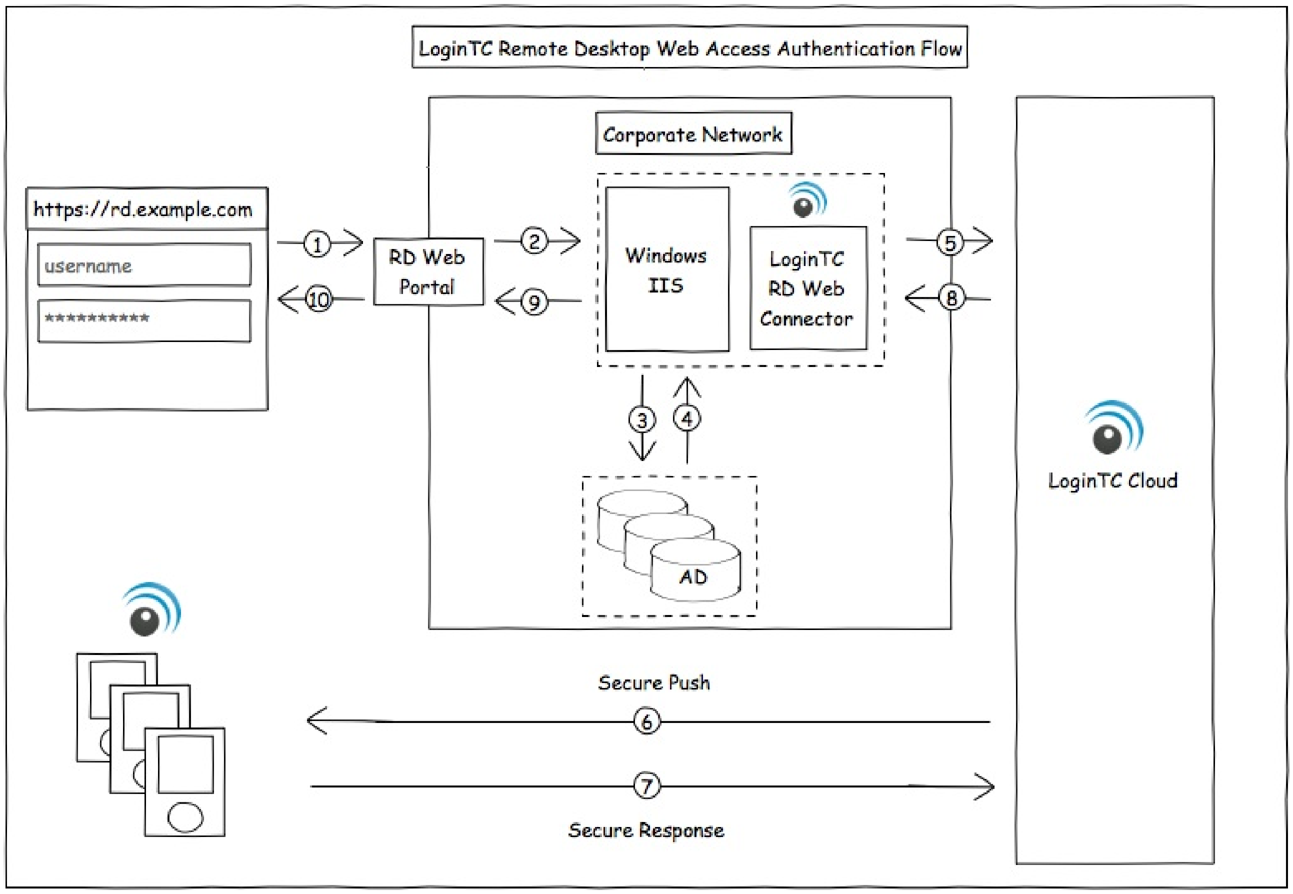
Two factor authentication for Microsoft Remote Desktop Web Access

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

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.



Architecture and Authentication Flow

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.

Prerequisites

Before proceeding, please ensure you have the following:

- LoginTC Admin account
- Microsoft Windows Server 2012 R2 or Windows Server 2016
- 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

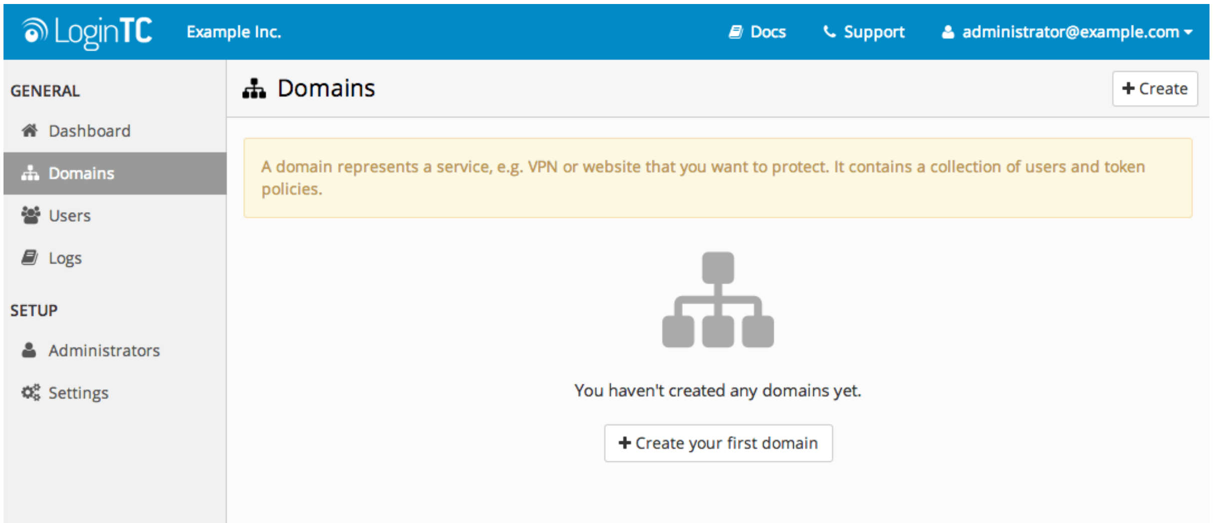
It is strongly recommended that you have a working and tested Remote Desktop Web Access deployment prior to adding LoginTC authentication.

LoginTC Domain Creation

Create a LoginTC domain in LoginTC Admin. The domain represents a service (e.g. your corporate Remote Desktop Web Access) 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.

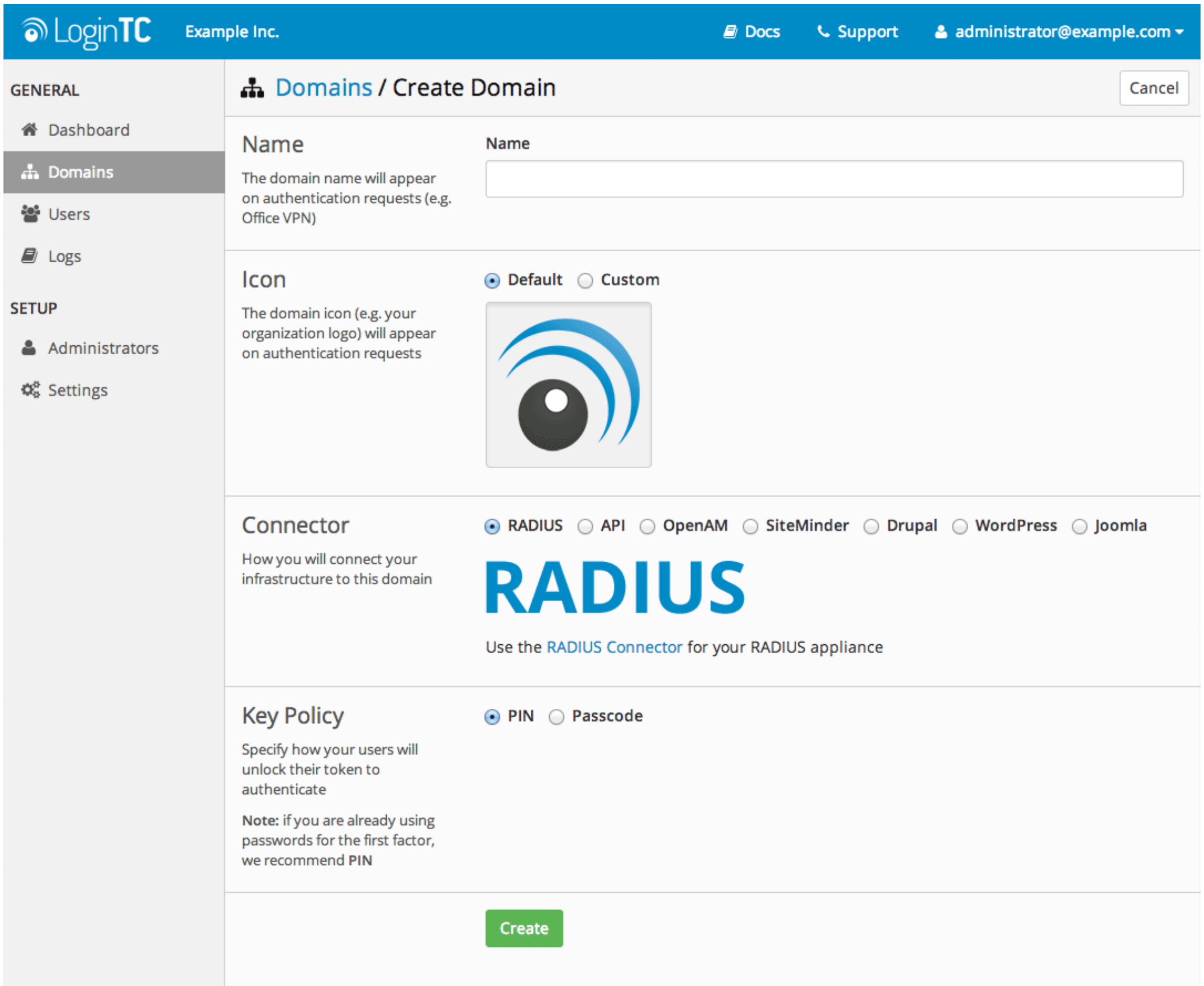
1. Log in to LoginTC Admin
2. Click **Domains**:
3. Click **Create Domain**:



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 domain information:



Domains / Create Domain

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

Connector

How you will connect your infrastructure to this domain

● RADIUS ○ API ○ OpenAM ○ SiteMinder ○ Drupal ○ WordPress ○ Joomla

Use the RADIUS Connector for your RADIUS appliance

Key Policy

Specify how your users will unlock their token to authenticate

Note: if you are already using passwords for the first factor, we recommend **PIN**

● PIN ○ Passcode

Select the **API** option in the Connector section

Installation (RD Web Access)

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

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:

Direct RD Gateway Access

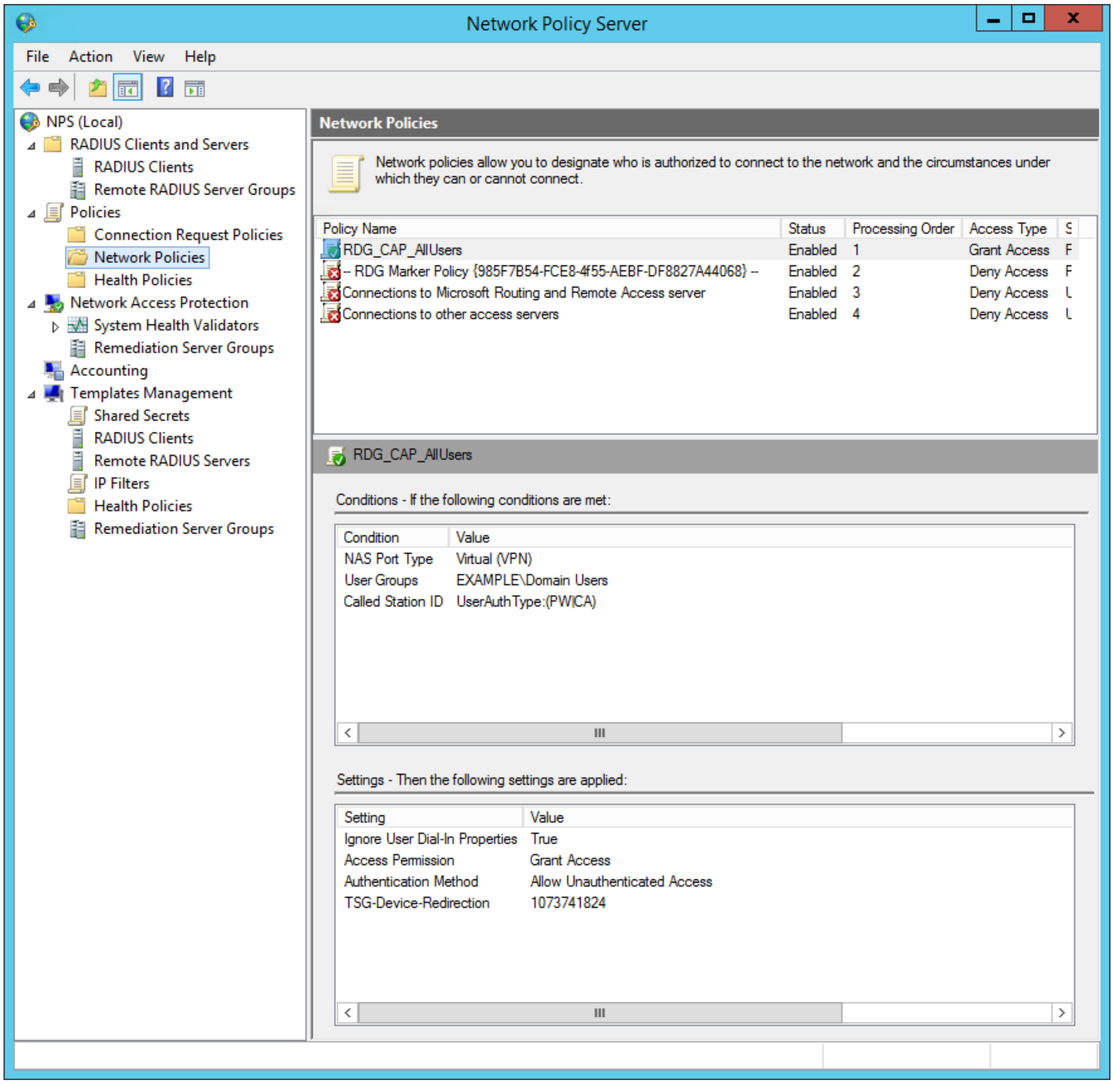
This RD Gateway will only work with RD Gateway SSO access tokens generated by the LoginTC RD Web Access Connector. If you would like your users to still correct directly to the gateway (instead of going through RD Web Access) then you will need a secondary RD Gateway host.

Configuration

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	L
Connections to other access servers	Enabled	4	Deny Access	L

RDG_CAP_AllUsers

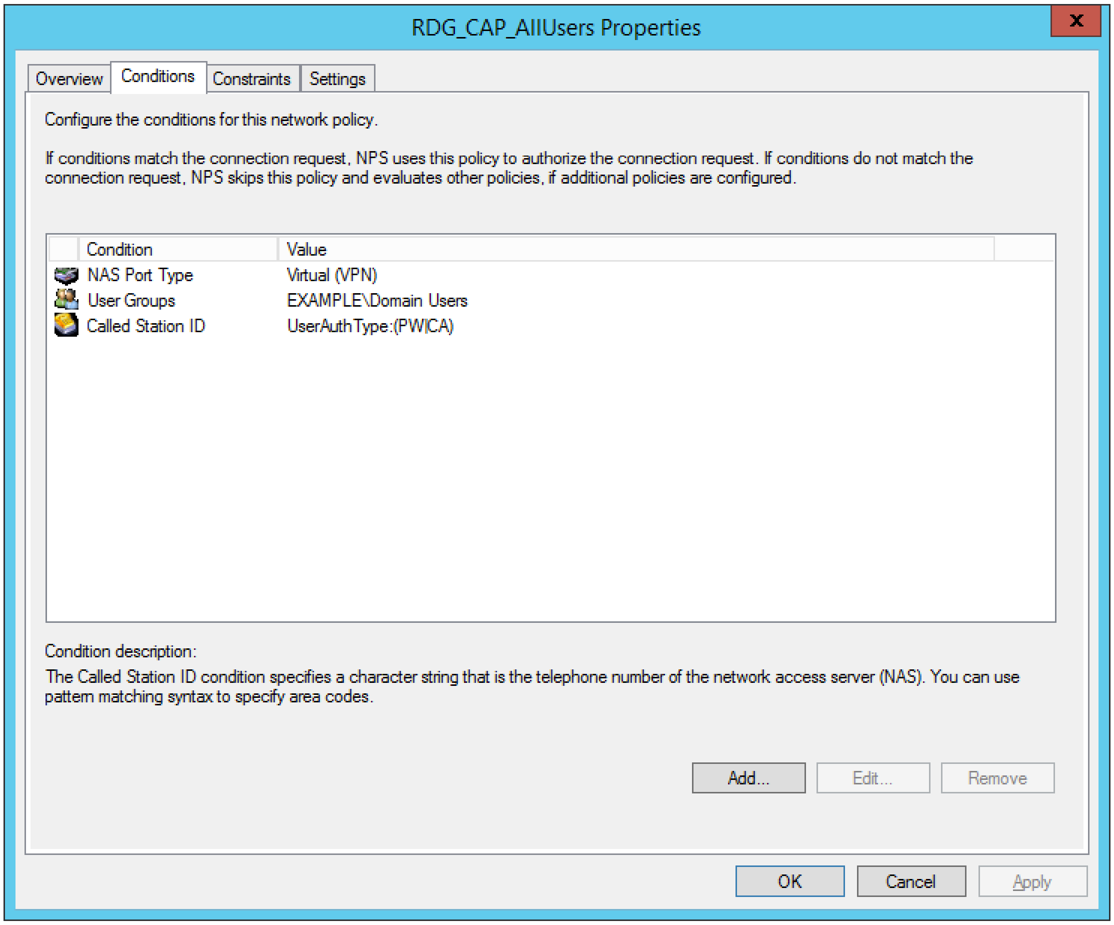
Conditions - If the following conditions are met:

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:

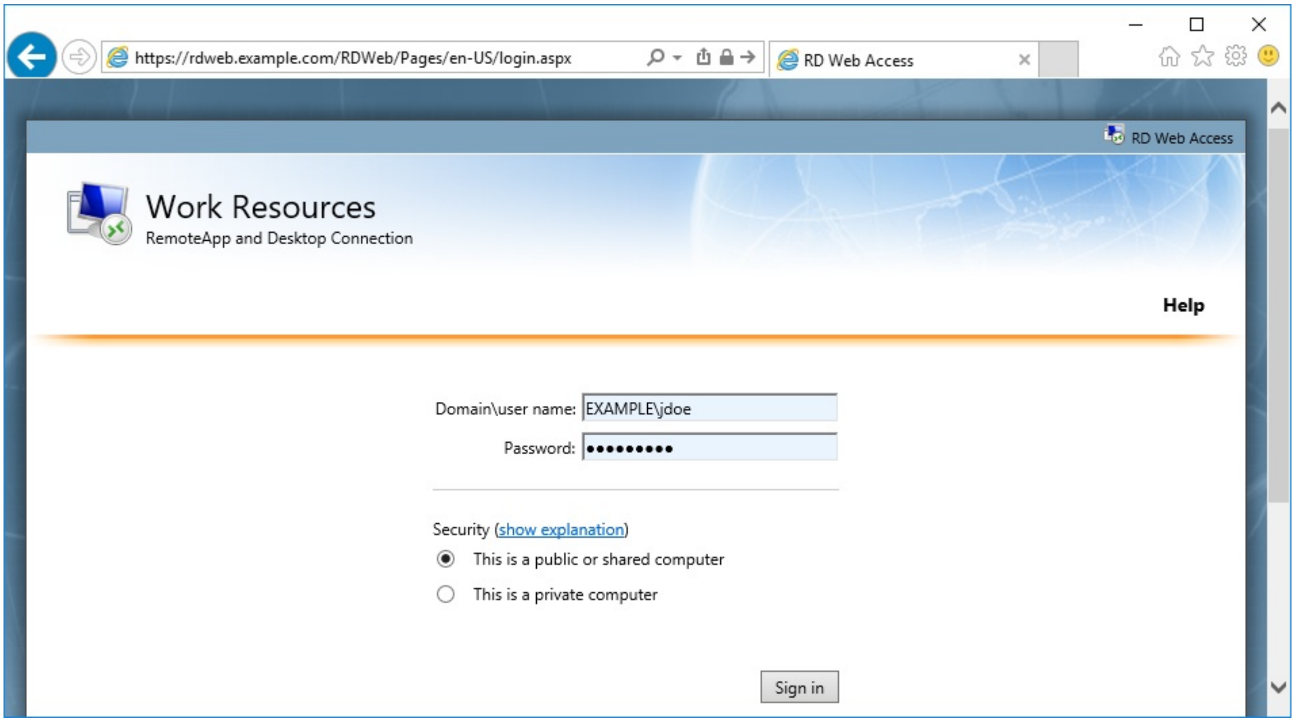
- Microsoft Windows 7 or higher
- IE8 or higher

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

Work Resources

RemoteApp and Desktop Connection

Domain\user name: EXAMPLE\jdoe

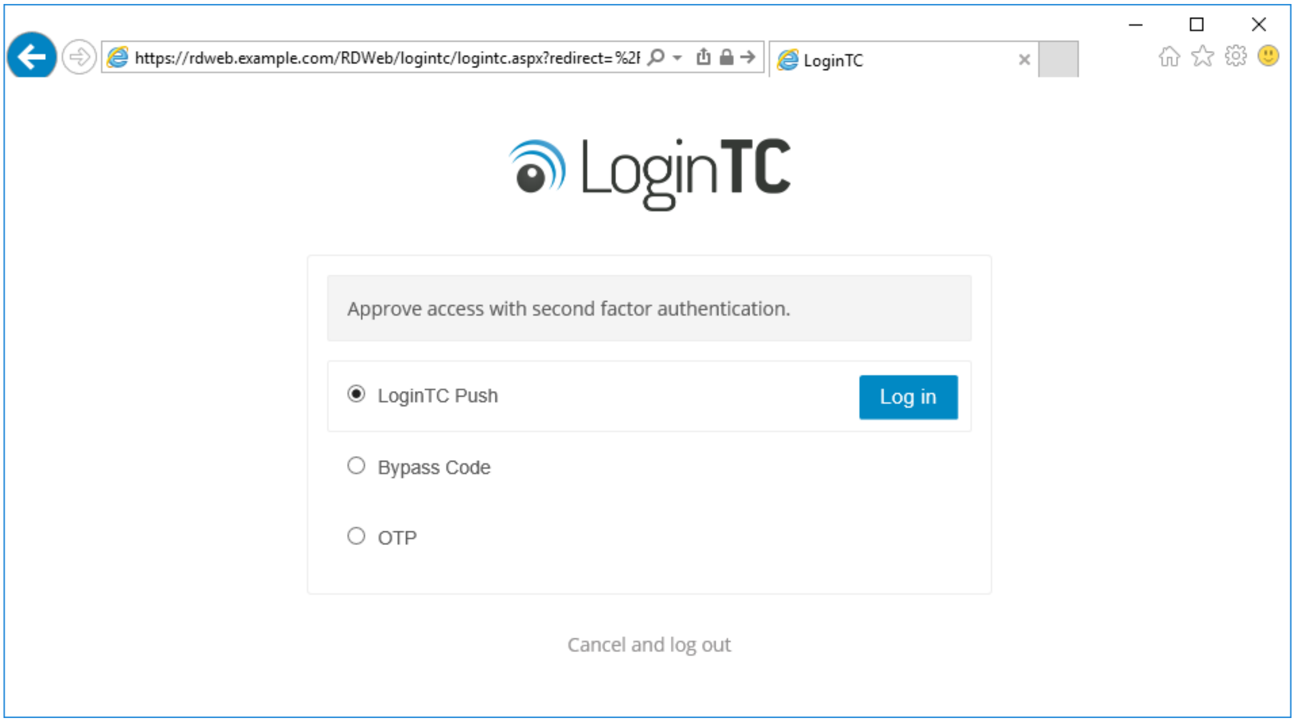
Password: ••••••••••

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

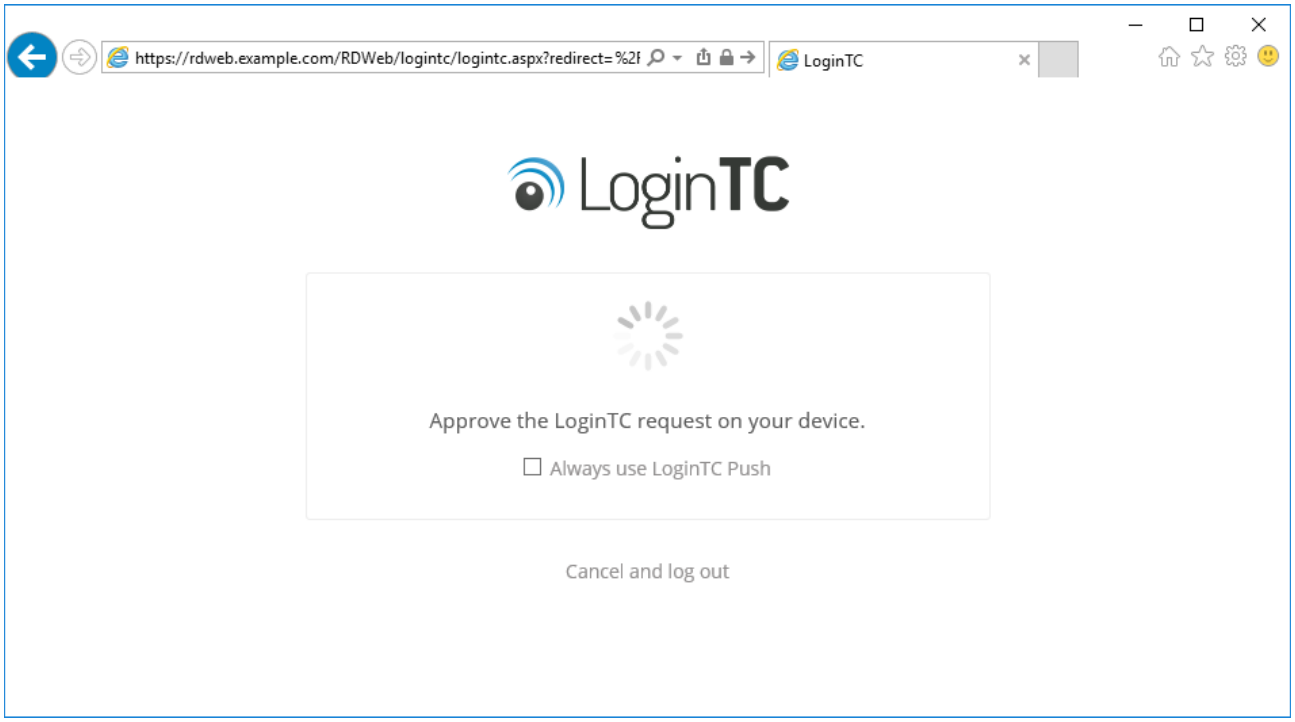
Approve access with second factor authentication.

● LoginTC Push

○ Bypass Code

○ OTP

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
LoginTC

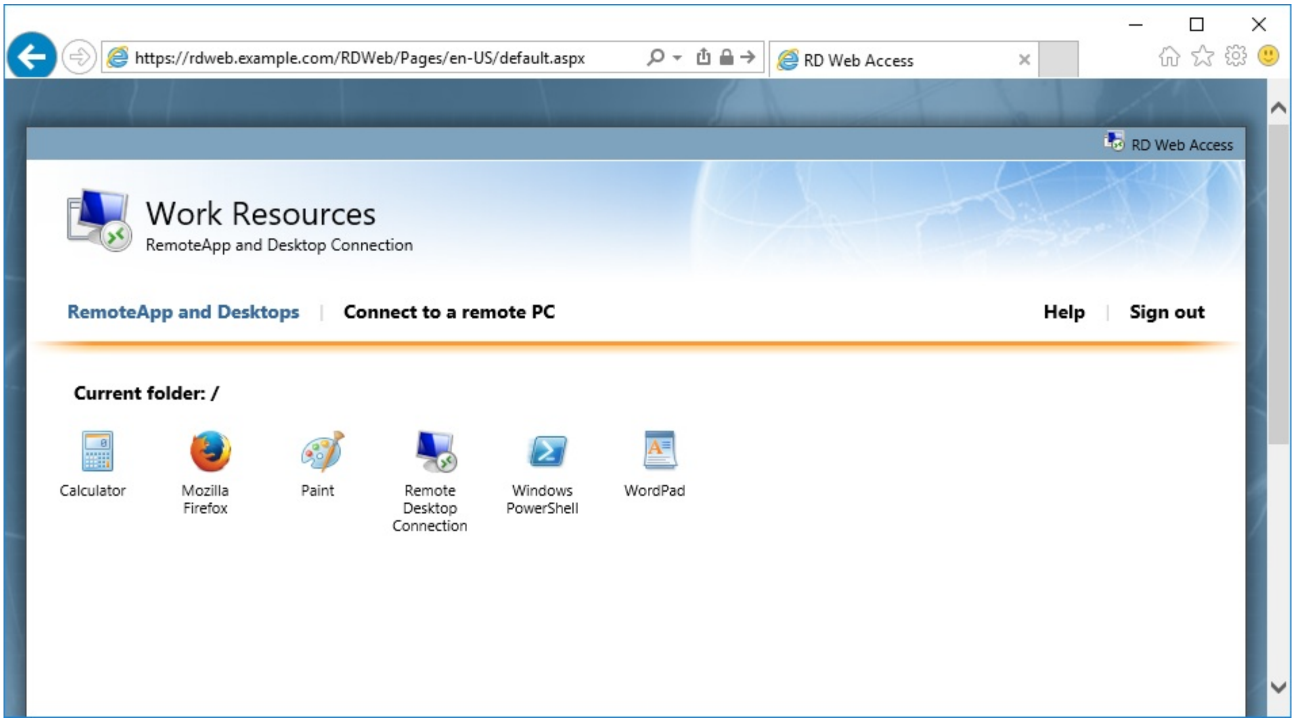
Approve the LoginTC request on your device.

☐ 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.

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.

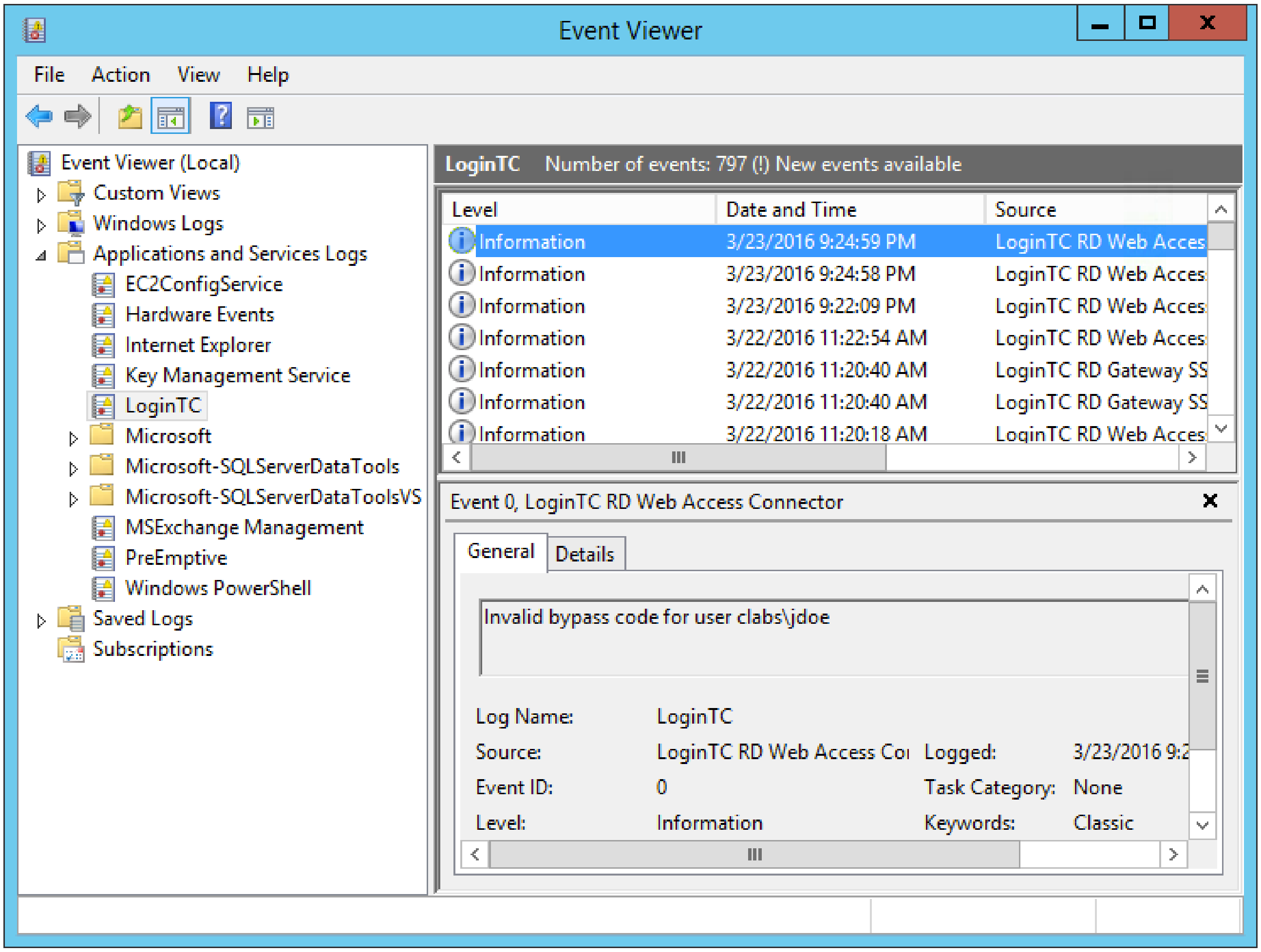
RemoteApp user flow:

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: 797 (!) New events available

Level	Date and Time	Source
Information	3/23/2016 9:24:59 PM	LoginTC RD Web Acces
Information	3/23/2016 9:24:58 PM	LoginTC RD Web Acces
Information	3/23/2016 9:22:09 PM	LoginTC RD Web Acces
Information	3/22/2016 11:22:54 AM	LoginTC RD Web Acces
Information	3/22/2016 11:20:40 AM	LoginTC RD Gateway SS
Information	3/22/2016 11:20:40 AM	LoginTC RD Gateway SS
Information	3/22/2016 11:20:18 AM	LoginTC RD Web Acces

Event 0, LoginTC RD Web Access Connector

Invalid bypass code for user clabs\jdoe

Log Name:	LoginTC		
Source:	LoginTC RD Web Access Coı	Logged:	3/23/2016 9:2
Event ID:	0	Task Category:	None
Level:	Information	Keywords:	Classic

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.

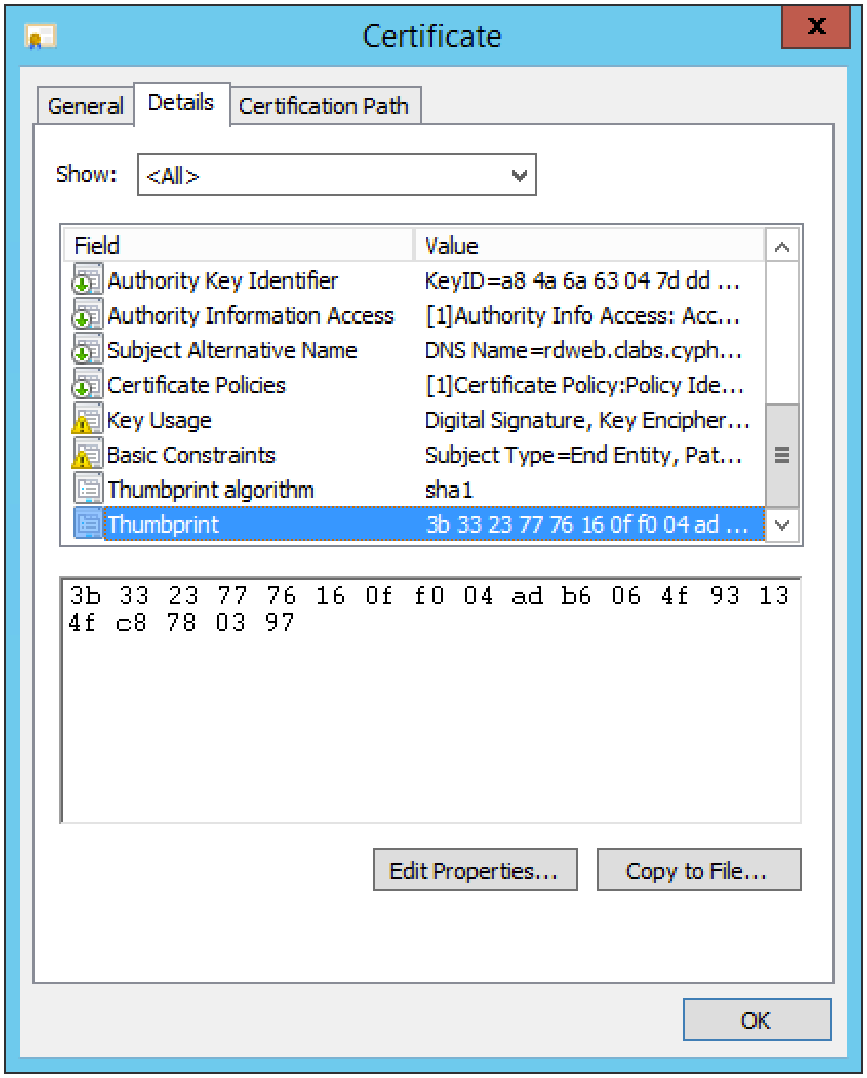
If the `groups.txt` file does not exist then all users will be challenged with LoginTC second-factor authentication (unless a static user list file exists).

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>

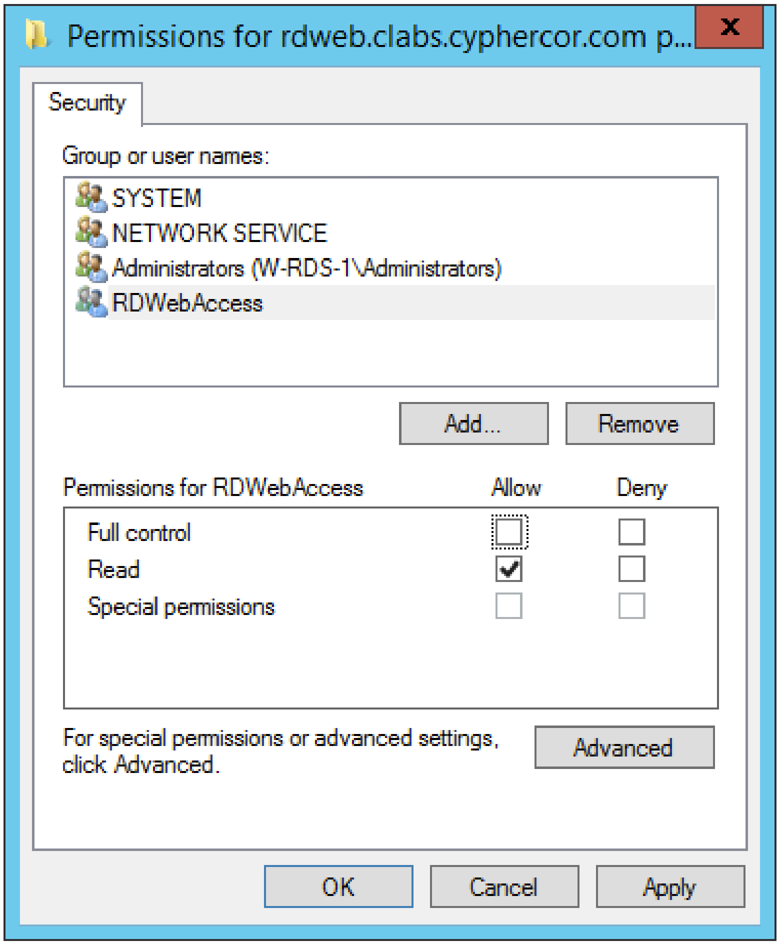
Field	Value
Authority Key Identifier	KeyID=a8 4a 6a 63 04 7d dd ...
Authority Information Access	[1]Authority Info Access: Acc...
Subject Alternative Name	DNS Name=rdweb.dabs.cyph...
Certificate Policies	[1]Certificate Policy:Policy Ide...
Key Usage	Digital Signature, Key Encipher...
Basic Constraints	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...

Security

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.

Email Support

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