



## MyID PIV

Version 12.11

# Windows Hello for Business Integration Guide

Lutterworth Hall, St Mary's Road, Lutterworth, Leicestershire, LE17 4PS, UK  
[www.intercede.com](http://www.intercede.com) | [info@intercede.com](mailto:info@intercede.com) | [@intercedemyid](https://twitter.com/intercedemyid) | +44 (0)1455 558111

## Copyright

© 2001-2024 Intercede Limited. All rights reserved.

Information in this document is subject to change without notice. The software described in this document is furnished exclusively under a restricted license or non-disclosure agreement. Copies of software supplied by Intercede Limited may not be used resold or disclosed to third parties or used for any commercial purpose without written authorization from Intercede Limited and will perpetually remain the property of Intercede Limited. They may not be transferred to any computer without both a service contract for the use of the software on that computer being in existence and written authorization from Intercede Limited.

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or any means electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Intercede Limited.

Whilst Intercede Limited has made every effort in the preparation of this manual to ensure the accuracy of the information, the information contained in this manual is delivered without warranty, either express or implied. Intercede Limited will not be held liable for any damages caused, or alleged to be caused, either directly or indirectly by this manual.

### Licenses and Trademarks

The Intercede® and MyID® word marks and the MyID® logo are registered trademarks of Intercede in the UK, US and other countries.

Microsoft and Windows are registered trademarks of Microsoft Corporation. Other brands and their products are trademarks or registered trademarks of their respective holders and should be noted as such. All other trademarks acknowledged.

### Apache log4net

Apache License Version 2.0, January 2004 <http://www.apache.org/licenses/>

#### TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

##### 1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

© You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions.

Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

Copyright [yyyy] [name of copyright owner]

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at

<http://www.apache.org/licenses/LICENSE-2.0>

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License. ---

## Conventions used in this document

- Lists:
  - Numbered lists are used to show the steps involved in completing a task when the order is important.
  - Bulleted lists are used when the order is unimportant or to show alternatives.
- **Bold** is used for menu items and for labels.

For example:

  - Record a valid email address in '**From**' email address.
  - Select **Save** from the **File** menu.
- *Italic* is used for emphasis:

For example:

  - Copy the file *before* starting the installation.
  - Do *not* remove the files before you have backed them up.
- ***Bold and italic*** hyperlinks are used to identify the titles of other documents.

For example: "See the ***Release Notes*** for further information."

Unless otherwise explicitly stated, all referenced documentation is available on the product installation media.
- A `fixed width` font is used where the identification of spaces is important, including filenames, example SQL queries and any entries made directly into configuration files or the database.
- **Notes** are used to provide further information, including any prerequisites or configuration additional to the standard specifications.

For example:

**Note:** This issue only occurs if updating from a previous version.
- Warnings are used to indicate where failure to follow a particular instruction may result in either loss of data or the need to manually configure elements of the system.

For example:

**Warning:** You must take a backup of your database before making any changes to it.

## Contents

<b>Windows Hello for Business Integration Guide</b>	<b>1</b>
<b>Copyright</b>	<b>2</b>
<b>Conventions used in this document</b>	<b>6</b>
<b>Contents</b>	<b>7</b>
<b>1 Introduction</b>	<b>8</b>
<b>2 Prerequisites</b>	<b>9</b>
2.1 Client operating system	9
2.2 MyID software	9
2.3 Controlling Windows Hello enrollment	9
2.4 Certificate policies	9
2.5 Hardware keystores	10
<b>3 Configuring MyID for Windows Hello</b>	<b>11</b>
3.1 Setting the Windows Hello configuration options	11
3.2 Creating the Windows Hello credential profile	11
3.2.1 Additional identities	13
3.2.2 Terms and conditions	13
3.3 Setting up Windows Hello for login	14
<b>4 Working with Windows Hello</b>	<b>15</b>
4.1 Requesting a Windows Hello credential	16
4.2 Collecting a Windows Hello credential	18
4.3 Erasing a Windows Hello credential	19
4.4 Canceling a Windows Hello credential	19
4.5 Updating a Windows Hello credential	20
4.5.1 Requesting an update for a Windows Hello credential	21
4.5.2 Reprovisioning a Windows Hello credential	21
<b>5 Troubleshooting</b>	<b>22</b>
5.1 Errors	22
5.2 Frequent questions	23
5.2.1 How do I test Windows Hello enrollment without MyID?	23
5.2.2 Why can't I see the Windows Hello option in the credential profile?	23
5.2.3 I've collected my certificates; why can't I log on to MyID using Windows Hello?	23
5.2.4 I've logged on to MyID using Windows Hello; why can't I see all my workflows?	24
5.2.5 How do I change or reset my Windows Hello PIN?	24
5.2.6 What happens if certificates that were issued by MyID are removed by other systems?	24
5.2.7 What happens to certificates issued by MyID when a destructive (or non-destructive) PIN reset happens on Windows Hello?	24
5.2.8 Why can't I see all the Windows Hello credentials on the computer in the Erase Card workflow?	25
5.2.9 Why does the Self-Service App or MyID Desktop say the device is not recognized?	25
5.2.10 What should I do if my computer DNS has changed?	25
5.3 Interoperability	26

## 1 Introduction

This manual describes how to set up MyID® to integrate with Windows Hello for Business.

Windows Hello for Business is a two-factor credential that provides a more secure alternative to passwords. Cryptographic keys are stored on your Windows PC; Windows Hello for Business allows you to access these keys through your configured authentication methods (PIN, facial biometrics, fingerprints, and so on) and thereby authenticate securely to your systems.

**Note:** MyID does not provide any configuration or management of the Windows Hello authentication methods – this is part of your Windows configuration. See your Microsoft documentation for details.

MyID allows you to set up Windows Hello credentials; you can specify which certificates you want to issue to the PC, request Windows Hello credentials for a specified user, and then collect the Windows Hello credentials onto a Windows PC using the MyID Self-Service App.

Once you have issued Windows Hello credentials to a PC, you can manage the lifecycle of the issued credentials; you can update the credentials, reprovision them entirely, or erase the certificates.

MyID can issue certificates to a new or existing Windows Hello credential; for an existing Windows Hello credential, MyID adds its certificates to those already present. MyID then manages its own certificates; it does not manage certificates added to Windows Hello by any other system.

You can also configure MyID to allow you to log on to your MyID system using your Windows Hello credentials as a logon mechanism.

**Note:** If you have configured Windows Hello to use the "Certificate Trust Model", MyID will not manage the primary authentication certificate used by Windows Hello. This is because Microsoft manages this certificate as part of the Windows Hello for Business infrastructure, and it is not currently possible for third-party systems such as MyID to take over this management. MyID can provide additional authentication, signing, and encryption certificates to Windows Hello; this allows you to use your own PKI and business processes for these certificates.



## 2 Prerequisites

Your system must be set up for Windows Hello for Business. MyID can manage the issuance of certificates to Windows Hello for Business credentials, but does not manage your Windows Hello for Business infrastructure.

Consult your Microsoft documentation for details of setting up Windows Hello for Business. The Microsoft docs website has a detailed guide:

- Docs / Windows Security / Identity and access protection / Windows Hello for Business

### 2.1 Client operating system

MyID's integration with Windows Hello for Business requires Windows 10 April 2018 Update (build 1803) or greater.

**Note:** To collect, update, or erase certificates to a Windows Hello for Business credential, you must be logged on to the PC directly – you cannot carry out these operations over a remote desktop connection.

### 2.2 MyID software

You must have the MyID Self-Service App installed on the client PC. This allows you to collect or update the Windows Hello credential.

If you want to be able to erase or reprovision a Windows Hello credential, you must also have MyID Desktop installed on the client PC.

### 2.3 Controlling Windows Hello enrollment

When the Microsoft group policy "Use Windows Hello for Business" is enabled, an additional option is available: "Do not start Windows Hello provisioning after sign-in". When this option has been selected, automatic enrollment when users log in to Windows is prevented. This allows MyID to start enrollment after appropriate processes have taken place, such as a self-service enrollment for derived credentials, or a request being created by a MyID operator.

### 2.4 Certificate policies

You must make sure that the certificate policies you select are suitable for Windows Hello.

- Support for ECC certificates with Windows Hello

Windows may prevent certain certificates policies from being used; for example, certificates with Elliptic Curve keys. Limitations may be dependent on the hardware configuration of the computer in use. Before deploying to production environments, you must validate the compatibility of the required certificate policies with Windows Hello.

## 2.5 Hardware keystores

Windows Hello may not use a TPM in some circumstances, depending on the capability of the computer and group policy configuration.

Wherever possible, Windows Hello for Business takes advantage of trusted platform module (TPM) 2.0 hardware to generate and protect keys. However, Windows Hello for Business does not require a TPM. Administrators can choose to allow key operations in software.

MyID treats Windows Hello as a hardware key store – this means that certificate policies that are configured in MyID to issue or recover to hardware will permit recovery to Windows Hello whether or not it is using a TPM. You must ensure that your Windows Hello configuration is appropriate to meet the key protection requirements of your certificate policies.

## 3 Configuring MyID for Windows Hello

To configure MyID for Windows Hello, you must set up the following:

- Set the Windows Hello configuration option.  
See section [3.1, \*Setting the Windows Hello configuration options\*](#).
- Create a Windows Hello credential profile.  
See section [3.2, \*Creating the Windows Hello credential profile\*](#).
- Optionally, set up Windows Hello as a logon mechanism for authenticating to MyID.  
See section [3.3, \*Setting up Windows Hello for logon\*](#).

### 3.1 Setting the Windows Hello configuration options

The **Windows Hello for Business supported within MyID** configuration option determines whether you can create or edit credential profiles for Windows Hello.

To allow MyID to issue Windows Hello:

1. From the **Configuration** category, select **Operation Settings**.
2. On the **Devices** tab, set the following:
  - **Windows Hello for Business supported within MyID** – ensure this option is set to **Yes**.
3. Click **Save changes**.

### 3.2 Creating the Windows Hello credential profile

**Important:** The **Windows Hello** option in the credential profile appears only when you have set the **Windows Hello for Business supported within MyID** configuration option. See section [3.1, \*Setting the Windows Hello configuration options\*](#) for details.

To set up a credential profile for Windows Hello:

1. From the **Configuration** category, select **Credential Profiles**.
2. Click **New**.
3. Type a **Name** and **Description**.

4. In the **Card Encoding** section, select **Windows Hello**.

The screenshot shows the 'Credential Profile' configuration interface. On the left, a sidebar lists various sections: Card Encoding (highlighted), Services, Issuance Settings, Self-Service Unlock Authentication, PIN Settings, PIN Characters, Biometric Settings, Mail Documents, Credential Stock, Device Profiles, and Authentication Types. The main content area has fields for 'Name', 'Description', and 'Device Friendly Name'. Below these is the 'Card Encoding' section, which contains a list of options: Contact Chip, Contactless Chip, Microsoft Virtual Smart Card, Magnetic Stripe (Only), Software Certificates (Only), Device Identity (Only), Identity Agent, Externally Issued (Only), Derived Credential, and Windows Hello (checked). A 'Next' button is located at the bottom right.

**Note:** You can also select the **Derived Credential** option if you want to issue certificates to Windows Hello as a derived credential through the Derived Credentials Self-Service Portal. For more information, see the *Creating a Windows Hello credential profile* section in the [Derived Credentials Self-Service Request Portal](#) guide.

5. In the **Services** section, select **MyID Logon** and **MyID Encryption**.
6. In the **Mail Documents** section, set up any mailing documents you may want to issue.  
See the *Mail Documents* section in the [Administration Guide](#) for details.
7. Click **Next**.
8. On the Select Certificates screen, select the certificates you want to issue to the Windows Hello credential.  
**Note:** You must use a certificate for **Signing** and **Encryption**; you cannot use MyID keys for signing and encryption operations on Windows Hello credentials.  
For more information on this screen, see the *Selecting certificates* section in the [Administration Guide](#).  
See also section 2.4, [Certificate policies](#).
9. Click **Next** and proceed to the Select Roles screen.  
See the *Linking credential profiles to roles* section in the [Administration Guide](#) for details.
10. Click **Next** and complete the workflow.  
You do not need to specify any card layouts.

### 3.2.1 Additional identities

In the credential profile, you can configure additional identities; certificates for any additional identities that have been set up for the end user are written to the Windows Hello credential at issuance.

This allows a user to have certificates for a different associated identity protected by their primary Windows Hello credentials; for example, you do not need to have a separate enrolled Windows Hello credential on the computer for an administrator account.

You can use additional identity certificates for signing and encryption, but they are not offered for logon or unlocking.

**Note:** The additional identity certificates use the Windows Hello authenticated state. If the user has not previously authenticated using Windows Hello during the current logon session, there will be a single Windows Hello authentication request. You are recommended to use this feature only when it aligns with your organization's own security policies.

For more information, see the *Additional identities* section in the [Administration Guide](#).

### 3.2.2 Terms and conditions

You can configure a credential profile for Windows Hello that requires the user to accept terms and conditions when the Windows Hello credential is issued or updated. With other credential types (for example, smart cards) the cardholder must authenticate to their credential with their PIN to sign the terms and conditions; with Windows Hello, the user does not have to authenticate to Windows Hello again, as they are already authenticated to the credential.

For more information on configuring terms and conditions, see the *Issuance Settings* section in the [Administration Guide](#).

### 3.3 Setting up Windows Hello for logon

You can configure MyID to use Windows Hello as a logon mechanism. This means that you can log on to the MyID system using your Windows Hello for Business credentials.

To set up Windows Hello logon:

1. From the **Configuration** category, select **Security Settings**.
2. On the **Logon Mechanisms** tab, set the following:
  - **Windows Hello Logon** – set this option to **Yes**.
3. Click **Save changes**.
4. From the **Configuration** category, select **Edit Roles**.
5. Click **Logon Methods**.

Logon Mechanisms

	Password	Smart Card	Windows Logon	Biometric Logon	Windows Hello
Cardholder (1)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Manager (2)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Security Chief (3)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Personnel (4)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Help Desk (6)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Contractor (20)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Foreign (21)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Emergency (22)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Signatory (23)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Adjudicator (24)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Admin (25)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Applicant (101)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Issuer (102)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Security Officer (103)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Registrar (104)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Sponsor (105)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Default SSA User (981)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
IdentityAgentEnrolled (982)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

OK

6. For each role you want to be able to log on using their Windows Hello for Business credentials, select the option in the **Windows Hello** column.
7. Click **OK**.
8. Click **Save Changes**.

## 4 Working with Windows Hello

MyID allows you to request, collect, erase, and update certificates on Windows Hello credentials.

**Important:** To carry out any operation on Windows Hello credentials (for example, collecting or erasing certificates) you must be logged on to Windows as the owner of the Windows Hello credential you want to work with. Even if the physical PC contains Windows Hello credentials for multiple Windows users, you can view and work only with your own Windows Hello credentials.

- Request certificates for a Windows Hello credential.  
See section [4.1, Requesting a Windows Hello credential](#).
- Collect certificates onto a Windows Hello credential.  
See section [4.2, Collecting a Windows Hello credential](#).
- Erase certificates from a Windows Hello credential.  
See section [4.3, Erasing a Windows Hello credential](#).
- Canceling certificates remotely from a Windows Hello credential.  
See section [4.4, Canceling a Windows Hello credential](#).
- Update certificates on a Windows Hello credential.  
See section [4.5, Updating a Windows Hello credential](#).

## 4.1 Requesting a Windows Hello credential

You can use the Request Device feature in the MyID Operator Client to request a Windows Hello credential for someone, who can then use the Self-Service App to collect the certificates onto their own PC.

**Note:** Do not attempt to use more than one MyID system to request certificates for the same Windows Hello credential; you will be unable to log on to the original MyID system using Windows Hello authentication if you collect certificates from a different MyID system onto your Windows Hello credential.

**Note:** You can also use the **Request Card** workflow in MyID Desktop to request a Windows Hello credential. See the *Requesting a card* section in the [Operator's Guide](#) for details.



To request a Windows Hello credential:

1. In the MyID Operator Client, search for a person, and view their details.

See the *Searching for a person* section in the [MyID Operator Client](#) guide for details of using the search form.

You can also view a person's details from any form that contains a link to their account.

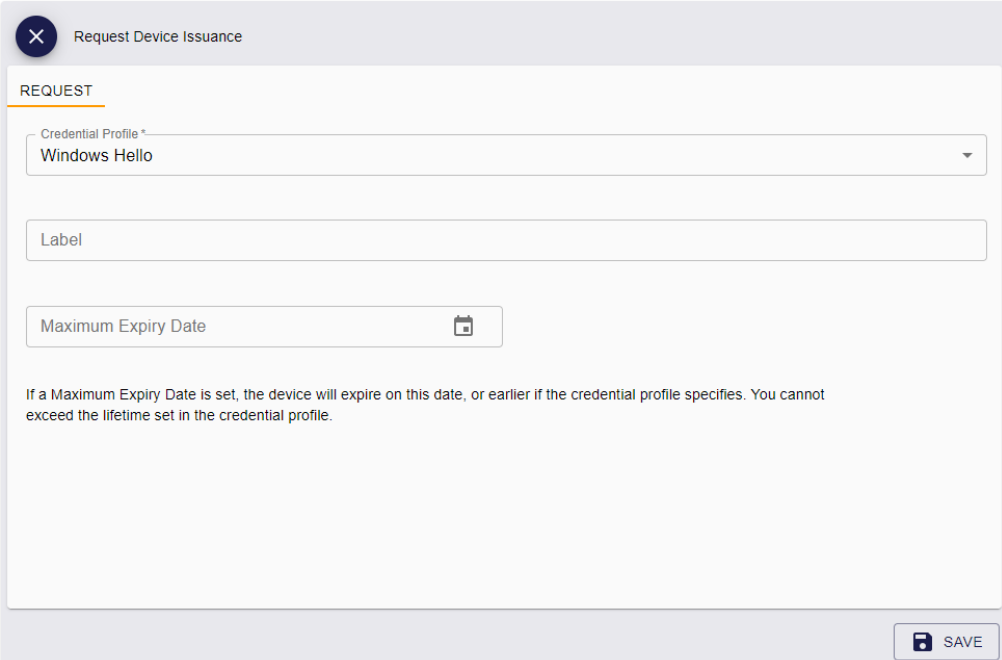
For example:

- Click the link icon  on the **Full Name** field of the View Request form.
- Click the link icon  on the **Owner** field of the View Device form.

2. Click the **Request Device** option in the button bar at the bottom of the screen.

You may have to click the ... option to see any additional available actions.

The Request Device Issuance screen appears:





3. From the **Credential Profile** drop-down list, select a credential profile that has been set up for Windows Hello.

See section [3.2, Creating the Windows Hello credential profile](#) for details.

4. Optionally, in the **Label** box, type a label for this request.

You can use the label to search for the request:

- In the Requests search form, select **Label** from the additional search criteria.

See the *Searching for a request* section in the [MyID Operator Client](#) guide.

- In the **Job Management** workflow in MyID Desktop, use the **Batch Label** box.

See the *Searching for jobs* section in the [Administration Guide](#).

5. Optionally, set the **Maximum Expiry Date**.

This option is available only if the **Set expiry date at request** option (on the **Issuance Processes** page of the **Operation Settings** workflow) is set to **Yes**.

See the *Requesting a device for a person* section in the [MyID Operator Client](#) guide for details of device expiry dates.

6. Click **Save** to make the request.

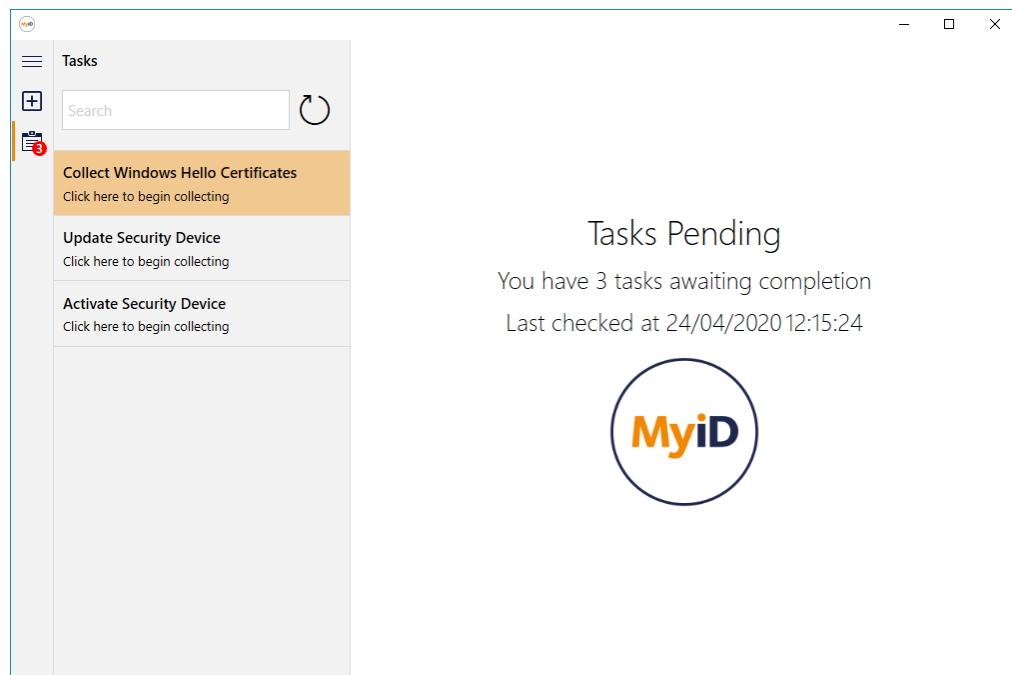
## 4.2 Collecting a Windows Hello credential

Once a Windows Hello credential has been requested, you can collect it onto your PC using the MyID Self-Service App.

To collect a Windows Hello credential:

1. Log on to the PC onto which you want to collect the Windows Hello credential.
2. Launch the MyID Self-Service App.

The Self-Service App checks your user account, and displays a list of the pending tasks; for example, collection or update jobs.



3. Click the **Collect Windows Hello Certificates** task and follow the on-screen prompts.

If you do not already have a Windows Hello credential, the Windows Hello enrollment procedure starts, allowing you to configure a PIN and fingerprint or facial biometrics as authentication mechanisms.

If you already have a Windows Hello credential, and have not already authenticated to Windows Hello, you must enter your PIN or provide your biometrics.

**Note:** The prompt to authenticate to Windows Hello appears in the taskbar rather than as a pop-up over the Self-Service App window; click the flashing icon to authenticate.

### 4.3 Erasing a Windows Hello credential

You can use the **Erase Card** workflow in MyID Desktop to remove the certificates from a Windows Hello credential. Only certificates that were issued by MyID are affected.

**Note:** You do not need to authenticate to Windows Hello to remove the certificates; Windows Hello does not require any authentication for this action. You do, however, need to be logged on to Windows as the owner of the Windows Hello credential.

To erase certificates from a Windows Hello credential:

1. Log on to the PC as the owner of the Windows Hello credentials.
2. Launch MyID Desktop and log on to the MyID server.
3. From the **Cards** category, select **Erase Card**.
4. From the list of cards, select your Windows Hello credential.
5. Click **Next**, and complete the workflow.

See the *Erasing a card* section in the [Operator's Guide](#) for details.

When you click **Erase**, MyID removes any certificates from the card that were issued by the current MyID system.

### 4.4 Canceling a Windows Hello credential

You can use the **Erase Card** workflow to remove the certificates from a Windows Hello credential on the local PC; however, this is only possible if you can log on to Windows as the owner of the Windows Hello credential.

If you cannot access the Windows Hello credential directly, you can use the Cancel Device option in the MyID Operator Client to cancel the owner's access to MyID and revoke the certificates that were issued to Windows Hello.

This does not *remove* the certificates from the PC, but *revokes* them on the certificate authority so they are no longer valid. You can then use Microsoft tools to remove the certificates from the Windows Hello credential; you can configure a group policy to remove revoked certificates from Windows Hello – see the Microsoft Windows Hello documentation for details.

**Note:** You can also use the **Cancel Credential** workflow in MyID Desktop to cancel a Windows Hello credential. See the *Canceling a credential* section in the [Operator's Guide](#) for details.

To cancel a Windows Hello credential:


1. Search for a device, and view its details.

From the **Device Type** drop-down list on the search form, select **Windows Hello**.

See the *Searching for a person* section in the [MyID Operator Client](#) guide for details of using the search form.

You can also view a device from any form that contains a link to the device.

For example:

- Click the item in the list on the **Devices** tab of the View Person form.
- Click the link icon  on the **Device Serial Number** field of the View Request form.

2. Click **Cancel Device** option in the button bar at the bottom of the screen.  
You may have to click the ... option to see any additional available actions.  
The Cancel Device screen appears.

Cancel Device

**CONFIRM DETAILS**

Provide the reason and any additional notes for carrying out this action. The reason you provide will affect subsequent actions that take place.

Reason \*

Required

Notes

Disposal Status

SAVE

3. Select the **Reason** for the cancellation from the drop-down list.  
This reason affects how MyID treats the certificates on the Windows Hello credential.  
See the *Certificate reasons* section in the [Operator's Guide](#) for details of how each reason affects the certificates.
4. Type any **Notes** on the cancellation.  
You can provide further information on your reasons for canceling the Windows Hello credential. This information is stored in the audit record.
5. Click **Save**.

## 4.5 Updating a Windows Hello credential

Once you have issued a Windows Hello credential, you can update the certificates if necessary.

If you have set the certificates for automatic renewal, MyID creates a job to renew the certificate when it comes within a specified number of days of expiry. You can collect the renewed certificates using the Self-Service App – if there are any certificate renewal jobs for your Windows Hello credential, they appear in the task list.

See the *Certificate renewal* section in the [Administration Guide](#) for details.

Alternatively, you can request an update for the certificates on the credential manually, or even reprovision the entire Windows Hello credential. Reprovisioning removes any existing certificates and writes a new set to the credential.

#### 4.5.1 Requesting an update for a Windows Hello credential

An operator can request an update for another person's Windows Hello credential; the credential owner can then use the Self-Service App to carry out the update.

To request an update for a Windows Hello credential:

1. From the **Cards** category, select **Request Card Update**.
2. Click **Search**.
3. Use the Find Person screen to search for the owner of the Windows Hello credential you want to update.
4. If the person has more than one issued device, select their Windows Hello credential from the list.
5. Select the type of update and the reason for the change from the options provided.  
See the *Requesting a card update* section in the [Operator's Guide](#) for details of the options and their effects.
6. Click **Continue**.

MyID creates a job to update the Windows Hello credential. Depending on the options you selected, this may be a simple update or a full reprovision. Use the Self-Service App to update the credential.

#### 4.5.2 Reprovisioning a Windows Hello credential

An operator can reprovision a Windows Hello credential directly using MyID Desktop.

To reprovision a Windows Hello credential:

1. From the **Cards** category, select **Reprovision Card**.  
You can also use the **Reprovision My Card** workflow, which restricts you to Windows Hello credentials that were issued to the logged-on MyID operator account.
2. In the Select Card dialog, select the Windows Hello credential.
3. Select the reason for the change from the options provided.  
See the *Reprovisioning cards* section in the [Operator's Guide](#) for details of the options.
4. Click **Next**.
5. Click **Continue**.

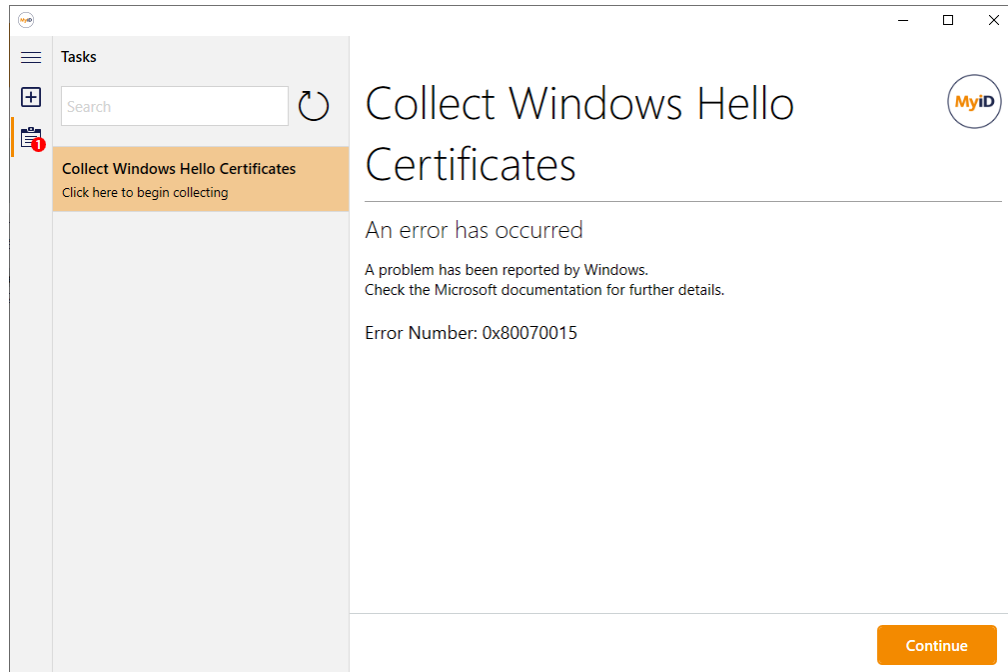
If you have not already authenticated to Windows Hello, you must enter your PIN or provide your biometrics. MyID then removes the existing certificates from the Windows Hello credential and writes new certificates.

## 5 Troubleshooting

This section contains information about errors that may occur, and answers to questions that are frequently asked.

### 5.1 Errors

MyID Desktop and the Self-Service App pass on any Windows errors that are produced by Windows Hello; for example:



Error number `0x80070015` is a general Windows error that means the device was not ready; you can check the following locations for more information on what may have caused the error:

- The MyID audit log
- Windows Event Viewer

See your Microsoft documentation for details of these errors.

The following additional errors may occur:

- 890599 – Failed to detect the Windows Hello reader.

Enrollment was reported as completing successfully, but MyID could not detect the Windows Hello device.

Check the Windows event log. If you have a persistent issue, see the *MyID Client Components* section in the [Configuring Logging](#) guide for information on how to enable MyID client logging for the `WHFB` (Windows Hello for Business) component.

- 890600 – An unknown error occurred with Windows Hello for Business.

This error is unexpected.

Check the Windows event log. If you have a persistent issue, see the *MyID Client Components* section in the [Configuring Logging](#) guide for information on how to enable MyID client logging for the `WHFB` component.

- 890601 – Cannot perform this operation over a remote desktop connection.

Windows Hello for Business is not supported over RDP.

Make sure you are logged on directly to the PC you want to work with.

- 890493 – An unknown error has occurred.

This may be caused by an attempt to issue certificates that are not suitable for Windows Hello. See section [2.4, Certificate policies](#).

- -9990003 – Certificate Issuance.

This may also be caused by an attempt to issue certificates that are not suitable for Windows Hello. See section [2.4, Certificate policies](#).

## 5.2 Frequent questions

This section contains answers to some questions that frequently occur.

### 5.2.1 How do I test Windows Hello enrollment without MyID?

Once you have configured your Windows Hello for Business infrastructure according to the instructions from Microsoft, to make sure that a user can carry out Windows Hello enrollment, in Windows go to **Settings > Accounts > Sign-in options** and select **Windows Hello PIN**. This takes you through the Windows Hello enrollment process without using MyID.

### 5.2.2 Why can't I see the Windows Hello option in the credential profile?

The **Windows Hello** option in the credential profile appears only when you have set the **Windows Hello for Business supported within MyID** configuration option.

See section [3.1, Setting the Windows Hello configuration options](#) for details.

### 5.2.3 I've collected my certificates; why can't I log on to MyID using Windows Hello?

You have to configure MyID to use Windows Hello as a logon mechanism. You must set the **Windows Hello** option on the **Logon Mechanisms** tab of the **Security Settings** workflow, and then use the **Edit Roles** workflow to configure one or more roles to use Windows Hello as its logon mechanism.

See section [3.3, Setting up Windows Hello for logon](#) for details.

#### 5.2.4 I've logged on to MyID using Windows Hello; why can't I see all my workflows?

The workflows that appear when you have logged on using Windows Hello depend on which roles you have selected that have Windows Hello as their logon mechanism; for example, you may have the following roles, providing access to different workflows:

- Cardholder – **Change My Security Phrases, Unlock My Security Phrases.**
- Operator – **View Person, Edit Person.**

If only the Operator role has Windows Hello assigned as a logon mechanism, when you log in to MyID using Windows Hello, you will only be able to see **View Person** and **Edit Person**. To see all of your workflows, make sure that the Cardholder role *also* has Windows Hello assigned as a logon mechanism.

#### 5.2.5 How do I change or reset my Windows Hello PIN?

You cannot change or reset your Windows Hello PIN using MyID Desktop or the Self-Service App. Instead, in Windows, go to **Settings > Accounts > Sign-in options** and select **Windows Hello PIN**.

#### 5.2.6 What happens if certificates that were issued by MyID are removed by other systems?

This should not occur, but certificates may be revoked externally to MyID. If this happens, an administrator can request an update for your Windows Hello credentials using the **Request Card Update** workflow and the reason "There is a problem with the device". This creates an update that you can collect using the Self-Service App. Alternatively, the administrator can use the **Cancel Credential** workflow to revoke the certificates, then repeat the issuance process.

#### 5.2.7 What happens to certificates issued by MyID when a destructive (or non-destructive) PIN reset happens on Windows Hello?

If a destructive PIN reset or any other process that completely resets Windows Hello occurs, you are recommended to cancel the previous credentials issued by MyID using the **Cancel Credential** workflow and repeat the original issuance process. You cannot simply reprovision the Windows Hello credential, as the serial number used by MyID to recognize Windows Hello on the computer will have changed. If the removed certificates persist in the user certificate store, you can refresh the certificate store using Microsoft tools such as PowerShell. You can trigger PowerShell scripts when the Self-Service App completes an activity - see the *Triggered scripts* section in the [Administration Guide](#) for details.

See the Microsoft documentation on Windows Hello for more information about destructive and non-destructive PIN reset.



### 5.2.8 Why can't I see all the Windows Hello credentials on the computer in the Erase Card workflow?

MyID cannot access Windows Hello containers on the computer that belong to user accounts other than the current logged-on Windows user. If you need to remove certificates issued by MyID and cannot access the required Windows user account, you are recommended to use **Cancel Credential** workflow in MyID to revoke all certificates issued by MyID, then use Microsoft tools to remove the certificates from Windows Hello.

See section [4.4, \*Canceling a Windows Hello credential\*](#) for details.

### 5.2.9 Why does the Self-Service App or MyID Desktop say the device is not recognized?

A process external to MyID may have caused Windows Hello to be reset; for example, if a destructive PIN reset has taken place. This causes the serial number, which is used by MyID to identify the Windows Hello instance on the computer, to change. This is likely to have also removed any certificates issued by MyID. You are recommended to cancel then reissue the previous credentials.

### 5.2.10 What should I do if my computer DNS has changed?

During collection of the certificates, MyID records the computer DNS and stores this information within the MyID database. This forms part of the audit record, and also is used to check for updates to the certificates on the computer, as the user may have credentials on other computers as well.

If the DNS of the computer changes, identification of any pending updates fails and no notification is received by the user. In this case, you must cancel and reissue the credentials on the computer. If you require further assistance when this occurs, contact Intercede quoting SUP-330.

## 5.3 Interoperability

During development and testing of this feature, some behaviors of Windows Hello were observed which may affect your experience with this solution. These issues are not always reproducible and have been seen when using Windows Hello without MyID software installed. Also, they may be specific to certain computers, environmental configurations, or the build of Windows in use. This is not a comprehensive list, and you are recommended to use Microsoft online resources for further troubleshooting guidance on these issues. Further information about these issues is also available on the Intercede customer portal.

- Unable to enroll Windows Hello for Business when logged on to the computer with a Microsoft Virtual Smart Card (VSC) or physical smart card

During enrollment of Windows Hello, it was not possible to set the PIN. An error was displayed in the Windows Hello enrollment user interface. This issue has been observed when attempting to upgrade from a VSC to Windows Hello. This may affect customers who are using MyID to trigger Windows Hello enrollment in this scenario. The issue also occurred when triggering enrollment of the PIN from the Windows control panel.

- Windows Credential UI graphical issues during enrollment

When authentication factors are enrolled for Windows Hello, the credential UI displayed by Windows has occasionally seen to be malformed. For example, control buttons may be partially hidden by Windows task bar during fingerprint enrollment, or missing buttons on the form. These have been observed when there is no MyID software installed as well as when enrollment is triggered by MyID.