Dropbox Two-Factor Authentication (2FA)

logintc.com/docs/connectors/adfs-dropbox

Overview

The LoginTC AD FS Connector protects access to your Microsoft Active Directory Federation Services (AD FS) by adding a <u>second factor</u> 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 Dropbox Enterprise account.

Subscription Requirement

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

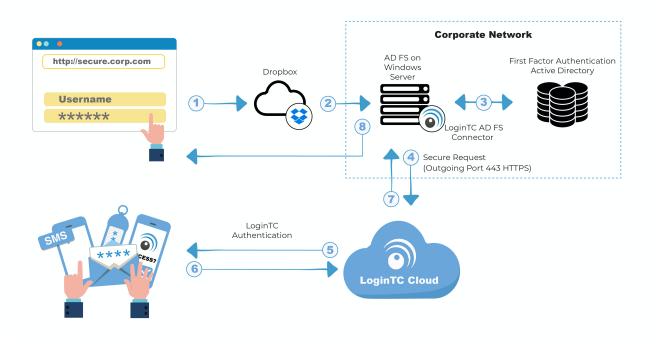
User Experience

After 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.

Θ
ਸ਼ੇ :
×
b ,

- LoginTC Push
- <u>OTP</u>

Architecture



Authentication Flow

- 1. A user attempts access to Dropbox 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)
- 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 Dropbox

Prerequisites

Before proceeding, please ensure you have the following:

- Dropbox configured with federation to your on-premise AD FS
- LoginTC Admin Panel account
- Active Directory Federation Services (AD FS) Host, Microsoft Windows Server 2016 (or Windows Server 2012)

Working Dropbox Federation Deployment

It is strongly recommended that you have a working Dropbox with federation against your on-premise AD FS prior to adding LoginTC multi-factor authentication. Please see the

guide, <u>How do I connect Dropbox to AD FS 3.0 for single sign-on (SSO)</u> to configure your Dropbox to use your on-premise AD FS.

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 <u>Installation</u>.

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".

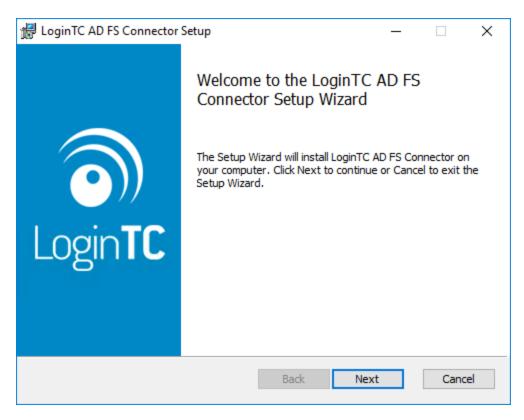
Configure Normalize Usernames from the Domain settings by navigating to **Domains >** Your Domain > Settings.

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



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

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.	LoginTC AD FS Connector Setup	—		>
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	End-User License Agreement		1	
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	Please read the following license agreement carefully			0
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				
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	End User License Agreement			^
	SOFTWARE AND DOCUMENTATION ("SOFTWARE"), TO THE TERMS OF THIS EULA. IF YOU DO NOT THE TERMS OF THIS EULA, DO NOT DOWNLOAD, ACCESS OR USE THE SOFTWARE. THIS EULA CON DISCLAIMERS OF WARRANTIES AND LIMITATIONS LIABILITY AND EXCLUSIVE REMEDIES. THE PRO	YOU AG AGREE INSTAI TAINS OF VISION	GREE TO LL,	×
	✓ I accept the terms in the License Agreement			
☑ I accept the terms in the License Agreement	Print Back Nex	+	Can	cel
	Phile Dock Nex		Can	

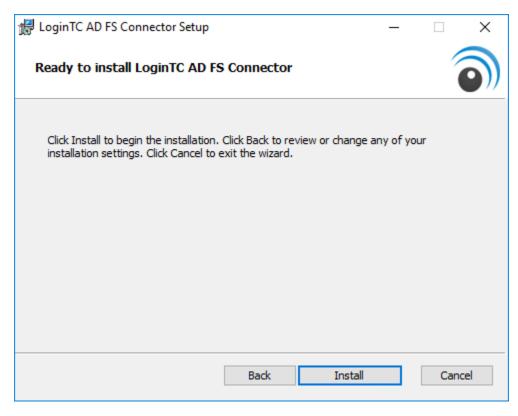
5. Change the **LoginTC API Host** only if you have a private enterprise LoginTC deployment. Press **Next**:

🖟 Configuration: LoginTC		_		×
Configuration: LoginTC			1	3
Configure how the connector communicates with Log	inTC		(D)
LoginTC API Host:				
cloud.logintc.com]
The fully qualified domain name (FQDN) of the LoginTC have a private LoginTC enterprise deployment. The de cloud.logintc.com.				
Bad	< Next		Cano	el

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		1	3
Configure how the connector communicates with LoginTC			D))
Application ID:			
The 40-character hexadecimal LoginTC application identifier.			
Application API Key:			
Appleadon Ari Ney.			
I The 64-character alphanumeric LoginTC application API key.			
The official acter alphanument Login C application Art key.			
Back	w.t	Cano	·al
DACK	Xt	Cano	.ei

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



Configuration for AD FS Dropbox 2FA

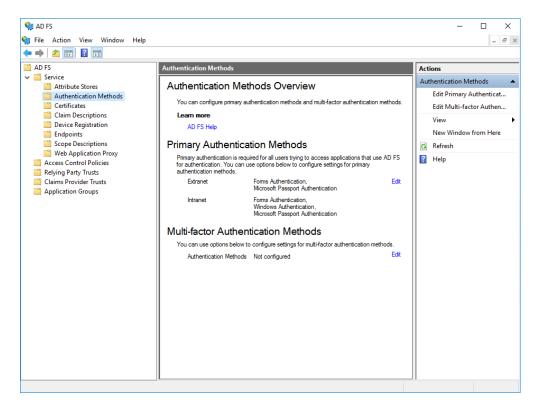
Windows Server 2016 (AD FS version 4.0)

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 <u>AD FS Configuration in Two-factor authentication for AD FS on Windows Server 2012 R2</u>.

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.



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

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

Select additional authentication methods. You must select at least one of the following methots or enable MFA:	rimary	Multi-factor	
Azure MFA	Select : to enab	Idditional authentication methods. You must select at least one of the following e MFA:	g method:
Azure MFA		ificate Authentication	
	🗌 Azu	re MFA	
What is multifactor authentication?	✓ Log	nTC	
What is multi-factor authentication?			
What is multifactor authentication?			
	What is	multi-factor authentication?	
	TTTIGE IS		
		OK Cancel	Apply

- 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

🐐 AD FS				– 🗆 X
翰 File Action View Window Help				- 8 ×
🗢 🔿 🗾 🖬				,
📫 AD FS	Relying Party Trusts			Actions
Service Attribute Stores	Display Name	Enabled T	Type Identifier	Relying Party Trusts
Attribute Stores	Microsoft Office 365 Identity Platform	Yes V	WS-T https://login.i	n Add Relying Party Trust
Certificates				View
Claim Descriptions				New Window from Here
Device Registration Endpoints				Q Refresh
Scope Descriptions				P Help
Web Application Proxy				
Access Control Policies Relying Party Trusts				
Claims Provider Trusts				
Application Groups				
	<		2	

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

9. Press Apply and OK

Ed	it Access Control Policy for Microsoft Office 3	65 Identity Platform	×
Ac	ccess 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 Permit everyone and require MFA from extranet		
	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		
		OK Cancel Apply	

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

Usage

<u>User Usage</u>

The user proceeds to the Dropbox sign in page as they normally would where they enter their username.

			– 🗆 X
 🔎 👻 🤷 Dropbox, Inc [US]	😻 Dropbox	×	슈 숬 铩 🙂
			×
			~
Sign in			
Sign in or create an account			
or create an account			
jdoe@logintcdemo.com	×		
Juoe@logintedenio.com	^		
Single sign-on enabled			
Remember me			
Continue			
or Log in with Dropbox credentia	als		
G Sign in with Google			

The user is brought to your on-premise AD FS where they are prompted to enter their username and password.

د الله الله://fs.logintcdemo.com/adfs/ls?RelayState=eyJwcm92aWRIcI91cm، ک	D - ① 畠 む <i>餐</i> Sign In 🛛 🗙	- □ × 命☆戀ಅ
	fs.logintcdemo.com	
	Sign in with your organizational account	
	jdoe@logintcdemo.com	×
	Password	
	Sign in	
	© 2016 Microsoft	

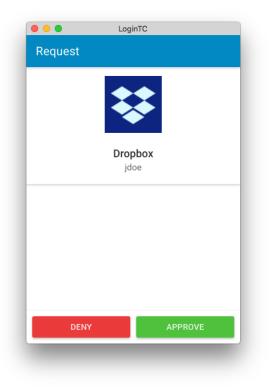
After successfully authenticating with their username and password, the user is presented with options to log in with LoginTC. The user may select to authenticate using LoginTC push, bypass codes, or OTPs.

https://fs.logintcdemo.com/adfs/ls?RelaySta		□ × 命☆戀 [@]
	fs.logintcdemo.com	
	For security reasons, we require additional information to verify your account (jdoe@logintcdemo.com)	_
	LoginTC Push	
	O Bypass Code	
	O <u>otp</u>	
	Language English	
	Sign out	
	© 2016 Microsoft	

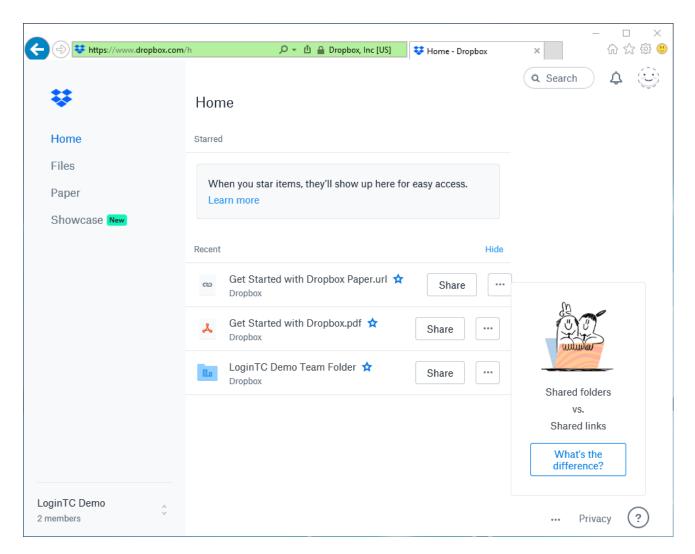
If the user selects LoginTC push, they are informed to approve the LoginTC request on their device. The user is also presented with an option to remember their LoginTC login choice. The next time the user logs in they will automatically receive a LoginTC push notification. The user may also cancel the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

Https://fs.logintcdemo.com/adfs/ls?RelaySt	ate=eyJwcm92aWRIcl91cmv
	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

The user receives a push notification on their device where they have provisioned their LoginTC token.



After successfully authenticating with LoginTC, the user is redirected back to Dropbox.



Logging

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

🛃 Event Viewer					-	×
File Action View Help						
🗧 🔿 📶 🔢 🖬						
	LeginTC Number Level information information information information information information information information information information	Date and Time 1/11/2018 9:03:47 PM 1/11/2018 9:03:39 PM 1/11/2018 8:57:54 PM 1/11/2018 9:52:40 PM 1/11/2018 9:52:28 PM 1/11/2018 8:51:46 PM 1/11/2018 8:50:23 PM	Source LoginTC AD FS Co LoginTC AD FS Co	nnector nnector nnector nnector nnector nnector	nt ID Task Cat 0 None 0 None 0 None 0 None 0 None 0 None	ĸ
	General Details	5 uthenticated LOGINTCDEMO\jr	doe			^

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.