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

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



Overview

The LoginTC Windows Logon and RDP Connector integrates natively with Windows Server and Windows Client operating systems to add <u>two-factor authentication</u> 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: <u>LoginTC RD Gateway with RADIUS Connector</u>.

Subscription Requirement

Your organization requires the **Business** or **Enterprise** plan to use the LoginTC Windows Logon and RDP Connector. See the <u>Pricing</u> 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 <u>Installation</u>.

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.

| LoginTC Windows Logon 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 BELOW FORM THE ESSENTIAL BASIS OF OUR AGREEMENT. | ¥ |
| Print Back Next Ca | ancel |

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 communicate | es with LoginTC | : | | |) |
| LoginTC API Host: | | | | | |
| cloud.logintc.com | | | | | |
| The fully qualified domain name (FQDN) of t have a private LoginTC enterprise deployme cloud.logintc.com. | he LoginTC AP ent. The defau | I host. Chang | ge this o | nly if you host is | |
| | <u>B</u> ack | Next | | Cano | el |

6. Enter your LoginTC **Application ID** and **Application API Key**. These values are found on your LoginTC Admin Panel (see <u>Managing your Application</u>. Press **Next**.

| 🕼 Configuration: LoginTC — 🗌 🗙 |
|--|
| Configuration: LoginTC 🦳 |
| Configure how the connector communicates with LoginTC |
| Application ID: |
| |
| The 40-character hexadecimal LoginTC application identifier. |
| |
| |
| API Key: |
| |
| 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 | | 1 | |
| Configure when to enforce LoginTC two-factor authentication | | (| D)) |
| Remote Logon (RDP) | | | |
| Kellote Logon (Kbr) | | | |
| 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 U prompts. | AC | | |
| | | | |
| Back Next | | Cano | el |

Protecting Local Logons

Note: After restarting the Windows host the LoginTC Windows Logon and RDP Connector will be fully installed and operational. See <u>Which Windows logon prompts does LoginTC protect?</u> 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. Vadious login options for the second-factor LoginTC authentication are presented. Once successfully authenticated with LoginTC the user is logged into the host.

|) | .ogínTC | | × | |
|--|-----------------------|------------------------------|-----------|--------|
| and the second second | Approve access with s | econd factor authentication. | | |
| | Authentication Method | LoginTC App (iOS) | ~ | |
| | Output LoginTC Push | Send me | a request | |
| | O LoginTC Passcode | | | |
| | | Language English 💙 | | |
| | | | | |
| | | | | in the |
| and the second sec | (idad) | | | |

After successfully logging in with their username and password, they are shown the LoginTC login page on the local host. Vadious 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:

 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.

|) La | aginTC Approve access with second factor authentication. | × |
|-----------------|---|------|
| | Authentication Method LoginTC App QR Scan | |
| | Launch the LoginTC app on your mobile device, tap the Settings icon and select "Scan QR Code". Enter the 6 digit LoginTC Passcode below and click Log in. | |
| Real Providence | LoginTC Passcode e.g. 234132 Log in | |
| | Language English 🗸 | 10-0 |

2. **Passcode Grid**. The user enters the 3-letter tuples corresponding to their own passcode grid. If the response is accurate their are logged in. To learn more see: <u>Passcode Grids</u>.

| | oginTC | | | × | Non and |
|----------------|---------------------|-------------------------|-------------|--------|------------|
| | Approve access wi | ith second factor auth | entication. | | |
| | Authentication Meth | Passcode Grid (• | 4345) | ~ | |
| and the second | D5 | C4 | D1 | | S |
| | | | | Log in | Carlos and |
| | | Language Engl | ish 🗸 | | |
| as the | 1 | Machine identifier: wɪ: | N10-E71F64 | | No an Zen |
| | | | | | |
| BEE | | | | | |
| 12 | | | | | 6.200 |
| area and | | | 1 | | |

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.

| LoginTC | × |
|--|--------|
| Approve access with second factor authentication. | n - en |
| Authentication Method Offline Bypass Code (9 digits) | |
| Offline Bypass Code e.g. 234132600 Log in | |
| Language English 🗸 | |
| Machine identifier: WIN10 | |
| | 1 - C |
| | |
| | |
| and the second of the second o | D'O |
| | 1 |

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 gird 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.

| စာ Login TC Exam | ple Inc. 👻 Business | 🖉 Docs 🔍 Support 🏼 & administrator@example.com 🕶 |
|--|---|---|
| GENERAL | Policies / Organization Polic | Cancel Cancel |
| Dashboard Users Applications Policies Groups Bypass Codes Devices Phones Hardware Tokens U2F Tokens | Offline Authentication Specify offline authentication behaviour. Settings take effect next time the user logs in online into the LoginTC Windows Logon Connector. | Offline Authentication |
| Authentication Logs User Logs SETUP Domains | | 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. |
| Administrators Admin Logs Settings Billing | | Offline Days Limit No Limit ✓ Allow users to login up to a certain number of days when offline. ✓ Successful Offline Login Limit ✓ |
| CUSTOMER ID 1797-364192 | | 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:

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



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

| Use Assent Central X Do you want to allow this app to make changes to your device? Image: Windows Command Processor Verified publisher: Microsoft Windows Down or addals To contrave, enter a addminuter name and publicord. DDMARK/Administrator Image: Down DOLMAN Veri No | | |
|---|---|--|
| Der Anzeut Cantel X Do you want to allow this app to make changes to your device? Mindows Command Processor Windows Command Processor Windows Command Processor Verified publisher. Microardt Windows See more addata To containe date allohin wait raine and passenott. DOMARNA/ministrator Domaine DOMANN © Ves Ne | | |
| Use Accurr Control X Do you want to allow this app to make changes to your device? X Image: No your device? X | | |
| Use Assess Control × Do you want to allow this app to make changes to your device? Image: Style of the style of | | |
| Use Account Central × Do you want to allow this app to make changes to your device? Image Sto your device? Windows Command Processor Werified publisher: Microsoft Windows Show mode challs To continue, enter an adminuter name and passend. DOMANNA/Administrator Image Domain DOMANN Yes | | |
| War Account Control X Do you want to allow this app to make changes to your device? Image: Control of the | | |
| User Account Control X Do you want to allow this app to make changes to your device? Image: Control of the | | |
| User Account Cetted X Do you want to allow this app to make changes to your device? Image: Changes to your device? Image: Windows Command Processor Wender publisher: Microsoft Windows Show more device? Image: Changes to your device? Image: Changes to your device? Image: Changes to your device? Image: Changes to your device? Image: Changes to your device? Image: Changes to your device? Image: Changes to your device? Image: Changes to your device? Image: Changes to your device? Image: Changes to your device? Image: Changes to your device? Image: Changes to your device? Image: Changes to your device? Image: Changes to your device? Image: Changes to your device? Image: Changes to your device? Image: Changes to your device? Image: Changes to your device? Image: Changes to your device? Image: Changes to your device? Image: Changes to your device? Image: Changes to your device? Image: Changes to your device? Image: Changes to your device? Image: Changes to your device? Image: Changes to your device? Image: Changes to your device? Image: Changes to your device? Image: Changes to your device? Image: Changes to your device? </td <td></td> <td></td> | | |
| User Accessed Central X Do you want to allow this app to make changes to your device? Image: Changes to your device? Image: Windows Command Processor Verified publisher: Microsoft Windows Show more defails To continue, enter an admin user name and password. DDMAIN Administrator Image: Change in the second | | |
| User Account Control × Do you want to allow this app to make changes to your device? Image: Windows Command Processor Verified publisher: Microsoft Windows Show more default To continue, enter an admin user name and password. DOMAINIAdministrator • Domain: DOMAIN • Mg No | | |
| User Account Control X Do yoou want to allow this app to make changes to your device? Image: Windows Command Processor Verified publisher: Microsoft Windows Show more details To continue; enter an admin user name and password. DOMAIN Administrator Image: DOMAIN Yes No | | |
| User Account Control Do you want to allow this app to make changes to your device? Image: Windows Command Processor Verifed publisher: Microsoft Windows Show more deals To continue, enter an admin user name and pastword. DOMAIN/Administrator Tomain: DOMAIN Verified publisher: No | | |
| Do you want to allow this app to make changes to your device? Image: Windows Command Processor Verified publisher: Microsoft Windows Sow more details To continue, enter an admin user name and password. DOMAINVAdministrator Image: DOMAIN Yes Yes | User Account Control X | |
| Changes to your device? Image: Windows Command Processor Verified publisher: Microsoft Windows Show more details To continue, enter an admin user name and password. DOMAINAMAInisitrator Image: DOMAIN Yer No | Do you want to allow this app to make | |
| Windows Command Processor Verified publisher: Microsoft Windows Show more details To continue, enter an admin user name and password. DDMAINAdministrator Image: Domain: DOMAIN Yes Yes | changes to your device? | |
| Windows Command Processor Verified publisher: Microsoft Windows Show more details To continue, enter an admin user name and password. DOMAINVAdministrator Image: Control Domain: DOMAIN Yes No | _ | |
| Verified publisher: Microsoft Windows Show more datals To continue, enter an admin user name and password. DOMAINV/dministrator occurrent Ormain: DOMAIN Yes No | Windows Command Processor | |
| Show more details To continue, enter an admini user name and password. DOMAINVAdministrator Comain: DOMAIN Yes No | Verified publisher: Microsoft Windows | |
| To continue, enter an admin user name and password. DOMAINVAdministrator Image: Continue, enter an admin user name and password. Domain: DOMAIN Yes No | Show more details | |
| DOMAIN/Administrator Image: Comparison of the second se | To continue, enter an admin user name and password. | |
| Comain: DOMAIN Ves No | DOMAIN\Administrator | |
| Domain: DOMAIN Yes No | •••••• | |
| Ves No | Domain: DOMAIN | |
| Yer No | | |
| | Yes No | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

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

| P Legint × | |
|---|--|
| Approve access with second factor authentication. Authentication Method LoginTC App (Android) | |
| Language English 🗸 | |
| | |

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.



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" CONFBYPASSUSERS=".\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 Applicatoin 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) | Θ |
| 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 <u>Challenge Groups</u> section for more information. | RemoteMFAUsers |
| CONFBYPASSGROUPS | (Optional) Groups whose members will be bypassed. Refer to <u>Bypass Groups</u> section for more information. | RemoteMFAUsers |
| CONFCHALLENGEUSERS | (Optional) Users which will be challenged. Refer to <u>Challenge</u> <u>Users</u> section for more information. | *\support |
| CONFBYPASSUSERS | (Optional) Users which will be bypassed. Refer to <u>Bypass</u> <u>Users</u> 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** \rightarrow LoginTC. LoginTC Windows Logon and RDP Connector event logs are helpful in debugging issues.

| 🛃 Event Viewer | | | | _ | | × |
|--------------------------------|--|--------------------------------|----------------|---------------------|------|---|
| File Action View Help | | | | | | |
| 🗢 🔿 📶 🖬 🖬 | | | | | | |
| Event Viewer (Local) | LoginTC Number o | f events: 86 | | | | |
| > 📑 Custom Views | Level | Date and Time | Source | | | ~ |
| > 🙀 Windows Logs | | | JUICE | | | |
| Applications and Services Logs | Information | 7/9/2019 9:47:36 AM | Login IC W | Indows Logon Conne | ctor | |
| Hardware Events | 1 Information | //9/2019 9:4/:12 AM | Login IC W | Indows Logon Conne | ctor | |
| 📔 Internet Explorer | 1 Information | 7/9/2019 9:34:01 AM | LoginTC W | indows Logon Conne | ctor | |
| Key Management Service | (i) Information | 7/9/2019 9:33:51 AM | LoginTC W | indows Logon Conne | ctor | |
| E LoginTC | (i) Information | 7/9/2019 9:32:54 AM | LoginTC W | indows Logon Conne | ctor | |
| > Microsoft | (i) Information | 7/9/2019 9:28:25 AM | LoginTC W | indows Loaon Conne | ctor | |
| > OpenSSH | | | | | | |
| Windows PowerShell | Event 0, LoginTC Wir | ndows Logon Connector | | | | × |
| Subscriptions | | | | | | |
| | General Details | | | | | |
| | | | | | | ^ |
| | User win10\local | admin was authenticated online | 2 | | | |
| | | | | | | |
| | | | | | | |
| | Log Name: | LoginTC | | | | |
| | Source: | LoginTC Windows Logon Cc | Logged: | 7/9/2019 9:47:36 AN | 1 | |
| | Event ID: | 0 | Task Category: | None | | |
| | Level | Information | Kenwords: | Classic | | |
| | Level. | NICA | Keywords. | Classic 1 40 | | ~ |
| | < Contraction of the second se | NI/ A | Computer | winto | | > |
| | | | | | | |
| | | | | | | |

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 rollying 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 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

| 🎬 Registry Editor | | | | - 🗆 X |
|---|-------|--|--|--|
| File Edit View Favorites Help | | | | |
| Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Cyphercor\Log | ginTO | Windows Logon Connector | | |
| v 💻 Computer | ^ | Name | Type | Data |
| HKEY_CLASSES_ROOT HKEY_CURRENT_USER HKEY_LOCAL_MACHINE BCD00000000 HARDWARE SAM SECURITY | | (Default) (b) (ApiHost (b) (ApplicationApiKey (b) (ApplicationId (b) (BypassGroups (b) (BypassUsers (b) (ChallengeGroups | REG_SZ REG_SZ REG_SZ REG_SZ REG_SZ REG_SZ REG_SZ | (value not set) cloud.logintc.com J0AePqWmNztjjerU21 8bbb2b969a11403a1c |
| SOFTWARE Classes Clients Cyphercor LoginTC Windows Logon Connector DefaultUserEnvironment Google | | ab ChallengeUsers ab CredentialProviderWhitelist ab Link1Label ab Link1URL ab Link2Label ab Link2URL | REG_SZ REG_SZ REG_SZ REG_SZ REG_SZ REG_SZ | |
| Intel Macromedia Microsoft OBBC OEM Partner Policies RegisteredApplications WOW6432Node | | 副 Machineld 麗 RdpOnly | REG_SZ REG_DWORD | A9B0BF 0x00000001 (1) |
| WOW6432Node | ~ | < | | |

3. Click to modify the ChallengeGroups field

| Edit String | | × |
|-----------------------|----|--------|
| Value name: | | |
| ChallengeGroups | | |
| Value data: | | |
| DOMAIN\RemoteMFAUsers | | |
| | ОК | Cancel |

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 |

5. 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:

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

| 👫 Registry Editor | | | | _ | | × |
|---|-------|-----------------------------|-----------|--------|-----------|----------|
| File Edit View Favorites Help | | | | | | |
| Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Cyphercor\Lo | ginT(| Windows Logon Connector | | | | |
| 🗸 💻 Computer | ^ | Name | Туре | Data | | |
| HKEY_CLASSES_ROOT | | (Default) | REG_SZ | (value | not set) | |
| | | ab ApiHost | REG_SZ | cloud | logintc. | com |
| | | ApplicationApiKey | REG_SZ | J0AeP | qWmNz | tjjerU21 |
| HARDWARE | | ab ApplicationId | REG_SZ | 8bbb2 | 2b969a11 | 403a1c3 |
| SAM | | ab BypassGroups | REG_SZ | | | |
| SECURITY | | ab BypassUsers | REG_SZ | | | |
| V SOFTWARE | | ab ChallengeGroups | REG_SZ | | | |
| > Classes | | (ab) ChallengeUsers | REG_SZ | | | |
| > Clients | | CredentialProviderWhitelist | REG_SZ | | | |
| ✓ Cyphercor | | LinklLabel | REG_SZ | | | |
| LoginTC Windows Logon Connector | | | REG_SZ | | | |
| DefaultUserEnvironment | | Link2Label | REG_SZ | | | |
| Soogle | | Link2URL | REG_SZ | | | |
| > Intel | | (ab) Machineld | REG_SZ | A9B0E | BF | |
| > Macromedia | | 👯 RdpOnly | REG_DWORD | 0x000 | 00001 (1) | |
| > Microsoft | | | | | | |
| S ODBC | | | | | | |
| > Detroit | | | | | | |
| > Paltner | | | | | | |
| Registered Applications | | | | | | |
| WOW6432Node | | | | | | |
| CVCTEM | ¥ | < | | | | > |

3. Click to modify the BypassGroups field

| Edit String | × |
|-----------------------|-----------|
| Value name: | |
| BypassGroups | |
| Value data: | |
| DOMAIN\RemoteMFAUsers | |
| | OK Cancel |

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 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

| 📲 Registry Editor | | | | - 🗆 X | |
|--|-------|--------------------------------|-----------|-------------------|----|
| File Edit View Favorites Help | | | | | |
| Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Cyphercor\Log | ginT(| C Windows Logon Connector | | | ٦ |
| v 💻 Computer | ~ | Name | Type | Data | 1 |
| HKEY_CLASSES_ROOT | | ab (Default) | REG SZ | (value not set) | |
| > HKEY_CURRENT_USER | | ab ApiHost | REG SZ | cloud.logintc.com | |
| | | ab Application ApiKey | REG SZ | I0AePaWmNztijerU2 | 1. |
| > BCD0000000 | | ab ApplicationId | REG SZ | 8bbb2b969a11403a1 | 2 |
| > HARDWARE | | ab BypassGroups | REG SZ | 00002030341110341 | - |
| SAM | | ab BypassUsers | REG SZ | | |
| | | ab ChallengeGroups | REG SZ | | |
| | | ab ChallengeUsers | REG SZ | | |
| Classes | | ab CredentialProviderWhitelist | REG SZ | | |
| | | b Link1Label | REG SZ | | |
| LoginTC Windows Logon Connector | | b Link1URL | REG SZ | | |
| DefaultUserEnvironment | | b Link2Label | REG_SZ | | |
| > Google | | b Link2URL | REG_SZ | | |
| > Intel | | ab Machineld | REG_SZ | A9B0BF | |
| > Macromedia | | RdpOnly | REG_DWORD | 0x00000001 (1) | |
| > 📙 Microsoft | | | | | |
| > ODBC | | | | | |
| > OEM | | | | | |
| > Partner | | | | | |
| > Policies | | | | | |
| RegisteredApplications | | | | | |
| > WOW6432Node | ~ | < | | 3 | 2 |

3. Click to modify the ChallengeUsers field

| Edit String | × |
|----------------|-----------|
| Value name: | |
| ChallengeUsers | |
| Value data: | |
| .\john.doe | |
| | OK Cancel |

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

| 📲 Registry Editor | | | | – 🗆 X | | | | | | | |
|--|-------------------------------|----------------------------------|-----------|---------------------|--|--|--|--|--|--|--|
| File Edit View Favorites Help | File Edit View Favorites Help | | | | | | | | | | |
| Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Cyphercor\LoginTC Windows Logon Connector | | | | | | | | | | | |
| 🗸 💻 Computer | ^ | Name | Type | Data | | | | | | | |
| HKEY_CLASSES_ROOT HKEY_CURRENT_USER | | (Default) | REG SZ | (value not set) | | | | | | | |
| | | ab ApiHost | REG SZ | cloud.logintc.com | | | | | | | |
| | | ab ApplicationApiKey | REG SZ | J0AePaWmNztijerU21 | | | | | | | |
| > BCD0000000 | | ab ApplicationId | REG SZ | 8bbb2b969a11403a1c3 | | | | | | | |
| Same Same | | ab BypassGroups | REG SZ | | | | | | | | |
| | | ab BypassUsers | REG_SZ | | | | | | | | |
| | | ab ChallengeGroups | REG_SZ | | | | | | | | |
| | | ab ChallengeUsers | REG_SZ | | | | | | | | |
| Clients | | ab Credential Provider Whitelist | REG_SZ | | | | | | | | |
| Cyphercor | | ab Link1Label | REG_SZ | | | | | | | | |
| LoginTC Windows Logon Connector | | 赴 Link1URL | REG_SZ | | | | | | | | |
| DefaultUserEnvironment | | ab Link2Label | REG_SZ | | | | | | | | |
| > Google | | b Link2URL | REG_SZ | | | | | | | | |
| > 🔒 Intel | | ab Machineld | REG_SZ | A9B0BF | | | | | | | |
| > 📙 Macromedia | | 👪 RdpOnly | REG_DWORD | 0x00000001 (1) | | | | | | | |
| > Microsoft | | | | | | | | | | | |
| > ODBC | | | | | | | | | | | |
| > OEM | | | | | | | | | | | |
| > Partner | | | | | | | | | | | |
| > Policies | | | | | | | | | | | |
| RegisteredApplications | | | | | | | | | | | |
| > WOW0432INOde | \mathbf{v} | < | | > | | | | | | | |

3. Click to modify the BypassUsers field

| Edit String | | × |
|-------------|----|--------|
| Value name: | | |
| BypassUsers | | |
| Value data: | | |
| .\john.doe | | |
| | ОК | Cancel |

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

| Registry Editor | | | | | - | | × | |
|--|---|--|--|--|---|--|---|--|
| File Edit View Favorites Help | | | | | | | | |
| Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers | | | | | | | | |
| Computer/HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\W Computer/HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\W CurrentVersion CurrentVersio | ^ | dows\CurrentVersion\Au Name (Default) (Default) (CredProvHelper (ProhibitFallbacks) | thentication\Creder Type REG_SZ REG_SZ REG_SZ REG_DWORD | ntial Providers Data (value not set) {FCA7405F-710E-4438-ADEE-FB358BF9BACD} {7C50E1E9-DB15-4410-89C5-D27F4B727368} 0x00000001 (1) 0x00000001 (1) | | | | |
| Capture Capture Casting Census ClickNote | ~ | | | | | | | |

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: <u>Automatic LoginTC Windows Logon and RDP Connector</u> <u>Deployment</u>.

Upgrade

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

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 the be the same version that's installed.

Troubleshooting

Email Support

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