



OPENOTP CREDENTIAL PROVIDER FOR WINDOWS

The specifications and information in this document are subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. This document may not be copied or distributed by any means, in whole or in part, for any reason, without the express written permission of RCDevs.

Copyright (c) 2010-2017 RCDevs SA. All rights reserved.

<http://www.rcdevs.com>

WebADM and OpenOTP are trademarks of RCDevs. All further trademarks are the property of their respective owners.

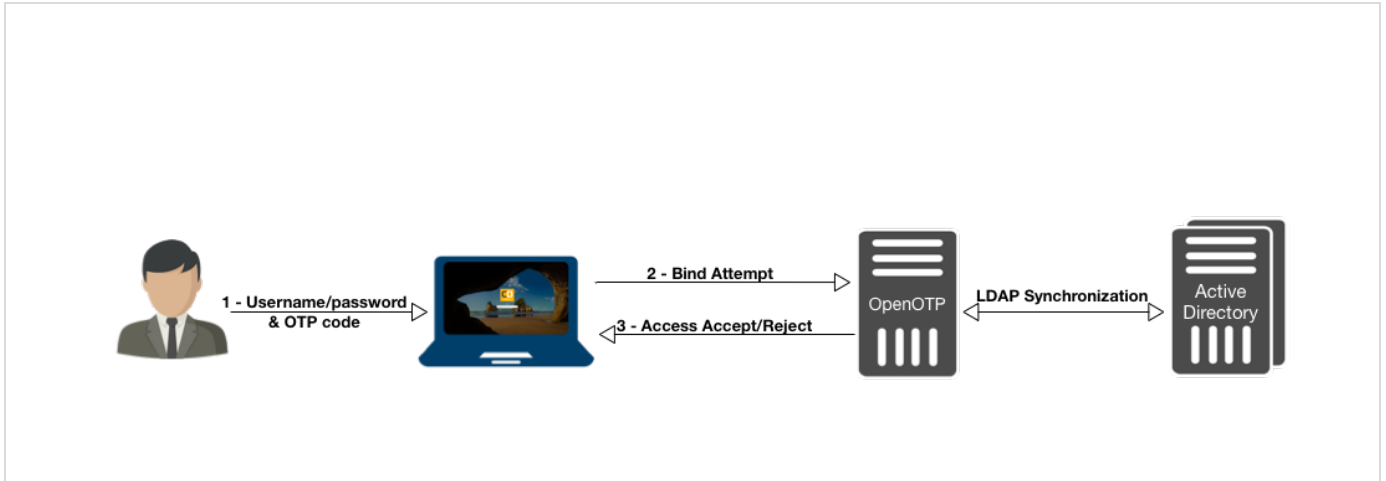
Limited Warranty

No guarantee is given for the correctness of the information contained in this document. Please send any comments or corrections to info@rcdevs.com.

OpenOTP Credential Provider for Windows

[Active Directory](#) [Windows](#) [Remote Desktop Services](#)

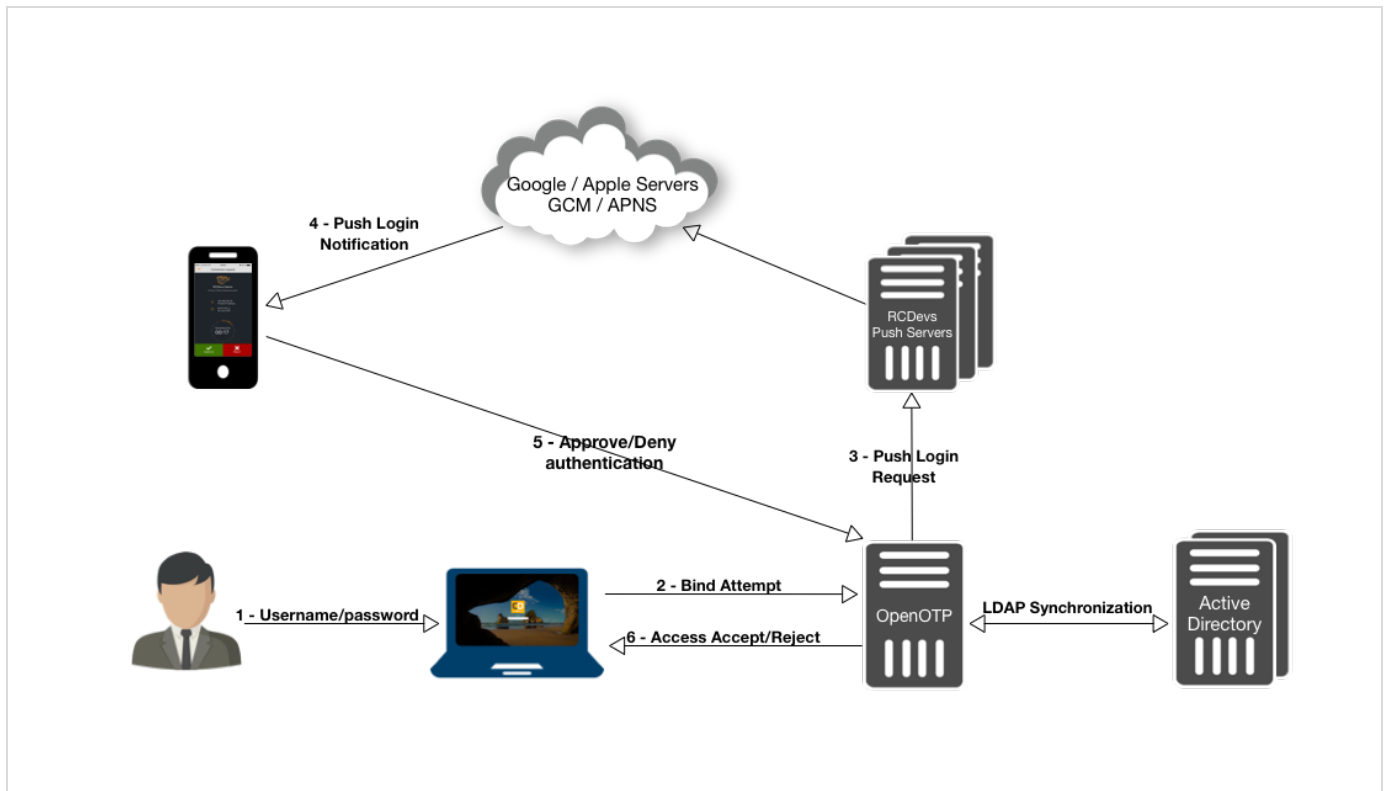
Normal Login flow



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 logon 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 setup 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) 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 logon 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.

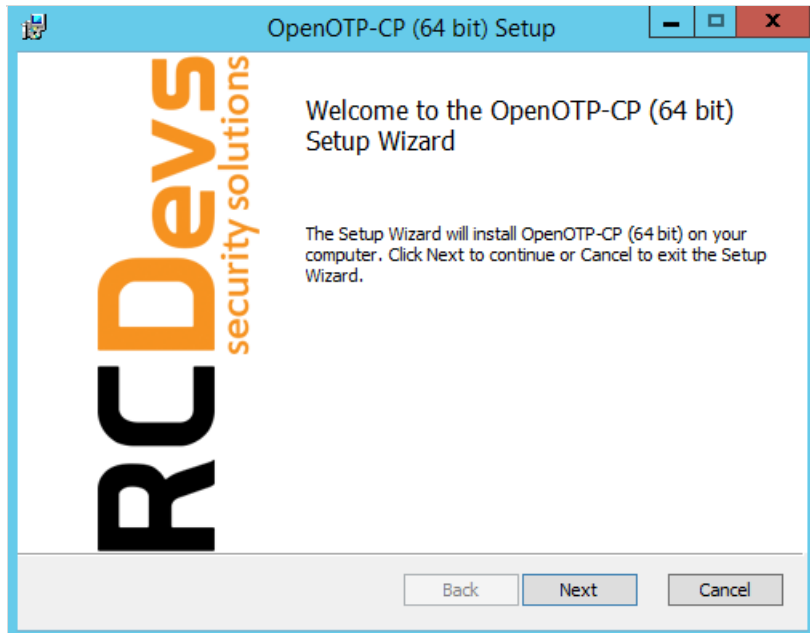
5. Installation and Configuration

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

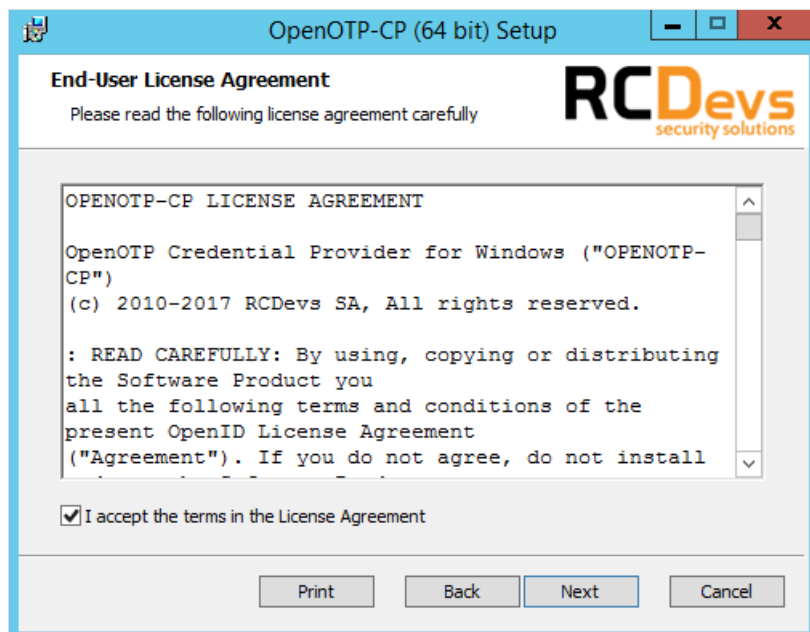
5.1. Local Installation

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 End-User license Agreement and click on **Next**.

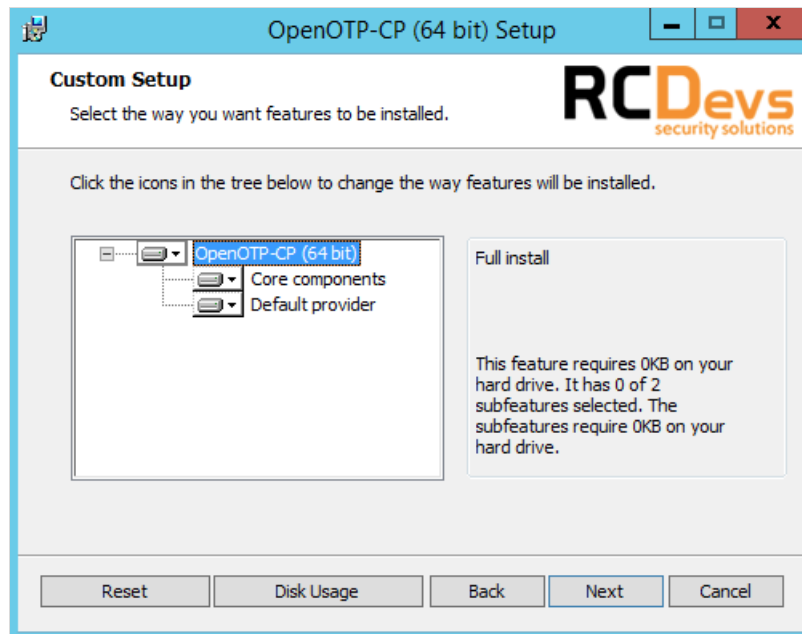


Now, you can select to install the Credential Provider as default. You may also change the default installation directory as you wish.

Click **Next** when you are done.

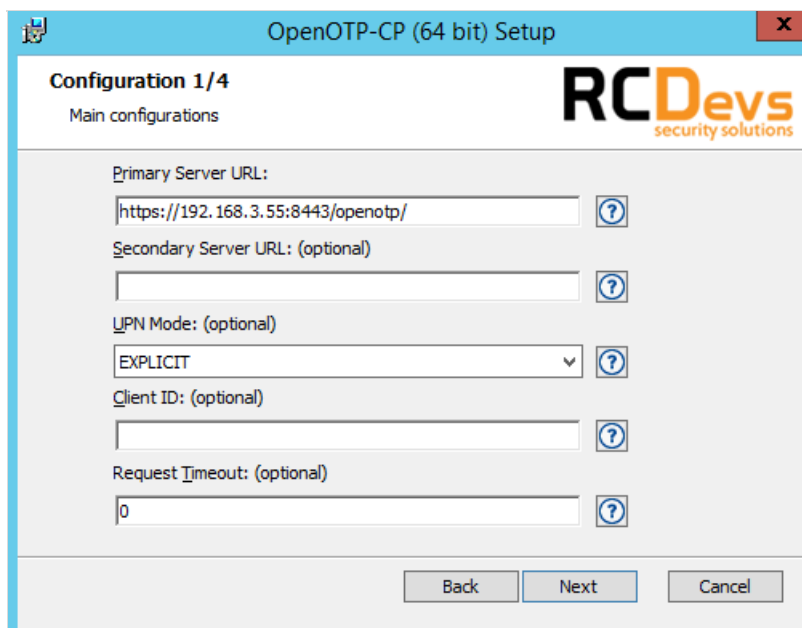
⚠ Note

Installing the provider as default disables all other credential providers on the target system. Only Credential Providers provided by RCDevs will be available for logon. If any problem occurs you can still logon with other providers using the Windows failsafe boot. It is possible to force OTP logon in failsafe mode. This is covered later. To login 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:

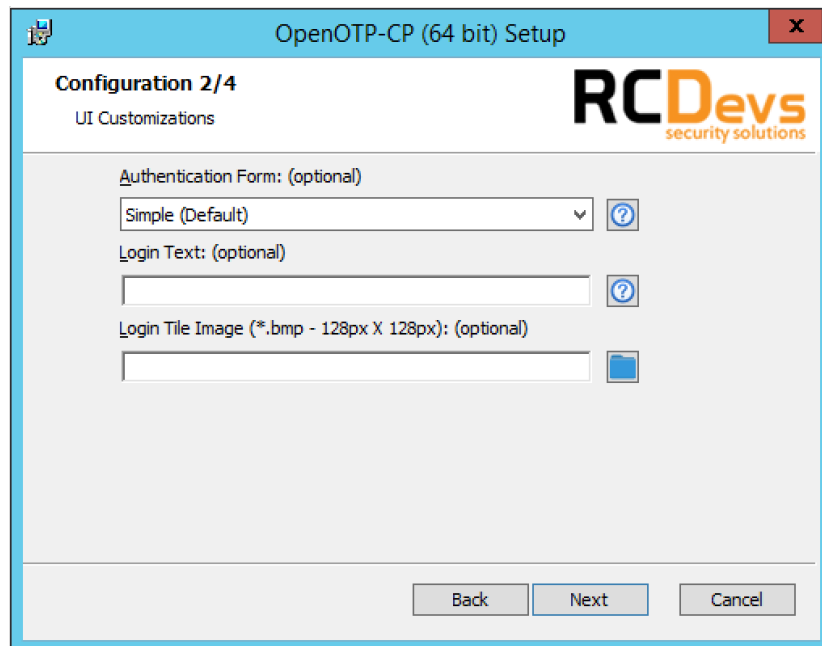
`https://your-webadm-ip-address-or-dns-name:8443/openotp/`. You can also define a Client ID referring to a client policy in WebADM. Click on **Next**.



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 `logon`, 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.



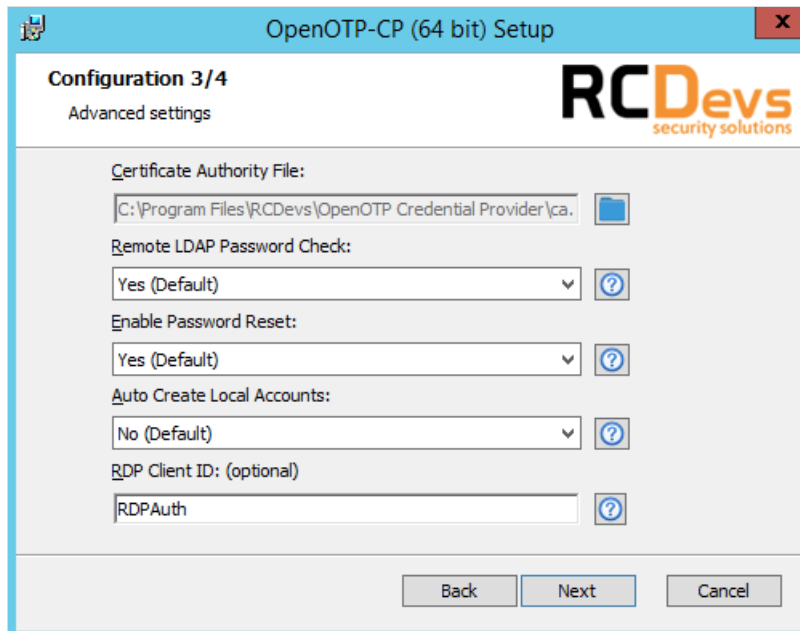
The next page allow you different things :

- > You can configure a CA file, mandatory for HTTPS.
- > The remote LDAP password check setting can be disable if you doesn'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.

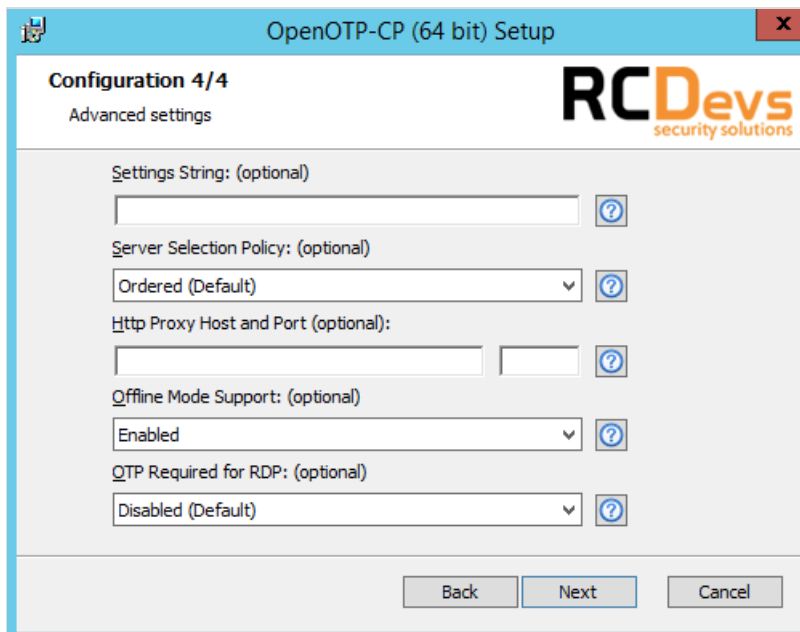
Keep all settings by default if your Windows clients are in a domain.

Note

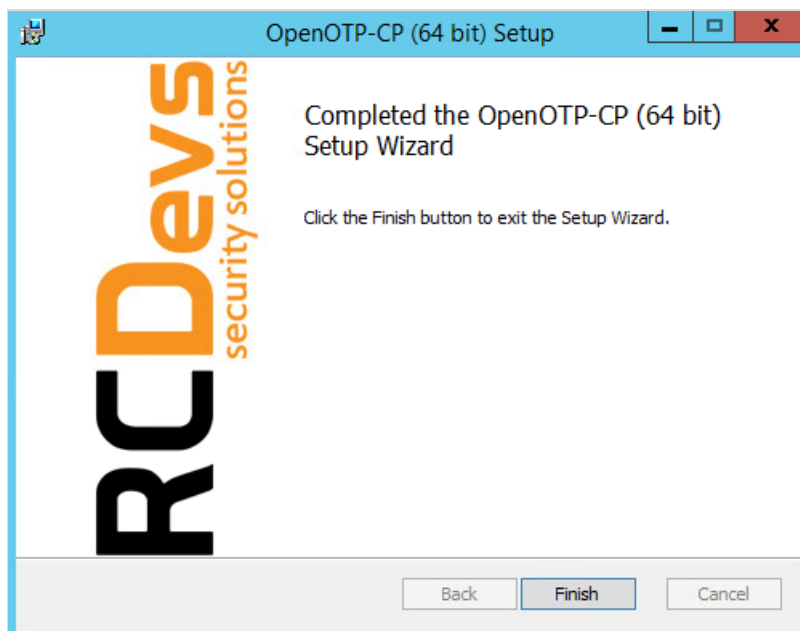
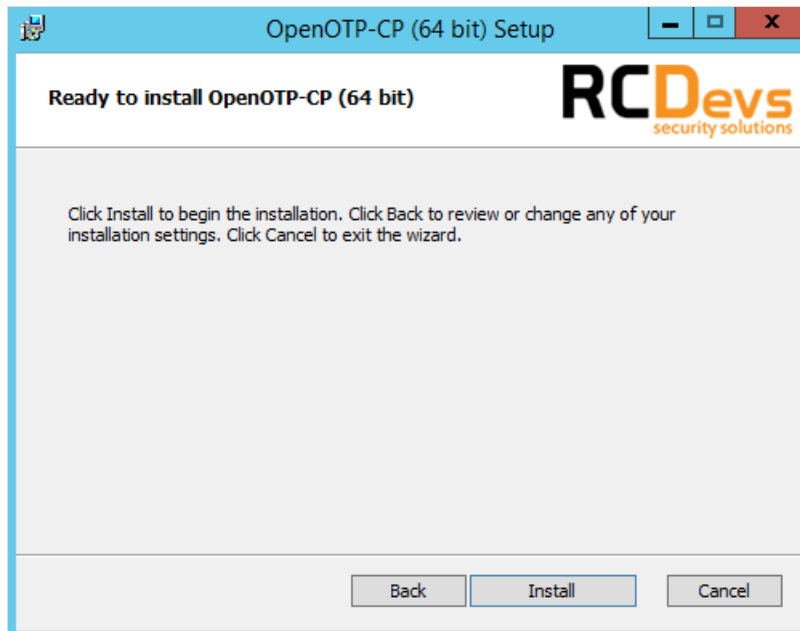
OpenOTP Credential Provider will automatically download the CA certificate on the default WebADM server port when you set the OpenOTP service URL. You can also obtain it manually with `https://mywebadmserver/cacert`.



The last configuration page allows you to configure an HTTP proxy, the failover setting, enforce custom settings for OpenOTP (deprecated feature, 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 allow you to disable OTP for RDP session. That means when this setting is disable, 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.



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.

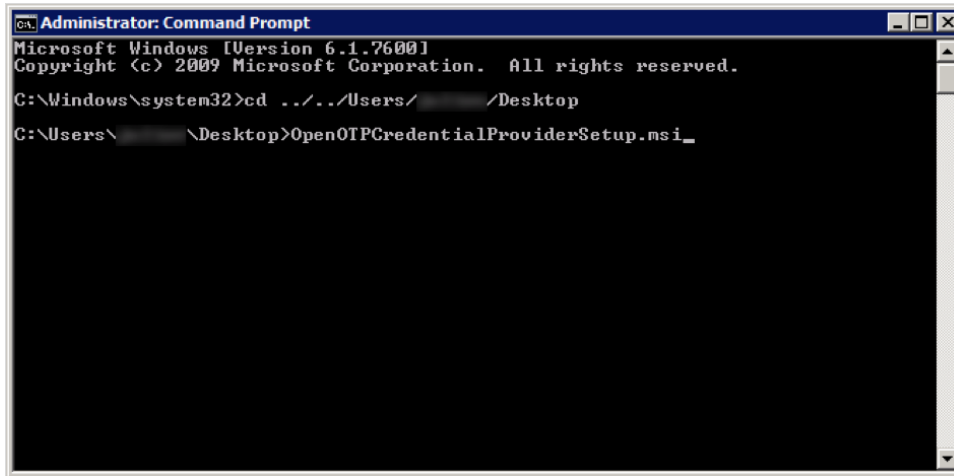
If OpenOTP Credential Provider is running in Production:

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 second node of your OpenOTP cluster. Optional.
DEFAULT_DOMAIN	Default domain to be used, when the user does not specify a domain during logon. Optional.
URI_MODE	According to this option OpenOTP will use the selected attribute for authentication

UPN_MODE	<p>According to this option OpenOTP will use the selected attribute for authentication.</p> <ul style="list-style-type: none"> > Default: Explicit UPN: Value of user's object's userPrincipalName attribute. > 2: Implicit UPN: Value of user's object's samAccountName attribute.
LOGIN_TEXT	<p>A text that is displayed on the Windows logon page.</p> <p>Default (Empty) "OpenOTP Login"</p>
CLIENT_ID	<p>Client ID which is sent to OpenOTP in the login requests.</p> <p>This client ID will appear in the WebADM audit database.</p> <p>Optional.</p>
CA_FILE	<p>The file-system path to a Certificate Authority (CA) file.</p> <p>Mandatory.</p> <p>Example: <i>c:/ca.crt</i></p>
CERT_FILE	<p>The file-system path to a user certificate.</p> <p>Optional.</p>
CERT_PASSWORD	<p>The user certificate's password.</p> <p>Optional.</p>
USER_SETTINGS	<p>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.</p> <p>Example: OpenOTP.LoginMode=LDAPOTP, OpenOTP.OTPType=TOKEN</p> <p>Optional.</p>
SOAP_TIMEOUT	<p>Request timeout when connecting to OpenOTP Authentication Server URL.</p> <p>Default is 30 seconds (If empty it will be 30s).</p> <p>Optional.</p>
LOGIN_METHOD	<p>There are two login methods available:</p> <ul style="list-style-type: none"> > Default: Simple: Only username and password inputs are displayed during logon, and if needed a Challenge appears on a next step. > 1: Normal: Username, password and OTP inputs are displayed during logon. <p>Simple mode uses OpenOTP SimpleLogin method where the semantic of the password input is handled by the OpenOTP server and based on the user login policy.</p> <p>Optional.</p>
V1_BITMAP_PATH	<p>The path of the image on the filesystem displayed on the logon page.</p> <p>Optional.</p>
PASS_RESET	<ul style="list-style-type: none"> > 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, LDAP password are 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.

Not: 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 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 login when server or network are 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 informations.

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 logon 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
```

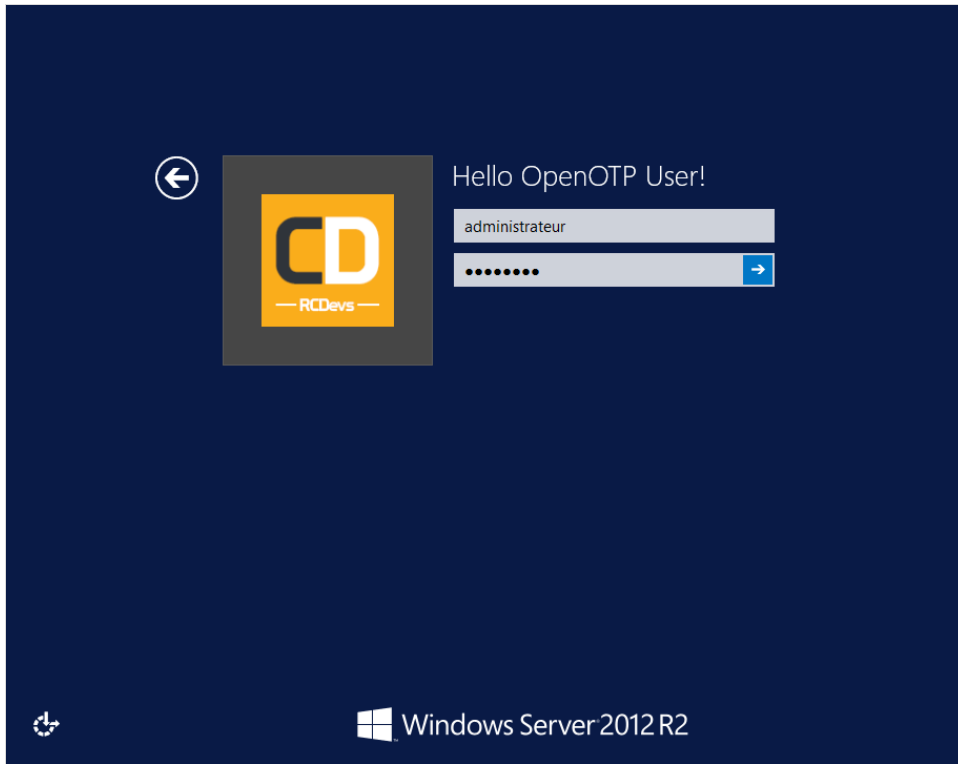
```
> To disable and unregister the failsafe enforcement copy the following text.
```

```
Windows Registry Editor Version 5.00
```

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

6. Online Authentication Test

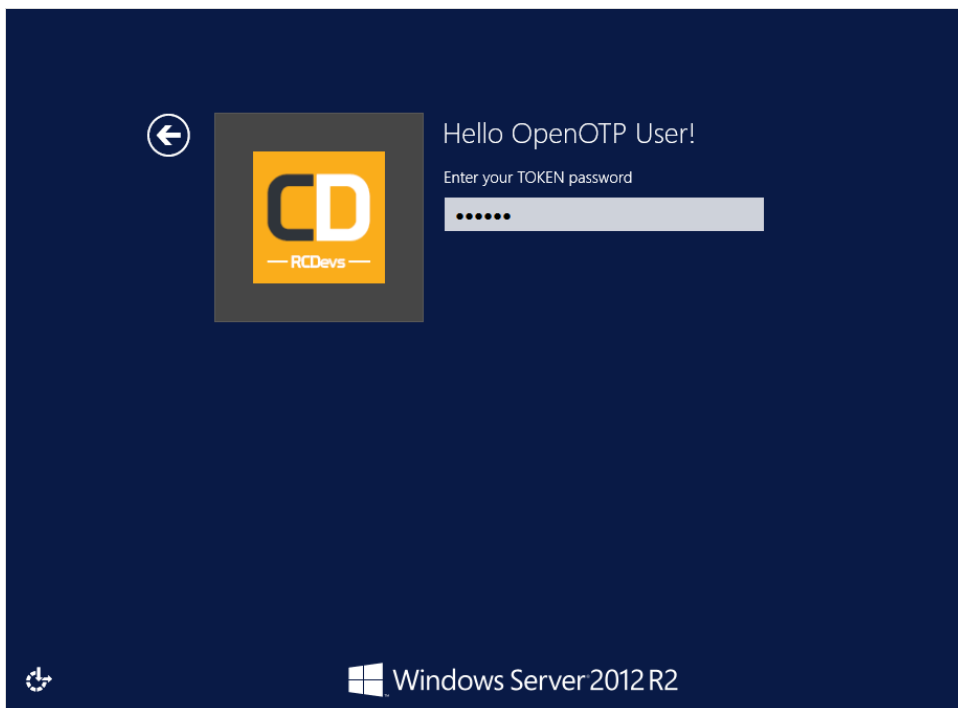
You are now able to logon your Windows machine in MFA. Please logout and enter your LDAP Credentials on the first screen.



🚩 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 Enrollement.](#)

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



7. Offline Authentication Test

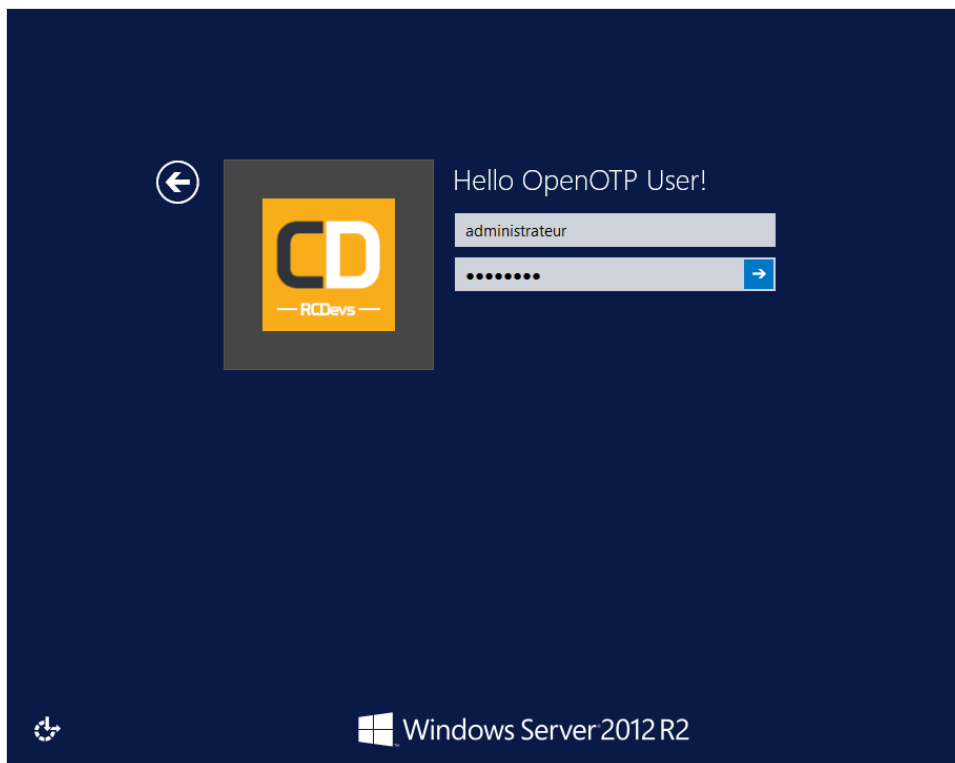
Note

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

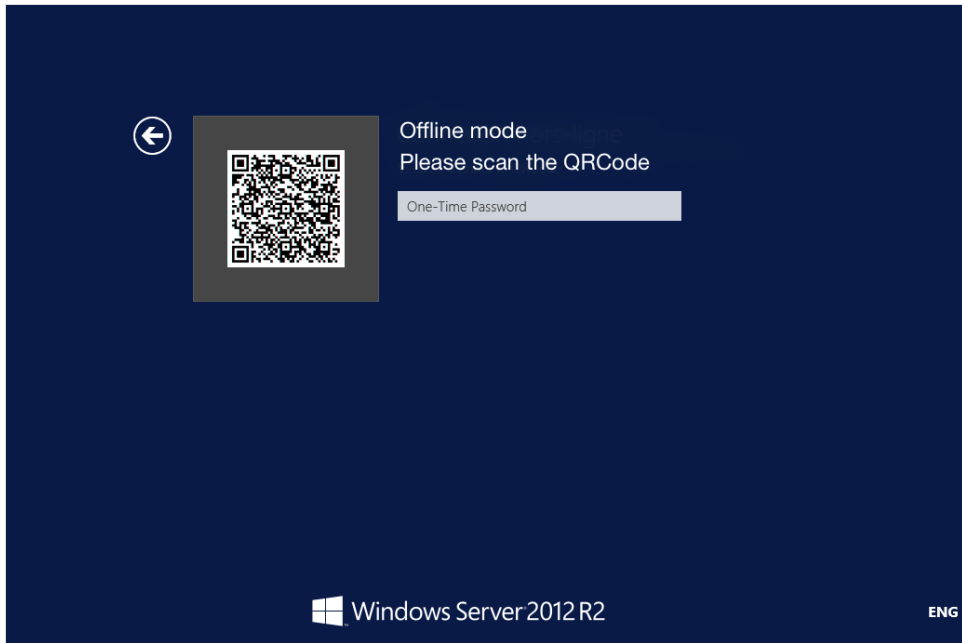
Prerequisites

A first online login is required to enable offline login mode! If you manage to directly login with an offline connection it will not work. You should have a Push Login infrastructure to use the offline mode.

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

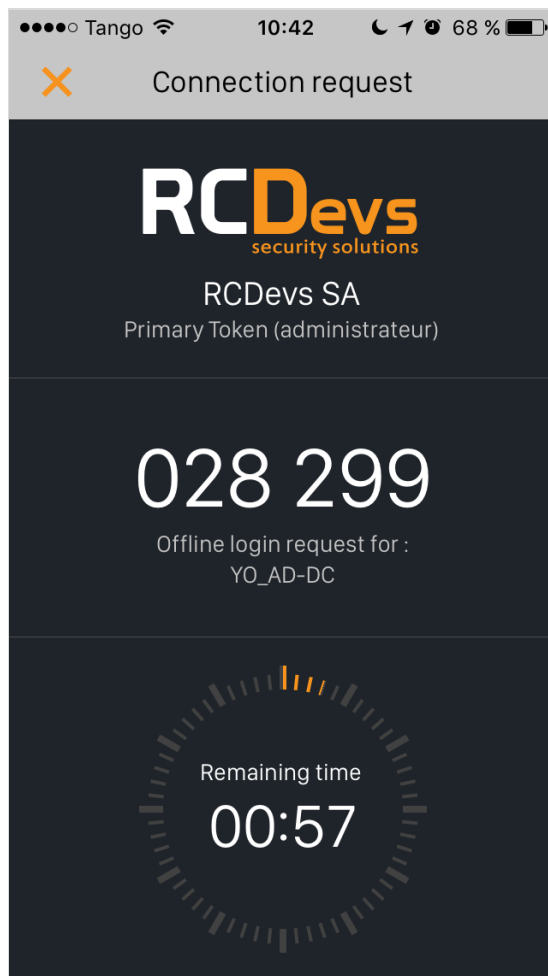


OpenOTP Credential Provider is not able to contact OpenOTP server so, it will switch automatically to the offline mode. The offline mode will prompt you a QRCode. You have to scan the QRCode with the OpenOTP Token application.



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

While debugging your installation and OpenOTP 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 client and server communicate, have a look at WebADM's SOAP log file (webadm.log). This log is located at `/opt/webadm/logs/`. To debug server-side problems, this should be the first place to look at.

9. Video Tutorial for Windows 10 and Server 2012R2

9.1 Online Authentication



9.2 Offline Authentication



This manual was prepared with great care. However, RCDevs S.A. and the author cannot assume any legal or other liability for possible errors and their consequences. No responsibility is taken for the details contained in this manual. Subject to alternation without notice. RCDevs S.A. does not enter into any responsibility in this respect. The hardware and software described in this manual is provided on the basis of a license agreement. This manual is protected by copyright law. RCDevs S.A. reserves all rights, especially for translation into foreign languages. No part of this manual may be reproduced in any way (photocopies, microfilm or other methods) or transformed into machine-readable language without the prior written permission of RCDevs S.A. The latter especially applies for data processing systems. RCDevs S.A. also reserves all communication rights (lectures, radio and television). The hardware and software names mentioned in this manual are most often the registered trademarks of the respective manufacturers and as such are subject to the statutory regulations. Product and brand names are the property of RCDevs S.A. © 2018 RCDevs SA, All Rights Reserved