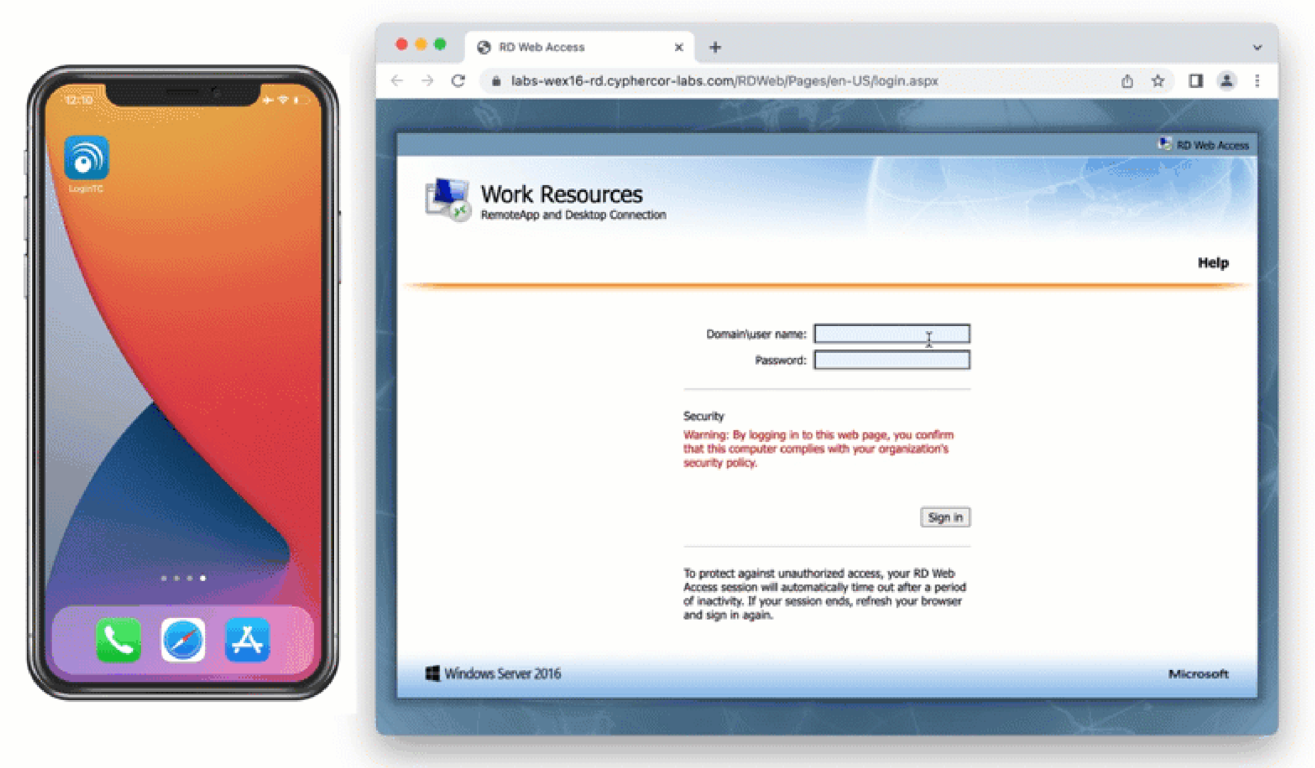
RDWeb 2FA Two-Factor Authentication - LoginTC

logintc.com/docs/connectors/rd-web-access


12:10
LoginTC
RD Web Access
labs-wex16-rd.cyphercor-labs.com/RDWeb/Pages/en-US/login.aspx
RD Web Access
Work Resources
RemoteApp and Desktop Connection
Help
Sign in
Windows Server 2016
Microsoft

Domain\user name:

Password:

Security

Warning: By logging in to this web page, you confirm that this computer complies with your organization's security policy.

To protect against unauthorized access, your RD Web Access session will automatically time out after a period of inactivity. If your session ends, refresh your browser and sign in again.

Overview

The LoginTC RD Web Access Connector protects access to your Microsoft Remote Desktop Web Access by adding a second factor LoginTC challenge to existing username and password authentication. The connector protects both web and RemoteApp web feed access, and works in conjunction with the LoginTC RD Gatway SSO Connector to provide a seamless and protected Remote Desktop experience.

If you would like to protect just your RD Gateway without protecting RD Web Access then you may be interested in the: LoginTC RD Gateway with RADIUS Connector.

Subscription Requirement

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

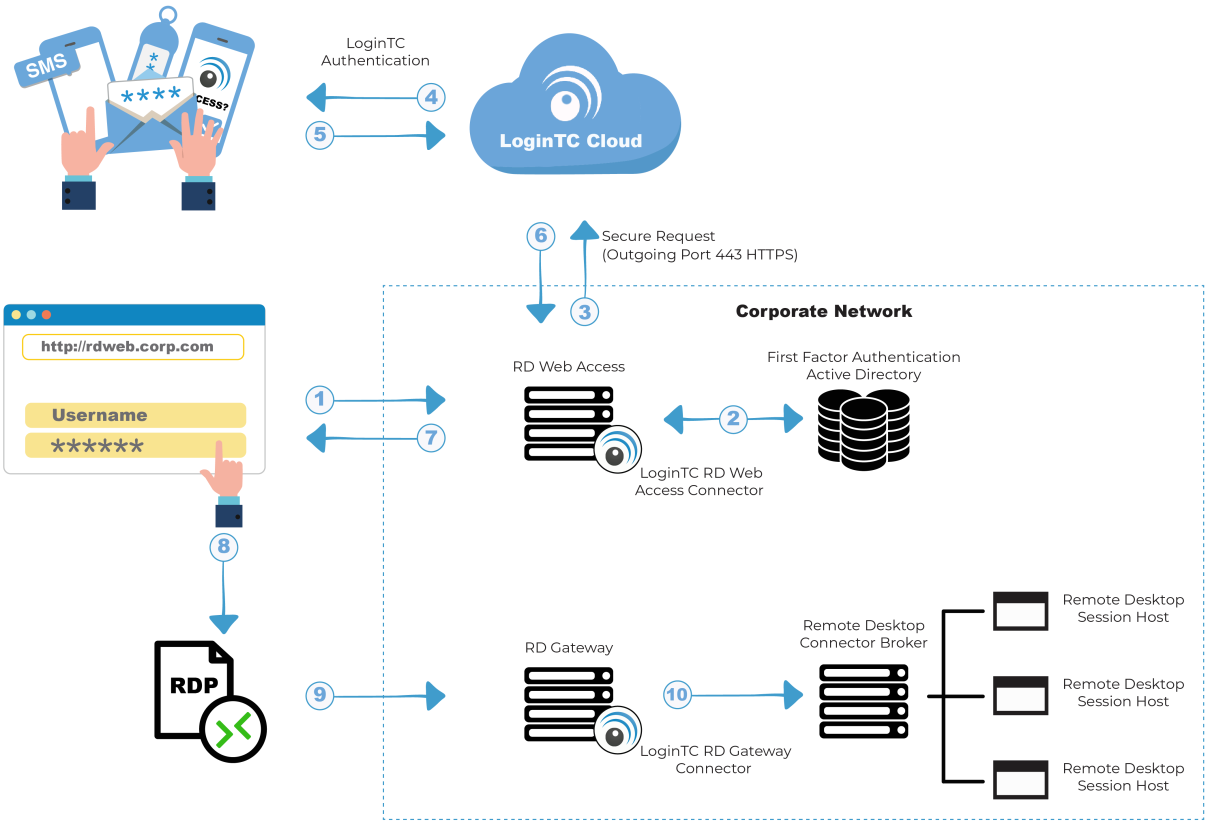
User Experience

After entering the username and password into the RD Web Access 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/1mc0rYjtQlI

Architecture



SMS
****
LoginTC Authentication
4
5
LoginTC Cloud
6
Secure Request (Outgoing Port 443 HTTPS)
3
Corporate Network
http://rdweb.corp.com
Username
******
1
7
RD Web Access
First Factor Authentication Active Directory
2
LoginTC RD Web Access Connector
8
RDP
9
RD Gateway
10
Remote Desktop Connector Broker
LoginTC RD Gateway Connector
Remote Desktop Session Host
Remote Desktop Session Host
Remote Desktop Session Host

Authentication Flow

1. A user attempts access to Remote Desktop Web Access with username / password
2. The username / password is verified against an existing first factor directory (i.e. Active Directory)
3. The request is trapped by LoginTC RD Web Access Connector and an authentication request is made to LoginTC Cloud Services
4. Secure push notification request sent to the user's mobile or desktop device
5. User response (approval or denial of request) sent to LoginTC Cloud Services
6. The LoginTC RD Web Access Connector validates the user response
7. User is granted access to RD Web Access portal
8. User clicks on one of the available applications / remote desktop sessions from the portal
9. The RDP file connects with Remote Desktop Gateway
10. The LoginTC RD Gateway Connector validates the RDP file and the user is granted access to remote resource

Prerequisites

Before proceeding, please ensure you have the following:

- LoginTC Admin Panel account
- Microsoft Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 or Windows Server 2022
- Remote Desktop Web Access role
- Remote Desktop RD Gateway role (may be on the same host as the RD Web Access role)
- Working Remote Desktop Web Access Deployment
- .NET Framework 4.5.2 or higher

Working Remote Desktop Web Access Deployment

It is strongly recommended that you have a working and tested Remote Desktop Web Access deployment 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 RD Web 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**.

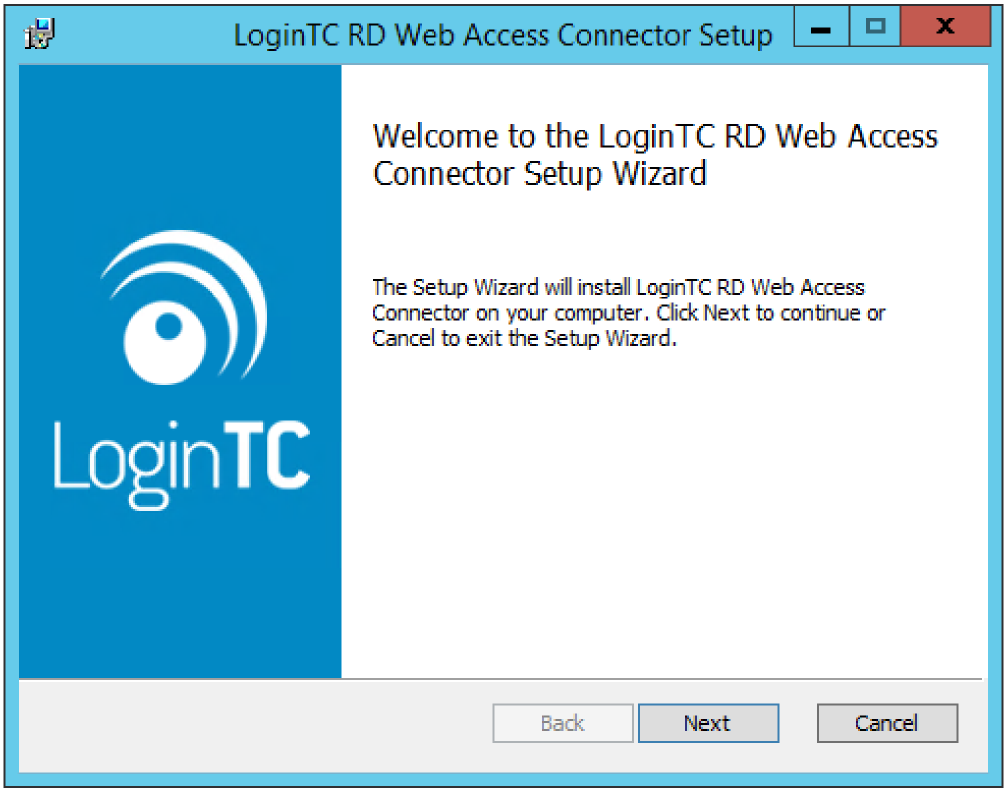
Select `Yes, Normalize Usernames` scroll down and click `Update`.

Installation (RD Web Access)

Follow the instructions to install the LoginTC RD Web Access Connector on a server with the RD Web Access role:

1. Download the latest version of the LoginTC RD Web Access Connector
2. Run the installer file as a privileged administrator user.

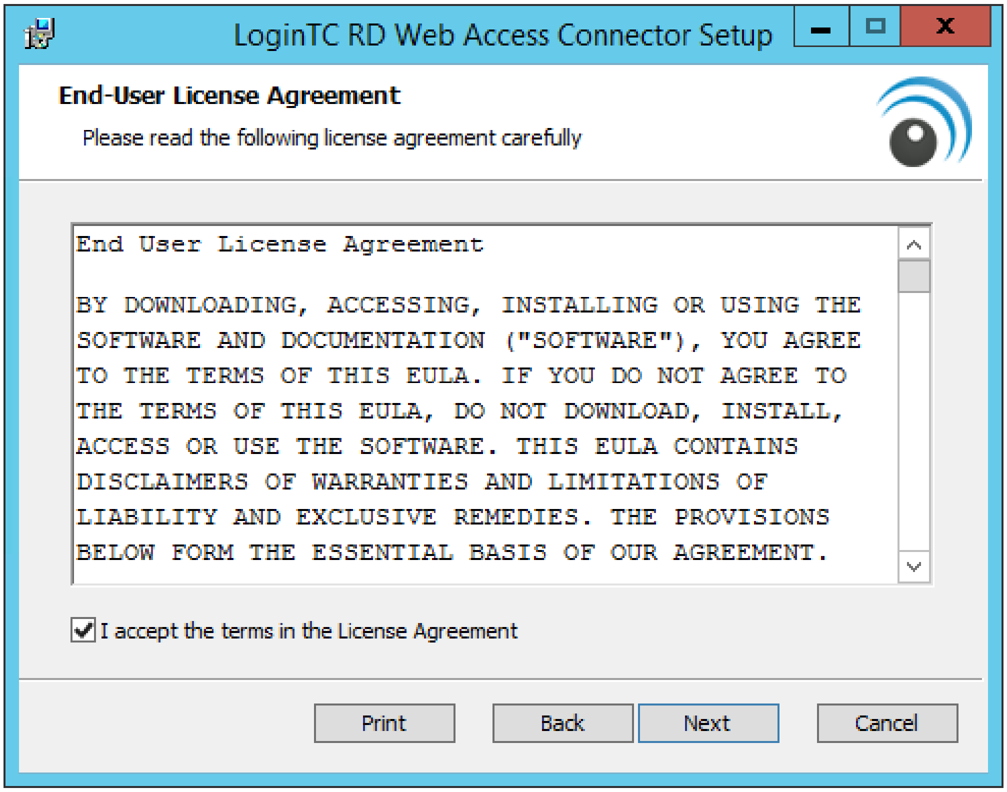
3. Press **Next**.



Welcome to the LoginTC RD Web Access Connector Setup Wizard

The Setup Wizard will install LoginTC RD Web Access 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.



End-User License Agreement

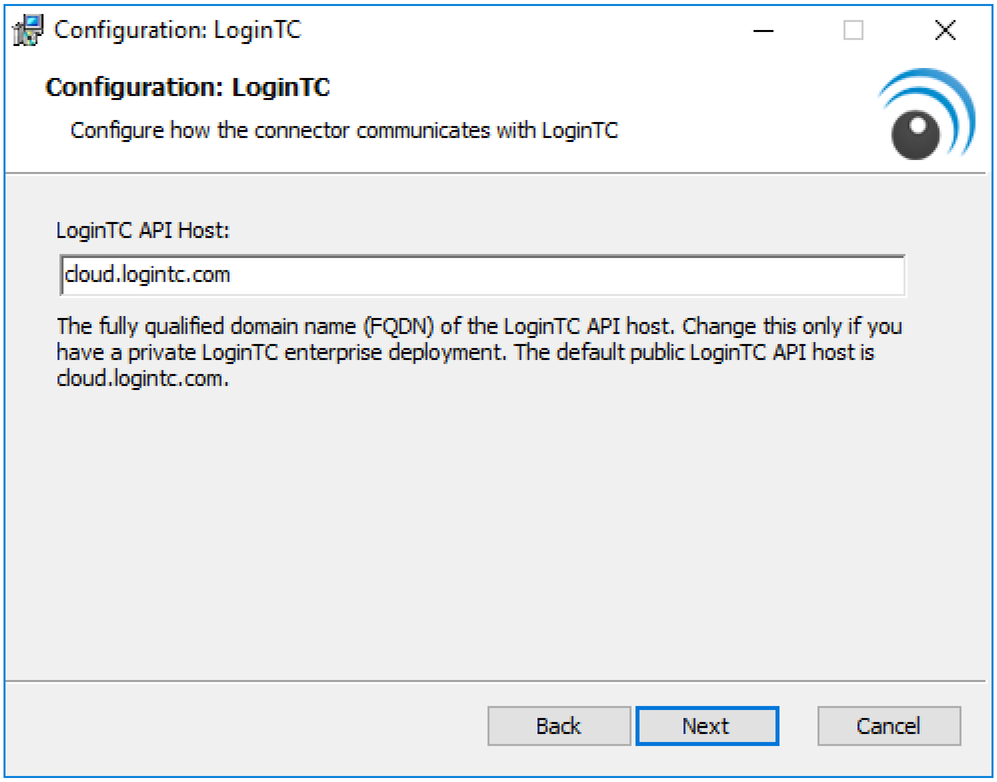
Please read the following license agreement carefully

```
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

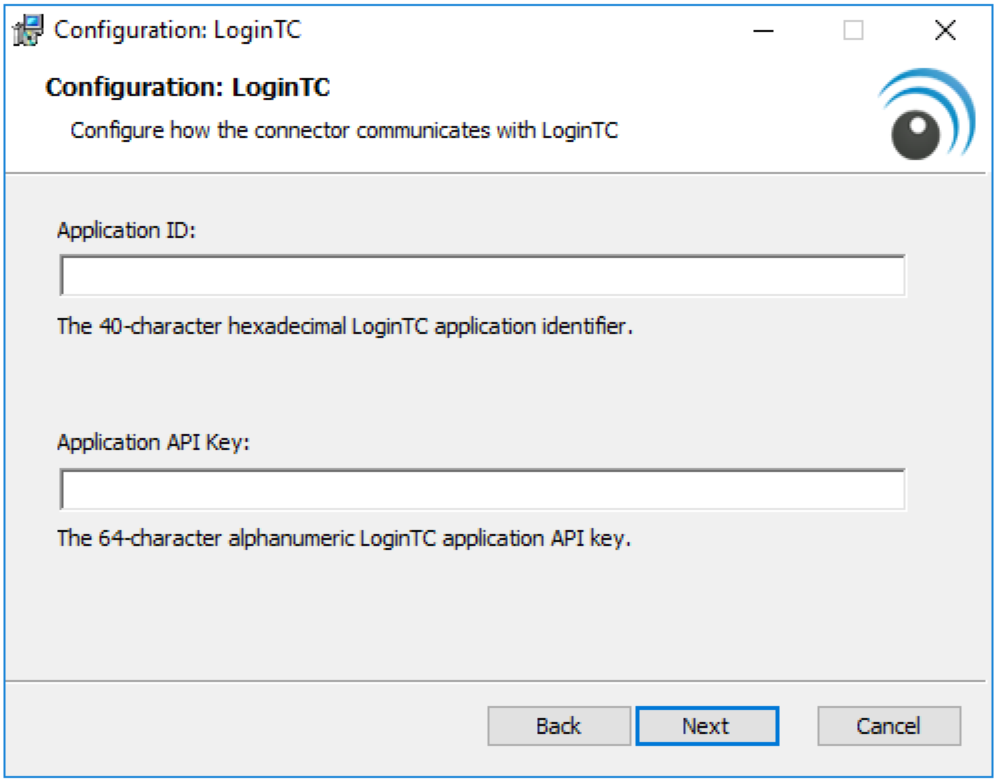
Configure how the connector communicates with LoginTC

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

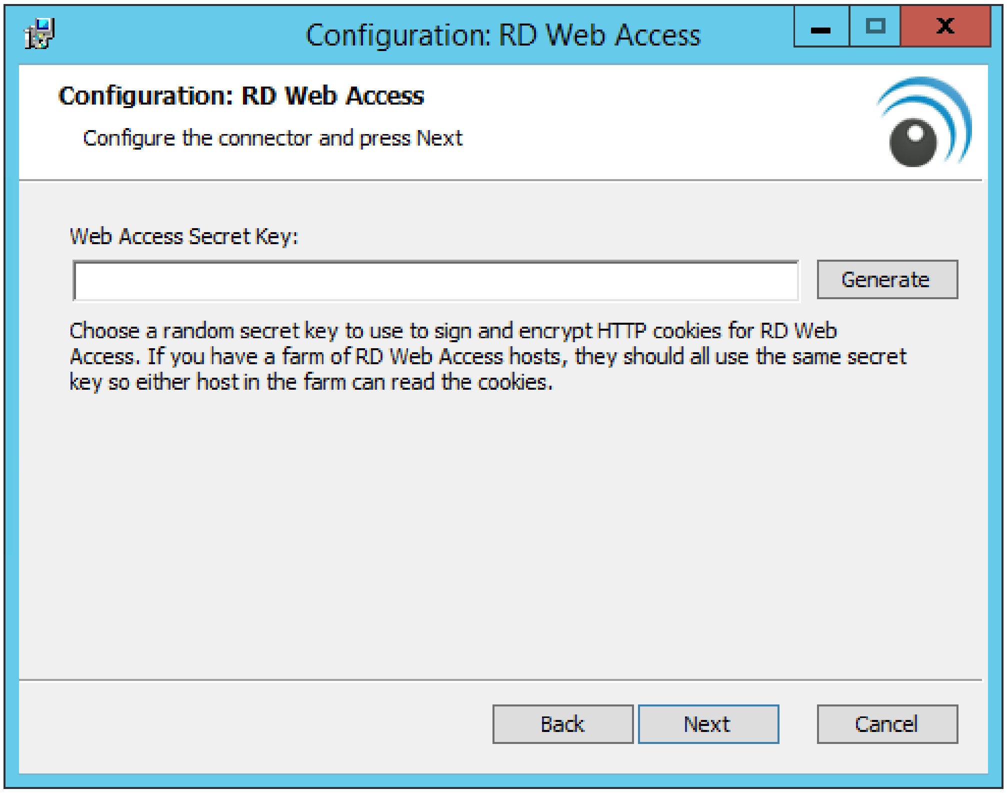
Application ID:

The 40-character hexadecimal LoginTC application identifier.

Application API Key:

The 64-character alphanumeric LoginTC application API key.

7. Choose a secret to use for encrypting and signing RD Web Access sessions. If you already have an RD Web Access secret key, then enter it. Press **Next**.



Configuration: RD Web Access

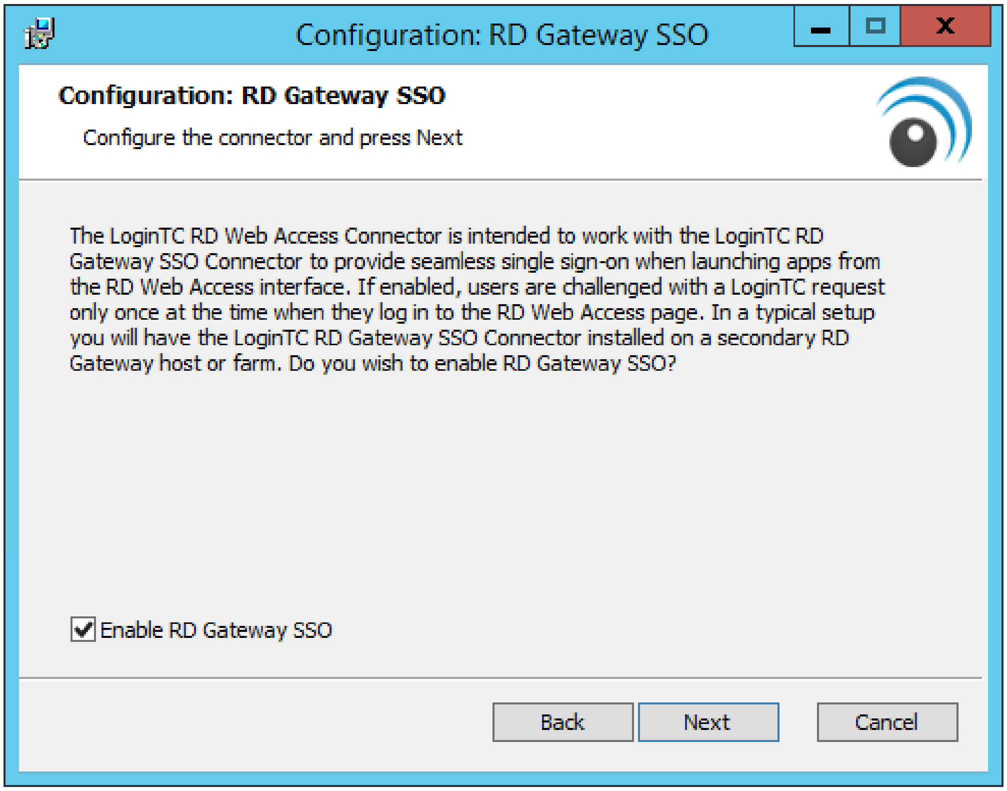
Configuration: RD Web Access

Configure the connector and press Next

Web Access Secret Key:

Choose a random secret key to use to sign and encrypt HTTP cookies for RD Web Access. If you have a farm of RD Web Access hosts, they should all use the same secret key so either host in the farm can read the cookies.

8. Enable **RD Gateway SSO** if you plan to install the LoginTC RD Gateway SSO Connector on your RD Gateway server. Press **Next**.



Configuration: RD Gateway SSO

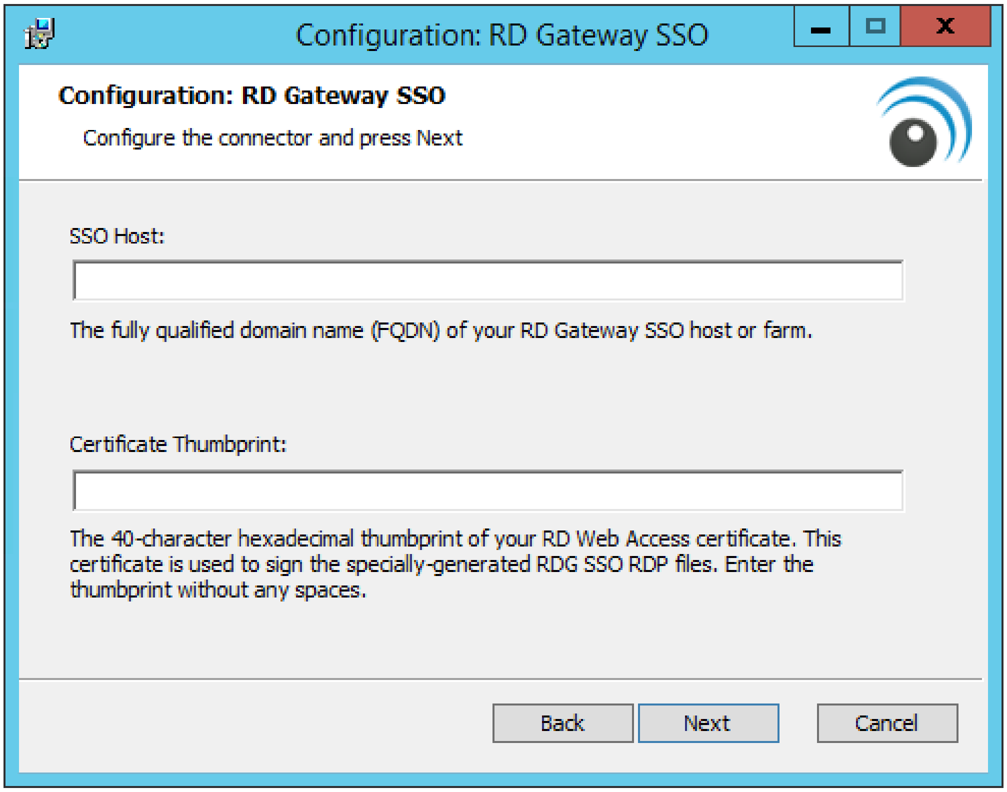
Configuration: RD Gateway SSO

Configure the connector and press Next

The LoginTC RD Web Access Connector is intended to work with the LoginTC RD Gateway SSO Connector to provide seamless single sign-on when launching apps from the RD Web Access interface. If enabled, users are challenged with a LoginTC request only once at the time when they log in to the RD Web Access page. In a typical setup you will have the LoginTC RD Gateway SSO Connector installed on a secondary RD Gateway host or farm. Do you wish to enable RD Gateway SSO?

☑ Enable RD Gateway SSO

9. Enter your RD Gateway details. See Appendix A: RDP Cert for more information about the signing certificate.



Configuration: RD Gateway SSO

Configuration: RD Gateway SSO

Configure the connector and press Next

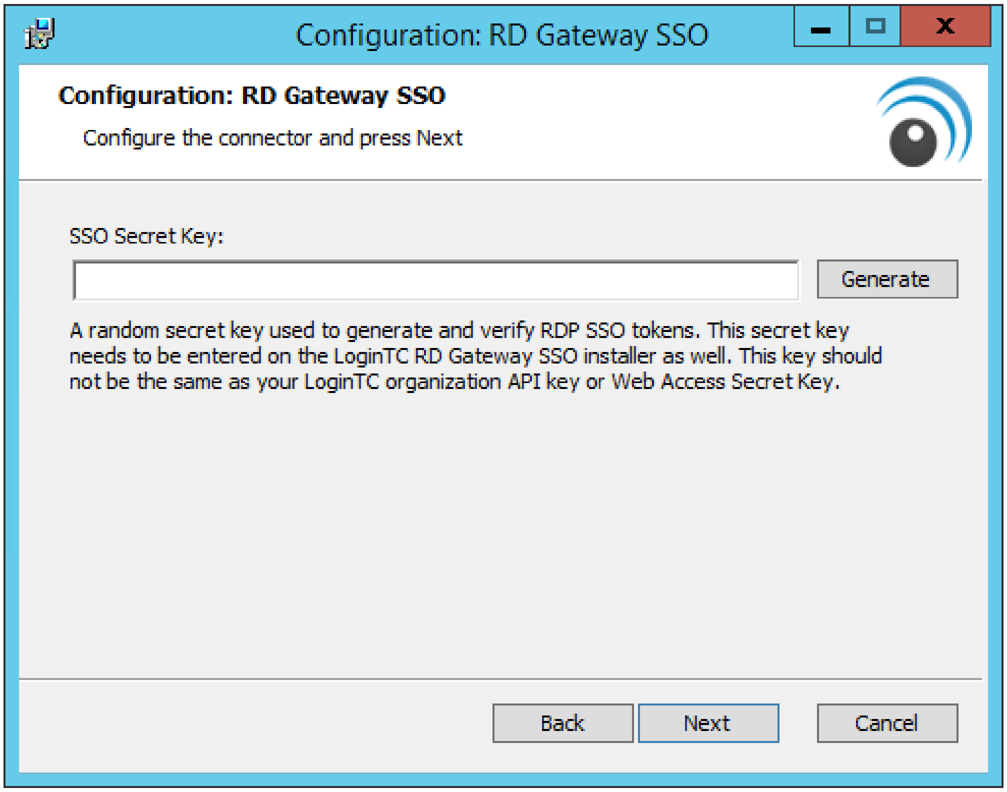
SSO Host:

The fully qualified domain name (FQDN) of your RD Gateway SSO host or farm.

Certificate Thumbprint:

The 40-character hexadecimal thumbprint of your RD Web Access certificate. This certificate is used to sign the specially-generated RDG SSO RDP files. Enter the thumbprint without any spaces.

10. Choose a RD Gateway **SSO Secret Key** to use to generate RDG SSO access tokens. Save this key as you will need it for the LoginTC RD Gateway SSO Connector installation. Press **Next**.



Configuration: RD Gateway SSO

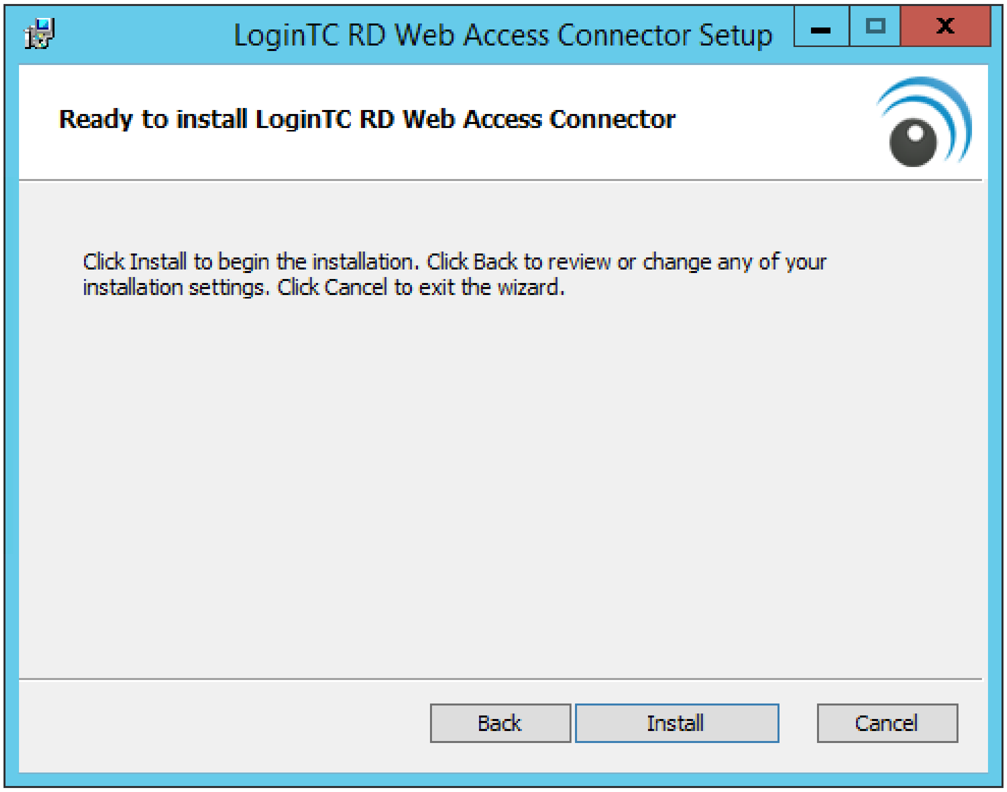
Configuration: RD Gateway SSO

Configure the connector and press Next

SSO Secret Key:

A random secret key used to generate and verify RDP SSO tokens. This secret key needs to be entered on the LoginTC RD Gateway SSO installer as well. This key should not be the same as your LoginTC organization API key or Web Access Secret Key.

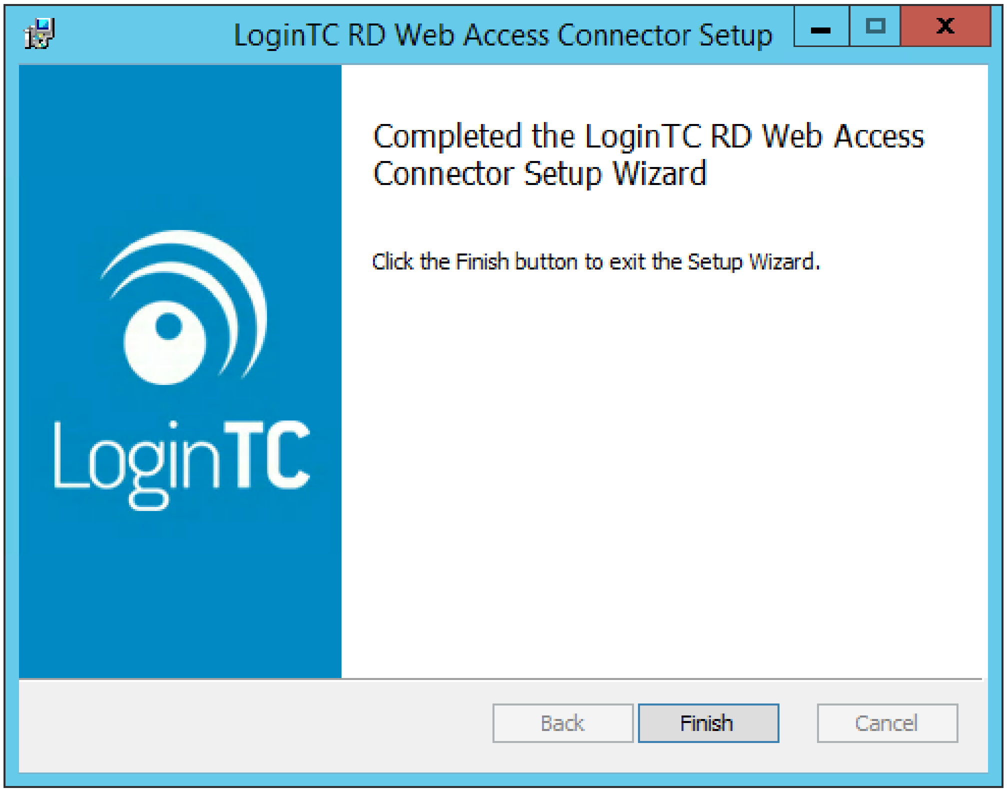
11. Press **Next**.



Ready to install LoginTC RD Web Access Connector

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

12. Press **Finish**



Completed the LoginTC RD Web Access Connector Setup Wizard

Click the Finish button to exit the Setup Wizard.

The LoginTC RD Web Access Connector is now installed and protecting your RD Web Access. If you selected to use RD Gateway SSO, you should now open the LoginTC RD Gateway SSO Connector Administration Guide and follow the instructions to install the LoginTC RD Gateway SSO Connector.

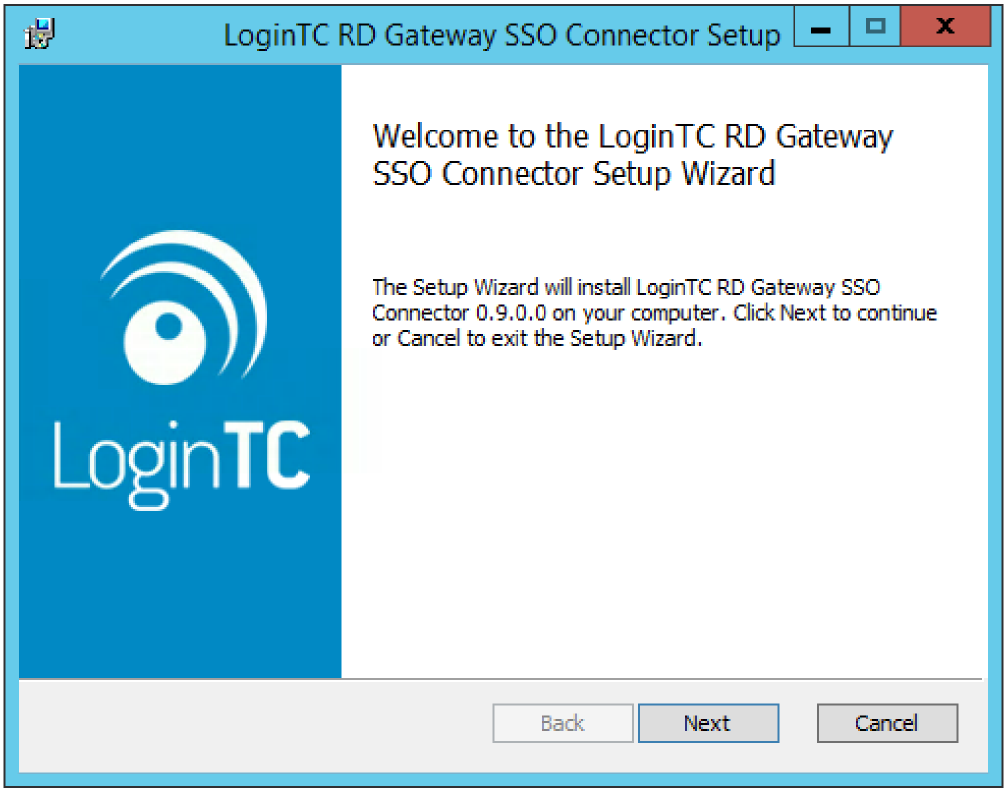
Installation (RD Gateway SSO)

The LoginTC RD Web Access Connector works in conjunction with the LoginTC RD Gateway SSO Connector to protect access to your Microsoft Remote Desktop Gateway with a second-factor LoginTC challenge. To install the LoginTC RD Gateway SSO Connector on a server with the RD Gateway role:

IIS service reset

The installer will restart IIS services upon completion and this will impact other dependent services. We recommend performing these actions during a change windows.

1. Download the latest version of the LoginTC RD Gateway SSO Connector
2. Run the installer file as a priviliged administrator user. The user must have permission to configure and restart IIS.
3. Press **Next**.

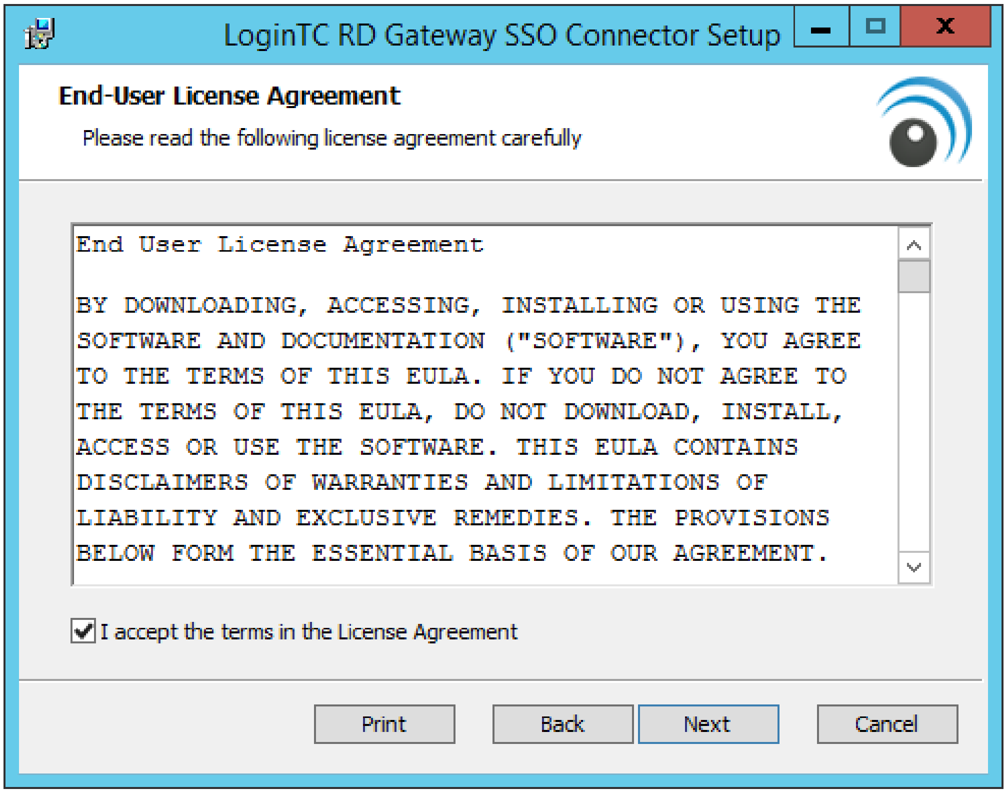


LoginTC RD Gateway SSO Connector Setup

Welcome to the LoginTC RD Gateway SSO Connector Setup Wizard

The Setup Wizard will install LoginTC RD Gateway SSO Connector 0.9.0.0 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.



End-User License Agreement

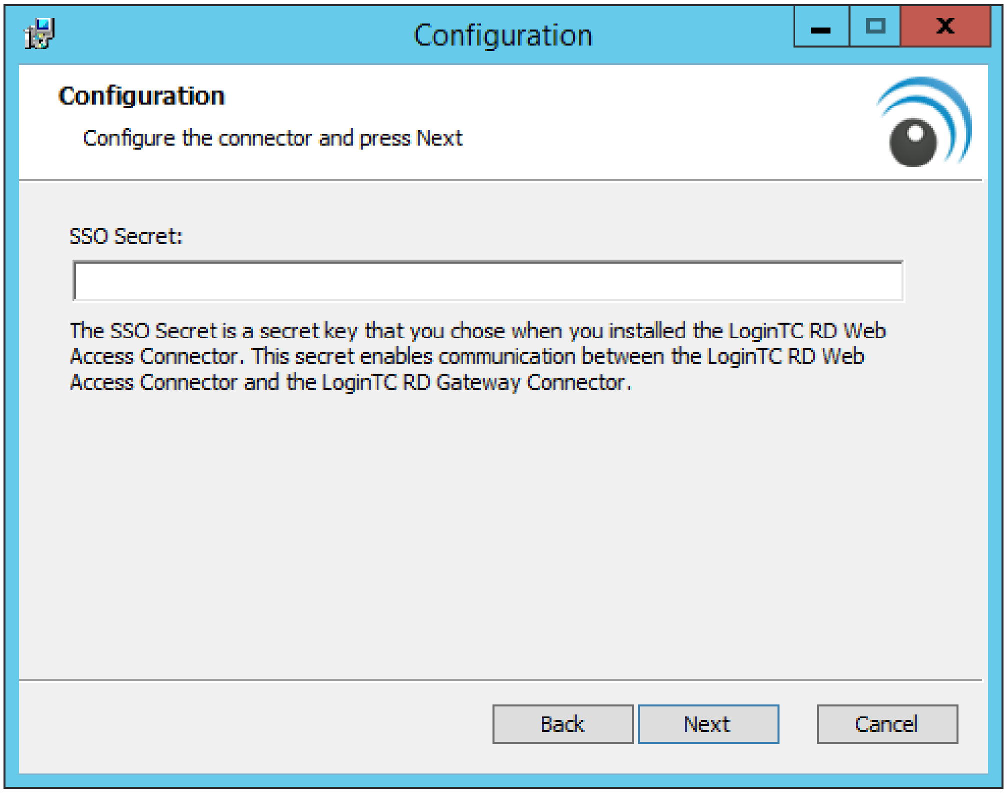
Please read the following license agreement carefully

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. Enter the **SSO Secret** that you set when you installed the LoginTC RD Web Access Connector. Press **Next**.



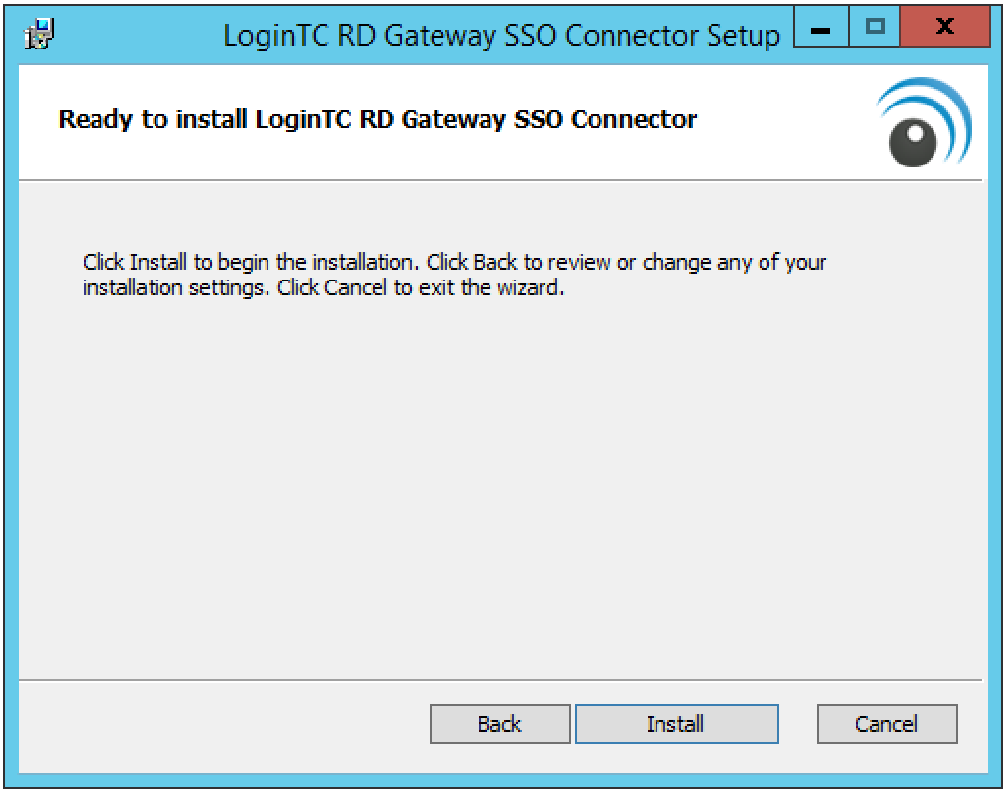
Configuration

Configure the connector and press Next

SSO Secret:

The SSO Secret is a secret key that you chose when you installed the LoginTC RD Web Access Connector. This secret enables communication between the LoginTC RD Web Access Connector and the LoginTC RD Gateway Connector.

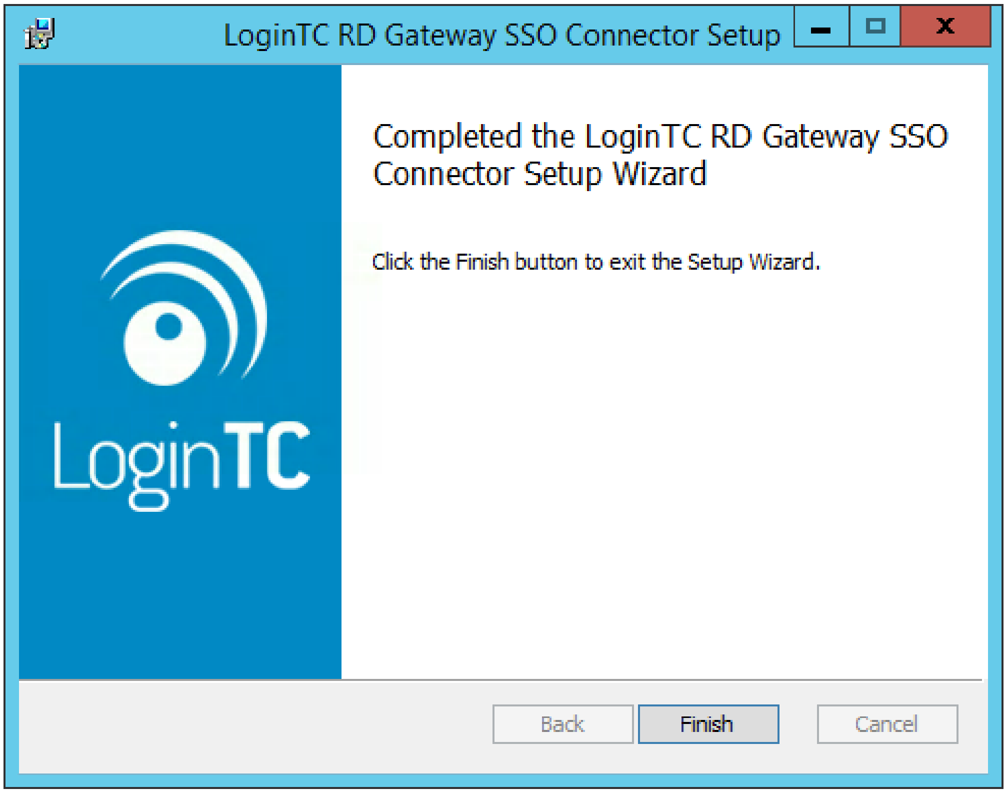
6. Press **Install**.



Ready to install LoginTC RD Gateway SSO Connector

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

7. Press **Finish**.



Completed the LoginTC RD Gateway SSO Connector Setup Wizard

Click the Finish button to exit the Setup Wizard.

Direct RD Gateway Access

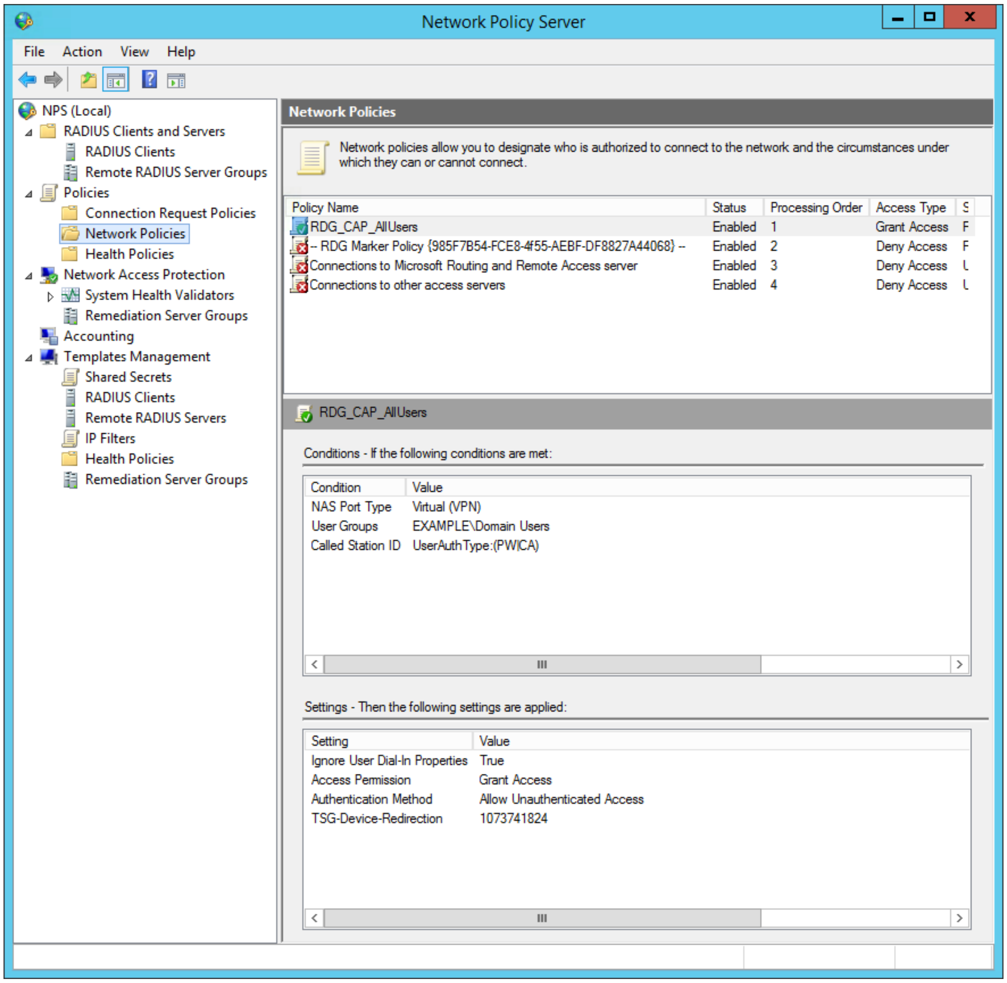
This RD Gateway will only work with RD Gateway SSO access tokens generated by the LoginTC RD Web Access Connector. If you would like your users to still correct directly to the gateway (instead of going through RD Web Access) then you will need a secondary RD Gateway host.

Configuration for RDWeb MFA

Network Policy Server

Perform the following steps on the host running the RD Gateway role where you installed the LoginTC RD Gateway SSO Connector.

1. Open **Network Policy Server** from the Start menu on your host running the LoginTC RD Gateway SSO Connector.
2. Expand the **Policies** → **Network Policies** tree in the side menu.



Network Policies

Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.

Policy Name	Status	Processing Order	Access Type	S
RDG_CAP_AllUsers	Enabled	1	Grant Access	F
-- RDG Marker Policy {985F7B54-FCE8-4f55-AEBF-DF8827A44068} --	Enabled	2	Deny Access	F
Connections to Microsoft Routing and Remote Access server	Enabled	3	Deny Access	U
Connections to other access servers	Enabled	4	Deny Access	U

RDG_CAP_AllUsers

Conditions - If the following conditions are met:

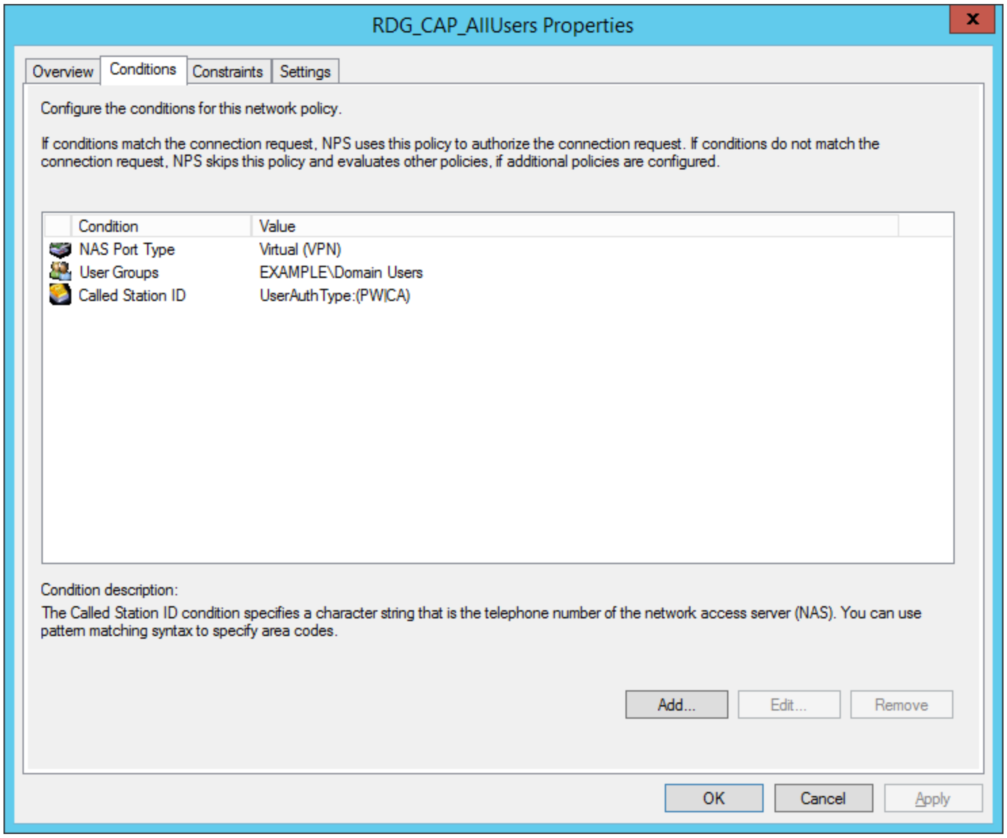
Condition	Value
NAS Port Type	Virtual (VPN)
User Groups	EXAMPLE\Domain Users
Called Station ID	UserAuthType:(PW|CA)

Settings - Then the following settings are applied:

Setting	Value
Ignore User Dial-In Properties	True
Access Permission	Grant Access
Authentication Method	Allow Unauthenticated Access
TSG-Device-Redirection	1073741824

3. Right click on the desired target **RDG CAP** policy (default is **RDG_CAP_AllUsers**) and click on **Properties**

4. Under the Conditions tab, ensure that `CA` is listed in the **Called Station ID** condition: `UserAuthType:(PW|CA)`.



Configure the conditions for this network policy.

If conditions match the connection request, NPS uses this policy to authorize the connection request. If conditions do not match the connection request, NPS skips this policy and evaluates other policies, if additional policies are configured.

Condition	Value
NAS Port Type	Virtual (VPN)
User Groups	EXAMPLE\Domain Users
Called Station ID	UserAuthType:(PW|CA)

Condition description:
The Called Station ID condition specifies a character string that is the telephone number of the network access server (NAS). You can use pattern matching syntax to specify area codes.

5. Press **Apply**.

Usage

Your users may interact with your RD Web Access deployment in several ways. This chapter details the user experience for each interaction.

User Prerequisites

For the best user experience, the end user should use the following environment to access RD Web Access features:

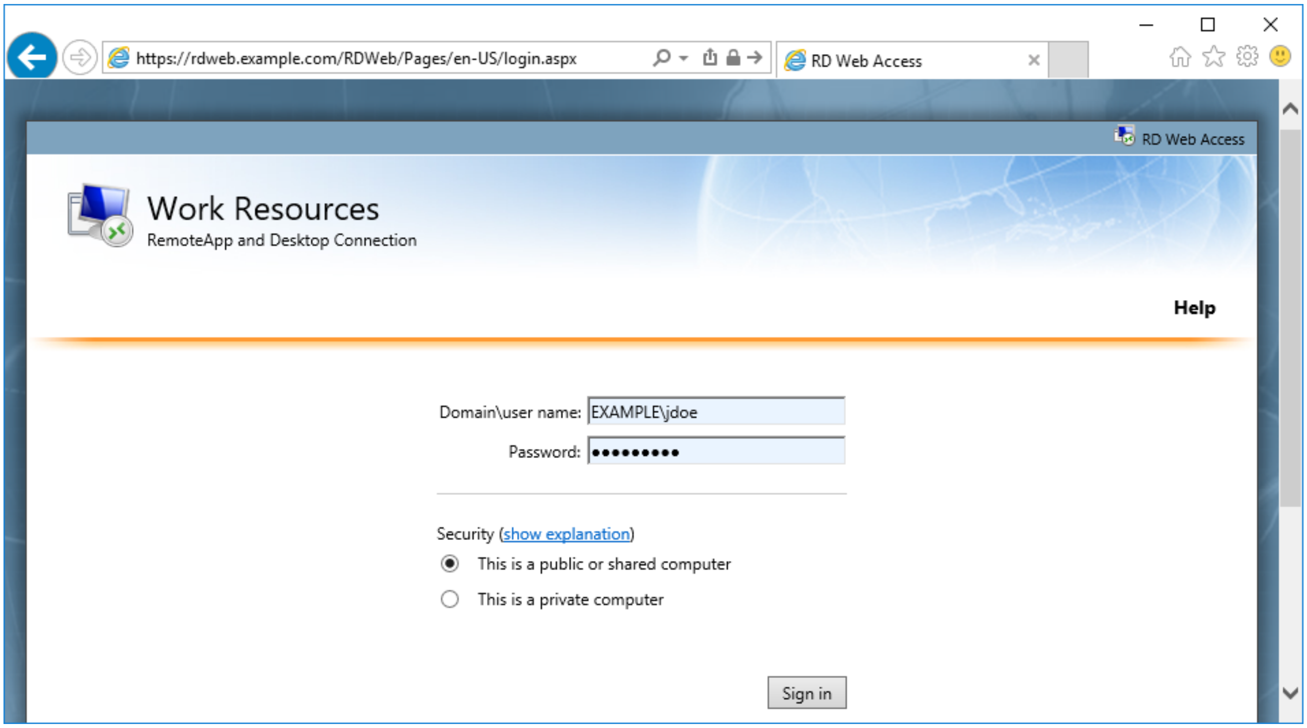
- Microsoft Windows 7 or higher
- IE8 or higher

Users running Windows with a non-IE browser can launch RDP files using the built-in Remote Desktop Client (supporting RDP 7.0 or higher). Users running OS X can launch RDP files using the Microsoft Remote Desktop Client for Mac.

RD Web Access Usage

When a user navigates to your RD Web Access end-point in their browser they are presented with the standard RD Web Access login page. After successfully logging in with their username and password, they are brought to the LoginTC login page which presents options for the second-factor LoginTC authentication. The user is then brought to the RD Web Access page after successfully authenticating with LoginTC.

The RD Web Access initial login page where the user enters their username and password is unmodified.



https://rdweb.example.com/RDWeb/Pages/en-US/login.aspx

RD Web Access

Work Resources

RemoteApp and Desktop Connection

Domain\user name: EXAMPLE\jdoe

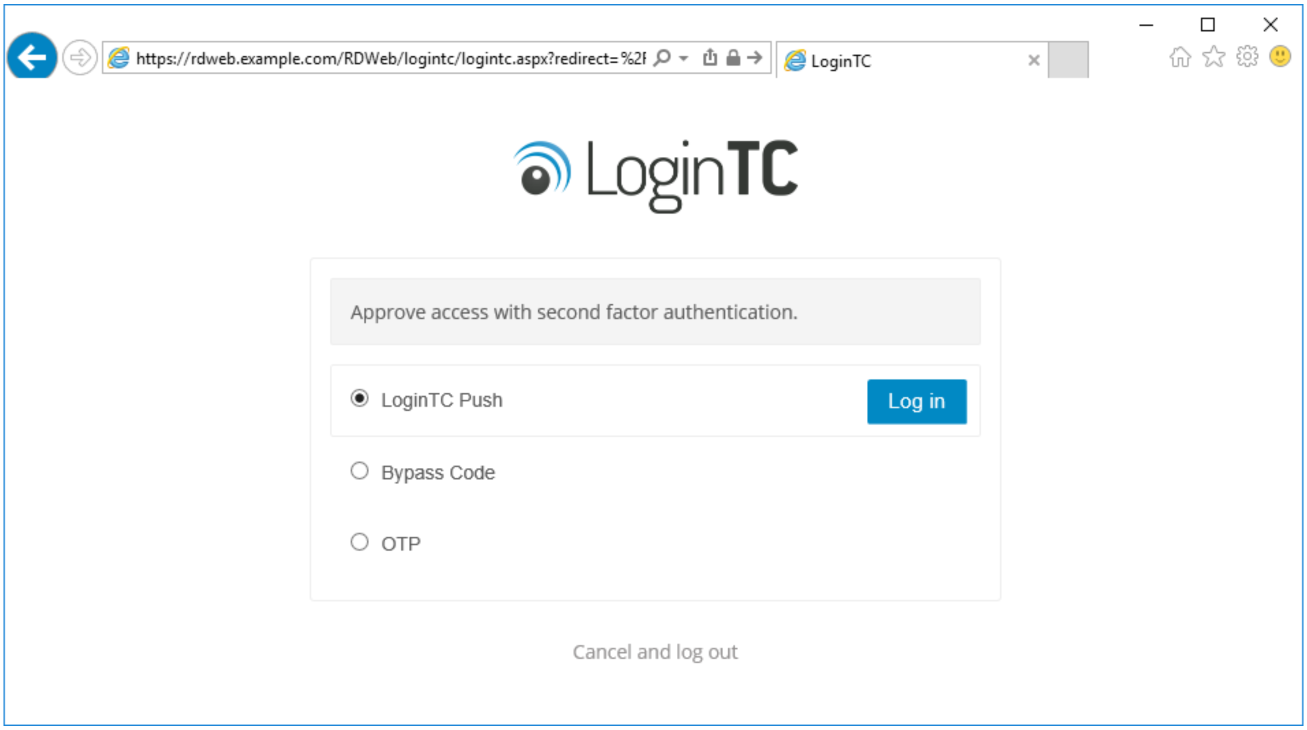
Password: •••••••••

Security (show explanation)

● This is a public or shared computer

○ This is a private computer

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://rdweb.example.com/RDWeb/logintc/logintc.aspx?redirect=%2f

LoginTC

Approve access with second factor authentication.

● LoginTC Push

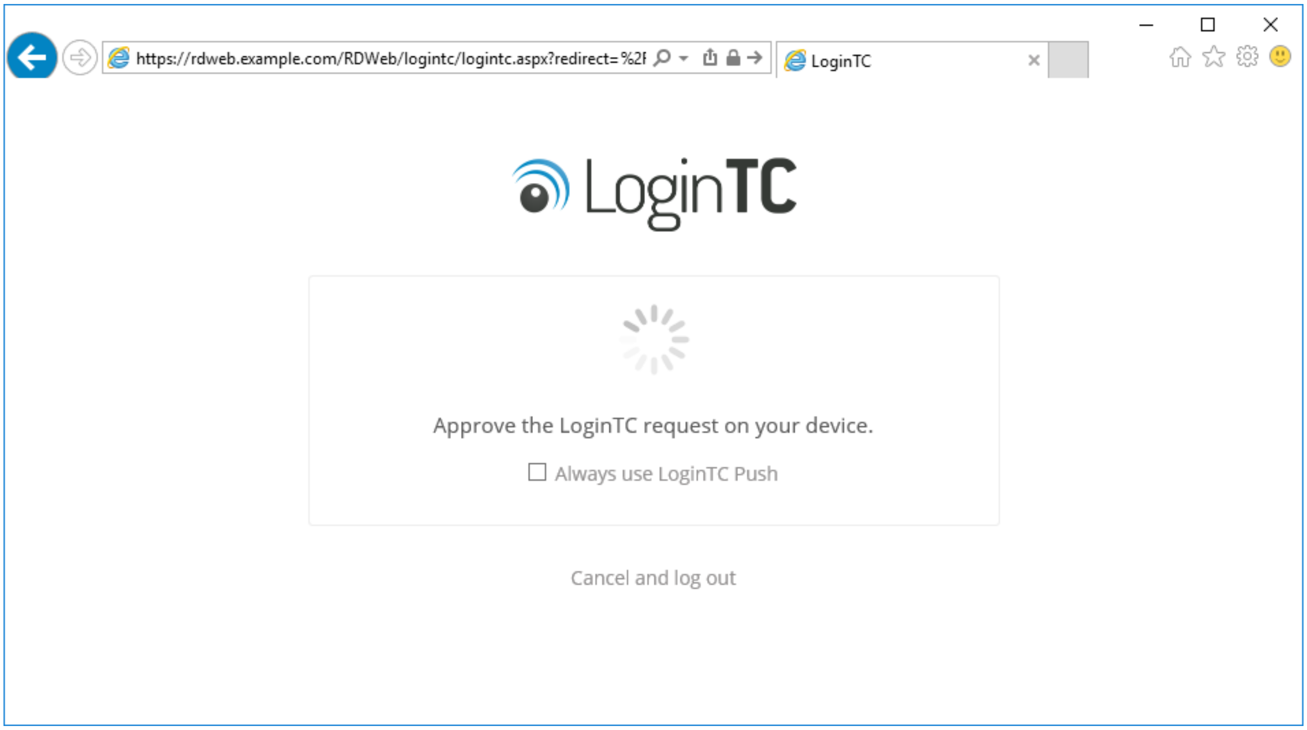
Log in

○ Bypass Code

○ OTP

Cancel and log out

If the user selects LoginTC push, they are informed to approve the LoginTC requst on their device. The user is also presented with an option to remeber 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://rdweb.example.com/RDWeb/logintc/logintc.aspx?redirect=%2f

LoginTC

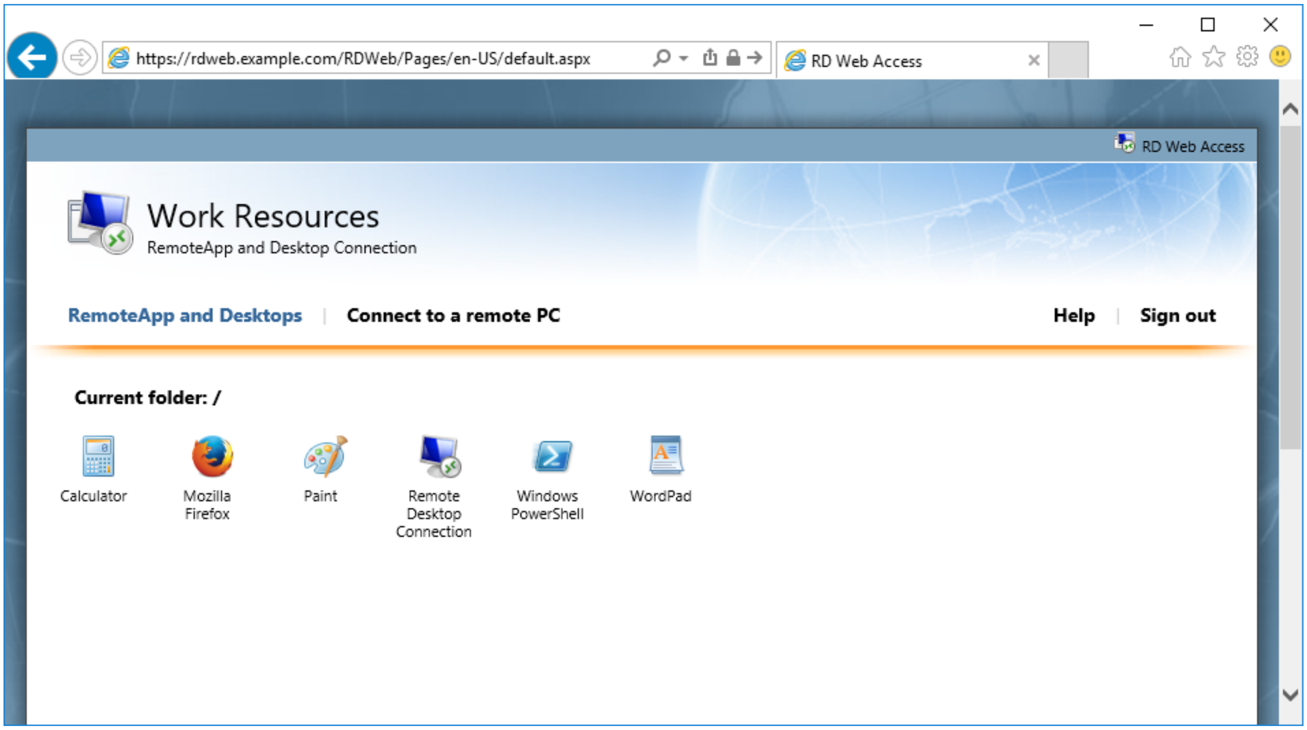
Approve the LoginTC request on your device.

□ Always use LoginTC Push

Cancel and log out

Published Apps Usage

Once logged in, a user launches a published app by clicking on an application icon, which downloads and launches a new dynamically generated RDP file containing an RDG SSO access token. This access token, which is only valid for 60 seconds, is sent to the RD Gateway running the LoginTC RD Gateway SSO Connector to authenticate with the gateway.



RDP File Launching

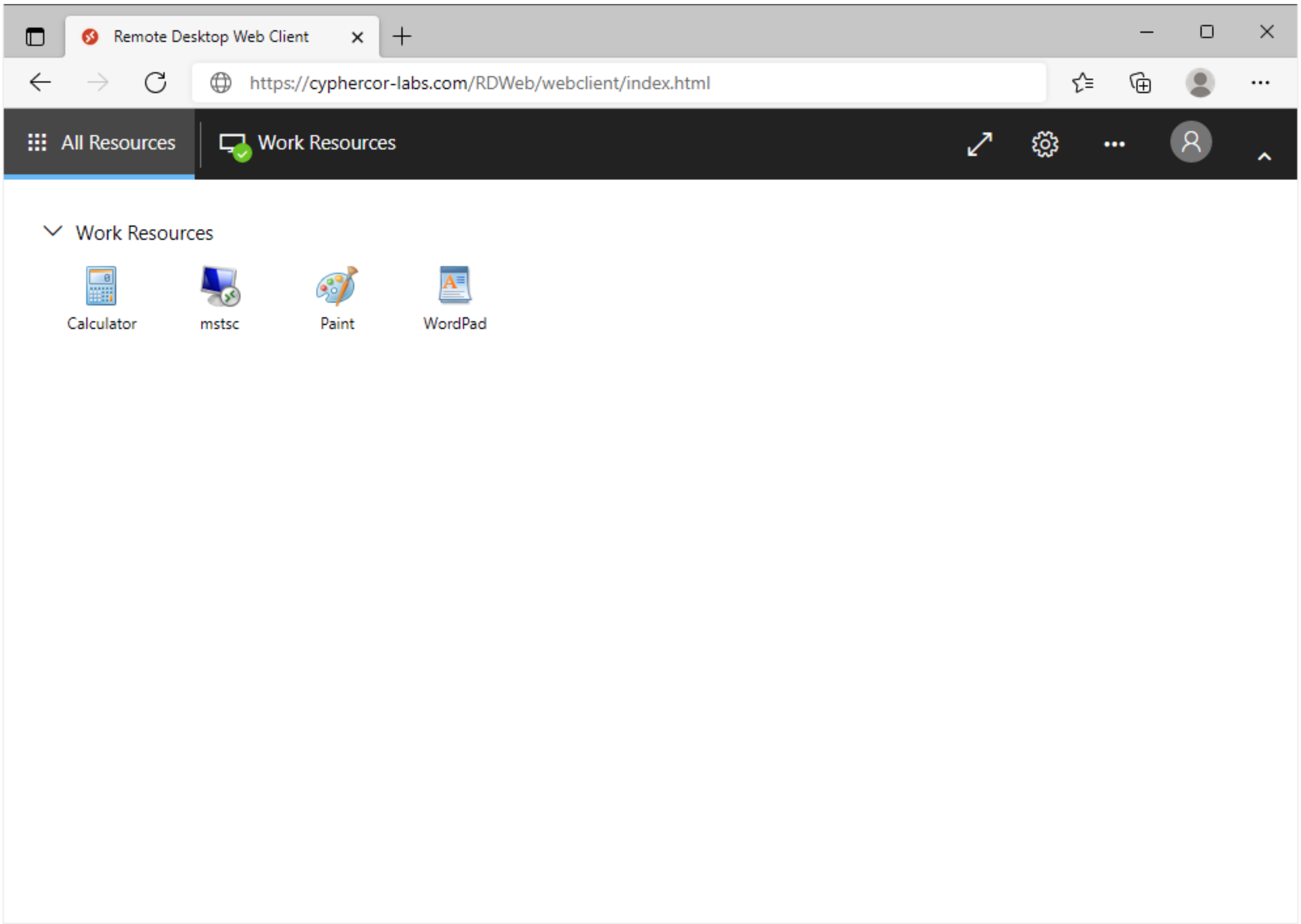
The RDP file is automatically launched when running Internet Explorer on Windows. All other browsers and operating systems download the RDP file, requiring the user to manually launch the RDP file.

Password Prompt

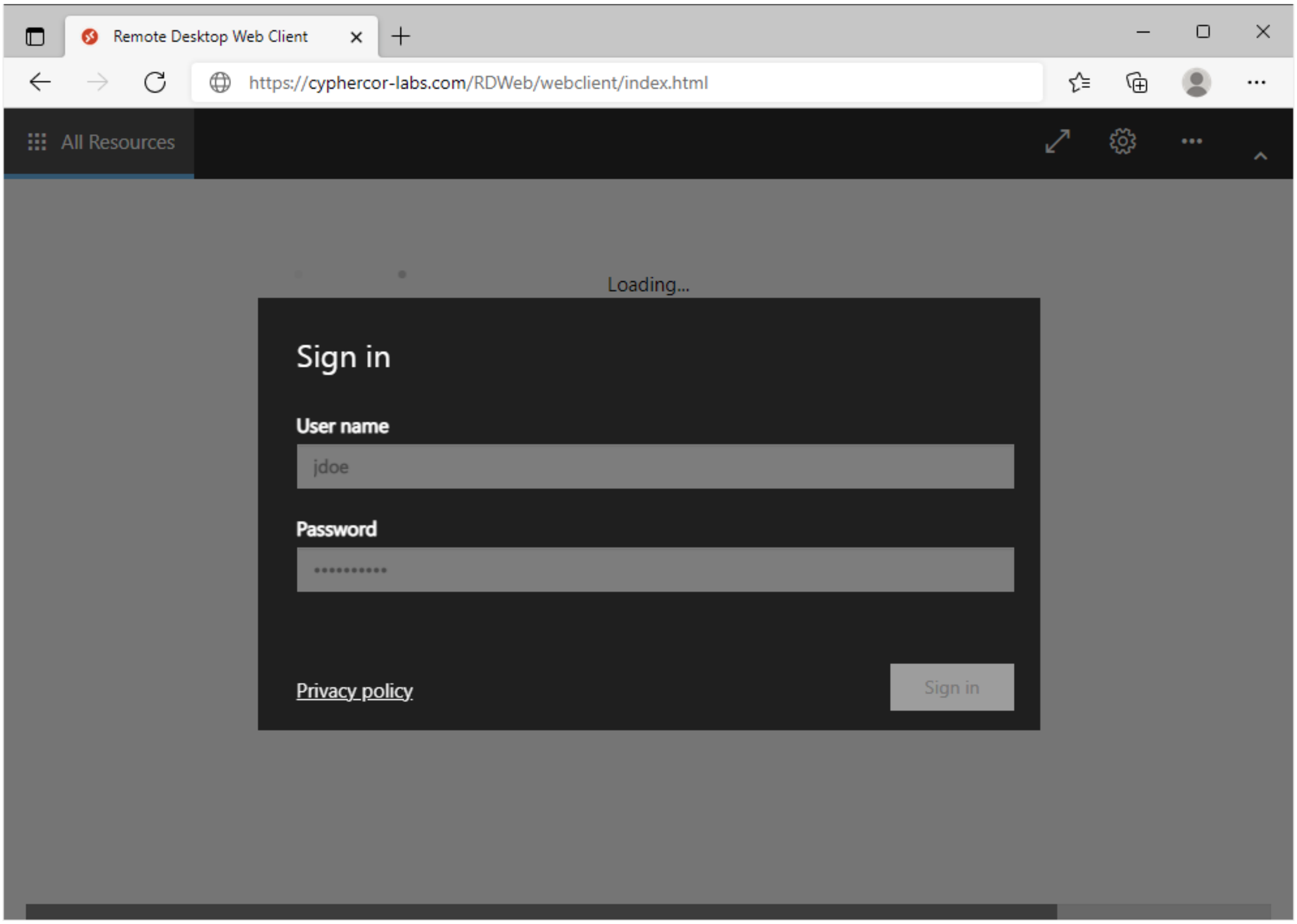
The RD Gateway SSO access token authenticates the user only to the RD Gateway. The user may still be prompted for their Windows credentials to authenticate with the RD session host if they are not using Windows, or this is their first time connecting, or the user's computer is not part of the RD session host domain, or the RD session host does not allow remote SSO credential passing. See Enable RDC Client Single Sign-On for Remote Desktop Services.

HTML5 Web Client Usage

After entering their username and password, the user is sent a LoginTC push request. After approving the request, the user is shown their available applications.


Remote Desktop Web Client
https://cyphercor-labs.com/RDWeb/webclient/index.html
All Resources
Work Resources
Work Resources
Calculator
mstsc
Paint
WordPad

The user can then click on an application to launch it.


Remote Desktop Web Client
https://cyphercor-labs.com/RDWeb/webclient/index.html
All Resources
Loading...

Sign in

User name

jdoe

Password

••••••••••

RD Gateway Considerations

The HTML5 Web Client does not support the LoginTC RD Gateway SSO Connector. To prevent single-factor authentication access directly to the RD Gateway, we recommend limiting RD Gateway access to the internal host running the RD HTML5 Web Client or installing the LoginTC Windows Logon & RDP Connector on the RD Session Host(s).

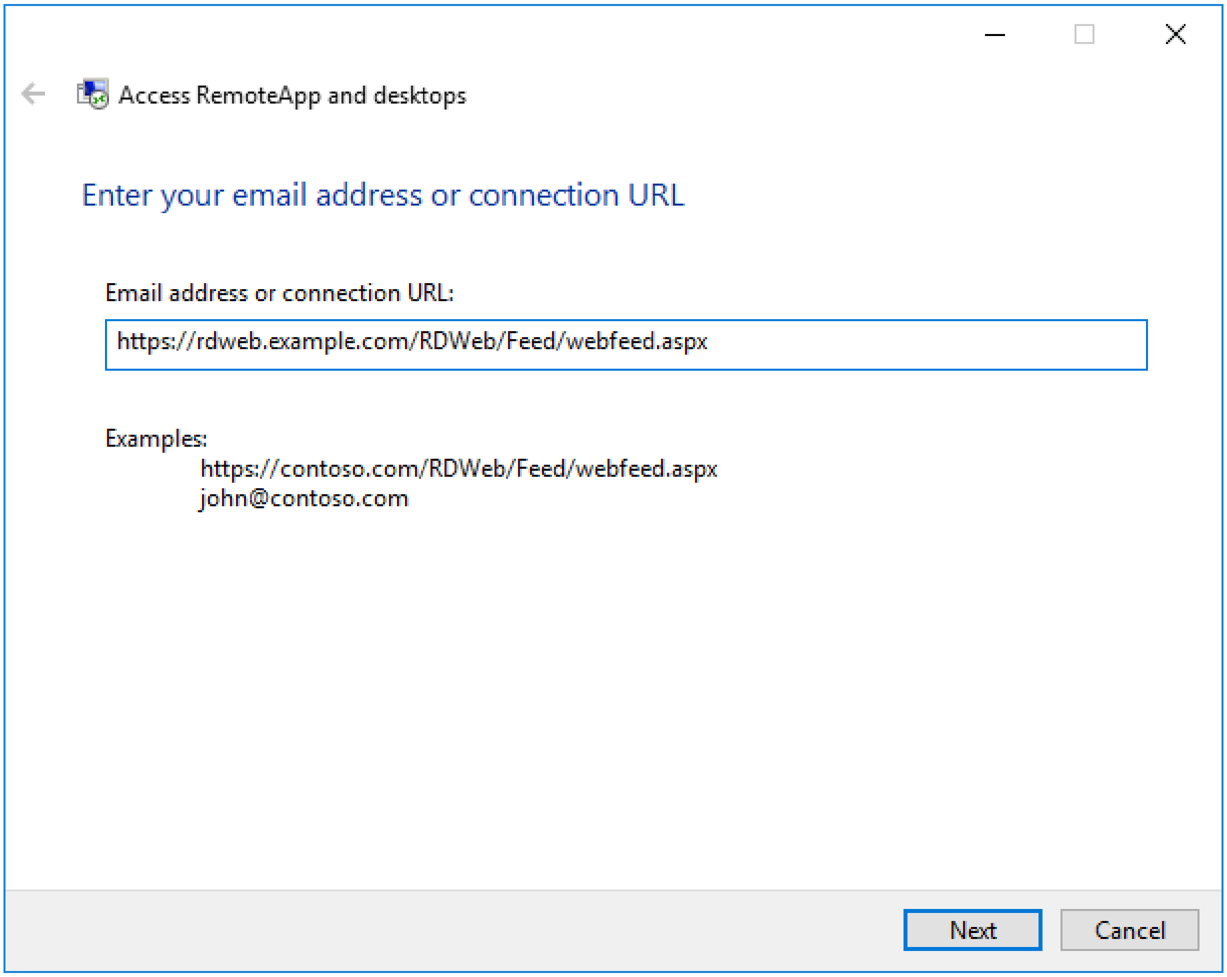
RemoteApp Usage

The RD RemoteApp web feed allows the user to see a list of the RemoteApp published apps available to them, directly from the Start menu. This is a convenient way for users to launch their remote applications.

The LoginTC RD Web Access Connector protects the Remote Desktop RemoteApp web feed login with an additional LoginTC two-factor challenge. Under normal conditions, a user only authenticates with the RemoteApp web feed once.

RemoteApp user flow:

1. The user begins by adding a RemoteApp connections, like normal.

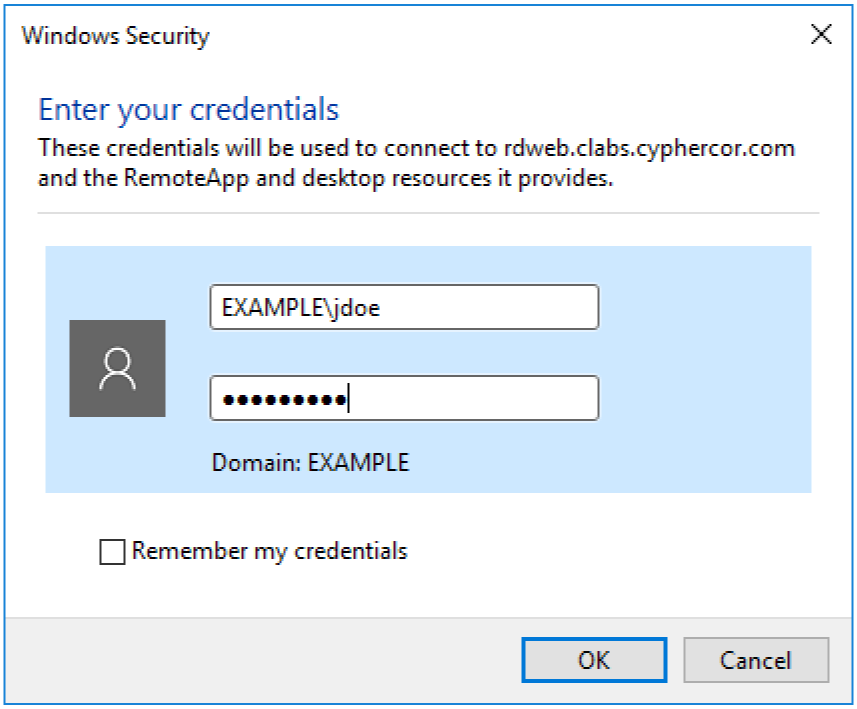


Enter your email address or connection URL

Email address or connection URL: https://rdweb.example.com/RDWeb/Feed/webfeed.aspx

Examples:
https://contoso.com/RDWeb/Feed/webfeed.aspx
john@contoso.com

2. The user then enters their username and password, like normal.



Enter your credentials

These credentials will be used to connect to rdweb.clabs.cyphercor.com and the RemoteApp and desktop resources it provides.

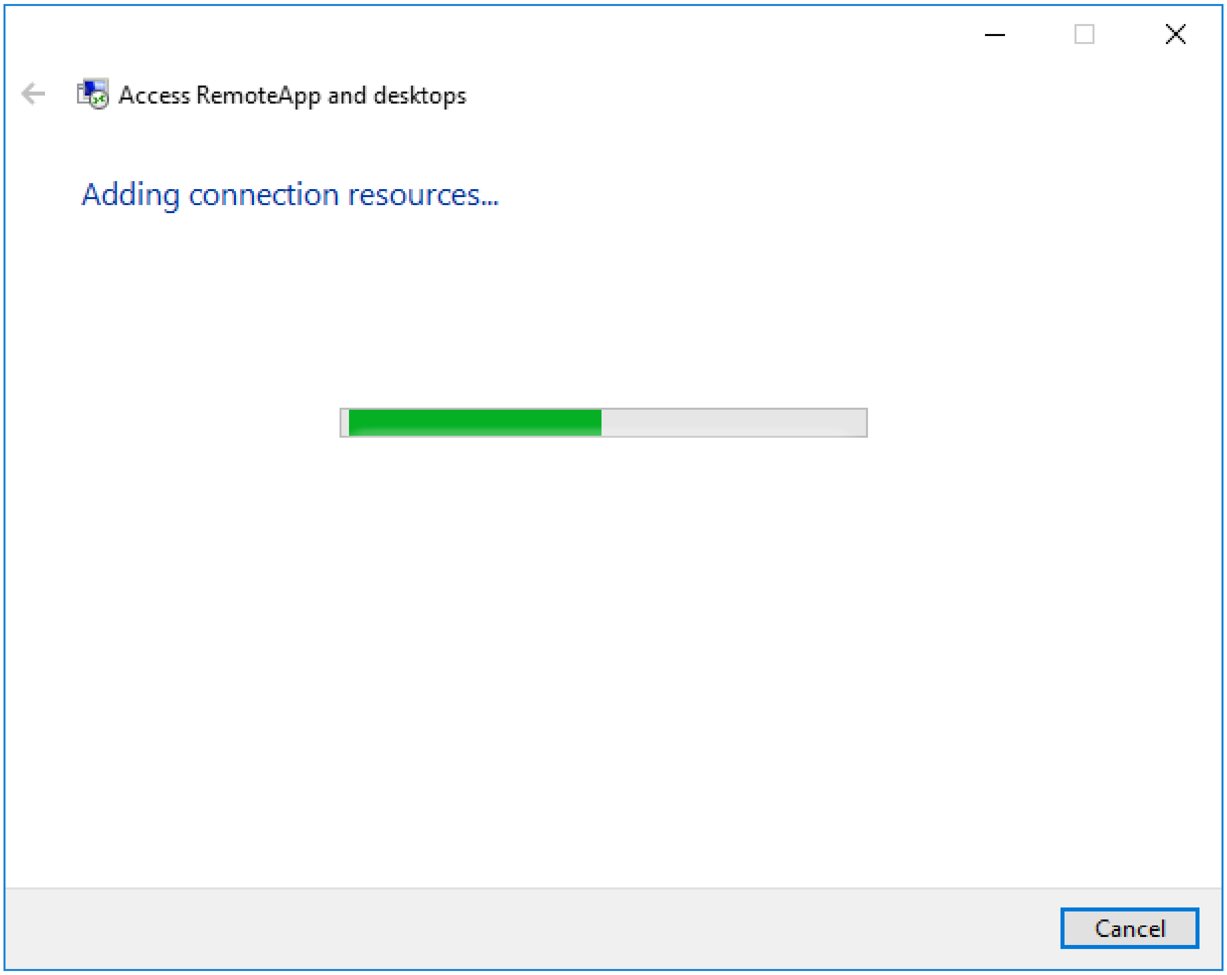
EXAMPLE\jdoe

●●●●●●●●●●

Domain: EXAMPLE

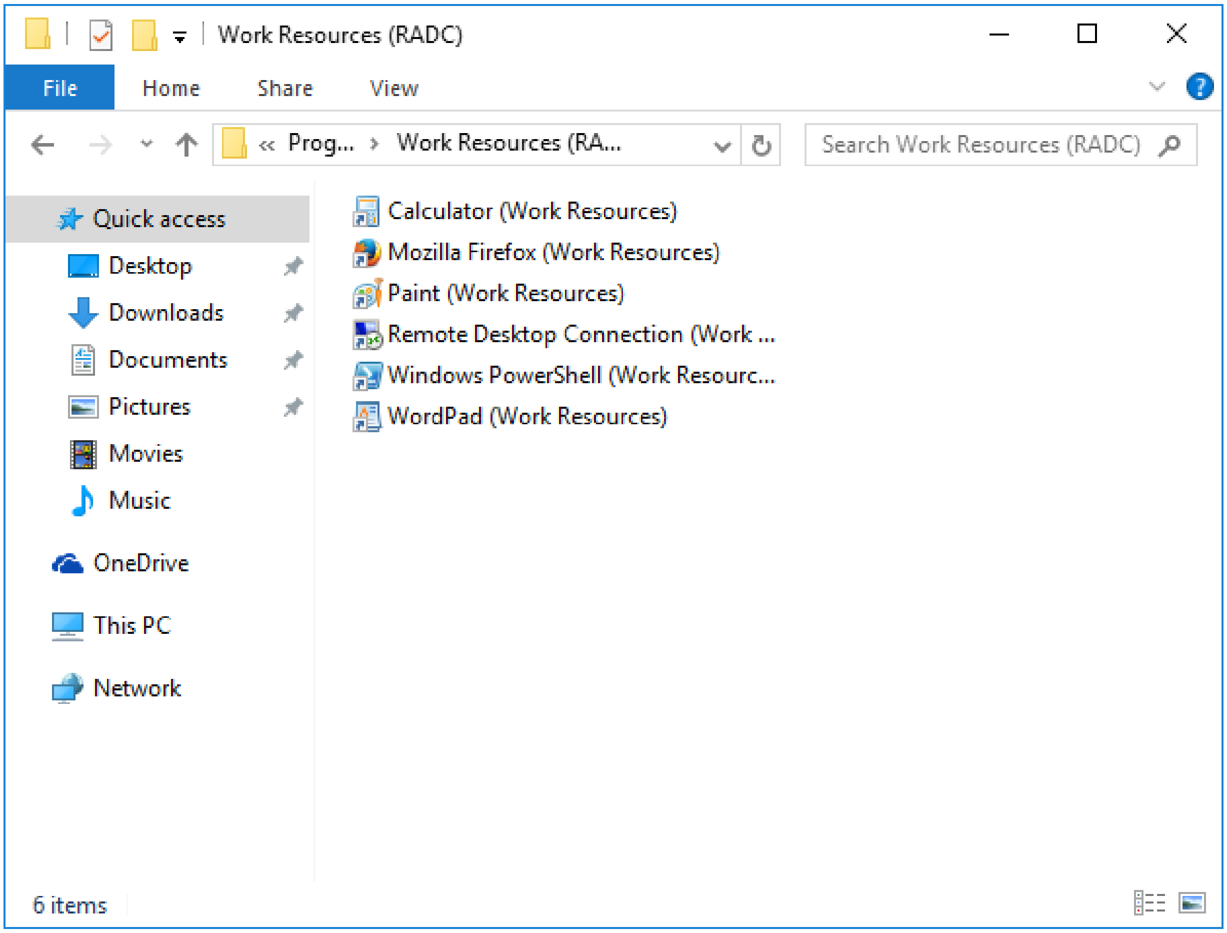
□ Remember my credentials

3. The user is presented with a loading spinner while a LoginTC push notification is sent to their device. The user has 60 seconds to approve the request.



Adding connection resources...

4. The user is presented with a list of their RemoteApp published apps (which can also be found in the Start menu). Starting a remote app will challenge the user for their Windows credentials and perform authentication with both the RD Gateway and the session host unless the user already has a connection established with the RD session host, in which case, the remote app will open without any additional challenges.

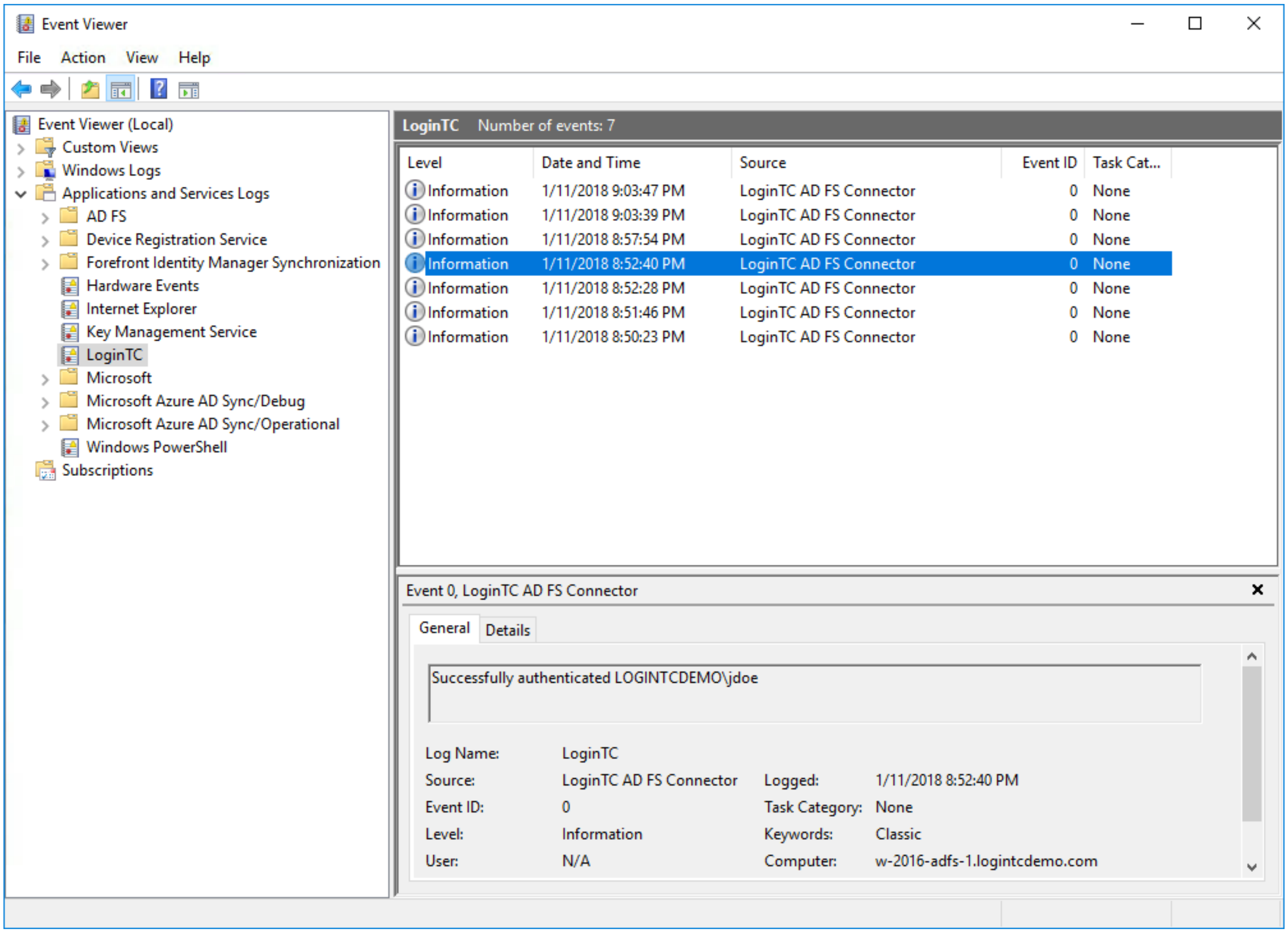

Work Resources (RADC)
File
Home
Share
View
« Prog... › Work Resources (RA...
Search Work Resources (RADC)
Quick access
Desktop
Downloads
Documents
Pictures
Movies
Music
OneDrive
This PC
Network
Calculator (Work Resources)
Mozilla Firefox (Work Resources)
Paint (Work Resources)
Remote Desktop Connection (Work ...
Windows PowerShell (Work Resourc...
WordPad (Work Resources)
6 items

Using RemoteApp and RDG SSO

If you installed the LoginTC RD Web Access Connector with the RDG SSO option then your deployment will require a secondary RD Gateway to support RD RemoteApp. This secondary RD Gateway must not use the LoginTC RD Gateway SSO Connector and must be set as the RD Gateway server in your Remote Desktop deployment configuration. We recommend that you configure this secondary RD Gateway to use the LoginTC RADIUS Connector for authentication so that it’s also protected with two-factor authentication.

Logging

The LoginTC RD Web Access Connector logs events to the Microsoft Event Viewer under **Applications and Service Logs** → **LoginTC**. LoginTC RD Web Access Connector event logs are helpful in debugging issues.



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

Passthrough

Passthrough allows you to specify which set of users should be challenged with LoginTC second-factor authentication, and which ones will not. This is often useful when testing and when rollying out a deployment to minimize the impact on others. The passthrough settings are configured on the host running the LoginTC RD Web Access role.

Static User List

Setting a static user list tells the LoginTC RD Web Access Connector which users must be challenged for LoginTC second-factor authentication. All other users will be passed through without requiring a second-factor authentication.

Instructions to set a static list of users to be challenged:

1. Navigate to `C:\Program Files\Cyphercor\LoginTC RD Web Access Connector` on the host running the RD Web Access role.
2. Create a new file `users.txt` in Notepad.
3. Populate the file with a list of users, one line at a time, in the following format: `DOMAIN\username`
4. Save the file.
5. Your change will be picked up by the connector within 60 seconds.

If the `users.txt` file does not exist then all users will be challenged with LoginTC second-factor authentication.

Group List

Setting a group list tells the LoginTC RD Web Access Connector which AD security group members must be challenged for LoginTC second-factor authentication. All other users not belonging to any of the listed AD security groups will be passed through without requiring a second-factor authentication.

Instructions to set a list of AD security groups to be challenged:

1. Navigate to `C:\Program Files\Cyphercor\LoginTC RD Web Access Connector` on the host running the RD Web Access role.
2. Create a new file `groups.txt` in Notepad.
3. Populate the file with a list of AD security groups, one line at a time.
4. Save the file.
5. Your change will be picked up by the connector within 60 seconds.

If the `groups.txt` file does not exist then all users will be challenged with LoginTC second-factor authentication (unless a static user list file exists).

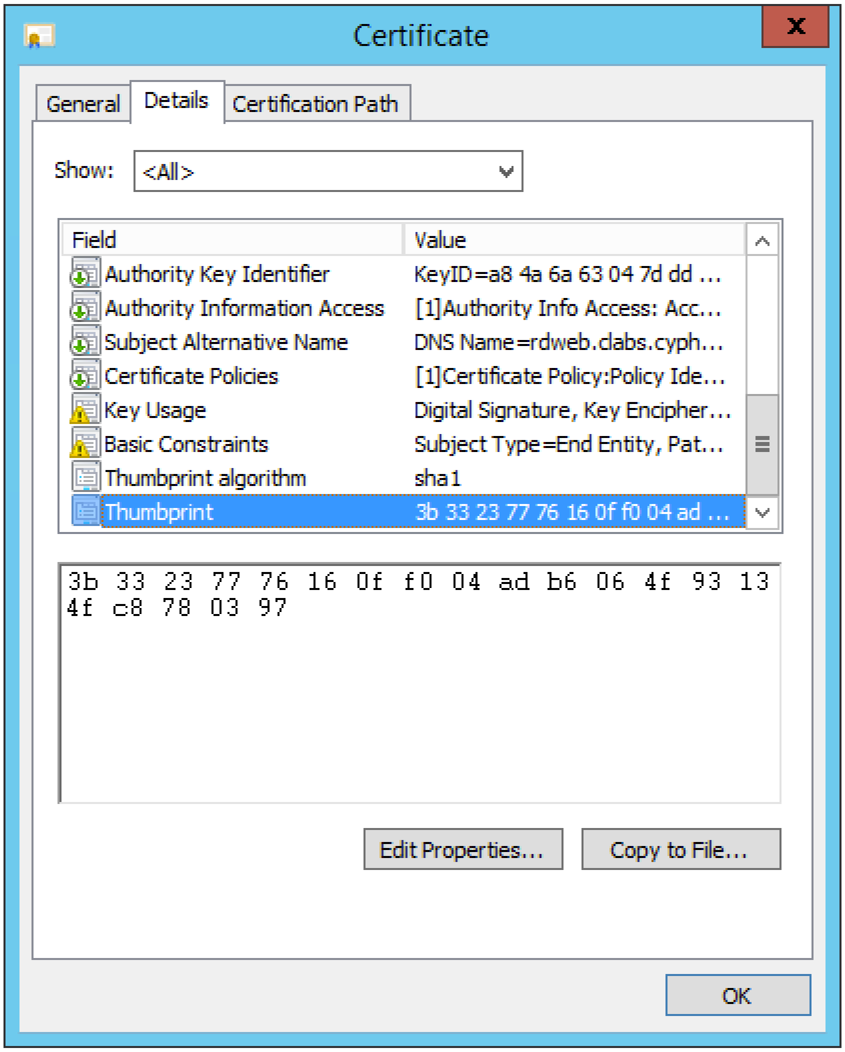
Appendix A: RDP Cert

The LoginTC RD Web Access Connector signs RDP files using your RD Web Access HTTP domain certificate. In order for the signing to work, you must provide the certificate thumbprint during the LoginTC RD Web Access Connector installation, and also grant read access to the IIS process for the certificate.

Follow these instructions to get your certificate thumbprint:

1. Run **certlm.msc** (Manage Computer Certificates) on the host running the RD Web Access role.
2. Find your RD Web Access domain certificate (usually under Personal → Certificates).
3. Double click on the certificate.
4. Press the **Details** tab.

5. Scroll to the bottom of the details and copy the **Thumbprint** value.



Show: <All>

Field	Value
Authority Key Identifier	KeyID=a8 4a 6a 63 04 7d dd …
Authority Information Access	[1]Authority Info Access: Acc…
Subject Alternative Name	DNS Name=rdweb.clabs.cyph…
Certificate Policies	[1]Certificate Policy:Policy Ide…
Key Usage	Digital Signature, Key Encipher…
Basic Constraints	Subject Type=End Entity, Pat…
Thumbprint algorithm	sha1
Thumbprint	3b 33 23 77 76 16 0f f0 04 ad …

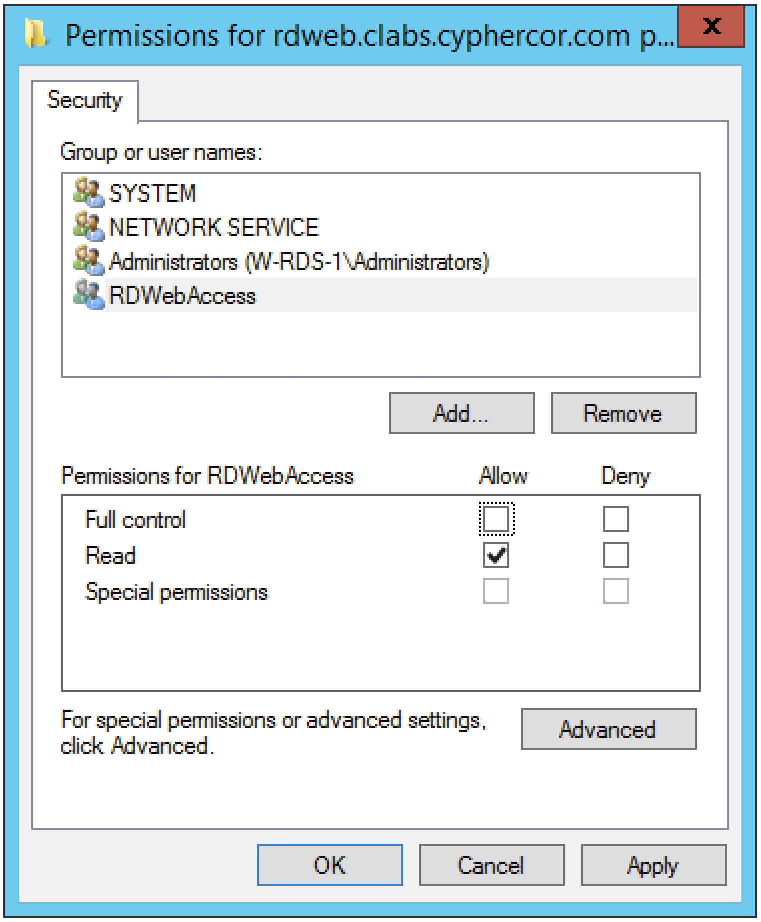
```
3b 33 23 77 76 16 0f f0 04 ad b6 06 4f 93 13
4f c8 78 03 97
```

Appendix B: RDP Cert Permissions

You must grant read access to your RDP signing certificate to the IIS RD Web Access user so the LoginTC RD Web Access module can sign the generated RDP files. To grant permission:

1. Run **certlm.msc** (Manage Computer Certificates) on the host running the RD Web Access role.
2. Find your RD Web Access domain certificate (usually under Personal → Certificates).
3. Right click on your certificate and click on **All Tasks** → **Manage Private Keys…**
4. Press the **Add** button to add a new permission.
5. Press the **Locations…** button and select the local computer.
6. Enter `IIS APPPOOL\RDWebAccess` into the textarea and press **OK**.
7. Uncheck Full control next to Allow since only Read permissions are necessary.

8. Press **Apply**.



Permissions for rdweb.clabs.cyphercor.com p...

Group or user names:

- SYSTEM
- NETWORK SERVICE
- Administrators (W-RDS-1\Administrators)
- RDWebAccess

Permissions for RDWebAccess	Allow	Deny
Full control	☐	☐
Read	☑	☐
Special permissions	☐	☐

For special permissions or advanced settings, click Advanced.

Uninstallation

To uninstall the LoginTC RD Web Access Connector / LoginTC RD Gatway SSO Connector, simply navigate to the **Add or remove programs** in the Windows **Control Panel**, find LoginTC RD Web Access Connector / LoginTC RD Gatway SSO Connector in the list and follow the prompts.

Troubleshooting

Email Support

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