OpenOTP™ Credential Provider Installation Guide – DRAFT

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

http://www.rcdevs.com/

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.

Content of this Guide

1. Product Documentation 5
2. Product Overview 5
3. System Requirements 5
4. Preliminary Information 6
5. Installation and configuration 6
   5.1 Local installation 6
   5.2 Modifying the Configuration 10
   5.3 Automatic Deployment 10
   5.4 Windows Failsafe Mode 11

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 library.

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.

The Credential Provider enables you to use all types of authentication tokes and authentication standards supported by the OpenOTP authentication module. That includes OATH/HOTP, OATH/TOTP, OATH/OCRA, Mobile-OTP, YubiKey, SMSOTP and MailOTP. Software tokens are provided by various publishers and for a variety of platforms including Android and iOS.

3. System Requirements

The OpenOTP 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 AD domain
- Network access
- An instance of WebADM and OpenOTP running in your network OR
- OpenOTP web-service reachable over the internet
- Open ports: 8080 or 8443 depending on your security settings
- 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 get the following information. You will need to enter during the installation process:

- The URI(s)s of the OpenOTP web-service(s) **(mandatory)**
- Your local domain (optional)
- A custom login text or tile caption (optional)
- A client ID (optional)
- 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 is done in about 5 Minutes. The installer is the only utility that is needed to setup and configure the provider.

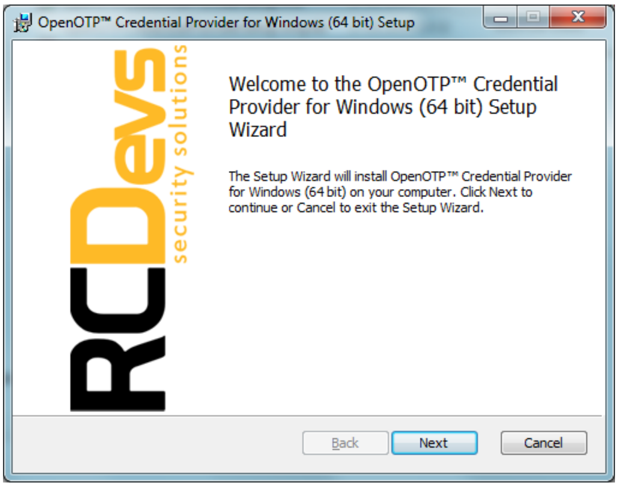
The provider can be automatically deployed to your clients. This is covered later.

5.1 Local installation

First, you need to download the latest version of the OpenOTP Credential Provider for Windows.

You can download it at RCDevs' website at http://www.rcdevs.com/downloads/.

After you downloaded the installer package and coped it to your client workstation just start the setup.

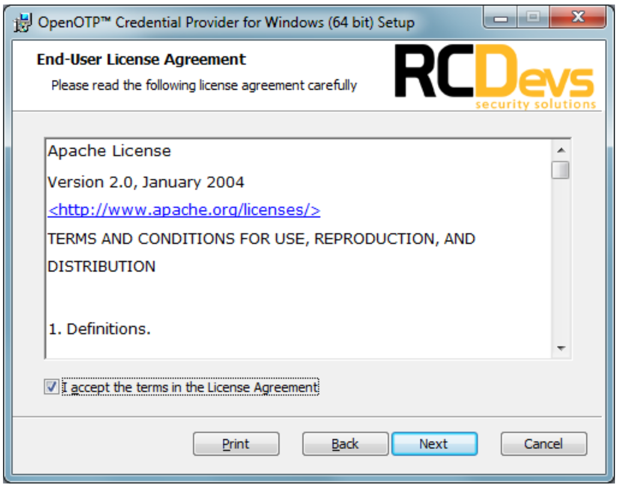


OpenOTP™ Credential Provider for Windows (64 bit) Setup

Welcome to the OpenOTP™ Credential Provider for Windows (64 bit) Setup Wizard

The Setup Wizard will install OpenOTP™ Credential Provider for Windows (64 bit) on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

Click “Next” and accept the License Agreement.



OpenOTP™ Credential Provider for Windows (64 bit) Setup

End-User License Agreement

Please read the following license agreement carefully

Apache License

Version 2.0, January 2004

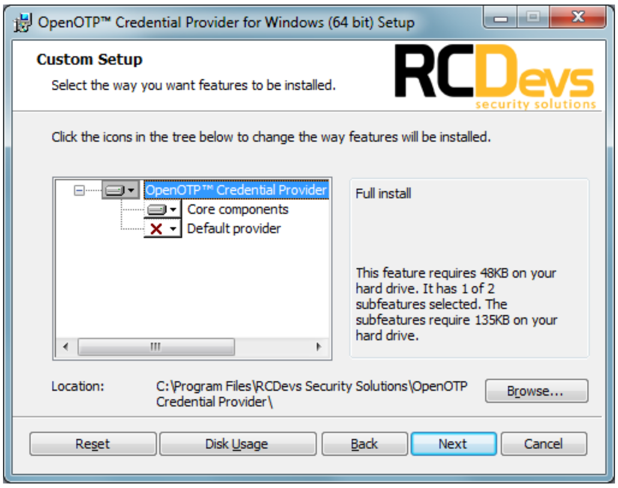
<http://www.apache.org/licenses/>

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

☑ I accept the terms in 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.



OpenOTP™ Credential Provider for Windows (64 bit) Setup

Custom Setup

Select the way you want features to be installed.

Click the icons in the tree below to change the way features will be installed.

- OpenOTP™ Credential Provider
  - Core components
  - ✗ Default provider

Full install

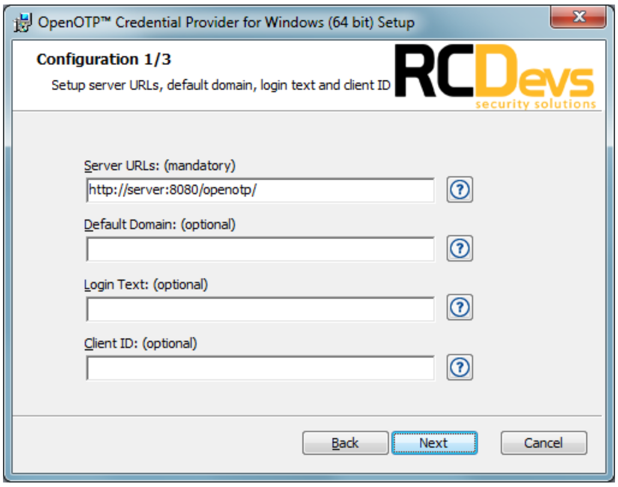
This feature requires 48KB on your hard drive. It has 1 of 2 subfeatures selected. The subfeatures require 135KB on your hard drive.

Location: C:\Program Files\RCDevs Security Solutions\OpenOTP Credential Provider\

Important 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 even disable failsafe logon using other providers. This is covered later.

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



OpenOTP™ Credential Provider for Windows (64 bit) Setup

Configuration 1/3

Setup server URLs, default domain, login text and client ID

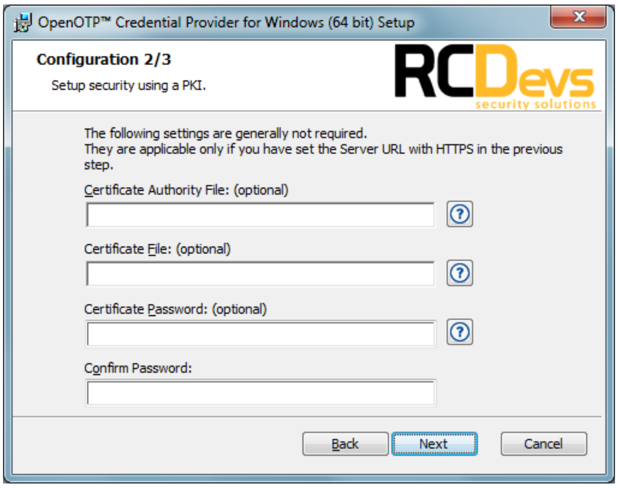
Server URLs: (mandatory) http://server:8080/openotp/

Default Domain: (optional)

Login Text: (optional)

Client ID: (optional)

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



OpenOTP™ Credential Provider for Windows (64 bit) Setup

Configuration 2/3

Setup security using a PKI.

The following settings are generally not required.
They are applicable only if you have set the Server URL with HTTPS in the previous step.

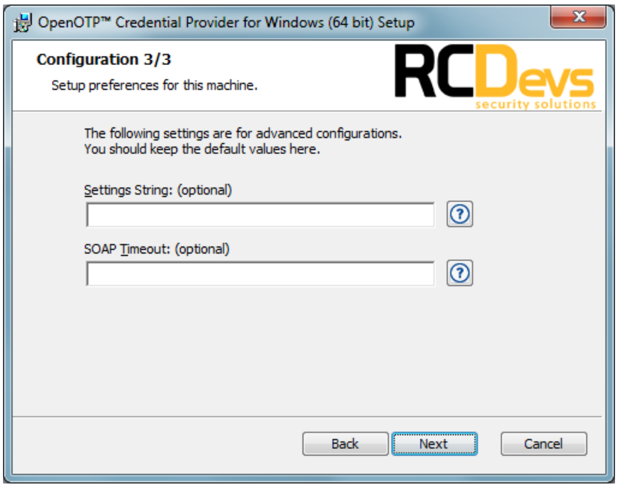
Certificate Authority File: (optional)

Certificate File: (optional)

Certificate Password: (optional)

Confirm Password:

Here you may setup a custom settings string for your WebADM and OpenOTP configuration. Further, you may change the default SOAP service timeout. Click “Next” when you are done.



OpenOTP™ Credential Provider for Windows (64 bit) Setup

Configuration 3/3

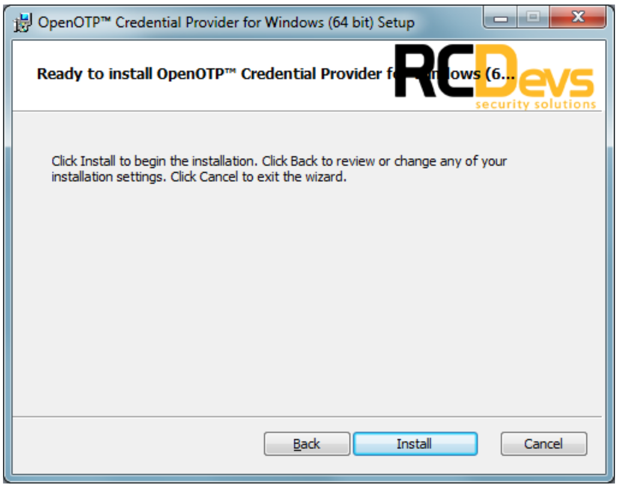
Setup preferences for this machine.

The following settings are for advanced configurations.
You should keep the default values here.

Settings String: (optional)

SOAP Timeout: (optional)

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

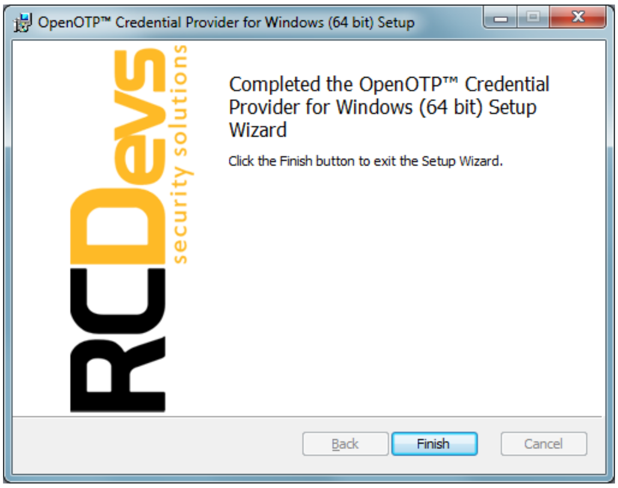


OpenOTP™ Credential Provider for Windows (64 bit) Setup

Ready to install OpenOTP™ Credential Provider for Windows (6...

Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

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



OpenOTP™ Credential Provider for Windows (64 bit) Setup

Completed the OpenOTP™ Credential Provider for Windows (64 bit) Setup Wizard

Click the Finish button to exit the Setup Wizard.

5.2 Modifying the Configuration

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.

5.3 Automatic Deployment

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 OpenOTP web-service. At least one is mandatory.
DEFAULT_DOMAI N	Default domain to be used, when the user does not specify a domain during logon. Optional.
LOGIN_TEXT	A text that is displayed on the Windows logon pane. Optional. Default “OpenOTP 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 OpenOTP settings. Optional.
SOAP_TIMEOUT	The SOAP timeout in seconds when connecting to the OpenOTP Authentication Server. Optional. Default is 15 seconds.

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

Deploy.bat contains:

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

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

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 note:

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\C
redential 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\C
redential Providers]
"ProhibitFallbacks"=-
```