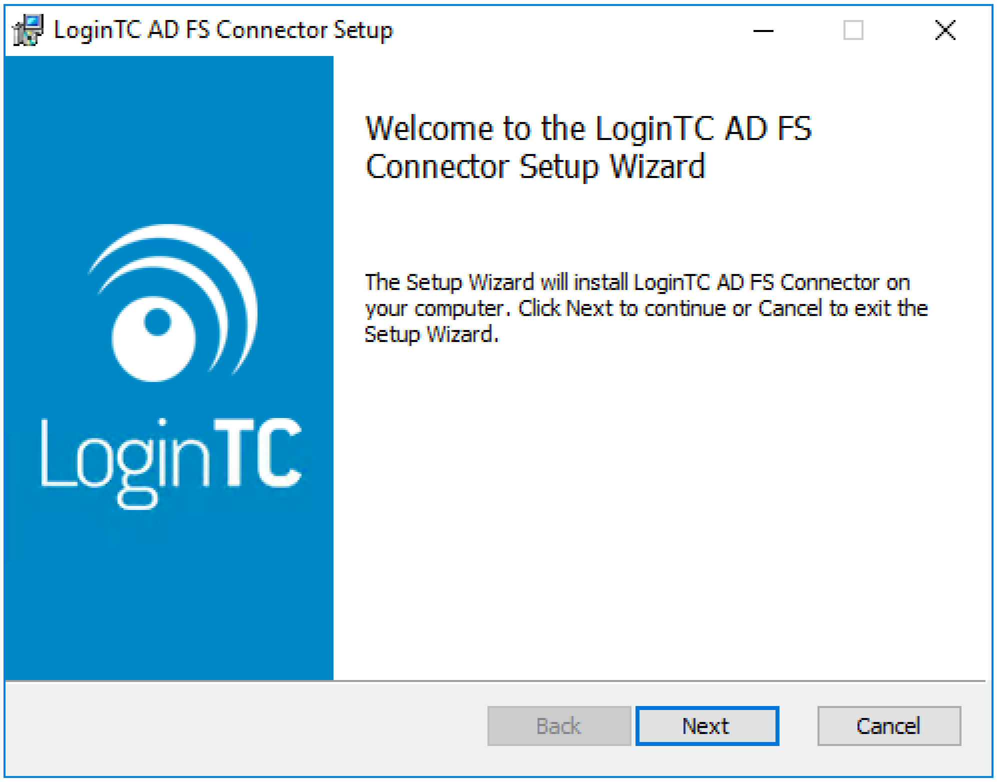
Configure `Normalize Usernames` from the Domain settings by navigating to **Domains > Your Domain > Settings**.

Select `Yes, Normalize Usernames` scroll down and click `Update`.

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**

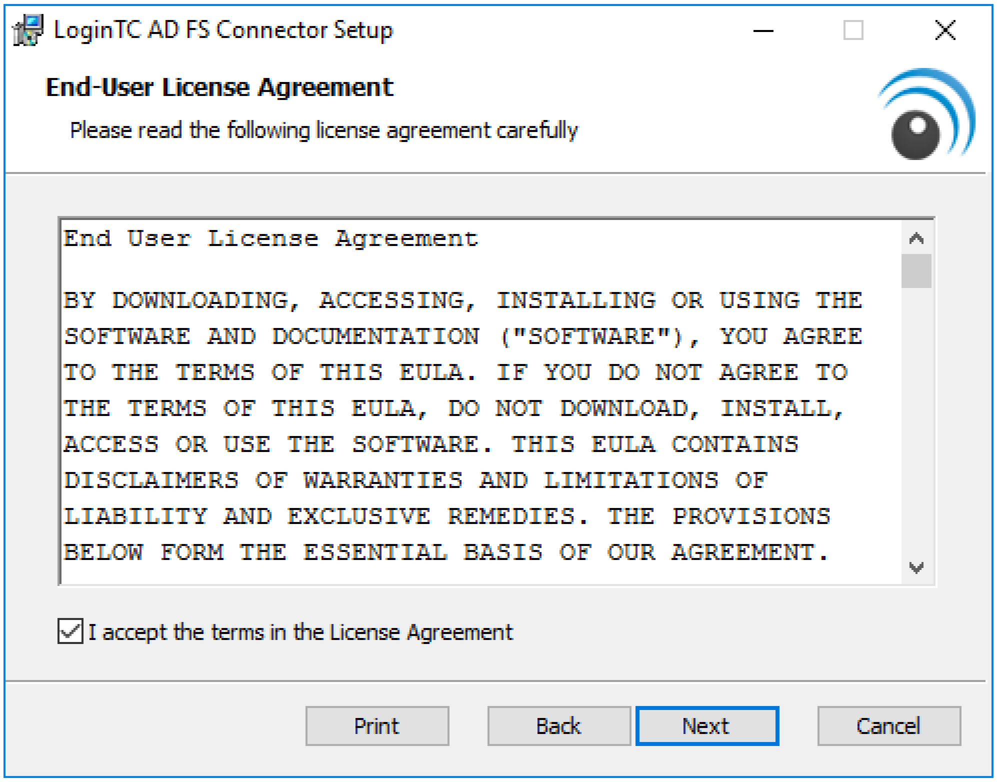


LoginTC AD FS Connector Setup

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

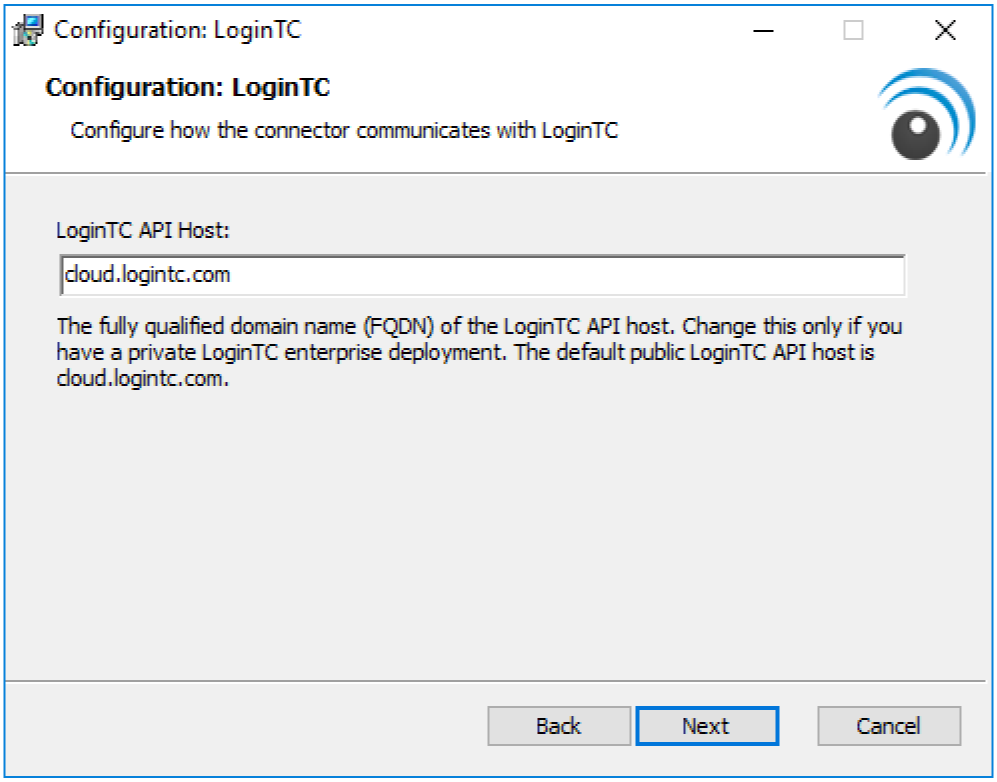
Please read the following license agreement carefully

```
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

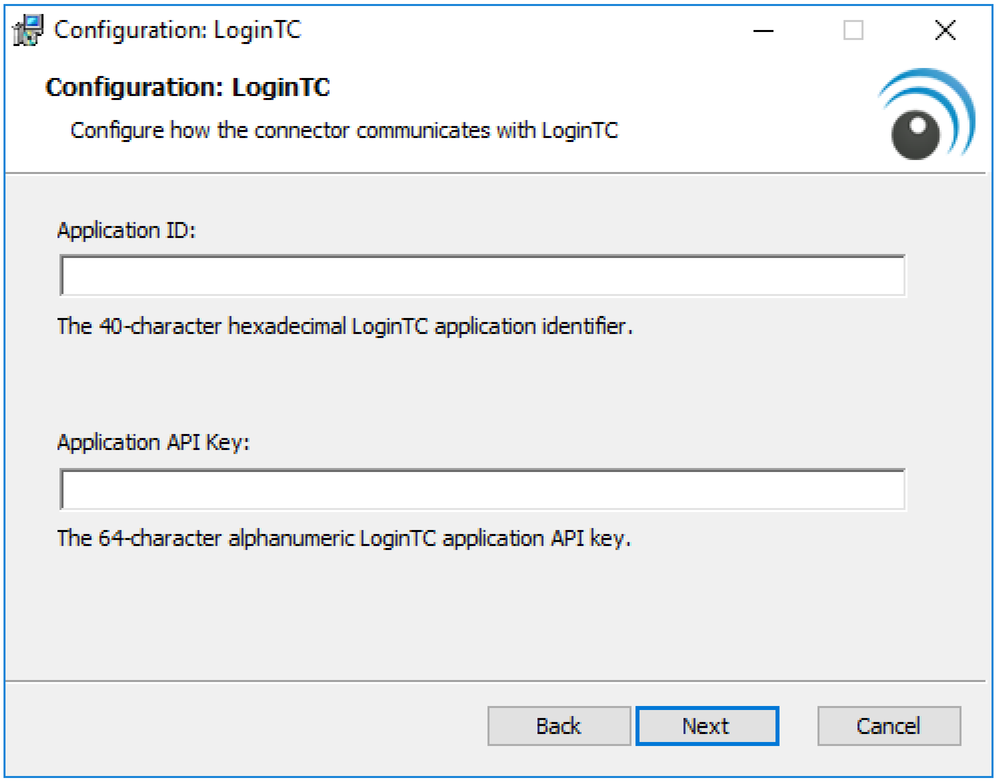
Configure how the connector communicates with LoginTC

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 **Application ID** and **Application API Key**. These values are found on your LoginTC Admin Panel. Press **Next**



Configuration: LoginTC

Configuration: LoginTC

Configure how the connector communicates with LoginTC

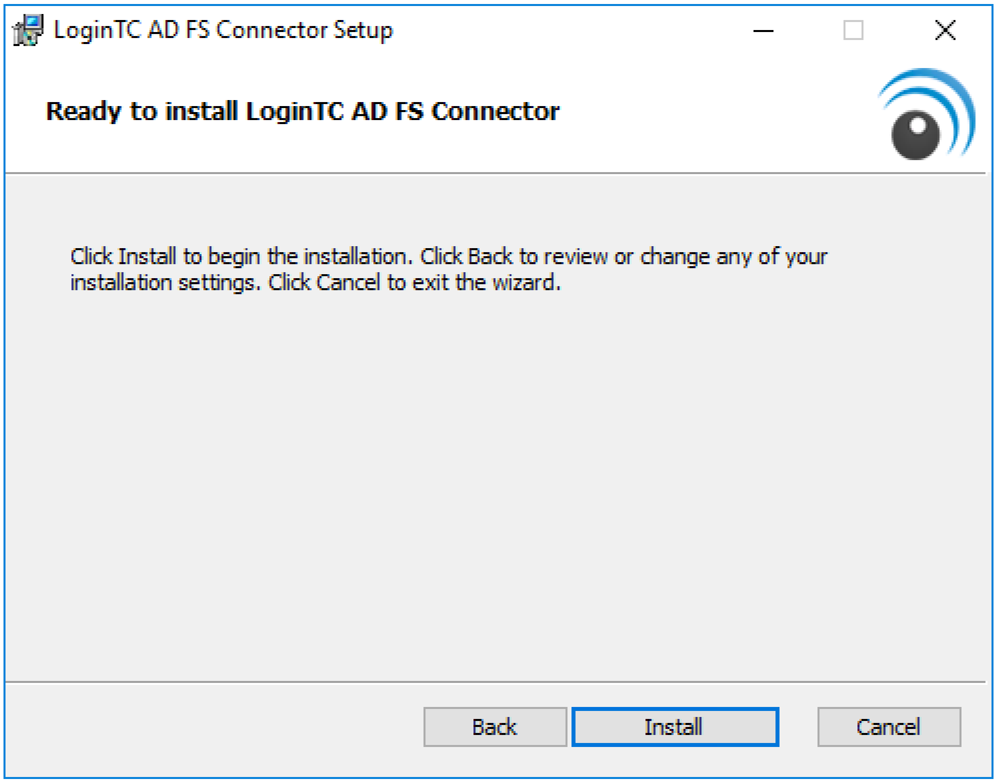
Application ID:

The 40-character hexadecimal LoginTC application identifier.

Application API Key:

The 64-character alphanumeric LoginTC application API key.

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



Ready to install LoginTC AD FS Connector

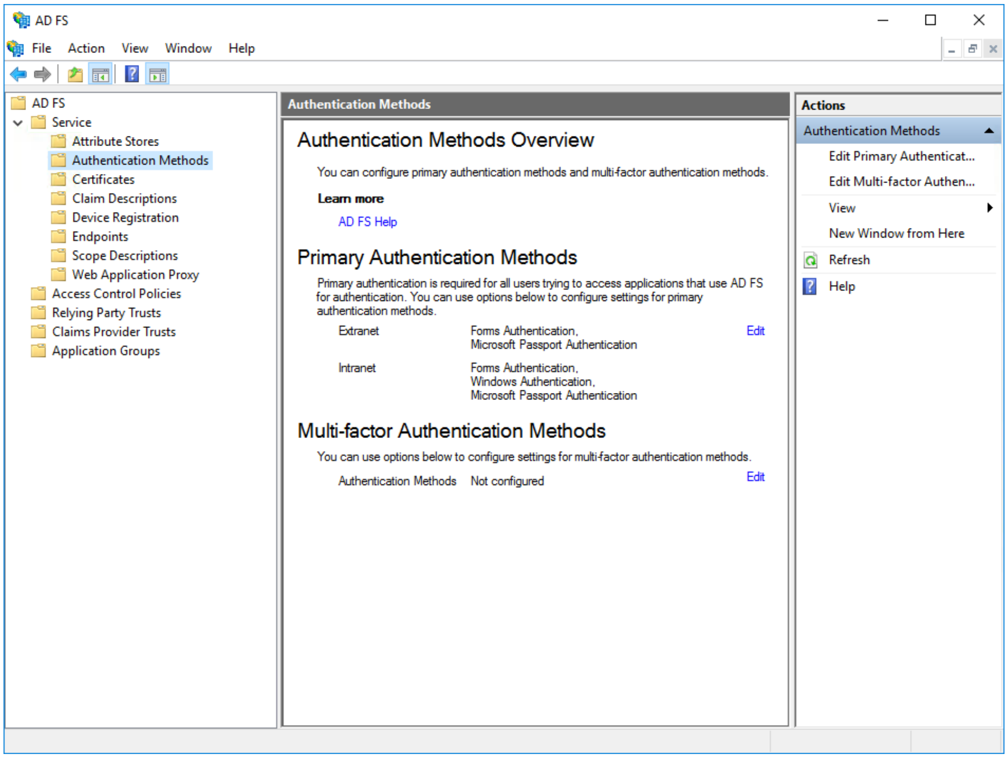
Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

Configuration for ADFS MFA

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	

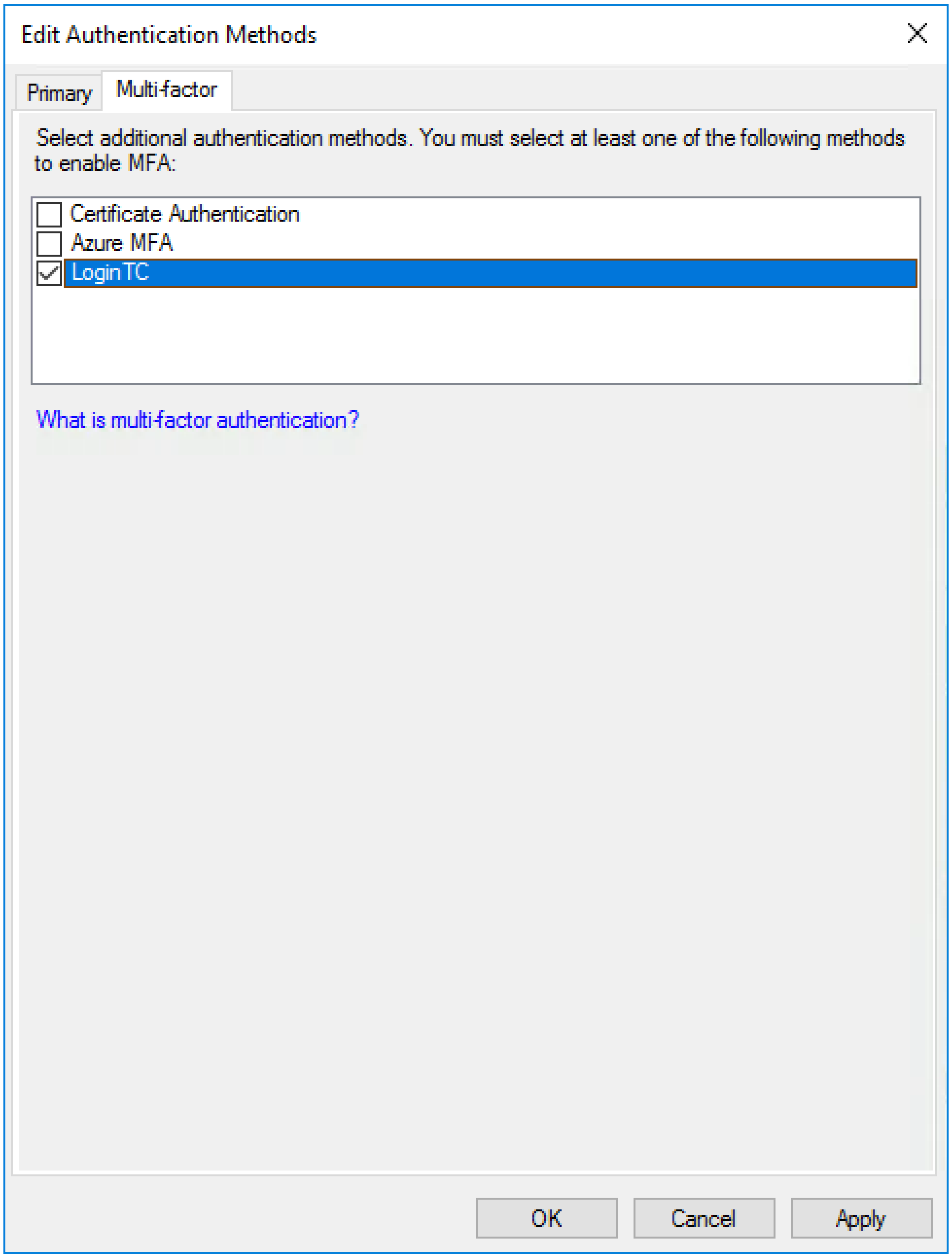
Multi-factor Authentication Methods

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.



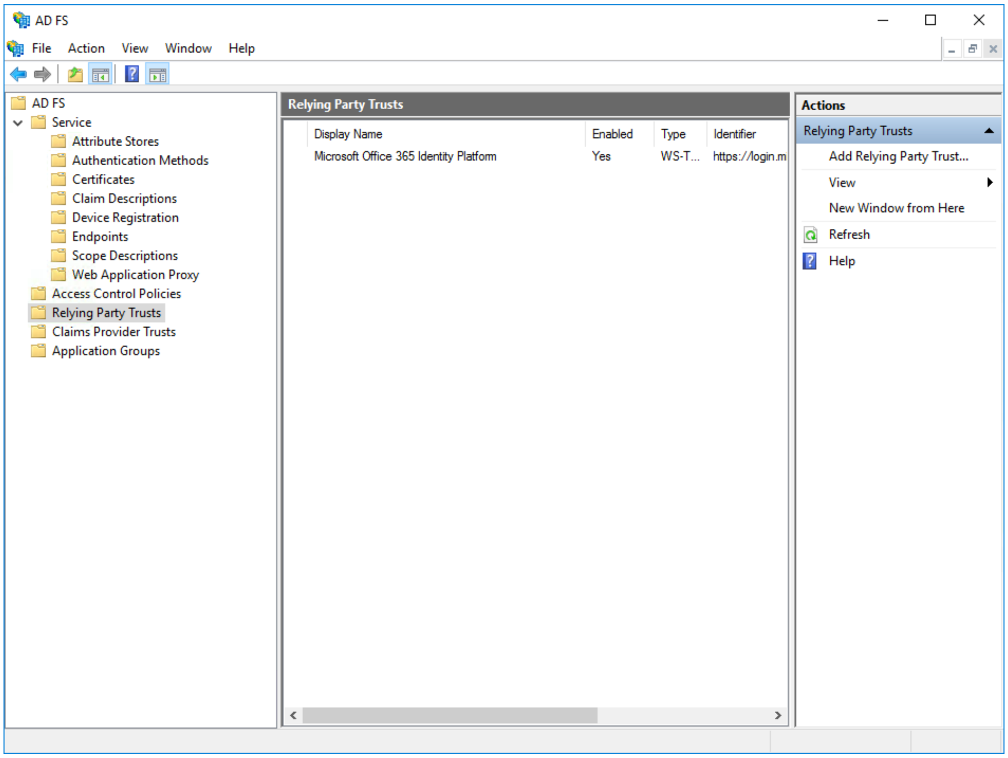
Edit Authentication Methods

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

- □ Certificate Authentication
- □ Azure MFA
- ☑ LoginTC

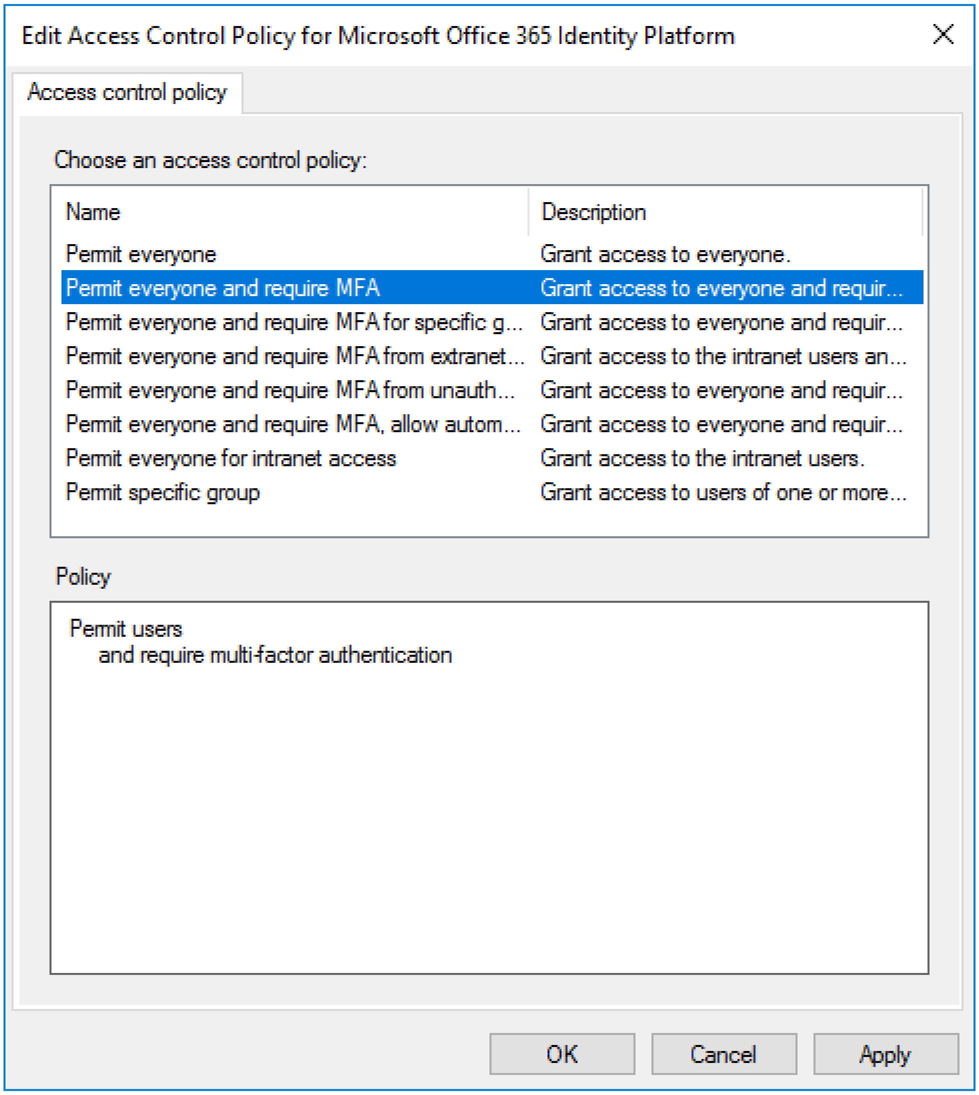
5. Click on **Relying Party Trusts** in the left side menu
6. Select the Relying Party you wish to add LoginTC MFA to

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



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

9. Press **Apply** and **OK**



Edit Access Control Policy for Microsoft Office 365 Identity Platform

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

Windows Server 2019

If you are installing the LoginTC AD FS Connector on Windows Server 2019 you are required to run the following PowerShell command to allow the AD FS login page to embed the LoginTC authentication options:

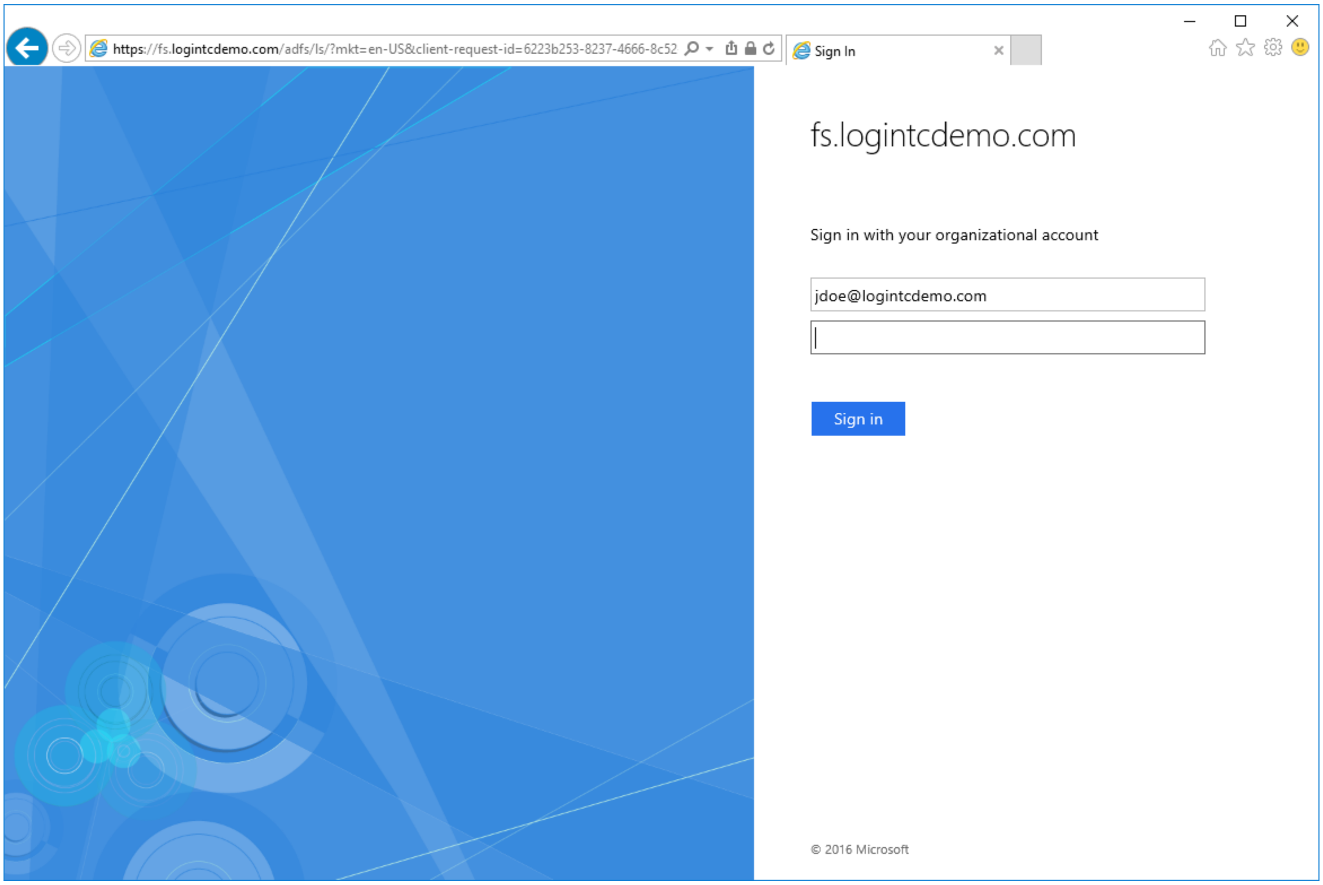
```
Set-AdfsResponseHeaders -SetHeaderName "Content-Security-Policy" -SetHeaderValue
"frame-src 'self' https://cloud.logintc.com"
```

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

Usage

User Usage

Users continue using AD FS-protected services as they did before, except now when they log in they will be presented with a second step to perform LoginTC authentication before they can access their AD FS-protected services.



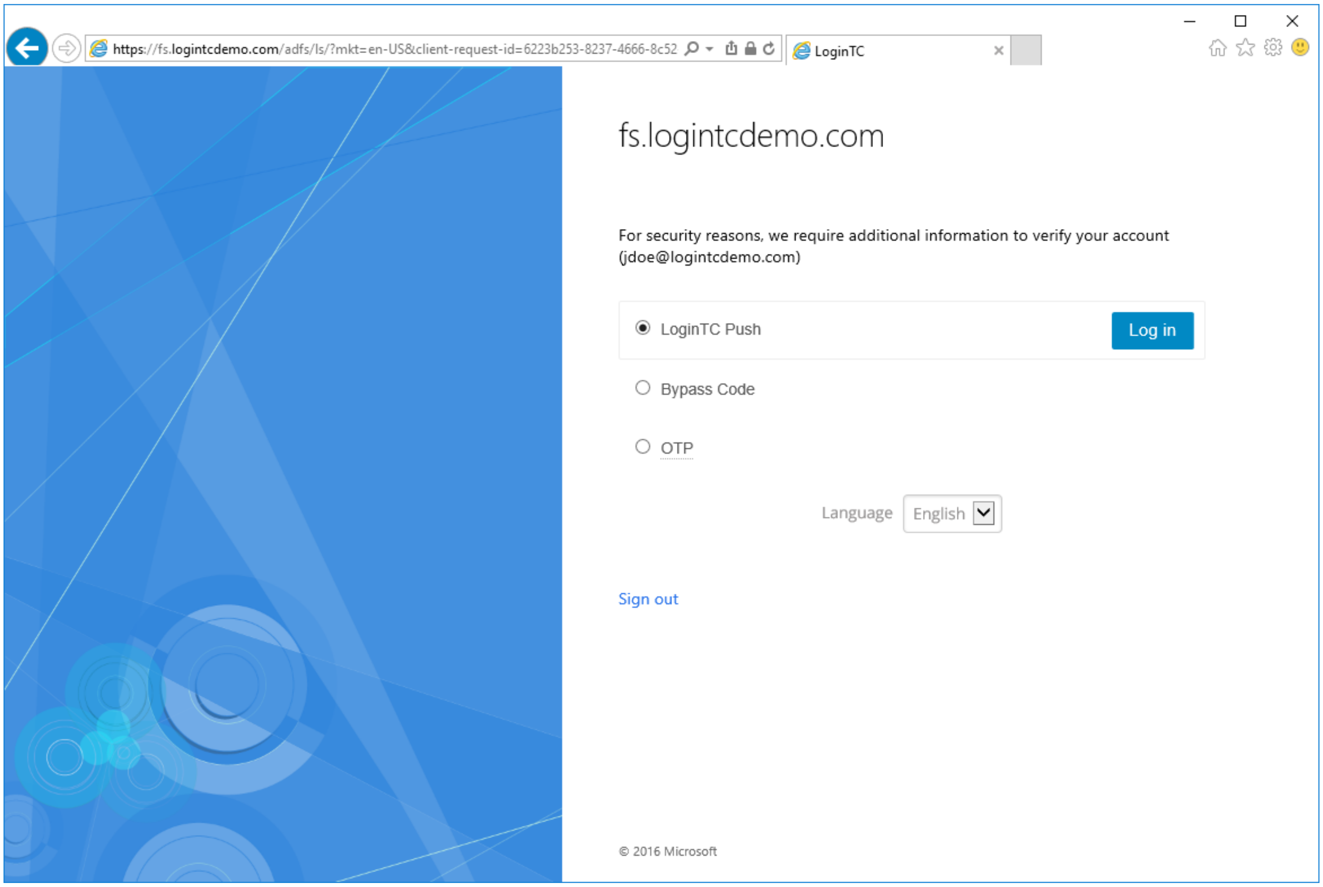
https://fs.logintcdemo.com/adfs/ls/?mkt=en-US&client-request-id=6223b253-8237-4666-8c52
Sign In

fs.logintcdemo.com

Sign in with your organizational account

jdoe@logintcdemo.com

© 2016 Microsoft



https://fs.logintcdemo.com/adfs/ls/?mkt=en-US&client-request-id=6223b253-8237-4666-8c52
LoginTC

fs.logintcdemo.com

For security reasons, we require additional information to verify your account (jdoe@logintcdemo.com)

● LoginTC Push

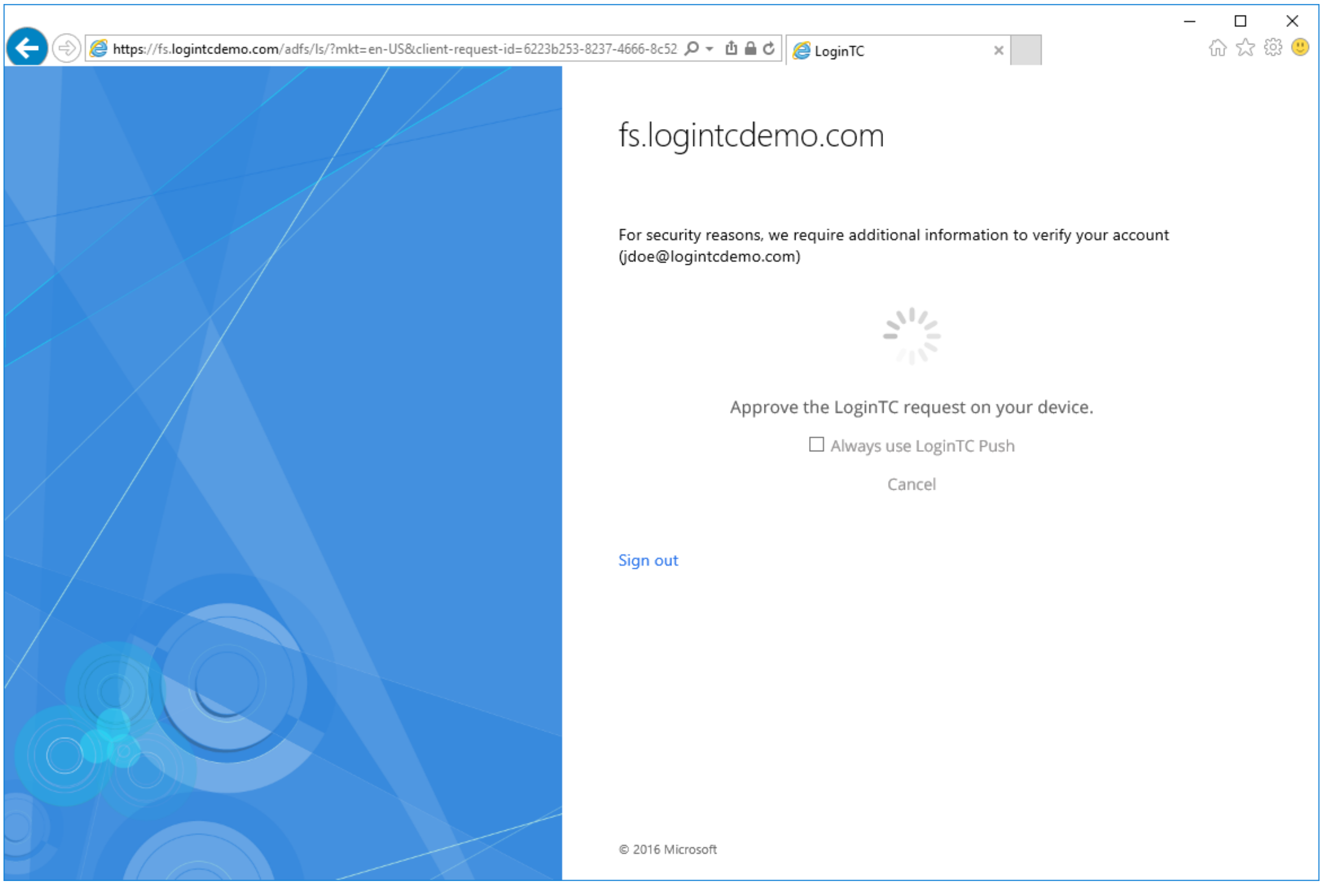
○ Bypass Code

○ OTP

Language English

© 2016 Microsoft

After successfully authenticating with their username and password, the user is presented with options to log in with LoginTC. The user may select to authenticate using LoginTC push, bypass codes, or OTPs. The page is presented to the user in French or English depending on the user's system and browser language settings.



https://fs.logintcdemo.com/adfs/ls/?mkt=en-US&client-request-id=6223b253-8237-4666-8c52
LoginTC

fs.logintcdemo.com

For security reasons, we require additional information to verify your account (jdoe@logintcdemo.com)

Approve the LoginTC request on your device.

☐ Always use LoginTC Push

Cancel

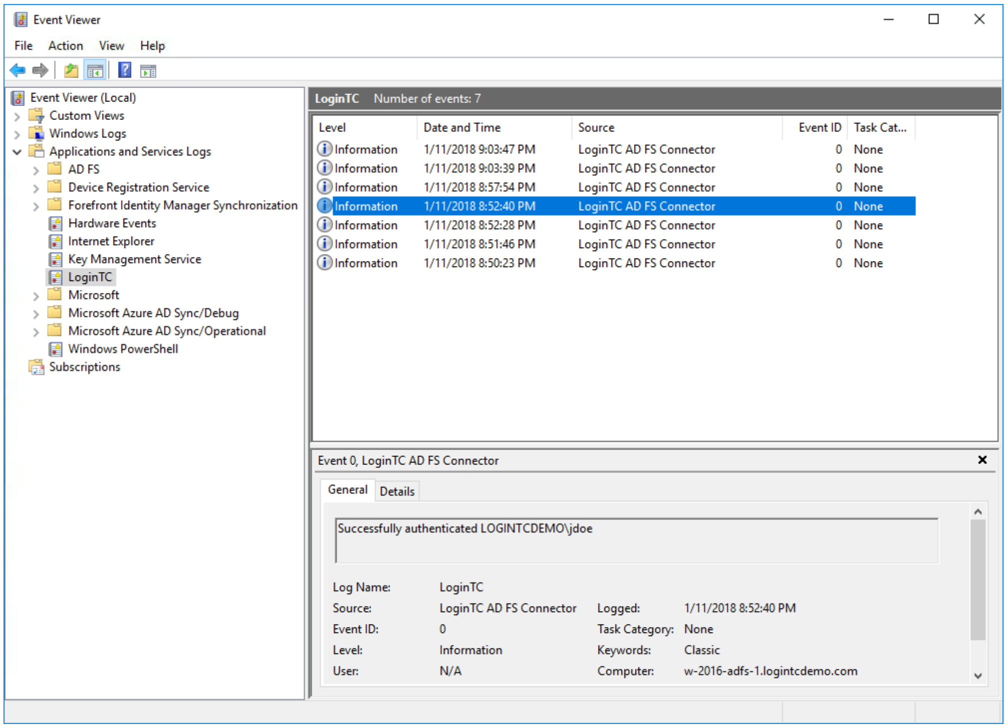
Sign out

© 2016 Microsoft

If the user selects LoginTC push, they are informed to approve the LoginTC request on their device. The user is also presented with an option to remember their LoginTC login choice. The next time the user logs in they will automatically receive a LoginTC push notification. The user may also cancel the login attempt and return to the login page.

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**.



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.