PROXIMITY FOR WINDOWS LOGIN

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.

Proximity for Windows login

Proximity Windows BLE

1. Overview

Windows Hello is a technology that allows Windows 10 users to authenticate to their PC with biometric identification, such as a fingerprint, iris scan or facial recognition. This enables users to log in to their PC faster and considerably more securely than using static passwords. None of us like passwords. They can be cumbersome to use and difficult to remember. Passwords are getting more and more insecure, being subject to phishing, massive leaks and other attacks that even the most security-savvy have trouble trying to stay ahead of. Regardless of these failings, we are not moving away from using passwords, as they remain familiar and universally supported. Windows Hello offers a solution that reduces the use of passwords, making our digital lives both easier but also considerably more secure. With the use of biometrics, Windows Hello introduces new concepts and technologies to workstation authentication. At RCDevs we believe that biometrics alone will not be sufficient to meet tomorrow's security requirements and external physical factors will still be required.

2. Prerequisites

2.1 WebADM/OpenOTP

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. Users who will use Proximity have to be activated under WebADM.

2.2 OpenOTP Token

Usage of OpenOTP Token Application is mandatory to perform a login with Proximity. OpenOTP Token version should be at least:

- For Android : 1.4.6
- For iOS : 1.4.8

Check the version you are running on your phone by opening the application on your smartphone and going to `Settings` tab:

Under the same menu, you have to enable the `Windows Login` setting to enable the Proximity feature on your OpenOTP Token Application.

The users who will use Proximity must already have a Token enrolled on their LDAP account with the OpenOTP Token else the user will not be able to pair its mobile device with its laptop/computer.

2.3 Windows 10 Build

Using Proximity required at least Microsoft Windows Version 1709 (OS Build 16294.1). To check your Windows build open the command line prompt or Powershell on your Windows machine and enter the following command:

```
winver
```

You should be prompted to the following window:

2.4 Bluetooth devices supported (Computer)

On your Windows machine, you have to check if your embedded Bluetooth chipset supports the Bluetooth low energy (BLE). To check it, open the `Device Manager` and expand the `Bluetooth` category.

Right-click on your Bluetooth adapter, click `Properties` and go to `Details` tab.

Click the drop-down under `Property` and select the option: `Bluetooth radio supports Low Energy Peripheral Role`. If the value is set to `true`, then your Bluetooth device manages BLE and can be used with Proximity. If the Value is set to `false`, then you can not use Proximity with that computer.

2.5 Bluetooth devices supported (Smartphone)

All smartphone with Bluetooth 4.0 should support BLE. Have a look on your phone model and Bluetooth specifications for your phone to check if BLE is managed by your device.

2.6 Sideload Apps

Sideload Apps feature is required for Proximity. To enable it, open `Windows Settings` > `Update & Security` > `For Developers`. Under `Use developer features` select the `Sideload apps` option.

Click `Yes` to confirm your choice and turn on app sideloading.

2.7 App data Sharing (Optional)

In order to share Proximity settings between different users accounts on the same machine, you have to enable the application data sharing. If only one user uses the machine where Proximity will be installed, then you don't need to configure the application data sharing.

To enable it, open the `Local Group Policy Editor` (gpedit) > `Computer Configuration` > `Windows Settings` > `Administrative Templates` > `Windows Components` > `App Package Deployment`. Change the key value of `Allow a Windows app to share data between users` to `Enabled`.

2.8 Installation Permissions

The installation of Proximity has to be done with a local Admin account or with a domain admin account if the computer is domain joined.

2.9 PIN Configuration

Proximity requires that PIN functionality of Windows 10 enabled. To enable it and set it, please go to Windows settings > Accounts Category.

On the next page, click on Sign-in options on the left.

In PIN section, click Add button.

Enter your password account.

And now configure your PIN.

Your PIN is now configured.

3. Proximity Installation

Download Proximity product on RCDevs website and extract files from the archive.

3.1 Certificate Installation

Before installing Proximity, we need to install the certificate available in the extracted folder.

The certificate has to be imported in the `Local Machine Certificates store` in the `Trusted Root Certification Authorities` certificate store. Click on `Install Certificate` button:

Select the `Local Machine Store` and click `Next` button.

On the next page, select the place where you want to import the certificate. The certificate should be installed in the `Trusted Root Certification Authorities`.

Click `Next` and `Finish` button:

The Certificate should be imported successfully. Press `Ok` and the certificate setup is done.

3.2 Proximity Installation

3.2.1 Through Powershell

Once files are extracted, execute the `Add-AppDevPackage` Powershell script:

Enter `A` on the following screen and press `Enter` to allow the script to be executed.

Once the script execution is done without any error message, then Proximity is now installed and ready to be configured with your OpenOTP server.

To check that Proximity is well installed, looking for `Proximity` in the Windows search:

The application should appear in your applications list. Installation is now complete.

3.2.2 Through Installer

Once files are extracted, execute the `APPXBUNDLE` file by double-clicking on it and the following window should be prompted:

Click on `Install` button…

When the installation is complete, then the following page should be prompted:

As mentioned in the prerequisites part, the OpenOTP Token application is mandatory to have Proximity working with OpenOTP. Click on the `Continue` button. Some checks are performed and you should arrive on the following page after checks complete:

Installation is now complete.

4. Proximity Configuration

Installation of Proximity is complete and we have now to configure it.
Run the Proximity application and the following screen should be opened:

Click on the `Settings` menu. On this page, you have first to configure the WebADM server URL. On my side, it's `https://192.168.3.54` and then press the `Configure` button.

If you are running a WebADM cluster, both URLs should be returned. The CA file status should change from `Not Configured` to `Configured`.

Optionally, a `Client ID` can be configured. The `Offline Login` mode can be enabled in case it's the computer is a laptop can will maybe not be able to communicate with the OpenOTP server. The debug mode can be enabled in case you need to troubleshoot. Click `Save` button to changes takes effect.

Proximity configuration is done.

5. Proximity Phone Enrollment

Always on the Proximity application, go to `Add Device` menu to pair your mobile device with your computer.

Open your OpenOTP Token application with a Token already register for your account and scan the QRCode prompted by Proximity application.

⚠ Multiple Tokens

If 2 Tokens are enrolled on your OpenOTP Token application, then after having scanned the QRCode prompted by Proximity, the OpenOTP Token application will ask you with which Account/Token you want to do the pairing. On my side, I have 2 Tokens for 2 different accounts, but I want to use Proximity with the RCDevs user.

⚠ Tuned on Bluetooth

Make sure that Bluetooth is turned on on your computer and on your phone before scanning the QRCode!

Click on the Camera button on your OpenOTP Token application and scan the Proximity QRCode. After scanning the QRCode, the mobile is trying to communicate with the computer.

As I have multiple Token enrolled for a different account, the OpenOTP Token ask me for which Token/Account I want to use Proximity.

I select the RCDevs account:

If the registration went well, then you should see the next screen on your phone after during the pairing with your computer:

You can check on your OpenOTP Token application if the pairing has been done successfully by checking the `Settings` menu of your OpenOTP Token app:

Click on `Manage Accounts` item:

And you should see an entry with the computer name, the account name and the Token used for Proximity login.

On the computer side, you will see the following during the enrollment process:

At this step of the enrollment/pairing, you are prompted on Windows to enter your PIN previously configured in the Prerequisites. The PIN can be used to unlock your session in case you forget your phone or if you encountered troubles with Bluetooth communications between the computer and the phone.

Enter your 4 digits PIN and the pairing will continue.

The pairing is done. You can now see your device in the `Manage Devices` menu of Proximity application.

6. Proximity Login

All steps are done. We can now try to login with Proximity over BLE. Note that the Proximity login works only when the session is locked (user session opened).

OpenOTP Token

Your OpenOTP Token application must be open to receive and prompt you the challenge login on the Token application.

Lock your Windows station. When you are on the locked screen, press space button or swipe with the mouse to have the following screen:

When your phone detects the computer you will see the following message on your computer:

At this time on your phone, you should be prompted to `Approve` or `Reject` the login request.

Click on `Approve` button and you are logged in.

7. Troubleshooting

7.1 Login/Enrollment Errors

If you encountered the following error during login or enrollment:

Check that no other devices (like a headset, earphones…), or any other devices which can consume a lot the Bluetooth bandwidth, are not connected to your smartphone over Bluetooth.

Windows policies must allow authentication with companion device. If you receive the below error, use `GPEdit.msc` to allow secondary authentication (`Local Computer Policy\Computer Configuration\Administrative Templates\Windows Components\Microsoft Secondary Authentication Factor\Allow`

7.2 Multiple Push received but login error

If you receive multiple push notifications on your Token for Proximity Login, and for all of them after few seconds, it's an automatic failure that means there is a timeout between the phone and the computer.

On the Windows side, the login screen is on that state:

For a proper login, the Windows login screen must be on that states with the message "Tap phone to sign in" to successfully login with Proximity.

7.3 Debug Mode

When the debug mode is enabled in the Proximity configuration, a log file is created at the following place:

```
C:\Users\<USER>\AppData\Local\Packages\bd01bd19-d124-49a4-8ce0-da850c3b7d91_pr788nnbe2qgy\LocalState\Log.txt
```

This log file is available only for the user who has installed the Proximity package.