



ELECTRONIC SIGNATURE FROM 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 Security.

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

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

Electronic Signature from Windows

[Advanced Signature](#) [Qualified Signature](#) [Standard Signature](#) [mobile Signature](#) [Windows](#)

1. Overview

This documentation describes the installation and usage of the OpenOTP Signature plugin for Windows OS. To install and use that signature plugin, you need to have WebADM & OpenOTP server(s) deployed, OpenOTP Token mobile application, Push mechanisms implemented, a push token registered on the user account through OpenOTP mobile application, a license which allow you the usage of signature feature of OpenOTP and signature credits.

The prerequisites for the Windows machines are :

- › Have .NET 6.0 Desktop Runtime installed,
- › Up-to-date Windows OS (minimal compatible version \geq Windows 10 version 2004, from mid 2020).

That plugin has been developed in order to provide an easy way to electronically sign a document/file for collaborators of your organization from their Windows machine just by right-clicking on the document.

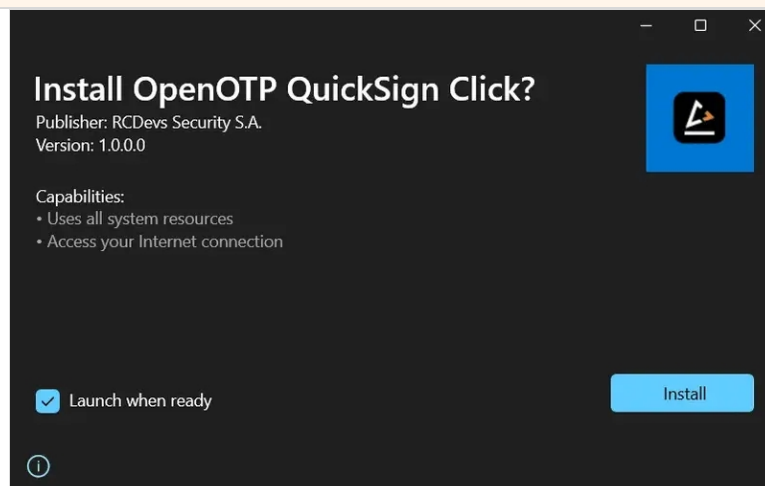
The plugin offer the 4 kinds of signatures supported by OpenOTP. Please refer to [OpenOTP Signature documentation](#) to get more details about different types of signature.

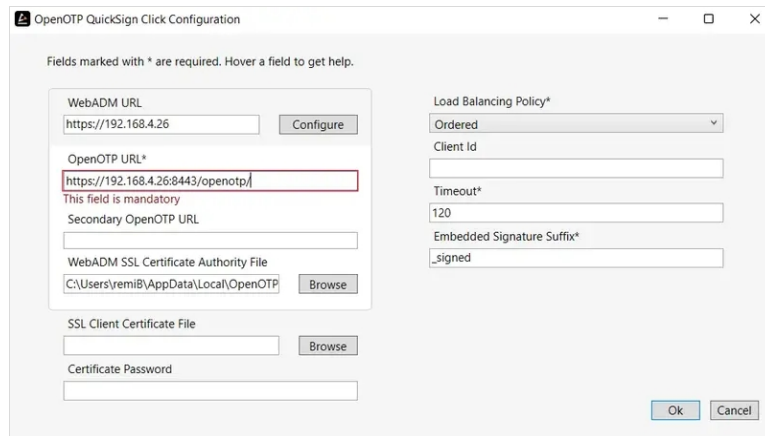
The signatory is always the person which initiate the signature workflow. You can not submit a document for signature to someone else through this integration. RCDevs provides other integrations for this purpose (Postfix mail server plugin).

Once the signature workflow has been completed, the signed document is automatically fetch from OpenOTP servers to the Windows machine. Both original and signed files are kept/saved at the same location. The extension “signed” is added to the signed files name.

OpenOTP API URL must be reachable directly or through a reverse proxy (WAProxy) in order to perform a signature. If OpenOTP backend is not reachable by the Windows machine, it is not possible to sign.

2. Installation and configuration





OpenOTP QuickSign Click Configuration

Fields marked with * are required. Hover a field to get help.

WebADM URL

OpenOTP URL*

This field is mandatory

Secondary OpenOTP URL

WebADM SSL Certificate Authority File

SSL Client Certificate File

Certificate Password

Load Balancing Policy*
 Ordered

Client Id

Timeout*

Embedded Signature Suffix*

First of all, after installing the product, you will be brought to the configuration page where you can put your WebADM URL and then click on **Configure**. It will automatically fill the below parameters. After that, you can still add other parameters such as the SSL Client Certificate File alongside its password if you have one. On the right of the window, you can also change other settings : the Load Balancing Policy which have 3 different configurations that can be seen below.

If two server URLs are defined in server URL, you can configure a request routing policy (ie. the server selection policy).

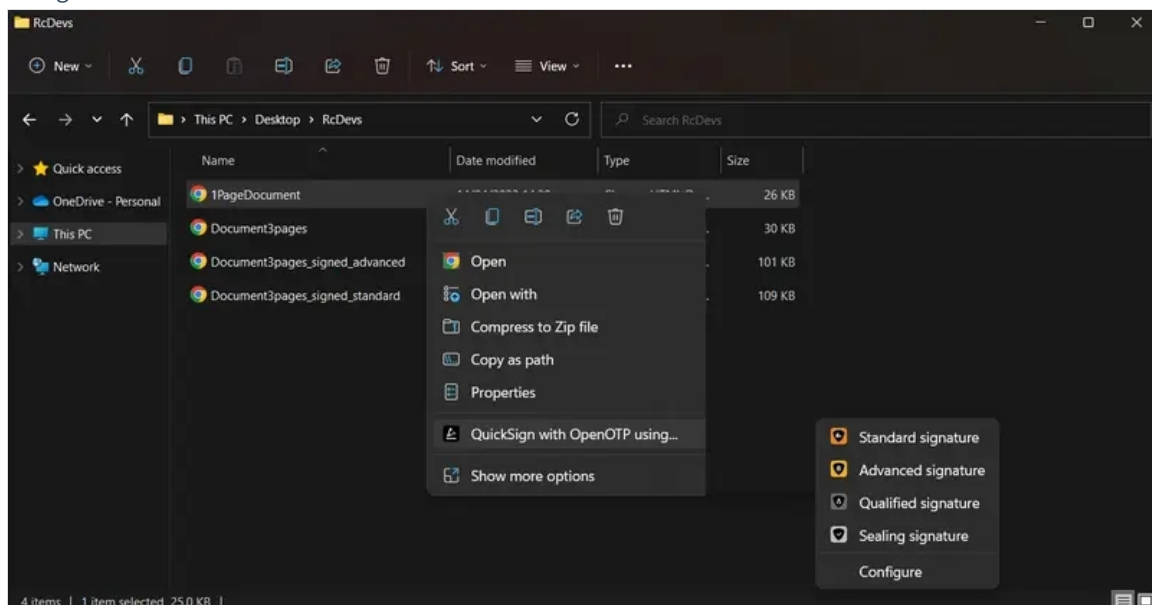
There are three policies available:

- Ordered: The first server is always preferred. When it does not respond, the second server is used. (Default)
- Balanced: The server is chosen randomly for each request. When it does not respond, the other is used.
- 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.

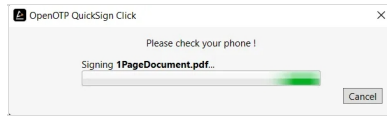
There is the possibility to change the client ID too, the timeout of the signature request and the Embedded Signature Suffix added at the end of the new document signed.

3. Usage

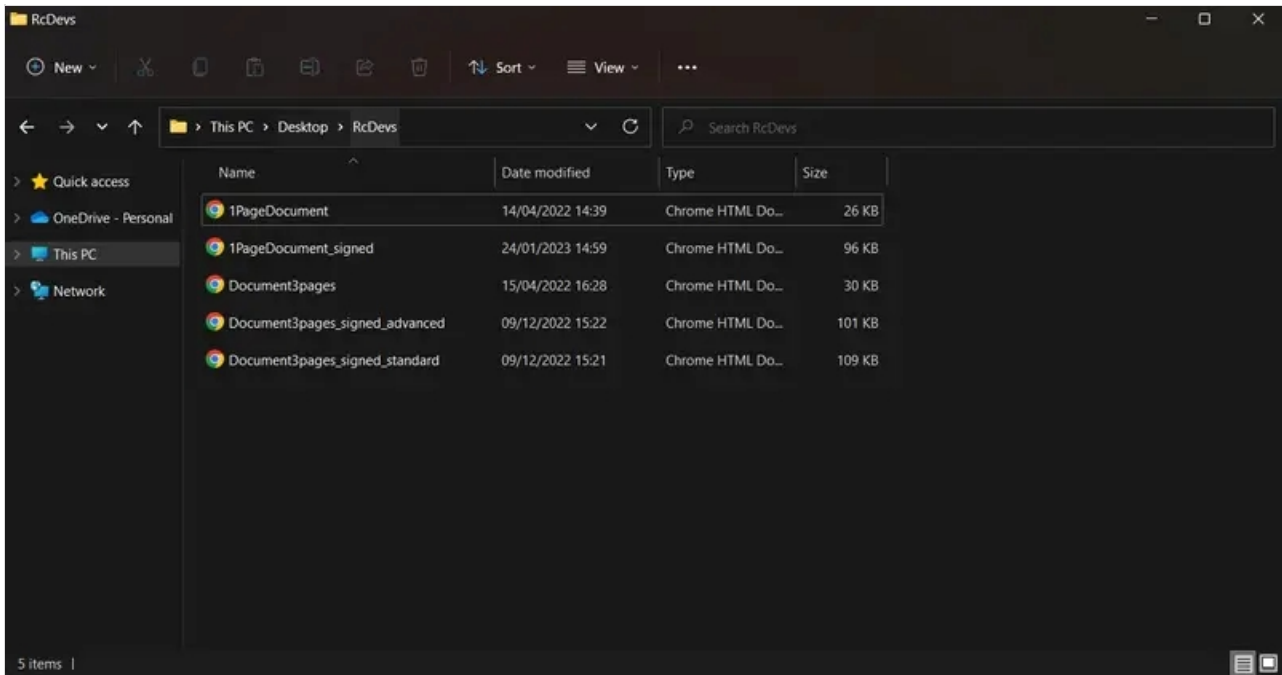
Once the signature plugin for Windows is installed and configured properly, you can right-click on a document and submit it to OpenOTP for signature.



The document is sent to OpenOTP backend. OpenOTP is going to prepare the transaction and send it on the user's mobile.



The user receives the signature request with the attached document. He can sign it and finalize the signature. After it's done, the signed document will appear below the original one with its new suffix.



This manual was prepared with great care. However, RCDevs Security 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 Security 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 Security 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 Security S.A. The latter especially applies for data processing systems. RCDevs Security 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 Security. © 2024 RCDevs Security S.A., All Rights Reserved