TIQR CREDENTIAL PROVIDER FOR WINDOWS

TiQR Credential Provider for Windows

Windows

1. Product Documentation

This document is an installation guide for the TiQR Credential Provider for Windows. Hence, the installation or configuration of WebADM, including token registration is not covered in this guide. For installation and usage guides to WebADM refer to the RCDevs WebADM Installation Guide and the RCDevs WebADM Administrator Guide available through the RCDevs' online documentation library.

2. Product Overview

The TiQR Credential Provider for Windows is a component that integrates the RCDevs TiQR QR-Code authentication into the Windows login process. RCDevs TiQR Authentication Server is a WebApp that is tightly coupled to the RCDevs WebADM application server. The Credential Provider enables you to use secure one-click QR-Code enrollment and secure authentication without having to re-type complicated codes. TiQR supports the OCRA suite of authentication protocols and is based on the AES 256-bit encryption and the SHA-family functions. The TiQR authentication application is provided for mobile platforms including Android and iOS.

3. System Requirements

The TiQR Credential Provider runs on any x86/x64 Windows platforms starting with Windows Vista. Your environment should fulfill the following requirements:

- x86/x64 Windows Vista or later.
- Workstation joined to an AD domain.
- Network access.
- An instance of WebADM and TiQR running in your network.
- Permanent connection to TiQR server's network API.
- NetBIOS over TCP/IP enabled and resolvable.
- DNS suffix set to match your AD domain.

4. Preliminary Information

Administrative/elevated permissions are necessary on any workstation to correctly setup and/or change the TiQR Credential Provider's configuration. To correctly set up the provider, please gather the following information. You will need to enter during the installation process:

- The URI(s)s of the TiQR web-service(s) (mandatory)
  - These URIs are mandatory, due to the client needs to know where the TiQR SOAP network API can be reached. They are entered as a comma-separated list. At least one URI is necessary.

- A custom login text or tile caption (optional)
  - A text that is displayed on the Windows login pane.
- A client ID (optional)
  - An ID to identify a particular client on the server-side.
- A certificate authority (CA) file (optional)
- A certificate file (optional)
- The certificate's password (optional)
- A custom settings string (optional)
- SOAP timeout delay (optional)

5. Installation and Configuration

The Credential Provider's setup and configuration are done in about 5 Minutes. The installer is the only utility that is needed to set up and to configure the provider. The provider can be automatically deployed to your clients. This is covered later.

5.1 Local Installation

First, you need to download the latest version of the TiQR Credential Provider for Windows. You can download it at RCDevs' website. After you've downloaded the installer package and copied it to your client workstation just start the setup.

Click `Next` and accept the License Agreement.

Now, you can select to install the Credential Provider as default. You may also change the default installation directory as you wish. Click `Next` when you are done.

> ⚠ Note
>
> Installing the provider as default disables all other credential providers on the target system. Only Credential Providers provided by RCDevs will be available for login. If any problem occurs you can still log in with other providers using the Windows failsafe boot. It is possible to force OTP login in failsafe mode. This is covered later. **While testing: Do not install as default provider!**

Now enter at least one TiQR web-service URI. To get help on the other fields, just click the `?` -Help buttons following each field. Click `Next` when you are done.

You can now set up any public-key infrastructure data you may have. This is completely optional. Click `Next` when you are done.

Here you may set up a custom settings string for your WebADM and TiQR configuration. Further, you may change the default SOAP service timeout. Click `Next` when you are done.

The Credential Provider is now ready to be installed. Click `Install`.

After the setup process is finished click “Finish” to close the installer. You are now ready to use the TiQR Credential Provider to logon to your workstation.

5.2 Modifying the Configuration

If you are under testing:

To configure the TiQR Credential Provider navigate to the Windows Control Panel and select `Programs and Features`. Search for `TiQR Credential Provider for Windows` and click `Change`. Now the installer shows up. Select `Change` and modify the provider’s configuration as you need.

If TiQR Credential Provider is running in Production:

To configure the TiQTR Credential Provider, you must get the MSI installer file, for the example on your Desktop. Run command line as administrator:

1. Click Start, click All Programs, and then click Accessories.
2. Right-click Command prompt, and then click Run as administrator.
3. If the User Account Control dialog box appears, confirm that the action it displays is what you want, and then click Continue.

Run the installer, and click `Change` to update settings.

5.3 Automatic Deployment / Quiet Installation

The MSI installer package is prepared to take all configuration parameters that can be set during local installation for auto-deployment in quiet mode. Hence, you can deploy the setup to any clients and automatically install the Credential Provider without user interaction.

The parameters are as follows:

Parameter	Value
SERVER_URL	A list of comma-separated URIs pointing to your TiQR web-service. At least one is mandatory.
LOGIN_TEXT	A text that is displayed on the Windows logon pane. Optional. Default “TiQR Login”
CLIENT_ID	An ID identifying the client on the server-side. Optional.
CA_FILE	The file-system path to a Certificate Authority (CA) file. Optional.
CERT_FILE	The file-system path to a user certificate. Optional.
CERT_PASSWORD	The user certificate’s password. Optional.
USER_SETTINGS	A comma-separated list of TiQR settings. Optional.
SOAP_TIMEOUT	The SOAP timeout in seconds when connecting to the TiQR Authentication Server. Optional. Default is 15 seconds.

The deployment process can be done, i.e. using a Batch-file. Here is an example of how to do this:

Deploy.bat contains:

```
msiexec /qb /i TiQRCredentialProviderSetup.msi SERVER_URL=http://server:8080/tiqr/
SOAP_TIMEOUT=10 ADDLOCAL=[MainInstall | InstallAsDefault | VCRedist]
```

The ADDLOCAL switch tells the installer which components should be included. To set up the Credential Provider as default provider the list needs to include “InstallAsDefault” as seen in the example above.

5.4 Windows Failsafe Mode

By default, Windows does not load custom credential providers in safe mode. The reason is covered in FAQ (Appendix A of the RTM Cred Provider Sample Overview):

> Q: My implementation of CredentialProviderFilter is not loaded in SAFE mode. Is this a bug? Is there a way to run my Filter in SAFE mode?

> A: This is not a bug. SAFE mode is intended to serve as a workaround in order to correct repair Operating Systems malfunctioning due to incorrectly configured components such as device drivers. By default, only the in-box Password Provider is loaded in SAFE mode. The in-box Smart Card Provider is also available if the machine is booted into SAFE mode with networking. This provides a fallback in case of a bad error. To over-ride the fallback logic and force logonUI to load Credential Provider filters in SAFE Mode, create and set the following registry key:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers] “ProhibitFallbacks”=dword:1
```

In order to force the use of the Credential Provider even in Windows failsafe mode, some registry changes need to be made.

⚠ Note

In case of failure during provider configuration or unreachable network, even failsafe mode will not help you to login to a workstation that is set-up to force the use of the Credential Provider.

› To register the Credential Provider enforcement, copy the following text to a new text file, name it register.reg and execute it.

Windows Registry Editor Version 5.00

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers]
"ProhibitFallbacks"=dword:1
```

› To disable and unregister the failsafe enforcement copy the following text.

Windows Registry Editor Version 5.00

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers]
"ProhibitFallbacks"=-
```

> ⚠ Warning
>
> Be sure what you are doing. If TiQR Credential Provider or any other custom CP misbehaves and you are not able to log in, you will experience that even safe mode can not help you!

6. Troubleshooting

While debugging your installation and TiQR environment have a look at the Windows Event Viewer. To pinpoint a specific client-side problem the Event Viewer may help you.

To see what is happening while the client and server communicate, have a look at WebADM's SOAP log file (soap.log). This log is located at `/opt/webadm/logs/`. To debug server-side problems, this should be the first place to look at.