

Two-Factor Authentication for Windows Login and RDP (2FA/MFA)

logintc.com/docs/connectors/windows-rdp-login



Overview

The LoginTC Windows Logon and RDP Connector integrates natively with Windows Server and Windows Client operating systems to add two-factor authentication for both remote desktop and local logins. LoginTC Windows Two-Factor Authentication solution adds an additional layer of security.

If you would like to protect your RD Web Access then you may be interested in the: [LoginTC RD Web Access Connector](#).

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 Windows Logon and RDP Connector. See the [Pricing](#) page for more information about subscription options.

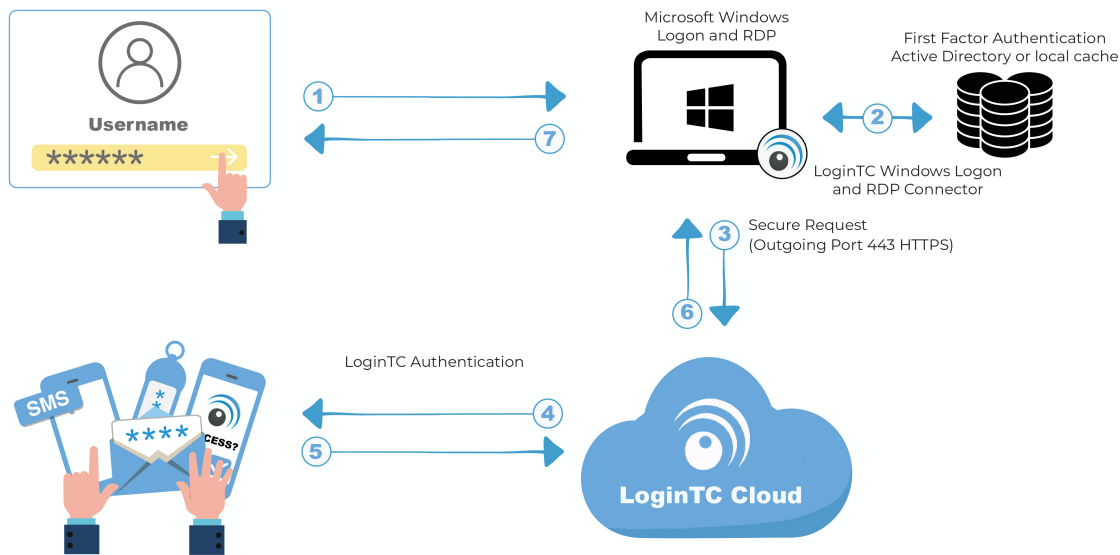
User Experience

After entering the username and password, 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.

How MFA for Windows Works

Watch Video At: <https://youtu.be/v0ki7hvGAuU>

Architecture



Windows 2FA/MFA Flow

1. A user attempts access with username / password
2. The username / password is verified against an existing first factor directory (i.e. Active Directory)
3. 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 Windows Logon and RDP Connector validates the user response
7. User is granted access to Windows laptop / desktop

System Requirements for LoginTC Two Factor Authentication (2FA/MFA)

Supported Windows Server versions:

- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

Supported Windows Client versions:

- Windows 8.1
- Windows 10
- Windows 11

Additional Requirements:

- [LoginTC Admin](#) account
- .NET Framework 4.6.1 or higher
- x64 architecture

Non-x64 architecture

LoginTC Windows Logon and RDP Connector is only compatible with x64 architecture systems. It will not run on systems, for example, that use ARM processors.

Start by creating a LoginTC Application for your Windows 2FA. An Application represents a service (e.g. RDP access to your Windows infrastructure) that you want to protect with LoginTC.

Create a LoginTC Application in [LoginTC Admin](#), follow [Create Application Steps](#).

If you have already created a LoginTC Application for your Windows 2FA, then you may skip this section and proceed to [Installation](#).

Normalize Usernames

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

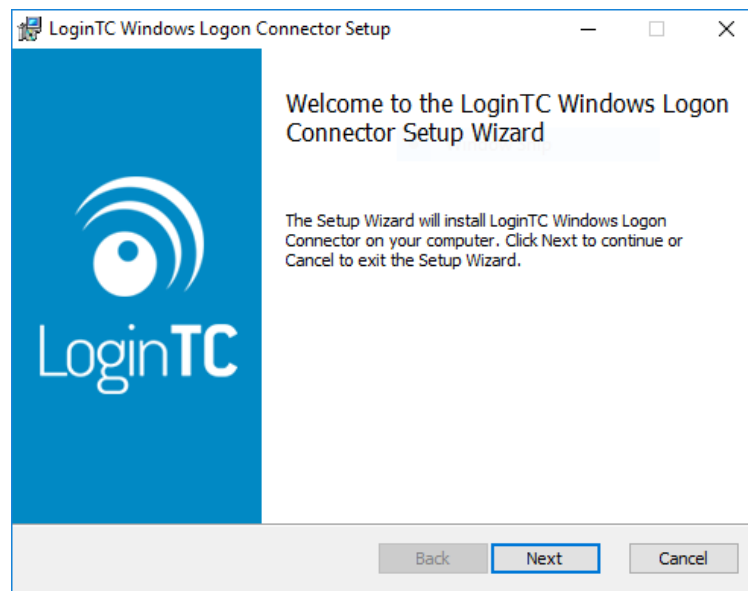
Configure **Normalize Usernames** from the Application settings by navigating to **Applications > Your Application > Settings**.

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

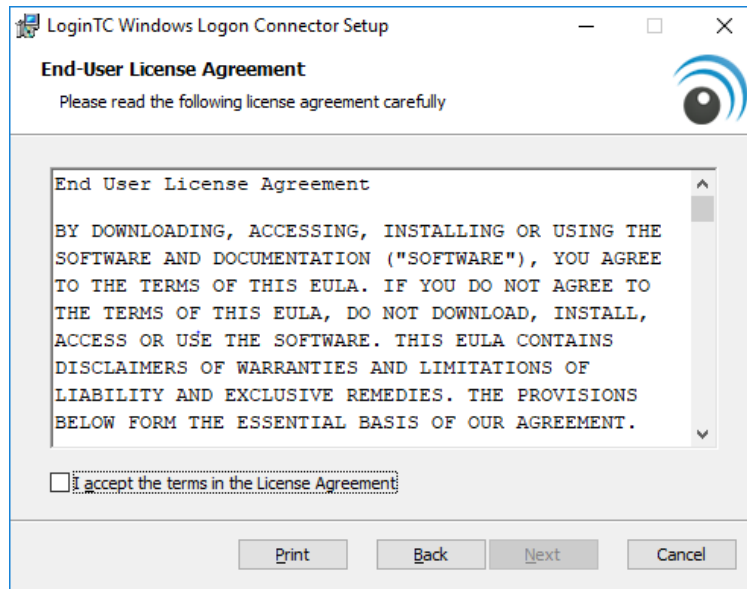
Windows Installer

Install the LoginTC Windows Logon and RDP Connector.

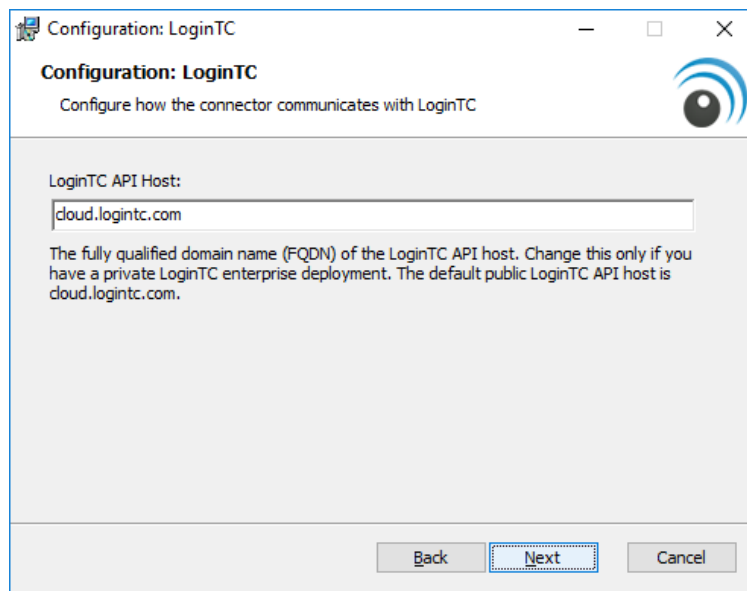
1. Download the latest version of the [LoginTC Windows Logon and RDP Connector](#)
2. Run the installer file as a privileged administrator user.
3. Press **Next**.



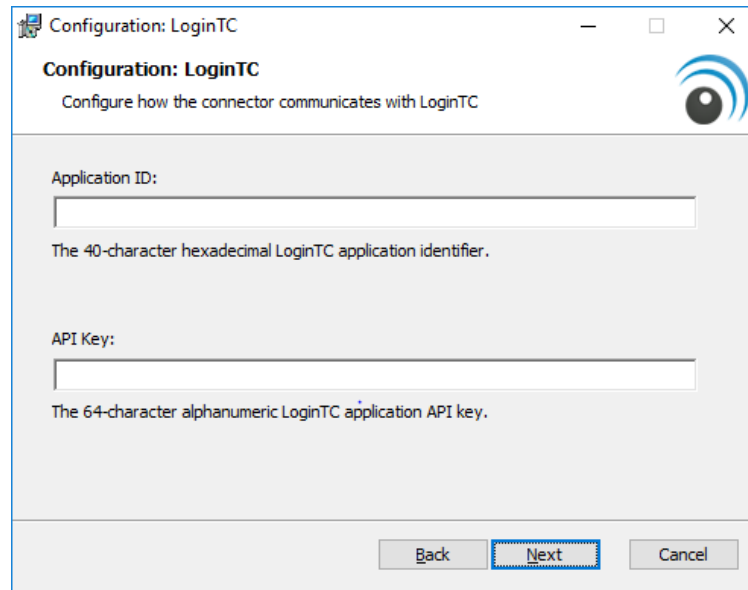
4. Read the License Agreement and press **Next** if you accept the terms.



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



6. Enter your LoginTC **Application ID** and **Application API Key**. These values are found on your LoginTC Admin Panel (see [Managing your Application](#)). Press **Next**.



Configuration: LoginTC

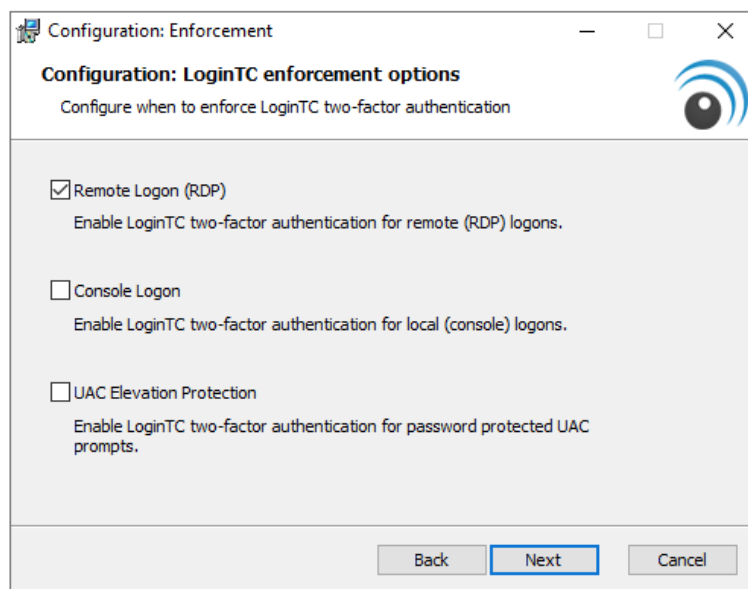
Configuration: LoginTC
Configure how the connector communicates with LoginTC

Application ID:
[Text Box]
The 40-character hexadecimal LoginTC application identifier.

API Key:
[Text Box]
The 64-character alphanumeric LoginTC application API key.

Back Next Cancel

7. Choose which logon types should be prompted for LoginTC. Press ****Next****.



Configuration: Enforcement

Configuration: LoginTC enforcement options
Configure when to enforce LoginTC two-factor authentication

☒ Remote Logon (RDP)
Enable LoginTC two-factor authentication for remote (RDP) logons.

☐ Console Logon
Enable LoginTC two-factor authentication for local (console) logons.

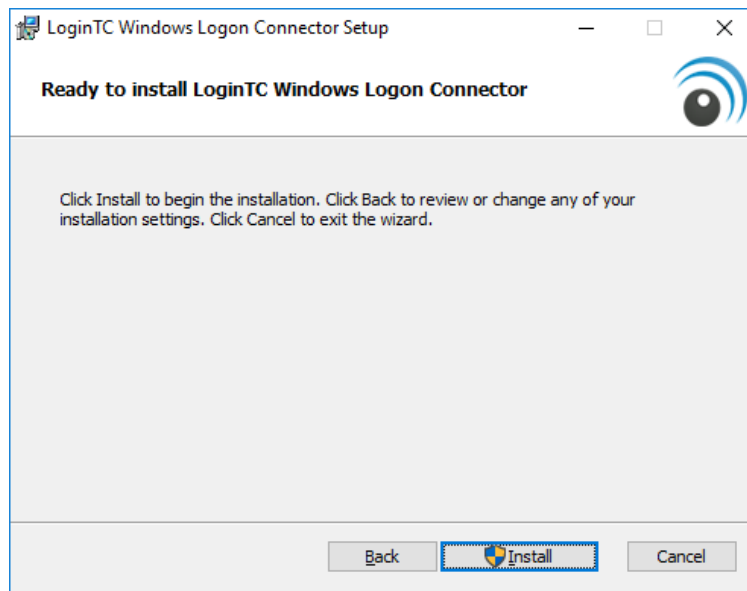
☐ UAC Elevation Protection
Enable LoginTC two-factor authentication for password protected UAC prompts.

Back Next Cancel

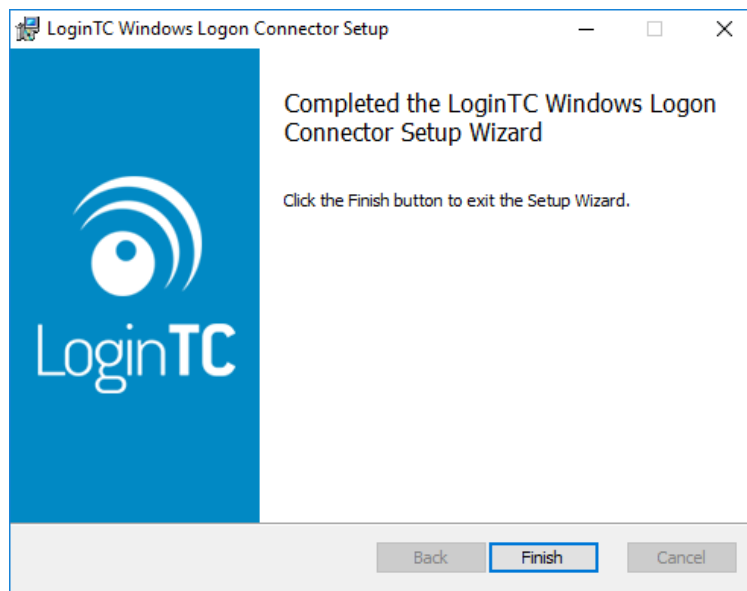
Protecting Local Logons

Note: After restarting the Windows host the LoginTC Windows Logon and RDP Connector will be fully installed and operational. See [Which Windows logon prompts does LoginTC protect?](#) for more information.

8. Press **Install**.



9. Press **Finish**



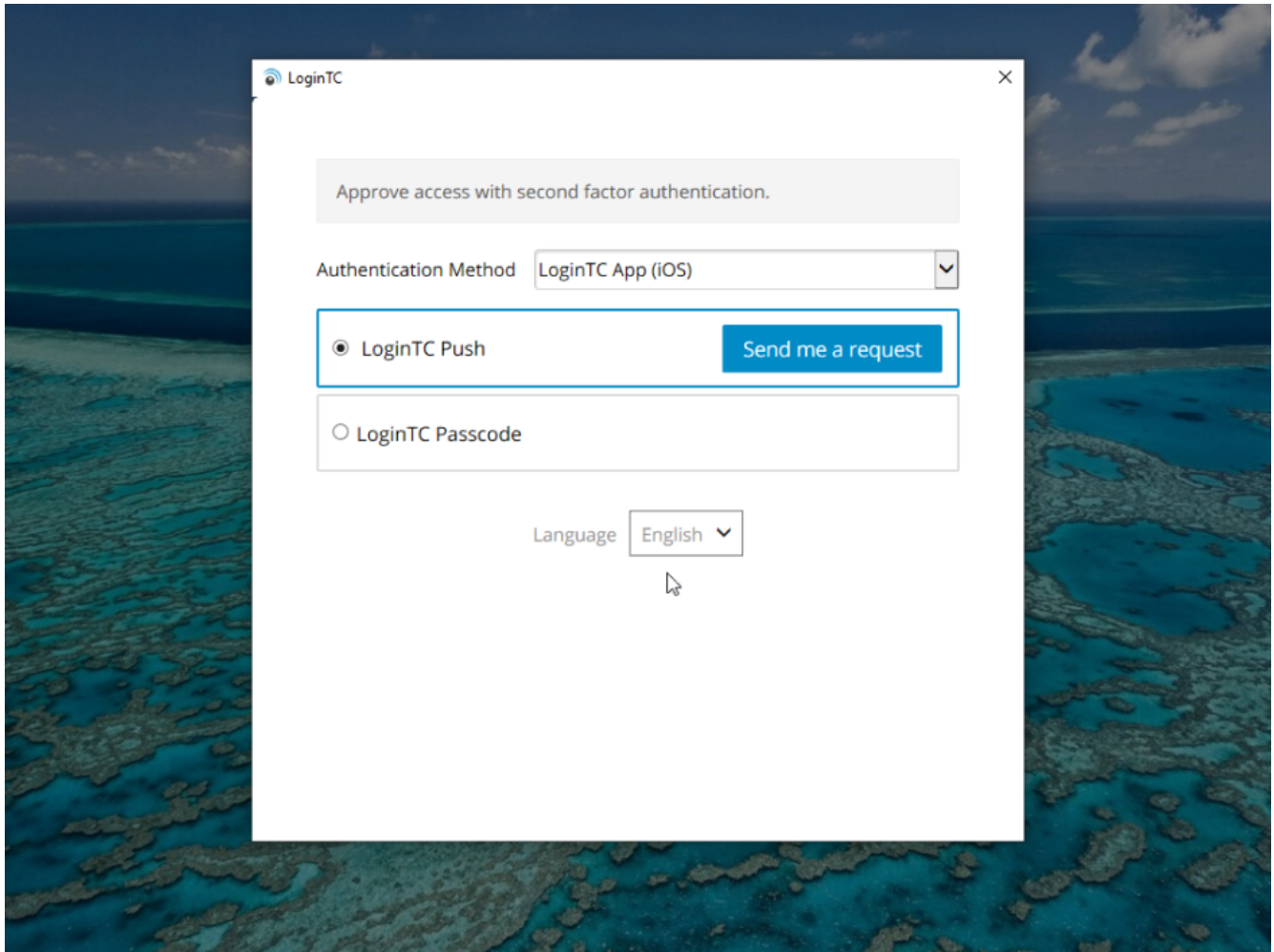
The LoginTC Windows Logon and RDP Connector is now installed. It will start protecting logins once the Windows host is restarted.

Usage

Your users may login in several ways. This chapter details the user experience for each interaction.

RDP Login

When a user launches their RDP client they will be presented with the standard login sequence. After successfully logging in with their username and password, they are shown the LoginTC login page on the remote host. Various login options for the second-factor LoginTC authentication are presented. Once successfully authenticated with LoginTC the user is logged into the host.

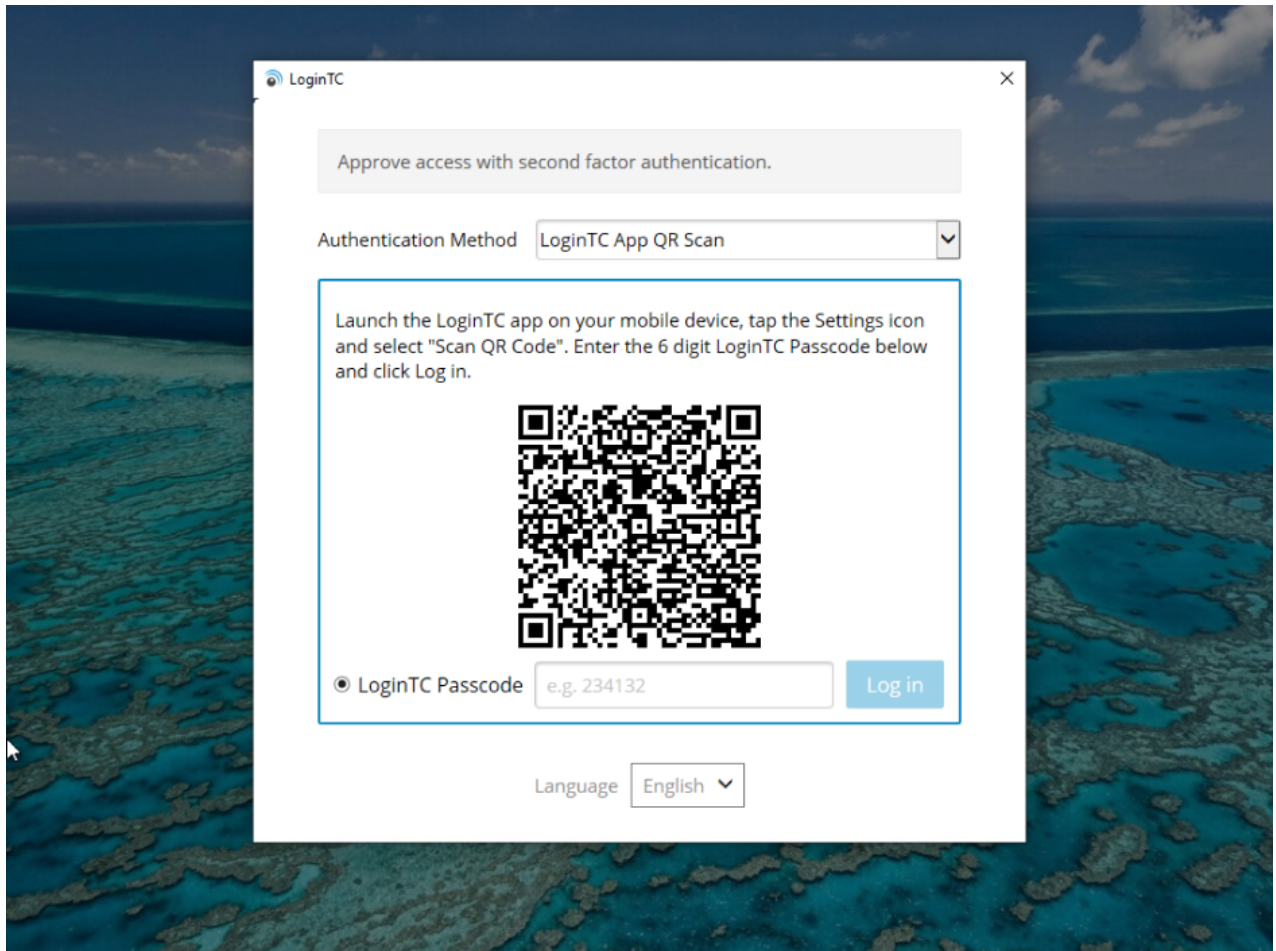


After successfully logging in with their username and password, they are shown the LoginTC login page on the local host. Various login options for the second-factor LoginTC authentication are presented. Once successfully authenticated with LoginTC the user is logged into the host.

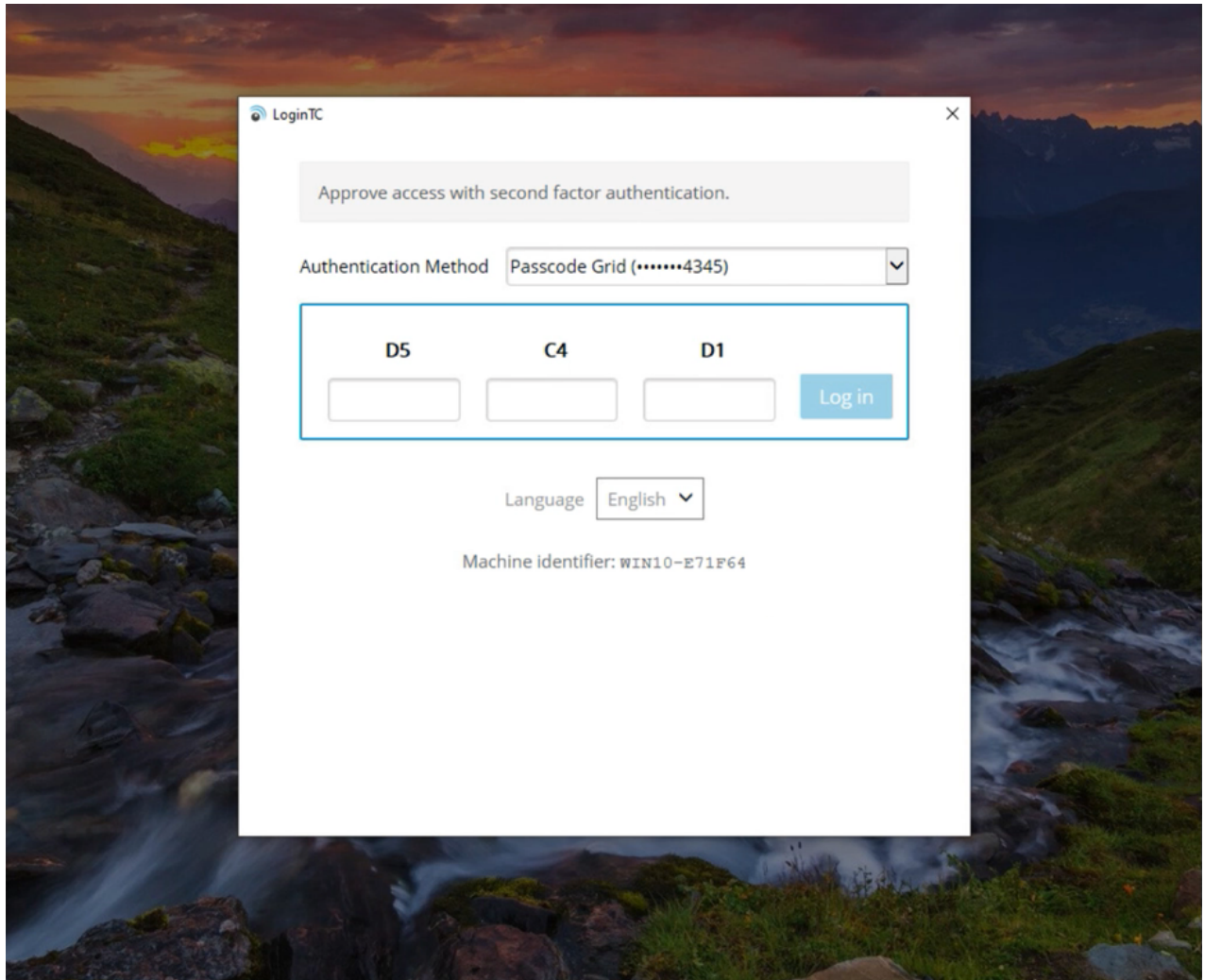
If the host does not have internet connectivity then after successfully logging in with their username and password, the user is shown options for logging in offline.

There are three methods of offline authentication:

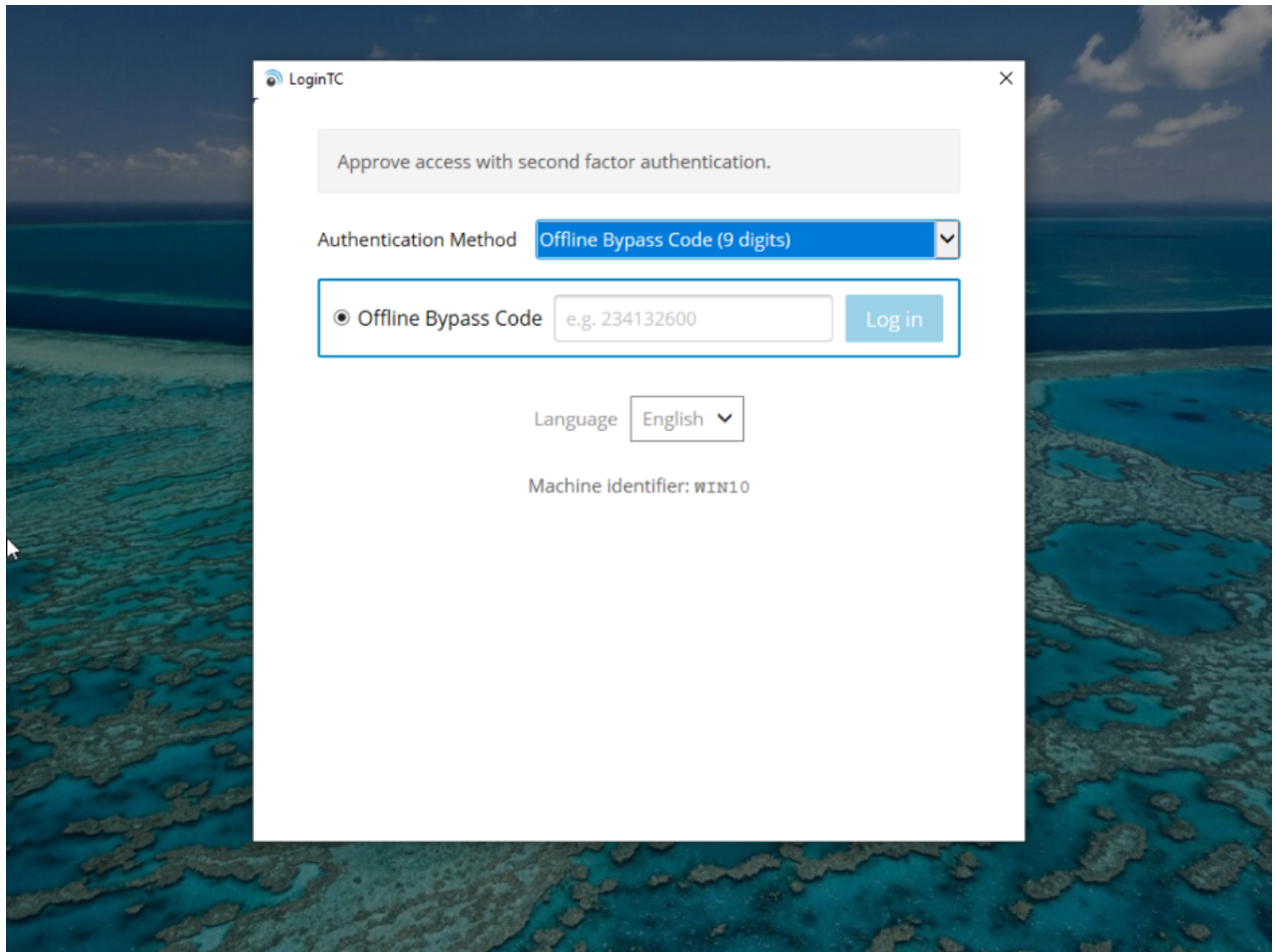
1. **QR Scan Authentication.** The user launches the LoginTC App, select **Settings > Scan QR Code** and then scan the displayed QR Code. If the scan is successful a 6-digit code is displayed for the user to enter and authenticate. QR Scan Authentication is only supported for LoginTC iOS App and LoginTC Android App.



2. **Passcode Grid.** The user enters the 3-letter tuples corresponding to their own passcode grid. If the response is accurate they are logged in. To learn more see: [Passcode Grids](#).



3. **Offline Bypass Code.** The user must enter a 9-digit Offline Bypass Code which is provided to them by their support desk. Codes are regenerated each time the user logs in online and can be found on the users page in the LoginTC Admin Panel under **Offline Bypass Codes**.

A screenshot of the LoginTC authentication window. The window has a title bar with the LoginTC logo and a close button. The main content area is white and contains the following elements: a grey instruction box at the top saying "Approve access with second factor authentication."; a dropdown menu for "Authentication Method" currently set to "Offline Bypass Code (9 digits)"; a section with a radio button selected for "Offline Bypass Code" and a text input field containing "e.g. 234132600"; a blue "Log in" button; a "Language" dropdown menu set to "English"; and a "Machine identifier: WIN10" label at the bottom. The window is overlaid on a background image of a coral reef.

Must login online prior to offline methods being available

Offline methods are online available if the user has logged in online at least once. If the users token or passcode grid is revoked and re-issued, QR Scan and Passcode Grid Authentication will only be displayed after again logging in online at least once.

Policies

Offline authentication methods must be enabled in the authentication **Policy**. Navigate to **Policies** then your policy (or **Organization Policy** for global coverage). Scroll down to **Offline Authentication** to enable.

LoginTC

Example Inc. ▾ Business

DocsSupportadministrator@example.com ▾

GENERAL

Dashboard

Users

Applications

Policies

Groups

Bypass Codes

Devices

Phones

Hardware Tokens

U2F Tokens

Authentication Logs

User Logs

SETUP

Domains

Administrators

Admin Logs

Settings

Billing

CUSTOMER ID

1797-364192

Policies / Organization Policy

Cancel

Offline Authentication

Specify offline authentication behaviour. Settings take effect next time the user logs in online into the LoginTC Windows Logon Connector.

Offline Authentication

Enabled

Disabled

Allow users to authenticate offline.

Offline QR Scan Authentication

Enabled

Disabled

Allow users to authenticate using offline QR Scan.

Passcode Grids

Enabled

Disabled

Allow users to authenticate with a passcode grid.

Offline Bypass Codes

Enabled

Disabled

Number Offline Bypass Codes Issued

5

Allow users to authenticate using offline bypass codes. Allow up to a certain number of issued codes. Codes are regenerated each time the user logs in online.

Offline Days Limit

No Limit

Allow users to login up to a certain number of days when offline.

Successful Offline Login Limit

No Limit

Allow users to login a certain number of times when offline.

Invalid Offline Login Limit

10

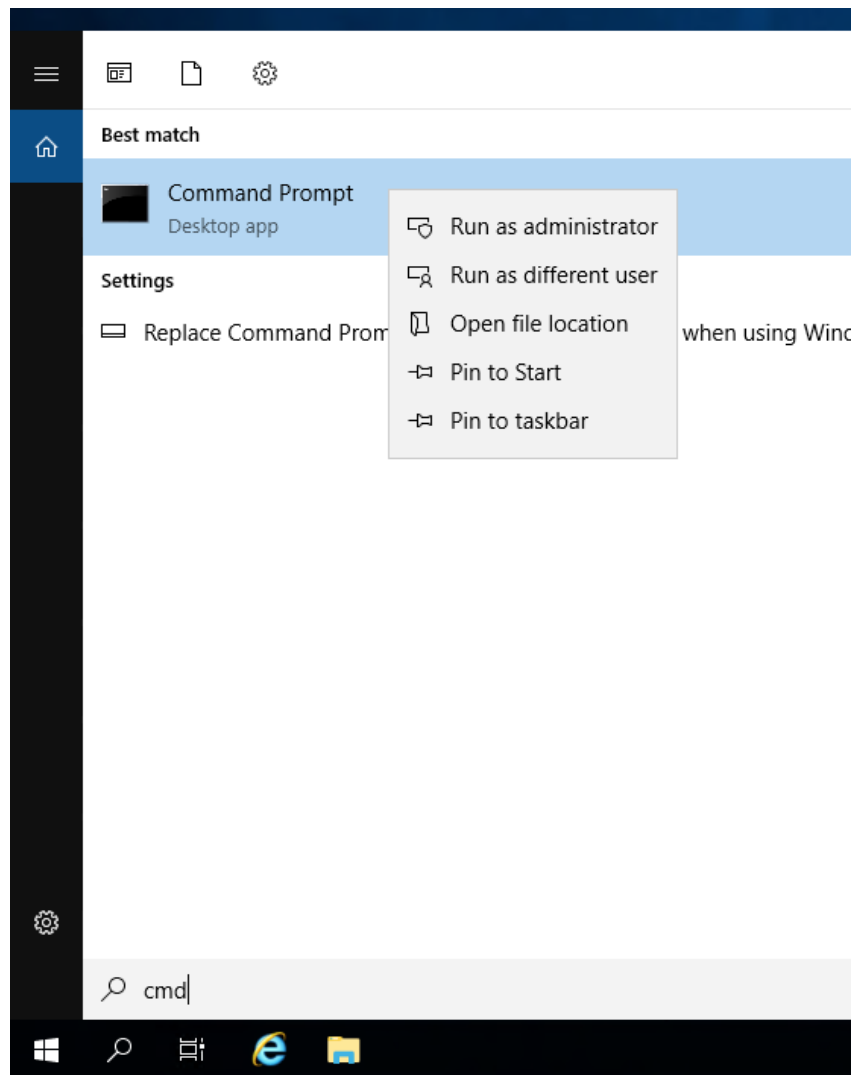
Limit invalid login attempts when offline.

UAC (Run as administrator)

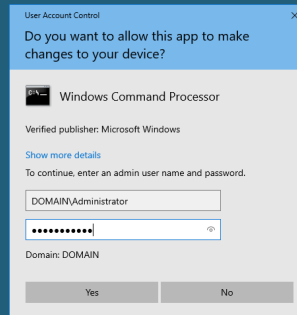
When LoginTC for UAC is enabled, the user requesting elevated privileges is prompted to authenticate with LoginTC:

11/22

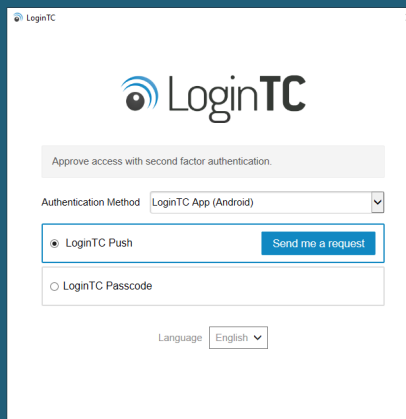
1. User right clicks on an application and clicks on Run as administrator



2. User is prompted to enter the credentials of an administrator



3. User is prompted to perform LoginTC authentication for that particular administrator



UAC Limitations

A LoginTC prompt is not prompted for the following scenarios: Run as different user; commandlets such as **Enter-PSSession**, **Invoke-Command**, and **Get-Credential**

Remembered Devices

Enforce a policy to allow a Windows device to be remembered for specified duration until the user signs out of their machine, reboots, logs in offline or changes networks. This feature applies to console unlock logons.

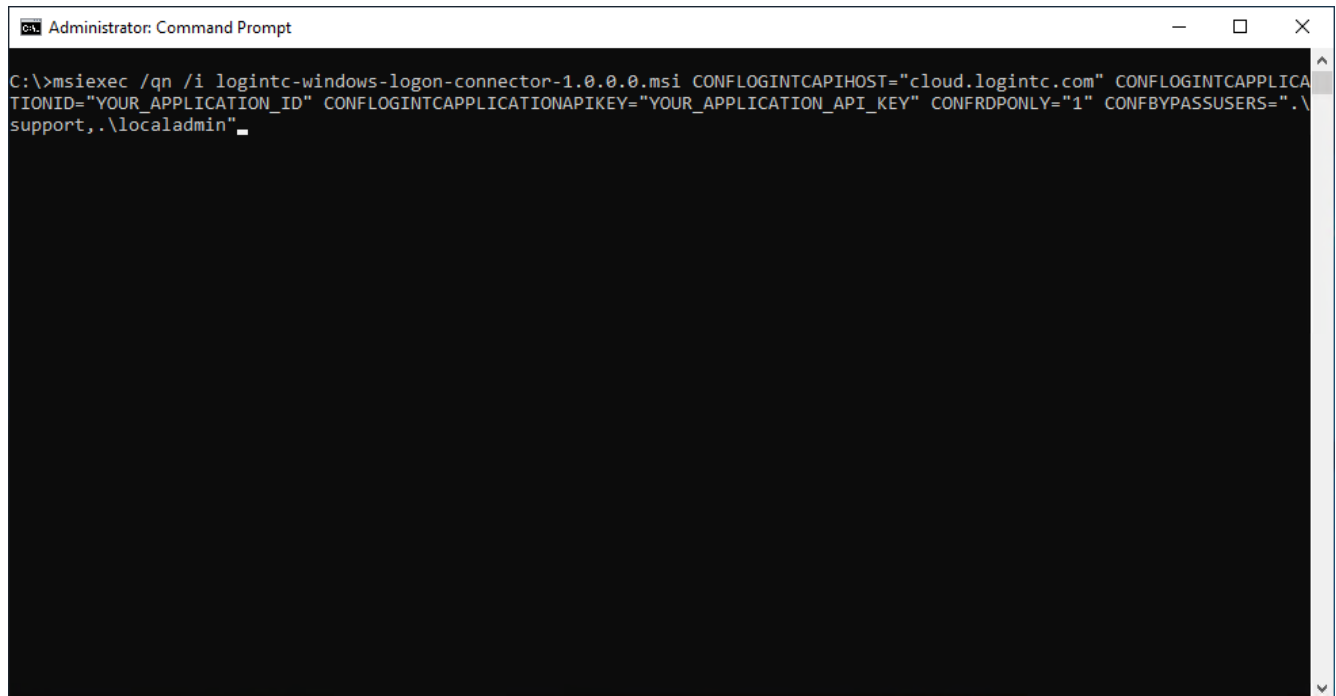
Remembered devices also works for offline logons.

Policies

Remembered Devices must be enabled in the authentication **Policy**. Navigate to **Policies** then your policy (or **Organization Policy** for global coverage). Scroll down to **Remembered Devices** to enable.

Command line Installation

You may also install the LoginTC Windows Logon and RDP Connector from the Command Prompt. This is particularly useful when deploying to a large number of machines.



```
Administrator: Command Prompt
C:\>msiexec /qn /i logintc-windows-logon-connector-1.0.0.0.msi CONFLOGINTCAPIHOST="cloud.logintc.com" CONFLOGINTCAPPLICA
TIONID="YOUR_APPLICATION_ID" CONFLOGINTCAPPLICATIONAPIKEY="YOUR_APPLICATION_API_KEY" CONFRDPONLY="1" CONFEBYPASSUSERS=".
support,.\localadmin"
```

To install from the Command Prompt:

1. Find the Command Prompt in the Start menu
2. Right Click and select "Run as administrator"
3. Enter the following command (refer to the table below for configuration options)

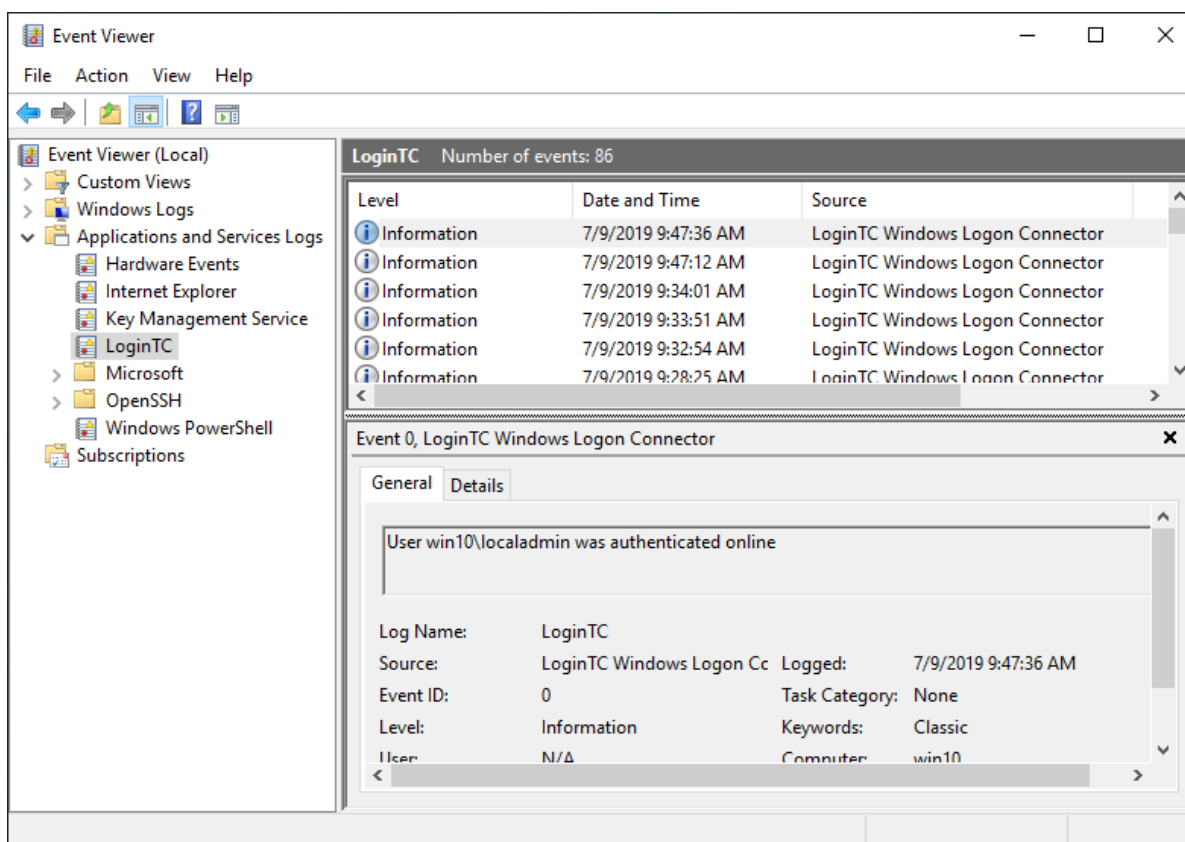
```
msiexec /qn /i logintc-windows-logon-connector-1.2.0.0.msi CONFLOGINTCAPIHOST="cloud.logintc.com"
CONFLOGINTCAPPLICATIONID="YOUR_APPLICATION_ID" CONFLOGINTCAPPLICATIONAPIKEY="YOUR_APPLICATION_API_KEY"
CONFENABLERDP="1" CONFENABLECONSOLE="0" CONFENABLEUAC="0" CONFEBYPASSUSERS=".support,.\localadmin"
```

Flag	Meaning	Example
CONFLOGINTCAPIHOST	The LoginTC API host	cloud.logintc.com
CONFLOGINTCAPPLICATIONID	The 40-character Application ID (found in the Admin Panel)	5de7c5b82a6972...
CONFLOGINTCAPPLICATIONAPIKEY	The 64-character Application API Key (found in the Admin Panel)	5R2EgzXB0Hx3RN...
CONFENABLERDP	1 to enable LoginTC for remote (RDP) logins, or 0 for all logins	1
CONFENABLECONSOLE	1 to enable LoginTC for console logins (or 0 to disable)	0
CONFENABLEUAC	1 to enable LoginTC for UAC (or 0 to disable)	0

Flag	Meaning	Example
CONFCHALLENGEGROUPS	(Optional) Groups whose members will be challenged. Refer to Challenge Groups section for more information.	RemoteMFAUsers
CONFBYPASSGROUPS	(Optional) Groups whose members will be bypassed. Refer to Bypass Groups section for more information.	RemoteMFAUsers
CONFCHALLENGEUSERS	(Optional) Users which will be challenged. Refer to Challenge Users section for more information.	*\support
CONFBYPASSUSERS	(Optional) Users which will be bypassed. Refer to Bypass Users section for more information.	*\support

Logging

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



Passthrough

There are several ways 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 rolling out a deployment to minimize the impact on others or to maintain operational access to the hosts. Bypass settings are configured on each host where the LoginTC Connector is installed for your Windows multi-factor authentication (2FA/MFA).

Challenge Groups

The [ChallengeGroups](#) attribute is a comma delimited list of groups for which all member users will be challenged with LoginTC second factor authentication. When either [ChallengeGroups](#) or [ChallengeUsers](#) is specified both [BypassGroups](#) and [BypassUsers](#) is ignored. If the user is not part of any challenge group, they are logged in without LoginTC two factor authentication (2FA/MFA).

Using Active Directory Groups

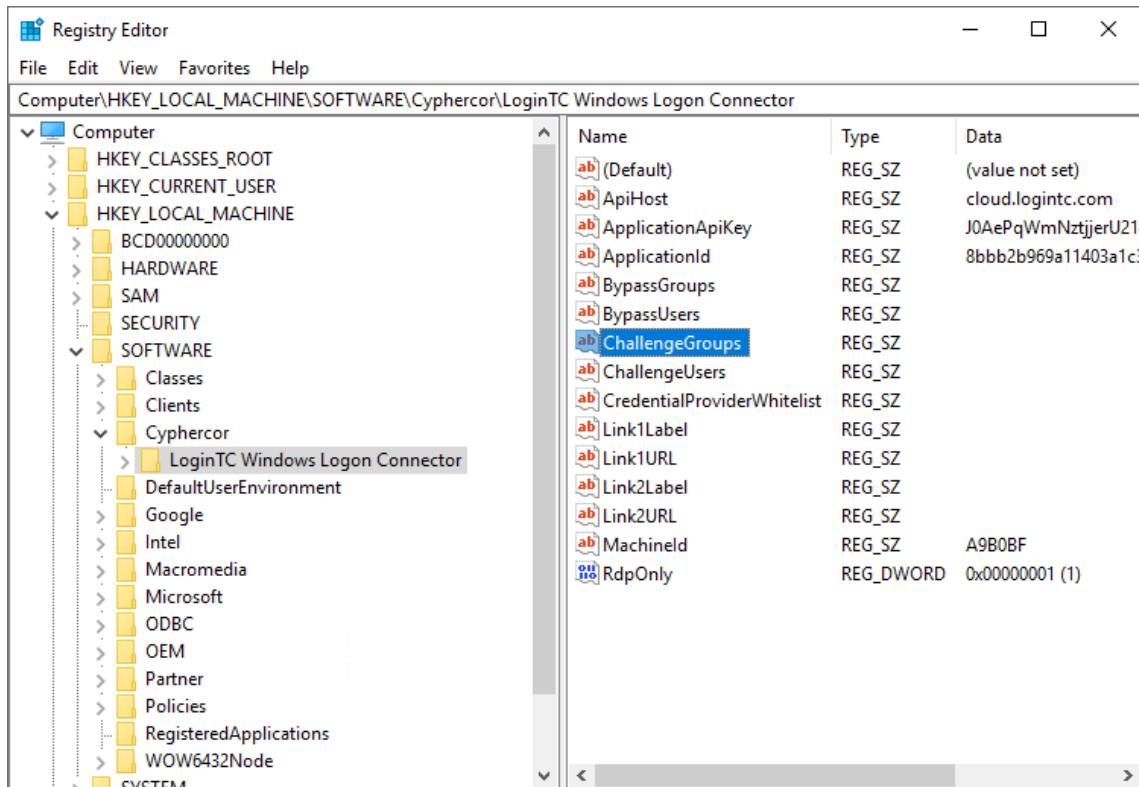
Note: Some groups cannot be retrieved by the LoginTC Windows Logon Connector like **Remote Interactive Logon**, **High Mandatory Level** and similar Special Identities and non-Active Directory based groups. Recommend using only groups defined and managed in Active Directory.

Offline Active Directory Groups

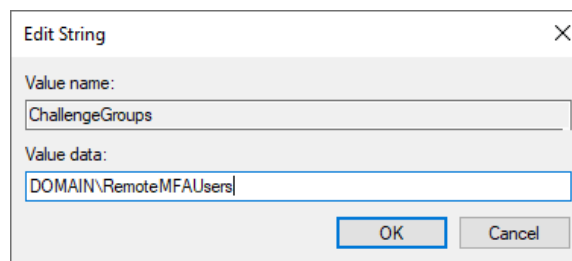
Note: Security identifiers (SIDs) should be used for Challenge and Bypass groups instead of group names when the machine is expected to be used offline (or when the Active Directory domain controllers are expected to be unreachable).

Instructions to set **ChallengeGroups** attribute:

1. Launch **regedit** (Registry Editor).
2. Navigate to **HKEY_LOCAL_MACHINE > SOFTWARE > Cyphercor > LoginTC Windows Logon Connector**



3. Click to modify the **ChallengeGroups** field



4. Enter a comma delimited list of challenge groups

Format	Meaning	Example
*\groupname	All groups part of any domain that have name groupname.	*\RemoteMFAUsers
DOMAIN\groupname	Groups with name groupname belonging to DOMAIN domain.	DOMAIN\RemoteMFAUsers
groupname	Local group with name groupname.	RemoteMFAUsers

Format	Meaning	Example
SID	Group security identifiers (SIDs)	S-1-5-21-...

- Click **OK** to save changes.

Bypass Groups

The **BypassGroups** attribute is a comma delimited of groups for which all member users will not be challenged with LoginTC second factor authentication. When either **ChallengeGroups** or **ChallengeUsers** is specified both **BypassGroups** and **BypassUsers** is ignored. If the user is not part of any bypass group, they are challenged with LoginTC second factor authentication.

Using Active Directory Groups

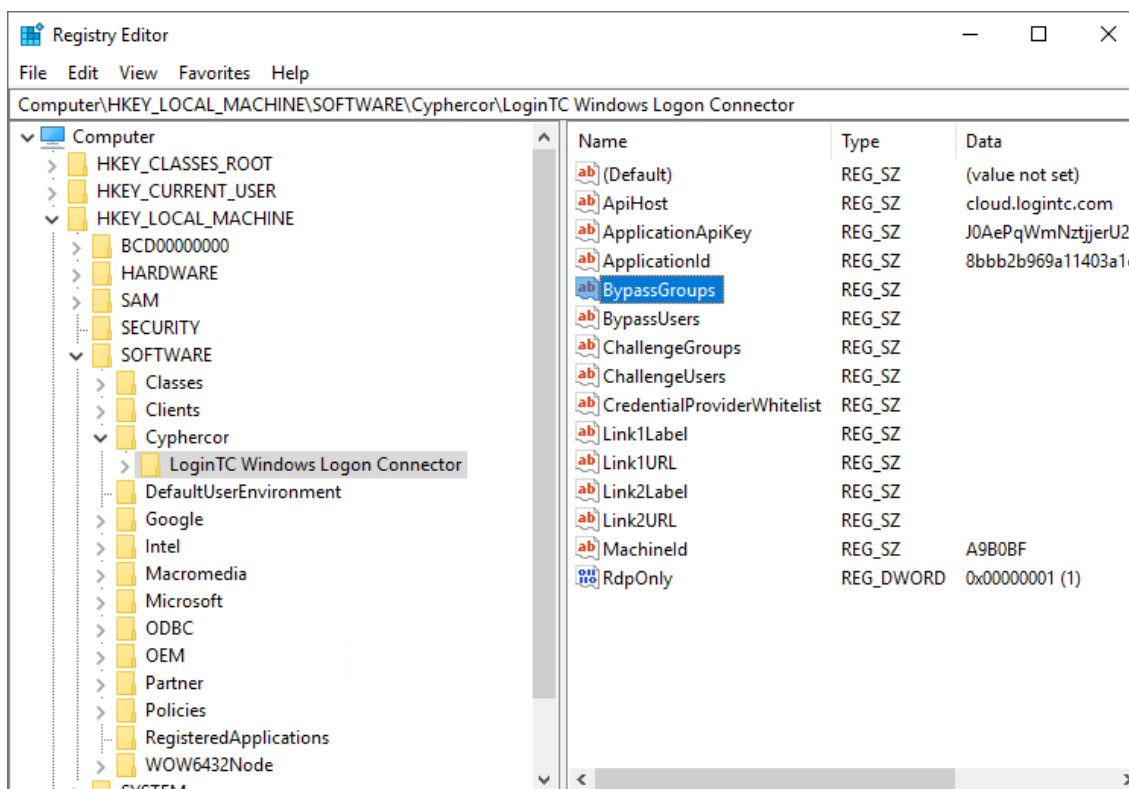
Note: Some groups cannot be retrieved by the LoginTC Windows Logon Connector like **Remote Interactive Logon**, **High Mandatory Level** and similar Special Identities and non-Active Directory based groups. Recommend using only groups defined and managed in Active Directory.

Offline Active Directory Groups

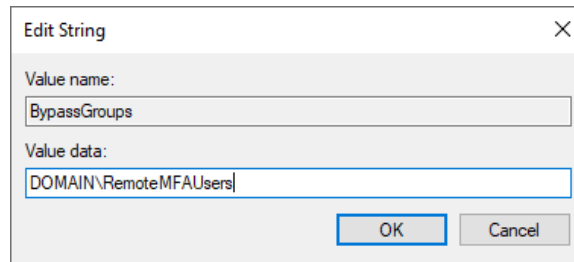
Note: Security identifiers (SIDs) should be used for Challenge and Bypass groups instead of group names when the machine is expected to be used offline (or when the Active Directory domain controllers are expected to be unreachable).

Instructions to set **ChallengeGroups** attribute:

- Launch **regedit** (Registry Editor).
- Navigate to **HKEY_LOCAL_MACHINE > SOFTWARE > Cyphercor > LoginTC Windows Logon Connector**



3. Click to modify the **BypassGroups** field



4. Enter a comma delimited list of challenge groups

Format	Meaning	Example
*\groupname	All groups part of any domain that have name groupname.	*\RemoteMFAUsers
DOMAIN\groupname	Groups with name groupname belonging to DOMAIN domain.	DOMAIN\RemoteMFAUsers
groupname	Local group with name groupname.	RemoteMFAUsers
SID	Group security identifiers (SIDs)	S-1-5-21-...

5. Click **OK** to save changes.

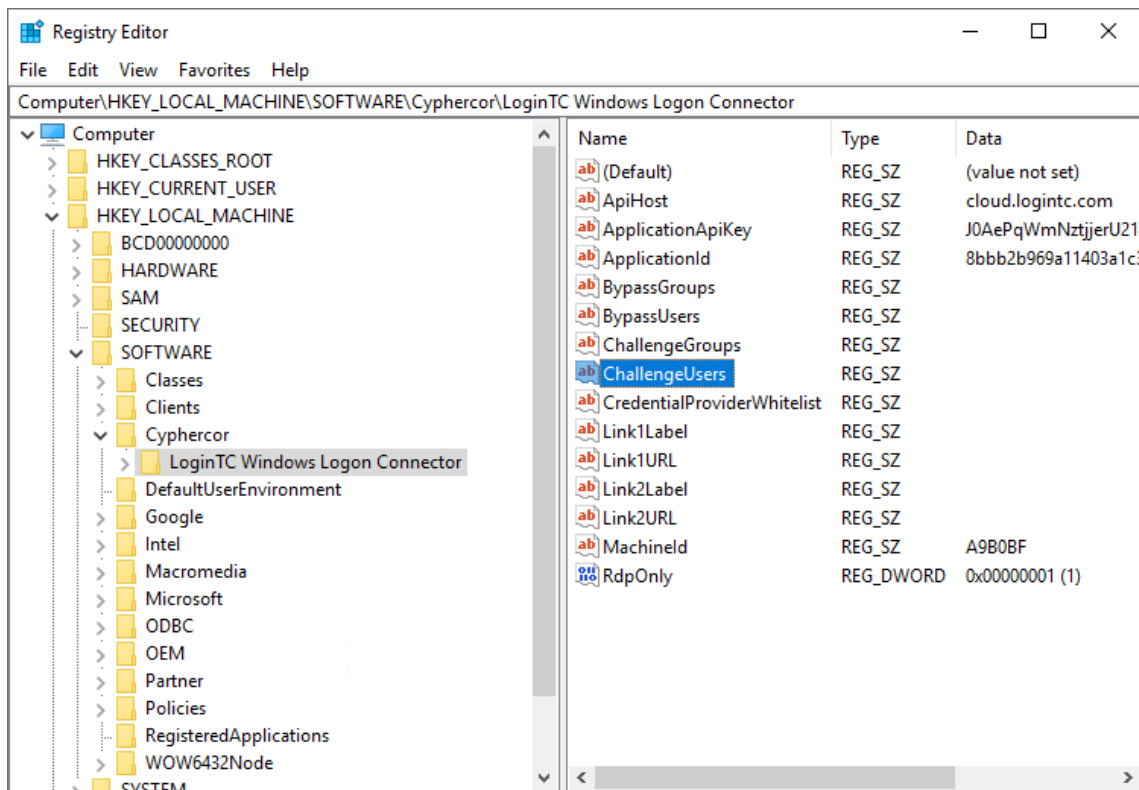
Challenge Users

The **ChallengeUsers** attribute is a comma delimited list of users which will be challenged with LoginTC second factor authentication. When either **ChallengeGroups** or **ChallengeUsers** is specified both **BypassGroups** and **BypassUsers** is ignored. If the user does not match any challenge user, they are logged in without LoginTC two factor authentication (2FA/MFA).

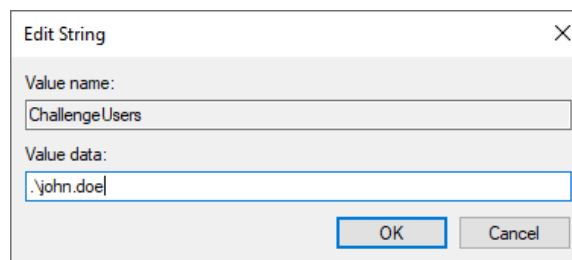
Instructions to set **ChallengeUsers** attribute:

1. Launch **regedit** (Registry Editor).

2. Navigate to **HKEY_LOCAL_MACHINE > SOFTWARE > Cyphercor > LoginTC Windows Logon Connector**



3. Click to modify the **ChallengeUsers** field



4. Enter a comma delimited list of challenge users, see format:

Format	Meaning	Example
*\username	All accounts, local or on any domain that have username username.	*\john.doe
.\username	Local account with username username.	.\john.doe
DOMAIN\username	Domain account with username username belonging to DOMAIN domain.	CORP\john.doe

5. Click **OK** to save changes.

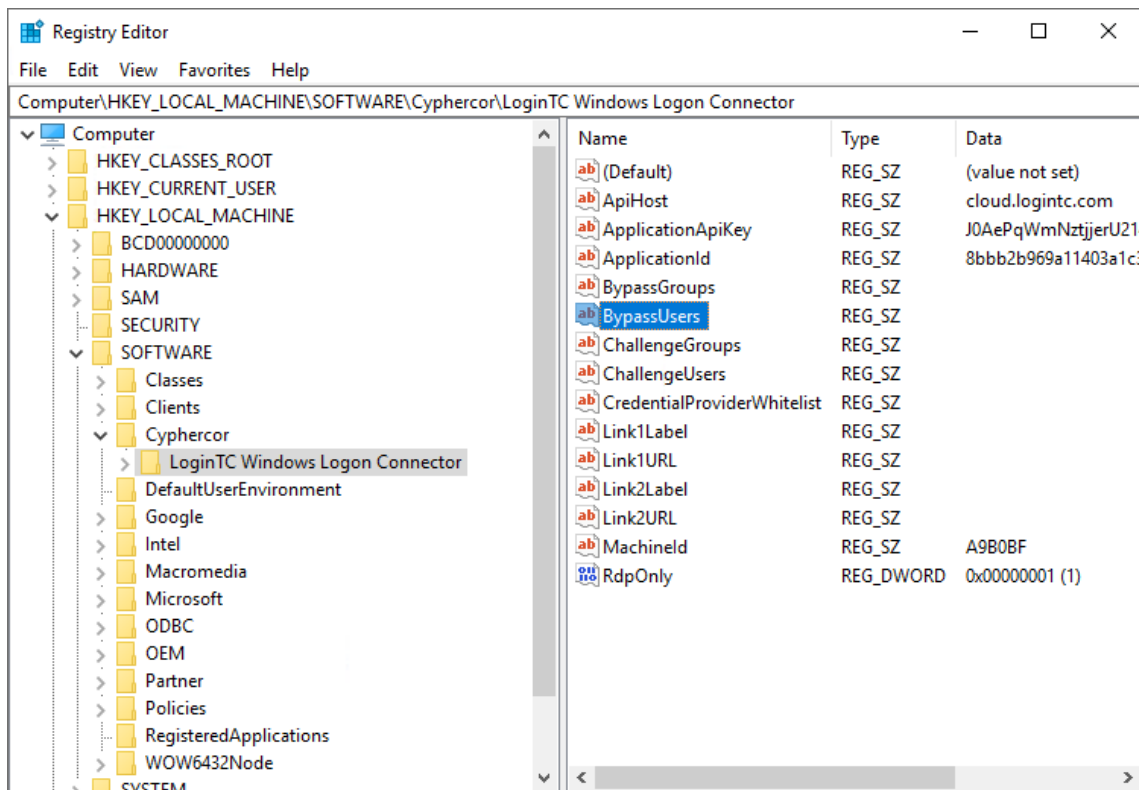
Bypass Users

The **BypassUsers** attribute is a comma delimited of users which will not be challenged with LoginTC second factor authentication. When either **ChallengeGroups** or **ChallengeUsers** is specified both **BypassGroups** and **BypassUsers** is ignored. If the user does not match any bypass user, they are challenged with LoginTC two factor authentication (2FA/MFA).

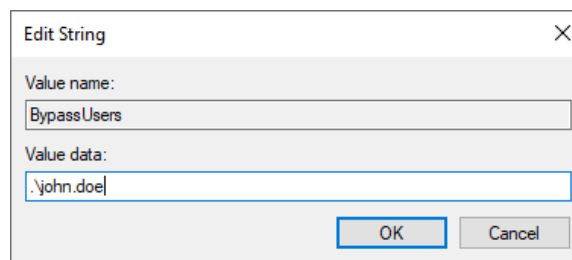
Instructions to set **BypassUsers** attribute:

1. Launch **regedit** (Registry Editor).

2. Navigate to **HKEY_LOCAL_MACHINE > SOFTWARE > Cyphercor > LoginTC Windows Logon Connector**



3. Click to modify the **BypassUsers** field



4. Enter a comma delimited list of challenge users, see format:

Format	Meaning	Example
*\username	All accounts, local or on any domain that have username username.	*\john.doe
.\username	Local account with username username.	.\john.doe
DOMAIN\username	Domain account with username username belonging to DOMAIN domain.	CORP\john.doe

5. Click **OK** to save changes.

FAQ

The LoginTC Windows two factor authentication (2FA/MFA) protects:

- Remote Desktop Logins
- Local Logins
- Run as administrator

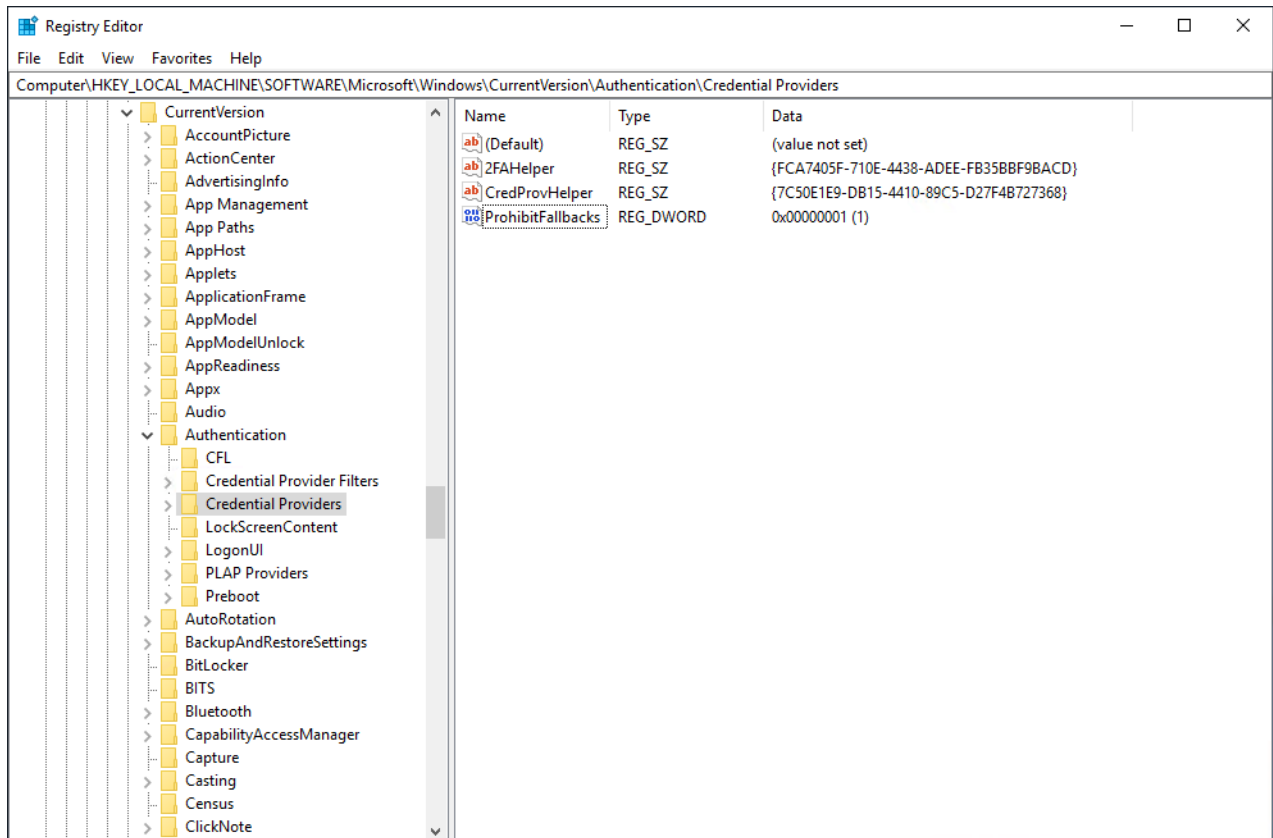
The LoginTC Windows two factor authentication (2FA/MFA) does not protect:

- “Run as different user”

- [RDP Restricted Admin Mode](#)
- Pre-Logon Access Providers (PLAPs) such as Always On VPN
- Noninteractive logins (e.g. batch process, mapping network drive, logon as a service, scheduled tasks)
- PowerShell cmdlets: “Get-Credential”, “Enter-PsSession”, “Invoke-Command”

By default, Windows disables all credential providers except the built-in password credential provider when in Safe Mode. If you wish to enable LoginTC in Safe Mode, you can do so by following these instructions:

1. Open the Registry Editor
2. Navigate to **HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Windows > CurrentVersion > Authentication > Credential Providers**
3. Create a key DWORD entry named **ProhibitFallbacks** with the value **1**



Does the LoginTC Windows Logon and RDP Connector support Microsoft/Live accounts?

No, the connector does not support Microsoft/Live accounts.

Can the installer be deployed automatically?

Yes, commandline installation is supported: [Command line installation](#)

An end to end sample guide on deploying using Group Policy: [Automatic LoginTC Windows Logon and RDP Connector Deployment](#).

Upgrade

To upgrade the LoginTC Windows Logon and RDP Connector, first uninstall the previous version and then install the newer version.

Uninstallation

To uninstall the LoginTC Windows Logon and RDP Connector, simply navigate to the **Add or remove programs** in the Windows **Control Panel**, find LoginTC Windows Logon and RDP Connector in the list and follow the prompts.

You may also uninstall the LoginTC Windows Logon and RDP Connector from the Command Prompt. This is particularly useful when deploying to a large number of machines.

To uninstall from the Command Prompt:

1. Find the Command Prompt in the Start menu
2. Right Click and select "Run as administrator"
3. Enter the following command

```
msiexec /uninstall logintc-windows-logon-connector-1.0.3.0.msi /norestart /quiet
```

NOTE: The msi file has to be the same version that's installed.

Troubleshooting

Email Support

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