MyID
Version 10.8 Update 2

Administration Guide

Copyright

© 2001-2018 Intercede Limited. All rights reserved.

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

The software or web site referred to in this manual may utilize or contain material that is © 1994-2000 DUNDAS SOFTWARE LTD., all rights reserved.

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

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

Licenses and Trademarks

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

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

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:
  - "Enter a valid email address in **'From' email address**"
  - "Select **Save** from the **File** menu"

- *Italic* is used for emphasis and to indicate references to other sections within the current document:

  For example:
  - "Copy the file *before* starting the installation"
  - "See *Issuing a Card* for further information"

- ***Bold and italic*** 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 installation CD.

- 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 occurs only 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.

Non-technical staff can use MyID to issue and manage credentials but an administrator must first configure the options that they can select.

MyID has a web-based interface that is used to:

- Enter information about individuals, either directly into the MyID database or by importing from an LDAP directory.

- Request, issue, update or cancel credentials containing appropriate pre-defined information. The details to be included when credentials are issued or updated are stored in profiles, created by an administrator.

- Respond to requests for assistance from the holders of credentials.

For an overview of the interface and the controls it contains, see section *1.4*, *The interface*.

1.1 Change history

Version	Description
ADM1744-01	First version provided with MyID 10.0.
ADM1744-02	Updates to wording and formatting.
ADM1744-03	Updated for MyID 10.1.
ADM1744-04	Updates to wording and formatting.
ADM1744-05	Updated for MyID 10.2.
ADM1744-06	Updated for MyID 10.3.
ADM1744-07	Updated for MyID 10.3 Update 1.
ADM1744-08	Updated for MyID 10.4.
ADM1744-09	Updated for MyID 10.5.
ADM1744-10	Updates to wording and formatting.
ADM1744-11	Updated for MyID 10.6.
ADM1744-12	Updated for MyID 10.6 Update 1.
ADM1744-13	Updated for MyID 10.7.
ADM1744-14	Updated for MyID 10.7 Update 1.
ADM1744-15	Updated for MyID 10.8.
ADM1744-16	Updated for MyID 10.8 Update 1.
ADM1744-17	Updated for MyID 10.8 Update 2.

1.1 Who should read this guide?

This guide is intended for anyone who is responsible for configuring or administering MyID. It describes each of the configuration options in detail.

You may also choose to read this document if you are:

- Investigating the use of MyID in your organization.

- Designing the deployment strategy for your organization.

1.1.1 What do you need to know?

This document assumes:

- If you are responsible for configuring MyID using the interface, you have a basic level of understanding of a web-based interface. For example, you understand the concepts of a hyperlink or a form and basic terminology such as labels, checkboxes and radio buttons.

- If you are responsible for installing MyID or making changes to the operating system, including installing and registering DLLs, you have a good understanding of Windows terminology and concepts. For example, you understand the concepts of file permissions, specifying an account under which a service is to run or taking a backup of files.

- If you are responsible for directly accessing the MyID database, running scripts and backing up or archiving data, you have a basic knowledge of SQL databases. For example, you understand the concepts of tables and relationships, terminology such as permissions and queries, and tools such as the Query Analyzer.

1.2 What is included in this guide?

This document describes all of the general configuration options available to MyID. It explains the relationships between them and indicates an efficient order for completing them.

This document also provides a basic introduction to using MyID.

Different people interact with MyID at different levels, and to differentiate between them the following conventions have been adopted in this guide:

- An *administrator* is a person responsible for configuring MyID. A higher level of access is granted to administrators, who see pages that other users do not.

- An *operator* is an individual who uses MyID on a regular basis. The types of task carried out by operators include adding people to the MyID database and editing their details; requesting, issuing and printing credentials; unlocking cards.

- A *manager* is responsible for a group of individuals. Managers can request credentials for the individuals who report to them, cancel credentials and request changes.

- An ordinary *holder* has minimal access to MyID. Holders can usually collect credentials that have been prepared for them and change their own security phrases and PINs. Everyone who is issued with credentials MyID has at least this level of access.

Each chapter includes an overview and explains how the options available to you differ depending on the deployment decisions your organization has made. It does *not* discuss the merits of the different deployment strategies that are available and does *not* provide installation instructions (these are provided in the *Installation and Configuration Guide*).

MyID is highly configurable. This means that your organization may have modified some aspects of the system to correspond more closely to your internal processes. The changes that can be made include:

- Changing the appearance of MyID, including colors and the basic layout of the screens

- Renaming workflows and stages within workflows (see section *1.4*, *The interface*, for an explanation of these elements)

- Changing the text displayed on the web pages

- Creating new workflows and adding stages or pages to existing ones

- Changing the access given to each of the roles specified above, and creating new roles to meet requirements.

This means that the information provided in the document may not correspond exactly to the screens you see when using MyID.

1.2.1 Where to find more information

Read the *Release Notes* for the current release of the software. This provides the latest information on the release, as well as where to get further information.

You must read the appropriate *Integration Guides* for any third-party products that you intend to use with MyID as they may contain details relevant to those products.

If you have not yet installed MyID, you must read the *Installation and Configuration Guide* before installing the software.

Documentation issued with software updates may contain information about new features that have been added or correct any errors that have been identified in the main product documentation.

1.3 Applying updates

Instructions for applying updates (patches and hotfixes) are provided with the individual update – see the documentation that comes with the update.

Note: If the update requires a change to the client components, you must uninstall these using the Windows Add or Remove Programs utility before installing the updated components, as described in section *2.1*, *Connecting a workstation*.

1.4 The interface

Note: A detailed explanation of the terminology used within MyID and this document is provided in section *1.5*, *Terminology*.

When you first log on to MyID, the system will look similar to the following:
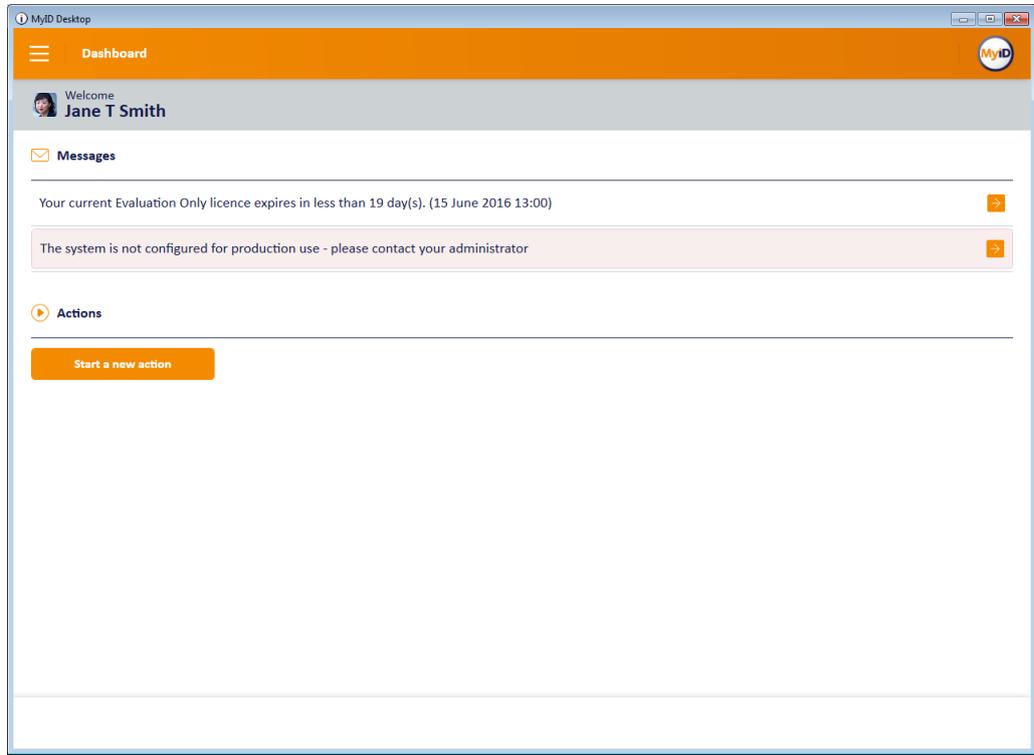
If there are any system messages, they appear at the top of the screen. For some messages, you can click the arrow [→] to take you to the appropriate workflow; for example, if your system is not set up for production use, clicking the arrow takes you to the **Security Settings** workflow to allow you 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**.
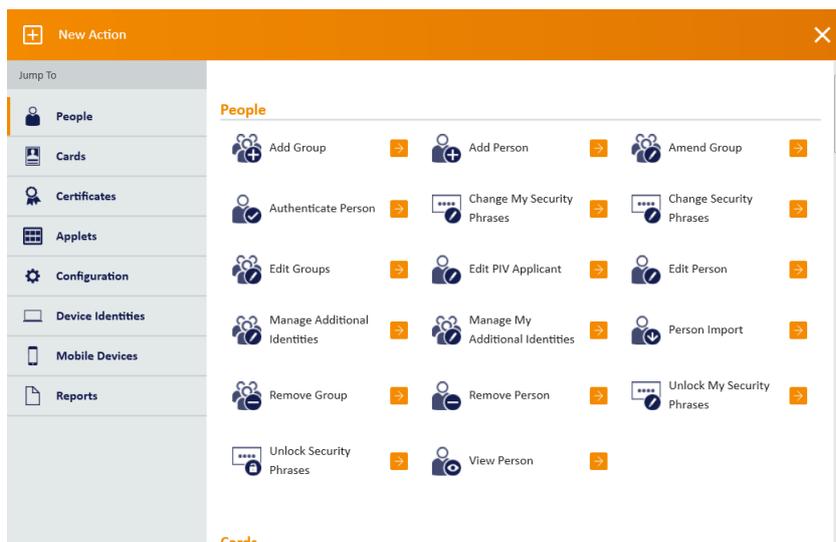
The list of categories and workflows will be tailored for you according to your role and the configuration of your system; fewer categories and options within these categories are shown if you have a lower level of access, or if fewer options have been installed.

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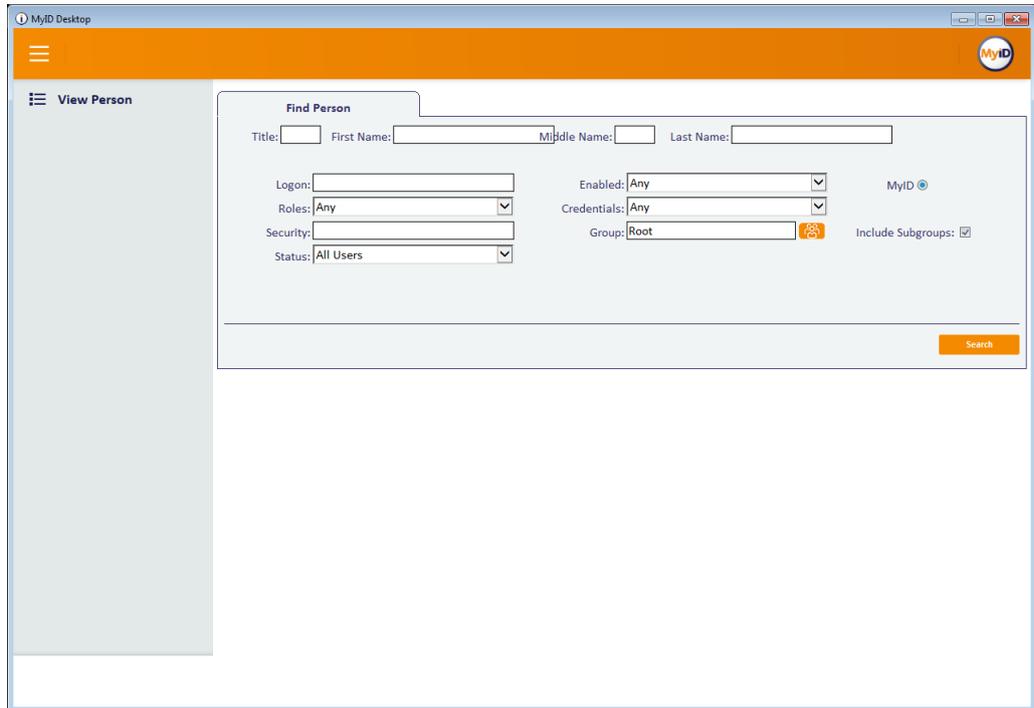
A form is displayed for each stage. Some forms, such as the **Person Details** form, consist of a number of named tabs.

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:

K	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.	Rows: Auto ▾	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.
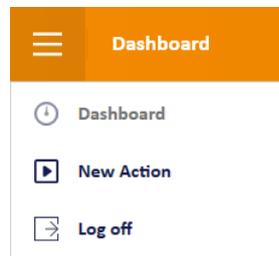
You can return to the dashboard when you are in a workflow, and you can start a new action when you are on the dashboard.

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; for example, if you attempted to change a PIN to the same as the original PIN before correctly changing it to a new PIN.
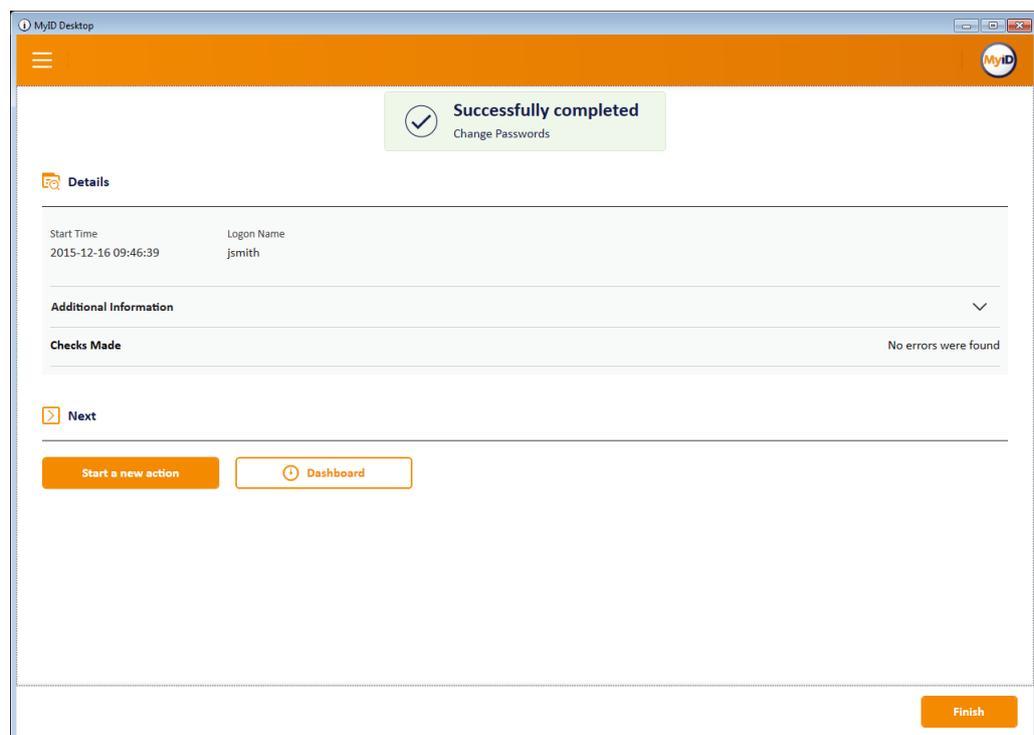
As you work with MyID, your most recent workflows will appear on your dashboard:
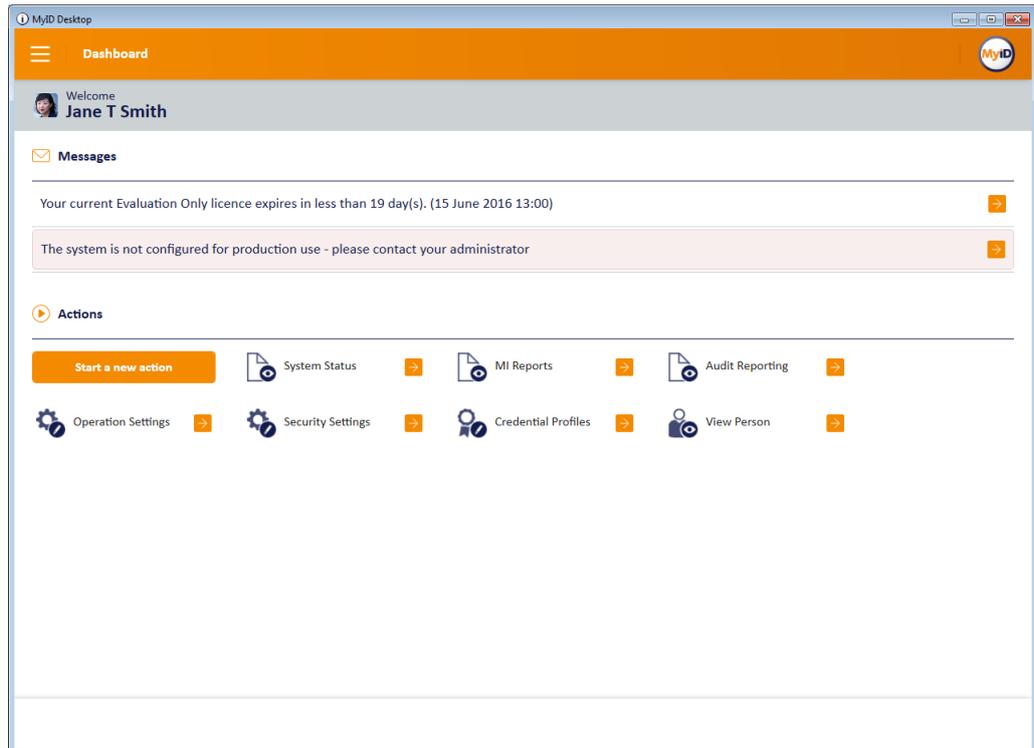
1.4.1 Selecting dates

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:

Click the appropriate day to select that day
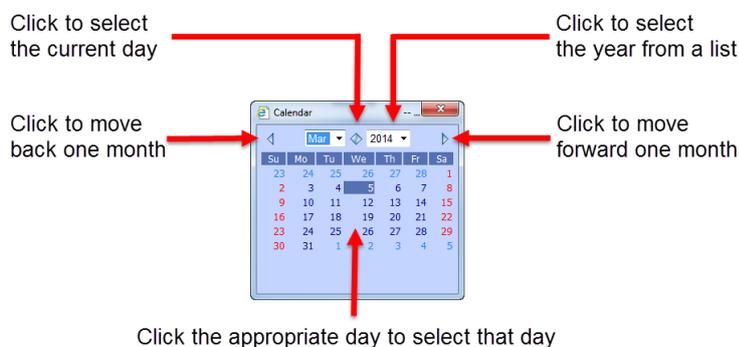
1.4.2 Entering search criteria

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`
- `company`
- `com`

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`

1.4.3 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**.

1.5 Terminology

The MyID documentation set uses the following terminology:

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	See *holder*.
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.
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.
holder	A person who has been issued a *card* or other *credentials*.
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*.
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.

2 Logging On for the First Time

Towards the end of the installation process, the person installing MyID is prompted to specify a passphrase for a user account that enables access to MyID.

The startup account is intended to give you enough time to configure the basic system and to arrange a permanent logon mechanism. It is good practice to create named accounts with appropriate roles as soon as possible and use those accounts to manage MyID. A number of options are available and your organization will have chosen the method most suited to its needs. See section 3, *Logon Mechanisms*, for brief explanations of the different methods and instructions for implementing them.

The *Installation and Configuration Guide* contains information on using GenMaster to set the passphrase for the startup user.

2.1 Connecting a workstation

See the *Installation and Configuration Guide* for details of installing and configuring MyID Desktop on your workstations.

2.2 Default security settings

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:
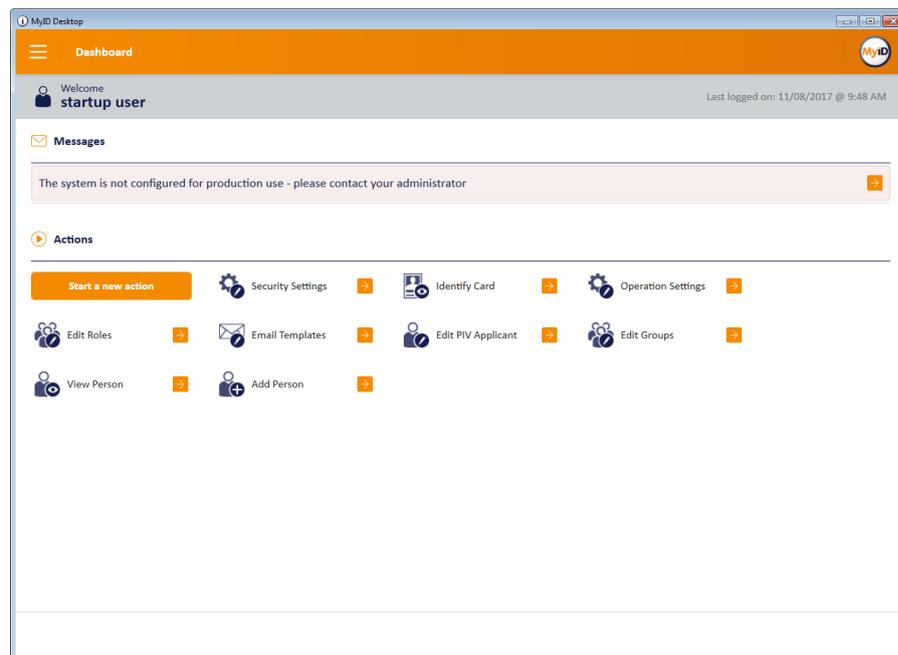
The message is:

```
The system is not configured for production use – please contact your
administrator.
```

If this warning appears, you must review the settings on the **Device Security** tab on the **Security Settings** workflow; see section *34.3*, *Device Security page (Security Settings)*.

The *System Security Checklist* document contains information about configuring SOPINs, GlobalPlatform keys, and PIV9B keys to ensure that your system is secure and configured for production use.

3 Logon Mechanisms

You can log on to MyID 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)

You can enable more than one method of accessing MyID. For example, you can select smart card as the logon method but enable logging on using security questions in case someone loses a card.
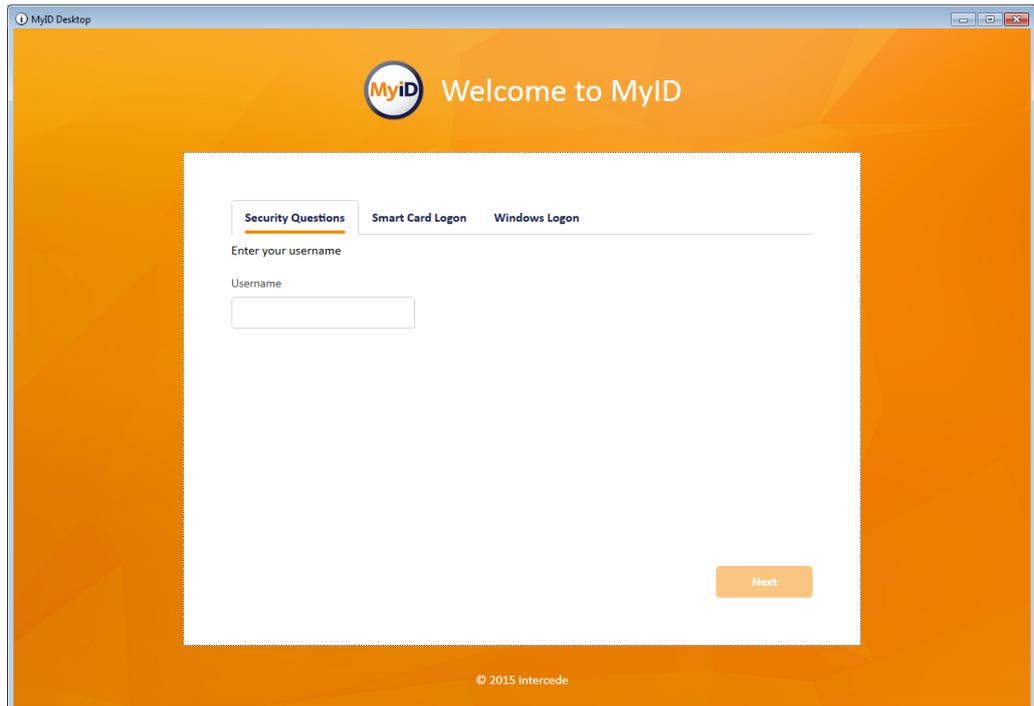
Click the tab for the logon method you want to use.

3.1 Authentication feedback

MyID incorporates features to limit the information being returned to clients before authentication; this provides additional security by preventing potential attackers from gleaning feedback from unsuccessful attempts.

The messages that appear when a user fails to log on do not provide the reason for the authentication failure, which would have allowed them to take corrective action; this may result in calls to your helpdesk from users unable to authenticate to the system. You can obtain details of the authentication failure from the **Audit Reporting** workflow. For some authentication operations, you may also want to check the information in the **System Events** workflow.

3.2 Using a card and PIN to log on to MyID

The usual way to log on to MyID is using a card (a smart card or a USB token). A PIN is issued to the holder of the card, and the card and PIN together authenticate the holder to MyID.

The requirements for the PIN are specified as part of the credential profile (see section *12*, *Managing Credential Profiles*) or by the token manufacturer. The actual value is set when the card or token is issued.

Note: To log on with a smart card and PIN, you do not need to make any changes to the default settings.

If you have previously changed the settings, you need to change them back:

1. From the **Configuration** category, select **Security Settings**.

2. On the **Logon Mechanisms** tab, make sure that **Smart Card Logon** is set to Yes.

3. Click **Save changes**.

4. In the **Edit Roles** workflow, make sure the user's role has the **Smart Card** logon mechanism assigned.

   See section *4.1.5*, *Assigning logon mechanisms* for details of using the **Edit Roles** workflow.

3.2.1 Smart card states

The color and icon used on the **Smart Card Logon** tab tell you the state of the card inserted in the card reader.

Valid card ready to be used for logon:
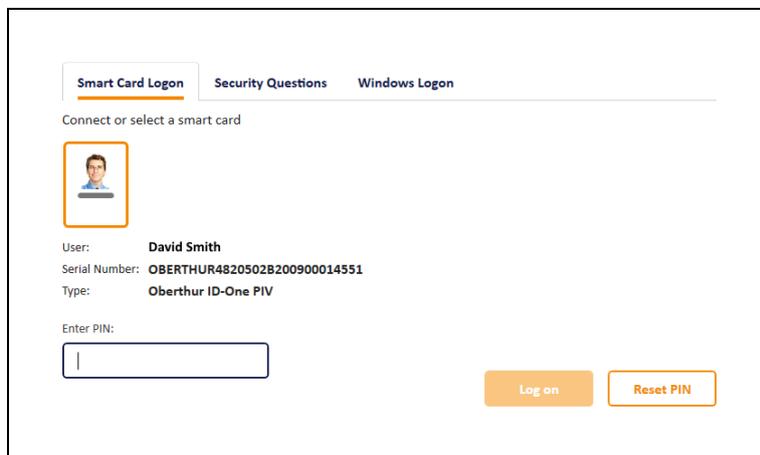
Locked card:
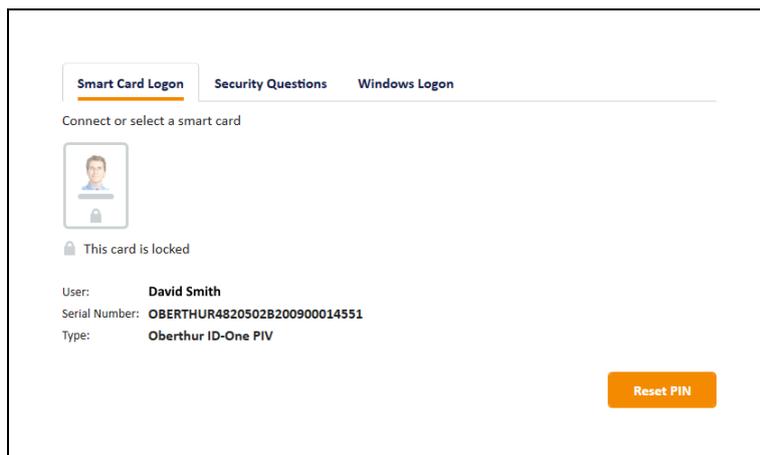
Card ready for activation:
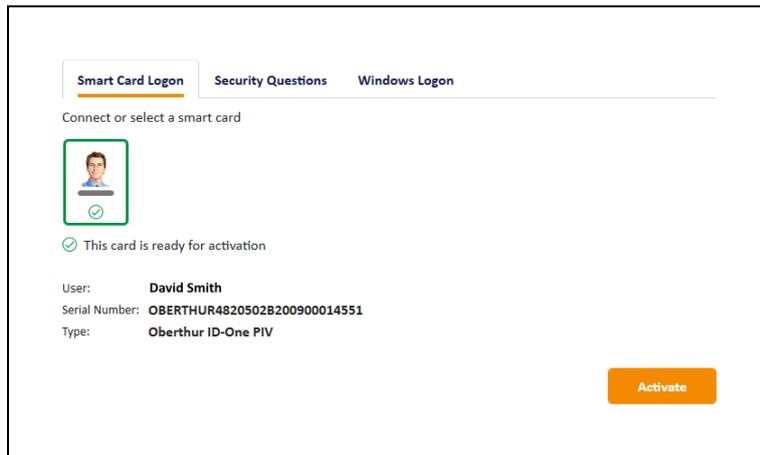
Invalid card:
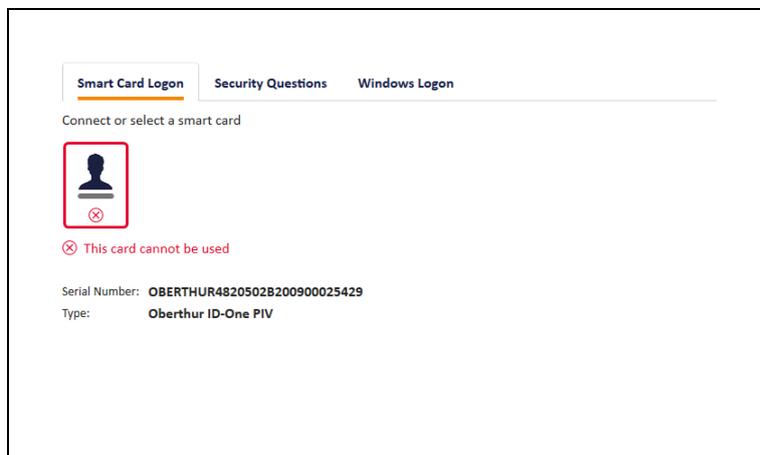
3.3 Using security questions to log on to MyID

You can log on to MyID using security questions, which grants limited access to the system.

If you want to allow the same security access with a security phrase as you would with a smart card and PIN, you must enable password logon for roles.

To allow password logon:

1. Select **Security Settings** from the **Configuration** category.

2. On the **Logon Mechanisms** tab, make sure that **Password Logon** is set to Yes.

3. Click **Save changes**.

4. In the **Edit Roles** workflow, make sure the user's role has the **Password** logon mechanism assigned.

    See section *4.1.5*, *Assigning logon mechanisms* for details of using the **Edit Roles** workflow.

5. Click **Save Changes**.

6. Set security phrases for the user using the **Change Security Phrases** workflow.

The user can now log on to MyID using the security phrase.

3.3.1 Setting rules for security phrases

Rules for security phrases can be specified by using a combination of configuration settings. See section *34.5*, *PINs page (Security Settings)*, for an explanation of the basic settings available:

- The maximum number of repeated characters in a security phrase
- The maximum number of sequential characters in a security phrase
- The minimum length of a security phrase
- The characters allowed in a security phrase
- Whether white space should be stripped from security phrases

The setting called **Security Phrase Complexity** enables you to configure additional rules for security phrases. By default, this complexity is not defined.

Note: Invalid rules are ignored, making it equivalent to having no rules. Invalid rules include:

- Not following the rule pattern.
- Setting the maximum length to 0.
- Including any characters not specified in the syntax.
- Setting the maximum to be less than the minimum.
- Not including *any* types of characters.

To set rules for security phrase complexity:

1. From the **Configuration** category, select **Security Settings** and then select the **PINs** tab.

2. Specify the complexity required for a security phrase using the following parameters in the following format:

   ```
   [mm-nn][u|U|][l|L][s|S][n|N]
   ```

   where:

`mm`	minimum length	If not specified, this defaults to 4
`nn`	maximum length	If not specified, this defaults to 8
`u`	may contain uppercase characters	*(If neither `u` nor `U` is present, the security phrase cannot contain uppercase characters)*
`U`	must contain uppercase characters	
`l`	may contain lowercase characters	*(If neither `l` nor `L` is present, the security phrase cannot contain lowercase characters)*
`L`	must contain lowercase characters	
`n`	may contain a number	*(If neither `n` nor `N` is present, the security phrase cannot contain numbers)*
`N`	must contain a number	
`s`	may contain a symbol	*Allowable symbols are:* `-!$%^&*()_+|~=\`{}[]:";'<>?,./@#\` *and* <space>
`S`	must contain a symbol	*(If neither `s` nor `S` is present, the security phrase cannot contain symbols)*

Note: You *must* include at least one type of allowable or mandatory character, or the rule will be invalid.

Examples:

`7-9ulns` – from seven to nine characters, may contain uppercase, lowercase, numbers or symbols:

```
12345678
abcdefgh
ABC123!?
```

`7-9ULNS` – from seven to nine characters, must contain uppercase, lowercase, numbers *and* symbols.

```
aBC123!?
123Abc#
```

`4-8ULns` – from four to eight characters, must contain uppercase and lowercase, and may also contain numbers or symbols.

```
ABCabc12
ABCabcAB
ABCabc1!
```

3. Click **Save changes**.

3.3.2 Setting the number of security phrases required to authenticate

If passphrase logon is enabled in MyID, and a user has the roles to enable password logon, and has at least one security phrase recorded, that user will be able to log on with security phrases, and will be prompted to answer some or all of the security phrases recorded for that user.

The following options on the **PINs** page of the **Security Settings** workflow control the number of security phrases required:

- **Number of security questions to register** – determines how many security phrases a user is required to enroll in the **Change Security Phrases** or **Change My Security Phrases** workflows.

- **Number of security questions for operator authentication** – determines the number of security phrases the user is required to provide when an operator asks them; for example, during the **Authenticate Person** or **Unlock Credential** workflows.

- **Number of security questions for self-service authentication** – determines the number of security phrases users are required to provide when authenticating themselves.

   Note: You can set a maximum value of `6` for these options.

Note: The startup user created by GenMaster has a single security phrase, so can still log on to MyID with the single security phrase even if the configuration option is set to a higher value. This is by design.

If required by customer specific security policy, you can change the **Number of security questions to register** configuration to a higher number, forcing users who set their security phrases to record more security phrases, and therefore enter more security phrases when they log on.

If you increase the **Number of security questions to register** option after users have already been enrolled, existing users will still be able to authenticate with their currently enrolled number of security phrases, as long as this is equal to or greater than the **Number of security questions for self-service authentication** or **Number of security questions for operator authentication** options as appropriate.

To force users to use the **Change My Security Phrases** workflow to increase the number of their security phrases, you can use the **Set Security Phrase at Logon** option:

1. From the **Configuration** category, select **Security Settings**.

2. On the **Logon** page, set the following option:

     ◆ **Set Security Phrase at Logon** – set this to the following value:

         1,110

         This identifies the **Change My Security Phrases** workflow – when a user attempts to authenticate, but has fewer than the configured **Number of security questions to register**, they will be required to complete this workflow before continuing.

3. Click **Save changes**.

Note: The **Set Security Phrase at Logon** option is supported in MyID Desktop from MyID 10.6 Update 1 onwards – make sure you have upgraded your clients.

3.3.3   Unlocking security phrases

If a user has locked their account by entering their security phrases incorrectly too many times, you can unlock their account and allow them to attempt to log on again.

To unlock a user's security phrases:

1. From the **People** category, select **Unlock Security Phrases**.

2. Use the Find screen to search for the user whose account you want to unlock.

3. Select the user from the list.

    The user's details appear on screen.
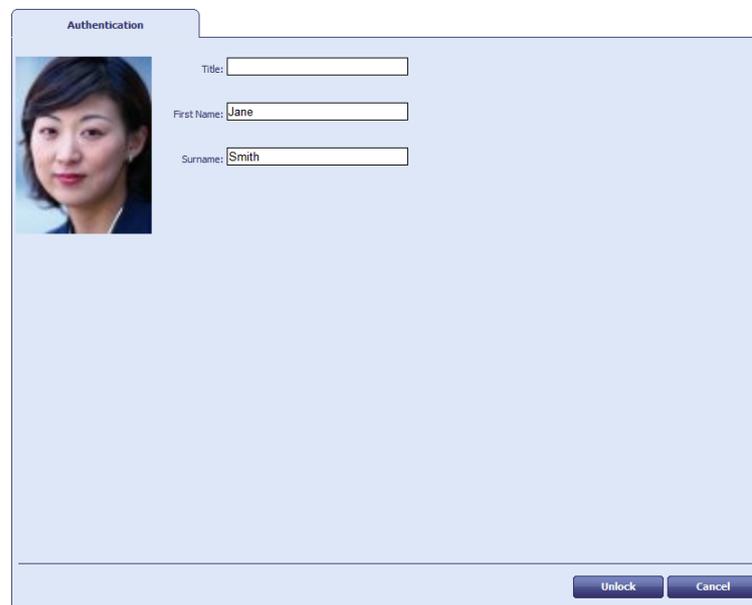
4. Click **Unlock**.

3.3.4 Unlocking your own security phrases

You can allow users to unlock their own security phrases by giving their role access to the **Unlock My Security Phrases** workflow. The user can authenticate to MyID with some other method (for example, smart card or logon code) then use this workflow to unlock their security phrases without any further authentication.

To unlock your own security phrases:

1. From the **People** category, select **Unlock My Security Phrases**.
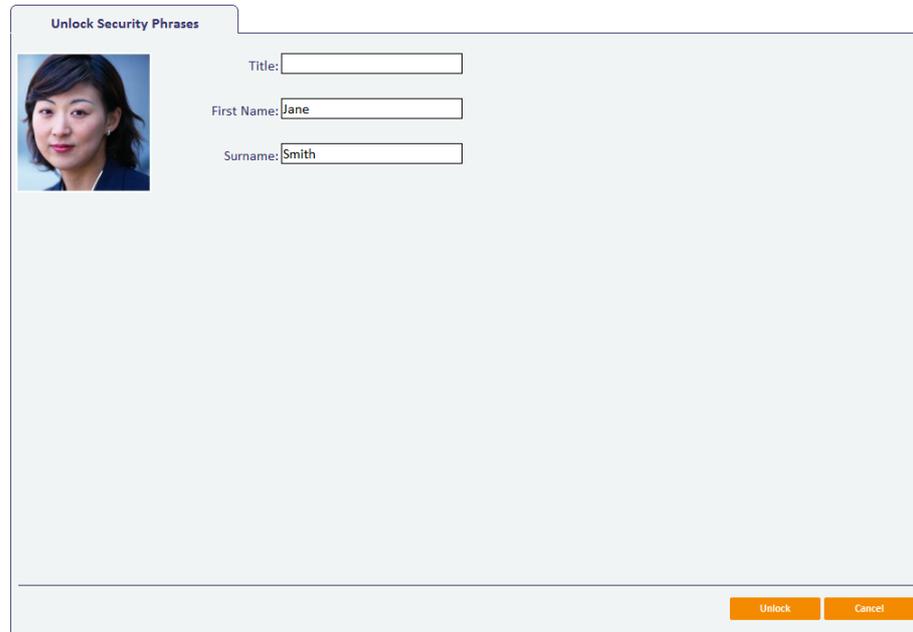
2. Click **Unlock**.

3.4 Logon codes

You can set up MyID to send an email message containing a one-time logon code to a cardholder. The cardholder can then use this code to authenticate to MyID and complete the operation; for example, to collect their card, request a replacement card, or collect soft certificates.

Note: If the cardholder makes several failed attempts to enter the logon code, as a security measure, they are prevented from making any further attempts. To allow the cardholder to proceed, you must use the **Job Management** workflow to cancel the original request, then request another credential for the cardholder. MyID will then send a new logon code.

3.4.1 Setting up logon codes

To set up MyID to send logon codes:

1. From the **Configuration** category, select **Security Settings**.

2. On the **Logon** tab, set the following options:

    ◆ **Allow Logon Codes** – set this option to Yes to allow MyID to send logon codes. If you set this option to No, MyID will not send logon codes and will ignore the **Generate Logon Code** option in the credential profile.

    ◆ **Simple Logon Code Complexity** – the complexity used when you select **Simple** from the **Generate Logon Code** drop-down list in the credential profile. By default, this is `12-12N`.

◆ **Complex Logon Code Complexity** – the complexity used when you select **Complex** from the **Generate Logon Code** drop-down list in the credential profile. By default, this is `12-12ULSN`.

Complexity settings (both simple and complex) take the format `mm-nnULSN`.

`Mm` = min length (must be greater than 0)

`nn` = max length (greater or equal to the min length, with a max of 99)

`U/u` = must/may contain upper case (optional)

`L/l` = must/may contain lower case (optional)

`S/s` = must/may contain symbols (optional)

`N/n` = must/may contain numbers (optional)

You must specify a min length, max length, and at least one of U, L, S, or N.

3. On the **Logon Mechanisms** tab, set the following option:

◆ **Password Logon** – set this option to `Yes`.

4. Click **Save changes**.

5. In the **Edit Roles** workflow, make sure the user's role has the **Password** logon mechanism assigned.

See section *4.1.5*, *Assigning logon mechanisms* for details of using the **Edit Roles** workflow.

6. From the **Configuration** category, select **Credential Profiles**.

7. Select the profile you want to edit, and click **Modify**.

8. Select the **Issuance Settings** section.

9. For **Generate Logon Code**, select one of the following:

◆ **None** – no logon code is generated.

◆ **Simple** – the logon code is generated using the complexity rules as defined by the **Simple Logon Code Complexity** configuration option.

◆ **Complex** – the logon code is generated using the complexity rules as defined by the **Complex Logon Code Complexity** configuration option.

Credentials using the profile will send an email message containing a logon code.

10. Click **Next** and complete the workflow.

3.4.2 Using logon codes

In the Self-Service Kiosk and the Self-Service App, the cardholder is prompted for the logon code automatically.

In MyID Desktop, if a user has been provided with a logon code, you must start the program using the `/lc` command-line option. MyID Desktop requests your username and logon code:
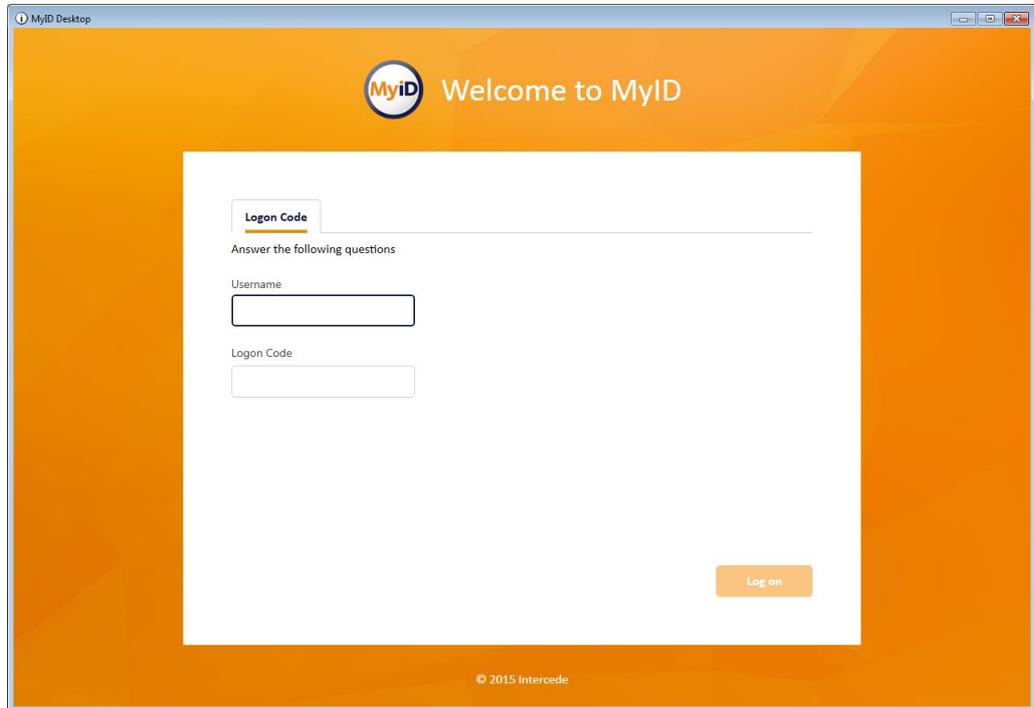
You must also specify a workflow using the `/opid` command-line option to determine the workflow that starts after the user has logged on.

For example:

```
MyIDDesktop.exe /lc /opid:216
```

You can include a hyperlink in the email notification. Use the **Email Templates** workflow to modify the **Job Logon Code** email template, and include a link to the Desktop application similar to the following:

```
myiddsk:///lc+/opid:216
```

Workflow IDs you may want to include for the `/opid` parameter include:

- `216` – **Collect My Card**

- `217` – **Request Replacement Card**

- `706` – **Collect My Certificates**

Note: Make sure you set email messages to be sent in HTML format (see section *14.1.2*, *Email format* for details) and use HTML formatting in your email message; for example:

```
<a href="myiddsk:///lc+/opid:216">Collect My Card</a>
```

Note: When logging on with the `/lc` option, the **Set Security Phrase at Logon** setting is not enforced – users are not required to set their security phrases, even if they do not have the minimum number required. See section *3.3.2*, *Setting the number of security phrases required to authenticate* for details of the **Set Security Phrase at Logon** setting.

3.5 Integrated Windows Logon

If you set up the MyID server to use Integrated Windows Logon, MyID Desktop can use the cardholder's currently logged-on Windows identity to authenticate to MyID without having to enter passphrases or use a smart card.

| Warning:	Back up your system before you make any changes for Windows Logon. If you misconfigure the system, you may no longer be able to log in to MyID.

To set up integrated Windows logon:

1. From the **Configuration** category, select **Security Settings**.

    a) On the **Logon Mechanisms** tab, make sure that **Integrated Windows Logon** is set to Yes.

    b) Click **Save changes**, then click **Save** to confirm your changes.

2. From the **Configuration** category, select the **Directory Management** workflow and set up a configuration-only directory for MyID.

    a) Click **New** and enter a new name – this can be any value.

    b) Select the **Retrieve Base DN** option.

    MyID attempts to connect to the directory and, if successful, displays a list of possible DNs. Select one of the DNs from the list.

    In most cases, you must select the DN that begins `CN=Configuration`.

    c) Click **Save**.

3. Edit the roles within MyID.

    a) From the **Configuration** category, select **Edit Roles**.

    b) Click the **Logon Methods** option, and select **Windows Logon** for each role you want to be able to log on with Integrated Windows Logon.

    c) Click **OK**.

    d) Click **Save Changes**.

Note: The fields `SAMAccountName` and `Domain` must be stored in MyID when using Integrated Windows Logon.

Note: Make sure that the web server has the following server role configured:

▪   Web Server (IIS)\Web Server\Security\Windows Authentication

    This server role is required for Integrated Windows Logon to work.

You must also carry out additional configuration on the web services for Integrated Windows Logon; see the ***Web Service Architecture Installation and Configuration Guide*** for details.

3.5.1 Integrated Windows Logon for existing user accounts

If you set up MyID for Integrated Windows Logon, and have existing user accounts in MyID that were already imported, you may have to resynchronize the user records before you can use those accounts with Integrated Windows Logon.

You can do this by selecting the user account in the **Edit Person** workflow, or by using the Batch Directory Synchronization Tool. See section *5.5*, *The Batch Directory Synchronization Tool* for details.

4 Roles, Groups and Scope

MyID uses roles, groups and scope to define access to workflows and to records.

- Roles are based on the tasks that people do as part of their jobs. Each role gives the person allocated that role access to a defined list of workflows within MyID.

- Scope determines which groups relative to their own group someone can work with for each of their roles. See section *4.5*, *Scope and security,* for more information.

- Groups provide the structure to contain the people. See section *4.6*, *Groups,* for more information.

For information on assigning roles and the scope of those roles to people, see section *26.2*, *Adding people*.

4.1 Roles

Operators assign roles to people when those people are first added to MyID, but these roles can be changed later, usually without needing to reissue credentials. One person can be allocated multiple roles, which reduces the number of individual roles you need to maintain.

A number of roles are already defined and are available for use when MyID is installed. Depending on the configuration of your MyID system, you may have a different set. You can view the workflows accessible to each of these roles in the **Edit Roles** workflow – not all roles are displayed when you access this workflow.

For example:

- **Cardholder**
- **Manager**
- **Security Chief**
- **Personnel**
- **Help Desk**
- **Startup User**
- **Device Account**
- **Unlock User**
- **Password User**
- **System**

Warning:	**System** and **Startup User** must not be allocated to end users. They are used for system administration and updates to the product may add operations to these roles. You must ensure that the ability to assign these roles to individuals is carefully controlled; see section *4.1.4*, *Controlling the assigning of roles*.

You can make changes to the workflows accessible to the different roles or add new roles to the default set using the **Edit Roles** workflow.

You can:

- Change existing roles
- Add new roles
- Delete roles

▪ **IKB-225 – Console Logon feature has been replaced**

The **Console Logon** option in the **Edit Roles** workflow was previously used to determine if a person holding that role could log on to MyID. This mechanism has now changed, and the **Console Logon** option has no effect. For each role, the ability to log on to MyID is controlled by the logon mechanism section of edit roles, and by having at least one workflow assigned to that role; to configure a role where logon is not available (for example, to control permissions to credential profiles) ensure the role has no logon mechanisms assigned. Logon mechanisms are also enabled/disabled globally in security settings.

4.1.1   Change an existing role

A subset of available roles is visible when you start the **Edit Roles** workflow. If the one you want to change is currently hidden, you must make it visible before you can make any changes. You may also want to hide some of the visible roles that you are not currently working on.

Note: Your choice of whether a role is visible or hidden is not saved.

1. In the **Configuration** category, select the **Edit Roles** workflow.

2. If necessary, use the **Show/Hide Roles** button in the bottom left corner of the page to open the **Show or Hide Roles** box at the top of the page.

Select which roles to **Show** and which to **Hide**, and then click **Close**.

Note: Do not click **Save Changes**. If you do, the page is refreshed and the default **Show** and **Hide** settings are used to set the display.

3. Locate the column heading of the role you want to change.

◆ The **Full Access to Manager Controlled Lists** option is reserved for future use.

◆ If a workflow is selected, it appears in the list of workflows available to people assigned that role when they access MyID.

◆ If a workflow box is cleared, it is not included in the list of workflows.

This selection works by deciding what to include; it does not exclude. If an individual is allocated more than one role, the combined set of included workflows is available to that person and each workflow is present only once.

Note: Some workflows contain two parts. If there is a workflow with the same name with **Part 2** appended to it, you must select both workflows.

Note: Some workflows have sub-options indented beneath them; for example, **View User Audit** and **View Full Audit**. Selecting and deselecting sub-options does not affect the category-level checkbox; for example, it is possible to select **View Full Audit** and deselect the **Reporting** category – in this case, no **Reporting** workflows will be available to the user. If you have any sub-options selected, make sure the category-level option is also selected; you may need to select the parent option for the sub-option if no other workflows in that category are selected.

Note: If you hover your mouse over the workflow name, MyID displays a tooltip that lists which clients can use the workflow.

If you make a mistake, click **Reset** to revert to the settings that were last saved.

4. Click **Save Changes** to save any changes. The workflow finishes and you must start it again to make any more changes.

4.1.2 Add a role

1. In the **Configuration** category, select the **Edit Roles** workflow.

2. Click **Add** at the bottom of the page. The **Add Roles** box opens.

3. Enter a name for the role in **Add Role called**.

4. In **Derived from**, select the access level that you want to be used as the basis for your new role.

   In addition to all existing roles, you can also choose from:

   ◆ **Allow None** – no access is granted to any workflow (this is the default).

   ◆ **Allow All** – access is granted to every workflow.

5. Click **Add**. Your new role is displayed to the right of the list of existing roles.

6. Change the workflow access available to the new role by selecting or clearing the boxes for each of the workflows.

7. Click **Save Changes** to save the new role and its associated workflow access.

Note: You can add a maximum of 100 custom roles to the system. The standard MyID system roles do not count towards this total.

4.1.3 Delete a role

1. In the **Configuration** category, select the **Edit Roles** workflow.

2. Click **Delete** at the bottom of the page. The **Delete Roles** box opens.

3. Select the role you want to delete from the list in **Delete a Role**.

4. Click **Delete**.

   You are prompted to confirm your action and are reminded that you must transfer people who had been allocated this role to another role.

5. A box called Transfer Users opens.

   Anyone who was allocated the deleted role is allocated to another role. You must select the role to be used.

Note: You must still select a replacement role even if there are no users currently using the role you are deleting.

6. Click **Close** to close the box and complete the transfer.

4.1.4 Controlling the assigning of roles

Roles are assigned to people when their accounts are created or edited. Unless you specify the roles that an individual must have to assign a particular role to someone else, anyone could assign any role. For example, you may specify that someone must have either the System role or the Security Officer role to be able to assign the Help Desk role to other users.

To set the roles that can manage (assign) a role:

1. Click the icon in the **Managed By** row, immediately below the role name.

The icon indicates whether the role already has any management restrictions:

The role can be managed by any roles.

The role has a restricted list of roles that can manage it.

2. In the box that opens, specify which roles can assign this role to someone.

Note: If you leave all the options unselected, this means the role you are editing can be managed by *any* role.

3. Click **OK**.

4. Click **Save Changes**.

Note: If a role is set as a manager for another role, you cannot delete the managing role without first removing the link between the roles. If you attempt to delete a role, you will see a message similar to:

```
The following roles are currently managed by the Audit Manager role:

Auditor

This role cannot be deleted at this time.
```

4.1.5   Assigning logon mechanisms

You must specify the logon mechanisms for each role. If a user has multiple roles, this allows you to provide a different set of workflows depending on their method of logging in; for example, you can restrict the workflows available when a user is logged on using security phrases, and provide a full set when the user is logged on with a smart card.

Note: The **PasswordUser** role is not available for selection when assigning roles; instead, it is automatically used by MyID to provide access to workflows when a user is logged on to MyID using security phrases.

To specify logon mechanisms:

1. From the **Configuration** category, select **Edit Roles**.

2. Click **Logon Methods** at the bottom of the page.

3. In the Logon Mechanisms box, select the logon mechanism you want to use for each role.

Logon Mechanisms	Password	Smart Card	Windows Logon	Biometric Logon
Cardholder (1)	☐	☑	☑	☑
Manager (2)	☐	☑	☑	☑
Security Chief (3)	☐	☑	☑	☑
Personnel (4)	☐	☑	☑	☑
Help Desk (6)	☐	☑	☑	☑
Startup User (986)	☑	☑	☑	☑
Device Account (987)	☐	☐	☐	☐
Windows Logon User (990)	☐	☐	☐	☐
Activation User (994)	☐	☐	☐	☐
Unlock User (995)	☑	☐	☐	☐
PasswordUser (998)	☑	☐	☐	☐
System (999)	☐	☑	☑	☑

OK
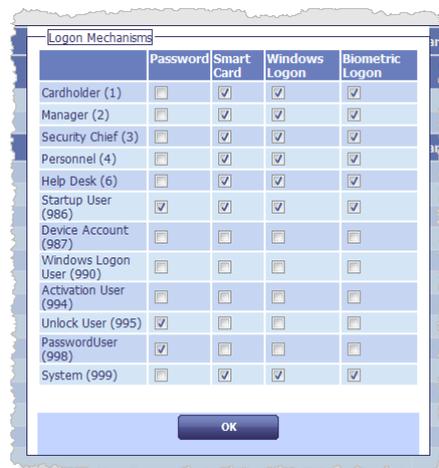
- **Password** is used for security phrase logon.

- **Smart Card** is used for smart card logon.

- **Windows Logon** is used for Integrated Windows Logon. See section *3.5*, *Integrated Windows Logon*.

- **Biometric Logon** is currently used only for resetting PINs. See section *27.7.5*, *Self-service PIN reset authentication*.

4. Click **OK**.

5. Click **Save Changes** to close the **Edit Roles** workflow.

4.2 Role inheritance

MyID allows you to specify whether the available roles for a group are inherited by their child groups.

With role inheritance, if you change the roles available to the parent group, these roles are filtered down to the child groups.

4.2.1 Role restriction option

The **Restrict Roles on Child Groups** configuration option determines whether groups inherit the restrictions on roles from their parent groups.

To set the role restriction option:

1. From the **Configuration** category, select **Security Settings**.
2. Click the **Process** tab.
3. Set the following option:
   - **Restrict Roles on Child Groups** – set to one of the following options:
     - **Yes** – the roles available to the group are restricted to the roles available to the group's parent. The **Inherit Roles** option appears on the Select Roles dialog.
     - **No** – the group may select from any roles in the system. The **Inherit Roles** option does not appear on the Select Roles dialog.
4. Click **Save changes**.

4.2.2 Setting a group to inherit roles

To specify whether a group inherits roles:

1. Start the **Add Group** or **Amend Group** workflow.
2. For the **Add Group** workflow, you must select the **Parent Group** before you can set the roles.
3. Click **Roles** box.

Note: The **Inherit Roles** box appears only if you have selected the **Restrict Roles on Child Groups** option. See section *4.2.1*, *Role restriction option* for details.

4. To inherit the available roles from the parent group, either:
   - Select the **Inherit Roles** option, *or*
   - Deselect all of the roles in the list.

   To specify a list of roles explicitly, select one or more roles from the list.

5. Click **OK** and complete the workflow.

4.2.3   Inherited roles example

- Initial setup.

  Assume your system has the roles `Help Desk`, `System`, `Manager`, and `Cardholder`.

  Set the **Restrict roles on child groups** configuration option to `Yes`.

  Create a group called `Administrators` with a parent group of `Root`. Add `System`, `Manager` and `Cardholder` as the available roles for the group.

  Create a new subgroup called `Admin North` beneath the `Administrators` group. Set the **Inherit Roles** option for the group. The new subgroup inherits `System`, `Manager` and `Cardholder` as the available roles for the group.

  Create a new subgroup called `Admin North System` beneath the `Admin North` group. Do not set the **Inherit Roles** option for the group; instead, explicitly select `System` and `Cardholder` as the available roles. (**Note:** You cannot select the `Help Desk` role, as that is not available to its parent.)

- Remove a role available to `Administrators`.

  Edit `Administrators` to remove the `Cardholder` role.

  `Administrators` now has the `System` and `Manager` roles.

  `Admin North` now has the `System` and `Manager` roles.

  `Admin North System` now has the `System` role.

- Add a role to `Administrators`.

  Edit `Administrators` to add the `Help Desk` role.

  `Administrators` now has the `Help Desk`, `System`, and `Manager` roles.

  `Admin North` now has the `Help Desk`, `System`, and `Manager` roles.

  `Admin North System` now has the `System` role. If a group has explicit roles set, it can only inherit the removal of roles from its parent; it cannot inherit the addition of roles. However, you can now edit the `Admin North System` group to add the `Help Desk` role manually.

4.3   Default roles

You can set default roles for each group. These roles are automatically assigned to any new account added to the group. The default roles can also be inherited by any subgroups that are created within the group.

4.3.1   Default roles example

Assume your system has the roles `Help Desk`, `System`, `Manager`, and `Cardholder`.

Create a group called `Administrators` with a parent group of `Root`. Add `System`, `Manager` and `Cardholder` as the available roles for the group, then add `System` and `Cardholder` as the default roles.

Create a new subgroup called `Admin North` beneath the `Administrators` group. The new subgroup inherits `System`, `Manager` and `Cardholder` as the available roles for the group, and inherits `System` and `Cardholder` as the default roles.

Add a new account `John Smith` to the `Admin North` group. This account is automatically assigned the `System` and `Cardholder` roles; you can also choose to add the `Manager` role if necessary by editing the user's record.

You cannot assign the `Help Desk` role to `John Smith`, as the group's permissions do not allow it.

Edit the `Administrators` group to change the default roles to `System`, `Manager` and `Cardholder`. The `Admin North` group is automatically updated to inherit `System`, `Manager` and `Cardholder` as default roles.

Add a new account `Jane Jones` to the `Admin North` group. This account is automatically assigned the `System`, `Manager` and `Cardholder` roles.

Note, however, that the `John Smith` account still has only the `System` and `Cardholder` roles: changing the default roles for a group *does not* affect the roles of existing users within the group.

Edit the `Admin North` group, and uncheck the **Inherit Roles** option on the Select Default Roles dialog. Now edit the `Administrators` group to change the default roles to `System` only. If you view the `Admin North` group, you can see that it still has `System`, `Manager` and `Cardholder` as default roles – deselecting the **Inherit Roles** option breaks the link between its default roles and its parent's.

If you now select the **Inherit Roles** option again for the `Admin North` group, the default roles change to `System` only – you have re-attached the link to the default roles of the parent group.

4.3.2 Setting up default roles

To create a group with default roles:

1. From the **People** category, select **Add Group**.

2. Type the **Group** name and **Description**.

3. Select the **Parent Group**.

    The **Roles** and **Default Roles** are inherited from the parent group.

    If you select **Root** as the **Parent Group**, the group does not inherit any roles or default roles from its parents.

4. Click the **Roles** box to select which roles will be available to users in this group.

    Note: If you do not select any roles, `0 Role(s)` is displayed in the box; this means that users in this group may have *any* role. See also *4.2.2, Setting a group to inherit roles* for details of inheriting roles.

5. Click the **Default Roles** box to select which roles will be assigned by default to users who are added to this group.
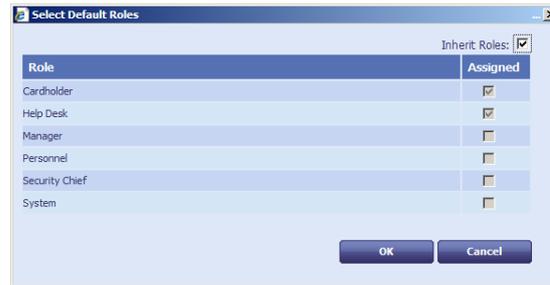
If you selected a parent other than **Root**, the **Inherit Roles** option is selected automatically, and the group inherits the default roles of its parent group. If you leave this option selected, any changes to the default roles of the parent group are inherited automatically by the child group.

If you deselect the **Inherit Roles** option, you can set the default roles for the group manually. The initial selection of default roles matches the inherited roles; you can now change these default roles to any of the available roles for the group. Any changes to the default roles of the parent group have no effect on the child group.

If you selected **Root** as the parent group, there are no roles to inherit. If you select the **Inherit Roles** option, the group is assigned the system default: `Cardholder` only.

If you do not want to inherit default roles, you must select at least one default role; if you deselect **Inherit Roles**, then deselect all of the individual roles, the group will inherit the default roles from its parent.

6. Click **OK**.

7. Click **Save** to create the group.

Note: You can also amend which roles are available to a group using the **Amend Group** workflow.

4.3.3 Known issues

There is currently an issue where you can configure your group role restrictions and group default roles in such a way that the inherited default roles exceed the role restrictions for the group. If this occurs, an entry appears in the Select Default Roles dialog with **(No longer available)** listed after the role name while the **Inherit Roles** option is selected.

If you add a user to MyID with the group's roles in this state, the operation will fail, as the default roles applied will exceed the allowed roles. To avoid this problem, make sure that the list of allowed roles includes all of the default roles that the group will inherit.

4.3.4 Synchronizing with LDAP

If you synchronize a user with LDAP, and this changes their group, the following actions occur:

- If there are any roles in the user's new group that are not permitted by the user's new role, these roles are removed.

- If there are any default roles in the user's new group that the user does not have already, these roles are added, using the default scope defined for the group.

  Note: LDAP linked roles take precedence over MyID group role restrictions. Do not apply role restrictions in a system that uses LDAP linked roles.

- These actions are audited.

These actions apply to synchronizations carried out through the Batch LDAP Sync tool or through the **Background update** option.

- **IKB-192 – Differences in role update processing on directory synchronization**

  When the Batch LDAP Sync tool identifies a user has moved between active directory Organizational Units, resulting in a change to the assigned MyID group, the associated roles for the user in MyID are updated. This does not occur when the user account is synchronized following a user interface action; for example, selecting a user account in person search results.

4.4 Linking roles to LDAP

You can set up roles in MyID that are linked to groups in your LDAP. If you link the role to a group in the LDAP, any users in the directory that belong to that group automatically get assigned the corresponding role in MyID.

Note: LDAP linked roles take precedence over MyID group role restrictions. Do not apply role restrictions in a system that uses LDAP linked roles.

You must create roles in MyID that have the same name as the groups in the directory.

When you add a user to MyID, the user is automatically assigned the corresponding role. If you change the user's group in the directory, the user is assigned the role corresponding to the new group, and has the existing linked group removed from their list of roles.

When you set up the link to the directory group, you can specify a scope for the role. This scope is used whenever MyID automatically assigns a linked role.

Note: If you have the **Update user information in the directory** configuration option set to `Yes`, users will not be able to be assigned roles based on groups in the LDAP; this is because this option indicates that MyID is the primary source for user data, and information is pushed from MyID to the directory but not the other way around. LDAP linked roles rely on synchronization from the LDAP to MyID, which does not occur when **Update user information in the directory** is set to `Yes`.

4.4.1 Default Active Directory groups

For your MyID roles, do not use the names of any of the groups present in Active Directory by default; for example:

- Domain Users

- Domain Admins

- Enterprise Users

and so on.

This is because MyID uses the `memberOf` LDAP function to retrieve information about the groups to which a member belongs, but this function does not retrieve information about the built-in Active Directory security groups.

You must create new groups in the directory to match the names of the roles within MyID.

4.4.2   Setting up linked roles

To set up a linked role:

1.   From the **Configuration** category, select **Edit Roles**.

2.   Click **Show/Hide Roles** and make sure that the role you want to link is displayed.

Note: The **Linked to LDAP Group** row appears only if you have set the **Link to LDAP Groups** option on the **LDAP** page of the **Operation Settings** workflow.

3.   Click the icon in the **Linked to LDAP Group** row.

When a role is linked, the icon is a green tick.

When a role is not linked, the icon is a red cross.

4.   To link the role to a directory group with the same name:

a)   Select the **Link Role to LDAP Group** checkbox.

b)   Select the default scope to be used for the role from the list.

c)   Click **OK**.

5.   Click **Save Changes**.

4.4.3 Example

For example, if you have the following groups in your directory:

- Sales
- Marketing
- Support

You would create three roles in MyID with the same names. You may also have roles in MyID that are not linked to any groups. For example, the roles in MyID may be:

- Sales – linked
- Marketing – linked
- Support – linked
- Cardholder – not linked
- Help Desk – not linked

Susan Smith works for your organization in the Sales department. When you add her account to MyID, she is automatically assigned the Sales role. You can also assign her any other roles that are not linked to groups; for example, the Cardholder role.

If Susan Smith moves departments to Marketing, her record in the directory is updated to move her from the Sales group to the Marketing group. When MyID synchronizes with the directory, her MyID account is assigned the Marketing role, and the Sales role is removed from her account. The Cardholder role, which was assigned to her account manually and is not linked to a group, is unaffected.

Note: If you manually assign a role that is linked to a directory group, the next time MyID synchronizes with the directory, the linked role is removed unless the user is in the linked group. For example:

- Susan Smith is in the Sales group. She is automatically assigned the Sales role. You manually add the Cardholder and Support roles to her account. When MyID synchronizes with the directory, Susan Smith retains the Sales and Cardholder roles, but the Support role is removed.

4.5 Scope and security

When a person is added to MyID, an operator assigns a role or roles and can also specify the scope of those roles. Five options are available; from narrowest to widest range, these are:

- **None** – the person is not assigned to this role.
- **Self** – this limits the scope to the person's own record.
- **Department** – all people in the same group as the holder.
- **Division** – all people in the same group as the holder or a sub-group of it.
- **All** – the role can be performed in relation to anyone.

Note: If a user is imported from an LDAP directory, scope affects not only which MyID groups that user can work with, but also which groups within the LDAP the user can work with using MyID. For example, a user who has a scope other than **All** may not be able to view all the users in the LDAP directory when trying to import users into MyID.

For more information about configuring LDAP and scope, contact customer support.

Scope can give a user the ability to make very significant changes for some workflows. For example, if a user has a scope larger than Self for the **Change Security Phrases** workflow, they can potentially change the logon security phrases for a large number of users without any further authentication or confirmation. We recommend that you assign workflows with the potential to make this level of change to a separate role, and grant this role to users with a scope of Self unless you want them to be able to change other users' devices and records.

Workflows that you may want to assign to a separate role and restrict to Self are:

- **Change Security Phrases**
- **Request Replacement Card**

The following workflows are safe to assign with a wider scope, as they are constrained to work on your own account or credentials whatever the scope:

- **Collect My Card**
- **Collect My Device**
- **Recover My Certificates**
- **Change My Security Phrase**

4.6 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.

The way you manage groups differs depending on whether or not you are integrating with an LDAP directory.

If you are integrating with an LDAP directory, your group structure may be based on the Organizational Units (OUs) within the directory. Alternatively, you may base your groups on the reporting structure of your organization or on geographical location.

The changes that you can make to your group structure are limited by the amount of integration with an LDAP directory you are implementing (see section 5, *Using an LDAP Directory*).

Groups are frequently associated with a particular OU (Organizational Unit) in your LDAP directory. This is especially important if you have a Certificate Authority using data from the same directory (for example, to support Windows smart card logon). MyID allows you to record such relationships and provides import and export options to help maintain consistency between the database and the LDAP directory.

If you are integrating with a directory, use the **Edit Groups** option (see section *4.6.4*, *Edit groups*) to import groups from your directory.

4.6.1 Adding a group

1. Select the **People** category and then select **Add Group**. The **General** page opens.
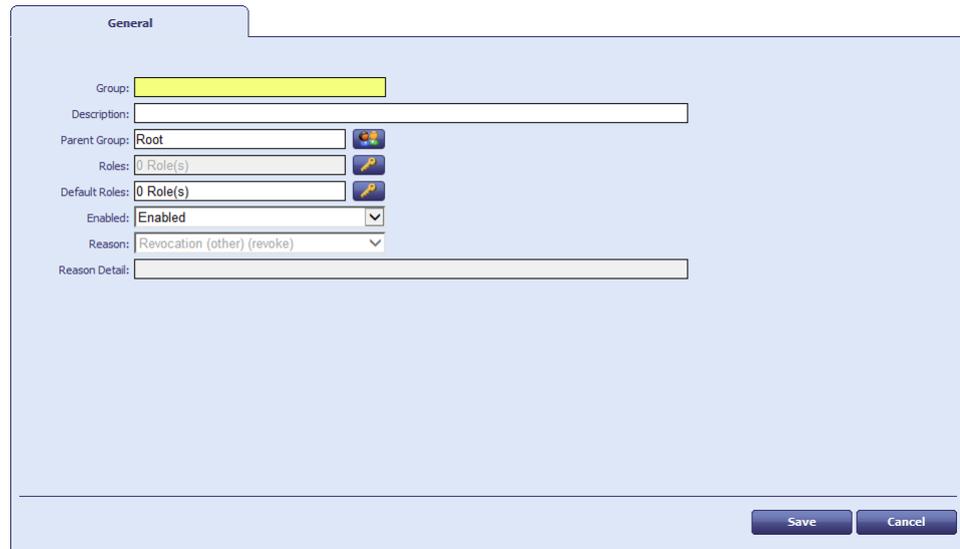
2. In **Group**, type the name of the group.

3. Enter a short **Description** for the group.

4. 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.

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.

6. 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.

7. 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 *29.5*, *Certificate reasons* for details.

4.6.2 Changing a group

You can make changes to the information recorded about a group when it was added, 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**.

   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.

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, but MyID does not add or remove roles from a user automatically.

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

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 *29.5*, *Certificate reasons* for details.

4.6.3 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.

   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.

4.6.4 Edit groups

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

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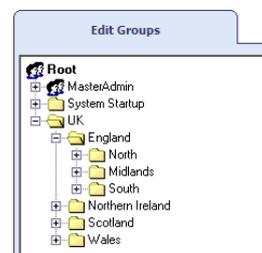
   Existing groups are displayed in a tree structure, and can be expanded or collapsed by clicking the plus (**+**) or minus (**-**) signs to the left of their names.

   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**.

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**.

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**.

Renaming a group

1. Right-click the name of the group that you want to rename.

2. Select **Rename Group** from the menu.

3. Highlight the existing name of the group and enter a new one.

4. Click **Save**.

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 either:

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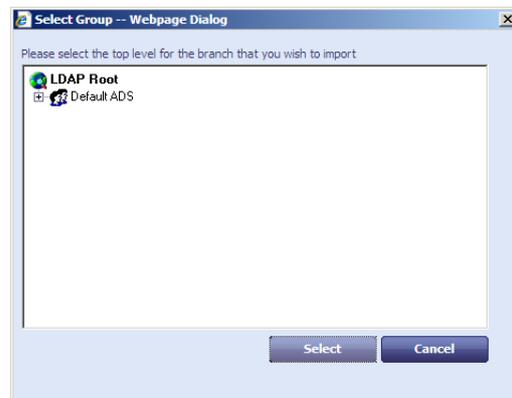
Locate and select the Organizational Unit (OU) that you want to import and click **Select**.

5. Click **Save**.

Removing a group

1. Right-click the name of the group you want to remove.

2. Select **Remove Group** from the menu.

3. Select either:

   ◆ **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**.

4.7 Administrative groups

Administrative groups enable an operator to manage user accounts located in MyID groups anywhere within the group hierarchy, including groups that are not directly connected to the operator's home group.

Prior to enabling administrative groups, scope (see section *4.5*, *Scope and security*) always relates to an operator's *home group*. Once administrative groups have been enabled, scope is extended to include additionally specified *administrative groups* as well as the home group.

Note: Administrative groups only affect workflows with a Department or Division scope, and are not available for group management workflows; for example, **Amend Group** or **Edit Group**.

4.7.1 Configuration settings

From the **Configuration** category, select **Security Settings**. The **Allow Administrative Groups** option is on the **Process** tab.

▪ When set to **Yes**, the scope available in workflows is extended to include any additionally specified administrative groups assigned to operators. The **Add Person** and **Edit Person** workflows are extended to allow management of administrative groups.

▪ When set to **No**, the scope in workflows is limited to operators' home groups, and it is not possible to manage operators' administrative groups in **Add Person** or **Edit Person**.

4.7.2 Assigning Administrative Groups

From the **People** category, select the **Add Person** or **Edit Person** workflow.

An **Administrative Groups** option is displayed immediately below the **Group** field:
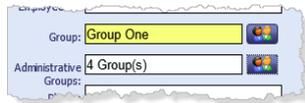
This displays the number of administrative groups assigned to this person. Hovering on the text box displays the names of the groups assigned.

Click the text box or icon to open the **Administrative Groups** dialog, which lists the fully qualified path to all the groups assigned to the person:

- To remove groups, select them and click the **Remove** button.

  Rows that are grayed out refer to administrative groups assigned to a user that the operator does not have within their scope, so cannot be removed by the operator.

- To add groups, click the **Add** button and use the **Select Group** dialog.

The **OK** button keeps any changes and returns you to the workflow. Changes made here are committed to MyID only when the person's record is saved; that is, when the **Add Person** or **Edit Person** workflow is completed.

The **Cancel** button closes the dialog without making any changes.

4.7.3 The Select Group dialog

The Select Group dialog appears in a number of places where the operator needs to select a single group.

If the **Allow Administrative Groups** option is set to **Yes** and the operator has been assigned a number of administrative groups, the operator will see an extra root node named **Administrative Groups** in all workflows where scope is greater than **Self**.

For example, the above dialog is shown to an operator who has **Department** scope in a particular workflow, as well as having administrative groups assigned to them. The operator has a home group of **Administration**, and two of their administrative groups are mapped to the LDAP directory (**Country A** and **Country B**).

When using the Select Group dialog, the operator could be searching either the MyID database or the LDAP directory.

- When searching the MyID database, all their administrative groups are returned.

- When searching the LDAP directory, only administrative groups that map to the LDAP directory are returned.

4.7.4 The Find Person stage

If the **Allow Administrative Groups** option is set to **Yes**:

- When searching for people from the MyID database, the **Group** field in the Find Person stage of all workflows is not pre-populated with the operator's home group. This allows people to be found from the operator's home group as well as the operator's administrative groups.

- When searching for people from the LDAP directory, it is still necessary to specify the LDAP group to search from.

  Note: If you are using administrative groups to search the LDAP directory, your own account must be a member of the LDAP directory too.

4.7.5 The View Person workflow

The View Person workflow shows how many administrative groups a user has been assigned, and displays the names of those groups when the mouse hovers over the text box.

Click on the text box or icon to open a read-only version of the **Administrative Groups** dialog, which lists the fully qualified path to all the groups assigned to the person. The grayed-out rows refer to groups that are not within the scope of the operator.

4.7.6 Group management

If a MyID group is deleted, the system will remove that group from the scope of all existing operators.

If a MyID group is moved, operators that have been assigned that group as an administrative group will continue to have that administrative group. The sub-groups available to the operators are always calculated based on the latest group structure.

If a MyID group has role restrictions, these restrictions only apply to operators with the group as their home group, and are not applied to an operator who is assigned the group as an administrative group.

4.7.7 The Import Account Details dialog

When using the **Add Person** workflow to add a person to MyID, you can retrieve user details from the LDAP directory by clicking on the **Import** button on the **Account** tab. If the operator has been assigned administrative groups that map to LDAP directory OUs, a second Administrative Groups node is shown with a list of their mapped administrative groups.
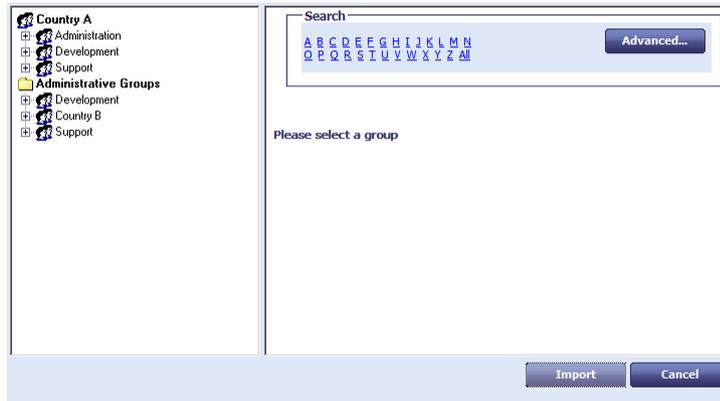
4.7.8 Scope calculations

When an operator enters a workflow, the effective scope for that operator (who he or she can see) is the addition of the scopes of all roles the operator has that include the workflow.

For example, Margaret's home group is **Support** in Country A and she has been given:

▪ Administrative group access to the **Country B** and **Country C** groups.

▪ **Division** rights for the **Registrar** role.

▪ **Department** rights for the **Issuer** role.

If Margaret enters a workflow such as **Issue Card** that is part of the **Issuer** role, but not part of the **Registrar** role, her effective scope would be **Department**.
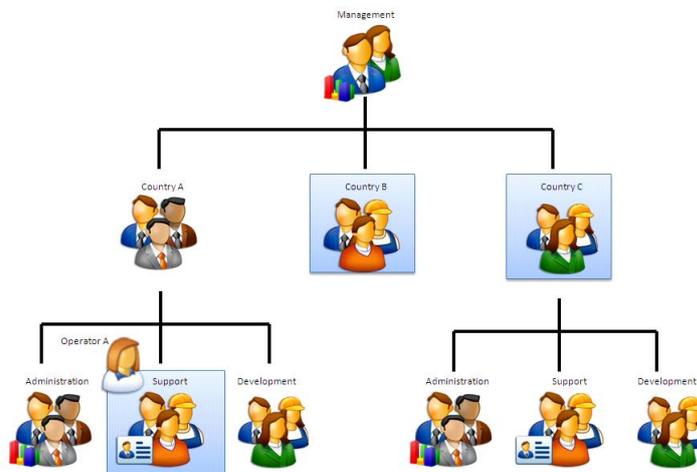
She would be able to manage her own Group and any Administrative Groups that she had been allocated (Country B and Country C). She cannot manage any child groups of these groups, so she cannot issue a card for someone in the Development group of Country C.

If she enters a workflow such as **Edit Person** which is included in the **Registrar** role, but not in the **Issuer** role, her effective rights would be **Division**. Now child groups are visible.
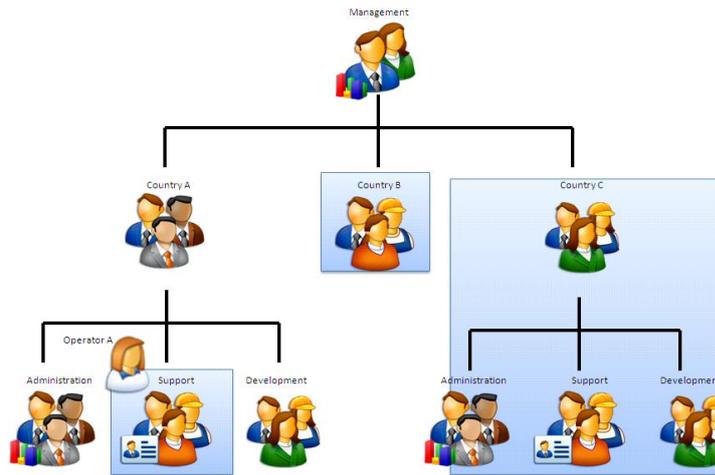
If a workflow is in both roles then, as rights are additive, she would have Division rights.

4.8 Witnessing a transaction

Some operations may be configured to require a witness before the operation is completed.

Witnessing requires a second user who has permission to witness the operation.

Note: The witness does *not* need the target user account or the operator user account to be within their scope.

By default, witnessing is only enforced when a credential profile requires validation and an attempt is made to issue, update or cancel in a single operation. If you want to use witnessing in other areas of MyID, contact Intercede support referencing SUP-91.

When a witness is required for a transaction, both the user who initiates the transaction and the witness must have signing keys on their cards. The **Client Signing** option (see section *34.2*, *Logon page (Security Settings)*) must be set to Yes.

To witness a transaction:

1. The Select Witness screen appears.

   You cannot witness a transaction if you initiated it.

2. Remove your card, and insert the card of the witness.

3. The witness must type their **PIN**, then click **Confirm**.

4. Remove the witness card and insert the original card.

5 Using an LDAP Directory

By default, MyID is set as your primary data source. You can import information into MyID from a directory and use it as a basis for your records, and all user selections are performed against data held in the MyID database. Any changes you make to the information in MyID will *not* be replicated in the directory by default and, if you want to keep the information synchronized, you will have to update the directory separately.

MyID is capable of using an LDAP directory as the primary data source for user records. In this case, user selection in most workflows will perform an LDAP search against the configured directory or directories rather than the MyID database. A copy of the data found is cached in the internal MyID database, but the latest data from the directory is used in preference to any cached data.

If you are using an LDAP directory as your primary data source, and you do not set **Update user information in the directory** to Yes, you will not be able to find any manually added users unless you change the configuration settings to allow a choice of search modes.

MyID can communicate with directory services using either standard or secure LDAP (Lightweight Directory Access Protocol). MyID has been successfully integrated with various directories; a full list of those currently supported is in the *Installation and Configuration Guide*.

Note: When MyID is installed, integration with ADS (Active Directory Service) is automatic, with MyID set as the primary data source.

Warning: You *must* specify a Distinguished Name (DN) for a person if you are going to issue certificates through MyID. One way to do this is to import the user from an LDAP directory.

Settings that determine how MyID and an LDAP directory interact are found on the **LDAP** page in the **Operational Settings** workflow (in the **Configuration** category). You can choose to update the information stored in MyID from an LDAP directory, and to update information in the directory based on details entered into MyID.

The **Add Person** workflow adds a new person record to the MyID database. To prevent someone being added directly to the MyID database, prevent anyone accessing the **Add Person** workflow (see section *4.1.1*, *Change an existing role*).

A user's details can be imported from an LDAP directory using the **Import person** workflow, using the **Import** button on **Add person** workflow or as a result of automatic import because an LDAP directory has been set as the primary data source. When a user's details have been imported, the data held in MyID and the LDAP directory are synchronized in the following ways:

- User data is synchronized using the **Edit person** workflow – this happens unless the **Edit directory information** or **Update user information in the directory** options are set to Yes.

- Information is automatically synchronized when a record is selected if **Background update** is set to Yes and **Edit directory information** is set to No.

- To copy a person's details from MyID to the LDAP directory, set **Update user information in the directory** to Yes.

  Note: You must configure your directory connection with appropriate write permissions to update it from information entered into MyID.

Processes within MyID may be triggered by changes to directory information. For example, certificates may be revoked when an account is disabled.

Warning:	Integration with Active Directory and the option to use the directory as the primary data source are selected by default during the installation of MyID.
	If you do *not* want to use an LDAP directory as your primary data source, follow the instructions in section *0*, *Note: If multiple MyID groups are mapped to* the same `OrgUnit` on a particular LDAP, this will prevent syncing from the relevant LDAP group. For more information, contact customer support quoting reference SUP-266.

Using an LDAP directory as the primary data source.

Note: This chapter assumes that you understand the concepts of an LDAP directory and have access to the documentation provided with the directory you are using.

5.1 What do you need to know?

Before you can configure MyID to connect to an LDAP directory, you need to decide:

- Do you want to specify whether records can be retrieved from just MyID or just the LDAP directory, or from both?

- Do you want to be able to change data within MyID and have those changes copied (replicated) to the directory?

The following information can all be provided by your LDAP directory administrator:

- What is the name of the machine hosting the directory?

- Which port is being used for LDAP communication?

- Is secure LDAP being used?

- What is the base distinguished name (DN) of the directory?

- Is a user DN and password required for connection? If so, what are they?

Note: MyID automatically detects the presence of Active Directory and creates a connection to it. However, Intercede recommends that you set a host, port and base DN.

For information on custom LDAP mappings and search filters, contact customer support quoting reference SUP-223.

During credential lifecycle events (such as issuance or revocation), MyID can send updates to a connected directory. This can be used to set specific attributes against a user; for example, setting or removing the requirement to log on to Windows using a smart card.

This feature requires careful configuration. For more information, contact customer support, quoting reference SUP-227.

5.2 Creating the connections

Warning:	If you have Active Directory installed in your environment but want to use a different directory service, you must change the association that was automatically created during installation to exchange data with the other directory service.

You can connect to multiple directories simultaneously and have multiple connection points within a single directory.

Note: All of the LDAP directories referenced by MyID must be provided by the same vendor and must use the same LDAP schema for any data linked to MyID records.

You configure LDAP connections within MyID.

1. From the **Configuration** category, select **Directory Management**.

2. If there is a directory in the **Select Directory** box, information about it is displayed.

    You can:

- Add a directory by clicking **New**.

- Edit an existing directory by selecting it in the **Select Directory** drop-down list and clicking **Modify**.

You are now in the **Edit Directory** stage.

Note: If you are modifying the details of a directory that was automatically detected, some of the information on this page may already be completed.
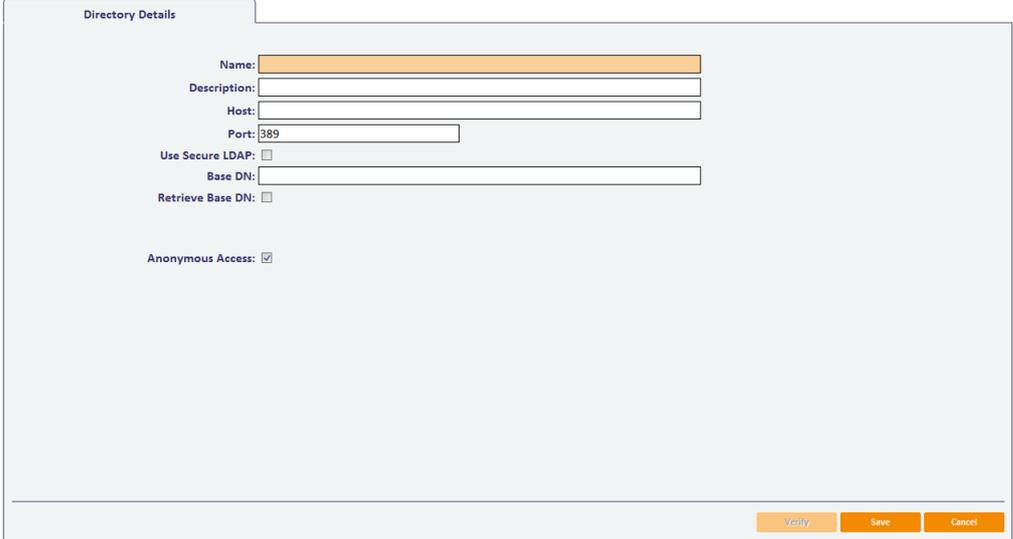
3. Give the directory a meaningful **Name** and **Description** to help you to recognize it.

4. Enter the name or IP address of the machine hosting the directory in the **Host** field. You may need to enter a fully qualified domain name if the machine is in a different domain from the MyID server.

5. Enter the **Port** that is being used for LDAP connections.

   The default port for standard LDAP connections is `389` and the default port for secure LDAP connections is `636`.

   Note: You must enter the port that the directory is using – check with your directory administrator.

6. If the directory you are connecting to is using secure LDAP, select the **Use secure LDAP** option.

7. Enter the **Base DN** for the directory. Either:

   - Type the information directly into the field.

   - Select the **Retrieve Base DN** option.

     MyID attempts to connect to the directory and, if successful, displays a list of possible DNs. Select one of the DNs from the list.

8. By default, MyID connects directories anonymously. For Active Directory, this means that MyID uses the interactive user; for MyID this is the MyID COM+ user account set up at installation. If you want to change this, and specify a user account:

   a) Clear the **Anonymous Access** option.

   b) Enter the **User DN** and the **Password** associated with the account that will be used to connect to the directory.

   Note: In some Active Directory setups, connecting anonymously using the interactive user may fail. You can set MyID to connect using a specific account; this can be the same account as that used by the interactive user.

Note: Whether you are using anonymous access or a specific user, you must ensure that the user (which is the MyID COM+ user in the case of anonymous access) has the appropriate permissions to update the directory.

Note: The introduction of User Account Control in Windows Server 2008 and Windows Vista has affected making modifications or additions to an LDAP directory. When a user is logged on to a DC with a restricted UAC Administrator token and using NULL credentials, any modification or addition to the directory, or any schema change operation, will fail with insufficient access rights. This includes DirSync searches, retrieving the SACL from an object's ntSecurityDescriptor attribute when using SecurityDescriptorFlags, and many other operations. If User Account Control is in effect when an administrator logs on to a DC, the administrator will get a restricted token in the logon session. If he or she then uses ldap_bind_s with NULL credentials, then operations that make modifications or additions will fail.

9. Click one of:

   ◆ **Verify** – MyID attempts to connect to the directory using the information you have provided.

   ◆ **Save** – to save the details you have entered.

   ◆ **Cancel** – to leave the workflow without saving any information.

5.3   Using and updating LDAP information

To specify the way that an LDAP connection is used, select the **Operation Settings** workflow from the **Configuration** category menu.

The settings relevant to your LDAP connections are on the **LDAP** page; see section *33.4*, *LDAP page (Operation Settings)* and cover:

- Whether to display Active Directory data in MyID

- Whether information in the LDAP directory is updated when it is updated in MyID

- Synchronizing information from LDAP to MyID.

Note: If multiple MyID groups are mapped to the same OrgUnit on a particular LDAP, this will prevent syncing from the relevant LDAP group. For more information, contact customer support quoting reference SUP-266.

5.4   Using an LDAP directory as the primary data source

If you want to use an LDAP directory as the primary data source, you need to make some changes to the configuration:

1. Select the **Configuration** category and then the **Operation Settings** workflow.

2. Click the **LDAP** tab.

3. Change the setting for **Search a Directory** to either **Yes** or **Ask**.

4. Click **Save changes**.

To prevent people adding people directly to the MyID database, remove access to the **Add Person** workflow. For instructions, see section *4.1.1*, *Change an existing role*.

Log out of MyID and log on again to see the changes.

5.5 The Batch Directory Synchronization Tool

MyID can be configured to update user information in MyID from the LDAP directory automatically when a user record is selected. This tool does the same thing for all accounts in MyID.

The Batch Directory Synchronization Tool is used to synchronize users imported into MyID with the latest information held in the directory. If MyID is integrated with multiple LDAP directories, all the directories will be included in the synchronization process.

You run the tool on the MyID application server, under the MyID COM user. You can run the tool from the **Start** menu, from the command line or as a scheduled task. For an installation containing a significant number of records, Intercede recommends that you run the synchronization tool as a scheduled task.

5.5.1 How does the Synchronization Tool work?

The Synchronization Tool processes all the records in the MyID database that are mapped to entries in an LDAP directory.

- If the record exists in MyID but the corresponding entry is no longer present in the LDAP directory, the tool can disable the user account and revoke the associated certificates.

- If the record exists in both MyID and the LDAP directory, any changes to the information held in the LDAP directory are copied to MyID.

  If the user account has been disabled in Active Directory, the user account in MyID can also be disabled and associated certificates suspended – you must set the **Disable on removal from directory** configuration option.

  Note: You can choose to revoke certificates instead of suspending them if the user account is suspended in the directory. Please contact customer support for details.

  Note: When you synchronize the records, if you have changed information in MyID, but not copied these changes to the directory, the changes will be overwritten by the information from the directory.

- If the **whenChanged** option is selected (either by selecting the **whenChanged** checkbox on the tool window, or by specifying the `-whenchanged` option on the command line) the tool processes only those records that have been updated since the last time the tool was run. The `whenChanged` attribute in the directory is used to identify these records. The date and time of start of the last run of the tool is stored in the MyID database.

- If the record exists in MyID, but the corresponding entry is no longer present in the directory, the behavior of the tool depends on whether the **whenChanged** option is selected:

  - If the **whenChanged** option *is* selected, the tool will not update the MyID database to reflect the removal of the user from the directory. In this case, you must use the Active Directory Deletion Tool to synchronize the deleted users. See section *5.8*, *Active Directory Deletion Tool* for details.

  - If the **whenChanged** option is *not* selected, the tool can disable the user account and revoke the associated certificates. This depends on whether the following options have been selected on the **LDAP** page of **Operation Settings** workflow in the **Configuration** category:

    - **Disable on removal from directory**.

    - **Revoke certificates if user is removed or disabled following background directory update**.

Note: When the tool is run for the first time since installation or upgrade, it runs without the **whenChanged** behavior, whatever options you select; this is to provide an initial successful run to set the start time of the last successful run in the database. If you select the **whenChanged** option, the tool displays a warning:
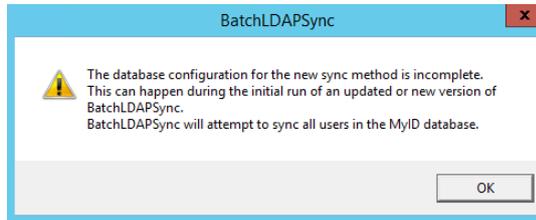
All changes are written directly to the MyID database and are fully audited.

5.5.2 Revoking certificates

The behavior of MyID in revoking certificates for users who have been removed from the directory depends on the combination of MyID configuration options:

Disable on removal from directory	Revoke certificates if user is removed or disabled	Behavior
NO	NO	User in MyID is unaffected.
NO	YES	User in MyID is unaffected.
YES	NO	User is disabled in MyID. Associated certificates are unaffected.
YES	YES	User is disabled in MyID and associated certificates are revoked.

5.5.3 Running the tool from the Start menu

By default, the tool runs in interactive mode from the **Start** menu. You can change this by editing the properties of the shortcut to incorporate the flags specified in section *5.5.4*, *Running the tool from the command line*.

Note: Run the utility under the MyID COM user account.

1. From the **Start** menu, run the **Batch Directory Synchronization Tool**.

2. To update only those records that have been changed since the last time the Batch Directory Synchronization Tool was run, select the **whenChanged** option.

3. Click **Synchronize**.
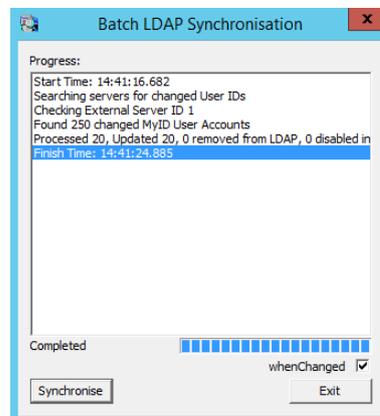
Progress is displayed both in the text area and in a progress bar towards the bottom of the dialog.

A summary of the records processed and the time taken are displayed.

For example:

```
Processed 122083, Updated 41752, 7027 removed from LDAP, 3161 disabled in LDAP
```

This means that the tool carried out the following:

- Parsed 122083 user records.
- Updated 41752 users with changes from the LDAP synchronized to MyID.
- Removed 7207 users from the LDAP.
- Disabled 3161 users in the LDAP.

Note: If the **Disable on removal from directory** option on the **LDAP** page of the **Operation Settings** workflow is set, the 7207 users removed from the LDAP and the 3161 users disabled in the LDAP will also be disabled in MyID.

5.5.4 Running the tool from the command line

Note: Run the utility under the MyID COM user account.

You can run the Batch Directory Synchronization Tool from the command line using the following command lines:

- Interactively – run `BatchLDAPSync.exe` without specifying any flags. The tool runs as described in section *5.5.3*, *Running the tool from the Start menu*.
- Automatic execution – run the program with the `-autorun` flag. The dialog is displayed as described in section *5.5.3*, *Running the tool from the Start menu*, the synchronization process starts automatically, and the dialog closes when the process has finished.
- Silently – run the program with the `-silent` flag. This works in the same way as `-autorun` but the dialog is not displayed. (Do not use both `-silent` and `-autorun` at the same time.)
- New changes only – run the program with the `-whenchanged` flag. Only those records that have been changed since the last time the Batch Directory Synchronization Tool was run are updated.

To record the details of the process to a specified file, add the `-trace` flag to the command. You can use this flag either alone or with the other flags. For example, you could run:

```
BatchLDAPSync.exe -silent -whenchanged -trace LDAPSync.log
```

If you do not specify a filename, `batchldap.log` in the current directory is used.

Note: You are recommended to use the `-trace` option when running in `-silent` mode.

5.5.5 Running as a scheduled task

You can run the Batch Directory Synchronization Tool as scheduled task using standard Windows functionality.

The program to be run is called `BatchLDAPSync.exe` and the flags available are described in section *5.5.4*, *Running the tool from the command line*.

5.5.6 Troubleshooting

- **Unable to communicate with server**

  If the Batch Directory Synchronization Tool experiences an error communicating with an LDAP server, it displays an error similar to:

  ```
  Checking External Server ID 2
  Error communicating with LDAP server, aborting
  ```

  This means that the tool has been unable to communicate with that particular server. Run the tool again once you have confirmed that the network is working correctly.

  Note: If you are running the tool in `-silent mode`, you will see this message only if you enable the `-trace` option and check the log after running the tool.

- **Inaccurate totals when running multiple instances**

  If you are running multiple instances of the Batch Directory Synchronization Tool concurrently, the total of updated users across all instances may not match the actual total of updated users – this is because the same update may be counted by more than one instance. The updates themselves are processed correctly; only the total is inaccurate.

- **Time and date discrepancies**

  The tool displays local time, while the database stores UTC time; this may lead to a perception of a discrepancy between the times and dates displayed.

- **Error during first run**

  If an error is encountered during the first attempted synchronization the database timestamp will not be updated. The next time you run the tool, it defaults to the non-whenChanged behavior. The following warning is displayed:
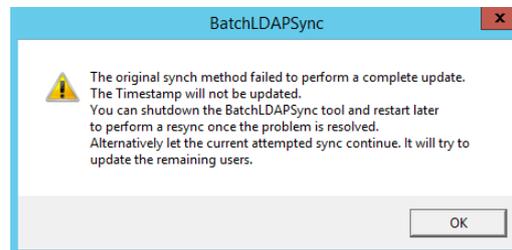
  If this occurs, you can:

  - Shut down the tool and restart it later to perform a synchronization when the problem has been resolved, *or*:

  - Allow the tool to attempt to synchronize the remaining users. The timestamp will not be updated, so all users changed since the previous run will have to be processed again the next time you run the tool.

- **First run with -silent and -whenchanged options**

  There is no need to specify `-whenchanged` on the first run; you are also recommended not to use `-silent` on the first run so that you can see the feedback from the tool on what has been processed.

- **No valid user accounts detected**

  If there are no users that require synchronization, and you do not have the **whenChanged** option selected, the tool displays a message similar to:

  ```
  Invalid user account IDs
  ```

  This means that there are no valid user account IDs to synchronize.

- **Permissions errors**

If you attempt to run the utility under a user other than the MyID COM user, you may see errors similar to the following:

```
Error occurred: 80070005
```

or:

```
Error occurred: 80004003
```

Exit the utility, then log in as the MyID COM user, and run the utility again.

5.6 Storing the NETBIOS name for a person

If systems require extra user information (for example, if your CA cannot determine the user correctly when requesting certificates – this may occur if you have multiple users with the same SAMAccountName in different domains, or if you are issuing certificates to a user who is not in the same domain as the CA), you may need to specify the NETBIOS name for the user.

You can choose to store the domain NETBIOS name for a user's domain. This NETBIOS domain name will then be prefixed to the account name, separated by a slash (\) when making certificate requests. This allows the certificate server to locate the correct domain for the user for whom the request is being made.

To set the **Force NETBIOS Name** option, see section *33.4*, *LDAP page (Operation Settings)*.

To ensure that MyID can view the domain\NETBIOS name, it must be able to access the configuration area of the directory. You must configure a BaseDN for your default directory within MyID. MyID automatically checks the configuration area for that BaseDN.

You must check whether MyID can import the NETBIOS name correctly. Import a person from the directory, save the person, then in the **View Person** workflow check the **Domain** item in the user's **Account** tab.

5.7 Setting up a configuration-only directory

If your directory's structure is too complex for MyID to read correctly, you may have to add a configuration-only directory to MyID using the **Directory Management** workflow. Set up a new directory with the same connection details as your existing directory, but set the BaseDN to the one where the configuration information is stored; this is typically `CN=Configuration`. This area of your directory may require different user authentication.

If your configuration information is *not* stored in `CN=Configuration`, you must create an LDAP attribute called `ADSConfigPrefix` and set it to the location of your configuration information.

Note: This directory is used to obtain configuration information only. In search screens, if you select the configuration-only directory for a user search, the result will not contain any users. Use the standard non-configuration directory for user searches.

For information on custom LDAP configuration, contact customer support quoting reference SUP-223.

5.8 Active Directory Deletion Tool

The Active Directory Deletion Tool allows you to synchronize Active Directory deletions ('Tombstone' markers). Use of this tool requires an administrator to configure a scheduled task which executes the tool periodically. This tool will not function with Global Catalogue instances, as they do not provide the necessary Tombstone deleted item information.

The active directory deletion synchronization tool is installed to the following location by default:

```
C:\Program Files (x86)\Intercede\MyID\Utilities\ADDeletionSync.exe
```

This is a command line tool that you can run on the MyID application server whenever you require it. It takes the following steps:

6 Connect to each of your configured Active Directory servers.

4. Checks for newly-deleted items on each of those servers.

5. Checks MyID for cardholders that match these deleted items.

6. Updates the matching cardholders accordingly.

    If the **Disable on removal from directory** option on the **LDAP** page of the **Operation Settings** workflow is set to **Yes**, the users are disabled in MyID, and their credentials cancelled, resulting in the revocation of their certificates.

To carry this out, the tool must run as a user with sufficient privileges to access the LDAP, and read and update the MyID database; you are advised to use a domain administrator.

You can run this tool on the command line, and (provided the user running the tool has sufficient privileges) it will update any new deletions in the Active Directory that are found in MyID. You are recommended to run the tool from the command line before setting up a scheduled task – the first run may encounter a large number of deletions in the database and it may take longer to process the list on this first run.

Note: The tool is not compatible with Global Catalogue Active Directory systems because they do not provide the Tombstone deleted item information needed to synchronize the MyID database.

6.1.1 Scheduled task repeat interval

Before configuring the scheduled task you should consider the repeat interval required. A longer interval will return more deleted records from the Active Directory and the task will take longer to execute, while a shorter frequency will result in fewer records being updated, but a finer grain of control over the synchronization.

We recommend that a 10 minute interval be considered initially, although when large numbers of deletions from Active Directory occur, the tool could end up running again while still executing from the previous timer. The frequency of the task should be monitored to ensure that the frequency of execution is meeting the needs of the system.

Things to consider when deciding how often to execute the task are:

- The number of deletions expected to be processed in each repeat interval.

- The required responsiveness of the whole system to deletions from Active Directory.

- The number of Active Directory servers which will be contacted each time the tool runs.

- The minimum interval for repeats is 1 minute, which can be safely used if deletions from Active Directory are infrequent.

6.1.2 Setting up a Scheduled Task

To set up a scheduled task, use the `ADDeletionSync.exe` tool in the `Utilities` folder that is part of your MyID installation. If you have installed MyID in the default location, this is:

```
C:\Program Files (x86)\Intercede\MyID\Utilities\
```

To set up a scheduled task:

1. Open the **Scheduled tasks** tool:

- In the Control Panel, open **System and Security > Administrative Tools > Task Scheduler**.

  or:

- From the Start menu, type schedule task into the **Search programs and files** box and select either **Task Scheduler** or **Schedule tasks**. (Both open the same tool.)

2. Click **Create Task**.

3. On the **General** tab:

   a) Type a **Name** for the task. For example, `Active Directory Deletion Synchronization`.

   b) Add a **Description** if required.

   c) Click **Change User or Group** and select a domain administrator.

   d) Under **Security options** select **Run whether user is logged on or not**.

4. On the **Triggers** tab:

   a) Click **New**.

   b) From the **Begin the task** drop-down list, select **On a schedule**.

   c) Under **Advanced settings**, set the following options:

      □ **Repeat task every** – set the check box, then from the drop-down list select your preferred repeat interval; for example, select **15 minutes**.

      □ Set the for a duration of option to **Indefinitely**.

      □ If you experience problems with slow directories or databases, you can set the **Stop task if it runs longer than** option and set a maximum duration.

      □ Make sure the **Enabled** box is selected.

5. Click **OK** to create the trigger.

6. On the **Actions** tab:

   a) Click **New**.

   b) From the **Action** drop-down list, select **Start a program**.

   c) Click the **Browse** button next to the **Program/script** field.

   d) Navigate to the `Utilities` folder that is part of your MyID installation. If you have installed MyID in the default location, this is:

   e) `C:\Program Files (x86)\Intercede\MyID\Utilities\`

   f) Select `ADDeletionSync.exe` and click **Open**.

   g) Leave the **Add arguments (optional)** and **Start in (optional)** fields blank.

   h) Click **OK** to add the action.

7. Check the **Conditions** and **Settings** tabs to ensure the settings meet with your company policies and procedures.

   You can use the default settings on these tabs.

8. Click **OK** to add the task.

9. If prompted, enter the password for the domain administrator.

The new scheduled task is now displayed in the Test Scheduler Library. If you need to edit the settings, you can double-click the task. If the task is set up correctly, you can close the Task Scheduler tool.

7 Certificate Authorities

MyID can integrate with a Certificate Authority (CA) provided by one of a number of vendors. A full list of the currently supported CAs is in the **_Installation and Configuration Guide_**.

You must install and configure the CA that you are going to use to issue and manage certificates before you install MyID. If you want to add support for a CA to an existing installation of MyID, you must modify your installation.

Note: Integration with a CA is optional. You can skip this section if you do not want to issue certificates through MyID.

Warning:	Instructions for configuring MyID to work with a specific CA are provided in the relevant **_Integration Guide_**, available from the product CD. This document provides only general instructions.

MyID supports certificates issued to hardware (written to smart cards or tokens) or soft certificates (stored in an individual's certificate store on the local machine). It may be possible to issue some certificates as both hard and soft certificates.

Normally, soft certificates are issued directly to the person to whom they relate, as that person must be logged on to the computer for the certificate to be written to the correct certificate store. MyID provides the facility for an operator to request a soft certificate on someone's behalf, save it to file, and then send it to the named person by any suitable method, such as email.

MyID automatically detects the presence of a Microsoft Certificate Services CA (if support was selected during installation). You must manually create a connection for all other CAs.

All certificate policies are initially disabled. You must manually enable the CA and the particular certificate policies that you want to issue.

7.1 Certificate refresh configuration

If you experience problems when collecting or updating cards, try increasing the **Certificate Refresh Threshold** option on the **Certificates** tab of the **Operation Settings** workflow to a higher value; for example, 45.

Increasing this value can help overcome performance issues related to the speed of the network or the speed of the certificate authority.

In the Self-Service Kiosk, for example, this problem may manifest when collecting a replacement card job with an error similar to:

```
One of the certificates that have been requested for you has failed to
issue. Please contact your administrator.
```

7.2 Connecting to a CA

You can edit an existing CA connection or create details for a new one. Configuring the certificates that can be issued is described in section *7.3*, *Enabling certificates on a CA*.

7.2.1 Recording a new CA

To create a CA connection:

1. From the **Configuration** category, select **Certificate Authorities**.

2. Click **New**.

3. Select the **CA Type** from the drop-down list.

   You can set the **CA Name** and **CA Description** for your CA.

   The rest of the options depend on the type of CA you are using.

   For information on setting the specific options for your CA, see the relevant *Integration Guide*.

4. Set the **Retry Delays** as a semi-colon separated list of elapsed times, in seconds.

   For example, `5;10;20` means:

   ◆ If the first attempt to retrieve details from the CA fails, a second attempt will be made after a `5` second delay.

   ◆ If this second attempt fails, the CA will be contacted again after `10` seconds.

   ◆ Subsequent attempts will be made to retrieve information every `20` seconds, until a response is received.

   If you want to limit the number of retry attempts, enter `0` as the last number in the sequence.

   The default is:

   `15;60;60;60;60;120;180;360;3600;86400;0`

   This retries after 15 seconds, then after a minute four times, then two minutes, three minutes, six minutes, an hour, 24 hours, then stops.

5. Click **Enable CA** to make the CA available in MyID.

6. Click **Save**.

7.2.2 Editing an existing CA

To edit details for an existing CA connection:

1. Select the CA connection from the list and click **Edit**.

2. You can change the **CA Description**, **Retry Delays** and clear or set **Enable CA**.

3. Click **Save**.

7.3 Enabling certificates on a CA

All certificate policies are detected when you add the CA to MyID, but they are all initially disabled. You can enable the specific policies you want to use.

To enable certificate policies for a CA:

1. From the **Configuration** category, select **Certificate Authorities**.

2. Select the configured Certificate Authority from the list.

3. Click **Edit**.

4. Make sure **Enable CA** is selected.

5. From the list of **Available Certificates**, select the Certificate Policy you want to work with.

6. To enable the certificate, click **Enable (Allow Issuance)**.

7. Edit the certificate policy options.

   The available attributes depend on the CA you are using. They may include: key length, duration, the certificate lifetime, whether the certificates can be issued to hardware (written to cards or tokens), as soft certificates (stored as a file on the computer), or both.

   See your CA integration guide for details.

8. Click **Save**.

Note: Changes made to certificate profiles do not take effect immediately, as the normal interval for MyID to poll for updates is 50 minutes. To force MyID to poll for changes immediately, you must manually restart the **eKeyServer** service, and then restart the **eCertificate** service.

7.4 Scheduled certificate revocation operations

MyID provides the ability to execute scheduled certificate request and revocation operations. This is typically used to perform regular maintenance tasks, such as automatically revoking certificates that have been suspended for a pre-configured length of time.

The detection and flagging of certificates to be revoked is typically performed by a stored procedure. The submission of these requests to the Certification Authority relies on processes carried out automatically by the MyID certificate service (eCertificate Server), which is set up during installation.

To set MyID to revoke suspended certificates after a given time period:

1. From the **Configuration** category, select the **Operation Settings** workflow.

2. Click the **Certificates** tab.

3. Set a value for the **Suspend to revoke period** option.

   Update the value to the number of days a certificate must be suspended before it is revoked. By default, this entry has a value of zero, which means that suspended certificates will not be automatically revoked.

7.5 Revoking timed-out certificates

MyID revokes any certificates that have timed-out when waiting for issuance or deferred issuance.

To set the timeout period for certificates:

1. From the **Configuration** category, select **Operation Settings**.

2. Click the **Certificates** tab.

3. Set the following options:

   - **Certificate Timeout For Deferred Collection** – for certificates that are waiting for deferred collection, the number of minutes before a certificate will be revoked. If the certificate is not collected within this time limit, the certificate is revoked.

   - **Certificate Timeout For Issuance** – for certificates that are being issued, the number of minutes before a certificate will be revoked. If the device fails to complete the issuance procedure within this time limit, the certificate is revoked.

4. Click **Save changes**.

7.6 Certificate renewal

If a certificate policy is set to **Automatic Renewal**, MyID creates a job to renew the certificate when it comes within a specified number of days of expiry. The number of days is specified in the `TaskCountdown` table; see section *14.3.1*, *Triggering the notification* for details.

When MyID performs a certificate renewal, a re-key will also take place (a new key will be generated, and the new certificate issued against the new key). If any changes to user data that appears on the certificate have taken place, the updated user data will appear on the new certificate.

If the certificate renewed is also present on any other devices, an update job is automatically created for these devices so that they will recover a copy of the new certificate.

Users can collect certificate renewal jobs in the following ways:

- Using the Self-Service App.

- Using the Self-Service Kiosk

- From a hyperlink in an email notification that launches MyID Desktop at the **Collect My Updates** workflow.

- From the **Collect My Updates** workflow in MyID Desktop.

The behavior of archived and non-archived certificates is different, and also the behavior of devices with managed containers (such as PIV cards) and non-managed devices.

For non-managed devices:

- Renewed archived certificates are placed in a new container on the device, and the credential profile historic certificate configuration determines whether to remove any previous certificates from the device so that the number of historic certificates does not exceed the configured limit.

- Non-archived certificates that have been renewed are removed from the device automatically after the new certificate is issued.

For managed devices:

- Archived certificates that have been renewed are overwritten by the new certificate and automatically recovered to historic containers according to the credential profile configuration.

- Non-archived certificates that have been renewed are overwritten by the new certificate and are therefore no longer present on the device.

- Historic archived certificates may be removed from the device so that the number of historic certificates does not exceed the configured limit in the credential profile.

7.7 Superseding certificate policies

You can supersede a certificate policy and assign a replacement policy to be used in its place for all future purposes.

Note: You cannot supersede a certificate policy if any credential profile is currently being edited. To supersede a policy, the process must have exclusive access to the credential profiles so that it can make any necessary changes.

To supersede a certificate policy:

1. From the **Configuration** category, select **Certificate Authorities**.

2. From the **CA Name** list, select the certificate authority that contains the certificate policy that you want to supersede.

3. Click **Edit**.

4. From the **Available Certificates** list, select the certificate policy that you want to supersede.

Note: A certificate policy must be enabled before you can supersede it.

5.   Click **Supersede**.

6.   Select the certificate authority containing the certificate policy you want to use as a replacement.

A list of the available enabled certificate policies appears.

Note: Do not select a policy that you have already superseded during this session in the **Certificate Authorities** workflow. Superseded certificate policies are not removed from the list of available policies until you click **Save** on this workflow to commit your changes.

7.   Select the certificate policy you want to use as a replacement.

8. Click **OK**.
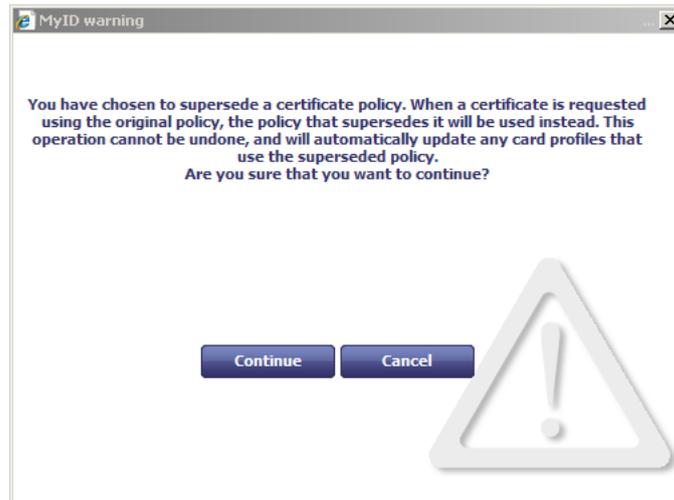
9. On the warning dialog, click **Continue**.

Warning:	After you click **Save** on this workflow, you cannot undo this action. Once you have superseded a certificate policy, it is permanently disabled, and you will never be able to use it again with this installation of MyID.

10. Click **Save**.

Note: You must click **Save** to commit the changes. If you click **Cancel** instead, the policy will not be superseded.

The certificate policy is now superseded. All credential profiles that used the superseded policy are updated to use the replacement policy. All jobs that contained the superseded policy are updated to use the replacement policy. In short, MyID will no longer issue any certificates based on the superseded certificate policy, but will issue certificates based on the replacement certificate policy instead.

Cardholders can continue to use the certificates that were issued using the superseded policy, but if they update their cards to the latest version of the credential profile, the superseded certificate is replaced.

7.7.1 Recovering superseded certificates

If you attempt to use the Recover Certificates workflow to recover a certificate that has been superseded, the recovery storage options are taken from the replacement certificate policy, not the original certificate policy.

7.7.2 Troubleshooting

▪ **Person already exists error**

You may experience an error similar to the following when saving your changes:

```
Error: This person already exists on the database.

-2147217873 BOL ComException catch handler for function : UpdateCA
iDispatch error #3119
Function : Add, catch handler. Error :
iDispatch error #3119
Violation of PRIMARY KEY contraint 'PK_CertificateProfiles'. Cannot
insert duplicate key in object 'dbo.CertificateProfiles'.
```

If you experience this error, make sure that you have not selected a replacement policy that is already used on the same credential profile as the policy being superseded; this situation would result in two certificates from the same policy being specified on the same credential profile, which is not possible.

▪ **Credential profile locking**

The following messages may appear when you are attempting to supersede a certificate:

◆ You are attempting to supersede a certificate while a credential profile is being edited. Please try again later.

◆ Credential Profile Lock Warning. You are not permitted to perform the operation at this time. A lock is currently active on credential profiles.

When you edit a credential profile, that credential profile is locked so that no other operators can edit it while you are working on it. Similarly, when you are editing any credential profile, no operator can supersede a certificate. When you finish editing the credential profile, the lock is released. However, if your system experiences a failure and your client closes unexpectedly, this lock is not released, preventing any operator from editing that credential profile or superseding any certificates; you must wait 20 minutes for the lock to be released automatically.

7.7.3 Viewing superseded certificate policies

If a certificate policy has been superseded, this is shown in the **Superseded** column on the Select a CA screen of the **Certificate Authorities** workflow.

If a credential profile has been updated due to a superseded certificate policy, you can see the details by clicking the **History** button on the Select Credential Profile screen in the **Credential Profiles** workflow.

8 Applets

Note: Using applets is optional. You can skip this section if you are not using Java-enabled smart cards.

Applets are small programs that execute on a smart card to provide applications such as electronic purses, password management and other functions that need to be run within the secure, local context of a smart card. MyID can manage the lifecycle of smart card applets, including loading, updating and deleting. At present, MyID supports applets that use GlobalPlatform Java keys.

Note: GlobalPlatform keys were previously known as Open Platform keys.

If your organization is using applets as part of its implementation of MyID, you must:

- Put the applet in a location accessible to the workstation you are using
- Be using Java-enabled devices in your implementation (see the appropriate *Integration Guide* for further information)
- Enter the GlobalPlatform keys provided by the card vendor – these are sometimes referred to as factory keys
- Create your organization's own GlobalPlatform keys (customer keys) to increase security
- Enter details of the applets and upload the applet files to the MyID server
- Specify the applets that are to be written to cards that are issued with each credential profile (see section *12, Managing Credential Profiles*)

From within the **Applets** category, you can:

- Enter customer and factory GlobalPlatform keys
- Add an applet to the list of those available to MyID
- Edit details of an existing applet
- Remove an applet from the list of those available

8.1 GlobalPlatform keys

Note: Your card vendor will provide you with the factory GlobalPlatform keys that enable MyID to work with your cards.

GlobalPlatform Keys and related specifications and protocols are defined in the GlobalPlatform Card Specification available at http://www.globalplatform.org/.

At manufacture time, the card is given a key set as defined by SCP1/SCP2/SCP03 (Secure Channel Protocol).

For MyID to communicate with the card using SCP, it has to know the key set. You need the GlobalPlatform keys to:

- Add or remove applets on the card.
- Perform device specific prepersonalization (for example, loading PKI applets onto a card during issuance).
- Change the 9B key on some PIV cards (for example, Oberthur PIV cards).
- Change the GlobalPlatform Keys to customer keys.

Note: These keys may be known by third parties and, unless you are just evaluating or testing MyID, you should enter a set of keys specific to your own organization (customer keys).

It is also possible that the card manufacturer has agreed to provide cards with a more secure diversified keyset. In this case, you will need to use the Key Ceremony option in the **Manage GlobalPlatform Keys** workflow to import the factory master key securely.

When you issue a card through MyID, the factory keys are used to authenticate to the card in order to manage applets on the card. You can issue a Java card through MyID without having entered the factory keys if no applet operations are required (for example, if you are working with certificates and the PKI applets are already installed).

If a customer key has been entered into MyID the factory keys on the smart card are then replaced by your own customer keys when the card is issued, which secure the card.

Canceling a card removes your customer keys and reinstates the factory keys: this enables the card to be re-used with this or another installation of MyID. Because the customer keys are specific to the installation of MyID in which they were stored, cards issued using customer keys cannot be canceled using another system.

Warning:	You must cancel any cards issued using customer GlobalPlatform keys before you uninstall MyID or you will not be able to use the cards again.

8.2 Check configuration setting

1. From the **Configuration** category, select **Security Settings**.

2. Click the **Device Security** tab.

3. Make sure the **Enable Customer GlobalPlatform Keys** option is enabled. If it is disabled, click the box to toggle between the two states.

   ✅ **Enabled**   ❌ **Disabled**

   If you do not have the **Enable Customer GlobalPlatform Keys** option set, you will be unable to write customer GlobalPlatform keys to your cards.

4. If you have changed anything, click **Save changes**. Otherwise click **Cancel**.

8.3 Manage GlobalPlatform keys

Warning:	You cannot change the keys that you save using the **Manage GlobalPlatform Keys** workflow.
Warning:	If new keys are imported to or generated on the HSM during this workflow, you should take a new backup of the HSM. Keys stored on the HSM are business critical data.

The **Manage GlobalPlatform Keys** workflow contains two pages – one for entering details of **Customer** keys and the other for **Factory** keys.

Note: You must complete and save the information for one keyset before re-entering the workflow to record information for the other keyset.

▪ Factory keys: you can enter multiple sets of factory keys, identified by the names you give them. Factory keys can be deleted but not modified.

▪ Customer keys: you can only enter a single set of customer keys at a time per **Key Algorithm**. You can delete old keys and add a new set; cards issued with the previous customer keys will still work, but all cards issued in the future will use the new customer key.

Intercede recommends you use HSM generated diverse customer keys for security. You can use any diversification algorithm for your customer keys; the diversification algorithm does not need to match the one used for the factory keys.

You can use diverse customer keys even if the factory keys are static.

The **Key Algorithm** must match the secure channel used for the factory keys. If you are issuing multiple types of GlobalPlatform cards (or SIMs or other form factors) using secure channel types associated with different key algorithms, you need to configure multiple Customer GlobalPlatform keys. For example, you will need to configure 2DES GP customer key for those using the SCP01 channel type, and an AES128 for those using the OT-SCP03 channel type.

Secure Channel Type	Key Algorithm
SCP01/SCP02	2DES
OT-SCP03	AES128
SCP03	AES128/AES192/AES256 (depends on card type)

Note: If you are evaluating or testing MyID, you may choose to use the provided factory keys only. You can return to this workflow and add customer keys later.

Note: The HSM options in the **Manage GlobalPlatform Keys** workflow are available only if you selected an HSM (in GenMaster) to store your MyID database keys. See the *Installation and Configuration Guide* for details.

8.3.1 Entering factory (vendor) keys

1. From the **Applets** category, select **Manage GlobalPlatform Keys**.

   The **Factory** page is displayed.

   Note: You can define multiple sets of factory keys – if one already exists, click **New** to create a new set. If multiple factory keys are defined for the same credential, the most recently entered factory key will take precedence.

2. Type a **Name** and a **Description** for the key set.

3. In **Key Type**, select either:

   ◆ **Static** – the key used is the same throughout.

   ◆ **Diverse** – the keys use a diversification algorithm.

   Different options appear based on your choice of **Key Type**.

4. In **Credential Type**, select the type of card that you are using. The contents of this list are based on the choices made when MyID was installed. The factory key you are entering will only apply to this credential type.

5. In **Secure Channel**, select the secure channel used to communicate with the cards.

   See the *Smart Card Integration Guide* for details of which secure channel your cards use.

6. You can optionally specify a range of card serial numbers in **Start Serial Number** and **End Serial Number**.

- ◆ The length of the **Start Serial Number** and **End Serial Number** must be the same – and are both set at a maximum of 50 characters (although they will normally be shorter).

- ◆ The numbers in **Start Serial Number** and **End Serial Number** define an inclusive range (they *are* the lowest and highest permitted numbers).

If you specify a serial number range, you can define multiple factory GlobalPlatform keys for the same credential type, each applying to different serial number ranges.

If you do not specify a range, the keys you enter will be used for all cards of the specified type.

7. Type the default factory SOPIN in the **Factory SOPIN** field.

Entering the factory SOPIN is optional – if not specified, the default SOPIN configured in the system for the credential type is used.

8. Enter a **Version** for the key set.

This version number should be available from your card manufacturer and will be a number between 0 and 127 or 255. A version of 255 should normally be used for cards delivered with an Initial Keyset.

9. Enter the value provided by the card vendor in **Card Manager AID**. This is the application identifier for the GlobalPlatform Card Manager applet.

Note: Take care when entering the AID. Some cards have very similar (but different) values.

10. If you selected **Static** keys, type the provided **MAC Key**, **Encryption Key** and **Key Encryption Key** values into the fields.

- ◆ The **MAC Key** is the Secure Channel Message Authentication Code Key (S-MAC).

- ◆ The **Encryption Key** is the Secure Channel Encryption Key (SENC).

- ◆ The **Key Encryption Key** is the Data Encryption Key (DEK).

11. If you selected **Diverse** keys:

a) Select the **Diversification Algorithm** from the list available.

The algorithm depends on the cards you are using. For example, GemPlus PIV cards use `Diverse1`, while Oberthur PIV cards use `Diverse3`.

Note: You have to obtain this information from the card vendor.

b) Select one of the following options:

- ▫ **Master Key** – type the key into the **Master Key** field.

- ▫ **HSM Label** – type the label of an existing HSM-resident master key into the **HSM Label** field.

- ▫ **Use Key Ceremony** – once you click **Continue**, you enter the parts of the transport key and encrypted master key in a key ceremony.

- ▫ **Import Keys from File** – once you click **Continue**, you import the key from an `XMLenc` format file.

12. If you are using a key ceremony or importing keys from file, you can specify the attributes of the key. These determine the possible uses of the key.

- ◆ **Data Encryption Key** – the key is used to encrypt data.

- ◆ **Allow Signing Operations** – the key can be used for signing operations.

- ◆ **Exportable** – the key can be exported after it has been imported. See section *8.3.4*, *Exporting keys* for details.

- ◆ **Key Encryption Key** – the key can be used to encrypt keys.

- ◆ **Allow Derivation** – the key can be used to derive individual keys.

Note: The keys entered must match the keys on the cards you intend to use – attempting to authenticate to a card with incorrect keys will eventually cause the card to lock permanently.

Note: If you need help in deciding which attributes to use, contact Intercede customer support quoting reference SUP-96.

13. Click **Continue**.

14. If you are using the **Use Key Ceremony** or **Import Keys from File** options, you must now provide the keys. See section *8.3.2 Using a key ceremony* or section *8.3.3 Importing keys from a file*.

8.3.2   Using a key ceremony

1. If you have installed support for an HSM, you are asked whether you want to store the key in the database or on the HSM.

   Note: Intercede recommends using an HSM if one is available as this offers additional protection to the keys.

2. If you have previously stored a transport key using the **Key Manager** workflow, you can select this key from the **Existing** list, or select **New** to enter a new key.

   See section *17.2*, *The Key Manager workflow* for details of storing a transport key using the **Key Manager** workflow.

3. If you are using a new transport key, in the **Key Ceremony** dialog, enter the first part of the transport key.
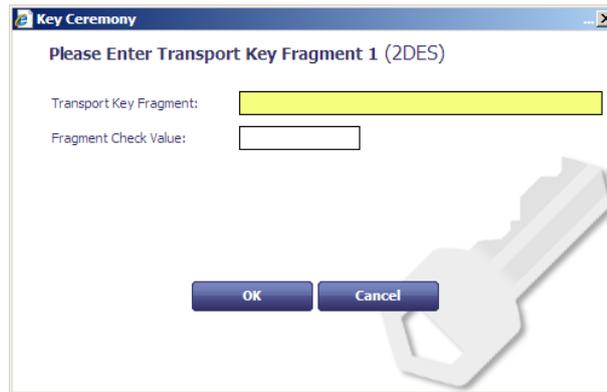
You can optionally enter the **Check Value** to ensure that you have entered the transport key fragment correctly. Check values are usually provided for each fragment by your card vendor.

If you are using a new transport key, it must be the same type as the new master key. The key type is displayed in the Key Ceremony dialog; for example, **(2DES)**.

4. Click **OK**, then enter the second and third parts of the transport key.

5. Enter the encrypted master key.

You can optionally enter the **Check Value** to ensure that you have entered the encrypted master key correctly.

6. Click **OK**.

8.3.3 Importing keys from a file

If you chose to import keys from a file:

1. Select the Key Information File in the file dialog.

The file must be in `XMLenc` format.

The file must contain information on the transport key used to encrypt the file; the system checks the contents of the `<ds:KeyName>` node in the XML import file against the names of the transport keys in the database, and against the Key Check Values (KCVs) of the keys' contents. If it finds a match against either the name or the KCV, it decrypts the key from the XML file.

2. Click **Open**.

The key is now added to the database or HSM.

8.3.4 Exporting keys

If you have set the key's attributes to allow exporting, you can export a key to an `XMLenc` format file, encrypted using a transport key. You can use this system to transfer a GlobalPlatform key from one MyID system to another.

1. From the **Applets** category, select **Manage GlobalPlatform Keys**.

2. Select the key you want to export.

3. Click **Export**.

4. Select the transport key you want to use to encrypt the key, then click **OK**.

5. Type the name of the XML file to which you want to save the key, then click **Save**.

   You can now import this GlobalPlatform key into another MyID system. You must have the same transport key on the target system as on the source system.

8.3.5 Deleting factory (vendor) keys

1. From the **Applets** category, select **Manage GlobalPlatform Keys**.

2. Select the key you want to delete from the **Select GlobalPlatform Keys** drop-down list.

3. Click **Delete**.

8.3.6 Entering customer (local) keys

1. Select the **Applets** category and then the **Manage GlobalPlatform Keys** workflow.

2. Click the **Customer** tab.

   The **Customer** page is displayed.
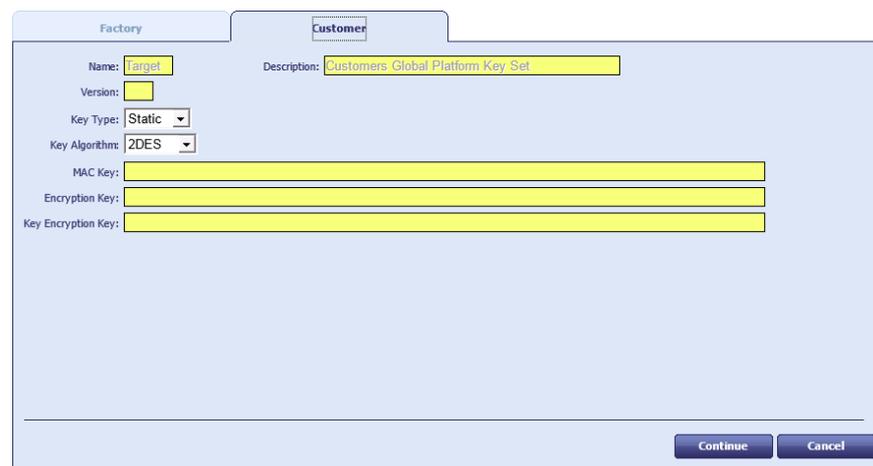
Note: You can define only a single set of local keys at one time per **Key Algorithm**; for example, if you are using both SCP01 cards and OT-SCP03 cards, you can define one 2DES customer key (for the SCP01 cards), and one AES128 customer key (for the OT-SCP03 cards). **Name** and **Description** cannot be changed. You can delete existing keys and enter a new key: cards issued with the previous customer keys will still work, but all cards issued in the future will use the new customer key. See section *8.3.7*, *Deleting customer (local) keys*.

3. Enter the **Version** of the key set.

This must be a different value from the version entered for the factory keyset. Also, if you have specified a factory keyset version of 255, you cannot use a customer keyset version of 1. The customer key version must be between 1 and 127 and not match the key version of any factory keys that use this algorithm.

For example, if an SCP01/SCP02 card has factory key version 255, and another SCP01/SCP02 card has a factory key version 3, a 2DES customer key can be created with key version 99. This is a number between 1 and 127, which is not 1, not 3 and leaves other lower key versions free for any other SCP01/SCP02 cards to use later.

4. In **Key Type**, select either:

   ◆ **Static** – the key used is the same throughout.

   Static customer keys are not recommended, and cannot be stored on an HSM.

   ◆ **Diverse** – the keys use a diversification algorithm.

   Different options appear based on your choice of **Key Type**.

5. Select the **Key Algorithm** to be used for the cards.

   For example, for cards that use the SCP01 channel, select **2DES**. For cards that use OT-SCP03, select **AES128**.

6. If you selected **Static** keys, type the provided **MAC Key**, **Encryption Key** and **Key Encryption Key** values into the fields.

   ◆ The **MAC Key** is the Secure Channel Message Authentication Code Key (S-MAC).

   ◆ The **Encryption Key** is the Secure Channel Encryption Key (SENC).

   ◆ The **Key Encryption Key** is the Data Encryption Key (DEK).

7. If you selected **Diverse** keys:

   a) Select the **Diversification Algorithm** from the list available.

   b) Select one of the following options:

      ▫ **Automatically Generate Key In Database** – this option generates a key in the database to be used for your cards.

      ▫ **Automatically Generate Key In HSM** – this option generates a diversification master key in the HSM, and is the most secure option.

      ▫ **Master Key** – type the key into the **Master Key** field.

      ▫ **HSM Label** – type the label of an existing HSM-resident master key into the **HSM Label** field.

      ▫ **Use Key Ceremony** – once you click **Continue**, you enter the parts of the transport key and encrypted master key in a key ceremony. See below.

      ▫ **Import Keys from File** – once you click **Continue**, you import the key from an XMLenc format file. See below.

   Note: For a production system Intercede strongly advises that you use a diversified customer key. This causes a unique key to be calculated for each card.

8. If you are automatically generating a key either in the database or the HSM, using a key ceremony, or importing keys from file, you can specify the attributes of the key. These determine the possible uses of the key.

   ◆ **Data Encryption Key** – the key is used to encrypt data.

   ◆ **Allow Signing Operations** – the key can be used for signing operations.

- ◆ **Exportable** – the key can be exported after it has been imported. See section *8.3.4*, *Exporting keys* for details.

- ◆ **Key Encryption Key** – the key can be used to encrypt keys.

- ◆ **Allow Derivation** – the key can be used to derive individual keys.

9. Click **Continue**.

10. If you are using the **Use Key Ceremony** or **Import Keys from File** options, you must now provide the keys. See section *8.3.2 Using a key ceremony* or section *8.3.3 Importing keys from a file*.

8.3.7   Deleting customer (local) keys

You can use the **Manage GlobalPlatform Keys** workflow to delete a customer key; this allows you to enter a new customer key. Cards issued with the previous customer key will still work, but all cards issued in the future will use the new customer key.

To delete a customer key:

1. Select the **Applets** category and then the **Manage GlobalPlatform Keys** workflow.

2. Click the **Customer** tab.

    The **Customer** page opens.
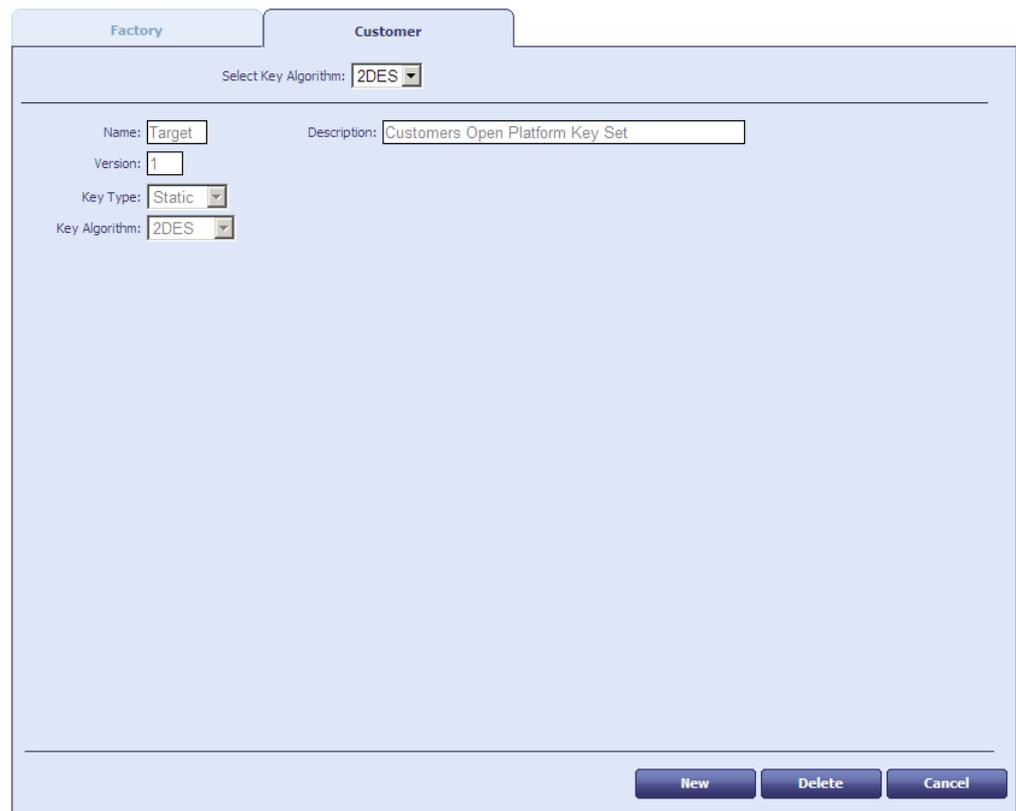
If a key is already present, the **Delete** button is available.

3. If you want to delete the customer key, click **Delete**.
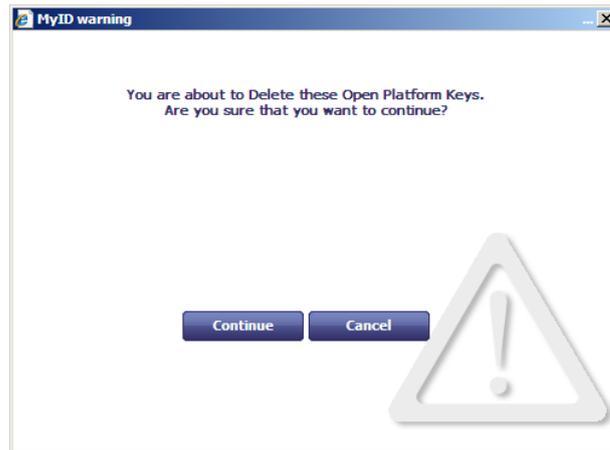
4. Click **Continue** to delete the keys.

   You can now start the workflow again to enter a new customer key.

8.4 Managing applets

Before applets can be issued to devices, you must enter their details into MyID. You can do this using the **Manage Applets** workflow.

Note: You must obtain values for **Load File AID** and **Executable AID** from the vendor or developer of the applet: these are mandatory fields within MyID. You may also need values for **Application AID** and **Application Privileges**: these are not mandatory fields within MyID but may be needed for the applet to function correctly.

There may be some restrictions on the applets that can be issued. For example, the capacity of the devices you are using affects the size of applet that can be written to them. For further information, see the appropriate *Integration Guide* and the vendor's own documentation.

8.4.1 Add an applet

To add an applet to the list of those available for issue within MyID:

1. Select the **Applets** category and then the **Manage Applets** workflow.

2. Click **New** to create a new applet record.

   There are three read-only fields on this page, which are populated when the record is saved:

   ◆ **Memory Requirements** initially displays `Unset`. It will show the size of the file referenced in **File to upload** in bytes.

   ◆ **Created Date** is the date that details of this applet are added to MyID.

   ◆ **Issued Date** is the date that the latest version of this applet is added to MyID – the first date that it could be issued.

3. In **Applet Name** and **Applet Description**, enter information that will allow you to identify this applet when editing, updating, or selecting it for inclusion in a credential profile.

4. Indicate whether the applet is to be enabled.

   ◆ Select **Enabled** to enable this applet – it is included in the list of applets for selection for a credential profile and when updating a card.

   ◆ Leave **Enabled** clear to prevent the applet being issued.

5. Enter the **Version** of this applet.

6. Indicate whether this applet can be removed from a card when it is cancelled by selecting or clearing **Removable**.

7. Enter the name of the **Vendor** of this applet.

8. Select the **File to upload**. Click **Browse** and navigate to the applet. Select the appropriate file and click **Open**.

    Note: The applet file is expected to be in IJC format.

9. Enter the **Load File AID** and **Executable AID** exactly as provided.

10. If provided, enter values for the **Application AID** and the **Application Privileges**.

11. Select the appropriate **Transport key** from the list if required:

    ◆   If the applet file uploaded is unencrypted, do not select a **Transport key**.

    ◆   If the supplied applet file is encrypted, select the appropriate **Transport key** (required for the applet to be decrypted) from the list. This **Transport key** must have been previously entered in the **Key Manager** workflow.

12. Click **Save**.

8.4.2   Edit an applet

This option allows you to correct any mistakes you made when entering information but does not allow you to upload a new file.

If you want to make changes to an entry for an existing version of an applet:

1. Select the **Applets** category and then the **Manage Applets** workflow.

2. Select the applet record you want to change and click **Edit**.

3. Make all necessary changes.

    You can change all of the information you entered when the record was created (see section *8.4.1*, *Add an applet*).

4. Click **Save**.

8.4.3   Upgrade an applet

This option allows you to make a later version of an applet available for issue and to specify whether credential profiles and cards using the earlier version should be updated.

If you want to upgrade to a later version of an applet:

1. Select the **Applets** category and then the **Manage Applets** workflow.

2. Select the applet record you want to change and click **Upgrade**.

3. Enter the new version number for the applet.

4. Click **Browse** and navigate to the applet. Select the appropriate file and click **Open**.

5. Select:

    ◆   **Disable old version** to disable previous versions of this applet.

    ◆   **Update credential profiles** to automatically update any credential profiles using this applet to issue the new version.

    ◆   **Update credentials** to create a job that updates any credentials that are currently using this applet to use the new version.

6. Click **Save**.

9 Designing Card Layouts

Note: You can use MyID without specifying any card layouts, so you may skip this section if you are not printing smart cards.

You can specify the content and layout of the information to be printed on a smart card when it is issued. Depending on your organization's requirements, you may need to specify multiple card layouts to enable different types of card or the different roles of cardholders to be visually distinguished. You may also need to print different information on the cards for the different roles held by cardholders.

For example, you may specify layouts that:

- Distinguish temporary cards – for visitors or contractors
- Identify cards belonging to individuals with a high security clearance
- Identify designated individuals, such those with Fire Officer responsibilities
- Incorporate the name of a designated contact for temporary staff

You can define multiple layout templates and you can associate each template with one or more credential profiles and each credential profile with one or more templates. For example:

- If every card is to look identical, you need only one card layout template that you can associate with every credential profile.
- If every role has its own credential profile and you want to be able to distinguish between the roles, create a card layout template for every profile.
- If you are using the same profiles for both permanent and temporary staff but need to be able to visually distinguish between them, you can either:
    - Create two layouts (one for permanent and one for temporary staff) and associate both with each credential profile.
    - Create two layouts for each credential profile.

Each template specifies the layout for one side of a card. To specify a layout for the reverse of a card, save it using the same name as the front with a `_back` suffix. For example, if the front layout is called `TempStaff`, save the reverse as `TempStaff_back`.

Note: The names given associate the correct reverse layout with the selected front layout, but you must still set your printer to duplex mode when printing the cards.

You can use the **Default Card Reverse Layout** configuration option (on the **Devices** page of the **Operation Settings** workflow) to specify a default layout to use for the reverse of any card. If a card has no defined reverse layout, if this configuration option contains the name of a valid card layout, the layout is used for the reverse of the card.

You can specify the appearance and position of both text and images. The content of these elements can be either:

- Static
    - Text that will be printed on every card, exactly as entered in the template. For example, your organization's name or address.
    - Standard images held on the server. For example, you may want to include your organization's logo or a background image for your card.
- Dynamic
    - Text held in the database, which may vary from card to card. For example, the card's serial number or the surname of the holder.
    - Images referenced in the database and associated with the cardholder. For example, you may want to print the holder's photograph or signature on the card.

9.1 Restricting access to card layouts

If the operator who creates a card layout belongs to a group that has a restricted set of available roles, the card layout will be available *only* to operators who have one of those roles.

If the operator who creates a card layout belongs to a group that has an unrestricted set of available roles (that is, the **Amend Group** workflow displays **0 Role(s)** in the **Roles** box) the card layout is made available to *all* existing roles.

Group:	Department of Education
Description:	
Roles:	0 Role(s)
Default Roles:	0 Role(s)
Enabled:	Enabled
Reason:	Revocation (other) (revoke)
Reason Detail:	

Note: If you subsequently add new roles to the system, they will not automatically inherit access to any card layouts. You can provide access to new roles by having an operator belonging to a group with unrestricted roles opening the card layout and saving it again.

Any initial card layouts installed by MyID (for example, the standard PIV layouts) are not subject to these restrictions, and are available to all roles; note, however, that if you edit these layouts, when you save them they will be subject to the same restrictions as other layouts.

9.2 Configuring the image location

Static images for card layouts (as inserted by the **Insert user image** ▨ button) are stored on the MyID web server. You must set the following configuration option:

- On the **Video** page of the **Operation Settings** workflow, set **Image Upload Server** to the name or IP address of the MyID web server.

If you do not set this option, the images will not appear correctly.

- **IKB-50 – Resolving host names**

  When obtaining the images for a card layout, MyID needs to know the location of the server on which the images are stored. The **Image Upload Server** configuration option contains the name of the server; however, this configuration option may contain an external URL used by clients and may not be resolvable on the MyID server, resulting in missing images.

  As a workaround, you can add an entry to the `hosts` file on the server hosting the MyID Web Service.

  For example, if the **Image Upload Server** configuration option contains `myserver.example.com`, which *should* resolve to the same server as the MyID Web Service, add the following lines to the following file:

  ```
  C:\Windows\System32\drivers\etc\hosts

  127.0.0.1  myserver.example.com
  ::1        myserver.example.com
  ```

9.3   Creating, saving and deleting layouts

You can create a completely new layout or base a new layout on an existing one. You can also open an existing layout to make changes to it.

Toolbar buttons used in this section:

Load – opens an existing layout for editing

Save – saves the current layout

Save As – save a layout using a different name

Delete – delete an existing layout

From the **Configuration** category, select the **Card Layout Editor** workflow.

The **Card Layout Editor** is displayed. Most of the page is taken up with the editing area, which opens a blank template, showing the position of the chip.
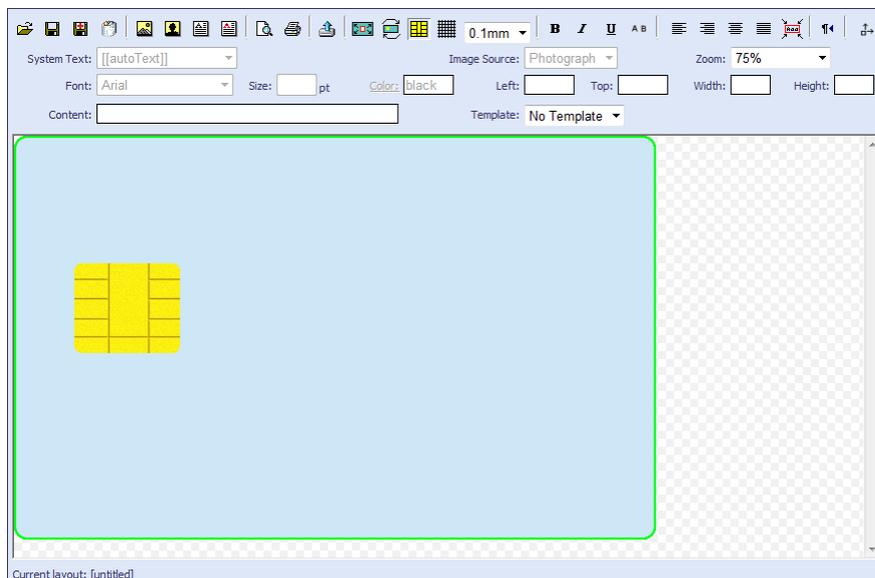
- If you are creating a layout that is *not* based on an existing layout, click **Save** and give the layout a name.

  Note: Make the name meaningful. If you are associating more than one layout with a credential profile, the operator will have to decide which to use when requesting or issuing a card.

  Note: Before you start to add text or images to your layout, make sure that the orientation of the card is correct. See section *9.4.1*, *Rotating the card*, for instructions.

- To make changes to an existing template or to base a new template on an existing one:

  a) Click the **Load** button on the toolbar and select the template from the list displayed. Click **Load**.

  b) Make any required changes.

  c) Either replace the existing template or save a new one:

    ▫ To save the template using a new name, click **Save As** and type a new name for the template. Click **Save**.

    ▫ To save changes to an existing template, click **Save**.

![intercede logo]

- To delete a layout, click the **Delete** button and select the template to delete from the list displayed. Click **Delete**.

9.4 Using the layout tools

Layout tools allow you to position elements precisely on the card template. These tools apply to the whole card layout.

The following toolbar buttons and options are described in this section:

Rotate – rotates the card through 90˚

Show chip – toggles the display of the chip

Show grid – toggles the display of a grid to help with positioning

Snap to – snap objects placed on the layout to the intervals specified
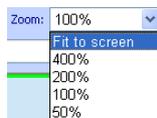
Zoom – enlarge or reduce the layout display

9.4.1 Rotating the card

Each time you click **Rotate**, the orientation of the card rotates 90˚ clockwise. Any text or images that you have placed on the layout do not rotate, even if that means they no longer fit on the surface of the card.

If you have rotated the card in error, click the **Rotate** button until the card is back to its starting position.

Note: Rotate the card with the chip showing, even if you are going to work on your design with it hidden, to make sure that you have the correct orientation.

9.4.2 Showing the chip

Click the **Show chip** button to toggle the display of the chip:

- If you are specifying a layout for a card that incorporates a chip, it is helpful to display the chip while you are working to make sure that you do not place important elements over it.

- Hide the chip if you are specifying the layout for a card that does not include a chip or for the back of a card with a chip.

9.4.3 Showing the grid, snapping elements and zooming

Show grid, **Snap to** and **Zoom** help you to position elements accurately in the space available. These options do not affect any objects already present in the layout.

- Click **Show grid** to toggle the display of a grid on the card's surface. The grid is marked in 1 mm intervals, with measurements from the top left corner shown in centimeters. The grid can help with alignment and also when following a design that specifies the positioning of elements.

- Select a value in the **Snap to** drop-down list to restrict the placement of elements to the intervals shown. The top-left corner of the image or the text box will be snapped to the grid at the intervals specified.

    Note: If you move an existing object when **Snap to** is switched on, it will snap to the interval specified.

- Use the **Zoom** setting by selecting a value from the drop-down list to decide how much of the card layout you want to be visible in the editing area.

9.5 Images and backgrounds

You can include either static or dynamic images as part of a card layout. These can be in either JPEG or GIF format.

- If you are using an image as background, it does not have to be the correct size but must be the correct aspect ratio.

- To set a background color for a card, use an image that is a single block of the required color.

The following toolbar buttons and options are described in this section:

	Insert picture – inserts a static image.
	Insert user image – inserts an image from the cardholder's record.
	Upload image – static images must be uploaded to the web server before they are available for selection.
	Fit image to card – resizes the selected image to fit the height or width of the card
Image Source: Photograph	**Image Source** – choose which user image to use from the cardholder's record.
or	**Maintain Aspect Ratio** – choose whether the aspect ratio of the image is retained when the card layout is printed.
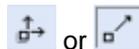
9.5.1 Uploading images to the web server

You can upload images at any time but if you have developed a library of static images to use when specifying card layouts, you can upload them all before the process begins.

Note: Give the images meaningful filenames as they are displayed when you are selecting an image to include on your layout.

1. Start the **Card Layout Editor** workflow.

2. Click the **Upload image** button.

3. Click **Browse** to locate the file you want to upload.

4. Select the file and click **Open**.

   A message is displayed stating that the file has been uploaded.

9.5.2 Specifying a background

1. Click **Insert picture**.

2. Double-click the image you want to use in the list of images displayed.

3. If the image is not in the top left corner of the card outline, move it into position. Place your mouse over the image and the cursor changes to a four-headed arrow. Click and drag the image to the correct position.

4. Re-size the image if necessary.

   - If the image is too large for the card outline, click **Fit to content**.

   - If the image is too small for the card, place your mouse over the small box at the bottom right of the red border to the image and drag down and right to enlarge the image.

   - Hold down the CTRL key and drag the resizing box to change the aspect ratio of the image.

5. Move your image to the back.

   Right-click the image and select **Send to back** from the menu displayed.

9.5.3 Fitting an image to a card

If you want to expand an image to the full width or height of the card, select the image then click **Fit image to card**.

Note: Be careful if your organization has placed restrictions on the size of images to be printed on the card.

Before selecting **Fit image to card**	After selecting **Fit image to card**
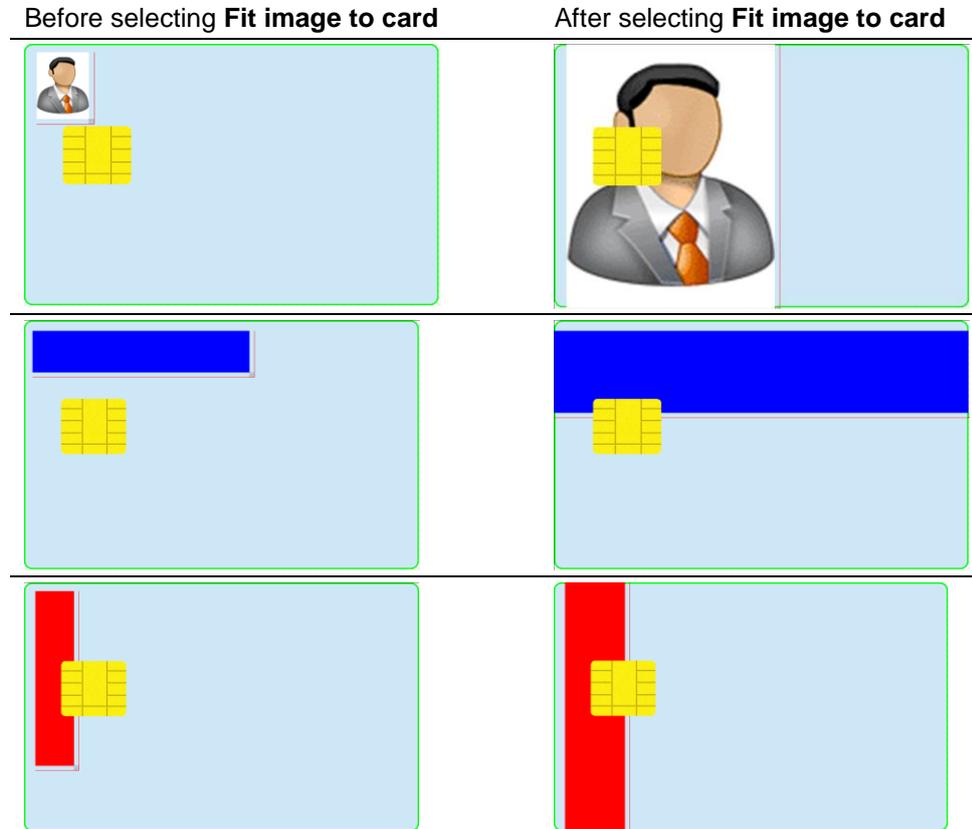
Warning:	There is no 'undo' facility, so save your work before using **Fit image to card** or you will have to restore original positions and sizes manually.

9.5.4 Adding static images

1. Click **Insert picture**.

2. Double-click the image you want to use in the list of images displayed.

3. Move the image into position by placing your mouse over the image and dragging the image to the correct location.

4. Resize the image if necessary. Place your mouse over the small box at the bottom right of the image's red border and drag the outline to the correct size.

   You can hold down the CTRL key and drag the resizing box to change the aspect ratio of the image.

9.5.5 Adding dynamic images

1. Click **Insert user image**.

2. Choose the image to be inserted by selecting an option in the **Image Type** drop-down list. A placeholder image is displayed, which will be replaced with the image specified in the cardholder's record when the card is printed.

3. Move the image into position by placing your mouse over the image and dragging the image to the correct location.

4. Re-size the image if necessary. To do this, place your mouse over the small box at the bottom right of the image's red border and dragging the outline to the correct size.

   Note: You cannot change the aspect ratio of a user image. Do not use the Height and Width controls to change the size of the image, as the image will be resized to maintain its aspect ratio when you print or view a print preview.

9.5.6 Custom image fields

To add a custom image field:

1. From the **Configuration** category, select **Card Layout Editor**.

2. On the toolbar, click **Insert User Image**.

3. From the **Image Source** drop-down list, select **Custom**.

4. In the **Content** box, type the URL for the image you want to use.

You can use the same field codes in this URL as you can use for custom text fields – see section *9.6.3*, *Custom text fields* for details. Any fields are substituted with the value for the user when the card is printed.

For example, if you have the following URL:

```
http://myserver/upimages/Banner[[OptionalLine1]].jpg
```

and the user has `Red` as the value in their Optional Line 1 field in their user record in MyID, then the image used on the printed card will be:

```
http://myserver/upimages/BannerRed.jpg
```

Create a file called `Banner[[OptionalLine1]].jpg` (with the unsubstituted field name included in the filename) in the `upimages` folder and this will be displayed in the Card Layout Editor. Create a copy of this file in the `upimages/UpimagesEditor` folder, as this will be used in the Print Preview dialog.
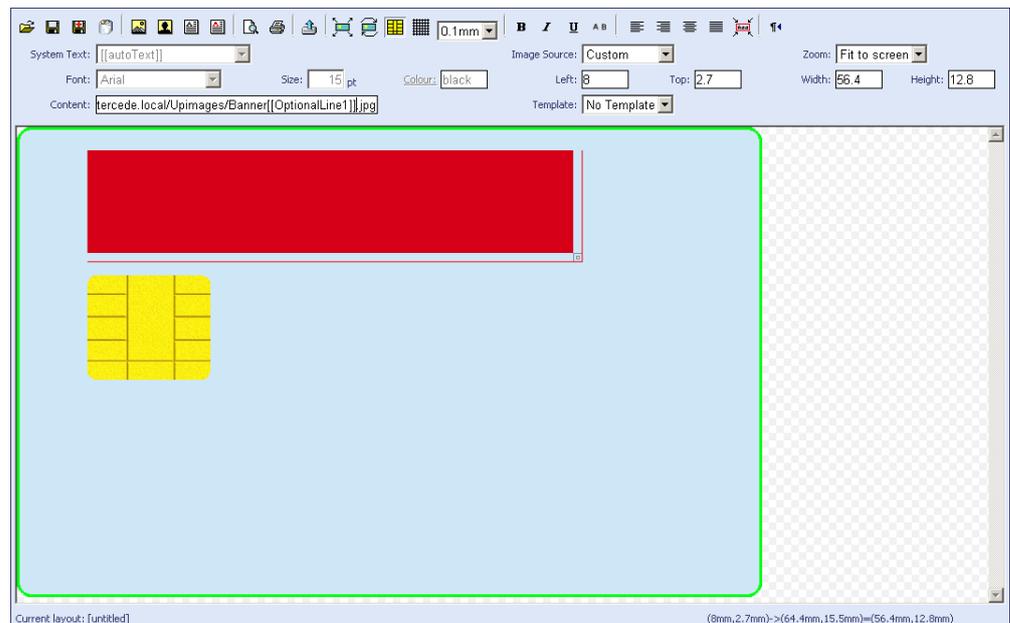
9.5.7 Externally formatted image fields

For some systems (for example, PIV systems) you may need to have more control of the size and position of some elements that the Card Layout Editor can provide. MyID provides the ability to use externally-formatted images for these elements – the elements are formatted exactly to your requirements and placed on the card design as an image.

To add an externally-formatted image field:

1. From the **Configuration** category, select **Card Layout Editor**.

2. Open the layout you want to work with.

3. On the toolbar, click **Insert User Image**.

4. From the **Image Source** drop-down list, select the name of the external formatter; for example, for a PIV name field, select **fips201name**.

5. Select the element, then select the correct **Template** and **Zone**.

9.5.8 Image aspect ratio

To force the image to retain its original aspect ratio regardless of the sizing of a placeholder, make sure the **Maintain Aspect Ratio** toolbar button (on the right of the top row of buttons) is selected. This makes the image appear in its correct ratio, centered within the placeholder image on the Card Layout Editor screen.

Maintain Aspect Ratio option is set for an on-screen element

Maintain Aspect Ratio option is not set

For example, if you have the following images on the card layout:
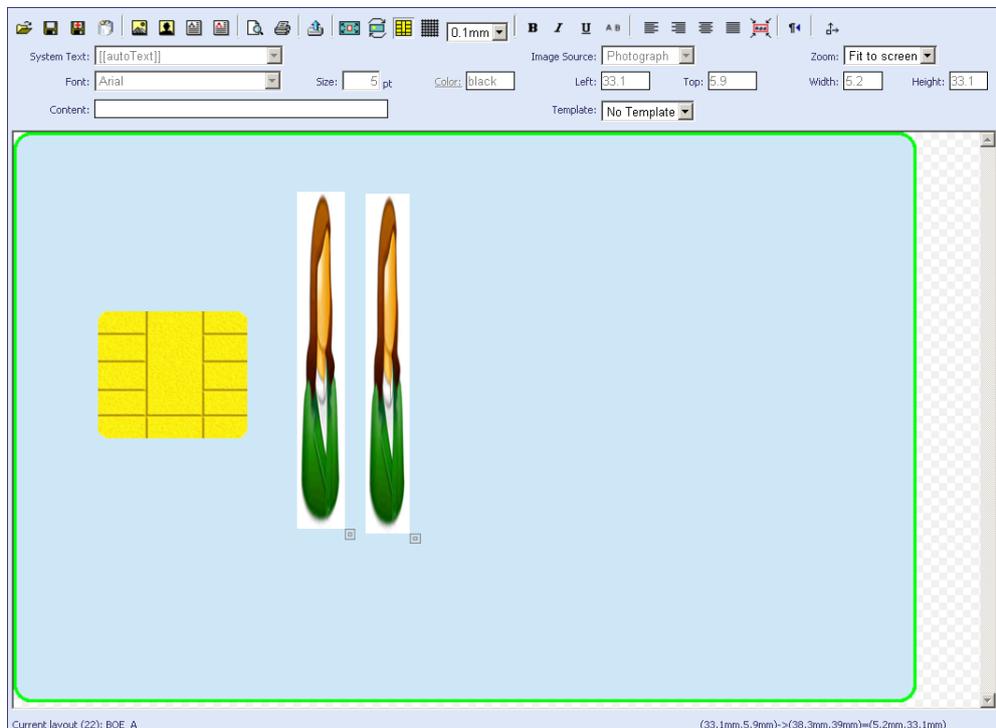
- Select the image on the left, and make sure the **Maintain Aspect Ratio** toolbar button is selected.

- Select the image on the right, and make sure the **Maintain Aspect Ratio** toolbar button is *not* selected.

Click the **Print Preview** button, and the images are displayed as they will appear on the printed card:
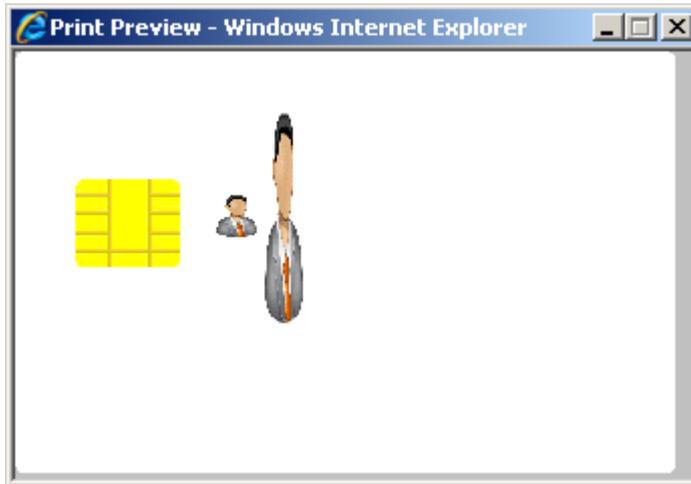
The image on the left is displayed in its original aspect ratio, centered within the area of the placeholder image on the layout. The image on the left is stretched to fit the placeholder image on the layout.

Note: The default for all new images that you add to card layouts is to maintain the aspect ratio.

9.6   Adding or changing text

The following toolbar buttons are used to insert text:

Insert text – type the words that you want to be printed in the **Content** field

Insert auto text – inserts the information from the cardholder's record that corresponds to your selection from the **System Text** drop-down list

Resize – resizes the text container to fit the text

9.6.1   Adding and changing static text

1. Click **Insert text**.

2. Type the text that you want to be displayed in the **Content** field. The text will wrap automatically in the box.

3. Move your mouse over the text in the layout area and drag it to the correct position.

4. Resize the text area. Either:

    ◆ Place your mouse over the small box at the bottom right of the red border and drag the outline to the correct size.

    ◆ Click the **Resize** button on the toolbar.

       Note: This removes the wrapping and sets the text to a single line.

5. To change standard text:

    a) Click the existing text to select it.

    b) Enter the new text in the **Content** field.

9.6.2 Adding dynamic text

1. Click **Insert auto text**.

2. Select the information you want to be displayed in the **System Text** field. In addition to the standard options, this list contains any fields that have been added to the **Add Person** workflow for your organization. The text wraps automatically in the box.

3. Move your mouse over the text in the layout area and drag it to the correct position.

4. Re-size the text area. Either:

   * Place your mouse over the small box at the bottom right of the red border and drag the outline to the correct size.

   * Click the **Resize** button on the toolbar.

     Note: This removes the wrapping and sets the text to a single line.

5. To change dynamic text:

   a) Click the existing text to select it.

   b) Select a different option in the **System Text** field.

9.6.3 Custom text fields

To add a custom text field:

1. From the **Configuration** category, select **Card Layout Editor**.

2. On the toolbar, click **Insert Auto Text**.

3. From the **System Text** drop-down list, select **Custom**.

4. In the **Content** box, type the codes for the fields you want to use.

To find out what codes you can use, select the other entries in the **System Tex**t drop-down list and take a note of the code. Field codes are enclosed in double square brackets (`[[ ]]`).

Note: Field codes are case-sensitive.

You can also include plain text in the **Content** box. For example, you can put a comma between the surname and first name:

`[[Surname]], [[FirstName]]`

which, for example, becomes `Smith, John` when the card is printed.
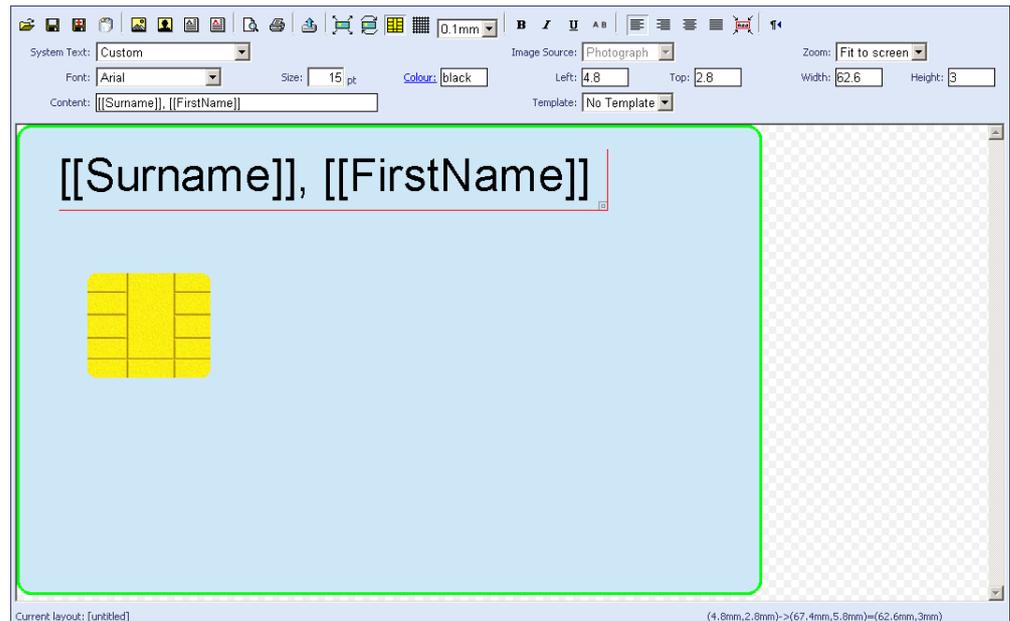
9.7 Formatting text

The options available for formatting text are similar to those found on a standard text editor. An additional option is available:

1. Select the text to be formatted by clicking it. A red border is displayed to the bottom and right of the text area.

2. Click the appropriate toolbar buttons to format the text. The options available are:

   ♦ **Bold**, **Italic** and **Underline** (buttons which toggle the effect)

   ♦ Text alignment: **Left align**, **Right align**, **Center align** and **Justify**

   ♦ **Font** – select from the drop-down list

   ♦ **Size** – type the font size in the box

   ♦ **Color** – change the color of the text (see section *9.8*, *Changing the text color* for details).

3. If the text is written in a language that is read from right to left, click the **Right to left text** button on the toolbar.

4. If you want to display the text vertically, click the **Descend** button on the toolbar.

9.8 Changing the text color

Select the text item that you want to change and then set the color. To do this, you can:

▪ Type the hexadecimal RGB value directly into the field. The value must be seven characters long and begin with #; for example, #FF0000 for red.

▪ Use the color picker to select a color.

9.8.1 Using the color picker

To start the color picker, click on the **Color** label.

- To apply a color to a selected block of text, click your chosen color either in one of the boxes (containing Basic or Custom colors) or in the color palette using the left mouse button, then click **Select**.

- To add colors to the set of custom colors displayed on to the right of the color picker, use the right mouse button to select the box you want to hold the color and then click on the palette with the right mouse button.

9.9 Positioning and sizing elements

To move an element:

1. Click an element to select it.

    You can also press TAB to cycle through all of the elements on the form.

2. Do one of the following:

    - Click and drag the element. You can drag the element in increments specified by the **Snap to** drop-down list; by default, 0.1mm.

    - Use the cursor keys to move the element. You can move the element in increments specified by the **Snap to** drop-down list; by default, 0.1mm. If you hold down CTRL, you move the element in increments of five times the snap setting.

    - Type the position of the element into the **Left** and **Top** boxes. You can specify values between 0 and 200.

To resize an element:

3. Click an element to select it.

    You can also press TAB to cycle through all of the elements on the form.

4. Do one of the following:

    - Click the bottom-right corner of the element, then drag the element to the required size. If you hold down CTRL, you can change the aspect ratio of the element.

    - Type the size in the **Width** and **Height** boxes. You can specify values between 0 and 200.

9.10 Defining data to store on magnetic stripes

You can use the **Card Layout Editor** to define the data stored on magnetic stripes if your cards support them.

To add a magnetic stripe:

1. Click **Insert Text** or **Insert Auto Text**.

2. Select the **Font** from the drop-down list.

   Select **Magnetic Stripe 1**, **2** or **3**. These fonts are used to specify that the text should not be printed to the card, but should be written to one of the three magnetic stripe tracks.

3. Select the **System Text** you want to write to the track, or type the **Content**.

   Note: Make sure that the text you provide is suitable for encoding on the specified magnetic stripe track. For example, track 1 contains alphanumeric and punctuation characters, while tracks 2 and 3 contain only numeric characters.

9.11 Using templates

Templates specify the locations of elements on your card layouts in a consistent and accurate way. Each template comprises a number of zones; each zone specifies a size and position for an element on the card layout. Each zone may also be associated with a field that associates the zone with a specific element.

For example, the template PIV Front may have a zone that contains the following information:

- `x="3.0"` – the element is positioned 3mm from the left of the card.

- `y="5.0"` – the element is positioned 5mm from the top of the card.

- `w="26.7"` – the element is 26.7mm wide.

- `h="36.0"` – the element is 36.0mm high.

- `n="z1"` – the internal unique ID of the zone.

- `f="[[Image]]"` – the zone is associated with the `Image` field – this is the user's photograph.

- `1  : Photo` – the name of the zone as it appears in the drop-down list.

Note: The provided PIV Front template assumes you have the card in a vertical orientation, while the PIV Back template assumes you have the card in a horizontal orientation.

9.11.1 Applying zone settings

To apply a zone to an element:

4. Within the Card Layout Editor, select a template from the **Template** drop-down list.

   For example, select **PIV Front**.

   The **Zone** drop-down list and **Apply this template to all items** appear when you have a template selected.

5. Select an element on the card layout.

   For example, select the user photograph.

6. From the **Zone** drop-down list, select the zone that corresponds to the element.

   For example, select the **1 : Photo** zone.

The Card Layout Editor positions and sizes the element as specified by the template. In the case of the user photo, this is 3mm from the left, 5mm from the top, 26.7mm wide and 36mm high.

The association of the element to the template and zone is stored with the card layout when you save it. You can override the size and position; the association is retained, and you can reset the element to the template settings by reselecting the zone from the **Zone** list.

To apply all the zones in a template:

1. Within the Card Layout Editor, select a template from the **Template** drop-down list.

   For example, select **PIV Front**.

2. Click **Apply this template to all items** .

   The Card Layout Editor applies the settings of each zone in the template to the elements on the card layout.

   The editor matches the template zone to the element based on the field content (for example, the user photograph) or the text content of text labels (for example, the Rank label). It cannot match any element that does not have a field or label; this means you must set the template zone for the photo border or name background manually.

9.11.2 Template XML structure

The templates are stored in the `templates.xml` file in the following folder:

`C:\Program Files (x86)\Intercede\MyID\Web\us\res\cardLayoutEditor\`

The XML uses the following format:

```
<?xml version="1.0" encoding="UTF-8"?>
<templates>
      <template name="name">
          <zone
                x="xpos"
                y="ypos"
                w="width"
                h="height"
                n="uniqueID"
                f="content"
                >zonelabel
          </zone>
          …
      </template>
      …
</templates>
```

where:

- `template` – a template. There may be multiple templates in the `<templates>` node. Each template may contain multiple zones. The template has the following attribute:

    - `name` – the name of the template. This is displayed within the Card Layout Editor in the **Template** drop-down list.

- `zone` – a zone on the card. The content of the node (the *zonelabel*) is displayed within the Card Layout Editor in **Zone** drop-down list. The zone has the following attributes:

    - `x` – the position in mm from the left of the card. This may be between 0 and 200.

    - `y` – the position in mm from the top of the card. This may be between 0 and 200.

- ◆ `w` – the width in mm of the element. This may be between 0 and 200.

- ◆ `h` – the height in mm of the element. This may be between 0 and 200.

- ◆ `n` – the unique identifier for the zone.

- ◆ `f` – the content of the element. This may be a field (for example, `[[Image]]` for the user photograph; `[[ExpiryDate]]` for the card's expiry date) or the content of a text label (for example, `Expires` for the label next to the expiry date). If the element does not have any content, omit this attribute.

  This attribute is used to match the template zone to the appropriate layout element.

Example templates.xml

```xml
<?xml version="1.0" encoding="UTF-8"?>

<templates>

   <template name="PIV Front">
      <zone x="3.0" y="5.0" w="26.7" h="36.0" n="z1" f="[[Image]]" >1 : Photo</zone>
      <zone x="3.2" y="41.5" w="51.5" h="5.0" n="z2a" f="[[Surname]]" >2a : Last Name</zone>
      <zone x="3.2" y="45.5" w="51.5" h="5.0" n="z2b" f="[[[FirstNameInitial]]]" >2b : First
Name</zone>
      <zone x="2.5" y="51.0" w="49.0" h="7.0" n="z3" f="[[Xu16]]" >3 : Signature</zone>
      <zone x="2.5" y="2.5" w="27.5" h="2.5" n="z4" >4 : Miscellaneous</zone>
      <zone x="42.0" y="62.0" w="12.0" h="3.6" n="z5" f="[[Xu1]]" >5 : Rank</zone>
      <zone x="42.0" y="60.0" w="6.0" h="3.1" n="z5L" f="Rank" >5L : Rank Label</zone>
      <zone x="2.5" y="2.5" w="27.5" h="2.0" n="z6" >6 : 2D Barcode</zone>
      <zone x="32.0" y="22.1" w="25.7" h="3.4" n="z8" f="[[Xu53]]" >8 : Affiliation</zone>
      <zone x="32.0" y="20.0" w="15.0" h="3.1" n="z8L" f="Affiliation" >8L : Affiliation
Label</zone>
      <zone x="2.5" y="2.5" w="27.8" h="2.5" n="z9" f="United States Government" >9 :
Header</zone>
      <zone x="32.0" y="26.9" w="21.0" h="5.6" n="z10" f="[[GroupName]]" >10 :
Organization</zone>
      <zone x="32.0" y="25.0" w="21.0" h="3.1" n="z10L" f="Agency / Department" >10L :
Organization Label</zone>
      <zone x="31.2" y="20.5" w="20.0" h="20.0" n="z11" f="[[Xg18]]" >11 : Seal</zone>
      <zone x="2.5" y="81.3" w="49.0" h="4.3" n="z12" >12 : Footer</zone>
      <zone x="32.0" y="34.0" w="21.0" h="3.4" n="z13" f="[[[IssueDate]]]" >13 : Issued</zone>
      <zone x="32.0" y="32.0" w="21.0" h="3.1" n="z13L" f="Issued" >13L : Issued Label</zone>
      <zone x="32.0" y="38.5" w="21.0" h="3.4" n="z14" f="[[[ExpiryDate]]]" >14 :
Expiration</zone>
      <zone x="32.0" y="36.5" w="21.0" h="3.1" n="z14L" f="Expires" >14L : Expiration
Label</zone>
      <zone x="2.5" y="41.7" w="49.0" h="8.5" n="z15" >15 : Name background</zone>
      <zone x="2.5" y="4.5" w="27.7" h="37.0" n="z16" >16 : Photo Border</zone>
      <zone x="2.5" y="2.5" w="27.7" h="2.5" n="z17" >17 : Miscellaneous</zone>
   </template>

   <template name="PIV Back">
      <zone x="20.0" y="48.5" w="22.0" h="3.0" n="z1" f="[[[SerialNumber]]]" >1 : Card
number</zone>
      <zone x="43.0" y="48.5" w="22.0" h="3.0" n="z2" f="[[[IssuerID]]]" >2 : Issuer ID</zone>
      <zone x="2.5" y="32.0" w="32.5" h="6.0" n="z4" >4 : Return to</zone>
      <zone x="2.5" y="29.6" w="32.5" h="2.5" n="z4L" f="Return to:" >4L : Return to
label</zone>
      <zone x="35.0" y="34.0" w="9.5" h="3.5" n="z5a" f="[[[Height]]]" >5 : Height</zone>
      <zone x="35.0" y="31.6" w="9.5" h="2.5" n="z5l" f="Height" >5L : Height Label</zone>
      <zone x="42.5" y="34.0" w="9.5" h="3.5" n="z5b" f="[[[EyeColor]]]" >5 : Eyes</zone>
      <zone x="42.5" y="31.6" w="9.5" h="2.5" n="z5m" f="Eyes" >5L : Eyes Label</zone>
      <zone x="50.0" y="34.0" w="9.5" h="3.5" n="z5c" f="[[[HairColor]]]" >5 : Hair</zone>
      <zone x="50.0" y="31.6" w="9.5" h="2.5" n="z5n" f="Hair" >5L : Hair Label</zone>
      <zone x="2.5" y="23.0" w="60.0" h="5.0" n="z6" >6 : Emgy Rspdr info</zone>
      <zone x="2.5" y="18.0" w="60.0" h="5.0" n="z7" >7 : Section 499</zone>
      <zone x="2.5" y="38.0" w="80.0" h="9.5" n="z8" >8 : Linear barcode</zone>
   </template>

</templates>
```

9.12   Reviewing and testing your layout

Print preview

Print

Use the **Print preview** and **Print** options to test your layout before it is used when issuing a card. Differences between printers may require you to make some minor adjustments.

Note: Your layout is not associated with a cardholder's record at this stage, so placeholders are used for any system text or user images. Fields that will be replaced are denoted by `[[FieldName]]`.

10 PIN Generation

You can set up MyID to generate PINs according to a known algorithm. To set up automatic PIN generation, you must set up a PIN Generation Key in Key Manager and set up a Credential Profile to use server generated PINs.

10.1 Adding a PIN Generation key

To add a PIN Generation key:

1. From the **Configuration** category, select **Key Manager**.

2. From the **Select Key Type to Manage** drop-down list, select **PIN Generation Key**.

3. Click **Next**.

4. Click **Add New Key**.

5. Type the **Key Name** and **Description**.

   Take a note of the **Key Name** – you will need it when you set up the credential profile. See section *10.2*, *Credential profile setup for PIN generation*.

6. Select the type of encryption from the **Encryption Type** drop-down list.

   Choose one of the following options:

   ◆ **2DES**

   ◆ **3DES** – the **EdeficePinGenerator** PIN generator in the current version uses 3DES keys.

   ◆ **AES128**

   ◆ **AES192**

   ◆ **AES256**

7. Select one of the following options:

   ◆ **Automatically Generate Encryption Key in Software and Store on Database** – the key is automatically generated and stored in the database.

      Note: If you select this option, you will be unable to share the key with a third party; therefore, you will be unable to generate the PINs outside MyID using the algorithm in section *10.3*, *PIN generation algorithm*.

   ◆ **Encryption Key** – type the key into the box.

---

8. Select the attributes for the key:

◆ **Exportable** – the key can be exported after it has been imported. This option is reserved for future use.

9. Click **Save**.

10.2 Credential profile setup for PIN generation

You must set up the credential profile to specify server-side PIN generation. See PIN Settings in section *12.3.1*, *Credential profile options*.

10.3 PIN generation algorithm

The PIN generation algorithm uses the card serial number as diversification data. A secret key is used to generate the PIN. If you have the card serial number, the same secret key that is used within MyID, and the details of the following algorithm, you can generate the same PINs as MyID.

Alternatively, you can use the user's logon name as the diversification data; this ensures that the user has the same PIN for all of their cards. To use the logon name, set the **Use logon name for server PIN generation** option on the **PINs** page of the **Security Settings** workflow.

10.3.1 Generating the PIN

The process for generating the PIN is as follows:

1. Use the card serial number as the input to a SHA1 hash.

   This generates a 20-byte hash value.

2. Truncate the 20-byte hash to the first 16 bytes. Encryption is carried out on 8-byte blocks, so we want to carry out the encryption on two blocks without padding.

3. Encrypt the hash with the PIN generation key.

   ◆ Use 3DES encryption in cipher block chaining mode. This generates a 16-byte hex value.

   ◆ You do not want any header information in the encrypted data.

   ◆ For the initialization vector, use 8 bytes of 0x00.

   ◆ Do not use any padding.

4. For each byte, divide by the alphabet size (numeric, alpha or alphanumeric) and take the remainder; in other words, *<byte>* modulo *<alphabet size>*.

   As there are 16 bytes, you can generate PINs up to 16 characters long. If the PIN is 6 characters long, for example, perform this operation on the first 6 bytes in the encrypted data.

5. Use this value as a look-up in the alphabet table – see section *10.3.2*, *Alphabet tables*.

   For example, if the byte is 2C, and the alphabet size is 10 (for numeric PINs):

   ```
   2C = 44 decimal
   44 modulo 10 = 4
   Entry 4 in the numeric table = '4'
   ```

10.3.2   Alphabet tables

Numeric

The numeric alphabet has size 10, and the following entries:

Index	0	1	2	3	4	5	6	7	8	9
Value	0	1	2	3	4	5	6	7	8	9

For example, a lookup of 0 returns 0, and a lookup of 7 returns 7.

Note: The **EdeficePinGenerator** PIN generator uses a numeric alphabet only.

Alpha

The alpha alphabet has size 52, and has the following entries:

Index	0	1	2	3	4	5	6	7	8	9
Value	a	b	c	d	e	f	g	h	i	j
Index	10	11	12	13	14	15	16	17	18	19
Value	k	l	m	n	o	p	q	r	s	t
Index	20	21	22	23	24	25	26	27	28	29
Value	u	v	w	x	y	z	A	B	C	D
Index	30	31	32	33	34	35	36	37	38	39
Value	E	F	G	H	I	J	K	L	M	N
Index	40	41	42	43	44	45	46	47	48	49
Value	O	P	Q	R	S	T	U	V	W	X
Index	50	51								
Value	Y	Z								

For example, a lookup of 0 returns a, and a lookup of 37 returns L.

Alphanumeric

The alphanumeric alphabet has size 62, and has the following entries:

Index	0	1	2	3	4	5	6	7	8	9
Value	0	1	2	3	4	5	6	7	8	9
Index	10	11	12	13	14	15	16	17	18	19
Value	a	b	c	d	e	f	g	h	i	j
Index	20	21	22	23	24	25	26	27	28	29
Value	k	l	m	n	o	p	q	r	s	t
Index	30	31	32	33	34	35	36	37	38	39
Value	u	v	w	x	y	z	A	B	C	D
Index	40	41	42	43	44	45	46	47	48	49
Value	E	F	G	H	I	J	K	L	M	N
Index	50	51	52	53	54	55	56	57	58	59
Value	O	P	Q	R	S	T	U	V	W	X
Index	60	61								
Value	Y	Z								

For example, a lookup of 0 returns 0, and a lookup of 37 returns B.

10.3.3 Example

If a numeric pin with a length of 6 characters is requested for a card with serial number `0000000002000304` the process is as follows:

1. The card serial number, `0000000002000304`, is hashed using SHA1 to produce:

   `A1CB37418AF6ADB8A18E0673A2198E683D4992D6`

2. This is then shortened to 16 bytes, as we want to encode two whole 8-byte blocks:

   `A1CB37418AF6ADB8A18E0673A2198E68`

3. This hash is then 3DES CBC mode encrypted using a shared key to produce, for example:

   `7849DE09B259DE772EC0DCFE269E9A40`

4. Each byte is used to look up into the numeric alphabet array (size 10). For a 6 character alphanumeric pin this results in:

   ```
   78 (hex) = 120 (dec) mod 10 = 0
   49 (hex) = 73  (dec) mod 10 = 3
   DE (hex) = 222 (dec) mod 10 = 2
   09 (hex) = 9   (dec) mod 10 = 9
   B2 (hex) = 178 (dec) mod 10 = 8
   59 (hex) = 89  (dec) mod 10 = 9
   ```

5. The PIN returned is `032989`.

C# example

The following is sample code that generates PINs using C#.

```csharp
using System;
using System.Collections.Generic;
using System.Text;
using System.Security.Cryptography;

namespace PINGeneration
{
   class Program
   {
      static void Main(string[] args)
      {
         // Alphabet and PIN size
         char[] alphabet = {'0', '1', '2', '3', '4', '5', '6', '7', '8', '9'};
         int alphabetsize = alphabet.Length;
         int pinlength = 8;

         // Encryption key
         byte[] key = { 0x31, 0x28, 0x7A, 0x5A, 0x36, 0x26, 0x35, 0x31, 0x32, 0x71, 0x71,
0x53, 0x3D, 0x2F, 0x33, 0xA7, 0x21, 0x4C, 0x3F, 0x61, 0x44, 0x31, 0x55, 0x38 };

         //Data to be encoded - device serial number
         string data = "1034";
         //Convert to a byte array
         Encoding ascii = Encoding.ASCII;
         byte[] databytes = ascii.GetBytes(data);

         // Create SHA1 hash of data
         SHA1 shaM = new SHA1Managed();
         byte[] hash = SHA1Managed.Create().ComputeHash(Encoding.Default.GetBytes(data));
         byte[] hash16 = new byte[16];

         // Copy the first 16 bytes of the hash array
         Array.Copy(hash,hash16,16);

         // Set the initialisation vector to 8 bytes of 0x0
         byte[] iv = {0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0 };

         string ciphertext = "";
```

```csharp
        string pin = "";
        string hashhex = "";
        string hashhex16 = "";

        // Set encryption options.
        TripleDESCryptoServiceProvider des = new TripleDESCryptoServiceProvider();
        des.KeySize = 192;
        des.Key = key;
        des.Mode = CipherMode.CBC;
        des.Padding = PaddingMode.None;
        des.IV = iv;

        // Encrypt hashed data
        IcryptoTransform ic = des.CreateEncryptor();
        byte[] enc = ic.TransformFinalBlock(hash, 0, 16);
        for (int i = 0; i < enc.Length; i++)
        {
            ciphertext = ciphertext + enc[i].ToString("X2");
        }

        // Generate PIN from the ciphertext
        for (int x = 0; x < pinlength; x++)
        {
            pin = pin + alphabet[Convert.ToInt32(ciphertext.Substring(x * 2, 2),16) %
alphabetsize];
        }

        for (int i = 0; i < hash.Length; i++)
        {
            hashhex = hashhex + hash[i].ToString("X2");
        }
        for (int i = 0; i < hash16.Length; i++)
        {
            hashhex16 = hashhex16 + hash16[i].ToString("X2");
        }

        Console.WriteLine("Sample PIN generation algorithm output");
        Console.WriteLine();
        Console.WriteLine("Alphabet size:        " + alphabetsize);
        Console.WriteLine("Required PIN length: " + pinlength);
        Console.WriteLine("Data:                 " + data);
        Console.WriteLine("SHA1 hash of data:    " + hashhex);
        Console.WriteLine("16 bytes of hash:     " + hashhex16);
        Console.WriteLine("Encrypted:            " + ciphertext);
        Console.WriteLine("\nPIN:                  " + pin);
        Console.WriteLine("\nPress any key to continue…");
        Console.ReadKey(true);
    }
  }
}
```

11 Importing Serial Numbers

You can import a range of serial numbers for cards, and then create a credential profile that will only issue cards that have been previously imported. The **Import Serial Numbers** workflow allows you to import card serial numbers, and the **Only Issue to Known Serial Numbers** option in the **Credential Profile** workflow allows you to configure the credential profile to restrict issue to those cards.

MyID must also know details of software and hardware tokens before it can issue them to people.

The **Import Serial Numbers** workflow also allows you to import a range of HID codes for integration with a PACS server.

Note: You are advised to import a maximum of 5000 records in a single file. You may experience problems if you try to import more serial numbers. If you have a large number to import, split the file into smaller files containing no more than 5000 records.

The *Serial Number Import Format* document contains details of the format of files used for the Generic Device type. To obtain this document, contact customer support, quoting reference SUP-204.

To import a list of serial numbers:

1. From the **Configuration** category, select **Import Serial Numbers**.

2. In **Import Format**, select the type of card.

   If your card type is not listed, it is possible it is not supported or that additional configuration is required to allow the details to be imported. Contact customer support for more information.

   If you select Generic Device from CSV, you can specify the **Default Device Type** in the final field on the screen.

3. Select the **External System** from the drop-down list.

   For example, select your authentication server or PACS server.

4. In **Valid Import File**, click the browse button and select the file containing the serial numbers.

5. If you selected Generic Device from CSV in **Import Format**, select a default card type from the **Default Device Type** drop-down list.

6. Click **Import**.

   The system starts to import the serial numbers. This process carries on in the background, as it may take some time depending on the quantity of numbers to be imported.

   You can confirm that the process has completed by checking the **Audit Reporting** workflow.

11.1 Troubleshooting and known issues with importing serial numbers

- **Multiple application servers**

  If you have multiple application servers, multiple instances of the job server will run. You must make sure that the file upload directory (set using the **File Import Directory** option on the **Import & Export** tab of the **Operation Settings** workflow) points to the same location and is accessible from all application servers.

- **Padding with leading zeroes**

  When importing serial numbers using the standard format for HID devices, if you provide a facility code of fewer than four digits, MyID automatically pads this to four digits using leading zeroes; similarly, if you provide a serial number of fewer than eight digits, MyID automatically pads this to eight digits using leading zeroes.

12 Managing Credential Profiles

Credential profiles collect together all of the elements that you want to be included when issuing credentials to a particular selection of people or devices.

Warning:	You cannot issue credentials without a credential profile.

Note: If you want a simple credential profile so you can issue some credentials to check the operation of the system, see section *12.2*, *Using the provided credential profile*.

Credential profiles define the following, some of which are optional:

▪ Basic credential profile details and usage

This includes the services that are available, how they are issued, PIN settings, the credential stock (physical media) to be used and any particular credential profiles to be incorporated.

▪ The certificates that may be written to the credential. (Optional)

The certificate authority must be installed, operational and configured to work with MyID, or certificate policies will not be available for selection. See section 7, *Certificate Authorities*.

▪ The applets available. (Optional)

Details of the applets must be entered into MyID or they will not be available for selection. See section 8, *Applets*.

▪ The roles associated with the profile: its availability.

A range of roles is available by default. See section 4, *Roles, Groups and Scope* for details.

A credential profile can be associated with one or more roles. You can:

◆ Associate each role with a different credential profile.

MyID selects the profile based on the role of the credential holder. The operator is not asked which profile to use when issuing credentials, unless the holder is associated with more than one role.

◆ Use the same credential profile for everyone.

The operator may have to select the correct card layout for printing a card if different groups of cardholders are issued cards that are visually distinctive.

◆ Associate more than one credential profile with a role.

The operator has to choose which profile to use when requesting and issuing credentials.

▪ The card layouts that can be used with this card. (Optional)

Card layouts must be defined before they can be associated with credential profiles. See section 9, *Designing Card Layouts*.

You can associate more than one card layout with a credential profile. If you do, the operator will have to choose the correct layout when issuing a card.

12.1 Setting default values

Some of the values specified as part of a credential profile (those displayed when you start the workflow) can be set as system-wide defaults. For example, you can specify the minimum and maximum length of a PIN and the maximum number of incorrect logon attempts permitted before the card is locked.

To access the settings, from the **Configuration Category** select **Security Settings**. The settings are on the **PINs** page and are described in section *34.5*, *PINs page (Security Settings)*

12.2 Using the provided credential profile

A credential profile called Manager is provided but cannot be used until you have associated it with at least one role. This profile does not have any certificates, applets or card layouts associated with it.

Note: You can modify this profile to incorporate additional features or delete it if necessary. The instructions in this section assume you only want to make the profile available so that some credentials can be issued.

1. From the **Configuration** category, select **Credential Profiles**.

    The Manager profile is displayed, showing the default values specified in the **Security Settings** workflow (see section *12.1*, *Setting default values*).

2. Click **Modify**.

3. Click **Next** until you reach the **Select Roles** stage.

4. Select the role or roles that you want to associate with this profile. Click **Next**.

5. Click **Next** until the workflow ends.

Note: You must add a comment to indicate what you have changed and why you have changed it.

You will now be able to issue credentials to people with any role you have associated with this credential profile.

12.3 Creating, modifying, copying and deleting credential profiles

The **Credential Profiles** workflow contains a number of stages. To move between the stages, click **Next**.

Note: You cannot go back to a previous stage. If you forget to select something, either start the workflow again immediately (all your changes will be lost) or complete the workflow and then modify the profile.

The **Credential Profiles** workflow is in the **Configuration** category. When you start the workflow, basic details of the profile shown in the **Select Credential Profile** field are displayed.

▪ To create a new profile, click **New**.

▪ To modify an existing profile, select it from the **Select Credential Profile** list then click **Modify**.

▪ To create a profile based on an existing profile, select the profile you want to copy from the **Select Credential Profile** list then click **Copy**.

▪ To delete a profile, select it from the list in **Select Credential Profile** then click **Delete**. You are prompted to confirm your request.

    Note: You cannot delete a profile that has issued credentials. You must cancel the credentials before you can delete the profile.

    Click **Details** to see the details of the credential profile.

12.3.1 Credential profile options

If you are creating a new profile, give the credential profile a **Name** and optional **Description**. You can change existing details if necessary.

Note: Operators may have to choose a profile when issuing or requesting credentials. Use the **Name** and **Description** to provide information on which profile to choose.

Each of the entries below the **Name** of the profile is associated with a set of configuration options, which are displayed below the **Description**. Depending on the type of card you are using, you may not see all of the entries.

Note: This section describes the options available to you without setting any further system configuration options. See section *12.3.2, Additional credential profile options*, for details of other credential profile options that may be available.

Card Encoding

Select the features you want to use on the card. You must select one or more of:

- **Contact Chip** – the card must contain a contact chip.

- **Contactless Chip** – the card must have a contactless chip.

  If the card has a single chip with two interfaces (contactless and contact) and you want to program both, do not select this option – the card will be programmed through the contact chip. Select this option for contactless-only issuance.

- **Magnetic Stripe (Only)** – the card contains no chips, but has only a magnetic stripe. If your card has a magnetic stripe in addition to a chip, you do not need to select this option.

- **Software Certificates Only** – no card is required, and the certificates are issued only in software.

  See section *12.5, Setting up a credential profile for soft certificates* for details.

- **Device Identity (Only)** – if these credentials are only going to be used to determine the identity of a device (a computer, router or other device), select this option.

  See section *30.3, Setting up a credential profile to use to issue device identities* for details.

- **Externally Issued (Only)** – used for credentials that were originally issued by a different system and have been imported into MyID; for example, this is used for derived credentials for unknown users.

  Note: For information on encoding options relating to mobile identities and derived credentials, see the *Mobile Identity Management Installation and Configuration Guide* and *Derived Credentials Installation and Configuration Guide*. You may need additional modules installed for some mobile options.

Services

Select the appropriate options if you want the credentials to be used to logon to MyID or to encrypt data using MyID keys.

If you want to issue archived certificates, the MyID Encryption service must be selected. If no certificates are mapped to the logon and encryption services, an additional Manager Keypair is generated for these services. Not all cards or devices support manager keypairs.

Issuance Settings

Specify how the credentials are issued and how long they remain valid.

- **Validate Issuance**

  If you set this option, credentials issued using this profile will require secondary authorization – either a witness during the issuance process, or a validation of the request.

- **Validate Cancelation**

  If you set this option, credentials issued using this profile will require secondary authorization when you cancel them.

- **Lifetime**

  The **Lifetime** is a mandatory setting that determines the number of days for which the credentials will be valid. The initial default value is 365 days.

- **Only Issue to Known Serial Numbers**

  If you set this option, MyID must already have a record of the serial number of the card or token before credentials can be issued to it. See section *11, Importing Serial Numbers*, for details.

- **Issue Via Bureau**

  If you are using a bureau to issue credentials, set this option.

  Note: Bureau issuance requires an additional module. Contact customer support quoting reference SUP-233.

- **Lock User PIN at Issuance**

  If you set this option, the card is locked after it is issued, and must be unlocked before it can be used.

  Note: If you set this option, it may fail in certain scenarios (for example, when certificates are written to a card using vendor middleware, MyID may be denied access to lock the card on completion).

- **Disable Card at Issuance**

  If you set this option, the card and credentials are issued in a disabled state. An operator must enable them before they can be used.

  You can use **Issue Card**, **Collect Card** or **Batch Collect Card** to issue the cards. This allows you to print and personalize the cards, but does not make them available for use.

  An operator must enable the card before the user can use it.

- **Issue Additional Identities**

  Used for additional identities. See section *32, Additional Identities*.

- **Key Recovery Only**

  Used for key recovery operations. See section *20, Key Recovery* for details.

- **Require Activation**

  Used for card activation. See section *28*, *Activating Cards* for details.

- **Pre-encode Card**

  Used for card activation. See section *28*, *Activating Cards* for details.

- **Require Facial Biometrics**

  - **System Default** – the requirement is based on the **PIV Facial Biometrics Required** configuration option.

    When you upgrade an existing system, the default value for existing credential profiles is **System Default**.

  - **Always** – facial biometrics are always required for issuance of cards using this credential profile. The **PIV Facial Biometrics Required** configuration option is ignored.

  - **Never** – facial biometrics are never required for issuance of cards using this credential profile. The **PIV Facial Biometrics Required** configuration option is ignored.

- **Terms and Conditions**

  Note: The primary use of Terms and Conditions is when the holder has to activate the card; for example, when you have set the **Require Activation** option. You can also use terms and conditions for self-service collection of cards that do not require activation, or for self-service collection of VSCs. Terms and conditions are not displayed in the **Collect Card** workflow, but are displayed for **Collect My Card**.

  For details, see section *28.2*, *Terms and conditions*.

- **Credential Group** – see *12.3.2*, *Additional credential profile options* for details.

- **Enforce Photo at Issuance** – select one of the following options:

  - **No** – you can issue cards if the cardholder does not have a photo.

  - **Request and Issuance** – you cannot request or issue a card if the cardholder does not have a photo.

  - **At Issuance Only** – you can request a card, but if the cardholder does not have a photo you will be unable to issue or activate the card.

- **Proximity Card Check**

  You can set up MyID to check the proximity serial numbers of the HID PROX-capable PIV cards you are issuing. See section *11, Importing Serial Numbers*, for instructions on importing serial numbers into MyID.

  Important: This feature requires that you are using a card reading device capable of detecting the proximity serial number; for example, a Fargo 5000 printer that contains an embedded Omnikey 5125 reader. If MyID cannot detect the proximity serial number using a prox reader, it will *not* issue the card if you have set this option to **Must be a Proximity Card** or **Must be a Known Proximity Card**.

  Note: Depending on the cards you are using, your system may need to be customized to allow MyID to use the proximity serial numbers. The default implementation expects the serial number to be in the "HID Corporate 1000" or "HID H10302" format. If you need to support other proximity serial number formats, contact customer support for more information quoting reference SUP-77.

MyID can integrate your PROX cards with your PACS operation; contact Intercede professional services for details.

Select from:

- **None** – MyID does not check for the existence of a proximity feature on the card. No association with the contactless chip is created.

- **Must be a Proximity Card** – MyID checks that the card is a proximity card. The contactless chip will be associated with the user.

- **Must be a Known Proximity Card** – MyID checks that the card is a proximity card, and that the proximity serial number has previously been imported to MyID using the **Import Serial Numbers** workflow. The contactless chip will be associated with the user.

- **Notification Scheme**

  The Notifications feature allows email and URL notification schemes to be triggered when specific events in MyID occur, such as issuing a card, cancelling a card or completing a workflow.

  Notification schemes require additional customization. Contact customer support quoting reference SUP-188 for details.

  MyID also supports two-way SSL for notifications.

- **Require user data to be approved**

  If you select this option, MyID prevents credentials from being issued unless the user has the User Data Approved flag set on their account. You can set this flag only through the Lifecycle API – see the *Lifecycle API* document for details.

- **Secondary Credential**

  Set this option if the credential being issued is not the cardholder's primary credential. MyID will not assign ownership of recovered historic certificates to secondary credentials.

- **Generate Logon Code**

  Used to send a one-time logon code to the cardholder when the credential is requested. The cardholder can use this code to log on to MyID and collect their credential. See section *3.4*, *Logon codes* for details.

- **Require Challenge**

  Used only when **Device Identity (Only)** is select in the **Card Encoding** section. When requesting a device identity for a SCEP-compliant device, you can choose whether to display the one-time challenge code on screen or send an email message containing the challenge code. See section *30.7*, *Requesting a device identity* for details.

- **Unrestricted Cancelation**

  Allows you to re-use a card without first cancelling it. Even if the card has already been issued, this allows you to issue the card or assign it to a request; the previous credentials will automatically be cancelled with a status mapping of Lost and a comment indicating that the card was cancelled by the unrestricted cancelation feature.

  This option allows you to use, for example, a pool of temporary cards for visitors that you can issue and re-use immediately without having to cancel them first.

  Note: In the **Collect Card** workflow, a card that has been issued with the **Unrestricted Cancelation** option is listed as **Not Issued** on the card selection screen.

  This option appears only if the **Enable unrestricted cancelation** option on the **Issuance Processes** tab of the **Operation Settings** workflow is set to `Yes`.

PIN Settings

Note: You may be able to create a set of PIN options that make it impossible to log in. For example, if you set the **Maximum PIN Length** to `4`, and the **Minimum PIN Length** to `4`, you might expect to be able to enter 4-digit PINs. However, if the card does not allow you to change the minimum length and has this value set to `6`, you end up with a card which cannot be issued – you cannot enter a PIN that is 4 characters or less, and 6 characters or more.

The options available depend on the card type you are using. You may not be able to change some options on all card types, as they are set at manufacture.

The mandatory settings, with initial default values shown in brackets, are:

- **Authentication Mode** (PIN)

  This setting specifies the authentication mode for the issued credential; that is, how the owner of the credential will authenticate to access the credentials. For example, most smart cards use the PIN as the method of authentication. Some device types have extended capabilities; for example, fingerprint match on card. Other device types may manage this setting externally from MyID. This field is usually automatically set depending on the encoding type selected in the credential profile; do not change this option unless specified in the appropriate integration guide for the device type.

- **Maximum PIN Length** (12)

- **Minimum PIN Length** (4)

- **Repeated Characters Allowed** (0)

  Set to the maximum number of repeated characters in the PIN.

  For example, if you set this value to 3:

  - `333999000` – is allowed.

  - `333399000` – is *not* allowed.

  Set this value to `0` to allow any number of repeated characters.

- **Sequential Characters Allowed** (0)

  Set to the maximum number of sequential characters in the PIN.

  For example, if you set this value to 3:

  - `123987456` – is allowed.

  - `123487456` – is *not* allowed.

  Set this value to `0` to allow any number of repeated characters.

- **Logon Attempts** (5)

- **PIN Inactivity Timer** (180 minutes)

- **PIN History** (0)

  Note: If the **PIN History** option is supported, it indicates the number of previous PINs to remember. You cannot reuse a remembered PIN. PIN history is not available on any currently-supported smart cards within MyID – for more information contact customer support, quoting reference SUP-186.

- From the **Issue With** drop-down list, select one of the following:

  - **User specified PIN** – the user types the PIN when the card is issued. This is the default option.

  - **Client Generated PIN** – the PIN is generated on the client PC. Type the **Length** for the PIN.

- ◆ **Server Generated PIN** – the PIN is generated by the MyID server. See section 10, *PIN Generation* for more information. Complete the following details:

    - ▫ **Length** – the length of the generated PIN.

    - ▫ **PIN Algorithm** – select the PIN generation algorithm. For example, select **EdeficePinGenerator**.

    - ▫ **Protected Key** – select the PIN generation key you added using the Key Manager workflow.

- ▪ **Email PIN**

    To email the PIN to the user when the card is issued, select the **Email PIN** option. This option is available only when the **Issue With** option is set to **Client Generated PIN** or **Server Generated PIN**.

PIN Characters

Specify the type of characters that must, may or must not be contained in the PIN.
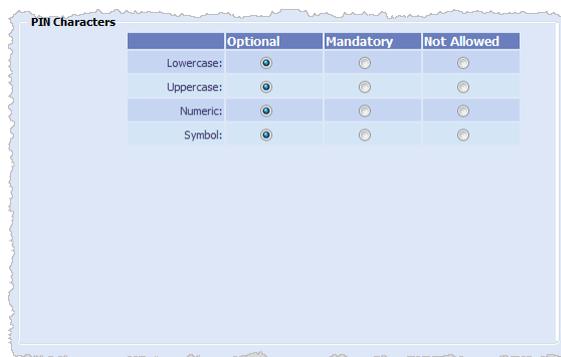
Note: Make sure that the cards you are using support the combination you select by checking the relevant *Integration Guide*. Some cards do not allow the PIN rule enforcement to be stored on the card; MyID will enforce the PIN rules, but external software may be able to change the PIN on the card without the rules being enforced.

If you are using an authentication server to issue one time passwords on the card, you must make sure that the PIN restrictions in the credential profile are the same as the PIN restrictions on the authentication server.

Mail Documents

There are two systems for mailing documents.

For Microsoft Word-based mailing documents:

- ▪ **Select Card Issuance Mailing Document** – select the Microsoft Word mail merge template to be used in the **Print Mailing Document** workflow.

- ▪ **Select Enable Card Mailing Document** – select the Microsoft Word mail merge template to be used when credentials issued with this profile are enabled.

    Note: The mail merge document should be stored on the workstation used for issuing credentials. See section *12.4*, *Setting up mail merge documents* for more details.

For HTML-based mailing documents:

- ▪ **Select PIN Mailing Document** – select the name of the HTML template stored in the MyID database to be used to generate a PIN mailing document for use in the **Collect Card** and **Batch Collect Card** workflows.

    For details of configuring templates, contact customer support, quoting reference SUP-255.

Credential Stock

This is used only if you are using a bureau to issue cards.

Device Profiles

The **Card Format** drop-down list contains the available data model files. These files are used to specify the structure of the electronic data written to cards. Select **None** from this list unless you are specifically instructed to select another option by the integration guide for your credentials; for example, for PIV cards you must select the correct PIV data model as detailed in the *PIV Integration Guide*.

When you import cards and tokens (for example, for one time password tokens) the capabilities of the object are stored in a data profile. Load this data profile to populate the credential profile with device-specific settings.

Requisite User Data

Note: This section appears only if you have selected the **Requisite User Data** option on the **Issuance Processes** tab of the **Operation Settings** workflow.

Contains a list of user attributes that must be present for this credential profile to be issued.

Currently, this is used only to restrict the issuance of derived credentials on VSCs to users with the appropriate attributes; for example, if your VSC derived credential is to be used for email signing, you must select **Email** from the list, and provide an appropriate certificate for email signing – only users who have the Email attribute mapped in their user account will be able to receive a derived credential VSC based on this credential profile. Similarly, if your VSC derived credential is to be used for Windows Logon, you must select **UPN** from this list, and provide an appropriate certificate for logging on to Windows.

12.3.2 Additional credential profile options

Additional credential profile options are shown if MyID has been configured to enable particular features.

Microsoft Virtual Smart Card

This additional Card Encoding option is shown if you are using MyID to issue Microsoft virtual smart cards. See the *Microsoft Virtual Smart Card Integration Guide* for details.

Intel Virtual Smart Card (Only)

This additional Card Encoding option is shown if you are using MyID to issue Intel virtual smart cards. See the *Intel Virtual Smart Card Integration Guide* for details.

Credential group

If you have set the **Active credential profiles per person** configuration option (see section *33.11*, *Issuance Processes page (Operation Settings)*) to **One per credential group**, you can specify the group to which the credential profile belongs. This enables you, for example, to issue a card, a token and so on to the same person.

When you enable a credential for a user, all other credentials issued to the user that belong to the same credential group are either disabled or cancelled, depending on the **Cancel Previously Issued Device** setting.

If you leave the **Credential Group** blank, a user can have many active credentials from this profile, even if the **One per credential group** option is set. Enabling credentials with a blank credential group does not disable or cancel any other credentials.

Note: If you change the configuration option from **Many** to **One** or to **One per credential group**, MyID does not automatically disable or cancel any of a user's credentials until the next time you enable credentials for that user. Similarly, if you change the option from **One** or **One per credential group** to **Many**, MyID does not automatically re-enable any disabled credentials for that user.

Note: If a user is disabled, and is re-enabled when the **Active credential profiles per person** setting does not allow the user to have all of the credentials previously issued to them, the credentials that are re-enabled for the user are the credentials with the highest ID (that is, the credentials that were added to the MyID system most recently), not necessarily the credentials that were active at the point when the user was disabled.

Cancel Previously Issued Device

If you set this option, instead of disabling any previously-issued device because of the action of the **Active credential profiles per person** configuration option and **Credential Group** setting in the credential profile, MyID *cancels* the previously-issued devices.

Authentication Service Settings

If you want to issue software one time passwords, if your credentials operate as a one-time-password hardware token, or if you want users to be able to use virtual one time password tokens, set the authentication service options.

Note: These options are only displayed if token logon is enabled.

If you selected a device profile, the number and type of options available here are limited to the capabilities of the selected device, and you do not need to click the add button. You must make sure that you have added authentication services that correspond to the device's capabilities using the **External Systems** workflow.

Click the add ![+] button. You can add several authentication services to a credential profile.

From the **Name** drop-down list, select the authentication service (as set up in the **External Systems** workflow for your authentication server – see the integration guide for your authentication server for details) then select **Hardware**, **Software** or **Virtual** from the **Type** drop-down list:

- **Hardware** – the card acts as a hardware one time password token.

- **Software** – the card contains software one time passwords.

- **Virtual** – the authentication server is informed that the user can use virtual one time passwords.
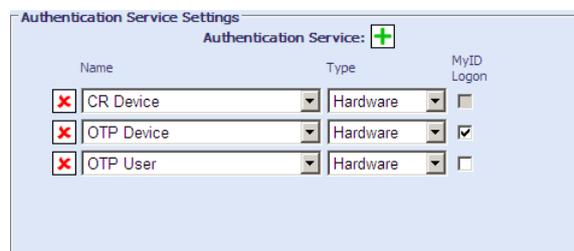
Authentication methods

The **Require Fingerprints at Issuance** and **Additional Authentication** options allow you to specify how the cardholder authenticates their identity to issue, activate or unlock their card.

Scenario	Require Fingerprints at Issuance	Additional Authentication
No authentication at issuance, activation or unlocking	Never Required	None
Biometric authentication at issuance or activation, but not at unlocking	Always Required	None
Biometric authentication at issuance, activation and unlocking	N/A	Biometric
Code authentication at activation and unlocking	Never Required	Authentication Code
Biometric authentication at issuance, biometric authentication and code authentication at activation, and code authentication at unlocking	Always Required	Authentication Code

Note: You cannot use authentication codes for face-to-face issuance.

Additional authentication

If you want to use the additional authentication system to use authorization codes to issue devices, you must carry out the following procedure.

1. In the **Configuration** category, select **Operation Settings**.

2. Click the **Biometrics** tab. Set the **Enable additional authentication options** to `Yes`.

    This makes the following options visible in the **Credential Profiles** workflow:

    - **Additional Authentication**

    - **Require Fingerprints at Issuance** – you are recommended to leave this set to **System Default**.

    - **Minimum fingerprint quality** – do not type a value. This setting is reserved for future use on biometric devices that support fingerprint quality ratings.

3. Set up your credential profile as follows:

    a) Set the **Require Activation** option to **Allow self collection** or **Assisted activation only**.

    b) Set the **Additional Authentication** option to one of the following:

        ▫ **Biometric** – biometric authentication is used to activate or unlock the card.

        ▫ **Authentication Code (Manual)** – an authentication code is required to activate or unlock the card. An operator must request an authentication code.

        ▫ **Authentication Code (Automatic)** – an authentication code is required to activate or unlock the card. An authentication code is emailed to the applicant when the card is issued.

4. Request a card for the applicant, specifying the credential profile that has the additional authentication options.

5. Collect the card for the applicant.

- ◆ If the **Additional Authentication** option was set to **Authentication Code (Automatic)**, an email that contains an authentication code is sent to the applicant.

- ◆ If the **Additional Authentication** option was set to **Authentication Code (Manual)**, you must request an authentication code using the **Request Auth Code** or **Card Ready Notification** workflow.

The card is now in a state in which it can be collected, and the applicant has the necessary authentication code sent by email.

6. If the **Require Activation** option was set to **Allow self collection**, the applicant takes their own card and logs in to MyID, and activates it using the automatic **Activate Card** workflow.

If the **Require Activation** option was set to **Assisted activation only**, an operator uses the **Assisted Activation** workflow to activate the card for the applicant.

12.3.3   Selecting certificates

Note: If you are not using certificates, click **Next** to skip this page.

This page lists all of the available certificate policies you can issue to a credential.

The **Unmanaged** option allows you to issue a certificate stored in a PFX file; for example, for mobile credentials.

You can click **Show inactive certificate policies** – this displays a list of certificate policies that were previously issued but are now disabled. You cannot issue new certificates based on these policies, but you *can* choose to recover a number of historic certificates.

To select certificates:

1. Select the **Required** checkbox for the certificate policy you want to issue to the credential.

2. If the certificate policy is set for key archival (there is an asterisk * next to the policy name) select the following options:

- ◆ **Action** – select one of the following options:

  - □ **Issue new** – a new certificate based on this policy will be issued.

    Note: For **Unmanaged** certificate policies, you cannot select **Issue new**. The certificate is recovered from the PFX file, not issued from the CA.

□ **Use existing** – if a certificate based on this policy has been issued to the user before, and the certificate is live and unexpired, it is recovered onto the credential. If there are no available archived certificates, a new certificate is issued.

Note: This option is not available if the **Card Encoding** is set to **Software Certificates Only**.

□ **Historic Only** – if a certificate based on this policy has been issued to the user before, the certificate is recovered onto the credential. If there are no available archived certificates, no new certificate is issued.

Note: This option is not available if the **Card Encoding** is set to **Software Certificates Only**.

Note: When you select an **Action** from the list, the **Number of historic certificates** field is reset to the default for that action.

◆ **Number of historic certificates** – the maximum number of historic certificates to recover onto the credential. If there are more historic certificates available than the maximum allowed, the most recent certificates are issued.

Note: If your credential supports storing fewer historic certificates than are specified in the credential profile, the most recent certificates are recovered; for example, if you specify four historic certificates in the credential profile, but your smart card can store only two historic certificates, the two most recent historic certificates are recovered.

3. For archived and non-archived policies, set the following options:

◆ **Signing** – if you selected **MyID Logon** in the **Services** section of the credential profile, you can select one certificate to be used for signing.

If you selected **MyID Logon** but do not select a certificate, MyID will generate a keypair for the credential to be used for signing instead of a certificate.

◆ **Encryption** – if you selected **MyID Encryption** in the **Services** section of the credential profile, you can select one certificate to be used for encryption.

Note: Do not select a certificate for encryption that has been marked as for signing in the **Certificate Authorities** workflow. You cannot use a signing certificate to perform encryption or decryption.

If you selected **MyID Encryption** but do not select a certificate, MyID will generate a keypair for the credential to be used for encryption instead of a certificate.

◆ **Default** – you can select one certificate on the credential to be used as the default certificate.

4. If the **Card Format** option (in the **Device Profiles** section of the credential profile) supports containers, select the container on the credential in which you want to store the certificate.

Note: If you are using certificate containers, you can select only one certificate for each container.

Note:

Once you have finished selecting your certificates, click **Next**.

12.3.4 Selecting applets

Select the applets you want to copy onto the card. Click **Next**.

For more information about applets, see section *8*, *Applets*.

12.3.5 Linking credential profiles to roles

On the Select Roles page, you must select which roles can receive credentials issued using this credential profile. Select the roles in the **Can Receive** column.

For information about roles, see section *4.1*, *Roles*.

Note: If you specify a role, the credential profile is immediately available for use. If you do not want it to be used yet, do not associate it with any roles.

Note: If you associate more than one credential profile with the same role, the operator must select the correct profile when requesting or issuing credentials.

12.3.6 Constrain credential profile issuer

If you have the **Constrain Credential Profile Issuer** option set, on the Select Roles page you can also select which roles can *request* credentials using this credential profile. Select the roles in the **Can Request** column.

MyID checks the operator's permissions to access credential profiles at the point at which the operator has to select a credential profile. The workflows affected include all card and ID request workflows, as well as requests for updates and replacements.

To set the option, in the **Configuration** category, select the **Security Settings** workflow and click the **Process** tab.

The default for this option depends on whether you were upgrading a system with existing credential profiles when you installed MyID.

- If you had existing credential profiles, this option is switched off.
- If you had no existing credential profiles or were performing a new installation, this option is switched on.

Note: If you are using a workflow that allows you to request and collect credentials in the same operation (for example, **Issue Card**) you need both the **Can Request** and **Can Collect** options.

12.3.7 Constrain credential profile validator

If you have the **Constrain Credential Profile Validator** option set, on the Select Roles page you can also select which roles can *validate* credentials using this credential profile. Select the roles in the **Can Validate** column.

To set the option, in the **Configuration** category, select the **Security Settings** workflow and click the **Process** tab.

12.3.8 Constrain credential profile collector

If you have the **Constrain Credential Profile Collector** option set, on the Select Roles page you can also select which roles can *collect* credentials using this credential profile. Select the roles in the **Can Collect** column.

To set the option, in the **Configuration** category, select the **Security Settings** workflow and click the **Process** tab.

The workflows affected include all card and ID collect workflows, batch collect, and activation workflows.

12.3.9 Constrain credential profile unlock operator

If you have the **Constrain Credential Profile Unlock Operator** option set, on the Select Roles page you can also select which roles can *unlock* credentials that were issued using this credential profile in the **Unlock Credential** and **Reset Card PIN** workflows. Select the roles in the **Can Unlock** column.

To set the option, in the **Configuration** category, select the **Security Settings** workflow and click the **Process** tab.

Note: This option does not affect the behavior of the **Unlock Card** or **Remote Unlock Card** workflows; it affects only the **Unlock Credential** and **Reset Card PIN** workflows.

12.3.10 Associating credential profiles with card layouts

Note: If you are not printing information on cards or have not yet designed your card layouts, you can click **Next** to skip this stage.

Select the card layouts that you want to be available when this credential profile is used. If you select more than one layout, the operator must decide which to use when issuing a card.

If you select more than one layout, you can click the name of the layout to select it as the default layout; this default layout will used in the **Batch Collect Card** workflow.

Note: To ensure that the print preview displays correctly, you must make sure that MyID is configured for the location of images. See section *9.2*, *Configuring the image location*.

Click **Next**.

12.3.11 Adding comments to the credential profile

You must provide a comment for the credential profile to cover either the initial creation of the credential profile or the changes you have made.

Click **Next** to complete the workflow.

12.4 Setting up mail merge documents

Note: This section refers only to mail merge documents as used by the **Print Mailing Document** workflow and when credentials are enabled. The **Collect Card** workflow uses a new system of mailing document templates that does not use Microsoft Word. For more details, contact customer support, quoting reference SUP-255.

To use the mail merge feature, you must have an installation of Microsoft Word on the client machine. As all the processing is carried out on the client machine, all the paths you enter must correspond to paths available on the client.

You print mailing documents after issuance using the **Print Mailing Document** workflow; note, however, that PINs are not available after issuance, as the PINs are not stored in the database.

In Microsoft Word, you add merge fields to a document that are replaced with values from MyID when the document is printed. The following instructions refer to the procedure for Word 2013; see your Microsoft Word documentation for the merge field procedures for other versions.

1. Type your letter or other mailing.

2. To insert a mail merge field:

   a) From the **Insert** tab, select the **Quick Parts** menu in the **Text** grouping.

   b) Select **Field**.

3. Select the **Mail Merge** category, and the **MergeField** field.
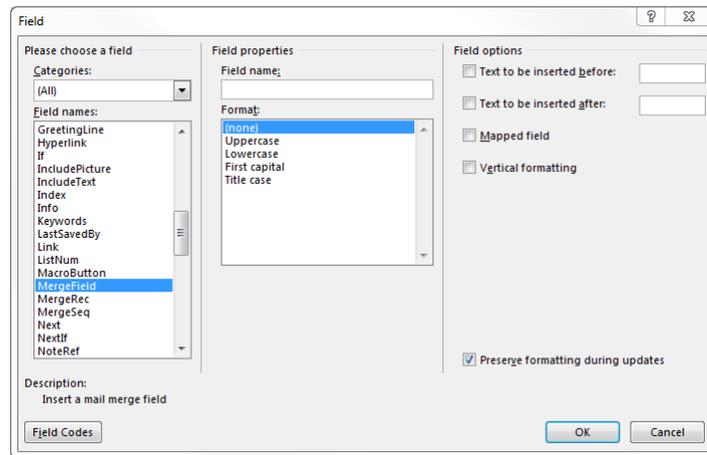
4. Type the name of the MyID field in the **Field name** box.

    You can use the following fields:

Field name	Description
Title	User's title.
FirstName	User's first name.
Surname	User's surname.
FullName	User's full name.
SerialNumber	Serial number of the device being issued.
DeviceTypeName	Device type name of the device being issued.
InitialPIN	Initial PIN of the device being issued. If you print the document after issuance, the PIN is not available – PINs are not stored in the database.
PINFull	Initial PIN of the device being issued. This appears as complete words; for example: ONE THREE SIX EIGHT. If you print the document after issuance, the PIN is not available – PINs are not stored in the database.
LogonName	User's logon name.
GroupName	User's group name.

    You can also include any extended user, credential, or group fields (Xu, Xd, and Xg fields) that may have been added to your installation.

5. Click **OK**.

6. Save your document in the Word 97-2003.doc format.

12.5 Setting up a credential profile for soft certificates

Note: You can select certificate policies for soft certificates only if they have a **Certificate Storage** option of **Software** or **Both** set in the **Certificate Authorities** workflow.

To set up a credential profile for issuing soft certificates:

1. From the **Configuration** category, select **Credential Profiles**.

2. Choose one of the following options:

   ◆ Select a profile to modify and click **Modify**.

   ◆ Select a profile to use as the basis for a new profile and click **Copy**.

   ◆ Click **New** to create a new profile.

3. Type a **Name** and optional **Description** for the credential profile.

4. In **Card Encoding**, select **Software Certificates (Only)**.

5. Click **Issuance Settings**.

   Set the following options:

   ◆ **Validate Issuance**

      If you set this option, certificates issued using this profile will require a validation of the request.

   ◆ **Validate Cancellation**

      If you set this option, certificates issued using this profile will require secondary authorization when you cancel them.

6. Click **PIN Settings** and **PIN Characters** to specify the format of the passwords used to protect PFX files containing the certificates.

7. Click **Mail Documents** to specify the document sent to the user when the certificate is issued, if required.

8. Click **Next**.

9. From the list of available soft certificates, select the certificates you want to issue.

   From the **Storage Method** list, select where you want the certificate to be stored:

   ◆ **Local Store** – the certificate is stored automatically in the certificate store of the logged-on user.

   ◆ **Password Protected PFX File** – the certificate is exported to a password-protected PFX file, which you can then install into a user's certificate store.

      You can use the following characters in PFX passwords:

      `a-z A-Z 0-9 ! \ " # $ % ' ( ) * + - . / : ; = ? @`

      Note: You cannot use spaces.

   ◆ **Choose During Issuance** – you can choose between the Local Store and PFX options when you issue the certificates.

      Note: If the certificate is not archivable, you cannot select **Choose During Issuance**.

10. Click **Next**.

11. Select the roles that can request this credential profile, the roles to which you want to be able to issue it, and the roles you want to be able to validate it.

12. Click **Next**.

12.6 Customizing terms and conditions

You can override the standard terms and conditions with a custom set.

Note: The terms and conditions text that is used depends on the workflow and the MyID client you are using:

Workflow	Client	Terms and conditions method
Activate Card	MyID Desktop	HTML template
Activate Card	SSA or SSK	Web service
Assisted Activation	MyID Desktop	HTML template
Collect My Card, Reprovision Card, Reprovision My Card, Update Card	MyID Desktop (PIV only)	SignedTCs.txt
Collect My Card, Reprovision Card, Reprovision My Card, Update Card	MyID Desktop (Non-PIV)	Translation method
Collect My Card, Update Card	Self-Service App	Web service

12.6.1 Customizing terms and conditions using the HTML template method

For the text that appears in the **Activate Card** and **Assisted Activation** workflows in MyID Desktop (on both PIV and non-PIV systems) you must set up an HTML template in the MyID database.

For information on adding HTML templates, contact customer support quoting reference SUP-255 to obtain a copy of the *Terms and Conditions* document.

Once you have set up a template in the MyID database, within the **Credential Profiles** workflow, you must select an option from the **Terms and Conditions Template** drop-down list to select which template to use when activating a card.

12.6.2 Customizing terms and conditions for the web service

The `TermsConditions.txt` file is located in the following folder by default:

`C:\Program Files\Intercede\MyID\SSP\MyIDProcessDriver\Content\`

These terms and conditions are displayed to a cardholder, who must agree to the conditions before being allowed to collect their device.

You can use a text editor to change the wording of this agreement.

After you have edited and saved the text file, recycle the **MyIDWebService** application pool in IIS to ensure that the web service is using the latest version of the file.

12.6.3 Customizing terms and conditions using the SignedTCs.txt method

For the text that appears in the **Collect My Card** workflow in PIV systems, you must edit a text file called `SignedTCs.txt` in the `res\custom\js\` folder for each language folder on the MyID web server. If the file does not exist, you can create it.

For example:

`C:\Program Files (x86)\Intercede\MyID\Web\us\res\custom\js`

and:

`C:\Program Files (x86)\Intercede\MyID\Web\en\res\custom\js`

This allows you to use different terms and conditions for different languages.

In the `SignedTCs.txt` text file, include the text that you want to display for terms and conditions. You can use HTML formatting and must make sure that the characters you use are safe to display within a web page; for example, you must specify ampersands as `&` and not as bare `&` symbols.

For example:

```
<p><strong>Terms &amp; Conditions</strong></p>
<p>You must agree to the following conditions:</p>
<ol>
<li>The card remains the property of Example Corporation.</li>
<li>Use of this card may be revoked at the sole discretion of Example
Corporation for violation of Example Corporation's policies and
procedures.</li>
<li>...</li>
</ol>
<p>If you do not accept these terms and conditions, click
<strong>Reject</strong>.</p>
```

12.6.4 Customizing terms and conditions using the translation method

For the text that appears in the **Collect My Card** workflow in non-PIV systems, customizing the terms and conditions on non-PIV systems requires the use of the MyID Translator tool. Translate the text for the following translation IDs:

- `21487` – Terms and Conditions heading.

- `21488` to `21495` – each paragraph of the terms and conditions.

You can use HTML formatting and must make sure that the characters you use are safe to display within a web page; for example, you must specify ampersands as `&` and not as bare `&` symbols.

For information about the MyID Translator tool, contact customer support quoting reference SUP-138.

12.6.5 Storing signed terms and conditions

If you set the **Persist terms and conditions** 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 MyID audit report.

This 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.

13 License Management

MyID is installed with a standard trial license that allows you to add up to 25 user accounts and credentials to the system for up to 30 days.

If you are evaluating MyID, this may be all you need. If you have purchased MyID, you must request the licenses that have been ordered when you are ready to install them on the system.

Note: It may be easier to configure your implementation completely before requesting and installing additional licenses, in case you need to re-install the software.

Your license count determines the number of user accounts and credentials you can have in your system. For example, if you have 100 licenses, you can add up to 100 user accounts *and* issue up to 100 credentials. If each of your users will be issued two credentials (for example, a smart card and a mobile identity), for 100 users you would need 200 licenses.

For example:

Current licenses	Users	Issued Credentials	Result
100	95	95	You can add more users and request more credentials.
100	95	100	You can add more users, but cannot request any more credentials. Obtain more licenses if you need to request any more credentials.
100	100	95	You can request more credentials, but cannot add any more users. Obtain more licenses if you need to add any more users.
100	100	100	You cannot add any more users or request any more credentials. Obtain more licenses if you need to add any more users or request more credentials.

A *credential* is any identity issued by MyID; for example, a smart card, a token, a VSC, a device identity, or a mobile identity. Because a single user may require multiple credentials, you are recommended to consider carefully the number of credentials you intend to issue when you request your license from Intercede.

If you reach your license limit with *either* user accounts or issued credentials, you must request more licenses.

As you approach your license limit, a message is displayed when you add people to the system or request credentials.

The warning message is displayed to the operator when the number of user accounts exceeds the warning limit, or the number of issued credentials *plus* requested credentials reaches the license limit.

Email messages may also be sent to the designated email address specified in the **Licensing** workflow (see section *13.4*, *Updating warning messages*) when the number of user accounts or the number of issued credentials reaches the warning limit.

Your license may be time-limited. As you get closer to the license expiry date, you are presented with a message when you log in – this message changes color as the expiry date draws closer. You can see this message only if you have access to the **Licensing** workflow. Email messages are also sent to the designated email address as you get closer to the license expiry date. When the license expires, you will not be able to access any workflows, unless you have permission to use the **Licensing** workflow, in which case you can access the **Licensing**, **System Status**, **Audit Reports** and **System Events** workflows.

Each license is tied to a particular MyID installation. If you are running multiple installations, each with it own unique database, you must have a license for each one. However, if you are running a system with multiple application or web servers against a single database, you need a single license for your system.

The **Licensing** workflow is used to:

- View current license status

- Generate requests for additional licenses

- Install received licenses

- Change the warning threshold and the email address for notifications.

13.1   View current license status

From the **Configuration** category, select the **Licensing** workflow to view current license status.

- **Current License** is displayed as **Initial License** until you have generated license requests, and received and installed your licenses.

- **Company Name** and **Company Location** are required information when you generate a license request and will display appropriate information when you have installed the licenses.

- **Current No. of Licenses** is the total number of current user accounts or credentials you can have. For example, 100.

- **Current No. of Users** is the number of current user accounts you have (the number created minus the number deleted). The maximum number is also displayed. This is not the number of users currently logged on to the system. For example, `25 / 100` means that you have 25 users out of a maximum of 100.

  As long as the first number is lower than the second number, you can add more users.

- **Current No. of Credentials** is the number of issued credentials. The maximum number is also displayed. This does not include any credentials that have been requested but not yet collected.

  As long as the first number is lower than the second number, you can request more credentials.

  Note: Under certain circumstances, you can request a number of credentials that will take you not just *up to*, but *over*, the license limit. End-users will still be able to collect these requested credentials; however, you must request more licenses as soon as possible, as once the number of *issued* credentials exceeds your license limit, you will be unable to request any more.

- **No. of Pending Requests** is the number of credentials that you have requested, but have not yet been collected.

  Note: This is not a real-time count. The number of pending requests is recalculated every two hours.

- **Warning Limit** is the number of users or credentials that must be reached for a warning email message to be triggered.

- **Warning Email Address** is the email address that will receive an automatically generated license warning email.
- **Expiry Date** is the date your current license expires.
- **Type** is the type of license; for example, Standard or Evaluation Only.

If you have additional license features installed, they are listed on this page.

From this page, you can:

- **Request** more licenses – see section *13.2*, *Requesting licenses*
- **Install** received license information – see section *13.3*, *Installing license details*
- **Update Warning** messages – see section *13.4*, *Updating warning messages*

13.2 Requesting licenses

When you request licenses, you generate a request that can either be sent by email directly to the application vendor or saved to disk and then submitted later.

1. From the **Configuration** category, select the **Licensing** workflow. Your current license status is displayed.
2. Click **Request**.
3. Enter your **Company Name**.
4. Enter your **Company Location**.
5. Specify the number of licenses you require.

   Note: This is the total number of licenses you require, not just an additional value. For example, if you already have 1000 licenses and have require an additional 500 licenses, you must enter 1500.
6. Click **Generate**.
7. The **License Request** is displayed. You can click:
   - **Save As** to save the details as a text file in the location of your choice.
   - **Email** to send the license request to your vendor. Your default email client opens, displaying the message.

   You can select one or both of these actions.
8. Click **Finish** to leave the workflow.

Note: If you make a mistake when generating a license request, return to the workflow and generate a replacement.

13.3 Installing license details

When you receive your updated license file, you must import the information it contains to MyID to make the licenses available.

1. From the **Configuration** category, select the **Licensing** workflow. Your current license status is displayed.
2. Click **Install**.
3. Either:
   - Copy and paste the contents of the license file into the **License** text area.
   - Click **Browse** and locate the file on your file system. The contents of the file are displayed in the **License** text area.
4. Check that your company name, location and number of licenses are correct. If they are not, do not continue.

5. The **Warning Limit** is set to 90% of the total number of licenses. Change this if appropriate.

6. Enter the **Warning Email Address** if it is required and not already displayed. You can change it if necessary.

7. Click **Install**.

13.4 Updating warning messages

You can update the threshold for generating a warning message and the email address to be sent notification messages at any time.

1. From the **Configuration** category, select the **Licensing** workflow.

2. Click **Update Warning**.

3. Enter the number of current user accounts or issued credentials that will trigger the warning in **Warning Limit** – the message will be sent when this number is reached.

4. Enter or change the **Warning Email Address** if necessary.

5. Click **Update**.

14 Email Notification

MyID can be configured to automatically send email messages to individuals, triggered by specified events. For example, a message may be sent to someone who has requested a card stating that the card is now ready for collection or to a cardholder when a certificate on the card is about to expire. The email message can contain instructions for the recipient and further messages can be sent if a required action is not completed in a specified time.

Note: You can skip this section if you do not want to change the provided email templates or the triggers for messages.

Warning: If you want to use email notification, you must set up an SMTP server within MyID – see the *Installation and Configuration Guide* for details.

14.1 System-wide email settings

14.1.1 Switching email notifications on or off

You can switch email notifications on or off.

Note: The default setting is email notifications switched off. If you want to send email notifications, switch this setting on.

1. From the **Configuration** category, select **Operation Settings**.

2. Click the **Notifications** tab.

3. Set the **Send Email Notification** option.

4. Click **Save changes** to save your changes.

14.1.2 Email format

To specify the email format:

1. From the **Configuration** category, click **Operation Settings**.

2. On the **Notifications** tab, select a value for the **Mail Format** option.

    You can use one of the following values:

    - ◆ `TEXT` – email messages are sent as plain text.

    - ◆ `HTML` – email messages are sent in HTML format.

3. Click **Save changes**.

14.1.3 Email codepage

The codepage determines which characters can be used in the email messages; for example, you may want to use Hebrew or Cyrillic characters in addition to the standard 128 ASCII characters.

For messages in TEXT format (see section *14.1.2*, *Email format*), the code page is automatically detected.

If you want to specify the code page for messages in HTML format, you can set the charset for your HTML; for example, for Hebrew, you can add the following to the HTML header:

```
<META HTTP-EQUIV="Content-Type" CONTENT="text/html; CHARSET=iso-8859-8">
```

For most email messages, the following charset is suitable:

```
<META HTTP-EQUIV="Content-Type" CONTENT="text/html; CHARSET=utf-8">
```

14.1.4 Email separator

The **Email separator** configuration option allows you to specify the separator used to divide multiple email addresses when sending email messages.

To change the email separator:

1. From the **Configuration** category, click **Operation Settings**.

2. On the **Notifications** tab, enter a value for the **Email Separator** option.

   The default is a semicolon (;).

3. Click **Save changes**.

14.1.5 Changing the recipient of administrator messages

The email address of the account that will receive all administrator messages is displayed and can be changed in the **Operation Settings** workflow.

Note: You can update the email address for licensing notifications using the **Licensing** workflow. See section *13.4*, *Updating warning messages*.

1. From the **Configuration** category, select **Operation Settings** and then the **Notifications** tab.

2. The current email address is displayed in **Administration Email**. Replace this with an updated address if necessary.

3. Click **Save changes** to save your changes.

14.1.6 Setting the number of email notifications

The **Single Email Notification** option allows you to specify whether a credential holder will receive one email message for all certificates on a card or device (when it is set to Yes) or a separate message for each certificate (when set to No). In either case, you can collect each of the renewed certificates.

To set the option:

1. From the **Configuration** category, select **Operation Settings**.

2. Click the **Notifications** tab.

3. Set the **Single Email Notification** option.

4. Click **Save changes**.

14.2 Changing email messages

You can edit the subject line and body of any of the provided email templates in MyID.

If you enable HTML format, you can send messages formatted in HTML (see section *14.1.2*, *Email format*) including embedded images. You can also specify the code page if you want to send messages using character sets other than the standard ASCII characters (see section *14.1.3*, *Email codepage*).

1. Select the **Configuration** category and then the **Email Templates** workflow.

2. Select the email template you want to edit. Click **Modify**.

   You are now in the **Edit Email Template** stage.

3. Edit the **Subject** for the template.

   This forms the subject line of the email and must contain some information. You can use variables that are substituted when the template is run. See step 5 for definitions of the substitutions.

4. Select or clear the **Enabled** option.

   If the **Enabled** option is cleared, the email specified by the template will not be sent.

5. Type the **Template Body**.

   This is the body of the email. You can use variables that are substituted when the template is used.

   Note: Some variables are replaced by the same information in all templates; others are substituted by different information depending on the event that triggers the email message.

Variable	Description
`%n`	A new line.
`%t`	A tab.
`%x`	The URL of the MyID installation. Not currently supported.
`%u`	The URL for mobile issuance. This is the content of the **Mobile Certificate Recovery Service URL** configuration option.
`%2`, `%3` and so on	Parameters that are substituted by the email trigger when the email is sent. For example, these might be the user's name, the card serial number, or a comment entered in the workflow by an operator. If the parameter value contains spaces (for example, a logon name) and you are using the parameter to build a URL (which does not allow spaces), you can use the following syntax to replace any spaces with + signs: `{%parameter:URI}` For example, `{%logonName:URI}` might become `Jane+Smith`. **Note:** If you want to include additional parameters to the existing, standard email templates, this will require custom changes to MyID. Contact Intercede professional services for details.

For example, an email template like this:

```
Your Certificate renewal date is soon approaching. You have %2 days
to implement your Certificate Renewal procedure. %nPlease follow the
instructions for renewing your certificate.
```

Will generate a message like this:

```
Your Certificate renewal date is soon approaching. You have 14 days
to implement your Certificate Renewal procedure.

Please follow the instructions for renewing your certificate.
```

6. From the **Transport** drop-down list, select one of the following:

   ◆ **Email** – the template is to be used for email messages.

   ◆ **SMS** – the template is to be used for SMS messages.

7. If you want to sign the email message, select the **Signed** option.

   Note: You must have the **Sign outgoing emails** option for the SMTP server in the **External Systems** workflow set. See the *Installation and Configuration Guide* for details.

8. Click **Save**.

14.3 Standard templates

Standard email templates and triggers are provided with MyID and are used unless you specify something different. The templates contain both fixed text, which is identical in every message, and variables, which are replaced with information stored in MyID and may contain different values in different messages.

Template Name	Description	ID
Apply Update Notification	Sent to cardholders when an update is available.	6
Apply Update Notification Mobile	Sent to mobile users when an update is available.	142
Authentication Code	Sent to a cardholder when an activation code has been issued.	27
Authentication Code Notification	Sent to a cardholder when an authentication code has been issued.	26
Automatic Job Cancellation Email	Sent to a cardholder when a job has been cancelled.	113
Cancel Card Notification	Sent to cardholders when a card has been canceled. Deprecated. IKB-173 – **Cancel Card** has been replaced by **Erase Card**. **Erase Card** does not have a pre-configured notification. If you want to send notifications when cards have been erased, contact customer support, quoting reference SUP-222.	5
Card PIN Notification	Sent to card or token holders to notify them of the PINs associated with their cards.	11
Certificate Authority Status	Sent to an administrator when an error has occurred with the certificate authority.	106
Credential Licence Limit approaching	Sent to an administrator (specified in the **Licensing** workflow) when the number of credentials is getting close to, has reached, or exceeds the number allowed by the license.	135
Credential Licence Limit exceeded		136
Credential Licence Limit reached		137
Email signing certificate invalid	Sent to an administrator when an application server's email signing certificate is incorrectly configured, or not present.	145
Failed Email Notification	Sent to an administrator when an email notification message has failed to reach its intended recipient.	12
Issue Card Notification	Sent to a cardholder when a card is ready for collection.	4
Issue Token Notification	Sent to a token holder when a token is ready for collection.	7
Job Logon Code	Sent to the cardholder when the card is ready for collection. Contains a one-time logon code.	134
Job OTP	A one-time password sent to a user to enable them to collect a job.	131
Job OTP No Device	A challenge code sent to a user to enable them to collect a job.	138
Job OTP With Device	A challenge code sent to a user to enable them to collect a job.	139

Template Name	Description	ID
License Limit approaching	Sent to an administrator (specified in the **Licensing** workflow) when the number of users is getting close to, has reached, or exceeds the number allowed by the license.	8
License Limit exceeded		9
License Limit reached		10
Logon Code Notification	Sent to a cardholder when a logon code has been issued.	104
LogonCodeLockout	Sent to the user when their logon code is answered incorrectly too many times and it becomes locked	140
Mobile Provisioning	Sent to a mobile user when their mobile identity is ready to be collected.	124
Mobile Soft Certificate Validated	Sent to a cardholder when credentials are ready for collection.	120
Notification Failed	Sent to an administrator when a URL notification has failed – and there will be no further attempts.	111
Notification Failure	Sent to an administrator when a URL notification has failed – and there will be further attempts.	105
Notification Success	Sent to an administrator when a URL notification has succeeded.	107
QALockout	Sent to a cardholder when their security questions are answered incorrectly too many times and the phrases are locked	132
Renew Card Notification	Sent to a card recipient when a card is approaching or has reached its expiry date.	121
Renew Card Notification First		122
Renew Card Notification Second		123
Renew Certificate Notification	Sent to a certificate holder when their certificates are nearing or have reached the expiry date.	3
Renew Certificate Notification Expired (SMS)	Sent to the certificate recipient when a certificate has expired.	127
Renew Certificate Notification Expired Mobile	Sent to a mobile certificate holder when their certificates are nearing or have reached the expiry date.	130
Renew Certificate Notification First	Sent to a certificate holder when their certificates are nearing or have reached the expiry date.	1
Renew Certificate Notification First (SMS)	Sent to the certificate recipient via SMS when a certificate is approaching its expiry date.	125
Renew Certificate Notification First Mobile	Sent to a mobile certificate holder when their certificates are nearing or have reached the expiry date.	128
Renew Certificate Notification First Mobile (SMS)	Sent to the certificate recipient when a certificate is approaching its expiry date	200
Renew Certificate Notification Second	Sent to a certificate holder when their certificates are nearing or have reached the expiry date.	2
Renew Certificate Notification Second (SMS)	Sent to the certificate recipient when a certificate is approaching its expiry date.	126
Renew Certificate Notification Second Mobile	Sent to a mobile certificate holder when their certificates are nearing or have reached the expiry date.	129

Template Name	Description	ID
Replacement Card Notification	Sent to a cardholder when a replacement card is ready for issue.	102
Reprovision Notification	Sent to the user when reprovision is ready for collection onto their devices.	143
Reprovision Notification Mobile	Sent to the user when reprovision is ready for collection onto their mobile devices.	144
Software Certificate Notification	Sent to a user who has a pending software certificate request.	112
Time License Expired	Sent to an administrator (specified in the **Licensing** workflow) when the license has expired.	101
Time License Expiring	Sent to an administrator (specified in the **Licensing** workflow) when the license has expired.	100
Unlock Code	Sent to a cardholder when an unlock code has been issued.	28

Note: Additional PIV-specific email templates are also available on PIV systems.

Three different templates are associated with card renewal, certificate renewal and the license limit. They are used to:

- Notify the recipient that some action is required.
- Remind the recipient that some action is required.
- Inform the recipient that the threshold has passed.

For more information on notifications, including certificate authority status notifications, contact customer support quoting reference SUP-222.

14.3.1 Triggering the notification

Notifications are triggered at specific times before the event, or on the event itself. The default settings are as follows:

Days left	Email template	Description
0	Apply Update Notification	Apply update
0	Cancel Card Notification	Cancel card task. Deprecated.
28	Renew Card Notification	CardRenewal
7	Renew Card Notification First	CardRenewal
3	Renew Card Notification First	CardRenewal
1	Renew Card Notification First	CardRenewal
0	Renew Card Notification Second	CardRenewal
28	Renew Certificate Notification First	CertRenewal
21	Renew Certificate Notification Second	CertRenewal
14	Renew Certificate Notification Second	CertRenewal
7	Renew Certificate Notification Second	CertRenewal
0	Renew Certificate Notification	CertRenewal
0	Issue Card Notification	Issue card task
0	Replacement Card Notification	Issue replacement card task

Days left	Email template	Description
0	Issue Token Notification	Issue Token Task
0	Reprovision Notification	Reprovision Card task
0	Software Certificate Notification	Request a soft (browser) certificate for a user

For example, for the CertRenewal notifications (shaded in the above table):

- An initial message is sent to the certificate holder 28 days before a certificate expiry date.

  When the first message is sent out, MyID creates a job to renew the user's certificate.

- A reminder message (the same template, but with a different number of remaining days being substituted for a variable) is sent at 21 days, 14 days and 7 days before the certificate expiry date.

- A message stating that the certificate has expired is sent on the certificate expiry date (0 days).

If you want to alter when these notifications are sent, contact customer support quoting reference SUP-222.

14.4 Adding a new email template

Note: This workflow allows you to create new email templates, but linking them to notification events in MyID requires further customization; you will be unable to use any new templates without this customization. For more information, contact customer support quoting reference SUP-222.

1. From the **Configuration** category, select **Email Templates**.

2. Click **New**.

   The **Edit Email Template** screen appears.

3. Type a **Subject** for the template.

   This forms the subject line of the email. You can use tokens that are substituted when the template is run; see the section on the **Template Body** in Step *7* below.

4. Type a **Template Name**.

5. Type a **Template Description**.

   This is an internal description that allows you to identify the purpose of the template; it does not appear in the email.

6. Select or clear the **Enabled** check box.

   If the **Enabled** check box is cleared, the email specified by the template will not be sent. You can use this to disable an email template.

7. Type the **Template Body**.

   This is the body of the email. You can use tokens that are substituted when the template is run:

Token	Description
`%n`	A new line.
`%t`	A tab.
`%x`	The URL of the MyID installation. Not currently supported.
`%appServer`	The hostname of the application server on which the email is processed.
`%2`, `%3` and so on	Parameters that are substituted by the email trigger when the email is sent. For example, these might be the user's name, the card serial number, or a comment entered in the workflow by an operator. If the parameter value contains spaces (for example, a logon name) and you are using the parameter to build a URL (which does not allow spaces), you can use the following syntax to replace any spaces with `+` signs: `{%parameter:URI}` For example, `{%logonName:URI}` might become `Jane+Smith`. **Note:** If you want to include additional parameters to the existing, standard email templates, this will require custom changes to MyID. Contact Intercede professional services for details.

For example, you can type a template body such as:

```
This is a message for %2. Your card of type %3 with the serial
number %5 has been cancelled.%nThe reason for the cancellation is:
%5.
```

Which would become:

```
This is a message for John Smith. Your card of type Datakey Model
330 with the serial number 30366716 has been cancelled.

The reason for the cancellation is: The card was reported lost.
```

When you set up the email trigger, you will set up substitutions for these tokens. MyID can then pull information from the current workflow and insert it into the email message.

8. Set up the **Substitution Legend**.

   Make sure you take a note of the tokens you have used and what they are going to represent. This information is required for any custom email triggers that are created to use this template.

   Click **Add substitution**, then type the **Token** and **Description**. Click **Add substitution** again to add more tokens to the legend.

9. From the **Transport** drop-down list, select one of the following:

  ◆ **Email** – the template is to be used for email messages.

  ◆ **SMS** – the template is to be used for SMS messages.

10. If you want to sign the email message, select the **Signed** option.

   Note: You must have the **Sign outgoing emails** option for the SMTP server in the **External Systems** workflow set. See the *Installation and Configuration Guide* for details.

11. Click **Save**.

Known issues

▪ **IKB-238 – Duplicate email template names will prevent a notification from being sent.**

   It is possible to create a new email template in MyID and save it using the same template name as an existing template. This prevents the notification from being sent.

14.5 Using the Notifications Management workflow

To view, resend, or cancel notifications:

1. From the **Configuration** category, select **Notifications Management**.
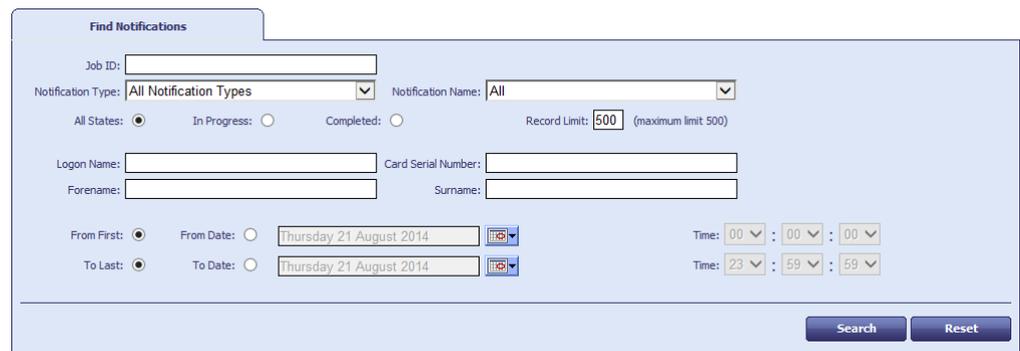
2. In the Find Notifications screen, enter some or all of the criteria for the notifications you want to find:

  ◆ **Job ID** – type the ID of the job for which the notification has been triggered.

  ◆ **Notification Type** – select one of the following:

     ▫ **All Notification Types** – returns notifications of all types.

     ▫ **EMAIL** – returns notifications that are sent by email.

     ▫ **URL** – returns notifications that are sent to a web listener.

     ▫ **SMS** – returns notifications that are sent to a mobile phone.

     ▫ **Web Service** – returns notifications that are sent to a web service.

  ◆ **Notification Name** – select a name of a notification from the drop-down list. These are the names assigned to different notifications in the `Notifications` table in the MyID database, appended with their notification ID.

  ◆ **All States/In Progress/Completed** – select whether you want to view all notifications, only those that are in progress, or only those that have been completed.

  ◆ **Record limit** – type the maximum number of records to return.

   The default limit is `500`. You can specify a number between `1` and `500`.

- **Logon Name** – type the MyID logon name of the person for whom the operation that triggered the notification was carried out; for example, for a card issuance notification, this is the user to whom the card was issued.

- **Card Serial Number** – type the serial number for the card involved in the notification.

- **Forename** and **Surname** – type the forename and surname of the person for whom the operation that triggered the notification was carried out

- **From** – either from the earliest initialization date in the database (**From First**) or from a specific date (**From Date**).

- **To** – either to the latest initialization date in the database (**To Last**) or to a specific date (**To Date**).

  Use the calendar buttons to select specific dates.

3. Click **Search**.

4. To view the details of a notification, double-click the line.

   Note: You can resend or cancel the notification from this pop-up screen as well as from the main screen.

5. To cancel notifications:

   a) Select one or more notifications that are **In Progress**.

      You cannot cancel notifications that have completed.

   b) Click **Cancel Notify**.

6. To resend notifications:

   a) Select one or more notifications.

   b) Click **Resend**.

   Note: You cannot resend email notifications that have completed.

7. Click **Done**.

   Note: After you have resent a notification, that notification's entry in the search results is disabled and grayed out in the list. This allows you to determine easily which notifications you have worked on. To make additional changes to the same notification, click the show form button and click **Search** again.

   If you cancel a notification, that notification's entry is removed from the list.

15 Changing List Entries

The **List Editor** is used to change the contents of drop-down lists associated with custom attributes within MyID. Custom attributes are fields that have been added to the standard application, either by your organization or by Intercede on your behalf. If any of these new fields are associated with drop-down lists, you can change their contents using this workflow.

For example, in a PIV system, you can change the lists for emergency roles and eye colors, and so on.

You can use the **List Editor** to change the list of document types used as Identity Documents to authenticate users. The lists of available documents are determined by the **Authenticate Person Document1** and **Authenticate Person Document2** lists.

Note: The information you enter into these lists is not translated.

1. From the **Configuration** category, select the **List Editor** workflow.

2. Select which list you want to edit in the **Picklist** field.

3. If you want to make changes to an existing item, select it.

    The item's current details are displayed at the bottom of the page.

    To delete the selected item, click **Delete Item**.

    Note: To select a different item, click the box next to the entry. To change your selection, click a different box. You can select only one item at a time. If you want to clear your selection, click **Deselect Item**.

4. To enter details for a list entry:

    a) In **Display Value**, enter or change the value that is displayed in the list.

    b) In **Value**, enter the value that is stored in the database when this option is selected.

    c) If you want this entry to be the default option when the list is displayed, select **Default**.

    d) Click either **Add New Item** (if this is a new list entry) or **Modify Item** if you are changing an existing entry.

        Note: Add New Item is disabled until you have entered the required details.

    Your new or modified list items are now available for selection.

Warning:	If you change the value of a list entry, records that contain the previous values will not be affected. You need to carefully consider how your changes will affect the consistency of your data.

16 Uploading and Working with Images

Note: Associating images with people's records is optional. If you are not capturing images, you can skip this section.

MyID 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 for new installations, images are stored as binary objects in the database. If you have upgraded from an older system, MyID may be set up to store images on the web server – contact customer support for more information, quoting reference SUP-103.

If you are storing images on the web server, you must specify the folder to use.

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.

16.1 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 section *33.5*, *Video page (Operation Settings)*.

16.1.1 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.

16.2 Creating a separate database to store images

You can set up MyID to store the binary objects in a separate database from the main MyID database. This works in a similar way to setting up a database for archived audit data – you must create an archive database, which is a copy of the MyID database with no operational data, and configure the `.udl` file to point at the correct database. By default this `.udl` file points to the main MyID database.

To set up a separate binary file storage database:

1. Create an archive database to use for your binary files.
2. Set the permissions for the MyID named COM+ user.

a) In Microsoft SQL Server Management Studio, expand the **Security** folder and select **Logins**.

b) Right-click the service account user and select **Properties**.

c) In the Select a page section, click User Mapping.

d) Select the database you created to hold the binary objects.

e) Grant the account the following roles for the database:

- `public`

- `db_owner`

- `db_datareader`

- `db_datawriter`

f) Click **OK**.

3. Update the `.udl` file to point to the correct database:

a) On the MyID application server, open the Windows `System32` or `SysWOW64` folder.

b) Double-click the binary `.udl` file; for example, `MyIDbinary.udl`. The name of the `.udl` file depends on the name you set for the MyID database; for example, if you specified the name `MyID2012` for the database, the `.udl` file for the binary objects will be `MyID2012binary.udl`.

c) Set the properties to point to the server and database you created to store the binary information.

16.3 Storing images on the web server

The following settings are only applicable if you are storing images on the web server.

Note: By default, new installations of MyID will store images in the database rather than in the web server; only systems that were upgraded from older systems will store images 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.

- 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.

- Set **Image Upload Server** to the name or IP address of the MyID server to which you want to upload images.

  You must have the following DLLs registered on the image upload server:

  - `FileTransfer.dll`

  - `DataExchange.dll`

  You can find these DLLs in the `Components\Core` folder in your MyID installation.

  Note: See also section *9.2*, *Configuring the image location* for details of configuring this value.

- 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 `C:\Program Files (x86)\Intercede\MyID\Web\upimages` folder on the web server.

  If you change this setting you must change the virtual directory in IIS. See section *16.3.3*, *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.

16.3.1   Using sub-folders

If you have a large number of images in your uploaded images folder (by default, `C:\Program Files (x86)\Intercede\MyID\Web\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.

16.3.2   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.

16.3.3 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 6. If you are using a later version of IIS, see your Microsoft documentation for information on how to carry out these changes.

2. Expand **Web Sites** then **Default Web Site**.

3. Map the `upimages` virtual directory at this level to the **File Store Location**.

   a) Right-click on the `upimages` virtual directory.

   b) Select **Properties** from the menu displayed.

   c) On the Virtual Directory page, click **Browse** 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) Click Default Web Site.

   b) Click the **Stop** button on the toolbar, then click the **Start** button on the toolbar.

   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
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
    <system.webServer>
        <handlers accessPolicy="Read" />
        <directoryBrowse enabled="false" />
        <httpErrors>
            <clear />
        </httpErrors>
    </system.webServer>
</configuration>
```

16.4 Working with 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.
- Use a signature pad to capture a signature.

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, scanners and signature pads 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

16.5 Obtaining an image

The basic **Image Capture** window is displayed. Depending on the options available to you, the window looks similar these examples.

In all cases, some of the buttons are disabled; they are enabled when they can be used. One version of the window enables you to choose between using a webcam (the **Video** option at the top of the window) and an existing image (the **Photograph** option).
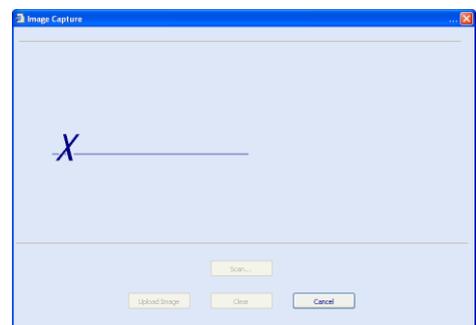
16.5.1   Using an existing image

To use an existing digital image:

1.   Click the **Photograph** 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**.
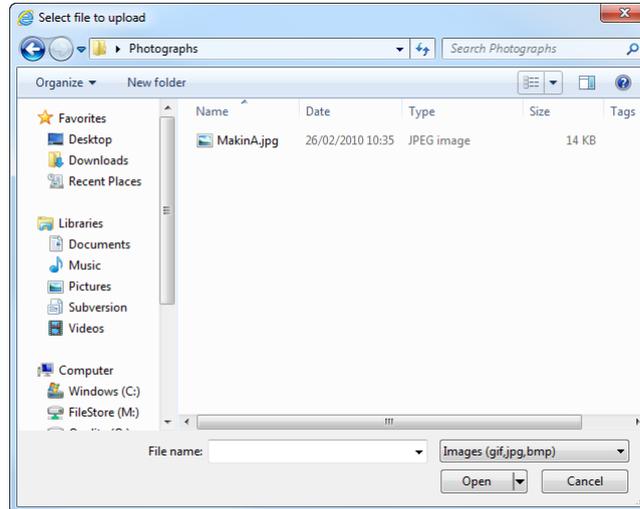
Your chosen image is now displayed in the "source" display area of the **Image Capture** window. The path to the file is displayed below the image.
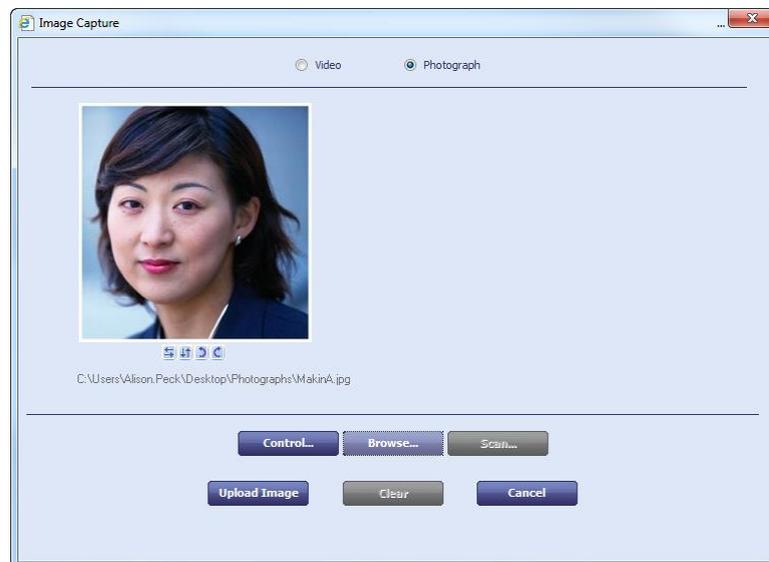
16.5.2   Using a webcam to capture an image

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. The current live feed (video) is displayed in the area to the left of the **Image Capture** window.
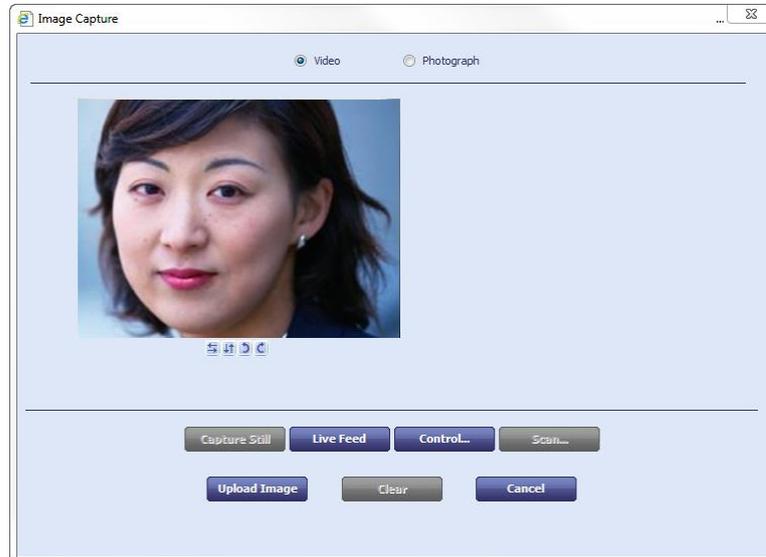
3. When the image you want is displayed, click **Capture Still** to freeze the frame.

    If you want to select a different image, click **Live Feed** to resume the video.

Changing the settings of the webcam

Two images are shown to the right of the picture, used to alter the quality of the image.

Click this image to display a window that enables you to change some settings for the video. For example, you may be able to change the resolution of the picture. The options available depend on the webcam you are using. An example is shown below.

Note: The **Settings** button also displays this window.
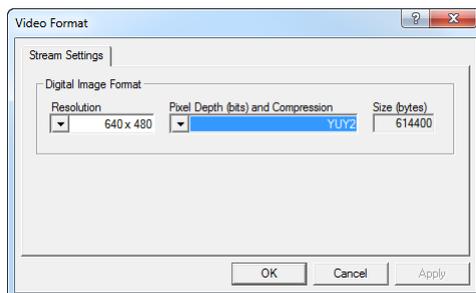
Click this image to display a window that enables you to change some of the settings associated with the webcam. The options available depend on the model of camera attached to your machine. An example is shown below.
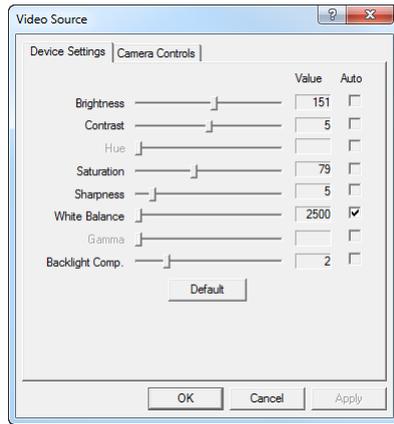
16.5.3 Using a scanner to capture an image

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.
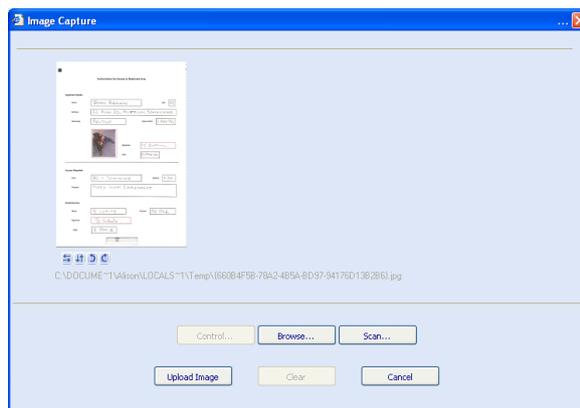
16.5.4 Capturing a signature using a signature pad

Click the placeholder image or an existing signature to open the **Image Capture** window. Ask the person whose signature you want to record to sign the signature pad using the stylus provided. It may take a few seconds for the signature to appear in the source area. A preview may also be displayed automatically.

To capture another signature, click the **Clear** button and ask the person to sign the pad again.

16.6 Rotating or flipping the image

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.

Note: This option is not available for signatures captured using a signature pad.

🔄 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 90º anti-clockwise.

↻ Rotates the image 90º clockwise

16.7 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.
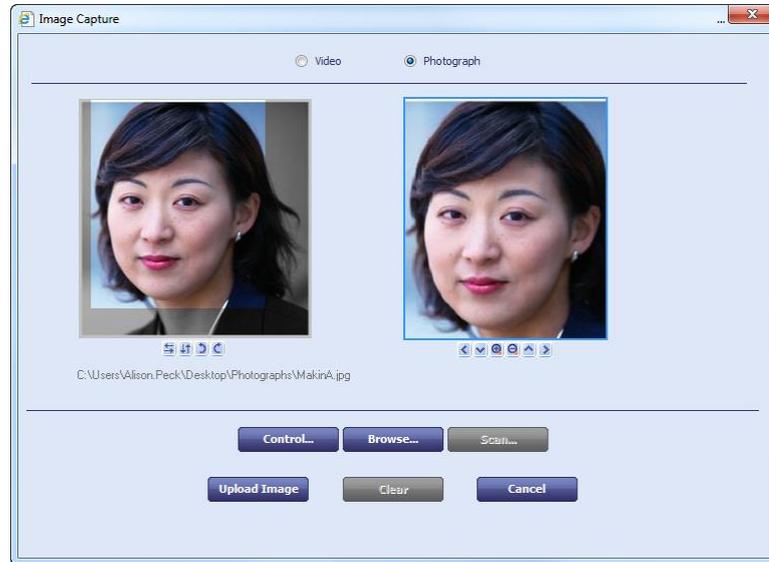
3. To change your selection, you can either:

   ◆ 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)

16.8 Enhancing the image

You can improve the appearance of your selection, by changing the contrast or brightness of the picture.
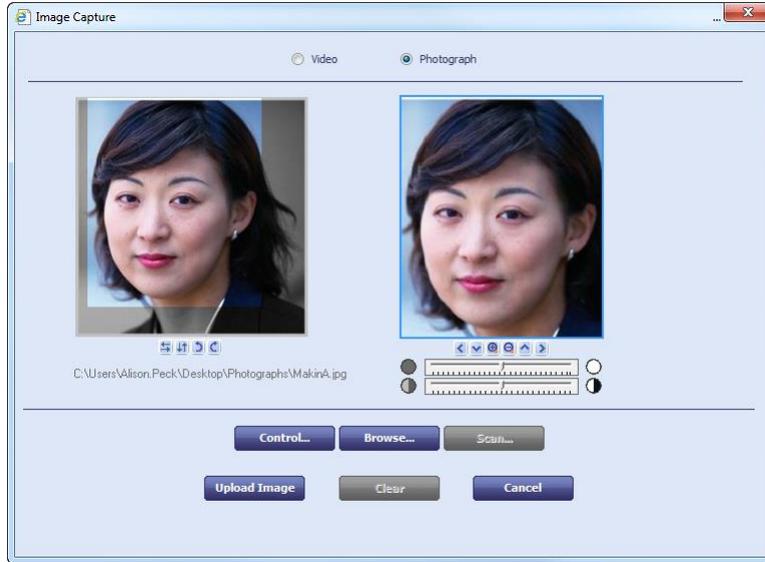
Note: The changes you make only affect your selection – the original image is not changed.

The **Control** button displays 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.

16.9 Uploading the image 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.

17   Managing Keys

MyID works with keys in a variety of ways. The GenMaster utility sets up the master keys for the system, and can be used to generate keys to work with HSMs.

The **Key Manager** workflow allows you to store transport keys, and allows you to work with 9B keys for FIPS 201/PIV systems.

The **Manage GlobalPlatform Keys** workflow allows you to work with factory and customer GlobalPlatform keysets. See section *8.3*, *Manage GlobalPlatform keys* for details.

17.1   Using GenMaster

GenMaster is used during the installation of MyID to decide how the master keys for the system will be stored and also to set the password for the startup user.

The GenMaster application remains accessible from the **Start** menu and can be used to reset the startup user password if necessary. It can also be used to generate secret keys to enable MyID to interoperate with other systems, including HSMs.

Further details on the use of GenMaster to generate secret keys are provided in the *Installation and Configuration Guide*.

17.2   The Key Manager workflow

The Key Manager workflow allows you to store keys; for example, the transport key for a key ceremony, or a PIV 9B key.

If you have a PIV system, you need to enter the values of secret shared keys to enable the smart card management system to authenticate (and therefore manage) the smart cards.

9B keys and related specifications are defined in *SP800-73-3 – Interfaces for Personal Identity Verification* available from the National Institute of Standards and Technology (NIST) website at http://www.nist.gov

For information on PIN generation keys, see section *10*, *PIN Generation*.

Warning:	If new keys are imported to or generated on the HSM during this workflow, you should take a new backup of the HSM. Keys stored on he HSM are business critical data.

17.2.1   Transport keys

To add a transport key (also known as a zone master key):

1. From the **Configuration** category, select **Key Manager**.

2. From the **Select Key Type to Manage** list, select **Transport Key(ZMK)** and click **Next**.

    Note: If you have only one key type defined in your system, MyID automatically selects that key and proceeds to the next stage.

3. Click **Add New Key**.

4. Type a **Key Name** and **Description**.

5. Select the **Encryption Type** from the drop-down list.

6. Select the attributes for the key:

    ◆ **Data Encryption Key** – the key is used to encrypt data (DEK).

    ◆ **Key Encryption Key** – the key is used to encrypt keys (KEK).

    ◆ **Allow Signing Operations** – the key is used for signing.

    ◆ **Exportable** – the key can be exported after it has been imported. This option is reserved for future use.

7. You can either enter the parts of the key using a key ceremony, or import the key from a file.

    ◆ To enter the key using a key ceremony:

8. Click **Enter Keys**.

9. If you have installed support for an HSM, you are asked whether you want to store the key in the database or on the HSM.

    If an HSM is available, Intercede recommends that you use it as it provides stronger protection for the key.

Select the location, then click **OK**.
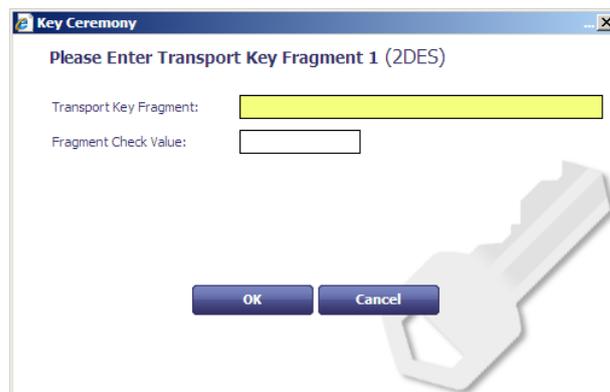
10. In the **Key Ceremony** dialog, enter the first part of the transport key.

    You can optionally enter the **Check Value** to ensure that you have entered the transport key fragment correctly. Check values are usually provided for each fragment the supplier of the transport key.

11. Click **OK**, then enter the second and third parts of the transport key.

    To import the key from an XML file:

    a) Click **Import Keys**.

    b) Select the file containing the key information, then click **Open**.

    c) Click **Save**.

    Note: you can not edit or delete a key once you have entered it. However, if you add a key with the same name as an existing key, it replaces the previous version, and increases the **Version** number of the key.

17.2.2 Factory 9B keys

When PIV cards are manufactured, they are provided with a factory key. You will have been given this factory 9B key by your smart card supplier; this is either 32 or 48 characters in hexadecimal format.

1. From the **Configuration** category, select **Key Manager**.

2. From the **Select Key Type to Manage** list, select **PIV 9B Card Administration Key** and click **Next**.

3. Click **Add New Key**.

4. Select the **Credential Type** from the drop-down list. This is the type of card you are using.

5. Select the attributes for the key if required:

   ◆ **Exportable** – the key can be exported after it has been imported. This option is reserved for future use.

6. Select **Factory** from the **Key Type** drop-down list. This means that you are using the key provided by your supplier.

7. From the **Key Diversity** drop-down list, select **Static** for static keys, or one of the Diverse options for diversified keys.

   See the *Smart Card Integration Guide* for the key diversity option for your type of card.

8. From the **Encryption Type** drop-down list, select the encryption used.

   See the *Smart Card Integration Guide* for the encryption option for your type of card.

Warning:	Make sure you select the **Encryption Type** supported by the devices you are using. If you select the wrong length of key, you will not be able to issue cards.

9. Type a **Description** for the key.

10. If you are storing the key in the database, choose one of the following options:

   ◆ **Automatically Generate Encryption Key in Software and Store on Database** – this option automatically creates an encryption key.

   ◆ **Encryption Key** – type the hexadecimal key in the box.

   ◆ **Use Key Ceremony** – if you have the key in key ceremony format (encrypted by a Transport Key), select this option. When you click **Enter Keys**, the key ceremony wizard will launch, allowing you to enter the key ceremony data into the database or HSM (if available).

11. If you are storing the key on an HSM, and have selected **Diverse** key diversity, select one of the following options:

   ◆ **Automatically Generate Encryption Key on HSM and Store on HSM** – this option generates a key on the HSM.

   ◆ **Existing HSM Key Label** – if you have an existing key on your HSM that you want to use, type its label.

   Note: If an HSM is available, Intercede recommends it is used as it provides stronger protection for the key.

12. Click **Save**.

17.2.3 Customer 9B keys

You can configure a customer 9B key for PIV systems. When issuing a card, MyID will change the factory 9B key to the customer 9B key.

Note: If the customer 9B key for a PIV card is not created, the card will continue to use the factory 9B key after issue. The factory 9B key may be known to third parties, so may not be secure. We recommend that a diverse customer 9B key is generated in the HSM for all PIV device types to be issued. PIV compliant installations *must* specify diverse customer 9B keys in the HSM.

This means that if you need to be able to reuse the card in different installations, you must cancel the card – canceling a card changes the customer 9B key back to the factory 9B key so the card can be reused.

Note: if you lose the key data held in the database, you will no longer be able to cancel or unlock the card.

1. From the **Configuration** category, select **Key Manager**.

2. From the **Select Key Type to Manage** list, select **PIV 9B Card Administration Key** and click **Next**.

3. Click **Add New Key**.

4. Select the **Credential Type** from the drop-down list. This is the type of card you are using.

5. Select the attributes for the key if required:

    ◆ **Exportable** – the key can be exported after it has been imported. This option is reserved for future use.

6. Select **Customer** from the **Key Type** drop-down list.

7. Select **Static**, **Diverse2**, or **Diverse108** from the **Key Diversity** drop-down list.

    Intercede recommends using diverse 9B customer keys as this enhances the security of the solution.

    See the *Smart Card Integration Guide* for the appropriate diversity option for your type of card. If the guide does not list the diversification algorithm for your card type, choose **Diverse2**.

8. Select the same **Encryption Type** as you specified for the factory key.

9. Type a **Description** for the key.

10. If you are storing the key in the database, choose one of the following options:

    ◆ **Automatically Generate Encryption Key in Software and Store on Database** – this option automatically creates an encryption key.

    ◆ **Encryption Key** – type the hexadecimal key in the box.

    ◆ **Use Key Ceremony** – if you have the key in key ceremony format (encrypted by a Transport Key), select this option. When you click **Enter Keys**, the key ceremony wizard will launch, allowing you to enter the key ceremony data into the database or HSM (if available).

    If you are storing the key on an HSM, and have selected **Diverse** key diversity, select one of the following options:

    ◆ **Automatically Generate Encryption Key on HSM and Store on HSM** – this option generates a key on the HSM.

    ◆ **Existing HSM Key Label** – if you have an existing key on your HSM that you want to use, type its label.

    Note: If an HSM is available, Intercede recommends it is used as it provides stronger protection for the key.

11. Click **Save**.

18   The Audit Trail

MyID retains an audit trail of operations carried out within the system. This trail can be accessed using an audit report, and the items audited can be configured; see section *18.3*, *Specifying the items to audit*.

Note: MyID records dates as UTC dates and the local server time of the database server. By default, searches use the local server time of the database server.

You can use a separate database for audit records, and for archived audit records; see the ***Installation and Configuration Guide*** for details of setting up an archive database for these purposes.

18.1   Audit scope

The range of audit records available to view depends on the following permissions in the **Edit Roles** workflow:

▪ The **View Full Audit** option (in the **Reports** section) allows the operator to view all audit records in the system without restriction.

Reports	☑
Audit Reporting	☑
View Full Audit	☑
MI Reports	☐
System Events	☐
System Status	☐

▪ The **View User Audit** permission (in the **People** section) restricts the visible audit records to records relating to users within the operator's scope.

View User Audit	☑

You do not need the **View User Audit** option if you have **View Full Audit**.

If you have neither permission, you cannot view *any* audit records.

These permissions also allow you to view details on the **History** tab of the **View Person** workflow.

Note: If you have the **View User Audit** permission, but have a scope of Self, you cannot view any records.

18.2   Running the audit report

The Audit Reporting tool enables you to list events for either a single workflow or task within MyID or for all operations. This list can be filtered according to specific criteria. For example, you might want to view all people added by a particular operator or all events for a named MyID user.

To run an audit report:

1. From the **Reports** category, select **Audit Reporting**.

2. Complete the form as appropriate and select **Search**.

   Note: The **Reset** button returns all fields on the form to their original values before any changes were made.

3. The results are displayed in the **Selected Events** table. This table shows the date on which the events started and ended, if applicable, the type of event (for

example, adding a person or canceling a token) and a message associated with the event.

An information symbol appears beside each operation. The color indicates the type of operation.

You can browse through the **Selected Events** table, change the number of rows displayed and toggle the display of the table/Audit Reporting form.

You can also browse through blocks of events.

4. To print the report, click the print button.

5. To save the report, select **XML**, **CSV**, or **Excel** to select the format, then click the save button.

18.2.1 Information icons

The information icon next to each event is color-coded to indicate the status of the operation. Pointing to the icon shows its type as a tooltip. The table below describes each type.

	Shows that the operation was successful, for example, a person import completed successfully.
	Shows that the operation started but did not complete. This occurs when the person closes the client or clicks on a top-level menu to cancel an operation.
	Shows that the operation failed. This may happen, for example if there is a failed logon attempt.
	Shows that the operation was canceled, for example, the user clicked **Cancel** during the **Edit Groups** workflow.
	Shows that an error occurred (such as a server error) preventing the workflow from completing.
	Shows that a warning occurred while the operation was in progress.

18.2.2 Browsing through blocks of events

You can browse through blocks of events; the number of events in each block depends on the value set in the **Event Limit** field on the **Audit Reporting** form.

For example, if the Event Limit value is set to 100, when you run the report, the first batch of 100 events is shown.

Clicking the following button shows the next batch of 100:

Clicking the following button shows the previous batch:

18.3 Specifying the items to audit

The Audited Items workflow allows you to choose which data items are audited at different stages of individual workflows.

To use the Audited Items workflow:

1. Select **Configuration**, **Audited Items** to start the **Audited Items** workflow.

The workflow moves on to the **Audited Items** stage and loads the **Workflow Stages** form. This enables you to edit the audit details for a workflow stage.

2. From the **Operation** list, select the workflow you want to audit.

    The items currently audited for this workflow are displayed in the center of the form. The form shows at which stage the item is audited, whether the item is mapped to one of the pre-determined indexes to allow improved searching in the **Audit Report** workflow, and which label is displayed in the reports for this item.

3. To edit an individual stage and add or remove the items audited, click the appropriate **Edit Stage Details** radio button.

    The **Workflow Stages – Audited Items** screen is displayed.

4. If the stage is auditable, add or remove audited data items by checking or clearing the **Audited** option next to the item name.

    Note: Full details of the Item names and explanations of their meaning can be discussed with customer support upon request.

5. For any selected item, you can select to which Index you want to map this data and type the **Alternate Label** it uses when displayed or reported upon.

6. When you have finished, click the **Back** button to return to the **Workflow Stages** screen.

7. To undo any changes you have made, click the **Revert to Saved** button. To save the changes and end the workflow, click the **Finish** button.

    If you have changed a workflow, MyID prompts you to restart the MyID administration client for these changes to take effect. If you do not restart, when you attempt to run this workflow again you are informed that this operation is invalid and cannot be used until you restart MyID.

19 Key Archiving

When you issue a certificate in MyID, the private key is generated on the card. If the holder loses the card, the key is lost.

For encryption certificates, you may want to archive the key on the MyID server. When the key is archived and the card is lost, you can recover the key onto a new card. This allows any encrypted data (for example, encrypted email) to be accessed.

You can set up key archiving on individual certificate policies. You should choose to archive keys only when necessary – for example, you should archive encryption certificates, but not signing certificates.

There are two forms of key archiving:

- Certificate Authority key archiving

  The certificate authority holds the archived keys.

- Internal MyID key archiving

  The MyID database holds the archived keys.

Note: It is not currently possible to issue a soft certificate that has been set for key archival.

19.1 MyID encryption

When you have a certificate that is set as archived you must have another method of encrypting keys for transferring archived certificates to a card. You can achieve this by adding another non-archived certificate to the card to be used for MyID encryption, or by using the MyID management keys.

This means you cannot use a certificate that is set for archival for MyID encryption in the credential profile.

19.2 Cards supported

Archived keys are only supported by cards that support certificates.

19.3 Certificate authority key archiving

Some certificate authorities support key archiving. The key is archived within the certificate authority rather than within the MyID database.

The following certificate authorities currently support key archiving with MyID:

- Microsoft Windows Certificate Authority
- Entrust JTK
- Symantec Certificate Authority
- Exostar

For information on how a certificate authority handles key archiving, see the relevant integration guide; for example, for Microsoft Windows Certificate Authority, see the *Microsoft Windows CA Integration Guide*.

19.4 MyID key archiving

You can store archive certificates in the MyID database. When a certificate that has been marked for internal archiving is issued, it is stored in the MyID database and protected by the MyID database key.

19.5 Setting up key archiving

Use the **Certificate Authorities** workflow in MyID to set up key archiving.

1. From the **Configuration** category, select **Certificate Authorities**.

2. From the **CA Name** list, select the name of the CA you want to edit.

3. Click **Edit**.

4. Select **Enable CA** if it is not already enabled.

5. For each policy you want to use for issuing certificates to MyID users.

   a) Select **Enable (Allow Issuance)**.

   b) Set the **Archive Keys** option to one of the following options:

      ▫ **None**

        The certificates issued with this profile will not be archived.

□ **Internal**

The certificates issued with this profile will be archived in the MyID database.

□ The name of the Certificate Authority (for example, **Microsoft** or **Entrust**)

The certificates issued with this profile will be archived in the Certificate Authority.

6. Click **Save**.

When you issue a card, any certificates marked for archival are stored on the card and also archived in either the MyID database or the certificate authority.

19.6 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 *29.5*, *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 *19.6.5*, *Temporary replacement credential profiles* for details.

19.6.1 Requesting card replacements

The **Request Replacement Card** workflow allows you to request a replacement card for yourself or for another user.

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

2. Select whether the replacement card is for **Yourself** or **Another User**.

3. If you selected Another User, use the **Find Person** page to find the person's record.

4. The credentials assigned to the person are listed. Select the credentials you want to replace.

5. Select a reason and provide **Details** for the replacement.

   The status determines whether the card will be replaced by a permanent or temporary replacement.

   See section *29.5*, *Certificate reasons* for details.

6. Click **Next**.

19.6.2 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.

19.6.3 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 *19.6.5, 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.

- 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.

19.6.4 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.

19.6.5 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 section *12, Managing Credential Profiles*) 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 cancelled. 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 *27.2.8*, *Issuing temporary replacement cards*, for details of the **Issue Temporary Replacement Card** workflow.

20 Key Recovery

MyID allows you to set up a credential profile for smart cards that are used to collect recovered keys. The smart cards are not fully-featured MyID cards; they are used only to collect recovered keys.

20.1 Setting up the credential profile

If you want to collect recovered keys onto smart cards, you must set up at least one credential profile with the **Key Recovery Only** option. Credential profiles with this option cannot be used for any other smart card requests.

To set up the credential profile:

1. From the **Configuration** category, select **Credential Profiles**.

2. Click **New**.

3. Type a **Name** and **Description** for the credential profile.

4. Click **Services**.

5. If you select the **MyID Encryption** option, the MyID keys on the card will be used to secure the transport of the recovered keys; otherwise, the software-based signing mechanism will be used. Both methods are secure, but the **MyID Encryption** option provides additional security.

    Note: Do not select the **MyID Logon** option. Key recovery cards must not be used to access MyID.

6. Click **Issuance Settings**.

7. Set the **Key Recovery Only** option.

    The **Validate Issuance** option is automatically selected. This allows you to use the **Approve Key Recovery** workflow to validate the key recovery request.

8. If you want to issue the card with a randomly-generated PIN:

   a) Click **PIN Settings**.

   b) From the **Issue With** drop-down list, select one of the following options:

      ▫ **Client Generated PIN**

      ▫ **Server Generated PIN**

   c) Either:

      ▫ Select the **Email PIN** option to send an email message containing the randomly-generated PIN for the card to the recipient.

      or:

      ▫ Click **Mail Documents**, then select the **Card Issuance Mailing Document**.

        This is a mail-merge document that contains information about the key recovery card, including the PIN. You can use this as an alternative to sending the PIN in an email message.

9. Click **Next**.

10. Complete the workflow. You can specify a card layout to be used on the printed key recovery cards.

20.2 Requesting a key recovery

If you need to recover keys onto a smart card, you can use the **Request Key Recovery** workflow.

To request a key recovery card:

1. From the **Certificates** category, select **Request Key Recovery**.

2. In the Select Certificate Owner screen, type the details of the certificate owner – the person whose keys you want to recover – then click **Search**.

3. Select the certificate owner from the search results.

4. In the Select Key Recovery Recipient screen, type the details of the recipient – the person you want to receive the card with the recovered keys – then click **Search**.

5. Select the recipient from the search results.

6. If there is more than one **Key Recovery Only** credential profile, select the credential profile you want to use, then click **OK**.
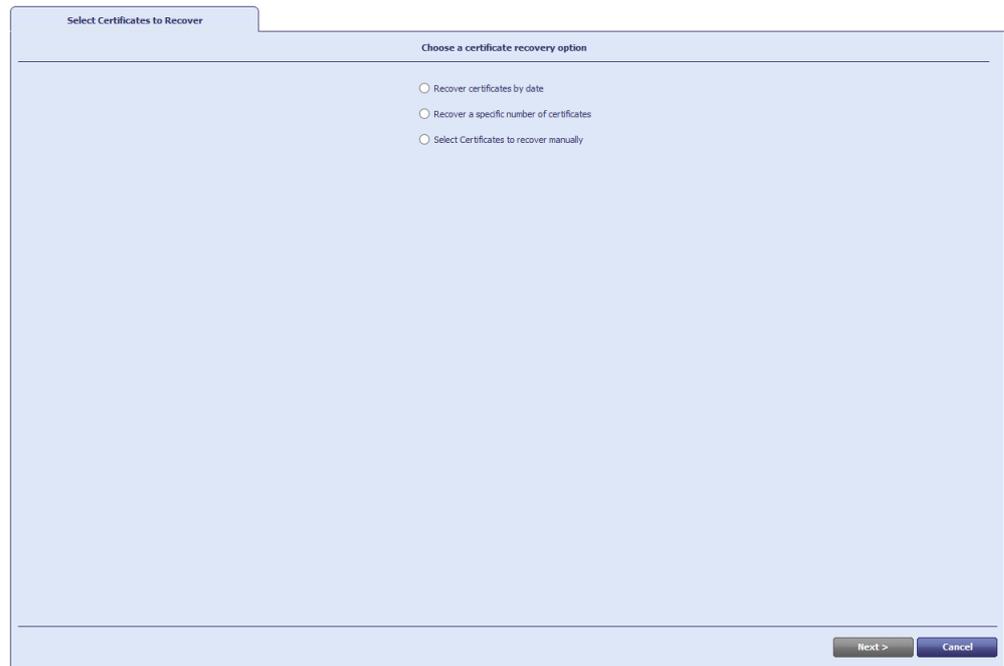
7. Select which certificates you want to recover:

   ◆ **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.

8. 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.

9. Type a **Reason for Recovery** in the text box.

10. Optionally, type a label in the **Assign Job Label** box – you can use this label to search for the recovery job in other workflows.

11. Click **Next**.

   If you selected a date or a number of certificates, the details of the certificates that will be recovered are displayed. If you want to make any changes, click **Back**.

12. Click **Next**.

If the credential profile you selected has the **Validate Issuance** option set, you must use the **Approve Key Recovery** workflow to approve the request. See section *20.3*, *Validating a key recovery request* for details.

If the credential profile you selected does *not* have the **Validate Issuance** option set, you can proceed to the **Collect Key Recovery** workflow. See section *20.4*, *Collecting a key recovery job for another user* for details.

20.3 Validating a key recovery request

If the credential profile used to request the key recovery has the **Validate Issuance** option set, you must use the **Approve Key Recovery** workflow to approve the request.

Note: A different MyID operator from the operator who requested the key recovery must approve the request. Similarly, a different MyID operator from the operator who approved the request must collect the key recovery. (Note, however, that the same operator can both request and collect the key recovery.)

To approve a key recovery request:

1. From the **Certificates** category, select **Approve Key Recovery**.

2. Use the Search Details screen to enter the details of the request you want to approve, then click **Search**.

3. On the Select Job screen, select the job you want to approve.

4. Review the details of the request. You can see the details of the certificates to be recovered on the **Certificate Details** tab.

5. Click **Accept** or **Reject** to approve or reject the request.

   If you reject the request, you must provide a reason.

20.4 Collecting a key recovery job for another user

Note: The **Collect Key Recovery** workflow allows you to collect a key recovery job for any target that is within your scope. You are recommended to make this workflow available to only a limited selection of operators. Use the **Collect My Key Recovery** workflow instead – this workflow ensures that you collect the key recovery job only when you are the target.

Use the **Collect Key Recovery** workflow to collect the key recovery job and write the certificates containing the recovered keys to a smart card.

Note: If the credential profile that was selected for the request has the **Validate Issuance** option set, you must use the **Approve Key Recovery** workflow to approve the request before you can collect it. See section *20.3*, *Validating a key recovery request* for details.

To collect a key recovery request:

1. From the **Certificates** category, select **Collect Key Recovery**.

2. Use the Search Details screen to enter the details of the request you want to collect, then click **Search**.

3. On the Select Job screen, select the job you want to collect.

4. Review the details of the request.

5. Click **Accept** or **Reject** to approve or reject the request.

6. If you accept the request, insert a smart card in a card reader and follow the on-screen instructions to collect the recovered keys onto the smart card and print the associated mailing document.

20.5　Collecting a key recovery job for yourself

Use the **Collect My Key Recovery** workflow to collect the key recovery job and write the certificates containing the recovered keys to a smart card.

Note: If the credential profile that was selected for the request has the **Validate Issuance** option set, you must use the **Approve Key Recovery** workflow to approve the request before you can collect it. See section *20.3*, *Validating a key recovery request* for details.

To collect a key recovery request:

1. From the **Certificates** category, select **Collect My Key Recovery**.

2. On the Select Job screen, select the job you want to collect.

3. Review the details of the request.

4. Click **Accept** or **Reject** to approve or reject the request.

5. If you accept the request, insert a smart card in a card reader and follow the on-screen instructions to collect the recovered keys onto the smart card and print the associated mailing document.

20.6　Viewing key recovery operations

You can view the details of all completed, cancelled, or in progress key recovery operations.

To view a key recovery operation:

1. From the **Certificates** category, select **View Key Recovery**.

2. Use the Search Details screen to enter the details of the key recovery operation you want to view, then click **Search**.

3. Select the key recovery operation you want to view, then click **Next**.

4. View the details of the key recovery operation.

   You can click the **Certificate Details** tab to view the details of the certificates.

5. Click **OK** to close the workflow.

21 External Systems

The **External Systems** workflow allows you to set up connections to external systems; for example, to PACS servers or authentication servers.

Your system must be configured to talk to external systems before you can use this workflow. See the integration guide for your external system for details.

To set up an external system:

1. From the **Configuration** category, select **External Systems**.

2. Click **New** to create a new system, or **Edit** to edit an existing system.

3. Type a **Name** and **Description** for the external system.

4. Follow the specific instructions for the external system provided in the relevant integration guide.

5. Click **Save**.

22 Archiving Deleted Users

You can configure MyID so that any users that are deleted (for example, using the **Remove Person** workflow) are archived in a separate table on the database, allowing you to keep track of all the users that have existed in the system.

The following tables hold the details of deleted users:

- `PeopleArchive`
- `SystemAccountsArchive`
- `UserAccountsArchive`
- `UserAccountsExArchive`

To switch this feature on, set the **Archive People Data** option on the **General** tab of the **Operation Settings** workflow.

23 Management Information (MI) Reports

You can use the **MI Reports** workflow to run management information 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 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, 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 Revocation History** – a list of cards that are revoked.

- **Card Cancellations** – a list of card cancellations.

- **People by group and affiliation** – a list of people including groups and affiliation. Scoped. PIV only.

- **Jobs** – a list of jobs.

- **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.

23.1 Running MI reports

To run a management information report:

1. From the **Reports** category, select **MI Reports**.
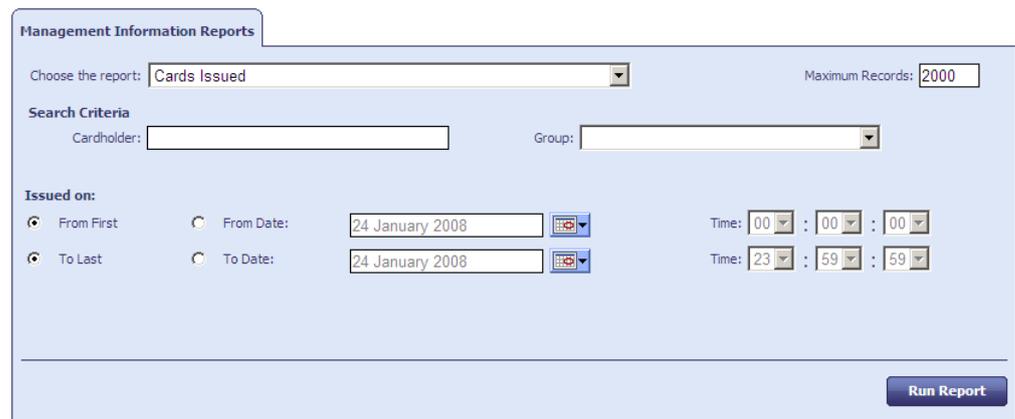
   Note: Make sure that you can view the **MI Reports** workflow. Use the **Edit Roles** workflow in the **Configuration** category to add the workflow to the roles you want to be able to run the reports.

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.

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 Explorer, see the *Installation and Configuration Guide*.

24 External Logon Providers

You can configure an external logon provider. This can allow users to log in when they do not have a valid card, for example.

Your environment must be set up with an external system that provides a logon service. Contact customer support for details.

1. From the **Configuration** category, select **Configure External Logon Providers**.

2. Select the **Logon Provider** from the list, then select the appropriate **External System** from the drop-down list.

    This sets up an association between the logon provider and the external system that provides the logon service.
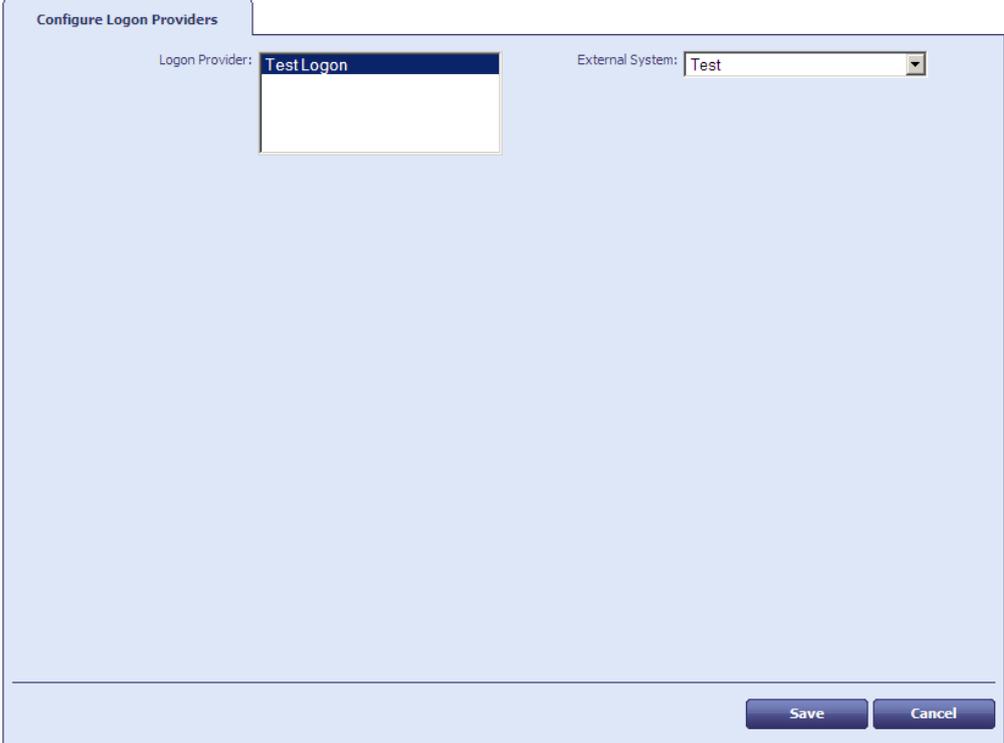
3. Click **Save**.

25   Job Management

Many of the tasks carried out within MyID are automatically allocated a job number by the system. You can use the job management workflow to:

- Locate a particular job and view information about it.

    For example, someone may contact you because credentials have been requested with the wrong profile. You can locate the appropriate job, find out its current status, and cancel it.

- Check the overall status of jobs, making sure the system is running smoothly.

    For example, you can regularly check the number of jobs that have a status of **Failed** or **Completed With Errors**. You can also see how many jobs are waiting validation to move to the next stage.

You can specify a wide range of criteria when searching for a particular job or a group of jobs. The results displayed are those that meet *all* the criteria you specify, so if you cannot find the job you are looking for, try removing some of them.

25.1   Searching for a job

To search for a job and view its details, from the **Configuration** category, select the **Job Management** workflow.

Specify the criteria for your search using the form displayed, which consists of the following pages:

- **General** – use this page to specify broad categories for your search.
- **Target** – the person who will be affected by the task; for example, a holder.
- **Initiator** – the person who started the task.
- **Validator** – the person who validated the task.
- **Actioned By** – the person who actioned the task.
- **Renewal** – due for renewal within a specified period.
- **Suspended** – use this page if you know the job you are looking for has been suspended.

Click **Search** to look for records that match the criteria you have specified.

To clear all criteria from all pages, click **Reset**.

25.1.1   General search criteria

On the **General** page you can specify:

- The **Job ID**

    This goes directly to the job you want to see.

- The type of task

    Task types indicate the type of the job. For example, tasks generated from the **Request Card** and the **Issue Card** workflows both have a task type of **IssueCard**.

- The status of the task

    You can specify more than one status. For example, you may look for all tasks that either **Failed** or **Completed With Errors** in a particular week.

- The **Batch Label**

   This is only applicable for jobs that are associated with bureau (bulk) requests. It is associated with a bulk request when the request is made.

You can also limit the number of results you want to be returned from your search. This prevents excessive processing if your criteria are too broad.

25.1.2 Searching by target

The target is the person who will be affected by the job. For example, if a card is requested for John Brown by his manager, John Brown is the target of the request.

On the **Target** page, you can specify:

- The **Target Logon Name**

   If you are looking for a particular job record and you know this information, you do not need to enter anything else on this page, as a logon name is unique.

- The name of the target or the group to which the target belongs.

   If you do not know the target's logon, you may know the target's name. You may also want to specify a target group if you want to narrow your search.

25.1.3 Searching by initiator, validator or actioned by

These pages work in the same way.

- The initiator is the person who started the job. For example, if John Brown's card was requested by his supervisor, his supervisor is the initiator.

- The validator is the person who confirmed that the task was correct. For example, if the department manager confirmed the request, the manager was the validator.

- The person who actioned the task is the person who ran the workflow; for example, the person who issued a card.

On any of these pages, you can specify:

- The logon name of the person

- The date and time range within which this phase of the job took place.

   To enable the calendars and time fields, select the **From Date** and **To Date** options (if applicable).

25.1.4 Searching by renewal or suspended dates

These two pages contain only the calendars and **Time** fields. To enable them, select the **From Date** and **To Date** options as appropriate.

25.2 Viewing job records

The results of the search are displayed in a table. You can specify the number of rows to be displayed at any one time. If more records have been returned than the number of rows specified, you can step through them one block of records at a time.

To see more details about a job, double-click anywhere on the text of the record. For example, if you double-click on a job with a task type of **IssueCard**, you will see the credential profile that was requested.

25.3   Managing jobs

From the **Job Management** workflow, you can:

- **Suspend** jobs, depending on their status. You cannot suspend a job if processing is complete.

- **Unsuspend** previously suspended jobs.

- **Cancel Jobs**

You can do this by either:

- Selecting the jobs in the list of results, using the boxes to the left of each row, and then clicking the appropriate button.

- Viewing the details of a job and using the buttons on the details form.

26 Working with the People Records in MyID

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.

26.1 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 *26.3*, *Editing people*; section *26.4*, *Security phrases*; and section *27, Requesting, Issuing and Managing Cards*) and many of the workflows related to managing credentials.
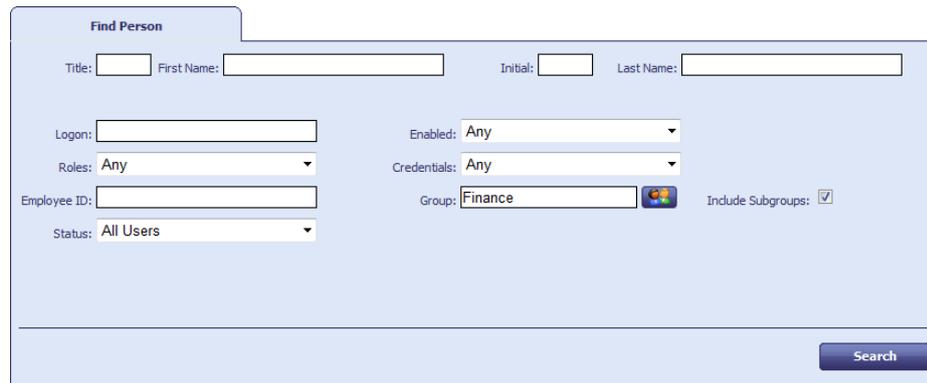
You can restrict your search to 'Users marked for attention' by selecting that **Status** from the list available.

26.2 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 section *5*, *Using an LDAP Directory*, for more information.

26.2.1 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; in this case, you can use the **Person Import** workflow to import your users.

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.

    Note: You must select a group – you cannot search from the LDAP root.

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.

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

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

6. You can change the person's picture: see section *16.4, Working with images* for details.

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

8. Click **Save**.

    Depending on how your system is set up, the **Witness** stage may appear. See section *4.8 Witnessing a transaction* section for details.

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 import more than one person at a time from your directory, use the **Person Import** workflow; see section *26.2.3*, *Importing a person*, for details.

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.

26.2.2 Adding a person and issuing a card

The **Add Person and Issue Card** workflow allows you to add a person to the database then issue a card to that person immediately.

The workflow combines the **Add Person** and the **Issue Card** workflows. See section *26.2.1*, *Adding a person manually*, and section *27.2.1*, *Issuing a card*, for details.

26.2.3 Importing a person

The **Person Import** workflow allows you to import a person from your directory into the MyID database.

1. From the **People** category, click **Person Import**.
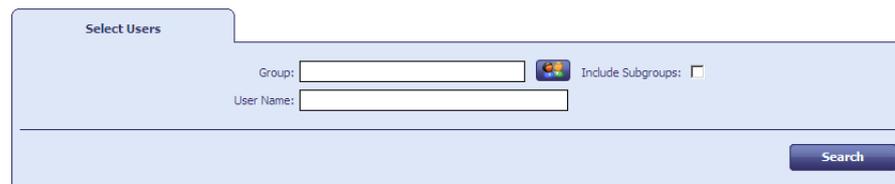
2. Click the **Group to search** button.

3. Select the directory branch from which you want to import a user. To import a user from that branch and any below it, select the **Include Subgroups** option.

4. Alternatively, type a **User Name** to search for within the directory.

   To specify all or part of a person's name, do one of the following:

   ◆ Type the person's full name: first name then last name. For example: `John Smith`.

   ◆ Enter part of a person's name, using asterisks (`*`) as wildcards where appropriate. The asterisk can be used to represent one or more letters.

   For example: `Jo* Smith` finds `John Smith` and `Joanne Smith`.

5. Click **Search**.

The results of the search are displayed in a standard table below the search criteria.

6. Select the boxes next to the people you want to import.

You can select all or none of the people using the **All/None** option.

7. Click **Import Selected**.

You can choose whether to use imported values or to specify a different value for many of the fields by clicking on the map pin to the right of the field.

Note: With the exception of the **Group** box pin, pins appear only if you have set the **Update user information in the directory** option on the **LDAP** page of the **Operation Settings** workflow set to `Yes`, or to `Ask`, followed by the operator selecting **Yes** to the prompt to synchronize details with LDAP. You can change the **Group** value whatever the update settings.

Each time you click the pin, you cycle through the following options:

- Imported values are used by default for most fields – the map pin is horizontal and the tooltip is **Import data for each record**.

- The specified value (for example, **Cardholder** is used by the **Roles** field) – the map pin is pressed in and the tooltip is **Keep this value** for all records.

- Information passed into this field by the LDAP directory is cleared – the image is of the end of a pencil with an eraser and the tooltip is **Clear field for each record**.

8. You can use the following options at the bottom of the page:

- **Save** – to save the currently displayed record

- **Save All** – to save all the records that you selected.

  Note: Every mandatory field must contain a value, either imported from the directory or entered manually and set to be used for all records, or the import will fail.

- **Skip** – skip the displayed record and move to the next.

- **Cancel** – stop the import process.

You are returned to the search results screen.

9. You can either select another user to import, or click **Finish** to complete the workflow.

Known issues

- **IKB-18 – There is no indication that the Person Import workflow is still processing imported records.**

  When you click **Finish** on the **Person Import** workflow, MyID begins importing the users in the background. If you have selected a large number of users, the import process may take some time to complete; there is currently no indication that the import process is still running.

- **IKB-29 – Problem using the Person Import workflow to import multiple users**

  If you are have logged in to MyID Desktop using a smart card, you may experience a problem when using the **Person Import** workflow to import several users. After importing a number of users, MyID becomes unresponsive, and users are no longer imported from the directory.

  As a workaround ,you can log on to MyID with security phrases; the issue with the **Person Import** workflow does not occur if you have not logged on with a smart card.

  If you need to import large volumes of user records, contact customer support quoting reference SUP-206.

26.3 Editing people

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

Note: If you are using an LDAP directory as the primary source of your data, you can use the **Edit Person** workflow to find a person and make their details available to MyID. See section *5*, *Using an LDAP Directory*, for more information.

26.3.1 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.

4. The **Person Details** stage displays the information about the person.

   The **Personal** and **Account** tabs are the same as those used to add a person to the system – see section *26.2.1*, *Adding a person manually* for details.

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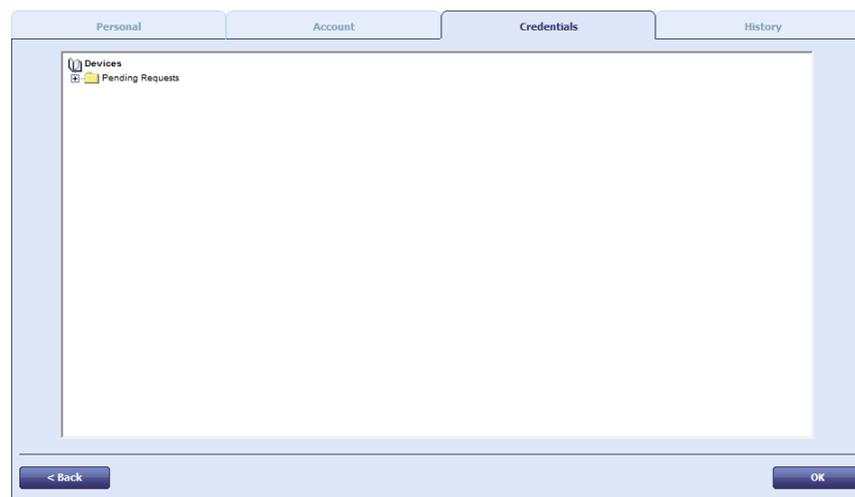
Note: The **Credentials** tab appears only if your role includes the **View Device Details** option in the **Cards** section of the **Edit Roles** workflow.

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 section *18.1*, *Audit scope* for details.

Click the links to view the detailed list of changes.

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

26.3.2   Editing a person

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

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.

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

   The **Personal** and **Account** tabs are the same as those used to add a person to the system – see section *26.2.1*, *Adding a person manually* for details.

   Note: If you use the Select Roles dialog to edit a user, if a role that the user previously held has been removed from all 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. 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 *29.5*, *Certificate reasons* for details of the different reasons.

   The **Credentials** and **History** tabs are the same as those used to view a person – see section *26.3.1*, *Viewing a person's details* for details.

6. To finish the workflow, click **Save**.

26.3.3   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 employee 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 *29.5*, *Certificate reasons* for details of the effect of the different reasons.

The person is removed from the system.

Note: If you have Entrust installed, a prompt may be displayed at the end of the workflow asking if you want to remove that user from Entrust.

26.4 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.

26.4.1 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.
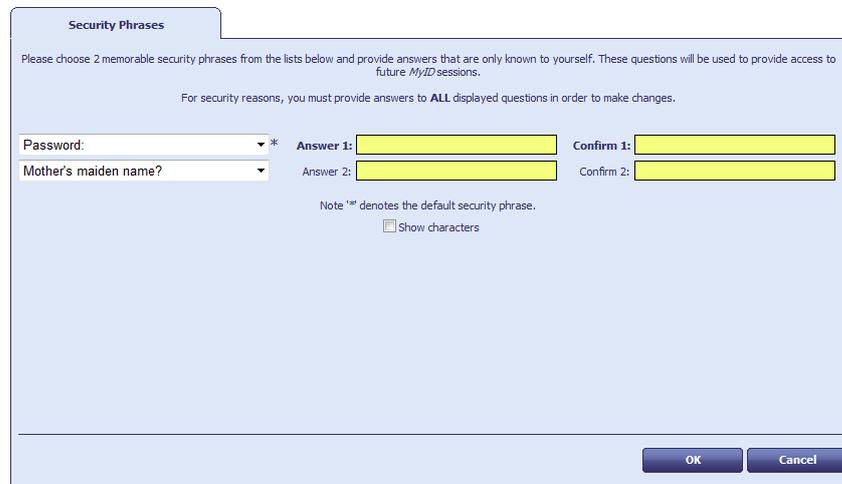
When you make changes to these answers, you must provide answers to all the questions displayed.

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 section *3.3.2*, *Setting the number of security phrases required to authenticate* for details.

3. Click **OK**.

26.4.2 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**.

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 section *3.3.2*, *Setting the number of security phrases required to authenticate* for details.

4. Click **OK**.

26.5 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 201-2, 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 **Authenticate Person Document1** and **Authenticate Person Document2** lists. To edit these lists, use the **List Editor**. See section *15, Changing List Entries* 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 section *3.3.2*, *Setting the number of security phrases required to authenticate*.

- **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:

Authenticate Person	☑
Match Enrolled Fingerprints	☑
Identity Documents	☑
Operator Approval	☑
Security Questions	☑

To authenticate a cardholder:

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

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 **Authenticate Person Document1** and **Authenticate Person Document2** lists. To edit these lists, use the **List Editor**. See section *15, Changing List Entries* 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 Secrets**.

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 section *3.3.2*, *Setting the number of security phrases required to authenticate*.

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.

27 Requesting, Issuing and Managing 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.

27.1 Setting expiry dates for a card

Credential profiles include a Lifetime setting (see section *12.3.1*, *Credential profile options*) that determines how long a card is valid.

It is possible to specify an expiry date for a specific 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.

An additional option is now displayed in the Select Credential profile stage, for example when issuing or requesting a card.

If this option is available, selecting it 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.

27.2 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.

27.2.1 Issuing a card

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 add a user and issue a card at the same time, use the **Add Person and Issue Card** workflow; see section *26.2.2*, *Adding a person and issuing 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 *27.1*, *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.

   a) 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.

   b) 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 generated PIN is displayed.

- If the type of password required is **None**, no PIN is displayed.

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 section *34.5*, *PINs page (Security Settings)*, 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**.

9. 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.

10. 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.

11. 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.

27.2.2   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 *27.1*, *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 cancelation, that match the search criteria are displayed. 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.

27.2.3 Validating a card request

Depending on how your system is set up, you may have to 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**.

	ID	Job For	Requested By	Request Date	Validator	Validation Date	Status	Task Type
☐	11	Angel Makin	startup user	03 April 2014			Awaiting Validation	Issue card task
☑	12	John Brown	Alison Peck	03 April 2014			Awaiting Validation	Issue card task

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 *27.1*, *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.

27.2.4 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**.
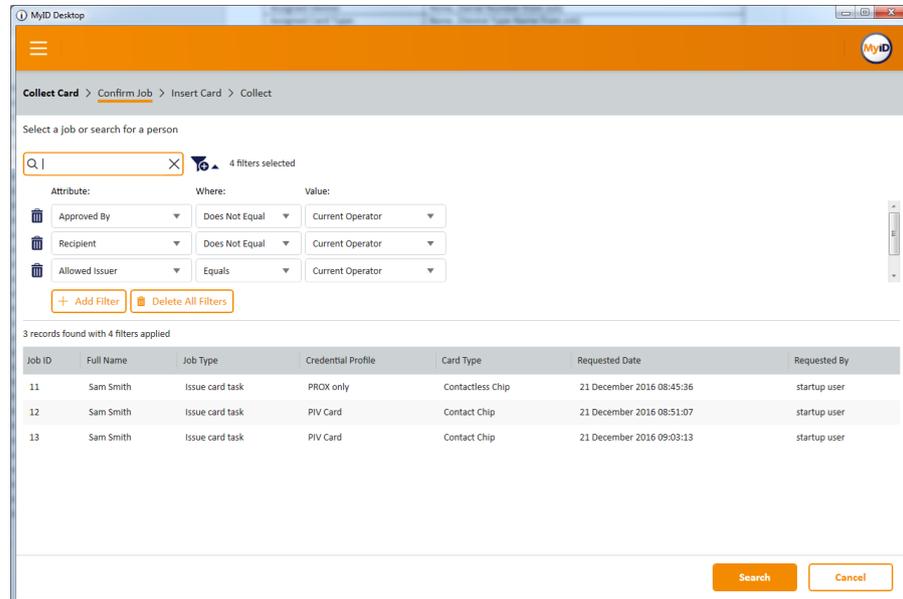
2. Enter the search details for the job, then click **Search**.

   For details of using search filters, see section *1.4.3, Using advanced search.*

3. Select the job from the list.
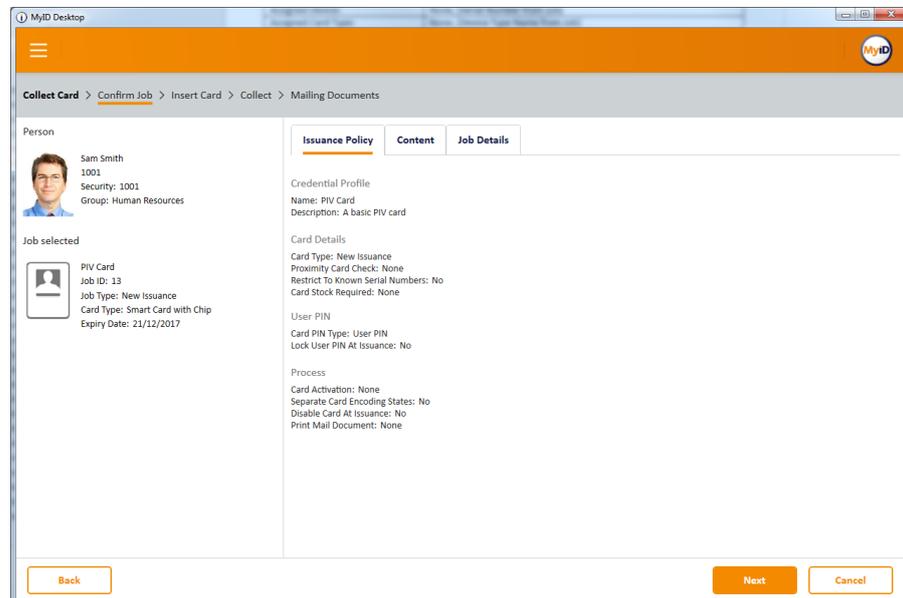
4. Make sure that the details of the job are correct. This screen lists the following:

   ◆ 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**.
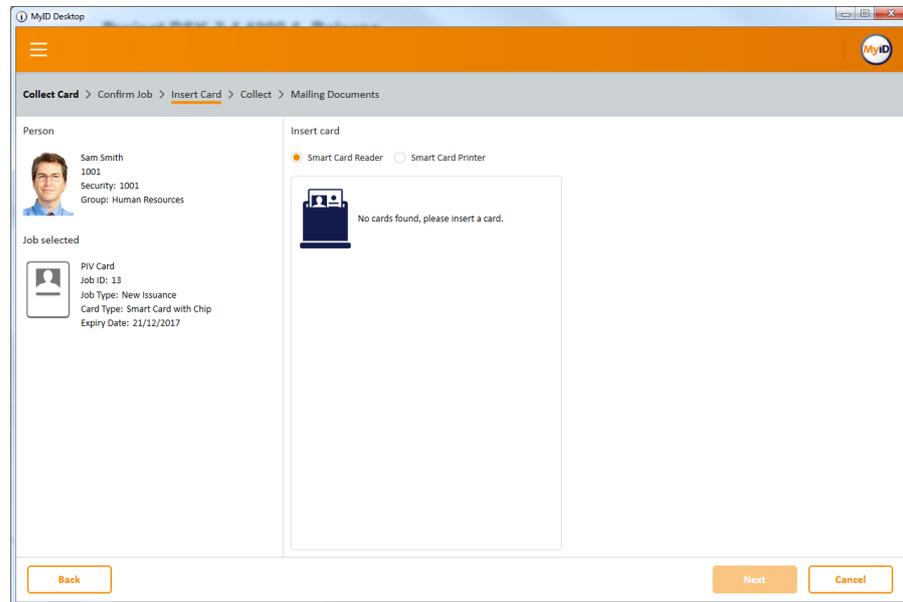
6. Select one of the following options:

◆ **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 section *27.2.9*, *Printing a card*.

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 section *34, Configuration – Security Settings*, 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 sections *28.4*, *Activate card* and *28.5*, *Assisted activation* for details.

11. If you are using a card printer, select the card layout you want to use.
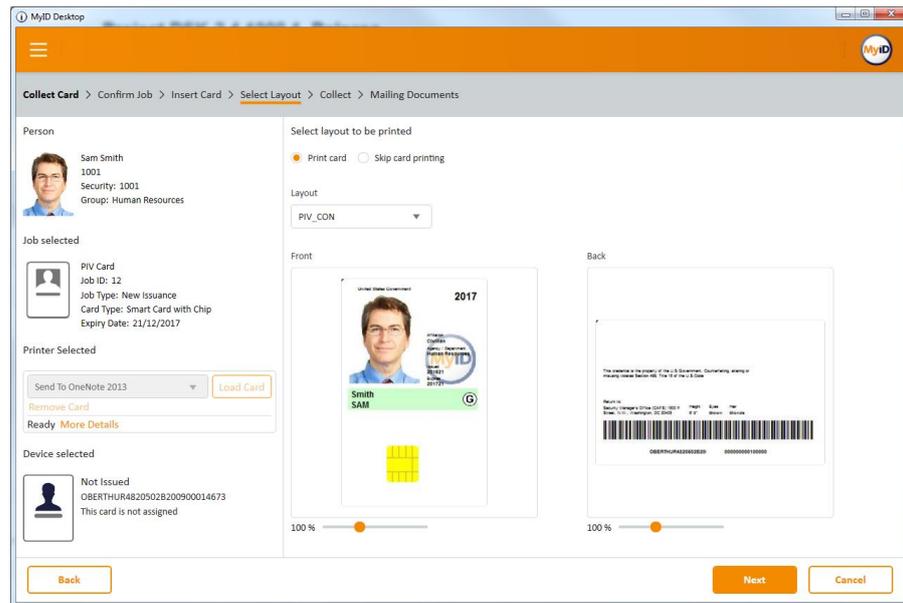
If you decide not to print at this stage, click **Skip card printing**.

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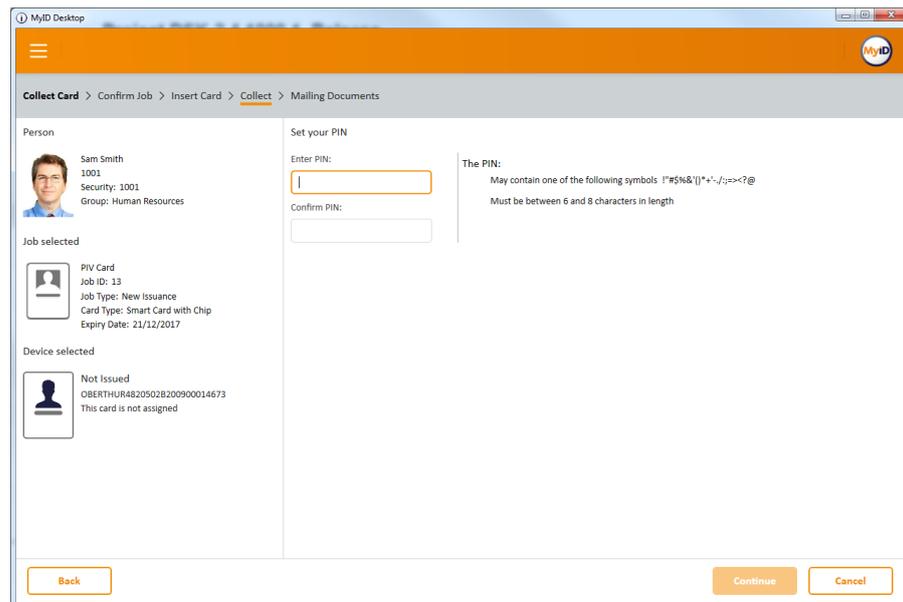
13. Type the PIN for the card in the **Enter PIN** box, then again in the **Confirm PIN** box.

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 *27.2.5*, *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.
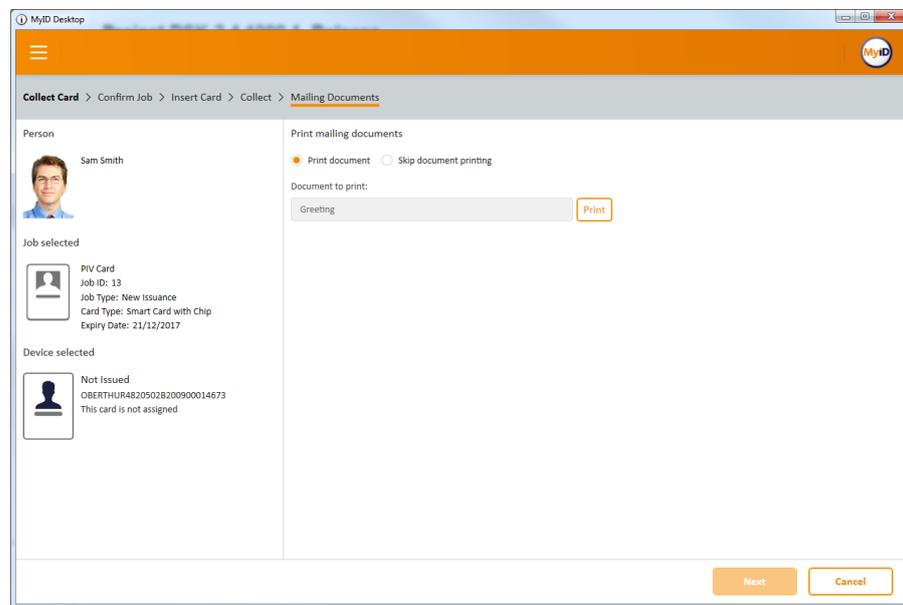
    Note: For details of configuring templates for mailing documents, contact customer support, quoting reference SUP-255.

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**

    It is not currently possible to use the **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.

27.2.5 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.

27.2.6   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**.

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.

27.2.7   Requesting a replacement card

The **Request Replacement Card** workflow allows you to request a replacement card for yourself or for another user.

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

2. Choose whether the recipient of the new card will be **Yourself** or **Another User**, then click **Next**.

    Note: In the PIV version of MyID, you cannot request a replacement card for yourself.

3. If you are requesting a replacement card for another user, use the Find Person screen to select the person.

    The cards assigned to the person are listed.

4. Select the card you want to replace.

5. Select a reason and provide **Details** for the card replacement, then click **Next**.

    See section *29.5*, *Certificate reasons* for details.

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.

27.2.8   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 *19.6.5*, *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.
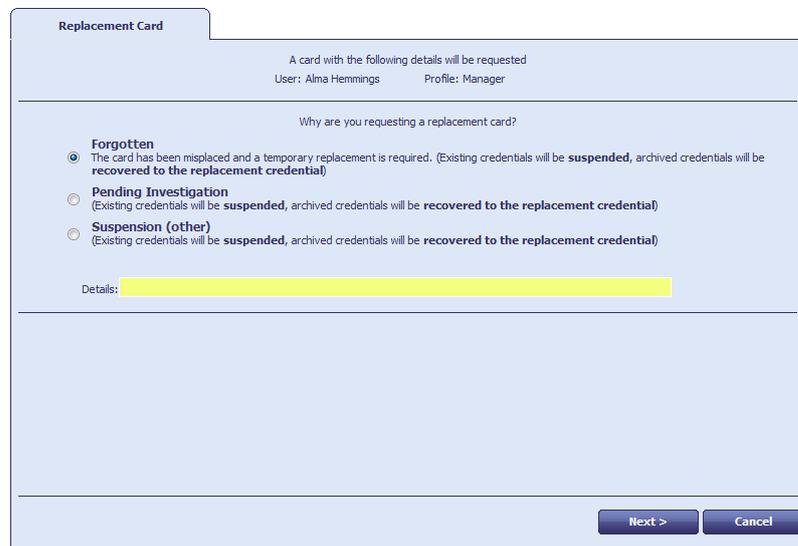
4.   Select the reason you are issuing a temporary card, then type the **Details**.

See section *29.5*, *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.

27.2.9 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**.
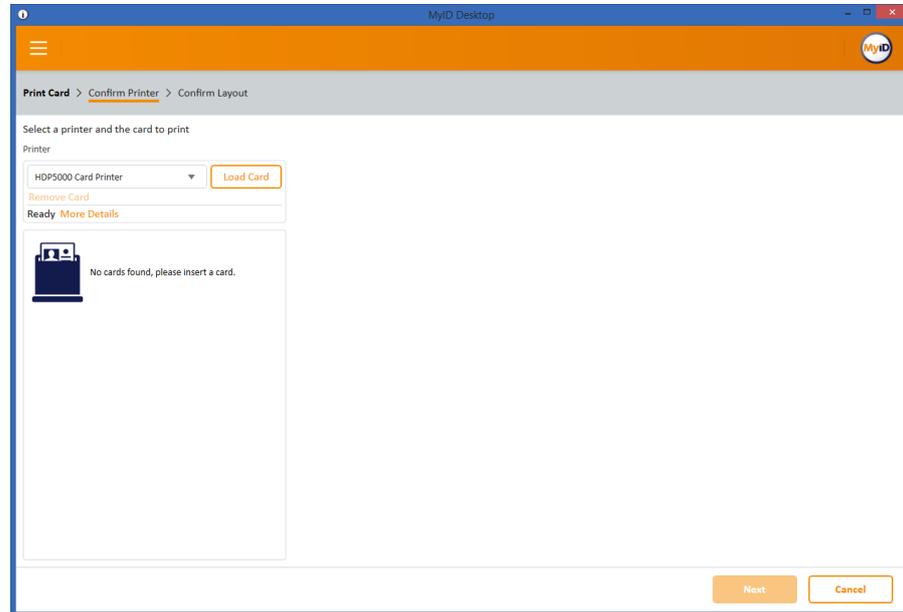
2. From the drop-down list, select the card printer you want to use.

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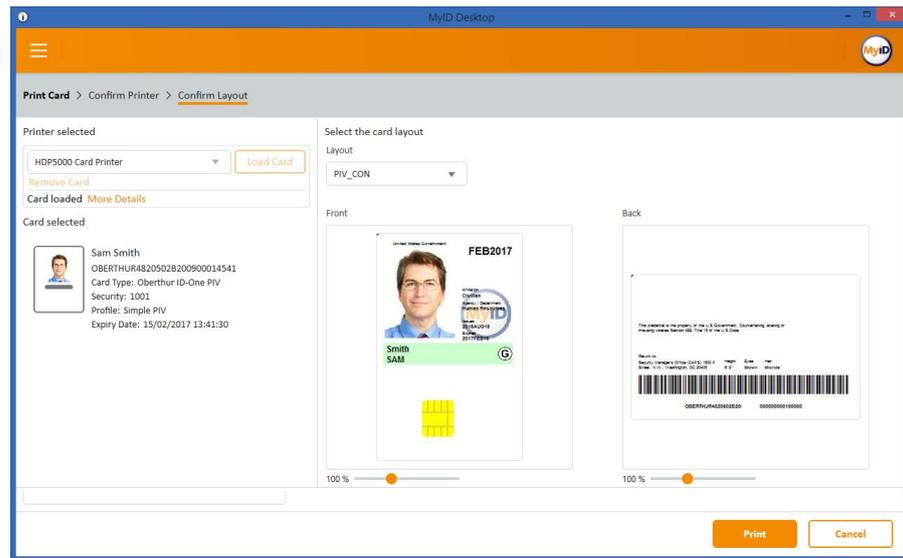
6. Select the card layout from the drop-down list.

    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.

27.3   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.

27.3.1   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. From the **Configuration** category, select **Operation Settings**.

2. On the **Devices** tab, set the **Deliver Card Before Activation** configuration option to Yes.

3. Click **Save changes**.

27.3.2 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.

27.3.3 Marking cards as delivered

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

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.

27.4   Batch issuing cards

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

27.4.1   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**.

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**.

   MyID validates the users, then displays the Select Credential Profile screen.

4. Select the credential profile you want to use from the list, then click **OK**.

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.

27.4.2 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**.

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 *1.4.3*, *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**.
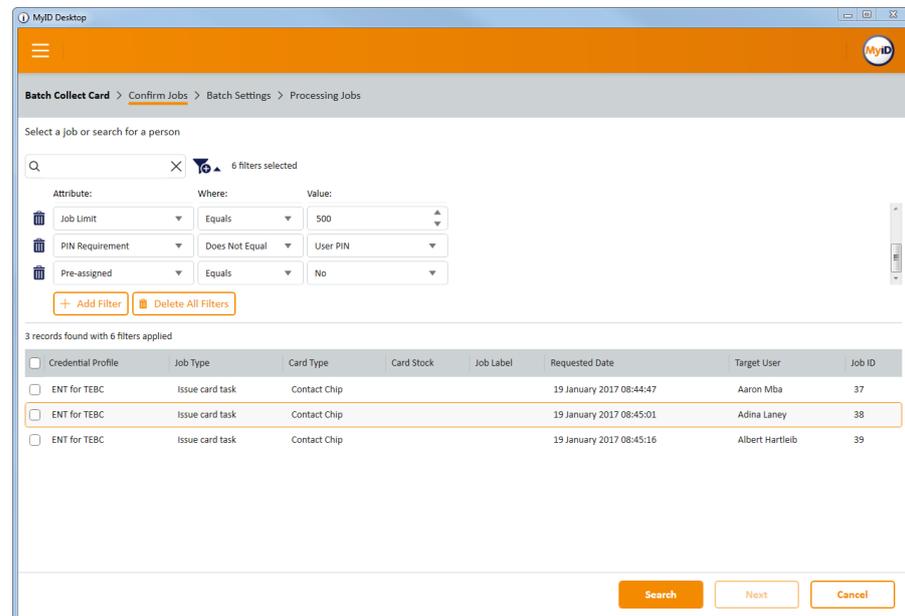
The list of matching jobs appears.

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**.
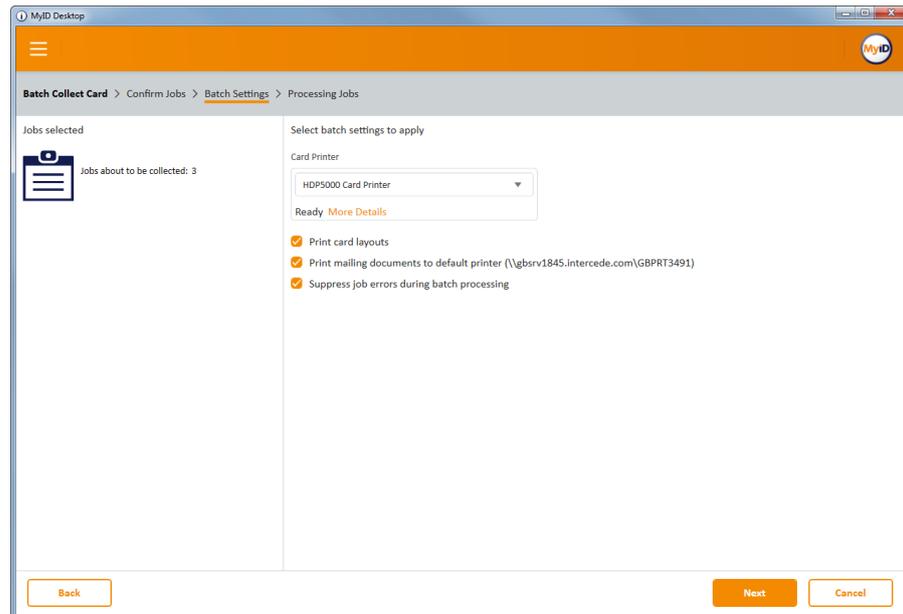
6. Set the options for issuing the card:

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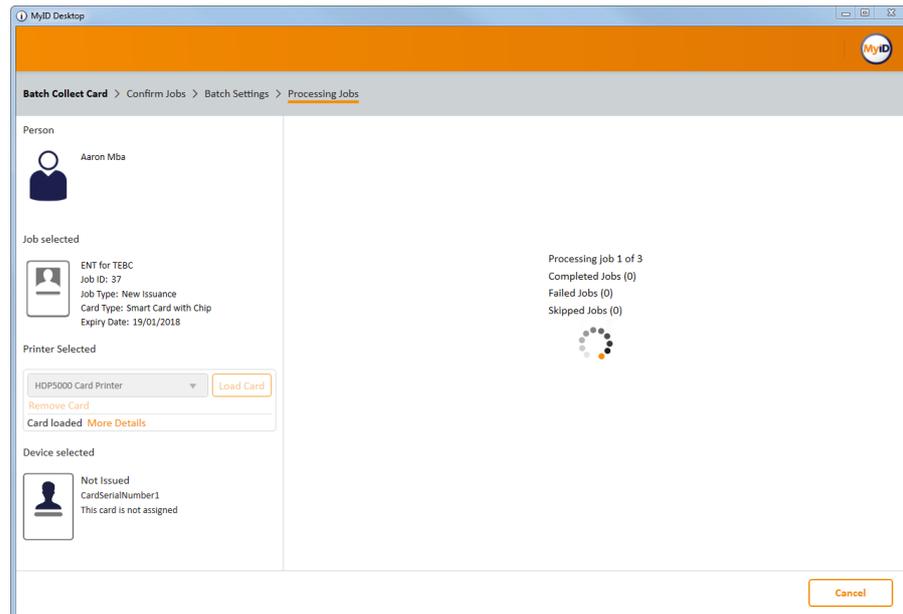
MyID issues and prints the cards one by one. If an individual collection job fails, it is returned to the list of available jobs, and you can re-run the **Batch Collect Card** workflow to collect it.

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

27.5 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.

27.5.1 Card update limitations

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.

In these situations, you are recommended to re-issue the card rather than update it.

27.5.2 Requesting a card update

The **Request Card Update** workflow allows you to create a job that updates a card. Users can then log in with their cards to collect the updates. You can request the update whether you have the card present or not.

To request a card update:

1. From the **Cards** category, click **Request Card Update**.
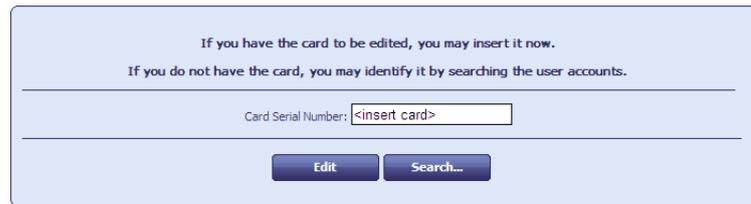
2. If you have the card present, insert it and click **Edit**.

   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.

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

   See section *29.5*, *Certificate reasons* for details.

5. Click **Continue**.

   MyID creates a job that will update the card. The cardholder can update the card using the **Collect My Updates** workflow.

Note: Depending on your configuration, an email notification may be issued to the appropriate person on completion of this workflow. For example: `"Your Card is ready for issue. Please follow the instructions for issuance of a new card".`

27.5.3   Updating a card

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

To update a card:

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

2. Insert the card you want to update, then click **Edit**.

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 *29.5*, *Certificate reasons* for details.

5. Click **Continue**.

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

    MyID updates the card.

27.5.4　Collect My Updates workflow

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

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.

27.6　Administering cards

You can carry out various administrative tasks on cards. For example, you can identify a card you have present, change the PIN of a card, or list the cards in the system.

27.6.1　Identifying a card

To identify a card:

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


```
If you have the card to be identified, you may insert it now.
If you do not have the card, you may identify it by searching the user accounts.

Card Serial Number: <insert card>

[ Identify ]   [ Search... ]   [ Token... ]   [ Device... ]
```

2.　To specify the card you want to identify, you can do one of the following:

　　◆　Insert the card.

　　◆　Click **Search**, then use the Find Person screen to find the person and the card.

　　◆　Click **Token**, then type the token's serial number and click **OK**.

　　◆　Click **Device** and find the device whose credentials you want to identify.

3.　Click **Identify**.

　　MyID reads the card and provides information on it. 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.

　　◆　**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.

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

27.6.2 Printing mail merge 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 section *12.4*, *Setting up mail merge documents.*

To print a mail merge document:

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

> If you have the card to be edited, you may insert it now.
> If you do not have the card, you may identify it by searching the user accounts.
>
> Card Serial Number: \<insert card\>
>
> **Select**   **Search...**
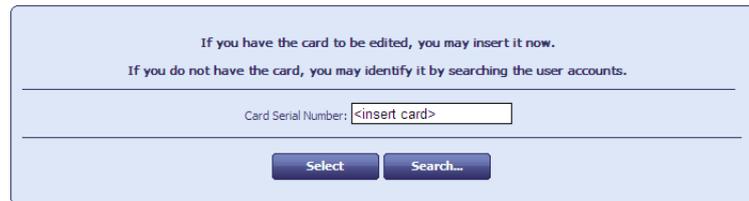
2. If you have the card present, insert it and click **Select Card**.

    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 you want to print the document for.

> Title:
> First Name: Jack
> Middle Name:
> Last Name: Regan
> Serial Number: 30366715
> Device Type: Datakey Model 330
> Card Profile: Manager
> Original Mailing Document: C:/Documents and Settings/John Fulton/My Documents/Mailing document.doc
> Print associated document to [Default Printer ▼]
>
> **< Back**   **Print**   **Cancel**
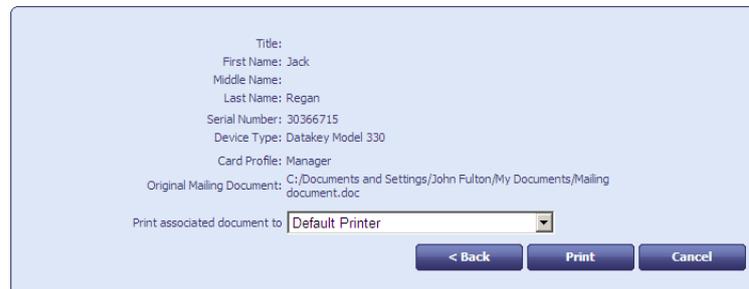
3. Select the printer to which you want to print the document, then click **Print**.

    MyID prints the mailing document to the selected printer.

27.7 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.

27.7.1 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**.

2. Insert the card you want to reset.
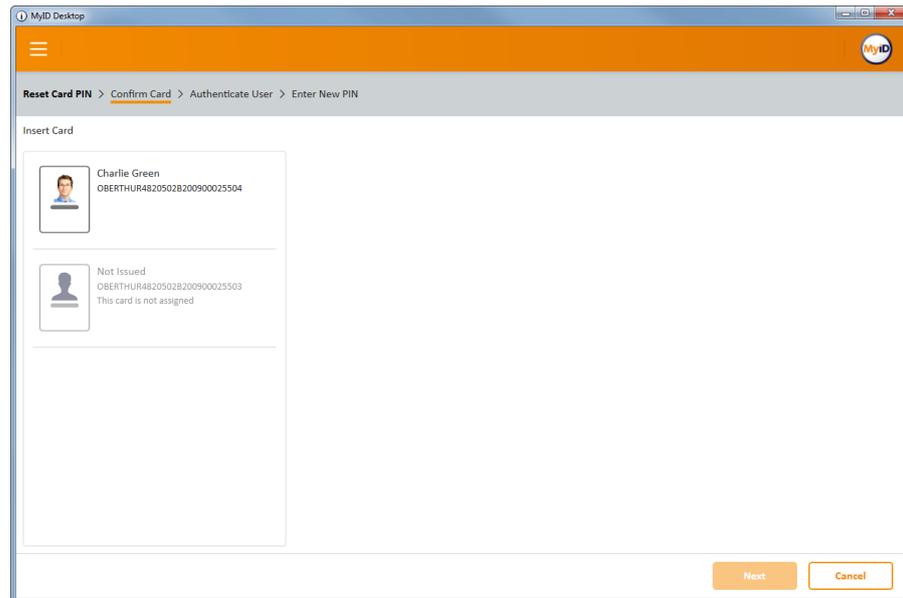
3. Select the card, then click **Next**.
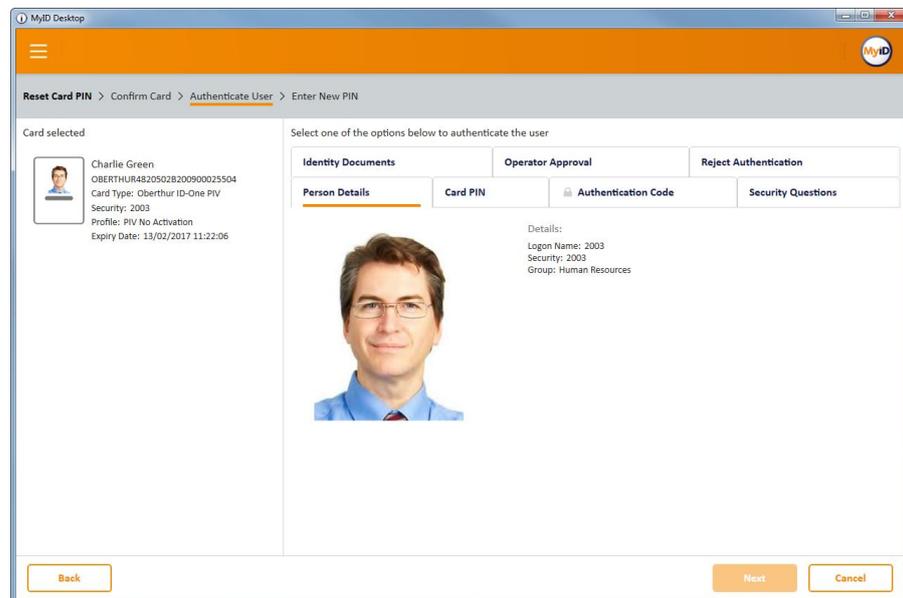
The **Person Details** tab displays the details for the cardholder – this allows you to confirm that the card belongs to the correct user.

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 *27.7.2*, *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.

   ◆ **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 *27.7.8*, *Requesting an authentication code* for details.

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

See section *3.3.2*, *Setting the number of security phrases required to authenticate* 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 section *15, Changing List Entries* 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**.

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

6. Type the new PIN and confirm it.

7. Click **Continue**.

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

27.7.2 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 section *15, Changing List Entries* 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**.

27.7.3 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 *27.7.5*, *Self-service PIN reset authentication* for details.

3. Provide your new PIN.
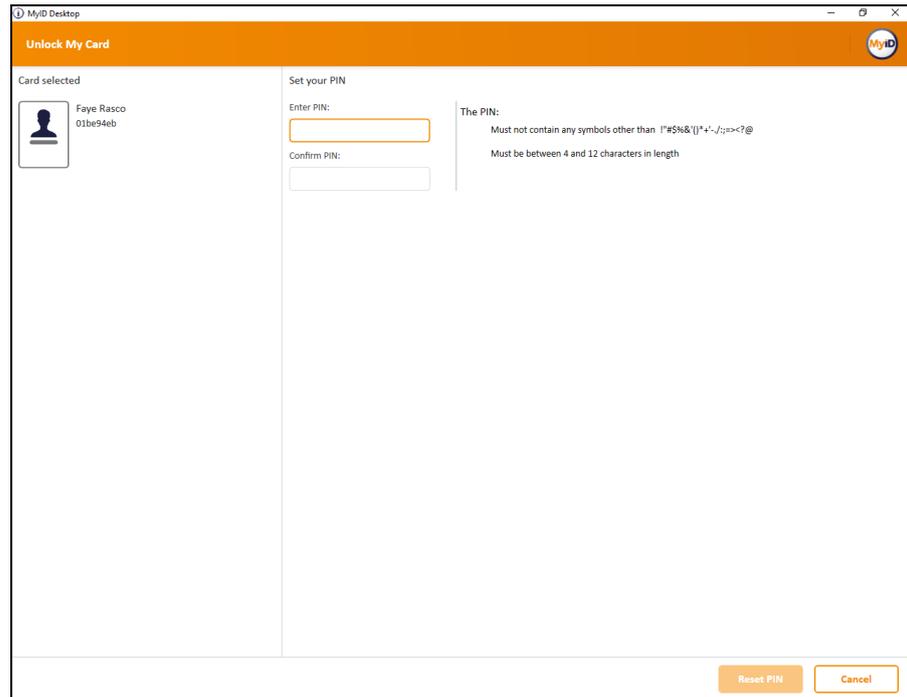
4. Click **Reset PIN**.

27.7.4 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 details of the `AllowSelfUnlockForPIV` option in the ***Web Service Architecture Installation and Configuration*** document for details.

27.7.5 Self-service PIN reset authentication

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

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

▪ **None** – no biometric or authentication codes are required. 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 unlock their card with their security phrases; otherwise, the user cannot unlock their card, and must contact a MyID operator.

▪ **System Default** – 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 must provide their security phrases to unlock their card.

If the **Verify fingerprints during card unlock** configuration option (on the **Biometrics** tab of the **Operation Settings** workflow) is set, the user must provide their fingerprints to unlock their card.

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

If both options are set, the user must provide both security phrases and biometrics to unlock their card.

▪ **Biometric** – biometric authentication is used to unlock the card.

- **Authentication Code (Manual)** – an authentication code is required to unlock the card. An operator must request an authentication code.

- **Authentication Code (Automatic)** – an authentication code is emailed to the applicant when the card is issued; this is not suitable for unlocking.

Note: 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.

27.7.6 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 *27.7.1*, *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**.
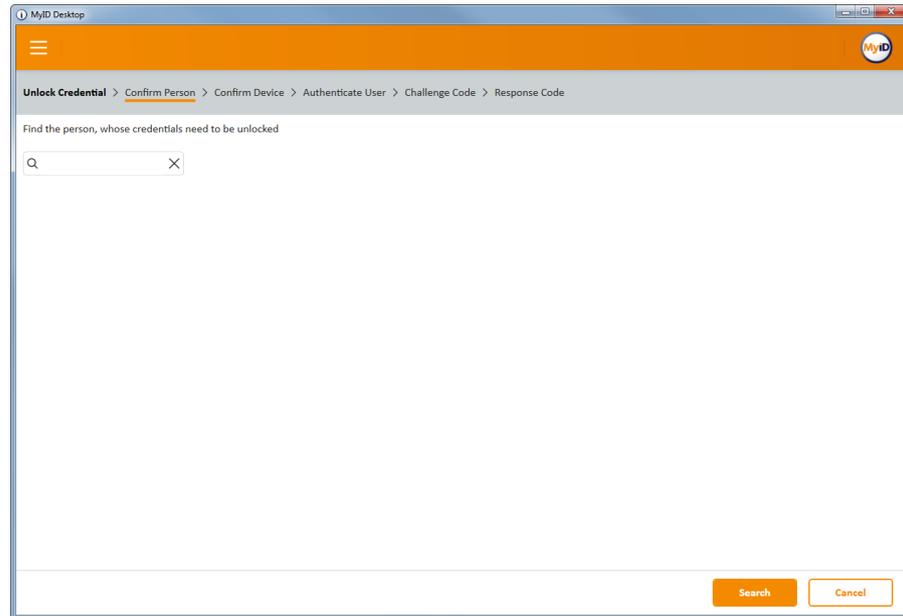
2. Enter the search criteria for the person who owns the credential you want to unlock, then click **Search**.

   See section *1.4.2*, *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.
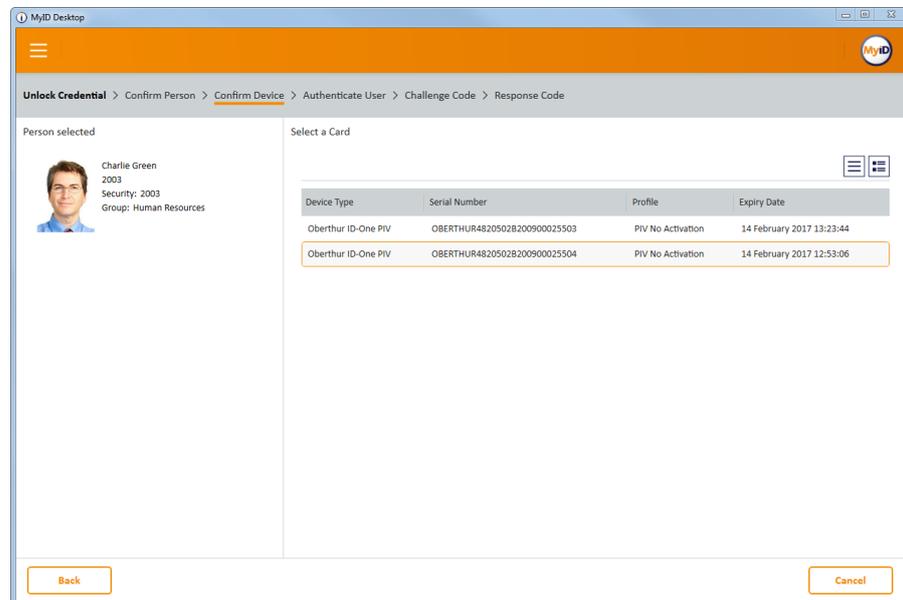
4. Select the device you want to unlock.
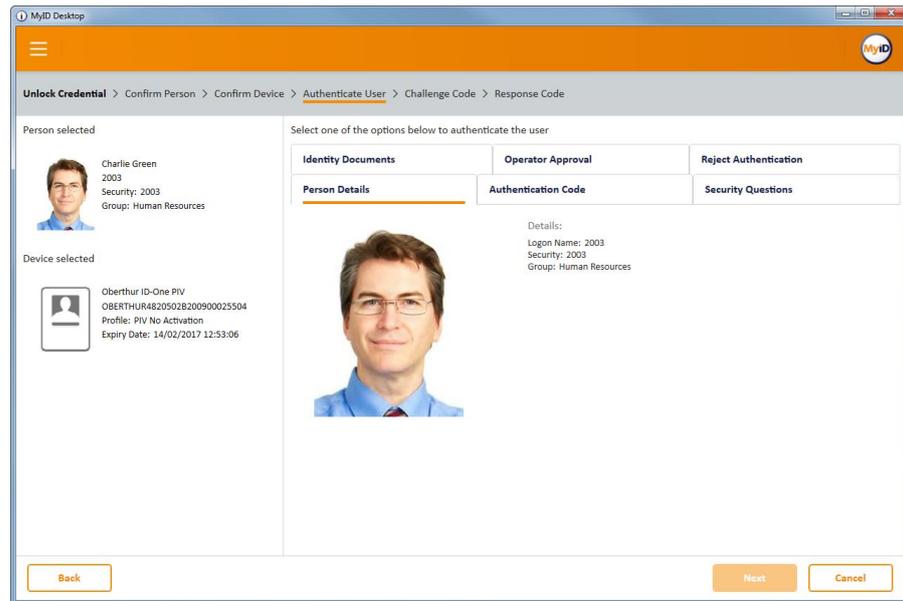
The **Person Details** tab displays the details for the cardholder – this allows you to confirm that the card belongs to the correct user.

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 *27.7.7*, *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 *27.7.8*, *Requesting an authentication code* for details.

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

   See section *3.3.2*, *Setting the number of security phrases required to authenticate* 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 section *15, Changing List Entries* 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**.
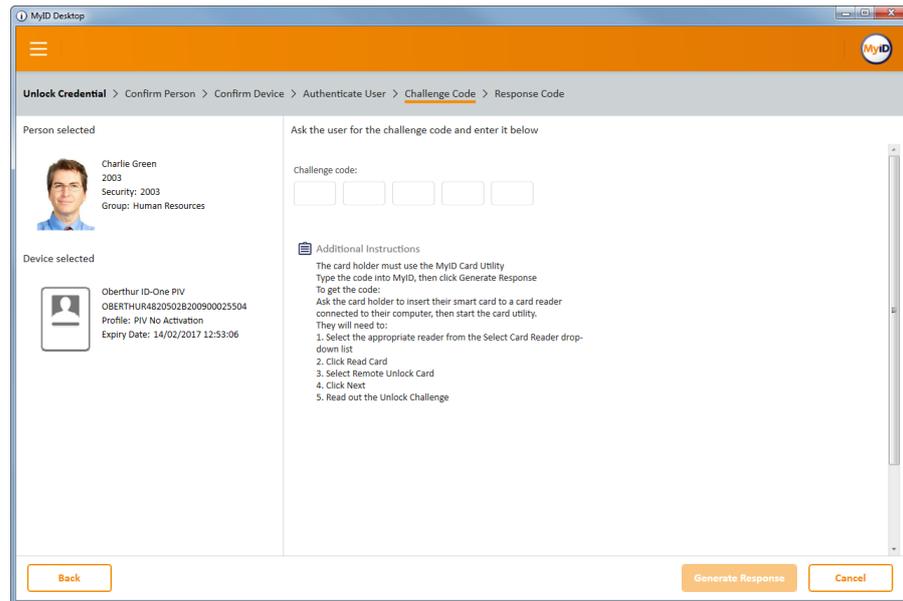
7. Ask the credential owner to read out the challenge code, and type it into the boxes provided.

8. Click **Generate Response**.
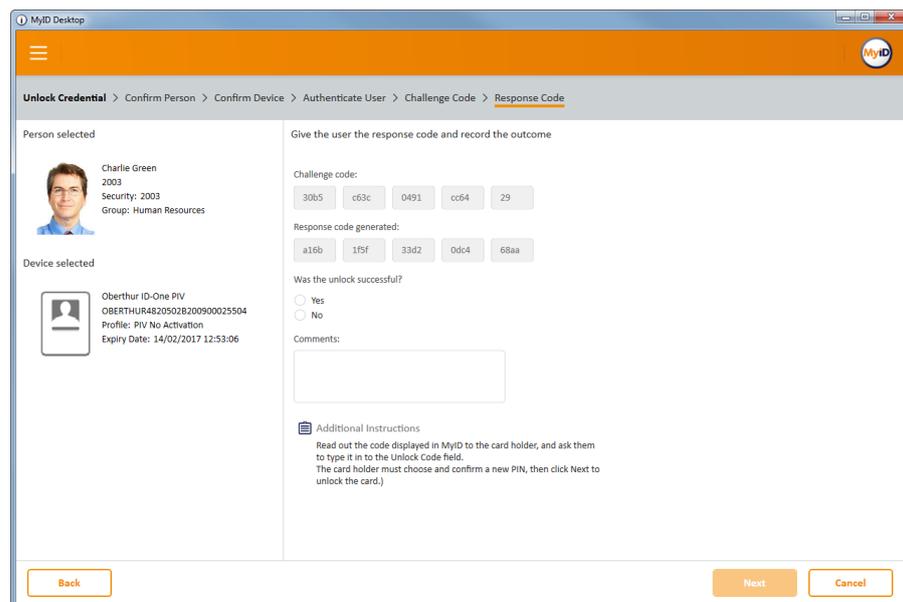
9. Read out the response code to the credential owner.

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.

27.7.7 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 section *15, Changing List Entries* 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**.

27.7.8 Requesting an authentication code

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

Authentication codes are used during card activation; see section *28.4, Activate card* 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 cancelled, 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 *27.7.3, Resetting your own PIN* for details.

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 *27.7.3*, *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 section *28.4*, *Activate card* for details.

27.8 Canceling cards

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

27.8.1 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.

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 select the card you want to enable or disable.

Card Status

Name: John Brown

Card Number: 1A853C713A8000041A853C71

Type: Gemalto .NET

Card Status: Enabled

Click continue to disable this card

Continue   Abort

3. To disable or enable a card (depending on its current state), click **Continue**.

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

    See section *29.5*, *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.

27.8.2 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 *27.8.3*, *Canceling a credential*.

Note: You cannot erase your own cards.

To cancel a card:

1. From the **Cards** category, select **Erase Card**.
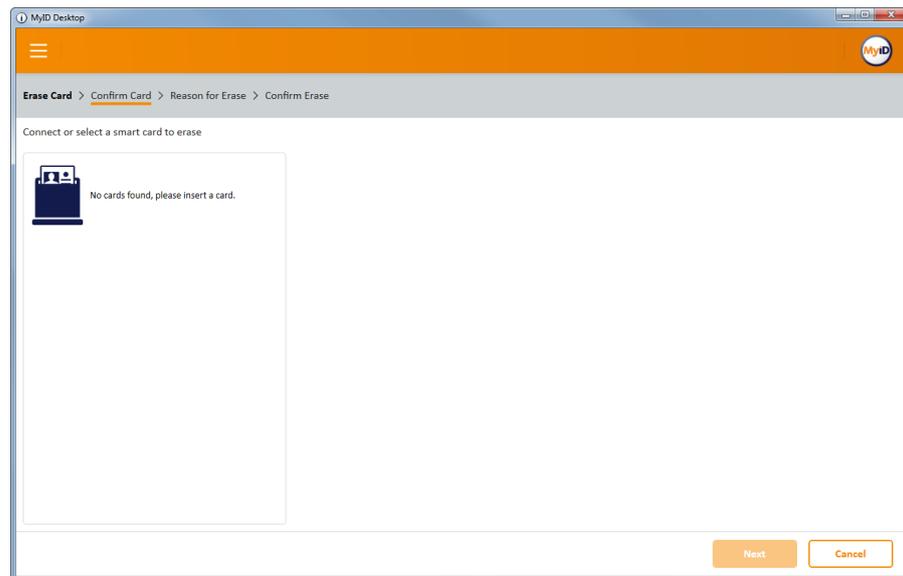
2. Insert the card you want to cancel and select it from the list.
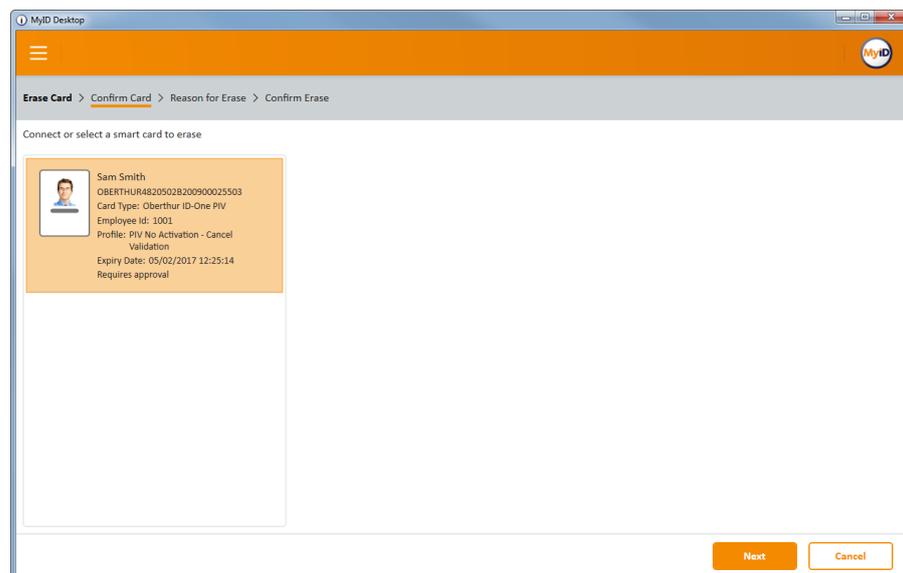
3. Click **Next**.
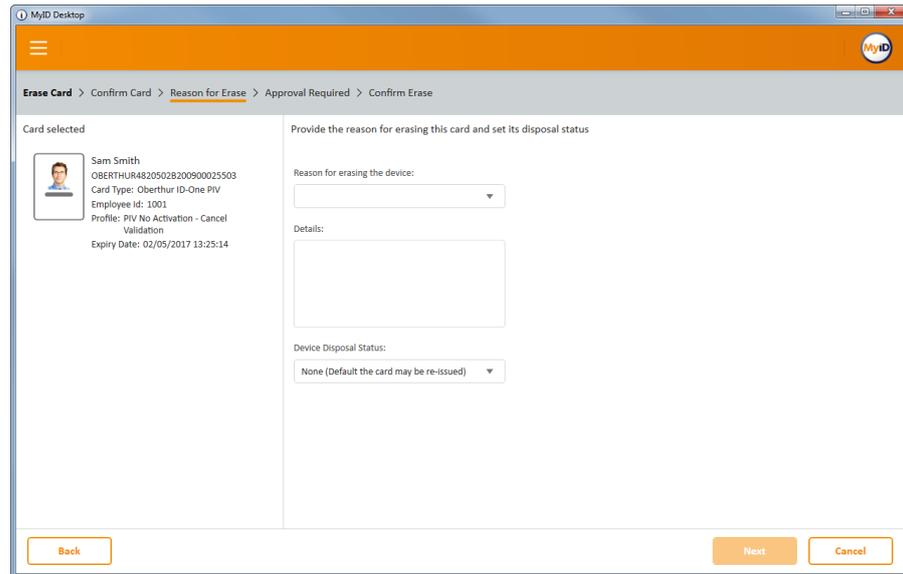
4. Provide the following information:

    - **Reason for erasing the device** – select the reason you are cancelling the card from the drop-down list. This reason affects how MyID treats the certificates on the card.

      See section *29.5*, *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 *27.12*, *Disposing of cards*.

5. Click **Next**.

6. If the credential profile used to issue the card had the **Validate Cancelation** 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 cancelled 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 cancelled 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.

27.8.3 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**.
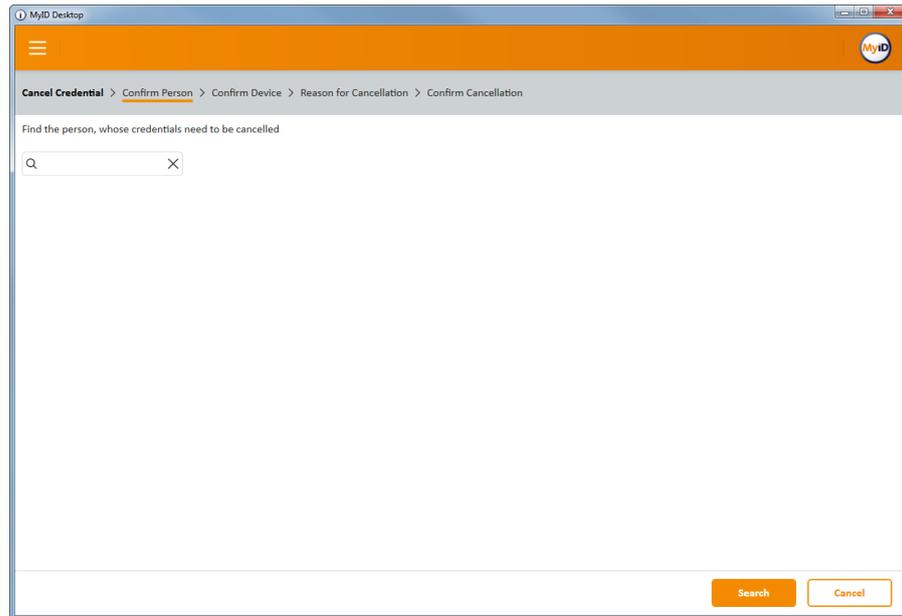
2. Enter the search criteria for the person who owns the credential you want to cancel, then click **Search**.

   See section *1.4.2*, *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.
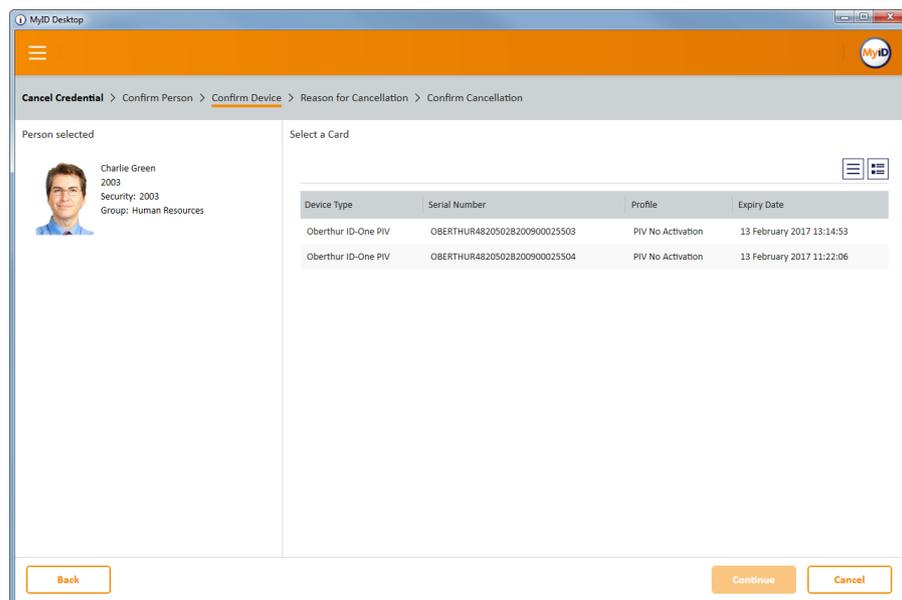
4. If the person has more than one credential, select the credential you want to cancel from the list.
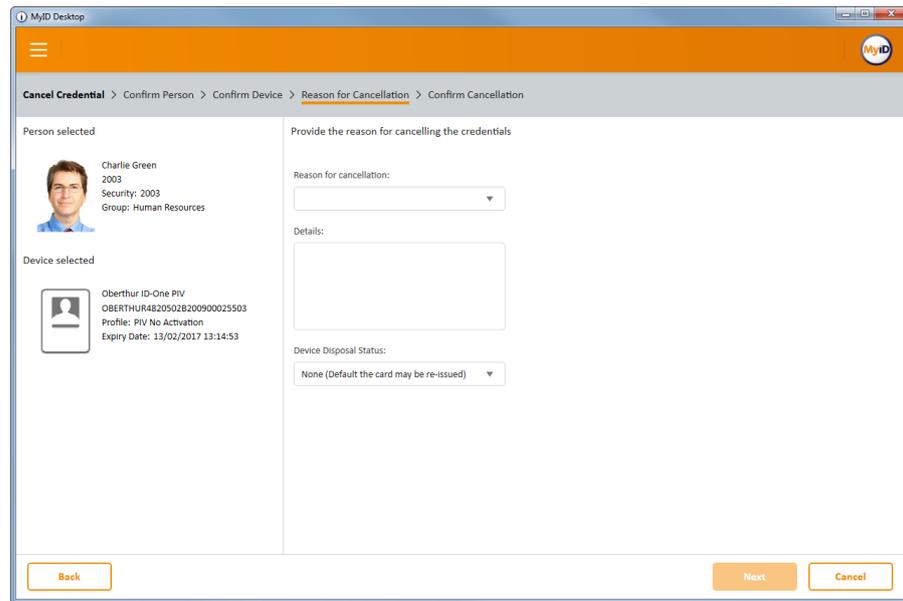
5. Provide the following information:

   ◆ **Reason for cancellation** – select the reason you are cancelling the credential from the drop-down list. This reason affects how MyID treats the certificates on the credential.

   See section *29.5*, *Certificate reasons* for details.

   ◆ **Details** – type further information on your reasons for cancelling 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 *27.12*, *Disposing of cards*.

6. Click **Next**.

7. If the credential profile used to issue the credential had the **Validate Cancelation** 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.

27.8.4   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 Credential Profiles.

▪ 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.

27.9   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**.

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**.

27.10 Batch Encoding

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.

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**.

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**.
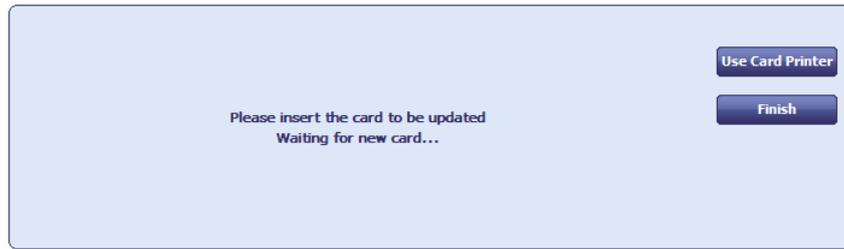
4. Insert the first card. If the card is in the correct state to be encoded, MyID encodes the card.
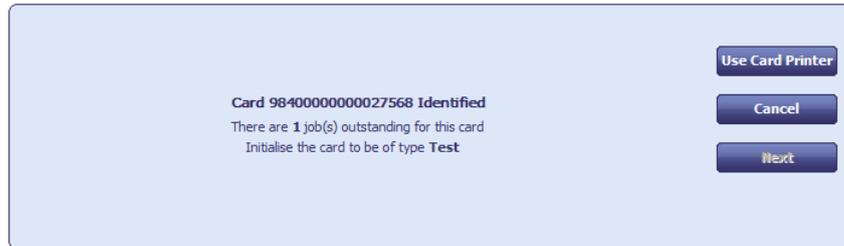
If you are using a hopper, the next card is inserted automatically. If you are using a card reader, insert the next card.

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.
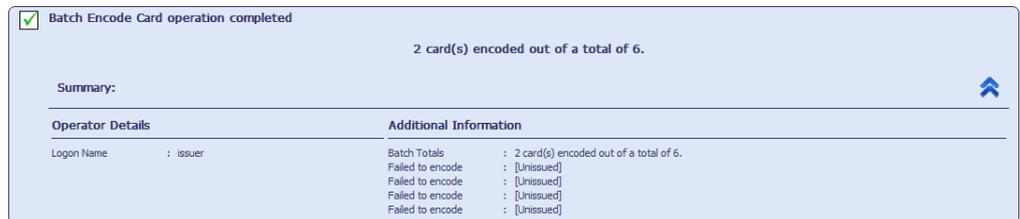
27.10.1   Timeout and automatic canceling

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.

27.11   Card ready notification

If you have set the **Additional 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.

27.12   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.

Note: You can also use the **Erase Card** workflow to set the disposal status of cards. See section *27.8.2*, *Erasing a card*.

To dispose of a card:

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

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

Alternatively, 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:

▫   **Disposed**

▫   **Legacy**

▫   **Collected**

▫   **Not Collected**

          □   **Lost**

Note: When you mark a card with the status Disposed, 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.

27.13   Reinstate Card

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.

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**.

27.14   Reprovision Card and Reprovision My Card

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

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

To reprovision a card:

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

    Note: 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.

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.

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

    See section *29.5, 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.

27.15 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.

27.15.1 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 section *11, Importing Serial Numbers* for details.

27.15.2 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. Insert the card you want to assign to the user in a card reader.

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.

27.15.3   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 without replacing it. Once you assign a card to a user, you can only unassign the card by assigning a different card.

28   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.

Self-collection of cards requiring activation allows you, for example, to send a locked card to a remote user, who can then use an authentication code or their enrolled biometrics to authenticate themselves to the MyID system and activate their card.

Operator-led collection of cards requiring activation allows you a greater range of authentication options; for example, you can require the operator to check the cardholder's identity documents, or simply allow the operator to authenticate the cardholder. You can configure MyID so that the operator can override the standard biometric authentication if, for example, the cardholder is unable to provide a match for their enrolled fingerprints because of an injury.

You can configure MyID to require the cardholder to read and sign a set of terms and conditions before their card can be activated.

You can also use the **Pre-encode Card** option to choose *when* MyID encodes the cards (that is, when MyID writes all of the personalized information to the card, including certificates). Your choices are:

- When the user activates the card – this is the quickest method for the operator, but the slowest for the end user, as the cardholder has to wait while the certificates are requested and written to their card.

- When the operator collects the card using **Collect Card** or **Batch Collect Card**.

- When the operator uses **Batch Encode Card** – this takes place *after* an operator has used **Collect Card** or **Batch Collect Card** to collect the card, or the cards have been returned from the bureau. This method allows you to separate the card printing process from the card encoding process.

28.1   Configuring a credential profile for activation

The **Require Activation** and **Pre-encode card** options in the Issuance Settings section of the credential profile determine if and how a card is to be activated.

- **Require Activation**

  This option means that MyID does not activate the card during collection. The card can be activated later by the applicant. The card is issued in a locked state; if possible, it is protected by the GlobalPlatform key, but it is also possible to activate cards that do not have GlobalPlatform keys, but are capable of having their PINs locked. The user must activate the card before it can be used. You can use this option with bureau-issued cards, and you can also use this option to issue cards from MyID.

  You can issue cards in the same state that a bureau returns cards. This allows you to activate cards for users in the same way as bureau cards are activated – you can print a batch of cards, then activate them one-by-one face-to-face with the users.

  Note: To support GlobalPlatform locking, you must set up GlobalPlatform Factory Keys and 9B keys for your cards before you can activate them.

From the **Require Activation** drop-down list, select one of the following options:

- **No** – the cards are not locked.

- **Allow self collection** – the cards are locked, and the applicants can collect the card using the **Activate Card** workflow in MyID Desktop, the Self-Service Kiosk, or the Self-Service App. See section *28.4, Activate card,* for details.

  This option also allows the applicant to use assisted activation with the help of an operator.

- **Assisted activation only** – the cards are locked, and the applicants must go to a MyID operator who collects the card for them using the **Assisted Activation** workflow. See section *28.5*, *Assisted activation*, for details.

Note: The **Require Activation** option locks the card when it is issued. Do not select the **Lock User PIN at Issuance** option, as this may cause an error.

Note: Do not set the **Issue With** option in the **PIN Settings** section to **Client Generated** or **Server Generated**. For cards that require activation, you must select **User specified PIN**.

You can then request and approve a number of cards, and use **Collect Card** or **Batch Collect Card** to issue them. This allows you to print the cards, but does not activate them.

By default, **Batch Collect Card** is not available to any of the standard roles. Use the **Edit Roles** workflow to add it.

For GlobalPlatform cards, in the Select Certificates stage, make sure that you select a certificate for signing. The card is issued with a blank chip that has its GlobalPlatform keys locked.

Note: You cannot use **Issue Card** for cards that require activation.

- **Pre-encode Card**

  From the **Pre-encode Card** drop-down list, select one of the following:

  - **None** – the card is encoded during activation.

  - **1-Step** – the card is encoded during collection.

  - **2-Step** – the card is encoded using the **Batch Encode Card** workflow after collection.

  Note: Both **1-Step** and **2-Step** pre-encode card options require activation.

28.1.1 Personalization and encoding scenarios

The **Require Activation** and **Pre-encode Card** options allow you to determine how the card is issued. You can determine whether the card is issued face-to-face, and whether the card is encoded by the cardholder when it is activated, when it is issued, or using the **Batch Encode Card** workflow.

Scenario	Require Activation	Pre-encode Card
Face to face issuance	☐	**None**
Bureau or batch issuance with cardholder encoding and activation	☑	**None**
Encoding using Collect Card or Batch Collect Card and cardholder activation	☑	**1-Step**
Bureau or batch issuance, encoding using Batch Encode Card, and cardholder activation	☑	**2-Step**

Note: If you select **Pre-encode Card** you must select **Require Activation**.

28.2 Terms and conditions

The **Terms and Conditions** and **Terms and Conditions Template** options in the Issuance Settings section of the credential profile determine whether the cardholder must read and sign a set of terms and conditions before activating their card.

- **Terms and Conditions**

  Select one of the following options:

  - **Explicitly Confirm** – the applicant must click a button to signify that they accept the terms and conditions.

  - **Silently Confirm** – the applicant is presumed to accept the terms and conditions by activating the card. The acceptance is audited and signed.

  - **Simple Confirmation** – as for **Explicitly Confirm**, but the applicant must accept the terms and conditions *before* specifying a new PIN for the card.

  - **Counter Sign** – as for **Explicitly Confirm**, but the operator must also enter their card's PIN to sign the terms and conditions with both the cardholder's and operator's credentials.

  - **None** – the applicant does not have to agree to terms and conditions to activate their card.

  You can amend the terms and conditions that users agree to when they activate their cards. See section *12.6*, *Customizing terms and conditions* for details.

  Note: You can also configure MyID to require users to sign terms and conditions when updating cards that have credential profiles that require them to sign terms and conditions when activating. See the **Terms and Conditions During Device Update** option in section *33.3*, *Devices page (Operation Settings)*.

  For explicit, silent, and countersigned terms and conditions, when the user accepts the terms and conditions, the acceptance is digitally signed using a signing certificate on the credential being issued. This means that if you are using these types of terms and conditions, you must make sure that you have configured a certificate for signing in the credential profile.

  For activations carried out using the **Activate Card** and **Assisted Activation** workflows, select a template from the **Terms and Conditions** drop-down list. See section *12.6*, *Customizing terms and conditions* for details.

28.3   Setting up authentication methods for activation

The authentication methods available for the **Activate Card** and **Assisted Activation** workflows are configured by a combination of the credential profile used to issue the card, global configuration options, and, in the case of **Assisted Activation** only, the operator's role configuration.

On the credential profile:

- **Require Fingerprints at Issuance** – to require fingerprints for activation, set to **Always Required**. If you set this to **System Default**, MyID looks at the **Additional Authentication** option.

- **Additional Authentication** – set to one of the following:

    - **Biometric** – biometric authentication is used to activate the card.

    - **Authentication Code (Manual)** – an authentication code is required to activate the card. An operator must request an authentication code.

    - **Authentication Code (Automatic)** – an authentication code is required to activate the card. An authentication code is emailed to the applicant when the card is issued.

    Note: If you want to use both biometrics and authentication codes, set the **Require Fingerprints at Issuance** option to **Always Required** and set the **Additional Authentication** option to an authentication code option.

    If you set the **Additional Authentication** option to **System Default**, MyID looks at the configuration options.

On the **Operation Settings** workflow:

- If the **Verify fingerprints during card creation** configuration option (on the **Biometrics** tab of the **Operation Settings** workflow) is set, and both **Require Fingerprints at Issuance** and **Additional Authentication** are set to **System Default** on the credential profile, the user must provide their fingerprints to activate their card.

- If both **Require Fingerprints at Issuance** and **Additional Authentication** are set to **System Default** on the credential profile, and the **Verify fingerprints during card unlock** configuration option is set to No, you must configure at least one operator override option for use in the **Assisted Activation** workflow (**Identity Documents** or **Operator Approval**) or you will be unable to complete the activation of the card.

    For the Assisted Activation workflow only, you can configure the operator override options using the **Edit Roles** workflow. The operator's role settings determine what options they can use if the cardholder cannot provide their fingerprints for some reason.

Note: The operator cannot override authentication codes.

In the **Edit Roles** workflow, under the **Assisted Activation** option for the operator's role, select the following options:

- **Biometric Bypass** – Select this option to allow the operator to bypass the fingerprint authentication stage if the cardholder cannot provide their fingerprints for some reason (for example, an injury). You must select this option if you want bypass the authentication; you must also select **Identity Documents** or **Operator Approval** to provide a method of continuing with the card activation.

- **Identity Documents** – Select this option to allow the operator to record details of the cardholder's identity documents as an alternative to fingerprint authentication.

- **Operator Approval** – Select this option to allow the operator to approve the authentication personally. The operator *must* provide a reason why they are providing approval.

- **Reject Authentication** – Select this option to allow the operator to complete the workflow without activating the card, while recording their observations and reasons for rejecting the authentication.

28.4   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 section *28.3*, *Setting up authentication methods for activation* for details.

   - If the credential profile is set up to require an authentication code, type it in the **Authentication Code** box.
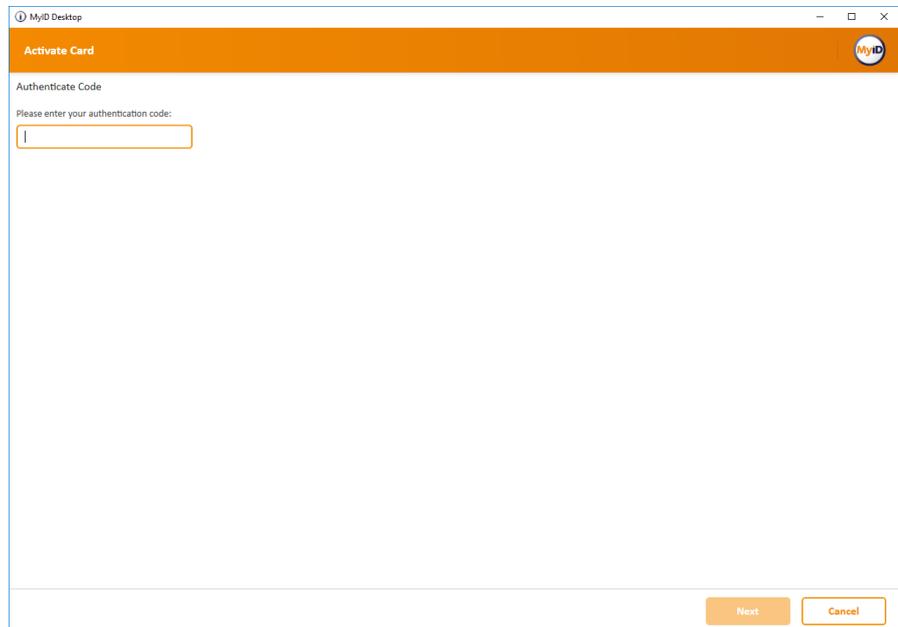
     You will have been sent an email containing the authentication code. If you make several invalid attempts to enter the code (as determined by the **Maximum Allowed OTP Failures** configuration option), the activation code is cancelled, and you must ask an administrator to generate another code.

     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.
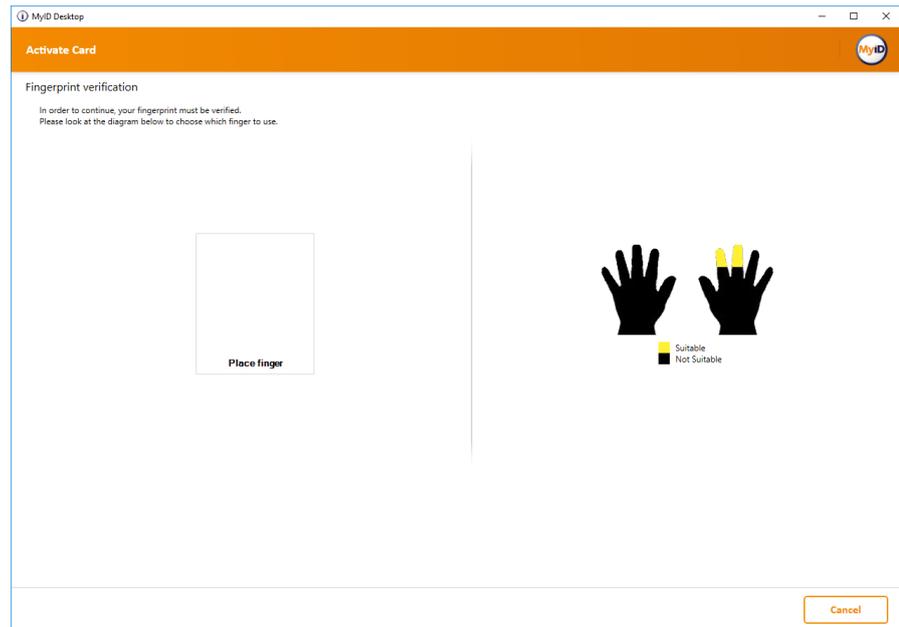
◆ If you are required to accept a set of terms and conditions, read the terms and conditions, then click **Accept**.
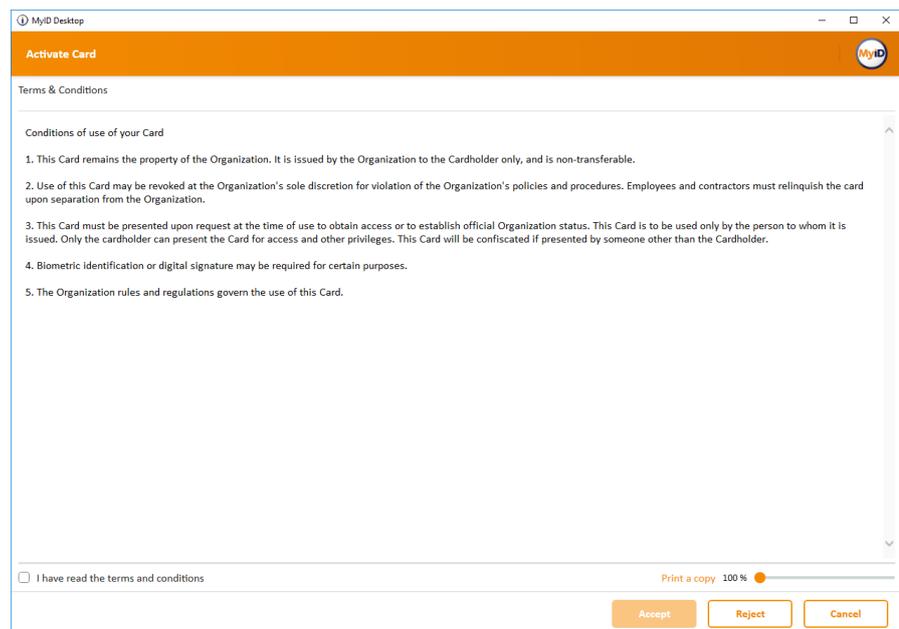
If you decline the terms and conditions, your authentication code (if you have one) cannot be used again, so you must request another code from an administrator.

Note: You can amend the terms and conditions that users agree to when they activate their cards. See section *12.6*, *Customizing terms and conditions* for details.

4. Enter your PIN, then click **Continue**.
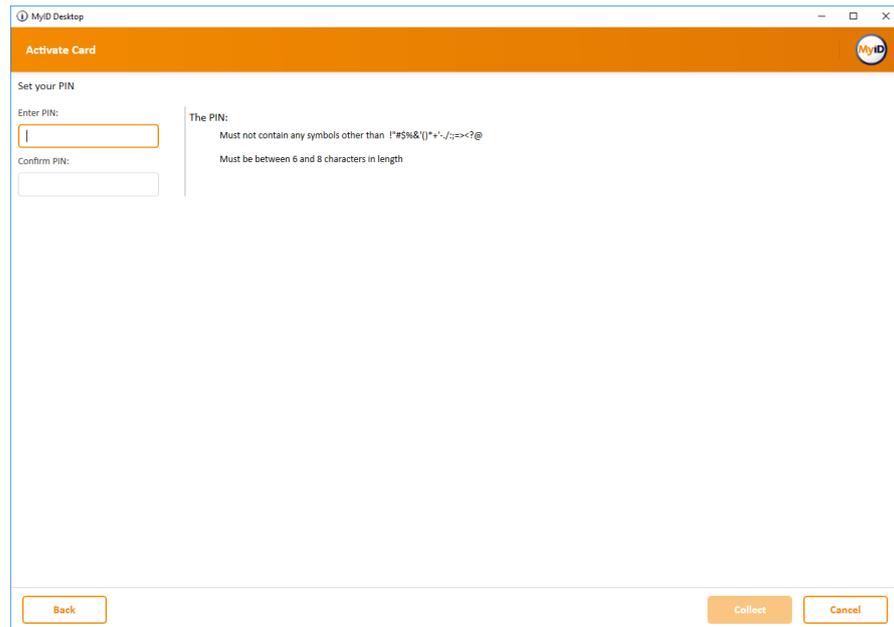
Your acceptance of the terms and conditions is digitally signed and audited.

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

28.5   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.

28.5.1   Carrying out an assisted activation

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 section *28.3*, *Setting up authentication methods for activation* 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.

   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.

29 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.

29.1 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 *29.3*, *Issuing soft certificates using a credential profile*, for details of working with soft certificates.

29.1.1 Collecting certificates

You can update a card to collect any pending certificates. You can collect certificates for another cardholder or for your own card.

Note: If you want to collect soft certificates, you must use the **Collect My Certificates** workflow.

To collect certificates:

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

   Please Insert card

   Card Serial Number: `<insert card>`

   Update

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 certificates for your own card:

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

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

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

29.1.2 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.

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.

29.2 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.

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.

5. Click **OK**.

6. Click **Revoke** to revoke or suspend the certificate:

7. Select the **Reason** from the drop-down list.

    See section *29.5*, *Certificate reasons* for details.

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

9. Click **Revoke**.

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.

29.3 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.

29.3.1 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 Profile** list, select a credential profile containing soft certificates.

   See section *12.5*, *Setting up a credential profile for soft certificates*, for details of setting up a profile.

5. Click **Request Card**.

29.3.2   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**.

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 settings in the credential profile:

- ◆ **Local Store** – the certificate is stored automatically in the certificate store of the logged-on user.

- ◆ **Password Protected PFX File** – 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.

- ◆ **Choose During Issuance** – select the output method.

29.3.3 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.

Certificate packages appear in the list of cards with names like "Certificate Package 1451".

29.4 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 passwords/security phrases.

29.4.1 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**.

2. Use the Find Person screen to select the person whose certificate you want to recover.
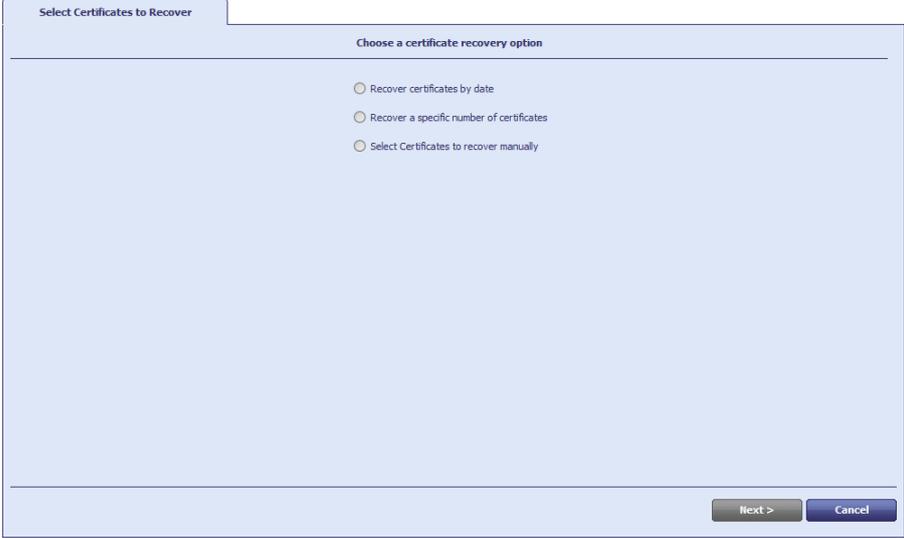
3. Select which certificates you want to recover:

   ◆ **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**.
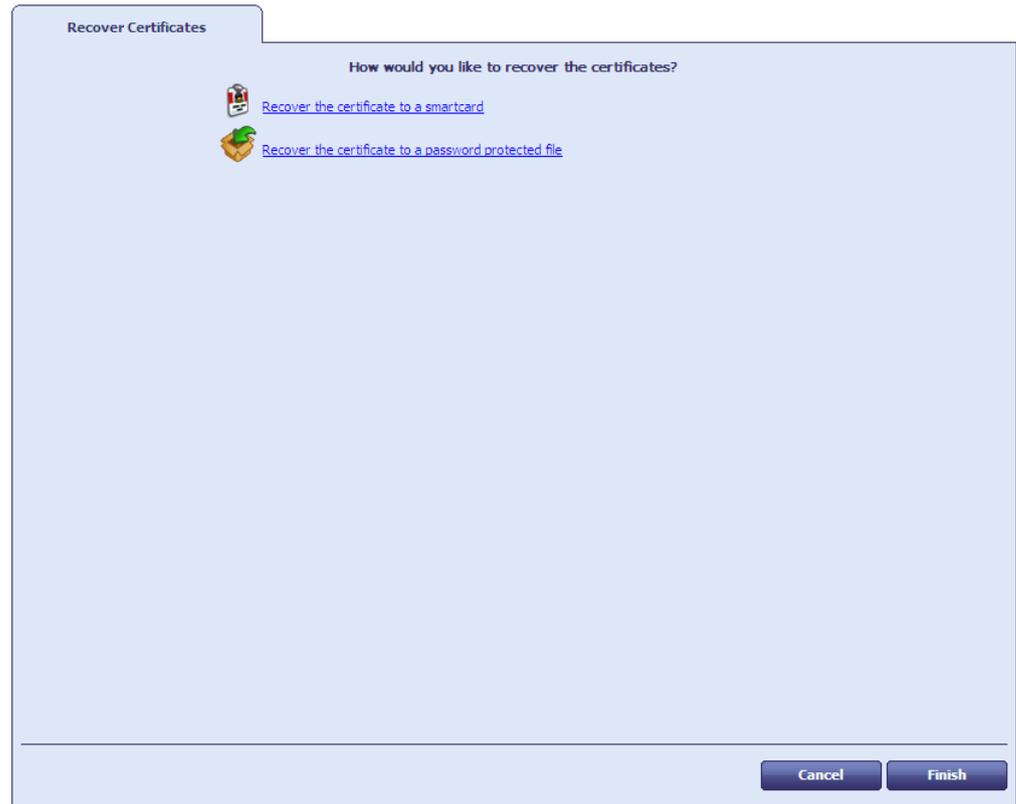
7. Select one of the following options:

- ◆ **Recover the certificate to a smartcard**

   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**

   Click **Choose destination**, then 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.

29.4.2   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**.
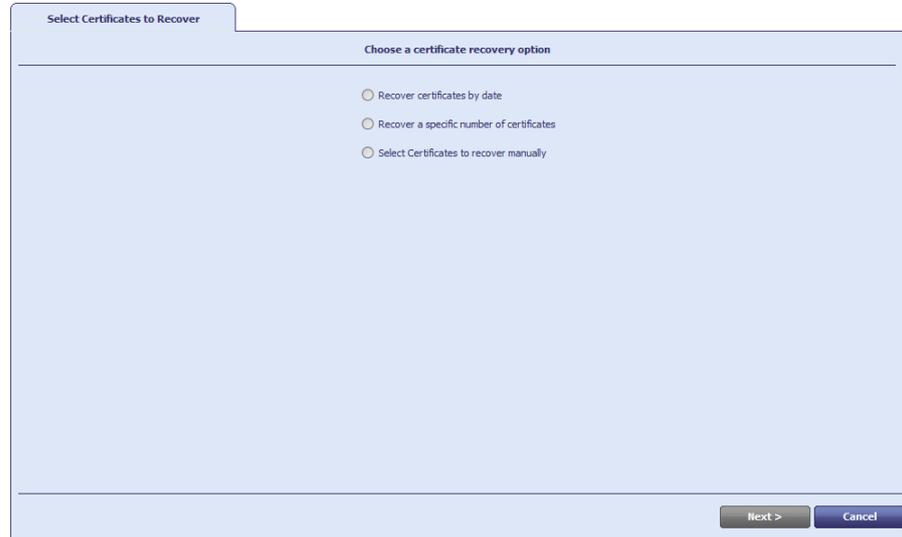
2. Select which certificates you want to recover:

    ◆ **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.

3. 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.

4. Type a **Reason for Recovery** in the text box.

5. Click **Next**.

---
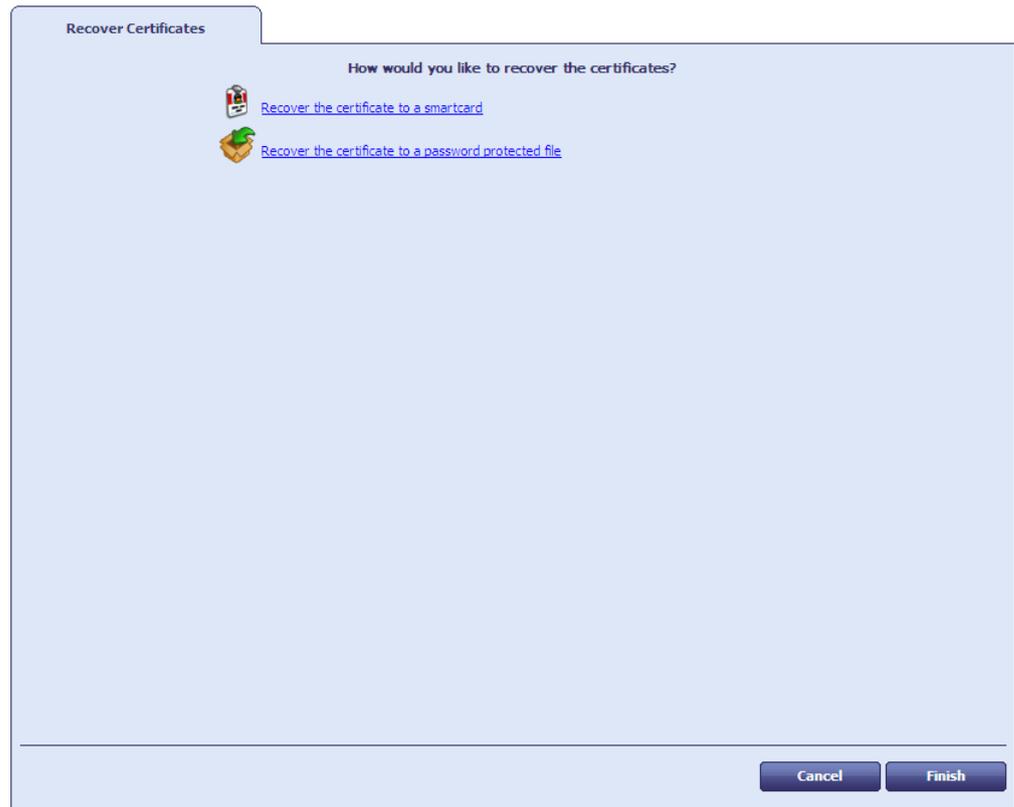
6. Select one of the following options:

♦ **Recover the certificate to a smartcard**

Click **Confirm** to confirm your card, type your **PIN**, then click **Next**. MyID writes the recovered certificates to the card.

♦ **Recover the certificate to a password protected file**

Click **Choose destination**, then 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.

If you want to recover the certificate to your local store, recover the certificate to a password protected file, then double-click the file to add it to your local store.

29.5   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 cancelling 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 cancelled 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.

- **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.

- **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.

- **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.

- **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.

- **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.

- **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.

- **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

- **Pending Investigation**

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:	None.

- **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

- **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

- **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

- **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

- **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.

- **Suspension (other)**

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:	None.

- **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

- **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

- **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.

- **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

- **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

- **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

- **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

- **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

- **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

- **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

- **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

- **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

- **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

- **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

- **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

- **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

- **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

29.5.1 Historic certificates

A historic certificate is any archived certificate that was assigned to the user (on any credential) using a particular certificate policies.

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. Cancelling 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.

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 cancelled, 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.

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)	

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.

29.6 Import and distribute certificates to devices

If you want to distribute certificates that have not been issued from a CA using MyID, you can import certificates in PFX files to MyID, then distribute them to your devices; for example, to your Identity Agent mobile identity.

29.6.1 Setting up the Unmanaged certificate authority

The Unmanaged entry in the **Certificate Authorities** workflow allows you to control the issuance of certificates uploaded from PFX files.

By default, a single active Unmanaged policy is provided, and an additional Unmanaged policy is provided in a disabled state. If you are going to use both unmanaged policies, you must use the **Certificate Authorities** workflow to enable the second policy; you are also strongly recommended to rename the unmanaged policies to allow you to distinguish between them.

If you need more policies, you must add the appropriate entries to the MyID database. For more information, contact customer support, quoting reference SUP-229.

Note: When you are setting up the Unmanaged certificate authority, if you choose to renew any of the Unmanaged certificates automatically, you must supersede the policy with a different policy on a CA that is not the Unmanaged CA.

29.6.2 Setting up a credential profile for PFX certificates

In the **Services** section of the credential profile, you must select the **MyID Encryption** option so that MyID can issue the PFX securely; you can then select a certificate to use for encryption on the Select Certificates stage. If you do not select a certificate for encryption, MyID will generate a keypair for the credential to be used for encryption (the MyID Encryption Keys) instead of a certificate.

Note: If you do not select the **MyID Encryption** option, when you try to issue a card you will see an error similar to:

```
Failed to recover key from server
```

When you set up a credential profile, on the Select Certificates stage, select the unmanaged policies you want to use to issue certificates from PFX files. By default, there is a single active option, named **Unmanaged**.

Select one of the following options:

- **Use Existing** – provide the user with the most recent active certificate.

  This option will not transfer the certificate if it has expired, therefore issuance of the credential profile will fail. If no imported certificate exists, issuance of the credential profile will fail. The user must have a valid imported certificate to receive a credential with this setting.

  If you select the **Use Existing** option, and you are using a data model with named containers, you must select an appropriate container for the certificate. If you do not want to place the certificate in a container, you must select **Historic Only** instead, and select the **Default** option for the container, which will place the certificate in one of the card's historic containers. You cannot select **Use Existing** and select the **Default** container.

- **Historic Only** – select this option to allow certificates to be transferred without checking the expiry date, or where the user may not have an imported certificate.

  This option may place the certificate in historic certificate containers on the device, depending on its capabilities; for example, devices that use a PIV Applet.

Note: You cannot select **Issue new**.

29.6.3 Uploading multiple PFX certificates

Each user can upload multiple PFX certificates to MyID, which will be recovered to that user's credential (for example, to Identity Agent) when an appropriately-configured credential profile is issued.

This is a self-service operation. An operator cannot upload PFX files on behalf of the user. You must make sure that the user has permissions to log into MyID, and their role has permissions to access the **Upload PFX Certificates** workflow.

To upload PFX certificates:

1. From the **Certificates** category, select **Upload PFX Certificates**.

2. Click the **Browse for a PFX certificate** button next to the **PFX Certificate** box, then select the PFX file you want to upload and click **Open**.

3. Type the **PFX Password**.

4. From the **Certificate Policy** drop-down list, select the unmanaged certificate policy you want to associate with this PFX.

    The list contains all enabled certificate policies that are currently assigned to the Unmanaged certificate authority. See section *29.6.1*, *Setting up the Unmanaged certificate authority* for details.

5. Click **Add**.

    The certificate is uploaded to the MyID database, and stored ready to be issued when you request it.

Note: If you attempt to upload a certificate you have previously uploaded to the same certificate policy, you are given a warning, and allowed to proceed or cancel the operation.
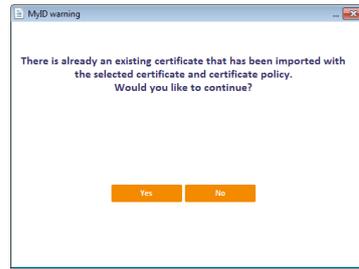
6. Click **Finish**.

29.6.4 Removing uploaded certificates

To remove an uploaded certificate:

1. From the **Certificates** category, select **Upload PFX Certificates**.

2. Click the **Delete this certificate** option next to the certificate you want to delete.

   Note: You cannot delete a certificate if it has been issued to a credential. Before you can delete the certificate, you must cancel all credentials to which it has been issued.

3. Click **Finish**.

30 Managing Devices

This document provides information on requesting device identities, validating device identity requests, and validating device identity cancelations. These identities can be assigned to computers and other equipment on the network.

MyID also supports the Simple Certificate Enrollment Protocol (SCEP) for issuing device identities. Support for SCEP requires an additional software module – contact your sales representative for more information. See the *SCEP Device Identities Integration Guide* for details on using MyID to issue SCEP device identities.

Note: In addition to the workflows within MyID, you can manage devices using the MyID Device Management API. See the *Device Management API* document for details.

30.1 Access to the workflows

You must use the **Edit Roles** workflow to create or amend roles to provide access to the following workflows:

- **Add Devices** and **Edit Devices** in the **Configuration** category are needed to make the devices available to MyID.

- **Confirm Cancel Device Request**, **Request Device Identity** and **Validate Device Request** in the **Devices** category are needed to manage credentials for devices.

   Note: The scope of the role with access to these workflows must be at least Department.

- **Collect Device Identity** is used in the MyID Self Service Application.

   This role must be accessible using Passwords, depending on how the operators are authenticating to the MyID Self Service Application.

- **View Devices** and **Register Credential** are currently not available.

You must also make sure that the MyID operator has access to the user's devices. If you are using an LDAP directory as the primary data source or are importing information into MyID from an LDAP directory, you must add the **(Devices)** group to the operator's list of administrative groups.

Note: To allow you to edit the administrative groups, you must set the **Allow Administrative Groups** option on the **Process** tab of the **Security Settings** workflow in the **Configuration** category.

Alternatively, you can set the operator's scope to **All**; however, this has the effect of granting the operator access to every user records in the MyID system, so is not recommended.

30.2 Installing client support software for device identities

Device identities are supported only on Windows 7 64-bit clients. You must install the MyID Middleware and TPM Software package on each Windows 7 client that you intend to use to collect device identities. To obtain this package, contact customer support, quoting reference SUP-120.

30.3 Setting up a credential profile to use to issue device identities

Before you can request a device identity, you must set up at least one credential profile to use for issuing device identities.

To set up a credential profile:

1. From the **Configuration** category, select **Credential Profiles**.

2. Click **New**.

3. In the **Card Encoding** section, select **Device Identity (Only)**.

4. Type a **Name** and **Description** for the credential profile.

5. Click **Issuance Settings**.

6. Select the following options:

    ◆ **Validate Issuance** – select this option if you want to ensure that all device identity requests are approved before the device identity can be collected.

    ◆ **Validate Cancelation** – select this option if you want to ensure that all device identity cancelations are approved before the device identity is canceled.

    ◆ **Require Challenge** – for SCEP device identities only. You can choose whether to display the one-time challenge code on screen or send an email message containing the challenge code. See section *30.7*, *Requesting a device identity* for details.

    Note: Do not select the **Require user data to be approved** option. The device identity is issued to a device, not a user, and therefore cannot have the user data approved flag set.

7. Click **Next**.

8. Select the certificate you want to issue to the device.

    Note: Do not select a certificate policy that has the **Automatic Renewal** option set in the **Certificate Authorities** workflow – device identities do not support automatic renewals. If you need to renew a device identity, you must request a new identity for the device.

    Note: You must not select any certificates policies that are marked as archived; you cannot issue device identities with archived certificates. If you attempt to collect a device identity using a credential profile that has an archived certificate, the collection will fail.

9. Click **Next** and complete the workflow.

30.4 Configuring number of certificates per device

If you want to support only a single certificate on each device, where any existing certificates are removed when a new certificate is collected, you can edit the card properties file for TPMs.

To edit the card properties file:

1. On the MyID application server, back up the TPM card properties file `CardPropertiesPTPM.xml`.

    By default, this is in the following folder:

    `C:\Program Files (x86)\Intercede\MyID\Components\Devices\`

2. Open the `CardPropertiesPTPM.xml` file in a text editor.

3. Locate the following line:

    `<restrictToSingleCertificate>0</restrictToSingleCertificate>`

4. Change the line to read:

```
<restrictToSingleCertificate>1</restrictToSingleCertificate>
```

5. Save the file.

30.5 Adding devices

To add devices to MyID, you use the **Add Devices** workflow (in the **Configuration** category). You can add details manually or you can search an LDAP directory for a device if you are using an LDAP directory as your primary data source.

To enable use of the **Add Devices** workflow, you must set the **Allow device management from the MyID user interface** option to Yes. See section *33.3*, *Devices page (Operation Settings)*.

To search for a device in an LDAP directory, you must set the **Allow LDAP Search for devices during Add Devices** option to Yes. See section *33.4*, *LDAP page (Operation Settings)*.

30.5.1 Adding devices manually

To add a device:

1. In the **Configuration** category, select the **Add Devices** workflow.

   If MyID is not configured to allow you to search the LDAP directory, the screen for manually adding devices is automatically displayed.

   Alternatively, click **Manually Add**.

2. Give the device a name and description to help identify it.

3. If you want it to be available, select **Device Active**.

4. You can optionally specify a **DN** for the device.

5. For mobile devices, you can specify the **Model** and **OS**.

   MyID does not provide any validation of this DN. If you specify a value in this field, you must ensure that it is a valid DN; the value will be used in the issued device identity certificate. For example:

   ```
   CN=mydevicename,DC=mydomain,DC=local
   ```

If you specify an invalid DN, you may see an error similar to the following:

```
Failed to get size of DN
```

6. Click **Finish**.

7. If you want to specify an owner for the device:

   a) Click **Yes** on the dialog.

   b) Use the Find Person screen to select the owner.

   If you specify an owner, the device can be managed only by the owner; for example, only the owner can cancel a device identity. In addition, the device owner is used as the target of the request device identity job.

30.5.2   Adding devices from an LDAP directory

To add a device from a directory:

1. From the **Configuration** category, select **Add Devices**.
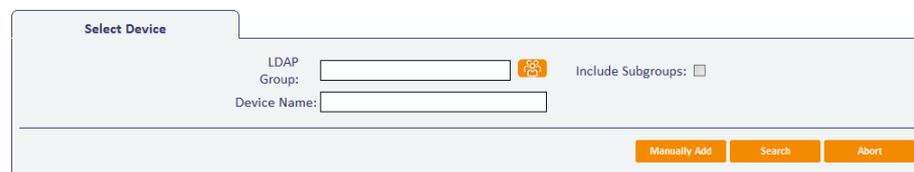
2. Click the button next to the **LDAP Group** field .

3. If you want to search subgroups of the directory, select the **Include Subgroups** option.

4. Select the branch of the directory that contains the device you want to add.

5. Click **Search**.

   If you need this search to return devices based on different criteria, contact customer support for assistance.

6. From the list, select the devices you want to add.

7. Click **Finish** to import all the devices.

   Alternatively, click **Edit Devices** to specify whether each device is active as you import it. A separate screen is displayed for each device; select or deselect the **Device Active** option, then click one of the following:

   ◆ **Import** – import the currently-displayed device and move on to the next.

   ◆ **Skip** – do not import the currently-displayed device and move on to the next.

   ◆ **Finish** – import the currently-displayed device and all following devices. Devices you have already imported or skipped are not affected.

   ◆ **Cancel** – cancel the import. No devices are imported.

8. If you want to specify an owner for the devices:

   ◆ Click **Yes** on the dialog.

   ◆ Use the Find Person screen to select the owner.

   If you specify an owner, the device can be managed only by the owner; for example, only the owner can cancel a device identity. In addition, the device owner is used as the target of the request device identity job.

30.6   Editing a device

To enable use of the **Edit Devices** workflow, you must set the **Allow device management from the MyID user interface** option to Yes. See section *33.3*, *Devices page (Operation Settings)*.

To make changes to details stored about a device:

1.   In the **Configuration** category, select the **Edit Devices** workflow.

2.   Type all or part of the device name and click **Search**.

3.   Select the device you want to edit from the list and click **Edit Device**.

4.   You can change the **Description**, whether the device is active or not, its **Model**, its **OS**, and its **DN**. Other information cannot be changed as that is what uniquely identifies the device.

5.   Click **Finish**.

---

6. If you want to specify an owner for the device:

   a) Click **Yes** on the dialog.

   b) Use the Find Person screen to select the owner.

If you specify an owner, the device can be managed only by the owner; for example, only the owner can cancel a device identity. In addition, the device owner is used as the target of the request device identity job.

30.7 Requesting a device identity

To request a device identity:

1. From the **Device Identities** category, select **Request Device Identity**.

2. Select the credential profile you want to use for the device identity.

3. If the credential profile contains the **Require Challenge** option, select how the one-time challenge code is provided:

    ◆ **Display Challenge Code** – displays the challenge code on screen.

    ◆ **Email Challenge Code** – sends the challenge code in an email message.

    ◆ **Both** – displays and sends the challenge code.

The **Require Challenge** option is currently available only for SCEP device identities.

Note: The **Output Mechanism for Job Challenge Code Generation** configuration option allows you to specify the setting for this feature globally; the default is **Choose at request**, which allows you to choose the way the one-time challenge code is provided when you request the device identity.

4. Click **Assign Device**.

5. Search for the device for which you are requesting the device identity.

You can type part of the name to restrict the search.

Click **Search**.

MyID returns a list of the devices that match your search. The list includes only devices without owners, or whose owners fall within your scope.

6. Select the device from the list, and click **Finish**.

If the credential profile contains the **Require Challenge** option, and you requested the challenge code to appear on screen, the challenge code is listed on the summary screen at the end of the workflow.

MyID creates a job for the collection of the device identity. If the credential profile used to request the device identity has the **Validate Issuance** option set, you must approve the request before the device identity can be collected; see section *30.8*, *Validating a device identity request* for details.

30.8   Validating a device identity request

If the credential profile used to request the device identity has the **Validate Issuance** option set, you must approve the request before the device identity can be collected.

To validate a device identity request:

1. From the **Device Identities** category, select **Validate Device Request**.
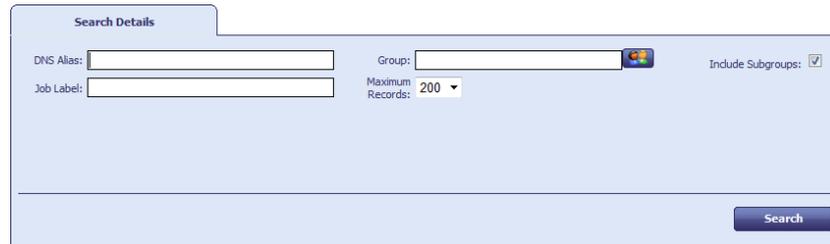
2. Search for the device identity you want to approve:

    a) Restrict the search using the **DNS Alias** for the device and the **Group** to which the device belongs.

    If you know the job label, use that to identify the record.

    b) Click **Search**.

3. Select the job from the list, and click **Next**.
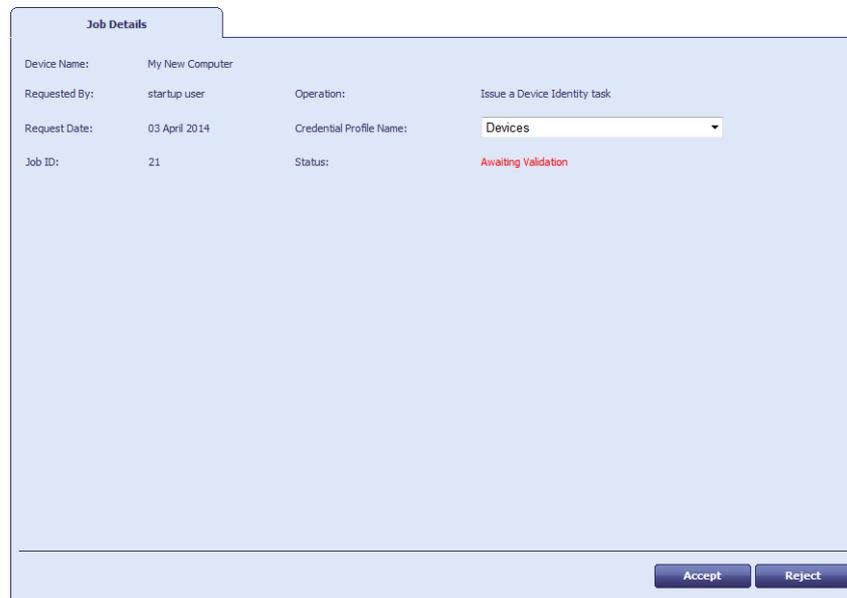
4. Review the details of the request.

    If necessary, you can change the credential profile used to issue the device identity – select the **Credential Profile Name** from the drop-down list.

5. Either **Accept** the request, or click **Reject** and supply a reason for not approving the request.
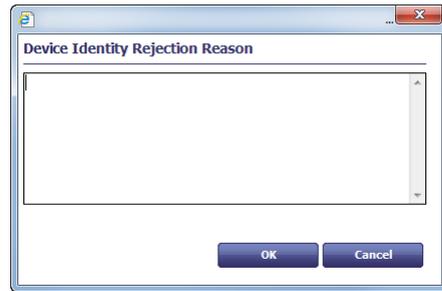
30.9 Collecting device identities

If the credential profile used to request the device identity has the **Validate Issuance** option set, you must approve the request before the device identity can be collected; see section *30.8*, *Validating a device identity request* for details.

Once the request has been approved (if necessary), the user can collect the device identity using the Self-Service App Automation Mode. See the ***Self-Service Installation and Configuration*** document for details.

Note: When you collect the device identity, if the PC previously had a device identity installed, any old certificates are removed from the TPM on the PC. Only the new certificate is retained.

For SCEP device identities, you can collect the device identity directly from the device using the MyID SCEP web page. See the ***SCEP Device Identities Integration Guide*** for details.

30.10   Canceling device identities

Note: When you cancel a device identity, MyID also cancels any outstanding device identity requests for the specified device. Accordingly, if you intend to reissue a device identity, you must cancel the device identity *before* you request the replacement.

You can request a device cancelation using the **Cancel Device Identity** workflow.

Note: The **Cancel Device Identity** workflow allows you to cancel a device identity that is unassigned, or is assigned to the currently logged-on MyID user. If you need to cancel a device identity that is assigned to anyone else, you must either remove the person assigned to the device, making it unassigned, or give the user access to the **Cancel Device Identity** workflow so that they can cancel their own device identity.

To cancel a device identity:

1.   From the **Device Identities** category, select **Cancel Device Identity**.
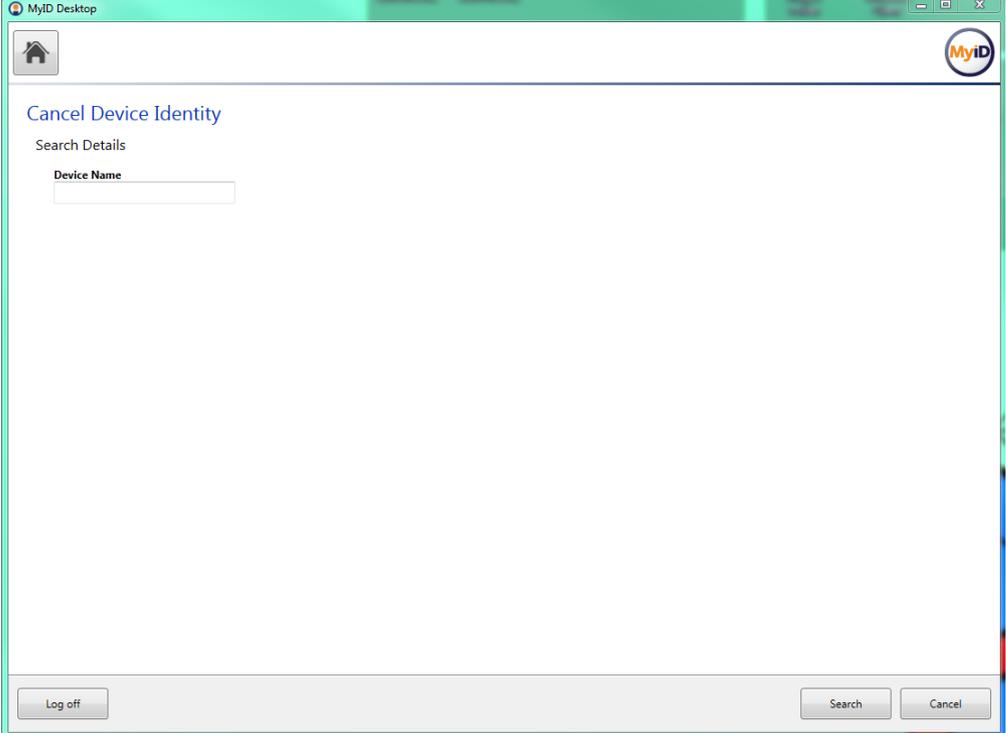
2.   Optionally, type the name of the device you want to search for.

    You can use * wildcards in the device name.

3.   Click **Search**.
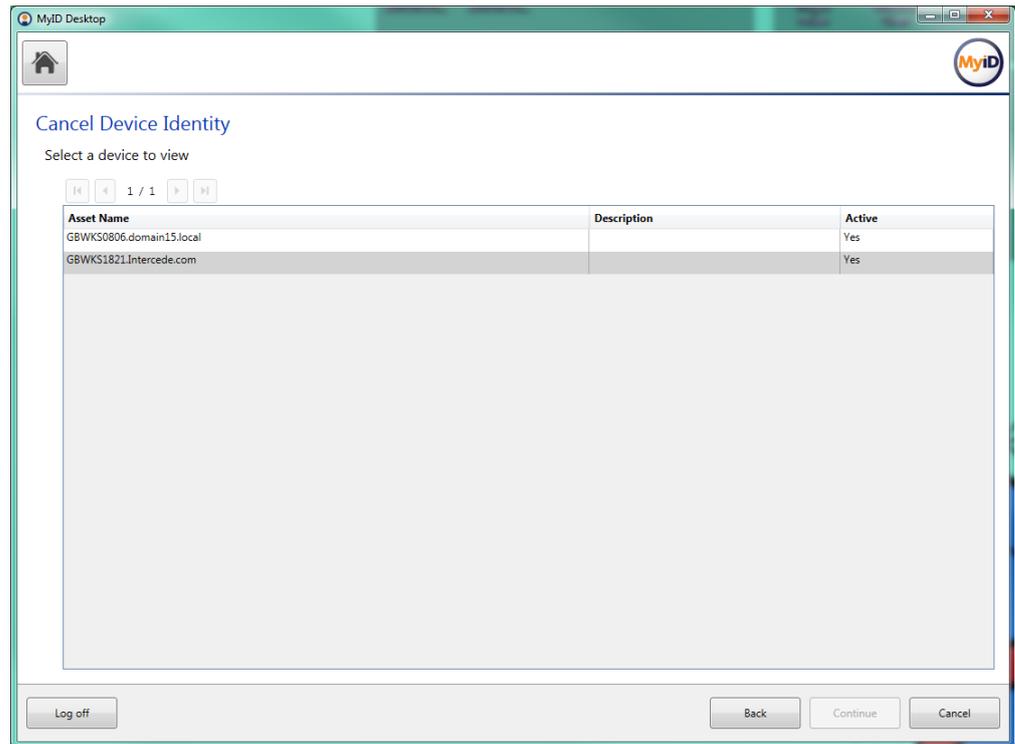
4. From the search results list, select a device, and click **Continue**.

   If the device does not have a currently-issued identity, MyID informs you.
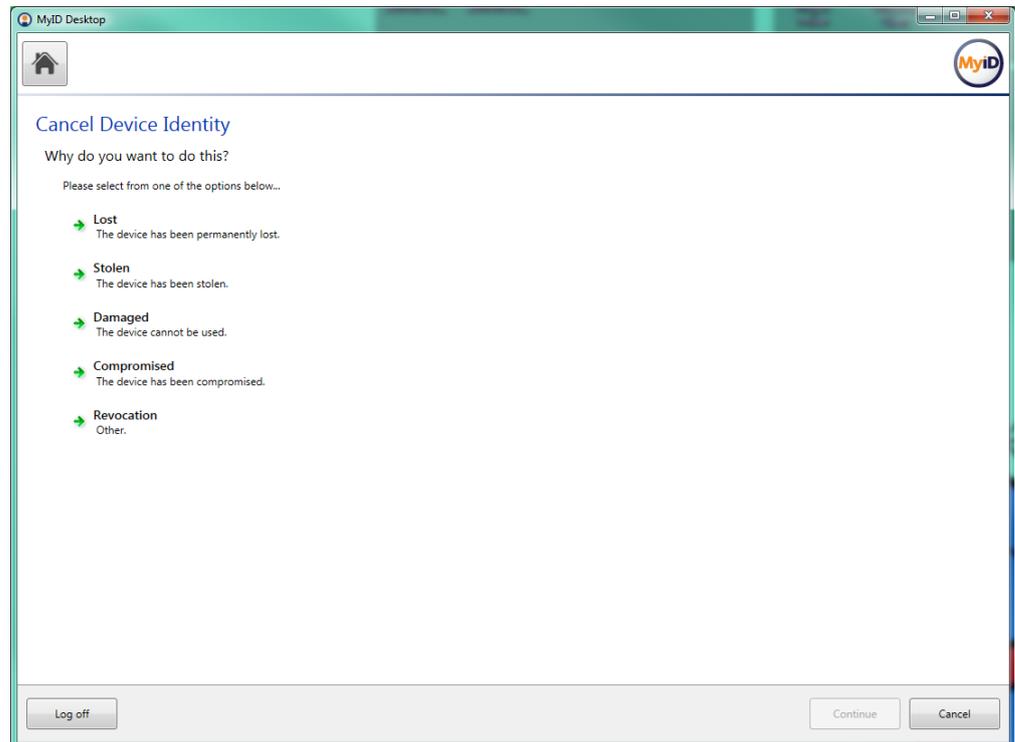
5. Select the reason for the cancelation, then click **Continue**.

   See section *29.5*, *Certificate reasons* for details.
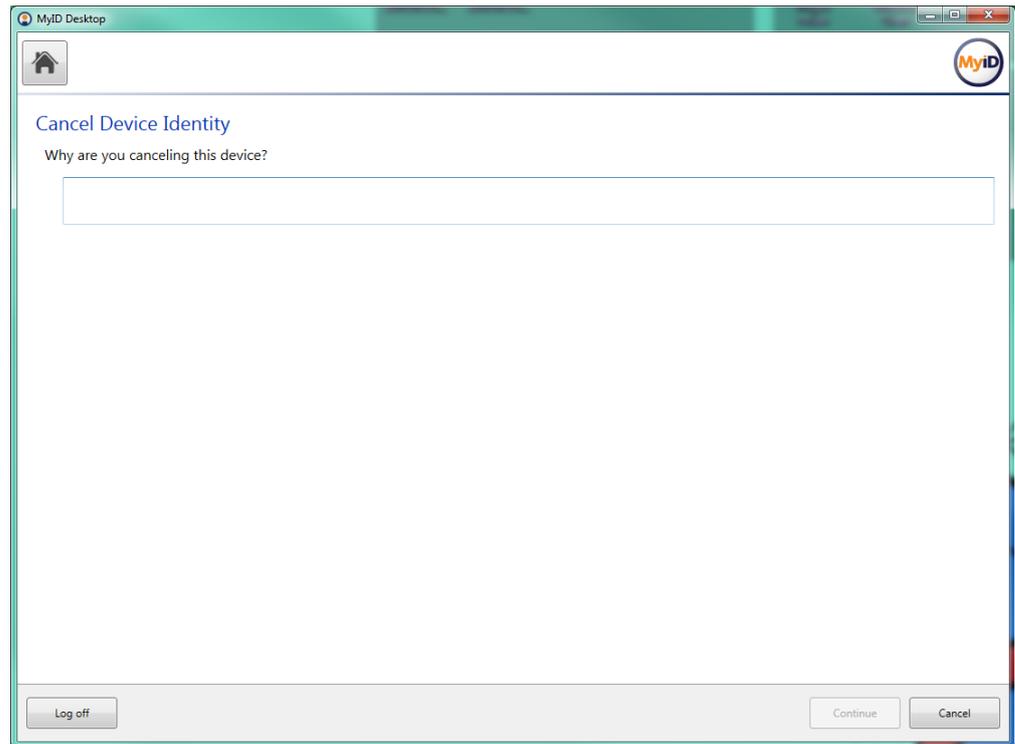
6. Type the reason you are cancelling the identity, then click **Continue**.

   If the credential profile does not have the **Validate Cancelation** option set, MyID cancels the device identity.

   If the credential profile *does* have the **Validate Cancelation** option set, you must use the **Confirm Cancel Device Request** workflow to approve the cancelation.

30.11 Approving device identity cancellations

If the credential profile used to request the device identity has the **Validate Cancelation** option set, you must approve the request before the device identity is canceled.

To approve a device identity cancelation request:

1. From the **Device Identities** category, select **Confirm Cancel Device Request**.
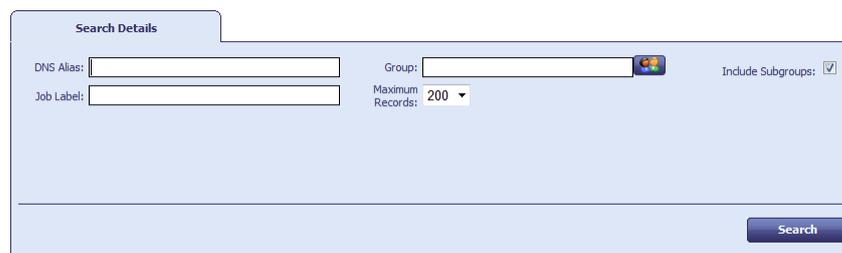
2. Search for the device identity you want to cancel:

   a) Restrict the search using the **DNS Alias** for the device and the **Group** to which the device belongs.

      Specify the Job Label if known to go straight to the correct record.

   b) Click **Search**.

3. Select the device cancelation job from the list.

4. Review the details of the cancelation, then either **Approve** the cancelation, or click **Reject** and supply a reason for not approving the cancelation.

30.12   Known issues

- **IKB-17 – Cannot open Device Identity workflows with a scope of Self**

    If you have access to the **Request Device Identity** and **Validate Device Request** workflows with a scope of Self, when you try to open the workflows, the workflows fail to open and you are returned to the main page. The audit may contain an error similar to:

    ```
    An error occurred inside CBOL_GetGroupsWeb::GetGroups An error
    occurred inside CBOL_GetGroupsImpl::GetGroups DAL std::exception
    catch handler Function : Get, catch hander. Error : Error:
    0x00000011 : Field is not an integer
    ```

    To stop this error from occurring, make sure your scope for the workflows is greater than Self.

31 Troubleshooting

In addition to the tools discussed in this section, you can use the standard operating system reports (Windows Event Viewer) and tools provided with third party products, such as middleware or certificate authorities, to identify issues.

31.1 System status report

To generate a System Status report, from the **Reports** category, select **System Status**.

You do not need to enter any criteria for this report.

It displays information on six pages:

- Basic **Details** about your installation, including the product version, supported card types, connected readers, enabled CAs, and directories.

- Details of the **Components** (DLLs) installed as part of your MyID system, giving the File Version, Product Version and Location of each of them.

- Current **License** information, as displayed in the Licensing workflow (see section *13, License Management*).

- An **Installation History**, detailing the SQL scripts that have been run.

- The current settings of the options in the Configuration table in the database. This shows all settings, not just those that can be accessed through the **Operation Settings** and **Security Settings** workflows (see *33* and *34).*

- A summary of the **Credentials** for each Credential Profile in the system, with details of the number of credentials issued to or pending for each profile.

You may be asked to provide a copy of the contents of this report if you need to raise a support call. Click the **Save As** button to save a copy of the whole report in HTML format.

31.2 System events report

The **System Events** report allows you to generate a user-defined report by completing one or more fields on the **Report Security Events** form. For example, you might want to display all events for a particular person or security device on a given date.

Note: All times are displayed in UTC.

To run a System Events report:

1. From the **Reports** category, select **System Events** to display the **Report Security Events** form.

   The **Report Security Events** form allows you to specify the information to be included in the **Selected Events** table. For example, you might want to display all events between two particular dates. To customize the listing, complete the form as appropriate.

   Note: To move the cursor to the next field, press TAB, not ENTER (pressing ENTER has the same effect as choosing **Search**).

   To return all fields to their original values, select **Reset**.

2. Complete this form as appropriate and select **Search**.

   A list of matching events is displayed in the **Selected Events** table at the bottom of the screen.

3. To print the report, click the print button.

4. To save the report, select **XML**, **CSV**, or **Excel** to select the format, then click the save button.

31.2.1 Archived System Events

You can set up MyID to archive the contents of the system events table in the MyID database periodically in a similar way to archiving the `Audit` table – see the ***Installation and Configuration Guide*** for details.

31.3 Expanded error messages

You can choose whether to display an error message with access (a link) to a detailed technical explanation of an error. The message can be saved to file, enabling it to be sent with a support call.

To set this option:

1. From the **Configuration** workflow, select **Operation Settings**.

2. On the **General** page, set the **Display additional error information** option:

   ◆ Yes – the more detailed technical error information is available.

   ◆ No – only basic error information is available.

Note: If you set this option to Yes, it affects all error messages across the implementation.

31.4 System security

If you see a logon message similar to:

```
The system is not configured for production use – please contact your
administrator.
```

you must review the settings on the **Device Security** tab on the **Security Settings** workflow; see section *34.3*, *Device Security page (Security Settings)*.

When attempting to issue a card, you may also see a message similar to the following:

```
System is not set up to issue this card
```

This is because MyID is not configured to issue this type of card in accordance with the security requirements on the **Device Security** tab.

The **System Events** report may include further information about the system security. The following codes appear in the report:

▪ `s` – MyID is not correctly configured to swap the SOPIN to a randomized value at issuance.

▪ `G` – MyID is not correctly configured to swap the GlobalPlatform key to a customer value at issuance.

▪ `P` – MyID is not correctly configured to swap the PIV9B key to a customer value at issuance.

The ***System Security Checklist*** document contains information about configuring SOPINs, GlobalPlatform keys, and PIV9B keys to ensure that your system is secure and configured for production use.

For further information on these system security messages, contact customer support quoting reference SUP-273.

32 Additional Identities

MyID allows you to set up additional identities from your LDAP on a user account. These additional identities allow you to add extra certificates to smart cards.

For example, you may require a certificate belonging to a separate user account that is used for server administration, which therefore has different logon credentials from your main employee account.

32.1 Overview

The process is as follows:

1. Set up one or more certificate policies for additional identities.

2. Set up one or more credential profiles that allow additional identities.

3. Add up to three additional identities from the LDAP to a user, specifying which additional identity certificate to use for each identity.

4. Request a card for the user using an additional identity credential profile.

5. Issue a card to the user – this card will contain, in addition to the standard certificates tied to the user's account, a certificate for each of the additional identities.

32.2 Setting up additional identities

To allow MyID to issue additional identities, you must set up the following:

- On the certificate authority, set up each certificate policy you want to use for additional identities to have the **Subject Name** set to **Supply in the Request**.

- In the **Certificate Authorities** workflow, for each certificate policy you want to use for additional identities:
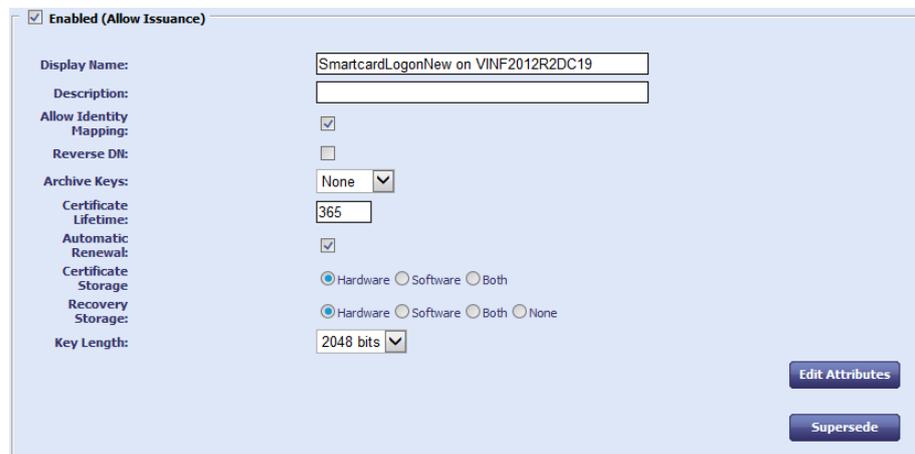
- Set the **Allow Identity Mapping** option on the certificate policy.

- Make sure the **Archive Keys** option is set to **None**.

- Click the **Edit Attributes** button:

  If the **Edit Attributes** button does not appear, you must run the following stored procedure in the MyID database:

  - `sp_SetMSCertExtensions`

  Set the **UserPrincipalName** and **Email** mappings to be dynamically mapped to the **User Principal Name** and **Email** user attributes.

- In the **Credential Profiles** workflow, edit the credential profile that you want to use to issue additional identities; in the **Issuance Settings** section, set the **Issue Additional Identities** option.

You can set the **Issue Additional Identities** option for credential profiles that have their card encoding option set to **Contact Chip** or **Microsoft Virtual Smart Cards**.

In the list of certificates, *do not* select the additional identity policies – these certificates are automatically added to the card if you have selected the **Issue Additional Identities** option and set up an additional identity for the cardholder.

32.3 Adding additional identities

You can use the **Manage Additional Identities** workflow to add up to three new identities (for example, accounts from other areas of the LDAP directory) and certificates that can then be included on the user's smart card.

If you have specified any additional identities for a user, when you issue a device to that user, new certificates based on the specified policies are requested from the appropriate certificate authority and written to the device.

To select additional identities:

1. From the **People** category, select **Manage Additional Identities**.

2. Use the Find Person stage to search for the user for whom you want to add additional identities.

3. Click the **Additional Identities** tab.
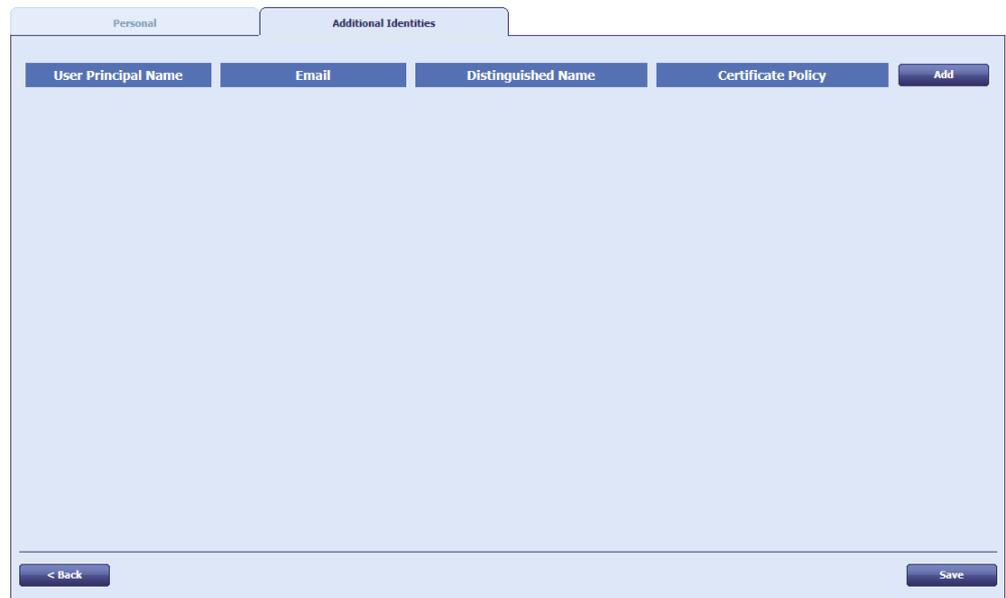
You can select up to three additional identities for the user.

4. For each additional identity:

   a) Click **Add**.
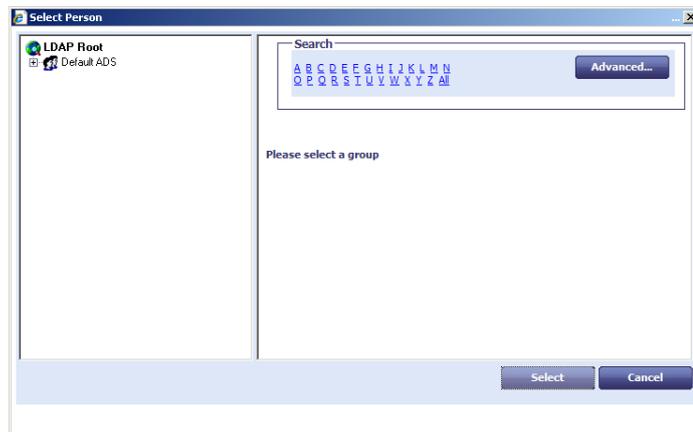
   The available entries in the directory are restricted to the Organizational Unit of the operator and below.

   b) Use the LDAP browser to select the directory account for the user.

   c) Select the required branch of the LDAP directory.

d) Select the initial letter of the person, click **All** to view all the people in the group, or filter the list:

    i   Click the **Advanced** button.

    ii   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.

    iii   Click **Search**.

e) Select the appropriate person.

f) Click **Select**.
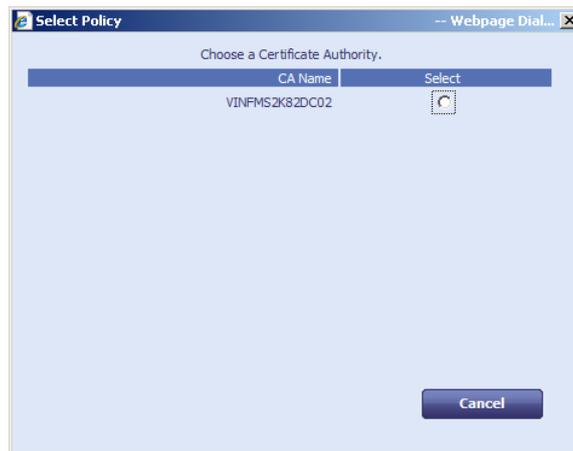
g) If you have more than one certificate authority set up for additional identity certificate policies, select the certificate authority you want to use.

h) Select the additional identity policy from the CA you want to use, then click **OK**.

5. Click **Save**.

32.4 Removing additional identities

To remove an additional identity:

1. From the **People** category, select **Manage Additional Identities**.

2. Use the Find Person stage to search for the user for whom you want to change additional identities.

3. Click the **Additional Identities** tab.
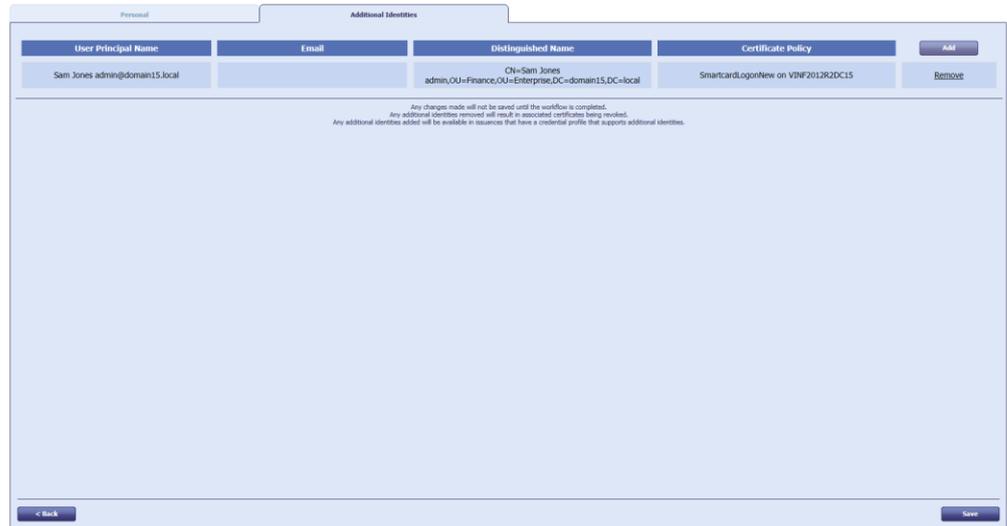
4. For the additional identity you want to delete, click **Remove**.

5. Click **Save**.

   The certificates for any identities that you have removed are now revoked.

32.5 Adding an additional identity for your own account

You can use the **Manage My Additional Identities** workflow to add or remove additional identities for your own account.

This workflow operates in the same was as the **Manage Additional Identities**, with the exception that you do not need to select a user using the Find Person stage; also, if your user account was imported from a directory, MyID displays a list of the users in the directory who have User Principal Names similar to your own account details.
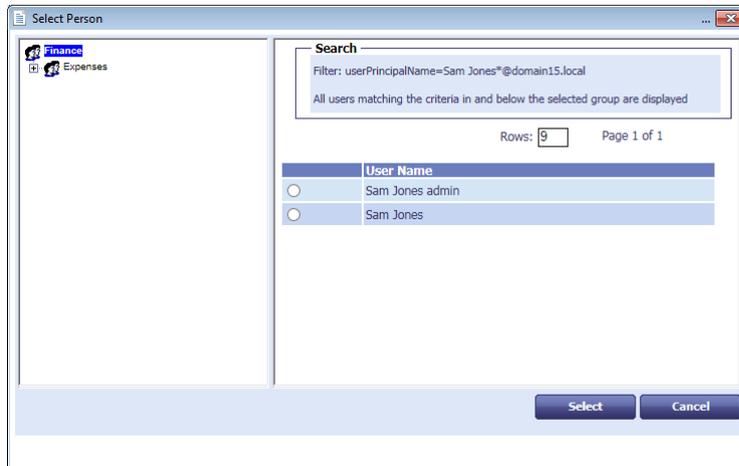
Note: You must have the appropriate scope to view the additional identities; for example, if you have a scope of Self, you will be able to see only your own record.

If this filtering does not meet your requirements, contact Intercede customer support, quoting reference SUP-184.

32.6 Known issues

- **IKB-71 – Cannot renew an additional identity certificate**

  Currently, you cannot renew certificates used for additional identities. Make sure that you do not set the certificates for automatic renewal; any certificates that are configured for automatic renewal will be issued to the primary identity, not the additional identity.

- **IKB-76 – Additional identities not supported on PIV or CIV systems**

  Additional identities are not supported on MyID PIV systems, or MyID systems with the CIV module installed.

33 Configuration – Operation Settings

The **Operation Settings** workflow is in the **Configuration** category. Many of the standard configuration settings can be modified using these pages. Each of the sections in this chapter refers to a page within the workflow.

33.1 Making configuration changes

When you make configuration changes, you must ensure that only one client machine at a time is making any changes to the settings. When you have saved your changes, all clients must close and restart their clients to pick up the changes.

To set the operation settings:

1. From the **Configuration** category, select **Operation Settings**.

2. Complete the form as appropriate.

3. Select **Save changes** to save the changes you have made or **Cancel** to cancel the workflow.

33.1.1 Changing the operation settings

The **Operation Settings** workflow is divided into tabs containing related configuration options. Click the tab to display the options.

Configuration options may be one of the following:

- ✅ – Yes

- ❌ – No

- ❓ – Ask

- a value; for example, the location of a server or a time limit.

Click the Yes/No/Ask image to cycle through the possible options.

To reset the settings, click **Revert to Saved**.

33.2 General page (Operation Settings)

Setting	Default value	Description	Further information
Archive People Data	No	Keeps a copy of users deleted from the main database. These deleted user accounts are stored in the PeopleArchive table in the database.	
Automatically Expire Web Pages	Yes	Whether web pages are to expire immediately, preventing use of the back button.	
Constrain screen on startup	No	Set this to constrain the screen size to 1024x768 on startup.	Does not affect MyID Desktop.
Display additional error information	Yes	Shows extended error details button if an error is displayed to an operator.	See section *31, Troubleshooting*
Display pending card requests	Yes	Whether pending card requests are displayed on the **Devices** tab in **Person Details**.	
Effective Revocation Immediate	Yes	Whether a certificate is revoked when the CA receives the request, or when the operator revoked the certificate in MyID.	See the *Microsoft Windows CA Integration Guide* for details.
Group Deletion Enabled	Yes	Whether groups can be deleted using the **Edit Groups** workflow.	Cannot be edited.
Maximum certificate server restart log entries	24	Set this to the maximum number of log entries for certificate service failures in the past 24 hours. For example, set this option to 10; if a failure and restart occurs, and ten logs of this error have already been recorded within in the past 24 hours (across all instances of the certificate service running against the same database), the new failure is not recorded. If nine or fewer log entries have been recorded in the previous 24 hours, the certificate service creates a new log entry.	
Maximum person search results	100	Maximum search results to return when searching for people before block paging takes place in certain workflows. Less than 200 is recommended.	
One Click Selection in Find Person	Yes	Whether you have to click a button after selecting a person in the **Find Person** screen.	

Setting	Default value	Description	Further information
Printers have External Prox Readers	No	Set this option to Yes to 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.	See section *27.2.5*, *Printers have external readers*.
Show duplicate person warning	Yes	Whether MyID warns you when you attempt to add a person who has the same name as an existing person in the MyID database. PIV only.	
SMS email notifications	No	Used for mobile identities.	See the *Mobile Identity Management Installation and Configuration* document for details.
SMS gateway URL for notifications		Used for mobile identities.	See the *Mobile Identity Management Installation and Configuration* document for details.
Temporary Credential Profile Name		Used for temporary cards issued by the Self-Service Kiosk.	See the *Self-Service Kiosk Installation and Configuration* document for details.
URL Path		Used for bureau operations to provide the location of the MyID website.	See the *Bureau Integration Guide* for details.
Web Server External Address		If you are experiencing problems with QR code generation for mobile issuance, set this option to the URL of the MyID web services server that hosts the ProcessDriver web service. Make sure this URL is accessible to your MyID clients.	See the *Mobile Identity Management Installation and Configuration* document for details.
Workflow Timeout Warning Delay	2	This is the time, in minutes, that the user is warned before a session timeout. If the option is set to 0, no warning is issued. The default is 2 minutes. The session timeout is dictated by the **Task number timeout** option on the **Process** tab in the **Security Settings** workflow.	

33.3 Devices page (Operation Settings)

Setting	Default value	Description	Further information
Allow Card Activation	Yes	Allows you to issue cards with their keys locked so users must activate them before use.	
Allow card serial number to be entered during Request Card workflow	No	Allows you to search for cards with specific serial numbers when requesting a card. You can use * and ? as wildcards when searching. Any unassigned devices, or devices with unrestricted cancelation, that match the search criteria are displayed. The limit is 10 records; if more than 10 devices match the search criteria, you must search again with more restrictive criteria.	See section *27.2.2*, *Requesting a card*.
Allow device management from the MyID user interface	No	If set to Yes, you can search for computers or other devices registered in MyID during some operations.	
Allow disposal of expired devices	Yes	If set to Yes, allows you to dispose of devices that have expired but not been cancelled.	See section *27.12*, *Disposing of cards* for details.
Allow virtual smart card creation with TPM reduced functionality	No	Set to Yes to allow Microsoft Virtual Smart card to be issued within MyID when the TPM is in reduced functionality state.	See the ***Microsoft Virtual Smart Card Integration Guide*** for details.
Auth Code Scope	Both	Whether Auth Codes, when required, affect Activate, Unlock or both workflows.	
Card activation expiration period	30	The number of days after which card activation jobs that have not been collected will expire.	
Card label	Yes	Allows a label to be written to a card.	

Setting	Default value	Description	Further information
Card Renewal Period	42	You can configure the length of time before expiry that you can request a card renewal using the **Request Replacement Card** workflow. For example, if the card has 60 days left before expiry, and you set the Card Renewal Period to 40, you cannot request a card renewal. If the card has 30 days left before expiry and you set the Card Renewal Period to 40, MyID allows you to request the card renewal.	
Check Content Signing Certificate Expiration	Yes	MyID checks that the PIV content signing certificate will not expire in the lifetime of the card.	
Credential Number Per Device		Identifies the field holding the credential number; this is used at card issuance. PIV only.	See the *PIV Integration Guide* for details.
Default Card Data Model	PivDataModel.xml	Sets the default data model to be used in a credential profile. The data model defines how the card is personalized.	In PIV systems, this is used to ensure the correct card personalization is done for FIPS-201.
Default Card Reverse Layout		If a card has no defined reverse layout, if this configuration option contains the name of a valid card layout, the layout is used for the reverse of the card.	
Deliver Card Before Activation	No	Set this to Yes to add a Delivery stage to the process for issuing a card, ensuring the card has been delivered to the recipient before it is activated.	See section *27.3*, *Delivering cards* for details.
Enable credentials when person is enabled	Yes	If set to Yes, enabling a user account in MyID automatically enables all issued but disabled credentials belonging to that user account.	
Enable Intel Virtual Smart Card support	No	Allows you to use MyID to manage Intel Virtual Smart Cards.	See the *Intel Virtual Smart Card Integration Guide* for details.

Setting	Default value	Description	Further information
Expiration Identity Batch	20	MyID updates the directory to remove the device certificate information when a device identity is cancelled or the certificate expires. This option configures the size of batches of records that are processed when updating the directory. You should not have to change this value.	
Issue MyID Signing Keys	Ask	Whether the option to use MyID management keys for logon is displayed in Services when designing a credential profile: **Ask** – option available for selection **No** – option not available and MyID keys not used for logon **Yes** – option not available and MyID keys are used for logon	See section *12.3.1, Credential profile options*.
Legacy virtual smart card fallback	No	For Windows 7, to support creating VSCs using the TPM-5.1.x client, set this option to `Yes`.	See the ***Microsoft Virtual Smart Card Integration Guide*** for details.
Microsoft virtual smart cards supported within MyID	No	Set to Yes to allow the use of Microsoft Virtual Smart Cards within MyID.	See the ***Microsoft Virtual Smart Card Integration Guide*** for details.
Mobile Provision Via Email	Yes		
Mobile Provision Via SMS	Yes		
MyID virtual smart card detection retry attempts	6	The number of attempts MyID will make to detect a VSC.	See the ***Microsoft Virtual Smart Card Integration Guide*** for details.
MyID virtual smart card detection retry interval	10	The number of seconds between retry attempts.	See the ***Microsoft Virtual Smart Card Integration Guide*** for details.
One Active Job Per Person	Yes	When set to Yes, the **Request Replacement Card** workflow cancels existing Issue Card, Update Card and Request Replacement Card jobs that exist for the applicant who is to be issued a replacement card.	
One Credential Profile Request Per Person	No	Setting this option limits the number of card requests to one per person per credential profile. The most recently created request job will take precedence.	

Setting	Default value	Description	Further information
Persist terms and conditions	No	When set to Yes, stores the terms and conditions that were signed as a binary object in the MyID database. This is then visible in the MyID audit report. This 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.	See section *12.6*, *Customizing terms and conditions*.
PIV Biometric Maximum Age	12	Set to the maximum age of the biometric data in years. MyID checks that the biometrics will not exceed this age in the lifetime of the card.	
PIV Facial Biometrics Required	Yes	When set to Yes, MyID checks that facial biometrics have been captured before authorizing card issuance.	
Preserve FASCN and UUID for card update	Yes	Set to Yes to prevent the FASC-N and UUID from being changed, or No to generate new FASC-N and UUID values during card repersonalization and reinstatement. PIV only.	Repersonalization and reinstatement are not currently supported.
Print Quality Confirmation	No	If set to Yes, allows the operator to confirm whether the card was printed correctly, and to offer an opportunity to retry the operation.	See section *27.2.4*, *Collecting a card*.
Secondary Serial Number		A series of field names separated by spaces which are used as a second serial number.	
Serial Number IIN	0123456789	Used to set the serial numbers for Oberthur PIV cards.	See the **Smart Card Integration Guide** for details.

Setting	Default value	Description	Further information
Terms and Conditions During Device Update	Just for New Certificates	Determines whether users have to sign the terms and conditions when updating cards that have credential profiles that require them to sign the terms and conditions when activating their cards. If the card is being updated to a new credential profile, MyID checks the **Terms and Conditions** setting of the *new* credential profile. Can be one of the following: **Yes** – users are required to sign the Terms and Conditions as required by the credential profile when collecting any kind of update for their card. **Just for New Certificates** – users are required to sign the Terms and Conditions as required by the credential profile only when the update they are collecting contains new certificates. **No** – users do not need to sign the Terms and Conditions when collecting card updates.	See section *12.3.1*, *Credential profile options*.
Token resync window	100	The window to be used when resynchronizing an OTP device. The larger the value, the longer the resync window.	If you are having difficulty resynchronizing tokens, increase this value.
Unblocking Credential	No	Whether this installation supports unblocking credentials.	See the *Smart Card Integration Guide* for details.

33.4   LDAP page (Operation Settings)

Setting	Default value	Description	Further information
Allow duplicate DN	Yes	Whether a user can be added if another user with the same DN already exists.	
Allow LDAP Search for devices during Add Devices	No	Set to Yes to allow an operator to add a device from the LDAP directory into the MyID database using the **Add Device** workflow.	

Setting	Default value	Description	Further information
Allow LDAP Search for devices during card requests	No	Set to Yes to allow an operator to add a device from the LDAP Directory into the MyID database when requesting a card.	
Automatically create MyID groups from the Organizational Unit of imported users	Yes No – in PIV systems	If you are using MyID as your primary data source, set this to Yes to automatically create MyID groups with the same names as the organizational units in the LDAP directory when importing users. **Note:** If you set this option to No, then move a user in the LDAP to an OU that does not have a corresponding MyID group, MyID displays a warning that the directory and the MyID database are no longer synchronized when you view the user's details in MyID.	
Background Update	No	When a record is accessed, MyID automatically checks the directory for any changes to an individual's details, and updates the information held in MyID.	
Create OU Chain	No	Whether the containers in the DN of a user account pushed to an LDAP directory will be created if they do not already exist.	Cannot be edited.
Custom LDAP mappings	No	Set to `Yes` before you upgrade your system if you want to prevent the installation program from overwriting any custom LDAP mappings.	See the *Installation and Configuration Guide* for details.
Disable on removal from directory	Yes No – in PIV systems.	Whether user accounts imported from a directory should be disabled if an attempt is made to synchronize the directory with MyID but the user no longer exists in the directory (whether because the directory has been updated independently, or with the Active Directory Deletion Tool). Historic information is retained but you cannot issue devices to this person. This option also determines whether user accounts imported from a directory should be disabled if the user has been *disabled* in the directory.	

Setting	Default value	Description	Further information
Edit Directory Information	No Yes – in PIV systems.	Whether the user is allowed to edit person data retrieved from the directory when **Update user information in the directory** is not enabled. Changes are stored in the MyID database and may be overwritten with information from the directory if MyID synchronizes with it.	
Edit DN	No	Whether the DN for a person can be manually edited.	
Enable ADS Fields	Yes No – in PIV systems.	Whether to display UPN and SAM account name fields during **Add Person** and **Edit Person**.	
Force NETBIOS name	No	Store the user's NETBIOS name instead of the DNS name. If you change this to Yes, we recommend you set the Background Update option to Yes to allow existing user accounts to be updated. When you import someone from an LDAP directory, the DNS-style domain name is shown in the Domain field on the Account tab. When you save the record, the domain name is converted to the NETBIOS-style name.	See section *5.6*, *Storing the NETBIOS name for a person*.
LDAP update cancel card		Used for LDAP updates.	For more information, contact customer support, quoting reference SUP-227.
LDAP update enable card		Used for LDAP updates.	For more information, contact customer support, quoting reference SUP-227.
LDAP update newissue card		Used for LDAP updates.	For more information, contact customer support, quoting reference SUP-227.
LDAP update permreplaceissue card		Used for LDAP updates.	For more information, contact customer support, quoting reference SUP-227.

Setting	Default value	Description	Further information
LDAP update search attribute		Used for LDAP updates.	For more information, contact customer support, quoting reference SUP-227.
LDAP update tempreplaceissue card		Used for LDAP updates.	For more information, contact customer support, quoting reference SUP-227.
Link to LDAP Groups	No	Allows you to link user roles to groups in the LDAP.	
Revoke certificates if user is removed or disabled following background directory update	Yes	Whether active certificates for a user are revoked or disabled if an attempt is made to synchronize the directory with MyID but the user no longer exists in the directory. MyID revokes certificates if the user is removed from the directory, and suspends certificates if the user is disabled in the directory.	See also section *5.5*, *The Batch Directory Synchronization Tool*.
Search a Directory	No Ask – in PIV systems.	Whether MyID or an LDAP directory are to be searched when looking for a person. ▪ Yes – restrict the search to the directory ▪ No – restrict the search to MyID ▪ Ask – the person entering the search criteria can choose where to search	
Display person details during confirm job	No	If set to Yes, displays an additional tab on the job confirmation screen of the **Collect Card** workflow.	
Skip Person Confirmation screen	Yes	Whether to skip the **Person Details** stage when finding a person. This stage provides further details but is not needed in your environment if sufficient information is shown in the list of potential matches.	
Track Entrust DN Changes	No	Determines whether MyID updates Entrust with changes to the DN.	See the *Entrust CA Integration Guide* for details.
Update exception groups		Used for LDAP updates.	For more information, contact customer support, quoting reference SUP-227.

Setting	Default value	Description	Further information
Update group information in the directory	No	Controls whether group details are pushed back to the directory when changes are made in MyID. **Note:** If this is set to No and **Background Update** is set to Yes, any changes may be overwritten if the directory has not been updated.	
Update user information in the directory	No	Controls whether user details are pushed back to the directory when changes are made in MyID. **Note:** If this is set to No and **Background Update** is set to Yes, any changes may be overwritten if the directory has not been updated.	

33.5 Video page (Operation Settings)

Setting	Default value	Description	Further information
File Store Location		The folder used to store images, mapped to the `upimages` virtual directory.	See section *16.1.1*, *General settings*.
HTTP Port for image upload	80	The port to be used when uploading images using HTTP.	See section *16.1.1*, *General settings*.
HTTPS Port for image upload	443	The port to be used when uploading images using HTTPS.	See section *16.1.1*, *General settings*.
Image Capture	Yes	Whether image capture is to be used.	See section *16.1.1*, *General settings*.
Image Crop Height	0	The height of captured images. PIV only.	
Image Crop Width	0	The width of captured images. PIV only.	
Image Upload Server		The name of the server to which images are uploaded. Used for upgraded systems that do not store images in the database. Also used for images used in the **Card Layout Editor**.	See section *16.3*, *Storing images on the web server* and section *9.2*, *Configuring the image location*.

Setting	Default value	Description	Further information
JPEG Compression Ratio	90	The compression ratio to use for any JPEG images.	See section *16.1.1*, *General settings*.
Maintain Aspect Ratio	Yes	Whether aspect ratio is to be retained when resizing images.	See section *16.1.1*, *General settings*.
Maximum Image Height	0	The maximum height of an image to be displayed in the image capture control.	See section *16.1.1*, *General settings*.
Maximum Image Width	0	The maximum width of an image to be displayed in the image capture control.	See section *16.1.1*, *General settings*.
Maximum Number Of Sub-Folders	0	The maximum number of sub-folders to be used when storing images.	See section *16.3*, *Storing images on the web server*.
Preload Images	No	Whether images are to be pre-loaded.	This option is not applicable if you are storing images as binary objects in the database. See section *16.1.1*, *General settings*.
Use SSL for Image Capture	Ask	Whether SSL is to be used for image capture. Used only for HTTP PUT.	
Validate Image Size	No	Whether the size of the image is to be validated by the server.	See section *16.3*, *Storing images on the web server*.
Video Capture	No Yes – in PIV.	Whether video (webcam) is to be used for capturing images.	See section *16.1.1*, *General settings*.

33.6   Certificates page (Operation Settings)

Setting	Default value	Description	Further information
Abort On Timeout?	Ask	Whether the issue process should be canceled if the certificate is taking so long to process that the timeout period is reached.	
Allow Collect Later?	Yes No – in PIV systems.	Whether a device holder can collect a certificate later if the certificate is taking a long time to issue.	
Automated Issuance Time Limit	45	The time to wait for a certificate to be issued when using an automated issuing process.	

Setting	Default value	Description	Further information
Cards Allowed for Derivation		A regular expression matching the ASCII value of the FASC-N for cards to determine whether you can use them to create derived credentials.	See the ***Derived Credentials Installation and Configuration Guide*** for details.
Certificate Polling Refresh Time	5	The number of seconds between subsequent attempts to collect certificates.	
Certificate Recovery Password Complexity	04-08N	Controls the complexity of the password automatically generated for PFX files. It takes the format `mm-nnULSN`. `Mm` = min length `nn` = max length `U/u` = must/may contain upper case (optional) `L/l` = must/may contain lower case (optional) `S/s` = must/may contain symbols (optional) `N/n` = must/may contain numbers (optional)	
Certificate Refresh Threshold	15	The number of seconds to wait for a certificate to be issued before deferring issue or canceling process. If you experience problems when collecting or updating cards, try increasing this option to a higher value; for example, `45`. This problem may manifest with an error similar to: `One of the certificates that have been requested for you has failed to issue.`	
Certificate Renewal Period	56	The number of days before certificate expiry that a new one can be requested.	
Certificate Timeout For Deferred Collection	4320	The number of minutes that a certificate will remain valid while waiting for collection. When this limit is reached, the certificate is revoked.	
Certificate Timeout For Issuance	20	The number of minutes that a certificate will remain valid while waiting to be issued. When this limit is reached, the certificate is revoked.	

Setting	Default value	Description	Further information
Derived credential certificate OID	2.16.840.1.101.3.2.1.3.13	The OID to be checked on the PIV Authentication certificate for derived credentials.	See the *Derived Credentials Installation and Configuration* document for details.
Derived credential signing certificate OID	2.16.840.1.101.3.2.1.3.6; 2.16.840.1.101.3.2.1.3.7; 2.16.840.1.101.3.2.1.3.16	A semicolon-delimited list of OIDs to be checked on the Digital Signature certificate for derived credentials.	See the *Derived Credentials Installation and Configuration* document for details.
Derived credential revocation check offset	7	The number of days after which MyID checks the original credentials that the cardholder used to request the derived credentials. If the original credentials have been revoked in this period, the derived credentials are also revoked.	See the *Derived Credentials Installation and Configuration* document for details.
Mask Certificate Revocation Code	No	Whether certificate revocation reasons are sent to the CA. (**Yes** means they are not sent.)	Cannot be edited.
Maximum certificate suspensions	-1	The number of times a certificate can be suspended before it is revoked. (**-1** means unlimited)	
Maximum keys per card to recover	0	Specifies the number of certificates to recover per card when creating key recovery jobs.	Not currently used.
Mobile Certificate Recovery Service URL		Specify the URL of the host that a mobile device must use to collect a mobile ID.	
Restrict certificate lifetimes to the card	Yes	Whether the lifetimes of the certificates are restricted to the lifetime of the card. This may not be supported by all certificate authorities.	
Retry On Collection?	No	If a certificate timeout period has been reached, must the request be resubmitted to the CA before the certificate can be collected.	
Revoke replaced certificate	No	Whether certificates that are being replaced during a card update are revoked.	

Setting	Default value	Description	Further information
Storage method allowed for certificate recovery	Both	Allows you to restrict the certificates recovered depending on the recovery method configured by the certificate profile. Can be one of the following: Local Store Save to PFX Both	
Suspend to revoke period	0	The time between suspension and revocation.	

33.7　　　Import & Export page (Operation Settings)

Setting	Default value	Description	Further information
Application Form Names			
Application Forms Folder			
File Export Directory		The folder on the application server in which files for export are created.	
File Import Directory		The folder on the application server in which files for import are placed.	**Note:** Changes to this setting do not take effect until you have restarted the eDB Data Import Server service.
Migrated Certificate Credential Profile		Type the name of the credential profile to be used for certificates imported against a 'dummy' device.	
Migrated Device Credential Profile		Type the name of the credential profile to be used as the default for devices imported through the Lifecycle API that do not specify a profile in the input data	
Migrated Encryption Certificate Policy		Type the name of a certificate policy to be used as the associated policy for imported archived certificates.	
Migrated Non-archived Certificate Policy		Type the name of a certificate policy to be used as the associated policy for imported non-archived certificates.	

33.8 Identity Checks page (Operation Settings)

Setting	Default value	Description	Further information
Applicants Re-Approve for Card Renewal	Yes	Set to Yes to require re enrollment for card renewals, or No to allow renewals without re enrollment. PIV only.	
Applicants Re-Enroll for Card Replacement	Yes	Set to Yes to require re-enrollment for card replacements, or No to allow replacements without re-enrollment. PIV only.	See the *PIV Integration Guide* for details.

The **Identity Checks** page also contains different settings based on whether you have any adjudication systems set up. See your integration guides for details.

33.9 Bureau & Job page (Operation Settings)

Setting	Default value	Description	Further information
Automatic cancellation timeout	0	Time in days after which issue card and update card jobs are cancelled automatically.	**Note:** This feature requires additional updates. For more information, contact customer support quoting reference SUP-272.
Automatic job cancellation credential profile filter		String that must be present in the credential profile name for jobs to be cancelled. Leave blank to cancel all jobs.	**Note:** This feature requires additional updates. For more information, contact customer support quoting reference SUP-272.
Automatic job cancellation email	113	ID of the email template sent to the target of the cancelled job. Leave blank to prevent email messages from being sent when jobs are cancelled. The default is the Automatic Job Cancellation Email template, with ID 113.	**Note:** This feature requires additional updates. For more information, contact customer support quoting reference SUP-272.
Cancel Outstanding Updates	Yes	Determines how duplicate update requests for the same device are handled.	
Job batch maximum size	0	Controls the maximum number of jobs in a batch. The bureau job batch utility produces multiple batches, where the maximum number of jobs in a batch equals this setting. Set the value to 0 for no limit on job batch size.	
Show Extended Job Details for Target	No	Controls whether to display additional information about the target in the job details window.	

33.10 Biometrics page (Operation Settings)

Note: The biometric options listed are dependent on having the MyID BioPack installed. This module is automatically installed with the PIV edition of MyID.

Setting	Default value	Description	Further information
Allow Biometric PIN Reset	Yes	Allows the user to log on with biometrics to complete a PIN reset. PIV only.	See section *27.7.5*, *Self-service PIN reset authentication*.
Aware Preface control allowed to capture non-compliant images?	No	Allows the Preface control to capture non-compliant images. PIV only.	For information on using Aware PreFace, contact customer support, quoting reference SUP-228.
Aware Preface Custom Profile (ISO Token)		Aware custom profile. PIV only.	For information on using Aware PreFace, contact customer support, quoting reference SUP-228.
Aware Preface Custom Profile (PIV Authentication)		Aware custom profile. PIV only.	For information on using Aware PreFace, contact customer support, quoting reference SUP-228.
Aware Preface Custom Profile (PIV Card)		Aware custom profile. PIV only.	For information on using Aware PreFace, contact customer support, quoting reference SUP-228.
Biometric matching library	Precise	Select the biometric matching library to be used. PIV only.	See the integration guide for your fingerprint readers.
Biometric matching threshold	50	Threshold of confidence of matching prints, 0-100. PIV only.	See the integration guide for your fingerprint readers.
BioSensitivity for Precise Biometrics	10000	Setting for Precise biometric readers. Must be in the range 250 to 2,500,000. PIV only.	See the *Precise Biometrics Integration Guide* for details.
BioSensitivity for U.are.U Biometrics	10000	The BioSensitivity value refers to the failure rate of mismatches for U.are.U biometric readers. Must be in the range 250 to 2,500,000.	See the *U.are.U Integration Guide* for details.

Setting	Default value	Description	Further information
Bypass fingerprint verification when no fingerprints enrolled?	No	Whether the cardholder can bypass fingerprint verification if there are no fingerprints available for the cardholder in the MyID database. PIV only.	See the integration guide for your fingerprint readers.
Capture threshold for U.are.U Biometrics	60	Threshold of acceptable of a captured fingerprint image. For PIV, a minimum of 60 is required, which maps to an NFIQ value of 3. Valid values are 20, 40, 60, 80, and 100, which map to NFIQ values 5, 4, 3, 2, and 1.	See the **U.are.U Integration Guide** for details.
Enable additional authentication options	No Yes – in PIV systems.	Allows the configuration of additional options in the **Credential Profiles** workflow.	See section *12.3.2*, *Additional credential profile options* for details.
Enable Facial Capture	No	Whether biometric facial capture is enabled for MyID.	See your facial capture system integration guide.
Fingerprint enrolment device	Precise 250 MC	Which fingerprint reader to use. PIV only.	See the integration guide for your fingerprint readers.
Number of fingerprint validation attempts		Number of attempts the cardholder can make when attempting to validate fingerprints. PIV only.	See the integration guide for your fingerprint readers.
Require fingerprints for derived credentials	Yes	If set to Yes, fingerprint authentication is required to collect derived credentials. PIV only.	See the **Derived Credentials Installation and Configuration** document for details.
SecuGen fingerprint reader brightness	0	Brightness for SecuGen fingerprint readers. PIV only.	See the **SecuGen Integration Guide** for details.
SecuGen minimum capture quality	50	Capture quality for SecuGen fingerprint readers. PIV only.	See the **SecuGen Integration Guide** for details.
Verify fingerprints during card creation	Yes	Controls when fingerprints are required. PIV only – requires a data model that writes fingerprints to the card. For example, the PIV data models are suitable, but the CIV data models are not.	See the **PIV Integration Guide** for details.

Setting	Default value	Description	Further information
Verify fingerprints during card unlock	Yes	Controls when fingerprints are required. PIV only.	See the **PIV Integration Guide** for details.
Verify fingerprints during card update	No	Controls when fingerprints are required. PIV only.	See the **PIV Integration Guide** for details.

33.11   Issuance Processes page (Operation Settings)

Setting	Default value	Description	Further information
Active credential profiles per person	One per credential group	This option allows you to control issuance of different types of credentials to users; for example, you might want to issue one smart card, one USB token, and so on.	See section *12.3.2*, *Additional credential profile options*.
Allow parent and child credential profiles	No	Used for VSCs.	See the **Microsoft Virtual Smart Card Integration Guide**.
App Download URL – ANDROID		The URL for the Android version of the MyID Identity Agent. Leave blank to hide this option. The URL is embedded into the QR code that is displayed to the user and allows them to download the Identity Agent app when using the Self-Service Kiosk to collect Derived Credentials.	See the **Derived Credentials Installation and Configuration Guide**.
App Download URL – BLACKBERRY		Deprecated. BlackBerry is no longer a supported mobile operating system. For more information contact customer support quoting reference SUP-49.	
App Download URL – IOS		The URL for the iOS version of the MyID Identity Agent. Leave blank to hide this option. The URL is embedded into the QR code that is displayed to the user and allows them to download the Identity Agent app when using the Self-Service Kiosk to collect Derived Credentials.	See the **Derived Credentials Installation and Configuration Guide**.

Setting	Default value	Description	Further information
App Download URL – WINDOWS		Deprecated. Windows Phone is no longer a supported mobile operating system. For more information contact customer support quoting reference SUP-49.	
Automated Card Issuance Time Limit	240	The time (in seconds) to be spent attempting to issue a card before canceling the process.	
Automated Detect Card Time Limit	40	The time (in seconds) to be spent attempting to detect a card before it is rejected.	
Automated Remove Card Time Limit	30	The time (in seconds) that MyID will wait before allowing another print command to be sent once the card has been removed from the printer.	
Automatic Completion of Issuance	Ask	Enable the automatic submission of the Print Card stage.	
Automatic Completion of Issuance Timeout	300	Timer value (in seconds) for automatically submitting certain forms.	
Automatic Update Collection	;2,245;2,255 2,245 in PIV	If a user logs in with pending jobs, run the first workflow listed that they have access to. Workflows should be listed as `option,operationid;option,operationid` and so on. For example: `2,245` – this automatically launches the **Activate Card** workflow.	
Batch Encode Card Timeout	15	The number of seconds to allow a card to be read before timing out in the **Batch Encode Card** workflow.	
Display credential profile details	Ask	Whether credential profile details are displayed when a card is issued.	
Enable unrestricted cancelation	No	Controls whether the **Unrestricted Cancelation** option appears in the **Issuance Settings** section of the **Credential Profiles** workflow. This option allows you to re-use a card without first cancelling it.	
Manual Card Update	No	Whether a card update can be performed manually.	
Maximum multiple credential requests	1	This is the maximum number of multiple credential requests that will be accepted.	

Setting	Default value	Description	Further information
Maximum unvalidated multiple credential requests	1	The maximum number of multiple credential requests that will be accepted without secondary validation.	
Output Mechanism for Job Challenge Code Generation	Choose at request	Determines how the one-time password for job authentication is delivered. Choose one of the following: Email Display on screen Both Choose at request	See section *30.7*, *Requesting a device identity*.
Print Card Timeout	5	The number of seconds between printing a card and issuing.	
Printer Request Buffer Delay	10	This is the time in seconds to pause between sending requests to the printer.	Used with the Fargo SDK for Fargo printers.
Reload Device Profile	No	Whether the device profile is reloaded onto the card during issuance. Used for Gemalto cards. Not available in PIV systems.	
Requisite User Data	No	Displays an extra option in the **Credential Profiles** workflow that allows you to restrict issuance to user accounts with specific user attribute mappings.	See section *12.3.1*, *Credential profile options* for details.
Restrict collection of replacement devices if expiry date within (Days)	0	Stops the issuance of a replacement credential if the date for the expiry is within the specified number of days.	
Set expiry date at request	No	If set to Yes, the operator can specify a date for expiry of credentials when they are issued.	
Show the Card Content button in the Audit Workflow	Yes	Set to Yes to display the Card Content button on the Audit workflow.	

33.12 Notifications page (Operation Settings)

Setting	Default value	Description	Further information
Administration Email		Email address of the administrator to be sent email notification messages.	See section *14.1.5*, *Changing the recipient of administrator messages*
Database Mail Profile Name	Default CMS	The email address or profile name to be used as the sender of email notifications.	Required only for legacy systems still using SQL Server Database Mail. See the ***Installation and Configuration Guide*** for details.
Email separator	;	Allows you to specify the separator used to divide multiple email addresses when sending email messages.	See section *14.1.4*, *Email separator* for details.
Expiration Notification Period	28	The number of days before the date the card expires that MyID sends an email notification.	
Issuance Notification URL		If you set this to an URL, MyID posts a form detailing information in XML format about each card issuance carried out using the **Collect Card** or **Collect My Card** workflows. If the option is empty, no post is attempted.	
Mail Format	HTML	The format of SMTP email notification messages. This can be `TEXT` or `HTML`.	See section *14, Email Notification*.
Notification Proxy URL		No longer used.	
Send Email Notifications	No	Global setting to determine whether notification email messages are sent.	See section *14, Email Notification*.
Send Mobile OTP via SMS	No	Set this option to allow the operator to send the OTP authentication code directly to the mobile device.	May require an update to MyID to support mobile identities. See the ***Mobile Identity Management Installation and Configuration Guide***.
Single Email Notification	Yes	Allows you to specify whether users receive multiple email messages when several certificates are being renewed.	See section *14, Email Notification*.

33.13 Identity Agent Policy page (Operation Settings)

These settings relate to the mobile module and are available only on systems that have been configured for mobile issuance. See the ***Mobile Identity Management Installation and Configuration Guide*** and ***Derived Credentials Installation and Configuration Guide*** for more information.

Setting	Default value	Description	Further information
Administrator email address		Set this to the email address to which Identity Agent will send logs for troubleshooting purposes.	
Log level	Error	Set this to the level of logging you want Identity Agent to produce. Higher levels result in more detail, but larger files. Set to one of the following: `0 – NONE` `1 – FATAL` `2 – ERROR` `3 – WARNING` `4 – INFO` `5 – DEBUG` `6 – VERBOSE`	
Maximum log storage space	20	The maximum amount of space (in MB) that log files will take up on a device. Once this limit is reached, log files will be deleted automatically, oldest first, to clear room for new files.	
Maximum number of log files	-1	The maximum number of log files to be stored on a device. Once this limit is reached, log files will be deleted automatically, oldest first, to clear room for new files. To allow as many files as will fit in the maximum log storage space, set this value to `-1`.	
Maximum retry attempts	5	The maximum number of times Identity Agent should attempt to reconnect to the server if connection is lost during an operation.	

Setting	Default value	Description	Further information
Minimum retry delay	10	The minimum delay, in seconds, between each attempt to contact the server after connection has been lost.	

![intercede](intercede logo)

34 Configuration – Security Settings

The **Security Settings** workflow is in the **Configuration** category. Many of the standard configuration settings can be modified using these pages. Each of the sections in this chapter refers to a page within the workflow.

34.1 Making configuration changes

When you make configuration changes, you must ensure that only one client machine at a time is making any changes to the settings. When you have saved your changes, all clients must close and restart their clients to pick up the changes.

To set the security settings:

1. From the **Configuration** category, select **Security Settings**.

2. Complete the form as appropriate.

3. Select **Save changes** to save the changes you have made or **Cancel** to cancel the workflow.

34.1.1 Changing the security settings

The **Security Settings** workflow is divided into tabs containing related configuration options. Click the tab to display the options available.

Configuration options may be one of the following:

- ✅ – Yes

- ❌ – No

- ❓ – Ask

- a value; for example, the location of a server or a time limit.

Click on the Yes/No/Ask image to cycle through the possible options.

To reset the settings, click **Revert to Saved**.

34.2 Logon page (Security Settings)

Setting	Default value	Description	Further information
Allow Logon Codes	No	Enables logon codes. Used as a global setting for all credential profiles – to send logon codes, you must set this option to `Yes` and set the **Generate Logon Code** option in the credential profile.	See section *3.4*, *Logon codes* for details.
Client Signing	Yes (Software or Card if available)	Whether the information passed from the client to the server is signed using a key or certificate stored on the card that was used to log in. This provides extra security. You can choose to use encryption keys from your smart card, or to use a software encryption key generated when you log on.	
Complex Logon Code Complexity	12-12ULSN	The complexity rule used to generate a logon code when the **Generate Logon Code** option in the credential profile is set to **Complex**. It takes the format `mm-nnULSN`. `Mm` = min length `nn` = max length `U/u` = must/may contain upper case (optional) `L/l` = must/may contain lower case (optional) `S/s` = must/may contain symbols (optional) `N/n` = must/may contain numbers (optional)	See section *3.4*, *Logon codes* for details.
Logon Name Required	No	Whether the logon name associated with the MyID account is used in addition to the password when logging on to MyID.	No longer supported. Will appear only on upgraded systems, but has no effect.
Maximum Allowed OTP Failures	5	Specify the maximum number of failed attempts a user can make when attempting to answer an OTP challenge. When this number is exceeded, the OTP is rendered unusable, and the user must request a new OTP.	

Setting	Default value	Description	Further information
Maximum allowed security question failures	3	Specify the maximum number of failed attempts a user can make when attempting to answer a security question. When this number is exceeded, the user's account can be locked out – see the **Action on maximum invalid phrases** option.	**Note:** If this is set to 0, the default value of 3 is used and the user's account is locked when three attempts have been made without success.
Minimum Supported Client Components Upgrade Action	FORCE	Select the action if the client components do not meet the specified minimum level.	No longer supported in MyID Desktop. For more information, contact customer support, quoting reference SUP-219.
Minimum Supported Client Components Version		Type the minimum version of the client components that you want to be able to access MyID.	No longer supported in MyID Desktop. For more information, contact customer support, quoting reference SUP-219.
Preferred Client Components Version		Type the preferred version of the client components.	No longer supported in MyID Desktop. For more information, contact customer support, quoting reference SUP-219.
Preferred Client Components Version Upgrade Action	FORCE	Select the action if the client components are between the specified minimum version and the preferred version.	No longer supported in MyID Desktop. For more information, contact customer support, quoting reference SUP-219.
Prevent Direct Password Logon	No	Allow password logon for self-service operations only when a card is present.	
Set Security Phrase at Logon		If a user logs into the system and the required number of security phrases have not been set up, run the first workflow listed that the user has access to. Workflows should be listed as `option,operationid;option,operationid` and so on. For example, `1,110` – this automatically launches the **Change My Security Phrases** workflow.	See section *3.3.2*, *Setting the number of security phrases required to authenticate* for details. **Note:** The **Set Security Phrase at Logon** option is supported in MyID Desktop from MyID 10.6 Update 1 onwards – make sure you have upgraded your clients.

Setting	Default value	Description	Further information
Show Full Name at Logon	No	Controls whether the card owner's full name is displayed on the **Logon** page when their card is inserted. **Note:** If you set this option to `No`, and either you have the **Show Photo at Logon** set to `No`, or the users do not have photos attached to their user accounts, if you insert more than one card you will not be able to tell which card belongs to which user except by the card serial number and device type (which is available when you hover your mouse over the image).	
Show Photo at Logon	Yes	Whether the holder's photograph is displayed at logon.	
Signed Logon	Yes	Whether the information passed to the server during logon is signed using the keys or certificate stored on the card.	
Simple Logon Code Complexity	12-12N	The complexity rule used to generate a logon code when the **Generate Logon Code** option in the credential profile is set to **Simple**. It takes the format `mm-nnULSN`. `Mm` = min length `nn` = max length `U/u` = must/may contain upper case (optional) `L/l` = must/may contain lower case (optional) `S/s` = must/may contain symbols (optional) `N/n` = must/may contain numbers (optional)	See section *3.4*, *Logon codes* for details.

Setting	Default value	Description	Further information
Validate logon certificate	No	If you set this option to Yes, when a user logs on to MyID with a certificate, MyID validates the certificate by verifying that it has not expired and checking it against the certificate revocation list. If the validation fails, MyID prevents the user from logging on. In addition, if you have an external system that allows you to link to an authentication server for certificate validation, the authentication server is used to validate the certificate after MyID as secondary validation.	**Note:** The application server must trust the Certificate Authority that issued the certificate being validated.

34.3   Device Security page (Security Settings)

Setting	Default value	Description	Further information
Display warnings for unsecured issuance	Yes	Displays a warning on the login screen if the system is not securely configured and an attempt is made to issue credentials. If you want to run MyID with secure settings disabled (for example, for test or demonstration systems) contact customer support to discuss your requirements, quoting reference SUP-273.	Cannot be edited
Enable Customer GlobalPlatform Keys	Yes	Whether the installation supports Java applets. If you do not have this option set, you will be unable to write customer GlobalPlatform keys to your cards.	See section 8, *Applets*.
Require Random Security Officer PIN	Yes	If this is set to Yes but the Security Officer PIN Type is set to Factory, cards cannot be issued.	
Security Officer PIN Type	Random	Random – Generate a random SOPIN and set it on the card to be initialized (higher security). Factory – Leave the default SOPIN on the card (low security).	
Show all devices	No	When set to `No`, restricts the list of devices on this page to the smart cards known to support GlobalPlatform or PIV 9B keys. When set to `Yes`, displays all devices known to MyID.	

Note: You can also set the requirements for customer GlobalPlatform and PIV 9B keys for each device type supported by your system. If the option is set to Yes, and the card supports the feature, MyID requires the customer key to be configured before issuing devices of this type.

If you change any of the options on this screen away from the default, your system will be potentially insecure, and MyID will display an appropriate warning when logging in to MyID or when issuing a smart card that would be affected. See section *31.4*, *System security* for more information.

34.4 Server page (Security Settings)

Setting	Default value	Description	Further information
Allow envelope version 1.2	No	Whether MyID supports clients using the older method of securing data between clients and the MyID server. This option may be required for some older clients and web services. See the **Release Notes** for details.	Do not deselect *both* **Allow envelope version 1.2** and **Allow envelope version 1.3** or you will be locked out of MyID. If this happens, contact customers support, quoting reference SUP-140.
Allow envelope version 1.3	Yes	Whether MyID supports clients using the newer method of securing data between clients and the MyID server. This option may not be supported on older clients. See the **Release Notes** for details.	

Setting	Default value	Description	Further information
Allow Legacy Data Models	No	Data model handling has been improved and is now more robust from MyID 10.7. However, if you have old MyID clients that need to activate cards, these old clients may not be compatible with the new data model handling mechanism, causing device personalization to fail, with the following error being written to MyID system events: `Legacy datamodel configuration is disabled` If this occurs, you are recommended to update the old MyID clients. However, if this is not possible, you can re-enable old data model processing behavior by setting this option to `Yes` for the interim period while MyID clients are updated. Once old clients are updated, set this option back to `No`.	
PIV Server hash algorithm	SHA256	PIV data can be hashed using SHA256 (which is required for PIV compliance) or SHA1 (for systems that do not require full PIV compliance). The default is SHA 256. PIV only.	See the *PIV Integration Guide* for details.
Server Encryption	Software based only	Whether the MyID server should send certain (sensitive) responses to the client encrypted using the public encryption key associated with the device of the holder currently logged on to MyID. **None** – Do not use encryption. **Yes (Software or Card if available)** – Use encryption keys from your smart card, if available. **Software based only** – Use a software encryption key generated when you log on.	Cannot be edited. Contact customer support for details.
Store Secret Keys	Yes	Whether secret (symmetric) keys can be stored in the MyID database, encrypted using the MyID 3DES key.	Cannot be edited. Contact customer support for details.

Setting	Default value	Description	Further information
Validate signing certificates	No	If you set this option to Yes, when a user submits data in a workflow that is signed by a certificate, MyID validates the certificate against the certificate revocation list. If the validation fails, MyID prevents the user from submitting the data. In addition, if you have an external system that allows you to link to an authentication server for certificate validation, the authentication server is used to validate the certificate after MyID as secondary validation.	**Note:** The application server must trust the Certificate Authority that issued the certificate being validated. **Note:** This option provides a great deal of security, as many transactions are signed by a certificate and validated at each point. However, this may involve a drop in performance when the certificate is validated: a single workflow may involve several signed bundles of data, each of which must be validated.

34.5 PINs page (Security Settings)

Setting	Default value	Description	Further information
Action on maximum invalid phrases	Lock security phrases	Determines what happens when a user has reached the **Maximum allowed security question failures** – can be one of the following: `Lock security phrases` – The user's account is locked. `None` – The user can retry as many times as they like.	
Ask Security Questions for Self Service Card Unlock	No	Whether the holder's security phrase is used when unlocking a card.	See section *27.7.5*, *Self-service PIN reset authentication*.
Case sensitive security questions	Yes	Whether the case of responses to security phrases is checked when authenticating.	
Default max PIN length	12	The default maximum PIN length.	See section *12.3.1*, *Credential profile options*.
Lock Card on Issuance	Ask	Whether the PIN assigned during issue is locked. If so, the holder must enter a new PIN on first use.	See section *12.3.1*, *Credential profile options*.

Setting	Default value	Description	Further information
Number of security questions for operator authentication	1	The number of security phrases the user is required to provide when an operator asks them; for example, during the **Authenticate Person** or **Unlock Credential** workflows.	See section *3.3.2*, *Setting the number of security phrases required to authenticate* for details.
Number of security questions for self-service authentication	2	The number of security phrases users are required to provide when authenticating themselves.	See section *3.3.2*, *Setting the number of security phrases required to authenticate* for details.
Number of security questions to register	2	The number of security phrases to enroll for a user in the **Change Security Phrases** or **Change My Security Phrases** workflows.	See section *3.3.2*, *Setting the number of security phrases required to authenticate* for details.
Offline Unlock Method	Challenge	Challenge – a dialogue between the holder and the helpdesk, passing challenges and responses to identify the holder and the device. Witness – another holder must witness the request. None – offline unlocking not possible.	Used for Giesecke & Devrient cards.
PIN Timeout	180	Period of inactivity (in minutes) before a PIN must be re-entered. This may be overruled by the device's own timeout period, if shorter.	
Prevent version 1 password enrollment	No	If you set this option to Yes, and the **Use Security Phrase algorithm version 2** option is set to Ask, security phrases are stored only with SHA256 hashes. This allows you to force a transition to SHA256 security phrases and gradually remove any SHA1 stored answers.	
Reload Device Profile	Yes	No longer used.	
Remote Unlock requires an Authentication Code prompt	No	If set to Yes, the user must provide an authentication code to remotely unlock a card or device.	No longer required. See section *27.7.6*, *Unlocking a credential remotely* for details of configuring MyID for remote unlock.

Setting	Default value	Description	Further information
Security Phrase allowable characters		The characters accepted in a security phrase. List individual characters or ranges. The only permissible ranges are a-z (all lowercase letters), A-Z (all uppercase letters) and 0-9 (all numbers). For example: `a-zA-Z!%&` The default (blank) means no restrictions.	**Note:** a-z and A-Z do not include accented characters. If required, these must be specified individually.
Security Phrase complexity format		Defines the rules for allowed security phrases. Leave blank to allow any format.	See section *3.3.1*, *Setting rules for security phrases*, for detailed instructions.
Security Phrase minimum length	0	The minimum number of characters accepted for a security phrase. Set to `0` to allow any security phrases with one or more characters.	
Security Phrase repeat character limit	0	The maximum number of repeated characters accepted in security phrases. 0 allows any number of repeated characters.	
Security Phrase sequential character limit	0	The maximum number of sequential characters – either numbers (1, 2, 3) or letters (a, b, c) – in security phrases. 0 allows any number of sequential characters.	
Security Phrase whitespace removal	No	Set to Yes to remove any spaces from security phrases before storing or checking the security phrase.	

Setting	Default value	Description	Further information
Set GlobalPlatform Card Status	No	Whether MyID can set the GlobalPlatform status for a device. When you use deferred activation, MyID must be able to set the card status from `SECURED` to `LOCKED`. If the card is shipped with the status `SECURED`, no further action is required. If the card is shipped with the status `OP_READY` or `INITIALIZED`, for example, you must set this option to `Yes` to allow MyID to change the card status to `SECURED` before it sets the status to `LOCKED` for deferred activation. **Note:** You must also make sure that you set up customer GlobalPlatform keys for your cards. The status change from `OP_READY` or `INITIALIZED` to `SECURED` occurs when MyID sets the customer keys for a card. See your card integration guide for whether you need to set this option.	
Show Generated PINs	Yes	Whether the PIN for a device (when this is a random or server-generated PIN) should be displayed when the device is issued.	
Transport PIN	12549856	Default PIN for canceled cards.	
Use logon name for server PIN generation	No	You can use the user's logon name as the diversification data for PIN generation; this ensures that the user has the same PIN for all of their devices.	See section *10.3*, *PIN generation algorithm* for details.
Use Security Phrase algorithm version 2	Ask	If you are upgrading from a previous system, and this option was previously set to No, this is set to Yes by the installer. This option is used to configure MyID to set security phrases to use SHA256 hashing.	See the ***Installation and Configuration Guide*** for details of upgrading the hashed security phrase answers stored in the MyID database.

34.6 Process page (Security Settings)

Setting	Default value	Description	Further information
Allow Administrative Groups	No	When set to **YES**, the scope available in workflows is extended to include any additionally specified administrative groups assigned to operators. The **Add Person** and **Edit Person** workflows are extended to allow management of administrative groups. When set to **NO**, the scope in workflows is limited to operators' home groups, and it is not possible to manage operators' administrative groups in **Add Person** or **Edit Person**.	See section *4.7*, *Administrative groups* for details.
Approve Replacement Cards	No	Whether requests for replacement cards require secondary authorization. **Yes** – All requests for replacement cards require secondary authentication. **No** – No requests for replacement cards require secondary authentication. **Ask** – Requests for replacement cards require secondary authentication only if the **Validate Issuance** setting is set in the credential profile. **Note:** The **Validate Issuance** setting in the credential profile affects replacement cards *only* if this option is set to **Ask**.	
Card Expiration Period (days)	365	Default period that all issued devices are valid.	See section *12.3.1*, *Credential profile options*.
Client Logon Keyset	Signing	Which keyset to use when signing data on the client during logon.	Cannot be edited.
Client Sign Keyset	Signing	Which keyset to use when signing data on the client.	Cannot be edited.

Setting	Default value	Description	Further information
Constrain Credential Profile Collector	Yes (if on installation there were no existing credential profiles) or: No (if on installation there were existing credential profiles).	Whether you can select which roles can collect individual credential profiles on the Select Roles screen in the **Credential Profiles** workflow. If this option is set to `No`, you can collect credentials using any role. For credential profiles that were created when this option was not set to `Yes` (for example, before installing the current version of MyID) if you subsequently set this option to `Yes`, the credential profile will automatically be set to add any roles to the **Can Collect** column that were already selected in any of the other columns: **Can Receive**, **Can Request**, or **Can Validate**.	See section *12.3.8*, *Constrain credential profile collector* for details.
Constrain Credential Profile Issuer	Yes (if on installation there were no existing credential profiles) or: No (if on installation there were existing credential profiles).	Whether you can select which roles can request individual credential profiles on the Select Roles screen in the **Credential Profiles** workflow.	See section *12.3.6*, *Constrain credential profile issuer* for details.
Constrain Credential Profile Unlock Operator	No	Whether you can select which roles can unlock credentials using the **Unlock Credential** and **Reset Card PIN** workflows.	See section *12.3.9*, *Constrain credential profile unlock operator* for details.
Constrain Credential Profile Validator	Yes	Whether you can select which roles can validate individual requests using the selected credential profile.	See section *12.3.7*, *Constrain credential profile validator* for details.
Restrict Roles on Child Groups	No	If you set this to `Yes`, the roles available to a group are restricted to the roles available to the group's parent. The **Inherit Roles** option appears on the Select Roles dialog. If you set this to `No`, the group may select from any roles in the system. The **Inherit Roles** option does not appear on the Select Roles dialog.	

Setting	Default value	Description	Further information
Show Audit Summary	Ask	Whether a summary of the audit information is displayed on completion of a workflow.	
Show Set Security Phrases Button	Yes No – in PIV systems.	Displays a link to the **Change Security Phrases** workflow at the end of **Add Person**.	
Sign Audit on Client	No	Whether audit data from client is signed on the client.	Cannot be edited.
Sign Audit on Server	Yes	Whether Audit Trail information is signed on the server.	Cannot be edited.
Task number timeout	30	The time in minutes before a task number will expire. Task numbers are allocated when you start a workflow; you must complete a workflow before the task number expires. This setting was previously stored in the `DatabaseVersion` table in the MyID database.	

34.7 Self-Service page (Security Settings)

Setting	Default value	Description	Further information
Allow self requests	No	Whether a user who has access to the **Request Card**, **Request Replacement Card**, **Issue Card**, **Request Card Update** or **Batch Request Card** workflows can create a request for a card for themselves.	
Auto-enroll from directory	No	Whether information about a person from an LDAP directory with a matching device serial number can be used to automatically populate the `People` table, allowing holders to self-enroll.	Cannot be edited.
Self-service	Yes	Whether users can edit their own device details.	Cannot be edited.
Self-service emergency password	Yes	Someone with a MyID account can set a temporary password for own use with authentication servers.	Cannot be edited.
Self-service Resynchronization	Yes	Whether users can resynchronize their own cards.	Cannot be edited.
Self-Service Unlock	Yes	Whether holders can unlock their own devices.	
Unknown card logon	No	Whether an unknown device can be used to self-enroll.	Cannot be edited.

34.8 Logon Mechanisms (Security Settings)

Setting	Default value	Description	Further information
Password Logon	Yes	Whether users can log on to MyID with their security phrases.	See section *3.3*, *Using security questions to log on to MyID*.
Smart Card Logon	Yes	Whether users can log on to MyID with their issued smart cards.	See section *3.2*, *Using a card and PIN to log on to MyID*.
Token Logon	No	Whether users can log on to MyID with their issued one time password tokens.	Not used in this version of MyID.
Integrated Windows Logon	No	Whether users can log on to MyID using integrated Windows logon.	See section *3.5*, *Integrated Windows Logon*.
Biometric Logon	Yes	Whether users can log on to MyID using biometrics. Currently used only for resetting PINs.	See section *27.7.5*, *Self-service PIN reset authentication*.

Index