Two-factor authentication for AD FS on Windows Server 2012 R2

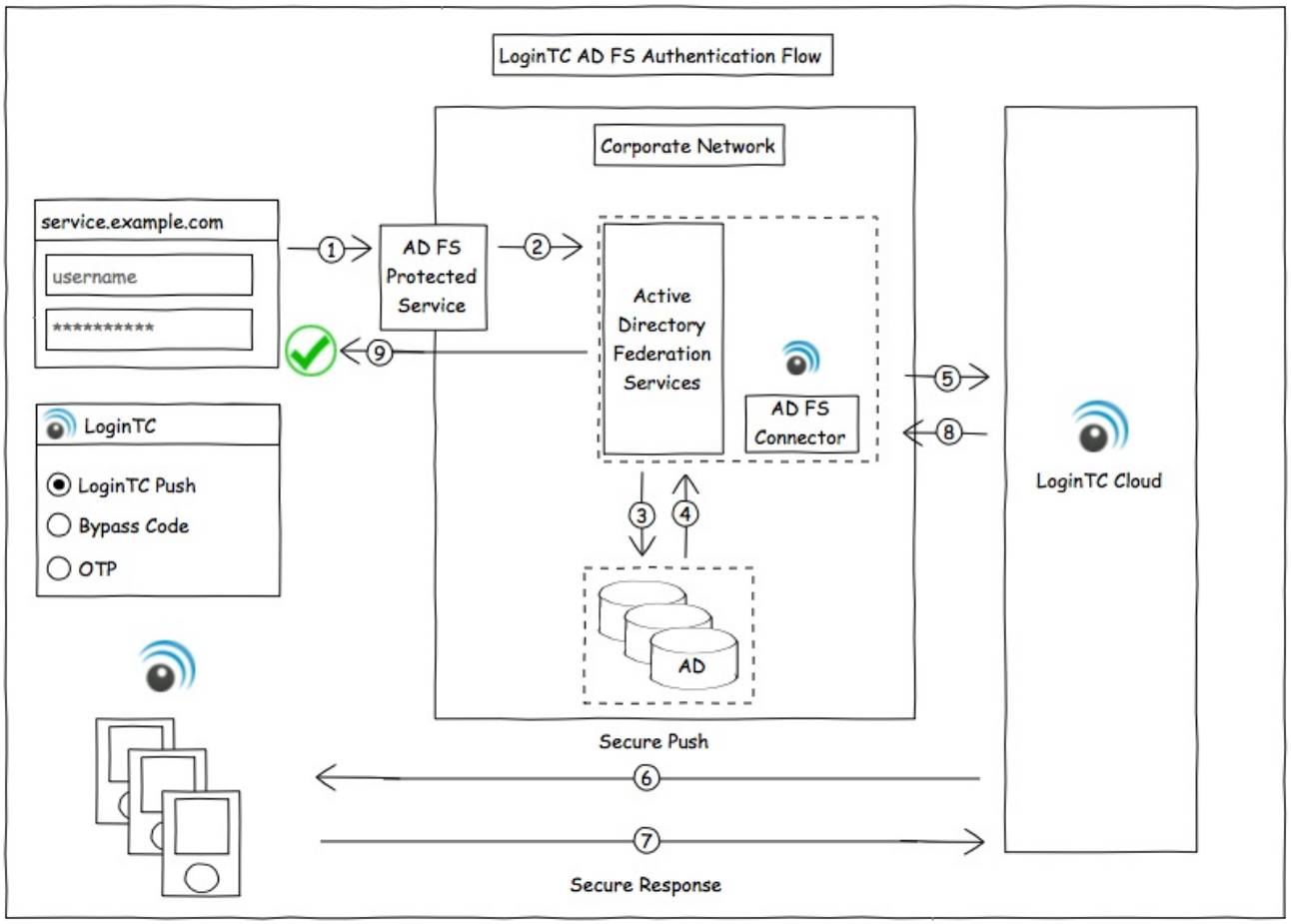
logintc.com/docs/connectors/adfs.html

Windows Server 2012 R2

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

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.



Architecture and Authentication Flow

Subscription Requirement

Your organizatoin 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.

Prerequisites

Before proceeding, please ensure you have the following:

- LoginTC Admin account
- Microsoft Windows Server 2012 R2
- Active Directory Federation Services (AD FS) role

Working AD FS Deployment

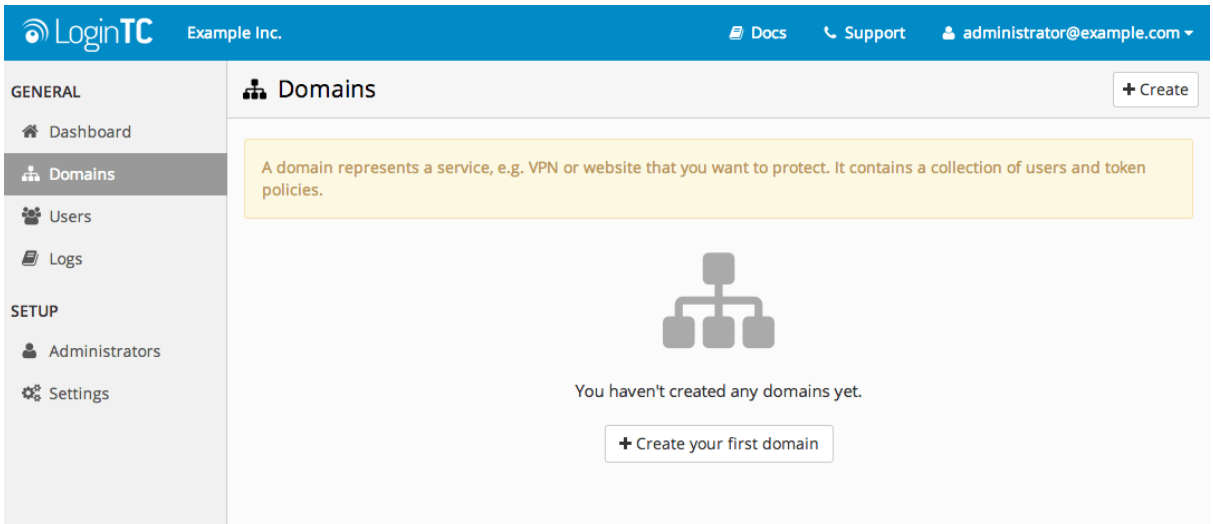
It is strongly recommended that you have a working and tested AD FS deployment with at least one service prior to adding LoginTC authentication.

LoginTC Domain Creation

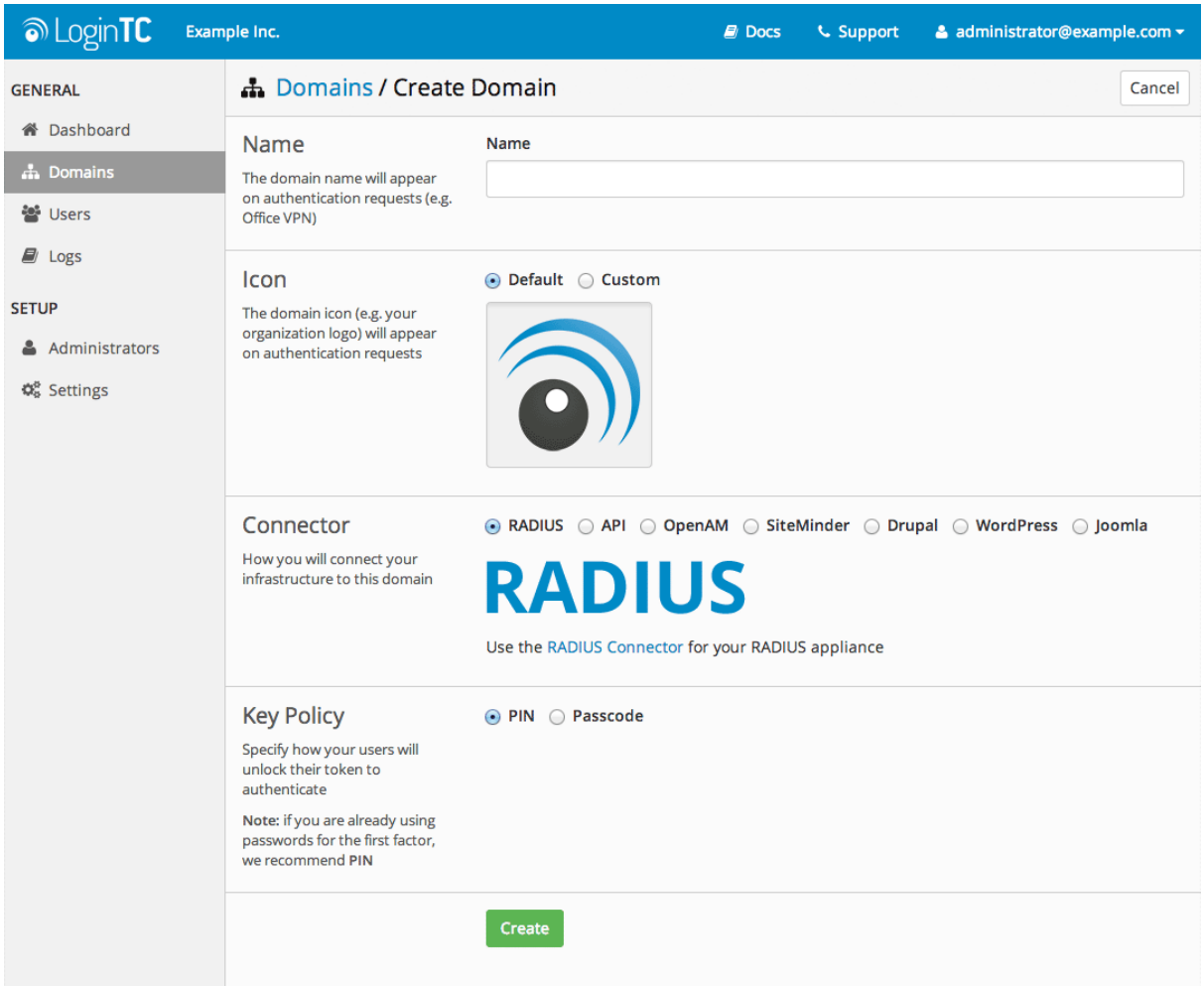
Create a LoginTC domain in LoginTC Admin. The domain represents a service (e.g. your corporate AD FS) that you want to protect with LoginTC. It will contain token policies and the users that access your service.

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**:



4. Enter domain information:

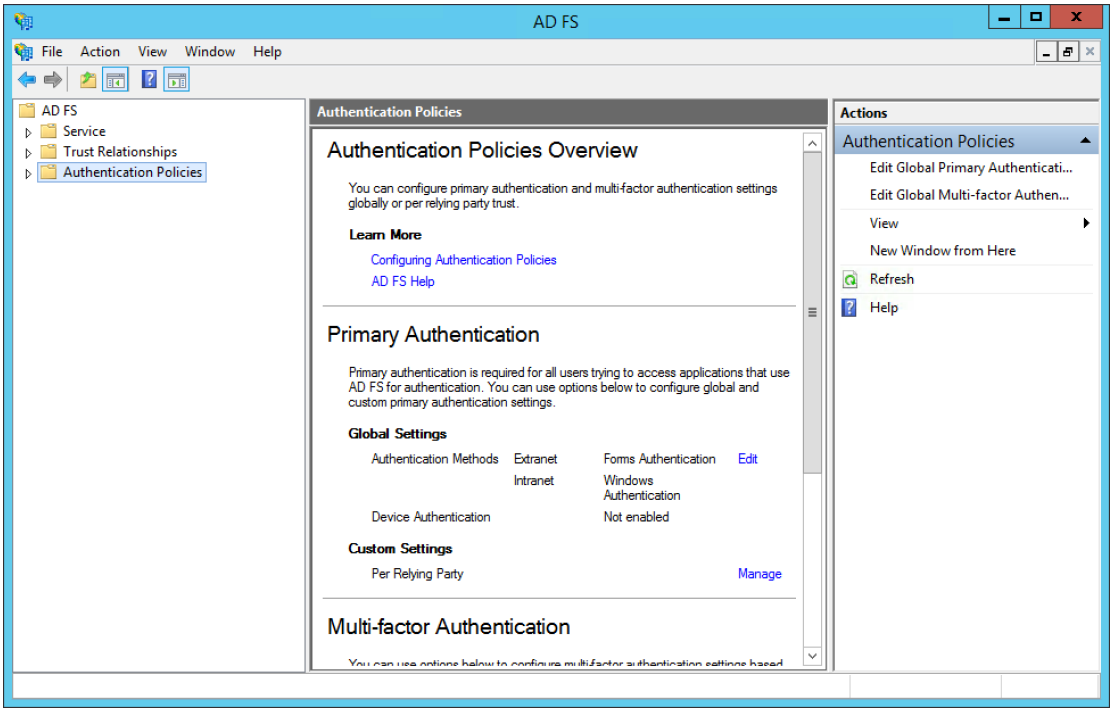


Installation

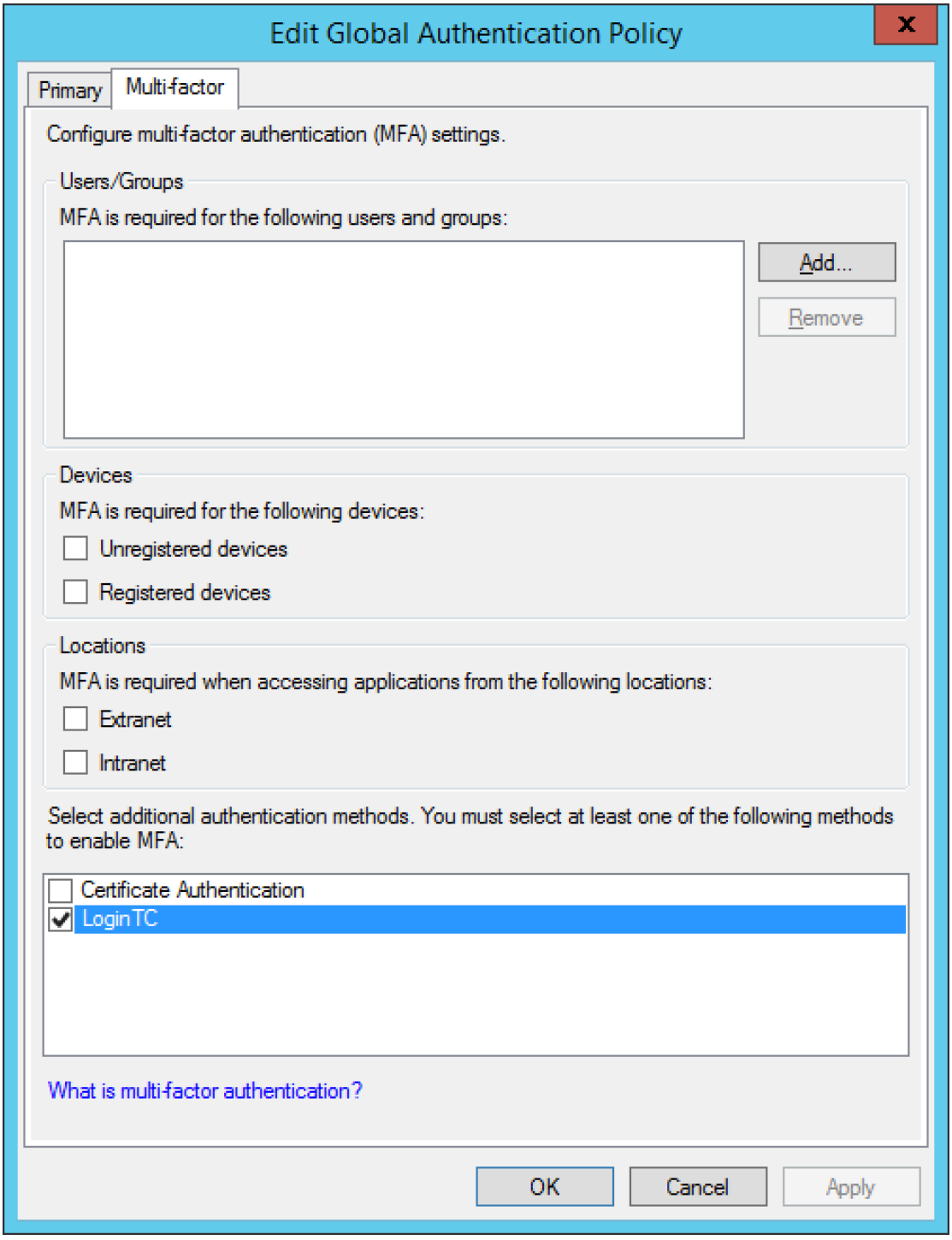
AD FS Configuration

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

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



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

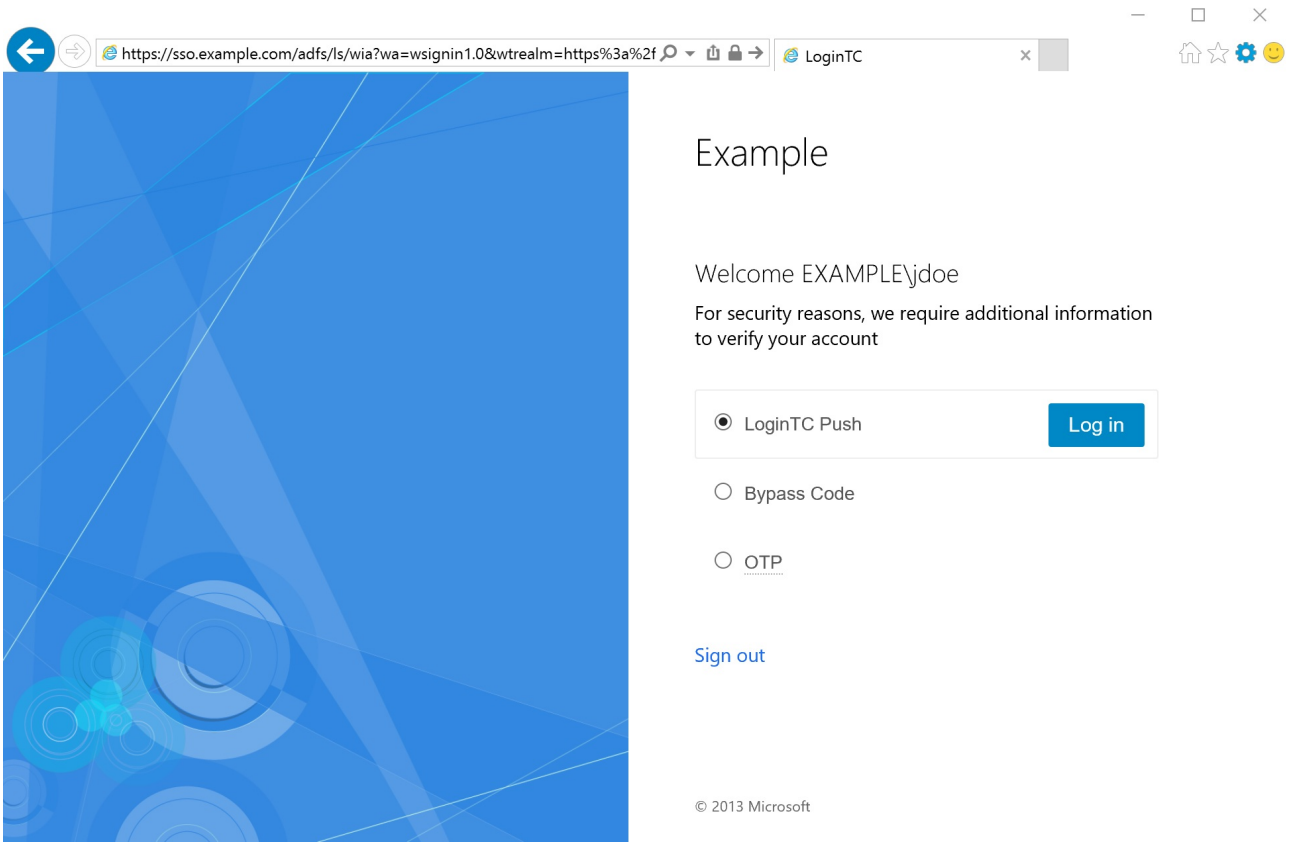


4. Configure which users are required to use MFA.
5. Check **LoginTC** in the list of MFA methods.
6. Press **Apply**.

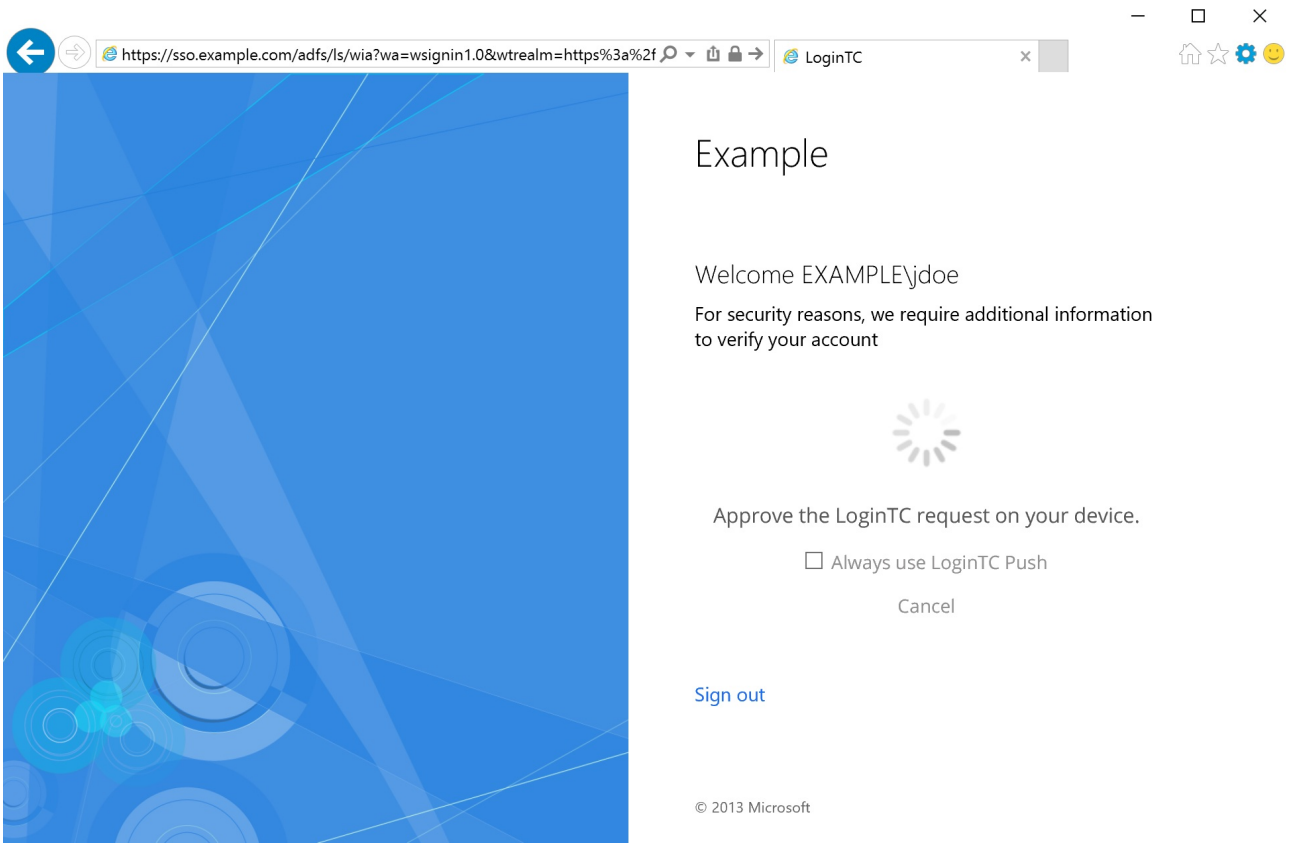
Usage

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.



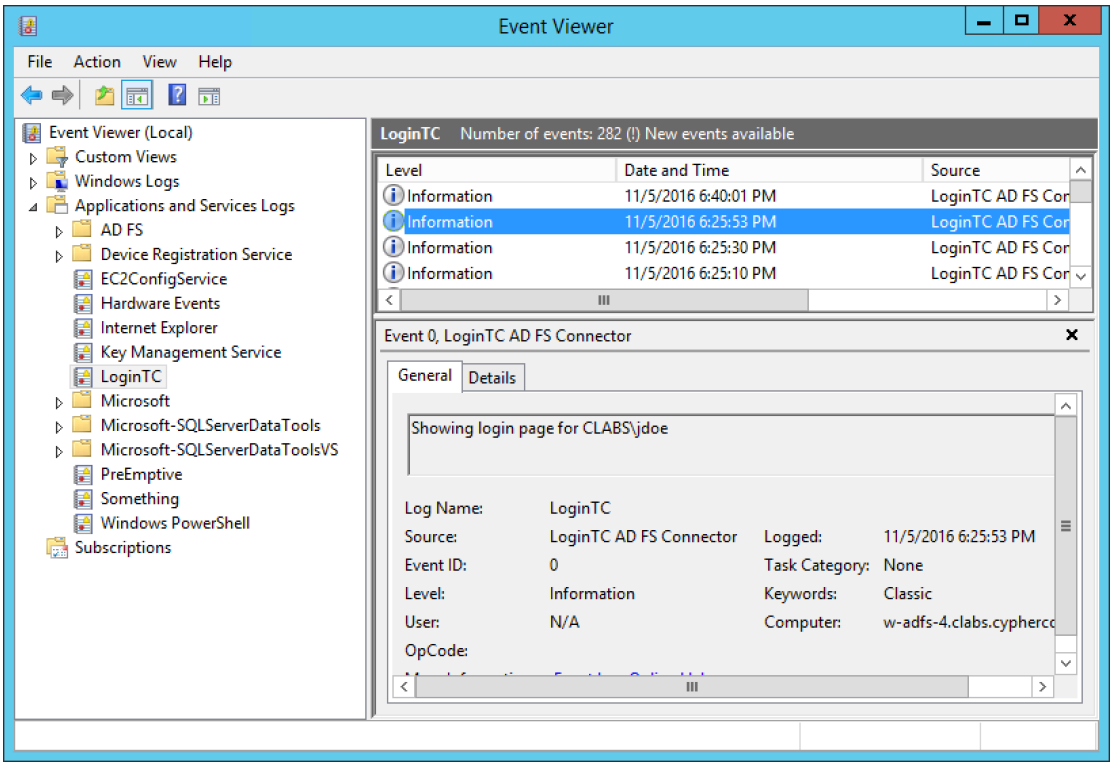
After successfully authenticating with their username and password, the user is presented with options to log in with LoginTC. The user may select to authenticate using LoginTC push, bypass codes, or OTPs. The page is presented to the user in French or English depending on the user's system and browser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



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**.



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.

Email Support

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