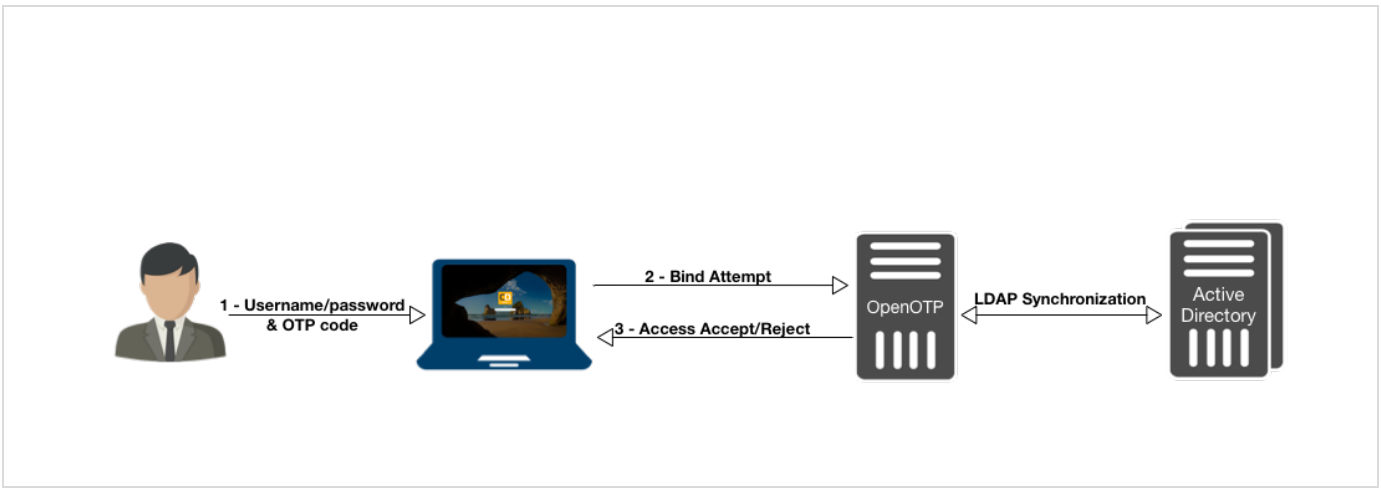
WINDOWS CREDENTIAL PROVIDER

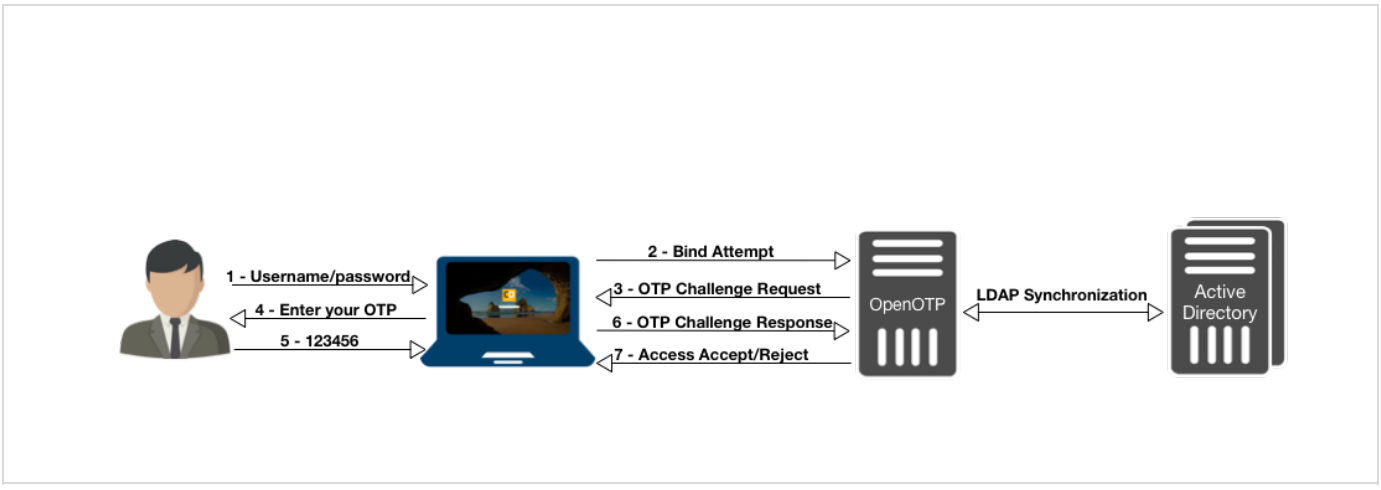
Windows Credential Provider

Active Directory Windows Remote Desktop Services

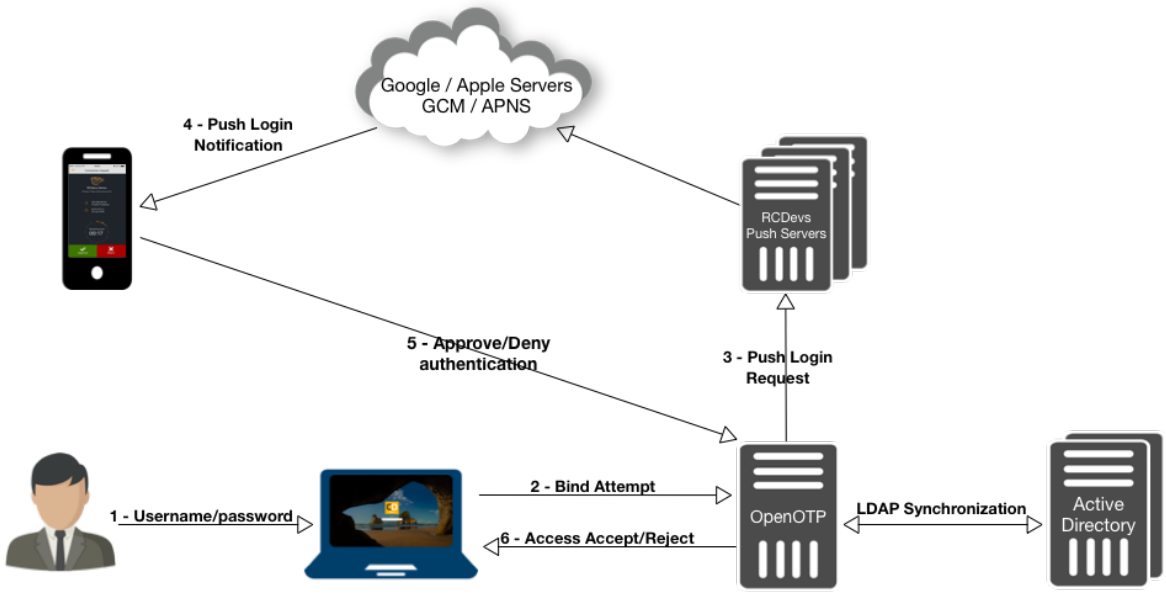
Normal Login flow



Simple Login flow



Push Login flow



1. Product Documentation

This document is an installation guide for the OpenOTP 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 Website.

2. Product Overview

The OpenOTP Credential Provider for Windows is a component that integrates the RCDevs OpenOTP one-time password authentication into the Windows login process. RCDevs OpenOTP Authentication Server is a WebApp that is tightly coupled to the RCDevs WebADM application server.

For this recipe, you will need to have WebADM/OpenOTP installed and configured. Please, refer to WebADM Installation Guide and WebADM Manual to do it.

3. System Requirements

The OpenOTP Credential Provider runs on any x86/x64 Windows platforms starting with Windows Vista and Windows Server from 2008 versions.

Your environment should fulfill the following requirements:

- x86/x64 Windows 2008 Server/Vista or later.
- Workstation joined to AD domain or not.
- Network access.

- An instance of WebADM and OpenOTP running in your network.
- Permanent connection to OpenOTP 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 set up and/or change the OpenOTP Credential Provider's configuration.

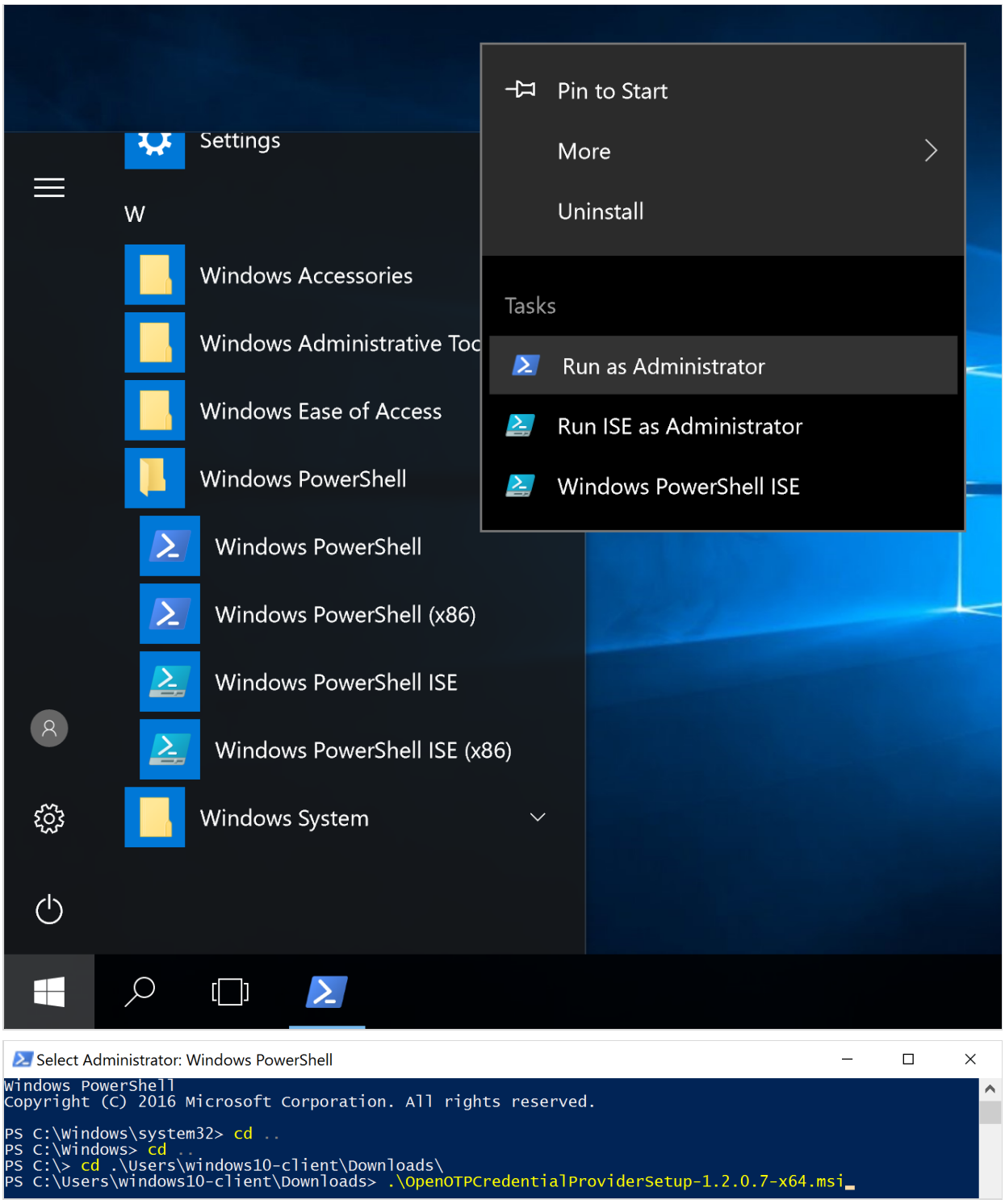
To correctly setup the provider, please gather the following information. You will need to enter during the installation process:

- The URI(s)s of the OpenOTP web-service(s) (mandatory)
  - These URIs are mandatory, due to the client needs to know where the OpenOTP SOAP network API can be reached. They are entered as a comma-separated list. At least one URI is necessary.
- Your local domain (optional)
  - Needed to force a domain, which is not set as default on the OpenOTP side.
- 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)
  - Should be set to "LoginMode=LDAPOTP", if you did not set LDAP+OTP as default login-mode in WebADM.
- SOAP timeout delay (optional) The login-mode LDAP+OTP must be set at server-side in WebADM, as the Windows Domain Controller (DC) needs the full credential (including LDAP password) to issue a Kerberos ticket.

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.

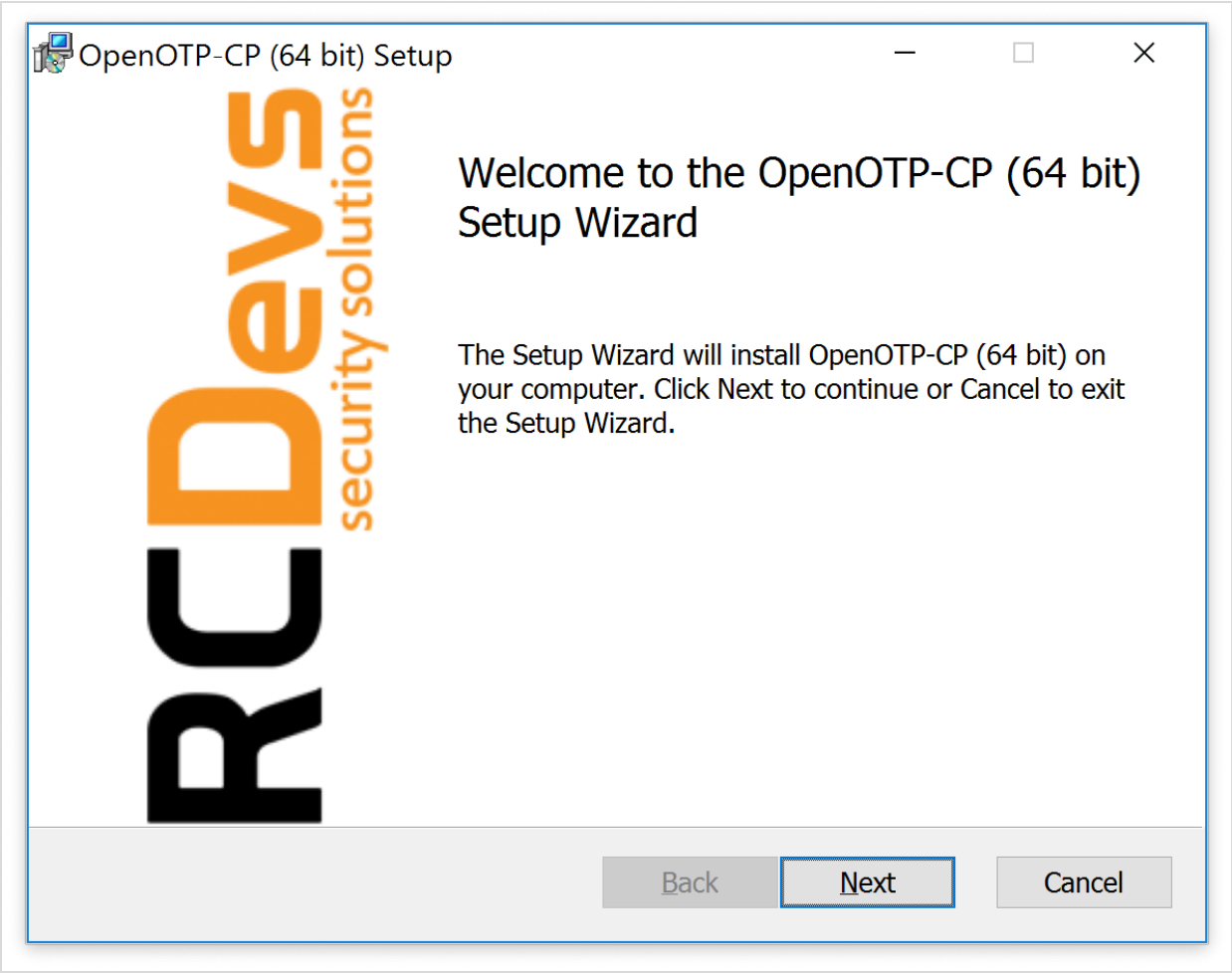
> ⚠ Note
>
> Administrative/elevated permissions are necessary on any workstation to correctly set up and/or change the OpenOTP Credential Provider's configuration. Please, run the Windows PowerShell as Administrator. Right click on the Windows PowerShell then select Run as Administrator.



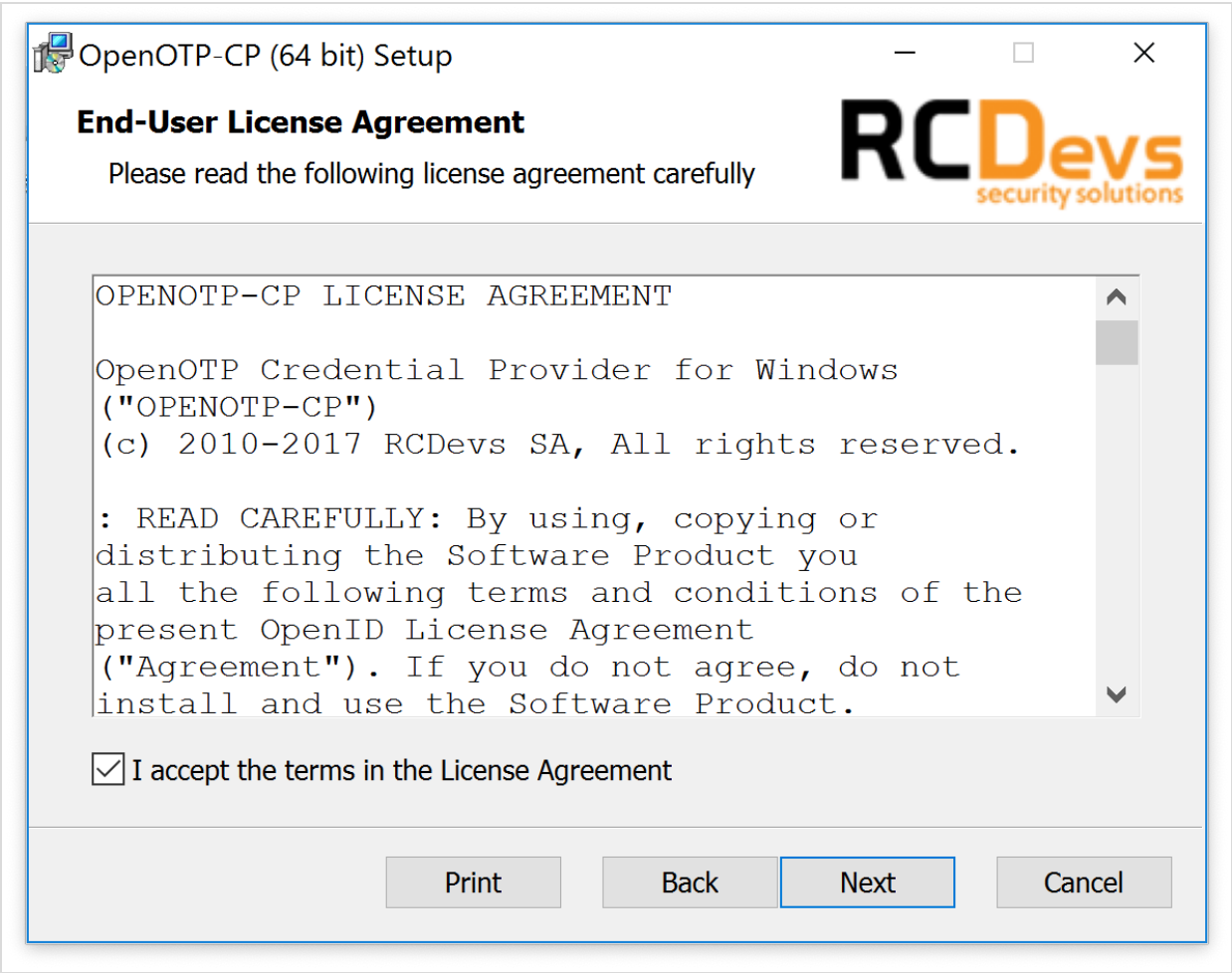
5.1 Local Installation

First, you have to download OpenOTP Credential Provider x86 or x64.

Extract files from the archive on your Windows machine(s), run the MSI file and click on `Next`.



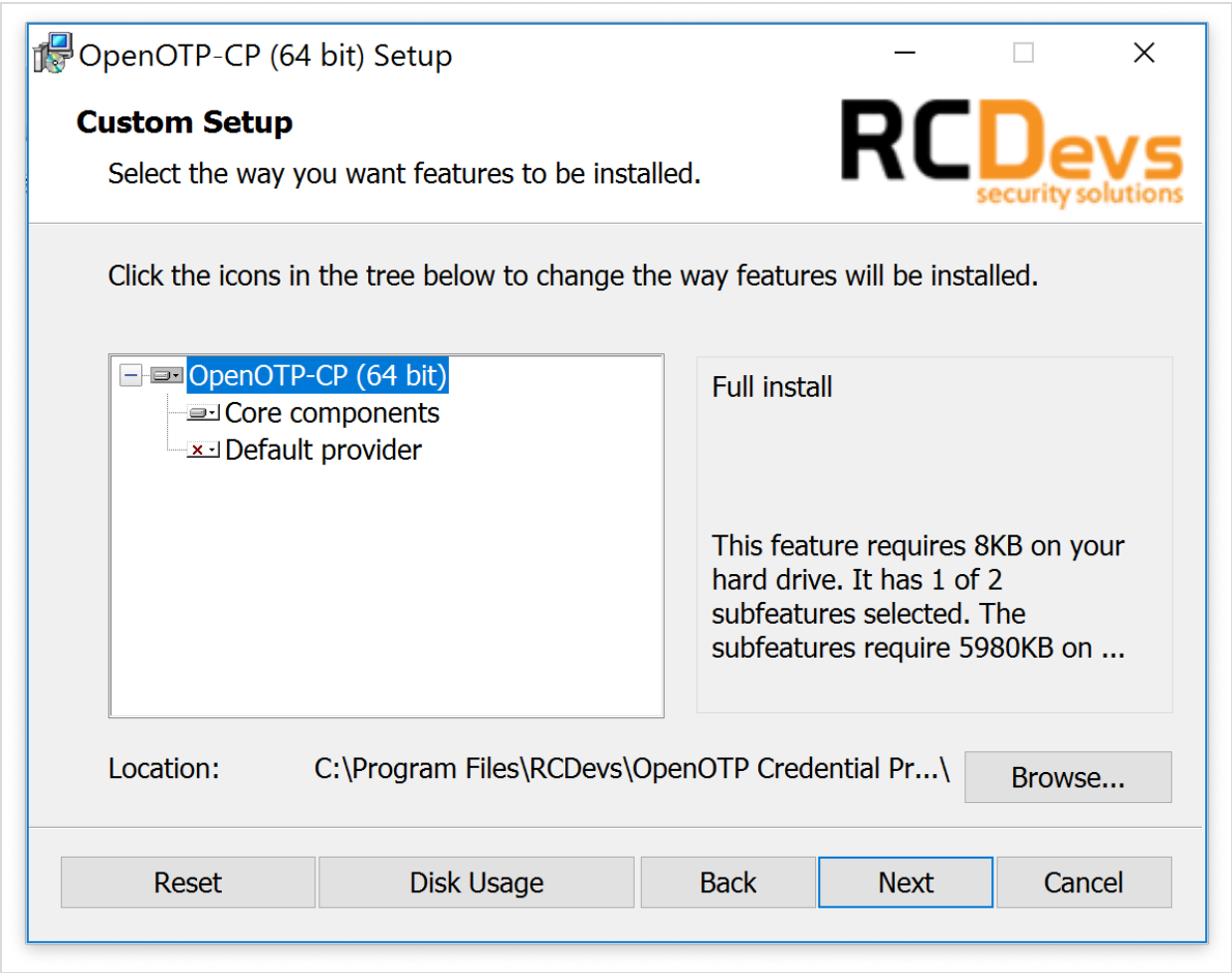
Accept the End-User License Agreement and click on `Next`.



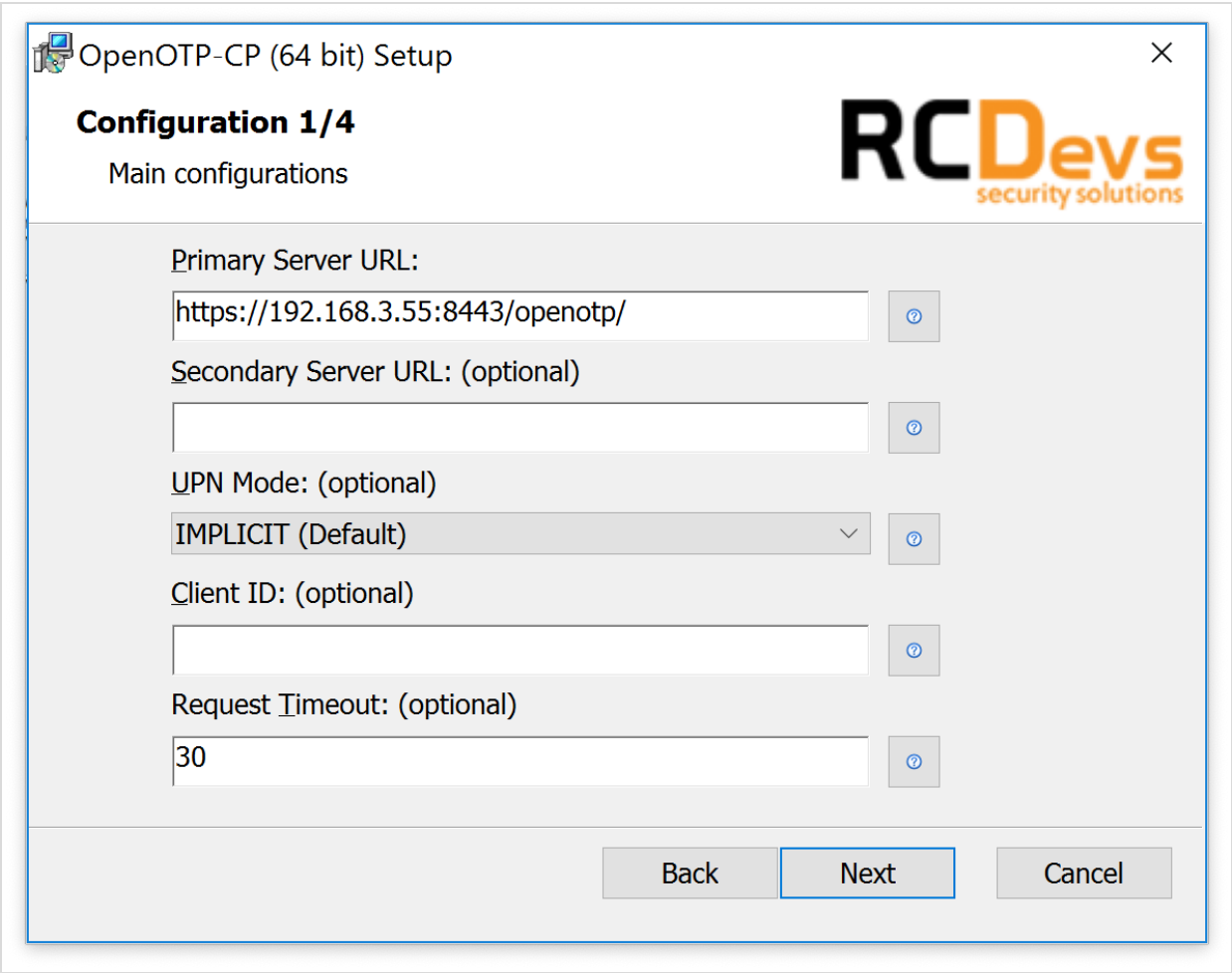
Now, you can select to install the Credential Provider as default. You may also change the default installation directory as you wish.

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. To log in on a Windows Server through RDP client with a One-Time Password, OpenOTP Credential Provider should be installed **by default** on the remote host to perform an OTP login. While testing: Do not install as default provider! Before choosing OpenOTP Credential Provider as default provider, perform a login test!



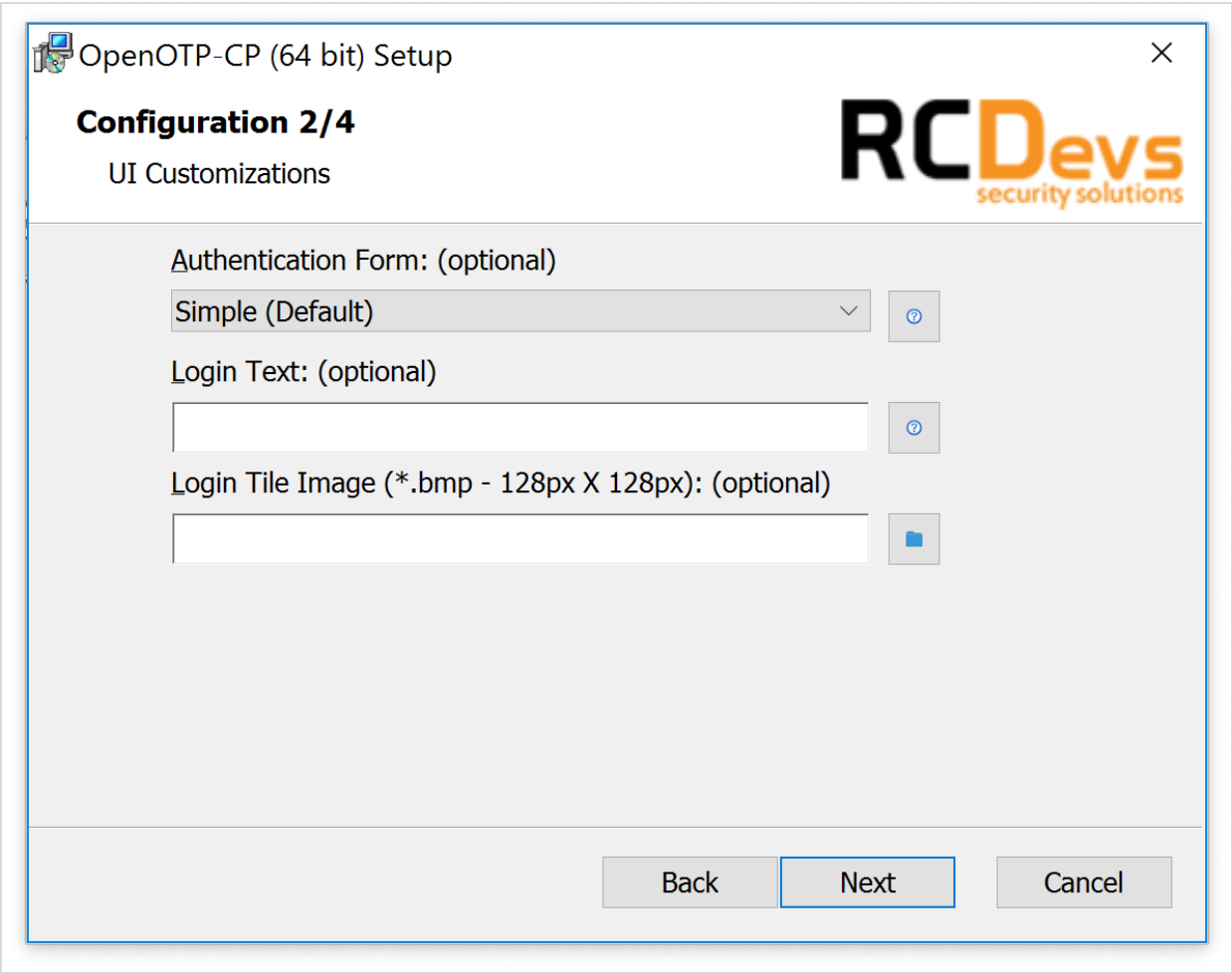
On this page, you have to configure at least one OpenOTP SOAP URL(s). Your WebADM SOAP endpoint should be: `https://your-webadm-ip-address-or-dns-name:8443/openotp/`. You can also define a Client ID referring to a client policy in WebADM. Click on `Next`.



On the next screen, you can define the authentication form. You have 2 choices:

- Simple: On the Windows login page, you will have 2 fields in the first step (Username and Password LDAP), after pressing `login`, you will have a second screen with the OTP field.
- Normal: With this option, you will have 3 fields on the login page, one for the Username, one for the LDAP password and the last one for the OTP.

You can also configure a message, image for the Windows login screen.



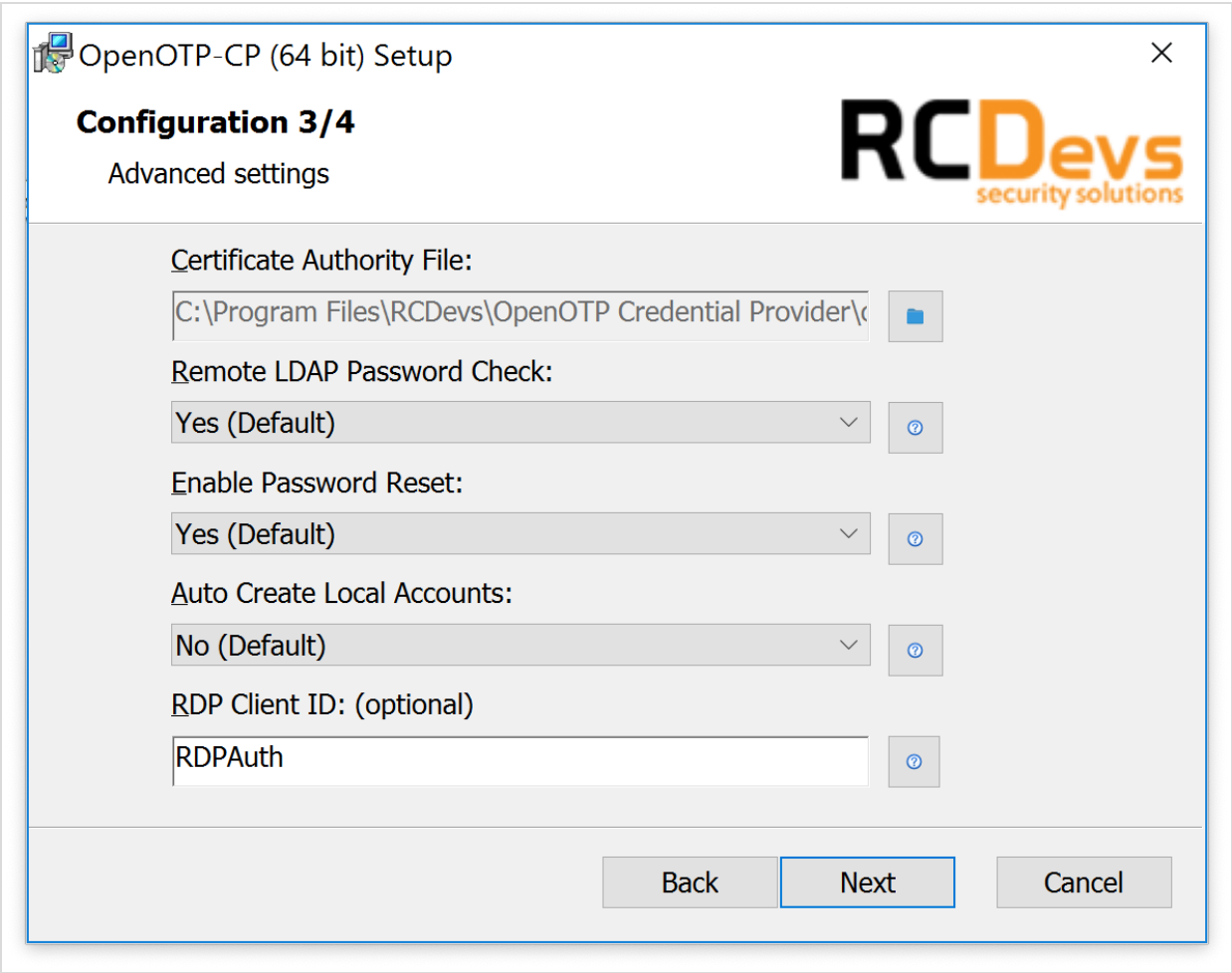
The next page allows you different things:

- You can configure a CA file, mandatory for HTTPS.
- The remote LDAP password check setting can be disabled if you don't want that WebADM check the LDAP password.
- Enable password reset setting if you want to have the possibility to reset the LDAP password when the user password is expired.
- Auto Create Local Account setting can be enabled when the host is not connected to a Windows domain and you want the Credential Provider to create user accounts at first login.
- RDP client ID can be used if you want to match a different client policy for RDP sessions.

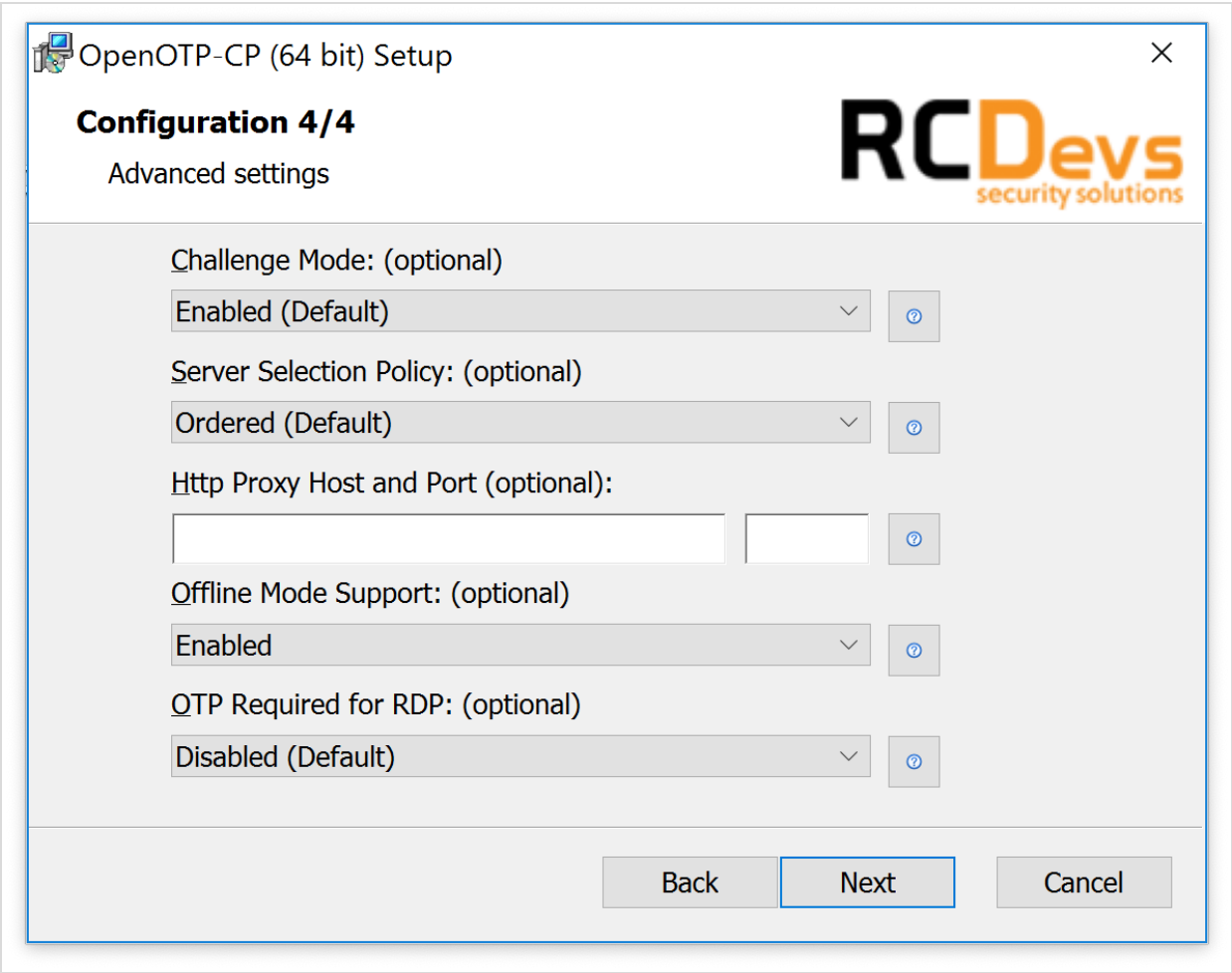
Keep all settings by default if your Windows clients are in a domain.

Note

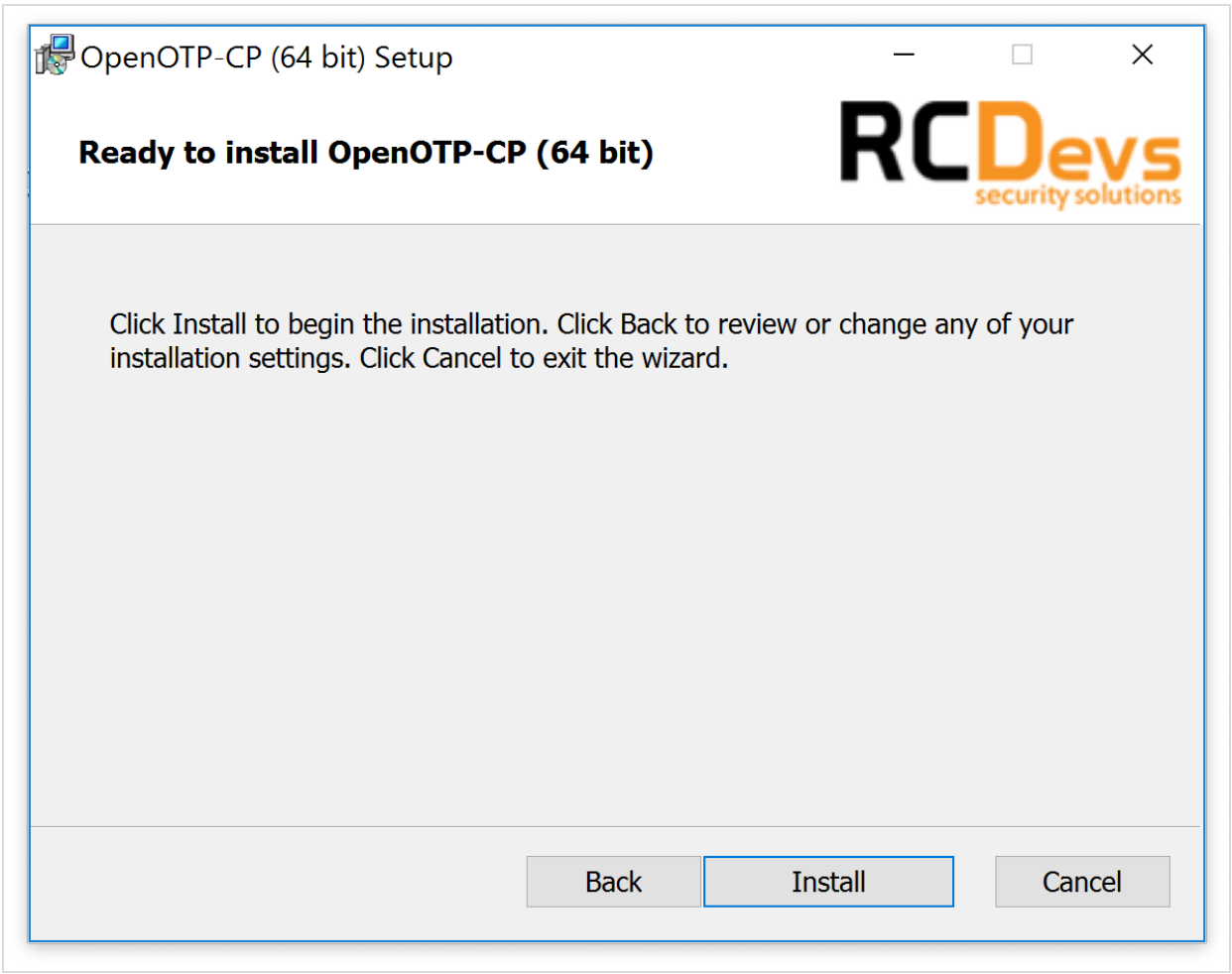
OpenOTP Credential Provider will automatically download the CA certificate on the default WebADM server port when you set the OpenOTP service URL. You can also obtain it manually with `https://mywebadmserver/cacert`.

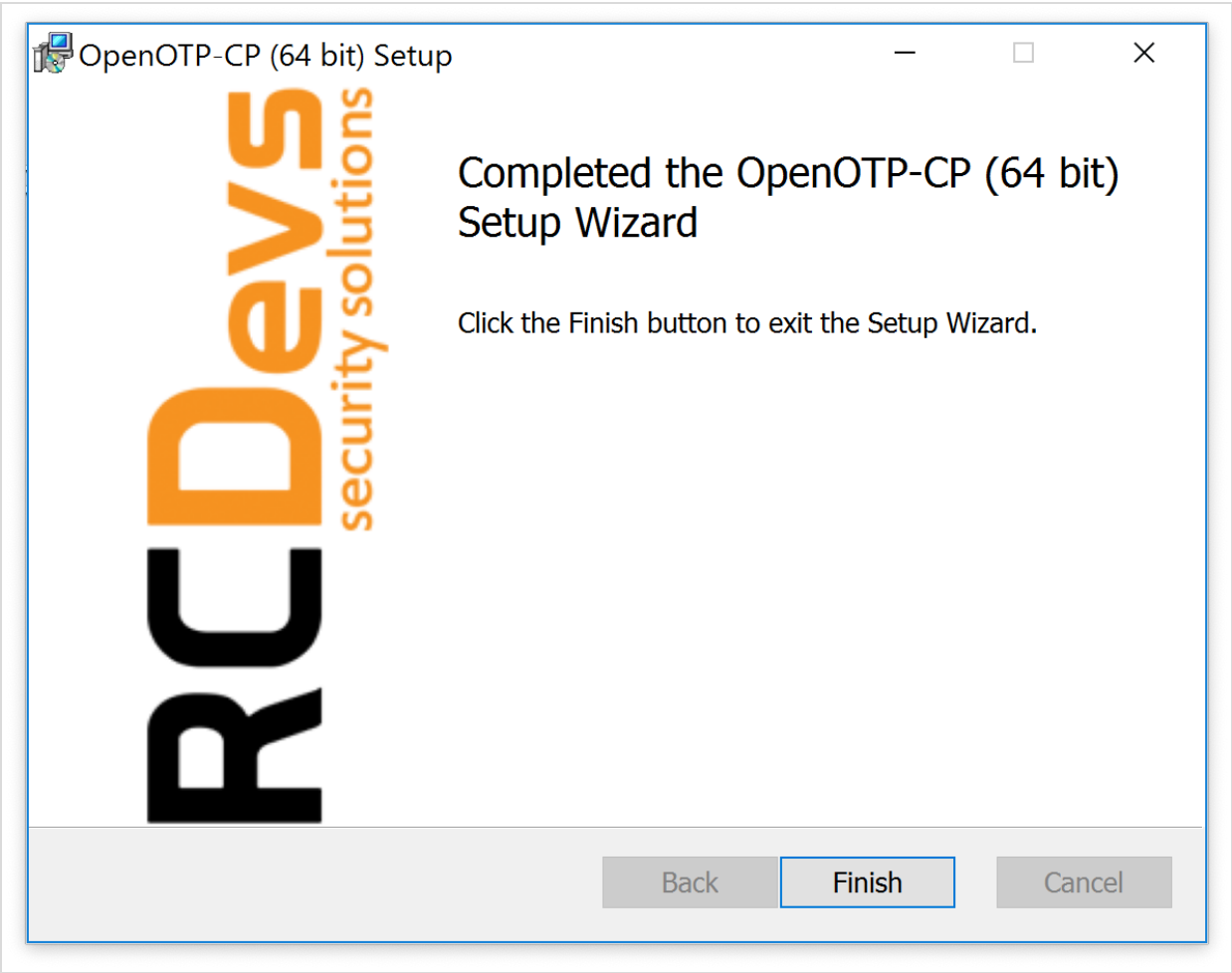


The last configuration page allows you to configure an HTTP proxy, the failover settings, enforce custom settings for OpenOTP (deprecated feature, the best practice is to create a client policy), enables offline mode for laptops when there are unable to contact the WebADM/OpenOTP server! The last setting allows you to disable OTP for RDP sessions. That means when this setting is disabled, you are able to select the default Windows credential provider during an RDP authentication. Note that this setting is only available when you install OpenOTP Credential Provider as a default provider.



Configuration is done, you can click on `Install` and `Finish` after the installation.


OpenOTP-CP (64 bit) Setup
Ready to install OpenOTP-CP (64 bit)
RCDevs
security solutions
Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.
Back
Install
Cancel



5.2 Modifying the Configuration

If you are under Testing:

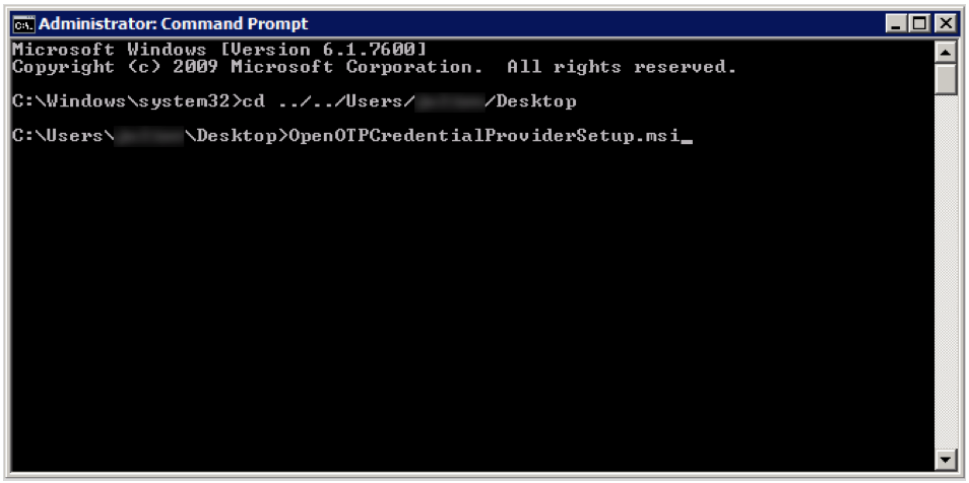
To configure the OpenOTP Credential Provider, navigate to the “Windows Control Panel” and select “Programs and Features”. Search for “OpenOTP Credential Provider for Windows” and click “Change”. Now the installer shows up. Select “Change” and modify the provider’s configuration as you need.

If OpenOTP Credential Provider is running in Production:

To configure the OpenOTP 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.

Example of quiet installation with PowerShell:

```
msiexec /qb /i OpenOTP_CredentialProvider.msi
SERVER_URL=https://webadm.test.local:8443/openotp/ CA_FILE=c:\ca.crt OFFLINE_MODE=1
CLIENT_ID=windows
```

The parameters are as follows:

Parameter	Value
SERVER_URL	URI pointing to one OpenOTP web-service. Example: *https://webadm.test.local:8443/openotp/* Mandatory.
SERVER_URL_2	URI pointing to the second node of your OpenOTP cluster. Optional.
UPN_MODE	According to this option OpenOTP will use the selected attribute for authentication. › Default: Explicit UPN: Value of user's object's userPrincipalName attribute. › *2*: Implicit UPN: Value of user's object's samAccountName attribute.
LOGIN_TEXT	A text that is displayed on the Windows login page. Default (Empty) "OpenOTP Login"
CLIENT_ID	Client ID which is sent to OpenOTP in the login requests.

	This client ID will appear in the WebADM audit database. Optional.
CA_FILE	The file-system path to a Certificate Authority (CA) file. Mandatory. Example: *c:|ca.crt*
CERT_FILE	The file-system path to a user certificate. Optional.
CERT_PASSWORD	The user certificate's password. Optional.
USER_SETTINGS	You can Pass some OpenOTP configurations from the client requests by setting a comma-separated list of settings here. These settings will override any server or user settings. Example: OpenOTP.LoginMode=LDAPOTP, OpenOTP.OTPType=TOKEN Optional.
SOAP_TIMEOUT	Request timeout when connecting to OpenOTP Authentication Server URL. The default is 30 seconds (If empty it will be the 30s). Optional.
LOGIN_METHOD	There are two login methods available: › Default: Simple: Only username and password inputs are displayed during login, and if needed a Challenge appears on a next step. › *1*: Normal: Username, password and OTP inputs are displayed during login. Simple mode uses the OpenOTP SimpleLogin method where the semantic of the password input is handled by the OpenOTP server and based on the user login policy. Optional.
V1_BITMAP_PATH	The path of the image on the filesystem displayed on the login page. Optional.
PASS_RESET	› Default: Password reset disabled. › *0*: Password reset enabled.
CHECK_LDAP	Enable this option if your OpenOTP server does not use your AD or if this host is not connected to the Windows Domain. By default, the LDAP password is checked by OpenOTP first and checked by the credential provider at session start. When disabled, the LDAP check is performed locally only. › Default: LDAP password check enabled in OpenOTP. › *1*: LDAP password check disabled in OpenOTP. Note: This option is not compatible with the Password Reset Option.
AUTO_CREATE_ACCOUNT	You can enable this option when this host is not connected to the Windows Domain and you want the Credential

AUTO_CREATE_ACCOUNT	You can enable this option when this host is not connected to the Windows Domain and you want the Credential Provider to create users accounts at first login. The local LDAP password is transparently reset at each login. › Default: disabled › *0*: enabled Note: This option is not compatible with Remote LDAP Password Check Option. Note: This Option is not compatible with the Password Reset Option.
POLICY	Routing Policy. If two server URLs are defined in server URL, you can configure a request routing policy (ie. the server selection policy). There are three policies available: › Default: Ordered: The first server is always preferred. When it does not respond, the second server is used. › *2*: Balanced: The server is chosen randomly for each request. When it does not respond, the other is used. › *3*: Consistent: The server selection depends on the user ID. A request for one specific user is also always routed to the same server. If it does not respond, the other server is used.
PROXY_HOST	This config is for HTTP proxy. If you are running OpenOTP behind an HTTP proxy you need to set the host and the port of the proxy.
PROXY_PORT	
OFFLINE_MODE	According to this option OpenOTP will permit users to log in when server/network is not reachable, using OpenOTP Token mobile Application. › Default: disabled › *1*: enabled PS: This mode requires at least one online login using push service to fetch its offline information.

In order to set the OpenOTP Credential Provider as the default credential provider in case of silent or remote deployment, the following registry key needs to be set. Please note that after setting this key, you will not be able to login to the machine in question without OpenOTP credential provider.

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential
Provider Filters\{5AE8C610-7541-4FF8-9845-C363410D574C}]
@="OpenOTPCredentialProviderFilter"
```

5.4 Windows FailSafe Mode

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

> ⚠ Important
>
> In case of failure during the 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
```

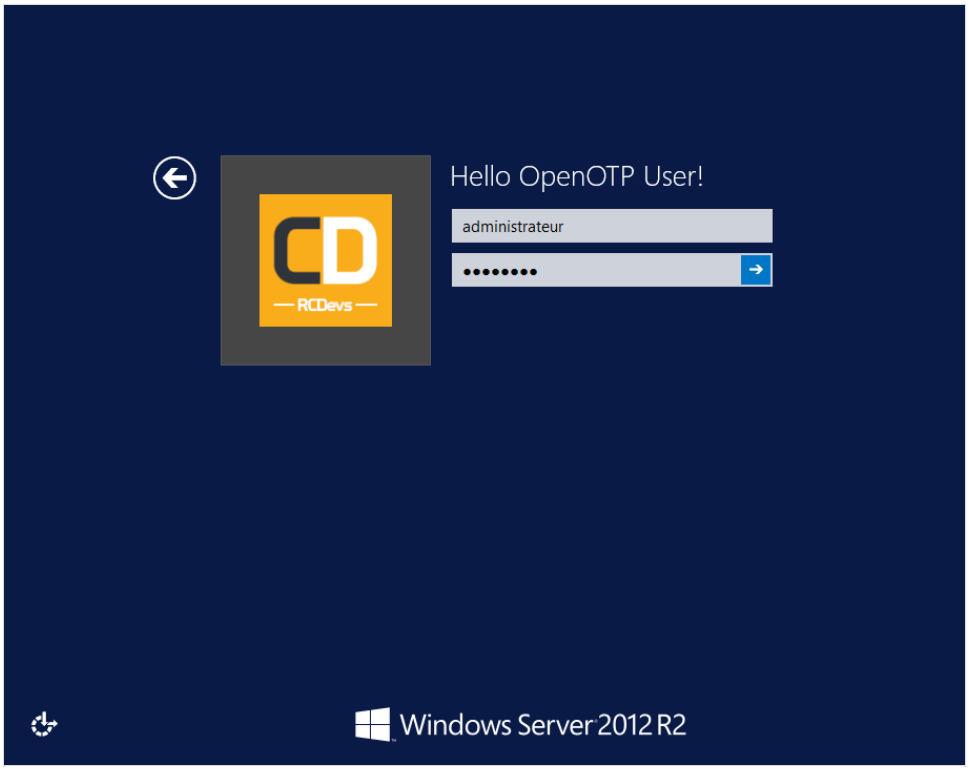
To disable and unregister the failsafe enforcement copy the following text.

```
Windows Registry Editor Version 5.00

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

6. Online Authentication Test

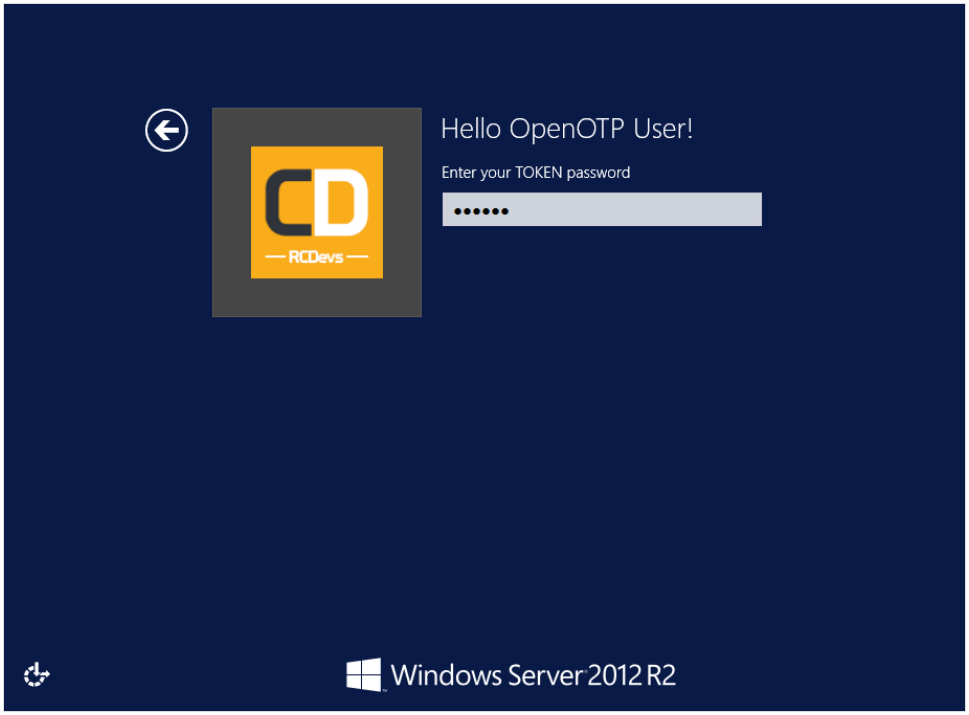
You are now able to log in your Windows machine in MFA. Please log out and enter your LDAP Credentials on the first screen.



Note

You should have a WebADM account activated and an OTP Token enrolled on your account. Follow this documentation to do this: User Activation & Token Enrollment.

On the next screen, your OTP is asked to finish the authentication. Enter your OTP and you are logged on.



7. Offline Authentication Test

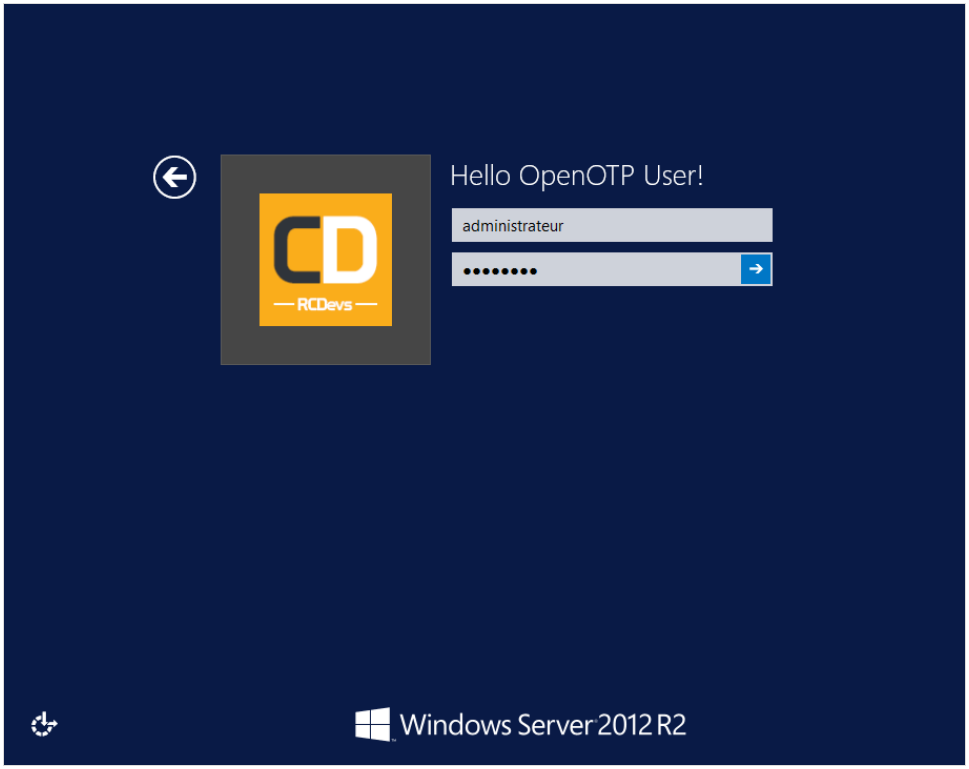
Note

Offline authentication is available for Windows and MacOS login, and requires at least the following versions: WebADM 1.6, OpenOTP 1.3.6, OpenOTP Token 1.4 and OpenOTP Credential Provider 1.2.

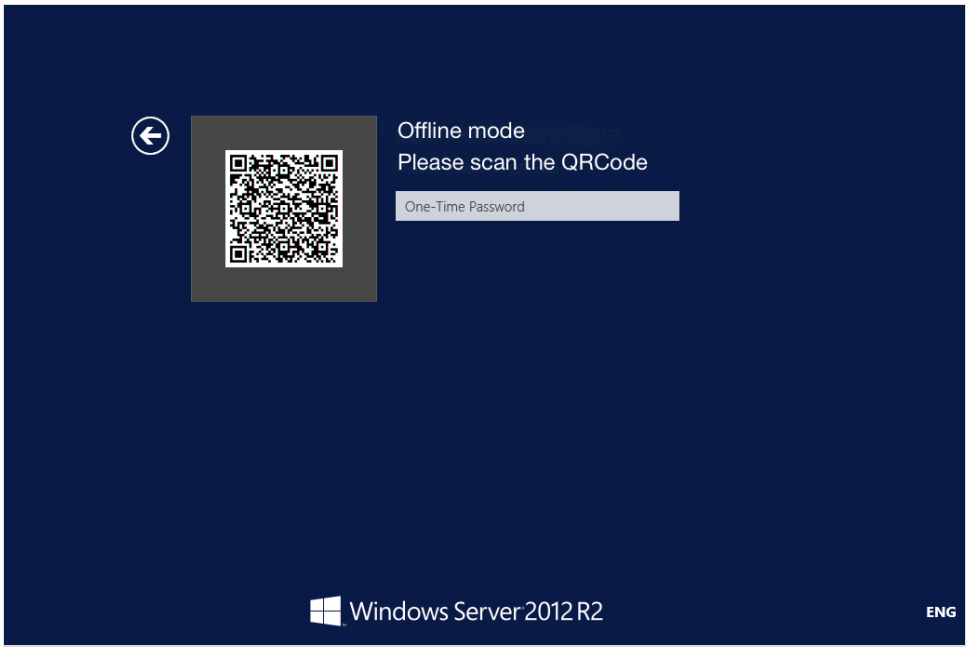
Prerequisites

One online login with Simple Push Login is required to enable offline login mode! This is specific to the user and computer where the login is made. Push Login infrastructure and push enable mobile tokens are mandatory requirements to use the offline mode.

When your laptop is offline, you are now able to login with an OTP. So for this test, I disable the network adapter to simulate the offline mode. Like above, enter your LDAP Credentials on the first screen.

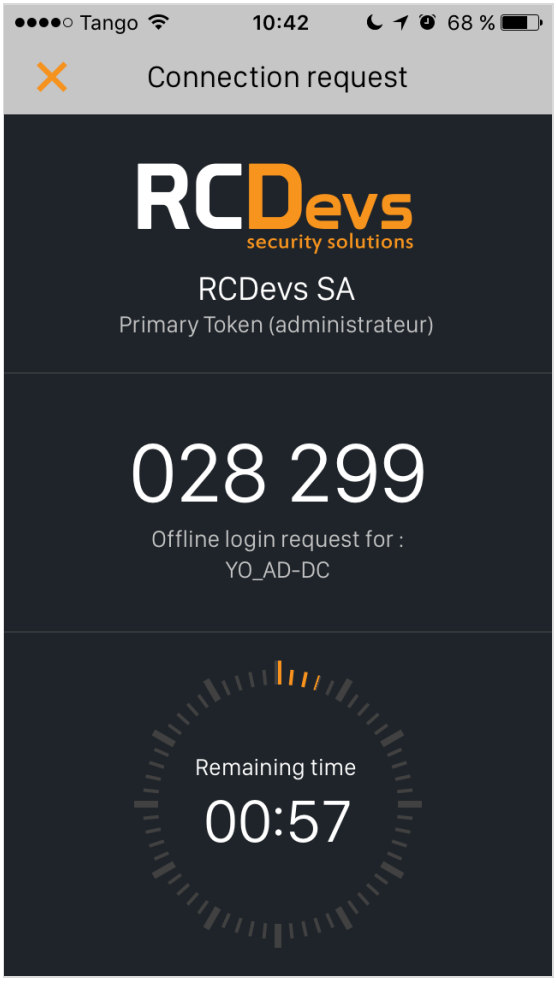


OpenOTP Credential Provider is not able to contact OpenOTP server so, it will switch automatically to the offline mode. The offline mode will prompt you a QRCode. You have to scan the QRCode with the OpenOTP Token application.



Open your OpenOTP Token application, press on the camera button and scan the QRCode.

After scanning the QRCode, a window with an OTP is displayed on your smartphone like below:



Enter your OTP and you are logged on.

8. Troubleshooting

Troubleshooting steps depend on the specific issue you are facing. Please consult the following chapters for instructions.

8.1 Authentication Issues

In case of failed authentication, the first check should be the webadm.log on the OpenOTP/WebADM server. This can be found on the server at `/opt/webadm/logs/webadm.log` or in the WebADM web-interface under Databases > WebADM Server Log Files.

This log should have a trace of the OpenOTP authentication and its result. In case the OpenOTP authentication is successful, but the Windows login fails, the reason is typically a missing local account or wrong local Windows password.

If the login fails and there is no trace of it in the webadm.log, then the installation is not correct. Please see chapter 8.3

8.2 Offline Authentication Issues

Offline authenticate requires a successful online login using mobile push-based authentication and RCDevs OpenOTP mobile soft token. This login must be done on the same Windows machine and with the same user account. If this prerequisite is not complete then you will receive error message: “Offline login is not available for this user.”

To configure mobile message push-based authentication, please see Configure Push Login with OpenOTP PUSH login Web-Service.

8.3 Installation Issues

Windows settings and permissions can cause the installation to fail for a various reason. While debugging your installation and OpenOTP environment have a look at the Windows Event Viewer.

In case the installation is completed but CP is not working, please check the following items:

- You should have an entry in the registry at `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\RCDevs\OpenOTP-CP`. If not please check that the user you are running the installer as has got write permissions to the registry folder: `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\`.
- You should also have these two files, if not then check the effective access of the installation user to the `System32` folder:

```
C:\Windows\System32\OpenOTPCredentialProvider.dll
C:\Windows\System32\OpenOTPCredentialProviderFilter.dll
```

8.4 Unable to login at all

In case you have installed the OpenOTP Credential Provider as the default credential provider and are unable to login at all, you

will have to boot to Windows Safe Mode to remove or repair the installation. Please refer to Microsoft documentation on how to boot to Safe Mode. Once in safe mode, rename or remove the two below files and reboot to log in with the regular Windows login.

```
C:\Windows\System32\OpenOTPCredentialProvider.dll
C:\Windows\System32\OpenOTPCredentialProviderFilter.dll
```

In case Safe Mode boot is not available (for example on cloud deployed Windows), you need to shut down the machine, mount the C: drive and rename/remove the two DLL files. After that you should be able to boot into regular login.

8.5 Push Login issue

If you have increased the `Mobile response timeout` setting under OpenOTP configuration, then you also have to increase the Windows 10 lock screen timeout and the RDP login timeout on the Windows machine. The SOAP timeout value at the OpenOTP Credential Provider level must be also configured in adequation of the mobile response timeout.

E.g : If my mobile response timeout under OpenOTP is configured to 45 seconds, then I have to configure the SOAP timeout and Windows timeouts to 60 seconds.

For the Windows lock creen timeout, you have to create a new registry key in the following container :

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\LogonUI\
```

Simply add a new DWORD value named `IdleTiemout` in that container and configure the timeout value in milliseconds. If your push timeout is configured to 45 seconds, then the value of the new `IdleTimeout` key must be at least 60 seconds. `60` seconds is equal to `60000` ms in decimal and `EA60` in hexadecimal.

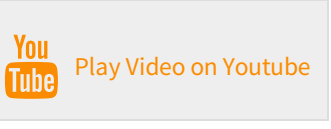
For the Windows RDP timeout, you have to create a new registry key in the following container only if NLA is enabled on the Windows side for RDP login :

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-
Tcp\
```

Simply create a new DWORD key named `LogonTimeout`, containing the timeout value in seconds. Restart the Terminal Services service to changes takes effect.

9. Video Tutorial for Windows 10 and Server 2012R2

9.1 Online Authentication



9.2 Offline Authentication