MyID PIV

Version 12.10

Operator's Guide

Lutterworth Hall, St Mary's Road, Lutterworth, Leicestershire, LE17 4PS, UK
www.intercede.com | info@intercede.com | @intercedemyid | +44 (0)1455 558111

Document reference: OPR1983-12.10.0-PIV

April 2024

Copyright

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

1 Introduction

MyID® is used to issue and maintain credentials that can be used to identify an individual. The credentials issued by MyID may contain personal information, digital certificates and applets. Smart cards may also include visual identification features; for example, a photograph of the holder or a distinctive background that indicates the holder belongs to a particular group.

This manual provides details of day-to-day operations, including:

- Adding, viewing, editing, and removing people records.
- Requesting, issuing, and managing smart cards.
- Working with certificates.
- Working with images.
- Running reports.

For information about administering MyID, see the ***Administration Guide***.

For an overview of the interface and the controls it contains, see section *2.2*, *The interface*.

2 Getting started

This chapter contains general information on MyID, including:

- How to log on to MyID Desktop for the first time.
- Default security settings.
- Information on the MyID Desktop interface.
- MyID terminology.

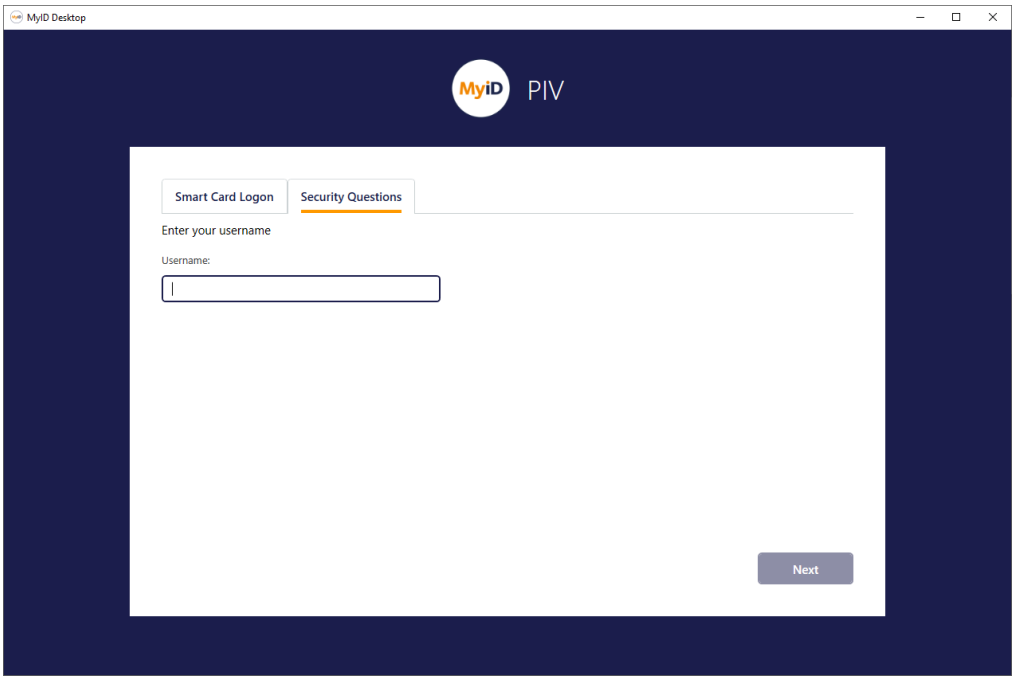
For information on launching MyID Desktop, see the *Launching MyID Desktop* section in the ***Installation and Configuration Guide***.

2.1 Logging on to MyID

You can log on to MyID Desktop using:

- Smart card logon (using a smart card and a PIN)
- Security Questions (a logon name and up to five passwords)
- Windows logon (using your Windows account to authenticate to MyID)

Your administrator may have enabled more than one method of accessing MyID. For example, your usual logon method may be to use your smart card, but your administrator may allow you to log on using security questions in case you have lost or forgotten your smart card. For more information, see the *Logon mechanisms* section in the ***Administration Guide***.

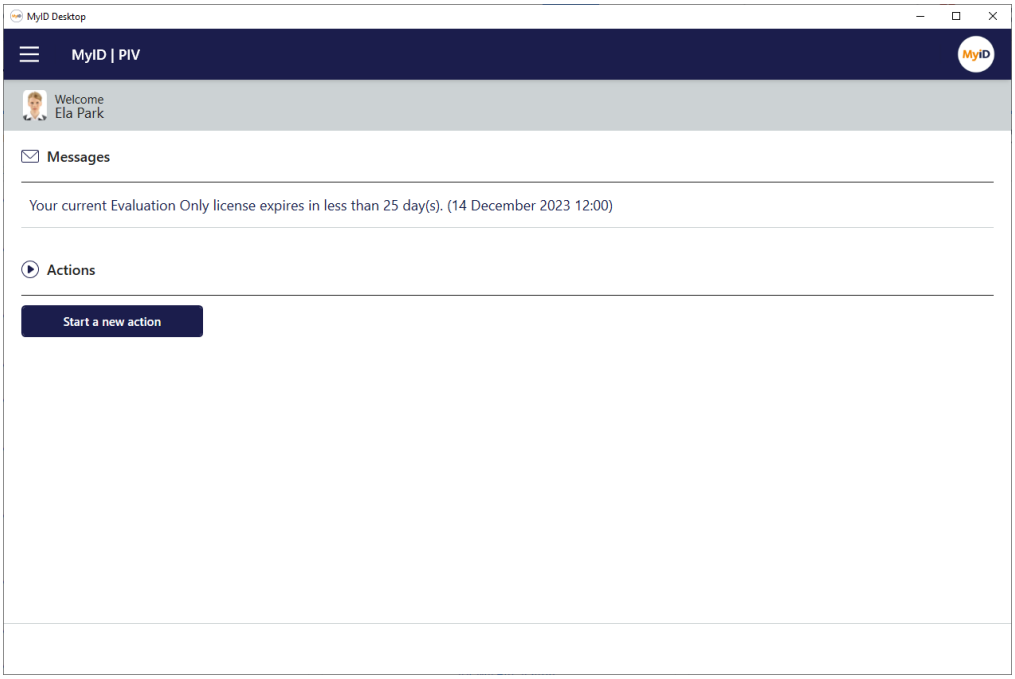


Click the tab for the logon method you want to use, then follow the on-screen instructions.

2.2 The interface

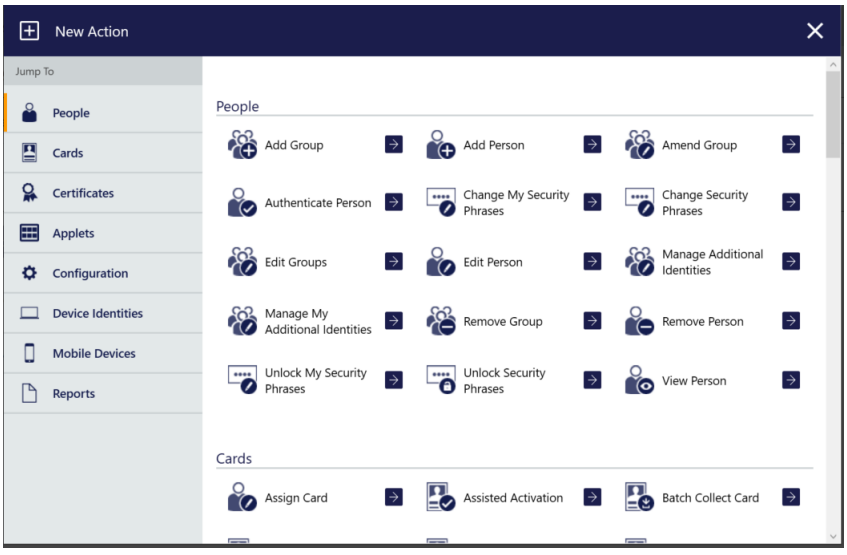
Note: A detailed explanation of the terminology used within MyID and this document is provided in section *2.3*, *Terminology*.

When you first log on to MyID Desktop, the system will look similar to the following:



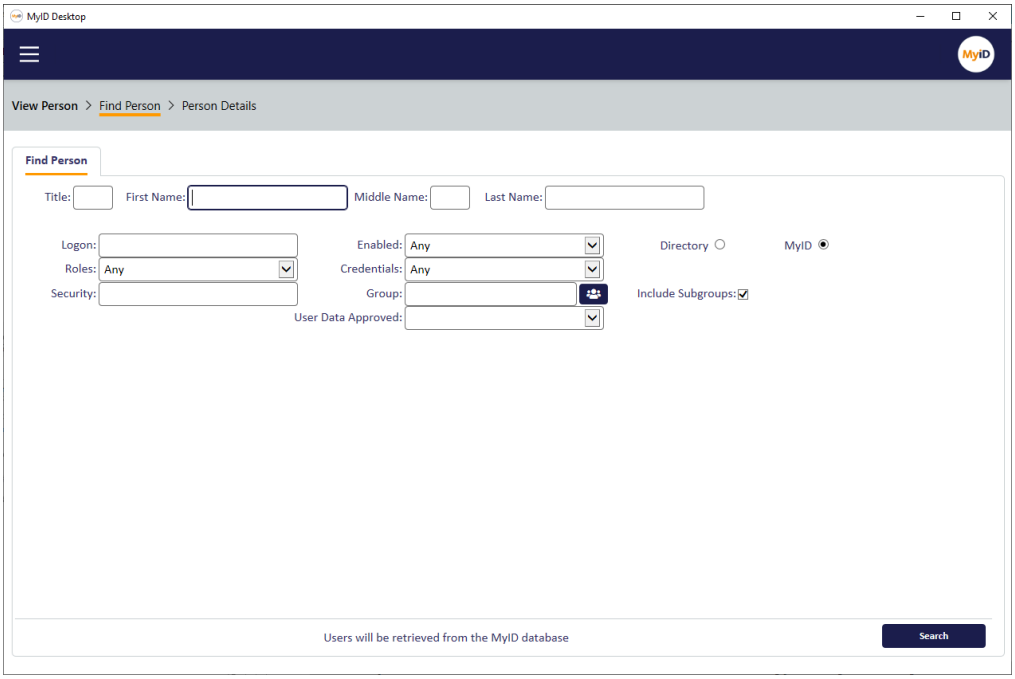
If there are any system messages, they appear at the top of the screen. For some messages, you can click the arrow to take you to the appropriate workflow; for example, if your system is not set up for production use, clicking the arrow takes you to the **Security Settings** workflow to allow you to set up your security options for production use; if your system's license is expiring soon, clicking the arrow takes you to the **Licensing** workflow.

To access a workflow, click **Start a new action**.



The list of categories and workflows will be tailored for you according to your role, the configuration of your system, and the edition of MyID you have installed; fewer categories and options within these categories are shown if you have a lower level of access.

Workflows guide you through the steps of a task. For example, to view the details of a person in the system, from the **People** category, select the **View Person** workflow. Each workflow comprises a series of stages and MyID automatically moves from one stage to the next in the correct order.



A form is displayed for each stage. Some forms, such as the **Person Details** form, consist of a number of named tabs.

Warning: If you restart the current workflow, or start a different workflow, before saving your changes, the changes are lost.

In addition to the standard Windows controls (select lists, text boxes and text areas, radio buttons and checkboxes), MyID uses a graphical representation of a checkbox that shows one of two or three states (**Ask** is not always applicable). You may be able to click the image to toggle between the available states.

Enabled, **True** or **Yes**

Disabled, **No** or **False**

Ask or **Prompt**

An information icon may provide additional information about a topic in the form of a tooltip.

You can use navigation buttons to move through pages of information. The buttons available depend on how many pages are available, which one you are currently viewing and whether you are viewing the results of a search:

 Show first page of information.

 Show last page of information.

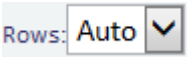
 Show previous page of information.

 Show next page of information.

 Show next block of information.

 Show only results.

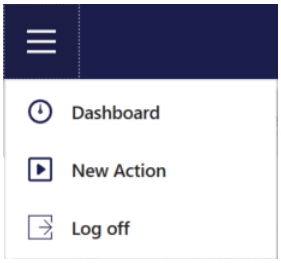
 Show search criteria.



Change the number of rows displayed.

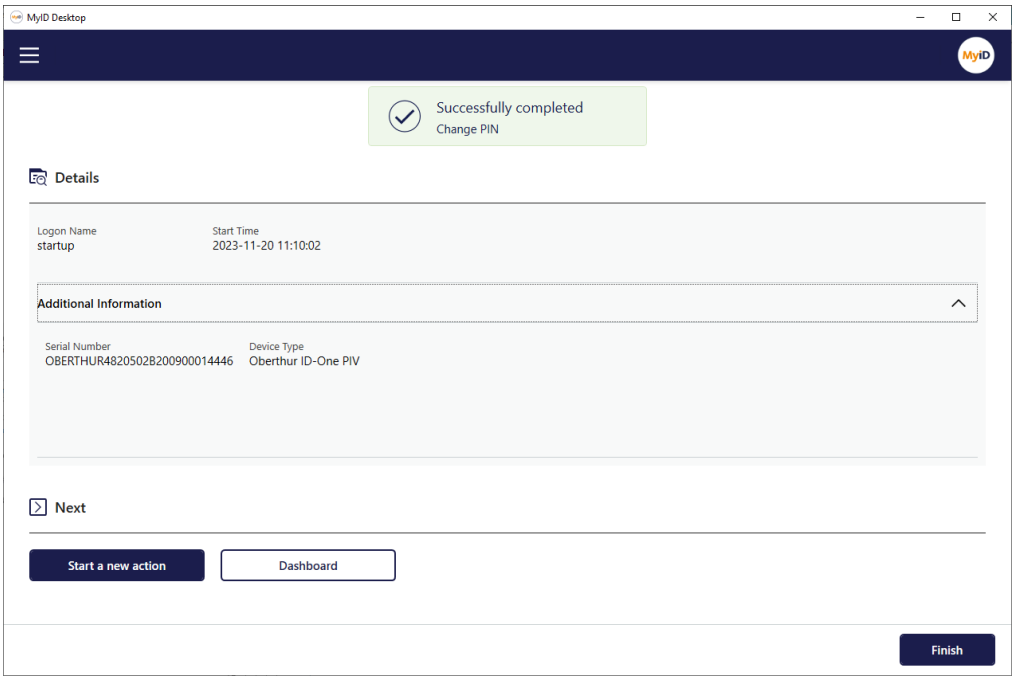
Note: Information displayed in a table can be sorted in ascending or descending order, based on a selected heading. Click a heading to sort by that value; click it again to reverse the sort order.

To return to the dashboard, start a new action, or log off, click the menu button at the top left.

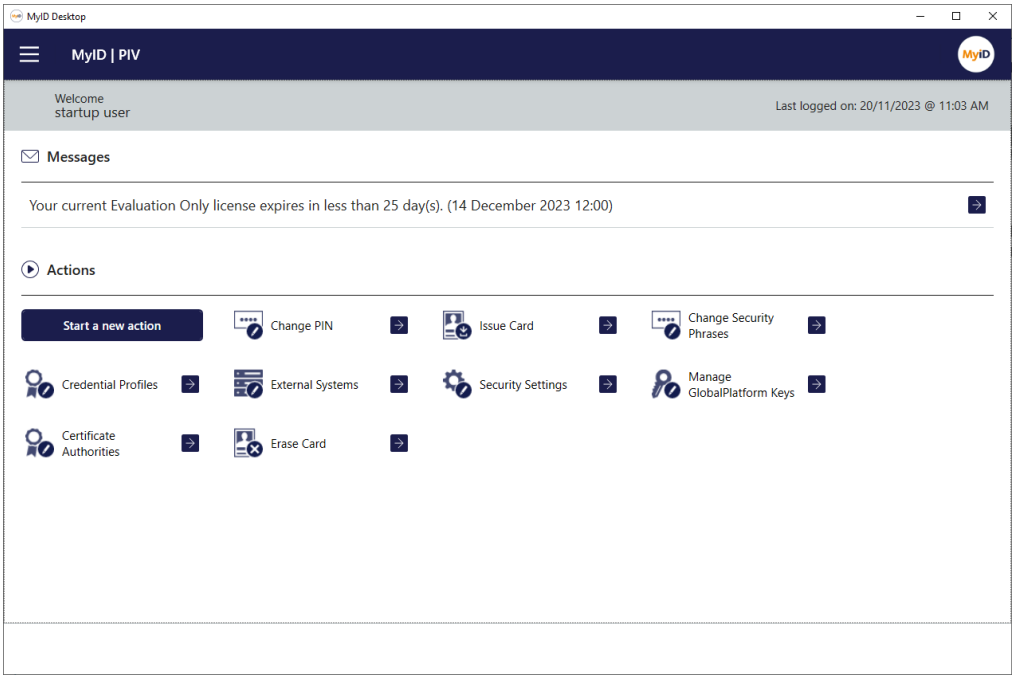


You can return to the dashboard when you are in a workflow, and you can start a new action when you are on the dashboard.

When you complete a workflow, the confirmation screen appears. This screen displays information for the workflow you have just completed. For some workflows, the **Checks Made** section displays any checks that occurred.



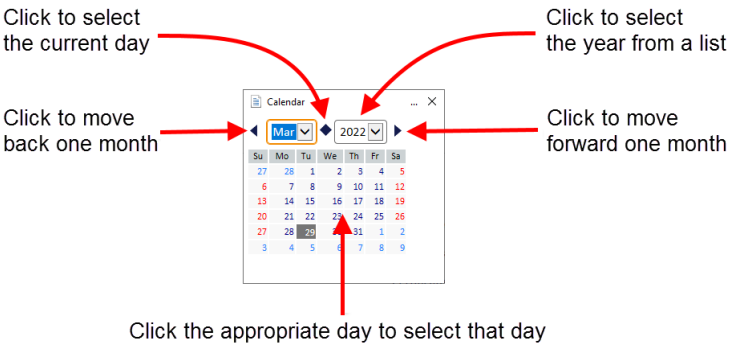
As you work with MyID, your most recent workflows will appear on your dashboard:



2.2.1 Selecting dates

Various workflows in the system allow you to enter a date. The date control works in the same way in all workflows.

To select a date, click the calendar button next to the field:



2.2.2 Entering search criteria

The method used for entering search criteria depends on the workflow you use. Some workflows use wildcard searching; in this case, this is detailed in the procedure for using that workflow.

Other workflows use a more sophisticated form of searching. In this case, the procedure for using the workflow contains a link to this section.

When searching within the search box, any criteria entered are automatically used as prefix criteria in a full text search against the logon name and full name fields.

For example, typing `sam` will find any users for whom an element of their logon name or full name *starts with* `sam`.

For example:

- `Samuel Smith`
- `John Samson`
- `Sam.jones@mycompany.com`

Note: It will *not* find the criteria within an element; for example:

- `MySam Jones`

You can enter multiple criteria, in which case a prefix match must be found in one of the fields for each criteria.

For example, `sam jon` will find:

- `Samuel Jones`
- `Jonathon Samson`

But not:

- `Sam Littlejohn`

Note: The prefix search applies to each element of the field. Fields are split up by any non-alphanumeric character with the exception of apostrophes.

For example, you can find `sam.jones@mycompany.com` using:

- `Sam`
- `Jones`
- `companycom`

Or any prefix of those elements.

You can find `John O'Reilly` using:

- `John`
- `O'Reilly`

But not:

- `Reilly`

You can find `Ralph Fiennes-Johnson` using:

- `Ralph`
- `Fiennes`
- `Johnson`

You can find any accented characters using their plain equivalent.

For example, you can find `Heinz Müller` using:

- `Heinz`
- `Muller`

Any numbers are automatically parsed numerically, so typing `1` will find:

- `1`
- `01`
- `001`
- `0001`

and so on.

If you enter a wildcard character such as `*` (asterisk) this is treated as a literal value; this means that you cannot find `Sam` using `S*m`.

Any separator characters are treated as separators and not explicitly matched. For example, you can use:

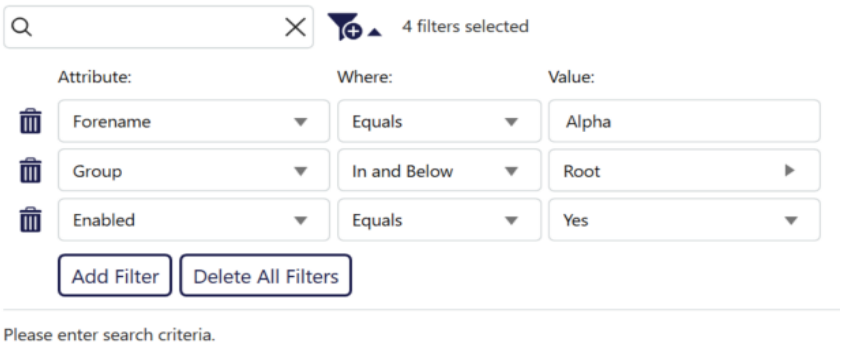
- `jones/sm`

to find:

- `jones-smith`

2.2.3 Using advanced search

In addition to using wildcard searching against the logon name and full name, some workflows allow you to filter the search based on other criteria.



- To add a filter, click **Add Filter**.
- To delete a filter, click the delete icon .
- To delete all filters, click **Delete All Filters**.
- To filter on a different attribute, select the attribute from the **Attribute** drop-down list.

The attribute you select determines what sort of comparisons you can use; for example, for operator-based attributes (such as **Approved By**) you can filter on jobs where the approver does not equal the current operator, or where the approver *does* equal the current operator; for group-based attributes, you can match a group, or match any groups in and below the selected group. For free text fields like the job label you can type the value you want to search for.

Set the **Where** and **Value** options to appropriate values for the attribute, then click **Search**.

2.3 Terminology

The MyID documentation set uses the following terminology:

Term	Description
administrator	A person who is responsible for the configuration and maintenance of MyID.
applet	A small program stored on a *card* and used to communicate directly with other systems or to process information.
card reader	Hardware connected to a computer that can read and write the information stored on a *smart card*.
card	A collective term for *smart cards* and *tokens* when there is no need to distinguish between them.
cardholder	A person who has been issued a *card* or other *credentials*.
category	*Workflows* are combined into related sets called categories. **Note:** The term 'group' is *not* used as this has a distinct meaning within MyID.
certificate	Proof of identity issued by a certification authority – this may be used to sign or encrypt information.

Term	Description
credential	The collective term for *cards* and *tokens* issued to a holder or a *device*.
device	A piece of equipment – a PC, server, router, cell phone or other hardware.
form	The information displayed during a stage. A form may consist of a single or multiple pages.
group	Groups provide the structures that contain the people in the database.
job	A queued task carried out by MyID.
operator	A person who uses MyID to issue and manage *smart cards* or *tokens*, but who is not responsible for configuration.
printer	A *smart card* printer – some printers also incorporate *card readers*.
smart card	A plastic card that can store information using a chip, a contactless chip, a magnetic stripe, or a combination.
stage	A step within a *workflow*.
token	*Credentials* using *smart card* technology in a different form that are used to hold identification details. For example, a USB token. A token may also refer to a one-time password software token.
Trusted Platform Module (TPM)	A secure cryptographic processor that may be installed in a variety of computing devices. Located on a *device*.S
Virtual Smart Card (VSC)	Microsoft Virtual Smart Card. A container that can hold credentials such as certificates and cryptographic keys. Stored on a *trusted platform module*.
workflow	A sequence of web pages forming a task within MyID.

3 Working with people

The people in the database are the credential holders, operators, managers and administrators of the system. You can organize people into groups, grant them roles that provide permissions to access parts of the system, import them from directories, view their details, and remove them from the system.

3.1 Finding people in MyID

The Find Person stage is used throughout MyID to locate the record of a particular individual. It forms the first stage of several workflows (for example, see section *3.4*, *Setting security phrases* and section *5*, *Working with cards*) and many of the workflows related to managing credentials.

For information about entering search criteria, including wildcards, see section *2.2.2*, *Entering search criteria*.

Note: When searching LDAP, the number of results returned may be limited by the directory; the default for Active Directory is 1000 records. You are recommended to use the search criteria to limit the results returned.

3.2 Adding people

You must add a person to the MyID database before you can issue credentials to that person. You can add a person manually, import the person from your directory, or import the person using the Lifecycle API.

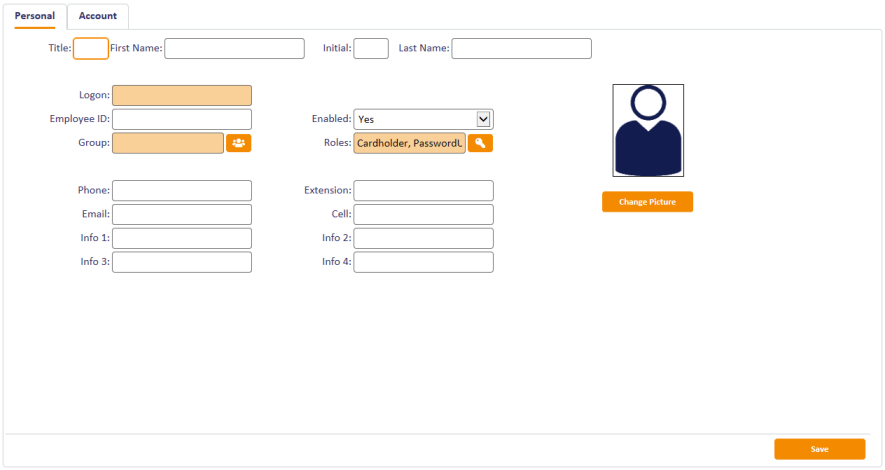
Note: If you are using an LDAP directory as the primary source of your data, you may use the **Edit Person** workflow to find a person and make their details available to MyID. The **Add Person** workflow may not be available. See the *Using an LDAP directory* section in the ***Administration Guide*** for details.

3.2.1 Adding a person manually

The **Add Person** workflow allows you to add a person to the MyID database without having to import that person from an LDAP directory. Depending on how your system is set up, you may not be able to add a user manually.

To add a person:

1. From the **People** category, click **Add Person**.



2. Type the **First Name** and **Last Name** of the person you want to add.

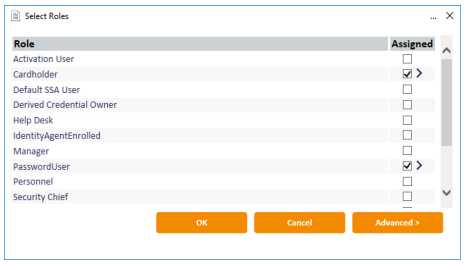
   You must provide either a first name or a last name.

3. Type a unique **Logon** name for the user. The user can use this to log on to MyID without using a card if your system is set up to allow logon using security phrases only.

4. Click the **Group** button, then select the group to which you want to add the person.

5. Click the **Roles** button.

   The Select Roles dialog appears.



   a. Select the roles you want to assign to the person. You can assign more than one role.

      Note: The group the person is in, together the role of the operator, determines which roles are available. See the *Roles, groups, and scope* section of the ***Administration Guide*** for details.

   b. Click the **Advanced** button. This allows you to set the scope for each of the person's roles.

      Note: You cannot set a scope higher than your own level.

   c. Click **OK** to save the changes to the roles and their scope.

6. You can change the person's picture: see section *7.3*, *Obtaining images*.

7. Use the **Account** tab to associate an LDAP account with the person. See section *3.2.2*, *Assigning an LDAP account to a person* below for details.

8. Click **Save**.

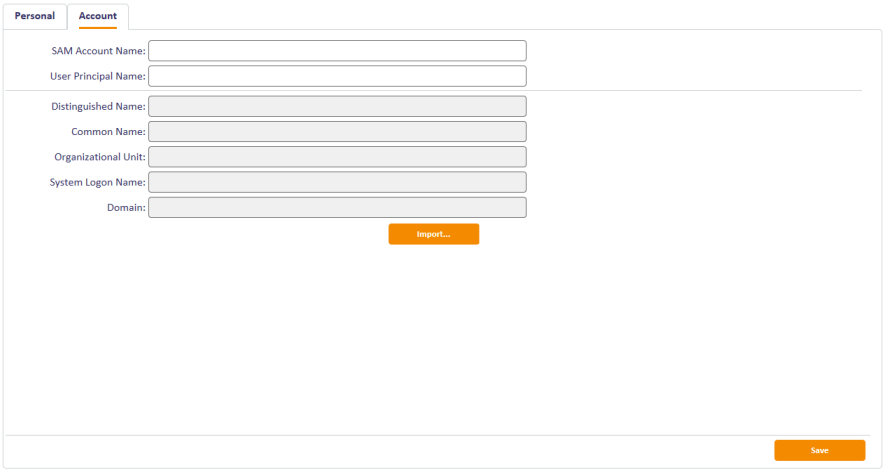
Depending on how your system is set up, the **Witness** stage may appear. See the *Witnessing a transaction* section of the ***Administration Guide*** for details.

3.2.2 Assigning an LDAP account to a person

Within the **Add Person** workflow, you can assign an LDAP account to a person by importing the details from your directory. This overwrites any information about the person that you have entered manually.

To assign an LDAP account to a person:

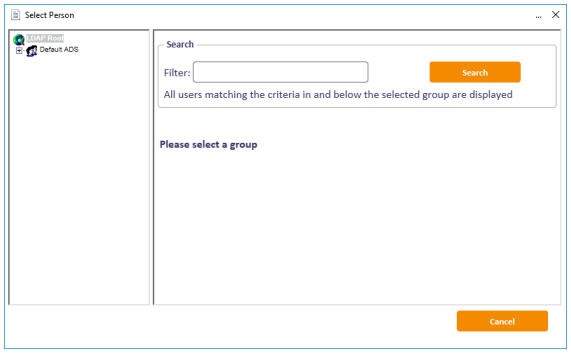
1. In the **Add Person** workflow, click the **Account** tab.



2. Click the **Import** button.

   The **Select Person** form is displayed.

3. Select the required branch of the LDAP directory.



4. Type the appropriate characters in the **Filter** field followed by an asterisk (`*`).

   For example, to find only people with first names starting with `Jo`, type `Jo*` in the **Filter** field.

5. Click **Search**.

6. Select the appropriate person from the list of people.

7. Click **Import**.

   The person's details are added to the **Add Person** form, overwriting any information that was previously entered. You can now amend the details if necessary and save the person's record in the MyID database.

3.3 Editing people

You can view or edit the records of people, or remove them from the database.

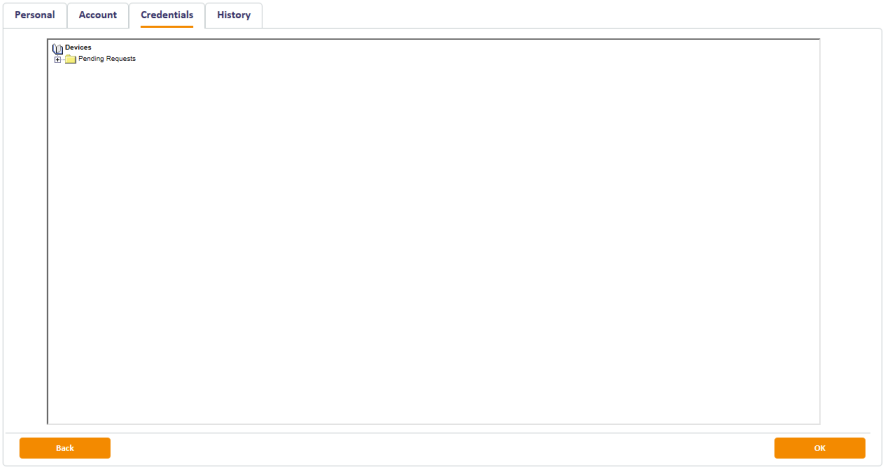
3.3.1 Viewing a person's details

1. From the **People** category, click **View Person**.
2. Use **Find Person** to search for the person whose details you want to see.
3. Click the box to the left of the name of the person whose details you want to see.

   The **Personal** tab displays the personal details of the user.

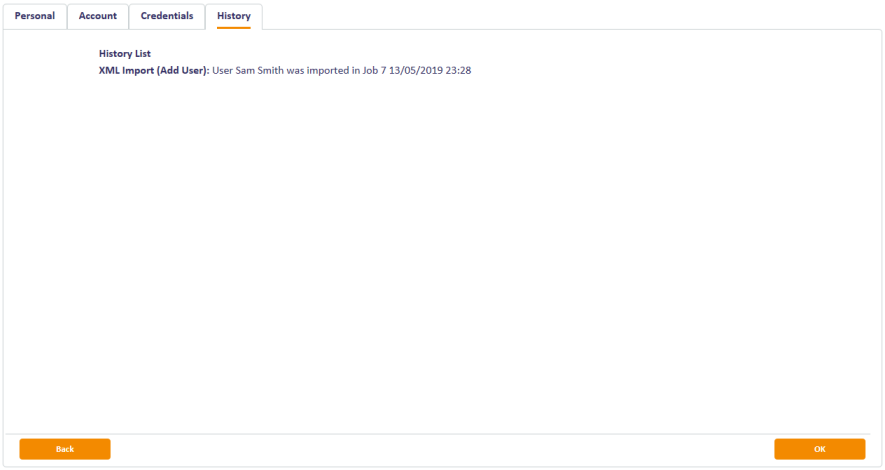
   The **Account** tab contains the details of the user's account in the directory.

   The **Credentials** tab displays information about all credentials related to the person's account; it displays pending requests and details of current credentials, including the history of each credential and information about the certificates it contains.



Note: The **Credentials** tab appears only if your role includes the **View Device Details** option in the **Cards** section of the **Edit Roles** workflow.

The **History** tab contains details of the person's account history.



Note: The **History** tab appears only if your role includes the **View Device Details** option in the **Cards** section of the **Edit Roles** workflow.

Note: You must have either the **View Full Audit** or **View User Audit** permissions to view the history for a user. See the *Audit scope* section of the ***Administration Guide*** for details.

Click the links to view the detailed list of changes.

4. To finish the workflow, click **OK**.

3.3.2 Editing a person

The **Edit Person** workflow allows you to edit the details of a person in the database.

You can also use the **Edit Person** workflow to find a person in your directory and make their details available to MyID if you are using an LDAP directory as the primary source of your data. See the *Using an LDAP directory* section of the ***Administration Guide*** for details of setting up the connection to your directory.

1. From the **People** category, click **Edit Person**.
2. Use the **Find Person** stage to search for the person whose details you want to edit.
3. Click the box to the left of the name of the person whose details you want to edit.

   The **Edit Details** stage displays existing information about the person.

   The **Personal** tab displays the details of the person.

   You cannot edit any details that have been populated from the directory if you have set up your system to use the directory as a primary data source, but you can edit any other details.
4. You can select the roles available to the person.

   If you clear all the roles assigned to a user, you can still save the user record; however, the user is not saved without any roles, but retains all of their previous roles.

   Note: If you use the Select Roles dialog to edit a user, if a role that the user previously held has been removed from the user's group, it appears in the list with **(No longer available)** appended after the name – when you click **OK**, any such roles will be removed from the user's roles.
5. You can change the person's picture: see section *7.3*, *Obtaining images*.
6. To enable or disable a person, select an option from the **Enabled** drop-down list.

   You must select a reason and type a comment if you disable a user. See section *6.5*, *Certificate reasons* for details of the different reasons.

   Note: You cannot enable or disable a person if you have set up your system to use the directory as a primary data source.
7. The **Account**, **Credentials**, and **History** tabs are the same as those used to view a person – see section *3.3.1*, *Viewing a person's details* for details.

   The **Credentials** and **History** tabs appear only after you have added the person to the MyID database; they do not appear while you are using the **Edit Person** workflow to add a person from the directory.
8. To finish the workflow, click **Save**.

3.3.3 Removing a person

You can remove a person from the system, revoking any certificates and canceling any devices that have been issued to them.

To remove a person:

1. From the **People** category, click **Remove Person**.
2. Use the **Find Person** stage to search for the person whose details you want to remove.

   The **Display Details** stage shows the person's title, first name, initial, last name and security ID.
3. If you are sure you have selected the correct person, click **Confirm**.
4. Select the reason you are removing the person and add a comment.

   See section *6.5*, *Certificate reasons* for details of the effect of the different reasons.

The person is removed from the MyID system. Removing a person from MyID does not remove the user from the directory.

3.4 Setting security phrases

If you log on to MyID without a smart card, or if your card is locked, you must identify yourself to the system using a series of security questions. The **Change My Security Phrases** and **Change Security Phrases** workflows allow you to set these responses.

3.4.1 Changing your own security phrases

You can use the **Change My Security Phrases** workflow to change the security phrases stored in the database for your own account.

1. From the **People** category, click **Change My Security Phrases**.
2. Select the security questions that will be used to confirm your identity from the drop-down lists, then type and confirm the answers to each of the questions.

When you make changes to these answers, you must provide answers to all the questions displayed.

If there is more than one security phrase, the default security phrase is marked with an asterisk (*). This is the phrase used for situations where only one password is required.

Note: Your system administrator can configure the number of security phrases. See the *Setting the number of security phrases required to authenticate* section of the ***Administration Guide*** for details.

3. Click **OK**.

3.4.2 Changing security phrases for a user

You can use the **Change Security Phrases** workflow to change the security phrases for any user on the system, assuming your role enables you to do so.

1. From the **People** category, click **Change Security Phrases**.

   You can also launch this workflow from the View Person screen in the MyID Operator Client; this launches the workflow with the person already selected. See the *Changing a person's security phrases* section in the ***MyID Operator Client*** guide for details.

2. Use the **Find Person** stage to search for the person whose security phrases you want to change.

3. Select the security questions that will be used to confirm the person's identity from the drop-down lists, then type and confirm the answers to each of the questions.

   When you make changes to these answers, you must provide answers to all the questions displayed.

   If there is more than one security phrase, the default phrase is marked with an asterisk (*). This is the phrase used for situations where only one password is required.

   Note: Your system administrator can configure the number of security phrases. See the *Setting the number of security phrases required to authenticate* section of the ***Administration Guide*** for details.

4. Click **OK**.

3.5 Authenticating users

The **Authenticate Person** workflow allows a MyID operator to authenticate the identity of a cardholder. The authentication is recorded in the MyID audit trail.

This workflow allows you to carry out authentication when required to by your process; for example, for FIPS 201-3, you must confirm the identity of the cardholder before carrying out changes on their card.

Note: MyID does not enforce the authentication of cardholders for operator-led workflows, but by recording the details of the authentication in the audit trail it allows you to verify that your operators have been following the process correctly.

The **Authenticate Person** workflow allows the following methods of authentication:

- **Match Enrolled Fingerprints** – the operator guides the cardholder through providing their fingerprint biometrics. The fingerprint is matched against the enrolled fingerprints in the MyID database.

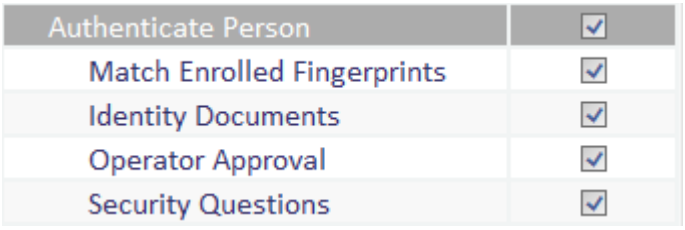
  Note: This feature is supported only if your system has been configured for biometrics. For more information, contact customer support, quoting reference SUP-142.

- **Identity Documents** – the operator checks the details of the provided identity documents and records their details, including expiry dates and serial numbers.

Note: The list of available documents is determined by the two **Title** lists. To edit these lists, use the **List Editor**. See the *Changing list entries* section of the ***Administration Guide*** for details.

- **Security Phrases** – the operator asks the user their security questions. For more information on setting the number of security phrases required to authenticate, see the *Setting the number of security phrases required to authenticate* section of the ***Administration Guide*** for details.
- **Operator Approval** – if the cardholder cannot provide fingerprints, identity documents, or provide their security phrases, the operator can override the check. The operator *must* provide a reason why they are providing approval.

You can control which methods of authentication are available to operators using the **Edit Roles** workflow. Underneath the **Authenticate Person** workflow in the list of available options, you can select which methods are available to operators with that role:



To authenticate a cardholder:

1. From the **People** category, select **Authenticate Person**.

   You can also launch this workflow from the View Person screen in the MyID Operator Client; this launches the workflow with the person already selected. See the *Authenticating a person* section in the ***MyID Operator Client*** guide for details.

2. In the Find Person screen, type the details of the person you want to authenticate, then click **Search**.
3. Select the person you want to authenticate from the list of search results.

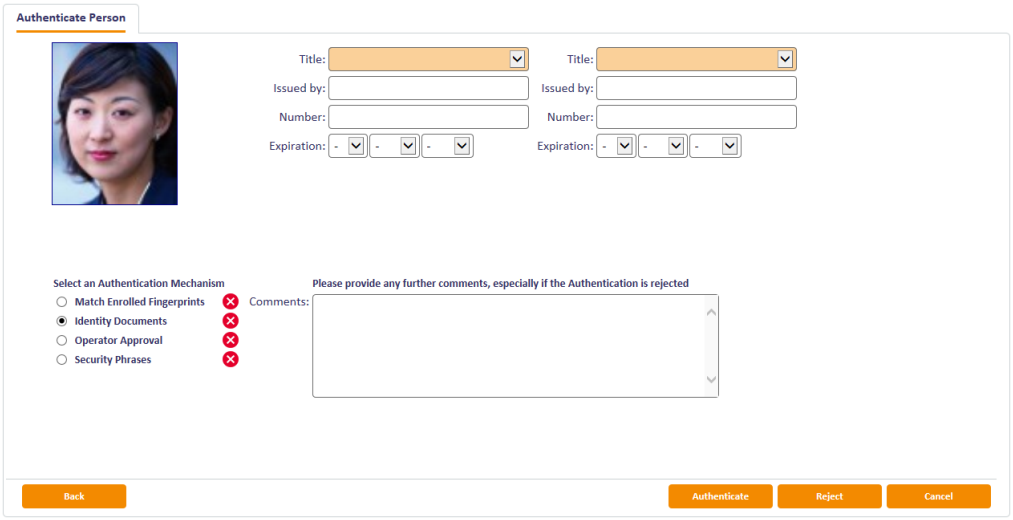
4. Select the authentication mechanism.

The list of available authentication mechanisms is determined by your MyID role permissions.

For **Match Enrolled Fingerprints**:

Select the fingerprint you want to match, and guide the cardholder to use the fingerprint scanner.

For **Identity Documents**:



Record the details of two identity documents provided by the cardholder, including:

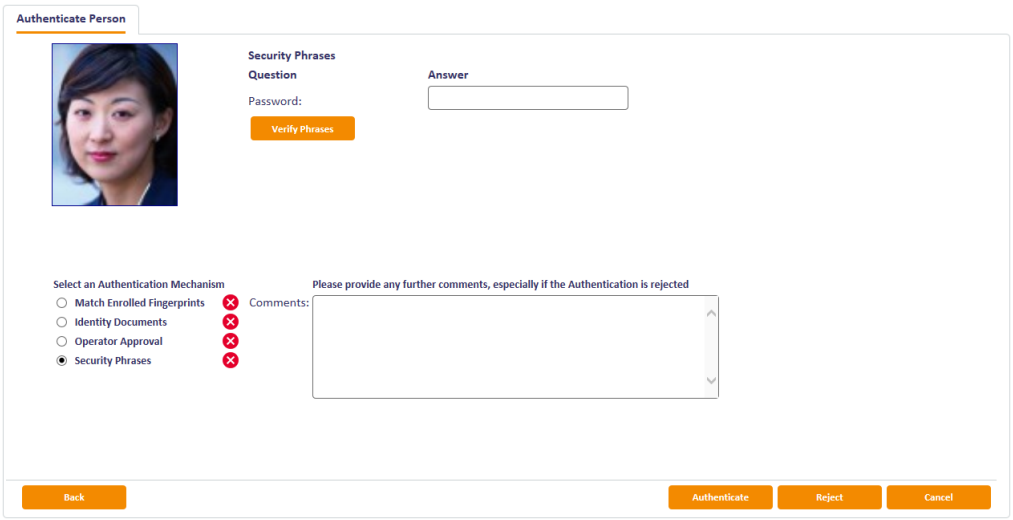
- **Title** – the type of document.
- **Issued by** – the issuer of the document.
- **Number** – the serial number of the document.
- **Expiration** – the expiration date of the document.

Note: The list of available documents is determined by the two **Title** lists. To edit these lists, use the **List Editor**. See the *Changing list entries* section of the ***Administration Guide*** for details.

For **Operator Approval**:

Provide the details of your manual authentication of the cardholder. Include as many details as possible as to why the cardholder could not provide fingerprints or identity documents.

For **Security Phrases**:



Ask the user their security questions and type the answers, then click **Verify Phrases**.

The number of questions you need to ask is independent of the number of questions the user has stored in the system – for example, the user may have four questions stored, and you may be required to ask two of them for operator-led authentication.

For more information on setting the number of security phrases required to authenticate, see the *Setting the number of security phrases required to authenticate* section of the ***Administration Guide*** for details.

5. Type your comments in the **Comments** box. These comments are included in the MyID audit trail.
6. Click **Authenticate** to approve the cardholder's identity or **Reject** if you are not satisfied.

4 Working with groups

MyID lets you organize people into groups. These form a hierarchy, with each person belonging exclusively to a single group. This structure normally represents the reporting structure within your organization, since it forms the basis for defining the security scope of each person.

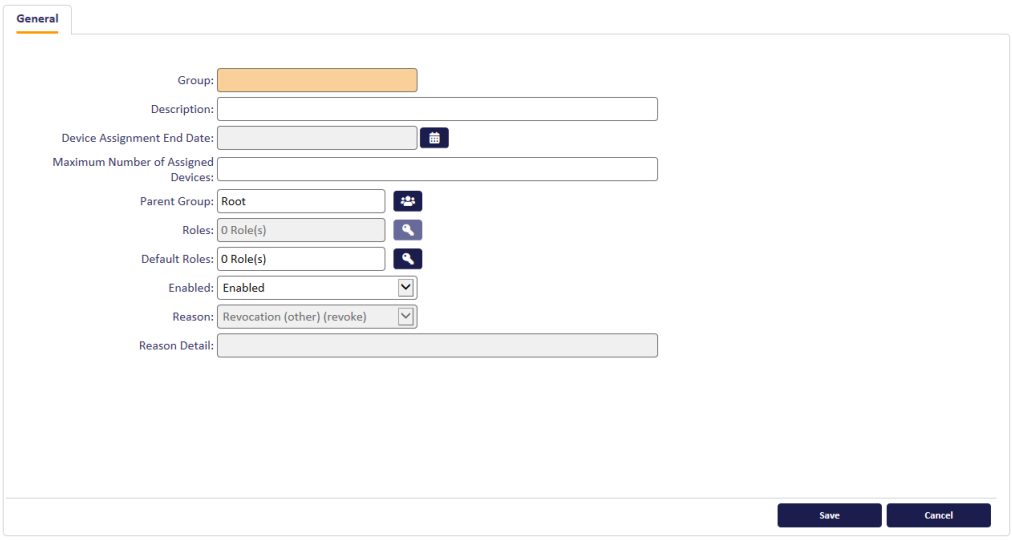
4.1 Adding a group

To add a new group:

1. Select the **People** category and then select **Add Group**.

   You can also launch this workflow from the **Group Management** section of the **More** category in the MyID Operator Client. See the *Using Group Management workflows* section in the ***MyID Operator Client*** guide for details.

   The **General** page opens.



   Note: In the PIV edition of MyID, there is an additional tab for the details of the user's **Agency**. See the *Manage agencies* section of the ***PIV Integration Guide*** for details.

2. In **Group**, type the name of the group.
3. Enter a short **Description** for the group.
4. Optionally, set the following license options:
   - **Device Assignment End Date** – select the last date on which you can assign or issue devices for this group. After this date, you will no longer be able to assign or issue devices to people in this group.
   - **Maximum Number of Assigned Devices** – type the maximum number of devices you can assign or issue to this group. Once the number of devices assigned or issued to people in this group reaches this number, you will no longer be able to assign or issue devices to people in this group.
5. Click the **Group** button to the right of **Parent group**. A list of available parent groups is displayed.

- If you are entering details of a top-level group, select **Root**.
- If you have already created other groups, select the one to contain the new group you are creating, if appropriate.

6. Click the icon to the right of **Roles** and select the roles that can be placed in this group from the list.

   Note: If you do not select any roles, and leave the option displaying **0 Role(s)**, this means that the group is unrestricted and all roles are available to the group.

7. Click **OK**. The number of roles that you have selected is displayed in the **Roles** box.

   Note: This number is purely a count of the roles – it does not relate to the number displayed next to a role name in the **Edit Roles** workflow.

8. Select whether the group is enabled or disabled.

   By default, a new group is **Enabled**.

   If you set a group to **Disabled**, you can specify a reason. A "no entry" sign is displayed against a disabled group when you view it in the **Parent Group** list.

   See section *6.5*, *Certificate reasons* for details.

4.2 Changing a group

You can make changes to a group, including which roles can be placed in the group and whether it is disabled or not.

1. Select the **People** category and then **Amend Group**.

   You can also launch this workflow from the **Group Management** section of the **More** category in the MyID Operator Client. See the *Using Group Management workflows* section in the ***MyID Operator Client*** guide for details.

   A list of available groups is displayed after a brief pause.

2. Select the group you want to change and click **Continue**.

   If you select the wrong group, click the **Group** button to display the list again.

3. Make your changes.

   You can change the basic details of the group, including whether it is enabled or disabled.

4. Optionally, set the following license options:

   - **Device Assignment End Date** – select the last date on which you can assign or issue devices for this group. After this date, you will no longer be able to assign or issue devices to people in this group.
   - **Maximum Number of Assigned Devices** – type the maximum number of devices you can assign or issue to this group. Once the number of devices assigned or issued to people in this group reaches this number, you will no longer be able to assign or issue devices to people in this group.

5. Click the icon to the right of **Roles** and select the roles that can be placed in this group from the list.

   Note: If you do not select any roles, and leave the option displaying **0 Role(s)**, this means that the group is unrestricted and all roles are available to the group.

Note: Changes to the roles that can be selected do not affect existing accounts; if you edit the roles for a user, you can select from the currently-available roles for the user's group, and must remove any roles that are no longer allowed, but MyID does not add or remove roles from a user automatically.

6. For information on setting up the **Default Roles**, see the *Default roles* section in the ***Administration Guide***.
7. From the **Enabled** drop-down list, select **Enabled** to enable the group, or **Disabled** to disable the group.

   Warning: If you disable a group, all accounts within it are also disabled.

   If you disable a group, you must select a reason. See section *6.5*, *Certificate reasons* for details.

4.3 Deleting a group

If you no longer require a group, you can delete it.

1. Select the **People** category and select the **Remove Group** workflow from the list.

   You can also launch this workflow from the **Group Management** section of the **More** category in the MyID Operator Client. See the *Using Group Management workflows* section in the ***MyID Operator Client*** guide for details.

   A list of available groups is displayed after a brief pause.
2. Select the group you want to remove and click **Remove**.

   If you select the wrong group, click the **Group** button to the right of **Select a Group** to display the list of groups again.

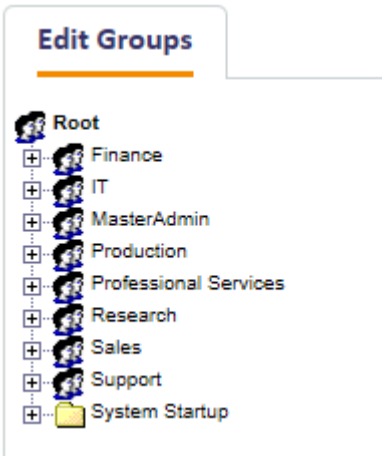
Note: You cannot remove a group that contains other entries. Instead, you must use the **Edit Groups** workflow, which asks you where to relocate the group's contents.

4.4 Editing groups

Using the **Edit Groups** option, you can add, rename, edit, and remove groups; you can also import an LDAP directory branch into your group structure.

1. From the **People** category, select **Edit Groups**.

   You can also launch this workflow from the **Group Management** section of the **More** category in the MyID Operator Client. See the *Using Group Management workflows* section in the ***MyID Operator Client*** guide for details.



Existing groups are displayed in a tree structure, and can be expanded or collapsed by clicking the plus (**+**) or minus (**-**) signs to the left of their names.

Click a group name to select it.

2. Right-click the name of a selected group to display a menu. From here you can:
   - Add a new group
   - Move a group to a new location in the tree structure
   - Rename a group
   - Import an LDAP directory branch, choosing whether to:
     - Import an Organizational Unit (OU) and its children
     - Import just the children of an OU
   - Remove a group, choosing whether to:
     - Remove a group, moving any groups it contains and the users to a new group
     - Remove the group and any groups it contains, moving just the users to a new group
3. When you have made all the necessary changes, click **Save**.

4.4.1 Adding a new group

1. Right-click the name of the group that you want to contain the new group.
2. Select **Add**, then **New Group** from the menu.

   A new group is created, called **New**.

   If the parent group is closed, you may not see the new group. Click the plus sign (**+**) sign next to the parent group to view it.
3. Right-click the name of the group and select **Rename Group** from the menu.
4. Select the existing name of the group and enter a new one.
5. Click **Save**.

4.4.2 Moving a group

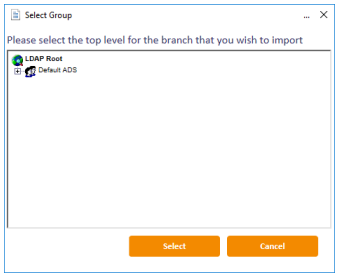
1. Right-click the name of the group that you want to move.
2. Select **Move Group** from the menu.
3. Click the name of the group that you want to contain it.
4. Click **Save**.

4.4.3 Renaming a group

1. Right-click the name of the group that you want to rename.
1. Select **Rename Group** from the menu.
2. Highlight the existing name of the group and enter a new one.
3. Click **Save**.

4.4.4 Importing an LDAP directory branch

1. Right-click on the name of the group into which you want to import a branch from an LDAP directory.
2. Select **Import LDAP Branch** from the menu.
3. Select one of the following options:
   - **OU and Children** to import the group and all its contents
   - **Just Children** to import just the contents of the group
4. The **Select Group** box opens.



   Locate and select the Organizational Unit (OU) that you want to import and click **Select**.
5. Click **Save**.

4.4.5 Removing a group

1. Right-click the name of the group you want to remove.
2. Select **Remove Group** from the menu.
3. Select one of the following options:
   - **Remove Group, Move Sub-Groups and Users** to delete the group but move any sub-groups and people to another group.
   - **Remove Group and Sub-Group, Move Users** to delete the group and any sub-groups within it but move the people to another group.

4. A message is prompts you to confirm that you want to delete the group. Click **Yes** to continue.
5. The **Reparent Users** box opens.

   Click the name of the group into which you want to move any sub-groups and people, then click **Select**.
6. Click **Save**.

5 Working with cards

The **Cards** category allows you to manage your smart cards or other devices. For example, you can issue, update, unlock and cancel cards. You can also identify cards and change their PINs.

For details of the smart card manufacturers, model numbers, and middleware versions supported, see the ***Smart Card Integration Guide***.

5.1 Issuing cards

You can issue a card directly, or you can request a card that the user can then pick up. Depending on how your system is set up, it may be necessary to validate a card request before the card can be collected.

5.1.1 Issuing a card

Note: If you are using archived certificates, and the user has chevrons <> in their PIV DN, you may see an error similar to the following when attempting to use the **Issue Card** workflow:

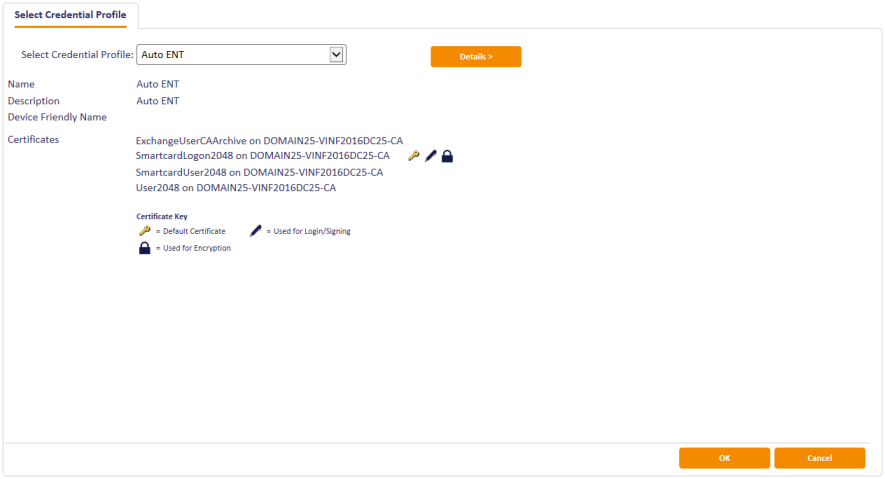
```
The certificate request is invalid or badly formed.
```

As a workaround, use **Collect Card** or the Self-Service App to collect the card instead. The **Issue Card** workflow is not recommended for PIV card issuance; see the *PIV card issuance* section in the ***PIV Integration Guide*** for details of the PIV card issuance process.

The **Issue Card** workflow allows you to issue a card to a MyID user. The user must already exist in the database before you can issue a card.

To issue a card:

1. From the **Cards** category, click **Issue Card**.
2. Use the **Find Person** stage to search for the person to whom you want to issue a card.
3. Select the person. The **Select Credential Profile** screen appears.

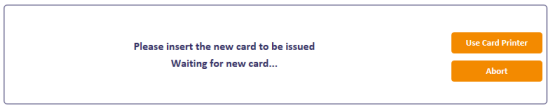


Click the **Details** button to view the details of the profile that is currently selected. Click **Hide** to return to the original view.

4. You may be able to specify an expiry date for this card (see section *5.2*, *Setting expiry dates for a card*).

Select the option to display a field where you can specify a date.

5. Select the profile you want to use from the drop-down list, then click **OK**.



6. Insert a blank card into the reader.

   If you want to print the card, click **Use Card Printer**. This allows you to either load a new card into the card printer or eject the card.

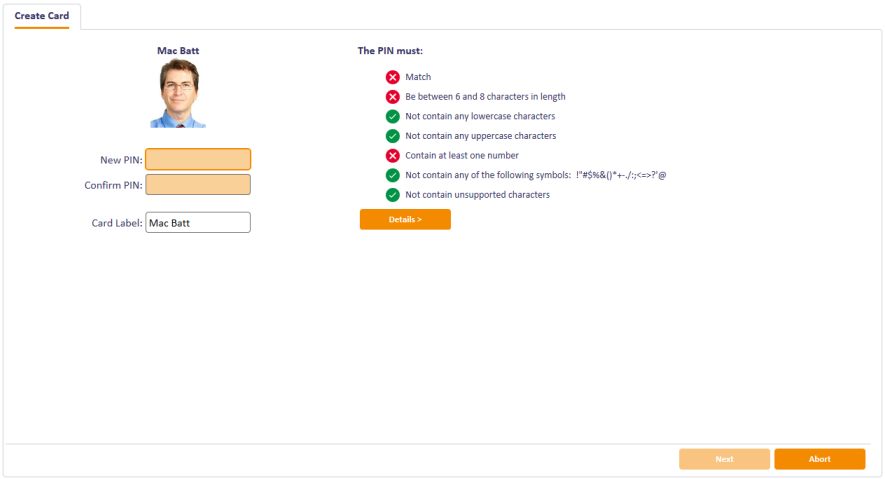
   Select the correct printer from the **Select Printer** list and click the **Load New Card** or **Eject Card** button.

7. In the **Create Card** stage, enter or view the PINs for the card:

   - If the card has a contact chip, type and confirm its PIN.
   - For each hardware and software one time password:
     - If the type of password required in the profile is **User**, type and confirm the PIN.
     - If the type of password required is **Device**, the PIN is the same as the PIN for the contact chip.
     - If the type of password required is **Server**, the PIN is generated.
     - If the type of password required is **None**, there is no PIN.

   Note: The **Show Generated PINs** configuration option must be set to Yes to allow the system to display the PINs for random or server-generated PINs. See the *PINs page (Security Settings)* section in the ***Administration Guide*** for details.

   Click **Details** to show details of the information that will be written to the card (see below). Click **Hide** to show the summary.



8. Click **Next**.

   If the credential profile requires secondary validation, a witness must insert their card to validate the issue of the card.

   MyID then writes any certificates to the new card.

9. The **Print Card** stage lists all card layouts that are available to the credential profile being issued. Clicking a layout shows you how the card will appear when printed, with the user image and dynamic fields populated automatically.

   Note: If the preview image of the card displays an error with the following:

   `Unable to retrieve card layout preview`

   see section *5.12.4*, *Troubleshooting card layout preview issues*.

10. Either click **Print** to print the card or click **Skip Printing** to end the workflow without printing the card.

If there is a problem when issuing the card, you may be able to select a different credential profile or card to attempt to issue the card again.

5.1.2 Requesting a card

The **Request Card** workflow allows you to request a card that can be collected later using the **Collect Card** or **Collect My Card** workflows. Depending on how your system is set up, it may be necessary to validate a card request before the card can be collected.

To request a card:

1. From the **Cards** category, click **Request Card**.
2. Use the **Find Person** stage to search for the person to whom you want to issue a card.
3. Select the person. The **Select Credential Profile** screen appears.
4. Select the credential profile you want to use from the drop-down list.
5. You may be able to specify an expiry date for this card (see section *5.2*, *Setting expiry dates for a card*).

   Select the option to display a field where you can specify a date.
6. To request a card using this profile, click **Request Card**.

   To pre-allocate a specific card, click **Assign Card**:

   - If the **Allow card serial number to be entered during Request Card workflow** option is set to `Yes`, you can enter the serial number.

     You can include `?` and `*` as wildcard characters; any unassigned devices, or devices with unrestricted cancellation, that match the search criteria are displayed; the device serial numbers must already be known to MyID. If more than 10 devices match the search criteria, you must search again with more restrictive criteria.
   - Alternatively, insert the card you want to allocate.

   MyID creates the card request job.

- **IKB-367 – Problem adding a user from Active Directory where the logon name already exists in MyID**

  A problem has been identified when the following scenario occurs:

  - A user account is added to MyID from Active Directory.
  - The user account is removed from Active Directory, but no removal of the account from MyID takes place.

- A new user account is created in Active Directory with the same logon name.
- An attempt is made to request credentials for that user account in MyID.

When this occurs, errors similar to the following appear:

- In the Request Card workflow in MyID Desktop:

  ```
  There has been a problem validating the user due to missing or invalid data
  ```

- In the Request Device screen in the MyID Operator Client:

  ```
  Validation problem, the value for 'logonName', 'Logon', already existsError number: WS40001
  ```

As a workaround, you can remove the user account from MyID using Remove Person and repeat the steps to create the new request.

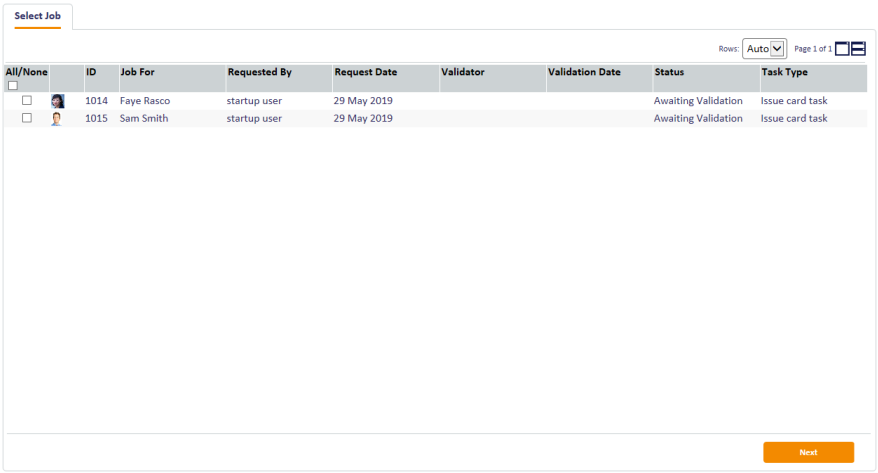
5.1.3 Validating a card request

If the credential profile has the **Validate Issuance** option set in the **Issuance Settings**, you must validate a card request before the card can be issued. The validator must be a different person than the person who requested the card or the person to whom the card will be issued.

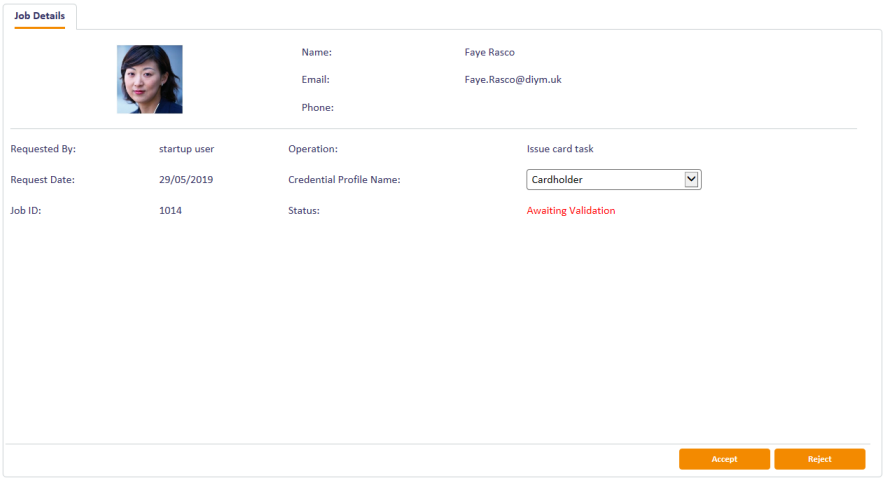
The **Validate Request** workflow allows you to validate a card request.

To validate a request:

1. From the **Cards** category, click **Validate Request**.
2. Enter the search details for the job, then click **Search**.



3. From the list of jobs, select the card request you want to validate, and click **Next**.



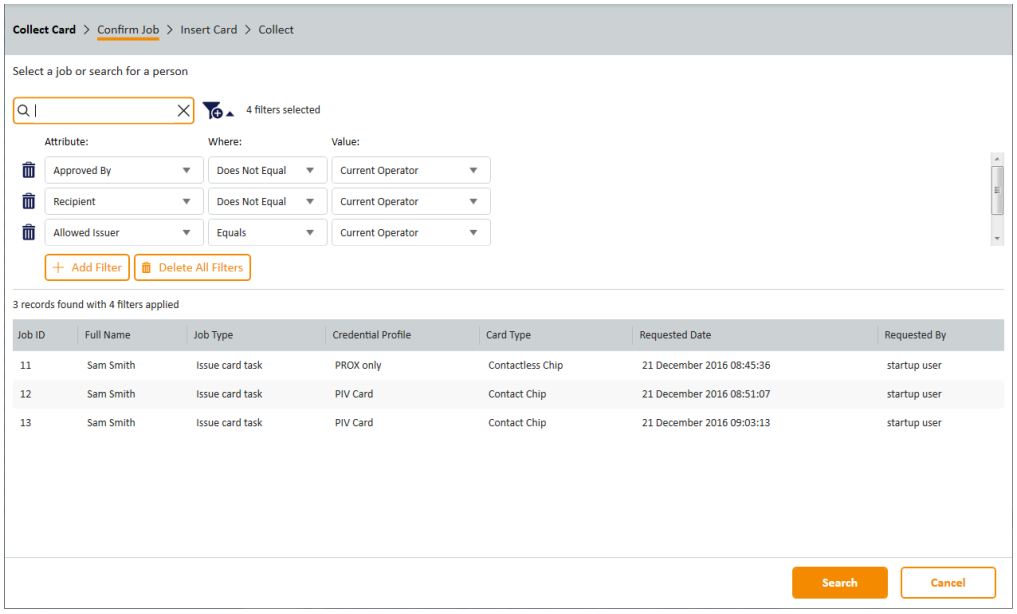
4. You can select a different credential profile from the list if necessary.
5. If the option to specify an expiry date has been enabled (see section *5.2*, *Setting expiry dates for a card*), you can set or change the expiry date for the card.
6. Click one of the following options:
   - **Accept** to validate the card request. The card can now be issued.
   - **Reject** to reject the card request. The card can not be issued.

5.1.4 Collecting a card

You can collect a card that has been requested for another user.

To collect a card:

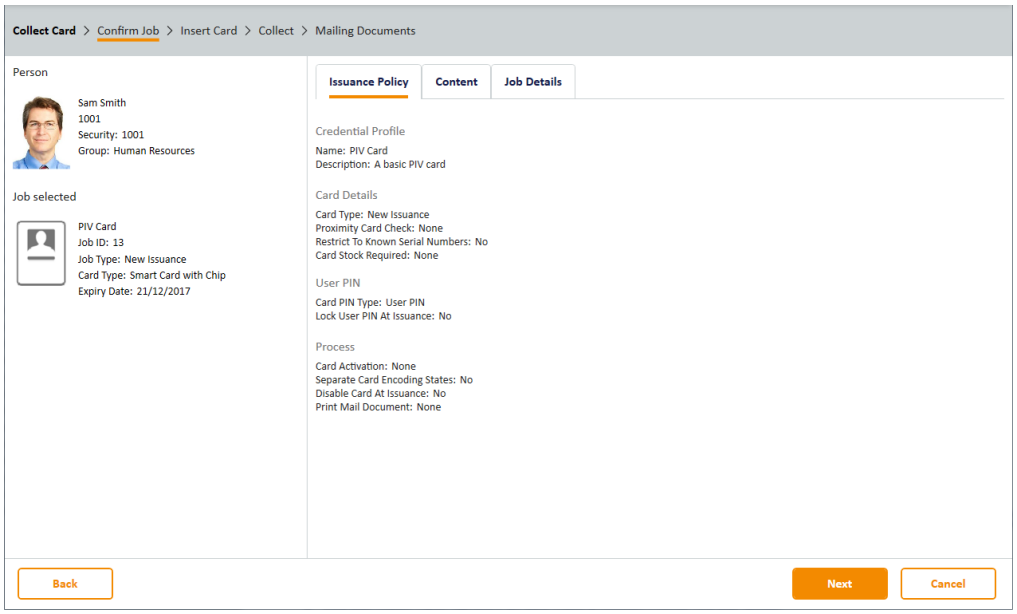
1. From the **Cards** category, click **Collect Card**.



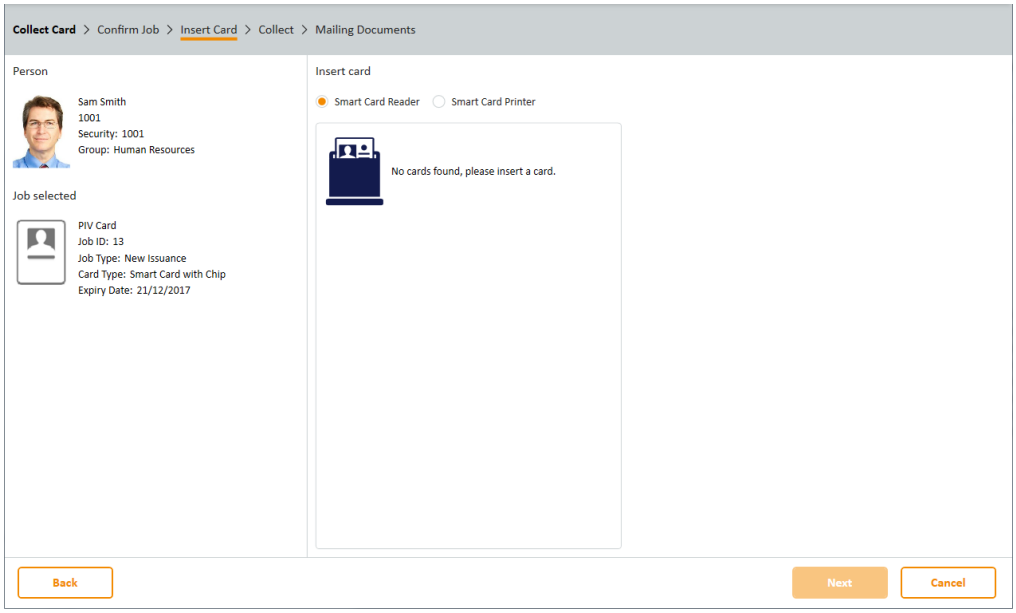
2. Enter the search details for the job, then click **Search**.

   For details of using search filters, see section *2.2.3*, *Using advanced search*.

3. Select the job from the list.



4. Make sure that the details of the job are correct. This screen lists the following:
   - On the **Issuance Policy** tab, details about the credential profile that will be used to issue the card.
   - On the **Content** tab, details about the card content, including format and certificates.
   - On the **Job Details** tab, details about the request and approval of the card, the job label, and any assigned card details.
   - If you have the **Display person details during confirm job** configuration option (on the **LDAP** tab of the **Operation Settings** workflow) set, an additional tab labeled **Person Details** is available.
5. Click **Next**.

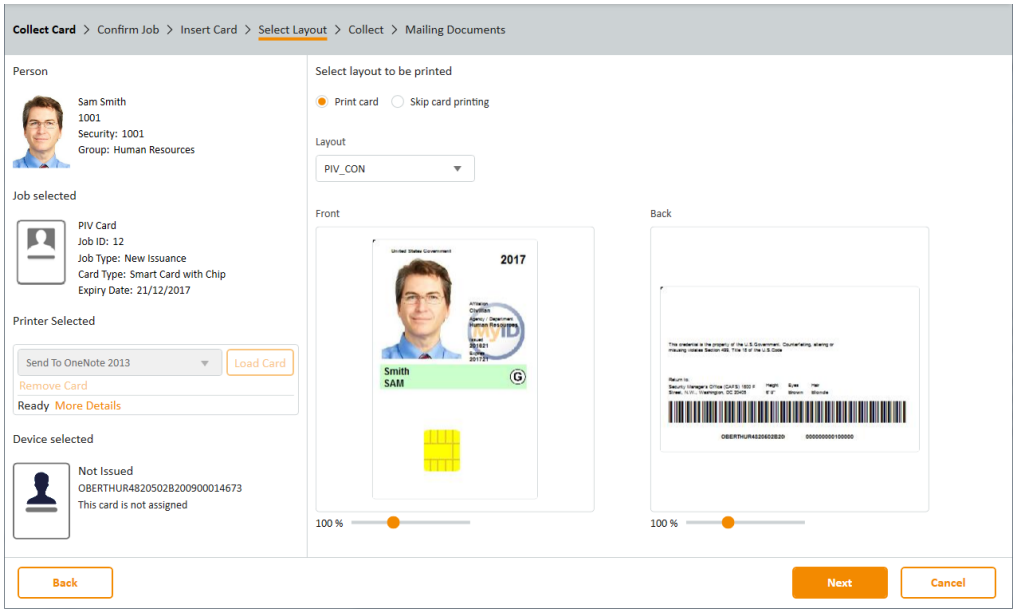


6. Select one of the following options:
   - **Smart Card Reader** – select this option to issue the card using a card reader attached to your PC.
   - **Smart Card Printer** – select this option to issue and print the card using a card printer attached to your PC.

   For more information about using a card printer, see the ***Printer Integration Guide***.
7. Insert a card into the card reader, or load a card into the card printer.

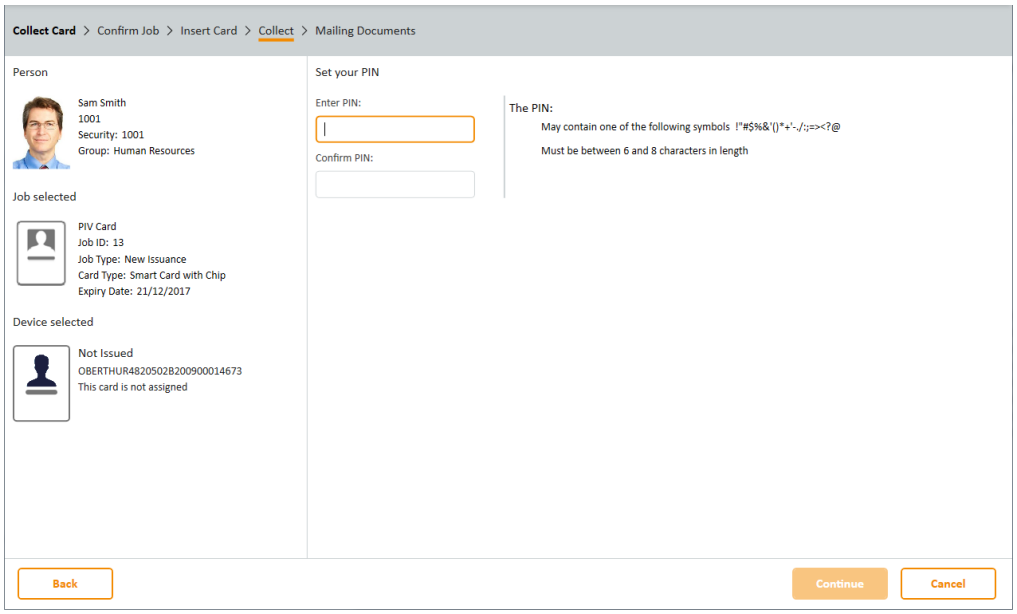
   If there is more than one suitable card inserted, select the card you want to use. If only one suitable card is inserted, the workflow automatically moves on to the next stage.
8. Depending on how your system is configured, you may see a warning at this stage; when you install MyID, the settings on the **Device Security** page of the **Security Settings** workflow are configured to require you to use customer GlobalPlatform keys and random Security Officer PINs (SOPINs). The system is also configured to display warnings if your system is not securely configured. See the *Device Security page (Security Settings)* section in the ***Administration Guide*** for details.
9. Click **Next**.
10. If the credential profile is set up for activation, the workflow ends here; to complete the issuance of the card, you must use an activation process.

    See section *5.4.1*, *Activate card*, section *5.4.2*, *Assisted activation*, and the *Activating cards* section in the ***Administration Guide*** for details.
11. If you are using a card printer, select the card layout you want to use.



If you decide not to print at this stage, click **Skip card printing**.

12. Click **Next**.



13. Type the PIN for the card in the **Enter PIN** box, then again in the **Confirm PIN** box.

    MyID provides feedback on-screen that the PIN meets the requirements configured in the credential profile. Once you have entered and confirmed a valid PIN, click **Continue**.

    MyID writes the user's details and any configured certificates to the card.

    Note: If you are issuing prox-only cards, or combination chip and prox cards, if the prox part of the card is not detected at this stage, check the following:

    - The card is a prox card.
    - The card is the correct prox card with the correct serial number.

- The prox portion of the card is working correctly.

You can also configure MyID to use a separate external prox reader. See section *5.12.3*, *Printers have external readers*.

14. If you are using a card printer, MyID prints the card at this point.

    Note: If you have the **Print Quality Confirmation** option (on the **Devices** tab of the **Operation Settings** workflow) set to **Yes**, you are asked to confirm that the card printed correctly:

    - **Did the card print OK?**

      If you respond **Yes**, the workflow completes.

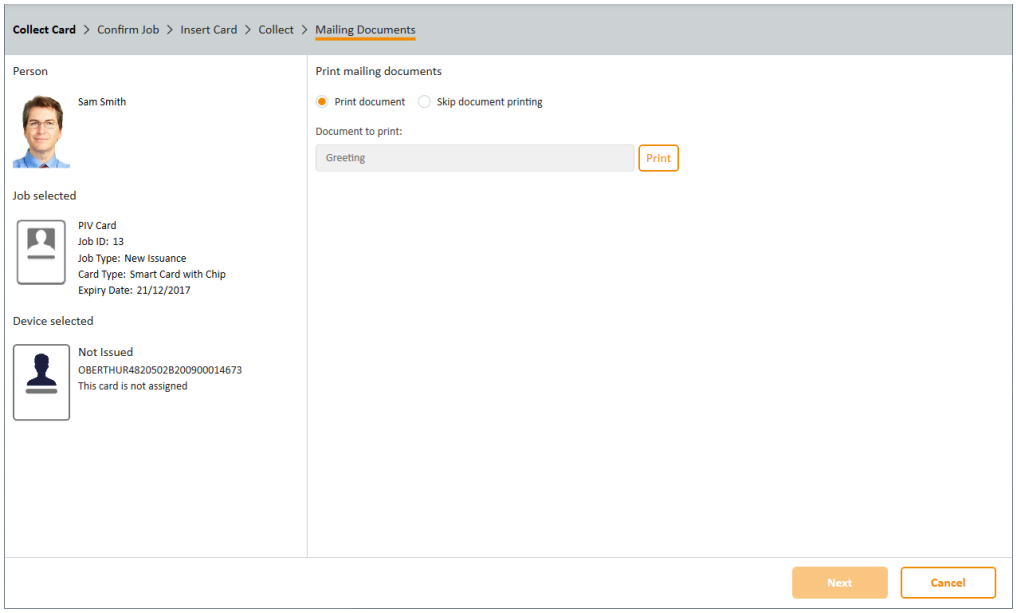
      If you respond **No**, MyID offers the following option:

    - **Do you want to retry the collection?**

      If you respond **Yes**, MyID cancels the card, revokes the certificates, then attempts to issue the card again.

      If you respond **No**, MyID cancels the card and revokes the certificates.

15. If the credential profile is configured for a mailing document, you can print it at this point.



    Note: For details of configuring templates for mailing documents, contact customer support, quoting reference SUP-255.

16. Either select **Print document**, then click the **Print** button, or select **Skip document printing**.

17. Click **Next**.

The workflow completes.

- **IKB-216 – Magnetic stripe only card issuance not supported in Collect Card or Batch Collect Card**

It is not currently possible to use the **Collect Card** or **Batch Collect Card** workflow to issue a card with magnetic stripe encoding only – that is, without additional contact chip or contactless encoding. Jobs that require magnetic stripe only are omitted from the search results.

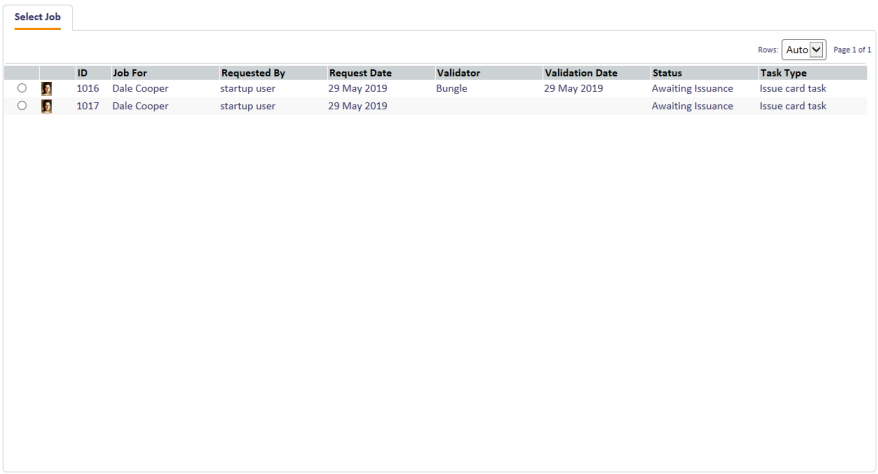
5.1.5 Collecting your own card

You can collect a card that has been requested for you. You may be able to log on with your security phrases to collect your new card. If you have logged on with a card, you can collect updates that an administrator has requested for that card using the **Request Card Update** workflow.

To collect a card or an update:

1. From the **Cards** category, click **Collect My Card**.

   If you have more than one card request waiting, the list of jobs available for your card appears.



2. Select the job you want to collect, then click **Next**.
3. If the card was pre-allocated using the **Assign Card** option when it was requested, you must present the same card. Either insert the card with the specified serial number, or type the serial number (for cards with no contact chip).

   Follow the instructions on screen to collect your card or updates.

   If there is a problem when issuing the card, you may be able to select a different card to try again.

5.1.6 Requesting multiple cards

You can configure MyID to request multiple cards for a single user; for example, for a team leader who may hold a stock of cards and issue them to their team members as and when required.

To configure MyID to issue multiple cards:

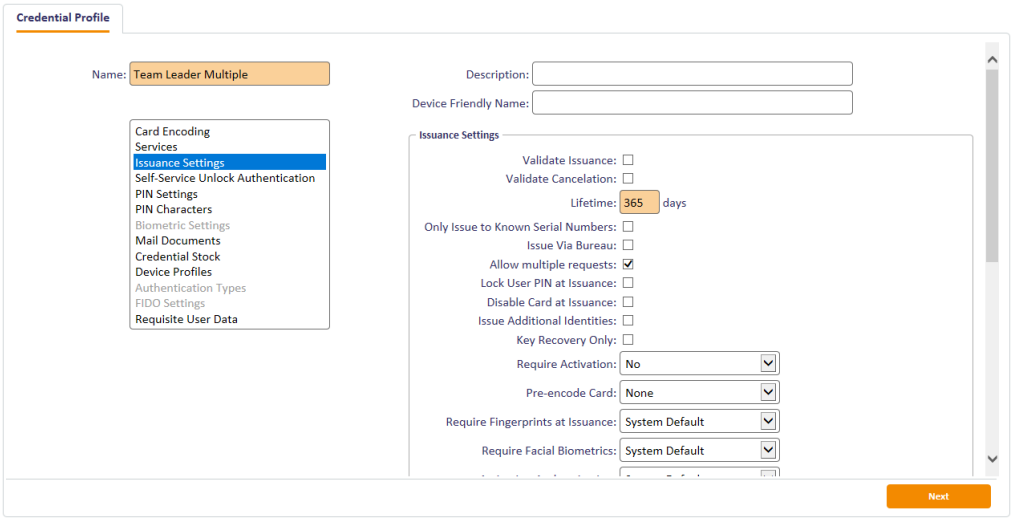
1. From the **Configuration** category, select **Operation Settings**.
2. On the **Issuance Processes** tab, set the following options:
   - **Maximum multiple credential requests** – set this to the maximum number of cards you want to request at one time. This option is for requests that require secondary

validation.

- **Maximum unvalidated multiple credential requests** – set this to the maximum number of cards you want to request at one time. This option is for requests that do *not* require secondary validation.

3. Click **Save changes**.
4. From the **Configuration** category, select **Credential Profiles**.
5. Create a new credential profile, or modify an existing profile.
6. In the **Issuance Settings** section, set the following option:
   - **Allow multiple requests** – set this option to allow operators to request multiple cards using this credential profile.

   Note: This option appears only if you have set **Maximum multiple credential requests** or **Maximum unvalidated multiple credential requests** to a value greater than 1.

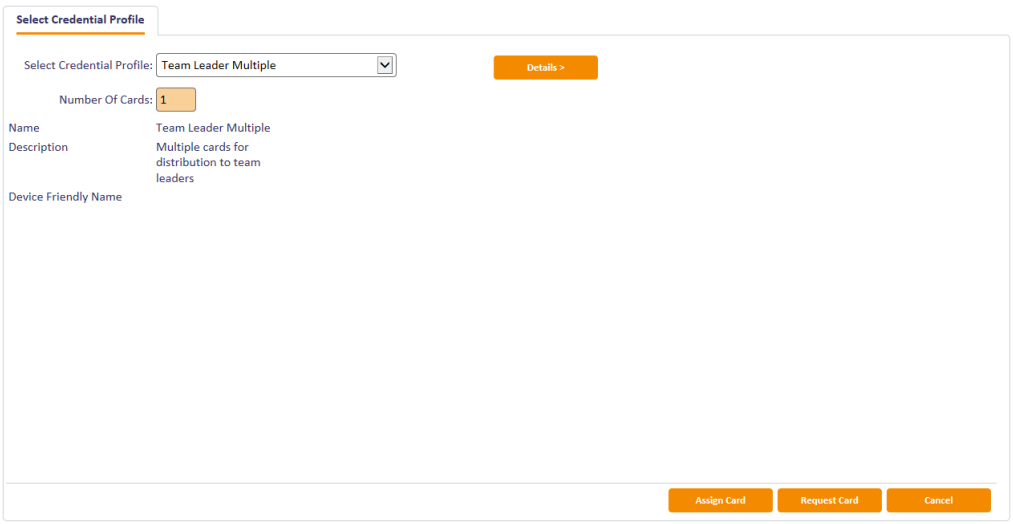


7. Complete the credential profile and save it.

To request multiple cards:

1. From the **Cards** category, select **Request Card**.
2. Select the user for whom you want to request multiple cards.

3. From the **Select Credential Profile** drop-down list, select a credential profile that has the **Allow multiple requests** option set.



4. In the **Number of Cards** box, type the number of cards you want to request for the user.
5. Click **OK**.

If you have requested more cards than are permitted by the **Maximum multiple credential requests** or **Maximum unvalidated multiple credential requests** option, MyID displays a warning, and you can adjust the number of cards requested.

5.2 Setting expiry dates for a card

Credential profiles include a **Lifetime** setting (see the *Credential profile options* section in the ***Administration Guide***) that determines either the lifetime of the card (the number of days for which it is valid).

It is possible to specify an expiry date for a specific card at the point at which you request the card. To enable this option:

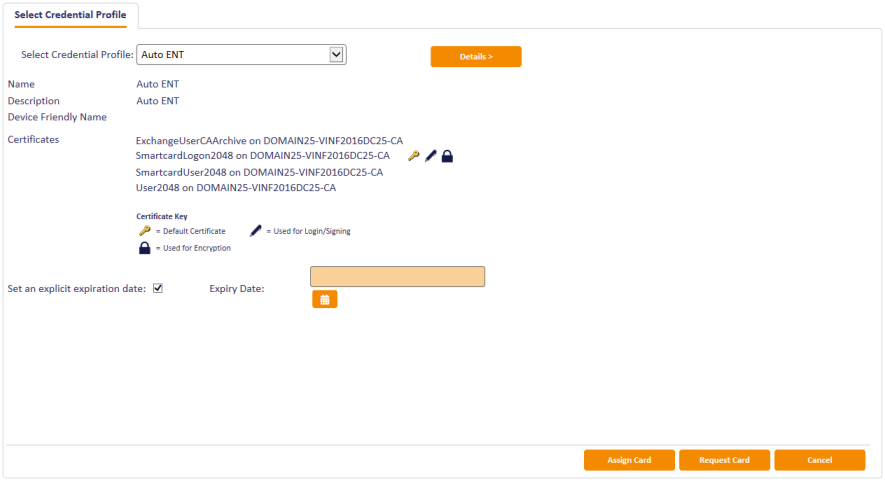
1. From the **Configuration** group, select **Operation Settings**.
2. Click the **Issuance Processes** tab.
3. Change the value of **Set expiry date at request** to Yes.
4. **Save** the changes.

The **Set an explicit expiration date** option is now displayed in the Select Credential profile stage; for example, when issuing or requesting a card.

Selecting this option displays an **Expiry Date** field where you can set a specific expiry date. This may be used, for example, if there is a fixed date from which the card is not required because someone is working on a fixed-length contract.

The card will expire at midnight on the date selected. If no date is specified, the card expires on the default date for the credential profile used. When the card is issued, the expiry date for the card is set at the shorter of the credential profile expiry date and the card-specific expiry date; for example:

- If a card is normally valid for one year but the card-specific expiry date is set for a date in 6 months' time, the card will expire in 6 months.
- If a card is normally valid for 30 days but the card-specific expiry date is set for a date in 2 months' time, the card will expire in 30 days.



Note: If you provide a date and this exceeds the **Maximum Expiry Date** set against the user account, the attempt to create the request is rejected. This does not occur if the credential profile requested has the **Ignore User Expiry Date** option enabled. The error recorded is:

```
Error: 0x800468e8 : A job cannot be created or updated as the specified expiry date exceeds the target users max request expiry date.
```

5.2.1 Known issues

- **IKB-324 – Removing an expiry date in the Validate Request workflow does not remove the date from the request**

  When using the **Validate Request** workflow in MyID Desktop, if the operator clears the explicit **Expiry Date** field, and the request is approved, the date is not removed from the request.

  This issue does not occur when using the MyID Operator Client.

  To work around this issue, cancel the request and repeat the request process, without specifying an expiry date.

5.3 Issuing replacement cards

When you request a replacement card, the type of replacement depends on the reason the card needs to be replaced.

- If the card is lost or destroyed permanently, the system cancels the card, revokes the certificates and requests a permanent replacement card.
- If the card is misplaced or forgotten, the system disables the card, suspends the certificates, and requests a temporary replacement card.

Certificates are treated differently, depending on whether they are archived, and whether the original certificates may have been compromised.

See section *6.5*, *Certificate reasons* for details of what happens to the certificates in the various card replacement scenarios.

For temporary replacement cards, you are strongly recommended to set up a temporary replacement credential profile. See section *5.3.7*, *Temporary replacement credential profiles* for details.

5.3.1 Issuing temporary replacement cards

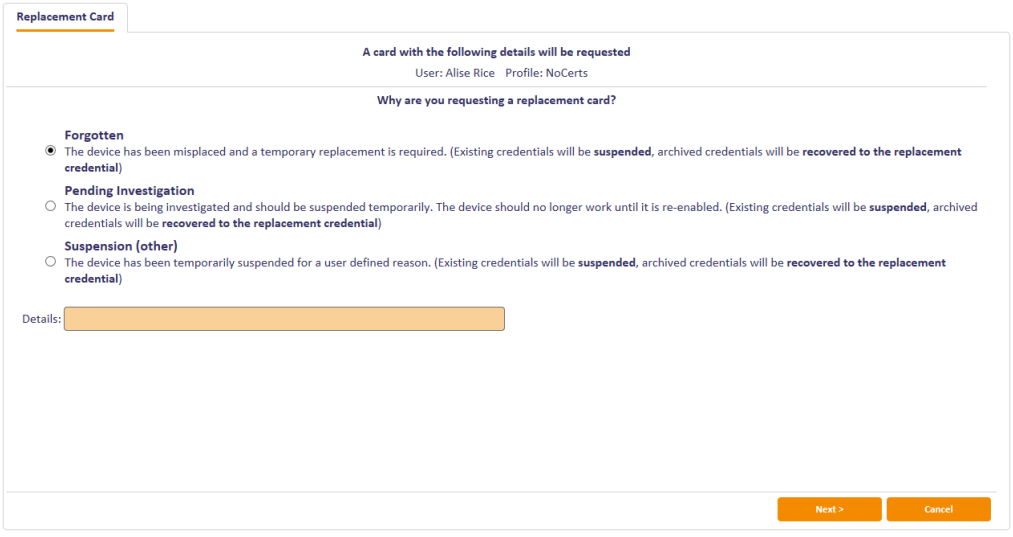
You can use the **Issue Temporary Replacement Card** workflow to issue a temporary replacement card to a user; for example, if the user has forgotten their card.

If there is a _temp credential profile for the card being replaced, it is used automatically. If there is no _temp credential profile available, the same profile as the original card is used. See section *5.3.7*, *Temporary replacement credential profiles* for instructions on creating a _temp credential profile.

To issue a temporary replacement card:

1. From the **Cards** category, select **Issue Temporary Replacement Card**.
2. Use the Find Person screen to search for the user to whom you want to issue a temporary replacement card.
3. Select the user from the list.

   The list of possible reasons for issuing a temporary replacement card appears.



4. Select the reason you are issuing a temporary card, then type the **Details**.

   See section *6.5*, *Certificate reasons* for details.
5. Click **Next**.
6. Insert the replacement card.
7. Type the **New PIN** and confirm it.
8. Click **Next**.
9. Print the card, if necessary.

5.3.2 Requesting a replacement card

The **Request Replacement Card** workflow allows you to request a replacement card.

Note: To allow you to select another person, you must have a role that has the **Choose Recipient** option selected under **Request Replacement Card** entry in the **Edit Roles** workflow.

1. From the **Cards** category, click **Request Replacement Card**.
2. To select the cardholder, use the Find Person screen to select the person.

   The cards assigned to the person are listed.
3. Select the card you want to replace.

   If the person has only one card, the workflow progresses to the next stage automatically.
4. Select a reason and provide **Details** for the card replacement.

   See section *6.5*, *Certificate reasons* for details.

   Note: If the **Delayed Cancellation Period** configuration option (on the **Devices** page of the **Operation Settings** workflow) is set to a value greater than `0`, there is an additional reason available: **Device Replacement (Delayed Cancellation)**. If you select this option, the device and its certificates are not canceled immediately, but are canceled after the number of hours specified in the configuration option.
5. To request a replacement card, click **Request Card**.

   To pre-allocate a specific replacement card, click **Assign Card**:

   - If the **Allow card serial number to be entered during Request Card workflow** option is set to `Yes`, you can enter the serial number.

     You can include `?` and `*` as wildcard characters; any unassigned devices, or devices with unrestricted cancellation, that match the search criteria are displayed; the device serial numbers must already be known to MyID. If more than 10 devices match the search criteria, you must search again with more restrictive criteria.
   - Alternatively, insert the card you want to allocate.

   MyID creates the replacement card request job.

The old card is canceled, and a job for a replacement card is created. The replacement card can be picked up using either the **Collect My Card** or the **Collect Card** workflow.

5.3.3 Permanent card replacement example

For a permanent replacement card, MyID issues a new card using the same profile as the old card.

The default behavior is as follows. Assuming that the card had two certificates, one of which was archived, the new card contains the following certificates:

- For the non-archived certificate, a new certificate using the same template.
- For the archived certificate, a new certificate using the same template. All future encryption is carried out using the new certificate.
- For the archived certificate, a number of historic recovered certificates.

The historic certificates allow you to decrypt any data encrypted with the original key.

MyID can determine whether archived or new encryption certificates are issued to a card based on the reason for the replacement; in situations when the card is still present, but is damaged or permanently blocked, MyID can issue archived encryption certificates instead of new certificates – the archived certificates are not revoked or suspended.

The behavior can be customized. Contact customer support for details.

5.3.4 Temporary card replacement example

For a temporary replacement card, MyID issues a new card.

If there is a _temp credential profile for the card being replaced, it is used automatically. If there is no _temp credential profile available, the same profile as the original card is used. See section *5.3.7*, *Temporary replacement credential profiles* for details.

Assuming that the card had two certificates, one of which was archived, the new card contains the following certificates:

- For the non-archived certificate, a new certificate using the same template.
- For the archived certificate, a copy of the archived certificate. As this is the same certificate, you can encrypt and decrypt data as if you were using the original card.

  Note, however, that if the credential profile has set the archived certificate to **Issue new**, a new certificate is issued instead. If you want a temporary replacement card to be issued a copy of the archived certificate, you must set the option for the archived certificate to **Use existing**.
- For the archived certificate, a number of historic recovered certificates.

By default, no historic recovered certificates are written to temporary cards. You can change the number of recovered certificates using the options on the credential profile.

5.3.5 Replacing temporary cards

A temporary replacement card should be used only for a short time. Temporary cards can be replaced in the following situations:

- The original card is found.

  Use the **Erase Card** workflow to cancel the temporary card, selecting the **Activate Original** reason. The temporary card is canceled, and the original card is re-enabled.
- The temporary card is forgotten.

  Use the **Request Replacement Card** workflow to request another card. The temporary card is canceled, and a new temporary replacement of the original card is issued.
- The temporary card is lost or stolen, or the original card is compromised.

  Use the **Request Replacement Card** workflow to request another card. The temporary card is canceled, the original card is canceled, and a permanent replacement card is issued.

5.3.6 Canceling temporary cards

If you cancel or erase a temporary card with any reason other than **Found Original**, the original card is also canceled.

5.3.7 Temporary replacement credential profiles

For temporary replacement cards, you are strongly recommended to set up a temporary replacement credential profile, to consider carefully who can receive the temporary card, to restrict its lifetime, and consider which certificates you want to include on it. If you do not specify a temporary replacement credential profile, the original credential profile is used instead – this may not be appropriate for your security policies.

You can specify an alternative credential profile to be used automatically for temporary replacement cards. Create a credential profile (see the *Managing credential profiles* section in the ***Administration Guide***) and give it the name `<profile>_temp`. For example, if your permanent card is issued with the profile `Employee`, create the alternative profile with the name `Employee_temp`.

Note: Credential profile names are case-sensitive.

Set up this profile to issue a signing certificate – this does not have to be the same as the signing certificate on the original card. When the card is issued, you can recover any historic encryption certificates to the card. The original signing certificate is suspended.

When the forgotten card is found, the temporary card is canceled. This revokes the temporary signing certificate, unsuspends the original signing certificate, and leaves the encryption certificate active.

`_temp` credential profiles do not apply to permanent replacement cards.

See section *5.3.1*, *Issuing temporary replacement cards* for details of the **Issue Temporary Replacement Card** workflow.

5.4 Activating cards

You can configure MyID to issue cards, but render them locked and unable to be used until the cardholder has gone through an activation process. This process allows the cardholder to enter a PIN for their card and to activate it, ready for use.

You can configure MyID to allow cardholders to activate their cards themselves (using MyID Desktop, the Self-Service App, or the Self-Service Kiosk) or to be guided through the process by an operator using the **Assisted Activation** workflow.

For information on setting up card activation, see the *Activating cards* section in the ***Administration Guide***.

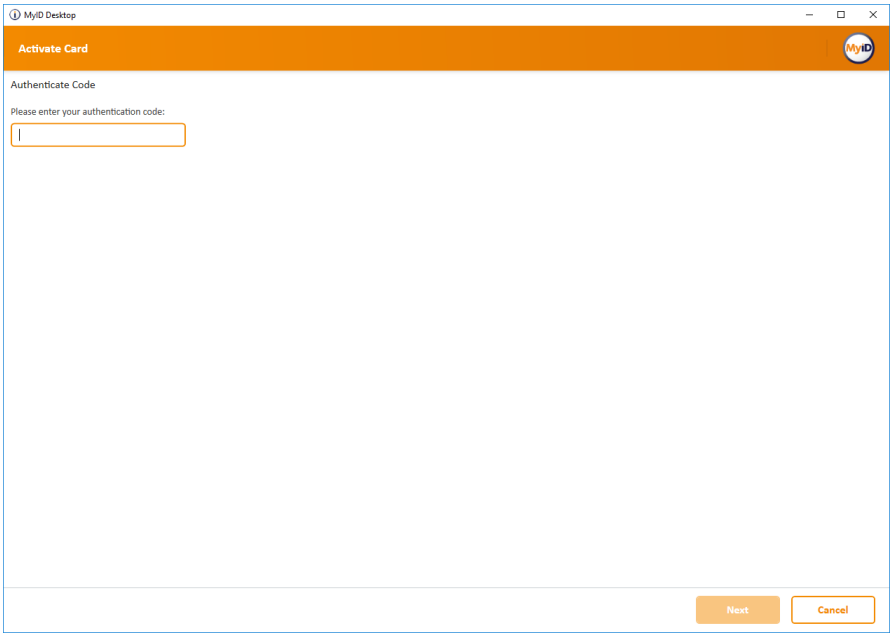
5.4.1 Activate card

When a card has been issued, encoded and distributed to an applicant, the applicant can activate the card using MyID.

1. Insert a card that has been issued.
2. Click **Smart Card Logon**.
3. Select the smart card, if there is more than one inserted into your card readers.

   The details of the activation process depend on how the credential profile is set up. See the *Setting up authentication methods for activation* section in the ***Administration Guide*** for details.

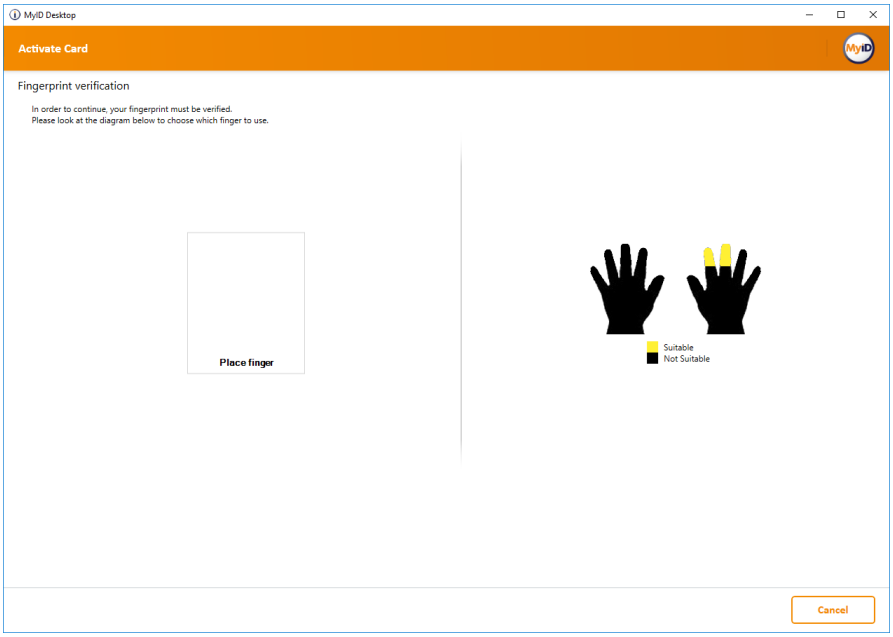
   - If the credential profile is set up to require an authentication code, type it in the **Authentication Code** box.



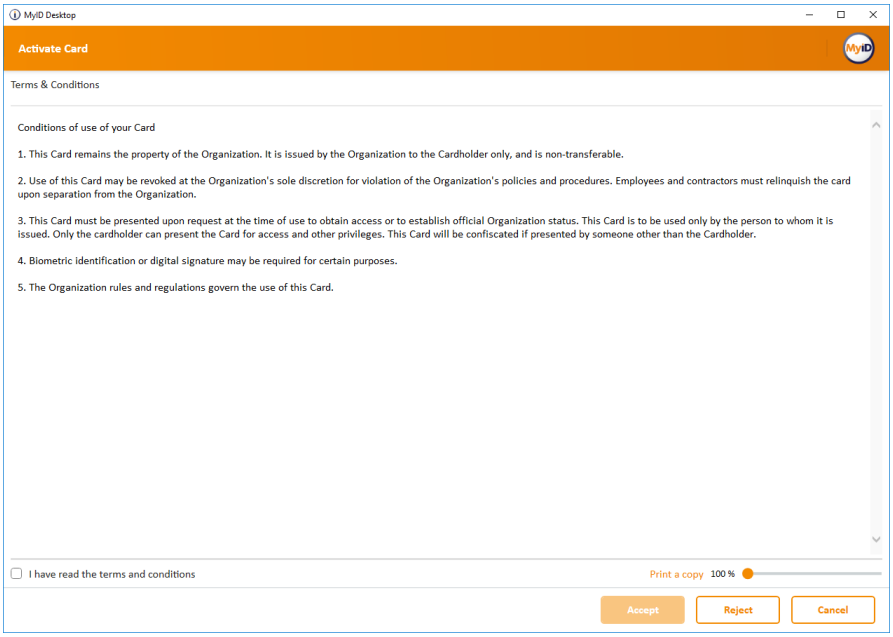
You will have been sent an email containing the authentication code. If you make several invalid attempts to enter the code (as determined by the **Maximum Allowed OTP Failures** configuration option), the activation code is canceled, and you must ask an administrator to generate another code.

As soon as the authentication code has been accepted, you cannot use it again, even if you quit the workflow without completing it. You must request another code from an administrator.

- If you are required to carry out biometric authentication, provide a biometric sample.



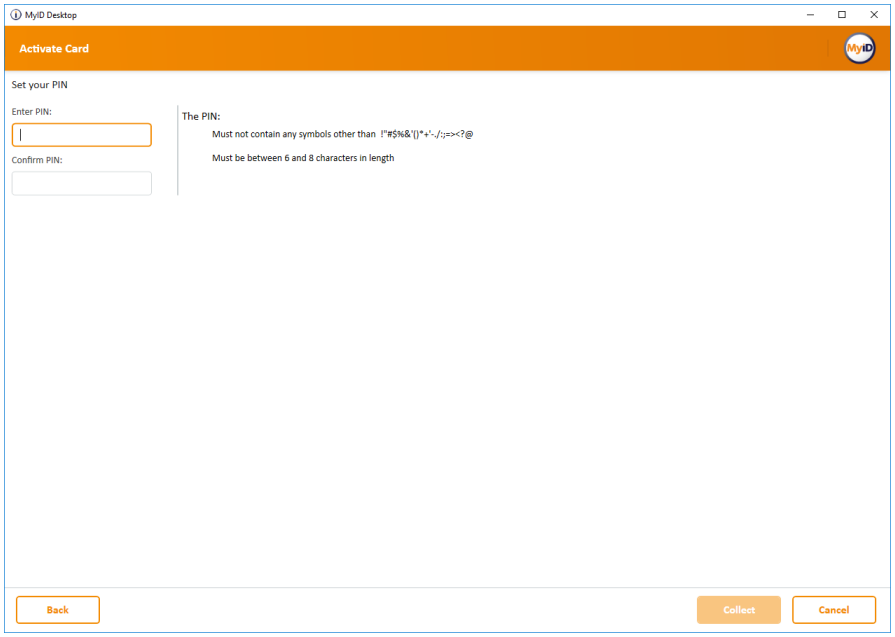
- If you are required to accept a set of terms and conditions, read the terms and conditions, then click **Accept**.



If you decline the terms and conditions, your authentication code (if you have one) cannot be used again, so you must request another code from an administrator.

Note: You can amend the terms and conditions that users agree to when they activate their cards. See the *Customizing terms and conditions* section in the ***Administration Guide*** for details.

4. Enter your PIN, then click **Continue**.



Your acceptance of the terms and conditions is digitally signed and audited.

5. Remove your card and click **Finish**.

5.4.2 Assisted activation

If you have set the **Require Activation** option in the credential profile to **Assisted Activation only**, the applicant must go to the trusted agent with the card to be activated. The trusted agent can then use the **Assisted Activation** workflow to activate the card for the applicant.

Note: The trusted agent must have access to the **Assisted Activation** workflow. Use the **Edit Roles** workflow to add the workflow to the required roles.

To perform an assisted activation:

1. From the **Cards** category, select **Assisted Activation**.
2. Insert the card to be activated into a card reader.

   MyID checks that the card is ready to be activated.
3. Complete the identity checks that authenticate the user.

   The cardholder may be asked to provide biometric authentication or a one-time authentication code.

   If the system is set up for biometric authentication, you may be able to select the **Operator Bypass** button and then provide alternative details of the user's authentication; for example, by reviewing their identity documents.

   You may have more than one operator authentication tab available; you do not need to complete more than one tab.

   See the *Setting up authentication methods for activation* section in the ***Administration Guide*** for details.
4. Click **Next**.
5. If you have configured the credential profile to require **Simple Confirmation** terms and conditions, ask the cardholder to read the Terms & Conditions, select the **I have read the terms and conditions** option, and click **Accept**.
6. Ask the cardholder to enter and confirm the PIN for their new card, then click **Continue**.
7. If you have configured the credential profile to require **Explicitly Confirm** or **Counter Sign** terms and conditions, ask the cardholder to read the Terms & Conditions, select the **I have read the terms and conditions** option, and click **Accept**.

   The terms and conditions template is configured in the credential profile. For details of configuring templates, contact customer support, quoting reference SUP-255.
8. If you have configured the credential profile to require **Counter Sign** terms and conditions, enter the PIN of your own operator card and click **OK**.

   For **Silent**, **Explicitly Confirm**, and **Counter Sign** terms and conditions, MyID digitally signs the terms and conditions with the signing certificate on the cardholder's card. For **Counter Sign** terms and conditions, the terms and conditions are additionally signed with the operator's signing certificate.

   If you set the **Persist terms and conditions** configuration option (on the **Devices** tab of the **Operation Settings** workflow) to Yes, MyID stores the terms and conditions that were signed as a binary object in the database. This is then visible in the audit report.

This **Persist terms and conditions** option allows you to review the terms and conditions as they stood when the cardholder accepted them, rather than the terms and conditions as they currently stand, which may be different if you have updated the text of the terms and conditions.

Note: The terms and conditions are stored in the database only if the credential profile is for configured for activation, and the cardholder accepts the terms and conditions during the device activation.

MyID then completes the card activation.

Note: If there is more than one credential profile version available, the version that was current when the card was collected is used.

5.5 Delivering cards

The **Deliver Card** workflow allows you to mark cards as delivered within MyID. This allows you to have a delivery stage within the card issuance process that allows you to confirm that the device has been delivered to the applicant; for example, a card issuance officer can hand over the card directly to the applicant, verifying the applicant's identity in the process, and then mark the card as safely delivered. This also provides an additional level of security, as it is not possible to activate the card until it is marked as delivered to the cardholder.

Once the card has been marked as delivered, the cardholder can proceed to activate the card, either through self-service, or through assisted activation, where an operator guides the applicant through the activation process.

Note: The **Deliver Card** workflow is not automatically assigned to any roles after installation. You must use the **Edit Roles** workflow to assign the **Deliver Card** workflow to the appropriate role.

5.5.1 Configuring the card delivery process for a delivery stage

To make sure that all card issuances that require activation must go through a delivery stage before the card can be activated, you must set the **Deliver Card Before Activation** configuration option to `Yes`.

This setting affects all issuances carried out using the MyID system.

To set the option:

1. Open the **Operation Settings** workflow:
   - In MyID Desktop, from the **Configuration** category, select **Operation Settings**.
   - In the MyID Operator Client, from the **More** category, select **Configuration Settings > Operation Settings**.
2. On the **Devices** tab, set the **Deliver Card Before Activation** configuration option to `Yes`.
3. Click **Save changes**.

5.5.2 Issuing a card that requires a delivery stage

You can issue cards that require a delivery stage either through a bureau or directly through MyID. You must make sure that the card profile is set up to require activation; you can include a delivery stage only as a precursor to card activation.

For bureau issuance, when the bureau returns the manifest file, MyID updates the card request to `Completed` status, and creates a card activation job with the status `Awaiting Delivery`. An operator must then mark the card as delivered before the applicant can activate the card.

For direct issuance, when the issuer uses MyID to issue the card (optionally including printing the surface of the card), MyID creates a card activation job with the status `Awaiting Delivery`. An operator must then mark the card as delivered before the applicant can activate the card.

5.5.3 Marking cards as delivered

The **Deliver Card** workflow allows you to mark cards as delivered.

Alternatively, you can use the **Accept Delivery** feature in the MyID Operator Client; see the *Accepting delivery for a device* section in the ***MyID Operator Client*** guide for details. This feature also allows you to accept delivery for several devices at the same time.

To mark cards as delivered:

1. From the **Cards** category, select **Deliver Card**.
2. On the Select Job screen, type the search details for the card activation job you want to mark as delivered.

   You can use an asterisk (`*`) as a 'wildcard' in either the name fields, to represent one or more characters. For example:

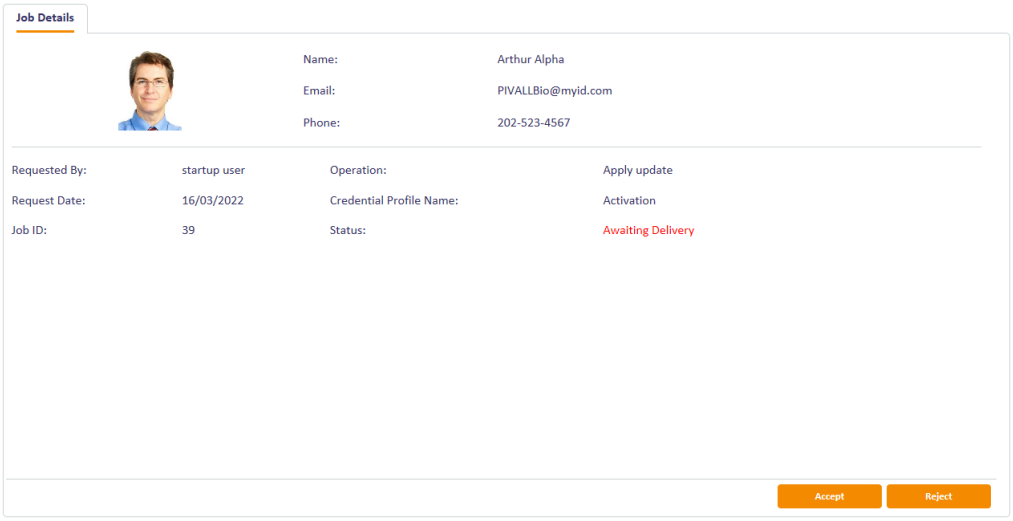
   - `El*` will find all names beginning with 'El'.
   - `*beth` will find all names ending in 'beth'.
   - `El*beth` will find all names that begin with 'El' *and* end with 'beth'.

   You can search for the agency the cardholder belongs to. Click **Include Subagencies** to search for agencies below the selected agency in the agency hierarchy.

   From the **Maximum Records** drop-down list, select the maximum number of records you want to return.
3. Click **Search**.

   The results of your search are displayed on screen.
4. Click on a job to select it.

   The Job Details screen displays the details of the card activation job. The **Status** field should display **Awaiting Delivery**.



5. Click **Accept** to accept the card activation job. The card activation job is set to `Awaiting Issue`. The cardholder can then activate their card.

   Click **Reject** to reject the card activation job. The card activation job is set to `Canceled`. The cardholder cannot now activate their card.

   If you reject the card activation job, you must provide a reason for the rejection; this reason is added to the audit trail.

   Note: If you reject a card, it remains on the system in its current state. To ensure that any existing certificates on the card are canceled and the card is no longer associated with the cardholder, you should cancel the card using the **Erase Card** workflow.

5.6 Batch issuing cards

If you have more than one card to issue, you can request and issue cards in batches using the **Batch Request Card** and **Batch Collect Card** workflows.

5.6.1 Requesting a batch of cards

You can request a batch of cards for people using the **Batch Request Card** workflow.

To request a batch of cards:

1. From the **Cards** category, click **Batch Request Card**.

   You can also launch this workflow from the **Batch** section of the **More** category in the MyID Operator Client. See the *Using Batch workflows* section in the ***MyID Operator Client*** guide for details.

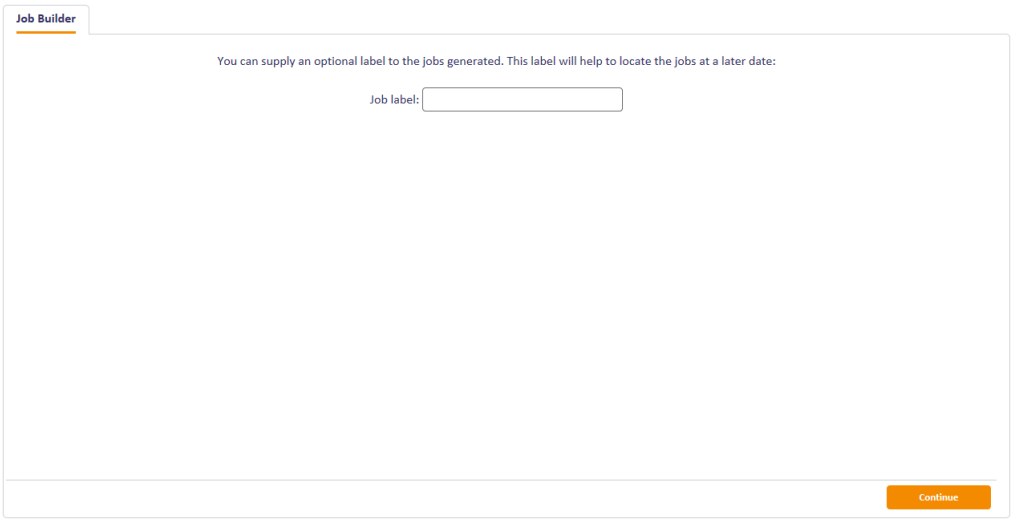
2. Use the Find Person screen to search for the people to whom you want to issue cards.
3. In the Search Results screen, select one or more people then click **Next**.
4. Select the credential profile you want to use from the list, then click **OK**.

   If the users are selected from your directory, they are added to the MyID database.

   MyID validates the users against the selected credential profile. If a user does not pass any requisite data checks set up on the credential profile (for example, if the credential

profile is designed for Windows logon, and the user does not have a UPN) no request is created for that user. See the *Requisite User Data* section in the ***Administration Guide*** for details.

5. Optionally, type a **Job label** then click **Continue**.



MyID creates card request jobs for each of the people you selected. If the credential profile you selected requires secondary validation, you must validate each request individually using the **Validate Request** workflow.

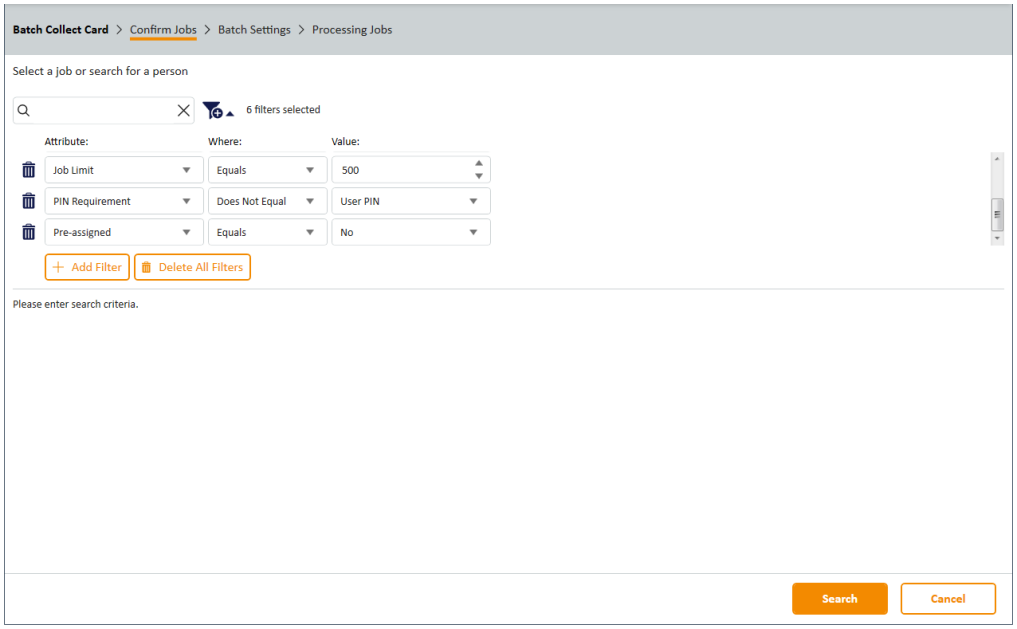
5.6.2 Collecting a batch of cards

You can collect a batch of cards in one operation. You can collect cards that have been requested as a batch, or cards that have been requested individually.

To collect a batch of cards:

1. From the **Cards** category, click **Batch Collect Card**.

   You can also launch this workflow from the **Batch** section of the **More** category in the MyID Operator Client. See the *Using Batch workflows* section in the ***MyID Operator Client*** guide for details.



2. Enter the search details for the job, then click **Search**.

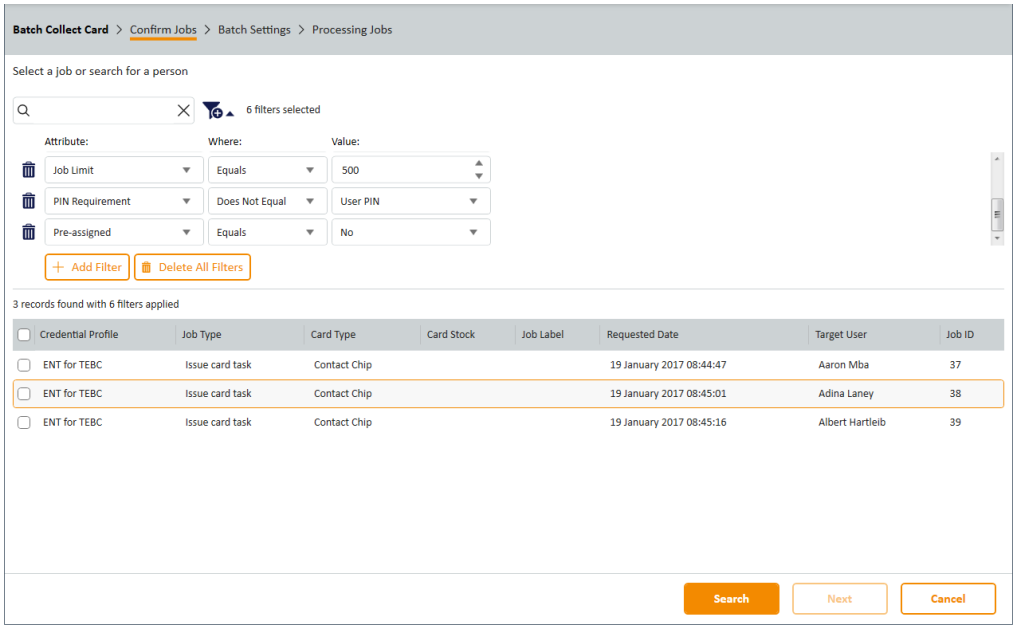
   If you entered a label for the job in the **Batch Request Card** workflow, you can add a **Job Label** field to the filter to search only those requests.

   The default filters provide a list of options that are suitable for the majority of batch collections. For example, you are recommended to use `PIN Requirement Does Not Equal User PIN`, and use an automatically-generated PIN instead; cards set for manual PIN entry are skipped by the workflow. You are also recommended to use `Pre-assigned Equals No`, as jobs that require a card with a specific serial number are skipped by the workflow.

   For details of using search filters, see section *2.2.3*, *Using advanced search*.

   Note: The search returns a maximum of 500 jobs. You can specify a lower number if you set a **Job Limit** in the filter. If more jobs match your search criteria than you specify in the **Job Limit**, these jobs are returned in database order, not necessarily date order, and may contain partial selections from several different batches. You are recommended to use the search filters to return only those records you want to process.

3. Click **Search**.

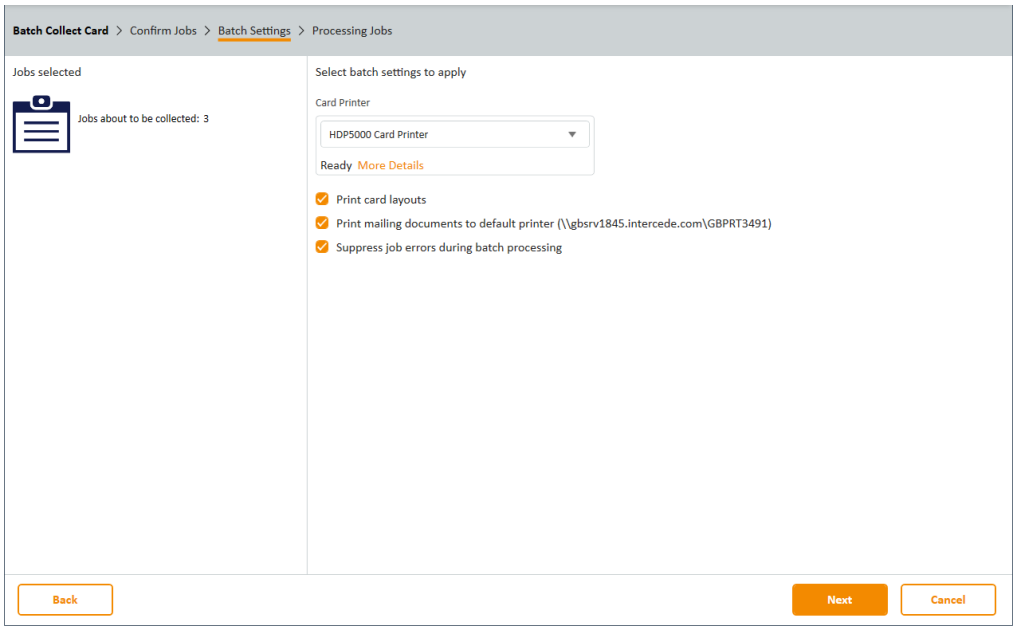


The list of matching jobs appears.

4. Select the jobs you want to collect.

   You can select some or all of the jobs in the list. To select all of the jobs, click the check box at the top of the list.

5. Click **Next**.



6. Set the options for issuing the card:

   - **Print card layouts** – the default card layout as specified in the credential profile, or the card layout specified through the Lifecycle API, is used to print each card.

- **Print mailing documents to default printer** – the mailing document specified in the credential profile for each card is sent to your Windows default printer.

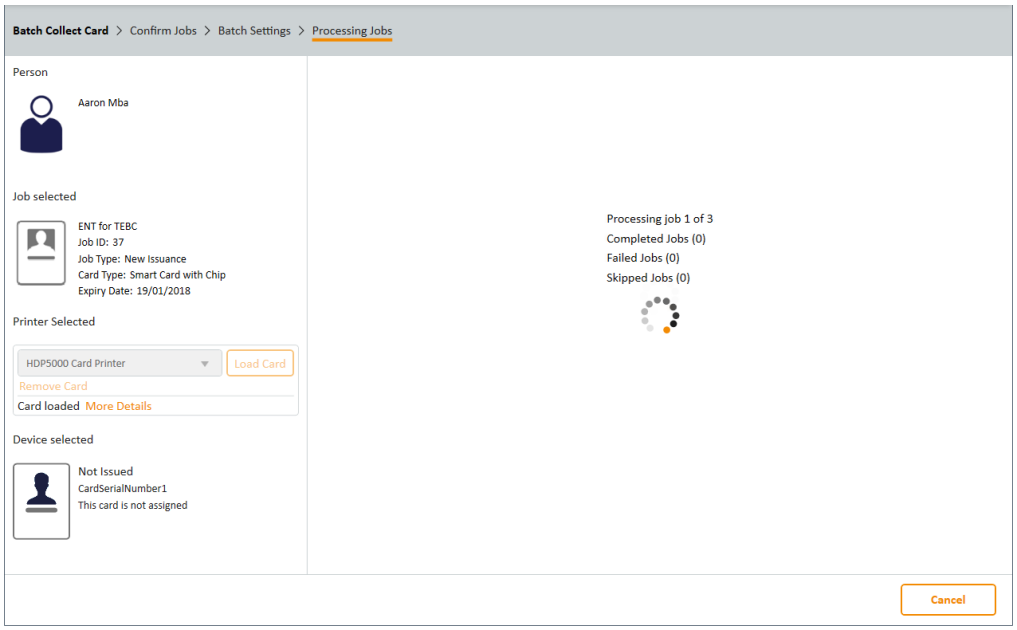
  Note: If you are printing mailing documents, make sure that your default printer is a document printer, and not a card printer.

- **Suppress job errors during batch processing** – any errors that occur are not displayed, but are included in the audit log.

Note: ATR errors, which are caused by MyID being unable to recognize the type of card being presented, will still appear on screen.

If you suppress job errors, a warning that the credential is not configured in accordance with your security settings (for example, GlobalPlatform keys have not been configured) results in the card not being issued; if you choose *not* to suppress job errors, you can override these warnings individually.

7. Click **Next**.



MyID issues and prints the cards one by one. If an individual collection job fails, it is returned to the list of available jobs, and you can re-run the **Batch Collect Card** workflow to collect it.

Information about the number of successfully-collected jobs and failed jobs is displayed at the end of the workflow.

- **IKB-216 – Magnetic stripe only card issuance not supported in Collect Card or Batch Collect Card**

  It is not currently possible to use the **Collect Card** or **Batch Collect Card** workflow to issue a card with magnetic stripe encoding only – that is, without additional contact chip or contactless encoding. Jobs that require magnetic stripe only are omitted from the search results.

5.7 Updating cards

You can update cards to the latest version of the credential profile, or update them to different credential profiles.

Note: When you update a card, it does not change the expiry date for the card, even if you have changed the lifetime in the credential profile. This also means that if you add a certificate to the card that is constrained to the card's lifetime, the certificate is constrained to the card's original lifetime, not the lifetime specified in the updated credential profile.

5.7.1 Updating a card

The **Update Card** workflow allows you to update a card that is present.

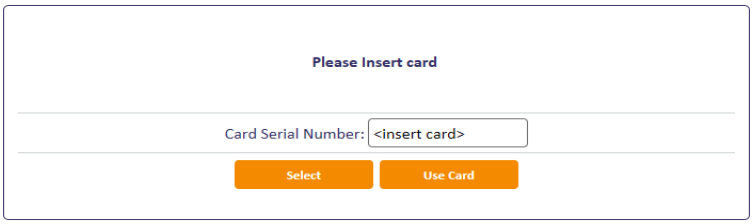
Note: You cannot carry out card updates in the following situations:

- When upgrading to a new credential profile or updated credential profile that has a different data model to the original card.
- When adding applets to an existing card.
- When changing which certificates are used for signing or encryption without replacing the certificates.

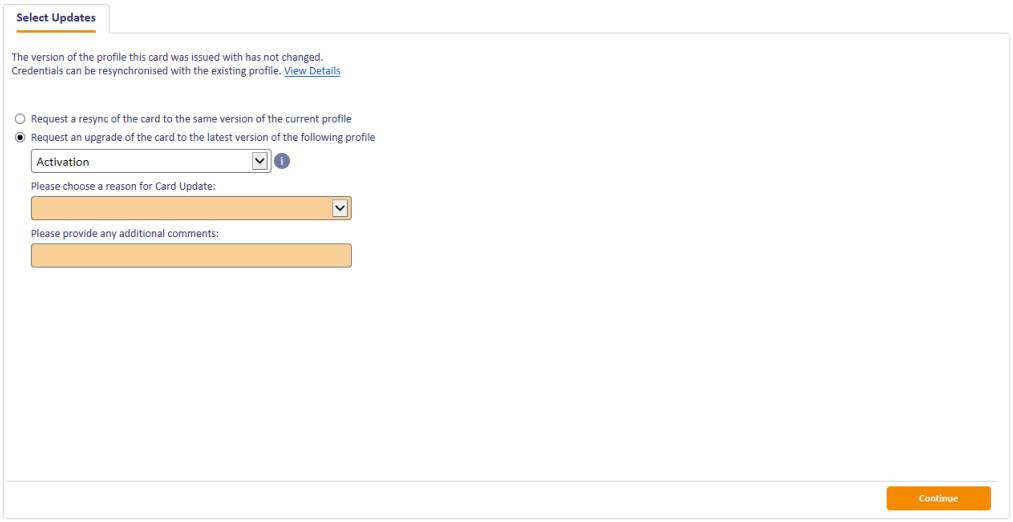
In these situations, you are recommended to reprovision the card (see section *5.17*, *Reprovisioning cards*) or request a card update with a reprovisioning reason, and let the cardholder update their card using the Self-Service App.

To update a card:

1. From the **Cards** category, click **Update Card**.



2. Insert the card you want to update, then select it from the list.



3. Select one of the following options:
   - **Request a resync of the card to the same version of the current profile** – MyID will resynchronize the card to match the credential profile at issuance; for example, if a certificate has been revoked on the card, an update job is created to issue a new certificate and remove the old one. This option is available only if the credential profile has not changed.

- **Request an upgrade of the card to the latest version of the current profile** – MyID will create an update job to upgrade the card to the latest version of its current profile. This option is available only if the credential profile has changed.
- **Request an upgrade of the card to the latest version of the following profile** – select a credential profile from the drop-down list, and MyID will update the card to use the latest version of the specified credential profile.

4. Select the reason for the card update from the drop-down list.

   See section *6.5*, *Certificate reasons* for details.

5. Click **Continue**.
6. Enter the card's PIN, then click **Next**.

   MyID updates the card.

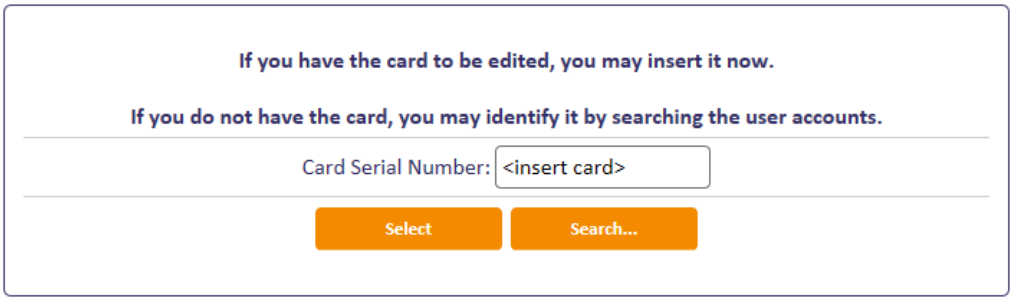
5.7.2 Requesting a card update

The **Request Card Update** workflow allows you to create a job that updates or reprovisions a card. Users can then use the Self-Service App to collect the updates, or an operator can collect the update using the **Collect Updates** workflow. You can request the update whether you have the card present or not.

Alternatively, you can use the **Request Update** feature on the View Device screen in the MyID Operator Client to request updates for a device. See the *Requesting an update for a device* section in the ***MyID Operator Client*** guide for details.

To request a card update:

1. From the **Cards** category, click **Request Card Update**.

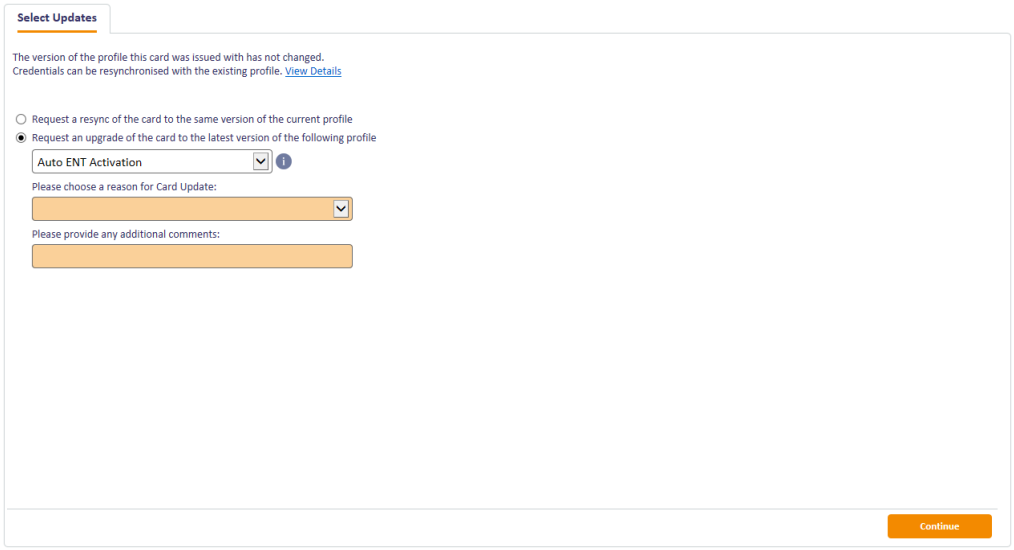


2. If you have the card present, insert it and click **Edit**.

   If you do not have the card present:

   a. Click **Search** then use the **Find Person** screen to find the user.

   b. If the user has more than one card, select the card you want to update.



3. Select one of the following options:
   - **Request a resync of the card to the same version of the current profile** – MyID will resynchronize the card to match the credential profile at issuance; for example, if a certificate has been revoked on the card, an update job is created to issue a new certificate and remove the old one. This option is available only if the credential profile has not changed.
   - **Request an upgrade of the card to the latest version of the current profile** – MyID will create an update job to upgrade the card to the latest version of its current profile. This option is available only if the credential profile has changed.
   - **Request an upgrade of the card to the latest version of the following profile** – select a credential profile from the drop-down list, and MyID will create an update job to update the card to use the latest version of the specified credential profile.

     Note: If the new credential profile has the **Validate Issuance** option set, an operator must validate the request before the cardholder can collect the update or reprovision job; see section *5.1.3*, *Validating a card request*. Updating to a newer version of the same credential profile does *not* require validation.
4. Select the reason for the card update from the drop-down list.
   - **User details have changed** – carries out a full reprovision of the card.
   - **There is a problem with the device** – carries out a full reprovision of the card.
   - **New credential profile needs to be applied** – carries out a full reprovision of the card.
   - **New certificates need to be added to the device** – carries out an update of the card. This option is intended to add new certificates to an existing card.

   If the reason you selected requires a full reprovision, the cardholder must collect the update using the Self-Service App, or an operator must use the **Collect Updates** workflow on their behalf.

Note: Reprovisioning erases and rewrites the card content. If you interrupt the reprovisioning process after the initial card authentication has taken place (for example, by pulling your card from the reader, canceling the workflow, or shutting down the Self-Service App) your smart card may be left in an unusable state. To remedy this, carry out the reprovisioning process again, or cancel and reissue the smart card.

For more information about reprovisioning, see section *5.17*, *Reprovisioning cards*.

If the reason you selected carries out a simple update, the cardholder can collect the update using the Self-Service App, or using the **Collect My Updates** workflow in MyID Desktop. An operator can collect the update on their behalf using the **Collect Updates** workflow.

Note: If you have an upgraded system, you may see additional options in this list, all of which carry out updates, not reprovisions; you are recommended to use the options listed above, but you may continue to use the options provided in previous versions of MyID. See section *6.5*, *Certificate reasons* for details of the behavior of these options.

5. Click **Continue**.

   MyID creates a job that will update or reprovision the card.

   If the **Cancel Outstanding Updates** configuration option (on the **Bureau & Job** page of the **Operation Settings** workflow) is set to Yes, any outstanding card update, certificate renewal, or reprovision card jobs that exist for the selected credential are automatically canceled.

   You can use the **Job Management** workflow to view and manage card update and reprovision jobs. See the *Job management* section in the ***Administration Guide*** for details.

Note: Depending on your configuration, an email notification may be issued to the cardholder on completion of this workflow. For example:

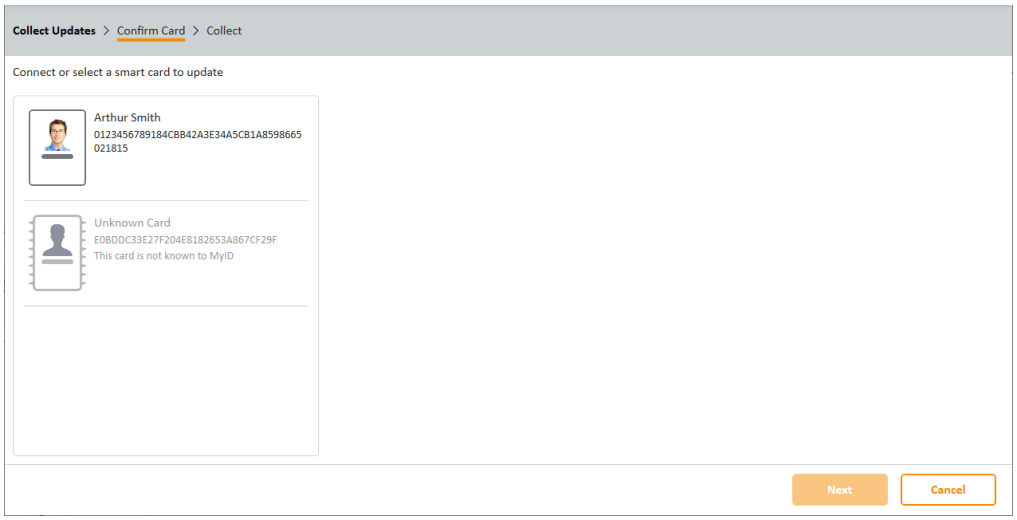
```
"Your Card is ready for issue. Please follow the instructions for issuance
of a new card".
```

5.7.3 Collect Updates workflow

The **Collect Updates** workflow allows you to collect an update that has been requested for another cardholder. You can collect both simple updates (including certificate renewals) and reprovisions using this workflow.

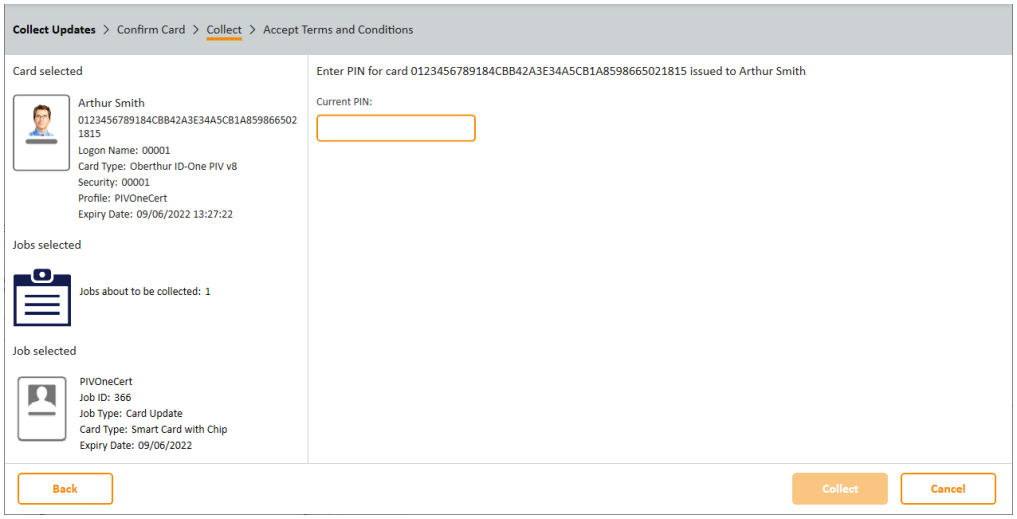
To collect an update:

1. From the **Cards** category, select **Collect Updates**.



2. Insert the card you want to update, select it from the list, then click **Next**.

   If the card has no updates available, the screen displays a message that there are no update jobs pending. Click **Cancel** to end the workflow.



3. Follow the on-screen prompts.

   If the **Verify fingerprints during card update** configuration option (on the **Biometrics** page of the **Operation Settings** workflow) is set, you may be asked to provide the cardholder's fingerprints, depending on the current setting of the **Verify Fingerprints During Card Update** option in the **Issuance Settings** section of the credential profile used to issue the device:

   - If **Verify Fingerprints During Card Update** is **Always**, you must provide fingerprint verification. If the cardholder does not have fingerprints enrolled, you cannot collect the update.
   - If **Verify Fingerprints During Card Update** is **Preferred**, you must provide fingerprint verification if the cardholder has fingerprints enrolled. If the cardholder does not have fingerprints enrolled, you can collect the update without fingerprint

verification.

- If **Verify Fingerprints During Card Update** is **None**, you can collect the update without fingerprint verification

Depending on the type of update, you may need to enter the card's current PIN (for a simple update or certificate renewal) or to provide a new PIN (for a reprovision).

4. Click **Collect**.

   MyID updates the card.

5.7.4 Collect My Updates workflow

The **Collect My Updates** workflow allows you to apply updates (for example, certificate renewals) to your card.

Note: You cannot use the **Collect My Updates** workflow to carry out updates that require a full reprovision. You must use the Self-Service App to collect reprovision jobs.

1. Log on to MyID using your card.
2. Click the **Cards** category.
3. Click the **Collect My Updates** workflow.

   The system checks to see if any updates are available. If there are updates available, the workflow continues.
4. Enter your PIN when prompted.

   The system applies the updates to your card one by one. If you have more than one update, you may be prompted to enter your PIN for each update.

5.8 Identifying cards

MyID provides the following workflows that allow you to view the details of a smart card or other device:

- **Identify Card** – provides basic information about the device.
- **Identify Device (Administrator)** – provides additional information, including the initial server-generated PIN, if available.

You can assign the appropriate workflow using the **Edit Roles** workflow, depending on what information is required by the operator. Do not assign the **Identify Device (Admin)** workflow to operators who do not need to view the additional information.

5.8.1 Using the Identify Card workflow

To identify a card:

1. From the **Cards** category, click **Identify Card**.

   The Select Card dialog appears.
2. To specify the card you want to identify, you can do one of the following:
   - Insert the card, then select it from the Select Card dialog
   - Close the Select Card dialog, click **Search**, then use the Find Person screen to find the person and the card.

MyID then displays the information for the selected card. The tabs provide the following information:

- **Details** – the details of the user and card, including logon name and the card's serial number.
- **Certificates** – details of the certificates present on the card.
- **Biometrics** – allows you to verify the cardholder's fingerprints. Select the biometric reader you want to use from the drop-down list, then click the fingerprint icon.

  Note: You must set the **Initialize and script ActiveX controls not marked as safe for scripting** option in Internet Options on the client PC to use this feature. See the *Configuring Internet Options* section in the ***Installation and Configuration Guide*** for details.
- **All** – a list of all cards issued to the cardholder.
- **Card History** – the history of the card, including details of issuance and when the card was used for various operations. This includes details of previous holders of the card. Double-click a row to view more details.

Note: The **Card History** tab appears only if your role includes the **View Device Details** option in the **Cards** section of the **Edit Roles** workflow.

3. Click **Identify**.
4. Click **Back** to identify another card, or **Finish** to complete the workflow.

5.8.2 Using the Identify Device (Administrator) workflow

To identify a device and view additional information:

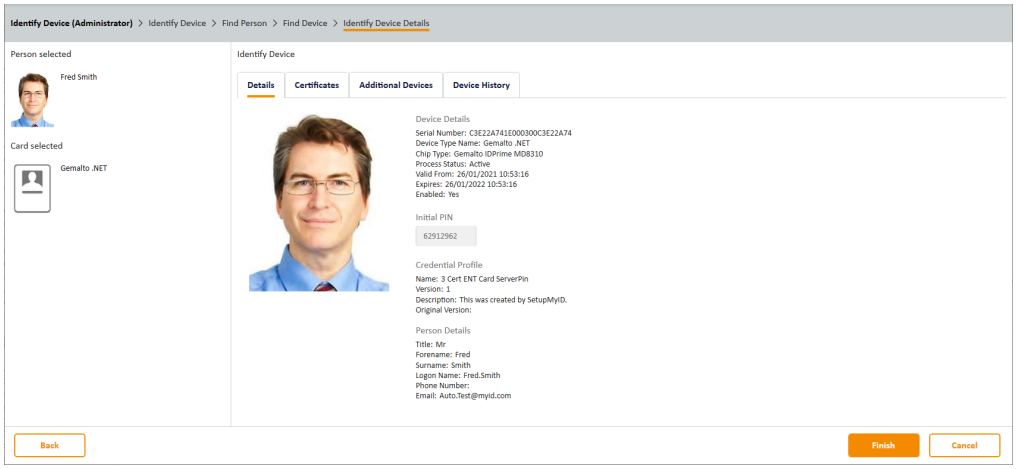
1. From the **Cards** category, click **Identify Device (Administrator)**.

   You can also launch this workflow from the View Device screen in the MyID Operator Client; this launches the workflow with the device already selected. See the *Viewing extended information about a device* section in the ***MyID Operator Client*** guide for details.
2. Select the device you want to identify.

   You can use the following methods:

   - Insert the device into the PC, *or*:
   - Click **Skip**, use the Find Person screen to select the device owner, then select the device from the person's list of issued devices.

   The Identify Device Details screen appears.



The following information is available:

- **Details** tab.

  Contains the following information:

  - Device Details – information about the device, including serial number, type, and expiry date.
  - Initial PIN – the PIN generated by MyID when the device was issued; this is available only if the credential profile specified a server-generated PIN that used the **EdeficePinGenerator** algorithm.

    Note: You can view PINs generated using the **EdeficePinGenerator** *or* **EdeficePolicyPinGenerator** algorithm on the View Device screen in the MyID Operator Client; see the *Viewing the initial PIN for a device* section in the ***MyID Operator Client*** guide for details.
  - Credential Profile – information about the credential profile used to issue the device, including the name, description, and version of the credential profile.
  - Person Details – information about the device owner, including name, logon name, and email address.

- **Certificates** tab.

  Contains details of all certificates present on the device, including any recovered certificates.

- **Additional Devices** tab.

  Contains a list of all devices assigned to the owner of the selected device.

- **Device History** tab.

  Contains the recent audit history for the selected device.

  For more information on the audit trail for the device, you can use the **Audit Reporting** workflow.

3. Click **Finish** to complete the workflow.

5.9 Printing mailing documents

The **Print Mailing Document** workflow allows you to print the mail merge document associated with a card. The workflow uses the credential profile the card was issued with; any changes to the credential profile made after to the card is issued (such as the location of the mailing document) are ignored.

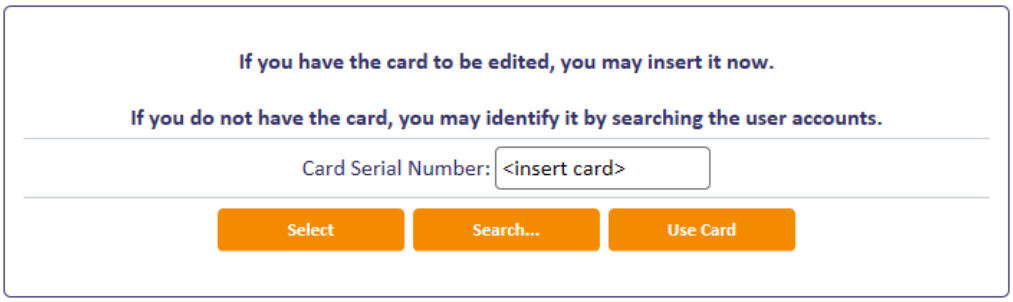
Note: These are not the same mailing documents that are used by the **Collect Card** workflow. The **Collect Card** workflow uses a new system that is currently available only in **Collect Card**.

For information on setting up mail merge documents for a credential profile, see the *Setting up mail merge documents* section in the ***Administration Guide***.

To print a mail merge document:

1. From the **Cards** category, click **Print Mailing Document**.

   You can also launch this workflow from the View Device screen in the MyID Operator Client; this launches the workflow with the card already selected. See the *Printing a mailing document* section in the ***MyID Operator Client*** guide for details.

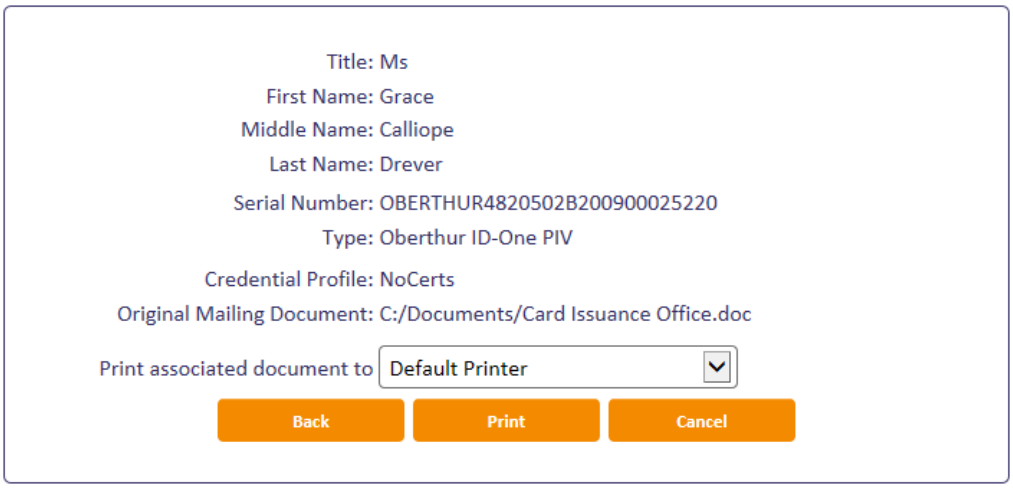


2. If you have the card present, insert it and select the card from the list.

   If you do not have the card present:

   a. Click **Search** then use the **Find Person** screen to find the user.

   b. If the user has more than one device, select the device for which you want to print the document.



3. Select the printer to which you want to print the document, then click **Print**.

   MyID prints the mailing document to the selected printer.

5.9.1 Troubleshooting

If you see an error similar to the following:

```
Microsoft Word is not installed on this machine. It is needed for Printing
the Document.
```

```
Automation server can't create object
```

Make sure you have set the **Initialize and script ActiveX controls not marked as safe for scripting** option. See the *Configuring Internet Options* section in the ***Installation and Configuration Guide*** for details.

Make sure you do not have Microsoft Word running already when you attempt to print the mailing document.

5.10 Unlocking cards and resetting PINs

If users type an incorrect PIN several times, their card is locked – this means they cannot use it to log in. Depending on how your system is set up, cardholders may be able to unlock the card themselves, or they may need to call a helpdesk.

5.10.1 Resetting a card's PIN

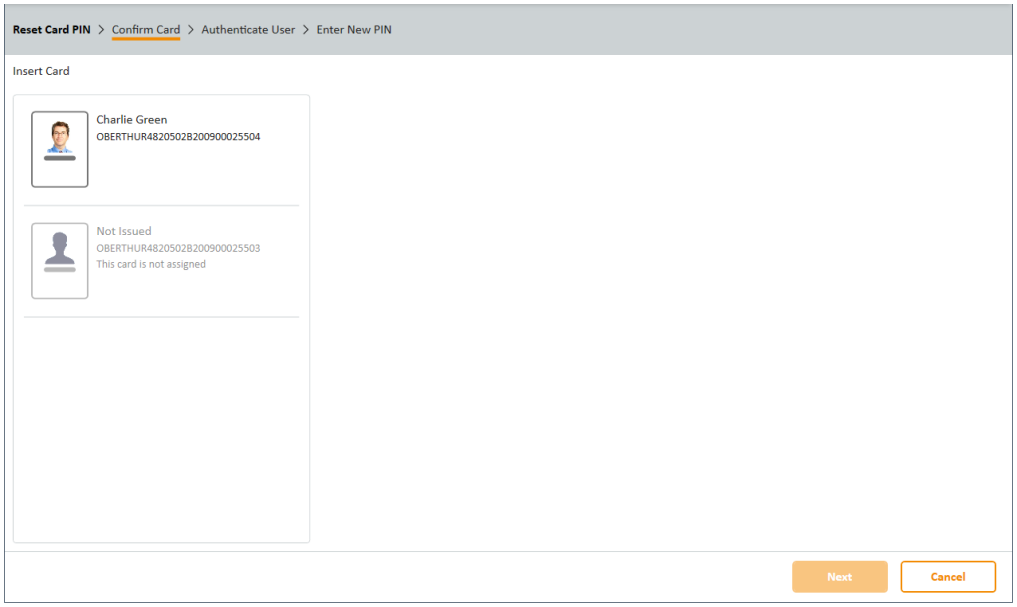
You can use the **Reset Card PIN** workflow to change the PIN of another user's card. This workflow allows you to set a new PIN when the card's PIN has become locked; an administrator can specify the authentication methods that you can use to reset the PIN.

To reset the PIN of a card:

1. From the **Cards** category, click **Reset Card PIN**.

   You can also launch this workflow from the View Device screen in the MyID Operator Client; this launches the workflow with the device already selected. See the *Resetting a device's PIN* section in the ***MyID Operator Client*** guide for details.

2. Insert the card you want to reset.

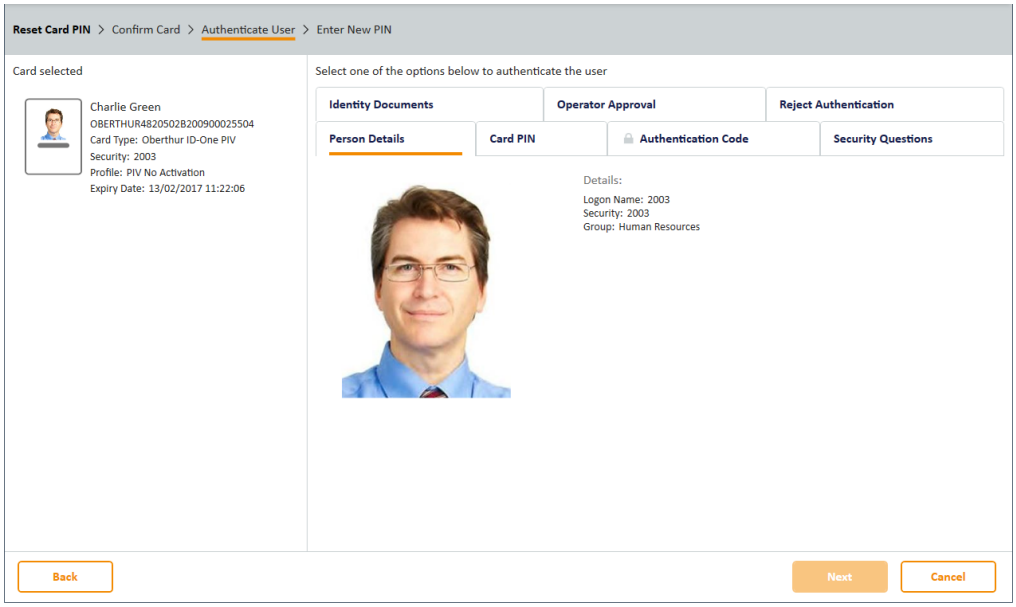


3. Select the card, then click **Next**.

   You may be asked to provide the cardholder's fingerprints, depending on the setting of the **Verify Fingerprints During Reset PIN** option in the **Issuance Settings** section of the credential profile used to issue the device:

   - If **Verify Fingerprints During Reset PIN** is **Always**, you must provide fingerprint verification. If the cardholder does not have fingerprints enrolled, or you exceed the number of allowed attempts (as specified by the **Number of fingerprint validation attempts** option on the **Biometrics** page of the **Operation Settings** workflow), you cannot reset the PIN.
   - If **Verify Fingerprints During Reset PIN** is **Preferred**, you must provide fingerprint verification if the cardholder has fingerprints enrolled. If the cardholder does not have fingerprints enrolled, or you exceed the number of allowed attempts (as specified by the **Number of fingerprint validation attempts** option on the **Biometrics** page of the **Operation Settings** workflow), you can proceed to the Authenticate User stage and provide alternative means of authenticating the user to reset the PIN.
   - If **Verify Fingerprints During Reset PIN** is **None**, you can proceed to the Authenticate User stage.

   If you provide a good fingerprint match, you skip the Authenticate User stage and proceed directly to the Enter New PIN stage.



The **Person Details** tab displays the details for the cardholder – this allows you to confirm that the card belongs to the correct user.

You can now choose how to authenticate the user's identity.

The authentication methods available depend on how your administrator has configured your system. See section *5.10.2*, *PIN reset authentication methods* for details.

4. Select the tab for the appropriate authentication method.

   - **Card PIN** – select this option if the user is present, knows their existing PIN, and the PIN on the card has not been locked. On the Enter New PIN stage after you click **Next**, you will provide the current PIN as well as the new PIN.

     Note: If you select this option, the **Reset PIN to Secure Value** option in the credential profile is ignored, and you must enter a new PIN manually; if you want to generate a new server-generated PIN for the device, select a different authentication method.

   - **Authentication Code** – select this option if the user has an authentication code. Type the code that has been provided in the **Authentication Code** box.

     See section *5.10.9*, *Requesting an authentication code* and the *Sending a code to unlock a device* section in the ***MyID Operator Client*** guide for details.

   - **Security Questions** – select this option to provide answers to a selection of the user's security questions.

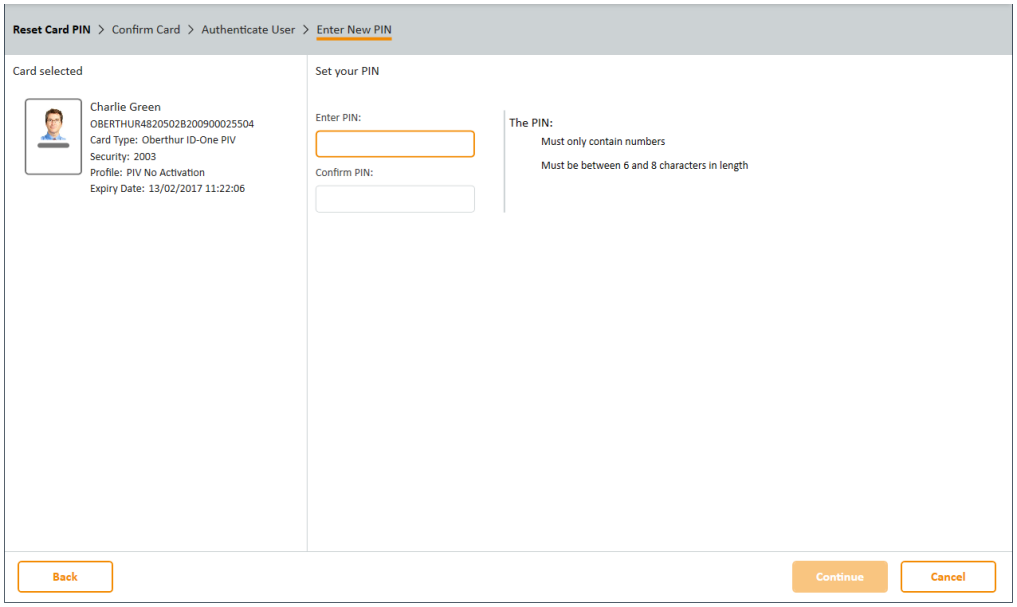
     See the *Setting the number of security phrases required to authenticate* section in the ***Administration Guide*** for details of configuring how many security phrases are required.

   - **Identity Documents** – select this option to record the details of the identity documents (for example, passport, driver's license) that the user has presented to you.

Note: The list of available documents is determined by the **Authenticate Person Document1** and **Authenticate Person Document2** lists. To edit these lists, use the **List Editor**. See the *Changing list entries* section in the ***Administration Guide*** for details.

- **Operator Approval** – select this option to record your observations and your reasons for accepting the user's identity.
- **Reject Authentication** – select this option to record your observations and your reasons for not accepting the user's identity; you cannot then reset the card's PIN.

5. Click **Next**.



6. If the credential profile is *not* configured for server-generated PINs (or you have selected **Card PIN** as the authentication method), you must enter a new PIN manually.

   Type the new PIN and confirm it, then click **Continue**.

   Note: If you selected the **Card PIN** authentication method, you must provide the current PIN as well as the new PIN.

   If the credential profile *is* configured for server-generated PINs (and you have not selected **Card PIN** as the authentication method), the workflow moves automatically to the next stage. For information on configuring the credential profile to use server-generated PINs for PIN reset, see the *Credential profile setup for PIN generation* section in the ***Administration Guide***.

   MyID resets the PIN on the card to the new value. Do not remove the card from the reader until the process is complete.

7. If the credential profile is configured to print PIN reset documents, you are given the option to **Print** the configured document or **Skip document printing**.

   Click **Next** to complete the workflow.

5.10.2 PIN reset authentication methods

You can configure which authentication methods are available in the **Reset Card PIN** workflow using the **Edit Roles** workflow. This allows you to select a different set of authentication methods for each role; for example, you may want only senior operators to be able to use the **Operator Approval** method, while all operators can use the **Authentication Code** method.

You can also configure MyID to skip the authentication step entirely.

To configure the PIN reset authentication methods:

1. From the **Configuration** category, select **Edit Roles**.
2. Under the **Reset Card PIN** option, select the following options:
   - **Identity Documents** – select this option to allow the operator to record the details of the documents the user presents (for example, passport, driver's license).

     Note: The list of available documents is determined by the **Authenticate Person Document1** and **Authenticate Person Document2** lists. To edit these lists, use the **List Editor**. See the *Changing list entries* section in the ***Administration Guide*** for details.
   - **Operator Approval** – select this option to allow the operator to confirm the user's identity without further evidence.
   - **Security Questions** – select this option to allow authentication using answers to the user's stored security questions.
   - **Reject Authentication** – select this option to allow the operator to reject the authentication for the user.
   - **Card PIN** – select this option to allow authentication using the current PIN.
   - **Authentication Code** – select this option to allow authentication codes.
   - **Bypass Authentication** – select this option to skip the authentication stage on the **Reset Card PIN** workflow. Do not select any other authentication methods in conjunction with this option.
3. Click **Save Changes**.

5.10.3 Resetting your own PIN

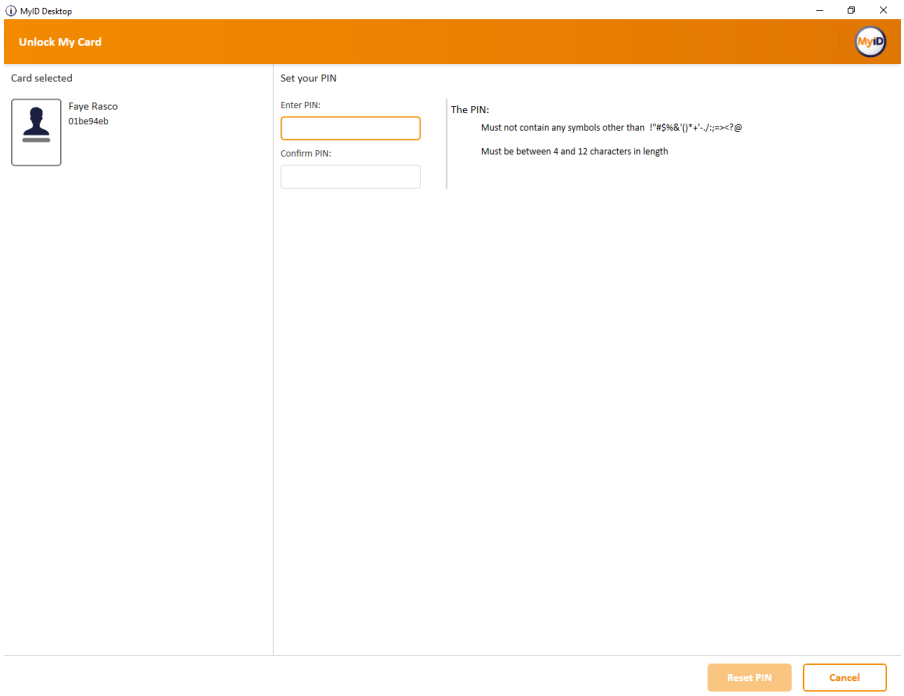
You can use the **Reset PIN** option to change your own PIN at the logon screen. You can use this option to reset your PIN at any time, including when your card has been locked by entering the PIN incorrectly too many times.

To reset your PIN:

1. At the logon screen, click **Reset PIN**.
2. Complete the authentication requested.

   For example, provide your fingerprints.

   The authentication you provide depends on the setup of your credential profile. See section *5.10.6*, *Self-service PIN reset authentication* for details.
3. Provide your new PIN.



4. Click **Reset PIN**.

5.10.4 Changing a card's PIN

You can use the **Change PIN** workflow to change the PIN of your own card, or of any other card present.

To change the PIN of a card:

1. From the **Cards** category, click **Change PIN**.

   You can also launch this workflow from the View Device screen in the MyID Operator Client; this launches the workflow with the device already selected. See the *Changing a device PIN* section in the ***MyID Operator Client*** guide for details.
2. Insert the card for which you want to change the PIN, then click **OK**.
3. Type the **Old PIN**.
4. Type the **New PIN**, then type it again in the **Confirm PIN** box.
5. Click **Change**.

MyID changes the PIN of the card.

5.10.5 Allowing self-service unlocking

You must have the **Self-service Unlock** option (on the **Self-Service** page of the **Security Settings** workflow) set to **Yes** to allow users to unlock their own cards.

For PIV systems, you also must configure the web service to allow self-service unlock. See the *Configuring self-unlock* section in the ***Web Service Architecture*** guide for details of the `AllowSelfUnlockForPIV` option.

Note: If your card data model has a 5FC101 container for a card authentication certificate, you cannot unlock a card that does not have a card authentication certificate in this container. If you attempt to carry out a self-service unlock on a PIV card that does not have this certificate, you will see an error similar to the following:

```
Error 890467 - Unable to authenticate card. Unlocking your own card is not allowed.
```

5.10.6 Self-service PIN reset authentication

Self-service card unlocking at the MyID Desktop logon screen enforces flexible authentication requirements based on the credential profile.

See the *Self-Service Unlock Authentication* section in the ***Administration Guide*** for details.

When you unlock your card using the **Reset PIN** option, MyID checks the latest version of the credential profile for the **Self-Service Unlock Authentication** setting.

Note: The latest version of the credential profile is always used. If you change the self-service authentication settings, you do not have to update existing issued smart cards.

- If the **Credential owners must authenticate using one of the methods below in the order shown** is *not* set:
  - If the **Ask Security Questions for Self Service Card Unlock** configuration option (on the **PINs** page of the **Security Settings** workflow) is set, the user can provide their security phrases to unlock their card.
  - If the **Biometric PIN Reset and Verify fingerprints during card unlock** configuration options (on the **Biometrics** tab of the **Operation Settings** workflow) are set, the user must provide their fingerprints to unlock their card.

    If neither option is set, the user cannot unlock their card.

    If you have configured both security questions and biometrics, the biometric authentication takes precedence, as it is the more secure option.
- If the **Credential owners must authenticate using one of the methods below in the order shown** *is* set:
  - The authentication methods listed in the credential profile are presented to the cardholder in order.
  - When the user is presented with a method of authentication, they can decline the option (for example, when presented with a smart card authentication screen, they can click the "I cannot authenticate with my device" option) and proceed to the next available logon mechanism.
  - Windows logon is always attempted first; if Windows authentication is successful, the user starts the action; if it is unsuccessful, the user is presented with the next logon mechanism in the list.

5.10.6.1 Allowing biometric authentication

To allow biometric authentication when logging on to MyID to perform a PIN reset, you must set the following:

- In the **Security Settings** workflow, on the **Logon Mechanisms** tab, set the **Biometric Logon** option.
- In the **Edit Roles** workflow, add the **Bio Unlock My Card** workflow to the permissions for the roles you want to be able to reset PINs using biometric authentication.
- In the **Edit Roles** workflow, on the **Logon Methods** screen, select **Biometric Logon** as a logon mechanism for the roles that have access to the **Bio Unlock My Card** workflow.
- In the **Operation Settings** workflow, on the **Biometrics** tab, set the **Allow Biometric PIN Reset** option.

5.10.6.2 Allowing authentication codes and security phrases

To allow authentication codes or security phrases to be used when logging on to MyID to perform a PIN reset, you must set the following:

- In the **Security Settings** workflow, on the **Logon Mechanisms** tab, set the **Password Logon** option.
- In the **Edit Roles** workflow, on the **Logon Methods** screen, select **Password** as a logon mechanism for the roles you want to be able to use authentication codes or security phrases to perform a PIN reset.
- If you want to allow password or authentication code logon to MyID for the purpose of PIN resets, but not for general logon, you can prevent password logon for cases where the user does not also have their card present; in the **Security Settings** workflow, on the **Logon** tab, set the **Prevent Direct Password Logon** option to Yes.

5.10.6.3 Using the Self-Service App or Self-Service Kiosk to unlock a card

You can use the Self-Service App or Self-Service Kiosk to unlock your card; note that you must have a role that has access to the **Unlock My Card** workflow to carry out this operation. See For further information, see the *Self-Service App features* section in the ***Self-Service App*** guide or the ***Self-Service Kiosk*** guide for details.

5.10.7 Unlocking a credential remotely

Users may need to contact their helpdesk to unlock their credentials (for example, smart cards, mobile devices, VSCs). The helpdesk operator can use the **Unlock Credential** workflow to provide a code that unlocks the card.

If the user has a locked smart card, and is physically present so that you can insert the card into a card reader on the operator's machine, you can use **Reset Card PIN** instead – see section *5.10.1*, *Resetting a card's PIN*.

Note: Some smart card types do not support remote unlocking. See the ***Smart Card Integration Guide*** for details of those that do.

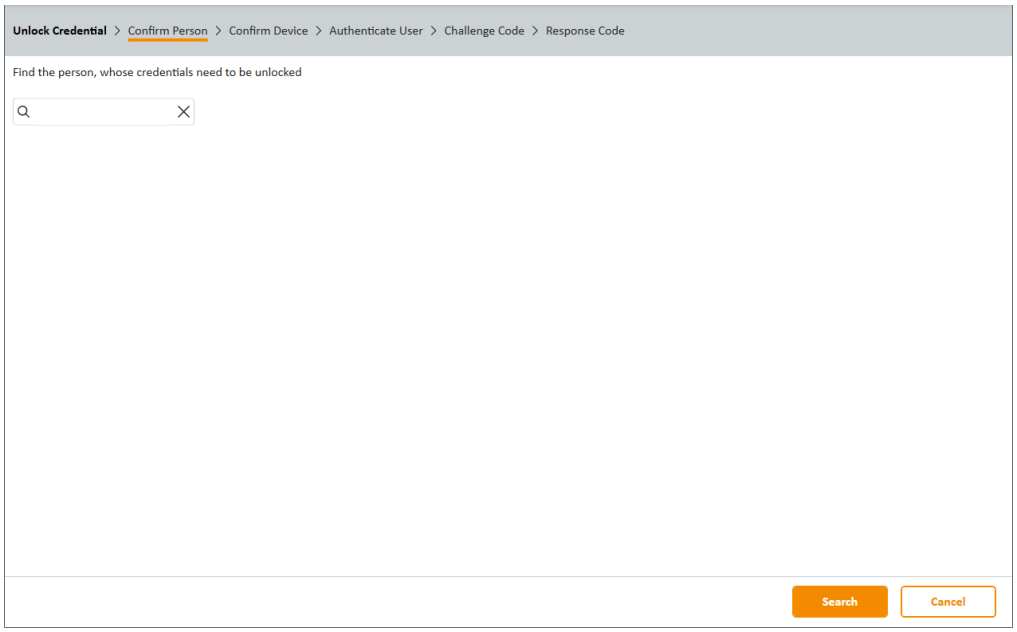
- **IKB-183 – MyID does not check expiry dates on identity documents**

  In the **Unlock Credential** workflow, MyID does not check the expiry date of any identity documents you provide to confirm the card holder's identity. If your organization's procedures require this check. you must verify the expiry date manually before proceeding.

To unlock a card remotely:

1. From the **Cards** category, click **Unlock Credential**.

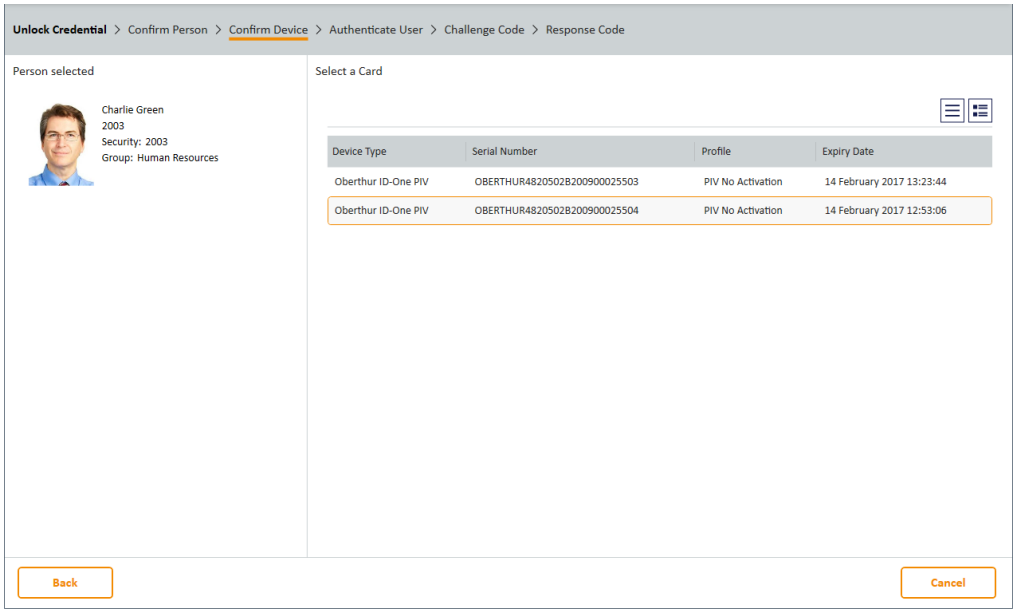
   You can also launch the **Unlock Credential** workflow from the View Device screen of the MyID Operator Client. The **Unlock Credential** workflow appears in a MyID Desktop window with the device already selected. See the *Unlocking a device* section in the ***MyID Operator Client*** guide for details.



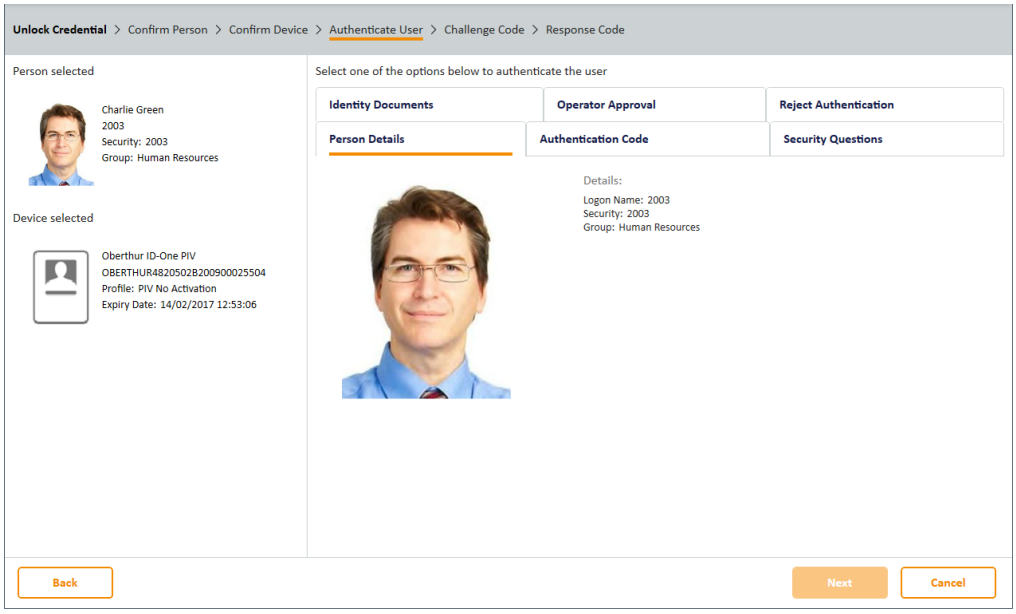
2. Enter the search criteria for the person who owns the credential you want to unlock, then click **Search**.

   See section *2.2.2*, *Entering search criteria* for details of entering search criteria.

3. From the list of matching records, select the person to search for any credentials belonging to them.



4. Select the device you want to unlock.



The **Person Details** tab displays the details for the cardholder – this allows you to confirm that the card belongs to the correct user.

You can now choose how to authenticate the user's identity.

The authentication methods available depend on how your administrator has configured your system. See section *5.10.8*, *Remote unlock authentication methods* for details.

5. Select the tab for the appropriate authentication method.

   - **Authentication Code** – select this option if the user has an authentication code. Type the code that has been provided in the **Authentication Code** box.

     See section *5.10.9*, *Requesting an authentication code* and the *Sending a code to unlock a device* section in the ***MyID Operator Client*** guide for details.

- **Security Questions** – select this option to provide answers to a selection of the user's security questions.

  See the *Setting the number of security phrases required to authenticate* section in the ***Administration Guide*** for details of configuring how many security phrases are required.

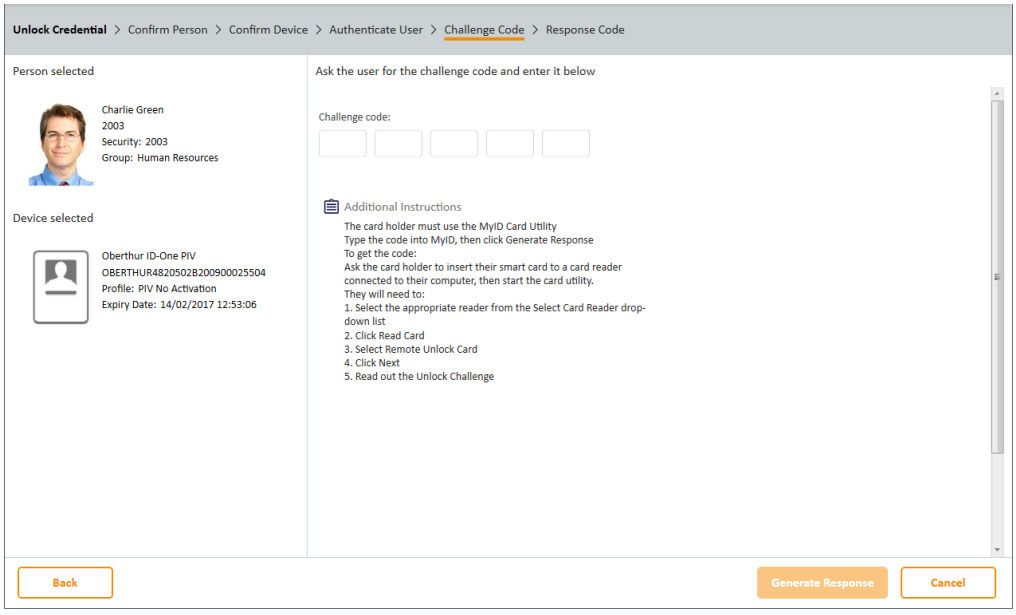
- **Identity Documents** – select this option to record the details of the identity documents (for example, passport, driver's license) that the user has presented to you.

  Note: The list of available documents is determined by the **Authenticate Person Document1** and **Authenticate Person Document2** lists. To edit these lists, use the **List Editor**. See the *Changing list entries* section in the ***Administration Guide*** for details.

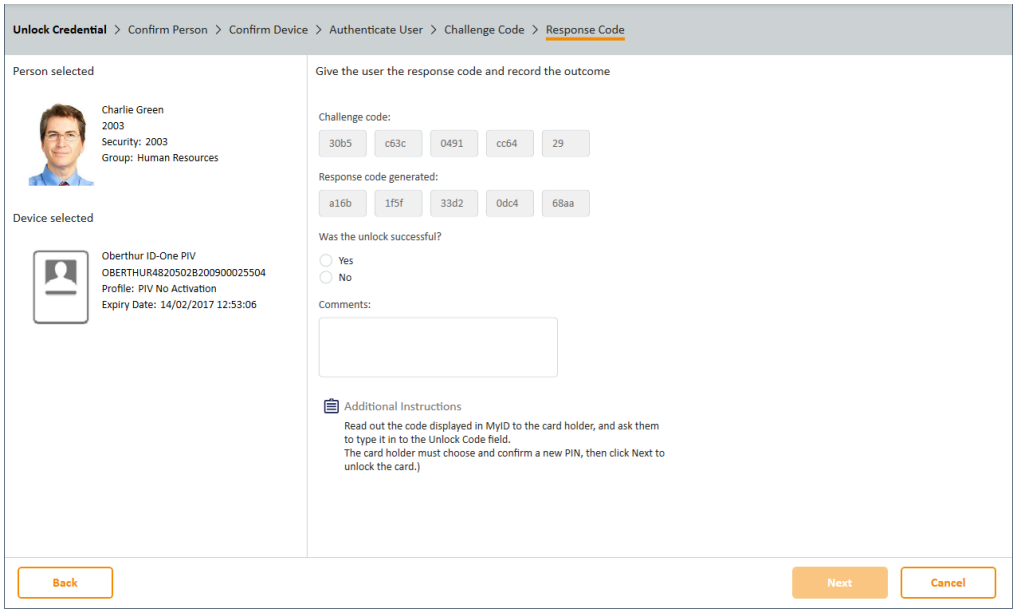
- **Operator Approval** – select this option to record your observations and your reasons for accepting the user's identity.

- **Reject Authentication** – select this option to record your observations and your reasons for not accepting the user's identity; you cannot then reset the card's PIN.

6. Click **Next**.



7. Ask the credential owner to read out the challenge code, and type it into the boxes provided.
8. Click **Generate Response**.



9. Read out the response code to the credential owner.
10. Provide details of the operation – whether the unlock was successful, and any details you want to add.
11. Click **Next** to complete the workflow.

5.10.8 Remote unlock authentication methods

You can configure which authentication methods are available in the **Unlock Credential** workflow using the **Edit Roles** workflow. This allows you to select a different set of authentication methods for each role; for example, you may want only senior operators to be able to use the **Operator Approval** method, while all operators can use the **Authentication Code** method.

You can also configure MyID to skip the authentication step entirely.

To set up authentication methods for unlocking:

1. From the **Configuration** category, select **Edit Roles**.
2. Under the **Unlock Credential** option, select the following options:
   - **Identity Documents** – select this option to allow the operator to record the details of the documents the user presents (for example, passport, driver's license).

     Note: The list of available documents is determined by the **Authenticate Person Document1** and **Authenticate Person Document2** lists. To edit these lists, use the **List Editor**. See the *Changing list entries* section in the ***Administration Guide*** for details.
   - **Operator Approval** – select this option to allow the operator to confirm the user's identity without further evidence.
   - **Security Questions** – select this option to allow authentication using answers to the user's stored security questions.

- **Reject Authentication** – select this option to allow the operator to reject the authentication for the user.
- **Authentication Code** – select this option to allow authentication codes.
- **Bypass Authentication** – select this option to skip the authentication stage on the **Unlock Credential** workflow. Do not select any other authentication methods in conjunction with this option.

Assign these options to the appropriate roles; for example, you may want users who have one role to use security questions, and users who have another role to use authentication codes.

3. Click **Save Changes**.

5.10.9 Requesting an authentication code

The **Request Auth Code** workflow allows you to request an authentication or unlock code for a user.

Note: You can also request an authentication code for card activation or unlocking using the MyID Operator Client. See the *Sending an authentication code to activate a device* and *Sending a code to unlock a device* sections in the ***MyID Operator Client*** guide for details.

Authentication codes are used during card activation; see the *Activating cards* section in the ***Administration Guide*** for details. If an applicant makes several invalid attempts to enter an authentication code (as determined by the **Maximum Allowed OTP Failures** configuration option), quits out of the **Activate Card** workflow, or declines the terms and conditions, the code is canceled, and the applicant must ask an administrator to generate another code.

If a cardholder enters their PIN incorrectly too many times, the card is locked. An administrator can generate an unlock code using this workflow. The cardholder can then unlock the card: see section *5.10.3*, *Resetting your own PIN*.

Note: Codes do not expire; they are valid until they are used. Only one code of each type can be assigned to a card – new codes supersede old codes.

The **Request Auth Code** workflow is not assigned to any roles by default; you must make sure that you use the **Edit Roles** workflow to assign the workflow to any roles that you want to be able to issue codes.

To generate a code:

1. From the **Cards** category, select **Request Auth Code**.
2. Use the Find Person screen to find the user for whom you want to generate a code.
3. Select the person.
4. If the user has more than one card, select the card.

   The screen shows if the user has any existing unlock or authentication codes in the **Existing Codes** column. If you generate a code of the same type, the previous code is deactivated, and can no longer be used.
5. To generate an unlock code, click **Unlock**.

   An email message is sent to the user containing a code that allows them to unlock the card. See section *5.10.3*, *Resetting your own PIN* for details.
6. To generate an authentication code, click **Activate**.

An email message is sent to the user containing a code that allows them to activate the card. see the *Activating cards* section in the ***Administration Guide*** for details.

Note: The lifetime of auth codes is determined by the **Auth Code Lifetime** option on the **Auth Code** page of the **Security Settings** workflow. By default, the lifetime is set for 720 hours; to set auth codes to have unlimited expiry, set this option to 0.

5.10.10 Remote PIN Management utility for PIV cards

The MyID Card Utility allows you to carry out a remote unlock or change the PIN on cards that support PIV applets.

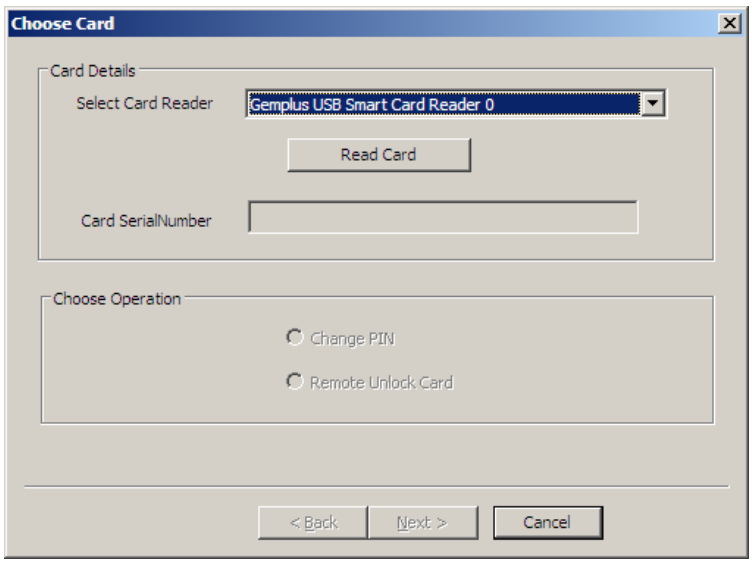
This utility has been developed with IDEMIA (PIV cards and ID-One PIV cards) and Gemplus PIV cards. You can also use the utility with Yubico devices, which support PIV features but are not PIV compliant. This utility supports Global PINs on smart cards that support that feature.

The `MyIDCardUtility.exe` file is installed to the `Utilities` folder on the MyID application server. You can copy this utility manually to any client PC you want to be able to use the functionality.

To use the card utility:

1. Copy the `MyIDCardUtility.exe` file to the client PC.
2. In Windows Explorer, double-click the `MyIDCardUtility.exe` file.

   You can also set up a shortcut to run this utility.



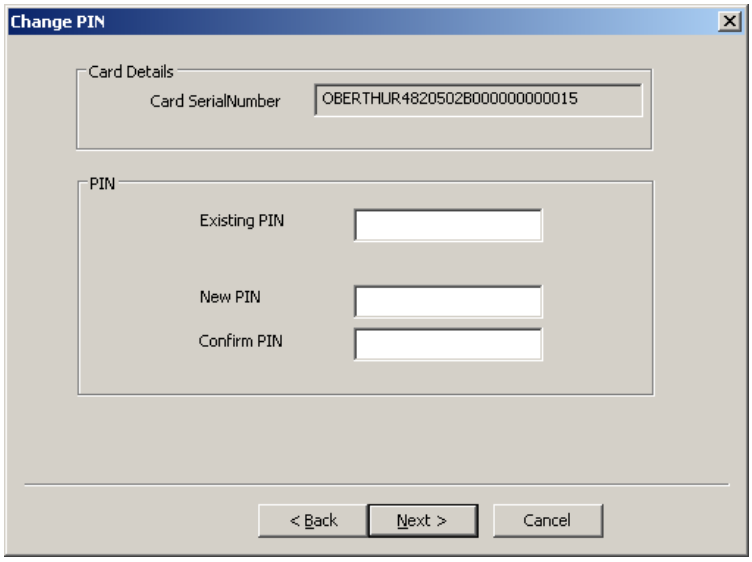
3. If you are using multiple card readers, select the appropriate reader from the **Select Card Reader** drop-down list.
4. Click **Read Card**.

   The utility reads the card, and the card serial number appears.
5. Select one of the following options:
   - **Change PIN**
   - **Remote Unlock Card**

To change the PIN:

a. Click **Change PIN**.

b. Click **Next**.



c. Type the card's **Existing PIN**.

d. Type the **New PIN**, and confirm the new PIN in the **Confirm PIN** box.

Note: The PIN must be the same length or longer than the current PIN.

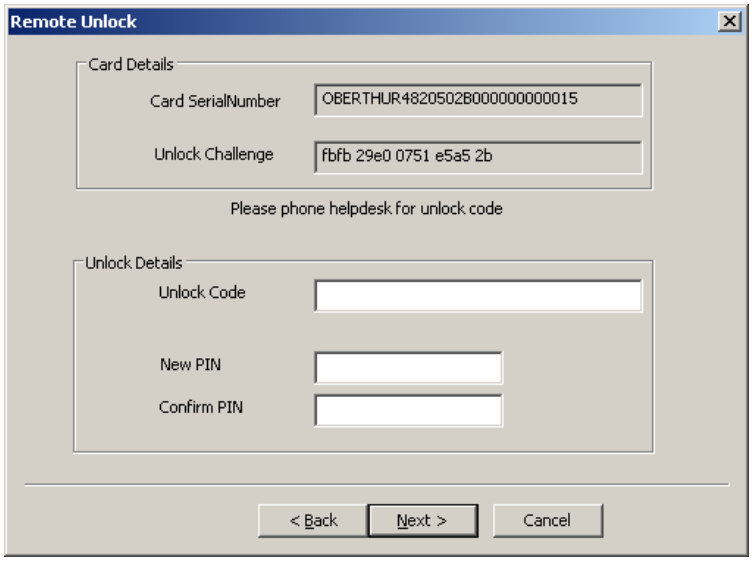
e. Click **Next**.

The card PIN is changed.

To remote unlock the card:

a. Click **Remote Unlock Card**.

b. Click **Next**.



c. Call the helpdesk and provide the **Unlock Challenge**.

d. The helpdesk operator must then open MyID, go to the **Unlock Credential** workflow, and type the **Unlock Challenge** into the **Challenge Code** boxes before clicking **Confirm**.

   The helpdesk operator can then read out the unlocking code.

   See section *5.10.7*, *Unlocking a credential remotely* for details of using the **Unlock Credential** workflow.

e. Type the unlocking code from the helpdesk operator into the **Unlock Code** box.

f. Type a **New PIN** and confirm the new PIN in the **Confirm PIN** box.

g. Click **Next**.

   The card is unlocked, and is given a new PIN.

5.10.11 Unlock credential provider

MyID provides an unlock credential provider that allows a user to unlock their PIV card from the Windows logon screen. This provides the same functionality as the MyID Card Utility for remotely unlocking cards (see section *5.10.10*, *Remote PIN Management utility for PIV cards* for details).

For details of installing and configuring the unlock credential provider, see the *Installing the unlock credential provider* section in the ***Installation and Configuration Guide***.

To unlock a PIV card:

1. At the Windows logon screen, insert your locked PIV card.
2. Select the **Unlock Credential Provider** tile.

   Note: The unlock credential provider displays a tile for each suitable logon certificate on the card; for example, a PIV card has both PIV Authentication and Card Authentication certificates, so the unlock credential provider displays two tiles. Click on any of the provided tiles to continue.

   The unlock credential provider generates and displays a random challenge.
3. Call the helpdesk and provide the **Challenge** code.
4. The helpdesk operator must then open MyID, go to the **Unlock Credential** workflow, and type the **Unlock Challenge** into the **Challenge Code** boxes before clicking **Confirm**.

   The helpdesk operator can then read out the unlocking code.

   See section *5.10.7*, *Unlocking a credential remotely* for details of using the **Unlock Credential** workflow.
5. Type the unlocking code from the helpdesk operator into the **Response** box.
6. Type a new **PIN** and confirm the new PIN in the **PIN Check** box.

   The card is unlocked and given a new PIN, and the user is logged on to Windows.

Note: The next time you log on to Windows after unlocking your card using the unlock credential provider, the **Unlock Credential Provider** tile is selected on the logon screen; this is because Windows remembers the last option you selected on this screen. Click your preferred sign-in option and continue.

5.10.12 Known issues

- **IKB-283 – Error if an incorrect certificate is selected for PIN unlock**

  If two or more Windows logon certificates are present for the same identity on a single device, an error can occur after successfully completing setting a new PIN for the device if the following sequence has occurred.

  - The user has initially logged on with a certificate on a device.
  - The user locks the PC.
  - The user attempts to unlock the computer but locks the PIN for the device by providing the incorrect PIN too many times.
  - The user selects a different logon certificate on the same device.
  - The user completes the unlock process and sets a new PIN.

  A Windows message is displayed:

  ```
  The user name or password is incorrect
  ```

  In this scenario, the PIN is successfully changed, but the user must re-select the certificate and enter their PIN to logon to Windows again.

5.11 Canceling cards

You can cancel cards that are present, cancel cards that are not present, and enable or disable cards temporarily.

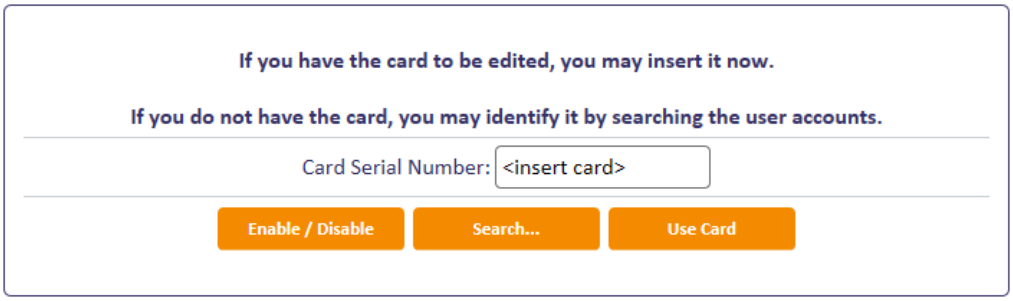
5.11.1 Enabling or disabling cards

You can enable or disable a card temporarily using the **Enable / Disable Card** workflow. You can enable or disable the card whether the card is present or not.

Note: As an alternative, you can use the **Enable Device** and **Disable Device** options in the MyID Operator Client. See the *Enabling and disabling devices* section in the ***MyID Operator Client*** guide for details.

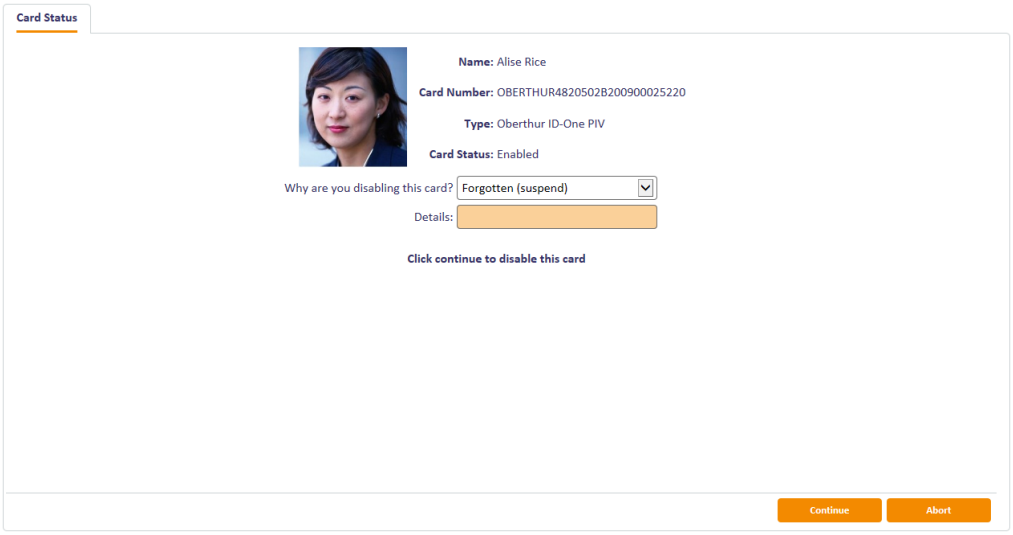
To enable or disable a card:

1. From the **Cards** category, click **Enable / Disable Card**.



2. If the card is present, insert it into an available card reader.

   If the card is not present, click **Search** then use the Find Person screen to find the cardholder, then (if the cardholder has more than one card) select the card you want to enable or disable.



3. Select a reason and type the details for canceling the card, then click **Continue**.

   See section *6.5*, *Certificate reasons* for details.

Note: If a card with existing suspended certificates is disabled, all active certificates on the card are suspended. If that card is then re-enabled, all certificates on the card (including those which were originally suspended) are enabled.

For example, a card has two certificates: one issued and the other suspended. If that card is disabled, the issued certificate is suspended. When the card is re enabled, both certificates are unsuspended.

5.11.2 Erasing a card

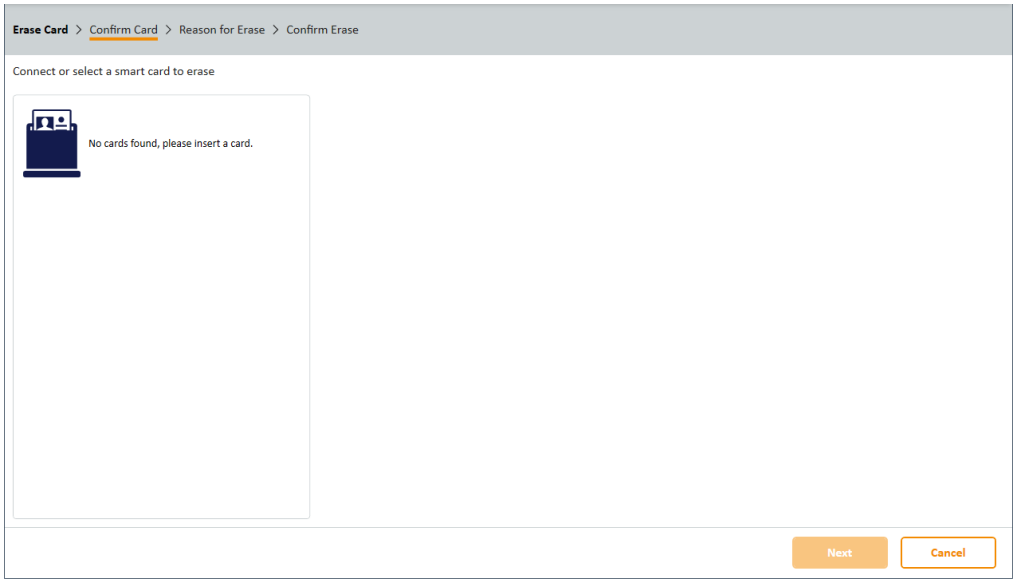
When you erase a card, MyID removes its details from the database, revokes and removes any certificates stored on it and – as much as possible – returns the card to its original state. You can erase smart cards that are physically present, and VSCs that are stored on the machine on which you are running MyID.

Note: If your card is contactless only, or it is not present, you cannot use the **Erase Card** workflow to cancel it. Instead, use the **Cancel Credential** workflow. See section *5.11.3*, *Canceling a credential*.

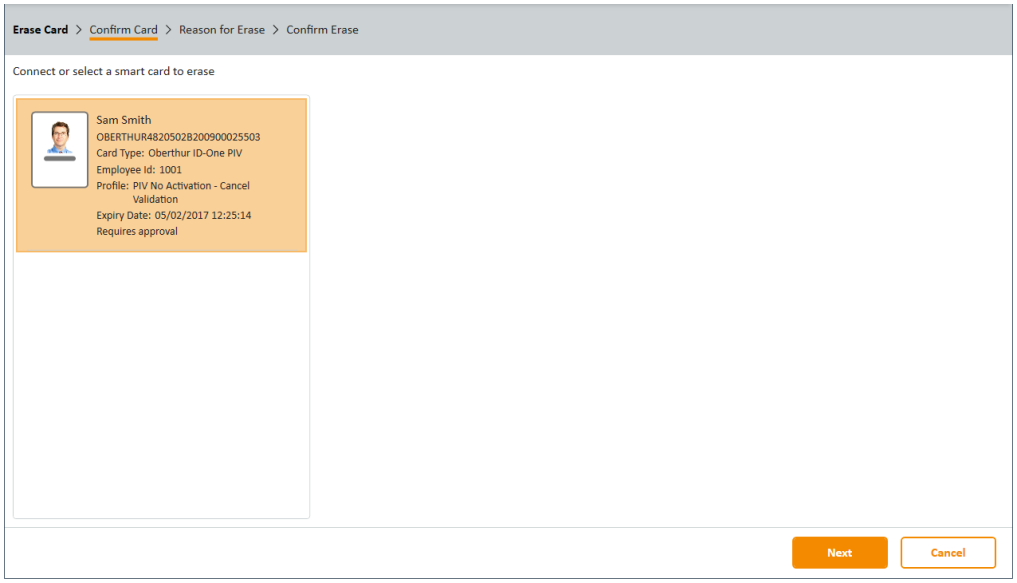
Note: You cannot erase your own cards.

To erase a card:

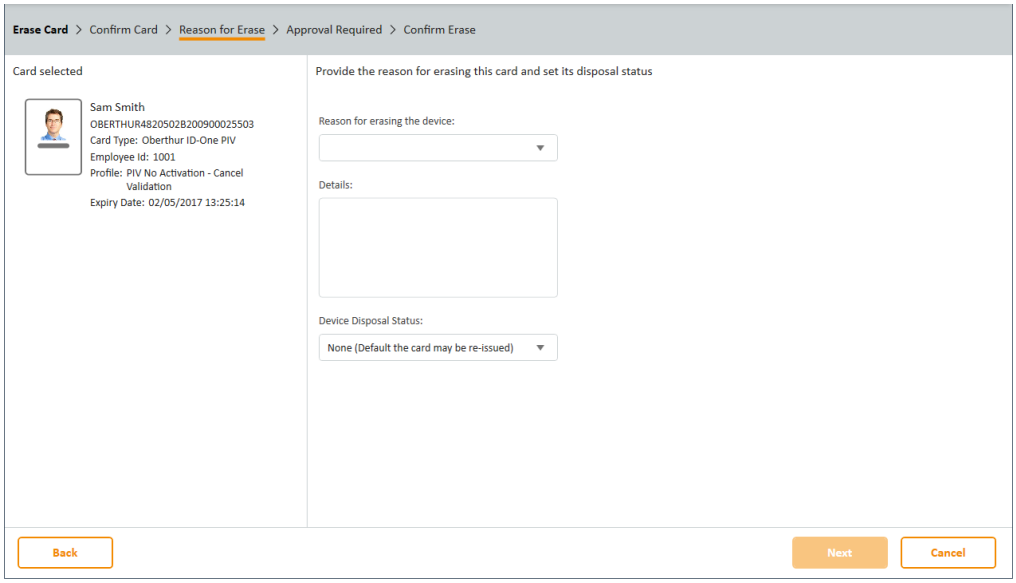
1. From the **Cards** category, select **Erase Card**.



2. Insert the card you want to cancel and select it from the list.



3. Click **Next**.



4. Provide the following information:
   - **Reason for erasing the device** – select the reason you are canceling the card from the drop-down list. This reason affects how MyID treats the certificates on the card.

     See section *6.5*, *Certificate reasons* for details.
   - **Details** – type further information on your reasons for erasing the card. This information is stored in the audit record.
   - **Device Disposal Status** – select what you want to happen to the physical card after cancellation. For example, you may want to prevent the card from being used again within MyID.

     See also the **Card Disposal** workflow – section *5.15*, *Disposing of cards*.
5. Click **Next**.
6. If the credential profile used to issue the card had the **Validate Cancellation** option selected, you must obtain the approval of another operator before you can erase the card.
   - If the approver is present, select **Approver Present**, click **Approve**, then ask the approver to insert their card and authenticate using their PIN.
   - If the approver is not present, select **Defer Approval** and click **Approve**.

   Note: MyID does not erase the card if you have deferred approval. Instead, MyID creates an approval job. Another operator must then use the **Validate Request** workflow to approve the approval job, at which point MyID will cancel the card remotely; this is effectively the same as using the **Cancel Credential** workflow, in that the card is canceled in the MyID database and its certificates are revoked; the physical card is not affected.

   If you still want to remove data from the physical card after it has been canceled remotely, you can use the **Erase Card** workflow again.
7. On the confirmation screen, click **Erase**.

MyID erases the card. The confirmation screen details what will happen to the credential and its certificates.

Note: Do not remove the card until the process has completed.

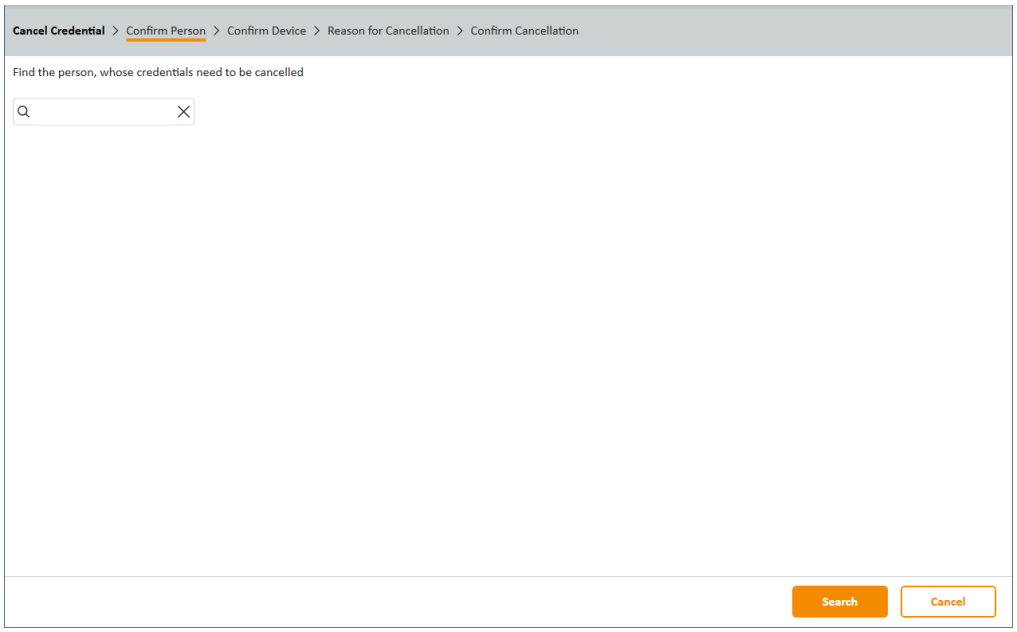
5.11.3 Canceling a credential

If a card is not present, or it is a type of credential that cannot be inserted into a card reader (for example, a VSC) you can cancel it remotely using the **Cancel Credential** workflow. This process does not change the contents of the credential itself, but cancels the holder's access to MyID and revokes any certificates.

You can use this workflow even if the card is present; however, the contents of the card are not altered.

To cancel a credential:

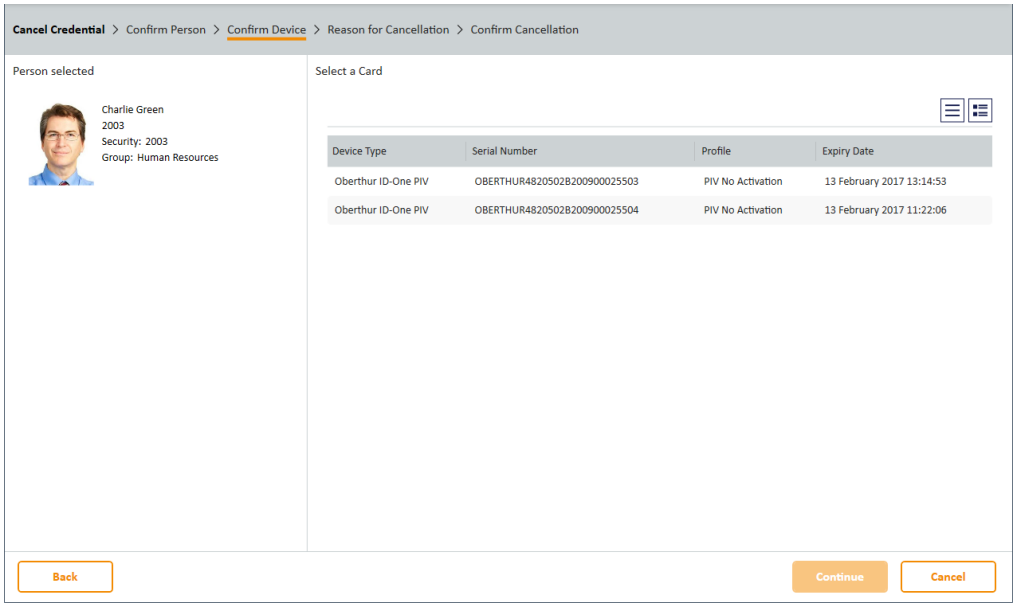
1. From the **Cards** menu, select **Cancel Credential**.



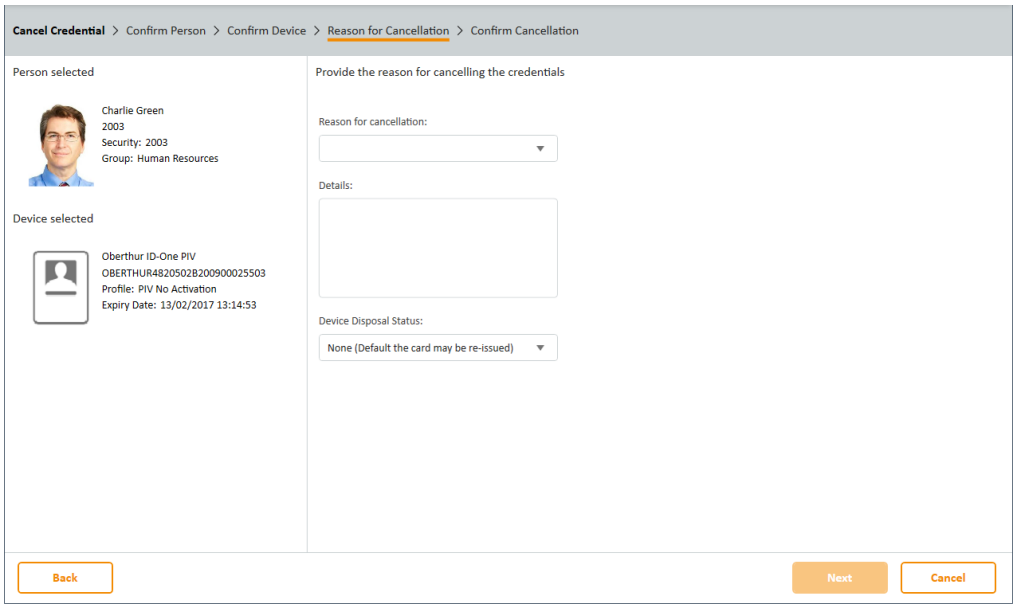
2. Enter the search criteria for the person who owns the credential you want to cancel, then click **Search**.

   See section *2.2.2*, *Entering search criteria* for details of entering search criteria.

3. From the list of matching records, select the person to search for any credentials belonging to them.



4. If the person has more than one credential, select the credential you want to cancel from the list.



5. Provide the following information:
   - **Reason for cancellation** – select the reason you are canceling the credential from the drop-down list. This reason affects how MyID treats the certificates on the credential.

     See section *6.5*, *Certificate reasons* for details.
   - **Details** – type further information on your reasons for canceling the credential. This information is stored in the audit record.
   - **Device Disposal Status** – select what you want to happen to the physical credential after cancellation. For example, you may want to prevent the credential from being used again within MyID.

Note: The **Device Disposal Status** option is not shown for credentials that cannot be disposed; for example, VSCs.

See also the **Card Disposal** workflow – section *5.15*, *Disposing of cards*.

6. Click **Next**.
7. If the credential profile used to issue the credential had the **Validate Cancellation** option selected, you must obtain the approval of another operator before you can erase the credential.
   - If the approver is present, select **Approver Present**, click **Approve**, then ask the approver to insert their credential and authenticate using their PIN.
   - If the approver is not present, select **Defer Approval** and click **Approve**.

     Note: MyID does not cancel the credential immediately if you have deferred approval. Instead, MyID creates an approval job. Another operator must then use the **Validate Request** workflow to approve the approval job, at which point MyID will cancel the credential.
8. On the confirmation screen, click **Confirm**.

   MyID cancels the credential in the MyID database, unassigns it from the user, and revokes any certificates as appropriate. The confirmation screen details what will happen to the credential and its certificates.

5.11.4 Validating card cancellations

If you want to ensure that any card cancellations are validated by another operator, you can set the **Validate Cancellation** option in the **Credential Profiles** workflow.

- An operator uses the **Erase Card** or **Cancel Credential** workflow.
- Either another operator enters their authentication details while the workflow is being used, or the original operator selects the **Defer Approval** option and the second operator uses the **Validate Request** workflow to approve the cancellation.

To set the **Validate Cancellation** option:

1. In the **Configuration** category, click **Credential Profiles**.
2. Select the profile you want to change, then click **Modify**.
3. Click **Issuance Settings**, then set the **Validate Cancellation** option.
4. Click **Next**, then complete the Credential profile.

   When an operator uses the **Defer Approval** option in the **Erase Card** or **Cancel Credential** workflow, MyID creates a job that must be validated by another operator before the card can be canceled.

To validate a request:

1. In the **Cards** category, click **Validate Request**.
2. In the **Task Type** drop-down, select **Cancellations**.
3. Click **Search** to find the appropriate cancellation requests.
4. The workflow moves on to the **Validate Request** stage. This stage gives details of the appropriate request and provides the option of either accepting or rejecting that request.

5. Either:
   - Choose **Accept** to validate the request, *or*
   - Choose **Reject** to reject the request, preventing the card from being canceled.

5.12 Printing cards

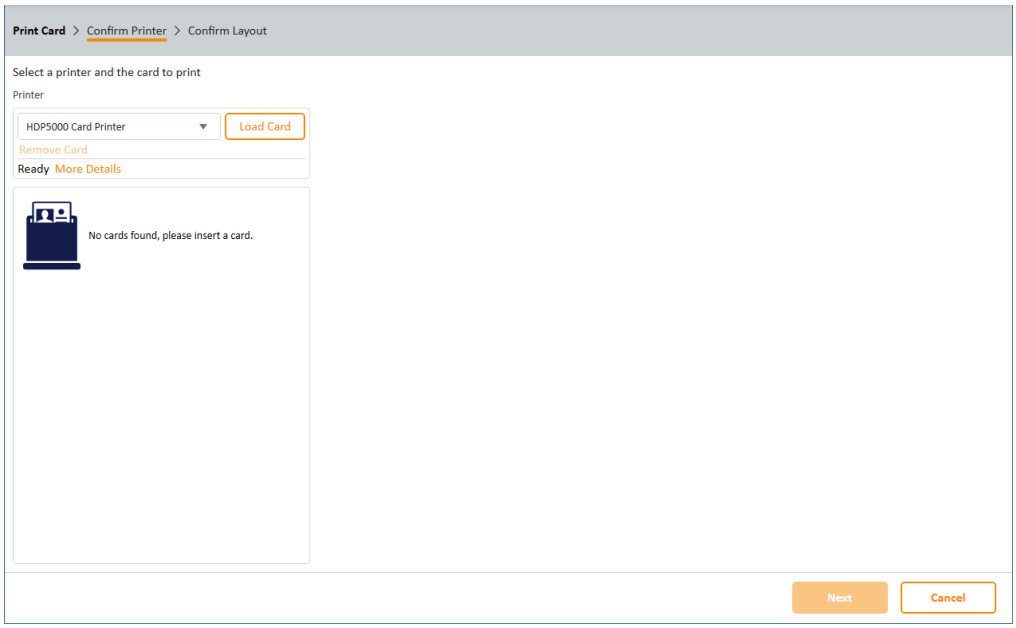
For information about card printers, see the ***Printer Integration Guide***.

5.12.1 Printing a card

You can use the **Print Card** workflow to print a card that has already been issued.

To print a card:

1. From the **Cards** category, select **Print Card**.



2. From the drop-down list, select the card printer you want to use.

   The first time you use this workflow, the selection is blank; on all subsequent uses, MyID remembers the last printer you selected (if it is still installed on your PC).

3. Insert the issued card you want to print into the card printer and click **Load Card**.

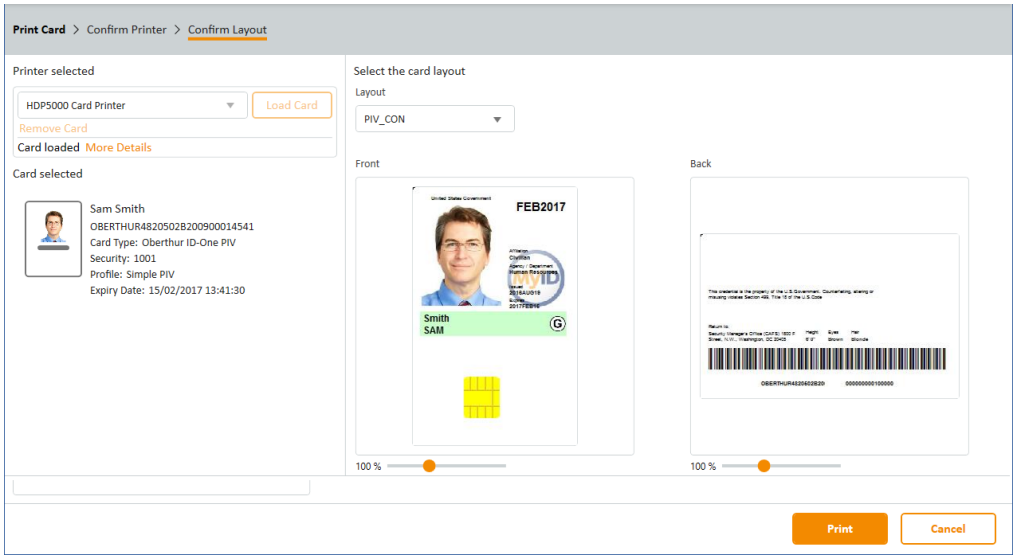
   Once the card has loaded, it appears in the card list.

   Note: At any point, if there are problems, you can click **More Details** to view information about the messages being returned from the card printer.

4. Select the card from the list.

   Note: MyID cannot differentiate between card readers attached to the PC and card readers attached through the card printer. If you have more than one card inserted, make sure you select the correct card from the list.

5. Click **Next**.



6. Select the card layout from the drop-down list.

   MyID displays a preview of the card layout using the details taken from the cardholder's account. You can zoom in and out on the front and back preview images.

7. Click **Print**.

   MyID prints the card. Do not disconnect the printer until it has finished printing.

5.12.2 Printing badges

The **Print Badge** workflow allows you to print a card layout for a specific user onto a card that does not have a chip.

To print a badge:

1. From the **Cards** category, select **Print Badge**.

   You can also launch this workflow from the View Person screen in the MyID Operator Client; this launches the workflow with the person already selected. See the *Printing a badge* section in the ***MyID Operator Client*** guide for details.

2. Use the Find Person screen to find the person for whom you want to print a badge.

3. Select the printer from the list, then click **Continue**.

4. Select a layout from the list.

   Note: You can print any layout that is associated with a credential profile available to the user's role. The user's role must have the **Can Receive** option selected in the credential profile.

5. Click **Print**.

5.12.3 Printers have external readers

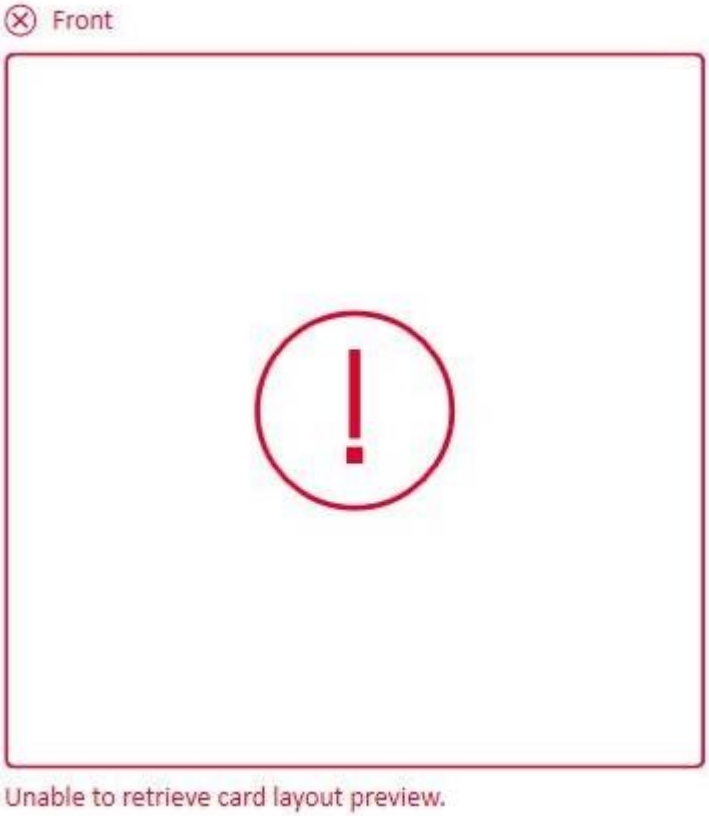
You can configure MyID to ask the operator to read the proximity serial number using an external prox reader before inserting the card into the printer when using the **Collect Card** workflow.

To enable this feature:

1. From the **Configuration** category, select **Operation Settings**.
2. Click the **General** tab.
3. Set the following option:
   - **Printers have External Prox Readers** – set to Yes to enable reading the proximity serial number before placing the card in the printer.
4. Click **Save changes**.

With this option enabled, in the **Collect Card** workflow, MyID reads the serial number of the proximity card, then instructs you to place the card in the printer hopper; you then click **Next** to print the card.

5.12.4 Troubleshooting card layout preview issues



If the preview image of the card displays an error with the following:

```
Unable to retrieve card layout preview
```

the issue may be caused by the following:

- Missing data in the user record.

  For example, there may be custom fields that are included on the card layout that are not populated for the cardholder.

- Missing image files.

  For example, if you have specified a dynamic custom image based on a field in the user record, and there is no corresponding file that matches the dynamically-generated filename.

- Problems accessing the CRL for the IIS SSL certificate.

  For https connections, the client PC must be able to access the CRL for the certificate used for the MyID website. If you are experiencing problems, you can disable the server certificate revocation check on the client; in **Internet Options**, on the **Advanced** tab, in the **Security** section, deselect the **Check for server certificate revocation** option.

Make sure that you have set the **Image Upload Server** option (on the **Video** page of the **Operation Settings** workflow) to the name of the MyID web server; for example:

```
myserver.example.com
```

5.13 Batch encoding cards

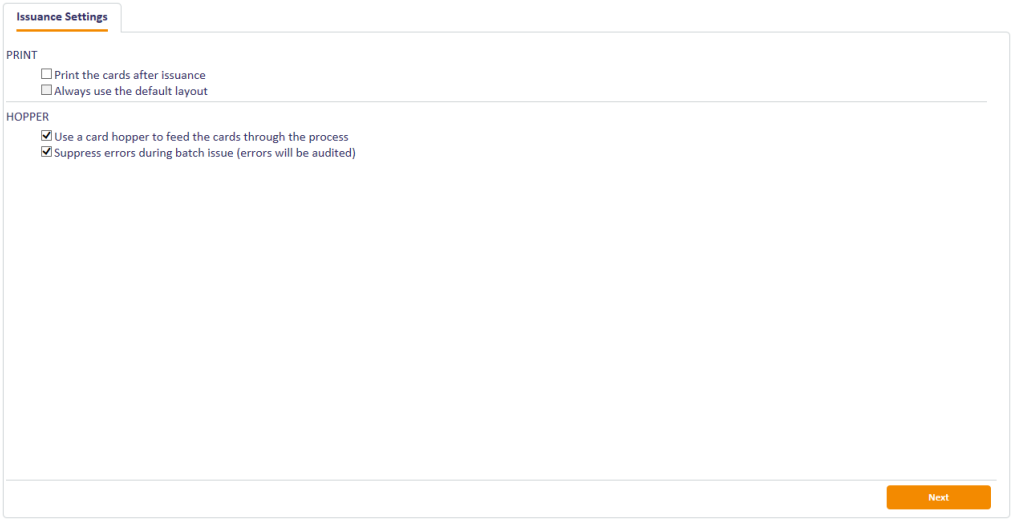
The **Batch Encode Card** workflow allows you to pre-encode cards with their personalization details. When you distribute the cards to the applicants, the applicants can then activate their cards quickly without having to encode them. You must configure the credential profile for these devices to use **2-Step** for the **Pre-encode Card** option; see the *Configuring a credential profile for activation* section in the ***Administration Guide***.

You use the **Batch Encode Card** workflow after you have issued the cards with their GlobalPlatform keys locked, or after they have come back from a bureau with their GlobalPlatform keys locked.

To pre-encode cards:

1. From the **Cards** category, select **Batch Encode Card**.

   You can also launch this workflow from the **Batch** section of the **More** category in the MyID Operator Client. See the *Using Batch workflows* section in the ***MyID Operator Client*** guide for details.



2. Select your encoding options:
   - **Print the cards after issuance**

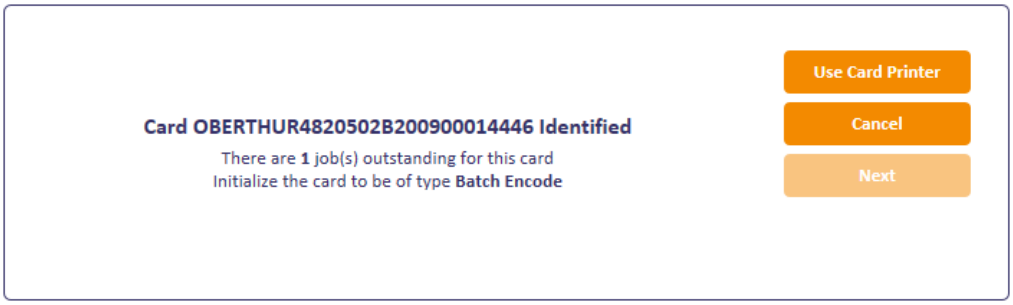
     If the cards have not already been printed, you can print them as you encode them.
   - **Always use the default layout**

     If you are printing the cards, you can select this option so you don't have to select a layout for each card.
   - **Use a card hopper to feed the cards through the process**

     Select this option if you are using a card hopper rather than a card reader to encode the cards.
   - **Suppress errors during batch issue (errors will be audited)**

     If you are using a card hopper for encoding, select this option so you can leave the process unattended. Any errors will be audited.
3. Click **Next**.

4. Insert the first card. If the card is in the correct state to be encoded, MyID encodes the card.

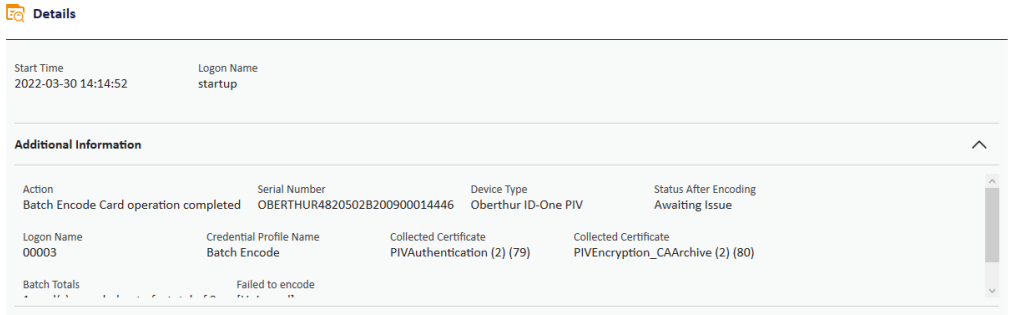


If you are using a hopper, the next card is inserted automatically. If you are using a card reader, insert the next card.

If you are using a card reader, click **Finish** when you have completed encoding all the cards you want to encode.

If you are using authentication codes, these are sent by email to the applicant at this stage.

When the process is complete, a summary is shown. Click **Additional Information** to display the details.



5.13.1 Timeout and automatic canceling

The **Batch Encode Card Timeout** setting (in the **Operation Settings** workflow, **General** tab) specifies how long between cards the **Batch Encode Card** workflow waits before it quits the workflow. By default this is set to 15 seconds.

If you are using a hopper, and two cards in a row are detected as invalid cards, MyID assumes the batch of cards is incorrect (for example, the cards may have been placed in the hopper the wrong way) and it quits the workflow.

5.14 Card ready notification

If you have set the **Activation Authentication** in the credential profile to **Authentication Code (Manual)**, an authentication code is required to activate or unlock the card. An operator must request an authentication code using the **Request Auth Code** or **Card Ready Notification** workflow.

Once you have requested and collected a card, you can use the **Card Ready Notification** workflow to mark the card as available for collection and send the authorization code by email.

To mark a card as ready for collection:

1. From the **Cards** category, select **Card Ready Notification**.
2. Insert the card.

   The card is marked as ready for collection, and the authorization code is sent by email to the applicant.

5.15 Disposing of cards

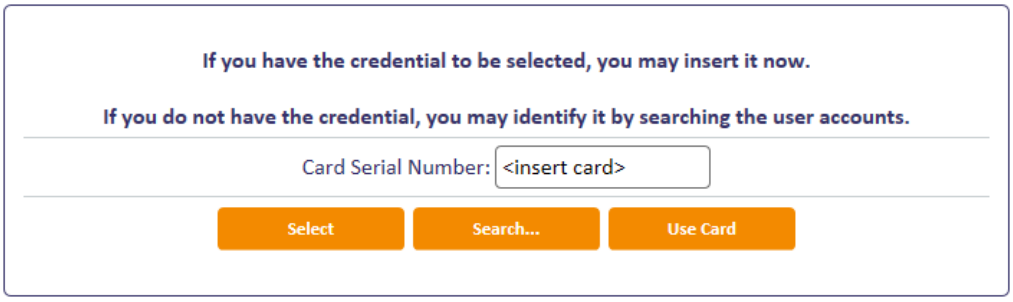
You can mark a card as disposed within MyID. This creates an audit trail of the date and time of the disposal along with the identity of the operator who disposed of the card. Before you can dispose of a card, you must cancel it and disassociate it from its user; however, if the card has expired, and the **Allow disposal of expired devices** configuration option is set to **Yes**, you can dispose of the card without canceling it.

Note: You can also use the **Erase Card** workflow to set the disposal status of cards. See section *5.11.2*, *Erasing a card*.

To dispose of a card:

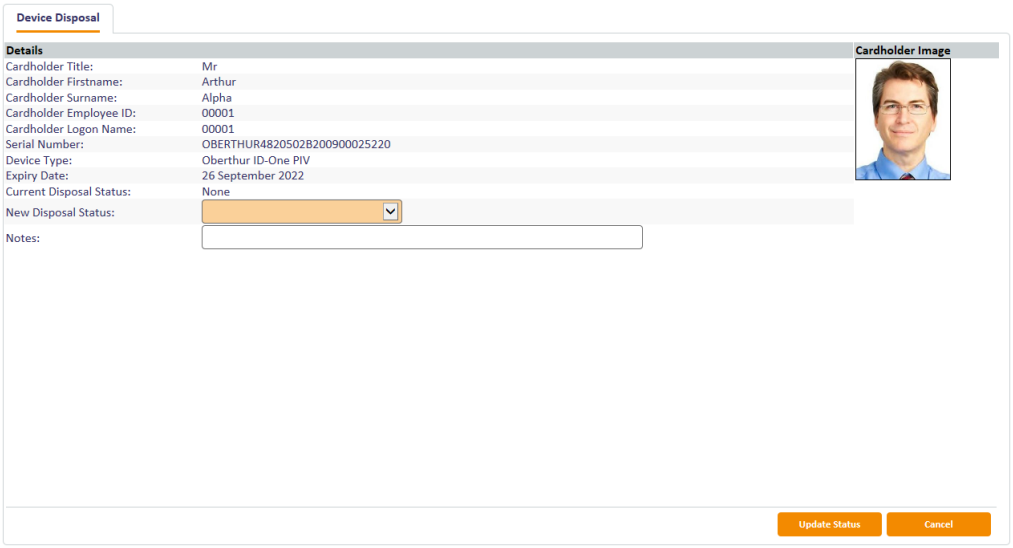
1. From the **Cards** category, select **Card Disposal**.

   Alternatively, you can use the **Change Disposal Status** option in the MyID Operator Client. See the *Disposing of a device* section in the ***MyID Operator Client*** guide for details.



2. If you have the card you want to dispose of, insert the card in the card reader.

   Alternatively, close the Select Card dialog, click **Search**, then use Find Person to find the person to whom the card is assigned, or to whom the card was previously assigned, then select the card you want to dispose of.



3. Set the following:
   - **New Disposal Status** – select one of the following statuses:
     - **Collected**
     - **Disposed**
     - **Legacy**
     - **Lost**
     - **None**
     - **Not Collected**

     Note: When you mark a card with the status **Disposed** or **Lost**, MyID prevents it from ever being issued again. If you select any of the other disposal statuses, you *can* issue the card again.
   - **Notes** – type information about the reason you are disposing of the card.
4. Click **Update Status**.

   The status of the card is updated in the MyID database, and the status change is recorded in the audit trail.

   The audit summary is displayed on completion of the workflow.

5.16 Reinstating cards

The **Reinstate Card** workflow allows you to reassign a canceled card to its original user. This may be useful if you cancel a card that does not need to be canceled; for example, if a cardholder reports their card as missing, then subsequently finds it before the replacement card has been issued.

Once you have reinstated a card, you must activate it before it can be used. The credential profile for the card must require activation. If the card is not present when you use the **Reinstate Card** workflow, you cannot use self activation; you must use the **Assisted Activation** workflow instead.

Note: You cannot reinstate a card that has expired.

The cardholder must have card issuance approved, and must be able to be issued the current version of the card profile. The operator who is using the **Reinstate Card** workflow must also have permissions to issue the card profile. Both the card profile and the cardholder must still exist in the MyID system – you cannot reinstate a card if either have been deleted.

Note: **Reinstate Card** is currently supported only for PIV cards.

As an alternative, you are recommended to use the **Reinstate** option on the View Device screen in the MyID Operator Client; this feature can reinstate canceled or erased smart card without requiring the credential profile to be set up for activation, and supports any smart card, not just PIV cards. See the *Reinstating a device* section in the ***MyID Operator Client*** guide for details.

To reinstate a card:

1. From the **Cards** category, select **Reinstate Card**.
2. Insert the card to be reinstated, or search for the card you want to reinstate remotely.

   If you search for the card, you must search for the cardholder, then select from the list of available devices for that cardholder.
3. On the person details screen, confirm that you have selected the correct person.
4. Click the **Details** tab and check that there are no pending card replacement requests.

   If there are any pending requests, you can continue with the reinstatement, but you must cancel the card replacement jobs manually.
5. Click **OK**.
6. On the Warning dialog, click **Yes** to continue.
7. Check the details of the card profile.

   Note: You cannot change the card profile for the card.
8. Click **OK** to reinstate the card.

   This completes the workflow.
9. Activate the card.

   Once the card has been reinstated, you must activate the card before you can use it.

   Note: If your system or the card profile is set up to require biometric verification for issuance, the cardholder must verify their biometrics to complete the activation. Make sure that you carry out the activation on a system that has a suitable biometric reader.

   - To activate a card yourself, insert the card into the card reader at the MyID logon screen and follow the instructions.
   - To activate a card for another user, from the **Cards** category, select **Assisted Activation**.

5.17 Reprovisioning cards

The **Reprovision Card** and **Reprovision My Card** workflows allow you to re-encode a card completely, based on the data in the MyID database, using the latest version of the credential profile used during issuance.

The card will have the same expiry date as the original card. New certificates may have longer expiration times than the original certificates, but these will not exceed the lifetime of the card itself. Certificates that were revoked externally to MyID will be replaced with new active certificates.

The card must not have been canceled or disabled, and the user's account in MyID must not have been disabled. For PIV systems, the cardholder must be approved for issuance.

Note: Reprovisioning erases and rewrites the card content. If you interrupt the reprovisioning process after the initial card authentication has taken place (for example, by pulling your card from the reader, canceling the workflow, or shutting down MyID) your smart card may be left in an unusable state. To remedy this, carry out the reprovisioning process again, or cancel and reissue the smart card.

These workflows are designed for reprovisioning smart cards only, not contactless tokens.

Validation is not required, even if the credential profile has the **Validate Issuance** option set.

Note: If you want to create a reprovision request then allow the cardholder to update their own smart card using the Self-Service App, you can use the **Request Card Update** workflow to request an update, selecting a reason that requires a reprovision. See section *5.7.2*, *Requesting a card update* for details.

To reprovision a card:

1. From the **Cards** category, select **Reprovision Card**.

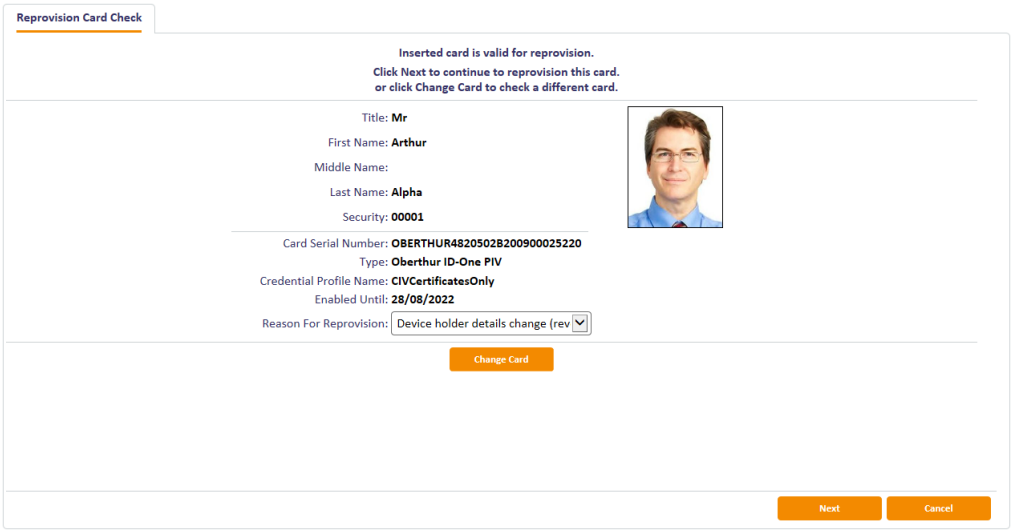
   The **Reprovision My Card** workflow works in the same way as the **Reprovision Card** workflow, with the exception that you can reprovision only those cards that are assigned to you.

   Notes:

   - You can also launch the **Reprovision Card** workflow from the View Device screen of the MyID Operator Client. See the *Reprovisioning a device* section in the ***MyID Operator Client*** guide for details.
   - You can also launch the **Reprovision My Card** workflow from the self-service menu in the MyID Operator Client. See the *Launching self-service workflows* section in the ***MyID Operator Client*** guide for details.

2. Insert a card to be reprovisioned.

   MyID checks the card and informs you if it can be reprovisioned.



Click **Change Card** to rescan the available card readers on your PC.

Note: The **Change Card** button does not appear if you launch this workflow from the MyID Operator Client.

3. Select the **Reason For Reprovision** from the drop-down list.

   See section *6.5*, *Certificate reasons* for details.

4. Click **Next**.

   A warning appears. The wording of this warning differs between the **Reprovision Card** and **Reprovision My Card** workflows; the **Reprovision Card** version provides more information to the operator about what happens to the card and account during the process of reprovisioning the card.

5. Click **Continue**.

6. Type the **New PIN** and confirm it, then click **Next**.

   The card is now re-encoded with the latest information.

5.18 Assigning cards

You can use the **Assign Card** workflow to assign a particular smart card to a card request job. The user can use only the card that has been assigned to that job in the **Collect Card** or **Collect My Card** workflows.

For example:

1. Using the Lifecycle API, import Jane Smith's details into MyID request a card for her.
2. Use the **Assign Card** workflow to assign the card with serial number 123456 to Jane Smith's card request job.
3. Hand the card with serial number 123456 to Jane Smith.

   Jane Smith can use this card as an ID badge, but it does not contain any electronic personalization; for example, certificates. No-one else can now use this card.

4. Jane Smith collects the card personalization using MyID. Jane can write this data onto the card with serial number 123456 only; no other card is accepted by MyID.

Note: If the card request job does not have a card assigned, the user can use any card that has not been assigned to another user.

5.18.1 Assigning known cards

You can restrict the **Assign Card** workflow to assign only cards that are known to MyID; that is, they have previously had their serial numbers imported. In the credential profile, set the **Only Issue to Known Serial Numbers** option.

See the *Importing serial numbers* section in the ***Administration Guide*** for details.

5.18.2 Assigning a card

To assign a card:

1. From the **Cards** category, select **Assign Card**.
2. On the Find Person stage, type the details for the user you to whom you want to assign a card, then click **Search**.
3. Select the user from the list.
4. If more than one card request exists for that person, select the card request you want to use; if there is a single card request, this is automatically selected.
5. If the **Allow card serial number to be entered during Request Card workflow** option is set to `Yes`, you can enter the serial number.

   Alternatively, insert the card you want to allocate.
6. If you have more than one card inserted in card readers, select the card you want to assign to the user.

   Note: You cannot assign a card that is already issued to another user. You can assign a card if the card is assigned to another card request, if the other card request is within your scope.

   The card is now assigned to the card request. The serial number of the assigned card is displayed in the summary at the end of the workflow.

5.18.3 Unassigning cards

Only one card can be assigned to a card request at any one time. If you assign card 123456 to Jane Smith's card request, and then you subsequently assign card 999999 to her card request, card 123456 is no longer assigned to her card request, and is therefore available to be assigned to another user.

You cannot remove an assigned card from a user's card request in MyID Desktop without replacing it. Once you assign a card to a user, you can only unassign the card by assigning a different card.

Alternatively, you can use the **Unassign Device** option in the MyID Operator Client to remove the association between the device and the request. See the *Unassigning a device* section in the ***MyID Operator Client*** guide.

6 Working with certificates

Digital certificates are pieces of data that use a digital signature to identify the holder of the certificate, and may provide information on what a person is allowed to access – for example, a certificate may allow someone to log on to Windows. Certificates are issued by Certificate Authorities (CAs) which use Public Key Infrastructure (PKI) to provide trusted third-party vetting for user identities.

Certificates can be stored on hardware such as smart cards and tokens, or (as soft certificates) stored in your web browser's certificate store.

6.1 Issuing certificates

Certificates are normally written to a card when it is issued; any pending card certificates can be collected later.

Soft certificates can be collected in a browser's certificate store. See also section *6.3*, *Issuing soft certificates using a credential profile* for details of working with soft certificates.

6.1.1 Collecting certificates

You can update a card using the **Update Card** or **Collect My Updates** workflows to collect any pending certificates. You can collect certificates for another cardholder or for your own card. See section *5.7*, *Updating cards* for details.

Note: If you want to collect soft certificates, you must use the **Collect My Certificates** workflow. If you want to collect updated certificates for a card that has already been issued, you must use the **Collect My Updates** workflow.

To collect certificates:

1. From the **Certificates** category, click **Collect Certificates**.

   You can also launch this workflow from the **Certificate Administration** section of the **More** category in the MyID Operator Client. See the *Using Certificate Administration workflows* section in the ***MyID Operator Client*** guide for details.

2. Insert the card onto which you want to collect the certificates, then click **Update**.

   MyID checks for any pending certificates, then writes them to the card.

To collect pending certificates for your own card:

1. From the **Certificates** category, click **Collect My Certificates**.

   MyID checks for any pending certificates, then writes them to the card.

Note: You must log on with the card to collect pending certificates. If your credential profile specifies a certificate to use for MyID Logon, you cannot log on with the card if the certificate has not yet been issued. You must ask an operator to use the **Collect Certificates** to collect the pending certificates onto your card instead.

MyID then checks for any pending soft certificates and writes them to the browser's certificate store.

6.1.2 Viewing pending certificate requests

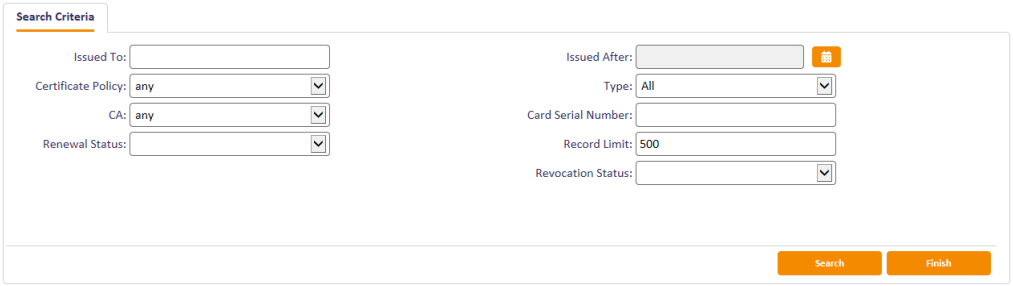
The **Certificate Requests** workflow allows you to view the status of all pending certificates in the system. You can also choose to pause the certificate request and resume it at a later date.

Note: This workflow provides system administration capabilities, so does not restrict information based on the scope of the operator.

Note: As an alternative to using the **Certificate Requests** workflow, you can use the Certificates search in the MyID Operator Client to pause and resume certificate processing. See the *Pausing and resuming certificate processing* section in the ***MyID Operator Client*** guide.

To view certificate requests:

1. From the **Certificates** category, click **Certificate Requests**.



2. Type the details for the certificates you want to view, then click **Search**.

   MyID displays the matching certificates in a table.

3. Select a certificate to view its details.

4. You can click **Pause** to prevent further processing of the certificate request, or **Resume** to resubmit the selected certificate for processing.

6.2 Administering certificates

You can list all the certificates that have been issued or revoked by the system; this allows you to revoke, suspend, or unsuspend certificates, as well as change the renewal details for them.

Note: This workflow provides system administration capabilities, so does not restrict information based on the scope of the operator.

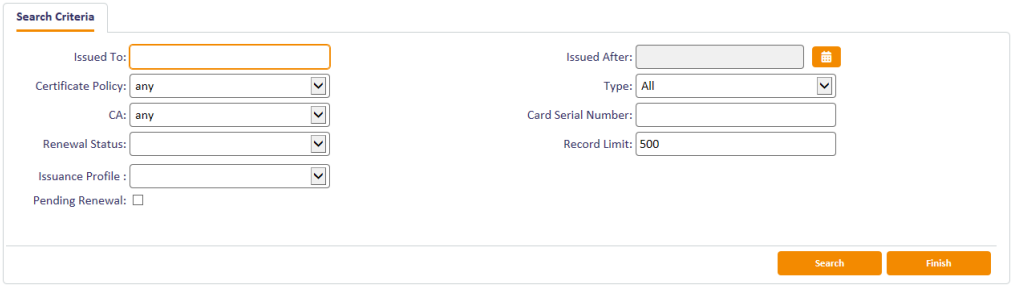
6.2.1 Viewing issued certificates

Note: As an alternative to using the **Issued Certificates** workflow, you can use the Certificates search in the MyID Operator Client to list the issued certificates, revoke or suspend any certificates if required, and change their renewal settings. See the *Searching for*

a certificate, *Revoking, suspending, and unsuspending certificates*, and *Changing renewal settings for a certificate* sections in the ***MyID Operator Client*** guide.

To view issued certificates:

1. From the **Certificates** category, click **Issued Certificates**.



2. Enter the details for the certificates you want to list, then click **Search**.

   MyID lists the certificates that match your search criteria in a table.

3. Click a certificate to view its details.

   You can select more than one certificate if you want to change the renewal settings or revoke multiple certificates at the same time.

4. Use the buttons to decide what to do next:
   - Click **New Search** to return to the start of the workflow.
   - Click **Change Renewal** to change the renewal date for the certificate.
   - Click **Auto Renewal** to change whether the certificate is automatically renewed:
     - Select **Yes** if you want the certificate to renew automatically.
     - Select **No** if you do not want the certificate to renew automatically.

       Click **OK**.
   - Click **Revoke** to revoke or suspend the certificate:
     a. Select the **Reason** from the drop-down list.

        See section *6.5*, *Certificate reasons* for details.

        Note: Make sure that the reason you select is appropriate for the certificate you have selected. For example, some reasons do not affect archived certificates.

     b. Type a description in the **Details** box.

     c. Click **Revoke**.

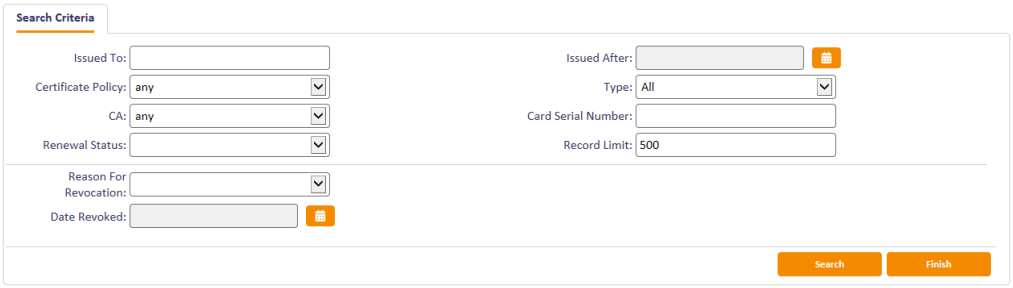
5. Click **Finish** to complete the workflow.

6.2.2 Viewing revoked certificates

Note: As an alternative to using the **Revoked Certificates** workflow, you can use the Certificates search in the MyID Operator Client to list the revoked certificates and unsuspend any certificates if required. See the *Searching for a certificate* and *Revoking, suspending, and unsuspending certificates* sections in the ***MyID Operator Client*** guide.

To view the revoked certificates:

1. From the **Certificates** category, click **Revoked Certificates**.



2. Enter the details for the certificates you want to list, then click **Search**.

   MyID lists the certificates that match your search criteria in a table.

3. Click a certificate to view its details.

4. If a certificate has been suspended, you can unsuspend it: click the **Unsuspend** button.

6.3 Issuing soft certificates using a credential profile

Soft (or browser) certificates are not stored on a device such as a card or token; they are stored on your PC. You can either request a certificate and allow the user to collect it using MyID, or you can create a certificate in a password-protected file that you can send to the user.

You issue soft certificate using a credential profile; this treats the package of certificates as a virtual card. Certificates are either added to the recipient's local store or exported as a PFX file. You can remotely administer these certificates as a card, allowing easy disabling, replacing and canceling of the certificates.

You can issue certificates issued using either a CSP or CNG/KSP.

Note: Issuing and recovering certificates with elliptic curve cryptography (ECC) keys to a software local store (CSP), or as a .pfx file, is not currently supported.

This section provides instructions for working with soft certificates using MyID Desktop. Alternatively, you can use the MyID Operator Client to work with soft certificates; the MyID Operator Client features also allow you to print transport and PIN mailing document for soft certificates. See the *Working with soft certificates* section in the ***MyID Operator Client*** guide for details.

- **IKB-392 – Software certificates fail to import on older Windows versions or Apple Devices**

  Changes were introduced to the method MyID uses to generate software certificates in MyID 12.7.

  When MyID issues software certificates, it encrypts the passwords protecting the PFX files using AES256/SHA2.

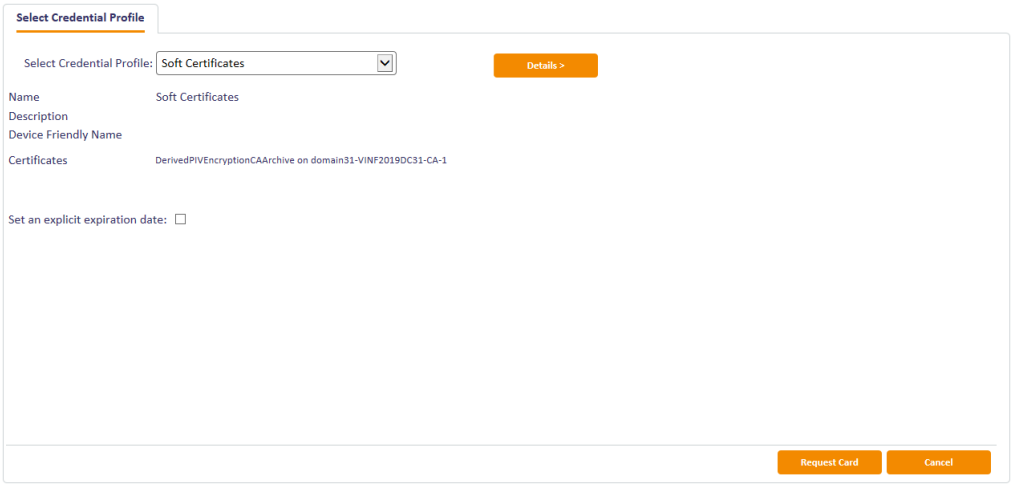
  This is a modern security standard, but it creates a problem when importing the certificates on devices that do not support this security standard; for example, any Apple OS (MacOS or iOS), any Windows Server OS lower than Windows 2019, and any Windows client OS lower than Windows 10 build 1709.

If you are affected by this issue, contact Intercede customer support for further assistance, quoting reference IKB-392.

6.3.1 Requesting soft certificates

To request soft certificates for another user:

1. From the **Cards** category, select **Request Card**.
2. Use the Find Person screen to find the person to whom you want to issue the certificates.
3. Select the person.



4. From the **Select Credential Profile** list, select a credential profile containing soft certificates.

   See the *Setting up a credential profile for soft certificates* section in the ***Administration Guide*** for details of setting up a profile.

5. Click **Request Card**.

You can also request soft certificates in the MyID Operator Client. See the *Requesting a device for a person* section in the ***MyID Operator Client*** guide for details.

6.3.2 Validating soft certificate requests

If the soft certificate credential profile has the **Validate Issuance** option set, you must validate the request before you can collect the soft certificates.

To validate a soft certificate request:

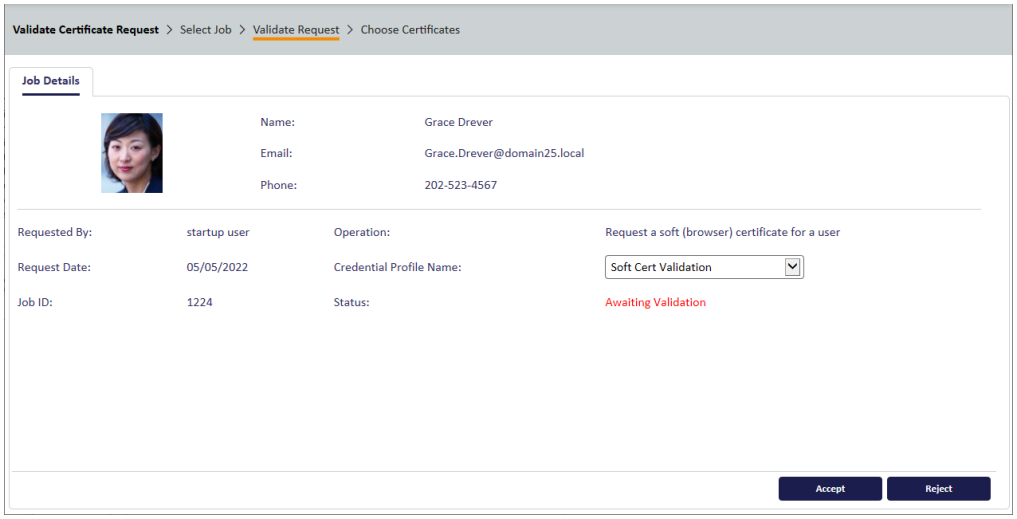
1. From the **Certificates** category, click **Validate Certificate Request**.

   You can also launch this workflow from the **Certificate Administration** section of the **More** category in the MyID Operator Client. See the *Using Certificate Administration workflows* section in the ***MyID Operator Client*** guide for details.

2. Use the search screen to enter the criteria for the request, then click **Search**.

   The list of requests that require validation is displayed.

3. Select the job you want to validate and view its details.
4. If required, you can change the credential profile for the request by selecting a different soft certificate credential profile from the drop-down list.



5. Click **Accept** to validate the request, or **Reject** to cancel the request. If you reject the request you must provide a reason.

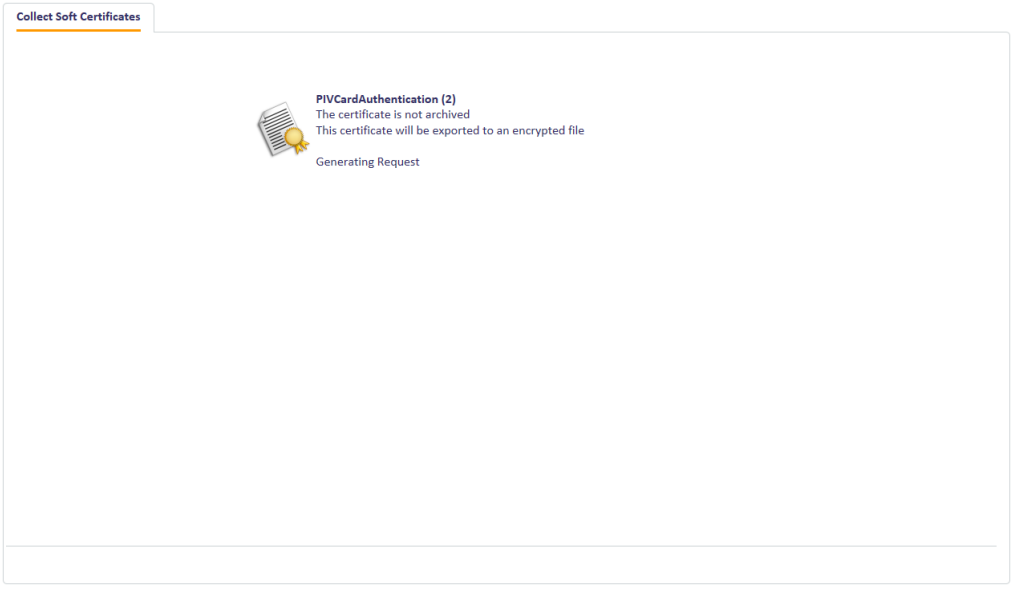
6.3.3 Collecting soft certificates

Once an administrator has requested a credential profile containing soft certificates, the user can collect the certificates.

To collect your certificates:

1. Log in to MyID using an existing card or passwords.
2. From the **Certificates** category, click **Collect My Certificates**.

   Note: You can also launch this workflow from the self-service menu in the MyID Operator Client. See the *Launching self-service workflows* section in the ***MyID Operator Client*** guide for details.

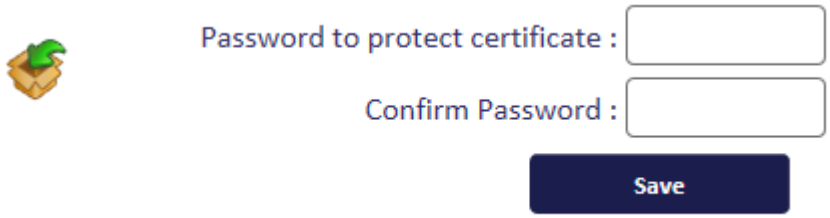


MyID checks for any pending soft certificates.

If the certificates are taking a long time to issue, you can:

- Click **Cancel** – you can exit the workflow and collect the certificates later.
- Click **Fail** – you can exit the workflow, but the certificates are failed. Any failed certificates must be requested again.

3. Once the certificates are ready, the next action depends on the **Storage Method** setting for the certificate policy in the credential profile:
   - **FileStore** – type and confirm the password for the PFX file, then click **Save**.



     You can use the following characters in PFX passwords:

     `a-z A-Z 0-9 ! \ " # $ % ' ( ) * + - . / : ; = ? @`

     Note: You cannot use spaces.

     Choose a location and name for the PFX file, then click **Save**.

     You can now double-click the PFX file, enter the password, and add it to your certificate store.

     Note: If you want to issue certificates using CNG/KSP, you must use the `certutil` utility to import the PFX rather than just double-clicking on the file, as double-clicking automatically loads the private key into the Microsoft Enhanced Cryptographic Provider; that is, a CSP rather than a KSP.

   - **SystemStore** – the certificate is stored automatically in the Personal certificate store of the logged-on Windows user.

   Note: If the **Storage Method** is set to **AutoSave**, the **Collect My Certificates** workflow behaves in the same way as with **SystemStore**. If you want to use the **AutoSave** option to save the certificate to a USB device automatically, you must use the MyID Operator Client to collect the soft certificate request instead.

6.3.4 Working with certificate packages

Once you have issued a certificate package, it is treated as a virtual card by MyID. For example, you can enable or disable the package using **Enable/Disable Card**, and the certificates will be suspended or unsuspended; you can cancel the package using **Cancel Credential**, and the certificates will be revoked.

You can cancel a soft certificate package in the MyID Operator Client; on the View Device screen, click **Cancel Device**. See the *Canceling a device* section in the ***MyID Operator Client*** guide for details.

You can request a renewal for a soft certificate package in the MyID Operator Client; on the View Device screen, click **Request Device Renewal**. See the *Renewing a device* section in the ***MyID Operator Client*** guide for details.

Certificate packages appear in the list of cards with names like "Certificate Package 1451".

6.4 Recovering certificates

If you have archived your issued certificates, you can recover them to a card if you need to. For example, if the card is lost, you can recover the certificate onto a new card so that any encrypted data (for example, encrypted email) can continue to be accessed.

Note: You must be logged in with a card to recover certificates. You cannot recover certificates if you have logged in to MyID using security phrases.

Note: When you recover certificates to a PIV card, all retired certificate containers are overwritten. This affects any smart card with a PIV applet.

- **IKB-392 – Software certificates fail to import on older Windows versions or Apple Devices**

  Changes were introduced to the method MyID uses to generate software certificates in MyID 12.7.

  When MyID issues software certificates, it encrypts the passwords protecting the PFX files using AES256/SHA2.

  This is a modern security standard, but it creates a problem when importing the certificates on devices that do not support this security standard; for example, any Apple OS (MacOS or iOS), any Windows Server OS lower than Windows 2019, and any Windows client OS lower than Windows 10 build 1709.

  If you are affected by this issue, contact Intercede customer support for further assistance, quoting reference IKB-392.

6.4.1 Recovering someone else's certificates

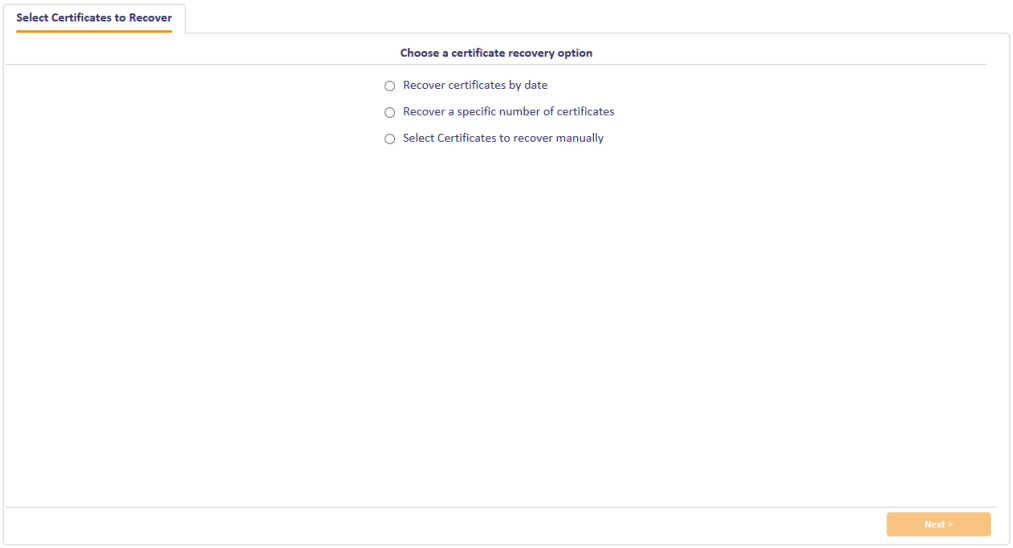
You can recover certificates to another user's card. You can also recover soft certificates to a PFX file.

To recover certificates to a card:

1. From the **Certificates** category, click **Recover Certificates**.

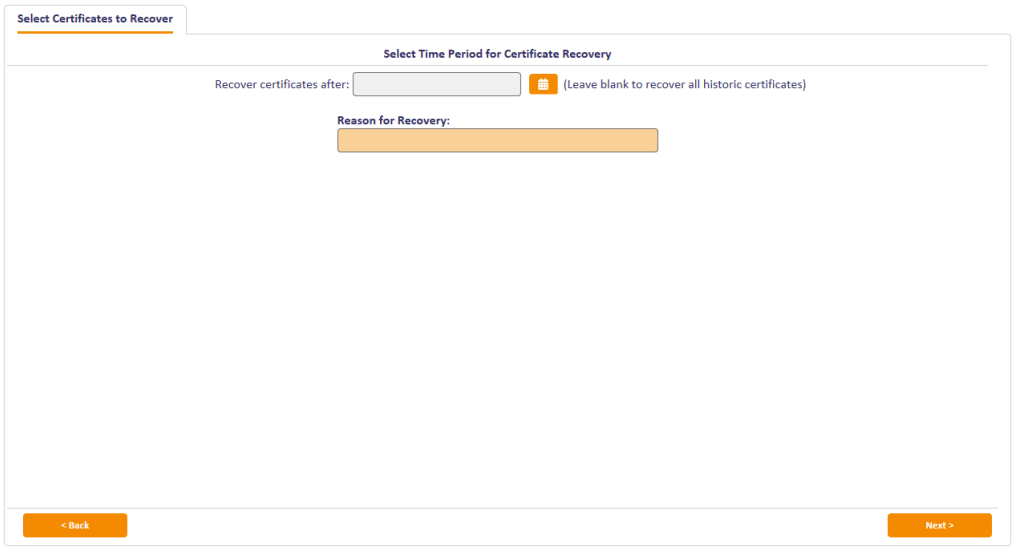
   You can also launch this workflow from the **Certificate Administration** section of the **More** category in the MyID Operator Client. See the *Using Certificate Administration workflows* section in the ***MyID Operator Client*** guide for details.

2. Use the Find Person screen to select the person whose certificate you want to recover.

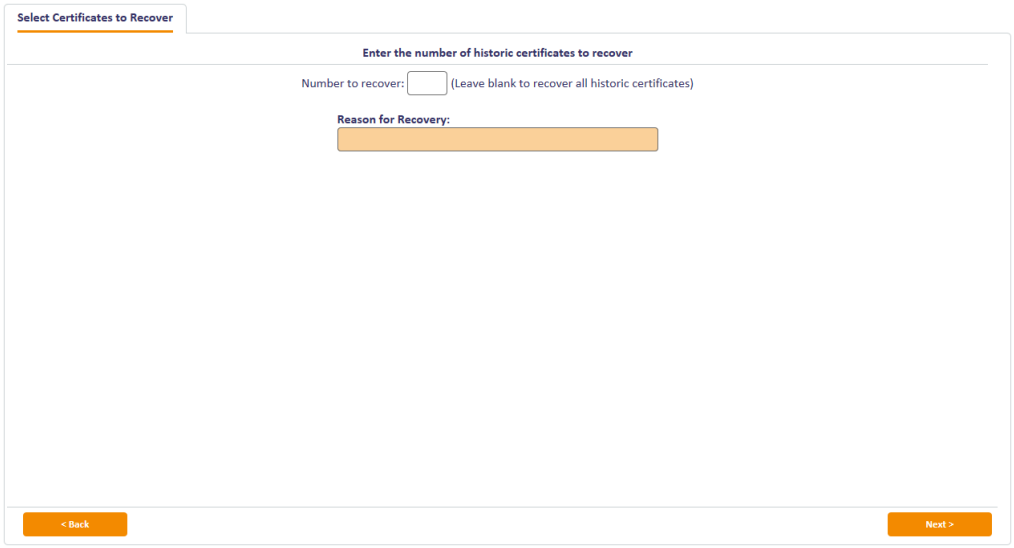


3. Select which certificates you want to recover:
   - **Recover certificates by date** – specify the issuance date after which any keys will be recovered.
   - **Recover a specific number of certificates** – specify the number of keys you want to recover. For example, if you specify `3`, the three most recent keys will be recovered.
   - **Select Certificates to recover manually** – select the certificates from a list of all available certificates.
4. Click **Next**.

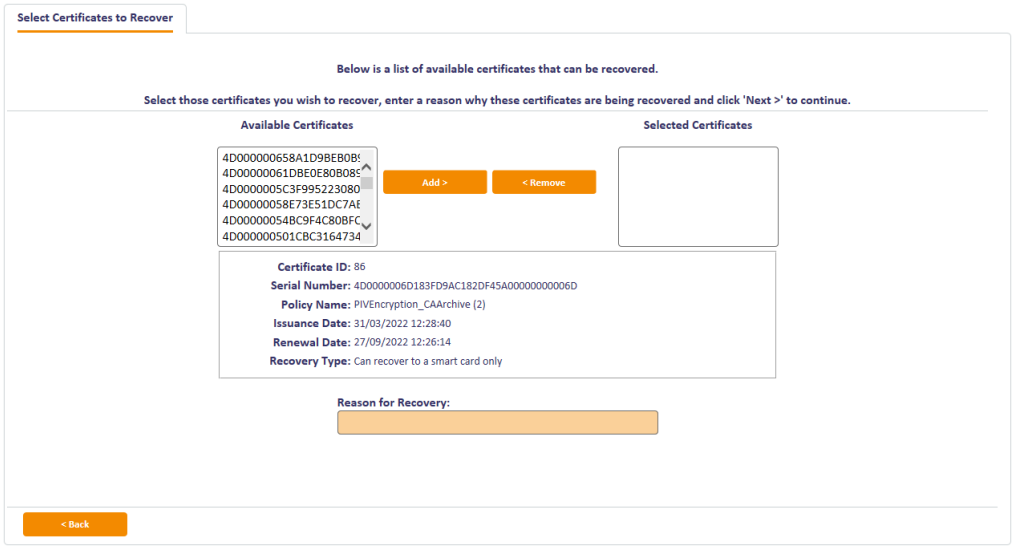
   Carry out one of the following, depending on the option you selected on the previous screen:
   - Select a date. All certificates issued after this date will be recovered.



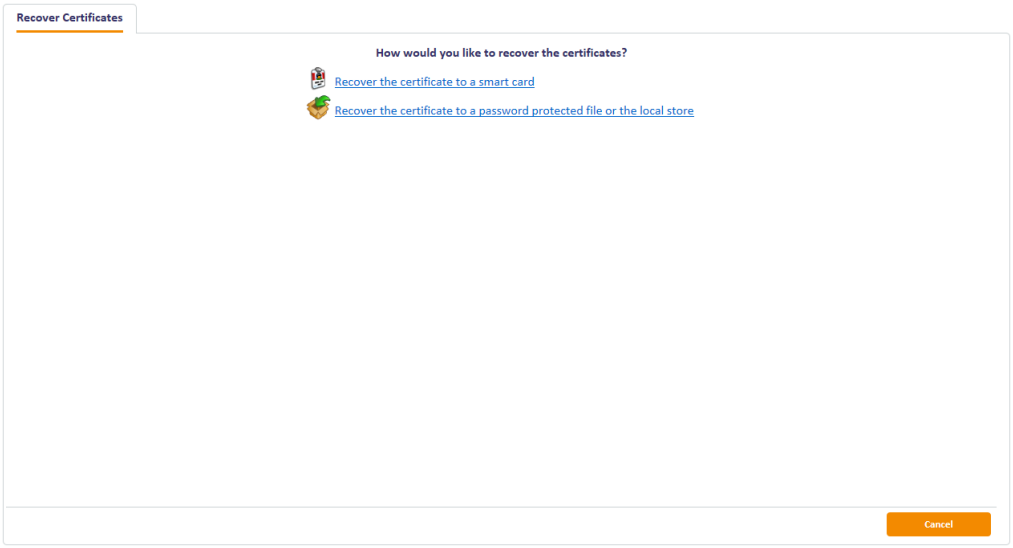
   - Type a number of certificates. That number of the most recent certificates will be recovered.



- Use the **Add** button to select certificates from the **Available Certificates** list.



5. Type a **Reason for Recovery** in the text box.
6. Click **Next**.



The options available depend on how the **Recovery Storage** option on the certificate policy is configured. See section *6.4.3*, *Options for recovering soft certificates*.

7. Select one of the following options:

   - **Recover the certificate to a smart card**

     Insert the card to which to you want to recover the certificate, click **Confirm** to confirm the card, type the **PIN**, then click **Next**. MyID writes the recovered certificates to the card.

   - **Recover the certificate to a password protected file or the local store**

     Note: The options available depend on how the **Storage method allowed for certificate recovery** configuration option is configured. This option may be labeled **Recover the certificate to a password protected file** or **Recover the certificate to the local store** if only those options are available instead of both. See section *6.4.3*, *Options for recovering soft certificates*.

     If both methods are available, choose one of the following subsequent options:

     - **Add the certificate to the local store**

       The certificate is added to the local store automatically.

     - **Export the certificate and private key as a PFX file**

       Click **Enter protection password then choose destination**, type the password for the certificate, and click **Save**.

       You can use the following characters in PFX passwords:

       ```
       a-z A-Z 0-9 ! \ " # $ % ' ( ) * + - . / : ; = ? @
       ```

       Note: You cannot use spaces.

Note: Using the **Recover Certificates** workflow on a card with named certificate containers will overwrite any existing certificates in historic certificate containers with the certificates you selected, or which were automatically selected for recovery. This includes any historic certificates written to the card during issuance. If an operator recovers their own certificates to the card, their current live encryption certificate may be recovered to a historic container (in addition to its presence in the live archived container).

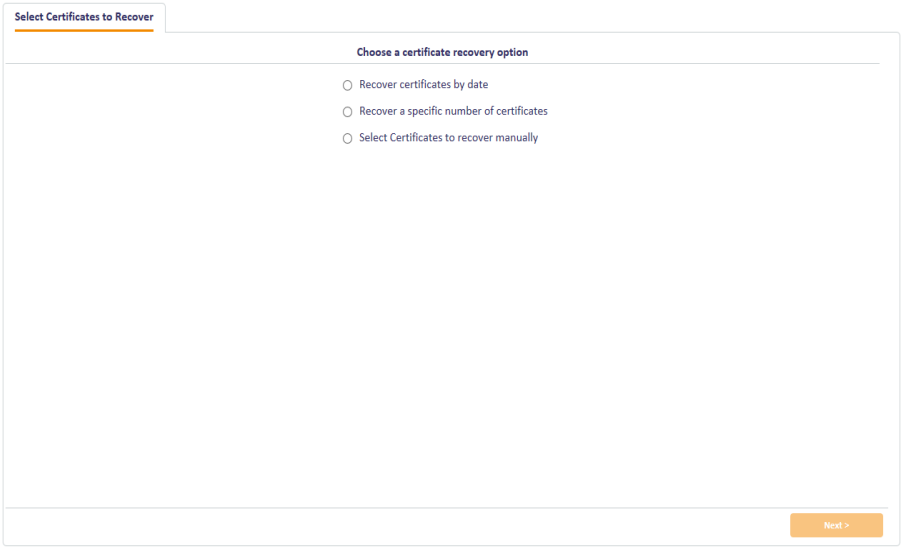
6.4.2 Recovering your own certificates

Note: The **Recover My Certificates** workflow is not automatically assigned to any roles. If you want people to be able to recover their own certificates, use the **Edit Roles** workflow to make it available.

To recover certificates to your own card:

1. From the **Certificates** category, click **Recover My Certificates**.

   Note: You can also launch this workflow from the self-service menu in the MyID Operator Client. See the *Launching self-service workflows* section in the ***MyID Operator Client*** guide for details.



2. Follow the same process as for the **Recover Certificates** workflow; see section *6.4.1*, *Recovering someone else's certificates* above.

6.4.3 Options for recovering soft certificates

The certificate recover method is determined at the point of recovery, rather than at the point of issuance; if you change the **Recovery Storage** option on the certificate policy, or change the global **Storage method allowed for certificate recovery** configuration option, it affects all issued soft certificates.

The following table describes how the **Recovery Storage** (certificate policy) and the **Storage method allowed for certificate recovery** (global configuration setting) options affect the recovery of soft certificates:

	Recovery Storage		
Storage method allowed for certificate recovery	**Hardware**	**Software**	**Both**
Save to PFX	Can recover to smart card.	Can recover to encrypted PFX.	Can recover to smart card or to encrypted PFX.
Local Store	Can recover to smart card.	Can recover to user's local certificate store.	Can recover to smart card or to user's local certificate store.
Both	Can recover to smart card.	Can recover to encrypted PFX or to user's local certificate store.	Can recover to smart card, to encrypted PFX, or to user's local certificate store.

6.5 Certificate reasons

When you carry out any action in MyID that can affect the state of certificates (for example, disabling a card, requesting a replacement card, or canceling a card) you are required to specify a reason for the change.

In some cases, a certificate may be a shared certificate – an archived certificate that exists on multiple devices.

This reason will affect how MyID updates the status of the certificates, what certificates are stored on the replacement card (if applicable) and what happens with archived certificates. The reason selected may affect shared certificates; for example, if the user has a mobile credential canceled that has a copy of an encryption certificate from a card, a card update job may be created to issue or recover a new encryption certificate onto all devices that have a copy of the shared certificate that is being revoked.

The list of available reasons depends both on the workflow and on your system configuration. Some reasons are generated by automatic processes – you will not see them in the user interface, but they will appear in the audit record.

6.5.1 Certificate reasons reference

This section lists each reason that you can specify, and details what happens to the card and its certificates in each case.

6.5.1.1 Lost

Current card:	Canceled.
Archived certificate on the current card:	Revoked.
Non-archived certificate on the current card:	Revoked.
Archived certificate on the replacement card:	New certificate created.
Non-archived certificate on the replacement card:	New certificate created.
Expiry date:	Inherited from original card.
Historic certificates:	Attempt to recover certificates, if the device supports historic certificates.

6.5.1.2 Damaged

Current card:	Canceled.
Archived certificate on the current card:	Non-PIV systems: Active. PIV systems: Revoked.
Non-archived certificate on the current card:	Revoked.
Archived certificate on the replacement card:	Non-PIV systems: Original certificate recovered. PIV systems: New certificate created.
Non-archived certificate on the replacement card:	New certificate created.
Expiry date:	Inherited from original card.
Historic certificates:	None.

6.5.1.3 Stolen

Current card:	Canceled.
Archived certificate on the current card:	Revoked.
Non-archived certificate on the current card:	Revoked.
Archived certificate on the replacement card:	New certificate created.
Non-archived certificate on the replacement card:	New certificate created.
Expiry date:	Inherited from original card.
Historic certificates:	Attempt to recover certificates, if the device supports historic certificates.

6.5.1.4 Forgotten

Current card:	Disabled.
Archived certificate on the current card:	Active.
Non-archived certificate on the current card:	Suspended.
Archived certificate on the replacement card:	Original certificate recovered.
Non-archived certificate on the replacement card:	New certificate created.
Expiry date:	Inherited from original card.
Historic certificates:	Attempt to recover certificates, if the device supports historic certificates.

6.5.1.5 Permanently Blocked

Current card:	Canceled.
Archived certificate on the current card:	Non-PIV systems: Active. PIV systems: Revoked.
Non-archived certificate on the current card:	Revoked.
Archived certificate on the replacement card:	Non-PIV systems: Original certificate recovered. PIV systems: New certificate created.
Non-archived certificate on the replacement card:	New certificate created.
Expiry date:	Inherited from original card.
Historic certificates:	None.

6.5.1.6 Compromised

Current card:	Canceled.
Archived certificate on the current card:	Revoked.
Non-archived certificate on the current card:	Revoked.
Archived certificate on the replacement card:	New certificate created.
Non-archived certificate on the replacement card:	New certificate created.
Expiry date:	Inherited from original card.
Historic certificates:	Attempt to recover certificates, if the device supports historic certificates.

6.5.1.7 Device holder on leave

Current card:	Disable temporarily
Archived certificate on the current card:	No action
Non-archived certificate on the current card:	Suspend
Archived certificate on the replacement card:	n/a
Non-archived certificate on the replacement card:	n/a
Expiry date:	No action
Historic certificates:	No action

6.5.1.8 Pending Investigation

Current card:	Disabled.
Archived certificate on the current card:	Suspended (for the **Revoke** option on the View Certificate screen in the MyID Operator Client, or using the MyID Core API with reason status mapping ID 93). Active (for all other operations).
Non-archived certificate on the current card:	Suspended.
Archived certificate on the replacement card:	Original certificate recovered.
Non-archived certificate on the replacement card:	New certificate created.
Expiry date:	Inherited from original card.
Historic certificates:	None.

6.5.1.9 Non-payment of services

Current card:	Disable permanently
Archived certificate on the current card:	Revoke
Non-archived certificate on the current card:	Revoke
Archived certificate on the replacement card:	n/a
Non-archived certificate on the replacement card:	n/a
Expiry date:	No action
Historic certificates:	Revoke

6.5.1.10 Device holder leaving or changing role

Current card:	Cancel
Archived certificate on the current card:	Revoke
Non-archived certificate on the current card:	Revoke
Archived certificate on the replacement card:	n/a
Non-archived certificate on the replacement card:	n/a
Expiry date:	No action
Historic certificates:	Revoke

6.5.1.11 Device holder details change

Current card:	Cancel
Archived certificate on the current card:	Revoke
Non-archived certificate on the current card:	Revoke
Archived certificate on the replacement card:	Issue new
Non-archived certificate on the replacement card:	Issue new
Expiry date:	Set new date
Historic certificates:	Revoke

6.5.1.12 Pending Activation

Current card:	Disable
Archived certificate on the current card:	No action
Non-archived certificate on the current card:	Suspend
Archived certificate on the replacement card:	n/a
Non-archived certificate on the replacement card:	n/a
Expiry date:	No action
Historic certificates:	No action

6.5.1.13 Revocation (other)

Current card:	Canceled.
Archived certificate on the current card:	Revoked.
Non-archived certificate on the current card:	Revoked.
Archived certificate on the replacement card:	New certificate created.
Non-archived certificate on the replacement card:	New certificate created.
Expiry date:	Inherited from original card.
Historic certificates:	Attempt to recover certificates, if the device supports historic certificates.

6.5.1.14 Suspension (other)

Current card:	Disabled.
Archived certificate on the current card:	Suspended (for the **Revoke** option on the View Certificate screen in the MyID Operator Client, or using the MyID Core API with reason status mapping ID 92). Active (for all other operations).
Non-archived certificate on the current card:	Suspended.
Archived certificate on the replacement card:	Original certificate recovered.
Non-archived certificate on the replacement card:	New certificate created.
Expiry date:	Inherited from original card.
Historic certificates:	None.

6.5.1.15 Found Original

Current card:	Cancel replacement card permanently
Archived certificate on the current card:	Recover to original
Non-archived certificate on the current card:	Recover to original
Archived certificate on the replacement card:	No action
Non-archived certificate on the replacement card:	No action
Expiry date:	No action
Historic certificates:	No action

6.5.1.16 Original Device Compromised

Current card:	Cancel
Archived certificate on the current card:	Revoke
Non-archived certificate on the current card:	Revoke
Archived certificate on the replacement card:	n/a
Non-archived certificate on the replacement card:	n/a
Expiry date:	n/a
Historic certificates:	Revoke

6.5.1.17 Request device Renewal

Current card:	No action.
Archived certificate on the current card:	No action.
Non-archived certificate on the current card:	Revoked.
Archived certificate on the replacement card:	New certificate created.
Non-archived certificate on the replacement card:	New certificate created.
Expiry date:	New expiry date calculated from the date of issuance plus the lifetime of the card.
Historic certificates:	Attempt to recover certificates, if the device supports historic certificates.

6.5.1.18 Batch Failed

Current card:	Cancel
Archived certificate on the current card:	Revoke
Non-archived certificate on the current card:	Revoke
Archived certificate on the replacement card:	Issue new
Non-archived certificate on the replacement card:	Issue new
Expiry date:	Set new date
Historic certificates:	Revoke

6.5.1.19 Bureau Failure

Current card:	Cancel
Archived certificate on the current card:	Revoke
Non-archived certificate on the current card:	Revoke
Archived certificate on the replacement card:	Issue new
Non-archived certificate on the replacement card:	Issue new
Expiry date:	Set new date
Historic certificates:	Revoke

6.5.1.20 Processing Failure

Current card:	Cancel
Archived certificate on the current card:	Revoke
Non-archived certificate on the current card:	No action
Archived certificate on the replacement card:	Issue new
Non-archived certificate on the replacement card:	Issue new
Expiry date:	Set new date
Historic certificates:	Revoke

6.5.1.21 Poor print quality

Current card:	Cancel
Archived certificate on the current card:	Revoke
Non-archived certificate on the current card:	Revoke
Archived certificate on the replacement card:	Issue new
Non-archived certificate on the replacement card:	Issue new
Expiry date:	Set new date
Historic certificates:	Revoke

6.5.1.22 Printing misaligned

Current card:	Cancel
Archived certificate on the current card:	Revoke
Non-archived certificate on the current card:	Revoke
Archived certificate on the replacement card:	Issue new
Non-archived certificate on the replacement card:	Issue new
Expiry date:	Set new date
Historic certificates:	Revoke

6.5.1.23 Poor lamination quality

Current card:	Cancel
Archived certificate on the current card:	Revoke
Non-archived certificate on the current card:	Revoke
Archived certificate on the replacement card:	Issue new
Non-archived certificate on the replacement card:	Issue new
Expiry date:	Set new date
Historic certificates:	Revoke

6.5.1.24 Incorrect layout printed

Current card:	Cancel
Archived certificate on the current card:	Revoke
Non-archived certificate on the current card:	Revoke
Archived certificate on the replacement card:	Issue new
Non-archived certificate on the replacement card:	Issue new
Expiry date:	Set new date
Historic certificates:	Revoke

6.5.1.25 Cancel device and leave Certificates

Current card:	Cancel
Archived certificate on the current card:	No action
Non-archived certificate on the current card:	No action
Archived certificate on the replacement card:	n/a
Non-archived certificate on the replacement card:	n/a
Expiry date:	No action
Historic certificates:	No action

6.5.1.26 Cancel Certificates and leave device

Current card:	No action
Archived certificate on the current card:	Revoke
Non-archived certificate on the current card:	Revoke
Archived certificate on the replacement card:	n/a
Non-archived certificate on the replacement card:	n/a
Expiry date:	n/a
Historic certificates:	Revoke

6.5.1.27 Derived Credential Notification Listener

Current card:	Cancel
Archived certificate on the current card:	Revoke
Non-archived certificate on the current card:	Revoke
Archived certificate on the replacement card:	n/a
Non-archived certificate on the replacement card:	n/a
Expiry date:	n/a
Historic certificates:	Revoke

6.5.1.28 Compromised – Reissue Shared Certificates

Current card:	Cancel
Archived certificate on the current card:	Revoke
Non-archived certificate on the current card:	Revoke
Archived certificate on the replacement card:	Issue new
Non-archived certificate on the replacement card:	Issue new
Shared certificate on other devices	Issue new
Expiry date:	Set new date
Historic certificates:	Revoke

6.5.1.29 Credential Profile Update (full revocation)

Current card:	Update or Reprovision (depends on workflow)
Archived certificate on the current card:	Revoke
Non-archived certificate on the current card:	Revoke
Archived certificate on the replacement card:	Issue new
Non-archived certificate on the replacement card:	Issue new
Expiry date:	Set new date
Historic certificates:	Revoke

6.5.1.30 Credential Profile Update (no revocation)

Current card:	Update or Reprovision (depends on workflow)
Archived certificate on the current card:	Leave
Non-archived certificate on the current card:	Leave
Archived certificate on the replacement card:	Leave
Non-archived certificate on the replacement card:	Leave
Expiry date:	Leave
Historic certificates:	Leave

6.5.1.31 Details Change – re-issue archived certificates

Current card:	Reprovision
Archived certificate on the current card:	Revoke, and issue new
Non-archived certificate on the current card:	Do not revoke, and issue new
Archived certificate on the replacement card:	n/a
Non-archived certificate on the replacement card:	n/a
Expiry date:	Leave
Historic certificates:	Recover

6.5.1.32 User details have changed

Current card:	Reprovision
Archived certificate on the current card:	Do not revoke, and issue new
Non-archived certificate on the current card:	Revoke, and issue new
Archived certificate on the replacement card:	n/a
Non-archived certificate on the replacement card:	n/a
Expiry date:	Leave
Historic certificates:	Recover

6.5.1.33 There is a problem with the device

Current card:	Reprovision
Archived certificate on the current card:	Do not revoke, and issue new
Non-archived certificate on the current card:	Revoke, and issue new
Archived certificate on the replacement card:	n/a
Non-archived certificate on the replacement card:	n/a
Expiry date:	Leave
Historic certificates:	Recover

6.5.1.34 New credential profile needs to be applied

Current card:	Reprovision
Archived certificate on the current card:	Do not revoke, and issue new
Non-archived certificate on the current card:	Revoke, and issue new
Archived certificate on the replacement card:	n/a
Non-archived certificate on the replacement card:	n/a
Expiry date:	Leave
Historic certificates:	Recover

6.5.1.35 New certificates need to be added to the device

Current card:	Update
Archived certificate on the current card:	Do not revoke, and issue new – for certificates affected by the update only
Non-archived certificate on the current card:	Revoke, and issue new – for certificates affected by the update only
Archived certificate on the replacement card:	n/a
Non-archived certificate on the replacement card:	n/a
Expiry date:	Leave
Historic certificates:	Recover

6.5.1.36 Device Replacement (Delayed Cancellation)

Current card:	Canceled.
Archived certificate on the current card:	Revoked.
Non-archived certificate on the current card:	Revoked.
Archived certificate on the replacement card:	New certificate created.
Non-archived certificate on the replacement card:	New certificate created.
Expiry date:	Inherited from original card.
Historic certificates:	Attempt to recover certificates, if the device supports historic certificates.

6.6 Historic certificates

A historic certificate is any archived certificate that was assigned to the user (on any credential) using a particular certificate policy.

Whether archived certificates are available for recovery as current certificates is determined by their replacement chain.

For a certificate to be recovered and used, it must never have become compromised and revoked; this will break the replacement chain. Canceling a smart card will revoke its certificates; in this case, you will be unable to continue to use the certificate; however, you will be able to recover the historic certificates.

When you set up the credential profile, for each archived certificate policy, you can select whether you want to recover the certificate, and how many historic certificates you want to store – this must be within the capacity of your credential.

6.6.1 Example smart card history for a PIV system

For example:

- The credential profile is set up with the following certificate profiles:
  - Authentication – set to **Issue New**.
  - Signing – set to **Issue New**.
  - Encryption (archived) – this certificate profile is set to **Use Existing**, and has a maximum number of historic certificates of 2.
- Card A is issued with the following certificates:
  - Authentication 1
  - Signing 1
  - Encryption 1
- Card A is lost, and replacement Card B issued. The following certificates are loaded onto card B:

    - Authentication 2
    - Signing 2
    - Encryption 2
    - Encryption 1 (historic)
- Card B damaged, and replacement Card C issued.
    - Authentication 3
    - Signing 3
    - Encryption 3
    - Encryption 2 (historic)
    - Encryption 1 (historic)
- Card C is forgotten.
    - Authentication 3 – suspended
    - Signing 3 – suspended.
- Temporary Card D is issued to replace Card C.
    - Authentication 4
    - Signing 4
    - Encryption 3 (archived) – this is the *same* certificate as was on Card C – as the credential profile stated **Use Existing**, and the encryption certificate has not been revoked, it can be recovered to the card as the live encryption certificate.
    - Encryption 2 (historic)
    - Encryption 1 (historic)
- Temporary Card D is canceled, as the original Card C has been found.
    - Authentication 4 – revoked.
    - Signing 4 – revoked.
- Card C now has the same certificates as previously – the suspended Authentication 3 and Signing 3 certificates are now active again.
    - Authentication 3
    - Signing 3
    - Encryption 3
    - Encryption 2 (historic)
    - Encryption 1 (historic)
- Card C stolen, and new Card E issued.
    - Authentication 5
    - Signing 5
    - Encryption 4

- Encryption 3 (historic)
- Encryption 2 (historic) – only two historic certificates are allowed, so the two most recent are recovered.

6.6.2 Example smart card history for a non-PIV system

There are some differences in behavior between PIV systems and non-PIV systems. For example, the Damaged and Permanently Blocked statuses have different behavior for recovering archived certificates.

In the example above, when Card B is damaged, instead of issuing a new Encryption 3 certificate, on a non-PIV system, MyID recovers Encryption 2 and uses that as the live encryption certificate:

PIV	Non-PIV
Authentication 3	Authentication 3
Signing 3	Signing 3
Encryption 3 (issue new)	Encryption 2 (recover)
Encryption 2 (historic)	Encryption 1 (historic)
Encryption 1 (historic)	

6.6.3 Example smart card history for a shared certificate

In some circumstances, an archived certificate may be stored on more than one credential – for example, on a smart card and on a mobile phone.

If you request a replacement for one credential using the **Compromised – Reissue Shared Certificates** reason, MyID generates an update job for all of your credentials that share the certificate so that they can be updated with the new certificate.

For example:

- The smart card credential profile is set up with the following certificate profiles:
  - Authentication – set to **Issue New**.
  - Signing – set to **Issue New**.
  - Encryption (archived) – this certificate profile is set to **Use Existing**, and has a maximum number of historic certificates of 0.
- The mobile credential profile is set up with the following certificate profiles:
  - Authentication – set to **Issue New**.
  - Signing – set to **Issue New**.
  - Encryption (archived) – this certificate profile is set to **Use Existing**, and has a maximum number of historic certificates of 0.
- Card A is issued with the following certificates:
  - Authentication 1
  - Signing 1
  - Encryption 1

- Mobile X is issued with the following certificates:
  - Authentication 2
  - Signing 2
  - Encryption 1 (the existing certificate is recovered onto the mobile device)
- Card A is compromised, and a replacement is requested with **Compromised – Reissue Shared Certificates** reason. Card B is issued with:
  - Authentication 3
  - Signing 3
  - Encryption 2
- When the replacement is requested, an update job is created for Mobile X, which is updated to have the following certificates:
  - Authentication 2
  - Signing 2
  - Encryption 2 (recovered)

Note: The update job for Mobile X and the card replacement job for Card B are created at the same time; if you collect the update for the Mobile first, Encryption 2 is created as a new certificate for the mobile, and Card B recovers the archived Encryption 2. The same certificates end up on the same credentials – it is purely a matter of which credential gets the original and which gets the copy.

7 Working with images

This chapter describes working with images when using MyID Desktop. For information on capturing images in the MyID Operator Client, see the *Configuring image capture* section in the ***MyID Operator Client*** guide.

Note: Associating images with people's records is optional. If you are not capturing images, you can skip this section.

MyID Desktop allows images to be captured either using a web camera or a scanner. You can also associate image files with a person's record. You can do this either when you add a person to the MyID database or when you update a person's record.

By default, images are stored as binary objects in the database. If you have upgraded from an older system, MyID may contain pre-upgrade images on the web server however, all new images will be stored in the database. For more information, contact customer support, quoting reference SUP-218.

If you are storing images on the web server, you must specify the folder to use.

You can set up MyID to store the binary objects in a separate database from the main MyID database; see the *Creating a separate database to store images* section in the ***Advanced Configuration Guide*** for details of setting up an archive database for these purposes.

Note: Before you make any attempt to scan images, make sure you have installed the correct scanner drivers for your scanner, and that Windows can detect the scanner correctly.

7.1 Changing settings for image capture

To change the settings for **Image Capture**:

1. From the **Configuration** category, select **Operation Settings**.
2. Click the **Video** tab. The **Video** page is displayed.

   A full list of the options available on this page is in the *Video page (Operation Settings)* section of the ***Administration Guide***.

7.1.1 General settings

The following options apply whether you are storing images in the database or in a folder on the web server.

- **Image Capture** must be selected to enable image capture within MyID.
- If you want to capture images using a web cam, select **Video Capture** to enable it.
- The **JPEG Compression Ratio** specifies the compression factor to be applied to an image. The lower the number, the greater the compression. The default is `90`.
- If **Maintain Aspect Ratio** is selected and an image is resized automatically, the height:width ratio is unaffected.
- The **Maximum Image Height** refers to the height of the image in the **Image Capture** control and is specified in pixels.
- The **Maximum Image Width** refers to the width of the image in the **Image Capture** control and is specified in pixels.

7.2 Storing images on the web server

Note: By default, MyID will store new images in the database rather than on the web server. If you need to switch your system over to storing images on the web server, contact customer support, quoting reference SUP-218.

Switching your system to store captured images on the web server affects only images captured using the Image Capture window in MyID Desktop; it does not affect images captured for facial biometrics using Aware PreFace or images imported through the Lifecycle API.

Important: Do not switch your system to storing images on the web server if you are using the MyID Operator Client to capture images. The MyID Operator Client will experience errors if you attempt to capture images when your system is configured to store images on the web server.

If your system has any images on the web server (for example, if you have an upgraded system, where previously-captured images are on the web server while new images are stored in the database), you must configure the rest.core web service with the image location, or the MyID Operator Client will be unable to display the images; see the *Displaying images stored on the web server* section in the ***MyID Operator Client*** guide for details.

The following settings are applicable only if you are capturing images and storing them on the web server.

- Set **Validate Image Size** if you want image capture to validate the size and type of the image. This makes sure that the images uploaded conform to the **Maximum Image Height** and **Maximum Image Width** settings.
- If the web services server is not the same server as the web server, you must set the **Image Upload Server** configuration option. See the *Setting the location of the web server* section in the ***Web Service Architecture*** guide.

  You must have the following DLL registered on the image upload server:

  `FileTransfer.dll`

  You can find this DLL in the `Components\Core` folder in your MyID installation.
- The **File Store Location** is the physical location used to store uploaded images. This folder is mapped to the `Upimages` virtual directory in MyID.

  Note: The named MyID COM and MyID web service users must have write permission to this folder.

  By default, MyID uses the `\Web\WebPIV\upimages` folder on the web server.

  If you change this setting you must change the virtual directory in IIS. See section *7.2.3*, *Changing the upload images virtual directory* for details.
- **Maximum Number Of Sub-Folders** specifies the maximum number of folders that will be created within the location specified in **File Store Location**. The default is `0`.
- **Preload Images** allows an existing image to be associated with a cardholder. Set this to:
  - **Yes** to automatically associate an image in the image store with the cardholder. The filename of the image must match the cardholder's logon name. For example, if the cardholder's logon name is `Jane Smith`, the filename may be `Jane Smith.jpg`.

- **No** (the default) ignores any existing images.
- **Ask** – if an operator saves a record without capturing an image and MyID finds one with the appropriate filename, the operator is asked if the image is to be used.

7.2.1 Using sub-folders

If you have a large number of images in your uploaded images folder (by default, `\Web\WebPIV\upimages`) you may find that this decreases performance when uploading and retrieving images. To remedy this, you can set MyID to create a number of subfolders within the uploaded images folder; new uploaded images will be uploaded to one of the subfolders, ensuring that no single folder contains too many images.

To set the number of subfolders:

1. From the **Configuration** category, select **Operation Settings**.
2. Click the **Video** tab.
3. Set the **Maximum Number Of Sub-Folders** option to the number of folders you want to use.

   For example, type `50`.

   The default is `0`, and the maximum is `1000`.
4. Click **Save changes**.

Once MyID has refreshed its configuration options (you may have to log out and log back in again) newly-uploaded images will be allocated to subfolders with names in the format `z000` to `z999`.

MyID handles all the relative paths to the images automatically.

7.2.2 Port settings

Image upload uses the same protocol (HTTP or HTTPS) as you use to access the MyID website. If you have changed the default port used when you access MyID, you can set the HTTP or HTTPS port for uploading images:

- **HTTP Port for image upload** – default `80`. Change this if you want to use image upload over HTTP with a different port number.
- **HTTPS Port for image upload** – default `443`. Change this if you want to use image upload over HTTPS with a different port number.

7.2.3 Changing the upload images virtual directory

If you are storing images in the file system and not in the database, you can change the value of the **File Store Location**. To do this:

- Map the `upimages` virtual directory to the new location.
- Copy any existing images from the original to the new location.
- Set the correct IIS execute permissions.

Use the Internet Information Services Manager to map the `upimages` virtual directory to the new location.

1. From the Control Panel, select **Administrator Tools**, then **Internet Information Services (IIS) Manager**.

   Note: These instructions assume you are using IIS 10. If you are using a different version of IIS, see your Microsoft documentation for information on how to carry out these changes.

2. Expand **Sites** then **Default Web Site**.
3. Map the `upimages` virtual directory at this level to the **File Store Location**.
   a. Select the `upimages` virtual directory.
   b. In the Actions pane, click **Basic Settings**.
   c. Click the browse button next to the **Physical path** box and navigate to the **File Store Location** you specified in **Operation Settings**.
   d. Click **OK**.
4. Make the same change to the `upimages` virtual directory in each of the language folders.

   For example, make the same change to the following virtual directories:

   - **Default Web Site > MyID > en > upimages**
   - **Default Web Site > MyID > us > upimages**

5. Restart IIS.
   a. Select the **Default Web Site**.
   b. In the Manage Website pane, click **Restart**.
   c. Copy any existing images to the new location.

Important: You must ensure that IIS execute permission is disabled on the `upimages` folder. If it is not already configured, you must create a file called `web.config` in the `upimages` folder, containing the following text:

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
    <system.webServer>
        <handlers accessPolicy="Read" />
        <directoryBrowse enabled="false" />
        <httpErrors>
            <clear />
        </httpErrors>
    </system.webServer>
</configuration>
```

7.3 Obtaining images

Your organization may have decided to include an image (a photograph, a signature or a scanned document) as part of a person's record. You may be able to obtain the image in a variety of ways, depending on how your system has been configured.

- Use an existing digital image, accessible from your local machine.
- Take a photograph using a webcam.
- Scan a photograph or another document.

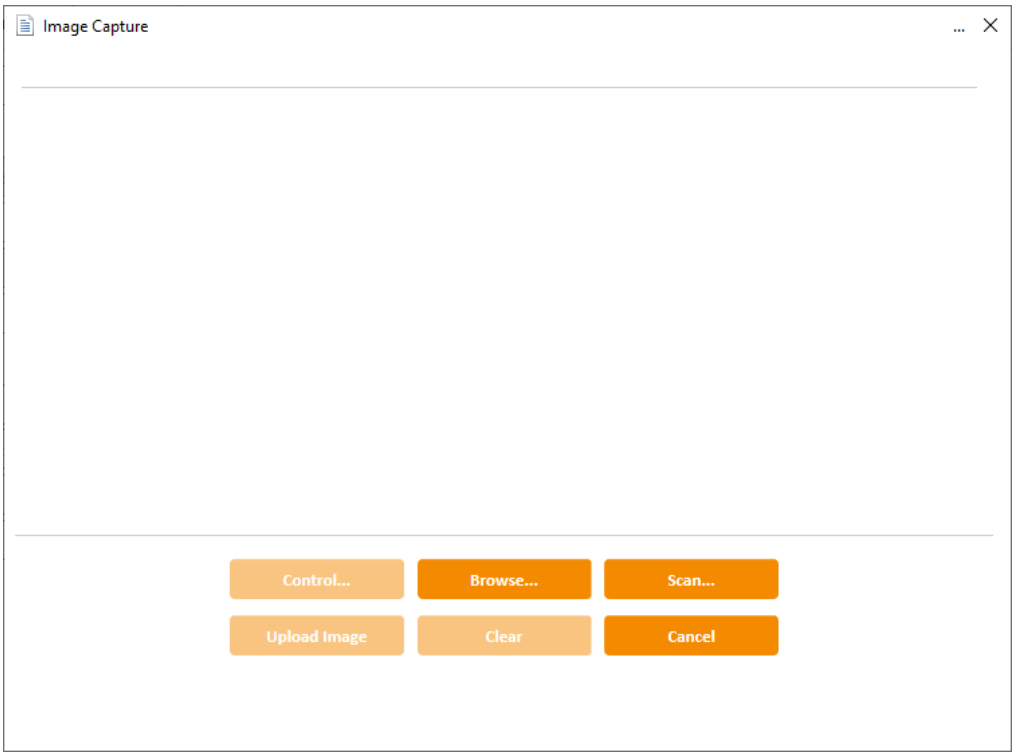
The option to obtain and modify an image is available as part of the **Add Person** and **Edit Person** workflows, in the **People** category. The option may also have been added to other workflows.

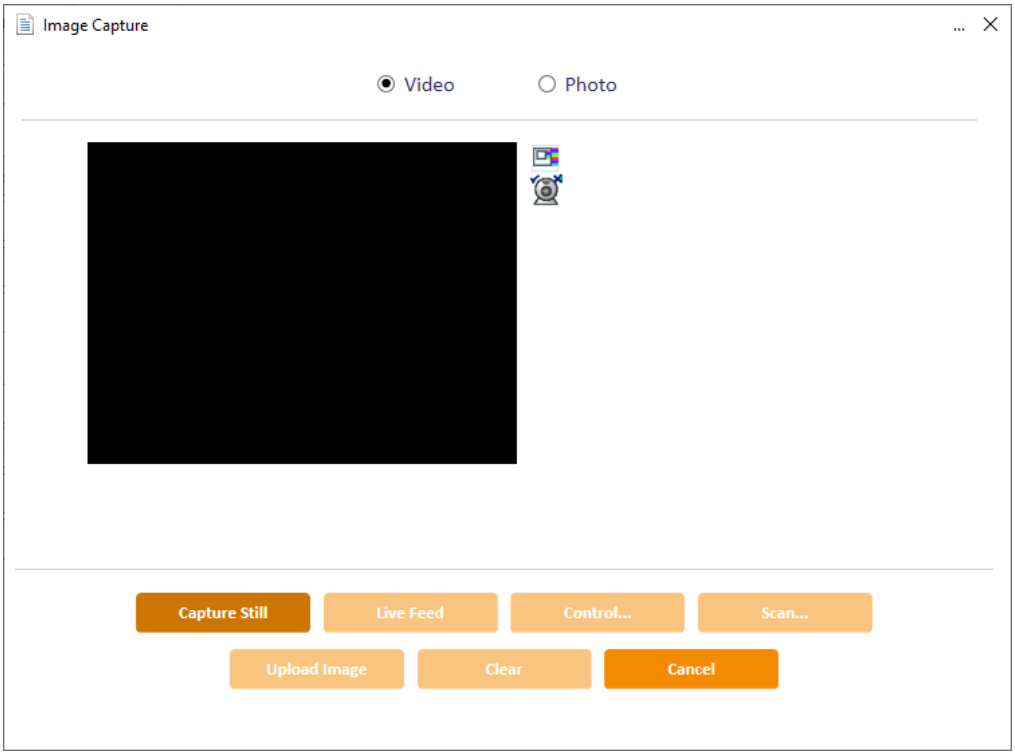
The use of webcams and scanners requires some changes to be made by an administrator.

To obtain (or change) an image, click either:

- The existing image (which may be a placeholder, as shown in the examples)
- The **Change Picture** button

The basic **Image Capture** window is displayed. Depending on the options available to you, the window looks similar these examples.





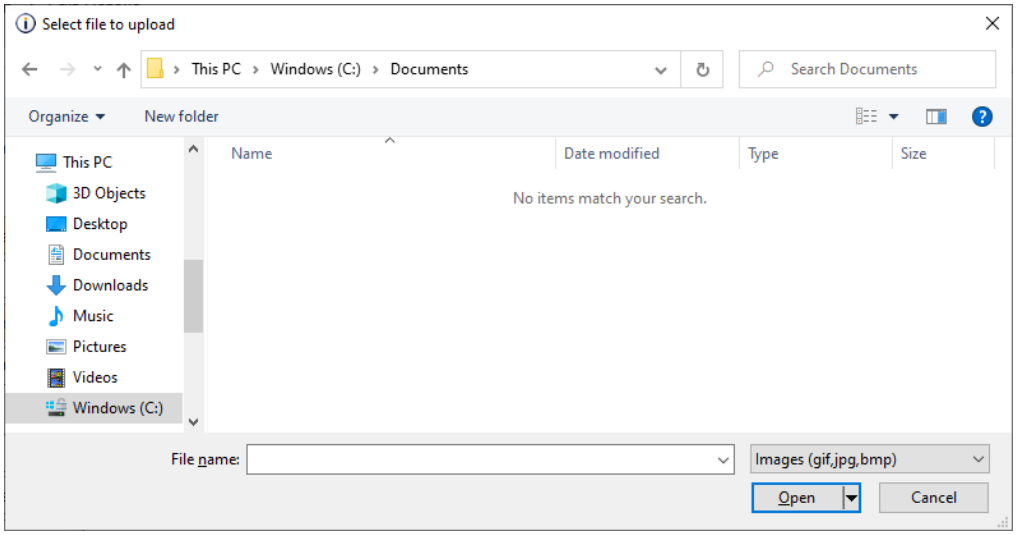
The **Video** option is available only when the **Video Capture** configuration option (on the **Video** page of the **Operation Settings** dialog) is enabled. In this case, you can switch between using a webcam (the **Video** option at the top of the window) and an existing image (the **Photo** option)

7.3.1 Using an existing image

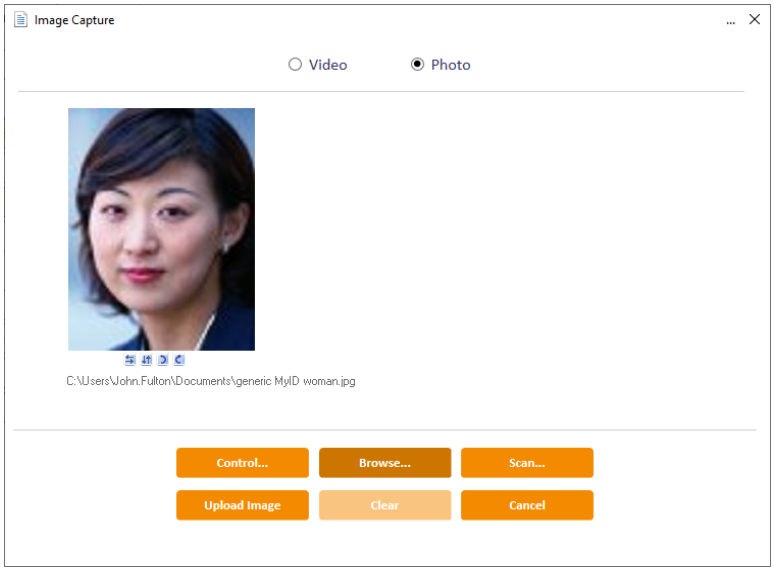
To use an existing digital image:

1. Click the **Photo** option to select it, if this is displayed.
2. Click the **Browse** button.

   A standard Windows browse dialog is displayed.
3. Navigate to the file you want to use, select it and click **Open**.



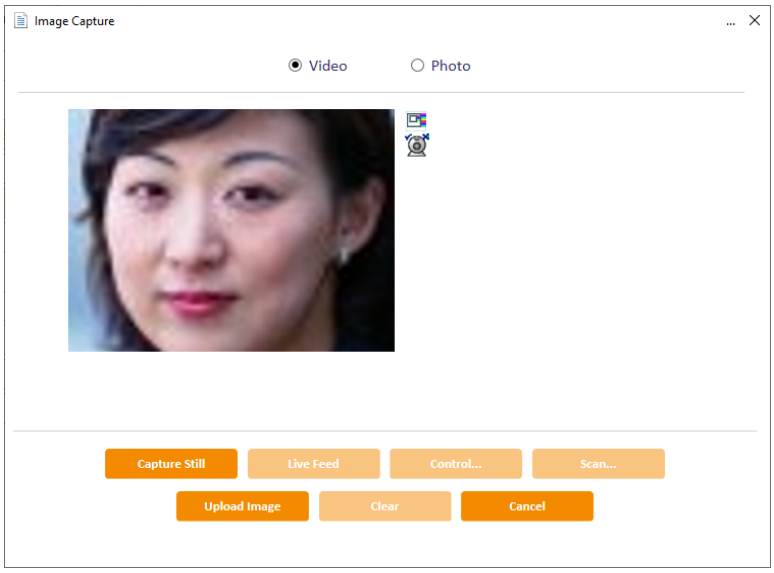
Your chosen image is now displayed in the "source" display area of the **Image Capture** window. The path to the file is displayed below the image.



7.3.2 Using a webcam to capture an image

To use a webcam to capture an image:

1. Click the **Video** option to select it. It may already be selected, as this is the default if a webcam is detected.
2. Set the options for your webcam:
   -  – set the video format for your webcam. The options available depend on the webcam you are using. Some webcams will not display resolutions or pixel depths that are too low.
   -  – set the camera settings, including brightness and contrast. The options available depend on the model of camera attached to your machine.
3. The current live feed (video) is displayed in the area to the left of the **Image Capture** window.



4. When the image you want is displayed, click **Capture Still** to freeze the frame.

   If you want to select a different image, click **Live Feed** to resume the video.

7.3.3 Using a scanner to capture an image

Note: Your system must also be set up to allow scanning; this may require extra customization. Contact customer support for details.

Make sure that the following option on the **Video** tab of the **Operation Settings** workflow are set:

- **Video Capture** option is set to `No`.

To use a scanner to capture an image:

1. Click the **Scan** button.

   This opens a connection to your scanner and may display some options that allow you to choose the area you want to scan and to specify the resolution you want to use. The options available to you depend the model of scanner you are using.

When you have chosen the most appropriate options, start the scan process.

2. The document (or portion of document) you have scanned is displayed in the left of the **Image Capture** window.

Note: MyID may have been set up to capture information from pre-printed paper forms, which may have been completed by hand. If the zones to be scanned have been set by your administrator, it is important to make sure that you place the paper form with the top-left corner of the form at the top-right corner of the scan bed.

7.4 Rotating and flipping images

Four small buttons are available under the "source" image. You can use them if, for example, you have placed a photograph upside down in a scanner.

 Flips the image around a vertical axis, from left to right.

 Flips the image around a horizontal axis, from top to bottom.

 Rotates the image 90° anti-clockwise.

 Rotates the image 90° clockwise

7.5 Selecting part of an image

You may want to select part of an image, possibly to remove excess background or to extract the head and shoulders section of a larger photograph.

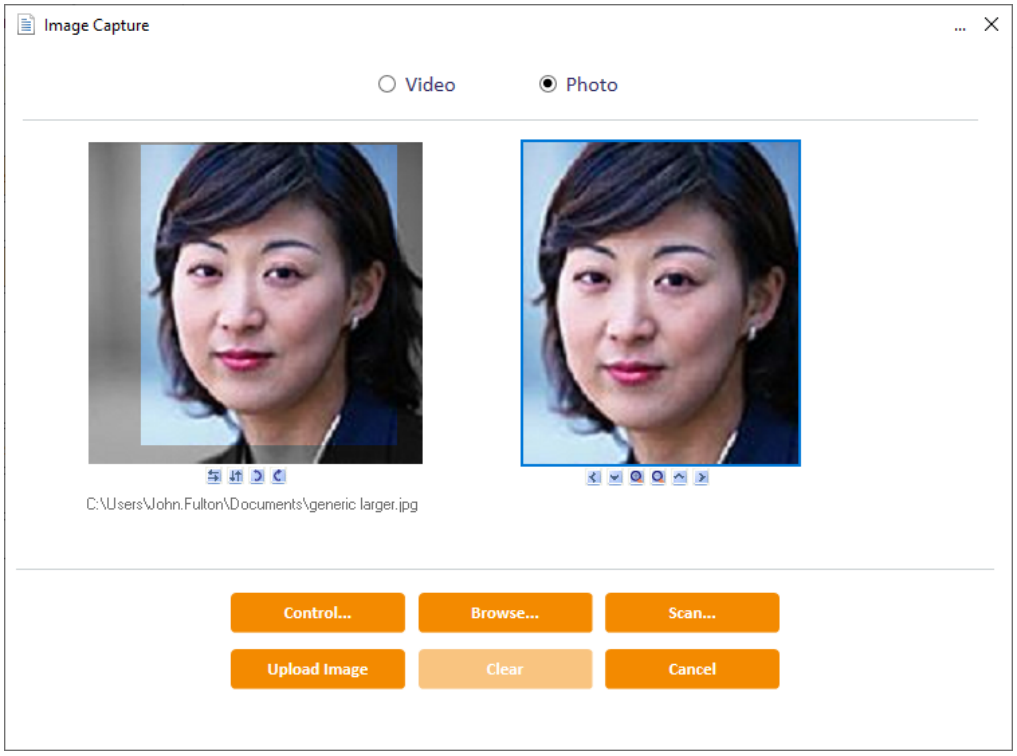
MyID may have been set up to capture images using a scanner from pre-printed paper forms, which may have been completed by hand. For example, you may be able to extract a photograph, an applicant's signature and an authorization signature from a form. In this case, you may find that more than one area of the form is scanned and you have a corresponding preview of each zone's contents. Each preview area is associated with its own set of controls.

Note: If a preview is displayed for a signature, MyID has attempted to automatically select the appropriate area. Click the preview to see the selected area in context and to adjust it using the "move" cursor (a 4-headed arrow). Changes to the selected area can also be made following the instructions in this section.

To select part of an image:

1. Place your mouse cursor over the source image – the pointer changes to an arrow. Position the arrow at a corner of the area you want to select.
2. Hold down the left mouse button and drag your mouse to the diagonally opposite corner of the area you want. A dashed line shows the outline of the area you are selecting. Release the mouse button to complete the selection.

   All areas of the source image outside of your selected area are dimmed, leaving your selection in the original colors. Your selection is also displayed in the area to the right of the source image – this is a preview of the image that will be uploaded to MyID.



3. To change your selection, you can either:
   - Click anywhere on the source image outside of your selected area. This clears the selection and you can repeat the previous steps to choose a new area.
   - Use the six buttons displayed under the preview image that enable you to reposition your selection. Choose this method of changing your selection if you only need to make relatively minor changes, as each change is small.

     The two buttons on the left and the two on the right move your selected area in the direction indicated by the arrow:

      Move your selection left.

      Move your selection right.

      Move your selection down.

      Move your selection up.

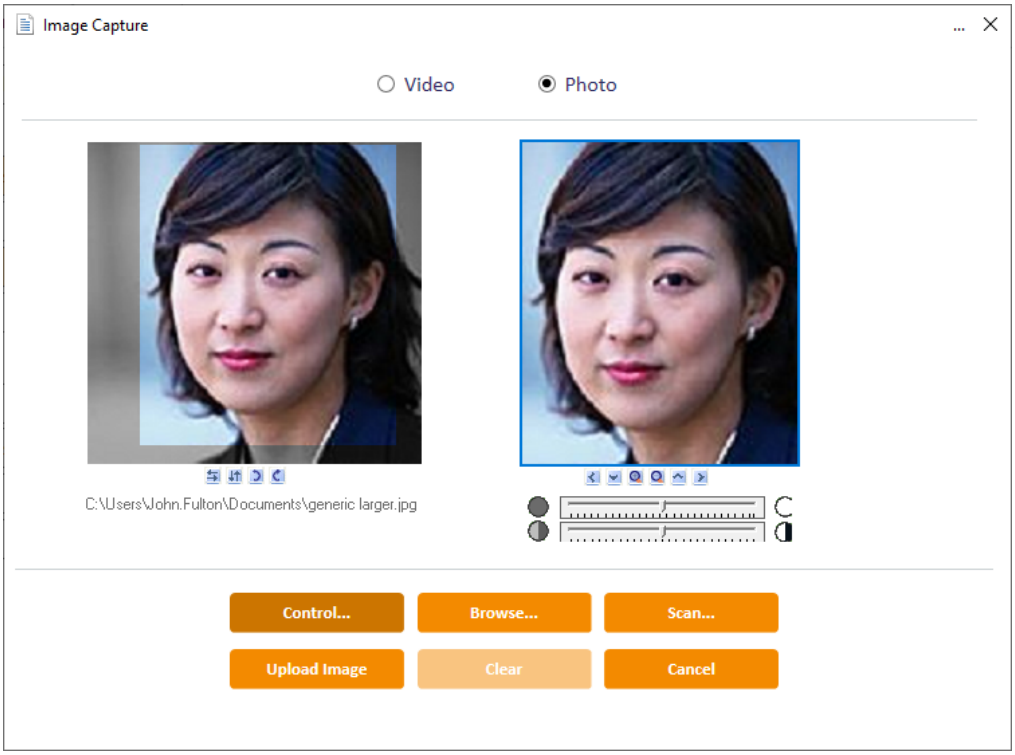
     The two buttons in the middle:

      Decrease the area of your original selection (zoom in).

      Extend your selection to include more of the original image (zoom out)

7.6 Enhancing images

You can improve the appearance of your selection by changing the contrast or brightness of the picture.



Note: The changes you make only affect your selection – the original image is not changed.

Click **Control** to display two sliding controls beneath the preview picture:

Move the slider to the right to lighten the image and to the left to darken it.

Move the slider to the right to increase the contrast in the image and to the left to decrease it.

7.7 Uploading images to MyID

When you are happy with the preview of the image, click **Upload Image** to transfer the image to MyID. The image is associated with the record that you created it in and can be viewed as part of that record.

If you want to alter an image after it has been uploaded to MyID, you must start the process again. You can replace an image associated with a record but cannot make changes to an existing image.

8 Working with reports

You can use the **MI Reports** workflow to run Management Information (MI) reports.

The reports available depend on the type of MyID system you are running. It is also possible to create and customize reports; contact customer support quoting reference SUP-329 for details.

Note: If the criteria for the report contain the group, you can select groups only from within your scope (including administrative groups), and the results contain only details for users within your scope. If the report does not contain the group as part of the criteria or search results, there is no scope checking applied to the report, and all results are returned.

The following reports are available by default:

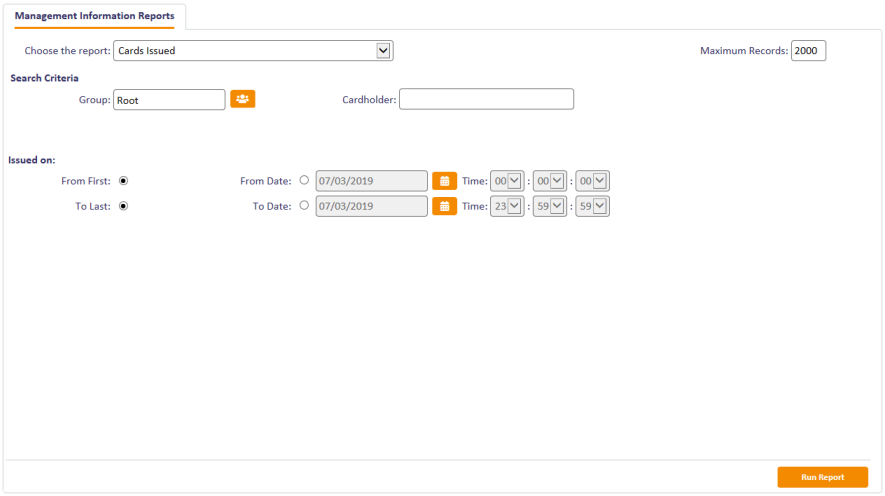
- **Cards Issued** – a list of all cards issued. Scoped.
- **Cards Expiring** – a list of cards expiring within a date range. Scoped.
- **Cards Revoked** – a list of cards that have been revoked, but remain assigned to a user. Scoped.
- **Cards Not Issued** – a list of cards in the database that have not been issued.
- **Card Cancellations** – a list of card cancellations.
- **People by group and affiliation** – a list of people including groups and affiliation. Scoped.
- **Jobs** – a list of jobs. Scoped.
- **All People** – a list of people. Scoped.
- **Audited Operations** – a list of audited operations.
- **Certificate Operations** – a list of certificate requests and revocations.
- **Credentials By Type** – a list of each type of credential issued, along with a report on the number of credentials issued for each type.
- **Certificates** – a list of the certificates in the system. Scoped.
- **SCEP Requests** – a list of all the SCEP requests for device identities.
- **Device Keys** – lists all issued devices that are not expired and that use GlobalPlatform or PIV 9B keys.

8.1 Running MI reports

To run a management information report:

1. From the **Reports** category, select **MI Reports**.

   You can also launch this workflow from the **Additional Reporting** section of the **More** category in the MyID Operator Client. See the *Using Additional Reporting workflows* section in the ***MyID Operator Client*** guide for details.



Note: Make sure that you can view the **MI Reports** workflow. Use the **Edit Roles** workflow in the **Configuration** category to add the workflow to the roles you want to be able to run the reports.

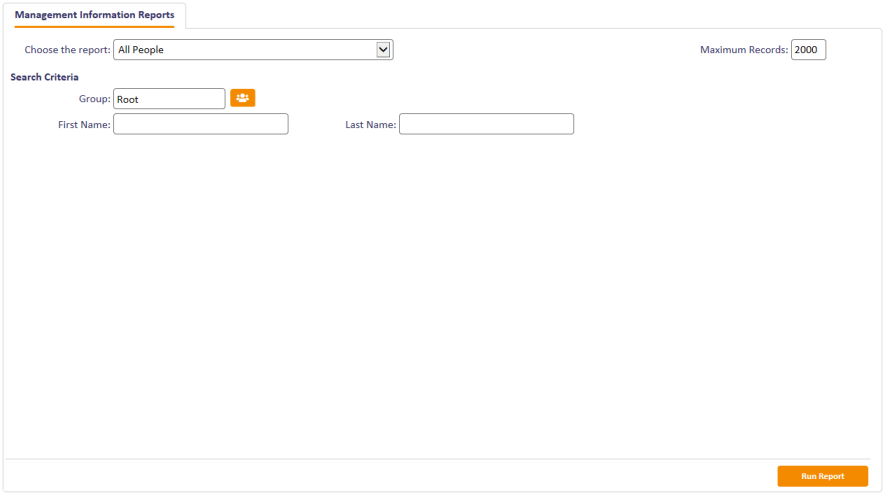
2. From the **Choose the report** drop-down list, select the report you want to run.

   The search criteria change according to the report you choose.

3. If you want to display a limited number of records, type a number in the **Maximum Records** box.

4. Complete the search criteria.

   For example, for the **All People** report, you can set the following search criteria:



   - **First Name** and **Last Name** – type the name of the person. You can use * as a wildcard; for example, `Ja*` finds people with the name Jack, Jason and Janet.
   - **Group** – select the users' group from the drop-down list.

5. Click **Run Report**.

The results of the report appear.

First Name	Last Name	Logon ID	Group	email
		(Devices)	(Devices)	
Arthur	Alpha	00001	Human Resources	PIVALLBio@myid.com
Chesney	Charlie	00003	Human Resources	PIVALLBio@myid.com
Eddie	Echo	00005	Human Resources	PIVALLBio@myid.com
Sam	Smith	1001	Human Resources	sam.smith@myid.com
Admin	User	Admin User	Department of Education	admin.user@domain19.local
Alise	Rice	Alise Rice	Department of Education	Alise.Rice@domain25.local
Avis	Lipps	Avis Lipps	Department of Education	Avis.Lipps@domain25.local
Ćhŗíš亻 ïåņ	ʺEяĭķᏕƐれ	Ćhŗíš亻 ïåņ ʺEяĭķᏕƐれ	Department of Treasury	intercede.test8@gmail.com
Grace	Drever	Grace Drever	Department of Education	Grace.Drever@domain25.local
Mac	Batt	Mac Batt	Department of Education	Mac.Batt@domain19.local
mobile	user	mobile	System Startup	
Sec	Officer	Sec Officer	Finance	sec.officer@domain19.local
Shay	Scott	Shay Scott	Department of Treasury	Alena.Castle@diym.uk
Signatory	Signatory	Signatory	Finance	signatory@domain19.local
startup	user	startup	System Startup	

6. To print the report, click the print button.
7. To save the report, select **XML**, **CSV**, or **Excel** to select the format, then click the save button.

   Note: To allow you to save reports to Excel, make sure you have the **Initialize and script ActiveX controls not marked as safe for scripting** option set for the MyID website in Internet Options. For more information about configuring Internet Options, see the *Configuring Internet Options* section in the ***Installation and Configuration Guide***.

8.1.1 Known issues

- **IKB-342 – Problem with reports returning no data**

  When a report returns no data, any subsequent searches that do return results do not show the results table.

  To work around this issue, restart the **MI Reports** workflow and rerun the report.

Index