



MyID Enterprise

Version 12.9

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

© 2001-2023 Intercede Limited. All rights reserved.

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

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

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

Licenses and Trademarks

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

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

Apache log4net

Copyright 2004-2021 The Apache Software Foundation

This product includes software developed at

The Apache Software Foundation (<https://www.apache.org/>).

Conventions used in this document

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

For example:

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

For example:

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

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

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

For example:

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

For example:

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

Contents

Administration Guide	1
Copyright	2
Conventions used in this document	3
Contents	4
1 Introduction	13
1.1 About this guide	13
1.1.1 Who should read this guide?	13
1.1.2 What do you need to know?	13
1.1.3 What is included in this guide?	14
1.1.4 Where to find more information	14
2 Getting started	16
2.1 Logging on to MyID for the first time	16
2.1.1 Connecting a workstation	16
2.1.2 Logging on to MyID	17
2.1.3 Default security settings	18
2.2 The interface	19
2.2.1 Selecting dates	23
2.2.2 Entering search criteria	23
2.2.3 Using advanced search	25
2.3 Terminology	25
3 Logon mechanisms	27
3.1 Authentication feedback	27
3.2 Logon using a smart card and PIN	27
3.2.1 Smart card states	28
3.3 Logon using security phrases	29
3.3.1 Setting rules for security phrases	30
3.3.2 Changing rules for security phrases	31
3.3.3 Setting the number of security phrases required to authenticate	32
3.3.4 Configuring the number of attempts to enter security phrases	33
3.3.5 Unlocking security phrases	33
3.3.6 Unlocking your own security phrases	34
3.4 Logon using codes	34
3.4.1 Setting up logon codes	35
3.4.2 Using logon codes	39
3.5 Logon using authentication codes	40
3.6 Integrated Windows Logon	43
3.6.1 Integrated Windows Logon for existing user accounts	44
3.6.2 Protected Users group in Active Directory	44
3.7 Windows Hello	44
4 Roles, groups, and scope	46
4.1 Roles	46
4.1.1 Change an existing role	47
4.1.2 Add a role	48

4.1.3 Delete a role	49
4.1.4 Controlling the assigning of roles	50
4.1.5 Assigning logon mechanisms	51
4.2 Role inheritance	52
4.2.1 Role restriction option	52
4.2.2 Setting a group to inherit roles	52
4.2.3 Inherited roles example	53
4.3 Default roles	54
4.3.1 Default roles example	54
4.3.2 Setting up default roles	54
4.3.3 Known issues	56
4.3.4 Synchronizing with LDAP	56
4.4 Linking roles to LDAP	57
4.4.1 Default Active Directory groups	57
4.4.2 Setting up linked roles	58
4.4.3 Example	59
4.5 Scope and security	59
4.5.1 Known issues	60
4.6 Groups	60
4.7 Administrative groups	61
4.7.1 Configuration settings	61
4.7.2 Assigning Administrative Groups	61
4.7.3 The Select Group dialog	62
4.7.4 The Find Person stage	63
4.7.5 The View Person workflow	63
4.7.6 Group management	63
4.7.7 The Import Account Details dialog	64
4.7.8 Scope calculations	64
4.8 Witnessing a transaction	65
5 Using an LDAP directory	67
5.1 Before you connect to the directory	68
5.2 Creating the connections	68
5.3 Using and updating LDAP information	70
5.3.1 Known issues	71
5.4 Using an LDAP directory as the primary data source	71
5.5 The Batch Directory Synchronization Tool	71
5.5.1 Configuring the Synchronization Tool for load sharing	72
5.5.2 How does the Synchronization Tool work?	72
5.5.3 Revoking certificates	73
5.5.4 Running the tool from the Start menu	74
5.5.5 Running the tool from the command line	77
5.5.6 Running as a scheduled task	78
5.5.7 Troubleshooting	78
5.6 Storing the NETBIOS name for a person	80
5.7 Setting up a configuration-only directory	80

5.8 The Active Directory Deletion Tool	81
5.8.1 Scheduled task repeat interval	81
5.8.2 Setting up a Scheduled Task	82
6 Certificate authorities	84
6.1 Certificate refresh configuration	84
6.2 Connecting to a CA	85
6.2.1 Recording a new CA	85
6.2.2 Editing an existing CA	86
6.2.3 Deleting a CA	86
6.3 Enabling certificates on a CA	87
6.4 Scheduled certificate revocation operations	88
6.5 Revoking timed-out certificates	88
6.6 Certificate renewal	89
6.6.1 Credential lifetimes and certificate renewal	89
6.7 Superseding certificate policies	90
6.7.1 Recovering superseded certificates	92
6.7.2 Troubleshooting	92
6.7.3 Viewing superseded certificate policies	93
6.8 Import and distribute certificates to devices	94
6.8.1 Setting up the Unmanaged certificate authority	94
6.8.2 Setting up a credential profile for PFX certificates	94
6.8.3 Uploading multiple PFX certificates	95
6.8.4 Removing uploaded certificates	96
6.9 Including user security identifiers in certificates	97
7 Applets	98
7.1 GlobalPlatform keys	98
7.2 Enabling GlobalPlatform keys	99
7.3 Managing GlobalPlatform keys	99
7.3.1 Entering factory (vendor) keys	100
7.3.2 Using a key ceremony	102
7.3.3 Importing keys from a file	104
7.3.4 Exporting keys	104
7.3.5 Deleting factory (vendor) keys	105
7.3.6 Entering customer (local) keys	105
7.3.7 Deleting customer (local) keys	108
7.3.8 Rotating customer keys	109
7.4 Managing applets	109
7.4.1 Add an applet	109
7.4.2 Edit an applet	110
7.4.3 Upgrade an applet	111
8 Designing card layouts	112
8.1 Restricting access to card layouts	113
8.2 Configuring the image location	113
8.2.1 Setting the list of allowed external server names	114
8.3 Creating, saving and deleting layouts	115

8.4 Using the layout tools	116
8.4.1 Rotating the card	116
8.4.2 Showing the chip	116
8.4.3 Showing the grid, snapping elements and zooming	117
8.5 Images and backgrounds	117
8.5.1 Uploading images to the web server	118
8.5.2 Specifying a background	118
8.5.3 Fitting an image to a card	119
8.5.4 Adding static images	119
8.5.5 Adding dynamic images	120
8.5.6 Custom image fields	120
8.5.7 Externally formatted image fields	121
8.5.8 Image aspect ratio	121
8.6 Adding or changing text	123
8.6.1 Adding and changing static text	123
8.6.2 Adding dynamic text	124
8.6.3 Custom text fields	124
8.7 Formatting text	125
8.8 Changing the text color	126
8.8.1 Using the color picker	126
8.9 Dynamically changing text size	127
8.10 Positioning and sizing elements	127
8.11 Adding barcodes	129
8.11.1 Adding a 1D barcode	130
8.11.2 Previewing a barcode	131
8.11.3 Known issues	133
8.12 Defining data to store on magnetic stripes	134
8.13 Using templates	134
8.13.1 Applying zone settings	134
8.13.2 Template XML structure	135
8.14 Reviewing and testing your layout	137
9 PIN generation	138
9.1 Adding a PIN generation key	139
9.2 Credential profile setup for PIN generation	140
9.2.1 PIN generation for issuance	141
9.2.2 PIN generation for reset	142
9.3 EdficePinGenerator PIN generation algorithm	142
9.3.1 Generating the PIN	142
9.3.2 Alphabet tables	143
9.3.3 Example	144
9.4 EdficePolicyPinGenerator PIN generation algorithm	147
9.4.1 Generating the PIN	147
9.4.2 Alphabet tables	148
9.4.3 Example	150
10 Importing serial numbers	156

10.1 Troubleshooting and known issues with importing serial numbers	157
11 Managing credential profiles	158
11.1 Setting default values	159
11.2 Using the provided credential profile	159
11.3 Working with credential profiles	159
11.3.1 Credential profile options	160
11.3.2 Additional credential profile options	175
11.3.3 Selecting certificates	179
11.3.4 Selecting applets	182
11.3.5 Linking credential profiles to roles	182
11.3.6 Constrain credential profile issuer	182
11.3.7 Constrain credential profile validator	182
11.3.8 Constrain credential profile collector	182
11.3.9 Constrain credential profile unlock operator	183
11.3.10 Associating credential profiles with card layouts	183
11.3.11 Adding comments to the credential profile	183
11.4 Setting up mail merge documents	183
11.4.1 Available fields	184
11.5 Setting up a credential profile for soft certificates	185
11.5.1 Upgraded credential profiles	187
11.6 Customizing terms and conditions	187
11.6.1 Client requirements for HTML templates	188
11.6.2 Customizing terms and conditions using the HTML template method	188
11.6.3 Customizing terms and conditions for the web service	188
11.6.4 Customizing terms and conditions using the SignedTCs.txt method	189
11.6.5 Customizing terms and conditions using the translation method	189
11.6.6 Storing signed terms and conditions	189
11.6.7 Emailing terms and conditions	190
11.7 Enforcing banned words in PINs	191
11.7.1 Dynamic word list	192
11.7.2 Static word list	192
11.7.3 Cache the word list	193
12 License management	194
12.1 View current license status	195
12.2 Requesting licenses	196
12.3 Installing license details	197
12.4 Updating warning messages	198
12.5 Controlling device assignments for groups	198
12.5.1 Limitations	199
13 Email notification	200
13.1 System-wide email settings	200
13.1.1 Switching email notifications on or off	200
13.1.2 Email format	200
13.1.3 Email codepage	200
13.1.4 Email separator	201

13.1.5 Changing the recipient of administrator messages	201
13.1.6 Setting the number of email notifications	201
13.2 Changing email messages	202
13.2.1 Available variables for email messages	203
13.2.2 URL encoded links	203
13.3 Standard templates	203
13.3.1 Triggering the notification	208
13.4 Adding a new email template	209
13.4.1 Known issues	210
13.5 Using the Notifications Management workflow	210
14 REST web service notifications	213
14.1 Configuring an external system for REST notifications	214
14.1.1 Enabling and disabling a notification	216
14.2 Standard REST notifications	217
14.2.1 REST Device Issued notification	219
14.2.2 REST Device Cancelled notification	220
14.2.3 EnableCard notification	221
14.2.4 DisableCard notification	222
14.2.5 REST Person Added notification	223
14.2.6 REST Person Edited notification	224
14.2.7 REST Person Deleted notification	225
14.2.8 REST Person Enabled notification	226
14.2.9 REST Person Disabled notification	227
14.2.10 REST Request Added notification	228
14.2.11 REST Request Updated notification	229
14.3 Creating a mapping file	231
14.3.1 Notification	231
14.3.2 DataSources	231
14.3.3 Endpoint	234
14.3.4 Body	235
14.4 Troubleshooting REST notifications	237
15 Changing list entries	238
16 Managing keys	239
16.1 Using GenMaster	239
16.2 The Key Manager workflow	239
16.2.1 Transport keys	239
16.2.2 Factory 9B keys	241
16.2.3 Customer 9B keys	242
16.2.4 Application keys	244
16.2.5 Exporting keys	245
16.2.6 Entering keys using a key ceremony	246
16.2.7 Known issues	249
16.3 Using RSA transport keys	249
16.3.1 Exporting RSA transport keys	251
16.3.2 Encrypting a key using the RSA public key	252

17 The audit trail	254
17.1 Audit scope	254
17.2 Running the audit report	255
17.2.1 Information icons	256
17.2.2 Browsing through blocks of events	256
17.2.3 Logging the client IP address and identifier	256
17.2.4 Specifying a custom client identifier	258
17.3 Specifying the items to audit	259
18 Key archiving	261
18.1 Archiving and encryption	261
18.1.1 MyID encryption	261
18.1.2 Cards supported	261
18.1.3 Certificate authority key archiving	261
18.1.4 MyID key archiving	261
18.2 Setting up key archiving	262
19 Key recovery	264
19.1 Setting up the credential profile	264
19.2 Requesting a key recovery	265
19.3 Validating a key recovery request	267
19.4 Collecting a key recovery job for another user	267
19.5 Collecting a key recovery job for yourself	268
19.6 Viewing key recovery operations	268
20 External systems	270
21 Archiving deleted users	271
22 Job management	272
22.1 Searching for jobs	272
22.1.1 General search criteria	272
22.1.2 Searching by target	273
22.1.3 Searching by initiator, validator or actioned by	273
22.1.4 Searching by renewal or suspended dates	273
22.2 Viewing job records	273
22.3 Managing jobs	274
22.4 Automatic job cancellation	275
22.4.1 Enabling the automatic job cancellation processor	275
22.4.2 Filtering the canceled jobs by credential profile	276
22.4.3 Specifying the email template for notifications	276
23 Activating cards	277
23.1 Configuring a credential profile for activation	277
23.1.1 Personalization and encoding scenarios	279
23.2 Terms and conditions	279
23.2.1 Viewing audited terms and conditions	280
23.2.2 Known issues	281
23.3 Setting up authentication methods for activation	281
24 Managing devices	283
24.1 Device management overview	283

24.2 Access to the device management workflows	283
24.3 Setting up the SCEP server on a separate machine	284
24.4 Signing and encryption certificates for SCEP	284
24.4.1 Signing certificate	284
24.4.2 Encryption certificate	285
24.4.3 Adding the certificates to the registry	285
24.5 Setting up a credential profile to use to issue device identities	285
24.6 Adding devices	286
24.6.1 Adding devices manually	287
24.6.2 Adding devices from an LDAP directory	288
24.7 Editing a device	289
24.8 Requesting a device identity	290
24.9 Validating a device identity request	291
24.10 Collecting device identities	292
24.11 Canceling device identities	293
24.12 Approving device identity cancellations	294
24.13 Known issues for device identities	294
25 Additional identities	295
25.1 Additional identities overview	295
25.1.1 Renewing additional identities	295
25.1.2 Additional identities on devices with PIV applets	296
25.1.3 User SIDs in additional identities	296
25.2 Setting up additional identities	296
25.3 Adding additional identities	300
25.4 Removing additional identities	302
25.5 Adding an additional identity for your own account	303
26 Triggered scripts	305
26.1 Configuring triggered scripts	305
26.1.1 Script security	306
26.2 Triggered script data format	306
26.2.1 Example output	307
26.2.2 Example script	308
27 Identity checks	309
27.1 User Data Approved checks	309
27.1.1 Configuring the credential profile	309
27.1.2 Allowing device requests before the user's data is approved	309
27.1.3 Setting the User Data Approved flag	309
27.2 Vetting date validity checks	310
27.2.1 Setting the vetting date validity period	310
27.2.2 The vetting date job processor	310
27.3 Certificate renewal checks	311
27.4 Certificate lifetime restrictions	311
27.5 Configuring the identity check email notifications	311
28 Checking card suitability	313
28.1 Creating a card suitability web service	314

28.1.1 Input for the web service	314
28.1.2 Output from the web service	315
28.1.3 Web service authentication	315
28.2 Setting up an external system for card suitability	316
28.2.1 Enabling and disabling the card suitability check	317
28.3 Using the card suitability service	319
29 Troubleshooting	321
29.1 System status report	321
29.2 System events report	322
29.2.1 Archived system events	322
29.3 Expanded error messages	322
29.4 System security	323
30 Operation Settings	324
30.1 General page (Operation Settings)	324
30.2 Devices page (Operation Settings)	329
30.3 LDAP page (Operation Settings)	338
30.4 Video page (Operation Settings)	345
30.5 Certificates page (Operation Settings)	351
30.6 Import & Export page (Operation Settings)	360
30.7 Identity Checks page (Operation Settings)	361
30.8 Bureau & Job page (Operation Settings)	362
30.9 Biometrics page (Operation Settings)	363
30.10 Issuance Processes page (Operation Settings)	363
30.11 Notifications page (Operation Settings)	373
30.12 Identity Agent Policy page (Operation Settings)	376
31 Security Settings	379
31.1 Logon page (Security Settings)	379
31.2 Device Security page (Security Settings)	383
31.3 Server page (Security Settings)	385
31.4 PINs page (Security Settings)	389
31.5 Process page (Security Settings)	396
31.6 Self-Service page (Security Settings)	400
31.7 Logon Mechanisms page (Security Settings)	401
31.8 Logon Priority page (Security Settings)	403
31.9 Auth Code page (Security Settings)	405
Index	409

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 [2.2, The interface](#).

1.1 About this guide

This section contains information about this Administration Guide.

1.1.1 Who should read this guide?

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

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

- Investigating the use of MyID in your organization.
- Designing the deployment strategy for your organization.

1.1.2 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 hyperlinks and forms as well as understanding 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, and 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.

1.1.3 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 *cardholder* has minimal access to MyID. Cardholders 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 [2.2, 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.

1.1.4 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.

2 Getting started

This chapter contains general information on MyID, including:

- How to log on to MyID Desktop.
- Information on the MyID Desktop interface.
- MyID terminology.

For information on launching MyID Desktop, see the *Launching MyID Desktop* section in the [Installation and Configuration Guide](#).

2.1 Logging on to MyID 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.

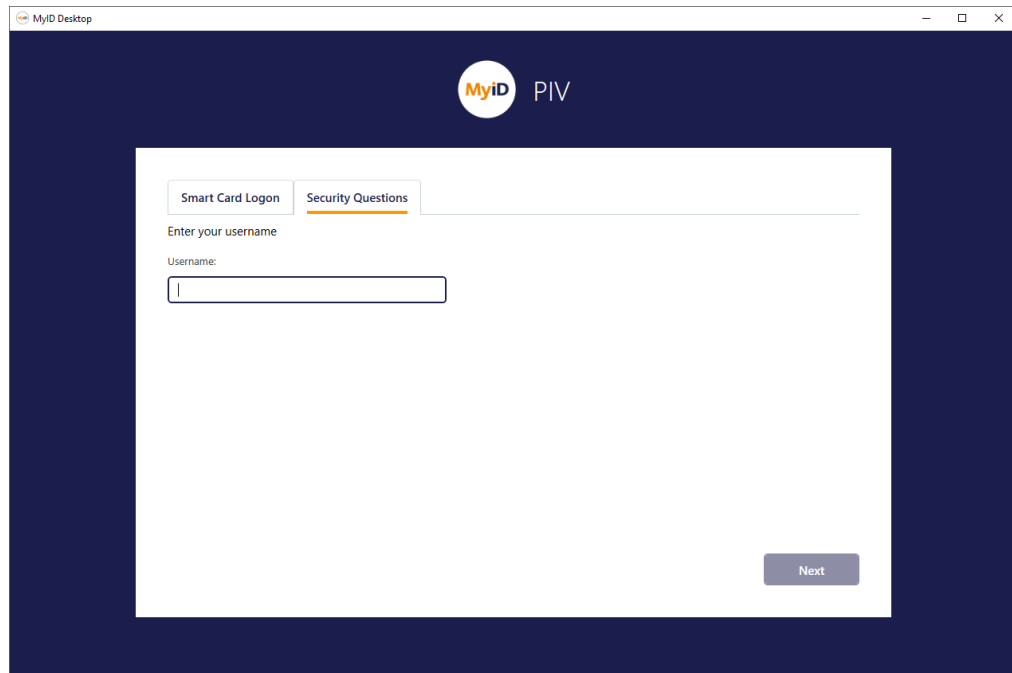
The [Installation and Configuration Guide](#) contains information on using GenMaster to set the passphrase for the startup user.

2.1.1 Connecting a workstation

See the [Installation and Configuration Guide](#) for details of installing and configuring MyID Desktop on your workstations.

2.1.2 Logging on to MyID

Your administrator may have enabled more than one method of accessing MyID. For example, your usual logon method may be to use your smart card, but your administrator may allow you to log on using security questions in case you have lost or forgotten your smart card. For more information, see section [3, Logon mechanisms](#).

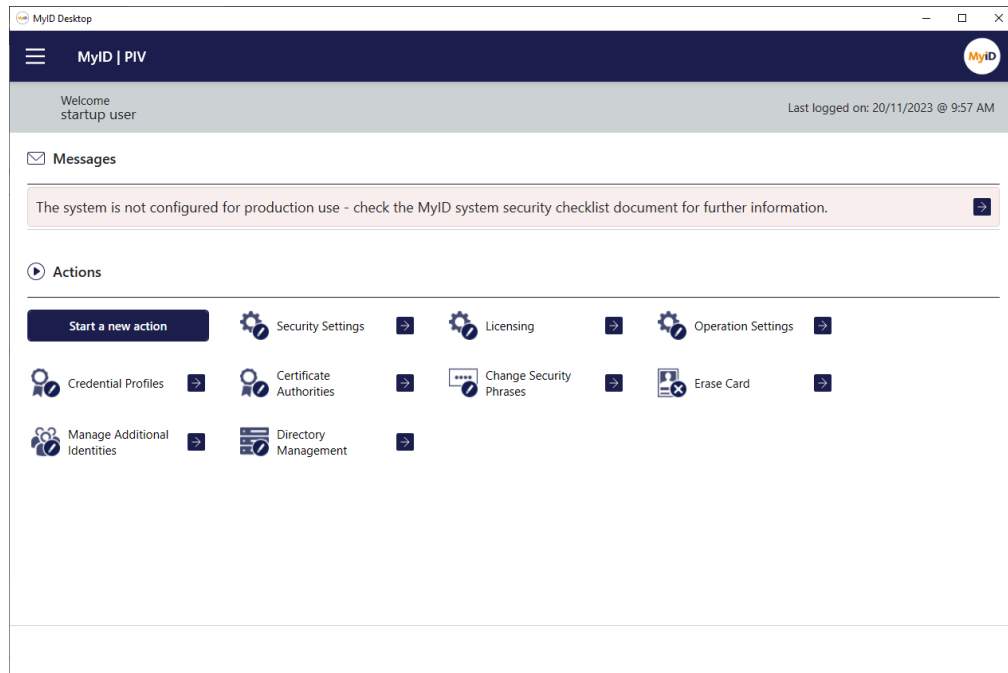


The screenshot shows a web browser window titled "MyID Desktop". The page has a dark blue header with the "MyID PIV" logo. Below the header, there are two tabs: "Smart Card Logon" and "Security Questions". The "Security Questions" tab is selected and highlighted with an orange underline. Below the tabs, the text "Enter your username" is displayed. Underneath, there is a label "Username:" followed by a text input field. A "Next" button is located at the bottom right of the form area.

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

2.1.3 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:

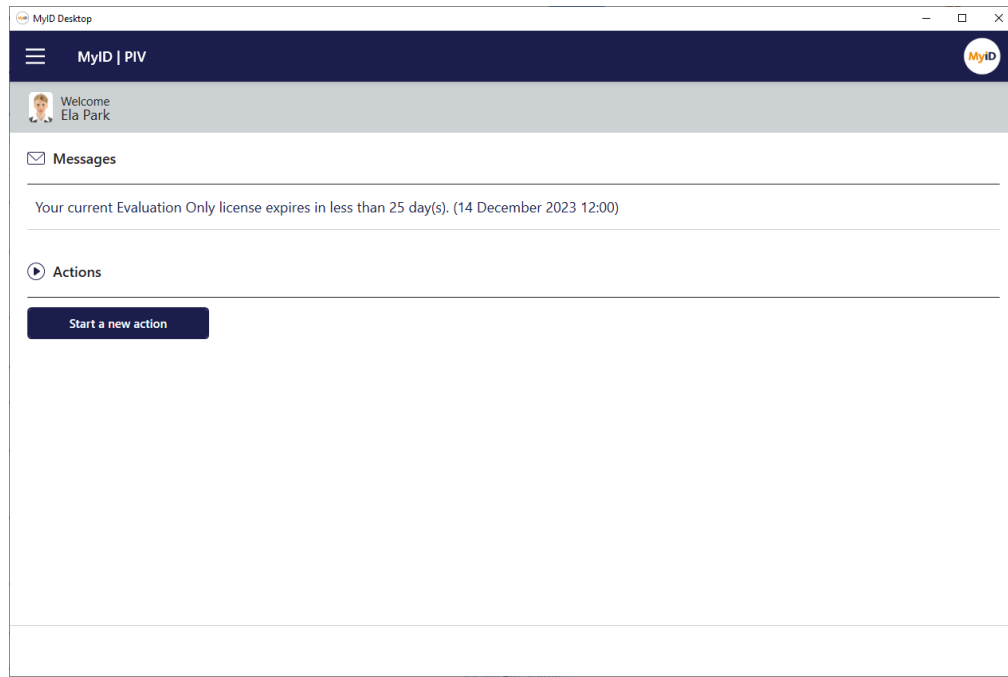
The system is not configured for production use - check the MyID system security checklist document for further information.


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.

2.2 The interface

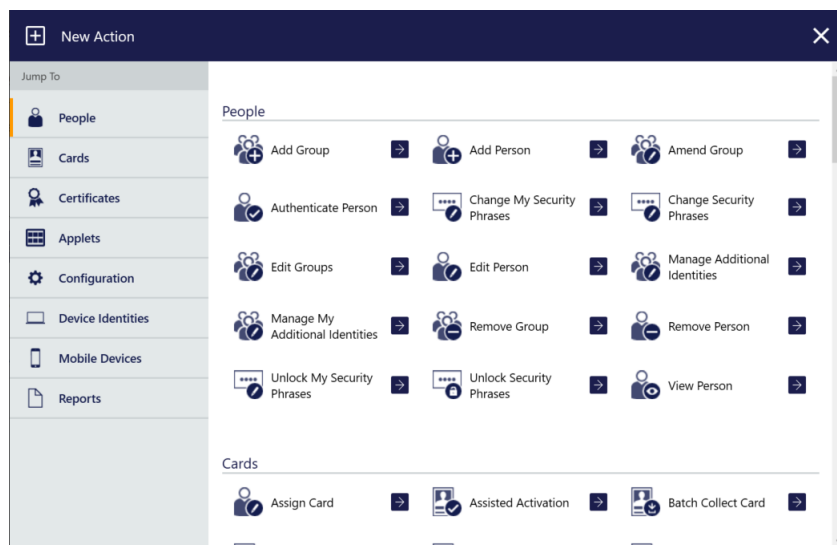
Note: A detailed explanation of the terminology used within MyID and this document is provided in section [2.3, Terminology](#).

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



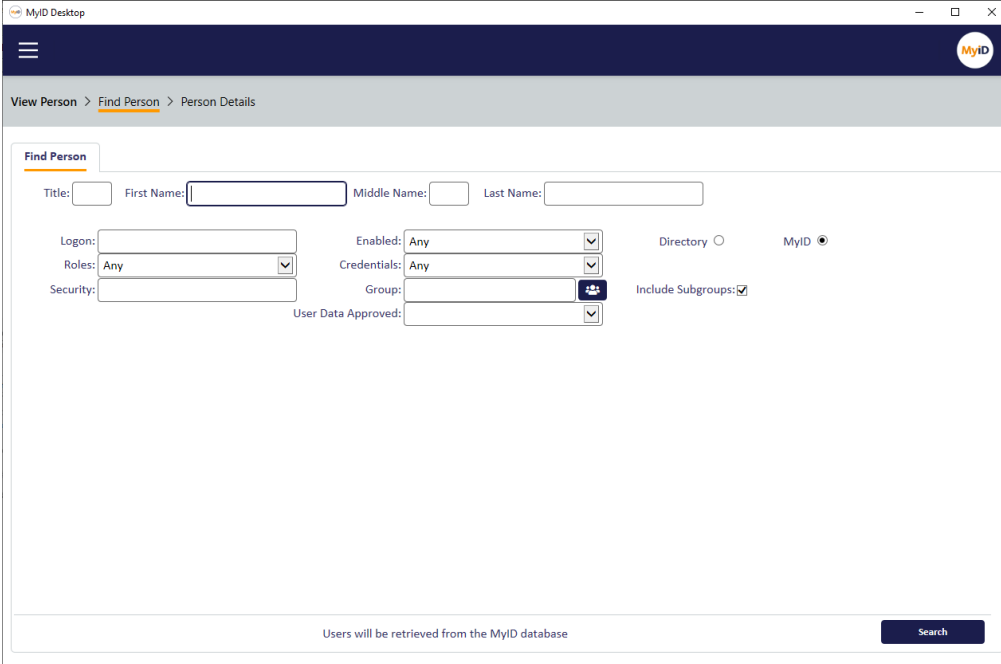
If there are any system messages, they appear at the top of the screen. For some messages, you can click the arrow  to take you to the appropriate workflow; for example, if your system is not set up for production use, clicking the arrow takes you to the **Security Settings** workflow to allow you to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

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



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

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



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

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

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



Enabled, True or Yes



Disabled, No or False




Ask or Prompt




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

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


 Show first page of information.


 Show last page of information.


 Show previous page of information.

 Show next page of information.

 Show next block of information.

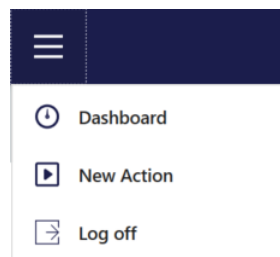
 Show only results.

 Show search criteria.

Rows:  Change the number of rows displayed.

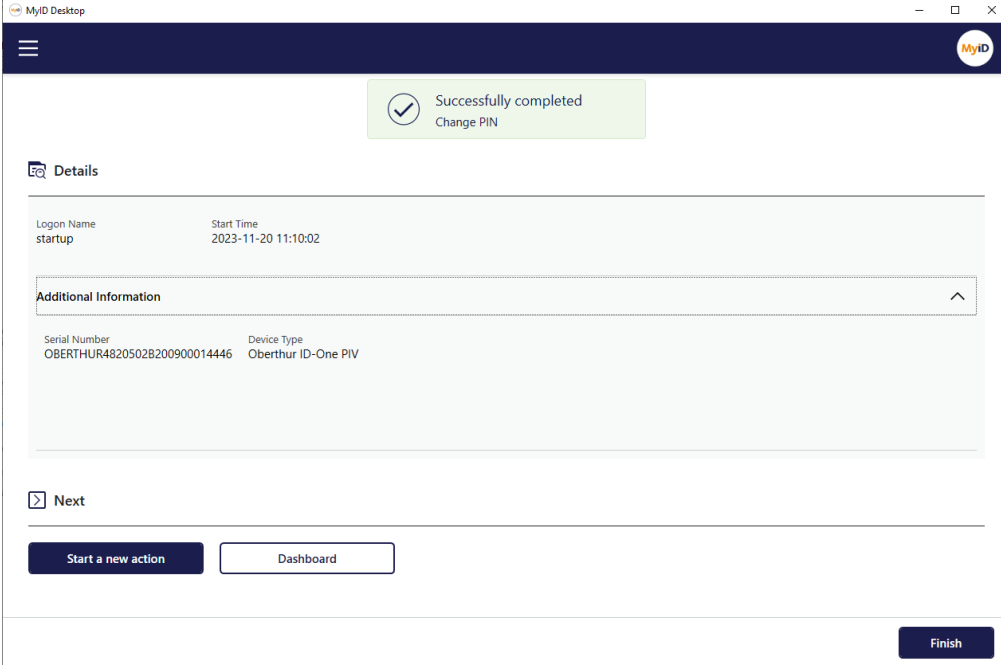
Note: Information displayed in a table can be sorted in ascending or descending order, based on a selected heading. Click a heading to sort by that value; click it again to reverse the sort order.

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



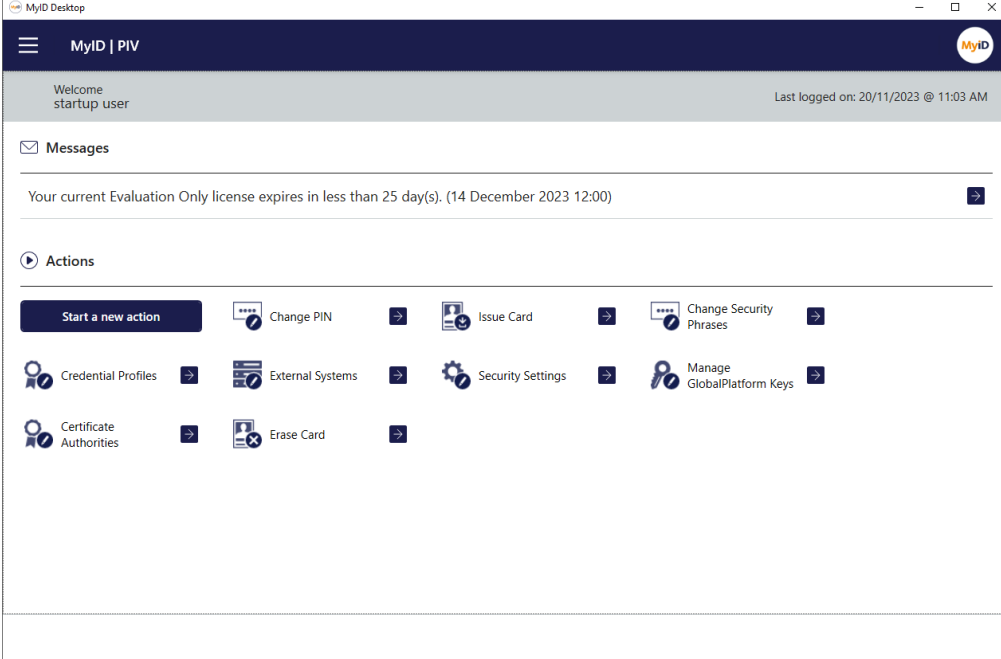
You can return to the dashboard when you are in a workflow, and you can start a new action when you are on the dashboard.

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.



The screenshot shows the 'MyID Desktop' application window. At the top, a green notification box states 'Successfully completed Change PIN'. Below this, the 'Details' section shows 'Logon Name: startup' and 'Start Time: 2023-11-20 11:10:02'. An 'Additional Information' section is expanded, showing 'Serial Number: OBERTHUR4820502B200900014446' and 'Device Type: Oberthur ID-One PIV'. At the bottom, there are buttons for 'Start a new action', 'Dashboard', and 'Finish'.

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

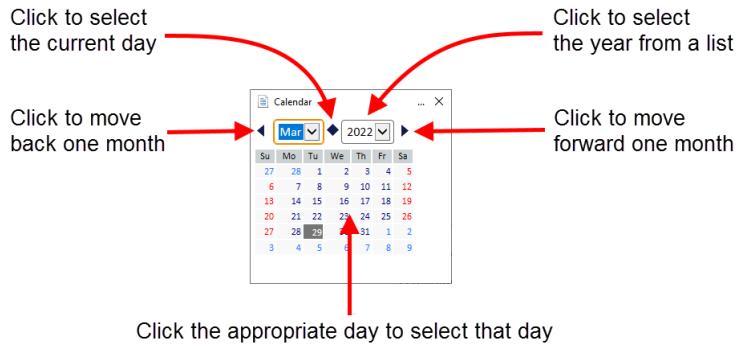


The screenshot shows the 'MyID | PIV' dashboard. It includes a welcome message for 'startup user' and the last login time '20/11/2023 @ 11:03 AM'. A 'Messages' section contains a notification about the 'Evaluation Only license' expiring on '14 December 2023 12:00'. The 'Actions' section features a grid of workflow buttons: 'Start a new action', 'Change PIN', 'Issue Card', 'Change Security Phrases', 'Credential Profiles', 'External Systems', 'Security Settings', 'Manage GlobalPlatform Keys', 'Certificate Authorities', and 'Erase Card'.

2.2.1 Selecting dates

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

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



2.2.2 Entering search criteria

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

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

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

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

For example:

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

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

- MySam Jones

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

For example, `sam jon` will find:

- Samuel Jones
- Jonathon Samson

But not:

- Sam Littlejohn

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

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

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

Or any prefix of those elements.

You can find `John O'Reilly` using:

- `John`
- `O'Reilly`

But not:

- `Reilly`

You can find `Ralph Fiennes-Johnson` using:

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

You can find any accented characters using their plain equivalent.

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

- `Heinz`
- `Muller`

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

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

and so on.

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

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

- `jones/sm`

to find:

- `jones-smith`

2.2.3 Using advanced search

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

Search bar: [X] [Filter Icon] 4 filters selected

Attribute:	Where:	Value:
Forename	Equals	Alpha
Group	In and Below	Root
Enabled	Equals	Yes

Add Filter **Delete All Filters**

Please enter search criteria.

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

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

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

2.3 Terminology

The MyID documentation set uses the following terminology:

Term	Description
administrator	A person who is responsible for the configuration and maintenance of MyID.
applet	A small program stored on a <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.

Term	Description
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.

3 Logon mechanisms

You can log on to MyID using:

- Smart card logon (using a smart card and a PIN) – see section [3.2, Logon using a smart card and PIN](#).
- Security Questions (a logon name and up to five passwords) – see section [3.3, Logon using security phrases](#)
- Logon codes (one-time codes that are sent by email to allow a cardholder to log on) – see section [3.4, Logon using codes](#).
- Windows logon (using your Windows account to authenticate to MyID) – see section [3.6, Integrated Windows Logon](#).
- Windows Hello (using your Windows Hello credentials to authenticate to MyID) – see section [3.7, Windows Hello](#).

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.

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 Logon using a smart card and PIN

The usual way to log on to MyID is using a card (a smart card, USB token, or VSC). 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**.

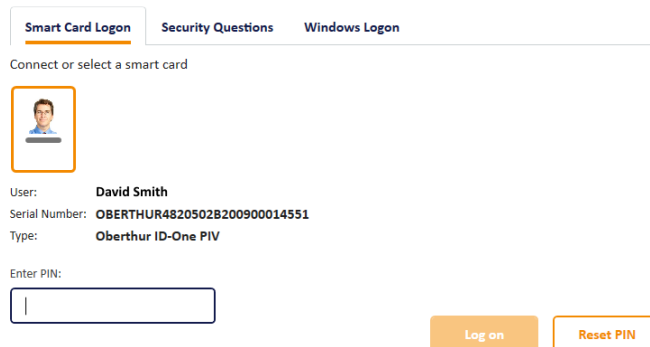
4. In the **Edit Roles** workflow, make sure the user's role has the **Smart Card** logon mechanism assigned.

See section [4.1.5, Assigning logon mechanisms](#) for details of using the **Edit Roles** workflow.

3.2.1 Smart card states

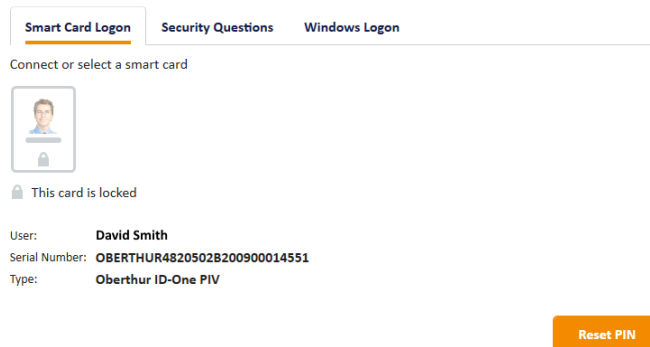
The color and icon used on the **Smart Card Logon** tab tell you the state of the card inserted in the card reader.

Valid card ready to be used for logon:



The interface shows the 'Smart Card Logon' tab selected. Below the tabs, it says 'Connect or select a smart card'. A card icon is displayed with a green border, indicating it is ready. Below the icon, the user information is shown: User: David Smith, Serial Number: OBERTHUR4820502B200900014551, Type: Oberthur ID-One PIV. There is a text input field labeled 'Enter PIN:' and two buttons: 'Log on' and 'Reset PIN'.

Locked card:




The interface shows the 'Smart Card Logon' tab selected. Below the tabs, it says 'Connect or select a smart card'. A card icon is displayed with a grey border and a lock icon, indicating it is locked. Below the icon, the user information is shown: User: David Smith, Serial Number: OBERTHUR4820502B200900014551, Type: Oberthur ID-One PIV. There is a button labeled 'Reset PIN'.

Card ready for activation:

Smart Card Logon
Security Questions
Windows Logon

Connect or select a smart card



✓ This card is ready for activation


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

Activate

Invalid card:

Smart Card Logon
Security Questions
Windows Logon

Connect or select a smart card



✗ This card cannot be used

Serial Number: **OBERTHUR4820502B200900025429**
 Type: **Oberthur ID-One PIV**

3.3 Logon using security phrases

You can log on to MyID Desktop or the MyID Operator Client 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 their security phrases.

3.3.1 Setting rules for security phrases

Rules for security phrases can be specified by using a combination of configuration settings. See section [31.4, 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:

Parameter		Notes
mm	minimum length	If not specified, this defaults to 4.
nn	maximum length	If not specified, this defaults to 8.
u	may contain uppercase characters	If neither <code>u</code> nor <code>U</code> is present, the security phrase cannot contain uppercase characters.
U	must contain uppercase characters	

Parameter		Notes
l	may contain lowercase characters	If neither l nor L is present, the security phrase cannot contain lowercase characters.
L	must contain lowercase characters	
n	may contain a number	If neither n nor N is present, the security phrase cannot contain numbers.
N	must contain a number	
s	may contain a symbol	Allowable symbols are: - ! \$ % ^ & * () _ + ~ = ` { } [] : " ; ' < > ? , . / @ # \ and <space>
S	must contain a symbol	

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:

12345678abcdefghABC123!?

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.

ABCabc12ABCabcABABCabc1!

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.

Important: Do not increase this value to a number greater than the number of security phrases your users already have registered. If a user does not have at least as many security questions registered as are required for self-service authentication, they will be unable to log on using security phrases.

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 randomly-selected security phrases from a larger number of different questions 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 MyID Desktop 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. This option does not affect the logon process when using the MyID Operator Client.

3.3.4 Configuring the number of attempts to enter security phrases

The **Maximum allowed security question failures** configuration option (on the **Logon** page of the **Security Settings** workflow) determines how many attempts a user is allowed to enter their security phrases before their security phrases are locked.

By default, this is three attempts.

Note: If you set this option to 0, the default value of 3 is used and the user's account is locked when three attempts have been made without success. If you want to provide unlimited attempts to enter security phrases, you can set the **Action on maximum security question failures** option (on the **PINs** page of the **Security Settings** workflow) to None.

3.3.5 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.

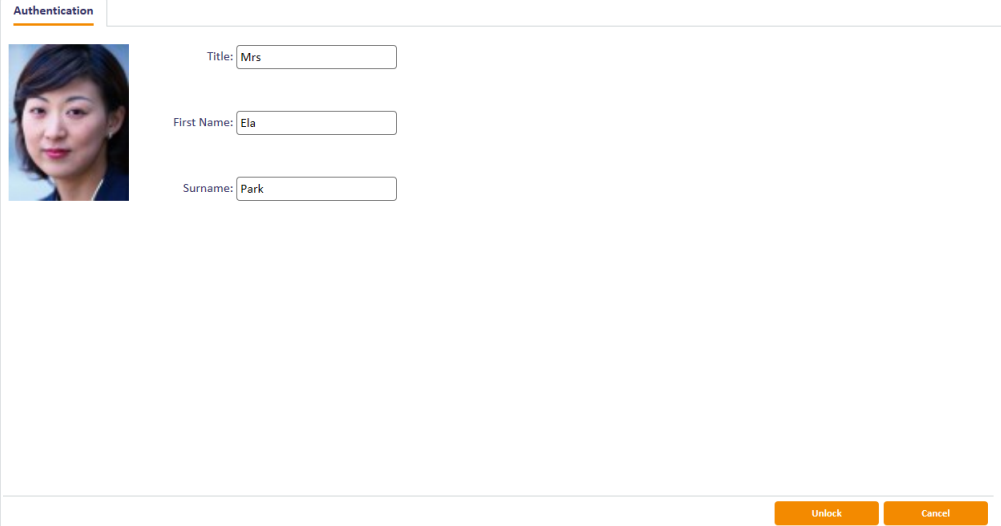
To unlock a user's security phrases:

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

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

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.



The screenshot shows a user interface for the 'Authentication' workflow. On the left, there is a profile picture of a woman. To the right of the picture, there are three text input fields: 'Title:' with 'Mrs' entered, 'First Name:' with 'Ela' entered, and 'Surname:' with 'Park' entered. At the bottom right of the form, there are two orange buttons: 'Unlock' and 'Cancel'.

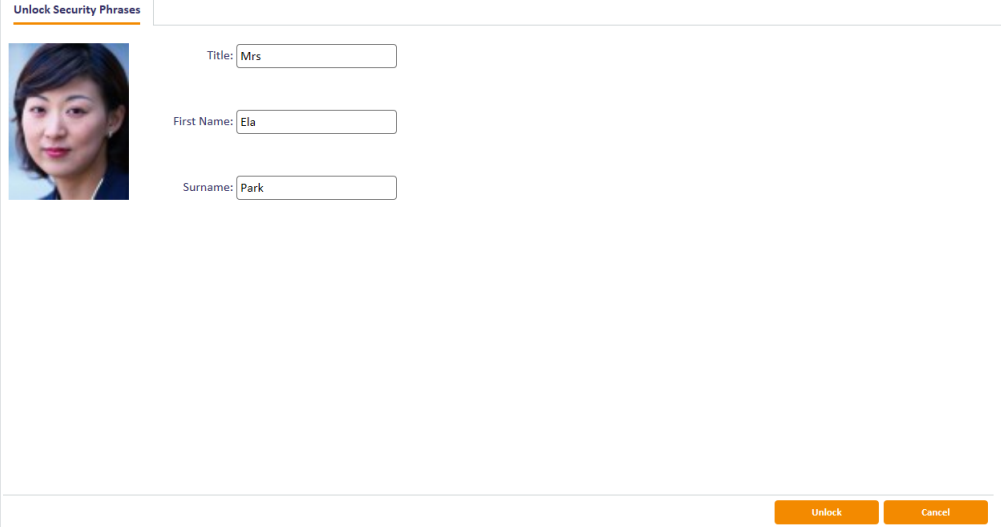
4. Click **Unlock**.

3.3.6 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**.



The screenshot shows a web interface for unlocking security phrases. It features a header 'Unlock Security Phrases' and a profile picture of a woman. To the right of the picture are three text input fields: 'Title: Mrs', 'First Name: Ela', and 'Surname: Park'. At the bottom right are two buttons: 'Unlock' and 'Cancel'.

2. Click **Unlock**.

3.4 Logon using 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 can request another code using the Send Auth Code feature on the View Request screen in the MyID Operator Client; alternatively, you can 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.

For systems that use the MyID authentication server (for example, the MyID Operator Client, or the MyID Core API) you can use authentication codes instead; see section [3.5, Logon using authentication codes](#).

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 use logon codes. If you set this option to No, MyID will send logon codes if the **Generate Code on Request** option in the credential profile is set, but you will be unable to use the codes to log on.
 - **Maximum allowed security question failures** – Specify the maximum number of failed attempts a user can make when attempting to enter a logon code or answer a security question.

Note: If you set this option to 0, the default value of 3 is used and the user's account is locked when three attempts have been made without success. If you want to provide unlimited attempts to enter logon codes, you can set the **Action on maximum security question failures** option (on the **PINs** page of the **Security Settings** workflow) to None.
3. On the **Logon Mechanisms** tab, set the following option:
 - **Password Logon** – set this option to **Yes**.
4. On the **Auth Code** tab, set the following option:
 - **Auth Code Complexity** – set this to the complexity you want to use for requests where the complexity is not specified in the credential profile or in the email template. Select one of the following:
 - **Complex** – uses the complexity determined by the **Complex Logon Code Complexity** configuration option. This is the default.
 - **Simple** – uses the complexity determined by the **Simple Logon Code Complexity** configuration option.
 - **Auth Code Lifetime for Immediate Use** – set this to the number of seconds for which a short lifetime authentication code is valid. To set short lifetime authentication codes for no expiry, set this value to 0. The default is 120 seconds (two minutes). This lifetime is used for codes sent manually from the View Request screen of the MyID Operator Client when you select the short lifetime from the drop-down list.

- **Complex Logon Code Complexity** – the complexity used when you select **Complex Logon Code** from the **Generate Code on Request** drop-down list in the credential profile. By default, this is 12-12ULSN[BGI10QDSZ].

This complexity is also used for codes sent manually from the View Request screen in the MyID Operator Client where the credential profile has the **Generate Code on Request** option set to **None** and the **Auth Code Complexity** option is set to **Complex**.

Complexity settings (both simple and complex) take the format `mm-nnULSN[<excluded>]`.

`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)

Specify any characters you do not want to use in the generated code in the `<excluded>` list; for example:

12-12UN[1IO0]

to exclude the number 1 and letter I, and number 0 and letter O.

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

Note: If you have set the **Case sensitive security questions** configuration option (on the **PINs** page of the **Security Settings** workflow) to No, make sure that you have not included `L` or `l` (must/may contain lower case letters) in your complexity format; otherwise, you will be unable to use the generated codes. Use a code like 12-12USN instead.

- **Logon Code Lifetime** – set this to the number of hours for which a logon code is valid for collecting a job. To set logon codes for no expiry, set this value to 0. The default is 720 hours (30 days).

This lifetime is used for codes sent automatically when the device is requested, and for codes sent manually from the View Request screen of the MyID Operator Client when you select the long lifetime from the drop-down list.

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

This complexity is also used for codes sent manually from the View Request screen in the MyID Operator Client where the credential profile has the **Generate Code on Request** option set to **None** and the **Auth Code Complexity** option is set to **Simple**.

5. Click **Save changes**.
6. In the **Edit Roles** workflow:
 - a. Make sure the cardholder's role has the **Password** logon mechanism assigned.
See section [4.1.5, Assigning logon mechanisms](#).

- b. If you want to request codes from the View Request screen in the MyID Operator Client, make sure the operator has the **Send Auth Code for Job Collection** or **View Auth Code for Job Collection** option selected for their role.
7. From the **Configuration** category, select **Credential Profiles**.
8. Select the profile you want to edit, and click **Modify**.
9. Select the **Issuance Settings** section.
10. For **Generate Code on Request**, select one of the following:
 - **None** – no logon code is generated when the device is requested. However, you can still send or view a code manually from the View Request screen in the MyID Operator Client; see the *Sending collection codes* section in the [MyID Operator Client](#) guide for details.
 - **Simple Logon Code** – the logon code is generated using the complexity rules as defined by the **Simple Logon Code Complexity** configuration option.
 - **Complex Logon Code** – the logon code is generated using the complexity rules as defined by the **Complex Logon Code Complexity** configuration option.

When the device is requested, if the **Generate Code on Request** option is **Simple Logon Code** or **Complex Logon Code**, MyID sends an email message containing the logon code.

Note: If you send a code manually from the View Request screen in the MyID Operator Client, the complexity of the code is determined by the **Generate Code on Request** option in the credential profile. If, however, the **Generate Code on Request** option is set to **None**, the complexity of the code is determined by the **Auth Code Complexity** option (on the **Auth Code** page of the **Security Settings** workflow).
11. Click **Next** and complete the workflow.
12. If you intend to send codes manually through email or SMS from the View Request screen in the MyID Operator Client, from the **Configuration** category, select **Email Templates**.

The methods of delivery for the authentication code are determined by the enabled status of the following email templates:

- **Job Collection Auth Code Email** – used to send an authentication code in an email message to the person's configured email address. By default, this delivery method is enabled.
This is the template used when you select **Collection Code Email** from the **Delivery Mechanism** drop-down list on the Send Collection Code screen.
- **Job Collection Auth Code SMS** – used to send an authentication code in an SMS message to the person's configured cell phone number. By default, this delivery method is disabled.
This is the template used when you select **Collection Code SMS** from the **Delivery Mechanism** drop-down list on the Send Collection Code screen.

Make sure the delivery methods you want to use are enabled. If you disable both email templates, the operator cannot send a collection code, but may still be able to view a collection code on screen using the View Auth Code feature.

Important: You can edit the content of the email templates, and enable or disable them, but do not change the **Transport** option, or the notifications will no longer work correctly.

13. Set up an SMTP server.

Note: If your business process requires operators to view codes on their screens, and you do not intend to send any codes from the MyID server through email or SMS, you do not have to set up an SMTP server.

See the *Setting up email* section in the [Advanced Configuration Guide](#) for details.

14. If you are using SMS to send the authentication codes, configure your system for SMS notifications:

- a. From the **Configuration** category, select **Operation Settings**.

- b. On the **General** tab, set the following:

- **SMS email notifications** – set to Yes.
- **SMS gateway URL for notifications** – set to the URL of your SMS gateway.

By default, SMS messages are sent to through an email to SMS gateway, in the format `<cellnumber>@<gateway>`, where:

- `<cellnumber>` – the cell phone number from the person's record.
- `<gateway>` – the URL from the **SMS gateway URL for notifications** option.

For example: 00447700900123@msggateway.com

If this is not suitable, you can customize the `sp_CustomPrepareSMS` stored procedure in the MyID database.

- c. Click **Save changes**.

15. Recycle the web service app pools:

- a. On the MyID web server, in Internet Information Services (IIS) Manager, select **Application Pools**.

- b. Right-click the **myid.web.oauth2.pool** application pool, then from the pop-up menu click **Recycle**.

- c. Right-click the **myid.rest.core.pool** application pool, then from the pop-up menu click **Recycle**.

This ensures that the MyID Operator Client picks up the configuration changes.

Note: You must recycle the app pools whenever you make a change to these settings; for example, when changing the availability of email templates or changing the value of a configuration option.

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 if there is a valid code available. Note, however, that if the logon code has expired, and your system is configured to allow logon using security phrases, the Self-Service Kiosk and the Self-Service App revert to asking for security phrases to authenticate.

In MyID Desktop, if a user has been provided with a logon code, you must start the program using the `/lc` command-line option. If the logon code has expired, MyID Desktop does not revert to asking for security phrases; you must close down MyID Desktop and open it again without the `/lc` command-line option if you want to log on with security phrases.

Important: When you specify the `/lc` command-line option, you must also specify a workflow using the `/opid` command-line option to determine the workflow that starts after the user has logged on.

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

- 216 – **Collect My Card**
- 217 – **Request Replacement Card**
- 706 – **Collect My Certificates**

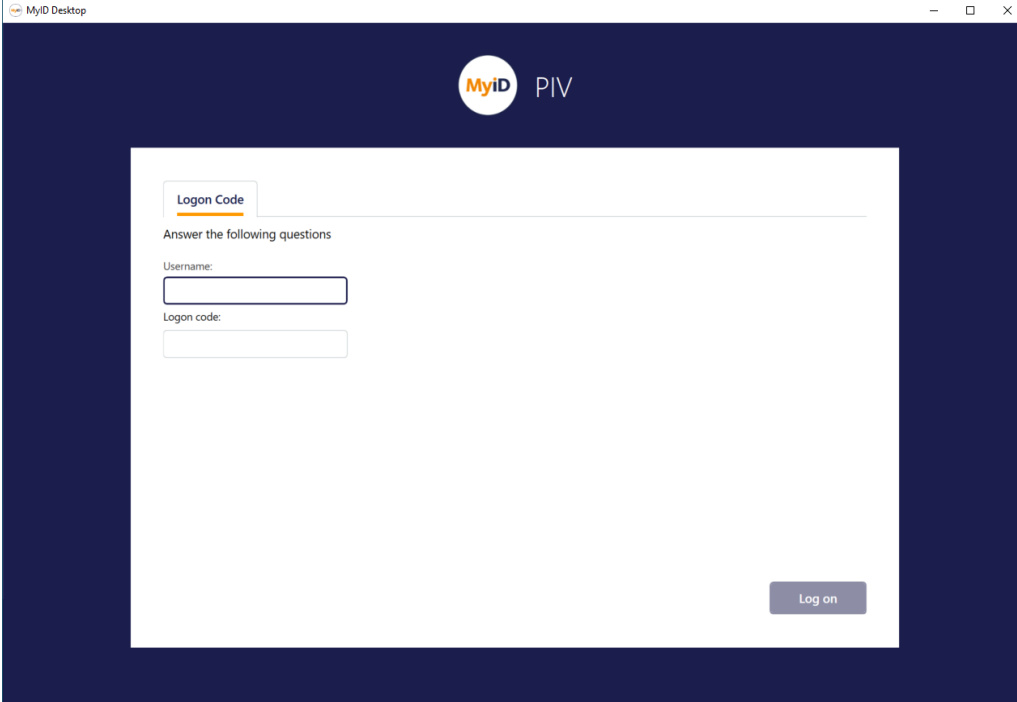
For example:

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

If you do not include an `/opid` parameter with the `/lc` parameter, MyID Desktop displays an error similar to:

```
Incorrect or duplicate command switch
```

MyID Desktop requests your username and logon code:



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
```

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 Logon using authentication codes

For systems that use the MyID authentication server, you can configure MyID to allow a person to request a single-use authentication code that is sent to their email address or as an SMS message to their cell phone.

Once you have received an authentication code, you can use it to authenticate to the MyID authentication server, and therefore access either your own external system or the MyID Operator Client. See the *Signing in using single-use authentication codes* section in the [MyID Operator Client](#) guide for details of requesting and using authentication codes.

For information on using this authentication mechanism to carry out end-user authentication for your own external systems; see the *Configuring the web service for OpenID Connect* section in the [MyID Authentication Guide](#).

Alternatively, you can configure MyID to allow an operator to request a single-use authentication code to be provided to another person for them to use to authenticate to the MyID authentication server. See the *Sending an authentication code to a person* and *Viewing an authentication code for a person* sections in the [MyID Operator Client](#) guide for details of sending or viewing authentication codes.

To set up MyID to use authentication codes:

1. Set the configuration options:
 - a. From the **Configuration** category, select **Security Settings**.
 - b. On the **Logon Mechanisms** tab, set the following:
 - **Authentication Code Logon** – set this option to Yes to allow logon using single-use authentication codes. If this option is set to No, the Authentication Code option does not appear on the sign in screen.
 - c. On the **Logon** tab, set the following:
 - **Maximum Allowed OTP Failures** – set this option to the maximum number of times you can attempt to enter a single-use authentication code. Once the number of failures exceeds this value, you cannot use the authentication code, and must request a new one.
 - d. On the **Auth Code** tab, set the following:

- **Auth Code Complexity** – specify the complexity of codes when there is no complexity specified in an email template (for example, when an operator views a code on screen).
 - **Complex** – uses the complexity determined by the **Complex Logon Code Complexity** configuration option. This is the default.
 - **Simple** – uses the complexity determined by the **Simple Logon Code Complexity** configuration option.
 - **Auth Code Lifetime** – set this to the number of seconds for which a long lifetime authentication code is valid. To set long lifetime authentication codes for no expiry, set this value to 0. The default is 720 hours.
 The long lifetime is used for operator-requested authentication codes when the operator selects the long lifetime at the request screen.
 - **Auth Code Lifetime for Immediate Use** – set this to the number of seconds for which a short lifetime authentication code is valid for logging on to the MyID Operator Client. To set short lifetime authentication codes for no expiry, set this value to 0. The default is 120 seconds.
 The short lifetime is used for self-requested authentication codes, and for operator-requested authentication codes when the operator selects the short lifetime at the request screen.
- e. Click **Save changes**.
2. Configure the logon methods for the roles:
 - a. From the **Configuration** category, select **Edit Roles**.
 - b. Click **Logon Methods**, and select the **Authentication Code** option for each role you want to be able to log on using an authentication code.
 - c. Click **OK**.
 - d. If you want an operator to be able to send or view codes from the View Person screen in the MyID Operator Client, make sure the operator has the **Send Auth Code for Logon** or **View Auth Code for Logon** options selected for their role.
 - e. Click **Save Changes**.
 3. From the **Configuration** category, select **Email Templates**.
 The methods of delivery for the authentication code are determined by the enabled status of the following email templates:
 - For authentication codes requested by the person at the login screen for their own use:
 - **Self Requested Authentication Code Email** – used to send an authentication code in an email message to the person's configured email address. By default, this delivery method is enabled.
 - **Self Requested Authentication Code SMS** – used to send an authentication code in an SMS message to the person's configured cell phone number. By default, this delivery method is disabled.

Make sure the delivery methods you want to use are enabled. You can choose one or both of the delivery methods. If you disable both templates, a person can still use an authentication code to log in, but it must be requested by an operator.

- For authentication codes requested by an operator for another person to use at the logon screen:
 - **Authentication Code Email** – used to send an authentication code in an email message to the person's configured email address. By default, this delivery method is enabled.
 - **Authentication Code SMS** – used to send an authentication code in an SMS message to the person's configured cell phone number. By default, this delivery method is disabled.

Make sure the delivery methods you want to use are enabled. You can choose one or both of the delivery methods. If you disable both templates, a person can still request an authentication code for their own use (providing the appropriate self request templates are enabled) or an operator can view an authentication code using the View Auth Code feature.

Note: The complexity of the code is determined by the **Complexity** option configured in the email template. See section [13.2, *Changing email messages*](#) for details.

Important: You can edit the content of the email templates, and enable or disable them, but do not change the **Transport** option, or the notifications will no longer work correctly.

4. Set up an SMTP server.

Note: If your business process requires operators to generate codes for other people and view codes on their screens, and you do not intend to send any codes from the MyID server through email or SMS, you do not have to set up an SMTP server.

See the *Setting up email* section in the [Advanced Configuration Guide](#) for details.

5. If you are using SMS to send the authentication codes, configure your system for SMS notifications:

- a. From the **Configuration** category, select **Operation Settings**.
- b. On the **General** tab, set the following:

- **SMS email notifications** – set to Yes.
- **SMS gateway URL for notifications** – set to the URL of your SMS gateway.

By default, SMS messages are sent to through an email to SMS gateway, in the format `<cellnumber>@<gateway>`, where:

- `<cellnumber>` – the cell phone number from the person's record.
- `<gateway>` – the URL from the **SMS gateway URL for notifications** option.

For example: `00447700900123@smsgateway.com`

If this is not suitable, you can customize the `sp_CustomPrepareSMS` stored procedure in the MyID database.

- c. Click **Save changes**.

6. Recycle the web service app pools:
 - a. On the MyID web server, in Internet Information Services (IIS) Manager, select **Application Pools**.
 - b. Right-click the **myid.web.oauth2.pool** application pool, then from the pop-up menu click **Recycle**.
 - c. Right-click the **myid.rest.core.pool** application pool, then from the pop-up menu click **Recycle**.

This ensures that the MyID Operator Client picks up the configuration changes.

Note: You must recycle the app pools whenever you make a change to these settings; for example, when changing the availability of email templates or changing the value of a configuration option.

3.6 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.

This section contains instructions for configuring MyID Desktop for Integrated Windows Logon. For information about configuring the MyID Operator Client for Integrated Windows Logon, see the *Signing in using Windows authentication* section in the [MyID Operator Client](#) guide.

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.
 - c. MyID attempts to connect to the directory and, if successful, displays a list of possible DNs. Select one of the DNs from the list.
 - d. In most cases, you must select the DN that begins `CN=Configuration`.
 - e. Click **Save**.

See section 5.7, [Setting up a configuration-only directory](#) for more information.

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. The `Domain` must contain the NetBIOS domain name and not the DNS format.

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 website 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 *Configuring the MyID web services for Integrated Windows Logon* section in the [Web Service Architecture](#) for details.

3.6.1 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.

3.6.2 Protected Users group in Active Directory

You cannot use Integrated Windows Logon with a user who is a member of the Protected Users group in Active Directory. Membership in the Protected Users group is designed to be restrictive and proactively secure by default.

If you attempt to use a member of this group to sign on to MyID using Integrated Windows Logon, you may see an error similar to the following:

```
800551 - Logon Denied.
```

You may also see an error similar to the following in the Windows Events:

```
NTLM authentication failed because the account was a member of the
Protected Users group.
```

3.7 Windows Hello

If you set up the MyID server to use Windows Hello, MyID Desktop can use the cardholder's Windows Hello for Business credentials to authenticate to MyID without having to enter passphrases or use a smart card.

For more information, see the *Setting up Windows Hello for logon* section in the [**Windows Hello for Business Integration Guide**](#).

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, 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

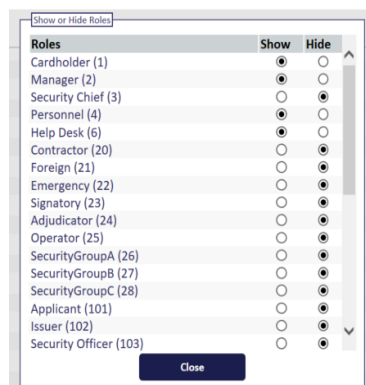
A subset of available roles is visible when you start the **Edit Roles** workflow. If the one you want to change is currently hidden, you must make it visible before you can make any changes. You may also want to hide some of the visible roles that you are not currently working on.

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

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

You can also launch this workflow from the **Configuration Settings** section of the **More** category in the MyID Operator Client. See the *Using Configuration Settings workflows* section in the [MyID Operator Client](#) guide for details.

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



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

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

3. Locate the column heading of the role you want to change.
 - The **Full Access to Manager Controlled Lists** option is reserved for future use.
 - If a workflow is selected, it appears in the list of workflows available to people assigned that role when they access MyID.
 - If a workflow box is cleared, it is not included in the list of workflows.

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

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

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

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

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

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

4.1.1.1 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. From the **Configuration** category, select the **Edit Roles** workflow.

You can also launch this workflow from the **Configuration Settings** section of the **More** category in the MyID Operator Client. See the *Using Configuration Settings workflows* section in the [MyID Operator Client](#) guide for details.

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. From the **Configuration** category, select the **Edit Roles** workflow.
You can also launch this workflow from the **Configuration Settings** section of the **More** category in the MyID Operator Client. See the *Using Configuration Settings workflows* section in the *MyID Operator Client* guide for details.
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.

Option	Cardholder	Manager	Personnel	Help Desk
Managed By				
Linked to LDAP Group				
Full Access to Manager Controlled Lists	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
People	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Add Group	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Add Person	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" 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)
- ☐ Manager (2)
- ☐ Security Chief (3)
- ☐ Personnel (4)
- ☐ Help Desk (6)
- ☐ Contractor (20)
- ☐ Foreign (21)
- ☐ Emergency (22)
- ☐ Signatory (23)
- ☐ Adjudicator (24)
- ☐ Operator (25)
- ☐ SecurityGroupA (26)
- ☐ SecurityGroupB (27)
- ☐ SecurityGroupC (28)
- ☐ Applicant (101)
- ☐ Issuer (102)
- ☐ Security Officer (103)
- ☐ Registrar (104)
- ☐ Sponsor (105)
- ☐ View Device Initial PIN (106)
- ☐ Default SSA User (100)

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:
AuditorThis role cannot be deleted at this time.

Note: Default group roles can override any managed roles you have set up; see section 4.3, [Default roles](#) for more information about default roles.

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.

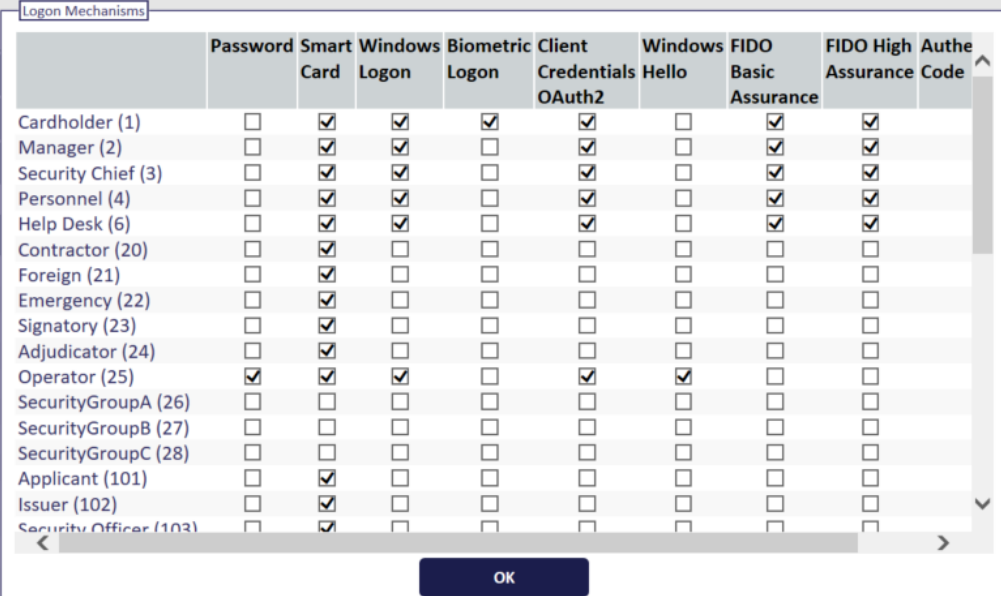
The logon mechanisms that you can use depend on which options you have selected on the **Logon Mechanisms** page of the **Security Settings** workflow; see section 3, [Logon mechanisms](#) for details.

To specify logon mechanisms:

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

You can also launch this workflow from the **Configuration Settings** section of the **More** category in the MyID Operator Client. See the *Using Configuration Settings workflows* section in the [MyID Operator Client](#) guide for details.

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	Client Credentials OAuth2	Windows Hello	FIDO Basic Assurance	FIDO High Assurance	Authn Code
Cardholder (1)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Manager (2)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input 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 type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Personnel (4)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input 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 type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Contractor (20)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Foreign (21)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Emergency (22)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Signatory (23)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Adjudicator (24)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Operator (25)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
SecurityGroupA (26)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
SecurityGroupB (27)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
SecurityGroupC (28)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Applicant (101)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Issuer (102)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Security Officer (103)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

- **Password** is used for security phrase logon. See section 3.3, [Logon using security phrases](#).
- **Smart Card** is used for smart card logon. See section 3.2, [Logon using a smart card and PIN](#).

- **Windows Logon** is used for Integrated Windows Logon. See section [3.6, *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](#).
- **Client Credentials OAuth2** is used for server-to-server authentication for the MyID Core API. See the *Configuring MyID for server-to-server authentication* section in the [MyID Core API](#) guide for details.
- **Windows Hello** is used for Windows Hello for Business. See the *Setting up Windows Hello for logon* section in the [Windows Hello for Business Integration 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.

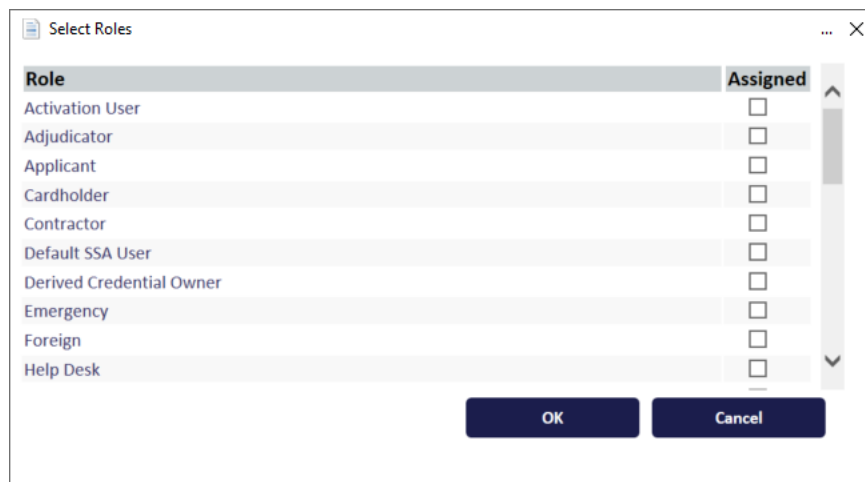
To set the role restriction option:

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 the **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, both on user account creation and when moving a user account to a different group.

Note: Previous versions of MyID automatically added the PasswordUser and Cardholder roles to every person account created where there were no default roles set by membership of a group; from MyID 11.6, however, this is no longer the case. Any person created receives the default roles specified by their group membership. By default, groups inherit the default roles from their parents, and the Root group is assigned the PasswordUser and Cardholder roles to replicate the previous behavior; you can edit the default roles for the Root group if necessary.

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 Admin North group to change the default roles to System, Manager and Cardholder.

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.

4.3.2 Setting up default roles

To create a group with default roles:

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

2. Type the **Group** name and **Description**.
3. Select the **Parent Group**.
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 section [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 select the **Inherit Roles** option, the default roles from the parent group are inherited. However, these roles are inherited only at the point of setting the option; if the default roles for the parent group subsequently change, this does not affect the child group.

If there are no explicit default roles set up for the parent group or any of its ancestors up to and including Root, the system default roles of `Cardholder` and `PasswordUser` are assigned instead. These roles are also assigned if you select the **Inherit Roles** option when editing the Root group.

- If you deselect the **Inherit Roles** option, you can set the default roles for the group manually. You can change these default roles to any of the available roles for the group. If the default roles for the parent group change, this does not affect the child group.

- If you deselect the **Inherit Roles** option, then deselect *all* of the roles in the list, the group is configured to inherit default roles from its parent, and a link is created between the group and its parent – if you change the default roles for the parent group, the child group's default roles are changed accordingly.

Note: If you have created a link to a parent group by deselecting all of the roles, and subsequently save the child group without *again* deselecting all of the roles, the link between the child and parent is broken, and the inherited default roles are converted into an explicit list of default roles.

If you want to set up the group to have *no* default roles, you must deselect the **Inherit Roles** option, deselect all of the roles in the list, then do the same for its parent group and all of its ancestors up to and including Root.

Note: If you deselect all the default roles for the Root group, any of its child groups that are linked to their parent do not lose their default roles; instead, the list of default roles they previously inherited through the link is changed to be an explicit list of default roles. However, the link between the child group and its parent is broken, and setting default roles for the parent no longer affects the child group.

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

- **IKB-307 – Default roles may attempt to exceed the maximum scope that can be assigned due to the operator's scope**

This is prevented in the MyID Operator Client, but when you click **Save** in MyID Desktop you may see an error similar to:

`Supplied logon name is invalid. Please enter a new logon name.`

Open the Select Roles dialog, then click the **Advanced** button and ensure that the scope for all of the roles is permitted; scope settings beyond your own operator scope are grayed out, but may have been automatically selected by the scope of the group's default role settings. Fix the scope settings, click **OK**, then try to save the person's record again.

If you import a person from a directory automatically, for example using **Request Card**, you are not presented with the opportunity to change the person's roles; to fix the scope, use the **Edit Person** workflow.

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.

You must create roles in MyID that have the same names 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 role 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.

Important: The roles assigned based on LDAP group membership cannot override the group role restrictions set up in MyID. When the account is synchronized with the directory, any invalid roles are removed; if you edit a person, any invalid roles are highlighted on screen, and you must remove them manually.

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**.

You can combine LDAP linked roles with group default roles; the user is assigned the roles linked to their LDAP group in addition to the roles set as defaults for their group within MyID. For details of setting up default roles, see section [4.3, Default roles](#).

4.4.1 Default Active Directory groups

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

- Domain Users
- Domain Admins
- Enterprise Users

and so on.

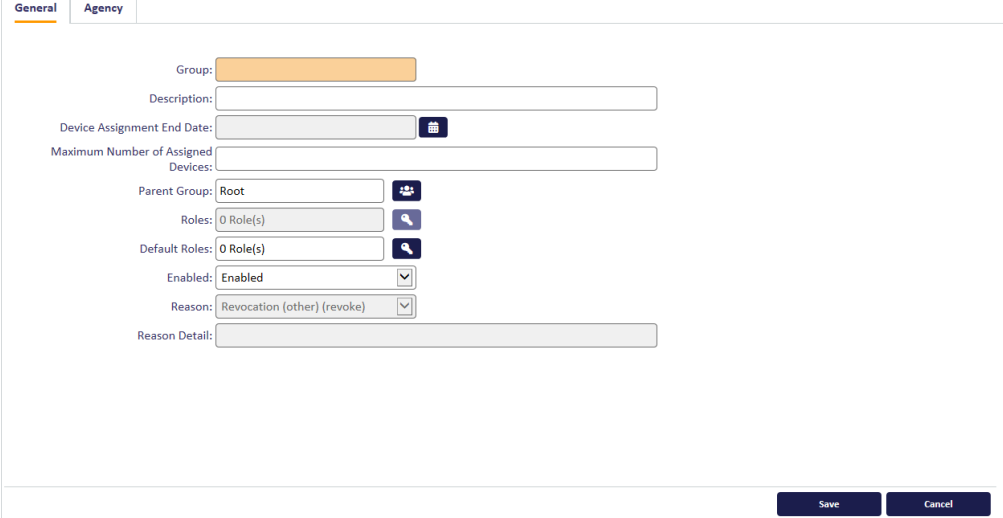
This is because MyID uses the `memberOf` LDAP function to retrieve information about the groups to which a member belongs, but this function does not retrieve information about the built-in Active Directory security groups.

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

4.4.2 Setting up linked roles

To set up a linked role:

1. From the **Configuration** category, select **Edit Roles**.
2. Click **Show/Hide Roles** and make sure that the role you want to link is displayed.



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

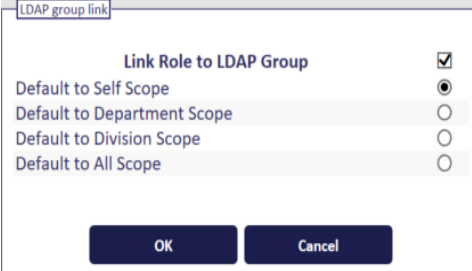
3. Click the icon in the **Linked to LDAP Group** row.

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

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

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:



- 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 directory 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.

You can use this feature to remove an obsolete role from all users in the MyID database. For example:

- The Cardholder role is no longer required for any users, but many users are still assigned the role. Create a dummy group in the directory that contains no users, then link the Cardholder role to that LDAP group. When MyID synchronizes with the directory, the Cardholder role is removed from all users.

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**

Note: When adding or editing another person's user account, you cannot set a scope higher than your own level.

4.5.1 Known issues

- **IKB-303 – Non-directory users have effective scope of All over the directory**

If you have a combination of directory users and non-directory users in your MyID system, any non-directory user has an effective scope of All over the directory; they can access the records of any directory users. Directory users are correctly given scope based on their position in the directory, but non-directory users do not have a position in the directory, and are therefore given a scope of All.

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 *Editing groups* section in 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, click **Security Settings**. On the **Process** tab, configure the **Allow Administrative Groups** option.

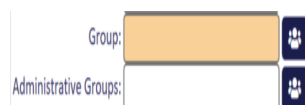
- When set to **Yes**, the scope available in workflows is extended to include any additionally specified administrative groups assigned to operators. The **Add Person** and **Edit Person** workflows are extended to allow management of administrative groups.
- When set to **No**, the scope in workflows is limited to operators' home groups, and it is not possible to manage operators' administrative groups in **Add Person** or **Edit Person**.

Once you have set your configuration, click **Save changes**.

4.7.2 Assigning Administrative Groups

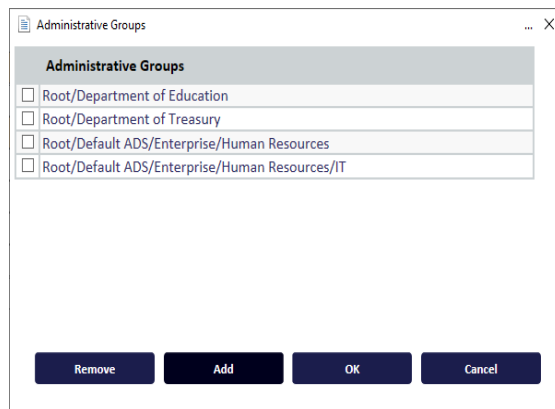
From the **People** category, select the **Add Person** or **Edit Person** workflow.

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, click the check boxes of the groups you wish to remove, then click the **Remove** button.
Any check boxes 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.

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.



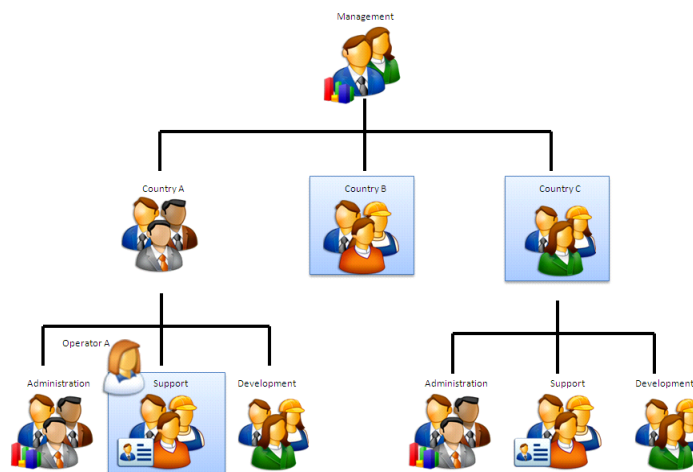
4.7.8 Scope calculations

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:

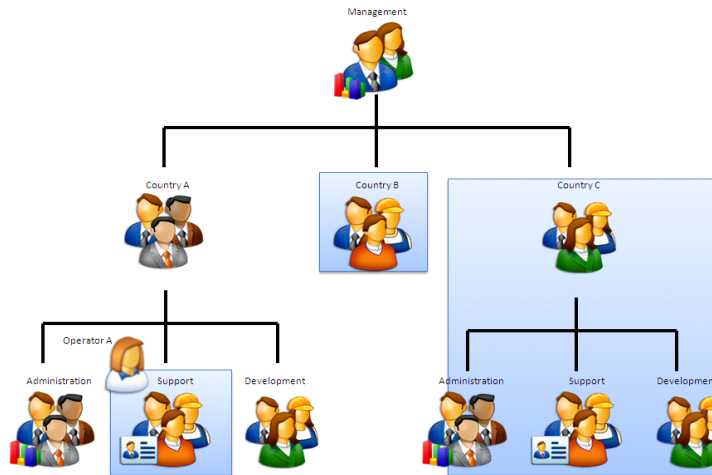
- Administrative group access to the **Country B** and **Country C** groups.
- **Division** rights for the **Registrar** role.
- **Department** rights for the **Issuer** role.

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.

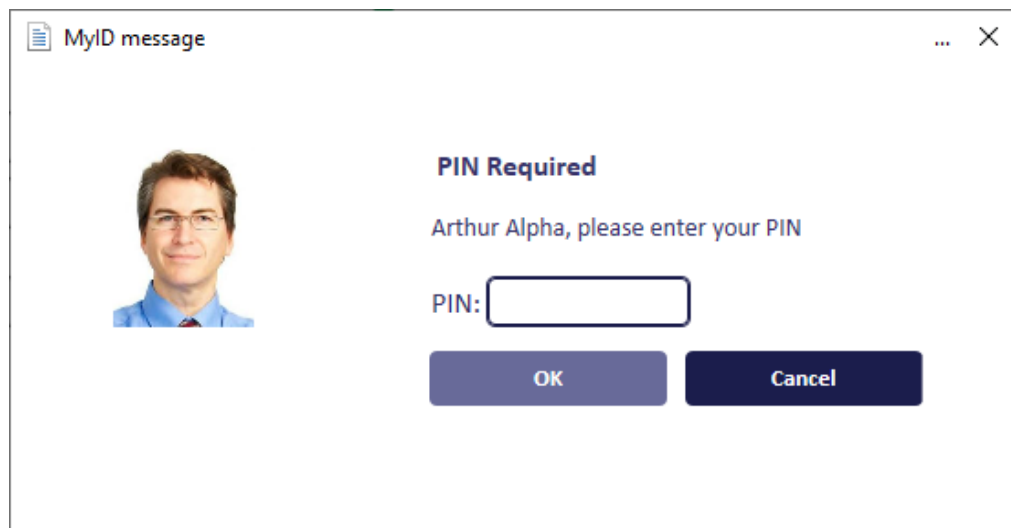
Note: The witness does *not* require the target user account to be within their scope; however the witness does require permission to the **Issue Card > Witness** option in the **Edit Roles** workflow.

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 [31.1, 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; see section 5.4, *Using an LDAP directory as the primary data source* for details of the **Search a Directory** option.

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

Note: When MyID is installed, it is preconfigured to operate with Microsoft Active Directory Domain Services (AD DS). This includes the use of attributes that do not exist in other LDAPv3-compliant directories. Integration with AD DS is automatic, with MyID set as the primary data source. You can integrate other LDAPv3-compliant directory providers with MyID; this requires additional configuration of MyID. For information on custom LDAP mappings and search filters, contact customer support quoting reference SUP-223.

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 **Operation 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 Before you connect to the directory

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**.

You can also launch this workflow from the **Connections and Notifications** section of the **More** category in the MyID Operator Client. See the *Using Connections and Notifications workflows* section in the [MyID Operator Client](#) guide for details.

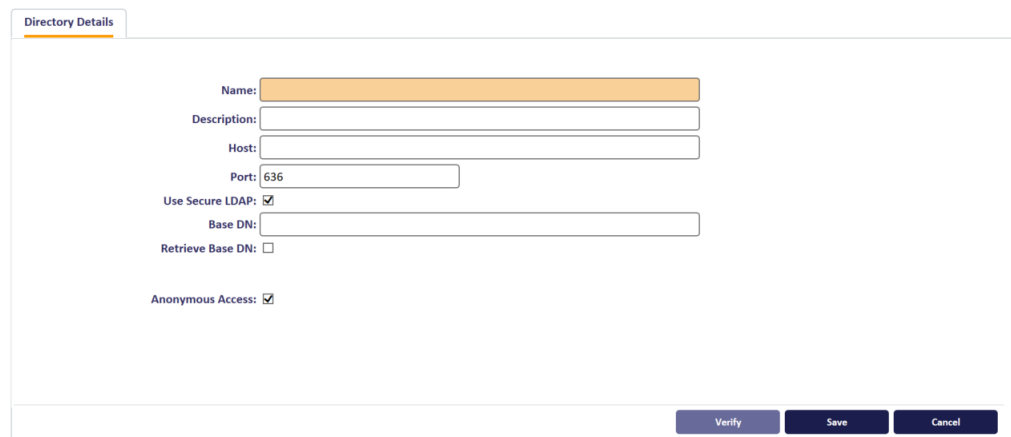
2. If there is a directory in the **Select Directory** box, information about it is displayed.

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.



The screenshot shows the 'Directory Details' form. It has the following fields and controls:

- Name:** A text input field with an orange border.
- Description:** A text input field.
- Host:** A text input field.
- Port:** A text input field with the value '636'.
- Use Secure LDAP:** A checkbox that is checked.
- Base DN:** A text input field.
- Retrieve Base DN:** A checkbox that is unchecked.
- Anonymous Access:** A checkbox that is checked.
- Buttons:** 'Verify', 'Save', and 'Cancel' buttons are located at the bottom right of the form.

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.

- 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:
 - Clear the **Anonymous Access** option.
 - 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.

- 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 [30.3, 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.

5.3.1 Known issues

- **IKB-305 – Cannot enable or disable a user linked to a directory**

If the following combination of configuration options is set:

- **Edit Directory Information** = No
- **Disable on removal from directory** = No
- **Search a Directory** = Yes or Ask

You may be unable to enable or disable a user in MyID, as the `Enabled` field is mapped to your directory. If you want to be able to enable or disable a user in MyID, you must remove the `Enabled` field from the `LDAPLookup` table in the MyID database. For information on custom LDAP mappings, contact customer support quoting reference SUP-223.

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 Configuring the Synchronization Tool for load sharing

Where multiple application servers are available, you can configure the Synchronization Tool to spread processing load over these servers.

Where load sharing is required, the records processed by each application server are specified by providing the range of records to be processed using start and end percentile range values.

To ensure that all records are processed by the servers, the specified percentile ranges must cover the full percentile range from 0 to 100%; for example, a simple split with two application servers may be:

- Server 1: 0 – 50%
- Server 2: 51 – 100%

To ensure that all the records are processed, the Synchronization Tool will process all records up to the top of the percentile range.

Important: Use of load sharing is enabled only when the **whenChanged** option has *not* been selected

5.5.2 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.

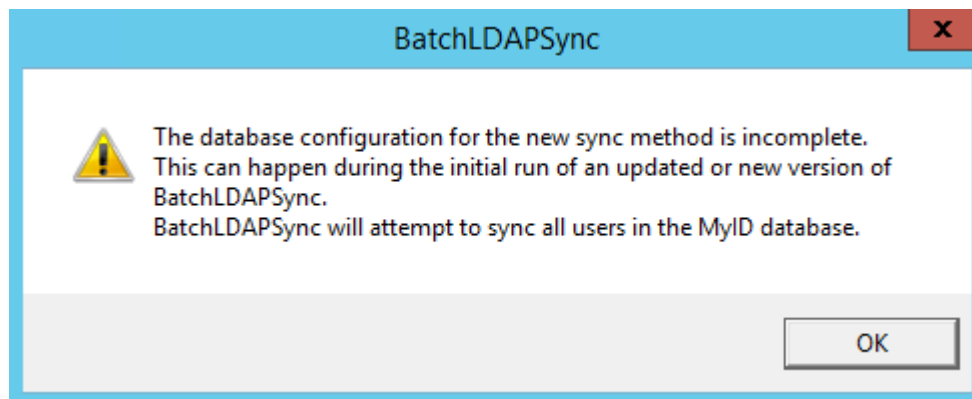
Note: You can choose to revoke certificates instead of suspending them if the user account is suspended in the directory. Please contact customer support for details.

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 **Start range** is specified, the first record processed will be at the start of the specified percentile. By default, this is 0%, which processes the records from the beginning.
- If the **End range** is specified, the last record to be processed will be at the top of the specified percentile range. By default, this is 100%, which processes up to the last record.

- 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, [The 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.

5.5.3 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.

5.5.4 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 [5.5.5](#), *Running the tool from the command line*.

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

A summary of the records processed and the time taken is displayed on completion of the synchronization process.

```
Checked against LDAP 12242, Updated 9191 ( removed from LDAP(2), disabled
in LDAP(3) )
```

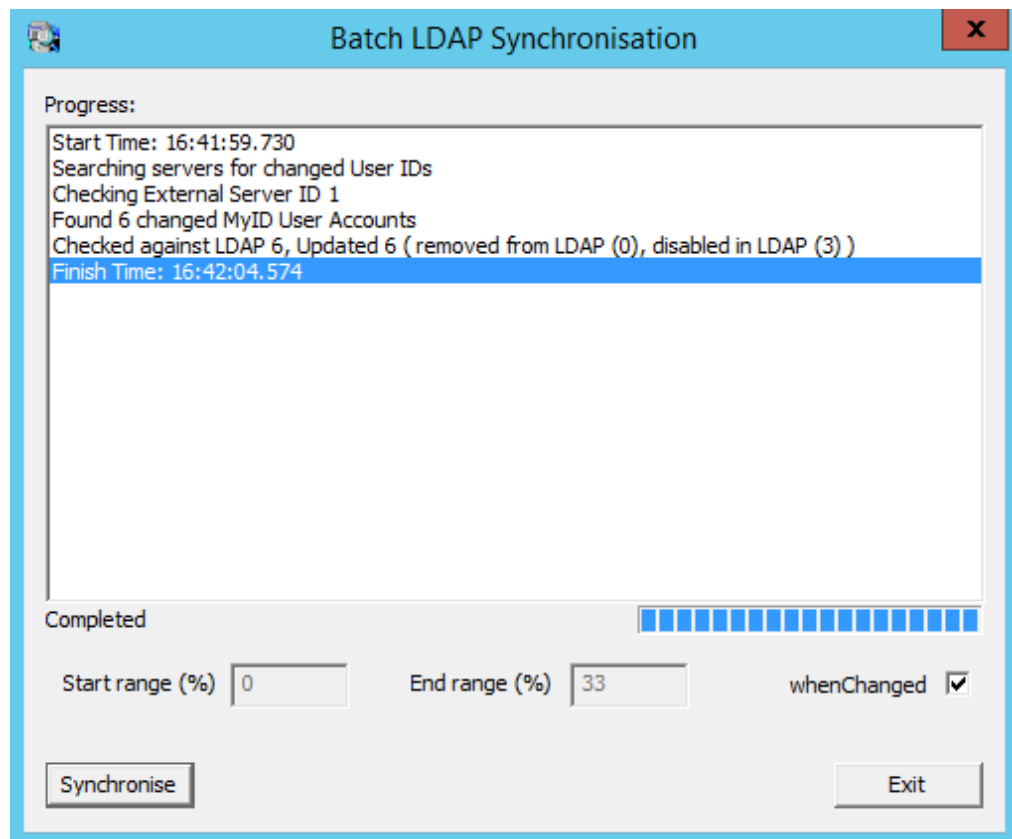
This means that the tool carried out the following:

- Parsed 12242 user records.
- Updated 9191 users with changes from the LDAP synchronized to MyID. This includes users removed or disabled in the LDAP.

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

5.5.4.1 Running the tool with the whenChanged option

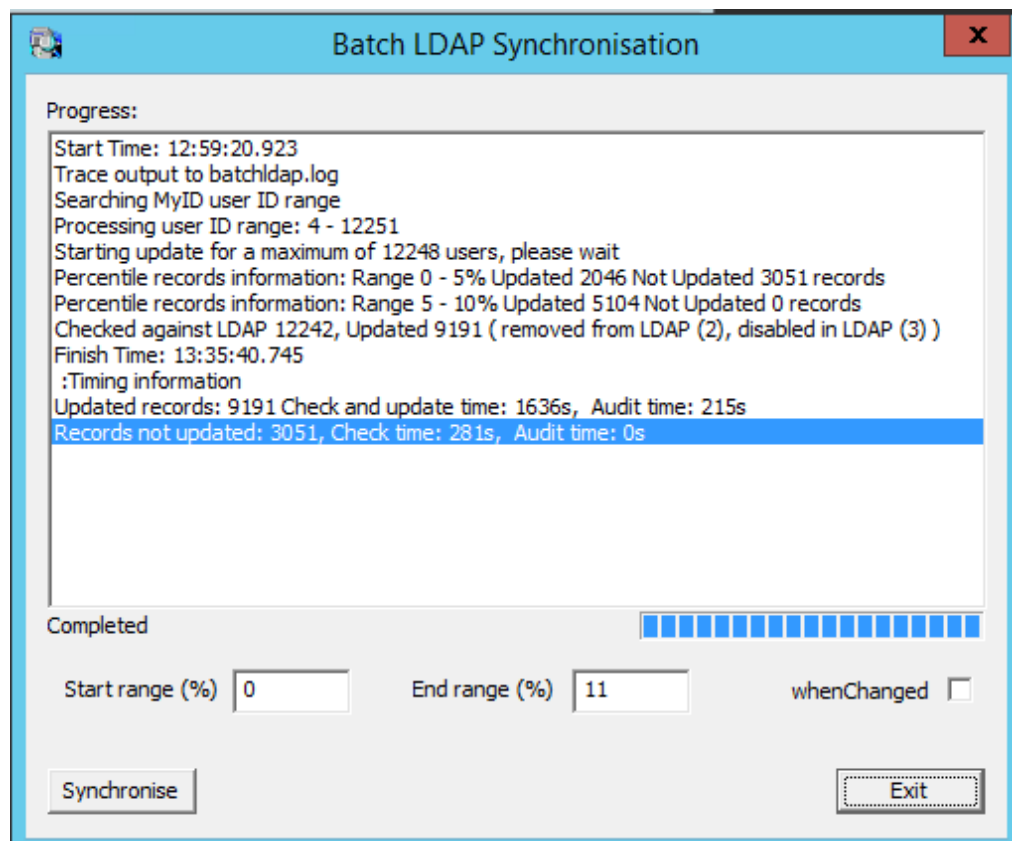
1. From the **Start** menu, run the **Batch Directory Synchronization Tool**.
2. To update only those records that have been changed since the last time the Batch Directory Synchronization Tool was run, select the **whenChanged** option.
3. Click **Synchronise**.



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

5.5.4.2 Running the tool by specifying a processing range

1. From the **Start** menu, run the **Batch Directory Synchronization Tool**.
2. Specify the **Start range** and **End range** to be processed by the tool.
3. Do *not* select the **whenChanged** option.
4. Click **Synchronise**.



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

The output displays the user ID range that is processed by the synchronization process.

Processing user ID range: 4 - 12251

When checking each user ID in the above range, the user ID is first checked in MyID to determine if:

- The user ID is associated with a user.
- The user is an LDAP user. This is determined by checking that the user has a DN and is marked as linked to an LDAP external server.

No further processing is required on any user ID that does not satisfy the criteria for being a valid LDAP user record within MyID; otherwise, the user data is compared against the corresponding user LDAP data. An update action, and audit, is performed as a result of this comparison if:

- The user has been disabled in LDAP but is enabled in MyID.
- The user is enabled in LDAP but disabled in MyID.
- The user is not found in LDAP.
- The checked user data does not match.

No update is required otherwise.

On completion, a summary of the action taken on the LDAP user records is provided; for example:

```
Checked against LDAP 12242, Updated 9191 ( removed from LDAP(2),
disabled in LDAP(3) )
```

In this example:

- 12242 LDAP records were checked.
- Of these, 9191 records met one or more of the criteria requiring an update. This count includes:
 - Users who have been removed from LDAP. Set to 2 in the above example.
 - The users who were found to be disabled in LDAP. Set to 3 in the above example.

A breakdown summary of the split in the processing time between updated and not updated records is also provided on completion:

```
Updated records 9191, Check and update time: 1636s, Audit time: 215s
Records not updated: 3051, Check time: 281s, Audit time: 0s
```

This means that:

- 9191 records required some sort of update, either to synchronize the LDAP change, or to remove or disable/enable a user.
- The total time spent on checking and updating these records was 1636 seconds.
- The total time spent on adding audit information for these records was 215 seconds.
- 3051 records were found to not require any update. The total time spent on processing these records is 281 seconds.

An intermediate summary of the records processed is provided every 5% percentile range:

```
Percentile records information: Range 0 - 5% Updated 2046 Not Updated
3051 records
```

5.5.5 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 the `-silent` or `-autorun` flags. The tool runs as described in section [5.5.4, Running the tool from the Start menu](#).
- Automatic execution – run the program with the `-autorun` flag. The dialog is displayed as described in section [5.5.4, 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.
- Range of records – for splitting the load, run the program with the `-startrangepercentile` and `-endrangepercentile` parameters. If you do not specify these parameters, the default values are 0 and 100 respectively. For example:
`-startrangepercentile 10 -endrangepercentile 20`

The percentile range setting is ignored if the `-whenchanged` option is set.

The case of the command-line options is not important. You can also use the first two letters of the command-line options instead of the full name; for example:

```
-st 10 -en 20
```

instead of:

```
-startrangepercentile 10 -endrangepercentile 20
```

If the tool detects an error in the command-line options, it displays a help dialog. This does not appear if you are using `-silent` or `-autorun`.

To record the details of the process to a specified file, including any command-line processing errors, 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 folder is used. The MyID COM+ user must have permission on this folder to create and write to the trace file.

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

5.5.6 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 Start menu*.

5.5.7 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

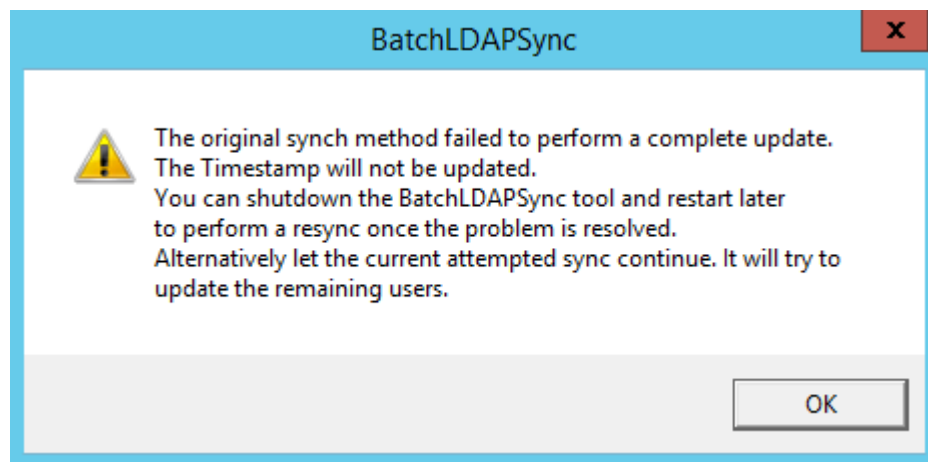
If you are running multiple instances of the Batch Directory Synchronization Tool concurrently, the total of updated users across all instances may not match the actual total of updated users – this is because the same update may be counted by more than one instance. The updates themselves are processed 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 [30.3, 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 Base DN for your default directory within MyID. MyID automatically checks the configuration area for that Base DN.

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 ADConfigPrefix 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.

In the MyID Operator Client, directories are displayed in alphabetical order; to ensure that the configuration-only directory does not appear as the default directory in the list, you can set the name to something like ZZZ AD Configuration.

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

5.8 The 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 Catalog 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\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 canceled, 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 Catalog 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\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:

C:\Program Files\Intercede\MyID\Utilities\

- e. Select `ADDeletionSync.exe` and click **Open**.
 - f. Leave the **Add arguments (optional)** and **Start in (optional)** fields blank.
 - g. 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. For a full list of the currently supported CAs, see the *Certificate authorities* section 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.

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**.

You can also launch this workflow from the **Connections and Notifications** section of the **More** category in the MyID Operator Client. See the *Using Connections and Notifications workflows* section in the [MyID Operator Client](#) guide for details.

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.

MyID Desktop

Certificate Authorities > Select a CA > Edit a CA

Select a CA

CA Name: DOMAIN36-ROOT-CA CA Description: DOMAIN36-ROOT-CA Certificate Authority

CA Type: Microsoft Enterprise

CA Enabled: ☒

Name	Description	Allow Issuance	Reverse DN	Archive Keys	Superseded
AdditionalIdentitiesCertificate on DOMAIN36-ROOT-CA		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
AdditionalIdentitiesSmartcardLogon on DOMAIN36-ROOT-CA		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
AdditionalIdentitiesSmartcardUser on DOMAIN36-ROOT-CA		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Administrator on DOMAIN36-ROOT-CA		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
CEPEncryption on DOMAIN36-ROOT-CA		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
CIVContentSigningCert on DOMAIN36-ROOT-CA		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
ClientAuth on DOMAIN36-ROOT-CA		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
DerivedPIVAuthentication on DOMAIN36-ROOT-CA		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
DerivedPIVEncryption on DOMAIN36-ROOT-CA		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
DerivedPIVEncryptionCAArchive on DOMAIN36-ROOT-CA		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
DerivedPIVSigning on DOMAIN36-ROOT-CA		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
DirectoryEmailReplication on DOMAIN36-ROOT-CA		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
DomainController on DOMAIN36-ROOT-CA		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
DomainControllerAuthentication on DOMAIN36-ROOT-CA		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
ECCVCSigningCert on DOMAIN36-ROOT-CA		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
ECCExchangeUser(SHA256) on DOMAIN36-ROOT-CA		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Delete New Edit

3. Click **Delete**.

6.2.3.1 Known issues

- **IKB-310 – Error when deleting a CA that has the same path as another CA**

If you erroneously add multiple CAs that have the same path, then attempt to delete one of the CAs, you may see an error similar to:

```
An error occurred inside CBOL_ManageCAWeb::DeleteCA Error: 0x80046010
IDispatch error #24080 An error occurred inside CBOL_
ManageCAImpl::DeleteCA Error: 0x80046010 : Multiple Records returned
Info: CA not uniquely found ----- Exception raised
in function: CAImpl::Delete In file CAImpl.cpp at line 514 In object
MyIDBOLImpl.BOL_ManageCAImpl.1
```

If this error occurs, the CA entry must be deleted from the database manually. For assistance with this, contact customer support, quoting reference IKB-310.

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. Set the **CA Name** to a configured Certificate Authority from the list.
3. Click **Edit**.

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

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

See your CA integration guide for details.

8. Click **Save**.

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

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 preconfigured 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.

Note: The original certificate is allowed to expire – it is not revoked.

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.

You must ensure that the replacement certificate policy has the appropriate attributes; for example, an additional identity certificate requires the **Allow Identity Mapping** option set, so the replacement policy must *also* have this option set.

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, click **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, click the certificate policy that you want to supersede.

The screenshot shows the 'Available Certificates' dialog box. On the left, a list of certificate policies is displayed, with 'AdditionalIdentitiesCertificate on DOMAIN36-ROOT-CA' selected. On the right, the configuration for this policy is shown. The 'Enabled (Allow Issuance)' checkbox is checked. The 'Display Name' is 'AdditionalIdentitiesCertificate on DOMAIN36-ROOT-CA'. The 'Description' field is empty. The 'Allow Identity Mapping' checkbox is unchecked. The 'Reverse DN' checkbox is unchecked. The 'Archive Keys' dropdown is set to 'None'. The 'Certificate Lifetime' is 365. The 'Automatic Renewal' checkbox is checked. The 'Certificate Storage' is set to 'Hardware'. The 'Recovery Storage' is set to 'Hardware'. The 'Key Algorithm' is 'RSA 2048'. The 'Key Purpose' is 'Signature and Encryption'. The 'Supersede' button is highlighted.

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

5. Click **Supersede**.

A list of the available certificate authorities appears.

Please choose the superseding Certificate Authority.

CA Name	Select
DOMAIN36-ROOT-CA	<input type="radio"/>

Cancel

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

A list of the available enabled certificate policies appears.

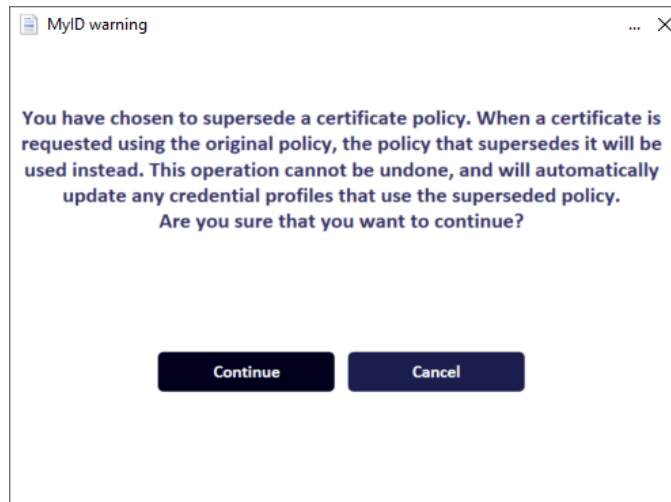
Please choose the superseding Policy.

Policy Name	Select
AdditionalIdentitiesSmartcardLogon on DOMAIN36-ROOT-CA	<input type="radio"/>
DerivedPIVAuthentication on DOMAIN36-ROOT-CA	<input type="radio"/>
DerivedPIVEncryptionCAArchive on DOMAIN36-ROOT-CA	<input type="radio"/>
DerivedPIVSigning on DOMAIN36-ROOT-CA	<input type="radio"/>
PIVCardAuthentication on DOMAIN36-ROOT-CA	<input type="radio"/>
PIVEncryption on DOMAIN36-ROOT-CA	<input type="radio"/>
PIVEncryption_CAArchive on DOMAIN36-ROOT-CA	<input type="radio"/>
PIVSigning on DOMAIN36-ROOT-CA	<input type="radio"/>

OK Cancel

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.

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

Select a CA					
CA Name:	DOMAIN36-ROOT-CA	CA Description: DOMAIN36-ROOT-CA Certificate Authority			
CA Type:	Microsoft Enterprise				
CA Enabled:					
Name	Description	Allow Issuance	Reverse DN	Archive Keys	Superseded
AdditionalIdentitiesCertificate on DOMAIN36-ROOT-CA					
AdditionalIdentitiesSmartcardLogon on DOMAIN36-ROOT-CA					
AdditionalIdentitiesSmartcardUser on DOMAIN36-ROOT-CA					
Administrator on DOMAIN36-ROOT-CA					
CEPEncryption on DOMAIN36-ROOT-CA					
CIVContentSigningCert on DOMAIN36-ROOT-CA					
ClientAuth on DOMAIN36-ROOT-CA					
DerivedPIVAuthentication on DOMAIN36-ROOT-CA					
DerivedPIVEncryption on DOMAIN36-ROOT-CA					
DerivedPIVEncryptionCAArchive on DOMAIN36-ROOT-CA					
DerivedPIVSigning on DOMAIN36-ROOT-CA					
DirectoryEmailReplication on DOMAIN36-ROOT-CA					
DomainController on DOMAIN36-ROOT-CA					
DomainControllerAuthentication on DOMAIN36-ROOT-CA					
ECCEXCSigningCert on DOMAIN36-ROOT-CA					
ECCEXchangeUser(SHA256) on DOMAIN36-ROOT-CA					
ECCEXchangeUser(SHA384) on DOMAIN36-ROOT-CA					
ECCEXchangeUser(SHA512) on DOMAIN36-ROOT-CA					
ECCEXchangeUserCAArchive(SHA256) on DOMAIN36-ROOT-CA					
ECCEXchangeUserCAArchive(SHA384) on DOMAIN36-ROOT-CA					
ECCEXchangeUserCAArchive(SHA512) on DOMAIN36-ROOT-CA					
ECCPIVAuthentication(SHA256) on DOMAIN36-ROOT-CA					
ECCPIVAuthentication(SHA384) on DOMAIN36-ROOT-CA					

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 check the permissions, use the **Edit Roles** workflow.

To upload PFX certificates:

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

Note: You can also launch this workflow from the self-service menu in the MyID Operator Client. See the *Launching self-service workflows* section in the [MyID Operator Client](#) guide for details.

The screenshot shows the 'Upload PFX Certificates' workflow interface. It features three input fields: 'PFX Certificate' with a file upload icon, 'PFX Password', and 'Certificate Policy' with a dropdown menu. Below these fields is an 'Add' button. A message states 'You currently have no issued certificates.' At the bottom right is a 'Finish' button.

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.

Upload PFX Certificates

PFX Certificate:

PFX Password:

Certificate Policy:

Please select...

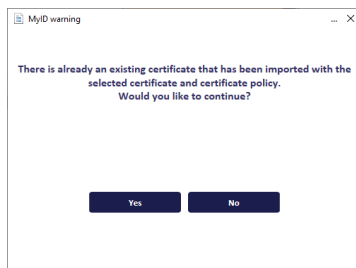
Add

Existing Certificates

Certificate Template	Certificate Serial Number	Issue Date (UTC)	Expiry Date (UTC)	File Name
Unmanaged	3B000000D22ADD2A3EDF427EFE000000000D2	2023-11-16 14:25:41	2023-12-28 14:35:31	00001_PIVCardAuthentication_(2).pfx

Finish

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:

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

- Click **Finish**.

6.9 Including user security identifiers in certificates

A user security identifier (user SID) is a unique identifier for a person that is stored in your directory. When you import a person from a directory, or carry out a directory synchronization, MyID obtains the user SID from the directory and stores it in the person's record.

You can view or edit a person's SID on the **Account** tab for a person's record in the MyID Operator Client; see the *Searching for a person* and *Editing directory information* sections in the [MyID Operator Client](#) guide.

You can use the additional search criterion **User SID Present** on the **People** report in the MyID Operator Client to identify people who do not have this information present; see the *People report* section in the [MyID Operator Client](#) guide.

You can import the user SID through the MyID Core API (by providing the `account:usersid` value when adding or updating a person) or through the Lifecycle API (by providing the `PivCardRequest/Agency/Applicant/Account/UserSID` or `CMSCardRequest/Group/User/Account/UserSID` value) when adding or updating a person.

You can include the user SID in the attribute mappings for certificate templates for Microsoft and PrimeKey EJBCA CAs. This is important to ensure compliance with the authentication requirements relating to Microsoft [KB5014754](#). See the *Enable certificate templates for issuance within MyID* and *User SID extensions* sections in the [Microsoft Windows CA Integration Guide](#) and the *Mapping the additional attributes* section in the [PrimeKey EJBCA Integration Guide](#) for details.

The user SID is also stored for additional identities; see section [25.1.3, User SIDs in additional identities](#). You can view the user SID for the additional identity using the **Additional Identities (AID)** report in the MyID Operator Client; see the *Additional Identities (AID) report* section in the [MyID Operator Client](#) guide.

In the credential profile, you can specify the user SID as a required attribute for a user to be issued a device, so that you cannot issue a credential to a person who does not have a user SID as part of their user record; see section [11.3.1.11, Requisite User Data](#) for details.

Note: You cannot import user SIDs if there is no association with the directory; for example, when importing a person using the Self-Service Request Portal but there is no match in the directory based on the person's DN and UPN. In this case, any user SID on the original credential is ignored.

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 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 Enabling GlobalPlatform keys

The **Enable Customer GlobalPlatform Keys** configuration option determines whether you can write customer GlobalPlatform keys to your cards. To check that this option is set:

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

7.3 Managing 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 *Using GenMaster* section in the [Installation and Configuration Guide](#) for details.

7.3.1 Entering factory (vendor) keys

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

You can also launch this workflow from the **Configuration Settings** section of the **More** category in the MyID Operator Client. See the *Using Configuration Settings workflows* section in the [MyID Operator Client](#) guide for details.

2. The **Factory** page is displayed.

3. **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.
4. Type a **Name** and a **Description** for the key set.

5. 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**.

6. 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.

7. 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.

8. 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.

9. 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.

10. 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.

11. 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.

12. 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).

13. 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.

14. 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.

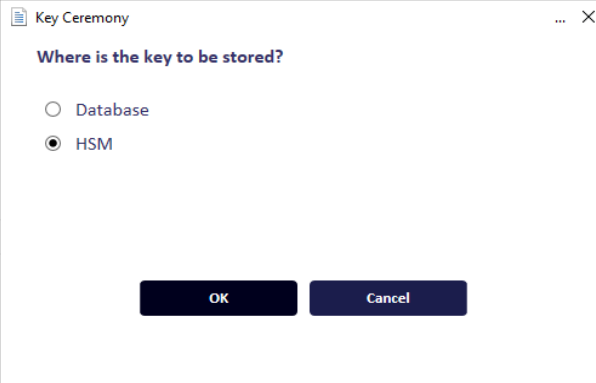
15. Click **Save**.

16. 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.



Key Ceremony

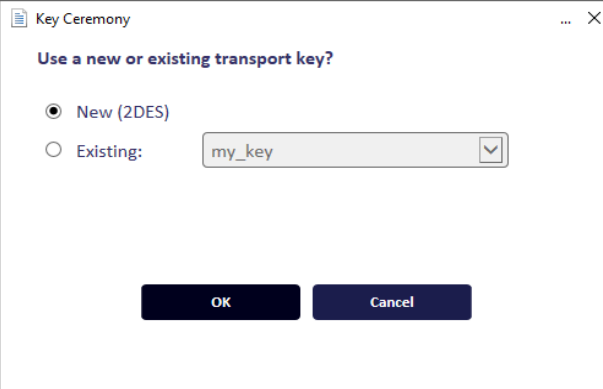
Where is the key to be stored?

☐ Database

☒ HSM

OK Cancel

- 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.



Key Ceremony

Use a new or existing transport key?

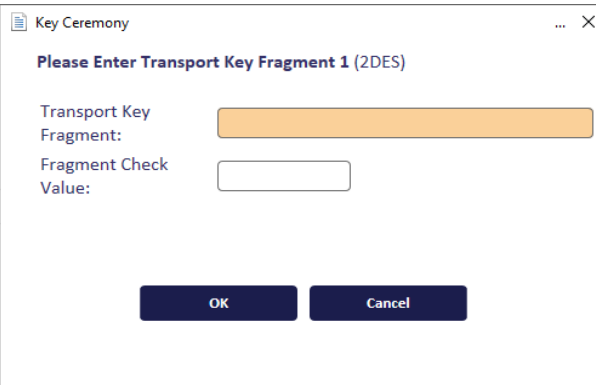
☒ New (2DES)

☐ Existing: my_key

OK Cancel

See section [16.2, The Key Manager workflow](#) for details of storing a transport key using the **Key Manager** workflow.

- If you are using a new transport key, in the **Key Ceremony** dialog, enter the first part of the transport key.



Key Ceremony

Please Enter Transport Key Fragment 1 (2DES)

Transport Key Fragment:

Fragment Check Value:

OK Cancel

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.

If you are using an RSA transport key, you must also select the **Padding Type** that was used to export and encrypt the key. See section [16.3, Using RSA transport keys](#) for details.

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**.

You can also launch this workflow from the **Configuration Settings** section of the **More** category in the MyID Operator Client. See the *Using Configuration Settings workflows* section in the [MyID Operator Client](#) guide for details.

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

To delete factory keys:

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

You can also launch this workflow from the **Configuration Settings** section of the **More** category in the MyID Operator Client. See the *Using Configuration Settings workflows* section in the [MyID Operator Client](#) guide for details.

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

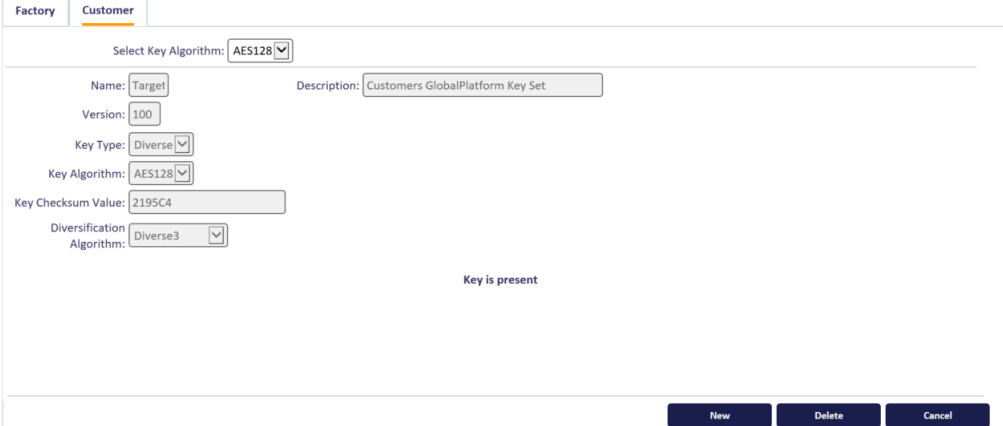
To enter customer keys:

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

You can also launch this workflow from the **Configuration Settings** section of the **More** category in the MyID Operator Client. See the *Using Configuration Settings workflows* section in the [MyID Operator Client](#) guide for details.

2. Click the **Customer** tab.

The **Customer** page opens.



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 **KeyChecksum 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. From the **Applets** category, select the **Manage GlobalPlatform Keys** workflow.

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

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.

7.3.8 Rotating customer keys

You can configure MyID to carry out additional processing whenever a card update (including certificate renewals) is collected to determine whether the GlobalPlatform or PIV 9B keys that are used by the device need to be updated. If either set of keys is out of date, during the collection of the update job MyID applies the latest sets of keys that are applicable to the device.

New issuance, reprovision, and replacement jobs continue to behave as before, swapping out factory keys for customer keys if appropriate customer keys have been configured for the type of device being issued.

To configure this option:

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

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

2. Click the **Issuance Processes** tab.

3. Set the following option:

- **Rotate Keys On Card Update** – set this option to Yes to enable the customer key rotation feature.

The default is No – MyID does not rotate the customer keys when carrying out a card update, and operates as previously.

4. Click **Save changes**.

Note: When creating a new version of a customer GlobalPlatform key, you must set the key **Version** to a value that is not already in use by an existing GlobalPlatform key with the same **Key Algorithm**. See section 7.3.6, *Entering customer (local) keys* for details of setting key version numbers.

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 Applet** 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 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. From the **Applets** category, select the **Manage Applet** workflow.

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

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 canceled 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. From the **Applets** category, select the **Manage Applet** workflow.

You can also launch this workflow from the **Configuration Settings** section of the **More** category in the MyID Operator Client. See the *Using Configuration Settings workflows* section in the [MyID Operator Client](#) guide for details.

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. From the **Applets** category, select the **Manage Applet** workflow.

You can also launch this workflow from the **Configuration Settings** section of the **More** category in the MyID Operator Client. See the *Using Configuration Settings workflows* section in the [MyID Operator Client](#) guide for details.

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.

To work with card layouts, from the **Configuration** category, select **Card Layout Editor**.

You can also launch this workflow from the **Credential Configuration** section of the **More** category in the MyID Operator Client. See the *Using Credential Configuration workflows* section in the [MyID Operator Client](#) guide for details.

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.

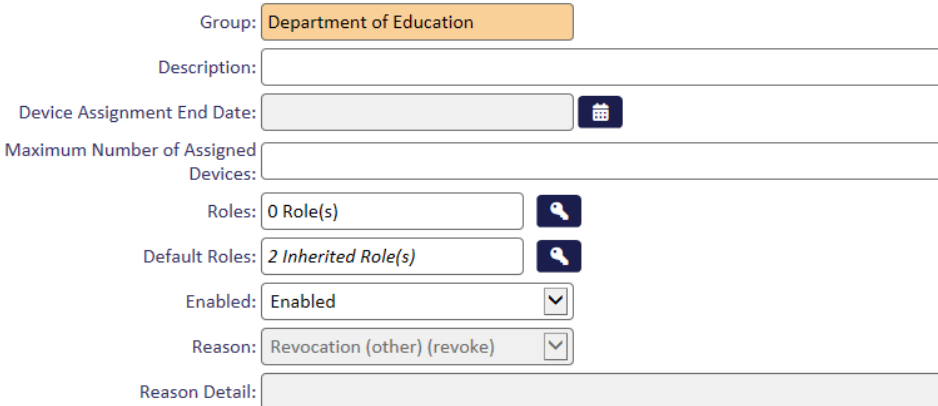
You can specify the appearance and position of both text and images. The content of these elements can be either:

- 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.




The screenshot shows a configuration form for a card layout. The fields are as follows:

- Group:** Department of Education (selected from a dropdown)
- Description:** (empty text field)
- Device Assignment End Date:** (empty date field with a calendar icon)
- Maximum Number of Assigned Devices:** (empty text field)
- Roles:** 0 Role(s) (text field with a magnifying glass icon)
- Default Roles:** 2 Inherited Role(s) (text field with a magnifying glass icon)
- Enabled:** Enabled (dropdown menu)
- Reason:** Revocation (other) (revoke) (dropdown menu)
- Reason Detail:** (empty text field)

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.

To ensure that MyID can access the images, you must set the **Image Upload Server** configuration option. On the **Video** page of the **Operation Settings** workflow, set **Image Upload Server** to the name or IP address of the MyID web server. Do not include `http` or `https`, any virtual directories, or any slashes – the IP address or server name are sufficient.

If the web services server is not the same server as the web server, see also the *Setting the location of the web server* section in the [Web Service Architecture](#) guide.

8.2.1 Setting the list of allowed external server names

If you have images in your card layout that use an absolute URL, and you are issuing devices through the rest.provision service (for example, mobile identities using the Identity Agent Framework, or mobile identity documents) you must configure the service to contain a list of accepted external server names.

If an absolute URL that is used that is not present in the `AllowedWebServers` list, an error similar to the following occurs:

PS82: "Unable to process image"

To set the list of allowed external server names:

1. As an administrator, open the `appsettings.Production.json` file in a text editor.

By default, this is:

```
C:\Program
Files\Intercede\MyID\rest.provision\appsettings.Production.json
```

This file is the override configuration file for the `appsettings.json` file for the web service. If this file does not already exist, you must create it in the same folder as the `appsettings.json` file.

2. In the `MyID` section, edit the `AllowedWebServers` section.

If this section does not exist, you must add it.

The format is:

```
{
  "MyID":{
    "AllowedWebServers": [
      "<servername1>",
      "<servername2>"
    ],
  }
}
```

For example, if you have an image with the following URL:

```
https://myserver.domain.com/images/logo.jpg
```

You must include the following:

```
{
  "MyID":{
    "AllowedWebServers": [
      "myserver.domain.com"
    ],
  }
}
```

```
}
}
```

3. Save the `appsettings.Production.json` file.
4. Recycle the web service app pool:
 - a. On the MyID web server, in Internet Information Services (IIS) Manager, select **Application Pools**.
 - b. Right-click the **myid.rest.provision.pool** application pool, then from the pop-up menu click **Recycle**.

This ensures that the web service has picked up the changes to the configuration file.

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



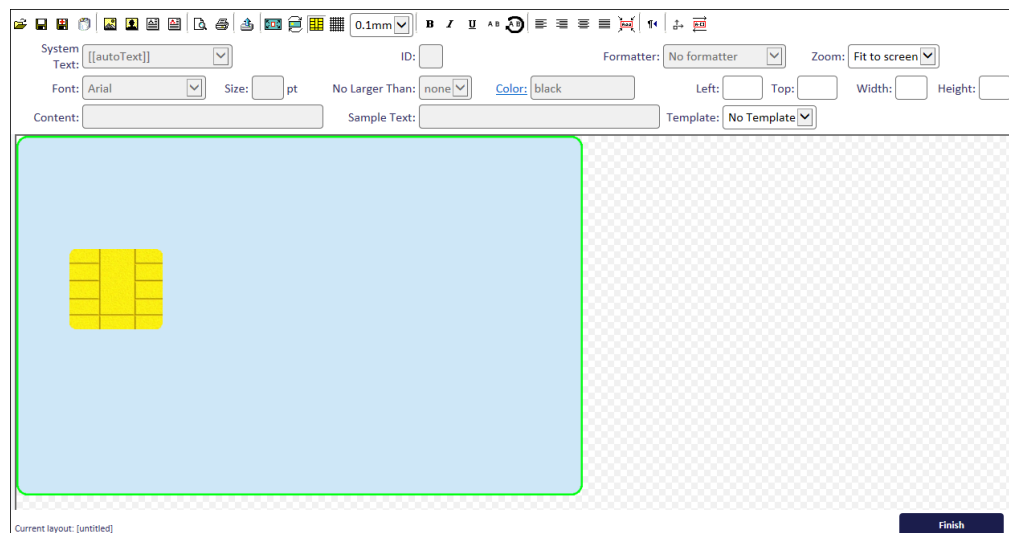
Save As – save a layout using a different name



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:
 1. Click the **Load** button on the toolbar and select the template from the list displayed. Click **Load**.
 2. Make any required changes.
 3. 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:



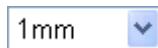
Rotate – rotates the card through 90°



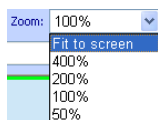
Show chip – toggles the display of the chip



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.



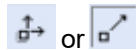
Upload image – static images must be uploaded to the web server before they are available for selection.



Fit image to card – resizes the selected image to fit the height or width of the card

Image Source:

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

To specify a background image:

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. Resize 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.

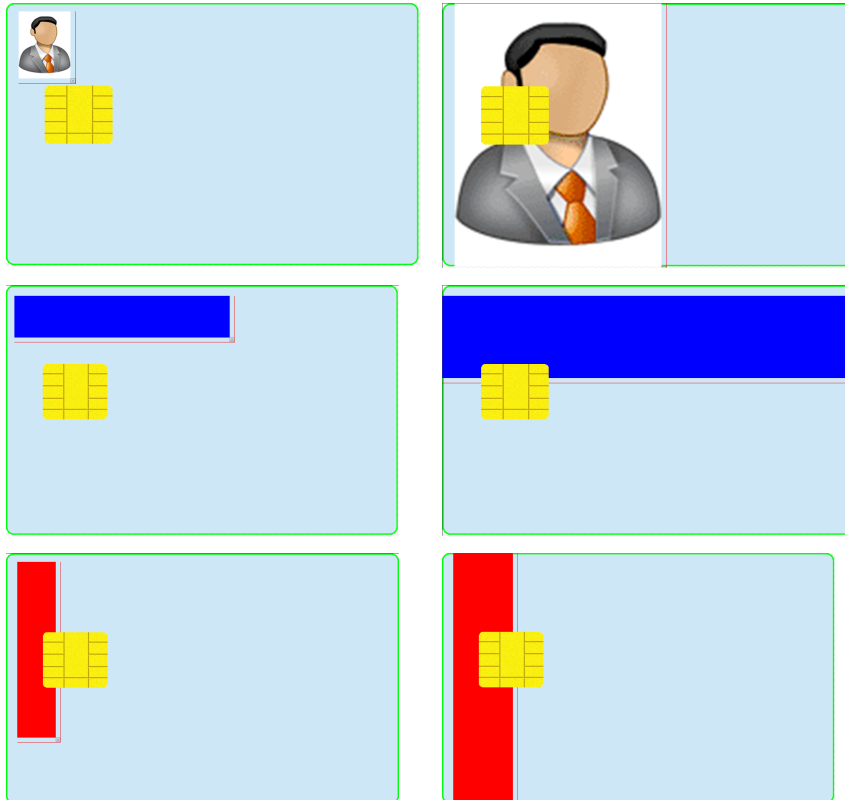
Right-click the image and select **Send to back** from the menu displayed.

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.

Before selecting Fit image to card After selecting Fit image to card



Warning: There is no 'undo' facility, so save your work before using **Fit image to card** or you will have to restore original positions and sizes manually.

8.5.4 Adding static images

To add a static image:

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 Source** 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. Resize 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.

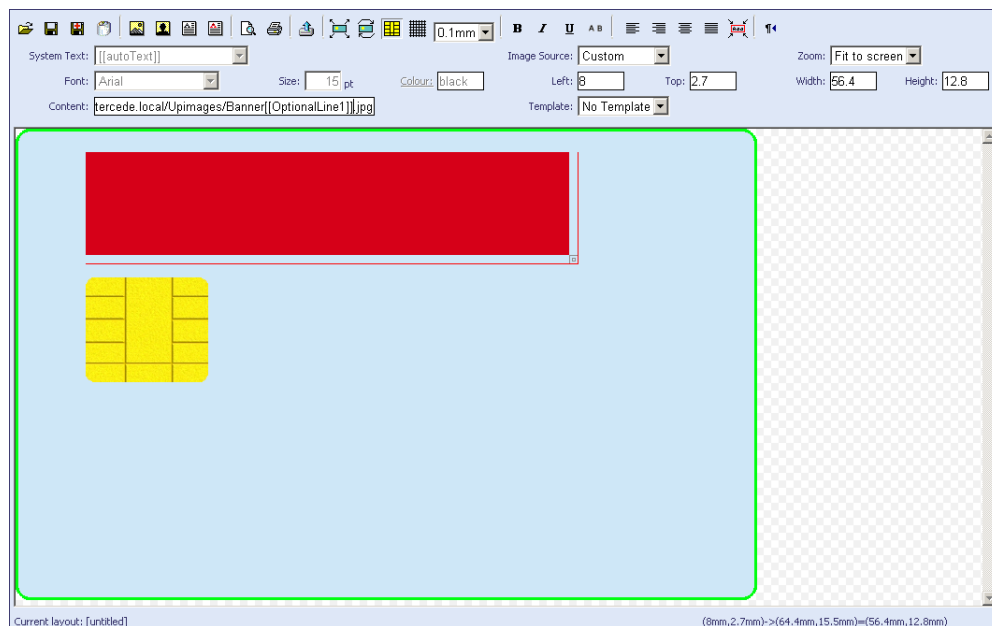
For example, if you have the following URL:

```
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.

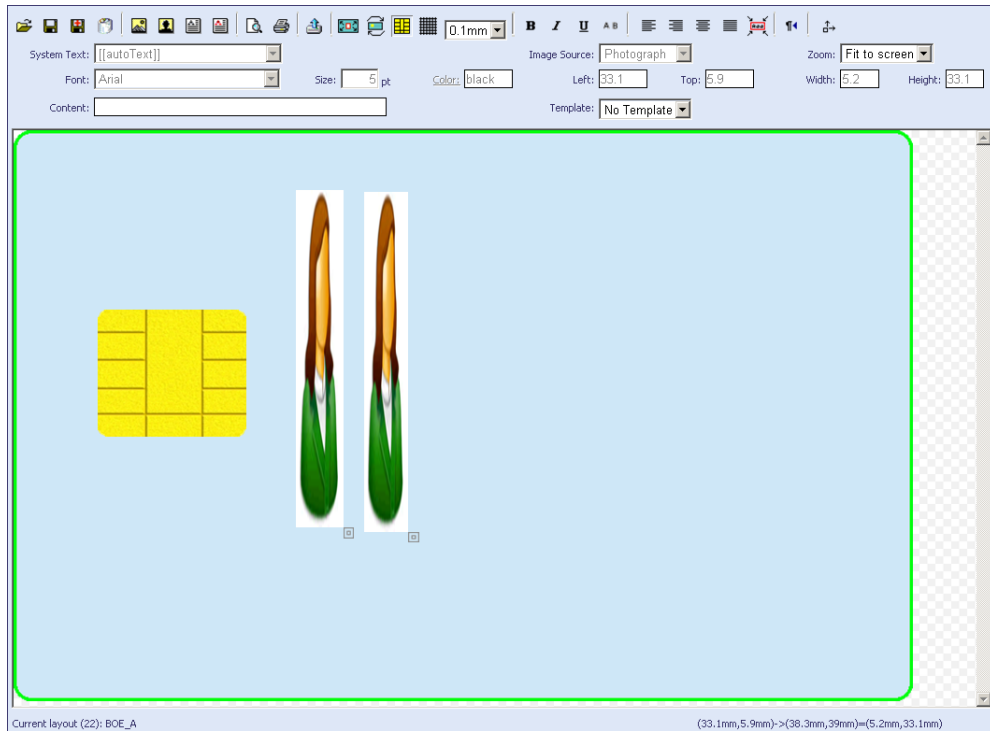




Maintain Aspect Ratio option is set for an on-screen element




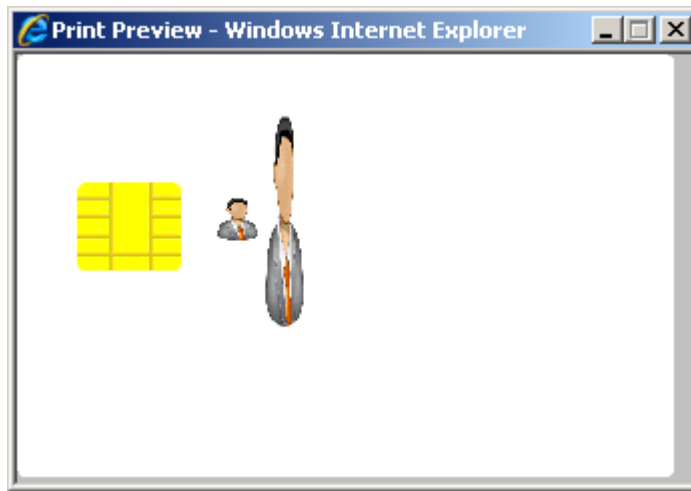
Maintain Aspect Ratio option is not set

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

To add 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

To add 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. 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 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

You can add a custom text field that combines dynamic fields with plain text.

To find out what field codes are available, select the other entries in the **System Text** drop-down list and take a note of the codes you want to use. Field codes are enclosed in double square brackets (`[[]]`). You can then include one or more of these codes in a single field, and include plain text; for example:

```
[[Surname]], [[FirstName]]
```

This combines two name fields and puts a comma between them; for example:

Smith, John

Telephone: [[PhoneNumber]]

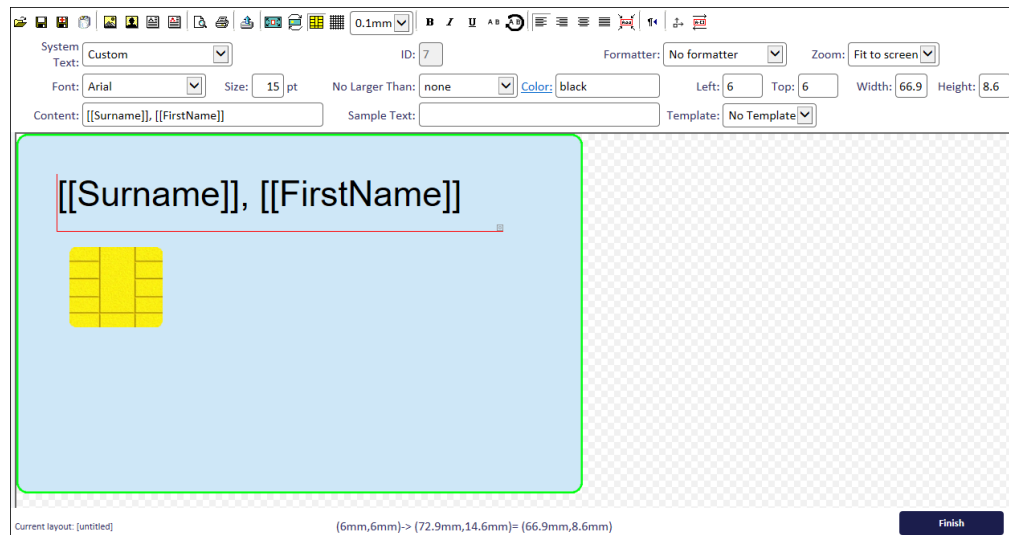
This combines plain text with the cardholder's telephone number; for example:

Telephone: 555-1234

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 along with any plain text.

Note: Field codes are case-sensitive.




8.7 Formatting text

The options available for formatting text are similar to those found on a standard text editor.

See also section [8.9, Dynamically changing text size](#) for advanced text formatting options.

1. Select the text to be formatted by clicking it. A red border is displayed.
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.

5. If you want to rotate the text, click the **Rotate Text**  button on the toolbar.

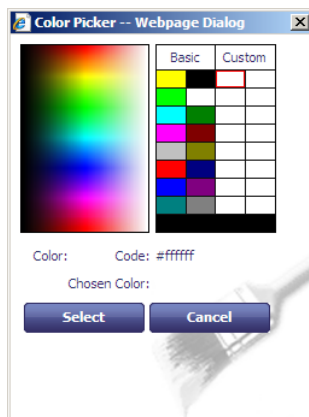
8.8 Changing the text color

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 Dynamically changing text size

You can apply a formatter to Auto Text boxes to ensure that the text size is reduced to allow the entire field to fit on the card when printed.

Note: The font size is reduced to a minimum of 4; if this is not sufficient, the text may still become truncated or wrap.

To resize the contents of an Auto Text box automatically:

1. In the Card Layout Editor, open the card layout you want to work with.
2. Select the Auto Text box you want to configure.
3. From the **Formatter** drop-down list, select **FitTextFormatter**.
4. Save the card layout.

You can also link two Auto Text boxes to ensure that they are scaled by the same amount. The font size of the two fields is reduced by the same percentage so that they both fit inside their respective widths; the font's family, size, and weight of each field may be different, but you are recommended to use the same values for both fields.

For example, to have two elements, `First Name` and `Initial` and `Surname` and `Suffix` scale by the same amount:

1. Create a custom Auto Text element with a value of `[[Firstname]] [[Initial]]` set to the maximum required font size.
2. Create a custom Auto Text element with a value of `[[Surname]] [[Suffix]]` set to the maximum required font size.
3. For each field, from the **Formatter** drop-down list, select **FitTextFormatter**.
4. Select the first field, then from the **No Larger Than** drop-down list, select the second field.
5. Select the second field, then from the **No Larger Than** drop-down list, select the second field.

8.10 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:

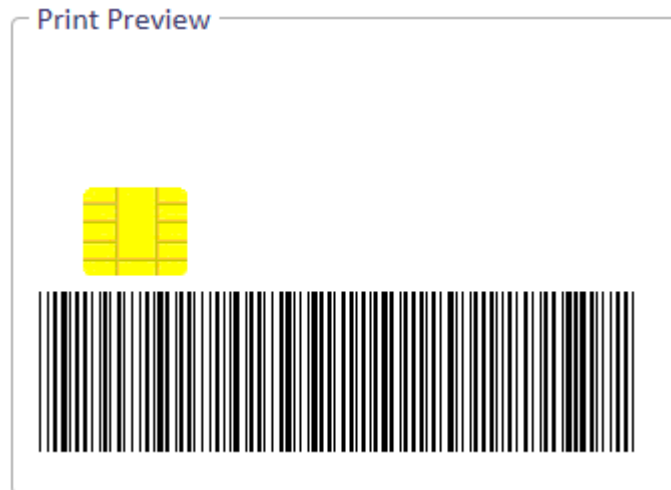
- Click the bottom-right corner of the element, then drag the element to the required size. If you hold down CTRL, you can change the aspect ratio of the element.
- Type the size in the **Width** and **Height** boxes. You can specify values between 0 and 200.

8.11 Adding barcodes

You can add barcodes to your card layouts; these barcodes can contain information from the cardholder's record.

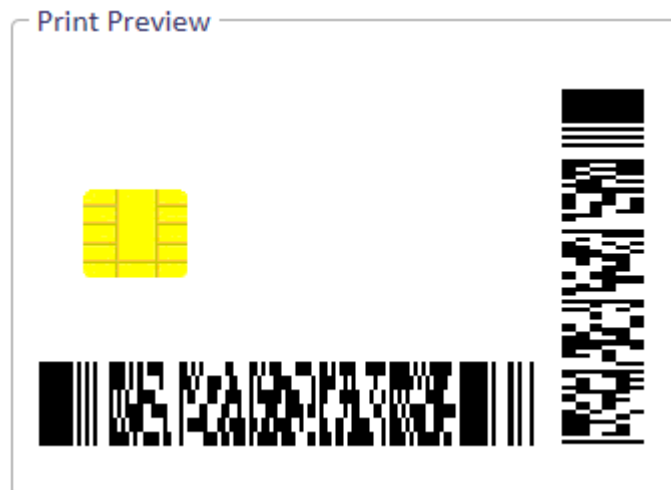
MyID supports the following formats for barcodes:

- 1D barcode.



This is a standard 1D barcode in Code 39 format. You can add a barcode in this format for any auto text field on a card layout by selecting the **Barcode** font. MyID supports the Code 39 Extended character set.

- 2D barcode.




These are PDF417 2D barcodes in either horizontal or vertical orientation. You must use custom attributes to hold the 2D barcode data.

Use of 2D barcodes requires customization using Project Designer. For more information, contact Intercede customer support, quoting reference SUP-155.

Note: 2D barcodes are supported on printed cards, the MyID Wallet app, and mobile apps developed using the Identity Agent Framework. You cannot use 2D barcodes in the MyID Identity Agent app.

8.11.1 Adding a 1D barcode

To add a 1D barcode to your card layout:

1. In the **Card Layout Editor**, open the layout to which you want to add the barcode.
2. In the toolbar, click **Insert Auto Text** .
3. From the **System Text** drop-down list, select the field you want to encode as the barcode.
4. From the **Font** drop-down list, select **Barcode**.
5. Resize the text box to the size you want to render the barcode.

Note: Currently, you cannot rotate a barcode. If you rotate the text box, the rotation is ignored when MyID renders the barcode.

6. Save the card layout.
7. If necessary, update the credential profile to add the card layout.

8.11.2 Previewing a barcode

The preview within the **Card Layout Editor** does not render the barcode. To preview the barcode, you must use the **Print Badge** workflow or one of the card issuance workflows that allow you to print cards.

Note: The **Print Badge** workflow can display user information, but cannot display device information, as there is no associated device; if your barcode contains device information (for example, the device serial number) you must use **Print Card** or **Collect Card**.

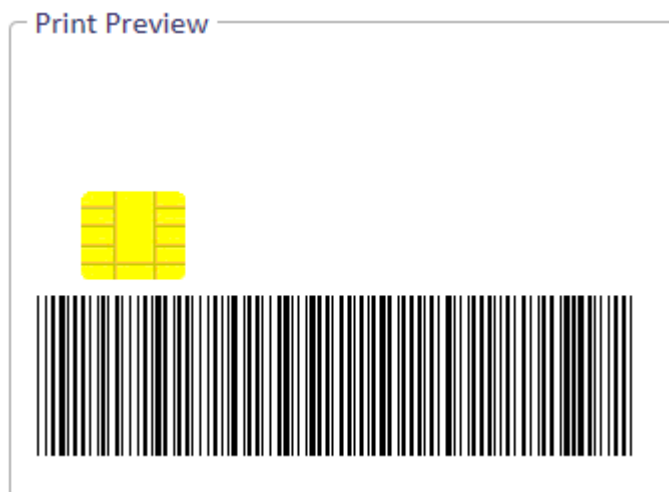
To preview a barcode using the **Print Badge** workflow:

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

You can also launch this workflow from the View Person screen in the MyID Operator Client. See the *Printing a badge* section in the [MyID Operator Client](#) guide for details.

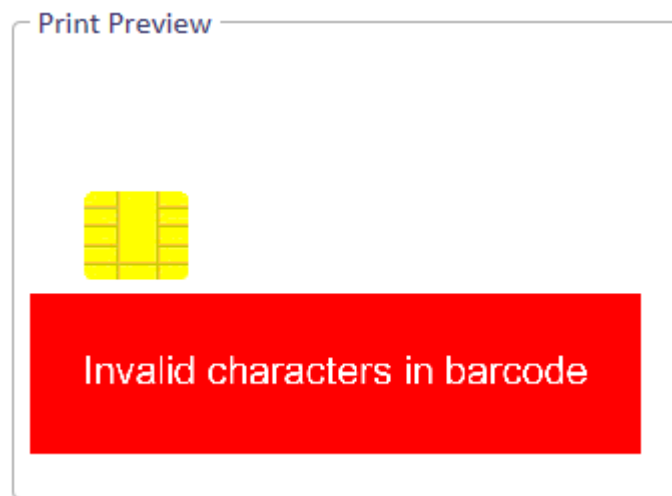
2. Search for the person and select their record.
3. Select your printer and click **Continue**.
4. Select the card layout from the list.

The card layout, complete with barcode, is displayed in the print preview.



Note: The **Print Badge** workflow displays a preview of only the front card layout. If you want to preview the back card layout, you must use **Print Card** or **Collect Card**.

If there is a problem rendering the barcode, a red box appears containing error information.



For example:

- Invalid characters in barcode

There are invalid characters that cannot be rendered as a barcode; MyID supports the Code 39 Extended character set.

- Missing data for barcode

There is no information in the person's record for the field selected for the barcode.

5. Click **Print** to print the card layout, or go back to the MyID Desktop dashboard using the menu button at the top left.

If you launched the workflow from the MyID Operator Client, you can close the MyID Desktop window.

8.11.3 Known issues

- **IKB-384 – Barcode limitations**

The standard code 39 character set is limited to the following characters.

0123456789 [Space] ABCDEFGHIJKLMNOPQRSTUVWXYZ- . \$ / + %

The extended code 39 character set allows a greater range, including the full ASCII character set.

Some barcode scanners may not support reading the Code 39 Extended character set, which, for example, can include lower case characters.

If you have mapped a MyID attribute to a 1D barcode, and the attribute includes Code 39 Extended characters, then the barcode is printed but may produce incorrect information when read by an incompatible scanner.

You can mitigate this issue for some fields available for use in a card layout, which will automatically change lower case characters to upper case. These are:

- Direct fields – MyID PIV
 - Full Name
 - Last Name
 - First Name
 - Agency Association
- Calculated fields – MyID PIV
 - Card Serial Number
 - Type
 - Issue Date
 - Expiration Date
 - Ex Date
 - First Initial
 - First Name and Initial
 - Last Name Comma
 - IssuerID
 - Hair Color (Readable)
 - Eye Color (Readable)
 - Height
 - Suffix
 - Full Name and Suffix
 - Last Name and Suffix
 - Nickname (UpperCase)

Note: Characters that are in the source MyID attribute that are outside of the Code 39 Extended set cause print preview or printing to show a message similar to:

```
Invalid characters in barcode
```

8.12 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.

8.13 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.

8.13.1 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.

8.13.2 Template XML structure

The templates are stored in the `templates.xml` file in the following folder:

`C:\Program Files\Intercede\MyID\Web\WebENT\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.

8.13.2.1 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>

```

8.14 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.

Produces numeric-only PINs.

See section [9.3, EdeficePinGenerator PIN generation algorithm](#) for details of the algorithm.

- **EdeficePolicyPinGenerator** – similar to the **EdeficePinGenerator** algorithm, but can be configured to produce PINs containing numbers, lower alpha, upper alpha, and symbol characters, based on the **PIN Characters** options in the credential profile.

See section [9.4, EdeficePolicyPinGenerator PIN generation algorithm](#) for details of the algorithm.

You can view PINs generated using the **EdeficePinGenerator** or **EdeficePolicyPinGenerator** algorithm on the View Device screen in the MyID Operator Client; see the *Viewing the initial PIN for a device* section in the [MyID Operator Client](#) guide for details.

- **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.

By default, the **RandomPINGenerator** produces numeric-only PINs. If you set the **Use PIN policy settings in random server PIN generation** configuration option (on the **PINs** page of the **Security Settings** workflow) the random PIN generator takes into account the allowed and mandatory PIN characters determined by the credential profile.

Both **EdeficePinGenerator** and **EdeficePolicyPinGenerator** require a PIN generation key to ensure the security of the PIN generation algorithm. See:

- section [9.1, Adding a PIN generation key](#).

You must set up your credential profile to configure the PIN generation options. See:

- section [9.2.1, PIN generation for issuance](#).
- section [9.2.2, PIN generation for reset](#).

9.1 Adding a PIN generation key

You require a PIN Generation key for PINs generated using the **EdeficePinGenerator** or **EdeficePolicyPinGenerator** 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**.

The screenshot shows the 'Add Key (PIN Generation Key)' form. It has a 'Key Name' field, a 'Description' field, and an 'Encryption Type' dropdown menu set to '2DES'. Below these are three radio button options: 'Automatically Generate Encryption Key in Software and Store on Database', 'Encryption Key' (which is selected), and 'Use Key Ceremony'. The 'Encryption Key' option has a 'Key Checksum Value' field. There is also a 'Key Attributes' section with an 'Exportable' checkbox. A 'Save' button is located at the bottom right of the form.

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** and **EdeficePolicyPinGenerator** PIN generators in the current version use 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](#) or section [9.4, EdeficePolicyPinGenerator PIN generation algorithm](#).

- **Encryption Key** – type the key into the box. Optionally, you can include the **KeyChecksum 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 [16.2.5, Exporting keys](#) for more information.
9. Click **Save**.

9.2 Credential profile setup for PIN generation

You can configure MyID to generate PINs when issuing smart cards, and also optionally to regenerate a PIN when resetting the card PIN using the **Reset Card PIN** workflow; see the *Resetting a card's PIN* section in the [Operator's Guide](#).

For details of the available options in the credential profile, see the *PIN Settings* section in section [11.3.1, Credential profile options](#).

You are recommended to set the **PIN Settings** and **PIN Characters** options in the credential profile to match the required PIN policy for the device. 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.

The PIN generators use the following PIN characters:

- **EdeficePinGenerator** – generates numeric-only PINs. You must set the **PIN Characters** options in the credential profile to numeric only.
- **EdeficePolicyPinGenerator** – generates PINs conforming to the **PIN Characters** options in the credential profile.
- **RandomPinGenerator** – by default, generates numeric-only PINs. If you want the random PIN generator to produce PINs conforming to the **PIN Characters** options in the credential profile, you must set the **Use PIN policy settings in random server PIN generation** configuration option (on the **PINs** page of the **Security Settings** workflow).

9.2.1 PIN generation for issuance

For smart card issuance, set the **Issue With** option to **Server Generated PIN**, then select the options you want to use in the credential profile to specify server-side PIN generation.

For example, to use a known algorithm to generate a repeatable 8-digit PIN, set the following options:

- **Issue With – Server Generated PIN**
- **Length** – 8
- **PIN Algorithm** – **EdeficePinGenerator** or **EdeficePolicyPinGenerator**
- **Protected Key** – select the key you added for PIN generation; see section [9.1, Adding a PIN generation key](#).
- **Select PIN Mailing Document** – optionally, select the HTML template you want to use to generate the PIN mailer. The generated PIN is not displayed on screen, so you may want to send the cardholder a PIN mailer.

You can use the known algorithm to generate the PIN on another system using the protected key and the card serial number, and provide the PIN to the cardholder that way as an alternative to using a PIN mailer. See section [9.3, EdeficePinGenerator PIN generation algorithm](#) or section [9.4, EdeficePolicyPinGenerator PIN generation algorithm](#) for details of using the algorithm to generate the PINs.

To use a random server-generated 8-digit PIN, set the following options:

- **Issue With – Server Generated PIN**
- **Length** – 8
- **PIN Algorithm** – **RandomPinGenerator**

Note: A PIN generated using the **RandomPinGenerator** is displayed on screen only during the **Issue Card** workflow; if you are using any other workflow to issue the card, you must either select the **Email PIN** option in the credential profile, and configure MyID to send email notifications, or select an HTML template from the **Select PIN Mailing Document** option in the credential profile, and print the mailing document when collecting the card.

9.2.2 PIN generation for reset

To generate PINs when resetting a smart card's PIN using the **Reset Card PIN** workflow, from the **Reset PIN to Secure Value** option in the **PIN Settings** section of the credential profile, select **EdeficePinGenerator**, **EdeficePolicyPinGenerator**, or **RandomPinGenerator**.

For example, to use a known algorithm to generate a repeatable 8-digit PIN, set the following options:

- **Length** – 8
- **Reset PIN to Secure Value** – **EdeficePinGenerator** or **EdeficePolicyPinGenerator**
- **Reset PIN Protected Key** – select the key you added for PIN generation; see section [9.1, Adding a PIN generation key](#).
- **Select PIN Reset Document** – optionally, select the HTML template you want to use to generate the PIN mailer. The generated PIN is not displayed on screen, so you may want to send the cardholder a PIN mailer. Alternatively, you can use the known algorithm to generate the PIN on another system using the protected key and the card serial number, and provide the PIN to the cardholder that way.

See section [9.3, EdeficePinGenerator PIN generation algorithm](#) or section [9.4, EdeficePolicyPinGenerator PIN generation algorithm](#) for details of using the algorithm to generate the PINs.

To use a random server-generated 8-digit PIN, set the following options:

- **Length** – 8
- **Reset PIN to Secure Value** – **RandomPinGenerator**
- **Select PIN Reset Document** – select the HTML template you want to use to generate the PIN mailer.

Note: A PIN generated using the **RandomPinGenerator** is not displayed on screen; you *must* select an HTML template from the **Select PIN Reset Document** option, and print the mailing document resetting the PIN.

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, $\text{<byte> modulo <alphabet size>}$.

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

9.3.2.1 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. If you want to generate PINs that use alphabetic or symbol characters, you are recommended to use the **EdeficePolicyPinGenerator** PIN generator instead; see section [9.4, EdeficePolicyPinGenerator PIN generation algorithm](#).

9.3.2.2 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.

9.3.2.3 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 numeric pin this results in:

78 (hex) = 120 (dec) mod 10 = 0

49 (hex) = 73 (dec) mod 10 = 3

DE (hex) = 222 (dec) mod 10 = 2

09 (hex) = 9 (dec) mod 10 = 9

B2 (hex) = 178 (dec) mod 10 = 8

59 (hex) = 89 (dec) mod 10 = 9

5. The PIN returned is 032989.

9.3.3.1 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) % alphabetsize];
}

for (int i = 0; i < hash.Length; i++)
{
    hashhex = hashhex + hash[i].ToString("X2");
}
for (int i = 0; i < hash16.Length; i++)
{
    hashhex16 = hashhex16 + hash16[i].ToString("X2");
}

Console.WriteLine("Sample PIN generation algorithm output");
Console.WriteLine();
Console.WriteLine("Alphabet size: " + alphabetsize);
Console.WriteLine("Required PIN length: " + pinlength);
Console.WriteLine("Data: " + data);
Console.WriteLine("SHA1 hash of data: " + hashhex);
Console.WriteLine("16 bytes of hash: " + hashhex16);
Console.WriteLine("Encrypted: " + ciphertext);
Console.WriteLine("\nPIN: " + pin);
Console.WriteLine("\nPress any key to continue...");
Console.ReadKey(true);
}
}
}
```

9.4 EdeficePolicyPinGenerator PIN generation algorithm

The **EdeficePolicyPinGenerator** PIN generation algorithm is similar to the **EdeficePinGenerator** PIN generation algorithm, but takes into account the PIN character settings configured on the credential profile. The 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, the details of the PIN character settings in the credential profile, 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.

Note: If the credential profile has a PIN policy that allows only numeric characters, the **EdeficePolicyPinGenerator** PIN generation algorithm generates the same results as the **EdeficePinGenerator** algorithm.

9.4.1 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 (which is determined by the PIN policy in the credential profile) and take the remainder; in other words, $\text{<byte> modulo <alphabet size>}$.

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.

Note: If you need to insert any mandatory characters (see below), reduce the length of the PIN accordingly; for example, for an 8-character PIN, if both symbols and numbers are mandatory, generate a 6-character PIN. You will insert extra characters for the mandatory character types later to reach the full PIN length.

5. Use this value as a look-up in the alphabet table – see section [9.4.2, Alphabet tables](#).

For example, if the byte is 2C, and the alphabet size is 32 (for a PIN that contains numbers and symbols):

`2C = 44 decimal`

`44 modulo 32 = 12`

`Entry 12 in the alphabet table = '\'`

6. Insert any mandatory characters.

If the PIN policy has more than one allowed character type, and the PIN policy has one or more mandatory character types, you must insert one character for each mandatory type. For example, if lower and upper case characters are optional, but numeric and symbol characters are mandatory, insert one number and one symbol.

If the PIN policy has only one type of character allowed (for example, only numeric) do *not* insert any mandatory characters; the PIN is already guaranteed to contain characters of that type.

To generate the mandatory characters, use the same method as for the other characters (take the next byte in the encrypted hash, and use it as an index into the alphabet table), but use the specific alphabet table for the category; for example, for mandatory symbol characters use the symbol table.

We do not want to append the mandatory characters to the end of the PIN; this is insufficiently random. To determine the position of the inserted character, take a byte from the *end* of the encrypted hash, and use this modulo the current PIN size plus one to determine the insertion point. For a second mandatory character, use the second-last byte from the encrypted hash, and so on.

For example, if the last byte is 36, and the current PIN length is 6 characters:

`36 = 54 decimal`

`54 modulo 7 = 5`

You can then insert the character at position 5 (this is zero indexed; if the PIN is currently six characters, modulo 7 produces a value between 0 and 6, where 0 means inserting the character at the start, and 6 means inserting the character at the end).

You must insert the mandatory characters in the following order:

- Numeric
- Lower alpha
- Upper alpha
- Symbol

9.4.2 Alphabet tables

The alphabet table is generated from the PIN policy, and may comprise the following:

- Numeric
- Lower alpha
- Upper alpha
- Symbol

If your PIN policy allows more than one character type, combine the tables in the above order.

9.4.2.1 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.

9.4.2.2 Lower alpha

The lower alpha alphabet has size 26, 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				
Value	u	v	w	x	y	z				

For example, a lookup of 0 returns a, and a lookup of 7 returns h.

9.4.2.3 Upper alpha

The upper alpha alphabet has size 26, 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				
Value	U	V	W	X	Y	Z				

For example, a lookup of 0 returns A, and a lookup of 7 returns H.

9.4.2.4 Symbol

The symbol alphabet has size 22, and has the following entries:

Index	0	1	2	3	4	5	6	7	8	9
Value		!	\	"	#	\$	%	&	'	(
Index	10	11	12	13	14	15	16	17	18	19
Value)	*	+	-	.	/	:	;	=	?
Index	20	21								
Value	@	^								

For example, a lookup of 0 returns a space character, and an lookup of 7 returns &.

9.4.2.5 Combined table

For example, for a PIN policy that requires numbers and symbols, the combined table would look like:

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		!	\	"	#	\$	%	&	'	(
Index	20	21	22	23	24	25	26	27	28	29
Value)	*	+	-	.	/	:	;	=	?
Index	30	31								
Value	@	^								

You must combine tables in the following order:

- Numeric
- Lower alpha
- Upper alpha
- Symbol

9.4.3 Example

If a PIN with a length of eight characters is requested for a card with serial number 1034, and the PIN policy allows numeric, lower alpha, upper alpha, and symbols, with both numeric and symbol characters mandatory, the process is as follows:

1. The card serial number, 1034, is hashed using SHA1 to produce:

```
290448489A06C6A2DC62E82491212444BD6E341F
```

2. This is then shortened to 16 bytes, as we want to encode two whole 8-byte blocks:

```
290448489A06C6A2DC62E82491212444
```

3. This hash is then 3DES CBC mode encrypted using a shared key to produce, for example:

```
1F60F51F7D6FF3C316E006C7D239DA36
```

4. The PIN required is eight characters, but there are two categories of mandatory characters, so create a 6-digit PIN to begin with. You will insert two mandatory characters later to produce a PIN of the required length.

All four categories of character are allowed (numeric, lower alpha, upper alpha, and symbols) so the alphabet table is a combination of all four, 84 characters in total.

The first six bytes from the encrypted hash are used to look up into the alphabet array (size 84). This results in:

Byte 1 of the encrypted string is 1F (hex) = 31 (dec) mod 84 = 31

Character 31 in the alphabet table is **v**

Byte 2 of the encrypted string is 60 (hex) = 96 (dec) mod 84 = 12

Character 12 in the alphabet table is **c**

Byte 3 of the encrypted string is F5 (hex) = 245 (dec) mod 84 = 77

Character 77 in the alphabet table is /

Byte 4 of the encrypted string is 1F (hex) = 31 (dec) mod 84 = 31

Character 31 in the alphabet table is v

Byte 5 of the encrypted string is 7D (hex) = 125 (dec) mod 84 = 41

Character 41 in the alphabet table is F

Byte 6 of the encrypted string is 6F (hex) = 111 (dec) mod 84 = 27

Character 27 in the alphabet table is r

The initial six-character PIN is:

vc/vFr

5. Insert the mandatory characters.

There are two mandatory character types in the eight-digit PIN, so the seventh and eighth bytes of the encrypted hash are used to determine the characters to use, and the last and penultimate bytes of the encrypted hash are used to determine the insertion positions of these characters.

To add the mandatory numeric character:

Byte 7 of the encrypted string is F3 (hex) = 243 (dec) mod 10 = 3

Character 3 in the numeric alphabet table is 3

For position, take the last byte of the encrypted hash, and find the modulo of 7 (the current PIN size plus 1):

Byte 16 of the encrypted string is 36 (hex) = 54 (dec) mod 7 = 5

Inserting 3 into vc/vFr at position 5 (zero indexed) produces a seven-digit PIN of:

vc/vF3r

To add the mandatory symbol character:

Byte 8 of the encrypted string is C3 (hex) = 195 (dec) mod 22 = 19

Character 19 in the symbol alphabet table is ?

For position, take the second-last byte of the encrypted hash, and find the modulo of 8 (the current PIN size plus 1):

Byte 15 of the encrypted string is DA (hex) = 218 (dec) mod 8 = 2

Inserting ? into vc/vF3r at position 2 (zero indexed) produces a final PIN of:

vc?/vF3r

This PIN matches the PIN policy in the credential profile – it is eight characters long, includes both symbols and numbers as mandatory characters, and allows both upper and lower case alpha characters.

9.4.3.1 C# example

The following is sample code that generates PINs using C#. The default settings in the sample code produce the same result as the worked example above.

```
using System;
using System.Collections.Generic;
using System.Linq;
using System.Text;
using System.Security.Cryptography;

namespace PINGeneration
{
    class Program
    {
        static void Main(string[] args)
        {
            char[] numeric = { '0', '1', '2', '3', '4', '5', '6', '7', '8', '9' };
            char[] alphaLower = { 'a', 'b', 'c', 'd', 'e', 'f', 'g', 'h', 'i', 'j', 'k', 'l',
'm',
            'n', 'o', 'p', 'q', 'r', 's', 't', 'u', 'v', 'w', 'x', 'y', 'z' };
            char[] alphaUpper = { 'A', 'B', 'C', 'D', 'E', 'F', 'G', 'H', 'I', 'J', 'K', 'L',
'M',
            'N', 'O', 'P', 'Q', 'R', 'S', 'T', 'U', 'V', 'W', 'X', 'Y', 'Z' };
            char[] symbols = { '!', '\\', '"', '#', '$', '%', '&', '\\', '(', ')', '*',
'+', '-', '.', '/', ':', ';', '=', '?', '@', '^' };

            // The policy values are:
            // 0 - Optional
            // 1 - Mandatory
            // 2 - Not allowed
            int numericPinPolicy = 1;
            int lowercasePinPolicy = 0;
            int uppercasePinPolicy = 0;
            int symbolsPinPolicy = 1;

            // Configure the available characters
            StringBuilder allowedSymbolsBuilder = new StringBuilder();
            char[] alphabet = { };
            if (numericPinPolicy != 2)
            {
                alphabet = alphabet.Concat(numeric).ToArray();
                allowedSymbolsBuilder.Append('N');
            }

            if (lowercasePinPolicy != 2)
            {
                alphabet = alphabet.Concat(alphaLower).ToArray();
                allowedSymbolsBuilder.Append('L');
            }

            if (uppercasePinPolicy != 2)
            {
                alphabet = alphabet.Concat(alphaUpper).ToArray();
                allowedSymbolsBuilder.Append('U');
            }

            if (symbolsPinPolicy != 2)
```



```

{
    alphabet = alphabet.Concat(symbols).ToArray();
    allowedSymbolsBuilder.Append('S');
}

var allowedSymbols = allowedSymbolsBuilder.ToString();

// Only need to configure mandatory character set if more than one character type is
// allowed in the PIN
StringBuilder mandatorySymbolsBuilder = new StringBuilder();
if (allowedSymbols.Length > 1)
{
    if (numericPinPolicy == 1)
        mandatorySymbolsBuilder.Append('N');

    if (lowercasePinPolicy == 1)
        mandatorySymbolsBuilder.Append('L');

    if (uppercasePinPolicy == 1)
        mandatorySymbolsBuilder.Append('U');

    if (symbolsPinPolicy == 1)
        mandatorySymbolsBuilder.Append('S');
}

var mandatorySymbols = mandatorySymbolsBuilder.ToString();

// 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");
}

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");
}

// Generate PIN from the ciphertext
int pinLength = 8;
int initialPinLength = pinLength - mandatorySymbols.Length;
for (int x = 0; x < initialPinLength; x++)
{
    pin = pin + alphabet[Convert.ToInt32(ciphertext.Substring(x * 2, 2), 16) %
alphabet.Length];
}

// Now insert the mandatory characters into the pin
for (int index = 0; index < mandatorySymbols.Length; index++)
{
    // Do not use the same hash values for selection of both the initial PIN
characters and the mandatory characters
    var y = index + initialPinLength;
    char character = ' ';
    switch (mandatorySymbols[index])
    {
        case 'N':
            character = numeric[Convert.ToInt32(ciphertext.Substring(y * 2, 2), 16) %
numeric.Length];
            break;

        case 'L':
            character = alphaLower[Convert.ToInt32(ciphertext.Substring(y * 2, 2), 16) %
alphaLower.Length];
            break;

        case 'U':
            character = alphaUpper[Convert.ToInt32(ciphertext.Substring(y * 2, 2), 16) %
alphaUpper.Length];
            break;

        case 'S':
            character = symbols[Convert.ToInt32(ciphertext.Substring(y * 2, 2), 16) %
symbols.Length];
            break;
    }
}

```

```
// Determine where to insert this character. Use the seed from reverse to
determine the character position.
    int position = Convert.ToInt32(ciphertext.Substring(ciphertext.Length - index * 2
- 2, 2), 16) % (pin.Length + 1);
    pin = pin.Insert(position, character.ToString());
}

Console.WriteLine("Sample PIN generation algorithm output");
Console.WriteLine();
Console.WriteLine("Alphabet size:         " + alphabet.Length);
Console.WriteLine("Allowed character set:  " + allowedSymbols);
Console.WriteLine("Mandatory character set: " + mandatorySymbols);
Console.WriteLine("Required PIN length:    " + pin.Length);
Console.WriteLine("Data:                   " + data);
Console.WriteLine("SHA1 hash of data:      " + hashhex);
Console.WriteLine("16 bytes of hash:      " + hashhex16);
Console.WriteLine("Encrypted:              " + ciphertext);
Console.WriteLine("PIN:                   " + 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 service 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 [31.4, 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 Working with 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.

You can also launch this workflow from the **Credential Configuration** section of the **More** category in the MyID Operator Client. See the *Using Credential Configuration workflows* section in the [MyID Operator Client](#) guide for details.

- 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 or the MyID Operator Client to help users select the appropriate card.

Credential Profile

Name:

Description:

Device Friendly Name:

Card Encoding

Option	Device Category
<input checked="" type="checkbox"/> Contact Chip	Card
<input type="checkbox"/> Contactless Chip	Card
<input type="checkbox"/> Magnetic Stripe (Only)	Card
<input type="checkbox"/> Microsoft Virtual Smart Card	VSC
<input type="checkbox"/> Windows Hello	VSC
<input type="checkbox"/> FIDO Authenticator (Only)	FIDO
<input type="checkbox"/> Identity Agent	Mobile
<input type="checkbox"/> Mobile Identity Document	Document
<input type="checkbox"/> Software Certificates (Only)	SoftCert
<input type="checkbox"/> Device Identity (Only)	Machine
<input type="checkbox"/> Externally Issued (Only)	Unmanaged
<input type="checkbox"/> Derived Credential	

Next

The **Device Category** groups the various card encoding options into logical categories; for example, contact chip cards, contactless cards, and magnetic stripe cards are all treated as part of the **Card** category. For more information, see the *Working with device categories* section in the *MyID Operator Client* guide. Note that Derived Credential does not have a category, as a derived credential always has another device type; for example, a VSC derived credential, or a contact card derived credential.

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.

11.3.1.1 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.
- **Microsoft Virtual Smart Card** – used for Microsoft VSCs. See the *Setting up a credential profile for VSCs* section in the [Microsoft VSC Integration Guide](#).
- **Windows Hello** – used for Windows Hello for Business credentials. See the *Creating the Windows Hello credential profile* section in the [Windows Hello for Business Integration Guide](#).
- **FIDO Authenticator (Only)** – used for FIDO credentials. See the *Setting up credential profiles for FIDO authenticators* section in the [FIDO Authenticator Integration Guide](#).
- **Identity Agent** – used for mobile identities.
See the *Setting up the Identity Agent credential profiles* section in the [Mobile Identity Management](#) guide.
- **Mobile Identity Document** – used for mobile identity documents.
See the *Creating the mobile identity document credential profile* section in the [Mobile Identity Documents](#) guide.
- **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 [24.5, *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.
- **Derived Credential** – used for derived credentials.
See the *Setting up the credential profiles for derived credentials* section in the [Derived Credentials Self-Service Request Portal](#) guide.

The **Device Category** for each type of card encoding is shown. For more information, see the *Working with device categories* section in the [MyID Operator Client](#) guide.

11.3.1.2 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.

11.3.1.3 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, which is set by the **Card Expiration Period (days)** configuration option – see section [31.5, Process page \(Security Settings\)](#). 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; see 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 [25, *Additional identities*](#).

- **Key Recovery Only**

Used for key recovery operations. See section [19, *Key recovery*](#) for details.

- **Require Activation**

Used for card activation. If you do not want to use activation, select **No**; for all other options, see section [23.1, *Configuring a credential profile for activation*](#).

- **Pre-encode Card**

Used for card activation. See section [23.1, *Configuring a credential profile for activation*](#) for details.

- **Require Fingerprints at Issuance**

Used to specify whether fingerprints are required when issuing a card. See section [11.3.2.7, *Authentication methods*](#) 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](#).
- **Terms and Conditions Template**

If you require the cardholder to sign terms and conditions, depending on the method used for the workflow, you may have to specify an HTML template to be used for the terms and conditions text.

For details, see section [11.6, Customizing terms and conditions](#).
- **Credential Group** – see section [11.3.2.1, Credential group](#) for details.
- **Exclusive Group** – see section [11.3.2.2, Exclusive Group](#) for details.
- **Block Multiple Requests for Credential Group** – see section [11.3.2.4, Block Multiple Requests for Credential Group](#) 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 MIFARE or HID PROX-capable PIV cards you are issuing. See section [10, Importing serial numbers](#) for instructions on importing serial numbers into MyID.

This option affects the **Collect Card** and **Batch Collect Card** workflows only; if you collect a card by any other method (for example, using the Self-Service App) this option is ignored.

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.

Support for MIFARE devices requires an additional update. Contact customer support quoting reference SUP-380 for more information.

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.

Note: If you want the serial number of a MIFARE card to be stored as a MIFARE Serial Number, as well as being stored as a standard Serial Number, you must set this option to **Must be a Proximity Card** or **Must be a Known Proximity Card**.

- **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, canceling a card or completing a workflow.

MyID provides notification schemes to be used when requesting a mobile device through the MyID Operator Client or MyID Core API; see the *Configuring SMS and email notifications for the MyID Operator Client* and *Creating the Identity Agent credential profile* sections in the [Mobile Identity Management](#) guide.

For non-mobile devices, 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.

See section [27.1, User Data Approved checks](#) for details of setting this option.

You can configure MyID to allow requests, but not issuance, before the user has their data approved using the **Allow requests without user data approved** configuration option; see section [27.1.2, Allowing device requests before the user's data is approved](#).

You can also use this feature in conjunction with the vetting date check to ensure that credentials are not issued to people whose identity checks have expired. See section [27, Identity checks](#) for details.

- **Constrain certificate lifetime to vetting date**

When certificates are issued to this device, their expiry date will not exceed the vetting date of the recipient, regardless of the expiry date of the device.

For more information about vetting dates, see section [27, Identity checks](#).

- **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 Code on Request**

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 using 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 [24.8, Requesting a device identity](#) for details.

- **Unrestricted Cancellation**

Allows you to re-use a card without first canceling 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 canceled with a status mapping of "Lost" (for **Collect My Card** and **Issue Card**) or "Cancel temporary card during replacement" (for **Collect Card**) and a comment indicating that the card was canceled 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**.

- **IKB-300 – Unrestricted Cancellation option not supported in the Self-Service App**

This feature is available only in MyID Desktop, and is not currently available in the Self-Service App.

- **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 [Setting up OPACITY](#) section in 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.

- **Ignore User Expiry Date** – set this option if you want to be able to issue devices with lifetimes that exceed the `MaxRequestExpiryDate` set for the person in the Lifecycle API.

Note: This setting affects requests made through the MyID Operator Client only. For more information, see the *Requesting a device for a person* section in the [MyID Operator Client](#) guide.

11.3.1.4 Self-Service Unlock Authentication

Note: Currently, you cannot use the **Self-Service Unlock Authentication** options to configure the authentication requirements for Identity Agent-based credential profiles.

To allow users to unlock their own credentials, you must set the **Self-service Unlock** option (on the **Self-Service** page of the **Security Settings** workflow) to Yes. This is a global setting.

You can set the following global authentication option for self-service unlock:

- **Ask Security Questions for Self Service Card Unlock** – on the **PINs** page of the **Security Settings** workflow.

You can also override these options using the Self-Service Unlock Authentication section of the credential profile.

Self-Service Unlock Authentication

Select the option below to override global configuration rules for unlock authentication

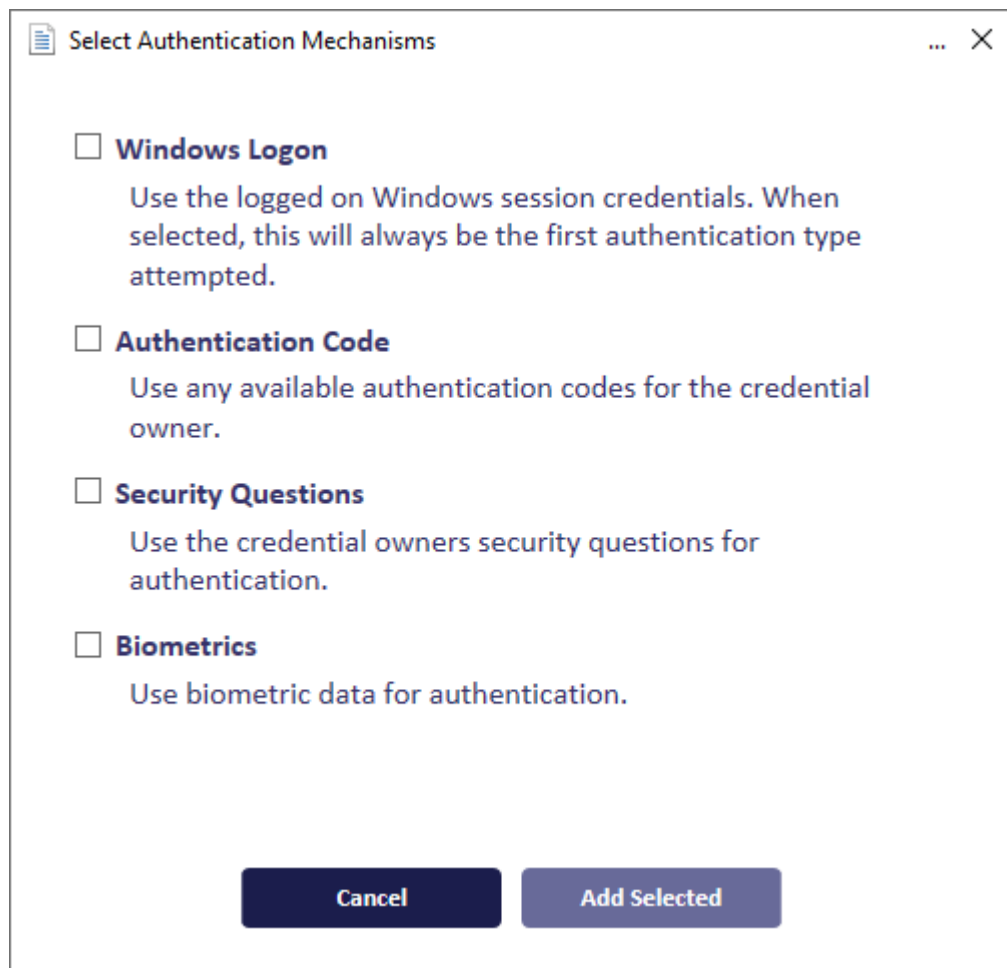
☐ Credential owners must authenticate using one of the methods below in the order shown

Authentication:

Move Up
Move Down
Add
Remove

To set the self-service authentication methods:

1. Select the **Credential owners must authenticate using one of the methods below in the order shown** option.
2. Click **Add**.



3. Select the authentication methods you want to use, then click **Add Selected**.

To change the order, select the logon mechanism and click **Move Up** or **Move Down**.

Note: If you have **Windows Logon** in your list, it stays at the top of the list – Windows authentication is carried out before any interactive authentication methods. If Windows authentication is successful, the user continues; if it is unsuccessful, the user is presented with the next logon mechanism in the list.

To remove an option, select the logon mechanism and click **Remove**.

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

11.3.1.5 MDM Restrictions

Available only if you have set the **Card Encoding** options to **Identity Agent** and **Derived Credential**.

Allows you to set restrictions for mobile identities issued using a Mobile Device Management system.

See the *Configuring credential profiles for MDM restrictions* section in the [Mobile Identity Management](#) guide for details.

11.3.1.6 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 *PIN policy settings* section of the appropriate chapter in 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](#) for details.

- 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.

- **Use Global PIN**

Set this option to issue the smart card with Global PIN support.

Global PIN is an alternative PIN for supported PIV cards that allows a wider range of characters than the standard numeric-only user PINs. The smart card must support this feature. See the *Global PIN support* section of the [Smart Card Integration Guide](#).

- **Reset PIN to Secure Value** – if you want to create a server-generated PIN when using the **Reset Card PIN** workflow, select one of the following options:
 - **EdeficePinGenerator** – uses the same algorithmic PIN generator as for issuance PINs above. If required, you can create a PIN mailer to be sent to the cardholder using the **Select PIN Reset Document** option in the **Mail Documents** section of the credential profile.
You must select the PIN generation key to use from the **Reset PIN Protected Key** drop-down list.
 - **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; you must set up MyID to issue a mailing document when the card PIN is reset using the **Select PIN Reset Document** option in the **Mail Documents** section of the credential profile.

See section 9, [PIN generation](#) for more information.

- **Reset PIN Protected Key** – select the PIN generation key you added using the **Key Manager** workflow. This option is required only if you select **EdeficePinGenerator** from the **Reset PIN to Secure Value** option.
- **Enforce Banned Words** – for user specified PINs, you can select this option to prevent the user from using particular words in their PINs.

See section 11.7, [Enforcing banned words in PINs](#) for more information.

11.3.1.7 PIN Characters

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

PIN Characters

	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 service 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 service.

11.3.1.8 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 *Distributing the pairing code* section in the [Smart Card Integration Guide](#) for details.

You can also use this template to print PIN mailing documents for soft certificate packages using the **Print Mailer Document** option in the MyID Operator Client. See section 11.5, [Setting up a credential profile for soft certificates](#).

- **Select PIN Reset 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 **Reset Card PIN** workflow.
- **Select Transport Document** – select the name of the HTML template stored in the MyID database to be used when collecting a soft certificate package. See section 11.5, [Setting up a credential profile for soft certificates](#).

For details of configuring HTML templates, contact customer support, quoting reference SUP-255.

11.3.1.9 Credential Stock

This is used only if you are using a bureau to issue cards.

11.3.1.10 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.

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.

11.3.1.11 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.

	Not Required	Required for Request	Required for Validate / Collect	Required Value(s)
Email <input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="text"/>
Employee ID <input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="text"/>
Info 1 <input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="text"/>
Info 2 <input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="text"/>
Info 3 <input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="text"/>
Info 4 <input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="text"/>
Mobile <input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="text"/>
User Principal Name <input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="text"/>
User SID <input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="text"/>

You can use this option to restrict the issuance of credentials to users with the appropriate attributes; for example, if the 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 credential based on this credential profile. Similarly, if your credential is to be used for Windows Logon, you must select **User Principal Name** from this list, and provide an appropriate certificate for logging on to Windows. For Windows authentication, you must select User SID in this list, and provide a certificate that has the user security identifier attribute mapped; see section [6.9, Including user security identifiers in certificates](#).

For each user attribute, you can select the following options:

- **Not required** – The user does not need a value set for this attribute.
- **Required for Request** – The user must have a value set for this attribute before a credential request can be created for the user, and also when validating or collecting the request.
- **Required for Validate / Collect** – The user must have a value set for this attribute before the credential request can be validated or the credential collected.
- **Required Value(s)** – Optionally, a comma-separated list of required values for the attribute. If the **Required for Request** or **Required for Validate / Collect** option is selected, and this field is blank, then any value is accepted. If one of the **Required...** options is selected, and this field contains one or more possible values, the attribute must contain one of these values to be accepted.

Note: You can use only the following characters in this field:

a-z A-Z 0-9 ' - @ .

and the space character.

Important: If you are using a field where the values are controlled by the `SelectOptions` table, the values you provide must match the entries in the `Value` field in the `SelectOptions` table, not the `DisplayValue` field. This does not currently apply to any of the default set of requisite fields, so you can ignore this requirement if your system does not have a customized list of requisite user data options.

You can select the following user attributes:

- **Email**
- **Employee ID**
- **Info1**
- **Info2**
- **Info3**
- **Info4**
- **Mobile**
- **User Principal Name**

Note: These are the default available fields; depending on your system, you may have a different list, or the names of the fields may be different; for example, the **Mobile** field may be called **Cell**; also, the **Address 1** field may be called **Info 1**, or another, custom, value. If your system implementation has customized the **Address1/Info 1** field, to ensure that a meaningful label is displayed in the user interface and in the audit record, you can update the `DisplayValue` for this option in the `SelectOptions` table in the database:

```
UPDATE [dbo].[SelectOptions]
SET [DisplayValue]=N'<insert translated text here>'
WHERE [SelectID]=N'CredentialProfile_Required'
AND [Value]=N'OptionalLine1';
```

11.3.1.12 Restricting the list of credential profiles displayed

You can configure your system to hide any credential profiles that do not meet the Requisite User Data requirements by setting the **Show Disqualified Credential Profiles** option to **No**.

Note: This setting affects the display of credential profiles in the MyID Operator Client only.

To hide disqualified credential profiles:

1. From the **Configuration** category, select **Operation Settings**.
2. Click the **Issuance Processes** tab.
3. Set the following option:
 - **Show Disqualified Credential Profiles** – set to **No** to hide any credential profiles that do not meet the Requisite User Data requirements.

The default value is **Yes**, which displays all credential profiles, whether or not they meet the Requisite User Data requirements
4. Click **Save changes**.

11.3.2 Additional credential profile options

Additional credential profile options are shown if MyID has been configured to enable particular features.

11.3.2.1 Credential group

If you have set the **Active credential profiles per person** configuration option – see section [30.10, 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 canceled, 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.

Note: A mobile identity on a single physical device may contain multiple logical devices (the Identity Agent itself, and separate devices for the credential stores) but for the purpose of this feature is treated as a single credential.

11.3.2.2 Exclusive Group

If you provide a value in this field, MyID prevents you from requesting or collecting credentials if the cardholder has an issued device or a request for a device that has a different value in its credential profile for its **Exclusive Group**.

You can request and collect as many credentials as you require that have the same **Exclusive Group** value. You can also request and collect as many credentials as you require that have no value in their **Exclusive Group**.

MyID checks the latest version of the relevant credential profiles, not the versions that were used to request or collect the device, when checking whether you can request or collect a device. MyID also checks the exclusive groups at request, validation, and collection; the cardholder's list of issued or requested devices, and the exclusive group settings of the credential profiles used to issue or request devices, may change between the request and the collection.

For example, if you have the following credential profiles:

- ContractorA – has an **Exclusive Group** of Contractor.
- ContractorB – has an **Exclusive Group** of Contractor.
- EmployeeA – has an **Exclusive Group** of Employee.
- UniversalA – has no **Exclusive Group**.

You can request and collect the following credentials to the same cardholder:

- ContractorA, ContractorB – a combination of two Contractor credentials.
- ContractorA, ContractorB, UniversalA – a combination of two Contractor credentials and one with no exclusive group.
- ContractorA, UniversalA – a combination of Contractor and no exclusive group.
- ContractorB, UniversalA – a combination of Contractor and no exclusive group.
- EmployeeA, UniversalA – a combination of Employee and no exclusive group.

But you *cannot* issue the following credentials to the same cardholder:

- ContractorA, EmployeeA – a combination of Contractor and Employee exclusive groups.
- ContractorB, EmployeeA – a combination of Contractor and Employee exclusive groups.

11.3.2.3 Exclusive group messages

The message when you attempt to request a device that is not permitted due to the exclusive group configuration is similar to the following:

- In the MyID Operator Client:

The user has an existing request or device that exists with a different exclusive group, the request cannot be added.

Error number: WS50055

- In MyID Desktop:

Error: Unable to request credential.

Cause: The credential could not be requested because the user has a request or a credential with a different exclusive group.

Solution: To request a new credential, either cancel any pending requests or credentials that are within a different group.

The message when you attempt to validate a device that is not permitted due to the exclusive group configuration is similar to the following:

- In the MyID Operator Client:

The user has an existing request or device that exists with a different exclusive group, the request cannot be validated.

Error number: WS50056

- In MyID Desktop:

Error: Unable to validate credential.

Cause: The credential could not be validated because the user has a request or a credential with a different exclusive group.

Solution: To validate this credential, either cancel any pending requests or credentials that are within a different group.

The message when you attempt to collect a device that is not permitted due to the exclusive group configuration is similar to the following:

- In the **Collect Card** workflow (whether launched from MyID Desktop or from the MyID Operator Client):

Validation Error

An existing request or device exists with a different exclusive group.

11.3.2.4 Block Multiple Requests for Credential Group

Set this option to prevent an operator from creating a request for a person if they already have an outstanding request for a device with the same credential group. The operator will also be prevented from approving a request if the person has an outstanding request for a device with the same credential group.

Note: This affects operations carried out in the MyID Operator Client only. It does not affect requests made through MyID Desktop or the Lifecycle API. This feature does not support mobile issuance.

11.3.2.5 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.

11.3.2.6 Issue over Existing Credential

This option affects only the following types of credential:

- Mobile derived credentials issued through an MDM.

For mobile derived credentials issued through an MDM, when this option is set, if the device is already issued to the target user, it is automatically canceled and then the new device issued. Existing signing certificates are revoked, but existing archived certificates are not revoked. If the device is issued to a different user, the collection fails.

Note: The credential profile used for the existing issuance does not affect this behavior; existing credentials are overwritten only if the credential profile for the new credential has the **Issue over Existing Credential** option set.

- Mobile identity documents.

For mobile identity documents, when this option is set, if the credential profile being issued is the same as previously-issued mobile identity document, the previous document is canceled, and a new document is issued. This does not affect the previous document on the mobile device.

11.3.2.7 Authentication methods

The **Require Fingerprints at Issuance** and **Activation Authentication** options allow you to specify how the cardholder authenticates their identity to issue or activate.

Scenario	Require Fingerprints at Issuance	Activation Authentication
No authentication at issuance or activation	Never Required	None
Biometric authentication at issuance or activation	Always Required	None
Biometric authentication at issuance or activation	N/A	Biometric
Code authentication at activation	Never Required	Authentication Code
Biometric authentication at issuance, and biometric authentication and code authentication at activation	Always Required	Authentication Code

Note: You cannot use authentication codes for face-to-face issuance.

11.3.2.8 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:

- **Require Fingerprints at Issuance** – you are recommended to leave this set to **System Default**.
 - **Activation Authentication** – allows you to specify biometric authentication or authentication codes for activation.
 - **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 **Activation 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 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.
 4. Request a card for the applicant, specifying the credential profile that has the activation authentication options.
 5. Collect the card for the applicant.
 - If the **Activation Authentication** option was set to **Authentication Code (Automatic)**, an email that contains an authentication code is sent to the applicant.
 - If the **Activation Authentication** option was set to **Authentication Code (Manual)**, you must request an authentication code using the **Request Auth Code** or **Card Ready Notification** workflow. You can also request an authentication code for card activation using the MyID Operator Client; see the *Sending an authentication code to activate a device* section in the [MyID Operator Client](#) guide for details.

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.

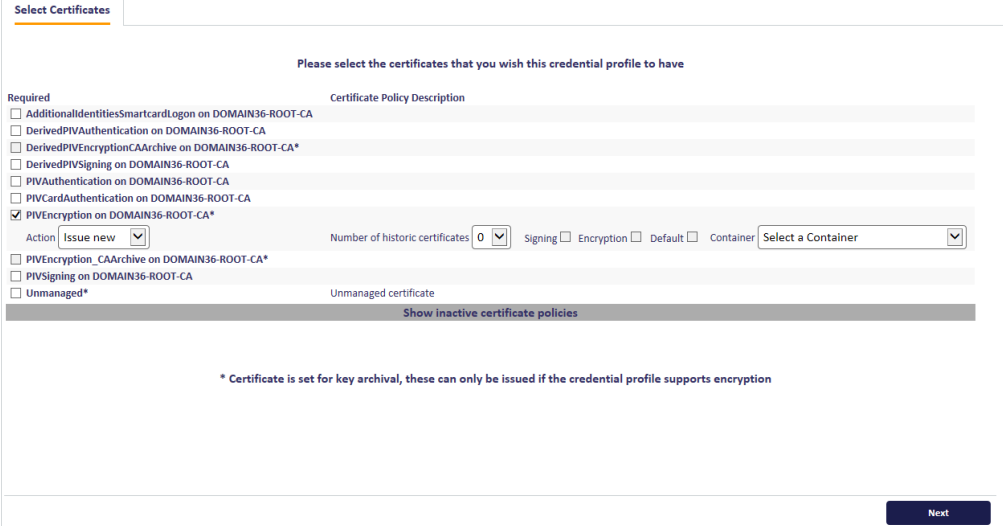
This page lists all of the available certificate policies you can issue to a credential.

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. Note, however, that PIV cards cannot use these generic keys, so you must select a certificate.

- **Encryption** – if you selected **MyIDEncryption** 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. Note, however, that PIV cards cannot use these generic keys, so you must select 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

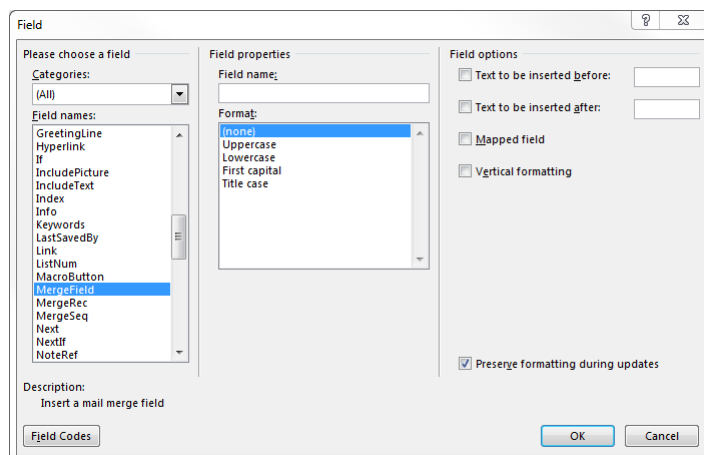
Note: This section refers only to mail merge documents as used by the **Print Mailing Document** workflow and when credentials are enabled. The **Collect Card** workflow uses a new system of mailing document templates that does not use Microsoft Word. For more details, contact customer support, quoting 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 for Office 365; 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, in the **Text** grouping, select the **Quick Parts** menu .
 - 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.
See section [11.4.1, Available fields](#) for a list of the fields you can use.
5. Click **OK**.
6. Save your document in the Word 97-2003.doc format.

Important: Do not save the document in .docx format.

Once you have saved the document on each client machine, you can set the location of the file in the credential profile using the **Select Card Issuance Mailing Document** or **Select Enable Card Mailing Document** options; see section [11.3.1.8, Mail Documents](#) for details. You must save the document in the same location on each client machine.

11.4.1 Available fields

You can use the following fields in your mail merge:

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.

Field name	Description
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 (x_u , x_d , and x_g fields) that may have been added to your installation.

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 issue a soft certificate through the MyID Operator Client, the certificate policy must also have the **Private Key Exportable** option set.

Once you have created your credential profile, you can request, issue, and manage soft certificate packages in the following ways:

- Using MyID Desktop.

MyID Desktop allows you to request, validate, collect, cancel, disable, and renew soft certificates.

See the *Issuing soft certificates using a credential profile* section in the [Operator's Guide](#) for details.

- Using the MyID Operator Client.

The MyID Operator Client allows you to request, validate, collect, cancel, disable, renew, and print transport and mailing documents for soft certificates.

See the *Working with soft certificates* section in the [MyID Operator Client](#) guide for details.

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.

If you want to send PIN mailing documents, you must set the **Issue With** option to **Server Generated PIN**, then set the **PIN Algorithm** to either **EdeficePinGenerator** or **EdeficePolicyPinGenerator**. You cannot use user-specified PINs or the **RandomPinGenerator**; the PIN will be blank in the mailing document, as MyID must be able to regenerate the PIN when creating the mailing document, and this is not possible with the **RandomPinGenerator** or if the user typed their own PIN.

See section 9, *PIN generation* for details of configuring your system to use the **EdeficePinGenerator** or **EdeficePolicyPinGenerator** algorithms.

If you want to email the PIN to the user, select the **Email PIN** option and configure MyID to send email notifications; these notifications use the **Card PIN Notification** email template. See section 13, *Email notification* for more information.

Important: If you use a server generated PIN, you must either configure an email notification, or configure a PIN mailing document that you can print and provide to the user. The PFX password is not displayed on screen.

7. Click **Mail Documents** to specify the document sent to the user when the certificate is issued, if required.

You can print mailing documents for soft certificate packages only through the MyID Operator Client. You cannot use the **Print Mailing Document** workflow. See the *Printing mailing documents for soft certificates* section in the *MyID Operator Client* guide for details.

Set the following options:

- **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 the soft certificate package.
- **Select Transport Document** – select the name of the HTML template stored in the MyID database to be used when collecting the soft certificate package. For example, you can create a document that provides the person's name and address to provide a cover letter if you are sending a soft certificate package to the user on a USB stick.

For details of creating HTML templates, contact customer support, quoting reference SUP-255.

8. Click **Next**.
9. From the list of available soft certificates, select the certificates you want to issue.

Note: If you select a certificate policy that is marked for archival, you can recover the certificates after they have been issued. See *Recovering certificates* section in the *Operator's Guide* for details.

10. From the **Storage Method** list, select where you want the certificate to be stored:

- **FileStore** – 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-zA-Z 0-9 ! \ " # \$ % ' () * + - . / : ; = ? @

Note: You cannot use spaces.

If you set the **Issue With** option to **Server Generated PIN**, and set the **PIN Algorithm** to either **EdeficePinGenerator** or **EdeficePolicyPinGenerator**, the PFX file is created with an automatically-generated password

- **SystemStore** – the certificate is stored automatically in the Personal certificate store of the logged-on Windows user.
- **AutoSave** – when collecting the request through the MyID Operator Client, the certificate package is automatically saved to the first empty USB device found attached to the PC. If you use the **Collect My Certificates** workflow in MyID Desktop to collect the request, however, the certificates are saved to the Personal certificate store of the logged-on Windows user, as for the **SystemStore** option.

When saving PFX files from the MyID Operator Client, the file names are automatically generated; you can customize the format if necessary. See the *Customizing certificate file names* section in the [MyID Operator Client](#) guide for details.

Note: You can select multiple certificate profiles, and choose a different **Storage Method** for each one. MyID allows you to collect the certificates at the same time.

11. Click **Next**.
12. 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.
13. Click **Next**.

11.5.1 Upgraded credential profiles

Previous versions of MyID had the following options for **Storage Method** for certificate policies for soft certificates:

- **Local Store** – equivalent to **SystemStore**.
- **Password Protected PFX File** – equivalent to **FileStore**.
- **Choose During Issuance** – no longer supported. Certificate policies that were marked as **Choose During Issuance** are treated as **FileStore** when you attempt to collect them in the MyID Operator Client, and are updated to specify **FileStore** when you modify the credential profile.

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, Self-Service App, Self-Service Kiosk	HTML template
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 My Card	Self-Service App	HTML template

11.6.1 Client requirements for HTML templates

Use of HTML template-based terms and conditions for activation in MyID Desktop, the Self-Service App, or the Self-Service Kiosk requires the installation of the Microsoft WebView2 Runtime on the client PC. See the *Microsoft WebView2 Runtime* section in the [Installation and Configuration Guide](#).

In addition, the use of HTML template-based terms and conditions for activation in the Self-Service App and the Self-Service Kiosk requires the clients provided with MyID 12.6 or later.

11.6.2 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) and for terms and conditions documents displayed in the Self-Service App or the Self-Service Kiosk, you must set up an HTML template in the MyID database.

For information on using the provided utility to add HTML templates, see the [MyID Document Uploader](#) guide.

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.

11.6.3 Customizing terms and conditions for the web service

If you are using the Self-Service App, but have not updated to a version of the client software as provided with MyID 12.6 or later, the Self-Service App does not use the HTML templates, but instead uses a text file stored in the `Content` folder of the MyIDProcessDriver 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.

11.6.4 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\Intercede\MyID\Web\WebENT\us\res\custom\js
```

and:

```
C:\Program Files\Intercede\MyID\Web\WebENT\en\res\custom\js
```

This allows you to use different terms and conditions for different languages.

In the `SignedTCs.txt` text file, include the text that you want to display for terms and conditions. You can use HTML formatting and must make sure that the characters you use are safe to display within a web page; for example, you must specify ampersands as `&` and not as bare `&` symbols.

For example:

```
<p><strong>Terms &amp; Conditions</strong></p>
<p>You must agree to the following conditions:</p>
<ol>
<li>The card remains the property of Example Corporation.</li>
<li>Use of this card may be revoked at the sole discretion of Example Corporation for violation of Example Corporation's policies and procedures.</li>
<li>...</li>
</ol>
<p>If you do not accept these terms and conditions, click
<strong>Reject</strong>.</p>
```

11.6.5 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. If you want to include a line break, use `
` – other formatting codes that may be used in other translation strings may not be displayed correctly or may prevent the terms and conditions from being displayed.

For information about the MyID Translator tool, contact customer support quoting reference SUP-138.

11.6.6 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 during device activation as a binary object in the database. This is then visible in the MyID audit

report.

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

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.

11.6.7 Emailing terms and conditions

For terms and conditions that use the HTML template method, if you set the **Email Terms and Conditions** option (on the **Devices** tab of the **Operation Settings** workflow) to Yes, MyID sends an email containing the signed terms and conditions to the cardholder, assuming they have an email address in their record within MyID. This allows the cardholder to retain a copy of the terms and conditions to which they agreed.

The email template used is **Terms and conditions accepted**; you can change the text of the email message by using the **Email Templates** workflow. Note that editing this email template does not alter the content of the terms and conditions themselves. You can include the following substitution codes in the email template:

- `%date` – the date of signed document.
- `%statement` – the full text of the signed Terms and Conditions document.
- `%Person:vPeopleUserAccounts:LogonName` – the cardholder's logon name.
- `%Person:vPeopleUserAccounts:FullName` – the cardholder's name.
- `%Person:vPeopleUserAccounts:EmployeeID` – the cardholder's Employee ID.
- `%Device:vDevicesWithDeviceID:SerialNumber` – the device serial number.

Note: If you want to send email from MyID, you must set up an SMTP server within MyID – see the *Setting up email* section in the [Advanced Configuration Guide](#) for details.

11.7 Enforcing banned words in PINs

If you set the **Enforce Banned Words** option in the credential profile, MyID prevents cardholders from using banned words as part of their device PINs.

The banned words include dynamic words (for example, the device serial number, or the person's logon name) and a static word list (for example, `password` or `admin`).

This list of banned words is enforced when setting the PIN through MyID using the following operations:

Client	Operation
MyID Desktop	Assisted Activation
MyID Desktop	Batch Collect Card
MyID Desktop	Change PIN
MyID Desktop	Collect Card
MyID Desktop	Reset Card PIN
Self-Service App	Activate Card
Self-Service App	Change My PIN
Self-Service App	Collect My Card
Self-Service App	Reset My PIN
Self-Service Kiosk	Activate Card
Self-Service Kiosk	Change My PIN
Self-Service Kiosk	Collect My Card
Self-Service Kiosk	Reset My PIN

The cardholder can still change their PIN to include words from the banned list using other methods; for example, the Windows Change PIN feature, smart card middleware utilities, and legacy MyID workflows not listed in the table above, such as Issue Card, Reprovision Card, Reprovision My Card, and so on. You are recommended to prevent access to these features to avoid cardholders circumventing the rules.

The list of banned words is also ignored when using client or server generated PINs, and when issuing mobile or FIDO devices.

11.7.1 Dynamic word list

By default, when you set the **Enforce Banned Words** option in the credential profile, MyID prevents the cardholder from using the following values:

- From the person's user account:
 - `UserAccountID`
 - `LogonName`
 - `EmployeeID`
 - `FirstName`
 - `LastName`
- From the device information:
 - `DeviceID`
 - `HIDSerialNumber`
 - `SerialNumber`

These are controlled by the following views in the MyID database:

- `vBannedUser` – contains the user attributes you want to ban.
- `vBannedDevice` – contains the device attributes you want to ban.

These views are configured by MyID Project Designer. If you edit them directly, when you upgrade MyID, your changes are overwritten, as these views are created on installation or upgrade, so this is not recommended. Contact your account manager for advice on using MyID Project Designer to amend and maintain these views.

11.7.2 Static word list

The word list is stored on the MyID web services server in the `PinPolicyBannedWordList.txt` file; by default, this file is installed to the following location:

`C:\Program Files\Intercede\MyID\SSP\MyIDProcessDriver\Content\`

You can edit the contents of this text file to add or remove words that you want to prevent people from incorporating in their PINs.

Note: If you have multiple web services servers, make sure you synchronize the contents of this file on each server.

By default, the file contains the following words:

```
password
1234
5678
admin
administrator
```

You are recommended to publish your list of banned words to your cardholders.

Note: The word list file is created on installation or upgrade. You must take a backup of this file before upgrading MyID and restore it once the upgrade is complete.

11.7.3 Cache the word list

If you add a large number of words to this file, you may want to configure MyID to cache the word list on the client. To do so, add the following to the `myid.config` file:

```
<add key="CacheBannedWordsList" value="true"/>
```

By default, the `myid.config` file is in the following location:

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

Note: MyID clients provided with version 12.5 onwards support the banned words feature, but MyID clients provided with 12.6 onwards support caching the word list.

12 License management

MyID is installed with a standard trial license that allows you to add up to 250 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 USB 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 in MyID Desktop when you add people to the system. The warning message is displayed to the operator when the number of remaining available user accounts drops to the warning limit.

You can also configure MyID to send email messages 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 drops to the warning limit, as specified by the **Warn When Available Licenses Reaches** value.

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 configure MyID to hide this message from users who do not have access to the **Licensing** workflow; set the **Show License Info to All Operators** configuration option on the **Notifications** page of the **Operation Settings** workflow to **No**.

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.
See section [12.1, View current license status](#).
- Generate requests for additional licenses.
See section [12.2, Requesting licenses](#).
- Install received licenses.
See section [12.3, Installing license details](#).
- Change the warning threshold and the email address for notifications.
See section [12.4, Updating warning messages](#).
- Setting maximum device numbers and end dates for individual groups.
See section [12.5, Controlling device assignments for groups](#).

12.1 View current license status

From the **Configuration** category, select the **Licensing** workflow to view current license status.

You can also launch this workflow from the **Configuration Settings** section of the **More** category in the MyID Operator Client. See the *Using Configuration Settings workflows* section in the [MyID Operator Client](#) guide for details.

- **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.
- **Warn When Available Licenses Reaches** is the number of remaining available 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.

Note: You must configure MyID to send email notifications; see the *Setting up email* section in the [Advanced Configuration Guide](#) for details.

- **Expiry Date** is the date your current license expires.
- **Type** is the type of license; for example, Issued or Evaluation.

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.

You can also launch this workflow from the **Configuration Settings** section of the **More** category in the MyID Operator Client. See the *Using Configuration Settings workflows* section in the [MyID Operator Client](#) guide for details.

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.

You can also launch this workflow from the **Configuration Settings** section of the **More** category in the MyID Operator Client. See the *Using Configuration Settings workflows* section in the [MyID Operator Client](#) guide for details.

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 **Warn When Available Licenses Reaches** value is set to 10% 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.

Note: You must configure MyID to send email notifications; see the *Setting up email* section in the [Advanced Configuration Guide](#) for details.

1. From the **Configuration** category, select the **Licensing** workflow.

You can also launch this workflow from the **Configuration Settings** section of the **More** category in the MyID Operator Client. See the *Using Configuration Settings workflows* section in the [MyID Operator Client](#) guide for details.

2. Click **Update Warning**.
3. Enter the number of remaining available user accounts or issued credentials that will trigger the warning in **Warn When Available Licenses Reaches** – the message is sent when the number of remaining available user licenses or credential licenses drops to this value.
4. Enter or change the **Warning Email Address** if necessary.
5. Click **Update**.

12.5 Controlling device assignments for groups

You may want to control the use of devices for individual groups; for example, you may have multiple subsidiary organizations using your MyID system, all of whom use the same license pool, but you may want to restrict one of the organizations to have a maximum number of devices, and to be able to assign and issue those devices for a limited time.

This feature helps control device assignments for individual group, but it does not override or modify how MyID system licenses are consumed, which are calculated for the entire installation.

To do this, you can create a new group to which you assign all users from that organization, or use an existing group that contains all users from that organization. Create or amend the group using the **Add Group** or **Amend Group** workflows, and set the following options:

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

You can also set these options through the MyID Core API by setting the `deviceLimit` and `expiryDate` options when adding or editing a group.

You can use the **Assigned Devices by Group** report in the MyID Operator Client to help monitor these limits. This report lists each group that has devices assigned or issued to it, and displays the limits you have set on the group. See the *Assigned Devices by Group report* section in the [MyID Operator Client](#) guide.

12.5.1 Limitations

This section contains information on limitations of this feature.

12.5.1.1 Error messages

Some legacy operations in MyID may display non-specific errors when these limits are triggered. For example, the following workflows fail with errors similar to:

```
MyID is not configured to issue this card. Contact your administrator to
check your system configuration.
```

- **Issue Card**
- **Collect My Card**
- **Request Device (Assign)**
- **Reinstate Card**

Error details capture in the MyID system events may include information stating that the target user's group has expired, or has exceeded the maximum number of devices.

In addition, assigning devices using Lifecycle API is not affected by the **Device Assignment End Date** or the **Maximum Number of Assigned Devices** options.

12.5.1.2 Changing groups

It is possible to exceed the number of assigned devices for a group if you change the group of a person who already has a device issued; for example, if Group A has a limit of 10 devices, and already has 10 devices issued, if you issue a device to a person in Group B, then change that person to Group A, Group A has 11 devices assigned; however, no further devices can be issued to people already in Group A.

12.5.1.3 Inheriting limits

This feature does not automatically inherit or assign limits to groups – where a limit needs to be placed on each group, you must set the value accordingly. Groups that are created automatically will not have any limits set unless you add the values to each.

12.5.1.4 Lifecycle API

You cannot add or amend group limits using the Lifecycle API.

13 Email notification

You can configure MyID to send email messages to individuals automatically, 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 *Setting up email* section in the [Advanced Configuration Guide](#) for details.

13.1 System-wide email settings

This section contains information about the configuration options relating to email notifications.

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.

You can also launch this workflow from the **Connections and Notifications** section of the **More** category in the MyID Operator Client. See the *Using Connections and Notifications workflows* section in the [MyID Operator Client](#) guide for details.

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.

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; see section [13.2.1, Available variables for email messages](#).

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.

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 the template is used to send auth codes, activation codes, or unlock codes, an additional option is available. Select the **Complexity** you want to use for the codes included in messages generated using this template:

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

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

Note: This option is not available for templates used to send job collection codes. For job collection codes, the complexity is determined by the credential profile, or if the credential profile does not contain a complexity setting, by the **Auth Code Complexity** configuration option.

8. 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 *Setting up email* section in the [Advanced Configuration Guide](#) for details.

9. Click **Save**.

13.2.1 Available variables for email messages

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.

13.2.2 URL encoded links

You can include URL encoded links in email notifications.

If, for example, you have an email notification that includes an URL containing %20 for a space or %3D for an = sign, you must escape these codes using %_ after the % sign – for example, %%_20 for space.

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
Activation Code Email	Sent to a user who has an activation code ready for a device	210
Activation Code SMS	Sent to a user who has an activation code ready for a device	211
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 Email	Sent to a user, who has had an authentication code for logon requested on their behalf, via email	212
Authentication Code Notification	Authentication code notification	26
Authentication Code SMS	Sent to a user, who has had an authentication code for logon requested on their behalf, via SMS	213
Automatic Job Cancellation Email	Sent to the issue card request recipient when a issuance job is canceled because it has not been collected in time.	113
Cancel Card	Sent to a user when one of their devices is canceled	219
Cancel Card Notification	Sent to a user whose card has been canceled	5
Card PIN Notification	Sent to inform a user of their new PIN number	11
Certificate Authority Status	Certificate authority status	106
Certificate Authority Status Normal	Certificate authority status	159
Certificate lifetime constrained. Vetting date	Certificate lifetime constrained to vetting date	204
Certificate lifetime not issued. Vetting date	Certificate lifetime not issued as the vetting validity date has expired	205
Certificate Renewal Not Permitted. User Data Not Approved	Used to inform a person that they cannot renew their certificates because their User Data Approved flag is not set.	202
Certificate Renewal Not Permitted. Vetting Expired	Used to inform a person that they cannot renew their certificates because their vetting has expired.	203
Certificate Server Error	Sent when an error is encountered communicating with a certificate server	156
Certificate Server Recovered	Sent when MyID has recovered from a certificate server error	157
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

Template Name	Description	ID
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
Derived Credential Requested	Sent to a user who has been requested a derived credential	218
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
FIDO Authenticator Registration Code	Sent to the user when their FIDO Authenticator is ready for registration	207
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 Collection Auth Code Email	Sent to a user who has an authentication code ready for a device that is awaiting job collection	216
Job Collection Auth Code SMS	Sent to a user who has an authentication code ready for a device that is awaiting job collection	217
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
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

Template Name	Description	ID
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
Pairing Code Notification	Sent to inform a user of their new Pairing Code	158
QALockout	Sent to the user when their security questions are answered incorrectly too many times and their security phrases become locked	132
Register FIDO Authenticator	Sent to a user who has a FIDO Authenticator awaiting registration	206
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
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

Template Name	Description	ID
Reprovision Notification Mobile	Sent to the user when reprovision is ready for collection onto their mobile devices	144
Self Requested Authentication Code Email	Sent to the user when they request an Authentication Code for logon by email	208
Self Requested Authentication Code SMS	Sent to the user when they request an Authentication Code for logon by SMS	209
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
Software Certificate Renewal Notification	Sent to a user who has a pending software certificate renewal or replacement	160
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
Unlock Credential Code Email	Sent to a user, who has had a credential unlock code requested on their behalf, via email	214
Unlock Credential Code SMS	Sent to a user, who has had a credential unlock code requested on their behalf, via SMS	215
User Vetting Date Expired	Sent to the administrator when a user's identity check has expired.	201

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
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:

- 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**.

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

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.
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; see section [13.2.1, Available variables for email messages](#) for details.

For example, you can type a template body such as:

```
This is a message for %2. Your card of type %3 with the serial number
%5 has been cancelled.%nThe reason for the cancellation is: %5.
```

Which would become:

```
This is a message for John Smith. Your card of type Datakey Model 330
with the serial number 30366716 has been cancelled.
The reason for the cancellation is: The card was reported lost.
```

When you set up the email trigger, you will set up substitutions for these tokens. MyID can then pull information from the current workflow and insert it into the email message.

8. Set up the **Substitution Legend**.

Make sure you take a note of the tokens you have used and what they are going to represent. This information is required for any custom email triggers that are created to use this template.

Click **Add substitution**, then type the **Token** and **Description**. Click **Add substitution** again to add more tokens to the legend.

9. From the **Transport** drop-down list, select one of the following:

- **Email** – the template is to be used for email messages.
- **SMS** – the template is to be used for SMS messages.

10. If you want to sign the email message, select the **Signed** option.

Note: You must have the **Sign outgoing emails** option for the SMTP server in the **External Systems** workflow set. See the *Setting up email* section in the [Advanced Configuration Guide](#) for details.

11. Click **Save**.

13.4.1 Known issues

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

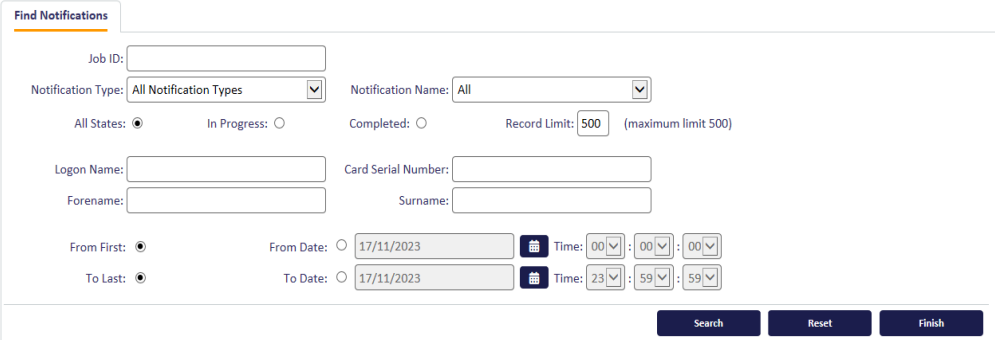
It is possible to create a new email template in MyID and save it using the same template name as an existing template. This prevents the notification from being sent.

13.5 Using the Notifications Management workflow

To view, resend, or cancel notifications:

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

You can also launch this workflow from the **Connections and Notifications** section of the **More** category in the MyID Operator Client. See the *Using Connections and Notifications workflows* section in the [MyID Operator Client](#) guide for details.



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.
 - **Rest Service** – returns notifications that are sent to a REST web service.

See section [14, REST web service notifications](#) for details of these notifications.
- **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.

Note: All dates in the **Notifications Management** workflow are stored and displayed in UTC. No local time offsets are applied.

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:

- Select one or more notifications that are **In Progress**.

You cannot cancel notifications that have completed.

- Click **Cancel Notify**

6. To resend notifications:

- Select one or more notifications.


- 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 REST web service notifications

You can configure MyID to send a notification to a REST web service for lifecycle events. For example, you can update a physical access control system (PACS) to enable or disable access for a particular card when it is issued or managed in MyID, or inform connected systems such as a workflow automation platform, endpoint management solution, or stock control system when credentials have been issued to a person.

MyID provides standard notifications for:

- Issuing, canceling, enabling, and disabling devices.
- Adding, editing, enabling, disabling, and deleting people.
- Adding and updating Issue Card requests.

To implement each of these notifications, you must set up an external system within MyID that provides details of your REST web service, including authentication details, and a mapping file that describes the format of the payload that you want to send to the web service endpoint. See section [14.1, *Configuring an external system for REST notifications*](#).

MyID provides sample mapping files for each of the standard notifications. You can write your REST web service to consume the payload provided by these notifications, or use the provided mapping files as a basis for your own requirements. See section [14.2, *Standard REST notifications*](#) for details of the data provided by the standard notifications.

For information on creating your own mapping files, see section [14.3, *Creating a mapping file*](#).

You can manage REST web service notifications using the **Notifications Management** workflow; see section [13.5, *Using the Notifications Management workflow*](#) for details. From the **Notification Type** drop-down list, select **Rest Service** to search for notifications sent to REST web services.

14.1 Configuring an external system for REST notifications

To enable a REST notification, you must create a connection to your REST web service using the **External Systems** workflow.

To create an external system:

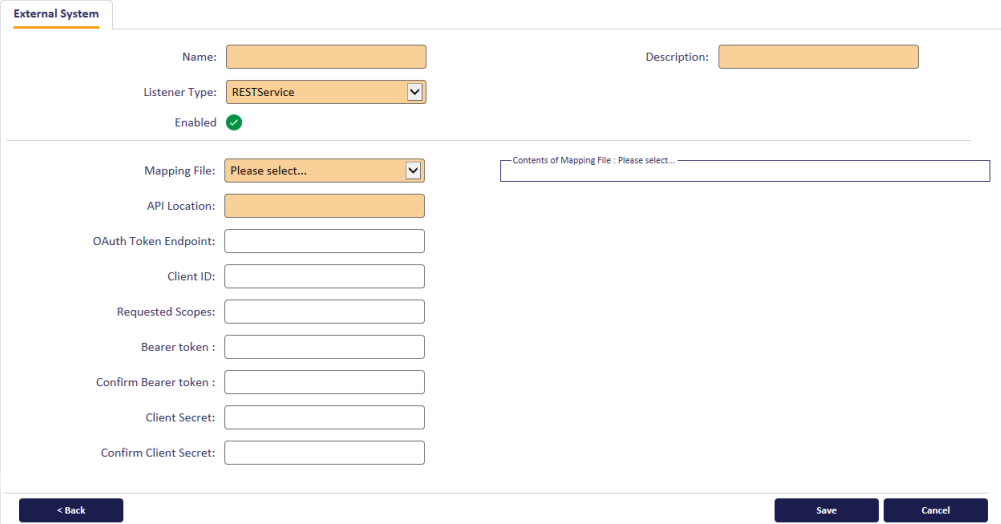
1. From the **Configuration** category, select **External Systems**.

You can also launch this workflow from the **Connections and Notifications** section of the **More** category in the MyID Operator Client. See the *Using Connections and Notifications workflows* section in the [MyID Operator Client](#) guide for details.

2. Click **New**.

3. From the **Listener Type** drop-down list, select **RESTService**.

The details for a REST notification external system appear.



The screenshot shows a web form titled "External System". At the top, there's a tab labeled "External System". Below the tab, there are several input fields and a dropdown menu. The "Name" field is empty. The "Description" field is empty. The "Listener Type" dropdown menu is set to "RESTService". The "Enabled" checkbox is checked, indicated by a green checkmark. Below these, there's a "Mapping File" dropdown menu set to "Please select...". To the right of this dropdown is a text area labeled "Contents of Mapping File : Please select...". Below the "Mapping File" dropdown is the "API Location" field. Below that are several other fields: "OAuth Token Endpoint", "Client ID", "Requested Scopes", "Bearer token", "Confirm Bearer token", "Client Secret", and "Confirm Client Secret". At the bottom of the form, there are three buttons: "< Back", "Save", and "Cancel".

4. Complete the following details:

- **Name** – Type the name of the notification you want to configure.

Important: This must match the notification generated by MyID for the device lifecycle event. By default, you can provide one of the following values:

- REST Device Issued
- REST Device Cancelled
- EnableCard
- DisableCard
- REST Person Disabled
- REST Person Enabled
- REST Person Edited
- REST Person Added
- REST Person Deleted
- REST Job Added
- REST Job Updated

These values are case sensitive. See section [14.2, Standard REST notifications](#) for details of these notifications.

- **Description** – Type a description for the external system.
- **Enabled** – Select this option to enable the notification, or deselect it to disable the notification. When the notification is disabled, MyID does not attempt to send this notification to the external system.
- **Mapping File** – Select the mapping file you want to use from the drop-down list.

Mapping files are stored on the MyID application server in the following folder by default:

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

For details of the provided standard mapping files, see section [14.2, Standard REST notifications](#).

For details of creating your own mapping file, see section [14.3, Creating a mapping file](#).

Once you have selected the mapping file, its contents appear on screen.

- **API Location** – Type the base URL of your REST web service API.

The endpoint for the notification is generated by taking this API location and appending the endpoint URL specified by the mapping file; for example, if your API Location is:

```
https://myserver.example.com/Notify
```

and the mapping file specifies:

```
<Endpoint Verb="POST" URL="/devices/deviceIssued" />
```

MyID sends a POST notification to:

```
https://myserver.example.com/Notify/devices/deviceIssued
```

5. Provide the authentication details for your web service.

You can either provide a pre-requested bearer token, or use an OAuth2 provider to request a bearer token.

To use a pre-requested bearer token, provide the following information:

- **Bearer token** – Type the bearer token you want to use.
- **Confirm Bearer token** – Type the bearer token again to confirm it.

Note: MyID does not validate the bearer token before using it to send the notification. You must ensure that the token is valid.

Alternatively, to use an OAuth2 provider to request a bearer token, provide the following information:

- **OAuth Token Endpoint** – Type the URL of the web service token provider.
- **Client ID** – Type the client ID that has been registered with the OAuth2 token provider.
- **Requested Scopes** – Optionally, provide the scopes you want for the requested token. If you do not provide any scopes, the default scope configured for the token provider is used.
- **Client Secret** – Type the shared secret you have configured for the token provider.
- **Confirm Client Secret** – Type the shared secret again to confirm it.

Note: The token is issued with the default validity period for the bearer token scope; you cannot specify a validity period. MyID caches the provided token and requests a new one once the token's validity period has expired.

6. Click **Save**.

14.1.1 Enabling and disabling a notification

To enable or disable a notification:

1. From the **Configuration** category, select **External Systems**.
2. From the Name drop-down list, select the external system you created for the notification you want to enable or disable.
3. Click **Edit**.
4. Set the **Enabled** option.

When the notification is disabled, MyID does not attempt to send this notification to the external system.

5. Click **Save**.

14.2 Standard REST notifications

By default, MyID provides the following standard REST notifications with corresponding mapping files:

Notification	Mapping file	Description
REST Device Issued	RESTDeviceIssued.xml	Sends a notification to a REST web service when a device is issued and has a status of Active. See section 14.2.1, REST Device Issued notification .
REST Device Cancelled	RESTDeviceCancelled.xml	Sends a notification to a REST web service when a device is canceled and therefore removed from association with any people. See section 14.2.2, REST Device Cancelled notification .
EnableCard	EnableCard.xml	Sends a notification to a REST web service when a device is enabled in MyID. See section 14.2.3, EnableCard notification .
DisableCard	DisableCard.xml	Sends a notification to a REST web service when a device is disabled in MyID. See section 14.2.4, DisableCard notification .
REST Person Added	RESTPersonAdded.xml	Sends a notification to a REST web service when a person is added to MyID. See section 14.2.5, REST Person Added notification .
REST Person Edited	RESTPersonEdited.xml	Sends a notification to a REST web service when a person is edited in MyID. See section 14.2.6, REST Person Edited notification .
REST Person Enabled	RESTPersonEnabled.xml	Sends a notification to a REST web service when a person is enabled in MyID. See section 14.2.8, REST Person Enabled notification .

Notification	Mapping file	Description
REST Person Deleted	RESTPersonDeleted.xml	Sends a notification to a REST web service when a person is deleted from MyID. See section 14.2.7, REST Person Deleted notification .
REST Person Disabled	RESTPersonDisabled.xml	Sends a notification to a REST web service when a person is disabled in MyID. See section 14.2.9, REST Person Disabled notification .
REST Person Deleted	RESTPersonDeleted.xml	Sends a notification to a REST web service when a person is deleted from MyID. See section 14.2.7, REST Person Deleted notification .
REST Request Added	RESTRequestAdded.xml	Sends a notification to a REST web service when an Issue Card request is added in MyID. See section 14.2.10, REST Request Added notification .
REST Request Updated	RESTRequestUpdated.xml	Sends a notification to a REST web service when an Issue Card request is updated in MyID. See section 14.2.11, REST Request Updated notification .

You can create an external system for each of these REST notifications. Use the name of the notification as the name of the external system, and select the corresponding mapping file. See section [14.1, Configuring an external system for REST notifications](#).

14.2.1 REST Device Issued notification

The `REST Device Issued` event sends a notification to a REST web service when a device is issued and has a status of Active.

If you configure an external system with the name `REST Device Issued` and specify the corresponding mapping file `RESTDeviceIssued.xml`, you can configure MyID to respond to the event with the following.

14.2.1.1 Endpoint

POST `/devices/deviceIssued`

14.2.1.2 Data

```
{
  "person": {
    "id": "<person guid>",
    "group": {
      "id": "<group guid>",
      "name": "<group name>"
    },
    "name": {
      "first": "<first name>",
      "last": "<surname>"
    },
    "contact": {
      "emailAddress": "<email address>"
    },
    "employeeId": "<employee ID / security number>",
    "photo": "<base 64 encoded user image>",
    "logonName": "<logon name>"
  },
  "device": {
    "id": "<device guid>",
    "sn": "<device serial number>",
    "dt": "<MyID device type>",
    "validity": {
      "from": "<ISO format issuance date>",
      "to": "<ISO format expiration date>",
      "enabled": <true|false>
    },
    "hid": {
      "serialNumber": "<HID loop ID>",
      "facilityCode": "<HID facility code>"
    }
  }
}
```

14.2.1.3 Expected response

A 200 OK response in the event of success.

14.2.2 REST Device Cancelled notification

The `REST Device Cancelled` event sends a notification to a REST web service when a device is canceled and therefore removed from association with any people. This may be caused by a variety of operations; for example, canceling a device, erasing a device, or reaching a limit of devices per person, for example.

If you configure an external system with the name `REST Device Cancelled` and specify the corresponding mapping file `RESTDeviceCancelled.xml`, you can configure MyID to respond to the event with the following.

14.2.2.1 Endpoint

`POST /devices/{device GUID}/deviceCancelled`

14.2.2.2 Data

```
{
  "person": {
    "id": "<person guid>",
    "group": {
      "id": "<group guid>",
      "name": "<group name>"
    },
    "name": {
      "first": "<first name>",
      "last": "<surname>"
    },
    "contact": {
      "emailAddress": "<email address>"
    },
    "employeeId": "<employee ID / security number>",
    "logonName": "<logon name>"
  },
  "device": {
    "id": "<device guid>",
    "sn": "<device serial number>",
    "dt": "<MyID device type>",
    "hid": {
      "serialNumber": "<HID loop ID>",
      "facilityCode": "<HID facility code>"
    }
  }
}
```

14.2.2.3 Expected response

A `200 OK` response in the event of success.

14.2.3 EnableCard notification

The `EnableCard` event sends a notification to a REST web service when a device is enabled in MyID.

If you configure an external system with the name `EnableCard` and specify the corresponding mapping file `EnableCard.xml`, you can configure MyID to respond to the event with the following.

14.2.3.1 Endpoint

POST `/devices/{device GUID}/deviceEnabled`

14.2.3.2 Data

```
{
  "device": {
    "id": "<device guid>",
    "sn": "<device serial number>",
    "dt": "<MyID device type>",
    "validity": {
      "from": "<ISO format issuance date>",
      "to": "<ISO format expiration date>",
      "enabled": <true|false>
    },
    "hid": {
      "serialNumber": "<HID loop ID>",
      "facilityCode": "<HID facility code>"
    }
  },
  "person": {
    "logonName": "<logon name>"
  }
}
```

14.2.3.3 Expected response

A 200 OK response in the event of success.

14.2.4 DisableCard notification

The `DisableCard` event sends a notification to a REST web service when a device is disabled in MyID.

If you configure an external system with the name `DisableCard` and specify the corresponding mapping file `DisableCard.xml`, you can configure MyID to respond to the event with the following.

14.2.4.1 Endpoint

POST `/devices/{device GUID}/deviceDisabled`

14.2.4.2 Data

```
{
  "device": {
    "id": "<device guid>",
    "sn": "<device serial number>",
    "dt": "<MyID device type>",
    "validity": {
      "from": "<ISO format issuance date>",
      "to": "<ISO format expiration date>",
      "enabled": <true|false>
    },
    "hid": {
      "serialNumber": "<HID loop ID>",
      "facilityCode": "<HID facility code>"
    }
  },
  "person": {
    "logonName": "<logon name>"
  }
}
```

14.2.4.3 Expected response

A 200 OK response in the event of success.

14.2.5 REST Person Added notification

The `REST Person Added` event sends a notification to a REST web service when a person's account is added to MyID.

If you configure an external system with the name `REST Person Added` and specify the corresponding mapping file `RESTPersonAdded.xml`, you can configure MyID to respond to the event with the following.

14.2.5.1 Endpoint

PATCH `/people/{People.ObjectID}/personAdded`

14.2.5.2 Data

```
{
  "person": {
    "id": "<object ID of the person>",
    "account": {
      "dn": "<person Distinguished Name>",
      "domain": "<domain>",
      "samAccountName": "<SAM account name>",
      "upn": "<UPN>"
    },
    "contact": {
      "emailAddress": "<email>"
    },
    "employeeId": "<employee id>",
    "enabled": "<0|1>",
    "name": {
      "first": "<first name>",
      "fullName": "<full name>",
      "last": "<last name>"
    },
    "group": {
      "id": "<object ID of the group>",
      "name": "<group name>"
    },
    "logonName": "<logon name>"
  }
}
```

14.2.5.3 Expected response

A 200 OK response in the event of success.

14.2.6 REST Person Edited notification

The `REST Person Edited` event sends a notification to a REST web service when a person's account is edited in MyID.

If you configure an external system with the name `REST Person Edited` and specify the corresponding mapping file `RESTPersonEdited.xml`, you can configure MyID to respond to the event with the following.

14.2.6.1 Endpoint

PATCH `/people/{People.ObjectID}/personEdited`

14.2.6.2 Data

```
{
  "person": {
    "id": "<object ID of the person>",
    "account": {
      "dn": "<person Distinguished Name>",
      "domain": "<domain>",
      "samAccountName": "<SAM account name>",
      "upn": "<UPN>"
    },
    "contact": {
      "emailAddress": "<email>"
    },
    "employeeId": "<employee id>",
    "enabled": "<0|1>",
    "name": {
      "first": "<first name>",
      "fullName": "<full name>",
      "last": "<last name>"
    },
    "group": {
      "id": "<object ID of the group>",
      "name": "<group name>"
    },
    "logonName": "<logon name>"
  }
}
```

14.2.6.3 Expected response

A 200 OK response in the event of success.

14.2.7 REST Person Deleted notification

The `REST Person Deleted` event sends a notification to a REST web service when a person's account is deleted from MyID.

If you configure an external system with the name `REST Person Deleted` and specify the corresponding mapping file `RESTPersonDeleted.xml`, you can configure MyID to respond to the event with the following.

14.2.7.1 Endpoint

`DELETE /people/{People.ObjectID}/personDeleted`

14.2.7.2 Data

```
{
  "person": {
    "id": "<object ID of the person>",
    "account": {
      "dn": "<person Distinguished Name>",
      "domain": "<domain>",
      "samAccountName": "<SAM account name>",
      "upn": "<UPN>"
    },
    "contact": {
      "emailAddress": "<email>"
    },
    "enabled": "0",
    "name": {
      "first": "<first name>",
      "fullName": "<full name>",
      "last": "<last name>"
    },
    "group": {
      "id": "<object ID of the group>",
      "name": "<group name>"
    },
    "logonName": "<logon name>"
  }
}
```

14.2.7.3 Expected response

A 200 OK response in the event of success.

14.2.8 REST Person Enabled notification

The `REST Person Enabled` event sends a notification to a REST web service when a person's account is enabled in MyID.

If you configure an external system with the name `REST Person Enabled` and specify the corresponding mapping file `RESTPersonEnabled.xml`, you can configure MyID to respond to the event with the following.

14.2.8.1 Endpoint

POST `/people/{People.ObjectID}/personEnabled`

14.2.8.2 Data

```
{
  "person": {
    "id": "<object ID of the person>",
    "account": {
      "dn": "<person Distinguished Name>",
      "domain": "<domain>",
      "samAccountName": "<SAM account name>",
      "upn": "<UPN>"
    },
    "contact": {
      "emailAddress": "<email>"
    },
    "employeeId": "<employee id>",
    "enabled": "1",
    "name": {
      "first": "<first name>",
      "fullName": "<full name>",
      "last": "<last name>"
    },
    "group": {
      "id": "<object ID of the group>",
      "name": "<group name>"
    },
    "logonName": "<logon name>"
  }
}
```

14.2.8.3 Expected response

A 200 OK response in the event of success.

14.2.9 REST Person Disabled notification

The `REST Person Disabled` event sends a notification to a REST web service when a person's account is disabled in MyID.

If you configure an external system with the name `REST Person Disabled` and specify the corresponding mapping file `RESTPersonDisabled.xml`, you can configure MyID to respond to the event with the following.

14.2.9.1 Endpoint

POST `/people/{People.ObjectID}/personDisabled`

14.2.9.2 Data

```
{
  "person": {
    "id": "<object ID of the person>",
    "account": {
      "dn": "<person Distinguished Name>",
      "domain": "<domain>",
      "samAccountName": "<SAM account name>",
      "upn": "<UPN>"
    },
    "contact": {
      "emailAddress": "<email>"
    },
    "enabled": "0",
    "name": {
      "first": "<first name>",
      "fullName": "<full name>",
      "last": "<last name>"
    },
    "group": {
      "id": "<object ID of the group>",
      "name": "<group name>"
    },
    "logonName": "<logon name>"
  }
}
```

14.2.9.3 Expected response

A 200 OK response in the event of success.

14.2.10 REST Request Added notification

The `REST Request Added` event sends a notification to a REST web service when an Issue Card request is created in MyID.

This notification is triggered when the Issue Card request reaches a status of `Awaiting Issue`.

If you configure an external system with the name `REST Request Added` and specify the corresponding mapping file `RESTRequestAdded.xml`, you can configure MyID to respond to the event with the following.

14.2.10.1 Endpoint

POST `/requests/{Requests.ObjectID}/requestAdded`

14.2.10.2 Data

```
{
  "request": {
    "target": {
      "id": "<object ID of the target of the request>",
      "name": "<target name>",
      "logonName": "<target logon name>"
    },
    "task": {
      "desc": "IssueCard"
    },
    "id": "<object ID of the request>",
    "initiationDate": "<date the request was created>",
    "status": "<request status>",
    "credProfile": {
      "id": "<object ID of the credential profile>",
      "name": "<credential profile name>"
    }
  }
}
```

14.2.10.3 Expected response

A `200 OK` response in the event of success.

14.2.11 REST Request Updated notification

The `REST Request Updated` event sends a notification to a REST web service when an Issue Card request is updated in MyID.

This notification is triggered when the Issue Card request reaches one of the following statuses:

- Cancelled
- AutoDisabled
- Await Bureau
- Cancelled
- Completed
- Completed With Errors
- Created
- Failed
- In Progress
- In Transit
- Suspended

If you configure an external system with the name `REST Request Updated` and specify the corresponding mapping file `RESTRequestUpdated.xml`, you can configure MyID to respond to the event with the following.

14.2.11.1 Endpoint

`PATCH /request/{Requests.ObjectID}/requestUpdated`

14.2.11.2 Data

```
{
  "request": {
    "target": {
      "id": "<object ID of the target of the request>",
      "name": "<target name>",
      "logonName": "<target logon name>"
    },
    "task": {
      "desc": "IssueCard"
    },
    "id": "<object ID of the request>",
    "initiationDate": "<date the request was created>",
    "status": "<request status>",
    "credProfile": {
      "id": "<object ID of the credential profile>",
      "name": "<credential profile name>"
    }
  }
}
```

14.2.11.3 Expected response

A 200 OK response in the event of success.

14.3 Creating a mapping file

MyID provides example mapping files for the four standard notifications; see section [14.2, *Standard REST notifications*](#) for details of these files and their output.

You can use these files as a basis for your own files, or create your own files from scratch. Do not edit the content of the provided files, as they may be overwritten if you update or upgrade your system.

Mapping files are stored in the following folder by default:

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

Any XML file you place in this folder is available for selection from the **Mapping File** drop-down list in the **External Systems** workflow.

14.3.1 Notification

The `<Notification>` node is the root node of the XML file. Each mapping file has one and only one `<Notification>` node, which contains the `<DataSources>`, `<Endpoint>`, and `<Body>` nodes.

14.3.2 DataSources

The `<DataSources>` node contains one or more `<DataSource>` nodes, each of which specifies the name of a table or view in the MyID database. You must specify which field in the table or view you are matching against the device, person, or job ID for the notification. You can also specify an optional WHERE clause to restrict the data further; MyID does not support multiple records in a notification, so if the data source and where clause result in multiple records, the first record is used.

Each `<DataSource>` node has the following format:

```
<DataSource ID="id" View="view or table name" Lookup="identifier" FieldName="field" />
```

where:

- **ID** – a unique identifier for the data source. You use this to identify the data you want to use in the endpoint and body.
- **View** – the name of the view or table in the MyID database that contains the data you want to use.
- **Lookup** – the identifier used to look up the appropriate record in the table or view. You can use the following values:
 - **DeviceID** – the ID of the device that is the subject of the notification.
 - **PersonID** – the ID of the person who is the subject of the notification.
 - **JobID** – the ID of the job of the operation that is being carried out.
- **FieldName** – optionally, if it is not the same as the **Lookup** value, the name of the field in the view or table to compare against the identifier.

For example:

```
<DataSources>
  <DataSource ID="People" View="vPeopleUserAccounts" Lookup="PersonID" />
  <DataSource ID="Devices" View="vDevices" Lookup="DeviceID" />
</DataSources>
```

This creates two data sources:

- A data source called `People` that contains the data from the `vPeopleUserAccounts` view in the MyID database. The ID of the person who is the subject of the notification is used to match against the `PersonID` in the view.
- A data source called `Devices` that contains the data from the `vDevices` view in the MyID database. The ID of the device that is the subject of the notification is used to match against the `DeviceID` field in the view.

You can now access any field in the `vPeopleUserAccounts` view for the person, or the `vDevices` view for that device; for example, to include the device GUID in the endpoint:

```
<Endpoint Verb="POST" URL="/devices/{Devices.ObjectID}/deviceCancelled" />
```

or, to include the person's email address in the body payload:

```
<Source Field="Email" Retrieval="People" />
```


14.3.2.1 Where clauses

Optionally, you can add one or more `<Where>` nodes inside the `<DataSource>` node. This node has the following format:

```
<Where FieldName="fieldname" FieldValue="fieldvalue" Operation="operation" Conjunction="
[and|or]" />
```

where:

- `FieldName` – the name of a field in the view or table.
- `FieldValue` – the value to compare against the content of this field.
- `Operation` – the comparison operation. You can use the following:

<code>=</code>	equal to – the default when a single field value is specified
<code>!=</code>	not equal to
<code>lt</code>	less than
<code>le</code>	less than or equal to
<code>gt</code>	greater than
<code>ge</code>	greater than or equal to
<code>like</code>	like
<code>isnull</code>	value is null
<code>notnull</code>	value is not null
<code>IN</code>	value is one of the listed values – the default when multiple values are specified
- `Conjunction` – optionally, the conjunction where you have multiple `<where>` nodes. You can use the following:

<code>and</code>
<code>or</code>

For example:

```
<DataSource ID="PivAuthCert" View="vCertInstances" Lookup="DeviceID">
  <Where>
    <FieldName>ContainerName</FieldName>
    <FieldValue>5FC105</FieldValue>
    <Operation>=</Operation>
  </Where>
</DataSource>
```

This returns the details from the `vCertInstances` view for the device that is the subject of the notification; as there are multiple certificates for a single device, the `<where>` node restricts the returned data to the certificate where the container name matches the name for the PIV Authentication certificate.

14.3.3 Endpoint

The `<Endpoint>` node specifies the REST web service endpoint to which MyID sends the notification. The format is:

```
<Endpoint Verb="verb" URL="url"/>
```

where:

- **Verb** – the HTTP verb used to call the REST web service. You can use the following:
 - POST (this is the default)
 - PUT
 - DELETE
 - PATCH
- **URL** – the endpoint on the server.

The URL to which MyID sends the notification is constructed from the **API Location** field in the external system (see section [14.1, *Configuring an external system for REST notifications*](#)) and the URL you provide in the mapping file.

You can include substitutions from your data sources in this endpoint; for example, you may want to include the device GUID. Use the following format:

```
{DataSource.FieldName}
```

For example:

```
{Devices.ObjectID}
```

For example:

```
<Endpoint Verb="POST" URL="/devices/{Devices.ObjectID}/deviceCancelled" />
```

If the **API Location** field in the external system is:

```
https://myserver/Notify
```

and the device GUID (as obtained from the `ObjectID` field in the `Devices` data source, which refers to the `vDevices` view in the database) is:

```
79036d80-8322-404f-b146-f37af6b016b4
```

then MyID sends a POST request to:

```
https://myserver/Notify/devices/79036d80-8322-404f-b146-f37af6b016b4/deviceCancelled
```

14.3.4 Body

The `<Body>` node specifies the data that is sent to the REST web service.

Within the `<Body>` node, you can include one or more `<Property>` nodes. Each `<Property>` node has a `JPath` attribute that specifies the location in the JSON output where the value is to be included, and a `<Source>` node that specifies the data to include in the JSON output for the specified `JPath`.

The format is:

```
<Property JPath="path">
  <Source
    Retrieval="datasource"
    Field="fieldname"
    EncodingFormat="format"
    DataType="type"
    Default="staticvalue" />
</Property>
```

where:

- `JPath` – the path in the JSON output to create.
For example, `device.id` creates a top-level element called `device` and within that an element called `id`.
- `Retrieval` – the name of the data source from which you want to obtain the data.
- `Field` – the name of the field in the data source you want to include.
- `EncodingFormat` – if you are retrieving Boolean or date information from the database, specify one of the following:
 - `Boolean` – the value is output as `true` or `false`.
 - `Date` – the value is output in ISO8601 date time format: `yyyy-MM-ddTHH:mm:ss.000Z`
- `DataType` – if you are retrieving image, base64, or GUID data from the database, specify one of the following:
 - `Image` – the image is stored as binary object data in the database.
Note: You cannot access image data when the data is stored as a file; you can access only image data that is stored as binary object data in the database.
 - `HexedB64Certificate` – the retrieved data is in hexed base64 format. The data is converted to base64 format and any carriage return or line feed characters are removed before they are written to the JSON body.
 - `Guid` – when retrieving a GUID from the database (for example, the `ObjectID` for a device) it is enclosed in braces `{ }` – you cannot include these in a JSON file. Specify a `DataType` of `Guid` to strip the braces from the GUID before writing it to the JSON body.

- **Default** – a static value to use if the retrieval from the database does not produce a value. Alternatively, you can use the `Default` attribute instead of the `Retrieval` and `Field` attributes to provide a static value.

If you do not provide a `Default` value, and the retrieval from the database does not produce a value, the path specified in the `JPath` is not included in the JSON output.

For example:

```
<Property JPath="device.validity.enabled">
  <Source EncodingFormat="Boolean" Field="Enabled" Retrieval="Devices" />
</Property>
```

This obtains the value for `Enabled` field in the `Devices` data source, which refers to the `vDevices` view in the database; this value is 0 or 1 in the database, but the `EncodingFormat` tells MyID to output it as `true` or `false` to the appropriate place in the JSON output; for example:

```
{
  "device": {
    "validity": {
      "enabled": true
    },
  }
}
```

14.3.4.1 Additional processing

Optionally, you can add a `<Processor>` node inside the `<Source>` node to carry out additional processing on the value obtained from the database. This node has the following format:

```
<Processor Type="type" P1="Param1" P2="Param2" />
```

where:

- **Type** – currently, this must be:
 - `substring` – obtains a part of the string value.
- **P1** – the first parameter. For `substring`, this is the start location (based on zero-based indexing).
- **P2** – the second parameter. For `substring`, this is the number of characters. If you do not specify a number of characters, the value returned is from the start location to the end of the string.

For example:

```
<Property JPath="device.fascn">
  <Source Field="SN3" Retrieval="Devices">
    <Processor Type="substring" P1="14" P2="6"/>
  </Source>
</Property>
```

This obtains the value for the `SN3` field in the `Devices` data source, which refers to the `vDevices` view in the database, then obtains a 6-character section of this value starting at position 14 (based on zero-based indexing).

If the `SN3` value is:

0011 - 0000 - 250018 - 1 - 1 - 0000000001 1 1234 4 - 28

the output is:

```
{
  "device": {
    "fascn": "250018"
  },
}
```

14.4 Troubleshooting REST notifications

Notifications are sent outside the main workflow process; this means that a failure to send a notification does not result in a workflow failure, is not audited, and does not appear in the system events.

If a notification cannot be sent, the notification remains in progress and MyID will retry on the following default schedule:

- After 10 minutes.
- After 30 minutes.
- After 60 minutes.
- After 4 hours.
- After 12 hours.
- After 24 hours.

If the notification has not been sent after this time, MyID stops attempting to send it.

You can view the status of the notification in the **Notifications Management** workflow; see section [13.5, Using the Notifications Management workflow](#) for details.

To view the reason for a failure to send a notification, you can check the `ServerResponse` field in the `NotificationsInProgress` table in the MyID database.

You can also configure logging for the Notifications.Net component; see the [Log4Net](#) section of the [Configuring Logging](#) guide for details.

15 Changing list entries

The **List Editor** is used to change the contents of drop-down lists associated with custom attributes within MyID. Custom attributes are fields that have been added to the standard application, either by your organization or by Intercede on your behalf. If any of these new fields are associated with drop-down lists, you can change their contents using this workflow.

You can use the **List Editor** to change the list of document types used as Identity Documents to authenticate users during **Assisted Activation**, **Reset Card PIN**, or **Unlock Credential**; the lists of available documents for these operations are determined by the **Authenticate Person Document1** and **Authenticate Person Document2** lists.

You can also change the list of document types used in the **Authenticate Person** workflow; the lists of available documents for this operation are determined by the **Primary Identification Document** and **Secondary Identification Document** lists.

Note: The information you enter into these lists is not translated.

1. From the **Configuration** category, select the **List Editor** workflow.

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

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 consider carefully how your changes will affect the consistency of your data.

16 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, *Managing GlobalPlatform keys* for details.

16.1 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 work with other systems, including HSMs.

Further details on the use of GenMaster to generate secret keys are provided in the *Using GenMaster* section of the *Installation and Configuration Guide*.

16.2 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*.

Some keys are used for specific device types:

- For information about initialization keys, see the *Initialization keys for eToken 51xx* section in the *Smart Card Integration Guide*.
- For information about PIV PUK and Configuration Lock Code keys for YubiKey devices, see the *Setting up the PIV PUK key* and *Setting up the Configuration Lock Code* sections in the *Smart Card Integration Guide*.

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 www.nist.gov.

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.

16.2.1 Transport keys

To add a transport key (also known as a zone master key):

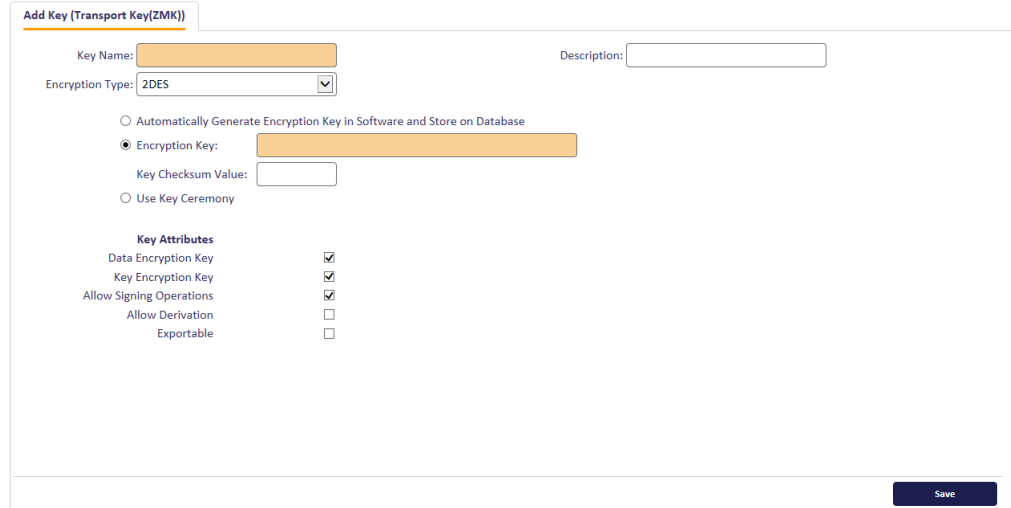
1. From the **Configuration** category, select **Key Manager**.

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

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.

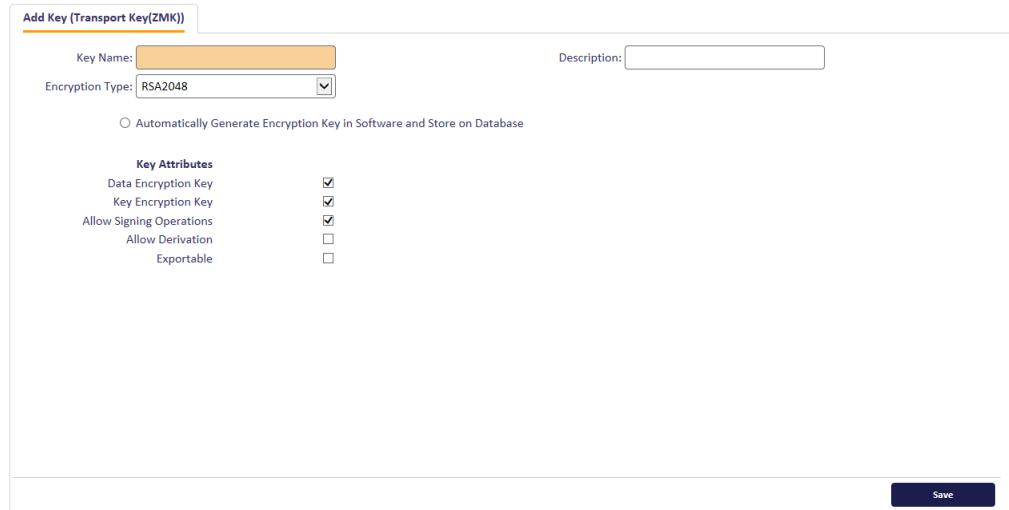
7. Select one of the following options:

- **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 **KeyChecksum 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). See section [16.2.6, Entering keys using a key ceremony](#).

Note: If you select **RSA2048** as the **Encryption Type**, the only options available are:

- **Automatically Generate Encryption Key in Software and Store on Database**
- **Automatically Generate Encryption Key on HSM and Store on HSM** (if your system is configured to use an HSM)

Once you have created the RSA 2048 key, you must export the public key so that you can send it to a third party; see section [16.3.1, Exporting RSA transport keys](#) for details.



Note: You cannot 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.

16.2.2 Factory 9B keys

When PIV cards are manufactured, they are provided with a factory key. You will have been given this factory 9B key by your smart card supplier; this is either 32 or 48 characters in hexadecimal format.

1. From the **Configuration** category, select **Key Manager**.

You can also launch this workflow from the **Configuration Settings** section of the **More** category in the MyID Operator Client. See the *Using Configuration Settings workflows* section in the [MyID Operator Client](#) guide for details.

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 **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 **KeyChecksum 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.

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.
- **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 HSM.

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

12. Click **Save**.

16.2.3 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**.

You can also launch this workflow from the **Configuration Settings** section of the **More** category in the MyID Operator Client. See the *Using Configuration Settings workflows* section in the [MyID Operator Client](#) guide for details.

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 **KeyChecksum 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**.

16.2.4 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 preset selection of key names for use with this functionality.

To add an application key:

1. From the **Configuration** category, select **Key Manager**.

You can also launch this workflow from the **Configuration Settings** section of the **More** category in the MyID Operator Client. See the *Using Configuration Settings workflows* section in the [MyID Operator Client](#) guide for details.

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:
☐ 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"/>

Save

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 **KeyChecksum 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 [16.2.5, Exporting keys](#) for more information.

10. Click **Save**.

16.2.5 Exporting keys

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

For information on exporting RSA transport keys to obtain the public key, see section [16.2.5, Exporting keys](#).

To export a key:

1. From the **Configuration** category, select **Key Manager**.

You can also launch this workflow from the **Configuration Settings** section of the **More** category in the MyID Operator Client. See the *Using Configuration Settings workflows* section in the [MyID Operator Client](#) guide for details.

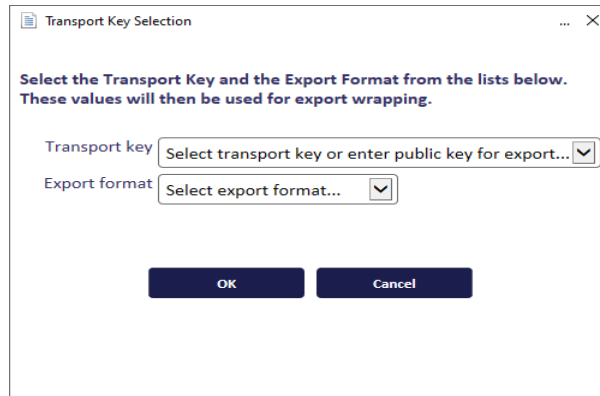
2. From the **Select Key Type to Manage** drop-down list, select the type of key you want to export, and click **Next**.

Existing Keys				
Export Key	Key Name	Version	Description	Key Checksum Value
<input type="radio"/>	my_key	1		EB463C
<input type="radio"/>	test1	1		97ED55
<input checked="" type="radio"/>	test2	1		DB2624
	Transport Internal	1	A non-exportable Transport Key	A221FB

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**.



The dialog box is titled "Transport Key Selection". It contains the following text: "Select the Transport Key and the Export Format from the lists below. These values will then be used for export wrapping." Below this text are two dropdown menus. The first is labeled "Transport key" and has the text "Select transport key or enter public key for export..." inside. The second is labeled "Export format" and has the text "Select export format..." inside. At the bottom of the dialog are two buttons: "OK" and "Cancel".

5. Select the transport key you want to use to encrypt the key.

If you are using a RSA key to secure the transport, select the **Enter a Public Key** option.

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.

Note: If you are using an RSA public key, you can select only the **KeyCeremony** option.

7. If you are using an RSA public key, provide the following additional information:

- **RSA Public Key** – paste the exported public key from the PEM file for the RSA transport key.
- **Padding Type** – select the type of padding you want to use on the encrypted key.

8. 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.

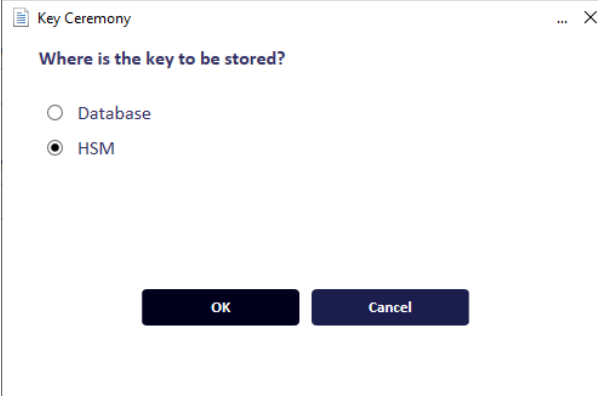
16.2.6 Entering keys using a key ceremony

Various key types allow you to enter the keys using a key ceremony.

To enter the key using a key ceremony:

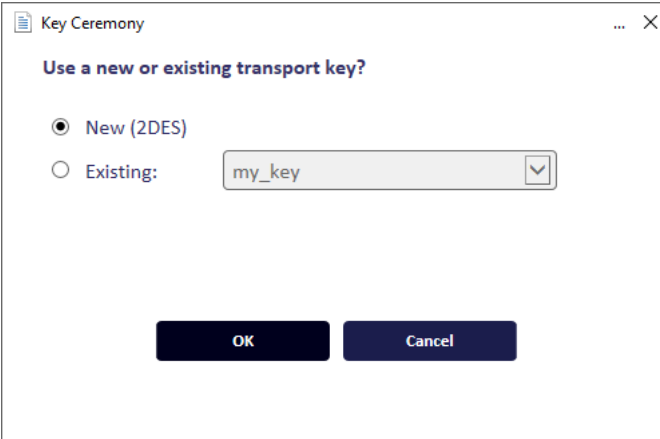
1. Click **Enter Keys**.
2. If you have installed support for an HSM, you are asked whether you want to store the key in the database or on the HSM.

If an HSM is available, Intercede recommends that you use it as it provides stronger protection for the key.



The dialog box is titled "Key Ceremony" and contains the question "Where is the key to be stored?". It has two radio button options: "Database" and "HSM". The "HSM" option is selected. At the bottom, there are "OK" and "Cancel" buttons.

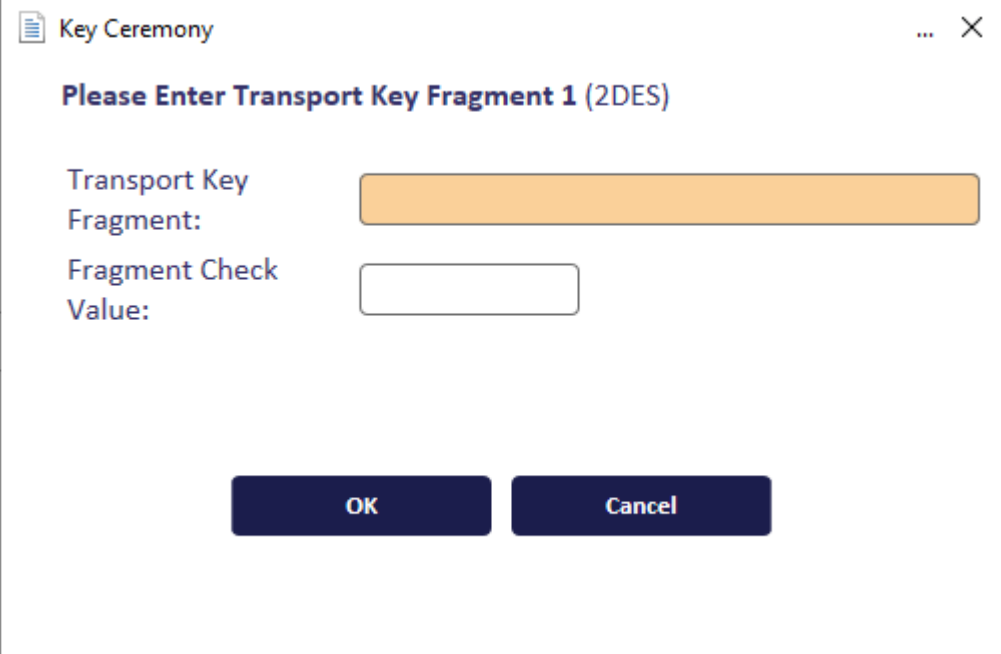
3. Select the location, then click **OK**.



The dialog box is titled "Key Ceremony" and contains the question "Use a new or existing transport key?". It has two radio button options: "New (2DES)" and "Existing:". The "New (2DES)" option is selected. Next to the "Existing:" option is a text field containing "my_key" and a dropdown arrow. At the bottom, there are "OK" and "Cancel" buttons.

4. 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 [16.2, The Key Manager workflow](#) for details of storing a transport key using the **Key Manager** workflow.

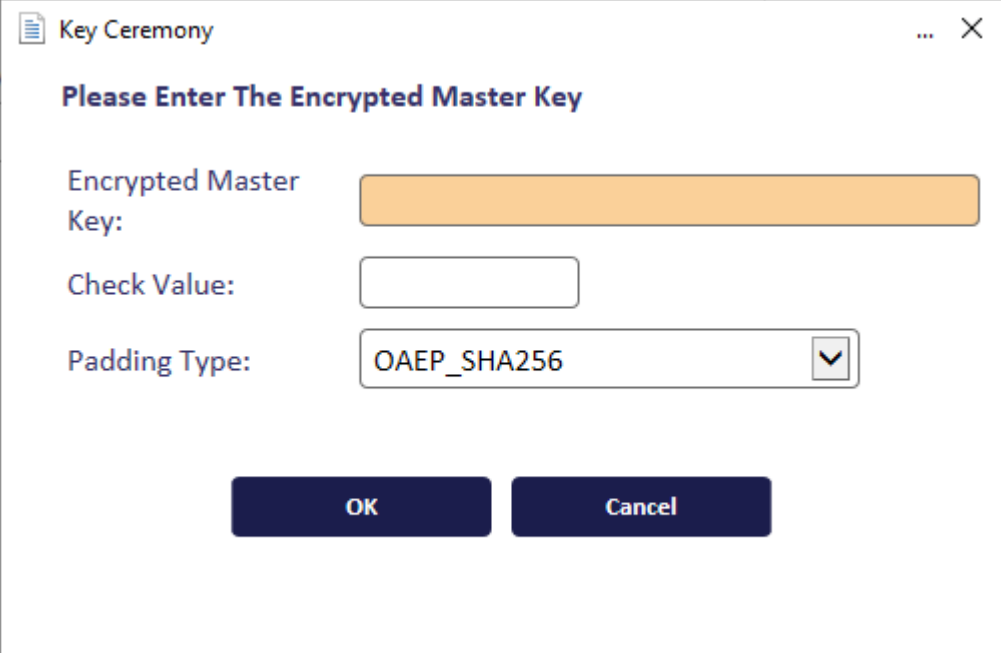


The dialog box is titled "Key Ceremony" and contains the instruction "Please Enter Transport Key Fragment 1 (2DES)". It features two input fields: "Transport Key Fragment:" with a wide orange text box, and "Fragment Check Value:" with a smaller white text box. At the bottom are "OK" and "Cancel" buttons.

5. 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 the supplier of the transport key.

6. Click **OK**, then enter the second and third parts of the transport key.
7. Enter the encrypted master key.



The dialog box is titled "Key Ceremony" and contains the instruction "Please Enter The Encrypted Master Key". It features three input fields: "Encrypted Master Key:" with a wide orange text box, "Check Value:" with a smaller white text box, and "Padding Type:" with a dropdown menu showing "OAEP_SHA256". At the bottom are "OK" and "Cancel" buttons.

Note: You must select the **Padding Type** only if you are using an existing RSA transport key. This must match the padding used when the key was exported and encrypted with the public key. See section [16.3, Using RSA transport keys](#) for details.

Alternatively, to import the key from an XML file:

1. Click **Import Keys**.
2. Select the file containing the key information, then click **Open**.

Note: The file must be in `XMLenc` format.

3. Click **Save**.

16.2.7 Known issues

- **IKB-354 – Cannot enter non-hex characters as the HSM Key Label**

A problem has been identified when entering HSM Key Labels that include non-hexadecimal characters such as hyphen (-), causing failure to update MyID with the key reference.

Error: There has been an error entering keys

Cause: The key data you are entering may be incorrect

Solution: Check and re-enter your keys and/or checksums

For assistance with this issue, contact Intercede customer support quoting reference IKB-354.

16.3 Using RSA transport keys

You can use RSA 2048-bit transport keys to secure the transfer of keys between systems.

The procedure is as follows:

1. Create an RSA transport key.

Use the Key Manager workflow to create a key of type **Transport Key(ZMK)**, and select an **Encryption Type** of **RSA2048**.

You can choose to create the key automatically in the database or in your HSM, if available. You cannot import a key of this type, and you cannot enter the key directly.

See section [16.2.1, Transport keys](#).

2. Export the public key.

You do not need to have selected the **Exportable** option; the exportable attribute restricts only the export of the *private* key, while the *public* key is always exportable.

The public key is a PEM (Privacy Enhanced Mail) format that encodes a `SubjectPublicKeyInfo` (rfc5280) that contains an RSA public key.

For example:

```
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA4d1+POf0845xssbC44RL
XkWMu00PJpG9QY62c17kJ21YMdcB0w0IXji+Y9kDx1bxw1XU+IJ/Z0ZDPsI/pPft
1fZcytuX9p6L04Mi6u/gmbc3CDhnRkRxxkKfGF1f1WoHUKWpgOesKV0xU4pZWw9B5
k3gJryVBqIsJvr9M42DFkknOyrIPrk/MpRqWehW4rHuqNhUhdKf2ZHLXyC/D39gp
```

```
CN7KWYOsNeiMK+n2/x4SgQot4C8uQcMoHR52j3y2BNreD8yevYi0/1XkQYBbqZV2
m0FCQBU8DqY196tfJZc4mHfGZJYDCKP3WmDiISkxNbHpyZnDHoVdBL/IBbqSQBf
8QIDAQAB
-----END PUBLIC KEY-----
```

See section [16.3.1, Exporting RSA transport keys](#).

3. Send the public key to the third party that holds the key you want to transport.
4. The third party then uses the public key to encrypt the key.

On a MyID system, you do this by selecting the **Enter a Public Key** option from the **Transport key** drop-down list on the Transport Key Selection dialog, then providing the public key from the PEM file and specifying the padding type you want to use on the encryption.

For information on encrypting a key using the RSA public key using your own system instead of using MyID, see section [16.3.2, Encrypting a key using the RSA public key](#).

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: Enter a Public Key

Export format: KeyCeremony

RSA Public Key: [Text Area]

Padding Type: OAEP_SHA1

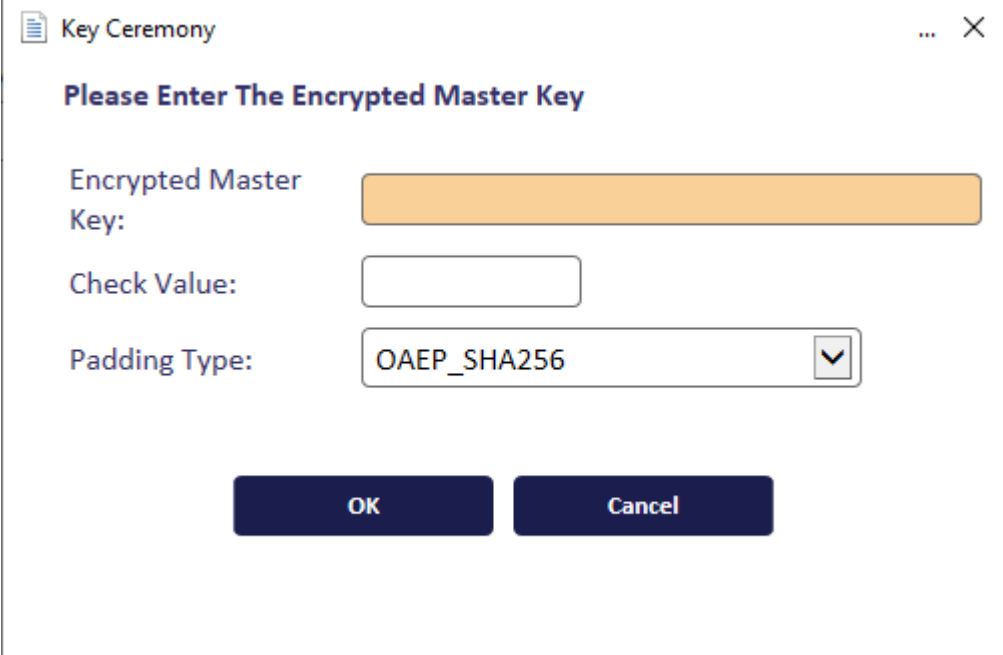
OK Cancel

The key is exported to a file that contains information on the public key used as a transport key, the encrypted key value, and the checksum. The file does not contain information on the padding used.

See section [16.2.5, Exporting keys](#) for details.

5. The third party sends the exported key to you, along with details of what padding was used.
6. You use the key ceremony option to import the key, selecting the RSA transport key related to the public key you provided to the third party.

When you select an RSA transport key in the Key Ceremony dialog, an additional option appears, allowing you to specify the padding used.

A screenshot of a 'Key Ceremony' dialog box. The title bar says 'Key Ceremony' with a document icon on the left and a close button on the right. The main heading inside is 'Please Enter The Encrypted Master Key'. Below this, there are three input fields: 'Encrypted Master Key:' with a large orange rectangular input field; 'Check Value:' with a smaller white rectangular input field; and 'Padding Type:' with a dropdown menu showing 'OAEP_SHA256' and a checkmark icon. At the bottom, there are two dark blue buttons labeled 'OK' and 'Cancel'.

Enter the **Encrypted Master Key**, optionally the **Check Value**, and select the **Padding Type** that was used for the exported key.

See section [16.2.6, Entering keys using a key ceremony](#) (for keys managed using the **Key Manager** workflow) and section [7.3.2, Using a key ceremony](#) (for GlobalPlatform keys managed using the **Manage GlobalPlatform Keys** workflow).

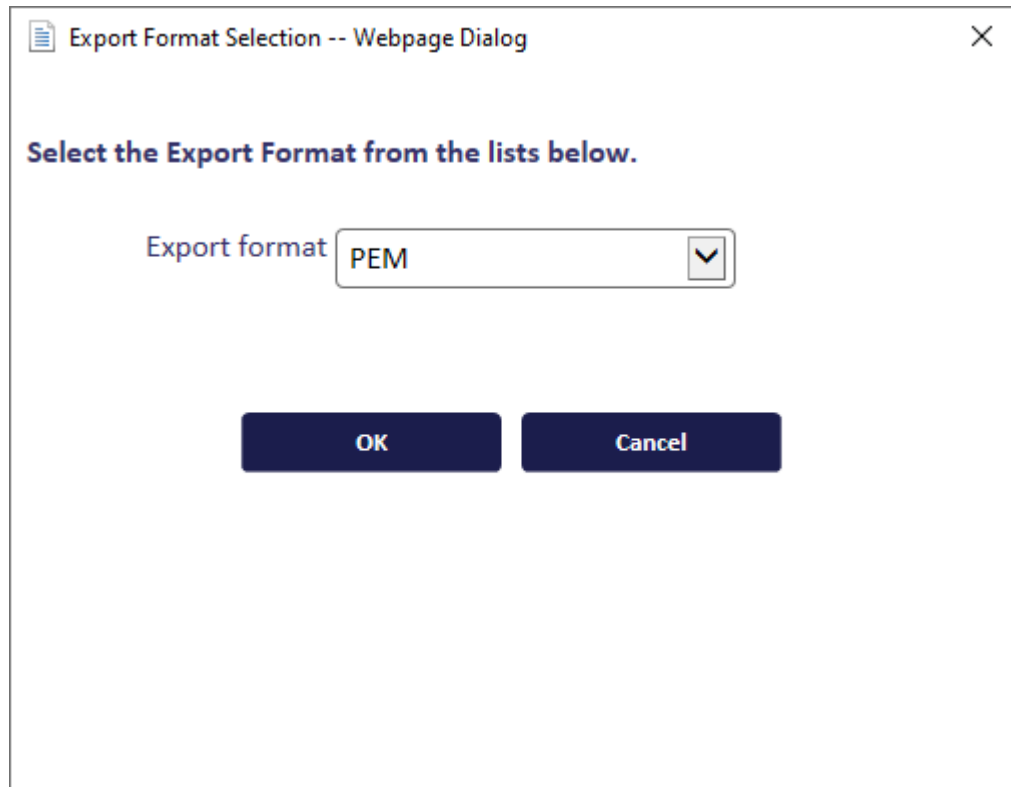
16.3.1 Exporting RSA transport keys

When you create a transport key and select **RSA2048** as the **Encryption Type**, the key is automatically created in the database or in the HSM. To use the key, you must export the public key.

Note: You do not have to set the **Exportable** option on an RSA transport key; the exportable attribute restricts only the export of the *private* key, while the *public* key is always exportable.

To export the public key of an RSA transport key:

1. From the **Configuration** category, select **Key Manager**.
2. From the **Select Key Type to Manage** drop-down list, select **Transport Key(ZMK)** and click **Next**.
3. Select the RSA transport key from the list.
4. Click **Export**.



5. Click **OK**.
6. Type a name for the PEM file and select the location, then click **Save**.
MyID saves the public key in a `.pem` (Privacy Enhanced Mail) format file.
7. Click **Continue**.

16.3.2 Encrypting a key using the RSA public key

If you need to encrypt a key on a third-party system for transport to a MyID system, you can use standard encryption tools.

For example, to use `openssl` to encrypt a key using an RSA public key, use the following settings:

1. Take your key, convert it to binary, and store it in a file.
2. Run `openssl` on the binary key file to encrypt it using the public key stored in the `.pem` file.

For example:

```
openssl pkeyutl -in BinaryKeyFile.txt -out EncryptedKeyFile.txt -pubin
-inkey RSAPublicKey.pem -keyform PEM -encrypt -pkeyopt rsa_padding_
mode:pkcs1
```

This example takes a binary key file `BinaryKeyFile.txt`, encrypts it using the public key stored in `RSAPublicKey.pem` using PKCS1 padding, and stores the resulting encrypted key in `EncryptedKeyFile.txt`.

To use a different padding format, use the appropriate `-pkeyopt` options; for example:

Padding type	openssl encryption options
PKCS1	<code>-pkeyopt rsa_padding_mode:pkcs1</code>
OAEP_SHA1	<code>-pkeyopt rsa_padding_mode:oaep -pkeyopt rsa_oaep_md:sha1 -pkeyopt rsa_mgf1_md:sha1</code>
OAEP_SHA256	<code>-pkeyopt rsa_padding_mode:oaep -pkeyopt rsa_oaep_md:sha256 -pkeyopt rsa_mgf1_md:sha256</code>
OAEP_SHA384	<code>-pkeyopt rsa_padding_mode:oaep -pkeyopt rsa_oaep_md:sha384 -pkeyopt rsa_mgf1_md:sha384</code>
OAEP_SHA512	<code>-pkeyopt rsa_padding_mode:oaep -pkeyopt rsa_oaep_md:sha512 -pkeyopt rsa_mgf1_md:sha512</code>

3. Take the content of the binary encrypted file, and convert it to hex.
4. Send the encrypted hex key to the MyID system, along with details of which padding you used.

17 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 [17.3](#), *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 *Archiving the audit trail* section in the [Advanced Configuration Guide](#) for details of setting up an archive database for these purposes.

17.1 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"/>
Additional Identities (AID)	<input type="checkbox"/>
All Requests	<input type="checkbox"/>
Archived Requests	<input type="checkbox"/>
Assign Device Search	<input type="checkbox"/>
Assigned Devices	<input type="checkbox"/>
Assigned Devices by Group	<input type="checkbox"/>
Audit Reporting	<input checked="" type="checkbox"/>
View Full Audit	<input checked="" 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 ☒

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.

17.2 Running the audit report

The Audit Reporting tool enables you to list events for either a single workflow or task within MyID or for all operations. This list can be filtered according to specific criteria. For example, you might want to view all people added by a particular operator or all events for a named MyID user.

To run an audit report:

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

You can also launch this workflow from the **Additional Reporting** section of the **More** category in the MyID Operator Client. See the *Using Additional Reporting workflows* section in the [MyID Operator Client](#) guide for details.

Alternatively, you can use the **History** tab of the View Person screen or the **Unrestricted Audit Report** in the MyID Operator Client to view the details recorded in the audit trail. See the *Working with the audit trail* section in the [MyID Operator Client](#) guide for details.

2. Complete the form as appropriate and select **Search**.

Note: The **Reset** button returns all fields on the form to their original values before any changes were made.

3. The results are displayed in the **Selected Events** table. This table shows the date on which the events started and ended, if applicable, the type of event (for example, adding a person or canceling a token) and a message associated with the event.

An information symbol appears beside each operation. The color indicates the type of operation.

You can browse through the **Selected Events** table, change the number of rows displayed and toggle the display of the table / Audit Reporting form.

You can also browse through blocks of events.

4. Double-click a result to display individual audit entries for the event.

A single event may have multiple audit entries.

5. Double-click an audit entry to display the audited information.



The Audit Information Gathered dialog appears.

The IP address and client identifier are displayed if this feature is enabled; see section [17.2.3, Logging the client IP address and identifier](#) for details.

You can also view additional information:

- **Signing Details** – displays any information about the signing that was used for the operation, if any.
- **Card Content** – displays the content of the card used for the operation, if any.
- **View Data** – displays the signed content for operation, if any.

Click **Close** to close the Audit Information Gathered dialog.

6. To print the report, click the print  button.
7. To save the report, select **XML**, **CSV**, or **Excel** to select the format, then click the save  button.

17.2.1 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 has not yet completed. This may also occur if the client closed unexpectedly.



Shows that the operation failed. This may happen, for example if there is a failed login 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.

17.2.2 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:



Note: This is separate from navigating *within* a batch, which is done using the following buttons:

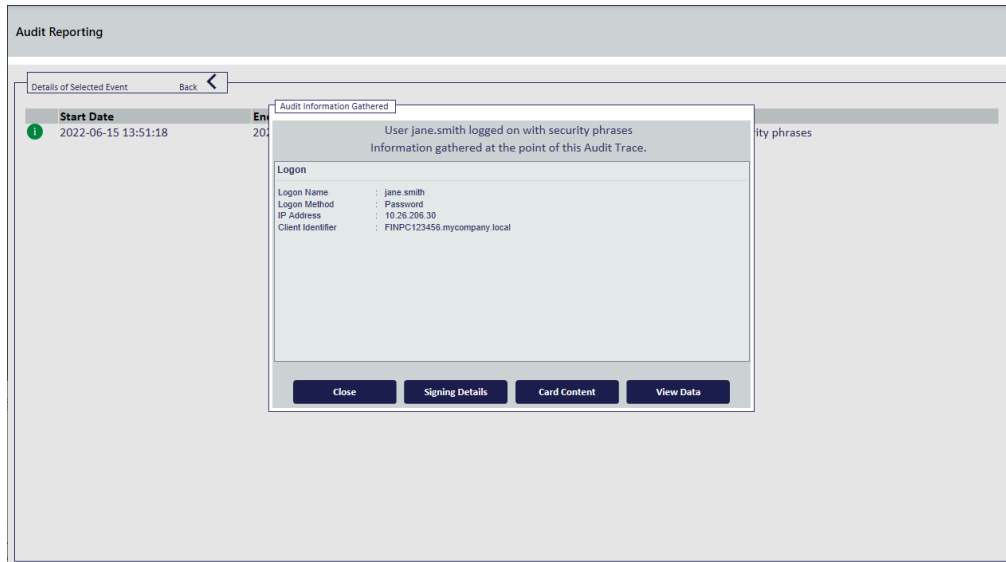


17.2.3 Logging the client IP address and identifier

By default, MyID captures the IP address and the client identifier of the workstation used to carry out the audited operation, and stores this information in the audit trail. By default, the client identifier is the fully-qualified domain name of the client PC; for example, `myworkstation.mydomain.local`. You can customize the client identifier; see section [17.2.4, Specifying a custom client identifier](#).

Note: MyID captures the IP address and client identifier if you have accessed the system through one of the client applications (MyID Desktop, Self-Service App, Self-Service Kiosk, the MyID Operator Client web page, or the MyID Client Service) or through the MyID Core

API. Other systems, such as certificate processes on the server, the Derived Credentials Self-Service Request Portal, mobile provisioning, or web service APIs, do not provide this information.



You can configure whether to capture this information:

1. From the **Configuration** category, select **Security Settings**.
2. On the **Server** page, set the following:
 - **Capture Client Identifier** – Set this option to Yes to capture the client identifier.
 - **Capture IP Address** – Set this option to Yes to capture the client IP address.

Note: MyID captures the IP address as reported to the web server; NAT or load balancing may affect this. Also, the IP address reported is the IPv4 address.
3. Click **Save changes**.

17.2.4 Specifying a custom client identifier

Instead of the default fully-qualified domain name, you can specify a custom identifier on the client PC in the configuration file or the registry.

To set a custom identifier in the configuration file:

1. On the client PC, shut down the application.
2. Back up the configuration file for the application.

The configuration file is as follows:

- **MyID Desktop** – `MyIDDesktop.exe.config` in the following folder by default:
`C:\Program Files (x86)\Intercede\MyIDDesktop\`
- **MyID Client Service** – `MyIDClientService.dll.config` in the following folder by default:
`C:\Program Files (x86)\Intercede\MyIDClientService`
- **Self-Service App** – `MyIDApp.exe.config` in the following folder by default:
`C:\Program Files (x86)\Intercede\MyIDApp\Self Service Application\`
- **Self-Service Kiosk** – `MyIDKiosk.exe.config` in the following folder by default:
`C:\Program Files (x86)\Intercede\MyIDSelfServiceKiosk\`

3. Add the following to the `<appsettings>` section of the configuration file:

```
<add key="ClientID" value="[unique_client_identifier]"/>
```

where:

- `[unique_client_identifier]` – the identifier you want to include in the audit for operations carried out using this installation of the application.

For example:

```
<add key="ClientID" value="Finance - Jane Smith - Laptop serial FINPC-123456"/>
```

Note: You can use the `KioskID` setting for the Self-Service Kiosk instead; for example:

```
<add key="KioskID" value="Kiosk Reception HQ"/>
```

4. Save the configuration file.
5. Restart the application.

To set a custom identifier in the registry:

1. On the client PC, shut down the application.
2. Open the Windows Registry Editor.
3. Navigate to the following:

```
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Intercede
```

4. Set the value of the following:

```
ClientID
```

If the entry does not exist, create a new String value.

5. Restart the application.

Note: The entry in the registry overrides any client identifier settings in the configuration file, and is used for all MyID applications on the current workstation.

17.3 Specifying the items to audit

The **Audited Items** workflow allows you to choose which data items are audited at different stages of individual workflows.

Note: This workflow does not cover the audited items for all workflows or all clients. Changes made in the workflow are not applied to the following:

- MyID Desktop workflows:
 - **Collect Card**
 - **Batch Collect Card**
 - **Assisted Activation**
 - **Reset Card PIN**
 - **Erase Card**
 - **Cancel Credential**
 - **Unlock Credential**
- MyID Operator Client
- Self-Service App
- Self-Service Kiosk
- Mobile clients

If you require further assistance, contact customer support quoting reference SUP-334.

To use the **Audited Items** workflow:

1. From the **Configuration** category, select **Audited Items**.

You can also launch this workflow from the **Configuration Settings** section of the **More** category in the MyID Operator Client. See the *Using Configuration Settings workflows* section in the [MyID Operator Client](#) guide for details.

2. 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.
3. 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.

4. 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.

5. If the stage can be audited, 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.

6. 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.
7. When you have finished, click the **Back** button to return to the **Workflow Stages** screen.
8. 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.

18 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.

18.1 Archiving and encryption

This section provides information on the different types of archiving, and the effect on MyID encryption.

18.1.1 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.

18.1.2 Cards supported

Archived keys are only supported by cards that support certificates.

18.1.3 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](#).

18.1.4 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.

18.2 Setting up key archiving

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

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

Select a CA

CA Name: CA Description: domain31-VINF2019DC31-CA-1 Certificate Authority

CA Type: Microsoft Enterprise

CA Enabled: ☒

Name	Description	Allow Issuance	Reverse DN	Archive Keys	Superseded
AdditionalIdentitiesCertificate on domain31-VINF2019DC31-CA-1		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
AdditionalIdentitiesSmartcardLogon on domain31-VINF2019DC31-CA-1		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
AdditionalIdentitiesSmartcardUser on domain31-VINF2019DC31-CA-1		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Administrator on domain31-VINF2019DC31-CA-1		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
CIVContentSigningCert on domain31-VINF2019DC31-CA-1		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
ClientAuth on domain31-VINF2019DC31-CA-1		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
DerivedPIVAuthentication on domain31-VINF2019DC31-CA-1		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
DerivedPIVEncryption on domain31-VINF2019DC31-CA-1		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
DerivedPIVEncryptionCAArchive on domain31-VINF2019DC31-CA-1		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
DerivedPIVSigning on domain31-VINF2019DC31-CA-1		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
DirectoryEmailReplication on domain31-VINF2019DC31-CA-1		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
DomainController on domain31-VINF2019DC31-CA-1		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
DomainControllerAuthentication on domain31-VINF2019DC31-CA-1		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
ECCVCSCSigningCertificate on domain31-VINF2019DC31-CA-1		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
ECCEXchangeUser(SHA256) on domain31-VINF2019DC31-CA-1		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
ECCEXchangeUser(SHA384) on domain31-VINF2019DC31-CA-1		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
ECCEXchangeUser(SHA512) on domain31-VINF2019DC31-CA-1		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
ECCEXchangeUserCAArchive(SHA256) on domain31-VINF2019DC31-CA-1		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
ECCEXchangeUserCAArchive(SHA384) on domain31-VINF2019DC31-CA-1		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
ECCEXchangeUserCAArchive(SHA512) on domain31-VINF2019DC31-CA-1		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
ECCPIVAuthentication(SHA256) on domain31-VINF2019DC31-CA-1		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
ECCPIVAuthentication(SHA384) on domain31-VINF2019DC31-CA-1		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Delete New Edit

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)**.

☒ **Enabled (Allow Issuance)**

Display Name:

Description:

Allow Identity Mapping: ☐

Reverse DN: ☐

Archive Keys:

Certificate Lifetime:

Automatic Renewal: ☒

Certificate Storage: ☒ Hardware ☐ Software ☐ Both

Recovery Storage: ☒ Hardware ☐ Software ☐ Both ☐ None

Key Algorithm:

Key Purpose:

Edit Attributes

Supersede

b. Set the **Archive Keys** option to one of the following options:

- **None**

The certificates issued with this profile will not be archived.

- **Internal**

The certificates issued with this profile will be archived in the MyID database.

- The name of the Certificate Authority (for example, **Microsoft** or **Entrust**)

The certificates issued with this profile will be archived in the Certificate Authority.

6. Click **Save**.

When you issue a card, any certificates marked for archival are stored on the card and also archived in either the MyID database or the certificate authority.

19 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. You can issue, cancel, erase, and manage the PIN of these cards, but you cannot carry out other operations (for example, device update or device renewal).

19.1 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 **Device Profiles**.
10. Select a **Card Format**.

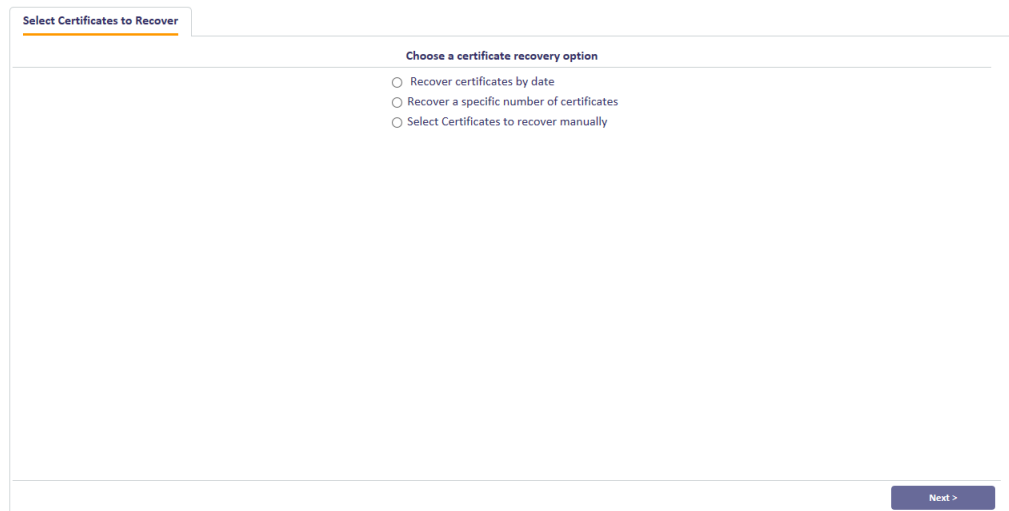
Note: Do not select a PIV data model if the cardholder does not have biometrics enrolled.
11. Click **Next**.
12. Complete the workflow. You can specify a card layout to be used on the printed key recovery cards.

19.2 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**.
You can also launch this workflow from the **Certificate Administration** section of the **More** category in the MyID Operator Client. See the *Using Certificate Administration workflows* section in the [MyID Operator Client](#) guide for details.
2. 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. If you are issuing a key recovery card with a randomly-generated PIN, confirm the email address to which the PIN will be sent in the **PIN notification email address** box.
 11. Optionally, type a label in the **Assign Job Label** box – you can use this label to search for the recovery job in other workflows.
 12. 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**.
 13. 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 [19.3, 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 [19.4, Collecting a key recovery job for another user](#) for details.
 - **IKB-248 – Cannot cancel key recovery jobs that are awaiting issue through job management**
If you request recovery of a certificate using the **Request Key Recovery** workflow, once the request has been approved (or if it does not require approval) you cannot subsequently use the **Job Management** workflow to prevent a recipient from picking up the job.
To cancel a key recovery job, use the **Reject** button on the **Collect Key Recovery** or **Collect My Key Recovery** workflow.

19.3 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**.

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

2. Use the Search 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.

19.4 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 19.3, *Validating a key recovery request* for details.

To collect a key recovery request:

1. From the **Certificates** category, select **Collect Key Recovery**.

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

2. Use the Search 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.

19.5 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 [19.3, Validating a key recovery request](#) for details.

To collect a key recovery request:

1. From the **Certificates** category, select **Collect My Key Recovery**.

Note: You can also launch this workflow from the self-service menu in the MyID Operator Client. See the *Launching self-service workflows* section in the [MyID Operator Client](#) guide for details.

2. 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.

19.6 Viewing key recovery operations

You can view the details of all completed, canceled, or in progress key recovery operations.

To view a key recovery operation:

1. From the **Certificates** category, select **View Key Recovery**.




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

2. Use the Search 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"/>	 18	David Balsam	startup user	13 July 2020			Awaiting Validation	Recover archived certificates
<input type="radio"/>	 19	Sam Smith	startup user	13 July 2020	Alex Slee	13 July 2020	Awaiting Issuance	Recover archived certificates
<input type="radio"/>	 20	David Samuel	startup user	13 July 2020			Awaiting Validation	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.

20 External systems

The **External Systems** workflow allows you to set up connections to external systems; for example, to email SMTP servers, PACS servers, or authentication services.

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.

For details of setting up an SMTP server for email, see the *Setting up email* section in the [Advanced Configuration Guide](#).

To set up an external system:

1. From the **Configuration** category, select **External Systems**.

You can also launch this workflow from the **Connections and Notifications** section of the **More** category in the MyID Operator Client. See the *Using Connections and Notifications workflows* section in the [MyID Operator Client](#) guide for details.

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**.

21 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.

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 jobs

To search for a job and view its details, from the **Configuration** category, select the **Job Management** workflow.

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

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.

22.4 Automatic job cancellation

MyID provides a job processor that allows you to cancel old jobs that have not been collected for a specified number of days since the job was created. When you install MyID, the automatic job cancellation processor is not configured to run; to enable the processor, you must specify number of days after which you want jobs to be canceled; see section [22.4.1, *Enabling the automatic job cancellation processor*](#)

Once enabled, the processor runs once a day, and cancels the following types of job:

- Issue Card
- Issue FIDO
- Issue Replacement Card
- Reprovision Card
- Request Soft Certificates
- Update Card
- Issue Machine Identity
- Issue Mobile Soft Cert
- Issue Token
- Recover Certificates
- Recover Cert Mobile

The processor cancels jobs of the above types that are in the following states:

- Created
- Awaiting Validation
- Awaiting Issue
- Awaiting Activation

If you want to customize the automatic job cancellation processor to cancel different types of jobs, or jobs at different statuses, contact customer support quoting reference SUP-352.

22.4.1 Enabling the automatic job cancellation processor

To specify the number of days after which old jobs are canceled:

1. From the **Configuration** category, select **Operation Settings**.
2. Click the **Bureau & Job** tab.
3. Set the following option:
 - **Automatic cancellation timeout** – set this to the number of days after which you want jobs to be canceled. To prevent the job processor from canceling old jobs, set this value to 0.
The default is 0.
4. Click **Save changes**.

22.4.2 Filtering the canceled jobs by credential profile

You can specify a string that must be present in the credential profile for the automatic job cancellation processor to cancel old jobs. For example, if you have the following credential profiles:

- User Card
- User Badge
- Admin Card
- Admin Badge

and set a filter of "User", only jobs for the User Card and User Badge credential profiles are automatically canceled; jobs for Admin Card and Admin Badge are not canceled.

To set a credential profile filter:

1. From the **Configuration** category, select **Operation Settings**.
2. Click the **Bureau & Job** tab.
3. Set the following option:
 - **Automatic job cancellation credential profile filter** – set this a string that must be present in the credential profile name for jobs to be canceled. Leave this option blank to cancel all jobs.

The default is blank.

4. Click **Save changes**.

22.4.3 Specifying the email template for notifications

By default, when the automatic job cancellation processor cancels old jobs, it sends a notification email to the administrator using the **Automatic Job Cancellation** email template (template ID 113). You can review and edit the content of this template using the **Email Templates** workflow; see section [13.2, *Changing email messages*](#) for details.

Note: If you want to use email notification, you must set up an SMTP server within MyID – see the *Setting up email* section in the [Advanced Configuration Guide](#) for details.

You can also change which email template is used. You must know the ID of the email template; see section [13.3, *Standard templates*](#) for a list of standard email templates and their IDs.

To change the email template used for automatic job cancellation email notifications:

1. From the **Configuration** category, select **Operation Settings**.
2. Click the **Bureau & Job** tab.
3. Set the following option:
 - **Automatic job cancellation email** – set this to the ID of the email template you want to use. To prevent email notifications from being sent, leave this option blank.

The default is 113.

4. Click **Save changes**.

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.

Note: To allow self collection, the system role **Activation User** must exist, and must have access to the **Activate Card** workflow; this system role is used because the cardholder is using a locked card. By default, this configuration is set up when you install MyID; do not use the **Edit Roles** workflow to change the **Activation User** role. If this role is not set up correctly, when you attempt to carry out self activation of a card, you may see an error similar to:

```
9004028 - You do not have permission to access this workflow
```

Note: When the **Restrict Self Activation** configuration option (on the **Self-Service** page of the **Security Settings** workflow) is set to **Yes**, you have access to the operations allowed by the **Activation User** role *only* if these operations are already permitted by your assigned roles; if the **Restrict Self Activation** configuration option is set to **No**, you have access to *all* operations allowed by the **Activation User** role, whether or not your own assigned roles provide access.

- **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.
- **Counter Signed and Witnessed** – as for **Counter Sign**, but an additional operator must act as a witness and enter their card's PIN to sign the terms and conditions with

the cardholder's, operator's, *and* witness's credentials. The witness's role must allow them to witness the operation.

- **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 [30.2, 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.

Important: You must make sure that the MyID application server trusts the issuing CA (that is, the CA is in the trusted root store) and can access the Certificate Revocation List (CRL) for the CA for each certificate in the signing certificate's chain.

- **Terms and Conditions Template**

For device operations that use the HTML template method for their terms and conditions document, select a template from the **Terms and Conditions Template** drop-down list.

See section [11.6, Customizing terms and conditions](#) for details.

23.2.1 Viewing audited terms and conditions

When the terms and conditions are accepted, and the signing event takes place, an audit record is created to capture the event and the signing detail. You can see this acceptance in the **Audit Reporting** workflow; select the audit record created by the activation process and locate the audit trace record:

```
"User: [target user logon name], card [device serial number], accepted terms and conditions"
```

If the **Assisted Activation** workflow has been used, and the system is configured to store terms and conditions (see section [11.6.6, Storing signed terms and conditions](#)) a link to the information displayed is included. Technical detail is held within the audit trace record:

```
"Validated data signed by [target user logon name]"
```

Double-click on this row to open the detailed view. Click **View Data** to show the signing details.

23.2.2 Known issues

- **IKB-321 – Error -99900041 reported when CA CRL is not accessible**

If the CRL is not accessible when signing terms and conditions, Error -99900041 is displayed. (Failed to communicate with MyID server. The application will now exit.). Check configuration steps required have been completed and that the CRL is accessible by the MyID Server.

See entry for error -99900041 in the *MyID Windows client error codes* section in the [Error Code Reference](#) guide for more information.

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 **Activation Authentication** option.
- **Activation 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 **Activation Authentication** option to an authentication code option.

If you set the **Activation 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 **Activation 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 **Activation 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.

Note: The list of available documents is determined by the **Authenticate Person Document1** and **Authenticate Person Document2** lists. To edit these lists, use the **List Editor**. See the section [15, Changing list entries](#) for details.

- **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](#) guide for details.

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

24.1 Device management 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 device management 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 required to make the devices available to MyID.
- **Confirm Cancel Device Request**, **Request Device Identity** and **Validate Device Request** in the **Devices** category are required 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\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\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 Signing and encryption certificates for SCEP

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:

- Request Handling Purpose: `Signature`
- Key Usage: `Digital Signature`

By default, MyID uses a hash algorithm of SHA256 for SCEP signing. The certificate that you use for signing must therefore have been produced using a KSP or CSP that supports SHA256; some older CSPs (for example, the Microsoft Strong Cryptographic Provider) do not support SHA256; the Microsoft Enhanced RSA and AES Cryptographic Provider does support SHA256, however.

If you want to use a SCEP signing certificate that does not support SHA256, you must configure MyID to use SHA1 for the SCEP hash algorithm:

1. From the **Configuration** category, select **Security Settings**.
2. On the **Server** tab, set the following option:

- **SCEP Hash Algorithm** – set to one of the following:
 - **SHA1** – use SHA1 for the hash algorithm. Set this option if your SCEP signing certificate does *not* support SHA256.
 - **SHA256** – use SHA256 for the hash algorithm. Set this option if your SCEP signing certificate *does* support SHA256.

3. Click **Save changes**.

24.4.2 Encryption certificate

The encryption certificate must have the following properties:

- Request Handling Purpose: `Encryption`
- Key Usage: `Key Encipherment`

24.4.3 Adding the certificates to the registry

To configure the signing and encryption certificates in the 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\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`

24.5 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 cancellation 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 [24.8, Requesting a device identity](#) for details.

Note: Do not select the **Require user data to be approved** option. The device identity is issued to a device, not a user, and therefore cannot have the user data approved flag set.

7. Click **Next**.
8. Select the certificate you want to issue to the device.

Note: Do not select a certificate policy that has the **Automatic Renewal** option set in the **Certificate Authorities** workflow – device identities do not support automatic renewals. If you need to renew a device identity, you must request a new identity for the device.

Note: You must not select any certificates policies that are marked as archived; you cannot issue device identities with archived certificates. If you attempt to collect a device identity using a credential profile that has an archived certificate, the collection will fail.

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

24.6 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 [30.2, 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 [30.3, LDAP page \(Operation Settings\)](#).

Alternatively, you can use the Device Management API; see the [Device Management API](#) guide for details.

24.6.1 Adding devices manually

To add a device:

1. In the **Configuration** category, select the **Add Devices** workflow.

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

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-based dialog titled "Add Device". It has a tab labeled "Add Device". The form contains the following fields and controls:

- Device Name:** A text input field, currently highlighted with an orange background.
- Description:** A text input field.
- Device Active:** A checkbox that is checked.
- DN:** A text input field.
- Model:** A text input field.
- OS:** A text input field.
- Buttons:** "Finish" and "Cancel" buttons are located at the bottom right of the dialog.

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.

24.6.2 Adding devices from an LDAP directory

To add a device from a directory:

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



2. Click the button next to the **LDAP Group** field .
3. If you want to search subgroups of the directory, select the **Include Subgroups** option.
4. Select the branch of the directory that contains the device you want to add.
5. Click **Search**.

If you need this search to return devices based on different criteria, contact customer support for assistance.

6. From the list, select the devices you want to add.
7. Click **Finish** to import all the devices.

Alternatively, click **Edit Devices** to specify whether each device is active as you import it. A separate screen is displayed for each device; select or deselect the **Device Active** option, then click one of the following:

- **Import** – import the currently-displayed device and move on to the next.
 - **Skip** – do not import the currently-displayed device and move on to the next.
 - **Finish** – import the currently-displayed device and all following devices. Devices you have already imported or skipped are not affected.
 - **Cancel** – cancel the import. No devices are imported.
8. If you want to specify an owner for the devices:
 - Click **Yes** on the dialog.
 - Use the Find Person screen to select the owner.

If you specify an owner, the device can be managed only by the owner; for example, only the owner can cancel a device identity. In addition, the device owner is used as the target of the request device identity job.

24.7 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 [30.2, Devices page \(Operation Settings\)](#).

To make changes to details stored about a device:

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

You can also launch this workflow from the **Device Identities** section of the **More** category in the MyID Operator Client. See the *Using Device Identities workflows* section in the [MyID Operator Client](#) guide for details.

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**.

The screenshot shows the 'Select Device' workflow. The 'Device Name' field contains 'Web'. Below the search bar are 'Search' and 'Abort' buttons. The 'Results' section displays a table with one device:

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

At the bottom right of the results section are 'Edit Device' and 'Abort' buttons. The table has 5 columns and 1 row of data. The 'Rows' dropdown is set to 'Auto' and 'Page 1 of 1' is shown.

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.

The screenshot shows the 'Edit Device' form. The fields are as follows:

- Device Name: WebServerABC123
- Description: Web server
- Device Active: ☒
- DN: (empty field)
- Model: (empty field)
- OS: (empty field)
- Type: Asset
- Serial No.: (empty field)

At the bottom right are 'Finish' and 'Cancel' buttons.

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.

24.8 Requesting a device identity

To request a device identity:

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

You can also launch this workflow from the **Device Identities** section of the **More** category in the MyID Operator Client. See the *Using Device Identities workflows* section in the [MyID Operator Client](#) guide for details.

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: Page 1 of 1

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

Edit Device

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

24.9 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**.

You can also launch this workflow from the **Device Identities** section of the **More** category in the MyID Operator Client. See the *Using Device Identities workflows* section in the [MyID Operator Client](#) guide for details.

Search Details

DNS Alias:

Group:

Include Subgroups:

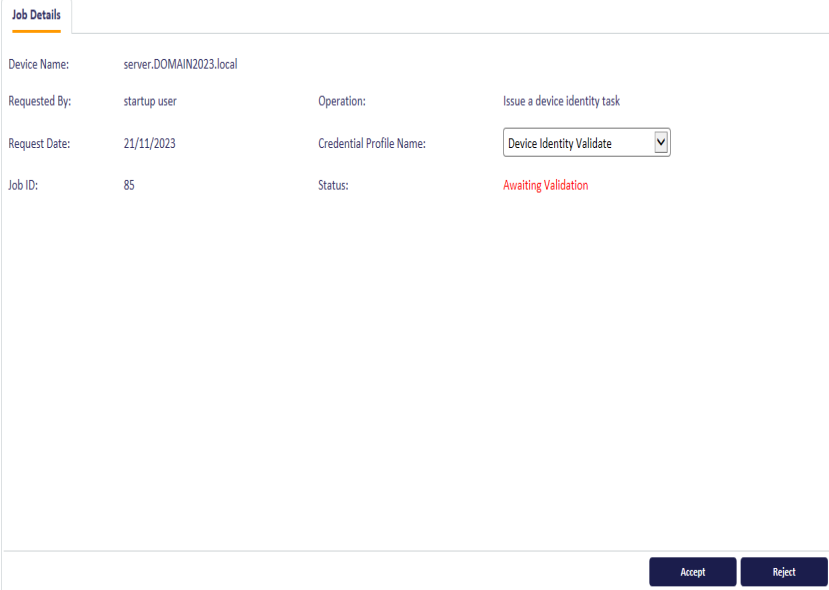
☒

Job Label:

Maximum Records:

Search

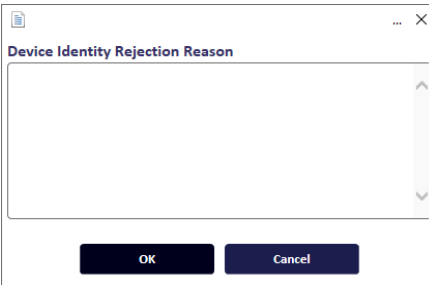
2. Search for the device identity you want to approve:
 - a. Restrict the search using the **DNS Alias** for the device and the **Group** to which the device belongs.
If you know the job label, use that to identify the record.
 - b. Click **Search**.
3. Select the job from the list, and click **Next**.



Job Details

Device Name:	server.DOMAIN2023.local		
Requested By:	startup user	Operation:	Issue a device identity task
Request Date:	21/11/2023	Credential Profile Name:	Device Identity Validate <input type="button" value="v"/>
Job ID:	85	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

24.10 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
```

24.11 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 cancellation 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**.

You can also launch this workflow from the **Device Identities** section of the **More** category in the MyID Operator Client. See the *Using Device Identities workflows* section in the [MyID Operator Client](#) guide for details.

2. Optionally, type the name of the device you want to search for.

You can use * wildcards in the device name.

3. Click **Search**.

4. From the search results list, select a device, and click **Continue**.

If the device does not have a currently-issued identity, MyID informs you.

5. Select the reason for the cancellation, then click **Continue**.

See the *Certificate reasons* section in the [Operator's Guide](#) for details.

6. Type the reason you are canceling 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.

24.12 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**.

You can also launch this workflow from the **Device Identities** section of the **More** category in the MyID Operator Client. See the *Using Device Identities workflows* section in the [MyID Operator Client](#) guide for details.

2. Search for the device identity you want to cancel:
 - a. Restrict the search using the **DNS Alias** for the device and the **Group** to which the device belongs.
Specify the Job Label if known to go straight to the correct record.
 - b. Click **Search**.
3. Select the device 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.

24.13 Known issues for device identities

- **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 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.

25.1 Additional identities overview

The process for issuing additional identities 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.

25.1.1 Renewing additional identities

You can renew certificates issued as additional identities; see section [6.6, Certificate renewal](#) for details.

Note, however, that in previous versions of MyID, you could not renew additional identity certificates. If you have additional identity certificates issued in versions of MyID earlier than 12.3, the workaround options are as follows:

- You can revoke the additional identity certificates using the **Issued Certificates** workflow, then update the device – new additional identity certificates will be issued.
You can request updates using the **Request Card Update** workflow in MyID Desktop, or the cardholder can use the Self-Service App if the self-Service device update feature is enabled; see the *Self-service device update* section in the [Self-Service App](#) guide.
- Reprovision the device, causing all certificates on the device to be re-issued.

For further assistance with this, contact Intercede customer support quoting reference SUP-358.

25.1.2 Additional identities on devices with PIV applets

If you want to issue additional identities to devices with PIV applets, you must have a Windows minidriver installed to make the certificates available for uses such as Windows logon. MyID has been tested issuing additional identities with the following:

- Yubikey devices in conjunction with the Yubikey minidriver.

See the *Additional identities for YubiKey tokens* section of the [Smart Card Integration Guide](#).

- IDEMIA PIV cards using the IDEMIA minidriver.

See the *Additional identities for IDEMIA PIV cards* section of the [Smart Card Integration Guide](#).

Note: You must use the `CivCertificatesOnly.xml` card format (from the **Card Format** drop-down list on the **Device Profiles** section of the **Credential Profiles** workflow) to issue your devices if you want to issue additional identities.

25.1.3 User SIDs in additional identities

When MyID adds an additional identity, it captures the user SID of the additional identity, which is required for Windows authentication. For information on user SIDs, see section 6.9, [Including user security identifiers in certificates](#)

Versions of MyID before MyID 12.6 did not capture the user SID for additional identities. As there is no way to synchronize additional identities with your directory to obtain this information, if you want to include the user SID in existing additional identities so that it can be incorporated into additional identity certificates, you must remove each additional identity that does not have a user SID and add it again from the directory.

To determine which additional identities are affected, you can view a list of additional identities, including the user SID for each additional identity where present, using the **Additional Identities (AID)** report in the MyID Operator Client; see the *Additional Identities (AID) report* section in the [MyID Operator Client](#) guide.

25.2 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: AdditionalIdentitiesCertificate on domain31-

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 Algorithm: RSA 2048

Key Purpose: Signature and Encryption

[Edit Attributes](#)

[Supersede](#)

- Select the **Enabled (Allow Issuance)** option for the certificate policy.
- Set the **Allow Identity Mapping** option on the certificate policy.
- Make sure the **Archive Keys** option is set to **None**.
- Click the **Edit Attributes** button:

Note: If the attribute value is not set, the attribute will not be supplied for the certificate. The subsequent behavior depends on how the certificate is configured and the CA being used. Note also that choosing to remove an attribute for a user's issuance may result in the certificate being unusable for its intended purpose, or the certificate may not be issued at all, depending on the CA and the attribute.

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**, **Email**, and **User Security Identifier** mappings to be dynamically mapped to the **User Principal Name**, **Email**, and **User Security Identifier** user attributes.

Policy Attributes

Attribute	Type	Value
FASC-N	Not Required	Not Required
UUID	Not Required	Not Required
NACI	Not Required	Not Required
UserPrincipalName	Dynamic	User Principal Name
Email	Dynamic	Email
User Security Identifier	Dynamic	User Security Identifier

* = Mandatory attribute
 # = Recommended attribute

Hide Attributes

Note: The **User Security Identifier** attribute is available for Microsoft and PrimeKey EJBICA CAs.

- Click **Save**.
- In the **Credential Profiles** workflow, select the credential profile that you want to use to issue additional identities then click **Modify**. In the **Issuance Settings** section, click the **Issue Additional Identities** option.

Issuance Settings

Validate Issuance: ☐
 Validate Cancellation: ☐
 Lifetime: 180 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 Fingerprints at Issuance: Never Required
 Require Facial Biometrics: Never Required
 Activation Authentication: System Default
 Terms and Conditions: None
 Terms and Conditions Template: None
 Credential Group :

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 do not need to 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.
- To set up a filter for the results returned from the LDAP when importing an additional identity from the directory, in the **Operation Settings** workflow, on the **LDAP** tab, set the following options:
 - **Additional Identity LDAP Operator User Filter** – set a query filter when importing an additional identity for another person.
 - **Additional Identity LDAP Self-Service User Filter** – set a query filter when importing an additional identity for your own account.

For example:

- `(&(objectClass=user)(cn=*ADMIN))` – Only show user accounts where the common name ends with ADMIN.
- `(&(objectCategory=person)(objectClass=user)(memberOf:1.2.840.113556.1.4.1941:=CN=Domain Admins,CN=Users,DC=mydomain,DC=local))` – Show people who are members of the domain's admin group.

For the **Additional Identity LDAP Self-Service User Filter** option, you can also include substitutions for the person's details; this allows you to restrict the available list of additional identities that a person can add to their own account.

Use the format:

```
[People.FieldName]]
```

where the `FieldName` is a field in the `vPeopleUserAccounts` field in the MyID database.

For example:

- `userPrincipalName=[[People.LogonName]] *`

This filters the list of directory entries to those with a `userPrincipalName` that begins with the user's logon name. For example, if you are logged on as Joan Smith, the filter becomes:

```
userPrincipalName=Joan Smith*
```

whereas if you are logged on as Susan Jones, the filter becomes:

```
userPrincipalName=Susan Jones*
```

- `userPrincipalName=[[People.LogonName]] *@DOMAIN.com`

All users that have a UPN that starts with the logon name of the user and ends with DOMAIN.com.

- `userPrincipalName=[[People.LogonName]] *@[[People.Domain]] .com`

All users that have a UPN that starts with the logon name of the user and ends with the user's domain, followed by .com.

- `SAMAccountName=[[People.LogonName]] *`

All users that have a `SAMAccountName` that starts with the user's logon name.

- `(&(ou=AdminAccounts)(sAMAccountName=[[People.LogonName]] *))`

All users that are part of the `AdminAccounts` OU and have a `SAMAccountName` that starts with the user's logon name.

Useful fields that you may want to use from the `vPeopleUserAccounts` view are:

- `LogonName`
- `Domain`
- `CommonName`
- `DistinguishedName`
- `UserPrincipalName`
- `SAMAccountName`
- `OrganisationalUnit`

Important: These LDAP user filters are applicable only when using the **Import Additional Identity** feature in the MyID Operator Client; see the *Importing an additional identity* section in the *MyID Operator Client* guide. These settings do not affect the **Manage Additional Identities** workflow in MyID Desktop.

Note: After changing these settings, you must recycle the web service app pools:

1. On the MyID web server, in Internet Information Services (IIS) Manager, select **Application Pools**.
2. Right-click the **myid.web.oauth2.pool** application pool, then from the pop-up menu click **Recycle**.
3. Right-click the **myid.rest.core.pool** application pool, then from the pop-up menu click **Recycle**.

This ensures that the MyID Operator Client picks up the configuration changes.

25.3 Adding additional identities

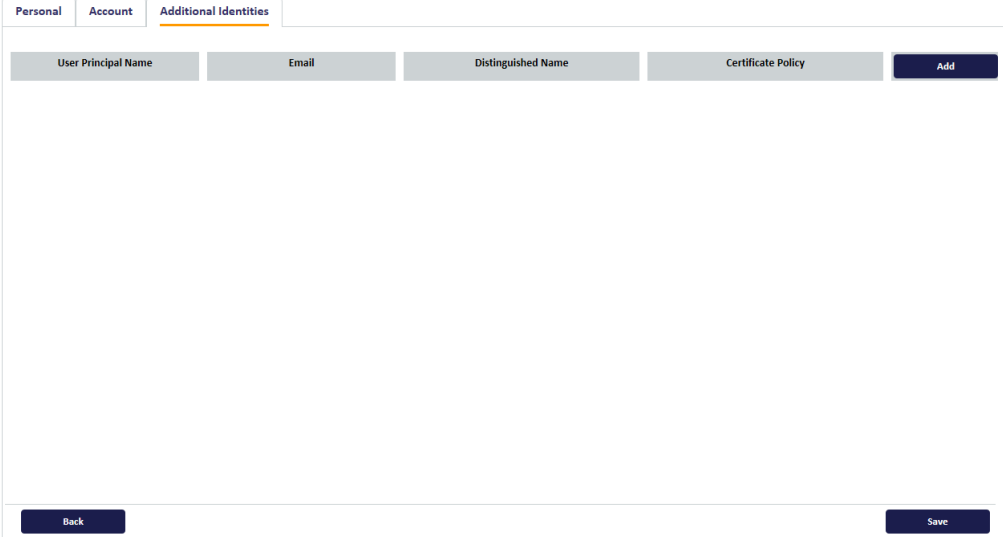
You can use the **Manage Additional Identities** workflow to add new identities (for example, accounts from other areas of the LDAP directory) and certificates that can then be included on the user's smart card.

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.

Note: Alternatively, you can use the features in the MyID Operator Client to manage your alternative identities. See the *Working with additional identities* section in the *MyID Operator Client* guide for details.

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 the 'Additional Identities' tab selected in a user management interface. The tab is part of a set including 'Personal' and 'Account'. Below the tabs, there are four input fields: 'User Principal Name', 'Email', 'Distinguished Name', and 'Certificate Policy'. To the right of these fields is an 'Add' button. At the bottom of the form, there are 'Back' and 'Save' buttons.

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 the directory structure: 'LDAP Root', 'Default ADS', and 'PIV ADS'. On the right, there is a search section with a 'Search' button and a 'Filter:' input field. Below the search section, it says 'All users matching the criteria in and below the selected group are displayed'. At the bottom, there is a 'Please select a group' prompt and a 'Cancel' button.

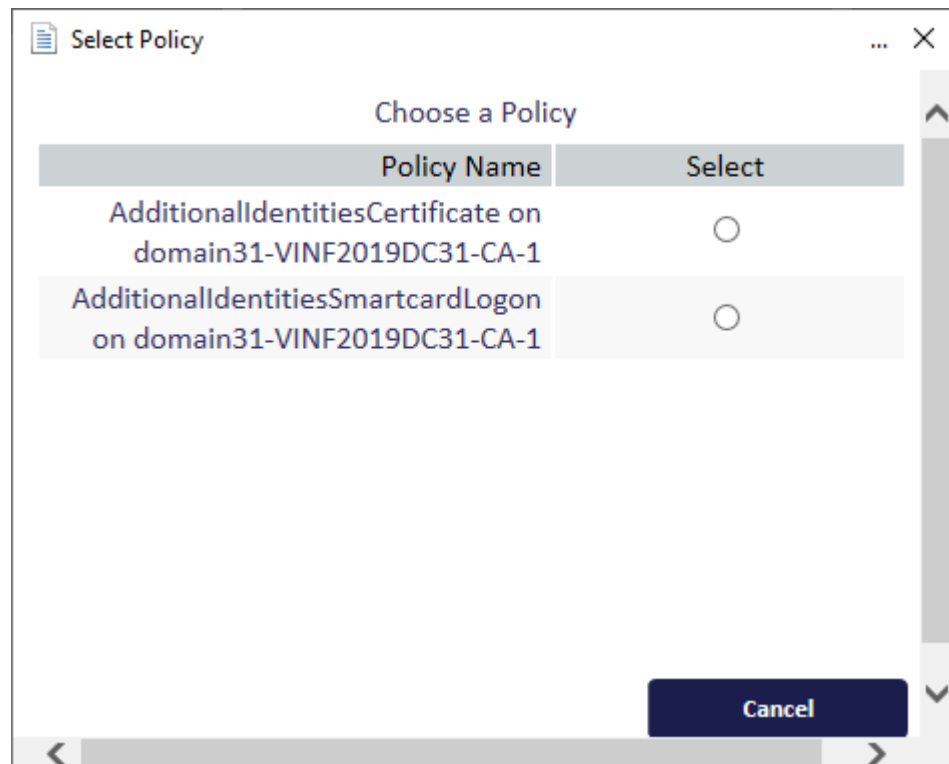
The available entries in the directory are restricted to the Organizational Unit of the operator and below.

- 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**.

If you have more than one certificate authority set up for additional identity certificate policies, you must select which one to use.

If you have only one certificate authority set up for additional identity certificate policies, MyID proceeds directly to the Select Policy dialog.



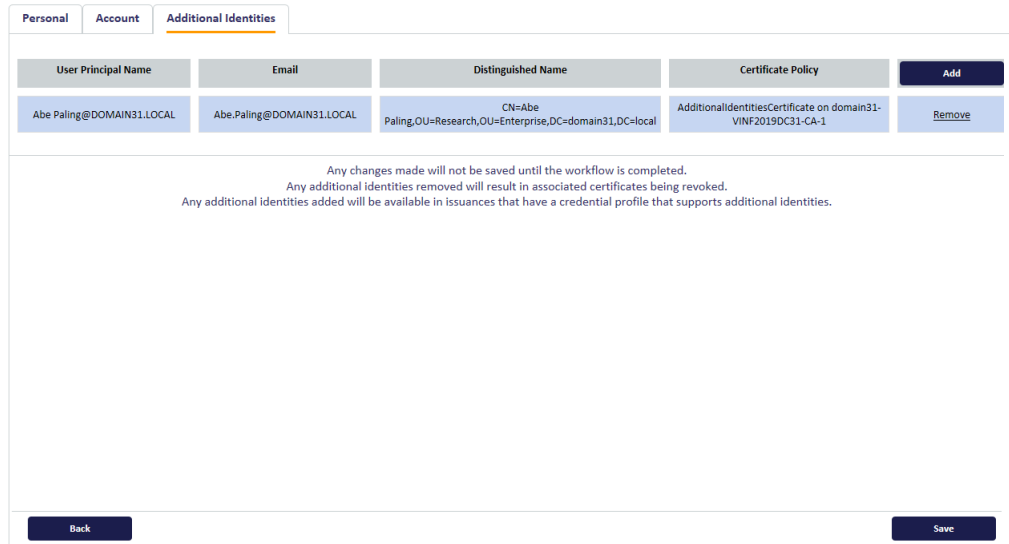
- g. Select the additional identity policy from the CA you want to use, then click **OK**.
5. Click **Save**.

25.4 Removing additional identities

Note: Alternatively, you can use the features in the MyID Operator Client to manage your alternative identities. See the *Working with additional identities* section in the [MyID Operator Client](#) guide for details.

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.



User Principal Name	Email	Distinguished Name	Certificate Policy	
Abe Paling@DOMAIN31.LOCAL	Abe.Paling@DOMAIN31.LOCAL	CN=Abe Paling,OU=Research,OU=Enterprise,DC=domain31,DC=local	AdditionalIdentitiesCertificate on domain31-VINF2019DC31-CA-1	Remove

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.

Back Save

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.

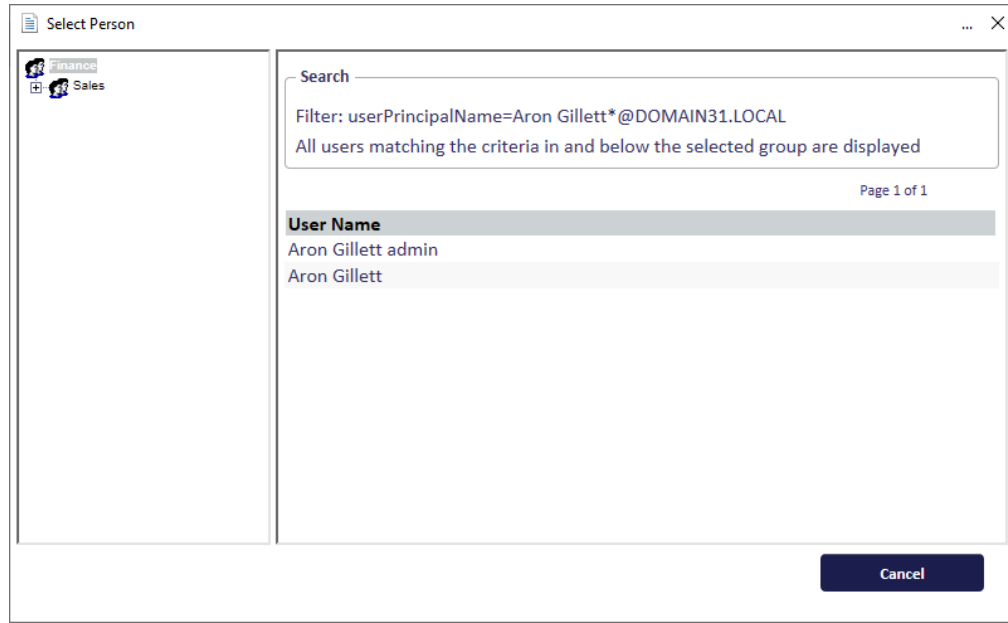
25.5 Adding an additional identity for your own account

You can use the **Manage My Additional Identities** workflow to add or remove additional identities for your own account.

Note: Alternatively, you can use the features in the MyID Operator Client to manage your alternative identities. See the *Working with additional identities* section in the **MyID Operator Client** guide for details.

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 Triggered scripts

You can configure MyID to trigger a PowerShell script at the end of selected actions; for example, collecting a card, or renewing certificates. This script runs on the client; you can write a script to provide the following information:

- The ID of the workflow that has been completed.
- The state of the workflow; that is, success or failure.
- Whether the workflow completed; for **Batch Collect Card**, the script is triggered multiple times during the workflow, once for each card that is being collected.
- The logon name of the user who is performing the action.
- The serial number of the credential being modified.
- The serial numbers of any certificates added to the credential during the workflow.
- The serial numbers of any certificates removed from the credential during the workflow.

The script is triggered by the following workflows:

- Self-Service App
 - **Activate Card**
 - **Collect My Card**
 - **Collect My Updates** (including reprovisioning)
- MyID Desktop
 - **Collect Card**
 - **Batch Collect Card**

Note: The script is triggered for each card in the batch, and again at the end of the workflow to indicate that the workflow has completed.

- **Assisted Activation**
- **Activate Card**
- **Erase Card**

26.1 Configuring triggered scripts

Once you have written the script, you must specify its location. The same script is used for all workflows; you can use the workflow ID that is passed to the script to determine what processing to carry out if you want to produce different results from different workflows.

The location of the script is relative to the client; you must either copy the script to the same location on the local drive of each client, or specify a network share that is accessible by all clients that run the script.

Note: If the client does not have access to the script, no error appears in the Self-Service App or MyID Desktop; the action fails silently. This allows you to configure some clients to run the scripts, and some clients not to run the scripts. Also, the failure to run the script is not logged; this prevents potentially personally-identifiable information from being logged.

To configure the location of the triggered script:

1. From the **Configuration** category, select **Operation Settings**.
2. On the **General** tab, set the following option:
 - **Post workflow PowerShell script** – set to the location of the script, relative to the client.

For example:

`C:\Scripts\myscript.ps1`

or:

`\\myserver\myshare\scripts\myscript.ps1`

3. Click **Save changes**.

26.1.1 Script security

It is highly recommended that the PowerShell script you intend MyID to execute is signed with a trusted code-signing certificate and that an appropriate PowerShell Execution Policy such as `AllSigned` is in place – this ensures that the script that is executed by MyID is trusted and has not been unexpectedly modified.

Note: MyID does not run PowerShell scripts in an interactive console, so your code-signing certificate must be installed as a Trusted Publisher certificate on your clients.

For more information on signing PowerShell scripts and configuring the PowerShell Execution Policy, see the Microsoft documentation.

26.2 Triggered script data format

The data passed to the script is in the form of a block of XML. You must create a script to capture this information that takes a single parameter named `MyIdData` of type `System.Xml.XmlDocument`.

The following nodes are available in the output:

- `TriggerInformation/Workflow/OperationId`

Contains the ID of the workflow that is triggering the script. The IDs are:

- **Activate Card** – 245
- **Assisted Activation** – 5007
- **Batch Collect Card** – 5003
- **Collect Card** – 5002
- **Collect My Card** – 216
- **Collect My Updates** – 242
- **Erase Card** – 296

- `TriggerInformation/Workflow/State`

Contains the status of the workflow. Can be one of the following:

- `Success`
- `Failure`

- `TriggerInformation/Workflow/IsWorkflowComplete`

Contains an indication of whether the workflow is complete. The **Batch Collect Card** workflow triggers the script after each card is collected, and again at the end of the workflow; all other workflows trigger the script only at the end of the workflow.

Can be one of the following

- `True`
- `False`
- `TriggerInformation/User/LogonName`
Contains the logon name of the user who is carrying out the workflow.
- `TriggerInformation/Device/SerialNumber`
Contains the serial number of the credential that is being modified by the workflow.
- `TriggerInformation/Device/DeviceTypeName`
Contains the type of the credential that is being modified by the workflow; for example, Oberthur ID-One PIV.
- `TriggerInformation/Device/Certificates/Added`
Contains one or more `Certificate/SerialNumber` blocks that contain the serial number of any certificates that were added to the credential during the workflow.
- `TriggerInformation/Device/Certificates/Removed`
Contains one or more `Certificate/SerialNumber` blocks that contain the serial number of any certificates that were removed from the credential during the workflow.

Note: The certificate information is available only if MyID performed the certificate actions during the workflow. For example, if you are using 2-step encoding, with a process of **Collect Card > Batch Encode Card > Activate Card**, the trigger information provided at the end of the **Collect Card** and **Activate Card** workflows does not contain certificate information; the certificate actions were carried out by the **Batch Encode Card** workflow, which does not support triggered scripts.

26.2.1 Example output

The following is an example of the XML output at the end of a workflow.

```
<TriggerInformation>
  <Workflow>
    <OperationId>216</OperationId>
    <State>Success</State>
    <IsWorkflowComplete>True</IsWorkflowComplete>
  </Workflow>
  <User>
    <LogonName>Alex Smith</LogonName>
  </User>
  <Device>
    <SerialNumber>OBERTHUR0123456789</SerialNumber>
    <DeviceTypeName>Oberthur ID-One PIV</DeviceTypeName>
    <Certificates>
      <Added>
        <Certificate>
          <SerialNumber>ABC0123456789</SerialNumber>
        </Certificate>
      </Added>
    </Certificates>
  </Device>
</TriggerInformation>
```

```

        </Certificate>
    </Added>
    <Removed>
        <Certificate>
            <SerialNumber>DEF0123456789</SerialNumber>
        </Certificate>
    </Removed>
</Certificates>
</Device>
</TriggerInformation>

```

26.2.2 Example script

The following PowerShell script reads the input XML and writes it to a file called `Log.txt`.

You can carry out further actions against the user certificate store with the information provided by these scripts; refer to Microsoft PowerShell documentation for the Certificate Provider feature.

```

param(
    [xml]$MyIdData
)

$log = "OperationID: $($MyIdData.TriggerInformation.Workflow.OperationId)"
$log = $log + "`r`n" + "WorkflowState: $($MyIdData.TriggerInformation.Workflow.State)"
$log = $log + "`r`n" + "IsWorkflowComplete: $($MyIdData.TriggerInformation.Workflow.IsWorkflowComplete)"
$log = $log + "`r`n" + "LogonName: $($MyIdData.TriggerInformation.User.LogonName)"
$log = $log + "`r`n" + "DeviceSerial: $($MyIdData.TriggerInformation.Device.SerialNumber)"
$log = $log + "`r`n" + "DeviceTypeName: $($MyIdData.TriggerInformation.Device.DeviceTypeName)"

foreach
(
    $serial
    in $MyIdData.TriggerInformation.Device.Certificates.Added.Certificate.SerialNumber)
{
    $log = $log + "`r`n" + "AddedCert: $serial"
}

foreach
(
    $serial
    in $MyIdData.TriggerInformation.Device.Certificates.Removed.Certificate.SerialNumber)
{
    $log = $log + "`r`n" + "RemovedCert: $serial"
}

Set-Content -Path .\Log.txt -Value $log

```

27 Identity checks

Many organizations apply stringent identity checking procedures before allowing credentials to be issued to their employees.

You can configure a credential profile to prevent issuance unless the person has passed their identity checks and has their user data marked as approved; see section [27.1, *User Data Approved checks*](#).

Often, policy requires that these checks are repeated at defined periods. In this case, you can use the vetting date feature in MyID to prevent the issuance of credentials when the validity period of the identity check has expired; see section [27.2, *Vetting date validity checks*](#).

This feature also prevents the renewal of certificates if the person has not passed their identity checks, or if their identity checks will expire before the expiry date or renewal date of the certificates being renewed; see section [27.3, *Certificate renewal checks*](#).

You can configure a credential profile to restrict the lifetime of certificates to the vetting date; see section [27.4, *Certificate lifetime restrictions*](#).

You can configure MyID to send identity check email notifications to administrators and end users; see section [27.5, *Configuring the identity check email notifications*](#).

27.1 User Data Approved checks

You can configure MyID to prevent issuance of credentials to people who have not passed their identity checks, or whose identity checks have expired, using the **User Data Approved** flag.

27.1.1 Configuring the credential profile

The **Require user data to be approved** option on a credential profile prevents credentials from being issued unless the user has the **User Data Approved** flag set on their account.

You can use this option to prevent a user from being issued credentials when they have not passed the required identity checks.

See section [11.3.1, *Credential profile options*](#) for details.

27.1.2 Allowing device requests before the user's data is approved

You may want to allow operators to request devices for users before their data has been approved; to do so, set the **Allow requests without user data approved** (on the **Issuance Processes** tab of the **Operation Settings** workflow) to **Yes**. This means that an operator can request a device for a user when the **Require user data to be approved** option is set on the credential profile and the user does not have the **User Data Approved** flag set on their account; note, however, that you still cannot *issue* the device until the user's data has been approved.

27.1.3 Setting the User Data Approved flag

The **User Data Approved** flag on a user record in MyID is an indicator that the user has passed all identity checks and is permitted to receive a credential. To set this flag:

- Use the `/api/People/{id}/approve` feature of the MyID Core API.

See the [MyID Core API](#) guide for details.

- Use the `UserDataApproved` node through the Lifecycle API.

See the [Lifecycle API](#) guide for details.

When you set the **User Data Approved** flag through the Lifecycle API or MyID Core API, you can also provide a `VettingDate` – see the API documentation for details.

The vetting date is used for the vetting date validity check; see section [27.2, Vetting date validity checks](#) for details.

27.2 Vetting date validity checks

If you have configured MyID to prevent issuance of credentials to users who have not passed their identity checks (see section [27.1, User Data Approved checks](#)) you may also want to configure MyID to check that these identity checks are still valid; your organization may require that checks are carried out again at defined intervals.

27.2.1 Setting the vetting date validity period

The vetting date validity period determines how long a person's identity checks remain valid. By default, this is 0; the validity check is not enforced. You can change this to a value of, for example, 2190 days – this is approximately six years, not counting leap years.

To configure the vetting date validity period:

1. From the **Configuration** category, select **Operation Settings**.
2. Click the **Identity Checks** tab.
3. Set the following option:
 - **Vetting Date Validity Period**
This is the number of days that a person's identity checks remain valid.
Setting this option to 0 disables the validity check.
4. Click **Save changes**.

27.2.2 The vetting date job processor

Once a day, the MyID server runs a job to check whether the identity check for each person in the system has expired.

- If the person does not have a vetting date set, their record is ignored.
- If the person does not have the **User Data Approved** flag set, their record is ignored.
- If the person has a vetting date set, has the **User Data Approved** flag set, and the vetting date has expired (based on the **Vetting Date Validity Period**), the following actions take place:
 - The person's **User Data Approved** flag is set to `No`.
 - A message is added to the audit.
 - If configured, an email message is sent to the administrator informing them that the person's vetting has expired and they are no longer approved for credential issuance.

See section [27.5, Configuring the identity check email notifications](#) for details.

By default the job runs for the first time on installation, and then at intervals of one day after each job run has completed. To configure the interval at which the job runs, or to change the run time, you must update the database. Contact customer support quoting reference SUP-331 for details.

27.3 Certificate renewal checks

Before MyID generates a request for a certificate renewal, it checks whether the credential profile has the **Require user data to be approved** option set; if so, MyID checks the following:

- The person who will receive the certificate renewal has their **User Data Approved** flag set to Yes.
- The certificate being renewed has a renewal date within the person's vetting date validity period. This renewal date is either the certificate's expiry date or, if set, the explicit renewal date set in the **Issued Certificates** workflow, whichever is earlier.

If either of these checks fails, MyID does not generate the certificate request; optionally, you can configure MyID to generate email notifications that inform the person that they are not permitted to receive a certificate renewal; see section [27.5, Configuring the identity check email notifications](#).

27.4 Certificate lifetime restrictions

You can set up a credential profile to restrict the lifetime of certificates to the vetting date.

If you set the **Constrain certificate lifetime to vetting date** option on the credential profile, when certificates are issued to this device, their expiry date will not exceed the vetting date of the recipient, regardless of the expiry date of the device.

See the *Issuance Settings* section.

27.5 Configuring the identity check email notifications

When the vetting date job processor finds a person whose vetting date validity check has expired, it can send an email notification to the administrator. In addition, if a certificate renewal is due, and either the person's **User Data Approved** flag is set to **No** or their vetting has expired, MyID can send an email to the person whose certificates cannot be renewed.

To enable email notifications:

1. Make sure your system is configured to send email notifications.

This involves setting up an SMTP server and switching on email notification configuration options within MyID. See section [13, Email notification](#) for details.

2. Make sure the email templates you want to use are enabled, and contain messages appropriate for your organization's users.

Use the **Email Templates** workflow to enable and edit the following templates:

- **User Vetting Date Expired** – used to inform an administrator that a person's vetting has expired. Enabled by default.

This template contains the following substitution codes that you can use in the body of the email message:

- %c1 – Full name of the person whose vetting has expired.
- %c2 – Logon name of the person whose vetting has expired.
- **Certificate Renewal Not Permitted. User Data Not Approved** – used to inform a person that they cannot renew their certificates because their **User Data Approved** flag is not set. Disabled by default.
- **Certificate Renewal Not Permitted. Vetting Expired** – used to inform a person that they cannot renew their certificates because their vetting has expired. Disabled by default.

See section [13.2, *Changing email messages*](#) for details of using the **Email Templates** workflow to enable or disable email notifications and to edit the content of the email messages.

28 Checking card suitability

You can configure MyID to call out to an external web service before collecting, updating, or activating a device, passing details of the device so that the external web service can determine whether the collection, update, or activation can proceed.

Using your own web service, you can carry out checks on the device and the cardholder to ensure that your organization's business processes have been followed before providing them with credentials for access.

For example, you may have a list of device serial numbers that should be retired; when the operator inserts the card, MyID passes the serial number to the web service, which is then checked against the list. If the device should be retired, the web service passes a response to MyID that the device is not suitable.

The process is as follows:

1. Create a web service that processes the output from MyID and returns a response.
2. Set up the details of this web service within MyID.
3. Carry out one of the following operations:
 - Collect Card
 - Batch Collect Card
 - Collect Updates
 - Assisted Activation

When you select the device to be used, MyID calls out to the external web service, and checks the response.

If the web service approves the device, the operation proceeds as usual, with no indication to the operator.

If the web service does not approve the device, the device is marked as unsuitable on screen, with a message passed from the external web service to inform the operator why the operation cannot proceed. The operator can then try a different device. The response from the web service is logged in the audit trail.

This chapter contains information on:

- Creating a web service to check card suitability.
See section [28.1, *Creating a card suitability web service*](#).
- Setting up an external system for the card suitability checking service.
See section [28.2, *Setting up an external system for card suitability*](#).
- The behavior of MyID when you are using a card suitability checking service.
See section [28.3, *Using the card suitability service*](#).

28.1 Creating a card suitability web service

Note: If you need any assistance creating a web service, contact Intercede quoting reference SUP-371.

Your card suitability web service must have a POST method called `checkCard` that can be called through the `/api` route.

28.1.1 Input for the web service

The body of this method is provided with a block of JSON in the following format:

```
{
  "serialNumber", "<serialNumber>",
  "deviceTypeName", "<deviceTypeName>",
  "userObjectID", "<userObjectID>",
  "credentialObjectID", "<credentialObjectID>"
}
```

where:

- `serialNumber` – the serial number of the card.
- `deviceTypeName` – the type of device; for example, Oberthur ID-One PIV.
- `userObjectID` – the ID of the cardholder. This corresponds to the `ObjectID` column in the `UserAccounts` table of the MyID database.
- `credentialObjectID` – the ID of the credential profile being used for the device. This corresponds to the `ObjectID` column in the `CardProfiles` table of the MyID database.

Note: The MyID database stores object IDs without the enclosing braces `{ }`.

For example:

```
{
  "serialNumber", "OBERTHUR4820502B200900025220",
  "deviceTypeName", "Oberthur ID-One PIV",
  "userObjectID", "{7E94C911-558A-4AD1-97B5-841876EA4F5A}",
  "credentialObjectID", "{5C94945D-FFA6-4B3E-B117-0436FD80BCEE}"
}
```

Your web service must use this information to determine whether the device is suitable.

28.1.2 Output from the web service

The `checkCard` method must return JSON in the following format:

```
{
  "suitable":true/false
  "error":"<error message>"
}
```

where:

- `suitable` – whether the device is suitable:
 - `true` – the device is suitable.
 - `false` – the device is not suitable.
- `error` – any additional details you want to provide to the operator.

For example:

```
{
  "suitable":false
  "error":"The card is not suitable for selection"
}
```

28.1.3 Web service authentication

You can use basic or anonymous authentication for the web service. If you use basic authentication, you must provide the username and password for the web service in the **External Systems** workflow; see section [28.2, *Setting up an external system for card suitability*](#).

28.2 Setting up an external system for card suitability

Once you have created and installed a web service to check the suitability of your devices, you must configure MyID with the details of this service using the **External Systems** workflow.

To set up an external system for card suitability:

1. From the **Configuration** category, select **External Systems**.

You can also launch this workflow from the **Connections and Notifications** section of the **More** category in the MyID Operator Client. See the *Using Connections and Notifications workflows* section in the [MyID Operator Client](#) guide for details.

2. Click **New**.

3. From the **Listener Type** drop-down list, select **CardSuitability**.

The required details of a card suitability checker web service appear.

The screenshot shows a web form for configuring an external system. The form has a title bar 'External System'. Below it, there are two rows of input fields: 'Name' and 'Description'. The 'Listener Type' is a dropdown menu currently showing 'CardSuitability'. Below that is an 'Enabled' checkbox which is checked with a green circle. A horizontal line separates the top section from the bottom section. The bottom section contains four input fields: 'Endpoint', 'User name', 'Password', and 'Confirm Password'. At the bottom of the form are three buttons: '< Back', 'Save', and 'Cancel'.


4. Complete the following details:

- **Name** – Type a name for the external system.
- **Description** – Type a description for the external system.
- **Enabled** – Select this option to enable or disable the external system. If you disable the external system, MyID does not attempt to call the card suitability check web service, and automatically allows any device to be used.
- **Endpoint** – type the URL of the web service. For example:
`https://myserver.example.com/checker/`
Note: This URL must be accessible from the MyID application server.
- **User name** – If you are using basic authentication, type the user name you configured for the web service. If you are using anonymous authentication, leave this field blank.
- **Password** – If you are using basic authentication, type and confirm the password for the account you configured for the web service. If you are using anonymous authentication, leave these fields blank.

5. Click **Save**.
6. Restart the Edefice_BOL component to ensure that MyID is working with the updated configuration.
To restart the component:
 - a. On the MyID application server, open Windows Component Services.
 - b. Expand **Component Services > Computers > My Computer > COM+ Applications**.
 - c. Right-click **Edefice_BOL**, then from the pop-up menu click **Shut down**.
The component will restart automatically the next time it is needed.
7. Recycle the MyIDWebService application pool:
 - a. On the MyID web server, in Internet Information Services (IIS) Manager, select **Application Pools**.
 - b. Right-click the **MyIDWebService** application pool, then from the pop-up menu click **Recycle**.

Important: Do not create more than one connection to a **CardSuitability** external system.

28.2.1 Enabling and disabling the card suitability check

You can disable the card suitability check by setting the **Enabled** option for the external system to No .

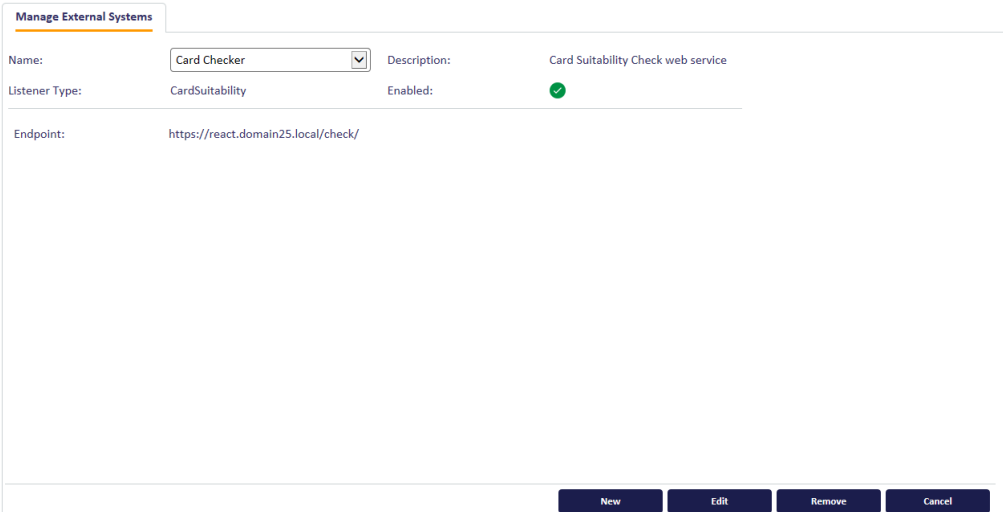
When you disable the external system, MyID does not attempt to call the card suitability check web service, and automatically allows any device to be used.


To enable or disable the card suitability check:

1. From the **Configuration** category, select **External Systems**.

You can also launch this workflow from the **Connections and Notifications** section of the **More** category in the MyID Operator Client. See the *Using Connections and Notifications workflows* section in the [MyID Operator Client](#) guide for details.

The External Systems screen appears.

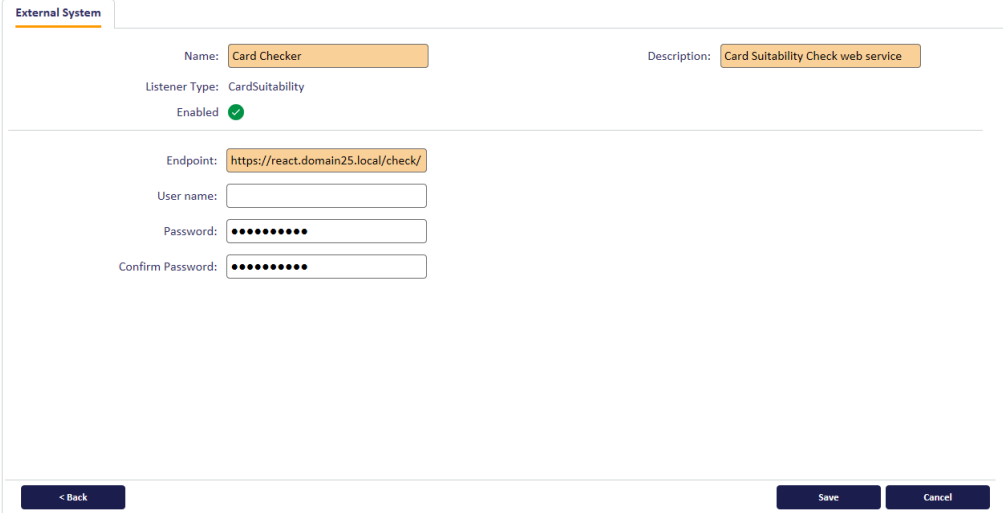


Manage External Systems			
Name:	Card Checker	Description:	Card Suitability Check web service
Listener Type:	CardSuitability	Enabled:	
Endpoint:	https://react.domain25.local/check/		

New Edit Remove Cancel

2. From the **Name** drop-down list, select the card suitability checker external system that you previously set up.
3. Click **Edit**.

The Edit External System screen appears.



4. Set the following option:
 - **Enabled** – Select this option to enable or disable the external system. If you disable the external system, MyID does not attempt to call the card suitability check web service, and automatically allows any device to be used.
5. Click **Save**.
6. Restart the Edefice_BOL component to ensure that MyID is working with the updated configuration.

To restart the component:

- a. On the MyID application server, open Windows Component Services.
- b. Expand **Component Services > Computers > My Computer > COM+ Applications**.
- c. Right-click **Edefice_BOL**, then from the pop-up menu click **Shut down**.

The component will restart automatically the next time it is needed.

Note: If you also change the value in the **Endpoint** field, you must also recycle the MyIDWebService application pool:

- a. On the MyID web server, in Internet Information Services (IIS) Manager, select **Application Pools**.
- b. Right-click the **MyIDWebService** application pool, then from the pop-up menu click **Recycle**.

28.3 Using the card suitability service

When you insert a device for use with one of the following processes:

- Collect Card
- Batch Collect Card
- Collect Updates
- Assisted Activation

MyID calls out to the card suitability check web service.

- If the check passes, you move on to the next stage transparently.
- If the check fails, MyID displays the response from the web service; for example:



The card is not suitable for selection

OBERTHUR4820502B200900025220

The card is not suitable for selection

If this occurs, you can attempt to use a different device.

- If MyID is unable to contact the web service, the message `Suitability check failure` is displayed instead:



Suitability check failure

OBERTHUR4820502B200900025220


Suitability check failure

If this occurs, you cannot proceed until you have resolved the connection problem with the web service; if necessary, you can disable the card suitability check: see section [28.2.1, *Enabling and disabling the card suitability check*](#).

- When using Batch Collect Card, if the check fails, or MyID is unable to contact the web service, the card is skipped, and the process continues with the next card. The number of failures is listed at the end of the workflow, and the failures are logged in the audit.

In addition, when you display the View Device screen in the MyID Operator Client, before MyID displays the **Collect Updates** or **Assisted Activation** buttons, MyID calls out to the card suitability check web service. If the check fails, or MyID is unable to contact the web service, MyID does not display these buttons, and an entry is written to the audit with the details.

If the card suitability check fails for any reason, or MyID cannot contact the web service, this is logged in the audit with error 9007152; for example:


View Audit

AUDIT
AUDIT DETAILS
SIGNING DETAILS
SIGNED DATA

Audit Summary

ID

9110

Operation Name

Collect Card

Audit Status

Started

Start Date Time

02/10/2023 09:33 am

End Date Time

Message

berthur ID-One PIV was detected and validated by startup. Reason: The card is not suitable for selection. Error code: 9007152.

Operator Details

Operator Logon Name

startup

Client

Operator Device SN

Unknown device

Client Identifier

FINPC-123456

Operator Device Type

IP Address

10.21.206.30

Log type

Trace

29 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.

29.1 System status report

To generate a System Status report, from the **Reports** category, select **System Status**.

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

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 section 30, *Operation Settings* and section 31, *Security Settings*).
- 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 the expiry of system credentials* 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.

29.2 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.

You can also launch this workflow from the **Additional Reporting** section of the **More** category in the MyID Operator Client. See the *Using Additional Reporting workflows* section in the [MyID Operator Client](#) guide for details.



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.

29.2.1 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 *Archiving the System Events* section in the [Advanced Configuration Guide](#) for details of setting up an archive database for these purposes

29.3 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.

29.4 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 *Securing Devices* section in 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.

30 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.

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**.

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

2. The **Operation Settings** workflow is divided into tabs containing related configuration options. Click the tab to display the options.
3. Complete the form as appropriate.

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.

4. Select **Save changes** to save the changes you have made, **Revert to Saved** to reset the settings, or **Cancel** to cancel the workflow.

30.1 General page (Operation Settings)

Setting	Allow Image Zoom
Default value	No
Description	Set this option to Yes to allow operators to expand images in read-only People workflows.
Further information	

Setting	Archive People Data
Default value	No
Description	Keeps a copy of users deleted from the main database. These deleted user accounts are stored in the <code>PeopleArchive</code> table in the database.
Further information	See for details.

Setting	Automatically Expire Web Pages
Default value	Yes
Description	Whether web pages are to expire immediately, preventing use of the back button.
Further information	

Setting	Disable Report Count
Default value	No
Description	When set to Yes, disables the retrieval of the count of records when running a report from the MyID Operator Client. This has been shown to improve the performance when working with large sets of data. When set to No, the number of records is retrieved as normal.
Further information	See the <i>Performance considerations for searching large sets of data</i> section in the MyID Operator Client guide.

Setting	Display additional error information
Default value	Yes
Description	Shows extended error details button if an error is displayed to an operator.
Further information	See section 29.3, Expanded error messages

Setting	Display pending card requests
Default value	Yes
Description	Whether pending card requests are displayed on the Devices tab in Person Details.
Further information	

Setting	Effective Revocation Immediate
Default value	Yes
Description	Whether a certificate is revoked when the CA receives the request, or when the operator revoked the certificate in MyID.
Further information	See the <i>Setting the effective revocation date</i> section in the Microsoft Windows CA Integration Guide for details.

Setting	Group Deletion Enabled
Default value	Yes
Description	Whether groups can be deleted using the Edit Groups workflow.
Further information	Cannot be edited.

Setting	Maximum certificate server restart log entries
Default value	24
Description	<p>Set this to the maximum number of log entries for certificate service failures in the past 24 hours.</p> <p>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.</p>
Further information	

Setting	Maximum person search results
Default value	100
Description	Maximum search results to return when searching for people before block paging takes place in certain workflows. Less than 200 is recommended.
Further information	Does not affect the MyID Operator Client.

Setting	One Click Selection in Find Person
Default value	Yes
Description	Whether you have to click a button after selecting a person in the Find Person screen.
Further information	

Setting	Page Timeout for Windows Clients
Default value	30
Description	Default timeout in seconds for MyID Desktop, the MyID Self-Service Kiosk, and the MyID Self-Service App.
Further information	<p>You can override the timeout for a particular installation on a client PC by editing its configuration file.</p> <p>See:</p> <ul style="list-style-type: none"> • The <i>Configuring timeouts</i> section in the Installation and Configuration Guide for MyID Desktop. • The <i>Kiosk page timeout</i> section in the Self-Service Kiosk guide. • The <i>Timeout</i> section in the Self-Service App guide.

Setting	Post workflow PowerShell script
Default value	
Description	The location of a PowerShell script that is triggered at the end of some workflows.
Further information	See section 26, Triggered scripts .

Setting	Printers have External Prox Readers
Default value	No
Description	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.
Further information	See the <i>Printers have external readers</i> section in the Operator's Guide .

Setting	SMS email notifications
Default value	No
Description	Used for collection codes and mobile identities.
Further information	See section 3.4.1, Setting up logon codes for details of configuring this option for authentication codes that allow you to log on and collect a device. See the <i>Configuring SMS and email certificate renewal notifications</i> section in the Mobile Identity Management document for details of using this option for mobile identities.

Setting	SMS gateway URL for notifications
Default value	
Description	Used for collection codes and mobile identities.
Further information	See section 3.4.1, Setting up logon codes for details of configuring this option for authentication codes that allow you to log on and collect a device. See the <i>Configuring SMS and email certificate renewal notifications</i> section in the Mobile Identity Management document for details of using this option for mobile identities.

Setting	Temporary Credential Profile Name
Default value	
Description	Used for temporary cards issued by the Self-Service Kiosk.
Further information	See the <i>Temporary credential profile</i> section in the Self-Service Kiosk guide for details.

Setting	URL path
Default value	
Description	Used to provide the location of the MyID website; for example, for bureau operations or FIDO registration messages.
Further information	See the <i>Setting the configuration options</i> section in the FIDO Authenticator Integration Guide or the bureau guide provided with your bureau for details.

Setting	Web Server External Address
Default value	
Description	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.
Further information	See the <i>Web service location</i> section in the Mobile Identity Management document for details.

Setting	Workflow Timeout Warning Delay
Default value	2
Description	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.
Further information	

30.2 Devices page (Operation Settings)

Setting	Allow Card Activation
Default value	Yes
Description	Allows you to issue cards with their keys locked so users must activate them before use.
Further information	

Setting	Allow card serial number to be entered during Request Card workflow
Default value	No
Description	Allows you to search for cards with specific serial numbers when requesting a card in MyID Desktop, or to search for devices to assign using the Assign Device (Search) feature in the MyID Operator Client.
Further information	See the <i>Requesting a card</i> section in the Operator's Guide and the <i>Assigning a device to a request</i> section in the MyID Operator Client guide.

Setting	Allow device management from the MyID user interface
Default value	No
Description	If set to Yes, you can search for computers or other devices registered in MyID during some operations.
Further information	

Setting	Allow disposal of expired devices
Default value	Yes
Description	If set to Yes, allows you to dispose of devices that have expired but not been canceled.
Further information	See the <i>Disposing of cards</i> section in the Operator's Guide .

Setting	Allow virtual smart card creation with TPM reduced functionality
Default value	No
Description	Set to Yes to allow Microsoft Virtual Smart card to be issued within MyID when the TPM is in reduced functionality state.
Further information	See the <i>Reduced functionality</i> section in the Microsoft VSC Integration Guide for details.

Setting	Auth Code Scope
Default value	Both
Description	Whether Auth Codes, when required, affect Activate, Unlock or both workflows.
Further information	

Setting	Card activation expiration period
Default value	30
Description	Not currently implemented.
Further information	This configuration option relates to custom functionality that is no longer implemented in MyID.

Setting	Card label
Default value	Yes
Description	Allows a label to be written to a card. This is an electronic label that is written to the card, not a physical label.
Further information	

Setting	Card Renewal Period
Default value	42
Description	<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>
Further information	See section 6.6.1, Credential lifetimes and certificate renewal .

Setting	Check Content Signing Certificate Expiration
Default value	Yes
Description	MyID checks that the PIV content signing certificate will not expire in the lifetime of the card.
Further information	

Setting	Default Card Data Model
Default value	PivDataModel.xml
Description	Sets the default data model to be used in a credential profile. The data model defines how the card is personalized.
Further information	

Setting	Default Card Reverse Layout
Default value	
Description	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.
Further information	

Setting	Delayed Cancellation Period
Default value	0
Description	<p>The time in hours that can be used to calculate a delay for when the original device and certificates are canceled when you replace a device.</p> <p>If the configuration option is not 0, an additional Reason appears in the list when you request a replacement: Device Replacement (Delayed Cancellation). If you select this option, the device and its certificates are not canceled immediately, but are canceled after the number of hours specified in this configuration option.</p> <p>Note: A device that is scheduled for delayed revocation can still be canceled through the actions of the Active credential profiles per person configuration option if the cardholder collects another device.</p>
Further information	See the <i>Requesting a replacement card</i> and <i>Certificate reasons</i> sections in the Operator's Guide , and the <i>Requesting a replacement device</i> section in the MyID Operator Client guide

Setting	Deliver Card Before Activation
Default value	No
Description	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.
Further information	See the <i>Delivering cards</i> section in the Operator's Guide for details.

Setting	Email Terms and Conditions
Default value	No
Description	Whether MyID emails a copy of the agreed terms and conditions to the cardholder. This feature relates to HTML-based terms and conditions templates only.
Further information	See section 11.6.7, <i>Emailing terms and conditions</i> .

Setting	Enable credentials when person is enabled
Default value	Yes
Description	If set to Yes, enabling a user account in MyID automatically enables all issued but disabled credentials belonging to that user account.
Further information	

Setting	Enable Intel Virtual Smart Card support
Default value	No
Description	Appears only on upgraded systems that previously had this option set to Yes.
Further information	MyID support for Intel Authenticate Virtual Smart Cards has now been deprecated. If you are currently using this solution or have further questions about it, contact Intercede for further details quoting SUP-349.

Setting	Expiration Identity Batch
Default value	20
Description	MyID updates the directory to remove the device certificate information when a device identity is canceled 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.
Further information	

Setting	Issue MyID Signing Keys
Default value	Ask
Description	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
Further information	See section 23.2, Terms and conditions .

Setting	Microsoft Virtual Smart Cards supported within MyID
Default value	No
Description	Set to Yes to allow the use of Microsoft Virtual Smart Cards within MyID.
Further information	See the Microsoft VSC Integration Guide for details.

Setting	Mobile Provision Via Email
Default value	Yes
Description	Set this option to allow the notification of mobile IDs to be sent to the user's email address.
Further information	

Setting	Mobile Provision Via SMS
Default value	Yes
Description	Set this option to allow the notification of mobile IDs to be sent to the user's mobile phone number.
Further information	

Setting	One Active Job Per Person
Default value	Yes
Description	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.
Further information	

Setting	One Credential Profile Request Per Person
Default value	No
Description	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.
Further information	Note: It is possible to bypass this feature if you have the Change Credential Profile At Approval configuration option set; at the approval stage, you can change the credential profile used for the request to a credential profile that has already been used to create a request for the person.

Setting	Persist terms and conditions
Default value	No
Description	<p>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.</p> <p>Note: The terms and conditions are stored in the database only if the credential profile is for configured for activation, and the cardholder accepts the terms and conditions during the device activation.</p> <p>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.</p>
Further information	See section 11.6.6, Storing signed terms and conditions .

Setting	PIV Biometric Maximum Age
Default value	12
Description	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.
Further information	

Setting	PIV Facial Biometrics Required
Default value	Yes
Description	When set to Yes, MyID checks that facial biometrics have been captured before authorizing card issuance.
Further information	

Setting	Print Quality Confirmation
Default value	No
Description	If set to Yes, allows the operator to confirm whether the card was printed correctly, and to offer an opportunity to retry the operation.
Further information	See the <i>Collecting a card</i> section in the Operator's Guide .

Setting	Secondary Serial Number
Default value	
Description	A series of field names separated by spaces which are used as a second serial number.
Further information	

Setting	Serial Number IIN
Default value	123456789
Description	Used to set the serial numbers for Oberthur PIV cards.
Further information	See the <i>Serial numbers for IDEMIA PIV cards</i> section in the Smart Card Integration Guide for details.

Setting	Terms and Conditions During Device Update
Default value	Just for New Certificates
Description	<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 new 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>
Further information	See section 23.2, Terms and conditions .

Setting	Token resync window
Default value	100
Description	The window to be used when resynchronizing an OTP device. The larger the value, the longer the resync window.
Further information	If you are having difficulty resynchronizing tokens, increase this value.

Setting	Unblocking Credential
Default value	No
Description	Whether this installation supports unblocking credentials.
Further information	See the Smart Card Integration Guide for details.

Setting	Windows Hello for Business supported within MyID
Default value	Yes
Description	Whether this installation supports Windows Hello for Business.
Further information	See the Setting the Windows Hello configuration options section in the Windows Hello for Business Integration Guide for details.

30.3 LDAP page (Operation Settings)

Setting	Additional Identity LDAP Operator User Filter
Default value	
Description	An LDAP search query that is performed to filter the results returned when you import an additional identity from the directory in the MyID Operator Client.
Further information	See section 25.2, Setting up additional identities .

Setting	Additional Identity LDAP Self-Service User Filter
Default value	
Description	<p>An LDAP search query that is performed to filter the results returned when you import an additional identity from the directory for your own account in the MyID Operator Client.</p> <p>You can include substitutions in this query using values from the <code>vPeopleUserAccounts</code> view in the MyID database; this allows you to restrict the available list of additional identities that a person can add to their own account.</p>
Further information	See section 25.2, Setting up additional identities .

Setting	Allow duplicate DN
Default value	Yes
Description	<p>Whether a user can be added if another user with the same DN already exists.</p> <p>Yes – duplicate DN values are allowed.</p> <p>No – duplicate DN values are not allowed.</p> <p>Ask – the operator is warned if a duplicate DN value is entered, but allowed to continue if required.</p>
Further information	

Setting	Allow LDAP Search for devices during Add Devices
Default value	No
Description	Set to Yes to allow an operator to add a device from the LDAP directory into the MyID database using the Add Device workflow.
Further information	

Setting	Allow LDAP Search for devices during card requests
Default value	No
Description	Set to Yes to allow an operator to add a device from the LDAP Directory into the MyID database when requesting a card.
Further information	

Setting	Assign unmatched new accounts to default directory
Default value	No
Description	When a new user account is created in MyID, the user OU may not be able to be matched to a MyID group that is linked to a directory OU; set this option to Yes to link the account to the default directory registered with MyID.
Further information	See the <i>MyID configuration options</i> section in the Derived Credentials Self-Service Request Portal guide.

Setting	Automatically create MyID groups from the Organizational Unit of imported users
Default value	Yes
Description	If you are using MyID as your primary data source, set this to Yes to automatically create MyID groups with the same names as the organizational units in the LDAP directory when importing users. Note: If you set this option to No, then move a user in the LDAP to an OU that does not have a corresponding MyID group, MyID displays a warning that the directory and the MyID database are no longer synchronized when you view the user's details in MyID.
Further information	

Setting	Background Update
Default value	No
Description	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.
Further information	

Setting	Create OU Chain
Default value	No
Description	Whether the containers in the DN of a user account pushed to an LDAP directory will be created if they do not already exist.
Further information	Cannot be edited.

Setting	Custom LDAP Mappings
Default value	No
Description	Set to Yes before you upgrade your system if you want to prevent the installation program from overwriting any custom LDAP mappings.
Further information	See the <i>Upgrading systems with custom LDAP mappings</i> section in the Installation and Configuration Guide for details.

Setting	Disable on removal from directory
Default value	Yes
Description	<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 disabled in the directory.</p>
Further information	

Setting	Display person details during confirm job
Default value	No
Description	If set to Yes , displays an additional tab on the job confirmation screen of the Collect Card workflow.
Further information	

Setting	Edit Directory Information
Default value	No
Description	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
Further information	

Setting	Edit DN
Default value	No
Description	Whether the DN for a person can be manually edited.
Further information	On new installations of MyID, this setting does not appear; by default, it appears only on systems that have been upgraded from a previous version of MyID. This setting has no effect unless you have installed an additional update to MyID that allows you to edit the Distinguished Name. For more information, contact customer support, quoting reference SUP-322.

Setting	Enable ADS Fields
Default value	Yes
Description	Whether to display the Account tab, including the User Principal Name and SAM Account Name fields, during View Person , Add Person and Edit Person . This option does not affect the MyID Operator Client.
Further information	

Setting	Force NETBIOS name
Default value	No
Description	<p>Store the user's NETBIOS name instead of the DNS name.</p> <p>If you change this to Yes, we recommend you set the Background Update option to Yes to allow existing user accounts to be updated.</p> <p>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.</p>
Further information	See section 5.6, Storing the NETBIOS name for a person .

Setting	LDAP update cancel card
Default value	
Description	Used for LDAP updates.
Further information	For more information, contact customer support, quoting reference SUP-227.

Setting	LDAP update enable card
Default value	
Description	Used for LDAP updates.
Further information	For more information, contact customer support, quoting reference SUP-227.

Setting	LDAP update exception groups
Default value	
Description	Used for LDAP updates.
Further information	For more information, contact customer support, quoting reference SUP-227.

Setting	LDAP update newissue card
Default value	
Description	Used for LDAP updates.
Further information	For more information, contact customer support, quoting reference SUP-227.

Setting	LDAP update permreplaceissue card
Default value	
Description	Used for LDAP updates.
Further information	For more information, contact customer support, quoting reference SUP-227.

Setting	LDAP update search attribute
Default value	
Description	Used for LDAP updates.
Further information	For more information, contact customer support, quoting reference SUP-227.

Setting	LDAP update tempreplaceissue card
Default value	
Description	Used for LDAP updates.
Further information	For more information, contact customer support, quoting reference SUP-227.

Setting	Link to LDAP Groups
Default value	No
Description	Allows you to link user roles to groups in the LDAP.
Further information	See section 4.4.2, Setting up linked roles for more information about linking user roles to LDAP groups.

Setting	Revoke certificates if user is removed or disabled following background directory update
Default value	Yes
Description	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.
Further information	See also section 5.5, The Batch Directory Synchronization Tool .

Setting	Search a Directory
Default value	No
Description	Whether MyID or an LDAP directory is to be searched when looking for a person. Yes – restrict the search to the directory No – restrict the search to MyID Ask – the person entering the search criteria can choose where to search
Further information	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 .

Setting	Skip Person Confirmation screen
Default value	Yes
Description	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.
Further information	

Setting	Synchronize new accounts with directory
Default value	No
Description	If this option is set to Yes , immediately after importing an unknown user MyID will attempt to pull extended details for that user from LDAP. A match will first be attempted using the DN of the certificate used to make the request. If no match is found, and the certificate contains a UPN, a second attempt will be made to match against the UPN. If both of these fail to match, no further data will be imported for the account.
Further information	See the <i>MyID configuration options</i> section in the Derived Credentials Self-Service Request Portal guide.

Setting	Track Entrust distinguished name changes
Default value	No
Description	Determines whether MyID updates Entrust with changes to the DN.
Further information	See the <i>Tracking Entrust DN changes</i> section in the Entrust CA Integration Guide for details.

Setting	Update group information in the directory
Default value	No
Description	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.
Further information	

Setting	Update user information in the directory
Default value	No
Description	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.
Further information	

30.4 Video page (Operation Settings)

Setting	File Store Location
Default value	
Description	The folder used to store images, mapped to the upimages virtual directory. Used only when storing images on the web server. Does not affect the MyID Operator Client.
Further information	See the <i>Storing images on the web server</i> section in the Operator's Guide .

Setting	HTTP Port for image upload
Default value	80
Description	The port to be used when uploading images in MyID Desktop using HTTP. Used only when storing images on the web server. Does not affect the MyID Operator Client.
Further information	See the <i>Storing images on the web server</i> section in the Operator's Guide .

Setting	HTTPS Port for image upload
Default value	443
Description	The port to be used when uploading images in MyID Desktop using HTTPS. Used only when storing images on the web server. Does not affect the MyID Operator Client.
Further information	See the <i>Storing images on the web server</i> section in the Operator's Guide .

Setting	Image Capture
Default value	Yes
Description	Whether image capture is to be used in MyID Desktop or the MyID Operator Client.
Further information	For MyID Desktop, see the <i>Changing settings for image capture</i> section in the Operator's Guide . For the MyID Operator Client, see the <i>Configuring image capture</i> section in the MyID Operator Client guide.

Setting	Image Crop Aspect Ratio
Default value	blank
Description	For the MyID Operator Client, set to the required image aspect ratio (width:height). For example, for a UK passport photo ratio, use 35:45. Does not affect MyID Desktop.
Further information	See the <i>Configuring image capture</i> section in the MyID Operator Client guide.

Setting	Image Crop Height
Default value	0
Description	<p>The height of captured images in pixels.</p> <p>In the MyID Operator Client, the MyID Image Editor displays an initial cropping rectangle. You can move and resize the cropping rectangle on the image to any position or size, automatically maintaining the aspect ratio of the specified Image Crop Height and Image Crop Width. When the MyID Image Editor uploads the resulting image to the server, it is scaled up or down to match the Image Crop Height and Image Crop Width. If Validate Image Size is not set, this option is ignored. If this option is set to 0, it is ignored.</p>
Further information	See the <i>Configuring image capture</i> section in the MyID Operator Client guide.

Setting	Image Crop Width
Default value	0
Description	<p>The width of captured images in pixels.</p> <p>In the MyID Operator Client, the MyID Image Editor displays an initial cropping rectangle. You can move and resize the cropping rectangle on the image to any position or size, automatically maintaining the aspect ratio of the specified Image Crop Height and Image Crop Width. When the MyID Image Editor uploads the resulting image to the server, it is scaled up or down to match the Image Crop Height and Image Crop Width. If Validate Image Size is not set, this option is ignored. If this option is set to 0, it is ignored.</p>
Further information	See the <i>Configuring image capture</i> section in the MyID Operator Client guide.

Setting	Image Upload Server
Default value	
Description	<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, and also for images used in the Card Layout Editor.</p> <p>This option is also required if you are using the Bureau module, even if the web services server is the same server as the web server.</p> <p>Set this option to the name or IP address of the MyID web server. Do not include <code>http</code> or <code>https</code>, any virtual directories, or any slashes – the IP address or server name are sufficient.</p> <p>If the web services server and the web server are on the same physical machine, and you are not using the Bureau module, leave this option blank.</p> <p>Does not affect the MyID Operator Client.</p>
Further information	See the <i>Setting the location of the web server</i> section in the Web Service Architecture guide.

Setting	JPEG Compression Ratio
Default value	90
Description	The compression ratio to use for any JPEG images.
Further information	<p>For MyID Desktop, see the <i>Changing settings for image capture</i> section in the Operator's Guide.</p> <p>For the MyID Operator Client, see the <i>Configuring image capture</i> section in the MyID Operator Client guide.</p>

Setting	Maintain Aspect Ratio
Default value	Yes
Description	<p>Whether aspect ratio is to be retained when resizing images.</p> <p>MyID Desktop only. Does not affect the MyID Operator Client.</p>
Further information	See the <i>Changing settings for image capture</i> section in the Operator's Guide .

Setting	Maximum Image Height
Default value	0
Description	The maximum height in pixels of an image to be displayed in the image capture control.
Further information	<p>For MyID Desktop, see the <i>Changing settings for image capture</i> section in the Operator's Guide.</p> <p>For the MyID Operator Client, see the <i>Configuring image capture</i> section in the MyID Operator Client guide.</p> <p>If this option is set to 0, it is ignored.</p>

Setting	Maximum Image Width
Default value	0
Description	The maximum width in pixels of an image to be displayed in the image capture control.
Further information	<p>For MyID Desktop, see the <i>Changing settings for image capture</i> section in the Operator's Guide.</p> <p>For the MyID Operator Client, see the <i>Configuring image capture</i> section in the MyID Operator Client guide.</p> <p>If this option is set to 0, it is ignored.</p>

Setting	Maximum Number Of Sub-Folders
Default value	0
Description	<p>The maximum number of sub-folders to be used when storing images.</p> <p>Used only when storing images on the web server.</p> <p>Does not affect the MyID Operator Client.</p>
Further information	See the <i>Storing images on the web server</i> section in the Operator's Guide .

Setting	Preload Images
Default value	No
Description	Whether images are to be preloaded by uploading them to the web server before adding the users to MyID. Does not affect the MyID Operator Client.
Further information	Note: This option is not applicable if you are storing images as binary objects in the database. See the <i>Storing images on the web server</i> section in the Operator's Guide .

Setting	Use SSL for Image Capture
Default value	Ask
Description	Determines how images are retrieved from the web server by MyID: <ul style="list-style-type: none"> • YES – MyID always attempts to retrieve images using https. • NO – MyID always attempts to retrieve images using http. • ASK – MyID attempts to retrieve images using https if the URL used to access MyID used https; otherwise, MyID uses http. Does not affect the MyID Operator Client.
Further information	If you are experiencing problems with retrieving images on your system, instead of leaving this option at the default of ASK, set the option to match your web server configuration: YES for https, or NO for http.

Setting	Validate Image Size
Default value	No
Description	Whether the size of the image is to be validated by the server. This makes sure that the images uploaded conform to the Maximum Image Height and Maximum Image Width settings.
Further information	For MyID Desktop, see the <i>Storing images on the web server</i> section in the Operator's Guide . For the MyID Operator Client, see the <i>Configuring image capture</i> section in the MyID Operator Client guide.

Setting	Video Capture
Default value	No
Description	Whether video (webcam) is to be used for capturing images in MyID Desktop. Does not affect the MyID Operator Client.
Further information	See the <i>Changing settings for image capture</i> section in the Operator's Guide .

30.5 Certificates page (Operation Settings)

Setting	Abort On Timeout
Default value	Ask
Description	Whether the issue process should be canceled if the certificate is taking so long to process that the timeout period is reached.
Further information	

Setting	Allow Collect Later
Default value	Yes
Description	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.
Further information	See the <i>Issuing certificates</i> section in the Operator's Guide .

Setting	Automated Issuance Time Limit
Default value	45
Description	The time to wait for a certificate to be issued when using an automated issuing process.
Further information	

Setting	Card Authentication Certificate ID Format
Default value	Decimal
Description	<p>Determines the format of the serial number within the DN of a certificate written to a Card Auth container on a PIV-compatible card. The default is for the numeric components to be decimal values separated by – symbols, but some legacy systems require the serial number in hexadecimal format.</p> <p>Select one of the following options:</p> <ul style="list-style-type: none"> • Decimal – this is the default. • Hex (lowercase) – the serial number is provided in lower-case hexadecimal characters. • Hex (uppercase) – the serial number is provided in upper-case hexadecimal characters.
Further information	<p>This setting affects only certificates written to the Card Auth container on a device. Note, however, that it does not affect certificates written to the Card Auth container on a mobile device, as the device must have a FASC-N, which mobile devices do not generate.</p> <p>You may experience problems if you attempt to switch between upper-case and lower-case hexadecimal serial numbers; cardholders with existing issued certificates may not obtain updated serial numbers when their device is reprovisioned. If this occurs, cancel the device, and issue it again as a new PIV credential, which ensures that the certificates are issued with serial numbers in the latest configured format.</p> <p>Note: This feature is intended for use with Entrust certificate authorities only. Also, this configuration flag is respected only when carrying out the following operations:</p> <ul style="list-style-type: none"> • Any Self-Service App operations. • Any Self-Service Kiosk operations. • MyID Desktop: <ul style="list-style-type: none"> • Activate Card • Assisted Activation • Batch Collect Card • Collect Card • Collect Updates <p>If you use any other operation that writes certificates to a device, the Card Auth certificate is issued with a decimal serial number, whatever the configured value for the Card Authentication Certificate ID Format configuration option.</p>

Setting	Cards Allowed For Derivation
Default value	
Description	A regular expression matching the ASCII value of the FASC-N for cards to determine whether you can use them to create derived credentials.
Further information	See the Derived Credentials Self-Service Request Portal for details.

Setting	Certificate Polling Refresh Time
Default value	5
Description	The number of seconds between subsequent attempts to collect certificates.
Further information	

Setting	Certificate Recovery Password Complexity
Default value	04-08N
Description	<p>Controls the complexity of the password automatically generated for PFX files. 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>
Further information	<p>This option is also used to determine the complexity of the authentication codes used for mobile device issuance. In this case, you must set the complexity to use numeric characters only; for example <code>04-08N</code> which means a code of 4 to 8 numbers.</p> <p>See the Setting the authentication code complexity section in the Mobile Identity Management guide for details.</p>

Setting	Certificate Refresh Threshold
Default value	15
Description	<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>
Further information	

Setting	Certificate Timeout For Deferred Collection
Default value	4320
Description	The number of minutes that a certificate will remain valid while waiting for collection. When this limit is reached, the certificate is revoked.
Further information	

Setting	Certificate Timeout For Issuance
Default value	20
Description	The number of minutes that a certificate will remain valid while waiting to be issued. When this limit is reached, the certificate is revoked.
Further information	

Setting	Derived credential certificate OID
Default value	2.16.840.1.101.3.2.1.3.13
Description	The OID to be checked on the PIV Authentication certificate for derived credentials.
Further information	See the Derived Credentials Self-Service Request Portal for details.

Setting	Derived Credential Revocation Check Interval
Default value	0
Description	The number of hours between repeated revocation checks of the original credentials.
Further information	Note: If you set this option to a value greater than 0, it overrides the Derived credential revocation check offset setting. See the Derived Credentials Self-Service Request Portal for details.

Setting	Derived credential revocation check offset
Default value	7
Description	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.
Further information	See the Derived Credentials Self-Service Request Portal for details.

Setting	Derived credential signing certificate OID
Default value	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
Description	A semicolon-delimited list of OIDs to be checked on the Digital Signature certificate for derived credentials.
Further information	See the Derived Credentials Self-Service Request Portal for details.

Setting	Entrust force new escrow
Default value	No
Description	When this option is set to Yes, if Entrust returns an existing escrow certificate in response to a request for a new certificate, MyID revokes the certificate and requests the new certificate again. Setting this option returns MyID to its previous behavior; you are recommended to keep this option at the default No for most systems, and set this option to Yes only if directed to by Intercede.
Further information	See the <i>Forcing the issuance of new certificates</i> section in the Entrust CA Integration Guide . Note: This option is not relevant for the Entrust CA Gateway.

Setting	iOS OTA Credential Profile
Default value	
Description	Set this option to the name of the Device Identity credential profile.
Further information	See the <i>Setting up iOS OTA provisioning</i> section in the Mobile Identity Management document for details.

Setting	iOS OTA Description
Default value	
Description	Set this option to the a description for the OTA update. This appears on the OTA provisioning message on the mobile device.
Further information	See the <i>Setting up iOS OTA provisioning</i> section in the Mobile Identity Management document for details.

Setting	iOS OTA Display Name
Default value	
Description	Set this option to a name for the OTA update. This appears on the OTA provisioning message on the mobile device.
Further information	See the <i>Setting up iOS OTA provisioning</i> section in the Mobile Identity Management document for details.

Setting	iOS OTA Organization
Default value	
Description	Set this option to the name of your organization. This appears on the OTA provisioning message on the mobile device.
Further information	See the <i>Setting up iOS OTA provisioning</i> section in the Mobile Identity Management document for details.

Setting	Limit derived credential lifetime to deriving credential
Default value	No
Description	When set to Yes, any derived credentials issued have their expiry date limited to the expiry date of the certificate used for derivation. Note: Some CAs do not allow control over the time portion of the certificate expiry. When MyID sets the lifetime of the derived credential, the date is aligned with the lifetime of the deriving certificate, but the time may not match exactly, depending on the certificate authority being used.
Further information	See the <i>MyID configuration options</i> section in the Derived Credentials Self-Service Request Portal for details.

Setting	Mask Certificate Revocation Code
Default value	No
Description	Whether certificate revocation reasons are sent to the CA. (Yes means they are not sent.)
Further information	Cannot be edited.

Setting	Maximum certificate suspensions
Default value	-1
Description	The number of times a certificate can be suspended before it is revoked. (-1 means unlimited)
Further information	

Setting	Maximum keys per card to recover
Default value	0
Description	Specifies the number of certificates to recover per card when creating key recovery jobs.
Further information	Not currently used.

Setting	Mobile Certificate Recovery Service URL
Default value	
Description	Specify the URL of the host that a mobile device must use to collect a mobile ID.
Further information	

Setting	Renew Expired Certs Via API
Default value	No
Description	Allow the renewing of expired certificates through calls to the Credential Web Service API.
Further information	See the Credential Web Service document for details.

Setting	Restrict certificate lifetimes to the card
Default value	Yes
Description	Whether the lifetimes of the certificates are restricted to the lifetime of the card. This may not be supported by all certificate authorities.
Further information	

Setting	Retry On Collection
Default value	No
Description	If a certificate timeout period has been reached, must the request be resubmitted to the CA before the certificate can be collected.
Further information	

Setting	Storage method allowed for certificate recovery
Default value	Both
Description	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
Further information	See the <i>Options for recovering soft certificates</i> section in the Operator's Guide .

Setting	Suspend to revoke period
Default value	0
Description	The time between suspension and revocation.
Further information	See section 6.4, Scheduled certificate revocation operations for more information on setting MyID to revoke suspended certificates after a given time period.

Setting	Update email address from derivation
Default value	No
Description	Whether MyID updates the user record with the email address obtained from the certificate used for derived credentials.
Further information	See the Derived Credentials Self-Service Request Portal for details.

Setting	Use Entrust default key update policy
Default value	No
Description	Whether MyID uses the Entrust CA default certificate lifetimes.
Further information	See the <i>Controlling certificate lifetimes</i> section in the Entrust CA Integration Guide . Note: This option is not relevant for the Entrust CA Gateway.

30.6 Import & Export page (Operation Settings)

Setting	File Export Directory
Default value	
Description	The folder on the application server in which files for export are created.
Further information	

Setting	File Import Directory
Default value	
Description	The folder on the application server in which files for import are placed.
Further information	Note: Changes to this setting do not take effect until you have restarted the eDB Data Import Server service.

Setting	Import Devices Sequential Range Limit
Default value	10000
Description	The maximum number of devices you can import at one time using the device import feature in the MyID Operator Client.
Further information	See the <i>Importing a range of devices</i> section in the MyID Operator Client guide.

Setting	Migrated Certificate Credential Profile
Default value	
Description	Type the name of the credential profile to be used for certificates imported against a 'dummy' device.
Further information	

Setting	Migrated Device Credential Profile
Default value	
Description	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
Further information	

Setting	Migrated Encryption Certificate Policy
Default value	
Description	Type the name of a certificate policy to be used as the associated policy for imported archived certificates.
Further information	

Setting	Migrated Non-archived Certificate Policy
Default value	
Description	Type the name of a certificate policy to be used as the associated policy for imported non-archived certificates. Used when importing operator credentials using the Lifecycle API.
Further information	See the <i>Importing operator credentials</i> section in the Lifecycle API document for details.

30.7 Identity Checks page (Operation Settings)

Setting	Enable Facial Capture
Default value	No
Description	Enables support for third-party facial capture software.
Further information	Requires additional customization. Contact your account manager to discuss your requirements.

Setting	Vetting Date Validity Period
Default value	2160
Description	This is the number of days that a person's identity checks remain valid.
Further information	See section 27.2, <i>Vetting date validity checks</i> .

The **Identity Checks** page also contains different settings based on whether you have any adjudication systems set up. See your integration guides for details.

30.8 Bureau & Job page (Operation Settings)

Setting	Automatic cancellation timeout
Default value	0
Description	Time in days after which issue card and update card jobs are canceled automatically.
Further information	See section 22.4.1, Enabling the automatic job cancellation processor.

Setting	Automatic job cancellation credential profile filter
Default value	
Description	String that must be present in the credential profile name for jobs to be canceled. Leave blank to cancel all jobs.
Further information	See section 22.4.2, Filtering the canceled jobs by credential profile.

Setting	Automatic job cancellation email
Default value	113
Description	ID of the email template sent to the target of the canceled job. Leave blank to prevent email messages from being sent when jobs are canceled. The default is the Automatic Job Cancellation Email template, with ID 113.
Further information	See section 22.4.3, Specifying the email template for notifications.

Setting	Cancel Outstanding Updates
Default value	Yes
Description	Determines how duplicate update requests for the same credential are handled. When MyID creates an update job, If this option is set to Yes, any outstanding card update, certificate renewal, or reprovision card jobs that exist for the selected credential are automatically canceled.
Further information	

Setting	Job batch maximum size
Default value	0
Description	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.
Further information	

Setting	Show Extended Job Details for Target
Default value	No
Description	Controls whether to display additional information about the target in the job details window.
Further information	

30.9 Biometrics page (Operation Settings)

Setting	Enable additional authentication options
Default value	No
Description	Allows the configuration of additional options in the Credential Profiles workflow.
Further information	See section 11.3.2, Additional credential profile options for details.

30.10 Issuance Processes page (Operation Settings)

Setting	Active credential profiles per person
Default value	One per credential group
Description	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.
Further information	See section 11.3.2, Additional credential profile options .

Setting	Allow derived credential requests to create accounts
Default value	No
Description	Must be set to Yes to allow SSRP to issue a derived credential to a cardholder whose original credential was issued by a different system. The unknown user is added to MyID.
Further information	See the <i>MyID configuration options</i> section in the Derived Credentials Self-Service Request Portal guide.

Setting	Allow parent and child credential profiles
Default value	No
Description	Used for VSCs.
Further information	See the <i>Setting up parent/child credential profiles for VSCs</i> section in the Microsoft VSC Integration Guide .

Setting	Allow requests without user data approved
Default value	No
Description	<p>Determines whether requests for credentials can be created if the person's user data approved status is not set.</p> <p>Set this option to Yes to allow an operator or the Lifecycle API to request credentials even if the person's user data approved status is not set. Even though the request can be created, if the Require user data to be approved option on the credential profile is set, the request cannot be approved or collected until the person's user data approved status is set.</p> <p>Set this value to No to prevent credentials from being requested when the person's user data approved status is not set and the Require user data to be approved option on the credential profile is set.</p>
Further information	See section 27.1, User Data Approved checks for more information.

Setting	App Download URL – ANDROID
Default value	
Description	<p>The URL for the Android version of the MyID Identity Agent.</p> <p>Leave blank to hide this option.</p> <p>If you click on a provisioning URL on a mobile device, but do not have the Identity Agent app installed, this link is displayed to allow you to download the app and try again.</p>
Further information	See the <i>Configuring SMS and email notifications</i> section in the Mobile Identity Management guide for details.

Setting	App Download URL – iOS
Default value	
Description	<p>The URL for the iOS version of the MyID Identity Agent.</p> <p>Leave blank to hide this option.</p> <p>If you click on a provisioning URL on a mobile device, but do not have the Identity Agent app installed, this link is displayed to allow you to download the app and try again.</p>
Further information	<p>See the <i>Configuring SMS and email notifications</i> section in the Mobile Identity Management guide for details.</p> <p>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.</p>

Setting	Automated Card Issuance Time Limit
Default value	240
Description	The time (in seconds) to be spent attempting to issue a card before canceling the process.
Further information	

Setting	Automated Detect Card Time Limit
Default value	40
Description	The time (in seconds) to be spent attempting to detect a card before it is rejected.
Further information	

Setting	Automated Remove Card Time Limit
Default value	30
Description	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.
Further information	

Setting	Automatic Completion of Issuance
Default value	Ask
Description	Enable the automatic submission of the Print Card stage.
Further information	

Setting	Automatic Completion of Issuance Timeout
Default value	300
Description	Timer value (in seconds) for automatically submitting certain forms.
Further information	

Setting	Automatic Update Collection
Default value	;2,245;2,255
Description	<p>If a user logs in with pending jobs, run the first workflow listed that they have access to.</p> <p>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.</p>
Further information	See the <i>Workflow IDs</i> section in the Installation and Configuration Guide for a list of the workflow IDs available in MyID.

Setting	Automatically create card update jobs when additional identities are modified
Default value	No
Description	Create card update jobs automatically on changes to additional identities.
Further information	See section 25, 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.

Setting	Batch Encode Card Timeout
Default value	15
Description	The number of seconds to allow a card to be read before timing out in the Batch Encode Card workflow.
Further information	

Setting	Change Credential Profile At Approval
Default value	No
Description	If set, an operator can change the credential profile when approving a request. Note: This affects requests approved through the MyID Operator Client only.
Further information	See the <i>Approving requests</i> section in the MyID Operator Client guide.

Setting	Display credential profile details
Default value	Ask
Description	Whether credential profile details are displayed when a card is issued.
Further information	

Setting	Enable unrestricted cancellation
Default value	No
Description	Controls whether the Unrestricted Cancellation option appears in the Issuance Settings section of the Credential Profiles workflow. This option allows you to re-use a card without first canceling it.
Further information	

Setting	Expire cards at end of day
Default value	No
Description	<p>If set, credentials will be issued with an expiry date set to the end of day, that is, 23:59:00 UTC.</p> <p>The time zone setting of the operator's workstation may affect the expiry date. Because the expiry time is 23:59:00 UTC, to ensure that the expiry time is in the future, if the operator's workstation is behind UTC (for example, PDT, which is UTC -7) the expiry is set to 23:59:00 UTC on the <i>following</i> date.</p> <p>This prevents the case where, for example, on January 1 at 20:00:00 PDT an operator requests a same-date expiry. An expiry date of 23:59:00 UTC on January 1 would be in the past, but an expiry date of 23:59:00 UTC on January 2 is still in the future.</p> <p>Note: This setting is designed for devices requested through the MyID Operator Client. Note, however, that even if the devices were requested through the MyID Operator Client, the expiry date is not set to the required value if the devices are collected through the Issue Card or Collect My Card workflows. All other methods of collecting devices work as expected.</p> <p>This setting affects requests made in MyID Desktop only under the following circumstances:</p> <ul style="list-style-type: none"> • The Expire cards at end of day option is set. • You do <i>not</i> set an explicit expiry date in Request Card. (Setting an explicit expiry date in MyID Desktop sets the time to 00:00:00 UTC.) • You do <i>not</i> collect the request using the Issue Card or Collect My Card workflows. (These workflows do not check the Expire cards at end of day option at all.) <p>Under the above circumstances, when you collect the device, the time is set to 23:59:00 UTC.</p> <p>When this option is set to the default NO, the time is set to 00:00:00 UTC (the start of the day).</p> <p>This setting also affects the <code>CardExpiryDate</code> and <code>MaxRequestExpiryDate</code> nodes in the Lifecycle API; if the Expire Cards at End of Day configuration option is set to Yes, the time portion of the expiry date is set to 23:59 UTC. If the Expire Cards at End of Day option is set to No, the time portion is set to 00:00 UTC.</p> <p>Note: This setting does not affect any existing expiry dates, whether for requests already created, or maximum credential expiry dates already set for users.</p> <p>Note: Some CAs do not allow control over the time portion of the certificate expiry. When MyID sets the lifetime of the certificate, the date is set as expected, but the time may not match exactly,</p>

	depending on the certificate authority being used.
Further information	See the <code>CardExpiryDate</code> and <code>MaxRequestExpiryDate</code> sections in the Lifecycle API document, the <i>Setting expiry dates for a card</i> section in the Operator's Guide , and the <i>Approving requests</i> section in the MyID Operator Client guide.

Setting	Manual Card Update
Default value	No
Description	Whether a card update can be performed manually. This allows you to select which updates to apply to the card from the list of available updates.
Further information	

Setting	Maximum multiple credential requests
Default value	1
Description	This is the maximum number of multiple credential requests that will be accepted.
Further information	See the <i>Requesting multiple cards</i> section in the Operator's Guide .

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

Setting	Output Mechanism for Job Challenge Code Generation
Default value	Choose at request
Description	Determines how the one-time password for job authentication is delivered. Choose one of the following: Email Display on screen Both Choose at request
Further information	See section 24.8, Requesting a device identity .

Setting	Print Card Timeout
Default value	5
Description	The number of seconds between printing a card and issuing.
Further information	

Setting	Printer Request Buffer Delay
Default value	10
Description	This is the time in seconds to pause between sending requests to the printer.
Further information	Used with the Fargo SDK for Fargo printers.

Setting	Reload Device Profile
Default value	No
Description	Whether the device profile is reloaded onto the card during issuance. Used for Thales authentication devices.
Further information	

Setting	Requisite User Data
Default value	No
Description	Displays an extra option in the Credential Profiles workflow that allows you to restrict issuance to user accounts with specific user attribute mappings.
Further information	

Setting	Restrict collection of replacement devices if expiry date within (Days)
Default value	0
Description	Stops the issuance of a replacement credential if the date for the expiry is within the specified number of days.
Further information	

Setting	Rotate Keys On Card Update
Default value	No
Description	When a card update is collected, any GlobalPlatform or PIV 9B keys associated with the device will also be updated if they are found to be out of date.
Further information	See section 7.3.8, Rotating customer keys for details.

Setting	Set Credential Profile On Renewal
Default value	No
Description	If set to Yes, the operator can specify a credential profile when renewing a device. Note: This setting affects devices renewed through the MyID Operator Client only.
Further information	

Setting	Set expiry date at request
Default value	No
Description	If set to Yes, the operator can specify a date for expiry of credentials when they are requested. Note: This setting affects the MyID Operator Client and MyID Desktop only. Requests created using APIs directly are not affected.
Further information	

Setting	Show Disqualified Credential Profiles
Default value	Yes
Description	Set to Yes to display all credential profiles, whether or not they meet the Requisite User Data requirements. Set to No to hide any credential profiles that do not meet the Requisite User Data requirements. Note: This setting affects the display of credential profiles in the MyID Operator Client only.
Further information	See section 11.3.1.11 , <i>Requisite User Data</i> .

Setting	Show the Card Content button in the Audit Workflow
Default value	Yes
Description	Set to Yes to display the Card Content button on the Audit workflow.
Further information	

30.11 Notifications page (Operation Settings)

Setting	Administration Email
Default value	
Description	Email address of the administrator to be sent email notification messages.
Further information	See section 13.1.5 , <i>Changing the recipient of administrator messages</i>

Setting	Database Mail Profile Name
Default value	Default CMS
Description	The email address or profile name to be used as the sender of email notifications.
Further information	Required only for legacy systems still using SQL Server Database Mail. This configuration option does not appear on new installations of MyID. See <i>Upgrading email support</i> section in the Installation and Configuration Guide for details.

Setting	Email separator
Default value	;
Description	Allows you to specify the separator used to divide multiple email addresses when sending email messages.
Further information	See section 13.1.4, Email separator for details.

Setting	Expiration Notification Period
Default value	28
Description	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.
Further information	

Setting	Issuance Notification URL
Default value	
Description	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.
Further information	

Setting	Mail Format
Default value	HTML
Description	The format of SMTP email notification messages. This can be TEXT or HTML.
Further information	See section 13.1.2, Email format .

Setting	Notification Proxy URL
Default value	
Description	No longer used. This option was previously used to specify the location of a redirection web page that MyID would use to send notifications to external systems.
Further information	

Setting	Send Email Notifications
Default value	No
Description	Global setting to determine whether notification email messages are sent.
Further information	See section 13.1.1, Switching email notifications on or off .

Setting	Send Mobile OTP via SMS
Default value	No
Description	Set this option to allow the operator to send the OTP authentication code directly to the mobile device.
Further information	See the <i>Configuring SMS and email notifications</i> section in the Mobile Identity Management document for details.

Setting	Show License Info to All Operators
Default value	Yes
Description	When set to Yes , displays the license expiry warning to all users. When set to No , displays the license expiry warning to users only if they have access to the Licensing workflow.
Further information	See section 12, License management for details.

Setting	Single Email Notification
Default value	Yes
Description	Allows you to specify whether users receive multiple email messages when several certificates are being renewed.
Further information	See section 13.1.6, Setting the number of email notifications .

30.12 Identity Agent Policy page (Operation Settings)

Setting	Administrator email address
Default value	
Description	Set this to the email address to which Identity Agent will send logs for troubleshooting purposes.
Further information	

Setting	Log level
Default value	Error
Description	Set this to the level of logging you want Identity Agent to produce. Higher levels result in more detail, but larger files. Set to one of the following: 0 – NONE 1 – FATAL 2 – ERROR 3 – WARNING 4 – INFO 5 – DEBUG 6 – VERBOSE
Further information	

Setting	Maximum log storage space
Default value	20
Description	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.
Further information	

Setting	Maximum number of log files
Default value	-1
Description	<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>
Further information	

Setting	Maximum retry attempts
Default value	5
Description	The maximum number of times Identity Agent should attempt to reconnect to the server if connection is lost during an operation.
Further information	

Setting	Maximum session count
Default value	-1
Description	<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>
Further information	

Setting	Minimum retry delay
Default value	10
Description	The minimum delay, in seconds, between each attempt to contact the server after connection has been lost.
Further information	

31 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.

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 **Security Settings**.

You can also launch this workflow from the **Configuration Settings** section of the **More** category in the MyID Operator Client. See the *Using Configuration Settings workflows* section in the [MyID Operator Client](#) guide for details.

2. The **Security Settings** workflow is divided into tabs containing related configuration options. Click the tab to display the options.
3. Complete the form as appropriate.

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.

4. Select **Save changes** to save the changes you have made, **Revert to Saved** to reset the settings, or **Cancel** to cancel the workflow.

31.1 Logon page (Security Settings)

Setting	Allow Logon Codes
Default value	No
Description	Enables logon codes. Used as a global setting for all credential profiles – to use logon codes, you must set this option to Yes and set the Generate Code on Request option in the credential profile.
Further information	See section 3.4, Logon using codes for details.

Setting	Allow Self-Service at Logon
Default value	Yes
Description	Determines whether the Manage My Credentials option appears on the MyID Authentication screen in the MyID Operator Client.
Further information	See the <i>Managing your credentials from the MyID Authentication screen</i> section in the MyID Operator Client guide.

Setting	Client Signing
Default value	Yes (Software or Card if available)
Description	<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>
Further information	

Setting	Logon Name Required
Default value	No
Description	Whether the logon name associated with the MyID account is used in addition to the password when logging on to MyID.
Further information	No longer supported. Will appear only on upgraded systems, but has no effect.

Setting	Maximum Allowed OTP Failures
Default value	5
Description	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.
Further information	

Setting	Maximum allowed security question failures
Default value	3
Description	Specify the maximum number of failed attempts a user can make when attempting to answer a security question or enter a logon code. When this number is exceeded, the user's account can be locked out – see the Action on maximum security question failures option in section 31.4, PINs page (Security Settings) .
Further information	Note: If you set this option to 0, the default value of 3 is used and the user's account is locked when three attempts have been made without success. For information on unlocking security phrases, see section 3.3.5, Unlocking security phrases and section 3.3.6, Unlocking your own security phrases .

Setting	Prevent Direct Password Logon
Default value	No
Description	Allow password logon for self-service operations only when a card is present.
Further information	

Setting	Set Security Phrase at Logon
Default value	
Description	<p>If a user logs into MyID Desktop and the required number of security phrases (as specified by the Number of security questions to register configuration option) 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>
Further information	<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. This option does not affect the logon process when using the MyID Operator Client.</p>

Setting	Show Full Name at Logon
Default value	No
Description	<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 No, and either you have the Show Photo at Logon set to No, or the users do not have photos attached to their user accounts, if you insert more than one card you will not be able to tell which card belongs to which user except by the card serial number and device type (which is available when you hover your mouse over the image).</p>
Further information	<p>This option affects both MyID Desktop and the MyID Operator Client.</p> <p>Note: If you enable this feature, it is possible to obtain cardholder names without authentication.</p>

Setting	Show Photo at Logon
Default value	No
Description	Whether the holder's photograph is displayed at logon.
Further information	<p>This option affects both MyID Desktop and the MyID Operator Client.</p> <p>Note: If you enable this feature, it is possible to obtain user photos without authentication.</p>

Setting	Signed Logon
Default value	Yes
Description	Whether the information passed to the server during logon is signed using the keys or certificate stored on the card.
Further information	

Setting	Validate logon certificate
Default value	No
Description	<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 service for certificate validation, the authentication service is used to validate the certificate after MyID as secondary validation.</p>
Further information	Note: The application server must trust the Certificate Authority that issued the certificate being validated.

31.2 Device Security page (Security Settings)

Setting	Display warnings for unsecured issuance
Default value	Yes
Description	Displays a warning on the login screen if the system is not securely configured and an attempt is made to issue credentials.
Further information	Review the System Security Checklist before disabling this option, and ensure that your system is configured appropriately according to the guidance provided and your own security policy. See the <i>Securing Devices</i> section in the System Security Checklist guide for details.

Setting	Enable Customer GlobalPlatform Keys
Default value	Yes
Description	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.
Further information	See section 7.2, Enabling GlobalPlatform keys .

Setting	Manage PIV 9E key on supported devices
Default value	No
Description	<p>Updates the PIV 9E Key, if it is supported by the device. The card symmetric 9E key is diversified from the 9B Master Key, and is changed to the customer master key during card issuance, and using the factory master key when the card is erased.</p> <p>Set this option to Yes to update the PIV 9E key on supported devices during issuance and erasure. Set this option to No to prevent any attempt to update the PIV 9E key on issuance or erasure.</p>
Further information	

Setting	Require Random Security Officer PIN
Default value	Yes
Description	If this is set to Yes but the Security Officer PIN Type is set to Factory , cards cannot be issued.
Further information	

Setting	Security Officer PIN Type
Default value	Random
Description	<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>
Further information	

Setting	Show all devices
Default value	No
Description	<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>
Further information	

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 29.4, *System security* for more information.

The *Securing Devices* section in the *System Security Checklist* document contains important information on securing your system.

31.3 Server page (Security Settings)

Setting	Allow envelope version 1.2
Default value	No
Description	Whether MyID supports clients using the older method of securing data between clients and the MyID server.
Further information	<p>This option may be required for some older clients and web services. See the <i>Supporting older clients</i> section in the <i>Installation and Configuration Guide</i> for details.</p> <p>Note: Do not deselect both Allow envelope version 1.2 and Allow envelope version 1.3 or you will be locked out of MyID.</p> <p>If this happens, contact customers support, quoting reference SUP-140.</p>

Setting	Allow envelope version 1.3
Default value	Yes
Description	<p>Whether MyID supports clients using the newer method of securing data between clients and the MyID server.</p> <p>This option may not be supported on older clients.</p>
Further information	See the <i>Supporting older clients</i> section in the <i>Installation and Configuration Guide</i> for details.

Setting	Allow Legacy Data Models
Default value	No
Description	<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>
Further information	

Setting	Capture Client Identifier
Default value	Yes
Description	Whether the identifier of the client workstation (by default, the fully-qualified domain name) is captured in the audit trail.
Further information	See section 17.2.3, Logging the client IP address and identifier .

Setting	Capture IP Address
Default value	Yes
Description	Whether the IP address of the client workstation is captured in the audit trail.
Further information	See section 17.2.3, Logging the client IP address and identifier .

Setting	Envelope Transport Key Algorithm
Default value	AES256 – on new installations 3DES – on upgraded systems
Description	Specifies the algorithm used to protect low level processes; for example, secure communication between MyID clients and servers. AES encryption is used for new MyID installations, while 3DES is used for upgraded systems to provide compatibility with older MyID clients.
Further information	<p>You can configure MyID to continue to use 3DES where technical constraints require this, or if you need to use MyID clients that were provided with a release earlier than MyID 12.6.</p> <p>Additionally, if you are issuing mobile identities using the following versions of the mobile apps (or earlier):</p> <ul style="list-style-type: none"> • iOS <ul style="list-style-type: none"> • MyID Identity Agent v4.2 • MyID Authenticator v1.5 • Android <ul style="list-style-type: none"> • MyID Identity Agent v4.1.2813 • MyID Authenticator v1.4.171 <p>you must set this configuration option to 3DES; a later update for these mobile apps will provide support for AES.</p> <p>Apps developed using Identity Agent Framework version 3.9 or later, which use the rest.provision provisioning API, can support AES; for apps developed using earlier versions, set the option to 3DES.</p> <p>The MyID Wallet app for mobile identity documents, which uses the rest.provision API, supports AES.</p>

Setting	SCEP Hash Algorithm
Default value	SHA256
Description	<p>The hash algorithm used for SCEP requests. Can be one of the following:</p> <ul style="list-style-type: none"> • SHA1 • SHA256
Further information	See section 24.4.1, Signing certificate for details.

Setting	Server Encryption
Default value	Software based only
Description	<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>
Further information	Cannot be edited. Contact customer support for details.

Setting	Store Secret Keys
Default value	Yes
Description	Whether secret (symmetric) keys can be stored in the MyID database, encrypted using the MyID 3DES key.
Further information	Cannot be edited. Contact customer support for details.

Setting	Validate signing certificates
Default value	No
Description	<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 service for certificate validation, the authentication service is used to validate the certificate after MyID as secondary validation.</p>
Further information	<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>

31.4 PINs page (Security Settings)

Setting	Action on maximum security question failures
Default value	Lock security phrases
Description	Determines what happens when a user has reached the Maximum allowed security question failures – see section 31.1, Logon page (Security Settings) . This can be one of the following: Lock security phrases – The user's account is locked. None – The user can retry as many times as they like.
Further information	

Setting	Ask Security Questions for Self Service Card Unlock
Default value	No
Description	Whether the holder's security phrase is used when unlocking a card.
Further information	See the <i>Self-service PIN reset authentication</i> section in the Operator's Guide .

Setting	Case sensitive security questions
Default value	Yes
Description	Whether the case of responses to security phrases or logon codes is checked when authenticating.
Further information	Important: See section 3.3.2, Changing rules for security phrases . For logon codes, if you set this option to No, make sure that you have not included <code>l</code> or <code>1</code> (must/may contain lower case letters) in your logon code complexity format; otherwise, you will be unable to use the generated codes. Use a code like <code>12-12USN</code> instead.

Setting	Default max PIN length
Default value	12
Description	The default maximum PIN length. You can override this setting in the credential profile using the Maximum PIN length option.
Further information	See section 11.3.1, Credential profile options .

Setting	FIDO Immediate Collect Timeout
Default value	120
Description	The number of seconds before timeout when performing immediate FIDO registration through the Self-Service Request Portal.
Further information	See the <i>Registering FIDO authenticators using the Self-Service Request Portal</i> section in the FIDO Authenticator Integration Guide .

Setting	Lock Card on Issuance
Default value	Ask
Description	Whether the PIN assigned during issue is locked. If so, the holder must enter a new PIN on first use.
Further information	See section 11.3.1, Credential profile options .

Setting	Number of security questions for operator authentication
Default value	1
Description	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.
Further information	See section 3.3.3, Setting the number of security phrases required to authenticate .

Setting	Number of security questions for self-service authentication
Default value	2
Description	The number of security phrases users are required to provide when authenticating themselves.
Further information	See section 3.3.3, Setting the number of security phrases required to authenticate .

Setting	Number of security questions to register
Default value	2
Description	The number of security phrases to enroll for a user in the Change Security Phrases or Change My Security Phrases workflows.
Further information	See section 3.3.3, Setting the number of security phrases required to authenticate .

Setting	Offline Unlock Method
Default value	Challenge
Description	<p>Challenge – a dialogue between the holder and the helpdesk, passing challenges and responses to identify the holder and the device.</p> <p>Witness – another holder must witness the request.</p> <p>None – offline unlocking not possible.</p>
Further information	Used for Giesecke & Devrient cards.

Setting	PIN Timeout
Default value	180
Description	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.
Further information	

Setting	Prevent version 1 password enrollment
Default value	No
Description	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.
Further information	

Setting	Reload Device Profile
Default value	Yes
Description	No longer used. Previously, this setting forced MyID to reload the device profile onto the card during issuance.
Further information	Appears only on upgraded systems.

Setting	Remote Unlock requires an Authentication Code prompt
Default value	No
Description	No longer required. Previously, if set to Yes , the user had to provide an authentication code to remotely unlock a card or device.
Further information	Appears only on upgraded systems. See the <i>Unlocking a credential remotely</i> section in the Operator's Guide for details of configuring MyID for remote unlock.

Setting	Security Phrase allowable characters
Default value	
Description	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.
Further information	Note: a-z and A-Z do not include accented characters. If required, these must be specified individually.

Setting	Security Phrase complexity format
Default value	
Description	Defines the rules for allowed security phrases. Leave blank to allow any format.
Further information	See section 3.3.1, Setting rules for security phrases for detailed instructions.

Setting	Security Phrase minimum length
Default value	0
Description	The minimum number of characters accepted for a security phrase. Set to 0 to allow any security phrases with one or more characters.
Further information	

Setting	Security Phrase repeat character limit
Default value	0
Description	The maximum number of repeated characters accepted in security phrases. 0 allows any number of repeated characters.
Further information	

Setting	Security Phrase sequential character limit
Default value	0
Description	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.
Further information	

Setting	Security Phrase whitespace removal
Default value	No
Description	Set to <code>Yes</code> to remove any spaces from security phrases before storing or checking the security phrase.
Further information	Important: See section 3.3.2, <i>Changing rules for security phrases</i> .

Setting	Set GlobalPlatform Card Status
Default value	No
Description	<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 the Smart Card Integration Guide for whether you need to set this option.</p>
Further information	

Setting	Show Generated PINs
Default value	Yes
Description	Whether the PIN for a device (when this is a random or server-generated PIN) should be displayed when the device is issued.
Further information	Only the Issue Card workflow can display generated PINs. Other issuance workflows will not display the user PIN that has been generated.

Setting	Transport PIN
Default value	12549856
Description	Default PIN for canceled cards. If you are using on-device PIN policies, you must set the transport PIN to match the PIN policy in the card properties file.
Further information	

Setting	Use logon name for server PIN generation
Default value	No
Description	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.
Further information	See section 9.3 , <i>EdeficePinGenerator PIN generation algorithm</i> for details.

Setting	Use PIN policy settings in random server PIN generation
Default value	No
Description	When set to No, the random PIN generator does not take into account the PIN policy determined by the credential profile. When set to Yes, the random PIN generator takes into account the PIN policy determined by the credential profile.
Further information	See section 9 , <i>PIN generation</i> for details.

Setting	Use Security Phrase algorithm version 2
Default value	Ask
Description	If you are upgrading from a previous system, and this option was previously set to No, this is set to Yes by the installer. This option is used to configure MyID to set security phrases to use SHA256 hashing.
Further information	See the <i>Upgrading security phrase security</i> in the Installation and Configuration Guide for details of upgrading the hashed security phrase answers stored in the MyID database.

31.5 Process page (Security Settings)

Setting	Allow Administrative Groups
Default value	No
Description	<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>
Further information	See section 4.7, Administrative groups for details.

Setting	Approve Replacement Cards
Default value	No
Description	<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 only if this option is set to Ask.</p>
Further information	

Setting	Block VSC unlock in Remote Unlock workflow
Default value	No
Description	Prevents an operator from using the Remote Unlock workflow to unlock VSCs.
Further information	

Setting	Card Expiration Period (days)
Default value	365
Description	Default period for which all issued devices are valid.
Further information	See section 11.3.1, Credential profile options .

Setting	Client Logon Keyset
Default value	Signing
Description	Which keyset to use when signing data on the client during logon.
Further information	Cannot be edited.

Setting	Client Sign Keyset
Default value	Signing
Description	Which keyset to use when signing data on the client.
Further information	Cannot be edited.

Setting	Constrain Credential Profile Collector
Default value	Yes (if on installation there were no existing credential profiles) or: No (if on installation there were existing credential profiles).
Description	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 .
Further information	See section 11.3.8, Constrain credential profile collector for details.

Setting	Constrain Credential Profile Issuer
Default value	Yes (if on installation there were no existing credential profiles) or: No (if on installation there were existing credential profiles).
Description	Whether you can select which roles can request individual credential profiles on the Select Roles screen in the Credential Profiles workflow.
Further information	See section 11.3.6, <i>Constrain credential profile issuer</i> for details.

Setting	Constrain Credential Profile Unlock Operator
Default value	No
Description	Whether you can select which roles can unlock credentials using the Unlock Credential and Reset Card PIN workflows.
Further information	See section 11.3.9, <i>Constrain credential profile unlock operator</i> for details.

Setting	Constrain Credential Profile Validator
Default value	Yes
Description	Whether you can select which roles can validate individual requests using the selected credential profile.
Further information	See section 11.3.7, <i>Constrain credential profile validator</i> for details.

Setting	Restrict Roles on Child Groups
Default value	No
Description	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.
Further information	See section 4.2, <i>Role inheritance</i> .

Setting	Show Audit Summary
Default value	Ask
Description	Whether a summary of the audit information is displayed on completion of a workflow.
Further information	

Setting	Show Set Security Phrases Button
Default value	Yes
Description	Displays a link to the Change Security Phrases workflow at the end of Add Person .
Further information	

Setting	Sign Audit on Client
Default value	No
Description	Whether audit data from client is signed on the client.
Further information	Cannot be edited.

Setting	Sign Audit on Server
Default value	Yes
Description	Whether Audit Trail information is signed on the server.
Further information	Cannot be edited.

Setting	Task Number Timeout
Default value	30
Description	<p>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.</p> <p>This setting was previously stored in the <code>DatabaseVersion</code> table in the MyID database.</p>
Further information	

31.6 Self-Service page (Security Settings)

Setting	Allow self requests
Default value	No
Description	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.
Further information	

Setting	Auto-enroll from directory
Default value	No
Description	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.
Further information	Cannot be edited.

Setting	Restrict Self Activation
Default value	No
Description	When set to <code>Yes</code> , you have access to the operations allowed by the Activation User role <i>only</i> if these operations are already permitted by your assigned roles; when set to <code>No</code> , you have access to <i>all</i> operations allowed by the Activation User role, whether or not your own assigned roles provide access.
Further information	See section 23.1 , <i>Configuring a credential profile for activation</i> .

Setting	Self-service
Default value	Yes
Description	This option determines whether users can edit their own device details or perform updates to devices that belong to them; for example, to cancel a device.
Further information	Cannot be edited.

Setting	Self-service emergency password
Default value	Yes
Description	Someone with a MyID account can set a temporary password for own use with authentication services.
Further information	Cannot be edited.

Setting	Self-service Resynchronization
Default value	Yes
Description	This option determines whether users can resynchronize their own cards.
Further information	Cannot be edited.

Setting	Self-service Unlock
Default value	Yes
Description	This option determines whether holders can unlock their own devices.
Further information	

Setting	Unknown card logon
Default value	No
Description	Whether an unknown device can be used to self-enroll.
Further information	Cannot be edited.

31.7 Logon Mechanisms page (Security Settings)

Setting	Password Logon
Default value	Yes
Description	Whether users can log on to MyID with their security phrases.
Further information	See section 3.3, Logon using security phrases .

Setting	Smart Card Logon
Default value	Yes
Description	Whether users can log on to MyID with their issued smart cards.
Further information	See section 3.2, Logon using a smart card and PIN .

Setting	Token Logon
Default value	No
Description	Whether users can log on to MyID with their issued one time password tokens.
Further information	Not used in this version of MyID.

Setting	Integrated Windows Logon
Default value	No
Description	Whether users can log on to MyID using integrated Windows logon.
Further information	See section 3.6, Integrated Windows Logon .

Setting	Biometric Logon
Default value	Yes
Description	Whether users can log on to MyID using biometrics. Currently used only for resetting PINs.
Further information	See the <i>Self-service PIN reset authentication</i> section in the Operator's Guide .

Setting	Client Credentials OAuth2 Logon
Default value	No
Description	Enables the use of OAuth2 client credential grant, which is used for server to server authentication for APIs.
Further information	See the <i>Configuring MyID for server-to-server authentication</i> section in the MyID Core API guide for details.

Setting	Windows Hello Logon
Default value	No
Description	Whether users can log on to MyID using their Windows Hello credentials.
Further information	See the <i>Setting up Windows Hello for logon</i> section in the Windows Hello for Business Integration Guide for details.

Setting	FIDO Basic Assurance Logon
Default value	No
Description	Whether users can log on to the MyID Operator Client using a FIDO authenticator that has been issued with a credential profile where the Assurance Level is set to Basic .
Further information	See the <i>Setting the FIDO logon configuration options</i> section in the FIDO Authenticator Integration Guide for details.

Setting	FIDO High Assurance Logon
Default value	No
Description	Whether users can log on to the MyID Operator Client using a FIDO authenticator that has been issued with a credential profile where the Assurance Level is set to High .
Further information	See the <i>Setting the FIDO logon configuration options</i> section in the FIDO Authenticator Integration Guide for details.

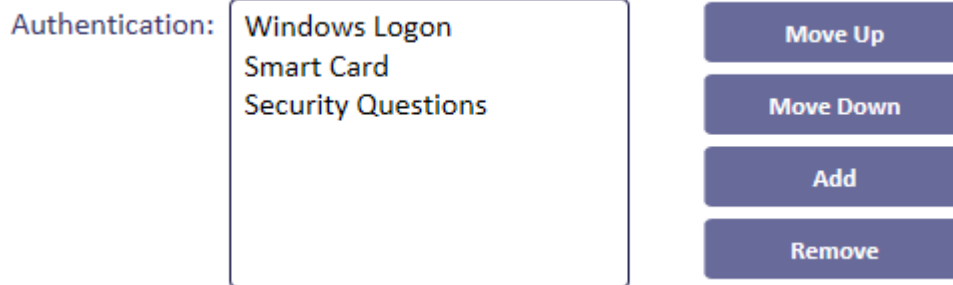
Setting	Authentication Code Logon
Default value	No
Description	Whether users can log on to the MyID Operator Client using a single-use authentication code.
Further information	See section 3.5, Logon using authentication codes .

31.8 Logon Priority page (Security Settings)

The **Logon Priority** page allows you to configure the order in which different logon mechanisms are presented to the user in the Self-Service App; for example, you may want your users to authenticate with a smart card first, and if that fails, to authenticate with security questions.

When the user is presented with a method of authentication, they can decline the option (for example, when presented with a smart card authentication screen, they can click the "I cannot authenticate with my device" option) and proceed to the next available logon mechanism.

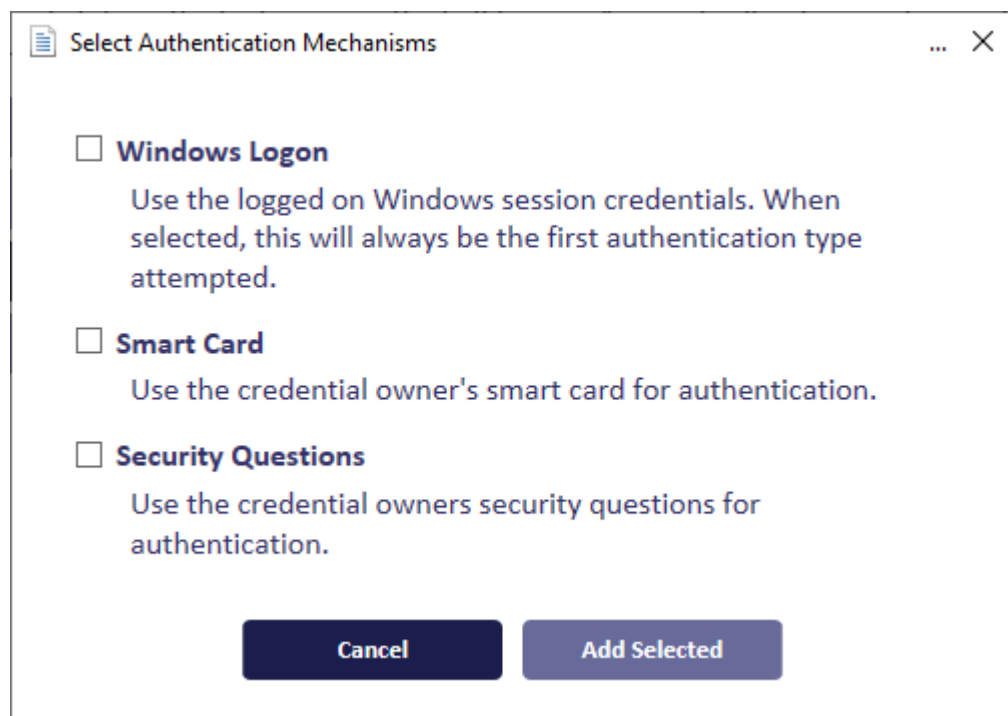
For information on which Self-Service App actions support this feature, see the *Authentication* section in the [Self-Service App](#) guide. Depending on the action used, other authentication considerations may take priority.



- To change the order, select the logon mechanism and click **Move Up** or **Move Down**.

Note: If you have **Windows Logon** in your list, it stays at the top of the list – Windows authentication is carried out before any interactive authentication methods. If Windows authentication is successful, the user starts the action; if it is unsuccessful, the user is presented with the next logon mechanism in the list.

- To remove an option, select the logon mechanism and click **Remove**.
- To add options, click **Add**:



Select one or more options, then click **Add Selected**.

Note: Logon mechanisms in MyID Desktop and the Self-Service Kiosk are not affected by this configuration.

31.9 Auth Code page (Security Settings)

Setting	Auth Code Complexity
Default value	Complex
Description	<p>Determines the complexity setting of the auth code, if the complexity was not determined by the email template or (for job collection codes only) the credential profile; for example, when sending a job collection code for a device based on a credential profile that did not have the Generate Code on Request option set, or when viewing an unlock code on screen.</p> <p>Can be one of the following options:</p> <ul style="list-style-type: none"> • Complex – uses the complexity determined by the Complex Logon Code Complexity configuration option. This is the default. • Simple – uses the complexity determined by the Simple Logon Code Complexity configuration option.
Further information	See section 3.4.1, Setting up logon codes .

Setting	Auth Code Lifetime
Default value	720
Description	The number of hours for which an authentication code is valid for activating or unlocking. To set authentication codes for no expiry, set this value to 0.
Further information	<p>See the <i>Requesting an authentication code</i> section in the Operator's Guide or the <i>Sending an authentication code to activate a device</i> section in the MyID Operator Client guide.</p> <p>See the <i>Unlocking a device</i> section in the MyID Operator Client guide for details of configuring and using authentication codes for unlocking.</p>

Setting	Auth Code Lifetime for Immediate Use
Default value	120
Description	The number of seconds for which a short lifetime authentication code is valid for activating a device, logging on to collect a job, unlocking a device, or logging on to the MyID Operator Client. To set short lifetime authentication codes for no expiry, set this value to 0.
Further information	<p>See section 3.5, Logon using authentication codes and the <i>Signing in using single-use authentication codes</i> section in the MyID Operator Client guide for details of requesting and using authentication codes for logging on to the MyID Operator Client.</p> <p>See the <i>Sending an authentication code to activate a device</i> section in the MyID Operator Client guide for details of configuring and using authentication codes for activation.</p> <p>See section 3.4.1, Setting up logon codes and the <i>Sending a collection code</i> section in the MyID Operator Client guide for details of configuring and using authentication codes for collection.</p> <p>See the <i>Unlocking a device</i> section in the MyID Operator Client guide for details of configuring and using authentication codes for unlocking.</p>

Setting	Complex Logon Code Complexity
Default value	12-12ULSN[BGI1OQDSZ]
Description	<p>The complexity rule used to generate a logon code when the Generate Code on Request option in the credential profile is set to Complex Logon Code, or the Complexity option in the email template or the Auth Code Complexity configuration option is set to Complex.</p> <p>It takes the format <code>mm-nnULSN[excluded characters]</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> <p>You can specify any characters you want to exclude because they are difficult to distinguish on screen. For example:</p> <p><code>12-12ULN[I11O0]</code></p> <p>generates 12-digit codes that have upper-case characters, lower-case characters, and numbers, but will not include the letter upper-case letter I, the lower-case letter l, the number 1, the letter O, or the number 0; you should be able to send notifications using these codes using any font without ambiguity.</p> <p>The default exclusion list <code>[BGI1OQDSZ]</code> specifies letters that are commonly mistaken for numbers. When using this list, you can tell your operators that when reading out the code, if it is unclear whether the character is a letter or a number, to assume that it is a number, as no numbers are excluded.</p>
Further information	See section 3.4, Logon using codes for details.

Setting	Logon Code Lifetime
Default value	720
Description	The number of hours for which a logon code is valid for collecting a job. To set logon codes for no expiry, set this value to 0.
Further information	See section 3.4.1, Setting up logon codes and the <i>Sending a collection code</i> section in the <i>MyID Operator Client</i> guide for details of configuring and using logon codes for collection.

Setting	Simple Logon Code Complexity
Default value	12-12N
Description	<p>The complexity rule used to generate a logon code when the Generate Code on Request option in the credential profile is set to Simple Logon Code, or the Complexity option in the email template or the Auth Code Complexity configuration option is set to Simple.</p> <p>It takes the format <code>mm-nnULSN[excluded characters]</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> <p>Optionally, you can specify any characters you want to exclude because they are difficult to distinguish on screen. For example:</p> <p><code>12-12UN[I1O0]</code></p> <p>generates 12-digit codes that have upper-case characters and numbers, but will not include the letter upper-case letter I, the number 1, the letter O, or the number 0; you should be able to send notifications using these codes using any font without ambiguity.</p>
Further information	See section 3.4, Logon using codes for details.

Index

- Abort On Timeout 351
- Access to card layouts 113
- Access to workflows 49
- Action on maximum security question failures 389
- Actioned by 273
- Activating cards 277
- Activation
 - authentication methods 281
 - credential profile 277
- Active credential profiles per person 363
- Active Directory 68
- Active Directory Deletion Tool 81
- Adding
 - a directory 69
 - customer keys 105
 - devices 286
 - factory keys 100
 - roles 48
- Additional identities 295
 - adding 300
 - adding for your own account 303
 - overview 295
 - removing 303
 - setting up 296
- Additional Identity LDAP Operator User Filter 299, 338
- Additional Identity LDAP Self-Service User Filter 299, 338
- Administration Email 201, 373
- Administration Guide 13
- Administrative groups 61
- Administrator email address 376
- Administrators 13, 25
- All scope 59
- Allow Administrative Groups 396
- Allow Card Activation 329
- Allow card serial number to be entered during Request Card workflow 329
- Allow Collect Later 351
- Allow derived credential requests to create accounts 364
- Allow device management from the MyID user interface 330
- Allow disposal of expired devices 330
- Allow duplicate DN 338
- Allow envelope version 1.2 385
- Allow envelope version 1.3 385
- Allow Image Zoom 324
- Allow LDAP Search for devices during Add Devices 339
- Allow LDAP Search for devices during card requests 339
- Allow Legacy Data Models 386
- Allow Logon Codes 35, 379
- Allow parent and child credential profiles 364
- Allow requests without user data approved 364
- Allow Self-Service at Logon 380
- Allow self requests 400
- Allow virtual smart card creation with TPM reduced functionality 330
- AllSigned PowerShell Execution Policy 305
- Anonymous access to LDAP directory 70
- App Download URL – ANDROID 365
- App Download URL – iOS 365
- Applets 25, 98
 - adding 109
 - adding to credential profiles 158
 - editing 110
 - upgrading 111
- Application AID 109
- Application privileges 109
- Approve Key Recovery 267
- Approve Replacement Cards 396
- Archive People Data 325
- Archiving 261
- Archiving deleted users 271
- archiving keys 261-262
- Ask Security Questions for Self Service Card Unlock 389
- Assign unmatched new accounts to default directory 339
- Assigning administrative groups 61
- Assigning logon mechanisms 51
- Audit Reporting workflow 255
- Audit scope 254
- Audit trail 254-255
- Audited Items workflow 259
- Auditing specified items 259

- Auth Code Complexity 35, 405
- Auth Code Lifetime 405
- Auth Code Lifetime for Immediate Use 406
- Auth Code Scope 330
- Authentication 27
- Authentication Code Logon 403
- Authentication methods for activation 281
- Auto-enroll from directory 400
- Auto-enroll from directoryRestrict Self Activation 278, 400
- Auto text on card layouts 123
- Automated Card Issuance Time Limit 365
- Automated Detect Card Time Limit 365
- Automated Issuance Time Limit 351
- Automated Remove Card Time Limit 366
- Automatic cancellation timeout 362
- Automatic Completion of Issuance 366
- Automatic Completion of Issuance Timeout 366
- Automatic job cancellation 275
- Automatic job cancellation credential profile filter 362
- Automatic job cancellation email 362
- Automatic Renewal 89
- Automatic Update Collection 366
- Automatically create card update jobs when additional identities are modified 367
- Automatically create MyID groups from the Organizational Unit of imported users 339
- Automatically Expire Web Pages 325
- Back of cards 112
- Background Update 340
- Backgrounds 118
- Base DN 68-69
- Batch Directory Synchronization Tool 71
 - scheduled task 78
- Batch Encode Card Timeout 367
- Batch issue, default card layout 183
- BatchLDAPSync.exe 77
- Biometric Logon 402
- Block Multiple Requests for Credential Group 164
- Block VSC unlock in Remote Unlock workflow 396
- Browsing reports 256
- CA connection
 - add 85
 - edit existing 86
- CacheBannedWordsList option 193
- Calendar control 23
- Cancel Outstanding Updates 362
- Canceling jobs 274
- Canceling notifications 210
- Capture Client Identifier 386
- Capture IP Address 386
- Card activation expiration period 330
- Card Authentication Certificate ID Format 352
- Card Encoding 161
- Card Expiration Period (days) 397
- Card label 331
- Card Layout Editor workflow 115
- Card layouts
 - access 113
 - adding 115
 - associating with credential profiles 158
 - default 183
 - deleting 115
 - designing 112
 - moving elements 127
 - printing 137
 - saving 115
 - sizing elements 127
 - xml 135
- Card logon 51
- Card readers 25
- Card Renewal Period 89, 331
- Card suitability 313
- Card suitability external system 316
- Card suitability service 319
- Card suitability web service
 - creating 314
- Cardholders 25
- CardIssuanceApproved node 309
- Cards 25
- Cards Allowed For Derivation 353
- CardSuitability external system 316
- Case sensitive security questions 36, 389
- Categories 25
- Ceremony
 - key 102, 107

- Certificate archiving 261
- Certificate authorities 84
 - connecting 85
- Certificate Authorities workflow 85
- Certificate authority key archiving 261
- Certificate lifetime restriction 311
- Certificate policies 87
 - superseding 90
- Certificate Polling Refresh Time 353
- Certificate Recovery Password Complexity 353
- Certificate Refresh Threshold 84, 354
- Certificate renewal 89
- Certificate renewal checks 311
- Certificate Timeout For Deferred Collection 88, 354
- Certificate Timeout For Issuance 88, 354
- Certificates 25
 - adding to credential profiles 158
 - enabling 87
 - issuing 67
 - revocation 88
 - revoking timed-out 88
- Change Credential Profile At Approval 367
- Changing list entries 238
- Check Content Signing Certificate Expiration 331
- checkCard method 314
- Checking card suitability 319
- Client Credentials OAuth2 Logon 402
- Client Logon Keyset 397
- Client Sign Keyset 397
- Client Signing 380
- Collect Key Recovery 267-268
- Collect My Key Recovery 267-268
- Color Picker dialog 126
- Colors
 - text 126
- Colour Picker dialog 126
- Command line for Batch Directory Synchronization Tool 77
- Complex Logon Code Complexity 36, 407
- Configuration-only directory 80
- Configuration options
 - operation settings 324
 - security settings 379
- Configuration report 321
- Connecting to a CA 85
- Connecting to an LDAP directory 69
- Constrain certificate lifetime to vetting date 311
- Constrain Credential Profile Collector 397
- Constrain Credential Profile Issuer 182, 398
- Constrain Credential Profile Unlock Operator 183, 398
- Constrain Credential Profile Validator 398
- Create OU Chain 340
- Credential Group 164
- Credential Profile workflow 159
- Credential profiles 158
 - back of cards 112
 - Card Encoding 161
 - creating 159
 - default values 159
 - soft certificates 185
- Credential Stock 173
- Credentials 26
 - issuing 158
- Custom LDAP Mappings 340
- Customer keys 99, 239
 - adding 105
 - deleting 108
- Customizing terms and conditions 187
- Database Mail Profile Name 374
- Dates 23
- Default Card Data Model 331
- Default card layouts 183
- Default Card Reverse Layout 112, 332
- Default max PIN length 389
- Default roles 54
- Delayed Cancellation Period 332
- Deleted users
 - archiving 271
- Deleting
 - customer keys 108
 - roles 49
- Deliver Card Before Activation 332
- Department scope 59
- Derived credential certificate OID 354
- Derived Credential Revocation Check Interval 355

- Derived credential revocation check offset 355
- Derived credential signing certificate OID 355
- Designing card layouts 112
- Device Assignment End Date 198
- Device identities
 - approving cancellations 294
 - canceling 293
 - collecting 292
 - credentials profile 285
 - known issues 294
 - managing 283
 - requesting 290
 - role permissions 283
 - scope 283
 - validating requests 291
- Device Identity (Only) 285
- Device Profiles 173
- Device security 323
- Device suitability external system 316
- Device suitability service 319
- Devices 26
 - adding 286
 - adding from an LDAP directory 288
 - editing 289
 - managing 283
- Directory 67
 - configuration-only 80
 - configuration options 70
 - creating connections 69
- Directory Management workflow 69
- Directory Synchronization Tool 71
- Disable on removal from directory 73, 340
- Disable Report Count 325
- DisableCard 217
- DisableCard notification 222
- Display additional error information 322, 325
- Display credential profile details 367
- Display pending card requests 325
- Display person details during confirm job 341
- Display warnings for unsecured issuance 383
- Diverse keys 101, 106, 239
- Division scope 59
- Documents
 - mail merge 183
- Dynamic text size 127
- EdeficePinGenerator 138
- Edit Directory Information 341
- Edit DN 341
- Edit Roles workflow 46-47
- Editing
 - applets 110
 - roles 46
- Effective Revocation Immediate 326
- Email address
 - for licenses 195
- Email notifications 200
 - identity checks 311
 - templates 203
- Email separator 201, 374
- Email server 270
- Email templates 209
 - editing 202
 - enabling 202
- Email Templates workflow 202
- Email Terms and Conditions 333
- Enable additional authentication options 363
- Enable ADS Fields 341
- Enable credentials when person is enabled 333
- Enable Customer GlobalPlatform Keys 99, 383
- Enable Facial Capture 361
- Enable Intel Virtual Smart Card support 333
- Enable unrestricted cancellation 368
- EnableCard 217
- EnableCard notification 221
- Enabling certificates 87
- Encryption 162, 261
- Encryption certificate
 - SCEP 284
- Enforce Banned Words 191
- Enforce Photo at Issuance 164
- Enforcing banned words in PINs 191
- Entrust force new escrow 355
- Envelope Transport Key Algorithm 387
- Error 273
- Error messages 322
- Evaluation license 194
- Event auditing 255
- Events report 322

- Exclusive Group 164
- Executable AID 109
- Expanded error messages 322
- Expiration Identity Batch 333
- Expiration Notification Period 374
- Expire cards at end of day 369
- External System
 - card suitability 316
- External Systems 270
- Factory keys 99, 239
 - adding 100
 - deleting 105
- FIDO Basic Assurance Logon 403
- FIDO High Assurance Logon 403
- FIDO Immediate Collect Timeout 390
- File Export Directory 360
- File Import Directory 157, 360
- File Store Location 345
- Find Person stage 63
- Fit image to card 116
- FitTextFormatter 127
- Force NETBIOS name 80, 342
- Formatting text 125
- Forms 26
- Generate Logon Code 36
- Generating PINs 138
- GenMaster 239
- Getting started 16
- GIFs on card layouts 117
- Global PIN 171
- GlobalPlatform keys 98-99
- Grid 116
- Group Deletion Enabled 326
- Groups 26, 46, 60
 - administrative 61
 - assigning administrative 61
- Hiding roles 47
- Host
 - LDAP directory 68
- HTTP Port for image upload 345
- HTTPS Port for image upload 346
- ID photos on card layouts 117
- Identities
 - additional 295
- Identity checks 309
 - email notifications 311
- Identity mapping 296
- Ignore User Expiry Date 167
- Image Capture 346
- Image Crop Aspect Ratio 346
- Image Crop Height 347
- Image Crop Width 347
- Image location 113
- Image Upload Server 113, 348
- Images
 - card layouts 117
- Import Devices Sequential Range Limit 360
- Import Serial Numbers workflow 156
- Importing
 - account details 64
- Inheriting roles 52
- Initiator 273
- Installation history 321
- Installing licenses 197
- Integrated Windows Logon 43, 402
- Intel Authenticate 333
- iOS OTA Credential Profile 356
- iOS OTA Description 356
- iOS OTA Display Name 356
- iOS OTA Organization 356
- Issuance Notification URL 374
- Issuance Settings 162
- Issue MyID Signing Keys 334
- Issue over Existing Credential 178
- Issuing
 - certificates 67
- Java cards 98
- Job batch maximum size 363
- Job cancellation 275
- Job management 272
- Job Management workflow 274
- Jobs 26
 - canceling 274
 - searching 272
 - suspending 274
 - targets 273
 - unsuspending 274
- JPEG Compression Ratio 348
- JPEGs on card layouts 117

- Key archiving 261
- Key Manager 139
- Key Manager workflow 239
- Key recovery 264
 - collecting 267-268
 - credential profile 264
 - requesting 265
 - validating 267
 - viewing 268
- Key Recovery Only 264
- Keys
 - archiving 261
 - ceremony 102, 107, 239
 - managing 239
 - transport 239
- Known issues
 - for device identities 294
- Layouts
 - associating with credential profiles 158
 - for cards 112
- LDAP
 - configuration-only 80
 - configuration options 70
 - linking roles 57
- LDAP directory 67
 - creating connections 69
 - integration 61
 - port 69
 - primary data source 71
- LDAP Directory Synchronization Tool 71
- LDAP update cancel card 342
- LDAP update enable card 342
- LDAP update exception groups 342
- LDAP update newissue card 342
- LDAP update permreplaceissue card 343
- LDAP update search attribute 343
- LDAP update tempreplaceissue card 343
- Leading zeroes 157
- Licenses 194
 - installing 197
 - requesting 195-196
 - status 195, 321
 - warning email address 195
 - warning messages 198
- Licensing 196
- Licensing workflow 194
- Lifetime restriction 311
- Lightweight Directory Access Protocol See LDAP
- Limit derived credential lifetime to deriving credential 357
- Link to LDAP groups 58
- Link to LDAP Groups 343
- Linking roles to LDAP 57
- List Editor 238
- Load File AID 109
- Lock Card on Issuance 390
- Log level 376
- Logging on 16, 27, 51
- Logon 162
- Logon code complexity 36
- Logon Code Lifetime 407
- Logon codes 34
- Logon failures 27
- Logon methods 27
- Logon Name Required 380
- Logon Priority 403
- Magnetic stripes on card layouts (magstripe) 134
- Mail Documents 172
- Mail Format 375
- Mail merge 172, 183
- Maintain Aspect Ratio 348
- Manage Additional Identities workflow 300
- Manage Applets workflow 109
- Manage GlobalPlatform Keys workflow 99
- Manage My Additional Identities workflow 303
- Manage PIV 9E key on supported devices 384
- Manager credential profile 159
- Managing device identities 283
- Managing jobs 272
- Managing keys 239
- Managing notifications 210
- Manual Card Update 370
- Mapping file
 - REST notifications 231
- Mask Certificate Revocation Code 357
- Master key 102, 107, 239
- Maximum Allowed OTP Failures 381
- Maximum allowed security question failures 381

- Maximum certificate server restart log entries 326
- Maximum certificate suspensions 357
- Maximum credential expiry date 167
- Maximum Image Height 349
- Maximum Image Width 349
- Maximum keys per card to recover 357
- Maximum log storage space 377
- Maximum multiple credential requests 370
- Maximum Number of Assigned Devices 198
- Maximum number of log files 377
- Maximum Number Of Sub-Folders 349
- Maximum person search results 326
- Maximum retry attempts 377
- Maximum session count 378
- Maximum unvalidated multiple credential requests 370
- Messages expanded 322
- Microsoft virtual smart cards supported within MyID 334
- Migrated Certificate Credential Profile 360
- Migrated Device Credential Profile 360
- Migrated Encryption Certificate Policy 361
- Migrated Non-archived Certificate Policy 361
- Minimum retry delay 378
- Mobile Certificate Recovery Service URL 358
- Mobile Provision Via Email 334
- Mobile Provision Via SMS 334
- Moving elements 127
- MyID encryption 261
- MyID key archiving 261
- Navigation buttons 21
- NETBIOS name 80
- Notification Proxy URL 375
- Notification Scheme 165
- Notifications 213
- Notifications Management workflow 210
- Number of security questions for operator authentication 390
- Number of security questions for self-service authentication 390
- Number of security questions to register 390
- Offline Unlock Method 391
- One Active Job Per Person 335
- One Click Selection in Find Person 327
- One Credential Profile Request Per
 - Person 335
- Operation Settings 324
- Operation Settings workflow 73
- Operators 26
- Organization chart 60
- Organizational Unit 60
- Organizing groups 60
- OU 60
- Output Mechanism for Job Challenge Code Generation 371
- Page Timeout for Windows Clients 327
- Password logon 16, 27, 51, 401
- Persist terms and conditions 335
- PFX files 94
- Photos on card layouts 117
- Picklists 238
- Pictures
 - card layouts 117
- PIN generation 138
 - adding a key 139
 - setup 141
- PIN Generation Key 139
- PIN Settings 169
- PIN Timeout 391
- PinPolicyBannedWordList.txt 192
- PINs
 - logon 27
- PIV Biometric Maximum Age 336
- PIV Facial Biometrics Required 336
- Policies
 - certificate 87
- Ports
 - LDAP directory 68-69
- Post-workflow PowerShell script 305, 327
- Post-workflow scripts 305
- PowerShell script format 306
- PowerShell script security 305
- PowerShell scripts 305
- Pre-encode card 277
- Preload Images 350
- Prevent Direct Password Logon 381
- Prevent version 1 password enrollment 391
- Primary data source 67, 71
- Print Card Timeout 371
- Print Quality Confirmation 336

- Printer Request Buffer Delay 371
- Printers 26
- Printers have External Prox Readers 327
- Printing card layouts 137
- Printing cards 112
- Production use 323
- Profiles
 - for credentials 158
- Proximity Card Check 164
- Random PINs 138
- RandomPINGenerator 138
- Registry
 - SCEP 284
- Reload Device Profile 371, 391
- Remote Unlock requires an Authentication Code prompt 392
- Renew Expired Certs Via API 358
- Renewal dates (jobs) 273
- Renewing certificates 89
- Reporting structure 60
- Request Key Recovery 265
- Requesting a device identity 290
- Requesting licenses 195-196
- Require Activation 277
- Require Challenge 290
- Require Random Security Officer PIN 384
- Require user data to be approved 309
- Requisite User Data 173, 372
- REST Device Cancelled 217
- REST Device Cancelled notification 220
- REST Device Issued 217
- REST Device Issued notification 219
- REST notifications 214, 217
 - troubleshooting 237
- REST web service notifications 213
- Restrict certificate lifetimes to the card 89, 358
- Restrict collection of replacement devices if expiry date within (Days) 372
- Restrict Roles on Child Groups 52, 398
- RESTService external system 214
- Retry delays 85
- Retry On Collection 358
- Reverse of cards 112
- Revoke certificates if user is removed or disabled following background directory update 73, 343
- Revoking timed-out certificates 88
- Right to left text 125
- Role inheritance 52
- Roles 46
 - adding 48
 - associating with credential profiles 158
 - default 54
 - deleting 49
 - editing 46
 - hiding 47
- Roles for card layouts 113
- Rotate 116
- Rotate Keys On Card Update 372
- RSA transport keys 249
- SCEP
 - certificates 284
 - registry entries 284
 - setting up 284
- SCEP Hash Algorithm 387
- Scheduled certificate revocation 88
- Scheduled task
 - Batch Directory Synchronization Tool 78
- Scope 46
- Scope of audit 254
- Script format 306
- Script security 305
- Scripts 305
- Search a Directory 71, 344
- Searching for jobs 272
- Secondary Serial Number 336
- Secret keys 239
- Secure LDAP directory port 69
- Security events 322
- Security Officer PIN Type 384
- Security Phrase allowable characters 392
- Security Phrase complexity format 392
- Security Phrase minimum length 392
- Security Phrase repeat character limit 393
- Security Phrase sequential character limit 393
- Security Phrase whitespace removal 393
- Security phrases
 - unlocking 33
- Security Settings 379
- Selecting dates 23
- Self-service 400

- Self-service emergency password 401
- Self-service Resynchronization 401
- Self-Service Unlock 401
- Self-service unlock authentication 167
- Self scope 59
- Send Email Notifications 375
- Send Mobile OTP via SMS 375
- Serial Number IIN 336
- Serial numbers 101
 - importing 156
- Server Encryption 388
- Server Generated PIN 141
- Set Credential Profile On Renewal 372
- Set expiry date at request 373
- Set GlobalPlatform Card Status 394
- Set Security Phrase at Logon 382
- Setting up additional identities 296
- Show all devices 384
- Show Audit Summary 399
- Show chip 116
- Show Disqualified Credential Profiles 373
- Show Extended Job Details for Target 363
- Show Full Name at Logon 382
- Show Generated PINs 394
- Show grid 116
- Show License Info to All Operators 195, 376
- Show Photo at Logon 382
- Show Set Security Phrases Button 399
- Show the Card Content button in the Audit Workflow 373
- Sign Audit on Client 399
- Sign Audit on Server 399
- Signed Logon 383
- SignedTCs.txt 187
- Signing certificate
 - SCEP 284
- Simple Certificate Enrollment Protocol See SCEP
- Simple Logon Code Complexity 36, 408
- Single Email Notification 376
- Sizing elements 127
- Skip Person Confirmation screen 344
- Smart card logon 51, 402
- Smart cards 26
- SMS email notifications 328
- SMS gateway URL for notifications 328
- SMTP Format 200
- SMTP server 270
- Snap to grid 116
- Soft certificates
 - credential profile 185
- Stages 26
- Standard REST notifications 217
- Static keys 101, 106, 239
- Status of jobs 272
- Status report 321
- Storage method allowed for certificate recovery 359
- Store Secret Keys 388
- Superseding certificate policies 90
- Suspend to revoke period 88, 359
- Suspended dates (jobs) 273
- Suspending jobs 274
- Synchronise new accounts with directory 344
- Synchronization Tool for LDAP directory 71
- Synchronize new accounts with directory 344
- System Events workflow 322
- System security 323
- System Status workflow 321
- Targets for jobs 273
- Task Number Timeout 399
- Templates 135
 - certificate 87
 - for email notifications 203
- Temporary Credential Profile Name 328
- Terminology 25
- Terms and conditions
 - customizing 187
 - options 279
- Terms and Conditions During Device Update 337
- Text
 - card layouts 123
 - formatting 125
- Text colors 126
- Timed-out certificates
 - revoking 88
- Token Logon 402
- Token resync window 337
- Tokens 26

- TPM 26
- Track Entrust distinguished name changes 344
- Transactions
 - witnessing 65
- Transport keys 102, 107, 239, 249
- Transport PIN 394
- Trial license 194
- TriggerInformation XML 306
- Triggering scripts 305
- Troubleshooting 321
 - REST notifications 237
- Trusted Platform Module See TPM
- Unblocking Credential 337
- Unknown card logon 401
- Unlock Security Phrases 33
- Unmanaged certificate authority 94
- Unsuspending jobs 274
- Update email address from derivation 359
- Update group information in the directory 345
- Update user information in the directory 57, 345
- Upgrading applets 111
- Uploading images 118
- Uploading PFX certificates 95
- URL encoded links 203
- URL path 328
- Use Entrust default key update policy 359
- Use key ceremony 102, 107
- Use logon name for server PIN generation 142, 147, 395
- Use PIN policy settings in random server PIN generation 395
- Use Security Phrase algorithm version 2 395
- Use SSL for Image Capture 350
- User Data Approved 309
- User images on card layouts 117
- User security identifiers 97
- User SIDs 97
- UserDataApproved node 309
- Users
 - archiving deleted 271
- Valid Period 162
- Validate Image Size 350
- Validate logon certificate 383
- Validate signing certificates 388
- Validator 273
- vBannedDevice 192
- vBannedUser 192
- Vetting checks 309
- Vetting date certificate lifetime 311
- Vetting date job processor 310
- Vetting Date Validity Period 310, 361
- Vetting dates 310
- VettingDate node 309
- Video Capture 351
- View Full Audit 254
- View Key Recovery 268
- View User Audit 254
- Viewing job records 273
- Virtual Smart Cards See VSCs
- Visible roles 47
- VSCs 25-26
- Warning Email Address 198
- Warning email address for licenses 195
- Warning Limit 198
- Warning messages for licensing 198
- Web Server External Address 329
- Web service notifications 213
- Windows Hello
 - credential profile option 161
 - logon mechanism 44
- Windows Hello for Business supported within MyID 337
- Windows Hello Logon 403
- Windows logon 16
- Windows Logon 43
- Witnessing transactions 65
- Workflow Timeout Warning Delay 329
- Workflows 26
 - access to 49
- XML
 - card templates 135
- Zoom 116