



MyID
Version 11.3

Administration Guide

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

Copyright

© 2001-2019 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 media.
- A `fixed width` font is used where the identification of spaces is important, including filenames, example SQL queries and any entries made directly into configuration files or the database.
- **Notes** are used to provide further information, including any prerequisites or configuration additional to the standard specifications.
For example:
Note: This issue 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.....	10
1.1	Change history.....	10
1.2	Who should read this guide?	10
1.2.1	What do you need to know?	10
1.3	What is included in this guide?	11
1.3.1	Where to find more information.....	11
1.4	Applying updates	12
1.5	The interface.....	13
1.5.1	Selecting dates	16
1.5.2	Entering search criteria	16
1.5.3	Using advanced search	18
1.6	Terminology.....	19
2	Logging On for the First Time	20
2.1	Connecting a workstation.....	20
2.2	Default security settings.....	20
3	Logon Mechanisms	21
3.1	Authentication feedback	21
3.2	Using a card and PIN to log on to MyID.....	21
3.2.1	Smart card states.....	22
3.3	Using security questions to log on to MyID	23
3.3.1	Setting rules for security phrases.....	24
3.3.2	Changing rules for security phrases	25
3.3.3	Setting the number of security phrases required to authenticate	25
3.3.4	Unlocking security phrases.....	26
3.3.5	Unlocking your own security phrases	27
3.4	Logon codes	28
3.4.1	Setting up logon codes	28
3.4.2	Using logon codes	29
3.5	Integrated Windows Logon	30
3.5.1	Integrated Windows Logon for existing user accounts.....	31
4	Roles, Groups and Scope.....	32
4.1	Roles	32
4.1.1	Change an existing role	33
4.1.2	Add a role	34
4.1.3	Delete a role	34
4.1.4	Controlling the assigning of roles.....	35
4.1.5	Assigning logon mechanisms	36
4.2	Role inheritance.....	37
4.2.1	Role restriction option	37
4.2.2	Setting a group to inherit roles.....	37
4.2.3	Inherited roles example	38
4.3	Default roles.....	38
4.3.1	Default roles example	38
4.3.2	Setting up default roles	39
4.3.3	Known issues.....	40
4.3.4	Synchronizing with LDAP.....	40
4.4	Linking roles to LDAP	41
4.4.1	Default Active Directory groups	41
4.4.2	Setting up linked roles	42
4.4.3	Example.....	43
4.5	Scope and security	43
4.6	Groups.....	44
4.7	Administrative groups	44
4.7.1	Configuration settings	45
4.7.2	Assigning Administrative Groups	45

4.7.3	The Select Group dialog	45
4.7.4	The Find Person stage	46
4.7.5	The View Person workflow.....	46
4.7.6	Group management.....	47
4.7.7	The Import Account Details dialog	47
4.7.8	Scope calculations	47
4.8	Witnessing a transaction.....	48
5	Using an LDAP Directory	50
5.1	What do you need to know?	51
5.2	Creating the connections	51
5.3	Using and updating LDAP information.....	53
5.4	Using an LDAP directory as the primary data source	53
5.5	The Batch Directory Synchronization Tool.....	54
5.5.1	How does the Synchronization Tool work?	54
5.5.2	Revoking certificates.....	55
5.5.3	Running the tool from the Start menu	55
5.5.4	Running the tool from the command line	56
5.5.5	Running as a scheduled task.....	56
5.5.6	Troubleshooting	57
5.6	Storing the NETBIOS name for a person.....	58
5.7	Setting up a configuration-only directory.....	58
5.8	Active Directory Deletion Tool.....	59
5.8.1	Scheduled task repeat interval.....	59
5.8.2	Setting up a Scheduled Task.....	60
6	Certificate Authorities	62
6.1	Certificate refresh configuration	62
6.2	Connecting to a CA.....	63
6.2.1	Recording a new CA.....	63
6.2.2	Editing an existing CA.....	64
6.2.3	Deleting a CA.....	64
6.3	Enabling certificates on a CA.....	65
6.4	Scheduled certificate revocation operations	66
6.5	Revoking timed-out certificates.....	66
6.6	Certificate renewal	66
6.6.1	Credential lifetimes and certificate renewal.....	67
6.7	Superseding certificate policies	68
6.7.1	Recovering superseded certificates	70
6.7.2	Troubleshooting	70
6.7.3	Viewing superseded certificate policies	71
6.8	Import and distribute certificates to devices	71
6.8.1	Setting up the Unmanaged certificate authority	71
6.8.2	Setting up a credential profile for PFX certificates	72
6.8.3	Uploading multiple PFX certificates	73
6.8.4	Removing uploaded certificates.....	74
7	Applets.....	75
7.1	GlobalPlatform keys.....	75
7.2	Check configuration setting.....	76
7.3	Manage GlobalPlatform keys.....	76
7.3.1	Entering factory (vendor) keys	77
7.3.2	Using a key ceremony	79
7.3.3	Importing keys from a file.....	80
7.3.4	Exporting keys	80
7.3.5	Deleting factory (vendor) keys	81
7.3.6	Entering customer (local) keys.....	81
7.3.7	Deleting customer (local) keys.....	83
7.4	Managing applets	84
7.4.1	Add an applet.....	85
7.4.2	Edit an applet.....	85
7.4.3	Upgrade an applet	86

8	Designing Card Layouts	87
8.1	Restricting access to card layouts	88
8.2	Configuring the image location	88
8.3	Creating, saving and deleting layouts	88
8.4	Using the layout tools	89
8.4.1	Rotating the card	90
8.4.2	Showing the chip	90
8.4.3	Showing the grid, snapping elements and zooming.....	90
8.5	Images and backgrounds.....	90
8.5.1	Uploading images to the web server.....	91
8.5.2	Specifying a background.....	91
8.5.3	Fitting an image to a card	91
8.5.4	Adding static images.....	92
8.5.5	Adding dynamic images.....	92
8.5.6	Custom image fields	93
8.5.7	Externally formatted image fields.....	93
8.5.8	Image aspect ratio	94
8.6	Adding or changing text	95
8.6.1	Adding and changing static text	95
8.6.2	Adding dynamic text	96
8.6.3	Custom text fields	97
8.7	Formatting text.....	97
8.8	Changing the text color	98
8.8.1	Using the color picker	98
8.9	Positioning and sizing elements.....	98
8.10	Defining data to store on magnetic stripes.....	99
8.11	Using templates	99
8.11.1	Applying zone settings.....	100
8.11.2	Template XML structure.....	100
8.12	Reviewing and testing your layout	102
9	PIN Generation.....	103
9.1	Adding a PIN Generation key	103
9.2	Credential profile setup for PIN generation.....	104
9.3	EdficePinGenerator PIN generation algorithm	105
9.3.1	Generating the PIN	105
9.3.2	Alphabet tables	105
9.3.3	Example.....	107
10	Importing Serial Numbers.....	109
10.1	Troubleshooting and known issues with importing serial numbers	109
11	Managing Credential Profiles	111
11.1	Setting default values	111
11.2	Using the provided credential profile.....	112
11.3	Creating, modifying, copying and deleting credential profiles	112
11.3.1	Credential profile options	113
11.3.2	Additional credential profile options	121
11.3.3	Selecting certificates	124
11.3.4	Selecting applets	125
11.3.5	Linking credential profiles to roles.....	126
11.3.6	Constrain credential profile issuer.....	126
11.3.7	Constrain credential profile validator.....	126
11.3.8	Constrain credential profile collector.....	126
11.3.9	Constrain credential profile unlock operator.....	127
11.3.10	Associating credential profiles with card layouts.....	127
11.3.11	Adding comments to the credential profile	127
11.4	Setting up mail merge documents	127
11.5	Setting up a credential profile for soft certificates	128
11.6	Customizing terms and conditions	130
11.6.1	Customizing terms and conditions using the HTML template method	130
11.6.2	Customizing terms and conditions for the web service	130

11.6.3	Customizing terms and conditions using the SignedTCs.txt method	130
11.6.4	Customizing terms and conditions using the translation method	131
11.6.5	Storing signed terms and conditions	131
12	License Management	132
12.1	View current license status	133
12.2	Requesting licenses.....	134
12.3	Installing license details	134
12.4	Updating warning messages.....	135
13	Email Notification	136
13.1	System-wide email settings	136
13.1.1	Switching email notifications on or off.....	136
13.1.2	Email format.....	136
13.1.3	Email codepage	136
13.1.4	Email separator.....	137
13.1.5	Changing the recipient of administrator messages	137
13.1.6	Setting the number of email notifications	137
13.2	Changing email messages.....	137
13.3	Standard templates.....	139
13.3.1	Triggering the notification.....	141
13.4	Adding a new email template.....	143
13.5	Using the Notifications Management workflow	145
14	Changing List Entries	147
15	Managing Keys	148
15.1	Using GenMaster	148
15.2	The Key Manager workflow	148
15.2.1	Transport keys	148
15.2.2	Factory 9B keys	150
15.2.3	Customer 9B keys	151
15.2.4	Application keys	152
15.2.5	Exporting keys	154
16	The Audit Trail.....	155
16.1	Audit scope	155
16.2	Running the audit report	155
16.2.1	Information icons	156
16.2.2	Browsing through blocks of events	156
16.3	Specifying the items to audit.....	156
17	Key Archiving.....	158
17.1	MyID encryption	158
17.2	Cards supported	158
17.3	Certificate authority key archiving	158
17.4	MyID key archiving	158
17.5	Setting up key archiving.....	158
18	Key Recovery	161
18.1	Setting up the credential profile	161
18.2	Requesting a key recovery	162
18.3	Validating a key recovery request.....	164
18.4	Collecting a key recovery job for another user.....	164
18.5	Collecting a key recovery job for yourself	165
18.6	Viewing key recovery operations	166
19	External Systems.....	167
20	Archiving Deleted Users	168
21	External Logon Providers.....	169

22	Job Management	170
22.1	Searching for a job.....	170
22.1.1	General search criteria	170
22.1.2	Searching by target.....	171
22.1.3	Searching by initiator, validator or actioned by	171
22.1.4	Searching by renewal or suspended dates.....	171
22.2	Viewing job records	171
22.3	Managing jobs	172
23	Activating Cards	173
23.1	Configuring a credential profile for activation	173
23.1.1	Personalization and encoding scenarios	174
23.2	Terms and conditions	175
23.3	Setting up authentication methods for activation	175
24	Managing Devices	177
24.1	Overview.....	177
24.2	Access to the workflows.....	177
24.3	Setting up the SCEP server on a separate machine.....	178
24.4	Certificates.....	178
24.4.1	Signing certificate	178
24.4.2	Encryption certificate	178
24.5	Registry entries.....	179
24.6	Setting up a credential profile to use to issue device identities	179
24.7	Adding devices	180
24.7.1	Adding devices manually	180
24.7.2	Adding devices from an LDAP directory	181
24.8	Editing a device	182
24.9	Requesting a device identity	183
24.10	Validating a device identity request	184
24.11	Collecting device identities.....	185
24.12	Canceling device identities	186
24.13	Approving device identity cancellations	188
24.14	Known issues.....	189
25	Troubleshooting	190
25.1	System status report.....	190
25.2	System events report.....	190
25.2.1	Archived System Events.....	191
25.3	Expanded error messages.....	191
25.4	System security	191
26	Additional Identities	193
26.1	Overview.....	193
26.2	Setting up additional identities	193
26.3	Adding additional identities	195
26.4	Removing additional identities	197
26.5	Adding an additional identity for your own account.....	198
26.6	Known issues.....	198
27	Configuration – Operation Settings.....	199
27.1	Making configuration changes	199
27.1.1	Changing the operation settings	199
27.2	General page (Operation Settings)	200
27.3	Devices page (Operation Settings)	202
27.4	LDAP page (Operation Settings)	206
27.5	Video page (Operation Settings).....	210
27.6	Certificates page (Operation Settings).....	212

27.7	Import & Export page (Operation Settings)	215
27.8	Identity Checks page (Operation Settings)	216
27.9	Bureau & Job page (Operation Settings)	217
27.10	Biometrics page (Operation Settings)	218
27.11	Issuance Processes page (Operation Settings)	220
27.12	Notifications page (Operation Settings)	223
27.13	Identity Agent Policy page (Operation Settings)	224
28	Configuration – Security Settings	226
28.1	Making configuration changes	226
28.1.1	Changing the security settings.....	226
28.2	Logon page (Security Settings).....	227
28.3	Device Security page (Security Settings).....	230
28.4	Server page (Security Settings)	231
28.5	PINs page (Security Settings).....	233
28.6	Process page (Security Settings).....	237
28.7	Self-Service page (Security Settings)	239
28.8	Logon Mechanisms (Security Settings)	240

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 [1.5, The interface](#).

1.1 Change history

Version	Description
ADM1944-01	Updated for MyID 11.0.
ADM1944-02	Updated for MyID 11.1.
ADM1944-03	Updated for MyID 11.2.
ADM1944-04	Updated for MyID 11.3. Day-to-day operations moved to the new <i>Operator's Guide</i> .
ADM1944-05	Minor updates and clarifications.

1.2 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.

1.2.1 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.

1.3 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 by 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 [1.5, 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.

1.3.1 Where to find more information

For day-to-day operation of MyID, see the [Operator's Guide](#).

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.

1.4 Applying updates

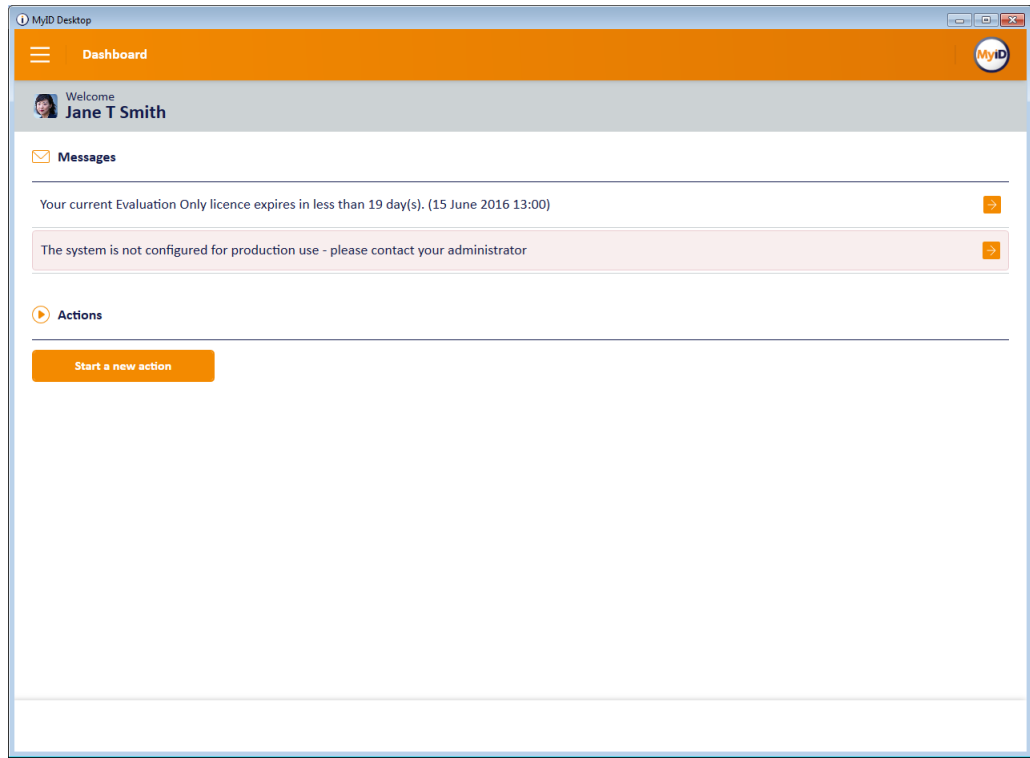
Instructions for applying updates (patches and hotfixes) are provided with the individual update – see the documentation that comes with the update.


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](#).

1.5 The interface

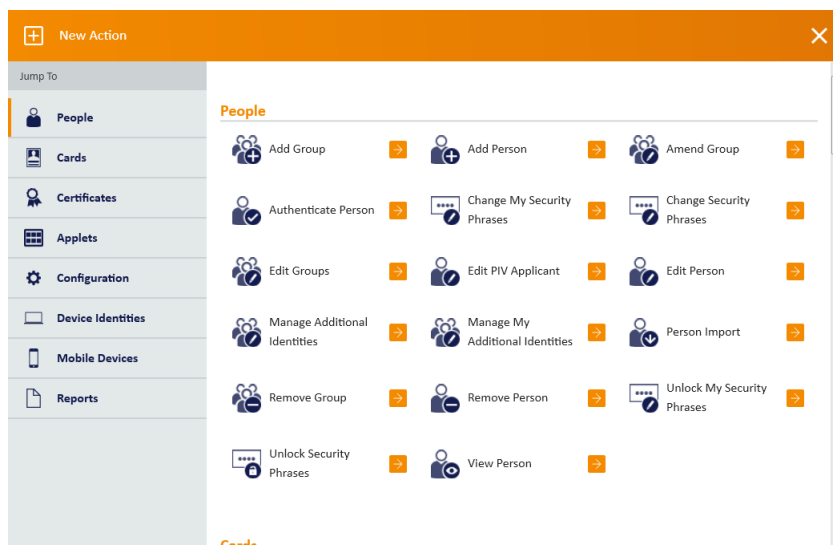
Note: A detailed explanation of the terminology used within MyID and this document is provided in section 1.6, *Terminology*.

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



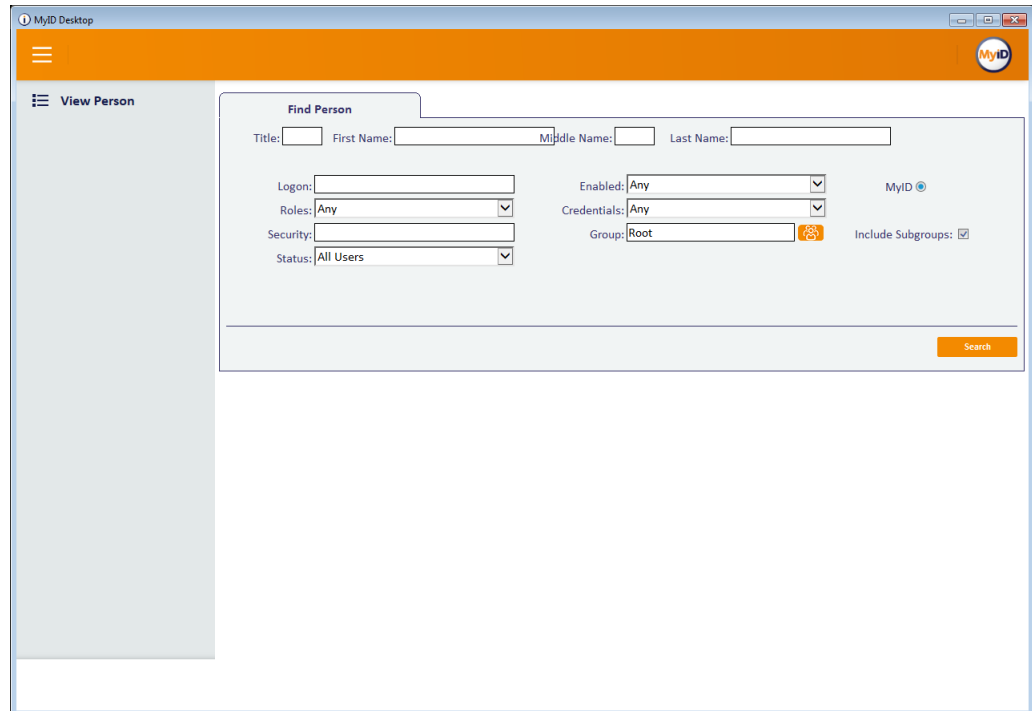
If there are any system messages, they appear at the top of the screen. For some messages, you can click the arrow  to take you to the appropriate workflow; for example, if your system is not set up for production use, clicking the arrow takes you to the **Security Settings** workflow to allow you to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








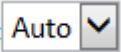


Ask or Prompt



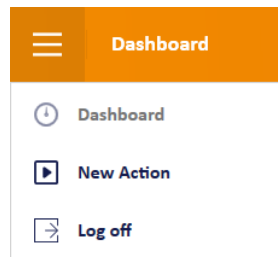
An information icon may provide additional information about a topic in the form of a tooltip.

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:

	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: 	Change the number of rows displayed.

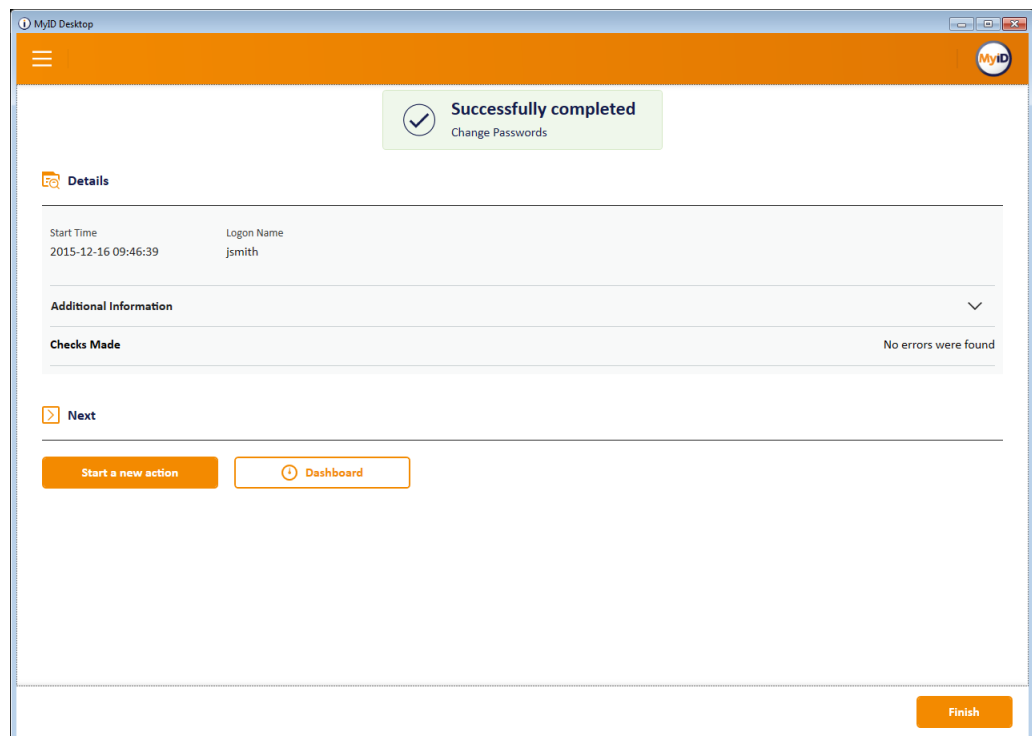
Note: Information displayed in a table can be sorted in ascending or descending order, based on a selected heading. Click a heading to sort by that value; click it again to reverse the sort order.

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

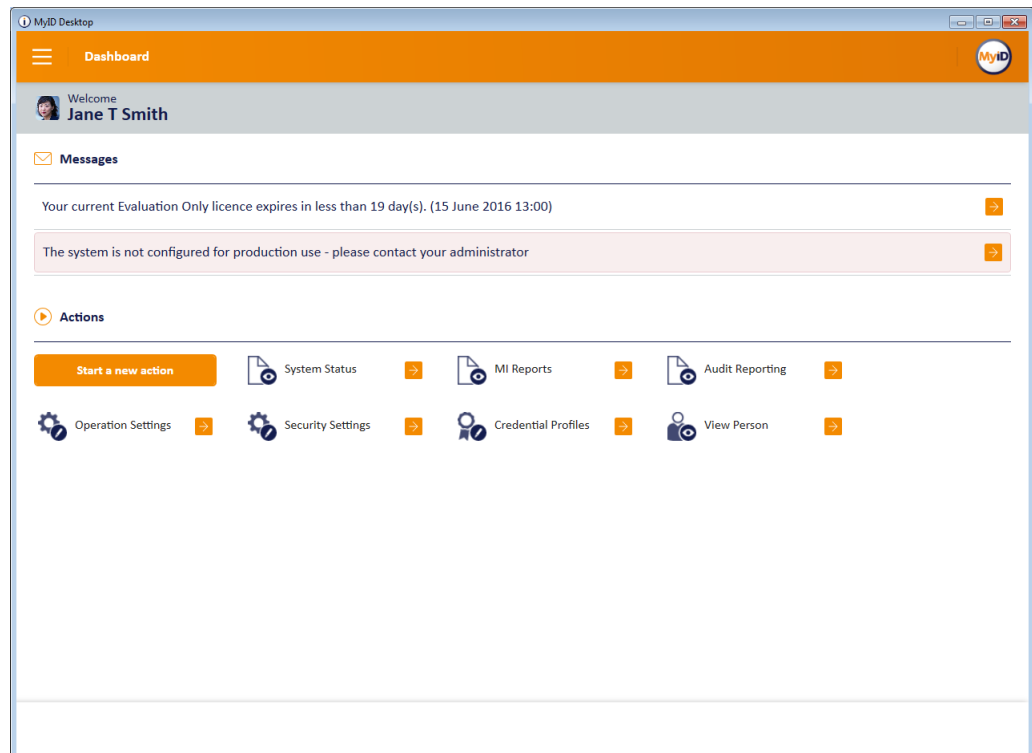


You can return to the dashboard when you are in a workflow, and you can start a new action when you are on the dashboard.

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.



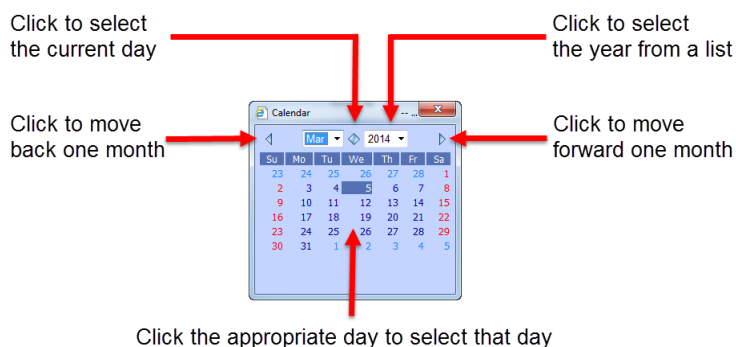
As you work with MyID, your most recent workflows will appear on your dashboard:



1.5.1 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:



1.5.2 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

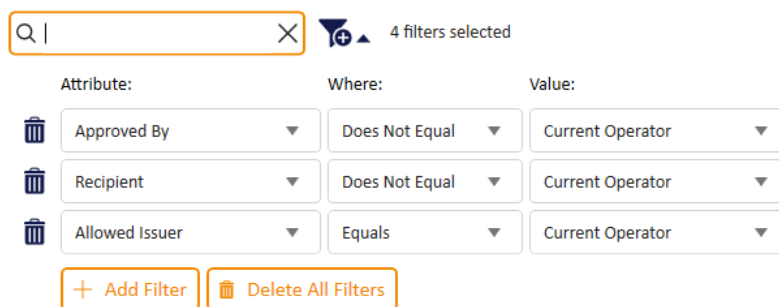
to find

- jones-smith




1.5.3 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.


Select a job or search for a person



The interface shows a search bar with a magnifying glass icon and a close button. To the right of the search bar is a filter icon and the text "4 filters selected". Below the search bar is a table with three columns: Attribute, Where, and Value. The table contains three rows of filter rules. Each row has a delete icon (trash can) to the left of the Attribute column. At the bottom of the table are two buttons: "+ Add Filter" and "Delete All Filters".

Attribute:	Where:	Value:
 Approved By	Does Not Equal	Current Operator
 Recipient	Does Not Equal	Current Operator
 Allowed Issuer	Equals	Current Operator

+ Add Filter Delete All Filters

- 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**.

1.6 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 <i>card</i> 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 <i>smart card</i> .
card	A collective term for <i>smart cards</i> and <i>tokens</i> when there is no need to distinguish between them.
cardholder	A person who has been issued a <i>card</i> or other <i>credentials</i> .
category	<i>Workflows</i> are combined into related sets called categories. Note: The term 'group' is <i>not</i> 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 <i>cards</i> and <i>tokens</i> issued to a holder or a <i>device</i> .
device	A piece of equipment – a PC, server, router, cell phone or other hardware.
form	The information displayed during a stage. A form may consist of a single or multiple pages.
group	Groups provide the structures that contain the people in the database.
job	A queued task carried out by MyID.
operator	A person who uses MyID to issue and manage <i>smart cards</i> or <i>tokens</i> , but who is not responsible for configuration.
printer	A <i>smart card</i> printer – some printers also incorporate <i>card readers</i> .
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 <i>workflow</i> .
token	<i>Credentials</i> using <i>smart card</i> 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 <i>device</i> .
virtual smart card (VSC)	Microsoft virtual smart card. A container that can hold credentials such as certificates and cryptographic keys. Stored on a <i>trusted platform module</i> .
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.

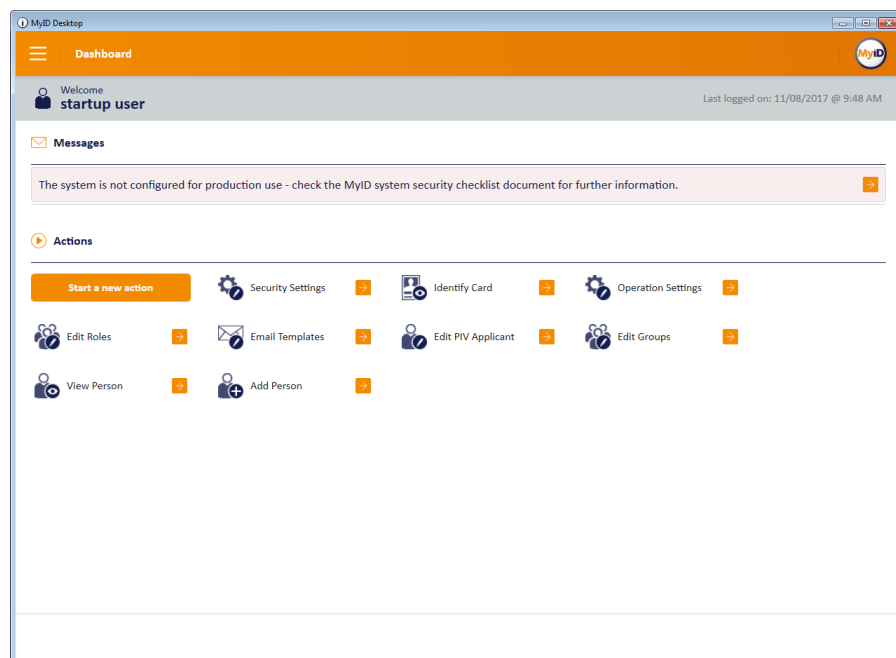
The [Installation and Configuration Guide](#) contains information on using GenMaster to set the passphrase for the startup user.

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 - check the MyID system security checklist document for further information.

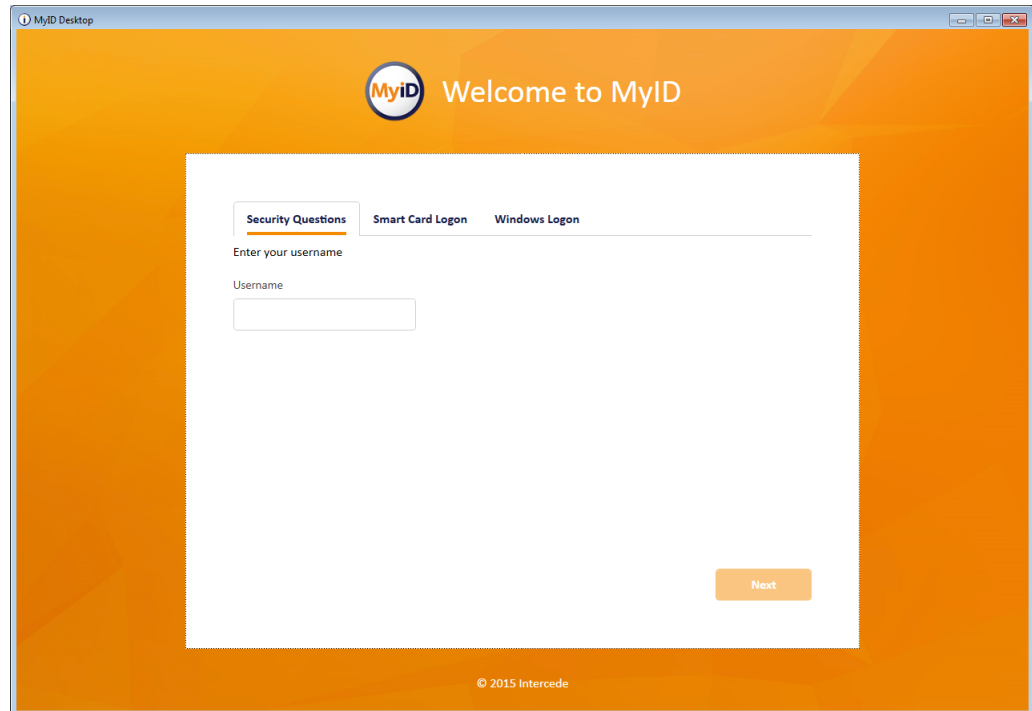
If this warning appears, you must review the settings on the **Device Security** tab on the **Security Settings** workflow; see the [System Security Checklist](#) document. This document also contains information about configuring SOPINs, GlobalPlatform keys, and PIV9B keys to ensure that your system 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 [11, 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:

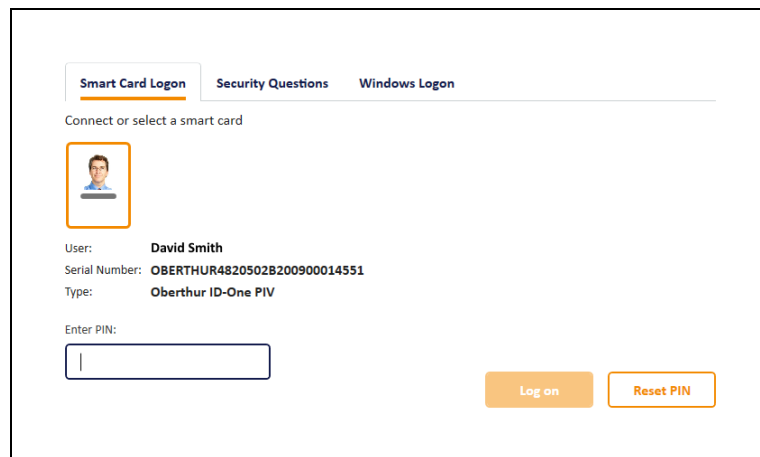
1. From the **Configuration** category, select **Security Settings**.
2. On the **Logon Mechanisms** tab, make sure that **Smart Card Logon** is set to Yes.
3. Click **Save changes**.
4. In the **Edit Roles** workflow, make sure the user's role has the **Smart Card** logon mechanism assigned.

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:

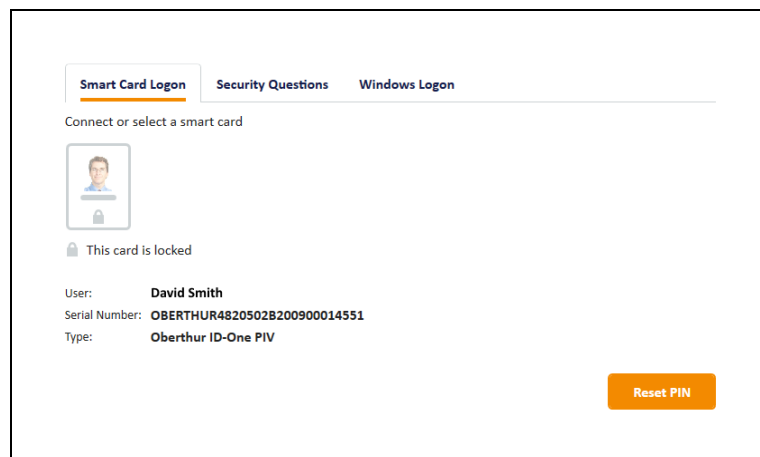


The screenshot shows the 'Smart Card Logon' tab selected. Below the tab, it says 'Connect or select a smart card'. There is a small icon of a person's face. Below the icon, the following information is displayed:

- User: **David Smith**
- Serial Number: **OBERTHUR4820502B200900014551**
- Type: **Oberthur ID-One PIV**

Below this information is a text input field labeled 'Enter PIN:'. To the right of the input field are two buttons: 'Log on' and 'Reset PIN'.

Locked card:

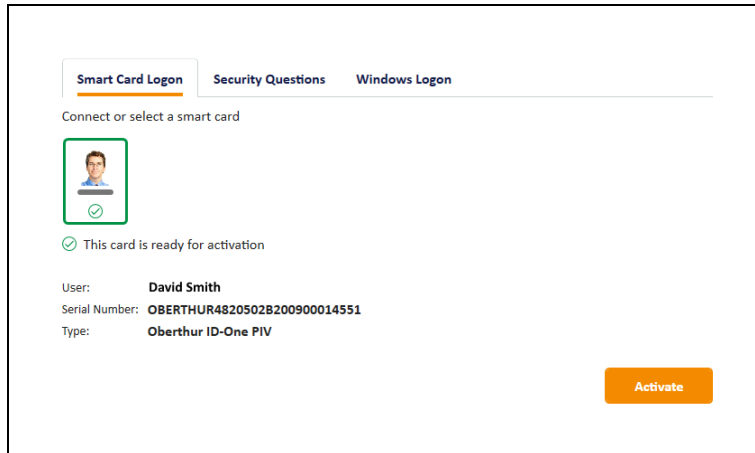


The screenshot shows the 'Smart Card Logon' tab selected. Below the tab, it says 'Connect or select a smart card'. There is a small icon of a person's face with a lock symbol over it. Below the icon, the following information is displayed:

- User: **David Smith**
- Serial Number: **OBERTHUR4820502B200900014551**
- Type: **Oberthur ID-One PIV**

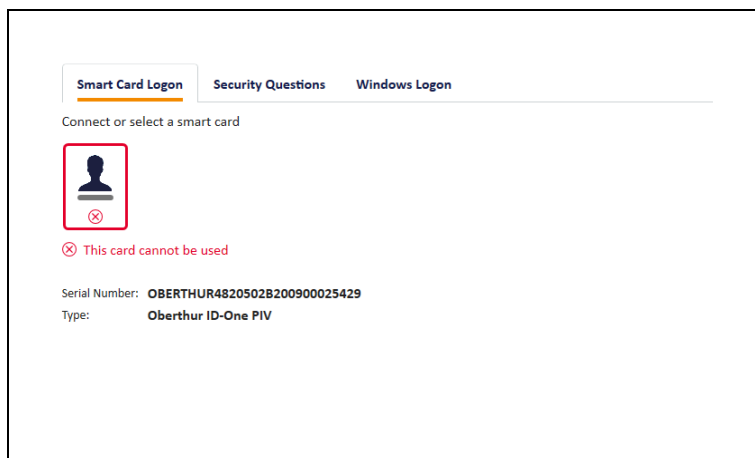
Below this information is a message: 'This card is locked'. To the right of the message is a button: 'Reset PIN'.

Card ready for activation:



The screenshot shows the 'Smart Card Logon' tab selected. Below the tabs, it says 'Connect or select a smart card'. A card icon with a green checkmark is displayed. Below the icon, it says 'This card is ready for activation'. The card details are listed: User: David Smith, Serial Number: OBERTHUR4820502B200900014551, and Type: Oberthur ID-One PIV. An 'Activate' button is located at the bottom right.

Invalid card:



The screenshot shows the 'Smart Card Logon' tab selected. Below the tabs, it says 'Connect or select a smart card'. A card icon with a red X is displayed. Below the icon, it says 'This card cannot be used'. The card details are listed: Serial Number: OBERTHUR4820502B200900025429, and Type: Oberthur ID-One PIV.

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 [28.5, 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 format** 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. In the **Security Phrase complexity format** option, 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:

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

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 Changing rules for security phrases

Important: If you have recorded pass phrases within MyID, then subsequently change any of the following options for security phrases:

- **Case sensitive security questions**
- **Security Phrase whitespace removal**

the existing security phrases stored in the database are likely to become invalid, and therefore you must re-enroll the security phrases for all of your users to allow them to authenticate again. You can do this using the Lifecycle API or using the **Change Security Phrases** or **Change My Security Phrases** workflows in MyID Desktop.

3.3.3 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.

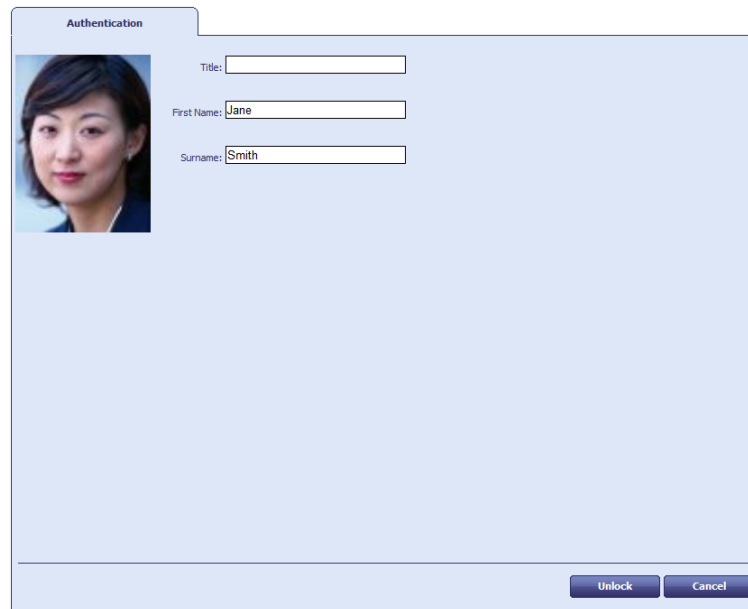
3.3.4 Unlocking security phrases

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.



Authentication



Title:

First Name:

Surname:

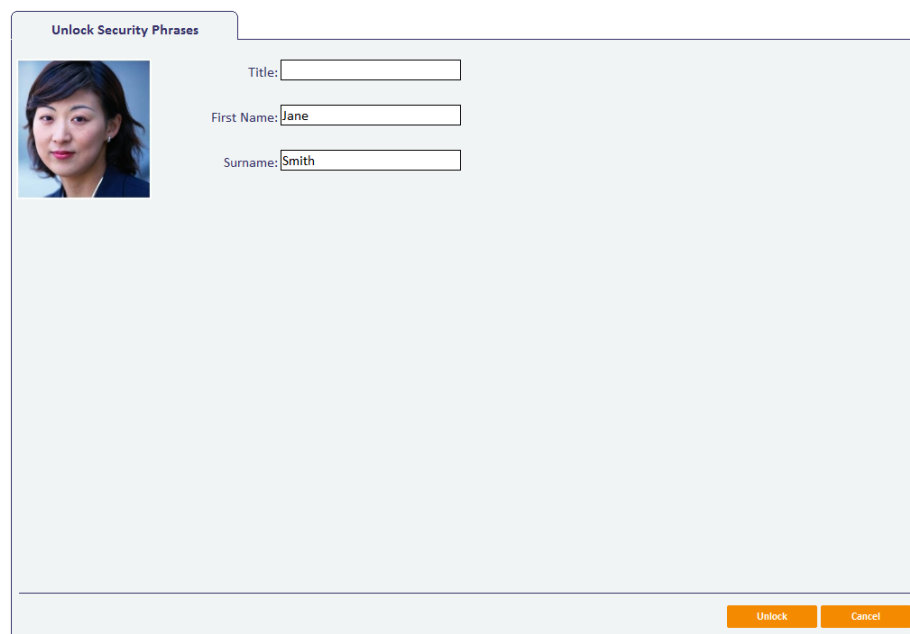
4. Click **Unlock**.

3.3.5 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**.



Unlock Security Phrases



Title:

First Name:

Surname:

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 13.1.2, [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 3.3.3, [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.

Note: You must make sure that the MyID web site has been included in the list of Trusted Sites in the Internet Options on each MyID Desktop client.

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 the *Adding people* section in the [Operator's Guide](#).

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:

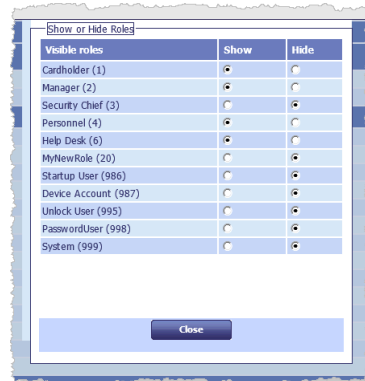
- Change existing roles
- Add new roles
- Delete roles

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.

Available workflows

The master list of workflows in the Edit Roles workflow may contain workflows that are not available for your clients. You can hover your mouse over the workflow name to display a tooltip that lists which clients can use the workflow.

In addition, the following MyID Desktop workflows are not available in any legacy web-based clients:

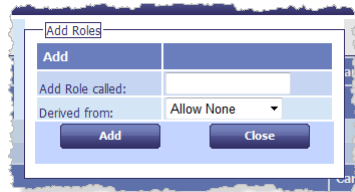
- **Assisted Activation**
- **Batch Collect Card**
- **Bio Unlock My Card**
- **Cancel Credential**
- **Cancel Device Identity**
- **Collect Card**
- **Erase Card**
- **Print Card**
- **Reset Card PIN**
- **Unlock Credential**

Also, the following Desktop Client (Web UI) workflow is not available in MyID Desktop – it has been replaced by the MyID Desktop workflow with the same name:

- **Assisted Activation**

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.

Edit Roles		
Option	Auditor	Audit Manager
Managed By		
Console Logon	<input type="checkbox"/>	<input type="checkbox"/>
Full Access to Manager Controlled Lists	<input type="checkbox"/>	<input type="checkbox"/>
	Auditor	Audit Manager
People	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Add Group	<input type="checkbox"/>	<input type="checkbox"/>
Add Person	<input type="checkbox"/>	<input type="checkbox"/>

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.

Who can allocate this role?

Cardholder (1)	<input type="checkbox"/>
Manager (2)	<input type="checkbox"/>
Security Chief (3)	<input type="checkbox"/>
Personnel (4)	<input type="checkbox"/>
Help Desk (6)	<input type="checkbox"/>
Startup User (986)	<input type="checkbox"/>
Device Account (987)	<input type="checkbox"/>
Windows Logon User (990)	<input type="checkbox"/>
Activation User (994)	<input type="checkbox"/>
Unlock User (995)	<input type="checkbox"/>
System (999)	<input type="checkbox"/>

OK
Cancel

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.

	Password	Smart Card	Windows Logon	Biometric Logon
Cardholder (1)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Manager (2)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Security Chief (3)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Personnel (4)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Help Desk (6)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Startup User (986)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Device Account (987)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Windows Logon User (990)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Activation User (994)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Unlock User (995)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
PasswordUser (998)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
System (999)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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 the *Self-service PIN reset authentication* section in the [Operator's Guide](#).
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.

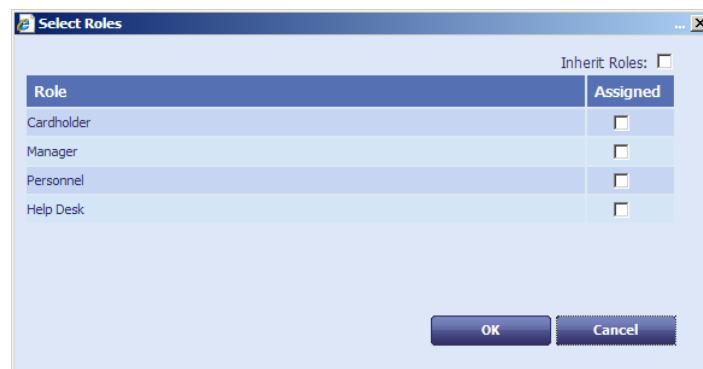
To set the role restriction option:

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.

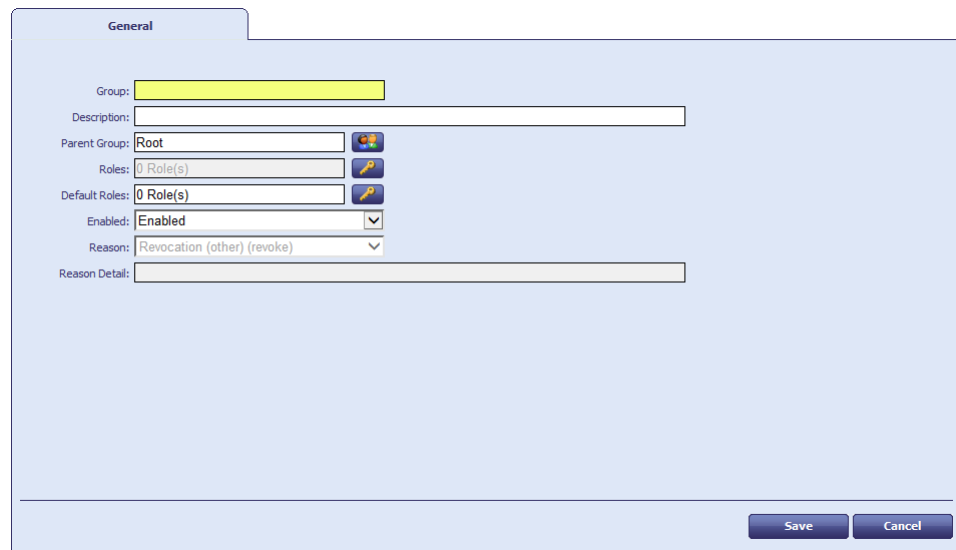
Edit the `Admin North` group, and uncheck the **Inherit Roles** option on the **Select Default Roles** dialog. Now edit the `Administrators` group to change the default roles to `System` only. If you view the `Admin North` group, you can see that it still has `System`, `Manager` and `Cardholder` as default 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:

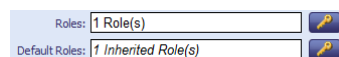
1. From the **People** category, select **Add Group**.



The screenshot shows a 'General' tab for a group creation form. The 'Group' field is highlighted in yellow. Below it is a 'Description' field. The 'Parent Group' is set to 'Root'. The 'Roles' field shows '0 Role(s)' and the 'Default Roles' field also shows '0 Role(s)'. The 'Enabled' checkbox is checked, and the 'Reason' is set to 'Revocation (other) (revoke)'. There is a 'Reason Detail' field at the bottom. At the bottom right are 'Save' and 'Cancel' buttons.

2. Type the **Group** name and **Description**.
3. Select the **Parent Group**.

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



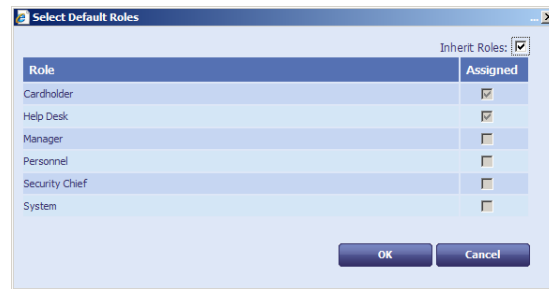
The screenshot shows the 'Roles' and 'Default Roles' fields. The 'Roles' field shows '1 Role(s)' and the 'Default Roles' field shows '1 Inherited Role(s)'. Both fields have a small icon to the right.

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.

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.

Option	Cardholder	Manager	Security Chief	Help Desk
Managed By				
Linked to LDAP Group	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Console Logon	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Full Access to Manager Controlled Lists	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Cardholder	Manager	Security Chief	Help Desk
People	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Add Person	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Add Group	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Edit Person	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Person Import	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Amend Group	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Remove Group	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Edit Groups	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Remove Person	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Change My Security Phrases	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
View Person	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Import From File	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Change Security Phrases	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Add Person and Issue Card	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Buttons: Show/Hide Roles, Delete, Add, Logon Methods, Save Changes, Reset

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.

Note: You cannot link system roles; for example, the Startup User role, or the Activation User role.

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

LDAP group link

Link Role to LDAP Group	
Default to Self Scope	<input checked="" type="radio"/>
Default to Group Scope	<input type="radio"/>
Default to Division Scope	<input type="radio"/>
Default to All Scope	<input type="radio"/>

Buttons: OK, Cancel

- 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 to import groups from your directory. See the [Operator's Guide](#) for details.

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

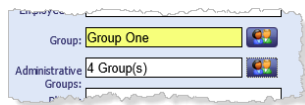
From the **Configuration** category, select **Security Settings**. The **Allow Administrative Groups** option is on the **Process** tab.

- 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**:

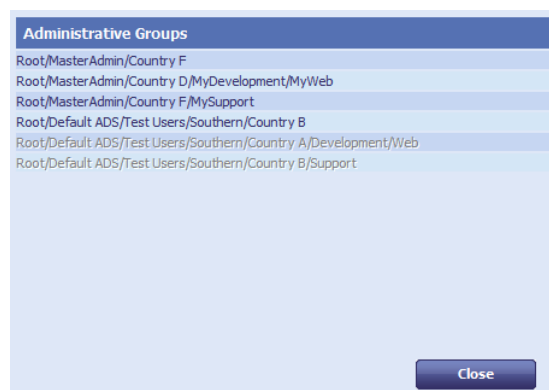
- When searching for people from the MyID database, the **Group** field in the Find Person stage of all workflows is not pre-populated with the operator's home group. This allows people to be found from the operator's home group as well as the operator's administrative groups.
- When searching for people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

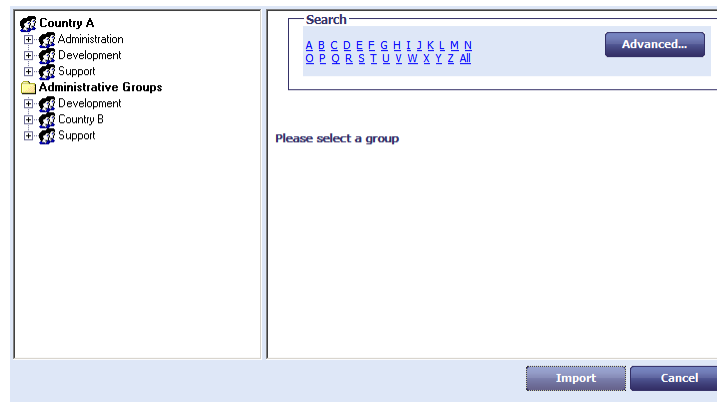
If a MyID group is deleted, the system will remove that group from the scope of all existing operators.

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.



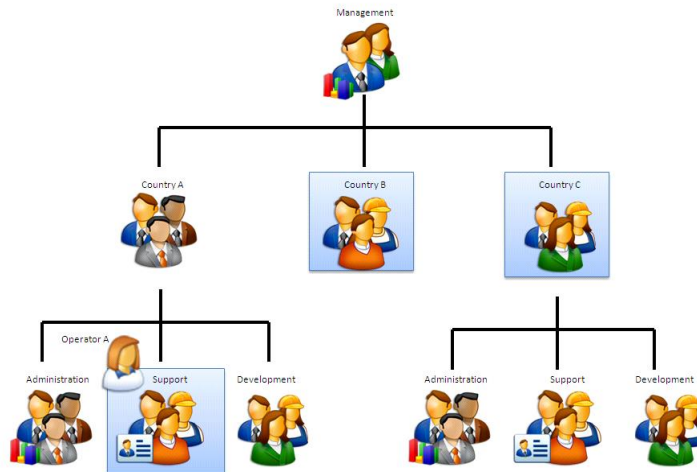
4.7.8 Scope calculations

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:

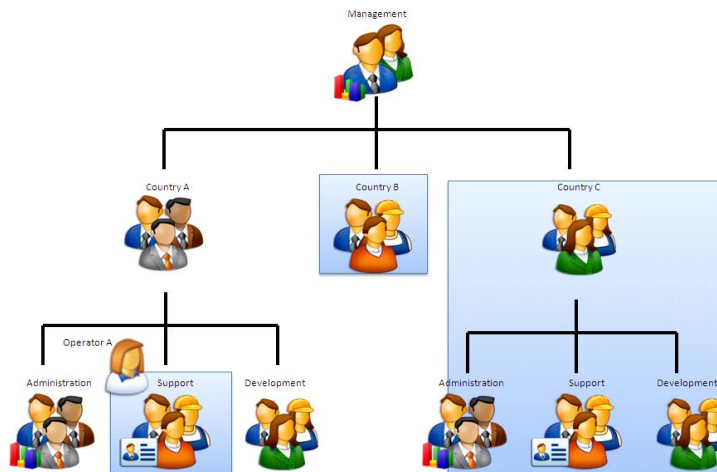
- Administrative group access to the **Country B** and **Country C** groups.
- **Division** rights for the **Registrar** role.
- **Department** rights for the **Issuer** role.

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 28.2, [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** 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 5.4, [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.

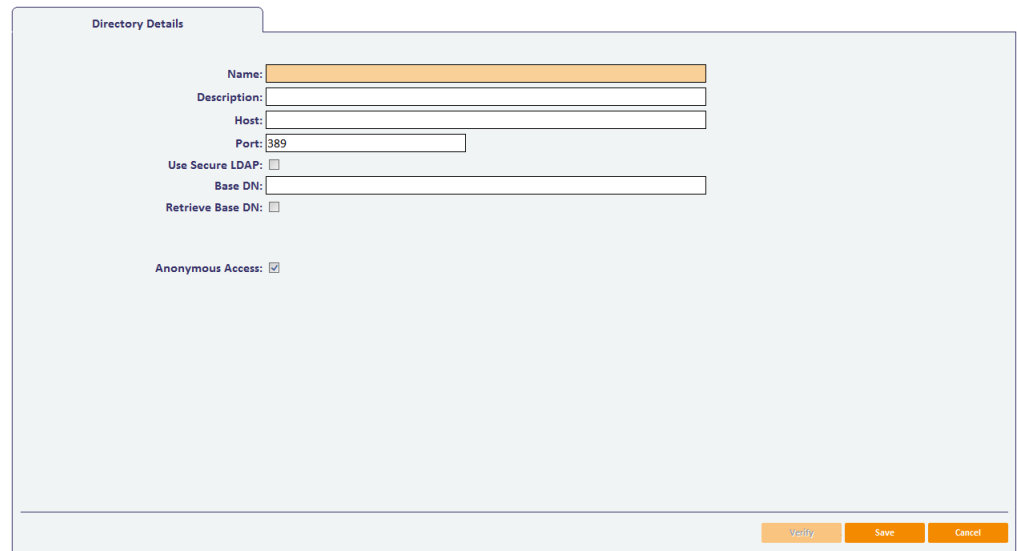
1. From the **Configuration** category, select **Directory Management**.
2. If there is a directory in the **Select Directory** box, information about it is displayed.

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.



Directory Details

Name:

Description:

Host:

Port:

Use Secure LDAP: ☐

Base DN:

Retrieve Base DN: ☐

Anonymous Access: ☒

Verify Save Cancel

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 [27.4, 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**.

Note: If this option is set to **Yes**, you cannot search the MyID database using, for example, the **View Person** workflow. If you want to be able to search the MyID database, set this option to **Ask** or **No**.

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.

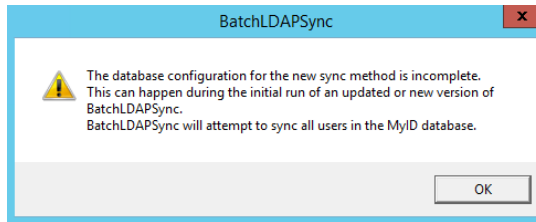
If the user account has been disabled in Active Directory, the user account in MyID can also be disabled and associated certificates suspended – you must set the **Disable on removal from directory** configuration option.

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:

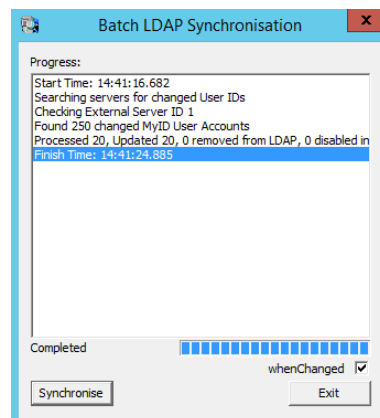
Disable on removal from directory	Revoke certificates if user is removed or disabled	Behavior
NO	NO	User in MyID is unaffected.
NO	YES	User in MyID is unaffected.
YES	NO	User is disabled in MyID. Associated certificates are unaffected.
YES	YES	User is disabled in MyID and associated certificates are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



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.

Note: The case of the command-line options is important. Use all lower-case; for example, use `-whenchanged`, not `-whenChanged`.

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**

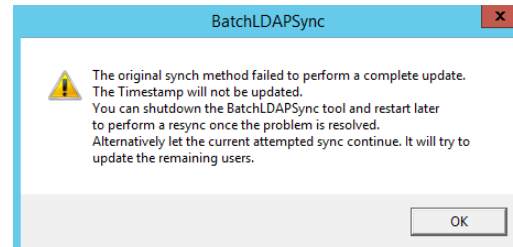
If you are running multiple instances of the Batch Directory Synchronization Tool concurrently, the total of updated users across all instances may not match the actual total of updated users – this is because the same update may be counted by more than one instance. The updates themselves are processed 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 [27.4, 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 `ADSSConfigPrefix` 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:

1. Connect to each of your configured Active Directory servers.
2. Checks for newly-deleted items on each of those servers.
3. Checks MyID for cardholders that match these deleted items.
4. 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.

5.8.1 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.

5.8.2 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.

6 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](#). 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.

6.1 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.
```

6.2 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 [6.3, *Enabling certificates on a CA*](#).

6.2.1 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**.

6.2.2 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**.

6.2.3 Deleting a CA

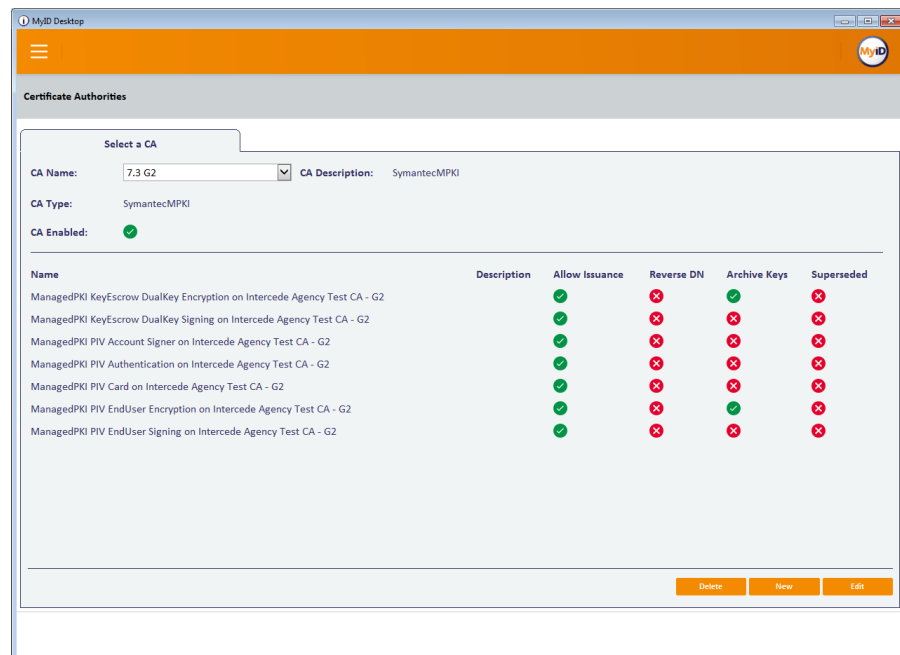
You can delete a CA from the list of available CAs if you no longer need to be able to work with it, or if you created it in error.

Notes:

- You cannot delete the Unmanaged CA.
- If any credentials have been issued that use policies from this CA, you cannot delete the CA.
- If there are policies on the selected CA that are being used by existing credential profiles, you cannot delete the CA. You must first edit or delete the credential profiles that refer to this CA.

To delete a CA:

1. From the **Configuration** category, select **Certificate Authorities**.
2. From the **CA Name** drop-down list, select the certificate authority you want to delete.



Name	Description	Allow Issuance	Reverse DN	Archive Keys	Superseded
ManagedPKI KeyEscrow DualKey Encryption on Intercede Agency Test CA - G2		✓	✗	✓	✗
ManagedPKI KeyEscrow DualKey Signing on Intercede Agency Test CA - G2		✓	✗	✗	✗
ManagedPKI PIV Account Signer on Intercede Agency Test CA - G2		✓	✗	✗	✗
ManagedPKI PIV Authentication on Intercede Agency Test CA - G2		✓	✗	✗	✗
ManagedPKI PIV Card on Intercede Agency Test CA - G2		✓	✗	✗	✗
ManagedPKI PIV EndUser Encryption on Intercede Agency Test CA - G2		✓	✗	✓	✗
ManagedPKI PIV EndUser Signing on Intercede Agency Test CA - G2		✓	✗	✗	✗

3. Click **Delete**.

6.3 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.
4. Click **Edit**.

3. Make sure **Enable CA** is selected.
4. From the list of **Available Certificates**, select the Certificate Policy you want to work with.
5. To enable the certificate, click **Enable (Allow Issuance)**.
6. 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.

7. 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.

6.4 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.

6.5 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**.

6.6 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 [13.3.1, 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.

6.6.1 Credential lifetimes and certificate renewal

The lifetime of the smart card, as configured in the credential profile, may have an effect on your certificate renewals.

- If the **Restrict certificate lifetimes to the card** configuration option is set to Yes, the certificates are issued with lifetimes that fall within the lifetime of the smart card. If this option is set to No, the renewed certificates may exceed the lifetime of the smart card.
- The **Card Renewal Period** configuration option determines whether you can request a renewed card or carry out automatic certificate renewals. By default this is set to 42; so, for example, if the card has 50 days left when the certificates expire, you cannot request a renewed smart card, but automatic certificate renewals take place; if the card has 30 days left when the certificates expire, you cannot automatically renew the certificates, but must request a replacement smart card instead.

Note: There is no automatic process for renewing smart cards like there is for renewing certificates. However, if the certificates expire within the Card Renewal Period window, this triggers a notification that the card holder must request a replacement smart card.

6.7 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.

☒ Enabled (Allow Issuance)

Display Name: SmartcardUser on VIN2012R2DC19

Description:

Allow Identity Mapping: ☐

Reverse DIT: ☐

Archive Keys: None

Certificate Lifetime: 365

Automatic Renewal: ☒

Certificate Storage: ☒ Hardware ☐ Software ☐ Both

Recovery Storage: ☒ Hardware ☐ Software ☐ Both ☐ None

Key Length: Default

Supersede

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

5. Click **Supersede**.

Please choose the superseding Certificate Authority.

CA Name	Select
VDEVW2K8ENDEVCA	<input type="radio"/>
ms2k3ca	<input type="radio"/>

Cancel

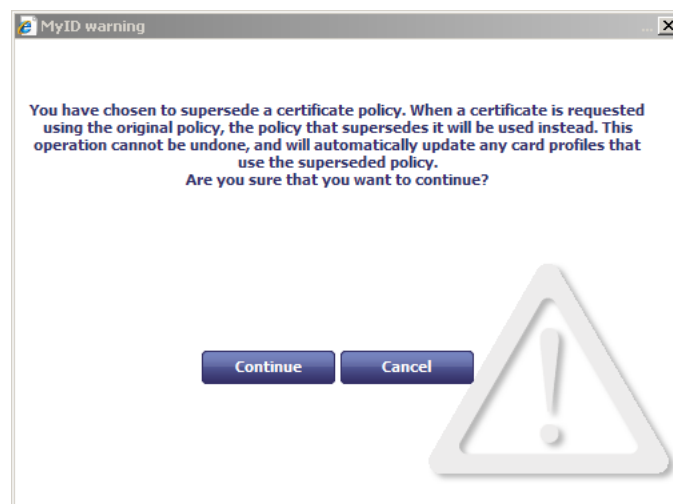
6. Select the certificate authority containing the certificate policy you want to use as a replacement.

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.

6.7.1 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.

6.7.2 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 constraint '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.

6.7.3 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.

Name	Description	Allow Issuance	Reverse DNI	Archive Keys	Superseded
PIVKeyManagement on ms2k3ca		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
PIVDigitalSignature on ms2k3ca		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
RequestSmartcardLogon on ms2k3ca		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
CAExchange on ms2k3ca		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
PIV1 on ms2k3ca		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
PIVContentSigning on ms2k3ca		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
PIVCardAuthentication on ms2k3ca		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
PIV4 on ms2k3ca		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
PIV3 on ms2k3ca		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
PIV2 on ms2k3ca		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
PIVEncryption on ms2k3ca		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
7DayEnrollmentAgent on ms2k3ca		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
OnlinePIVContentSigning on ms2k3ca		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
ClientAuthentication on ms2k3ca		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
ClientAuth on ms2k3ca		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

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.

6.8 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.

6.8.1 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 Imported 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.

6.8.2 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**.

6.8.3 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.

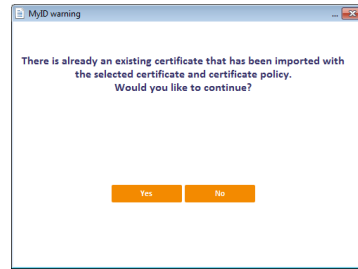
The list contains all enabled certificate policies that are currently assigned to the Unmanaged certificate authority. See section [6.8.1, Setting up the Unmanaged certificate authority](#) for details.

5. Click **Add**.

The certificate is uploaded to the MyID database, and stored ready to be issued when you request it.

Certificate Template	Certificate Serial Number	Issue Date (UTC)	Expiry Date (UTC)	File Name
Unmanaged	620000002209FDD724FCADB21C000100000022	2015-09-09 13:24:00	2016-09-08 13:33:57	test.pfx

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**.

6.8.4 Removing uploaded certificates


To remove an uploaded certificate:

1. From the **Certificates** category, select **Upload PFX Certificates**.

The "Upload PFX Certificates" interface shows fields for "PFX Certificate:", "PFX Password:", and "Certificate Policy:". Below these is a "Not" button. A section titled "Existing Certificates" contains a table with the following data:

Certificate Template	Certificate Serial Number	Issue Date (UTC)	Expiry Date (UTC)	File Name	
Unmanaged	620000002209FDD724FCADB21C000100000022	2015-09-09 13:24:00	2016-09-08 13:33:57		✖
Unmanaged	620000002209FDD724FCADB21C000100000022	2015-09-09 13:24:00	2016-09-08 13:33:57		✖

At the bottom right of the interface is a "Finish" button.

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**.

7 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 [11, 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

7.1 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.

7.2 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**.

7.3 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)

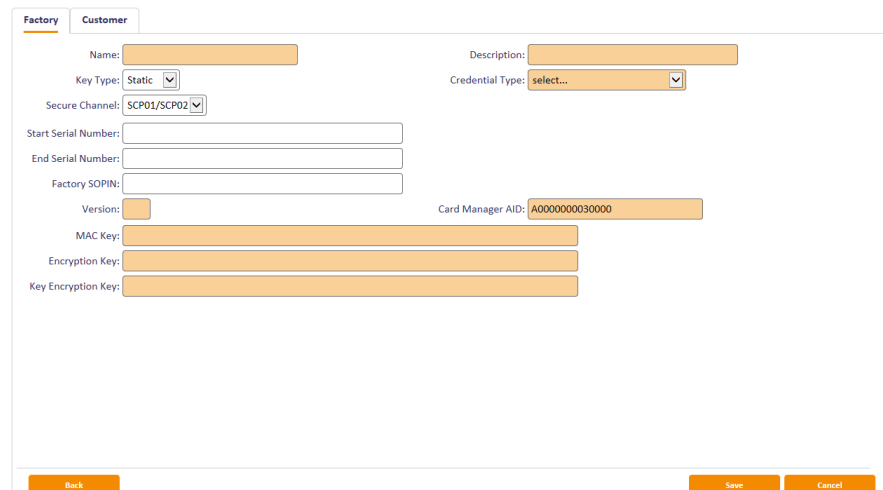
Note: If you are evaluating or testing MyID, you may choose to use the provided factory keys only. You can return to this workflow and add customer keys later.

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.

7.3.1 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. Optionally, you can include the **Key Checksum Value**.
 - **HSM Label** – type the label of an existing HSM-resident master key into the **HSM Label** field.
 - **Use Key Ceremony** – once you click **Save**, you enter the parts of the transport key and encrypted master key in a key ceremony.
 - **Import Keys from File** – once you click **Save**, 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 [7.3.4, 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.

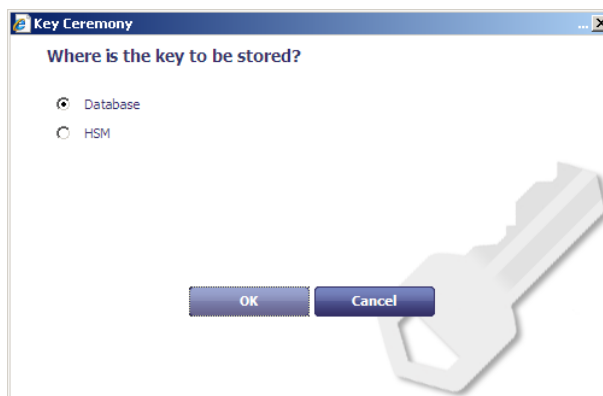
Note: If you need help in deciding which attributes to use, contact Intercede customer support quoting reference SUP-96.

13. Click **Save**.
14. If you are using the **Use Key Ceremony** or **Import Keys from File** options, you must now provide the keys. See section [7.3.2 Using a key ceremony](#) or section [7.3.3 Importing keys from a file](#).

7.3.2 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.

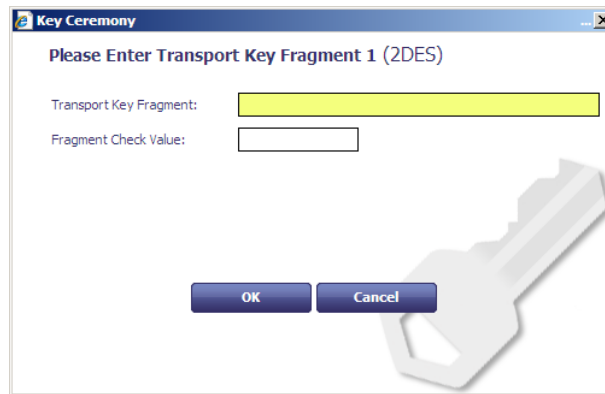


2. If you have previously stored a transport key using the **Key Manager** workflow, you can select this key from the **Existing** list, or select **New** to enter a new key.



See section [15.2, 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**.

7.3.3 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.

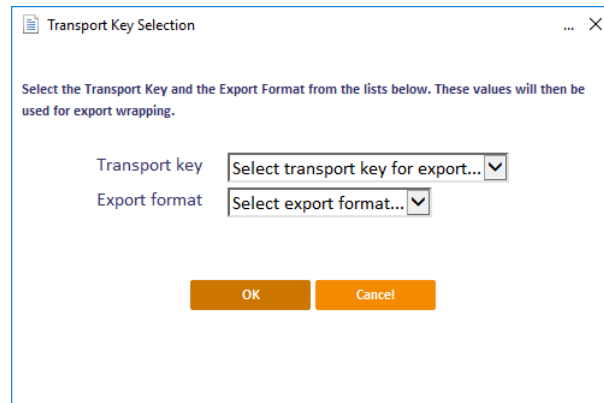
2. Click **Open**.

The key is now added to the database or HSM.

7.3.4 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.
5. Select the export format:
 - ♦ **XMLenc** – when you click **OK**, MyID saves the exported key to an XML file.
 - ♦ **KeyCeremony** – when you click **OK**, MyID saves the exported key to a text file containing the key name, type, algorithm, transport key, encrypted key value and the checksum.
6. Click **OK**, select the file to which you want to export the key, then click **Save**.

Note: There is a mandatory witness stage for key export. You must have another operator available who has the **Witness Key Export** permission under **Manage GlobalPlatform Keys** set up in the **Edit Roles** workflow.

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.

7.3.5 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**.

7.3.6 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 7.3.7, *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. Optionally, you can include the **Key Checksum Value**.
- **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 [7.3.4, 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 [7.3.2 Using a key ceremony](#) or section [7.3.3 Importing keys from a file](#).

7.3.7 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.

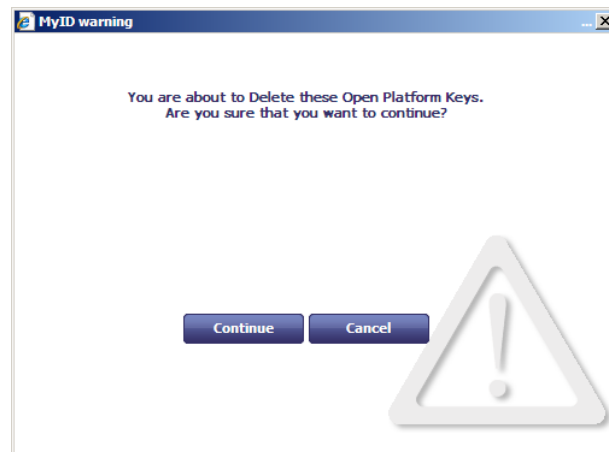
To delete a customer key:

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.

7.4 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.

7.4.1 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**.

7.4.2 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 [7.4.1, Add an applet](#)).

4. Click **Save**.

7.4.3 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**.

8 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.

8.1 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.

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.





8.2 Configuring the image location

Static images for card layouts (as inserted by the **Insert user image**  button) are stored on the MyID web server. If the web services server is not the same server as the web server, you must set the **Image Upload Server** configuration option. See the *Setting the location of the web server* section in the [Web Service Architecture](#) guide.

8.3 Creating, saving and deleting layouts

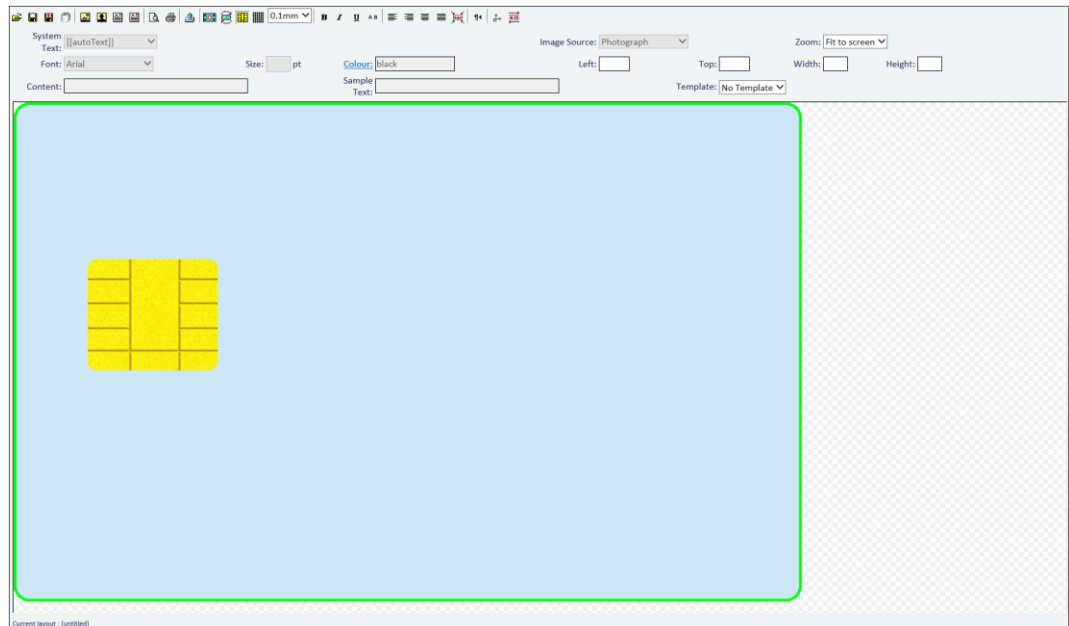
You can create a completely new layout or base a new layout on an existing one. You can also open an existing layout to make changes to it.

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 [8.4.1, 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**.
- To delete a layout, click the **Delete** button and select the template to delete from the list displayed. Click **Delete**.

8.4 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:



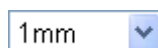
Rotate – rotates the card through 90°



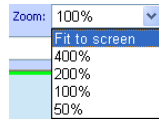
Show chip – toggles the display of the chip



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

8.4.1 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.

8.4.2 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.

8.4.3 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.

8.5 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.
- MyID supports printing of 24-bit JPEG images. If you have 32-bit JPEG images – for example, JPEG images using the YCCK color transform – you must save them as standard 24-bit JPEG images before adding them to a card layout.

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

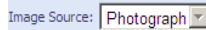


Image Source – choose which user image to use from the cardholder's record.



or



Maintain Aspect Ratio – choose whether the aspect ratio of the image is retained when the card layout is printed.

8.5.1 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.

8.5.2 Specifying a background

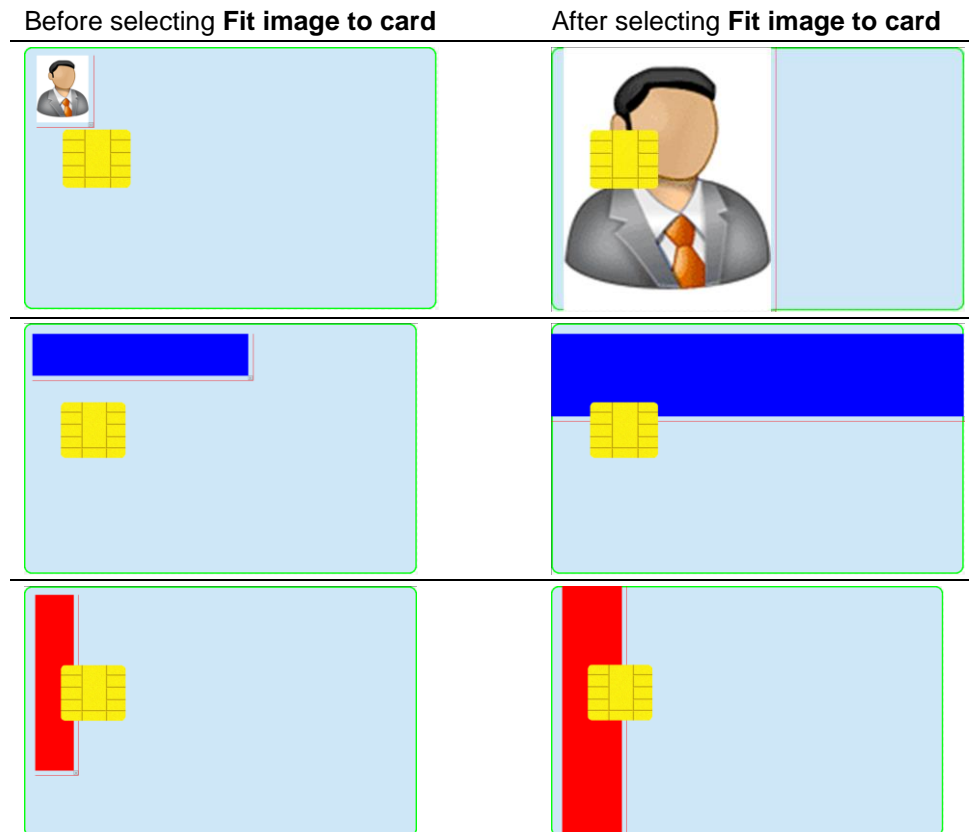
1. Click **Insert picture**.
2. Double-click the image you want to use in the list of images displayed.
3. If the image is not in the top left corner of the card outline, move it into position. Place your mouse over the image and the cursor changes to a four-headed arrow. Click and drag the image to 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.

8.5.3 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.



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.

8.5.4 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.

8.5.5 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.

8.5.6 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 8.6.3, *Custom text fields* for details. Any fields are substituted with the value for the user when the card is printed.

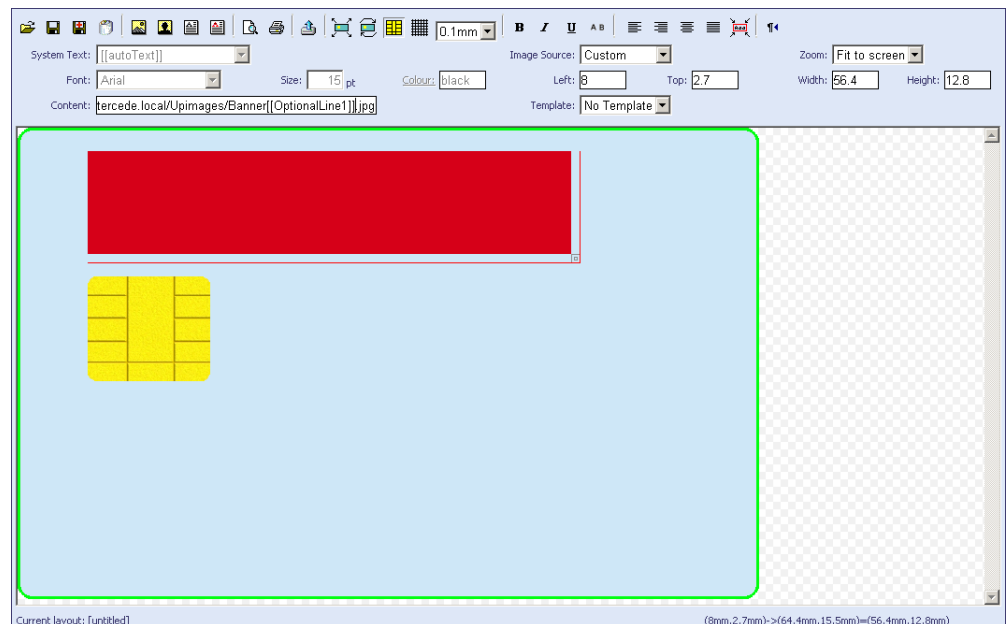
For example, if you have the following URL:

`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.



8.5.7 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**.

8.5.8 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.

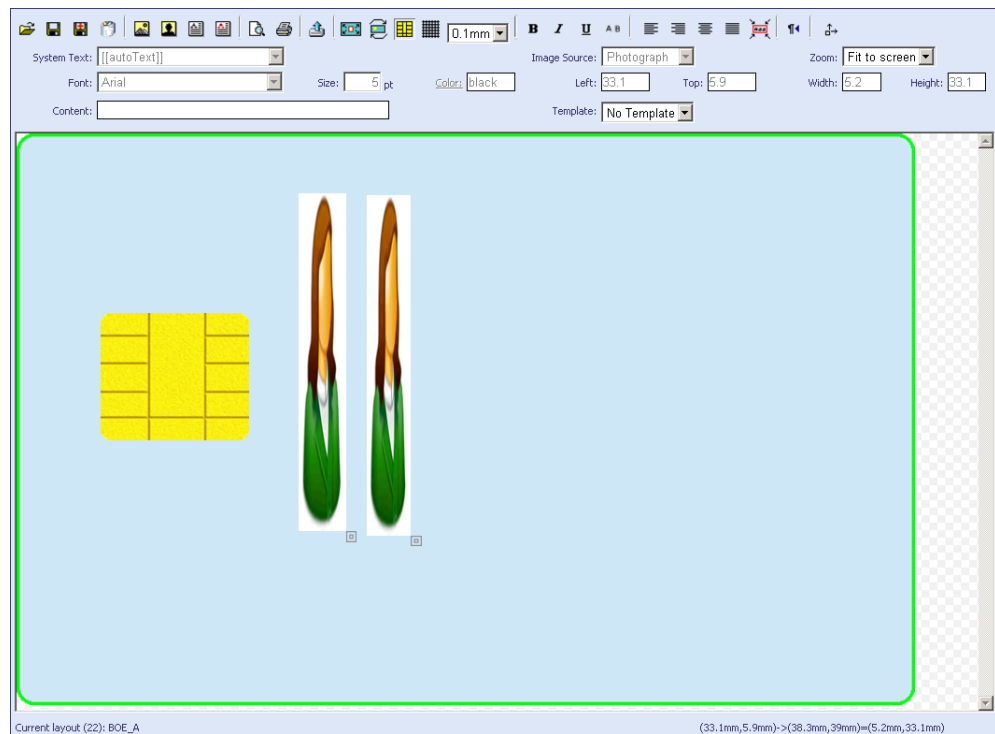


Maintain Aspect Ratio option is set for an on-screen element




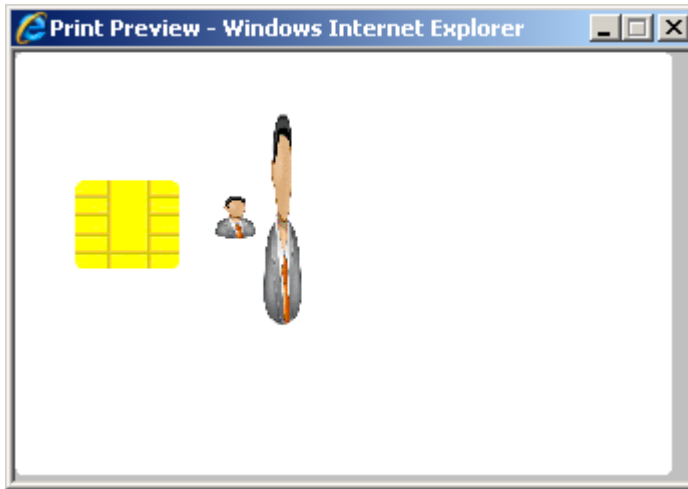
Maintain Aspect Ratio option is not set

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 right 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.

8.6 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
-  **Toggle Sample Text** – Changes auto text fields into sample text

8.6.1 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.

8.6.2 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.

To supply a representative sample value for the dynamic text to help you design your layouts, type into the **Sample Text** field. In cases where the created layout has dense information, you can make the sample text appear as a small string regardless of content by setting it to the Minimalist Text value; you can select this text more easily in densely-populated layouts.

To toggle between the **System Text** value, the **Sample Text** value, and the

Minimalist Text value, click the **Toggle Sample Text** button .

Note: To view sample text in the print preview, select the print preview when the **Sample Text** mode is active.

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.

8.6.3 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.

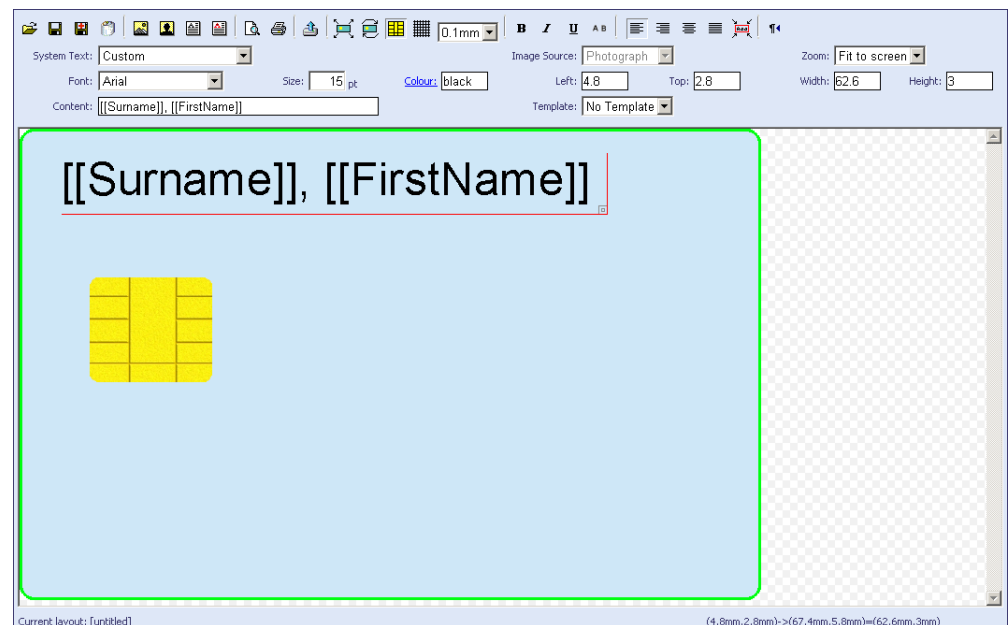
To find out what codes you can use, select the other entries in the **System Text** drop-down list and take a note of the code. Field codes are enclosed in double square brackets (`[[]]`).

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.



8.7 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 8.8, *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.

8.8 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.

8.8.1 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.

8.9 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:

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 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.

8.10 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.

8.11 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.

8.11.1 Applying zone settings

To apply a zone to an element:

1. 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.

2. Select an element on the card layout.
For example, select the user photograph.

3. 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.

8.11.2 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 *zone/label*) 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 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>

```

8.12 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]]]`.

9 PIN Generation

You can set up MyID to generate PINs on the server when you issue smart cards. Currently, you can select one of the following PIN generation algorithms:

- **EdeficePinGenerator** – creates a PIN using a known algorithm, a PIN generation key, and the card serial number as diversification data. You can regenerate the same PIN on another system as long as you have the algorithm, PIN generation key, and the card serial number. You can also set up MyID to issue a PIN notification email when the card is issued.
- **RandomPINGenerator** – uses a CNG random number generator to create a random numeric PIN that is guaranteed not to contain the user's logon name or employee ID. This PIN is not stored and cannot be regenerated. The **Issue Card** workflow displays the PIN on screen, but other issuance workflows do not display the PIN – you must set up MyID to issue a PIN notification email or print a PIN mailing document when the card is issued.

9.1 Adding a PIN Generation key

You require a PIN Generation key for PINs generated using the **EdeficePinGenerator** algorithm; this is *not* required for PINs generated using the **RandomPINGenerator** algorithm.

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**.

Add Key (PIN Generation Key)

Key Name: Description:

Encryption Type: 2DES

☐ Automatically Generate Encryption Key in Software and Store on Database
☒ Encryption Key: Key Checksum Value:
☐ Automatically Generate Encryption Key on HSM and Store on HSM
☐ Existing HSM Key Label:
☐ Use Key Ceremony

Key Attributes

Exportable ☐

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 [9.2, 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 [9.3, EdeficePinGenerator PIN generation algorithm](#).
 - ♦ **Encryption Key** – type the key into the box. Optionally, you can include the **Key Checksum Value**.
 - ♦ **Automatically Generate Encryption Key on HSM and Store on HSM** – this option generates a key on the HSM.
Note: The HSM options appear only if your system is configured to use an HSM.
 - ♦ **Existing HSM Key Label** – if you have an existing key on your HSM that you want to use, type its label.
 - ♦ **Use Key Ceremony** – click **Enter Keys** and provide the key in multiple parts. Alternatively, click **Import Keys** and select a file containing the key ceremony data.
8. Select the attributes for the key:
 - ♦ **Exportable** – the key can subsequently be exported.
See section [15.2.5, Exporting keys](#) for more information.
9. Click **Save**.

9.2 Credential profile setup for PIN generation

You must set up the **Server Generated PIN** options in the credential profile to specify server-side PIN generation. See PIN Settings in section [11.3.1, Credential profile options](#).

Note: You are recommended to set the **PIN Settings** and **PIN Characters** options in the credential profile to match the PINs that the PIN generation algorithm will produce. 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, but you are recommended to make sure the options match the generated PINs to prevent any conflict with the PIN rules on the card.

9.3 EdeficePinGenerator PIN generation algorithm

The **EdeficePinGenerator** PIN generation algorithm uses the card serial number as diversification data. The PIN generation key is used to generate the PIN. If you have the card serial number, the same 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.

9.3.1 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 [9.3.2, 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'`

9.3.2 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.

9.3.3 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:

$$78 \text{ (hex)} = 120 \text{ (dec)} \bmod 10 = 0$$

$$49 \text{ (hex)} = 73 \text{ (dec)} \bmod 10 = 3$$

$$DE \text{ (hex)} = 222 \text{ (dec)} \bmod 10 = 2$$

$$09 \text{ (hex)} = 9 \text{ (dec)} \bmod 10 = 9$$

$$B2 \text{ (hex)} = 178 \text{ (dec)} \bmod 10 = 8$$

$$59 \text{ (hex)} = 89 \text{ (dec)} \bmod 10 = 9$$
5. The PIN returned is 032989.

C# example

The following is sample code that generates PINs using C#.

```
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 = "";
```

```

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) %
alphabet.size];
}

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: " + alphabet.size);
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);
}
}
}

```

10 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.

10.1 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.

11 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 [11.2, 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 6, [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 7, [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 8, [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.

11.1 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 [28.5, PINs page \(Security Settings\)](#)

11.2 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 [11.1, 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.

11.3 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.

11.3.1 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.

You can also specify a **Device Friendly Name** that will be displayed during card selection operations in the Self-Service App to help users select the appropriate card.

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 [11.3.2, 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 [11.5, 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 [24.6, 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 following options:

- **MyID Logon** – select this option if you want the credentials to be used to logon to MyID.
- **MyID Encryption** – select this option if you want to be able to encrypt data.

If you want to issue archived certificates, you must select the **MyID Encryption** service.

You can select certificates to be mapped to these services; the signing certificate is used for MyID Logon, and the encryption certificate is used for MyID encryption.

If no certificates are mapped to the logon and encryption services, an additional Manager Keypair is generated on the smart card for these services.

Note: Not all cards or devices support manager keypairs. You are recommended to select certificates for signing and encryption.

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 Cancellation**

If you set this option, credentials issued using this profile will require secondary authorization when you cancel them.

- **Lifetime**

The **Lifetime** setting determines the number of days for which the credentials will be valid. The initial default value is 365 days. Mandatory.

Note: You can also choose to set an explicit expiry date at the point at which you request the card, rather than when you set up the credential profile; see the [Setting expiry dates for a card](#) section in the [Operator's Guide](#) for details.

Note: You must make sure that the lifetime of the credential is appropriate for your purposes; once the credential expires, you can no longer issue new certificates to the card, and you must request a replacement (for example, using the **Request Replacement Card** workflow); collecting the replacement (even to the same physical smart card) resets the credential lifetime and issues new certificates.

If you do not require a fixed lifetime, and do not want to request card replacements periodically, you are recommended to set a **Lifetime** value of 999999 and use the certificate renewal process to refresh the credentials.

The lifetime also affects the renewal of certificates; section [6.6.1, Credential lifetimes and certificate renewal](#).

- **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 [10, 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 [26, Additional Identities](#).

- **Key Recovery Only**

Used for key recovery operations. See section [18, Key Recovery](#) for details.

- **Require Activation**

Used for card activation. See section [23, Activating Cards](#) for details.

- **Pre-encode Card**

Used for card activation. See section [23, 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 [23.2, Terms and conditions](#).

- **Credential Group** – see [11.3.2, 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 [10, 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 [24.9, Requesting a device identity](#) for details.

- **Unrestricted Cancellation**

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 cancellation 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 Cancellation** option is listed as **Not Issued** on the card selection screen.

This option appears only if the **Enable unrestricted cancellation** option on the **Issuance Processes** tab of the **Operation Settings** workflow is set to **Yes**.

- **OPACITY**

Select one of the following options:

- ♦ **None** – Do not attempt to perform OPACITY personalization.
- ♦ **OPACITY without Pairing Codes** – Personalize the OPACITY CVC but do not set an OPACITY pairing code.
- ♦ **OPACITY with Pairing Codes** – Personalize the OPACITY CVC and generate and set an OPACITY pairing code.

For more information on setting up OPACITY, see the [Smart Card Integration Guide](#).

- **Send Pairing Code Emails**

When the card is issued, send an email to the cardholder containing the OPACITY pairing code.

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.

Note: You must make sure that the PIN settings you select match the capabilities of the smart cards you are issuing. Note also that some workflows within MyID (for example, batch and activation workflows) may generate temporary random PINs for the card, based on the settings you have specified in the **PIN Settings** section of the credential profile; if these settings do not match the PIN capabilities of the smart card, the batch issuance or encoding may fail.

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 sequential characters.
- **Logon Attempts (5)**

Set to the number of incorrect PINs you can enter before the card is locked.

Note: This setting is supported only for cards that support on-card PIN policy settings; see the [Smart Card Integration Guide](#) for details.
- **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. If your smart cards support this feature, it will be specified in the *PIN policy settings* section of the appropriate chapter in the [Smart Card Integration Guide](#).

- 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 9, [PIN Generation](#) for more information. Complete the following details:
 - **Length** – the length of the generated PIN. The maximum length is 16 characters.
 - **PIN Algorithm** – select the PIN generation algorithm. You can select one of the following:

EdeficePinGenerator – creates a PIN using a known algorithm, a PIN generation key, and the card serial number as diversification data. You can regenerate the same PIN on another system as long as you have the algorithm, PIN generation key, and the card serial number.

RandomPINGenerator – creates a random numeric PIN that is guaranteed not to contain the user's logon name or employee ID. This PIN is not stored and cannot be regenerated; additionally, only the **Issue Card** workflow displays the PIN on screen – if you are using any other workflows to issue the card, the PIN is never displayed; this means that you must set up MyID to issue a PIN notification email when the card is issued.
 - **Protected Key** – select the PIN generation key you added using the Key Manager workflow. This option is required for **EdeficePinGenerator** but not for **RandomPINGenerator**.

- **Email PIN**

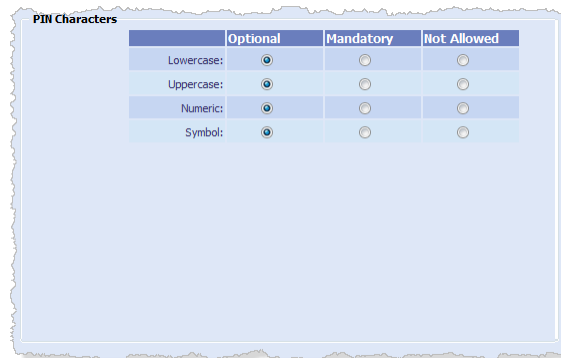
To email the PIN to the user when the card is issued, select the **Email PIN** option. This option is available only when the **Issue With** option is set to **Client Generated PIN** or **Server Generated PIN**.

Important: If you are using the **RandomPINGenerator** algorithm for server generated PINs, the PIN is displayed on screen only during the **Issue Card** workflow – if you are using any other workflows to issue the card, you *must* do one of the following:

- ♦ Select the **Email PIN** option, and configure MyID to send email notifications; if you do not email the PIN to the cardholder when the card is issued, it is not possible to determine the PIN.
- ♦ From the **Select PIN Mailing Document** option, 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.

PIN Characters

Specify the type of characters that must, may or must not be contained in the PIN.



	Optional	Mandatory	Not Allowed
Lowercase:	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Uppercase:	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Numeric:	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Symbol:	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

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 [11.4, 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.

You can also use this mailing document to provide OPACITY pairing codes. See the [Smart Card Integration Guide](#) for details.

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.

11.3.2 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 Authenticate virtual smart cards. See the [Intel Authenticate Integration Guide](#) for details.

Credential group

If you have set the **Active credential profiles per person** configuration option (see section 27.11, [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.

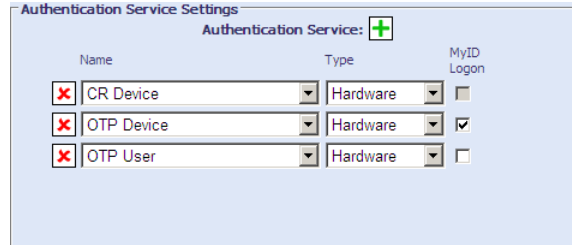
Note: These options are only displayed if token logon is enabled.




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.



Name	Type	MyID Logon
 CR Device	Hardware	<input checked="" type="checkbox"/>
 OTP Device	Hardware	<input checked="" type="checkbox"/>
 OTP User	Hardware	<input checked="" type="checkbox"/>

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

Scenario	Require Fingerprints at Issuance	Additional Authentication
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. Make sure the **Enable additional authentication options** option is set 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.

11.3.3 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.

This option determines which key is used to protect sensitive data such as archived keys in transit to the client:

- For PIV cards, this key is not used for archived certificates; however, you must still select the **MyID Encryption** in the **Services** section of the credential profile, and select a certificate to be used for encryption.
- For cards that use minidrivers, this key is used for protecting archived key material, and must be an RSA key that supports signature and key exchange. If you attempt to use an ECC key or a signature-only key, archived certificate issuance will fail.

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**.

11.3.4 Selecting applets

Select the applets you want to copy onto the card. Click **Next**.

For more information about applets, see section 7, [Applets](#).

11.3.5 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.

11.3.6 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.

11.3.7 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.

11.3.8 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.

11.3.9 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.

11.3.10 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 be 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 8.2, [Configuring the image location](#).

Click **Next**.

11.3.11 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.

11.4 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.

11.5 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**.

11.6 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

11.6.1 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.

11.6.2 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.

11.6.3 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 & 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>
```

11.6.4 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.

11.6.5 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.

12 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 [12.4, 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 its 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.

12.1 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 [12.2, Requesting licenses](#)
- **Install** received license information – see section [12.3, Installing license details](#)
- **Update Warning** messages – see section [12.4, Updating warning messages](#)

12.2 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.

12.3 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**.

Note: The message about your license expiry on the MyID Desktop dashboard will disappear after you log out and log back in again.

12.4 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**.

13 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 [Advanced Configuration Guide](#) for details.

13.1 System-wide email settings

13.1.1 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.

13.1.2 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**.

13.1.3 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 [13.1.2, 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">
```


13.1.4 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**.

13.1.5 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 [12.4, 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.

13.1.6 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**.

13.2 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 [13.1.2, 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 [13.1.3, 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**.

13.3 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 a user who has an update for their card waiting	6
Apply Update Notification Mobile	Sent to the user when update are ready for collection onto their mobile devices	142
Authentication Code	Authentication code for account	27
Authentication Code Notification	Authentication code notification	26
Automatic Job Cancellation Email	Sent to the issue card request recipient when a issuance job is cancelled because it has not been collected in time.	113
Cancel Card Notification	Sent to a user whose card has been cancelled	5
Card PIN Notification	Sent to inform a user of their new PIN number	11
Certificate Authority Status	Certificate authority status	106
Certificate Server Recovered	Sent when MyID has recovered from a certificate server error	157
Certificate Server Status	Sent when an error is encountered communicating with a certificate server	156
CertificateExpired	Sent when a certificate has expired	153
CertificateExpiring	Sent when a certificate is about to expire	152
Credential Licence Limit approaching	Sent to an administrator when the system is approaching the license limit	135
Credential Licence Limit exceeded	Sent to an administrator when the system has exceeded its license limit	136
Credential Licence Limit reached	Sent to an administrator when the system has reached license limit	137
CredentialExpired	Sent when a credential has expired	155
CredentialExpiring	Sent when a credential is about to expire	154
DC Job Logon Code	Sent to the user when their smart card is ready for collection	147
Email signing certificate invalid	Send when an application servers email signing certificate is incorrectly configured, or not present.	145
Failed Email Notification	Sent to an administrator when an email has failed to send	12
Issue Card Notification	Sent to a user who has a card awaiting issuance	4
Issue Token Notification	Sent to a user who has a token awaiting issuance	7
Job Logon Code	Sent to the user when their smart card is ready for collection	134
Job OTP	Sent to the user for Job based OTP	131
Job OTP No Device	Sent to the user when their job is ready for collection	138

Template Name	Description	ID
Job OTP With Device	Sent to the user when their job is ready for collection	139
Licence Limit approaching	Sent to an administrator when the system is approaching the license limit	8
Licence Limit exceeded	Sent to an administrator when the system has exceeded its license limit	9
Licence Limit reached	Sent to an administrator when the system has reached license limit	10
Logon Code Notification	Logon code notification	104
LogonCodeLockout	Sent to the user when their logon code is answered incorrectly too many times it becomes locked	140
Mobile Provisioning	Email sent during Request ID when Email option selected	124
Mobile Provisioning Code	Sent during mobile provisioning to authenticate the phone recipient.	141
Mobile Soft Certificate Validated	Mobile soft certificate validated	120
Notification Failed	URL notification failure	111
Notification Failure	URL notification failure	105
Notification Success	URL notification success	107
QALockout	Sent to the user when their security questions are answered incorrectly too many times and their security phrases become locked	132
Renew Card Notification	Sent to the card recipient when a card is approaching its expiry date	121
Renew Card Notification First	Sent to the card recipient when a card is approaching its expiry date	122
Renew Card Notification Second	Sent to the card recipient when a card has expired	123
Renew Certificate Notification	Sent to the certificate recipient when a certificate has expired	3
Renew Certificate Notification Expired	Sent to the certificate recipient when a certificate has expired	127
Renew Certificate Notification Expired Mobile	Sent to the certificate recipient when a certificate is approaching its expiry date	130
Renew Certificate Notification First	Sent to the certificate recipient via SMS when a certificate is approaching its expiry date	1
Renew Certificate Notification First	Sent to the certificate recipient when a certificate is approaching its expiry date	125
Renew Certificate Notification First Mobile	Sent to the certificate recipient when a certificate is approaching its expiry date	128
Renew Certificate Notification First Mobile	Sent to the certificate recipient when a certificate is approaching its expiry date	200
Renew Certificate Notification Second	Sent to the certificate recipient when a certificate is approaching its expiry date	2
Renew Certificate Notification Second	Sent to the certificate recipient when a certificate is approaching its expiry date	126

Template Name	Description	ID
Renew Certificate Notification Second Mobile	Sent to the certificate recipient when a certificate is approaching its expiry date	129
Replacement Card Notification	Sent to a user who has a card replacement awaiting issuance	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
ServicePasswordExpired	Sent when a user account has expired	151
ServicePasswordExpiring	Sent when a user account is about to expire	150
Software Certificate Notification	Sent to a user who has a pending software certificate request	112
Time Licence Expired	Sent to inform the admin their time based license has expired	101
Time Licence Expiring	Sent to inform the admin of impending time based license expiry	100
Unlock Code	Unlock code for account	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.

13.3.1 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. No longer used. This notification appears only on upgraded systems.
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

Days left	Email template	Description
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
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.

13.4 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.

Token	Description
%2, %3 and so on	<p>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.</p> <p>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:</p> <pre>{%parameter:URI}</pre> <p>For example, {%logonName:URI} might become Jane+Smith.</p> <p>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.</p>

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

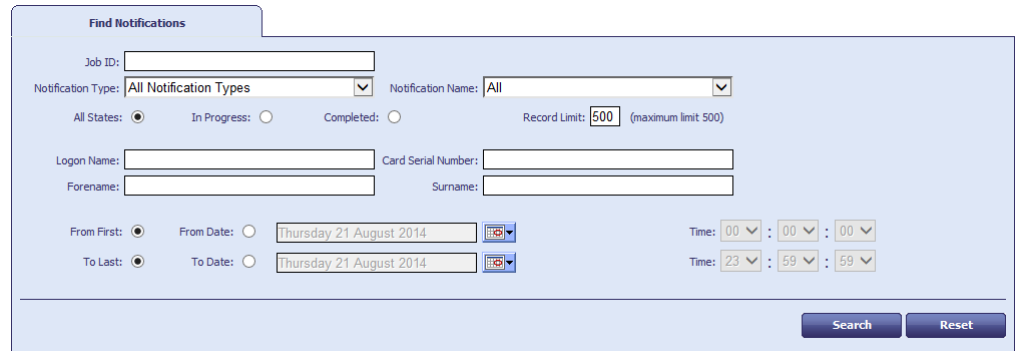
- **IKB-238 – Duplicate email template names will prevent a notification from being sent.**

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.

13.5 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.
 - **SMS** – returns notifications that are sent to a mobile phone.
 - **SNMP** – returns notifications that are sent to an SNMP Trap Listener.
 - **URL** – returns notifications that are sent to a web listener.
 - **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 can resend email notifications that have completed in the following cases:

- ♦ The notification is linked to a job that has not been deleted.
- ♦ The notification is linked to a job, and the job status is not one of the following:
 - Completed
 - Completed With Errors
 - Cancelled
 - Failed
 - AutoDisabled

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.

14 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.

15 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 application keys, transport keys, PIN generation 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 [7.3, Manage GlobalPlatform keys](#) for details.

15.1 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](#).

15.2 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.

For information about PIN generation keys, see section [9.1, Adding a PIN Generation 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 *SP800-73-4 – 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 [9, 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 the HSM are business critical data.
-----------------	---

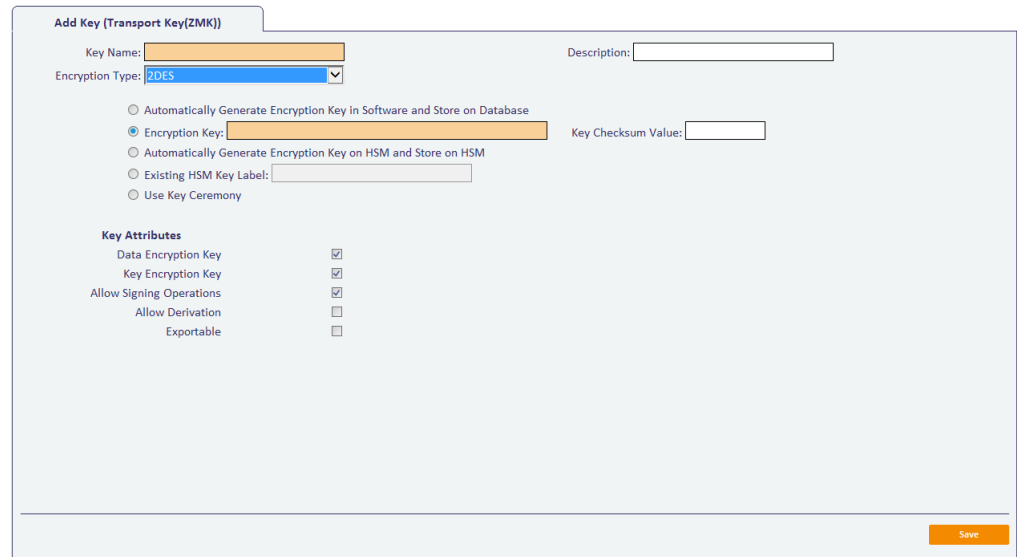
15.2.1 Transport keys

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.
- ♦ **Allow Derivation** – the key can be used to derive individual keys.
- ♦ **Exportable** – the key can subsequently be exported.

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.
- ♦ **Encryption Key** – type the key into the box. Optionally, you can include the **Key Checksum Value**.
- ♦ **Automatically Generate Encryption Key on HSM and Store on HSM** – this option generates a key on the HSM.

Note: The HSM options appear only if your system is configured to use an HSM.

- ♦ **Existing HSM Key Label** – if you have an existing key on your HSM that you want to use, type its label.
- ♦ **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).

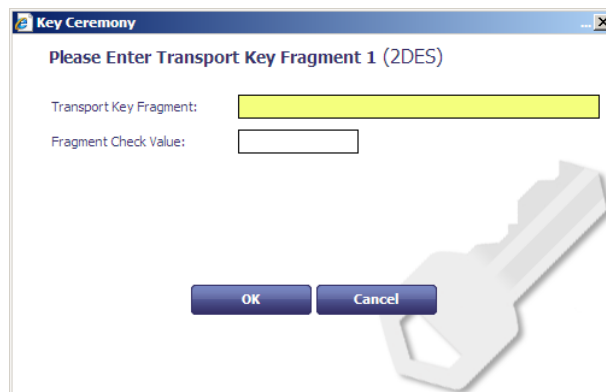
To enter the key using a key ceremony:

- a) Click **Enter Keys**.
- b) 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.



- c) Select the location, then click **OK**.



- d) 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.
- e) Click **OK**, then enter the second and third parts of the transport key.
Alternatively, to import the key from an XML file:
- Click **Import Keys**.
 - Select the file containing the key information, then click **Open**.
- Note:** The file must be in `XMLenc` format.
- 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.

15.2.2 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.

- From the **Configuration** category, select **Key Manager**.
- From the **Select Key Type to Manage** list, select **PIV 9B Card Administration Key** and click **Next**.
- Click **Add New Key**.
- 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 subsequently be exported.
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. Optionally, you can include the **Key Checksum Value**.
 - ♦ **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**.

15.2.3 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 subsequently be exported.
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. Optionally, you can include the **Key Checksum Value**.
 - ♦ **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.

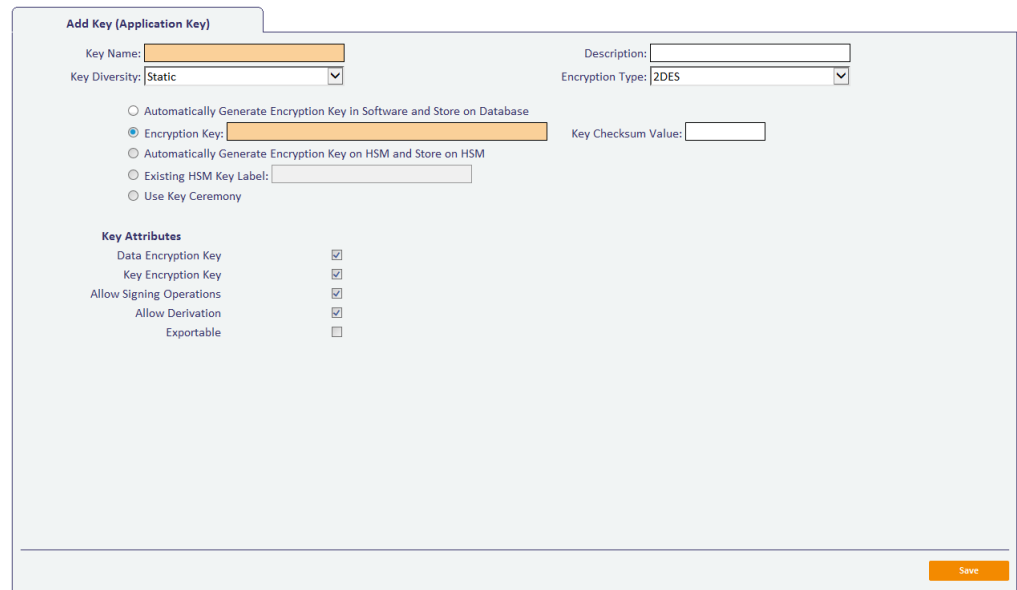
Note: If an HSM is available, Intercede recommends it is used as it provides stronger protection for the key.
11. Click **Save**.

15.2.4 Application keys

Application keys are used to secure parts of the MyID application; typically, they are used for custom functionality. Your system may have been customized with a pre-set selection of key names for use with this functionality.

To add an application key:

1. From the **Configuration** category, select **Key Manager**.
2. From the **Select Key Type to Manage** drop-down list, select **Application Key**.
3. Click **Next**.
4. Click **Add New Key**.



Add Key (Application Key)

Key Name: Description:

Key Diversity: Encryption Type:

☐ Automatically Generate Encryption Key in Software and Store on Database
☒ Encryption Key: Key Checksum Value:
☐ Automatically Generate Encryption Key on HSM and Store on HSM
☐ Existing HSM Key Label:
☐ Use Key Ceremony

Key Attributes

Data Encryption Key	<input checked="" type="checkbox"/>
Key Encryption Key	<input checked="" type="checkbox"/>
Allow Signing Operations	<input checked="" type="checkbox"/>
Allow Derivation	<input checked="" type="checkbox"/>
Exportable	<input type="checkbox"/>

5. Type the **Key Name** and **Description**.
6. Select an option from the **Key Diversity** drop-down list.
You can choose **Static**, which uses the same key for all purposes, or one of the **Diverse** options, which use a diversification algorithm for the key.
7. Select the type of encryption from the **Encryption Type** drop-down list.
8. 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.
 - ♦ **Encryption Key** – type the key into the box. Optionally, you can include the **Key Checksum Value**.
 - ♦ **Automatically Generate Encryption Key on HSM and Store on HSM** – this option generates a key on the HSM.
Note: The HSM options appear only if your system is configured to use an HSM.
 - ♦ **Existing HSM Key Label** – if you have an existing key on your HSM that you want to use, type its label.
 - ♦ **Use Key Ceremony** – click **Enter Keys** and provide the key in multiple parts. Alternatively, click **Import Keys** and select a file containing the key ceremony data.
9. 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.
 - ♦ **Allow Derivation** – the key can be used to derive individual keys.
 - ♦ **Exportable** – the key can subsequently be exported.

See section [15.2.5, Exporting keys](#) for more information.
10. Click **Save**.

15.2.5 Exporting keys

If your key has been created using the **Exportable** option, you can export it using the **Key Manager** workflow.

To export a key:

1. From the **Configuration** category, select **Key Manager**.
2. From the **Select Key Type to Manage** drop-down list, select the type of key you want to export, and click **Next**.

Existing Keys				
Export Key	Key Name	Version	Description	Key Checksum Value
<input type="radio"/>	Gem csd	1		D2E732
<input type="radio"/>	GemCSD	2		46A423
<input type="radio"/>	PinGen	1		1BA44F

Keys that are exportable have a radio button available in the **Export Key** column.

3. Select the key you want to export.
4. Click **Export**.

Transport Key Selection

Select the Transport Key and the Export Format from the lists below. These values will then be used for export wrapping.

Transport key

Select transport key for export...

Export format

Select export format...

OK

Cancel

5. Select the transport key you want to use to encrypt the key.
6. Select the export format:
 - ♦ **XMLenc** – when you click **OK**, MyID saves the exported key to an XML file.
 - ♦ **KeyCeremony** – when you click **OK**, MyID saves the exported key to a text file containing the key name, type, algorithm, transport key, encrypted key value and the checksum. For transport keys, MyID saves the exported key to three different text files containing fragments of the transport key; you can distribute these fragments to three trusted custodians, who can subsequently combine their fragments to import the transport key into another system.
7. Click **OK**, select the file to which you want to export the key, then click **Save**.

Note: There is a mandatory witness stage for key export. You must have another operator available who has the **Witness Key Export** permission under **Key Manager** set up in the **Edit Roles** workflow.

16 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 [16.3, *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 [Advanced Configuration Guide](#) for details of setting up an archive database for these purposes.

16.1 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	<input checked="" type="checkbox"/>
Audit Reporting	<input checked="" type="checkbox"/>
View Full Audit	<input checked="" type="checkbox"/>
MI Reports	<input type="checkbox"/>
System Events	<input type="checkbox"/>
System Status	<input type="checkbox"/>

- 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	<input checked="" type="checkbox"/>
-----------------	-------------------------------------

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.

16.2 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:

- From the **Reports** category, select **Audit Reporting**.
- 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.



- 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.

16.2.1 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 card issuance 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.

16.2.2 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:



16.3 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.

17 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.

17.1 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.

17.2 Cards supported

Archived keys are only supported by cards that support certificates.

17.3 Certificate authority key archiving

Some certificate authorities support key archiving. The key is archived within the certificate authority rather than within the MyID database.

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](#).

17.4 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.

17.5 Setting up key archiving

Use the **Certificate Authorities** workflow in MyID to set up key archiving.

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

Name	Description	Allow Issuance	Reverse DN	Archive Keys
KeyRecoveryAgent on DEVGENERALCA		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
UserSignature on DEVGENERALCA		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
ExchangeUserSignature on DEVGENERALCA		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
ExchangeUser on DEVGENERALCA		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
ExchangeUserwithArchival on DEVGENERALCA		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
RequestSmartcardLogon on DEVGENERALCA		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
RequestSmartcardUser on DEVGENERALCA		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
RequestedSmartcardUser on DEVGENERALCA		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Server on DEVGENERALCA		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
PIV4 on DEVGENERALCA		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
SmartcardLogon on DEVGENERALCA		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
SmartcardUser on DEVGENERALCA		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
EnrollmentAgent on DEVGENERALCA		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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.

18 Key Recovery

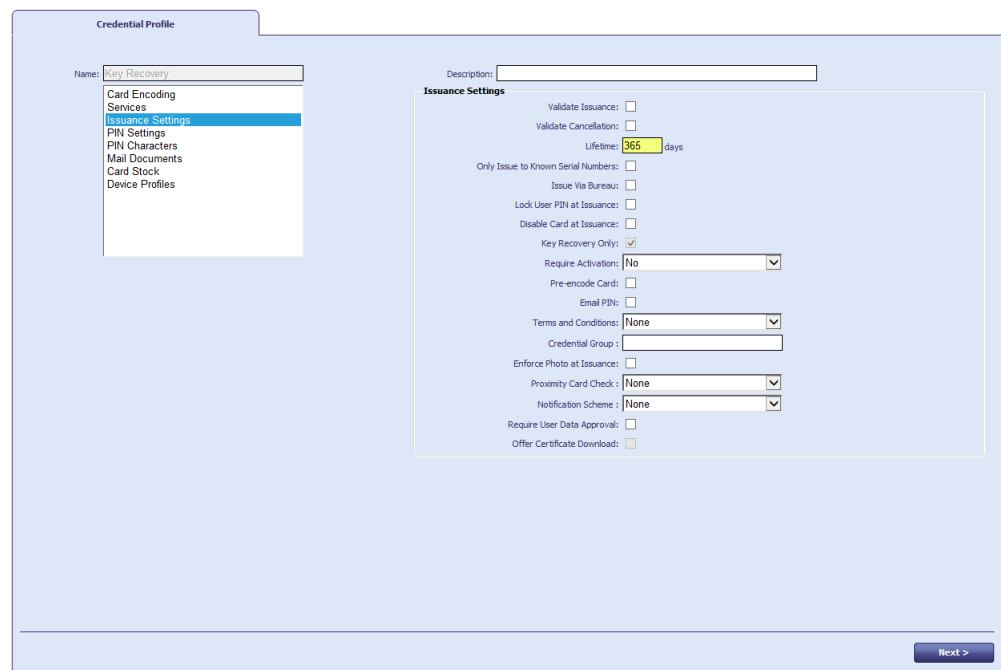
MyID allows you to set up a credential profile for smart cards that are used to collect recovered keys. The smart cards are not fully-featured MyID cards; they are used only to collect recovered keys.

18.1 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.

18.2 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 [18.3, 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 [18.4, Collecting a key recovery job for another user](#) for details.

- **IKB-248 – Cannot cancel key recovery jobs that are awaiting issue**

If you request recovery of a certificate using the **Request Key Recovery** workflow, there is currently no method of canceling the job once it is ready for collection; for example, if the request has no approval step required, or approval has already been given.

To prevent collection from taking place, disable the user account that was designated as the Key Recovery Recipient when the request was created; this will prevent collection from taking place. You can identify the recipient using the **View Key Recovery** workflow. For guidance on cancelling the job, contact customer support quoting reference IKB-248.

18.3 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.

18.4 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 [18.3, 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.

18.5 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 [18.3, *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.

18.6 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**.

Select Job

Rows: Auto Page 1 of 1

	ID	Job For	Requested By	Request Date	Validator	Validation Date	Status	Task Type
<input type="radio"/>	121	Angel Makin	startup user	03 July 2014			Awaiting Issuance	Recover archived certificates
<input type="radio"/>	122	Angel Makin	startup user	03 July 2014			Awaiting Issuance	Recover archived certificates
<input type="radio"/>	123	Angel Makin	startup user	03 July 2014	Angel Makin	03 July 2014	Awaiting Issuance	Recover archived certificates

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.

19 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**.

20 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.

21 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.

The screenshot shows a window titled "Configure Logon Providers". Inside, there are two dropdown menus. The first, labeled "Logon Provider:", has "TestLogon" selected. The second, labeled "External System:", has "Test" selected. Below these is a large empty rectangular area. At the bottom right, there are two buttons: "Save" and "Cancel".

3. Click **Save**.

22 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.

22.1 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**.

22.1.1 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.

22.1.2 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.

22.1.3 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).

22.1.4 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.

22.2 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.

22.3 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.

23 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.

23.1 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 the *Activate card* section in the [Operator's Guide](#) 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 the *Assisted activation* section in the [Operator's Guide](#) 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.

23.1.1 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	<input type="checkbox"/>	None
Bureau or batch issuance with cardholder encoding and activation	<input checked="" type="checkbox"/>	None
Encoding using Collect Card or Batch Collect Card and cardholder activation	<input checked="" type="checkbox"/>	1-Step
Bureau or batch issuance, encoding using Batch Encode Card, and cardholder activation	<input checked="" type="checkbox"/>	2-Step

Note: If you select **Pre-encode Card** you must select **Require Activation**.

23.2 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 [11.6, 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 [27.3, 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 [11.6, Customizing terms and conditions](#) for details.

23.3 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.

24 Managing Devices

MyID supports the Simple Certificate Enrollment Protocol (SCEP) for issuing 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.

Note: Issuing and recovering certificates with elliptic curve cryptography (ECC) keys using the MyID SCEP interface is not currently supported.

24.1 Overview

MyID allows you to issue device identities to devices that support SCEP; for example, you can issue a certificate to a router.

The procedure is as follows:

1. Add a device to MyID.
2. Create a credential profile for a SCEP device identity.
3. Request a device identity for the device.
4. Optionally, validate the device identity request.
5. On the SCEP client (for example, a router) request the device identity from the MyID SCEP server.
6. MyID issues a device identity to the device containing one or more certificates.

24.2 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.

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.

24.3 Setting up the SCEP server on a separate machine

To install the SCEP server, select the **SCEP API** option on the MyID installation program.

You can install the SCEP web service server on the MyID application server, or on a separate machine.

Note: As the SCEP service is a web service, you must have the IIS Role on the server onto which you install the SCEP software. By default, the MyID application server does not require this role; you must add it if you intend to use the application server as the SCEP server.

If you install the SCEP web service on a separate machine to the application server, you must transfer the COM proxy to allow communication between the SCEP web service server and the application server.

To do this, you must run the `MyIDSCEPHandler.msi` file that's located in the following folder on the application server:

```
C:\Program Files (x86)\Intercede\MyID\Components\Export
```

To run the COM proxy installer, either:

- From the SCEP server, browse to a share on the MyID application server and run the `MyIDSCEPHandler.msi` installer directly. For example, browse to:

```
\\<app>\C$\Program Files (x86)\Intercede\MyID\Components\Export
```

where `<app>` is the name of your MyID application server. Run the `.msi` file directly.

Note: You must add the application server to the list of Trusted Sites on the SCEP server.

or:

- Copy the `MyIDSCEPHandler.msi` file to the SCEP server and run the installer from there.

24.4 Certificates

The SCEP application server requires a signing certificate and an encryption certificate.

24.4.1 Signing certificate

The signing certificate must have the following properties:

- Application policy: `Certificate Request Agent`.
- Request Handling Purpose: `Signature`.
- Key Usage: `Digital Signature`.

24.4.2 Encryption certificate

The encryption certificate must have the following properties:

- Application policy: `Certificate Request Agent`.
- Request Handling Purpose: `Encryption`.
- Key Usage: `Key Encipherment`.

24.5 Registry entries

To configure the SCEP registry:

1. On the SCEP application server, log in using the MyID COM+ account.
2. Request the previously-created SCEP signing and encryption certificates that will be placed in the CAPI store.

Note: Do not enable strong private key protection on the certificates, as this will prevent processing of the request by the MyID account.

3. Once the certificates have been generated, install and save them as `.cer` files in Base64/PEM format.

You must save them in a location accessible to the MyID application; for example, the MyID installation folder. By default, this is:

```
C:\Program Files\Intercede\MyID\
```

4. Enter the filenames of the certificates in the system registry:

Note: You must log in as a user with sufficient privileges to edit the registry.

- a) Run the Windows `regedit` utility.

- b) Navigate to:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Intercede\Edefice
```

- c) If not already present, create the key `SCEP`.

- d) Create or set the following string values to the full path of the related certificate:

- `SigningCertificate`

- `EncryptionCertificate`

24.6 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 Cancellation** – select this option if you want to ensure that all device identity cancellations are approved before the device identity is canceled.
 - ♦ **Require Challenge** – You can choose whether to display the one-time challenge code on screen or send an email message containing the challenge code. See section [24.9, Requesting a device identity](#) for details.
7. Click **Next**.

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.

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.

24.7 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 [27.3, 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 [27.4, LDAP page \(Operation Settings\)](#).

Alternatively, you can use the Device Management API.

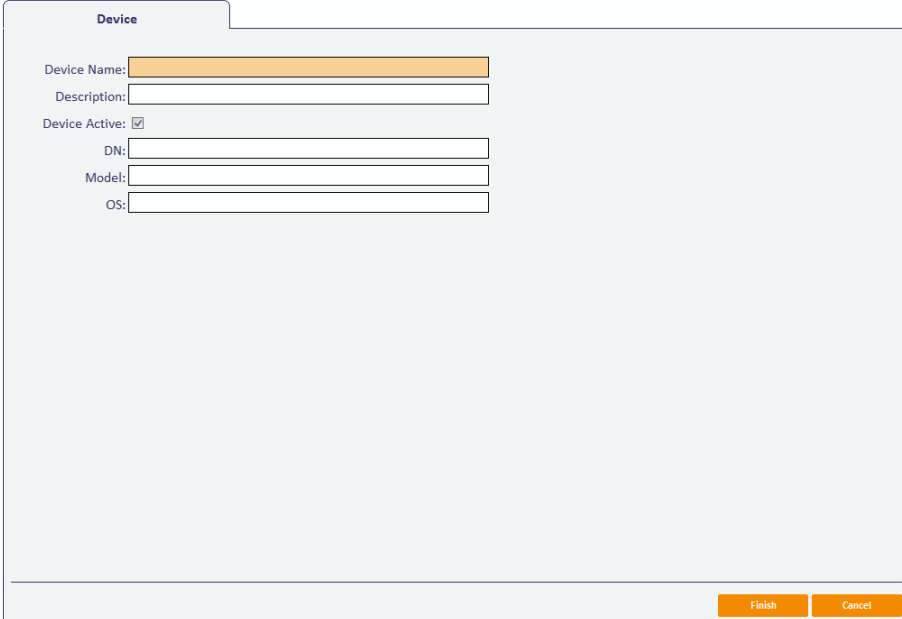
24.7.1 Adding devices manually

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**.



The screenshot shows a web form titled "Device". It contains the following fields and controls:

- Device Name:** A text input field with an orange border.
- Description:** A text input field.
- Device Active:** A checkbox that is currently checked.
- DN:** A text input field.
- Model:** A text input field.
- OS:** A text input field.
- Buttons:** At the bottom right, there are two orange buttons labeled "Finish" and "Cancel".

2. Give the device a name and description to help identify it.

When you add a device, make sure that the **Device Name** field will match one of the following in the SCEP request:

- ♦ The DNSName in the Subject Alternative Name
 - ♦ The CN of the device's DN.
3. If you want it to be available, select **Device Active**.
 4. You can optionally specify a **DN** for the device.

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
```

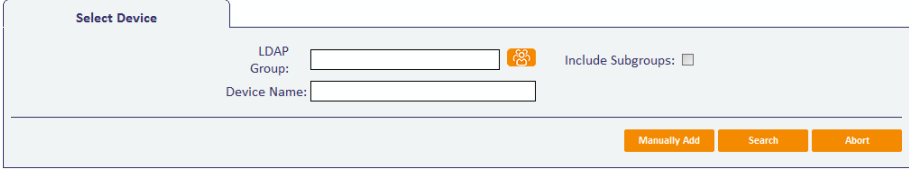
5. **Model** and **OS** are not currently supported.
6. Click **Finish**.
7. If you want to specify an owner for the device:
 - a) Click **Yes** on the dialog.
 - b) Use the Find Person screen to select the owner.

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.


24.7.2 Adding devices from an LDAP directory

To add a device from a directory:

1. From the **Configuration** category, select **Add Devices**.



The screenshot shows a 'Select Device' dialog box. It has a title bar with the text 'Select Device'. Inside, there are two input fields: 'LDAP Group' and 'Device Name'. To the right of the 'LDAP Group' field is a small icon of three people. To the right of the 'Device Name' field is a checkbox labeled 'Include Subgroups'. At the bottom right of the dialog are three buttons: 'Manually Add', 'Search', and 'Abort'.

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.

24.8 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 [27.3, 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**.

Select Device

Device Name:

Search
Abort

Results

Rows: Auto
Page 1 of 1

Device Name	Description	Status	Model	OS
<input type="checkbox"/> WebServerABC123	Web server	Enabled		

Edit Device
Abort

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.

Device

Device Name: WebServerABC123

Description: Web server

Device Active: ☒

DN:

Model:

OS:

Type: Asset

Serial No.: 395F5AC9-BF20-427f-A787-E528F3B277B9

Finish

Cancel

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.

24.9 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**.

Select Device

Device Name:

Search Abort

Results

Rows: Auto Page 1 of 1

	Device Name	Description	Active	Retrieved From
<input type="checkbox"/>	TechAuth1	My Main PC	Active	Database

Finish Abort

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 [24.10, Validating a device identity request](#) for details.

24.10 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**.

Search Details

DNS Alias:

Group:

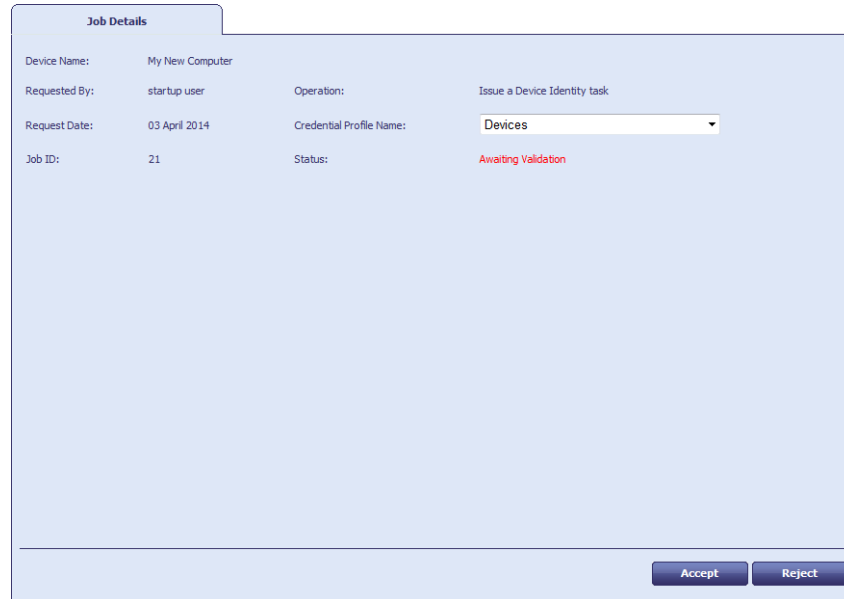
Include Subgroups: ☒

Job Labels:

Maximum Records: 200

Search

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**.



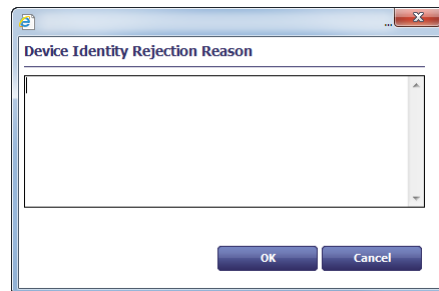
Job Details

Device Name:	My New Computer		
Requested By:	startup user	Operation:	Issue a Device Identity task
Request Date:	03 April 2014	Credential Profile Name:	Devices
Job ID:	21	Status:	Awaiting Validation

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.



Device Identity Rejection Reason

24.11 Collecting device identities

To collect a SCEP device identity, you must send a request from your SCEP-compliant device; for example, your router.

The SCEP device creates a PKCS#10 certificate request within a PKCS#7 container.

Note: The PKCS#10 request must meet the minimum key size requirements of the credential profile you have set up for the SCEP device identity.

This request can also contain the challenge code, which was either displayed on screen when you requested the device identity, or sent in an email message to the device owner.

The request is sent to the MyID SCEP server. The URL is:

`http://<SCEPserver>/MyIDSCEP/MyIDSCEP.ashx`

where:

- `<SCEPserver>` is the name of the machine on which you installed the MyID SCEP server; for example:

`http://myserver.example.com/MyIDSCEP/MyIDSCEP.ashx`

24.12 Canceling device identities

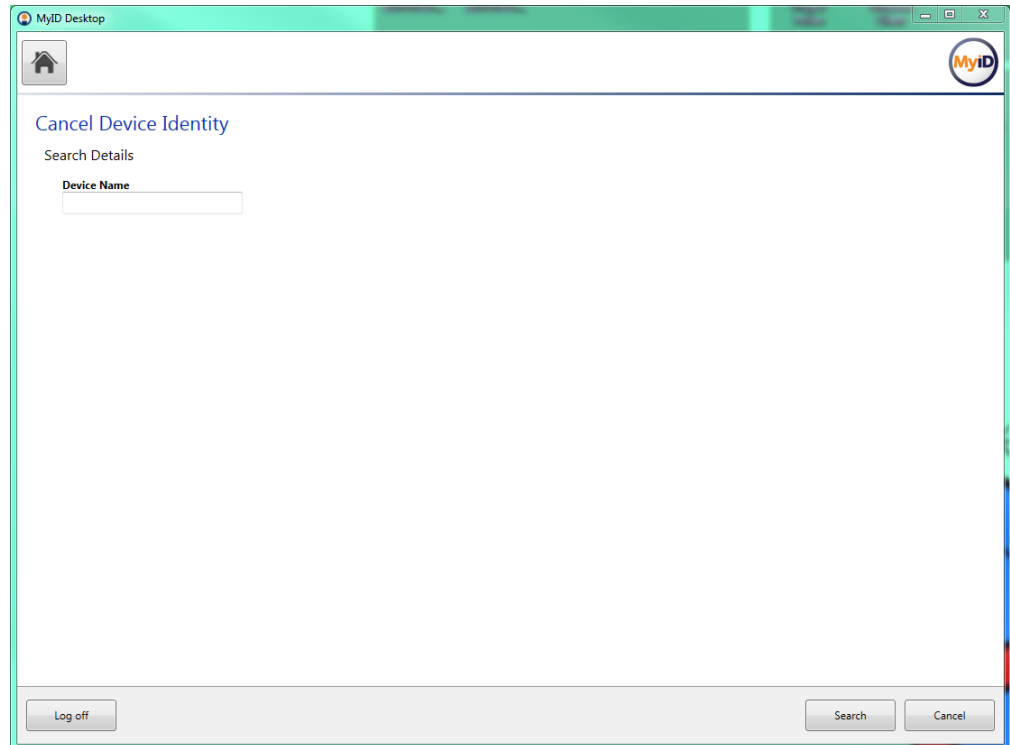
Note: When you cancel a device identity, MyID also cancels any outstanding device identity requests for the specified device. Accordingly, if you intend to reissue a device identity, you must cancel the device identity *before* you request the replacement.

You can request a device cancelation using the **Cancel Device Identity** workflow.

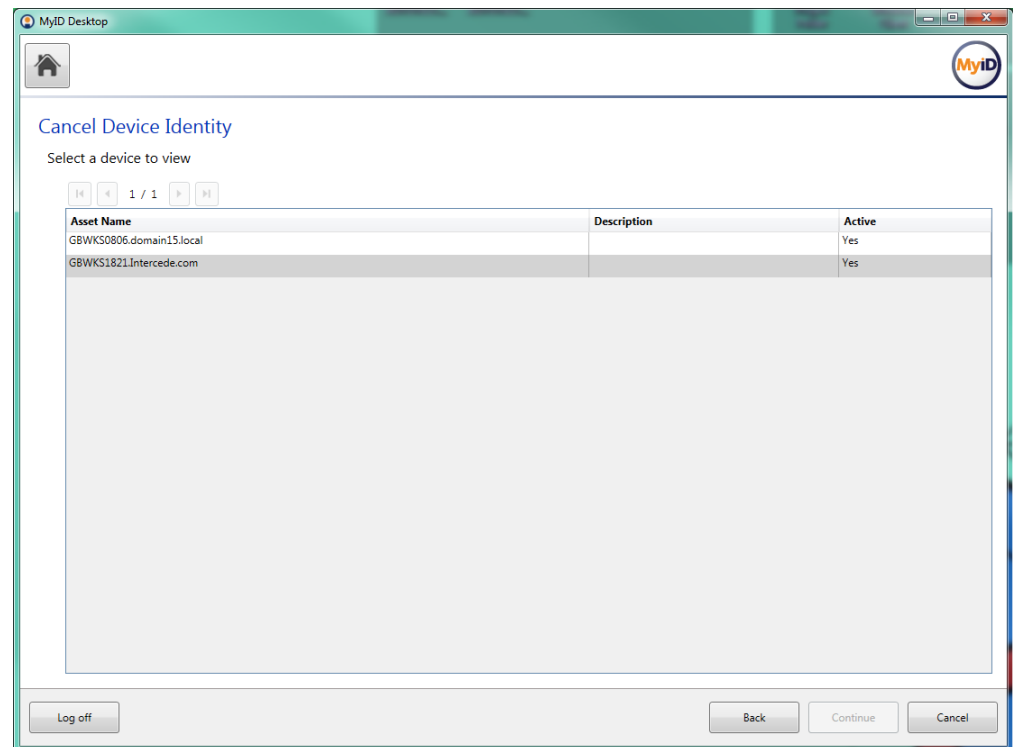
Note: The **Cancel Device Identity** workflow allows you to cancel a device identity that is unassigned, or is assigned to the currently logged-on MyID user. If you need to cancel a device identity that is assigned to anyone else, you must either remove the person assigned to the device, making it unassigned, 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:

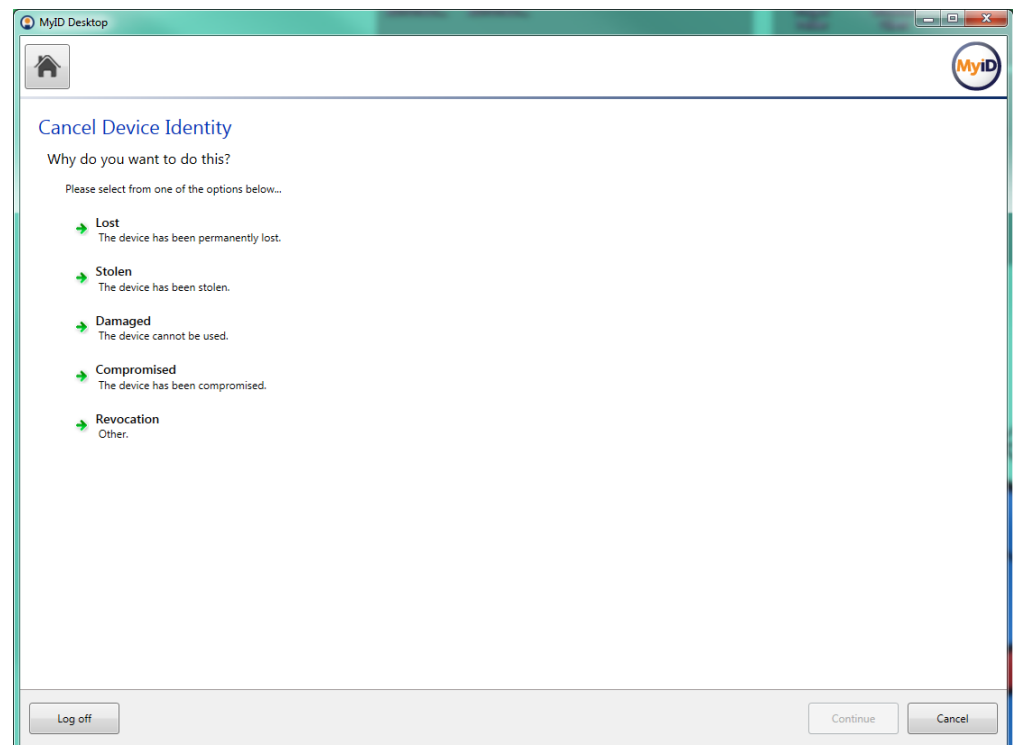
1. From the **Device Identities** category, select **Cancel Device Identity**.

The screenshot shows a web application window titled "MyID Desktop". The interface has a light blue header bar with a home icon on the left and the "MyID" logo on the right. Below the header, the main content area is titled "Cancel Device Identity" in blue text. Underneath this title, there is a section labeled "Search Details" which contains a text input field labeled "Device Name". At the bottom of the window, there is a grey footer bar containing three buttons: "Log off" on the left, and "Search" and "Cancel" on the right.

2. Optionally, type the name of the device you want to search for.
You can use * wildcards in the device name.
3. Click **Search**.



- From the search results list, select a device, and click **Continue**.
If the device does not have a currently-issued identity, MyID informs you.



- Select the reason for the cancelation, then click **Continue**.
See the *Certificate reasons* section in the [Operator's Guide](#) for details.

6. Type the reason you are cancelling the identity, then click **Continue**.

If the credential profile does not have the **Validate Cancellation** option set, MyID cancels the device identity.

If the credential profile *does* have the **Validate Cancellation** option set, you must use the **Confirm Cancel Device Request** workflow to approve the cancellation.

24.13 Approving device identity cancellations

If the credential profile used to request the device identity has the **Validate Cancellation** option set, you must approve the request before the device identity is canceled.

To approve a device identity cancellation 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**.

Select Job

Rows: Auto Page 1 of 1

ID	Job For	Requested By	Request Date	Validator	Validation Date	Status	Task Type
1009	GBWKS0707.domain09.local	startup user	24 January 2014	startup user	24 January 2014	Awaiting Validation	Cancel a Device Identity task

3. Select the device cancellation job from the list.
4. Review the details of the cancellation, then either **Approve** the cancellation, or click **Reject** and supply a reason for not approving the cancellation.

24.14 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 handler. 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.

25 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.

25.1 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 [12, 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 [27](#) and [28](#)).
- 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.
- A summary of the **System Credentials** – the system Windows user accounts and signing certificates – including when they will expire.

For more information about the **System Credentials** report and the notifications it provides, see the *Monitoring MyID* section in the [Advanced Configuration](#) guide.

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.

25.2 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.

25.2.1 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.

25.3 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.

25.4 System security

If you see a logon message similar to:

The system is not configured for production use - check the MyID system security checklist document for further information.

you must review the settings on the **Device Security** tab on the **Security Settings** workflow; see the [System Security Checklist](#) document.

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.

26 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.

26.1 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 ten 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.

26.2 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:

☒ Enabled (Allow Issuance)

Display Name: SmartcardLogonNew on VIN2012R2DC19
 Description:
 Allow Identity Mapping: ☒
 Reverse DN: ☐
 Archive Keys: None
 Certificate Lifetime: 365
 Automatic Renewal: ☒
 Certificate Storage: ☒ Hardware ☐ Software ☐ Both
 Recovery Storage: ☒ Hardware ☐ Software ☐ Both ☐ None
 Key Length: 2048 bits

[Edit Attributes](#)
[Supersede](#)

- ♦ Set the **Allow Identity Mapping** option on the certificate policy.

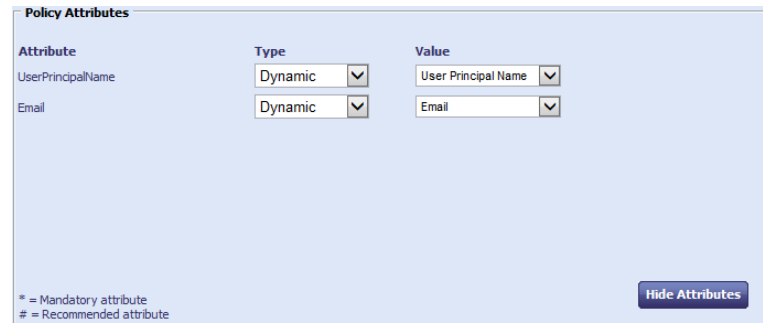
Important: If you set the **Allow Identity Mapping** option on a certificate policy, you cannot select that certificate policy as part of a credential profile. Certificate policies with the **Allow Identity Mapping** option set are excluded from the list of available certificate policies in the **Credential Profiles** workflow; also, if you edit a certificate policy that has already been included in a credential profile to set the **Allow Identity Mapping** option, the next time you attempt to edit the credential profile, you will see a warning, and you must edit the list of certificate policies.

- ♦ 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 a stored procedure in the MyID database. See your CA integration guide for details.

Set the **UserPrincipalName** and **Email** mappings to be dynamically mapped to the **User Principal Name** and **Email** user attributes.

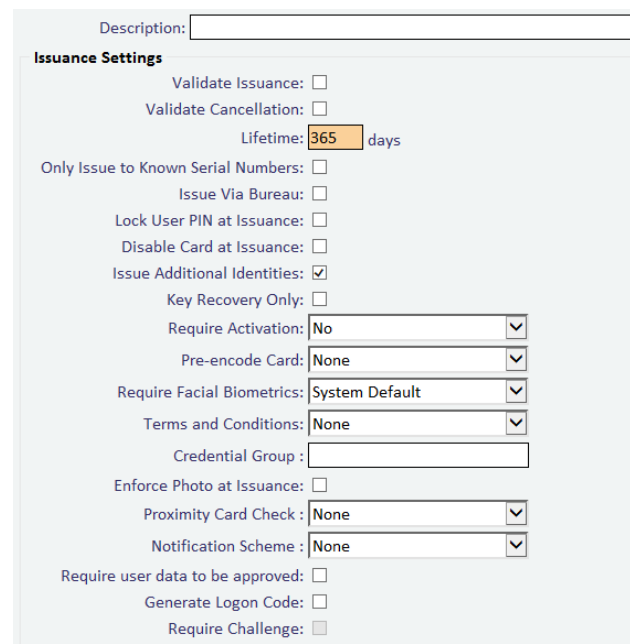


Attribute	Type	Value
UserPrincipalName	Dynamic	User Principal Name
Email	Dynamic	Email

* = Mandatory attribute
= Recommended attribute

Hide 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.



Description:

Issuance Settings

Validate Issuance: ☐

Validate Cancellation: ☐

Lifetime: 365 days

Only Issue to Known Serial Numbers: ☐

Issue Via Bureau: ☐

Lock User PIN at Issuance: ☐

Disable Card at Issuance: ☐

Issue Additional Identities: ☒

Key Recovery Only: ☐

Require Activation: No

Pre-encode Card: None

Require Facial Biometrics: System Default

Terms and Conditions: None

Credential Group:

Enforce Photo at Issuance: ☐

Proximity Card Check: None

Notification Scheme: None

Require user data to be approved: ☐

Generate Logon Code: ☐

Require Challenge: ☐

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, you cannot 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.

- If you want to create a card update job whenever an additional identity is modified, in the **Operation Settings** workflow, on the **Issuance Processes** tab, set the **Automatically create card update jobs when additional identities are modified** option to Yes.

26.3 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.

The screenshot shows a web interface with two tabs: 'Personal' and 'Additional Identities'. The 'Additional Identities' tab is active. Below the tabs, there are four columns: 'User Principal Name', 'Email', 'Distinguished Name', and 'Certificate Policy'. To the right of these columns is an 'Add' button. The main area below the columns is empty. At the bottom left is a '< Back' button, and at the bottom right is a 'Save' button.

You can select up to ten additional identities for the user.

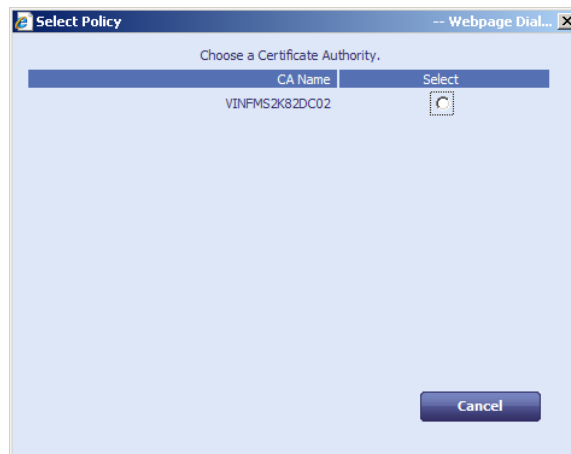
4. For each additional identity:
 - a) Click **Add**.

The screenshot shows a 'Select Person' dialog box. On the left, there is a tree view showing 'LDAP Root' and 'Default ADS'. On the right, there is a search area with a 'Search' label, an alphabetical index (A-Z), and an 'Advanced...' button. Below the search area, it says 'Please select a group'. At the bottom, there are 'Select' and 'Cancel' buttons.

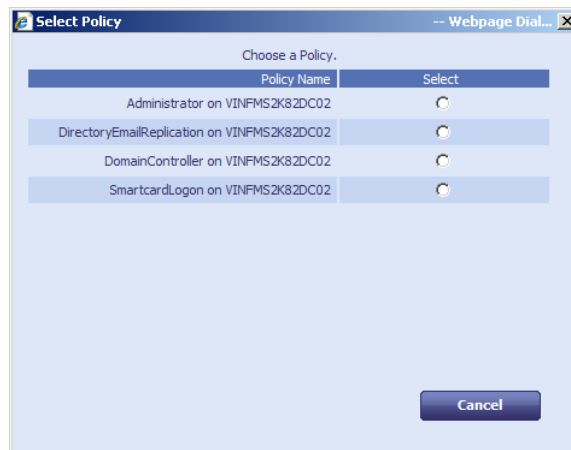
The available entries in the directory are restricted to the Organizational Unit of the operator and below.

- 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**.

26.4 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.

The screenshot shows the 'Additional Identities' tab for a user named Sam Jones. The interface includes a table with the following columns: User Principal Name, Email, Distinguished Name, and Certificate Policy. The table contains one entry for Sam Jones. To the right of the table is an 'Add' button and a 'Remove' button. Below the table, there is a large blue area with a warning message: 'Any changes made will not be saved until the workflow is completed. Any additional identities removed will result in associated certificates being revoked. Any additional identities added will be available in issuances that have a credential profile that supports additional identities.' At the bottom of the form are 'Back' and 'Save' buttons.

User Principal Name	Email	Distinguished Name	Certificate Policy
Sam Jones admin@domain15.local		CN=Sam Jones admin,OU=Finance,OU=Enterprise,DC=domain15,DC=local	SmartcardLoginNew on VNF2012R2DC15

Any changes made will not be saved until the workflow is completed.
Any additional identities removed will result in associated certificates being revoked.
Any additional identities added will be available in issuances that have a credential profile that supports additional identities.

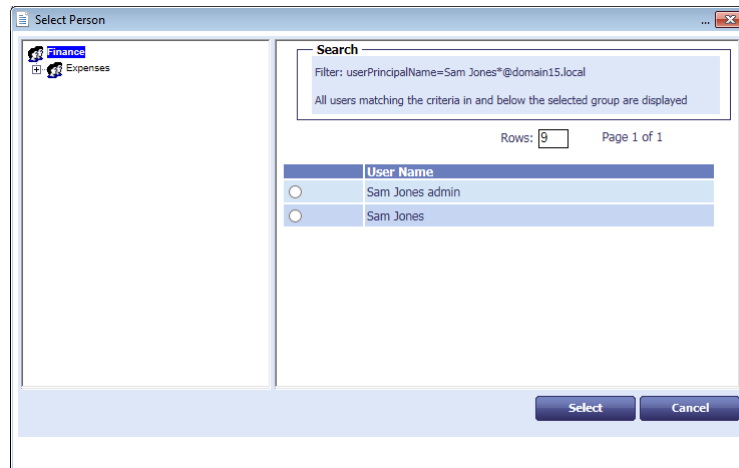
4. For the additional identity you want to delete, click **Remove**.
5. Click **Save**.

The certificates for any identities that you have removed are now revoked.

26.5 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 way 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.

26.6 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, or non-PIV systems using cards with PIV applets**

Additional identities are not supported on MyID PIV systems, or MyID systems with the CIV module installed. You also cannot issue additional identities to any cards that have PIV applets; for example YubiKey tokens.

27 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.

27.1 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.

27.1.1 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**.

27.2 General page (Operation Settings)

Setting	Default value	Description	Further information
Allow Image Zoom	No	Set this option to Yes to allow operators to expand images in read-only People workflows.	
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.	
Display additional error information	Yes	Shows extended error details button if an error is displayed to an operator.	See section 25, 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 the <i>Printers have external readers</i> section in the Operator's Guide .
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.	

27.3 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	<p>Allows you to search for cards with specific serial numbers when requesting a card.</p> <p>You can use * and ? as wildcards when searching.</p> <p>Any unassigned devices, or devices with unrestricted cancelation, that match the search criteria are displayed.</p> <p>The limit is 10 records; if more than 10 devices match the search criteria, you must search again with more restrictive criteria.</p>	See the <i>Requesting a card</i> section in the Operator's Guide .
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 the <i>Disposing of cards</i> section in the Operator's Guide 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	<p>You can configure the length of time before expiry that you can request a card renewal using the Request Replacement Card workflow.</p> <p>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.</p> <p>This option also affects the behavior of automatic certificate renewals; if the card is within the Card Renewal Period window, automatic certificate renewals do not get triggered, but instead a notification is sent to the cardholder that they must request a replacement card.</p>	See section 6.6.1, Credential lifetimes and certificate 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 the Delivering cards section in the Operator's Guide for details.

Setting	Default value	Description	Further information
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 Authenticate Virtual Smart Cards.	See the Intel Authenticate Integration Guide for details.
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 11.3.1, Credential profile options .
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		
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 11.6, 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 the <i>Collecting a card</i> section in the Operator's Guide .
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	<p>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.</p> <p>If the card is being updated to a new credential profile, MyID checks the Terms and Conditions setting of the <i>new</i> credential profile.</p> <p>Can be one of the following:</p> <p>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.</p> <p>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.</p> <p>No – users do not need to sign the Terms and Conditions when collecting card updates.</p>	See section 11.3.1, 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.

27.4 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	<p>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.</p> <p>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.</p>	
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.	<p>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.</p> <p>This option also determines whether user accounts imported from a directory should be disabled if the user has been <i>disabled</i> in the directory.</p>	

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 exception groups		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.

Setting	Default value	Description	Further information
LDAP update permreplaceissue card		Used for LDAP updates.	For more information, contact customer support, quoting reference SUP-227.
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. <ul style="list-style-type: none"> 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 	If this option is set to Yes, you cannot search the MyID database using, for example, the View Person workflow. If you want to be able to search the MyID database, set this option to Ask or No.
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 distinguished name changes	No	Determines whether MyID updates Entrust with changes to the DN.	See the Entrust CA Integration Guide for details.

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.	

27.5 Video page (Operation Settings)

Setting	Default value	Description	Further information
File Store Location		The folder used to store images, mapped to the <code>upimages</code> virtual directory.	See the <i>Changing settings for image capture</i> section in the Operator's Guide .
HTTP Port for image upload	80	The port to be used when uploading images using HTTP.	See the <i>Changing settings for image capture</i> section in the Operator's Guide .
HTTPS Port for image upload	443	The port to be used when uploading images using HTTPS.	See the <i>Changing settings for image capture</i> section in the Operator's Guide .
Image Capture	Yes	Whether image capture is to be used.	See the <i>Changing settings for image capture</i> section in the Operator's Guide .
Image Crop Height	0	The height of captured images. PIV only.	
Image Crop Width	0	The width of captured images. PIV only.	

Setting	Default value	Description	Further information
Image Upload Server		<p>If the web services server is not the same server as the web server, this must contain the name or IP address of the server to which images are uploaded. Used for upgraded systems that do not store images in the database.</p> <p>If the web services server and the web server are on the same physical machine, leave this option blank.</p> <p>Also used for images used in the Card Layout Editor.</p>	See the <i>Setting the location of the web server</i> section in the Web Service Architecture guide.
JPEG Compression Ratio	90	The compression ratio to use for any JPEG images.	See the <i>Changing settings for image capture</i> section in the Operator's Guide .
Maintain Aspect Ratio	Yes	Whether aspect ratio is to be retained when resizing images.	See the <i>Changing settings for image capture</i> section in the Operator's Guide .
Maximum Image Height	0	The maximum height of an image to be displayed in the image capture control.	See the <i>Changing settings for image capture</i> section in the Operator's Guide .
Maximum Image Width	0	The maximum width of an image to be displayed in the image capture control.	See the <i>Changing settings for image capture</i> section in the Operator's Guide .
Maximum Number Of Sub-Folders	0	The maximum number of sub-folders to be used when storing images.	See the <i>Changing settings for image capture</i> section in the Operator's Guide .
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 the <i>Changing settings for image capture</i> section in the Operator's Guide .
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 the <i>Storing images on the web server</i> section in the Operator's Guide .

Setting	Default value	Description	Further information
Video Capture	No Yes – in PIV.	Whether video (webcam) is to be used for capturing images.	See the <i>Changing settings for image capture</i> section in the Operator's Guide .

27.6 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. This option is available only in the Issue Card workflow. Other card issuance workflows do not allow you to collect certificates later.	See the <i>Issuing certificates</i> section in the Operator's Guide .
Automated Issuance Time Limit	45	The time to wait for a certificate to be issued when using an automated issuing process.	
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 <code>mm-nnULSN</code> . 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)	

Setting	Default value	Description	Further information
Certificate Refresh Threshold	15	<p>The number of seconds to wait for a certificate to be issued before deferring issue or canceling process.</p> <p>If you experience problems when collecting or updating cards, try increasing this option to a higher value; for example, 45.</p> <p>This problem may manifest with an error similar to:</p> <pre>One of the certificates that have been requested for you has failed to issue.</pre>	
Certificate Renewal Period	56	If you have configured automatic certificate renewals, the certificates automatically renew only if they have a remaining lifetime (in days) that is lower than this value.	Not currently implemented.
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.	
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.
iOS OTA Credential Profile		Set this option to the name of the Device Identity credential profile.	See the Mobile Identity Management document for details.

Setting	Default value	Description	Further information
iOS OTA Organization		Set this option to the name of your organization. This appears on the OTA provisioning message on the mobile device.	See the Mobile Identity Management document for details.
iOS OTA Display Name		Set this option to a name for the OTA update. This appears on the OTA provisioning message on the mobile device.	See the Mobile Identity Management document for details.
iOS OTA Description		Set this option to the a description for the OTA update. This appears on the OTA provisioning message on the mobile device.	See the Mobile Identity Management 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.	
Renew Expired Certs Via API	No	Allow the renewing of expired certificates through calls to the Credential Web Service API.	See the Credential Web Service document for details.
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 software certificates recovered depending on the recovery method configured by the certificate profile. Can be one of the following: Local Store Save to PFX Both	See the <i>Options for recovering soft certificates</i> section in the Operator's Guide .
Suspend to revoke period	0	The time between suspension and revocation.	

27.7 Import & Export page (Operation Settings)

Setting	Default value	Description	Further information
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.	

27.8 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.

27.9 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.	

27.10 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 the <i>Self-service PIN reset authentication</i> section in the Operator's Guide .
Allow Aware Preface control 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 11.3.2, 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.

27.11 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 11.3.2, 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 – 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 . Note: Due to restrictions imposed by Apple, the URL must be opened in the Safari browser and must link to a page that contains a link to the app to download; the user can then select this link. The URL <i>cannot</i> be a direct link to the app file itself.
Automated Card Issuance Time Limit	240	The time (in seconds) to be spent attempting to issue a card before canceling the process.	

Setting	Default value	Description	Further information
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 <code>option,operationid;option,operationid</code> and so on. For example: <code>2,245</code> – this automatically launches the Activate Card workflow.	
Automatically create card update jobs when additional identities are modified	No	Create card update jobs automatically on changes to additional identities.	See section 26, Additional Identities for details. Note: Changes carried out using the Credential Web Service API create update jobs whether this option is set to Yes or No. See the Credential Web Service document for details.
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.	

Setting	Default value	Description	Further information
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.	See the <i>Requesting multiple cards</i> section in the Operator's Guide .
Maximum unvalidated multiple credential requests	1	The maximum number of multiple credential requests that will be accepted without secondary validation.	See the <i>Requesting multiple cards</i> section in the Operator's Guide .
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 24.9, 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 11.3.1, 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.	

27.12 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 13.1.5, 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 13.1.4, Email separator for details.
Expiration Notification Period	28	If a certificate renewal job is required for a card that has less than this number of days of lifetime remaining, a card renewal job is created instead.	
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 <code>TEXT</code> or <code>HTML</code> .	See section 13, Email Notification .
Notification Proxy URL		No longer used.	
Send Email Notifications	No	Global setting to determine whether notification email messages are sent.	See section 13, 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 13, Email Notification .

27.13 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	<p>Set this to the level of logging you want Identity Agent to produce. Higher levels result in more detail, but larger files.</p> <p>Set to one of the following:</p> <ul style="list-style-type: none"> 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	<p>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.</p> <p>To allow as many files as will fit in the maximum log storage space, set this value to -1.</p>	
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.	
Maximum session count	-1	<p>This determines the number of concurrent sessions (whether from mobile clients or other clients such as MyID Desktop, the Self-Service App, or the Self-Service Kiosk) that are allowed by the server while still allowing mobile issuance and update operations.</p> <p>Values:</p> <ul style="list-style-type: none"> 0 – Do not allow mobile issuances or updates. -1 – No limits. <p>Any other number determines the number of client sessions allowed. If this number is exceeded, the server returns HTTP 503 – service unavailable – to all mobile clients. This will also be recorded in the local event log.</p> <p>Only mobile clients are prevented from connecting.</p>	See the Mobile Identity Management Installation and Configuration Guide for details.

28 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.

28.1 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.

28.1.1 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**.

28.2 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)	<p>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.</p> <p>Choose:</p> <p>Yes (Software or Card if available) – Use a signing key from your smart card if available (if you select the MyID Logon option in the Services section of the credential profile, you can either select a certificate to be used for signing, or use a signing key generated on the card by MyID at issuance). If neither a certificate nor a manager keypair is available, use a temporary software signing key generated by MyID when you log on.</p> <p>No – Do not sign data.</p> <p>Software signing only – use a temporary software signing key generated by MyID when you log on.</p>	

Setting	Default value	Description	Further information
Complex Logon Code Complexity	12-12ULSN	<p>The complexity rule used to generate a logon code when the Generate Logon Code option in the credential profile is set to Complex.</p> <p>It takes the format <code>mm-nnULSN</code>.</p> <p>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)</p>	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.	
Maximum allowed security question failures	3	<p>Specify the maximum number of failed attempts a user can make when attempting to answer a security question.</p> <p>When this number is exceeded, the user's account can be locked out – see the Action on maximum security question failures option.</p>	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.
Prevent Direct Password Logon	No	Allow password logon for self-service operations only when a card is present.	

Setting	Default value	Description	Further information
Set Security Phrase at Logon		<p>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.</p> <p>Workflows should be listed as <code>option,operationid;option,operationid</code> and so on. For example, <code>1,110</code> – this automatically launches the Change My Security Phrases workflow.</p>	<p>See section 3.3.3, Setting the number of security phrases required to authenticate for details.</p> <p>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.</p>
Show Full Name at Logon	No	<p>Controls whether the card owner's full name is displayed on the Logon page when their card is inserted.</p> <p>Note: If you set this option to <code>No</code>, and either you have the Show Photo at Logon set to <code>No</code>, 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).</p>	
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	<p>The complexity rule used to generate a logon code when the Generate Logon Code option in the credential profile is set to Simple.</p> <p>It takes the format <code>mm-nnULSN</code>.</p> <p><code>Mm</code> = min length <code>nn</code> = max length <code>U/u</code> = must/may contain upper case (optional) <code>L/l</code> = must/may contain lower case (optional) <code>S/s</code> = must/may contain symbols (optional) <code>N/n</code> = must/may contain numbers (optional)</p>	See section 3.4, Logon codes for details.

Setting	Default value	Description	Further information
Validate logon certificate	No	<p>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.</p> <p>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.</p>	Note: The application server must trust the Certificate Authority that issued the certificate being validated.

28.3 Device Security page (Security Settings)

Setting	Default value	Description	Further information
Display warnings for unsecured issuance	Yes	<p>Displays a warning on the login screen if the system is not securely configured and an attempt is made to issue credentials.</p> <p>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.</p>	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 7, 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	<p>Random – Generate a random SOPIN and set it on the card to be initialized (higher security).</p> <p>Factory – Leave the default SOPIN on the card (low security).</p>	
Show all devices	No	<p>When set to No, restricts the list of devices on this page to the smart cards known to support GlobalPlatform or PIV 9B keys.</p> <p>When set to Yes, displays all devices known to MyID.</p>	

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 25.4, [System security](#) for more information.

The [System Security Checklist](#) document contains important information on securing your system.

28.4 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 Installation and Configuration Guide for details.	Do not deselect <i>both</i> 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 Installation and Configuration Guide for details.	

Setting	Default value	Description	Further information
Allow Legacy Data Models	No	<p>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:</p> <pre>Legacy datamodel configuration is disabled</pre> <p>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.</p> <p>Once old clients are updated, set this option back to No.</p>	
PIV Server hash algorithm	SHA256	<p>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.</p> <p>PIV only.</p>	See the PIV Integration Guide for details.
Server Encryption	Software based only	<p>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.</p> <p>None – Do not use encryption.</p> <p>Yes (Software or Card if available) – Use encryption keys from your smart card, if available.</p> <p>Software based only – Use a software encryption key generated when you log on.</p>	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	<p>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.</p> <p>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.</p>	<p>Note: The application server must trust the Certificate Authority that issued the certificate being validated.</p> <p>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.</p>

28.5 PINs page (Security Settings)

Setting	Default value	Description	Further information
Action on maximum security question failures	Lock security phrases	<p>Determines what happens when a user has reached the Maximum allowed security question failures – can be one of the following:</p> <p><code>Lock security phrases</code> – The user's account is locked.</p> <p><code>None</code> – The user can retry as many times as they like.</p>	
Ask Security Questions for Self Service Card Unlock	No	Whether the holder's security phrase is used when unlocking a card.	See the <i>Self-service PIN reset authentication</i> section in the Operator's Guide .
Case sensitive security questions	Yes	Whether the case of responses to security phrases is checked when authenticating.	Important: See section 3.3.2, <i>Changing rules for security phrases</i> .
Default max PIN length	12	The default maximum PIN length.	See section 11.3.1, <i>Credential profile options</i> .
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 11.3.1, <i>Credential profile options</i> .

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 3.3.3, 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 3.3.3, 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 3.3.3, 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 the <i>Unlocking a credential remotely</i> section in the Operator's Guide 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.	Important: See section 3.3.2, Changing rules for security phrases .

Setting	Default value	Description	Further information
Set GlobalPlatform Card Status	No	<p>Whether MyID can set the GlobalPlatform status for a device.</p> <p>When you use deferred activation, MyID must be able to set the card status from <code>SECURED</code> to <code>LOCKED</code>. If the card is shipped with the status <code>SECURED</code>, no further action is required. If the card is shipped with the status <code>OP_READY</code> or <code>INITIALIZED</code>, for example, you must set this option to <code>Yes</code> to allow MyID to change the card status to <code>SECURED</code> before it sets the status to <code>LOCKED</code> for deferred activation.</p> <p>Note: You must also make sure that you set up customer GlobalPlatform keys for your cards. The status change from <code>OP_READY</code> or <code>INITIALIZED</code> to <code>SECURED</code> occurs when MyID sets the customer keys for a card.</p> <p>See your card integration guide for whether you need to set this option.</p>	
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.	Only the Issue Card workflow can display generated PINs. Other issuance workflows will not display the user PIN that has been generated.
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 9.3, EdeficePinGenerator PIN generation algorithm for details.
Use Security Phrase algorithm version 2	Ask	<p>If you are upgrading from a previous system, and this option was previously set to No, this is set to Yes by the installer.</p> <p>This option is used to configure MyID to set security phrases to use SHA256 hashing.</p>	See the Installation and Configuration Guide for details of upgrading the hashed security phrase answers stored in the MyID database.

28.6 Process page (Security Settings)

Setting	Default value	Description	Further information
Allow Administrative Groups	No	<p>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.</p> <p>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.</p>	See section 4.7, Administrative groups for details.
Approve Replacement Cards	No	<p>Whether requests for replacement cards require secondary authorization.</p> <p>Yes – All requests for replacement cards require secondary authentication.</p> <p>No – No requests for replacement cards require secondary authentication.</p> <p>Ask – Requests for replacement cards require secondary authentication only if the Validate Issuance setting is set in the credential profile.</p> <p>Note: The Validate Issuance setting in the credential profile affects replacement cards <i>only</i> if this option is set to Ask.</p>	
Card Expiration Period (days)	365	Default period that all issued devices are valid.	See section 11.3.1, 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 11.3.8, 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 11.3.6, 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 11.3.9, 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 11.3.7, 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 <code>DatabaseVersion</code> table in the MyID database.	

28.7 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 <code>People</code> 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.

28.8 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, <i>Using security questions to log on to MyID</i> .
Smart Card Logon	Yes	Whether users can log on to MyID with their issued smart cards.	See section 3.2, <i>Using a card and PIN to log on to MyID</i> .
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, <i>Integrated Windows Logon</i> .
Biometric Logon	Yes	Whether users can log on to MyID using biometrics. Currently used only for resetting PINs.	See the <i>Self-service PIN reset authentication</i> section in the <i>Operator's Guide</i> .

Index

Abort On Timeout	212	Allow LDAP Search for devices during card requests.....	207
access to workflows	34	Allow Legacy Data Models	232
Action on maximum security question failures	233	Allow Logon Codes	227
Actioned by	171	Allow parent and child credential profiles ...	220
Active credential profiles per person	220	Allow self requests	239
Active Directory	50	Allow virtual smart card creation with TPM reduced functionality	202
adding		anonymous access to LDAP directory	52
a directory	51	App Download URL – ANDROID	220
customer keys	81	App Download URL – IOS	220
devices	180	applets	19, 75
factory keys	77	adding.....	84
roles	34	adding to credential profiles	111
Additional identities	193	editing.....	85
Administration Email.....	137, 223	upgrading	86
administrative groups	44	Applicants Re-Approve for Card Renewal..	216
administrator	19	Applicants Re-Enroll for Card Replacement	216
Adminstrator email address.....	224	Application AID	84
Agency Deletion Enabled	200	application privileges	84
all scope	43	applying updates	
Allow Administrative Groups	237	to MyID	12
Allow Aware Preface control to capture non-compliant images	218	Approve Replacement Cards.....	237
Allow Biometric PIN Reset	218	archive deleted users.....	168
Allow Card Activation	202	Archive People Data	168, 200
Allow card serial number to be entered during Request Card workflow.....	202	archiving keys	158
Allow Collect Later.....	212	Ask Security Questions for Self Service Card Unlock	233
Allow device management from the MyID user interface	202	assigning administrative groups	45
Allow disposal of expired devices.....	202	assigning logon mechanisms.....	36
Allow duplicate DN	206	Audit Reporting workflow	155
Allow envelope version 1.2.....	231	Audit summary	239
Allow envelope version 1.3.....	231	Audit trail	155
Allow Image Zoom.....	200	Audited Items workflow	156
Allow LDAP Search for devices during Add Devices	206	auditing specified items	156
		Auth Code Scope.....	202
		auto text on card layouts.....	95
		Auto-enroll from directory	239

Automated Card Issuance Time Limit	220	canceling jobs	172
Automated Detect Card Time Limit	221	Capture threshold for U.are.U Biometrics...	219
Automated Issuance Time Limit	212	capturing images	210
Automated Remove Card Time Limit	221	Card activation expiration period	202
Automatic cancellation timeout.....	217	Card Encoding	113
Automatic Completion of Issuance.....	221	Card Expiration Period (days).....	237
Automatic Completion of Issuance Timeout	221	Card label.....	202
Automatic job cancellation credential profile filter	217	Card Layout Editor workflow.....	88
Automatic job cancellation email	217	card layouts	
Automatic Update Collection	221	adding.....	88
Automatically create card update jobs when additional identities are modified	221	associating with credential profiles	111
Automatically create MyID groups from the Organizational Unit of imported users	207	default.....	127
Automatically Expire Web Pages	200	deleting.....	88
Aware Preface Custom Profile (ISO Token)	218	designing.....	87
Aware Preface Custom Profile (PIV Authentication)	218	printing.....	102
Aware Preface Custom Profile (PIV Card) ..	218	saving.....	88
back of cards	87	xml.....	100
Background Update.....	207	card logon	36
backgrounds	91	card readers.....	19
Base DN	51, 52	Card Renewal Period.....	203
Batch Directory Synchronization Tool	54	cardholders	19
scheduled task	56	cards	19
Batch Encode Card Timeout	221	Cards Allowed for Derivation	212
batch issue, default card layout.....	127	Case sensitive security questions	233
BatchLDAPSync.exe	56	categories	19
Biometric Logon.....	240	ceremony, key	79, 83
Biometric matching library	218	certificate archiving	158
Biometric matching threshold	218	certificate authorities	62
BioSensitivity for Precise Biometrics	218	connecting.....	63
BioSensitivity for U.are.U Biometrics.....	218	Certificate Authorities workflow.....	63
browsing reports	156	certificate policies	65
Bypass fingerprint verification when no fingerprints enrolled	219	Certificate Polling Refresh Time	212
CA connection		Certificate Recovery Password Complexity	212
add	63	Certificate Refresh Threshold	213
edit existing	64	Certificate Renewal Period	213
calendar control	16	Certificate Timeout For Deferred Collection	213
Cancel Outstanding Updates	217	Certificate Timeout For Issuance.....	213
		certificates.....	19
		adding to credential profiles	111
		collecting later	212
		enabling.....	65
		issuing	50
		revocation.....	66
		revoking automatically.....	209
		challenge/response.....	234

Change Security Phrases workflow.....	239	Default roles.....	38
Check Content Signing Certificate Expiration	203	deleted users, archiving.....	168
client components		deleting	
uninstalling.....	12	customer keys.....	83
Client Logon Keyset	237	roles.....	34
Client Sign Keyset	237	Deliver Card Before Activation.....	203
Client Signing	227	department scope	43
Color Picker dialog	98	Derived credential certificate OID	213
colors, text	98	Derived credential revocation check offset	213
command line for Batch Directory Synchronization Tool	56	Derived credential signing certificate OID ..	213
Complex Logon Code Complexity.....	228	designing card layouts	87
Configuration report.....	190	Device Profiles.....	120
connecting to a CA	63	devices.....	19
Connecting to an LDAP directory	51	adding.....	180
Constrain Credential Profile Collector	238	adding from an LDAP directory	181
Constrain Credential Profile Issuer.....	126, 238	directory	50
Constrain Credential Profile Unlock Operator	127, 238	creating connections	51
Constrain credential profile validator	238	Directory Management workflow	51
conventions	3	directory Synchronization Tool	54
Create OU Chain	207	Disable on removal from directory	54, 207
Credential Number Per Device.....	203	Display additional error information	191, 200
Credential Profile workflow	112	Display credential profile details	221
credential profiles	111	Display pending card requests	200
back of cards.....	87	Display person details during confirm job ...	209
Card Encoding	113	Display warnings for unsecured issuance ..	230
creating	112	diverse keys.....	77, 82, 148
soft certificates	128	division scope	43
Credential Stock	120	DN, duplicate	206
credentials	19	document conventions.....	3
issuing.....	111	documentation	11
Custom LDAP mappings	207	documents, mail merge	127
customer keys	76, 148	duplicate DN	206
adding	81	Edit Directory Information	208
deleting	83	Edit DN.....	208
Database Mail Profile Name.....	223	Edit Roles workflow	32, 33
dates	16	editing	
Default Card Data Model	203	applets.....	85
default card layouts	127	roles.....	32
Default Card Reverse Layout.....	87, 203	Effective Revocation Immediate	200
Default max PIN length	233	email address	
		administrator	223
		for licenses	133
		email notifications	136

templates	139	grid	89
Email separator	137, 223	Group Deletion Enabled	200
email templates		groups	19, 32, 44
editing	137	administrative	44
enabling	137	assigning administrative	45
Email Templates workflow	137	creating from LDAP	207
Enable additional authentication options	219	hardware tokens	122
Enable ADS Fields	208	hiding roles	33
Enable credentials when person is enabled	204	host, LDAP directory	51
Enable Customer GlobalPlatform Keys	76, 230	HTTP Port for image upload	210
Enable Facial Capture	219	HTTPS Port for image upload	210
Enable Intel Virtual Smart Card support	204	ID photos on card layouts	90
Enable unrestricted cancelation	221	Identities	
enabling certificates	65	additional	193
Enforce Photo at Issuance	116	Image Capture	210
Error	170	Image Crop Height	210
Error messages	191, 200	Image Crop Width	210
evaluation license	132	Image Upload Server	211
Event auditing	155	images	
events report	190	card layouts	90
Executable AID	84	Import Serial Numbers workflow	109
Expanded error messages	191, 200	importing	
Expiration Identity Batch	204	account details	47
Expiration Notification Period	223	information, where to find it	11
Expiring web pages	200	Inheriting roles	37
External Logon Providers	169	Initiator	171
External Systems workflow	167	installation history	190
factory keys	76, 148	installing licenses	134
adding	77	Integrated Windows Logon	30, 240
deleting	81	iOS OTA Credential Profile	213
File Export Directory	215	iOS OTA Description	214
File Import Directory	215	iOS OTA Display Name	214
File Store Location	210	iOS OTA Organization	214
Find Person stage	46	Issuance Notification URL	223
Fingerprint enrolment device	219	Issuance Settings	114
fit image to card	89	Issue MyID Signing Keys	204
Force NETBIOS name	208	issuing	
formatting text	97	certificates	50
forms	19	Java cards	75
GenMaster	148	Job batch maximum size	217
GIFs on card layouts	90	Job management	170
GlobalPlatform keys	76	Job Management workflow	172
		jobs	19

canceling	172	Mail Documents	120
searching	170	Mail Format	223
suspending.....	172	mail merge	120, 127
targets	171	Maintain Aspect Ratio	211
unsuspending.....	172	Manage Additional Identities workflow	195
JPEG Compression Ratio	211	Manage Applets workflow	85
JPEGs on card layouts	90	Manage GlobalPlatform Keys workflow	76
Key Manager workflow	148	Manage My Additional Identities workflow..	198
keys	204	management keys	204
archiving.....	158	Manager credential profile	112
ceremony	79, 83, 148	Managing jobs	170
managing	148	managing keys.....	148
transport.....	148	Manual Card Update.....	222
layouts		Mask Certificate Revocation Code	214
associating with credential profiles	111	master keys.....	79, 83, 148
for cards.....	87	Maximum Allowed OTP Failures	228
LDAP directory	50	Maximum allowed security question failures	228
creating connections	51	Maximum certificate server restart log entries	200
integration	44	Maximum certificate suspensions.....	214
port.....	52	Maximum Image Height.....	211
primary data source	53	Maximum Image Width	211
pushing containers.....	207	Maximum keys per card to recover	214
pushing group details.....	210	Maximum log storage space.....	224
pushing user details	210	Maximum multiple credential requests	222
LDAP Directory Synchronization Tool	54	Maximum number of log files.....	224
LDAP update cancel card.....	208	Maximum Number Of Sub-Folders	211
LDAP update enable card	208	Maximum person search results.....	200
LDAP update exception groups.....	208	Maximum retry attempts	224
LDAP update newissue card	208	Maximum session count	225
LDAP update permreplaceissue card	209	Maximum unvalidated multiple credential	
LDAP update search attribute	209	requests.....	222
LDAP update tempreplaceissue card.....	209	Messages expanded.....	191
licenses.....	132	Microsoft virtual smart cards supported within	
installing	134	MyID	204
requesting	133	Migrated Certificate Credential Profile	215
status	133, 190	Migrated Device Credential Profile	215
warning email address	133	Migrated Encryption Certificate Policy	215
Licensing workflow	132	Migrated Non-archived Certificate Policy ...	215
Lightweight Directory Access Protocol	See	Minimum retry delay	225
LDAP directory			
Link to LDAP Groups.....	209		
Load File AID.....	84		
Lock Card on Issuance.....	233		
Log level	224		
logging on	20, 21, 36		
Logon Name Required	228		
Logon Providers	169		
magnetic stripes on card layouts (magstripe)	99		

Mobile Certificate Recovery Service URL ...	214	PIV Server hash algorithm.....	232
Mobile Provision Via Email.....	204	policies, certificate	65
Mobile Provision Via SMS	204	port, LDAP directory	51, 52
MyID Encryption	114	Preload Images.....	211
MyID Logon	114	Preserve FASCN and UUID for card update	205
navigation buttons	15	Prevent Direct Password Logon	228
Notification Proxy URL	223	Prevent version 1 password enrollment	234
Notification Scheme	116	primary data source	50, 53
Number of fingerprint validation attempts ...	219	Print Card Timeout.....	222
Number of security questions for operator authentication.....	234	Print Quality Confirmation.....	205
Number of security questions for self-service authentication.....	234	Printer Request Buffer Delay	222
Number of security questions to register.....	234	printers	19
Offline Unlock Method	234	Printers have External Prox Readers	201
One Active Job Per Person	204	printing card layouts.....	102
One Click Selection in Find Person.....	200	printing cards	87
One Credential Profile Request Per Person.....	204	profiles for credentials.....	111
Operation Settings workflow.....	54, 199	Proximity Card Check	116
operators	19	Reload Device Profile	222, 234
organization chart.....	44	Remote Unlock requires an Authentication Code prompt.....	234
Organizational Unit.....	44	Renew Expired Certs Via API.....	214
organizing groups	44	renewal dates (jobs)	171
OU	44	reporting structure.....	44
OU chain.....	207	requesting licenses	133
Output Mechanism for Job Challenge Code Generation	222	Require fingerprints for derived credentials	219
PACS.....	167	Require Random Security Officer PIN.....	230
password logon	21, 36	Requisite User Data.....	121, 222
Password Logon.....	240	restarting workflows	14
Persist terms and conditions	205	Restrict certificate lifetimes to the card	214
Person Details, skipping	209	Restrict collection of replacement devices if expiry date within (Days).....	222
photos on card layouts	90	Restrict Roles on Child Groups	37, 238
pictures		retry delays	63
card layouts.....	90	Retry On Collection.....	214
PIN Settings.....	118	reverse of cards	87
PIN Timeout.....	234	Revoke certificates if user is removed or disabled following background directory update	54, 209
PINs		Revoke replaced certificate	214
length	233	right to left text	97
logon	21		
PIV Biometric Maximum Age.....	205		
PIV Facial Biometrics Required.....	205		

Role inheritance.....	37	Server Encryption	232
roles	32	Set expiry date at request.....	222
adding	34	Set GlobalPlatform Card Status	236
associating with credential profiles	111	Set Security Phrase at Logon	229
deleting	34	Show all devices	230
editing	32	Show Audit Summary	239
hiding	33	show chip	89
Roles		Show duplicate person warning.....	201
default	38	Show Extended Job Details for Target	217
rotate	89	Show Full Name at Logon	229
SAM field	208	Show Generated PINs	236
scheduled certificate revocation	66	show grid.....	89
scheduled task		Show Photo at Logon	229
Batch Directory Synchronization Tool	56	Show Set Security Phrases Button.....	239
scope	32	Show the Card Content button in the Audit Workflow.....	222
Search a Directory.....	53, 209	Sign Audit on Client	239
searching for jobs	170	Sign Audit on Server	239
Secondary Serial Number	205	Signed Logon.....	229
secret keys	148	signing keys	204
SecuGen fingerprint reader brightness	219	Simple Logon Code Complexity	229
SecuGen minimum capture quality	219	Single Email Notification	223
secure LDAP directory port	52	Skip Person Confirmation screen	209
security events.....	190	smart card logon	36
Security Officer PIN Type.....	230	Smart Card Logon	240
Security Phrase allowable characters	235	smart cards	19
Security Phrase complexity format.....	235	SMS email notifications	201
Security Phrase minimum length.....	235	SMS gateway URL for notifications	201
Security Phrase repeat character limit	235	SMTP Format	136
Security Phrase sequential character limit	235	snap to grid	89
Security Phrase whitespace removal	235	soft certificates	
Security phrases.....	233, 234	credential profile	128
unlocking.....	26	software tokens.....	122
selecting dates.....	16	SOPINs	230
self scope	43	stages	19
Self-service	239	static keys	77, 82, 148
Self-service emergency password	239	Status of jobs	170
Self-service Resynchronization	239	status report	190
Self-Service Unlock	239	Storage method allowed for certificate recovery.....	215
Send Email Notifications	223	Store Secret Keys.....	232
Send Mobile OTP via SMS.....	223		
Serial Number IIN.....	205		
serial numbers	78		
importing	109		

Suspend to revoke period	66, 215	Update group information in the directory ..	210
suspended dates (jobs)	171	Update user information in the directory	210
suspending jobs.....	172	updates	12
Synchronization Tool for LDAP directory	54	upgrading applets	86
System Events workflow	190	uploading images.....	91
System Status workflow	190	UPN field.....	208
targets for jobs.....	171	URL Path	201
Task number timeout.....	239	use key ceremony.....	79, 83
templates	<i>See card layouts</i>	Use logon name for server PIN generation	105, 236
certificate.....	<i>See certificate policies</i>	Use Security Phrase algorithm version 2 ...	236
for email notifications	139	Use SSL for Image Capture.....	211
Temporary Credential Profile Name	201	user images on card layouts.....	90
terminology	19	users, archiving deleted	168
Terms and Conditions During Device Update	206	Valid Period.....	114
terms and conditions, options.....	175	Validate Image Size	211
text		Validate logon certificate.....	230
card layouts.....	95	Validate signing certificates	233
formatting	97	Validator	171
text colors	98	Verify fingerprints during card creation	219
Timeout.....	212	Verify fingerprints during card unlock	220
Token Logon.....	240	Verify fingerprints during card update	220
Token Resync Window.....	206	Video Capture	212
tokens	19	virtual smart card	19
Track Entrust distinguished name changes	209	visible roles	33
transactions, witnessing	49	warning email address for licenses	133
transport keys	79, 83, 148	Windows Logon	30
Transport PIN	236	witness	234
trial license.....	132	witnessing transactions.....	49
Troubleshooting.....	190	Workflow Timeout Warning Delay	201
trusted platform module.....	19	workflows	19
Unblocking Credential	206	access to	34
uninstalling client components	12	restarting	14
Unknown card logon.....	239	xml, card templates.....	100
Unlock Security Phrases	26	zoom	89
unsuspending jobs	172		