intercede
MyiD CMS

MyID Enterprise

Version 12.14

MyID Operator Client

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

Document reference: INT1993-12.14.0-Enterprise March 2025

Copyright

© 2001-2025 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.

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.

Licenses

This software includes packages provided under a variety of licenses. The *About the documentation* page in the HTML version of the MyID CMS documentation, available with the MyID CMS software or on the Intercede customer portal website, contains a full list.

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

MyID Operator Client 1
Copyright 2
Conventions used in this document 3
Contents 4
1 Introduction 12
2 Overview 14
2.1 Requirements 15
2.1.1 Supported browsers 15
2.1.2 Required software 15
2.2 SSL/TLS 15
2.3 Terminology 16
3 Using the MyID Operator Client 18
3.1 Selecting the server 18
3.1.1 Specifying the server for the MyID Client Service 18
3.1.2 Troubleshooting server connection issues 19
3.2 Signing in 20
3.2.1 Signing in using a smart card 20
3.2.2 Signing in using security phrases 21
3.2.3 Signing in using Windows Hello 21
3.2.4 Signing in using FIDO 22
3.2.5 Signing in using single-use authentication codes 22
3.2.6 Signing in using Windows authentication 23
3.2.7 Signing in using an external identity provider 25
3.2.8 Signing in to MyID 26
3.2.9 Managing your credentials from the MyID Authentication screen 32
3.2.10 Timeouts and re-authentication 33
3.3 MyID Operator Client user interface 34
3.3.1 Using the button bar 36
3.3.2 Launching MyID Desktop, Self-Service App, or MyID Client for Windows workflows 37
3.3.3 Displaying dates and times 37
3.3.4 Entering dates and times 38
3.3.5 Using the browser location bar 39
3.3.6 Opening a new tab or window 40
3.3.7 Selecting a group 41
3.4 Working with tables of records 45
3.4.1 Working with columns 45
3.4.2 Sorting 47
3.4.3 Grouping 48
3.4.4 Filtering 49
3.4.5 Changing the row spacing 50
3.4.6 Working on multiple records 51
3.4.7 Performance considerations for searching large sets of data 54
3.5 Roles and groups 54

3.5.1 Roles example 59
3.5.2 Scope 60
3.5.3 Administrative groups 60
4 Working with people 61
4.1 Searching for a person 62
4.1.1 Viewing a person's history 65
4.1.2 Wildcards 66
4.2 Adding a person 66
4.2.1 Adding a person manually 66
4.2.2 Adding a person from a directory 69
4.2.3 Adding multiple people from a directory 70
4.3 Editing a person 71
4.3.1 Editing directory information 72
4.4 Capturing images 73
4.4.1 Requirements for image capture 73
4.4.2 Configuring image capture 74
4.4.3 Capturing an image from a webcam 76
4.4.4 Uploading an existing image file 78
4.4.5 Cropping and editing user images 79
4.4.6 Troubleshooting image capture 81
4.4.7 Viewing images 82
4.5 Requesting a device for a person 82
4.5.1 Requesting a device 82
4.5.2 Requesting devices for multiple people 85
4.5.3 Known issues 87
4.6 Requesting a mobile device for a person 87
4.6.1 Requesting a mobile device 87
4.6.2 Requesting mobile devices for multiple people 90
4.7 Synchronizing a person 92
4.8 Enabling or disabling a person 93
4.8.1 Disabling a person's user record 93
4.8.2 Enabling a person's user account 95
4.9 Working with administrative groups 96
4.9.1 Selecting an administrative group 96
4.9.2 Assigning administrative groups 96
4.10 Removing a person 98
4.11 Authenticating a person 99
4.12 Sending an authentication code to a person 99
4.13 Viewing an authentication code for a person 101
4.14 Working with security phrases 103
4.14.1 Changing a person's security phrases 103
4.14.2 Unlocking a person's security phrases 104
4.15 Printing a badge 104
4.16 Working with relationships 105
5 Working with devices 106

5.1 Searching for a device 107
- 5.1.1 Viewing a device's history 110
- 5.1.2 Wildcards 111

5.2 Reading a device 112
5.3 Working with device categories 114
5.4 Requesting a replacement device 114
5.5 Requesting a replacement mobile device 116
5.6 Renewing a device 119
5.7 Canceling a device 120
- 5.7.1 Canceling a device 120
- 5.7.2 Canceling multiple devices 122
- 5.7.3 Requesting a cancellation for a device 125

5.8 Resetting a device's PIN 126
5.9 Changing a device PIN 127
5.10 Activating a device 127
5.11 Erasing a device 129
5.12 Unlocking a device 129
5.13 Sending an authentication code to activate a device 130
- 5.13.1 Configuring authentication codes for activation 131
- 5.13.2 Sending an authentication code for activation 133
- 5.13.3 Viewing an authentication code for activation 135

5.14 Sending a code to unlock a device 136
- 5.14.1 Configuring authentication codes for unlocking 139
- 5.14.2 Sending an unlock code 141
- 5.14.3 Viewing an unlock code 143

5.15 Updating a device 145
- 5.15.1 Collecting updates for your own device 145
- 5.15.2 Collecting updates for another person's device 146

5.16 Reprovisioning a device 147
5.17 Requesting an update for a device 147
- 5.17.1 Requesting an update 147
- 5.17.2 Requesting updates for multiple devices 149

5.18 Managing VSCs 151
- 5.18.1 Requesting, updating, and canceling VSC locks 151
- 5.18.2 Providing time-limited VSC access 152

5.19 Reinstating a device 153
5.20 Disposing of a device 155
- 5.20.1 Setting the disposal status of a device 156
- 5.20.2 Setting the disposal status of multiple devices 158

5.21 Printing a mailing document 160
5.22 Enabling and disabling devices 160
- 5.22.1 Disabling a device 161
- 5.22.2 Enabling a device 163

5.23 Viewing extended information about a device 164
5.24 Importing a range of devices 165

5.24.1 Example serial number import 166
5.25 Importing devices from a manifest file 167
5.26 Viewing imported devices 168
5.26.1 Viewing device import requests 169
5.27 Accepting delivery for a device 170
5.27.1 Configuring the card delivery process for a delivery stage 170
5.27.2 Issuing a card that requires a delivery stage 170
5.27.3 Marking a device as delivered 170
5.27.4 Marking multiple devices as delivered 171
5.28 Viewing the initial PIN for a device 173
5.28.1 Configuring the View Device Initial PIN role 173
5.28.2 Viewing the initial PIN on the View Device screen 174
6 Working with requests 175
6.1 Searching for a request 175
6.2 Approving, rejecting, and canceling requests 178
6.2.1 Approving requests 178
6.2.2 Rejecting requests 180
6.2.3 Canceling requests 181
6.2.4 Approving multiple requests 182
6.2.5 Rejecting multiple requests 185
6.2.6 Canceling multiple requests 188
6.3 Collecting a device request 191
6.4 Sending a collection code 192
6.4.1 Sending a collection code by email or SMS 193
6.4.2 Viewing a collection code on screen 195
6.5 Assigning a device to a request 197
6.5.1 Assigning a device directly 198
6.5.2 Searching for a device to assign 199
6.5.3 Unassigning a device 201
6.5.4 Auditing for device assignment 201
7 Working with reports 202
7.1 Granting access to reports 203
7.2 Running reports 204
7.2.1 Paging of results 204
7.2.2 Running reports through the MyID Core API 205
7.3 Available reports 207
7.3.1 People report 208
7.3.2 Requests report 210
7.3.3 Locations report 212
7.3.4 Stock Limits report 213
7.3.5 Assigned Devices report 214
7.3.6 Device Import Requests report 216
7.3.7 Unrestricted Audit Report 217
7.3.8 Requests for review report 220
7.3.9 Print PIN Mailer report 221

7.3.10 Reprint PIN Mailer report 222
7.3.11 Person Status Summary report 225
7.3.12 Request Fulfillment report 227
7.3.13 People with Restricted Access to Operations report 229
7.3.14 Devices report 231
7.3.15 Archived Requests report 233
7.3.16 Mobile Devices report 235
7.3.17 All Requests report 237
7.3.18 Unassigned Devices report 239
7.3.19 Available Device Stock report 241
7.3.20 Assign Device Search report 243
7.3.21 Awaiting Delivery report 245
7.3.22 Device Disposal report 247
7.3.23 Certificates report 248
7.3.24 Stock Transfers report 251
7.3.25 Stock Per Location report 252
7.3.26 Additional Identities (AID) report 252
7.3.27 Issued devices by category report 255
7.3.28 Assigned Devices by Group report 256
7.3.29 My Devices report 257
7.3.30 SecureVault Usage report 259
7.3.31 Passkeys report 260
8 Working with inventory management 262
8.1 Setting up inventory roles 264
8.2 Editing inventory lists 266
9 Working with locations 268
9.1 Adding a location 269
9.2 Searching for a location 270
9.3 Editing a location 272
10 Working with stock limits 273
10.1 Adding a stock limit 274
10.1.1 Adding a stock limit from the View Location screen 275
10.2 Searching for a stock limit 276
10.3 Editing a stock limit 278
10.4 Deleting a stock limit 279
10.5 Checking stock limits 280
10.5.1 Checking stock limits using the Stock Per Location report 280
10.5.2 Checking stock limits on the View Location screen 282
11 Working with stock transfers 283
11.1 Adding a stock transfer 284
11.1.1 Adding a stock transfer from the View Location screen 285
11.2 Searching for a stock transfer 286
11.3 Editing a stock transfer 288
11.4 Adding devices to a stock transfer 289
11.4.1 Adding a batch of devices to a stock transfer 289

11.4.2 Adding a single device to a stock transfer 293
11.5 Canceling a stock transfer 294
11.6 Checking the contents of a stock transfer 296
11.7 Dispatching a stock transfer 297
11.8 Failing a stock transfer 298
11.9 Receiving a stock transfer 300
12 Working with additional identities 301
12.1 Creating an additional identity 301
12.2 Editing an additional identity 303
12.3 Importing an additional identity 306
12.4 Removing an additional identity 310
13 Working with certificates 312
13.1 Viewing a certificate 312
13.1.1 Searching for a certificate 313
13.1.2 Viewing a person's certificates 314
13.1.3 Viewing a device's certificates 315
13.1.4 View an additional identity's certificates 316
13.1.5 Viewing a certificate's details 317
13.2 Revoking, suspending, and unsuspending certificates 318
13.2.1 Revoking or suspending a certificate 319
13.2.2 Revoking or suspending multiple certificates 320
13.2.3 Unsuspending a certificate 322
13.2.4 Unsuspending multiple certificates 323
13.3 Pausing and resuming certificate processing 325
13.3.1 Pausing certificate processing 326
13.3.2 Pausing processing for multiple certificates 327
13.3.3 Resuming processing 329
13.3.4 Resuming processing for multiple certificates 331
13.4 Changing renewal settings for a certificate 333
13.4.1 Changing a certificate's renewal settings 334
13.4.2 Changing the renewal settings for multiple certificates 335
14 Working with soft certificates 337
14.1 Collecting a soft certificate 339
14.2 Printing mailing documents for a soft certificate package 343
14.2.1 Printing a transport document 345
14.2.2 Reprinting a transport document 346
14.2.3 Printing a mailing document 347
14.2.4 Reprinting a mailing document 349
14.2.5 Printing multiple mailing documents 351
14.3 Customizing certificate file names 353
14.3.1 File name formats for individual certificate policies 355
14.3.2 Example custom file name format 356
15 Recovering keys 357
15.1 What is key recovery? 358
15.1.1 Use cases 358

15.2 Setting up permissions for key recovery 359
15.3 Requesting a key recovery 361
  15.3.1 Recovering certificates to an existing device through the View Person screen. 361
  15.3.2 Recovering certificates to an existing device through the View Device screen 365
  15.3.3 Recovering certificates to a new device or soft certificate package 366
15.4 Collecting recovered keys 368
  15.4.1 Collecting recovered keys to a new smart card 368
  15.4.2 Collecting recovered keys as soft certificates 369
  15.4.3 Collecting recovered keys to an existing device 370
  15.4.4 Known issues 370
16 Working with the audit trail 371
16.1 Viewing audit details 372
17 Launching administrative workflows 374
17.1 Using Certificate Administration workflows 376
17.2 Using Batch workflows 377
17.3 Using Bureau workflows 378
17.4 Using Additional Reporting workflows 378
17.5 Using Group Management workflows 379
17.6 Using Device Identities workflows 379
17.7 Using Credential Configuration workflows 380
17.8 Using Connections and Notifications workflows 381
17.9 Using Configuration Settings workflows 382
18 Carrying out self-service operations 384
18.1 Collecting self-service requests 385
18.2 Launching self-service workflows 385
19 Troubleshooting and advanced configuration 387
19.1 Viewing the Audit Report 387
19.2 Known issues 387
  19.2.1 .NET Core Desktop Runtime versions 388
  19.2.2 Full size images with Narrator on Microsoft Edge 388
19.3 MyID Operator Client error messages 388
  19.3.1 MyID Client Service versions 389
19.4 MyID Operator Client advanced configuration 390
  19.4.1 The rest.core web service configuration file 390
  19.4.2 The web.oauth2 web service configuration file 391
  19.4.3 2-way SSL/TLS 391
  19.4.4 Displaying images stored on the web server 392
  19.4.5 Changing the port 393
  19.4.6 Load balancing 394
  19.4.7 Setting the issuer for load-balanced systems 397
  19.4.8 MyID Operator Client pass-through authentication with a load balancer 399
  19.4.9 Translating the MyID Operator Client 399
  19.4.10 Setting the location of MyID Desktop or the Self-Service App 400
  19.4.11 Signature validation 401
  19.4.12 Fast user switching 402

- 19.4.13 Configuring the timeout for launching external applications 403
- 19.4.14 Changing the number of buttons displayed in the button bar 403
- 19.4.15 Configuring re-authentication timeout periods 404
- 19.4.16 Enabling or disabling re-authentication 405
- 19.4.17 Changing the number of Add buttons 406
- 19.4.18 Changing the size of the authentication pop-up window 407
- 19.4.19 Configuring certificate saving and printing 408
- 19.4.20 Configuring the priority for self-service applications 409

19.5 Refreshing the cache 409
- 19.5.1 Cached information 409
- 19.5.2 Excluded data 410
- 19.5.3 Configuring the cache refresh time 411
- 19.5.4 Refreshing the cache through the MyID Core API 412

19.6 Troubleshooting MyID Client Service connection issues 412
- 19.6.1 Connection issues 412
- 19.6.2 Mismatched client software versions 415
- 19.6.3 Server name does not resolve 415

1 Introduction

The MyID® Operator Client is a browser-based client that allows operators to work with MyID to manage people, request devices (smart cards, USB tokens, virtual smart cards, and so on), and view requests.

This document describes using the MyID Operator Client, including:

- An overview of the MyID Operator Client, including requirements and terminology.

  See section 2, *Overview*.
- Using the MyID Operator Client interface.

  See section 3, *Using the MyID Operator Client*.
- Using the MyID Operator Client to manage people.

  See section 4, *Working with people*.
- Using the MyID Operator Client to manage devices.

  See section 5, *Working with devices*.
- Using the MyID Operator Client to view requests.

  See section 6, *Working with requests*.
- Using the MyID Operator Client to run reports.

  See section 7, *Working with reports*.
- Using the inventory management features of the MyID Operator Client

  See section 8, *Working with inventory management*.
- Using the MyID Operator Client to manage locations.

  See section 9, *Working with locations*.
- Using the MyID Operator Client to set stock limits.

  See section 10, *Working with stock limits*.
- Using the MyID Operator Client to carry out stock transfers.

  See section 11, *Working with stock transfers*.
- Using the MyID Operator Client to manage additional identities.

  See section 12, *Working with additional identities*.
- Using the MyID Operator Client to manage certificates.

  See section 13, *Working with certificates*.
- Using the MyID Operator Client to manage soft certificates.

  See section 14, *Working with soft certificates*.
- Viewing the audit trail in the MyID Operator Client.

  See section 16, *Working with the audit trail*.
- Launching administrative workflows from the MyID Operator Client.

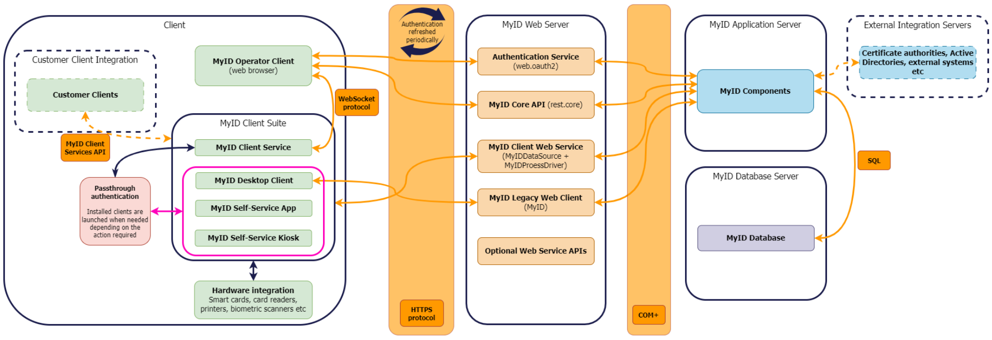
  See section 17, *Launching administrative workflows*.
- Carrying out self-service operations for the logged-in user.

  See section 18, *Carrying out self-service operations*.

- Troubleshooting, error messages, and advanced configuration.

  See section *19*, *Troubleshooting and advanced configuration*.

2 Overview


Client
Customer Client Integration
Customer Clients
MyID Client Services API
MyID Operator Client
(web browser)
WebSocket protocol
MyID Client Suite
MyID Client Service
Passthrough authentication
Installed clients are launched when needed depending on the action required
MyID Desktop Client
MyID Self-Service App
MyID Self-Service Kiosk
Hardware integration
Smart cards, card readers, printers, biometric scanners etc
Authentication refreshed periodically
HTTPS protocol
MyID Web Server
Authentication Service
(web.oauth2)
MyID Core API (rest.core)
MyID Client Web Service
(MyIDDataSource + MyIDProessDriver)
MyID Legacy Web Client
(MyID)
Optional Web Service APIs
COM+
MyID Application Server
MyID Components
External Integration Servers
Certificate authorities, Active Directories, external systems etc
SQL
MyID Database Server
MyID Database

The MyID Operator Client is a browser-based application that allows operators to log on to MyID to carry out day-to-day operations, such as adding people to the MyID database and requesting devices for them.

The system works as follows:

- The operator opens their browser and navigates to the MyID Operator Client website.

  This is a REST-based web service that is installed on the MyID web server. This web service communicates with the MyID components on the MyID application server, which access the MyID database.
- The MyID Operator Client website accesses the MyID Client Service through the operator's browser.

  The MyID Client Service allows the browser to access local hardware such as smart cards and VSCs. The operator can now use their smart card to log on to MyID. The MyID Client Service communicates with the MyID MWS web services on the MyID web server, which in turn communicate with the MyID components on the MyID application server, and ultimately the MyID database.

Other configurations are possible; for example, the web components and application server components may be installed on the same server, or the MyID Operator Client website may be installed on a different server to the MyID MWS web services. However, the principles remain the same.

2.1 Requirements

This section contains information about the requirements for using the MyID Operator Client.

2.1.1 Supported browsers

The MyID Operator Client is designed to work on a range of browsers running on Windows 10 or Windows 11. You are recommended to use one of the following:

- Google Chrome
- Microsoft Edge (Chromium version)
- Mozilla Firefox.

There are some limitations when using Firefox to capture images from a webcam. See section *4.4.1*, *Requirements for image capture*.

Note: Due to the browser technology used, you cannot use Internet Explorer to access the MyID Operator Client. If you attempt to use Internet Explorer to access the MyID Operator Client website, you are presented with the following error:

- `OC10002 - This web browser cannot be used. Please use an alternative web browser.`

2.1.2 Required software

To allow the browser to access smart cards, capture images, issue soft certificates, print mailing documents, or access features of MyID Desktop or the Self-Service App, you must install the MyID Client Service on each Windows PC on which you want to use the MyID Operator Client.

If an operator does not require access to these features, you do not need to install the MyID Client Service on their PC. For example, an operator who logs on to MyID using security phrases or integrated Windows logon, then uses the MyID Operator Client to run management information reports or create device requests, does not need the MyID Client Service; however, if they want to log on using their operator smart card, or to collect device requests, they do need the MyID Client Service to be installed and running.

See the *Installing the MyID Client Service* section in the ***Installation and Configuration Guide*** for instructions on installing the MyID Client Service.

You must have Microsoft .NET Core installed both on the client PCs and on the web services server.

See the *Prerequisites* section in the ***Installation and Configuration Guide*** for details of obtaining and installing the correct version of .NET Core.

2.2 SSL/TLS

Important: The web services used by the MyID Operator Client (`rest.core` and `web.oauth2`) require SSL/TLS; if you do not connect through HTTPS, you cannot use the MyID Operator Client. For information on setting this up, see the *Configuring SSL/TLS (HTTPS)* section in the ***Securing Websites and Web Services*** document.

2.3 Terminology

The terminology used in the MyID Operator Client documentation is as follows:

Term	Description
account	The details of a person that are stored in a directory.
administrator	A person within MyID who can log on to the MyID system to carry out administrative tasks; for example, creating profiles, editing roles, and setting configuration options.
card reader	A piece of hardware that connects to a PC and allows the PC to read and write to a smart card.
certificate	A piece of information issued by a certificate authority that is used to identify a person, and may be used to sign or encrypt information. Certificates can be stored on a device.
credential profile	A definition of a set of information about a user that can be written to a device. This may include certificates, printed card layouts, and details of PIN requirements.
device	A generic term for smart cards, USB tokens, virtual smart cards, and mobile devices (cellphones and tablets). A device can hold information about the person who has been issued the device, such as certificates and applets. In MyID Desktop, a device refers to a piece of equipment – a PC, server, router, cell phone or other hardware – that is used to store a *device identity*.
directory	A store of information about people external to MyID; for example, Microsoft Active Directory. MyID can work with people stored in a directory or in the MyID database, and can synchronize with the directory if appropriate.
group	The position of a person within the hierarchical structure; for example, the Payroll group within the Finance group.
LDAP	Lightweight Directory Access Protocol – the protocol used to access directories such as Microsoft Active Directory.
MyID Desktop	The Windows application that is used by operators and administrators to configure and use MyID to issue devices to people.
MyID Operator Client	The browser-based application that is used by operators to work with people and request devices.
MyID Self-Service App	The Windows application that is used by end users to collect, activate, and update their devices on their own PC.
MyID Self-Service Kiosk	The Windows application that is used by end users to collect, activate, and update their devices on a shared PC, or to request and collect temporary or replacement devices.
operator	A person within MyID who can log on to MyID Desktop or the MyID Operator Client to carry out operator's tasks; for example, adding people, or requesting devices.

Term	Description
person	A user record within MyID. A person can be an end user who has been issued a device to allow them to access their organization's systems, or a MyID operator or administrator.
request	A task in MyID that was created by an operator to carry out an action for a person; for example, to request a device for a person.
role	A security permission granted to a person that allows them to access particular features of the software; for example, an operator role might allow a person to add people and request devices; an administrator role might allow a person to create credential profiles; and an end user role might allow a person only to collect their own devices.
scope	A security permission granted to an operator or administrator's role that determines which other people are visible and available to carry out tasks, depending on their group; for example, an administrator might have a scope of All, which allows them to carry out tasks on any person in the system; an operator might have a scope of Department, which allows them to carry out tasks only on people in their own group; and an end user might have a scope of Self, which allows them only to carry out tasks for themselves, such as collecting their own devices.
smart card	A physical card containing a chip that can store applets, certificates, and other information. This is managed as a device in MyID.
subgroup	A group that has a parent group. For example, when searching the Finance group, you may want to search for people included in subgroups of the Finance group such as Payroll and Billing.
USB token	A device that has the same features as a smart card, but instead of a chip that requires a card reader, can be plugged into a USB socket.
Virtual Smart Card (VSC)	A device that can contain certificates like a smart card, but instead of a separate physical device, is built in to a PC. The hardware component in a PC that stores VSCs is the trusted platform module (TPM). The VSC is managed as a device in MyID.
Windows Hello	A Microsoft two-factor authentication system; with a credential stored on a PC or mobile device combined with a biometric identifier or PIN, a person can authenticate to their system (for example, Active Directory). Windows Hello for Business is the commercial version where the credential is backed by key-based or certificate-based authentication, in contrast with the personal version where the credential may be secured by a simple password hash. The Windows Hello credential is managed as a device in MyID.

3 Using the MyID Operator Client

This chapter contains information on the following:

- Connecting to the MyID server.

  See section *3.1*, *Selecting the server*.
- Signing in to the MyID system.

  See section *3.2*, *Signing in*.
- Navigating the MyID Operator Client user interface.

  See section *3.3*, *MyID Operator Client user interface*.
- Working with roles and groups.

  See section *3.5*, *Roles and groups*.

3.1 Selecting the server

SIU reference: SIU-301.

To access the MyID server:

1. Open your web browser.

   For a list of supported browsers, see section *2.1.1*, *Supported browsers*.
2. In the address bar, type the server address.

   For example:

   ```
   https://myserver.domain.com/MyID/OperatorClient/
   ```

   Important: The REST-based services that are used for the MyID Operator Client require SSL/TLS; if you do not connect through HTTPS, you cannot use the MyID Operator Client. For more information, see the *REST-based web services* section in the ***System Interrogation Utility*** guide.
3. Press Enter.

3.1.1 Specifying the server for the MyID Client Service

You specify the address of the MyID web services server for the MyID Client Service when you install the service on the client PC.

See the *Installing the MyID Client Service* section in the ***Installation and Configuration Guide*** for instructions on installing the MyID Client Service.

If you need to change the web services server address after you have installed it, you must edit the `MyIDClientService.dll.config` file in the MyID Client Service program folder.

Open the file with a text editor, and edit the following line:

```
<add key="Server" value="https://myserver.domain.com"/>
```

Note: You must include only the server name in the address; do not include the full MyID web service URL.

3.1.1.1 Synchronizing the server URL with the Self-Service App

Instead of providing the details of the MyID server in the MyID Client Service configuration file, you can point the MyID Client Service at the configured server for your installation of the MyID Self-Service App. This means that if you need to change the server URL, you need only change it in the Self-Service App configuration file, and the MyID Client Service will be automatically updated to use the same MyID server.

To synchronize the MyID Client Service with the Self-Service App:

1. In the `MyIDClientService.dll.config` file, remove or comment out the following lines:

   ```
   <add key="Server" value="https://myserver.domain.com"/>
   <add key="DataSource" value="MyIDDataSource/dataSource.asmx"/>
   ```

2. Add the following line:

   ```
   <add key="SsaPath" value="C:\Program Files\Intercede\MyIDApp\Self
   Service Application\MyIDApp.exe"/>
   ```

   Replace the `value` with the actual location of the Self-Service App program file on the client PC.

3.1.1.2 Access control

You can also update the list of access control URLs (that is, the websites that are allowed to access the MyID Client Service) in the same file. You can specify more than one URL; use commas to separate the URLs.

Edit the following line:

```
<add key="AccessControlAllowOrigin"
value="https://myserver.domain.com,https://myserver2.domain.com"/>
```

Note: You must include only the server name in the access control list; do not include the full MyID Operator Client URL.

For evaluation systems, you may want to disable the list of access control URLs; to do this, include the following line in the configuration file:

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

This is not recommended for production systems, as it affects the security of the MyID Client Service as it allows any client to communicate with it.

3.1.2 Troubleshooting server connection issues

If you have issues when connecting to the server, you are recommended to use the System Interrogation Utility to check your system configuration. SIU test ID 301 specifically checks the connection to the operator client URL.

If you experience problems, check the IIS logs on the web server, and ensure that there are no DNS issues that prevent the client PC from resolving the server URL. You may also want to restart IIS on the web server.

3.2 Signing in

You can sign in to MyID using the MyID Operator Client using the following methods:

- Card and PIN logon (smart card, USB token, or VSC).

  See section 3.2.1, *Signing in using a smart card*.
- Security phrases (passwords).

  See section 3.2.2, *Signing in using security phrases*.
- Windows Hello.

  See section 3.2.3, *Signing in using Windows Hello*.
- FIDO.

  See section 3.2.4, *Signing in using FIDO*.
- Single-use authentication codes.

  See section 3.2.5, *Signing in using single-use authentication codes*.
- Windows authentication.

  See section 3.2.6, *Signing in using Windows authentication*.
- An external identity provider.

  See section 3.2.7, *Signing in using an external identity provider*.

You can also launch the MyID Self-Service App from the screen to allow you to change your security phrases, for example, or reset your PIN; see section 3.2.9, *Managing your credentials from the MyID Authentication screen*.

3.2.1 Signing in using a smart card

For an operator to sign in to MyID using the MyID Operator Client with a smart card:

- The operator must have been issued a card (smart card, USB token, or VSC) through MyID.
- The smart card must have been issued with a credential profile that has the **MyID Logon** option set, and contain either a certificate selected for signing or a manager keypair to be used for logon signing operations.
- The smart card must not be disabled or have expired.
- The operator's MyID account must be enabled in MyID.
- In MyID Desktop, in **Configuration > Edit Roles**, the operator's role must have the **Smart Card** logon mechanism assigned.
- In MyID Desktop, in **Configuration > Edit Roles**, the operator's role must have access to one or more features in the MyID Operator Client.

  See section 3.5, *Roles and groups* for details of which roles in MyID Desktop map to features in the MyID Operator Client.
- In MyID Desktop, in **Configuration > Security Settings > Logon Mechanisms** tab, the **Smart Card Logon** option must be set to Yes.

For more information on configuring MyID for smart card logon, see the *Logon using a smart card and PIN* section in the ***Administration Guide***.

3.2.2 Signing in using security phrases

For an operator to sign in to MyID using the MyID Operator Client with security phrases:

- The operator must have security phrases recorded for their account using the **Change Security Phrases** or **Change My Security Phrases** workflows.

  See the *Setting security phrases* section in the ***Operator's Guide***.

  Important: The operator must have at least as many security phrases recorded as the value set in the **Number of security questions for self-service authentication** configuration option.
- The operator's MyID account must be enabled in MyID.
- In MyID Desktop, in **Configuration > Edit Roles**, the operator's role must have the **Password** logon mechanism assigned.
- In MyID Desktop, in **Configuration > Edit Roles**, the operator's role must have access to one or more features in the MyID Operator Client.

  See section *3.5*, *Roles and groups* for details of which roles in MyID Desktop map to features in the MyID Operator Client.
- In MyID Desktop, in **Configuration > Security Settings > Logon Mechanisms** tab, the **Password Logon** option must be set to Yes.

For more information on configuring MyID for security phrase logon, see the *Logon using security phrases* section in the ***Administration Guide***.

3.2.3 Signing in using Windows Hello

For an operator to sign in to MyID using the MyID Operator Client with a Windows Hello credential:

- The operator must have been issued a Windows Hello credential through MyID.
- The Windows Hello credential must not be disabled or have expired.
- The operator's MyID account must be enabled in MyID.
- In MyID Desktop, in **Configuration > Edit Roles**, the operator's role must have the **Windows Hello** logon mechanism assigned.
- In MyID Desktop, in **Configuration > Edit Roles**, the operator's role must have access to one or more features in the MyID Operator Client.

  See section *3.5*, *Roles and groups* for details of which roles in MyID Desktop map to features in the MyID Operator Client.
- In MyID Desktop, in **Configuration > Security Settings > Logon Mechanisms** tab, the **Windows Hello Logon** option must be set to Yes.

For more information on configuring MyID for Windows Hello logon, see the *Setting up Windows Hello for logon* section in the ***Windows Hello for Business*** guide.

3.2.4 Signing in using FIDO

For an operator to sign in to MyID using the MyID Operator Client with a FIDO authenticator:

- The operator must have been issued a FIDO authenticator through MyID.
- The FIDO authenticator must not be suspended.
- The operator's MyID account must be enabled in MyID.
- In MyID Desktop, in **Configuration > Edit Roles**, the operator's role must have the **FIDO Basic Assurance** or **FIDO High Assurance** logon mechanism assigned. You are recommended to configure logon to MyID using **FIDO High Assurance** rather than **FIDO Basic Assurance**.
- In MyID Desktop, in **Configuration > Edit Roles**, the operator's role must have access to one or more features in the MyID Operator Client.

  See section *3.5*, *Roles and groups* for details of which roles in MyID Desktop map to features in the MyID Operator Client.
- In MyID Desktop, in **Configuration > Security Settings > Logon Mechanisms** tab, the **FIDO Basic Assurance Logon** or **FIDO High Assurance Logon** option must be set to Yes.

For more information on setting up MyID for FIDO logon, see the *Configuring MyID for FIDO logon* section in the ***Passkey Integration Guide***.

3.2.5 Signing in using single-use authentication codes

For an operator to sign in to MyID using the MyID Operator Client with an authentication code:

- The operator's MyID account must be enabled in MyID.
- To receive an email message or SMS containing the authentication code, the operator must have an email address or cell phone number recorded, and MyID must be configured to send email or SMS notifications.
- In MyID Desktop, in **Configuration > Edit Roles**, the operator's role must have the **Authentication Code** logon mechanism assigned.
- In MyID Desktop, in **Configuration > Edit Roles**, the operator's role must have access to one or more features in the MyID Operator Client.

  See section *3.5*, *Roles and groups* for details of which roles in MyID Desktop map to features in the MyID Operator Client.

For more information on setting up MyID for authentication code logon, see the *Configuring authentication codes for the MyID authentication server* section in the ***Administration Guide***.

3.2.6 Signing in using Windows authentication

For an operator to sign in to MyID using their Windows credentials:

- The operator's MyID account must be enabled in MyID.
- In MyID Desktop, in **Configuration > Edit Roles**, the operator's role must have the **Windows Logon** mechanism assigned.
- In MyID Desktop, in **Configuration > Edit Roles**, the operator's role must have access to one or more features in the MyID Operator Client.

  See section *3.5*, *Roles and groups* for details of which roles in MyID Desktop map to features in the MyID Operator Client.
- In MyID Desktop, in **Configuration > Security Settings > Logon Mechanisms** tab, the **Integrated Windows Logon** option must be set to Yes.
- The operator's browser must be configured to pass on their Windows credentials; see section *3.2.6.1*, *Configuring browsers for Windows authentication*.
- 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.
- The user must not be a member of the Protected Users group in Active Directory; see the *Protected Users group in Active Directory* section in the ***Administration Guide***.

3.2.6.1 Configuring browsers for Windows authentication

By default, browsers do not pass your Windows authentication details to websites. You must configure your browser to allow it to send this information to the MyID website, or the browser will display a pop-up prompting for your Windows username and password.

You may want to configure the browsers for your organization using Group Policy.

To configure your browser for Windows authentication:

- For Chrome:

  Set the `AuthServerAllowlist` key in the Windows registry to include the location of the MyID web server:

  ```
  Windows Registry Editor Version 5.00

  [HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome]
  "AuthServerAllowlist"="myserver.domain.com"
  ```

  If the setting does not already exist, you can add it. If the setting already exists, add the MyID web server to the list. You can include several server names by separating them with commas, and can include `*` as a wildcard. For example:

  `"AuthServerAllowlist"="*.domain.com,myserver2.domain2.com"`

  Note: You must restart the PC after making the registry change to ensure that Chrome picks up the latest settings.

  Alternatively, you can specify the MyID web server on the command line; for example:

  `chrome.exe --auth-server-allowlist="myserver.domain.com"`

  Note: Chrome 85 and earlier use `AuthServerWhitelist` in the registry and `--auth-server-whitelist` on the command line instead.

- For Firefox:

  1. In the Firefox browser address bar, type:

     `about:config`

  2. Click **Show All**.
  3. Set the following options:
     - `network.automatic-ntlm-auth.trusted-uris` – type the server name of the MyID web server. You can include several server names by separating them with commas.
     - `network.automatic-ntlm-auth.allow-proxies` – set to TRUE.
     - `network.negotiate-auth.allow-proxies` – set to TRUE.

- For Edge:
  1. In Internet Options, on the **Security** tab, add the MyID web server to the **Local Intranet** list.
  2. Ensure the following options are set:
     - **Security** tab:

       Local Intranet > Custom Level > User Authentication > Logon > Automatic logon only in Intranet zone
     - **Advanced** tab:

       Security > Enable Integrated Windows Authentication

3.2.7 Signing in using an external identity provider

You can configure MyID to set up an external OpenID Connect identity provider (for example, Microsoft Entra or Google) to provide authentication to the MyID Operator Client or any other system that uses the MyID web.oauth2 authentication service.

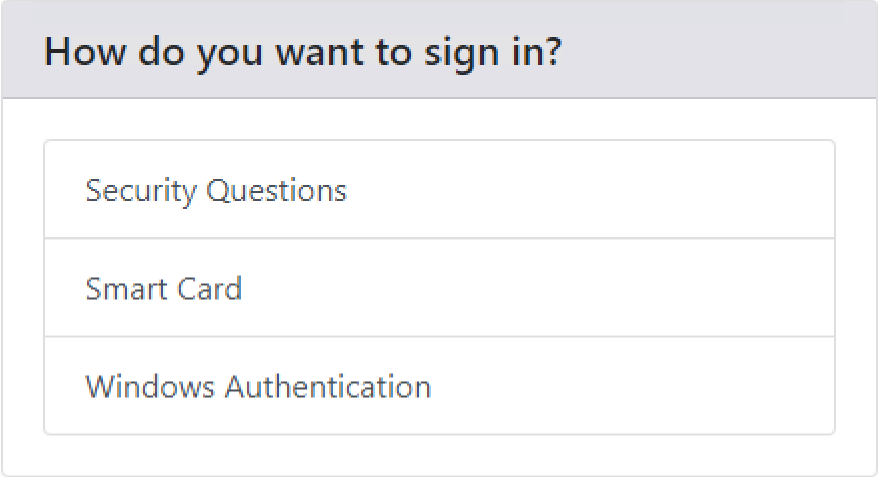
See the *Setting up an external identity provider* section in the ***MyID Authentication Guide*** for details.

3.2.8 Signing in to MyID

To sign in to MyID:

1. From the MyID Operator Client landing page, click **Sign In**.

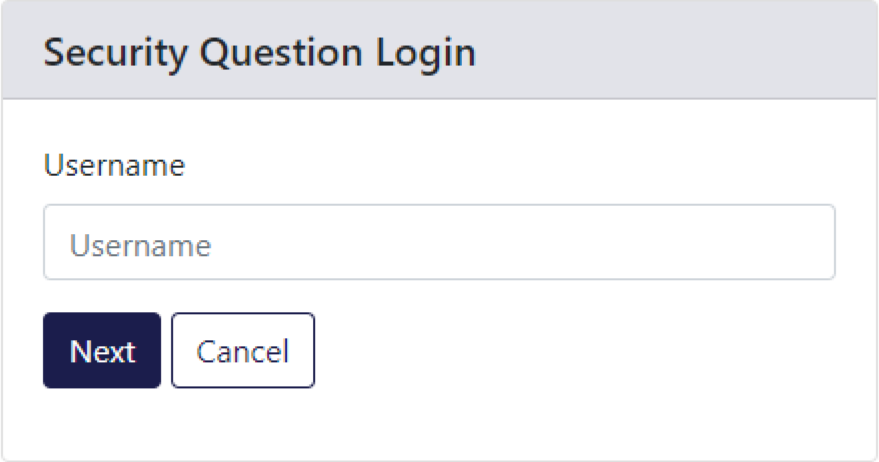
   If more than one logon mechanism is configured for your system, you are prompted to select which one to use.

   How do you want to sign in?

   Security Questions
Smart Card
Windows Authentication

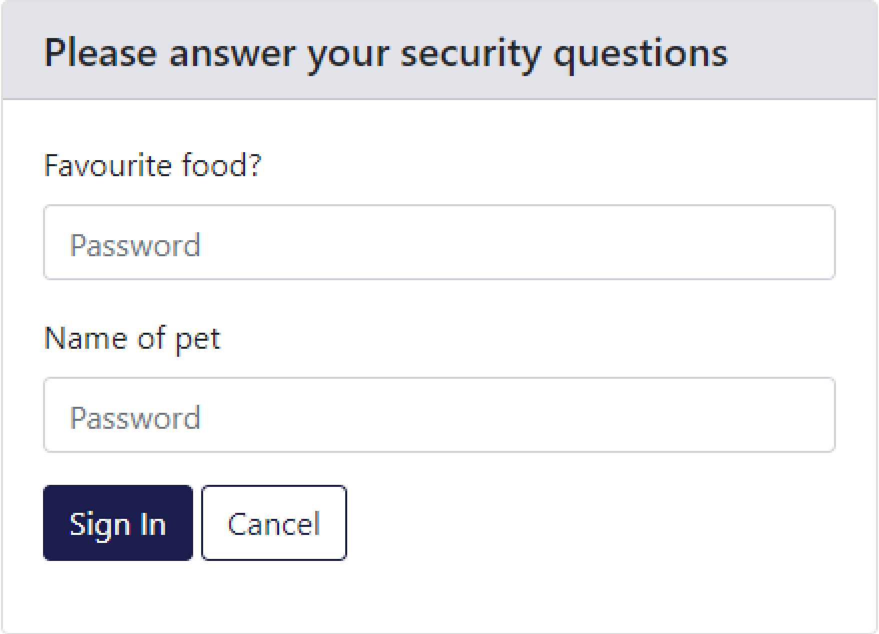
2. To log on with security questions:
   a. Select the **Security Questions** logon mechanism.
   b. Type your **Username**:

      Security Question Login

      Username
Username
Next
Cancel

   c. Click **Next**.
   d. Type the responses to your security questions:


Please answer your security questions
Favourite food?
Password
Name of pet
Password
Sign In
Cancel

The number of security questions you must answer depends on the **Number of security questions for self-service authentication** configuration option. If you have more security phrases recorded than are required (for example, if you have four security phrases recorded, and you need two to log on) MyID prompts you for a random selection of questions.

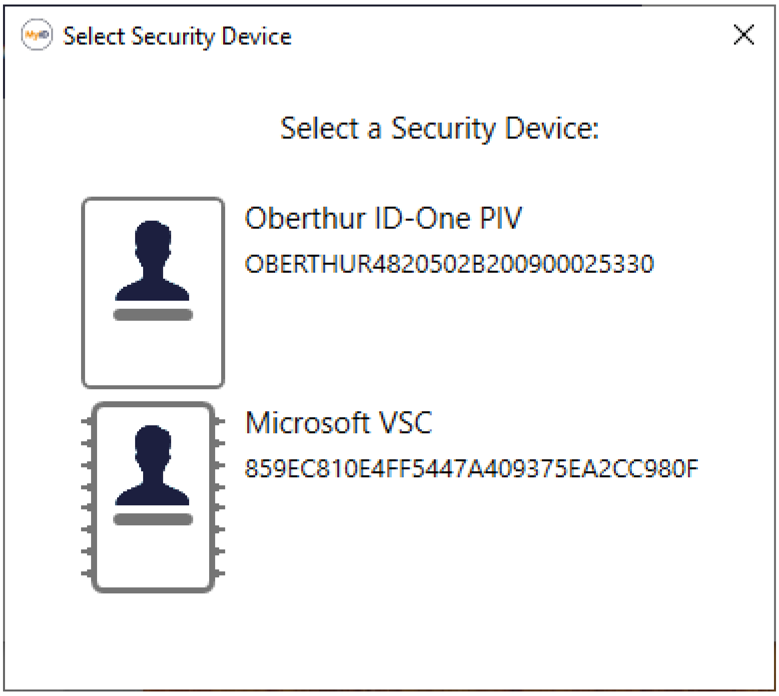
e. Click **Sign In**.

   The MyID Operator Client dashboard appears.

3. To log on with a smart card or VSC:

a. Select the **Smart Card** logon mechanism.

b. The Select Security Device dialog appears, listing all of the smart cards (including virtual smart cards) currently attached to your PC.



Select Security Device

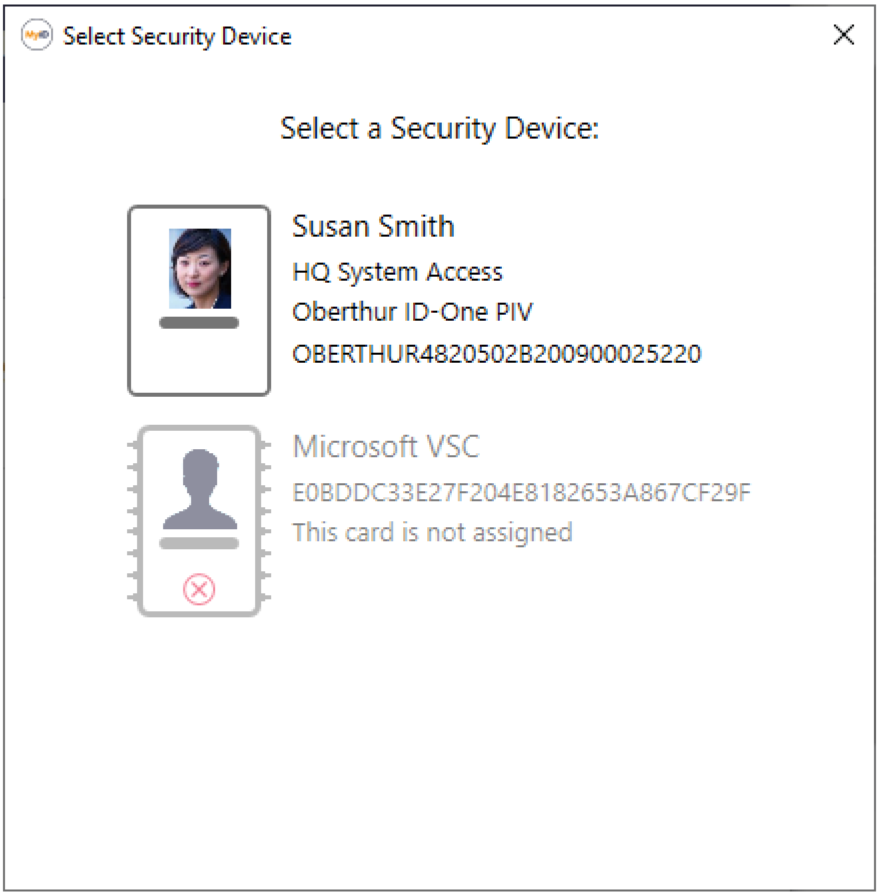
Select a Security Device:

Oberthur ID-One PIV
OBERTHUR4820502B200900025330

Microsoft VSC
859EC810E4FF5447A409375EA2CC980F

If there is a **Device Friendly Name** specified in the credential profile that was used to issue the device, this is displayed next to the smart card.

Note: You can set the **Show Full Name at Logon** and **Show Photo at Logon** options (on the **Logon** page of the **Security Settings** workflow) to configure this screen to display the associated user image and full name of the cardholder.



Select Security Device

Select a Security Device:

Susan Smith
HQ System Access
Oberthur ID-One PIV
OBERTHUR4820502B200900025220

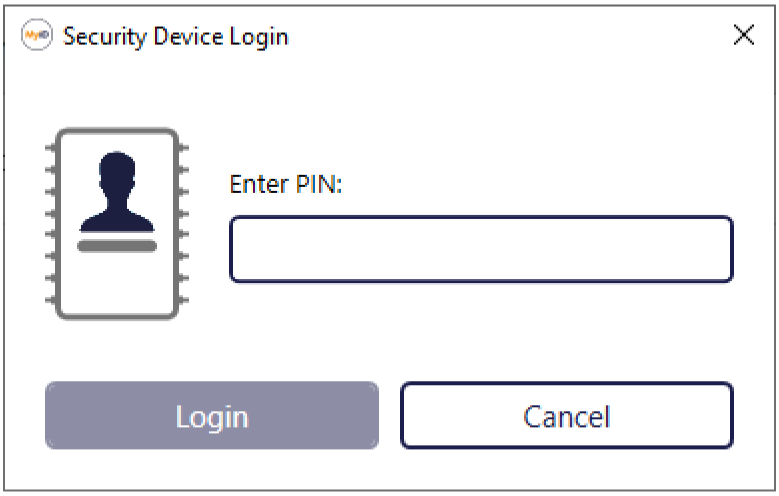
Microsoft VSC
E0BDDC33E27F204E8182653A867CF29F
This card is not assigned

Note: If you enable this feature, it is possible to obtain user photos and cardholder names without authentication.

c. Select the smart card you want to use to log on.

You can log in with a physical smart card inserted into a card reader on your PC, or with a virtual smart card (VSC) installed on your PC.

You must now authenticate to your security device.


Security Device Login
Enter PIN:
Login
Cancel

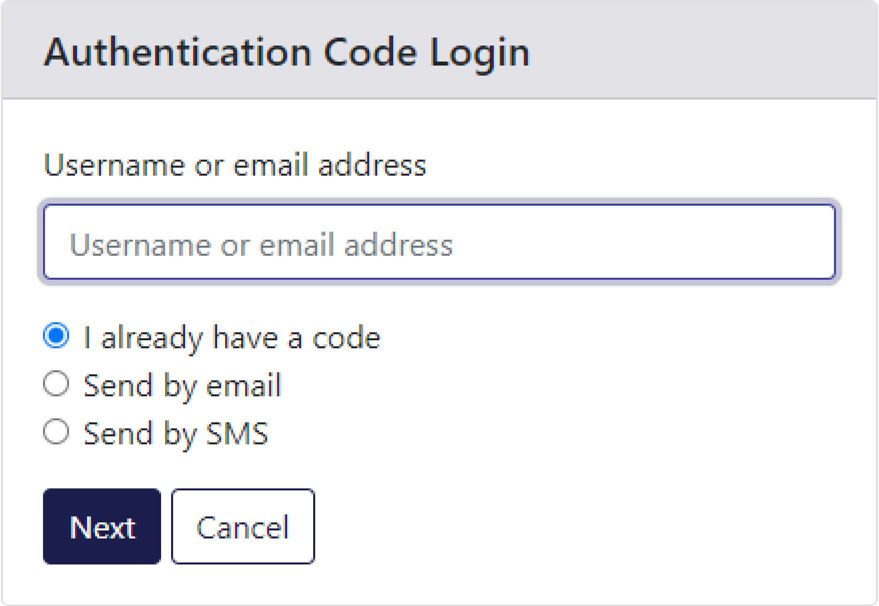
d. Type your PIN, then click **Login**.

   The MyID Operator Client dashboard appears.

4. To log in with an authentication code:

   a. Select the **Authentication Code** logon mechanism.

      The Authentication Code Login screen appears:


Authentication Code Login
Username or email address
Username or email address
● I already have a code
○ Send by email
○ Send by SMS
Next
Cancel

   b. Type your **Username or email address**.

   c. Select the option for obtaining your authentication code:

      - **I already have a code** – select this option if you have already been provided with an authentication code.
      - **Send by email** – select this option if you want to receive your code in an email message to the email address stored in your person record in MyID. This option is available only if the **Self Requested Authentication Code Email** email template is enabled.

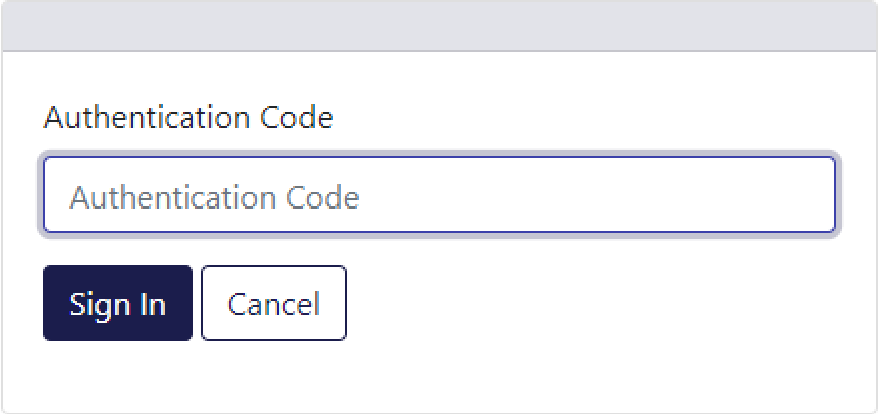
- **Send by SMS** – select this option if you want to receive your code in an SMS message to the cell phone number stored in your person record in MyID. This option is available only if the **Self Requested Authentication Code SMS** email template is enabled.

If neither the email nor SMS options appear, you can still use an authentication code to log on if an operator requests one on your behalf.

Note: The complexity of the code is determined by the **Complexity** option configured in the email template. See the *Changing email messages* section in the ***Administration Guide*** for details.

d. Click **Next**.

The authentication code entry screen appears:



e. Type your **Authentication Code**, and click **Sign In**.

The MyID Operator Client dashboard appears.

5. To log in with your Windows credentials:

   a. Select the **Windows Authentication** logon mechanism.

   Note: This logon mechanism supports single-click login. If the only logon mechanism available is Windows authentication, when you click **Sign In** on the landing page, the MyID Operator Client completes the sign-in process without further interaction.

   b. MyID checks your Windows authentication.

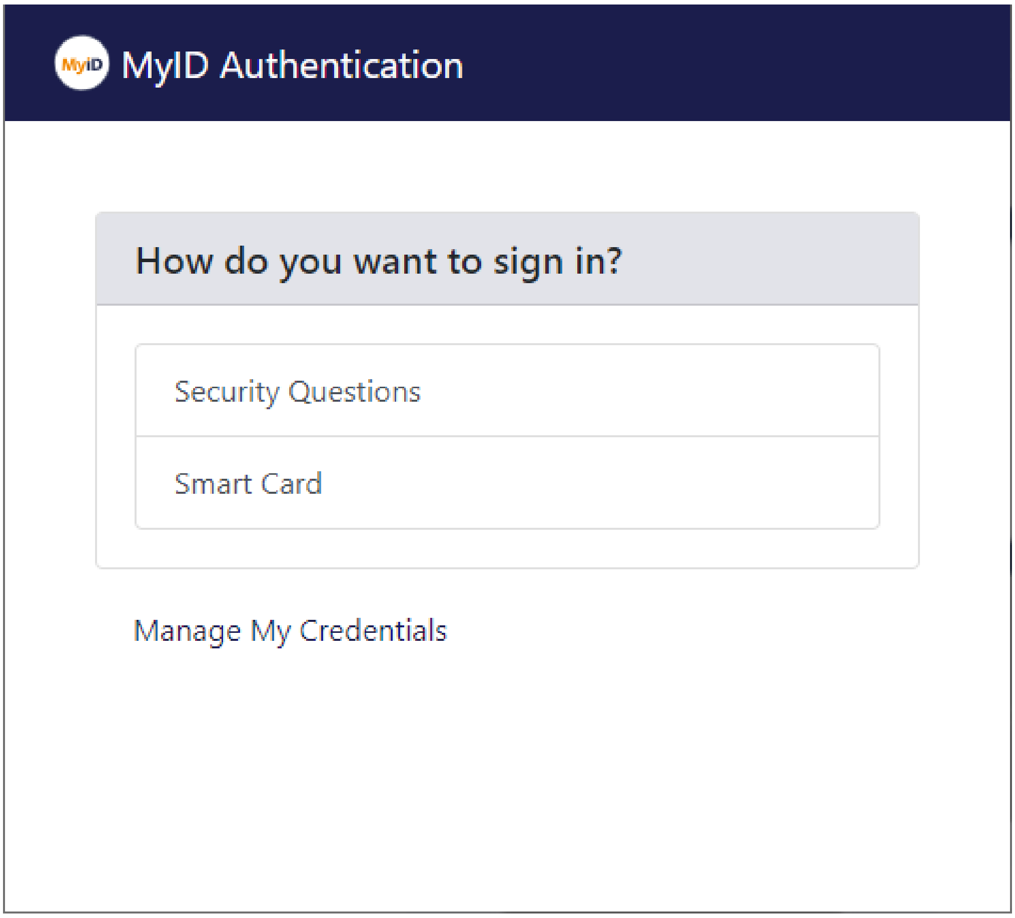
   Note: If a popup appears asking for your Windows username and password, you may not have configured your browser correctly. See section *3.2.6.1*, *Configuring browsers for Windows authentication*.

   The MyID Operator Client dashboard appears.

3.2.9 Managing your credentials from the MyID Authentication screen

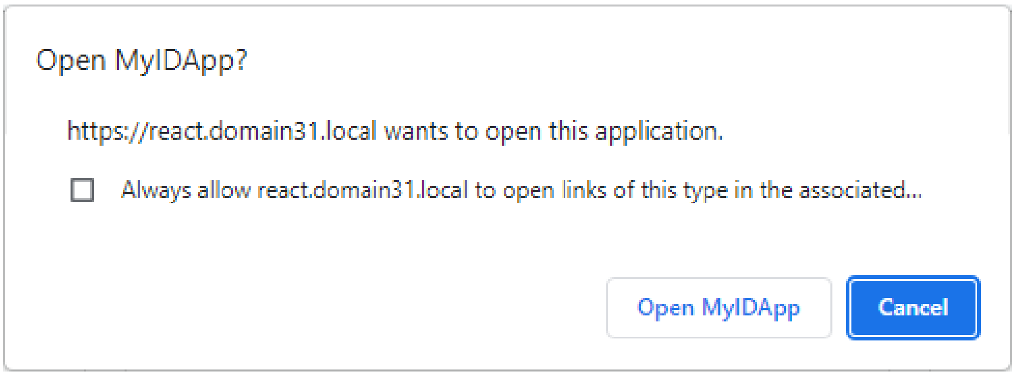
To carry out self-service operations on your credentials (for example, changing your security phrases, or resetting your device PIN) before signing in to the MyID Operator Client, click the **Manage My Credentials** option on the MyID Authentication screen.

Note: The **Allow Self-Service at Logon** configuration option (on the **Logon** tab of the **Security Settings** workflow) must be set for this option to appear.


MyID Authentication
How do you want to sign in?
Security Questions
Smart Card
Manage My Credentials

You must have the MyID Self-Service App installed, and the MyID Client Service app installed and running, to use this feature.

Depending on your browser settings, you may need to confirm that you want to allow the browser to open the Self-Service App; for example:



Open MyIDApp?

https://react.domain31.local wants to open this application.

☐ Always allow react.domain31.local to open links of this type in the associated...

The MyID Self-Service App starts. For more information, see the ***Self-Service App*** guide.

3.2.10 Timeouts and re-authentication

When you authenticate to the MyID Operator Client, for example by using your smart card, or by typing your username and security questions, you are granted access for one hour (3600 seconds). However, if you continue working with the MyID Operator Client, this access can be extended every time you make a call to the server; for example, by opening a new screen, saving data, or running a report. You can extend your authentication period at any point up to two hours (7200 seconds) after last using the MyID Operator Client.

However, if you attempt to use the MyID Operator Client *more* than two hours after last using it, you must re-authenticate to be able to continue. The MyID Authentication dialog appears, and you must provide your authentication details; once you have done so, you can carry on working with the MyID Operator Client.

Important: You must authenticate with the same user *and* the same logon method. If you authenticate with a different user or logon method, the operation is canceled, and you are returned to the main screen.

Extended authentication is available only for sessions in the same tab or window for security reasons; if you open another tab or window, when the initial access period (one hour) expires, you must re-authenticate, after which you can continue to extend the authentication in that tab or window as before.

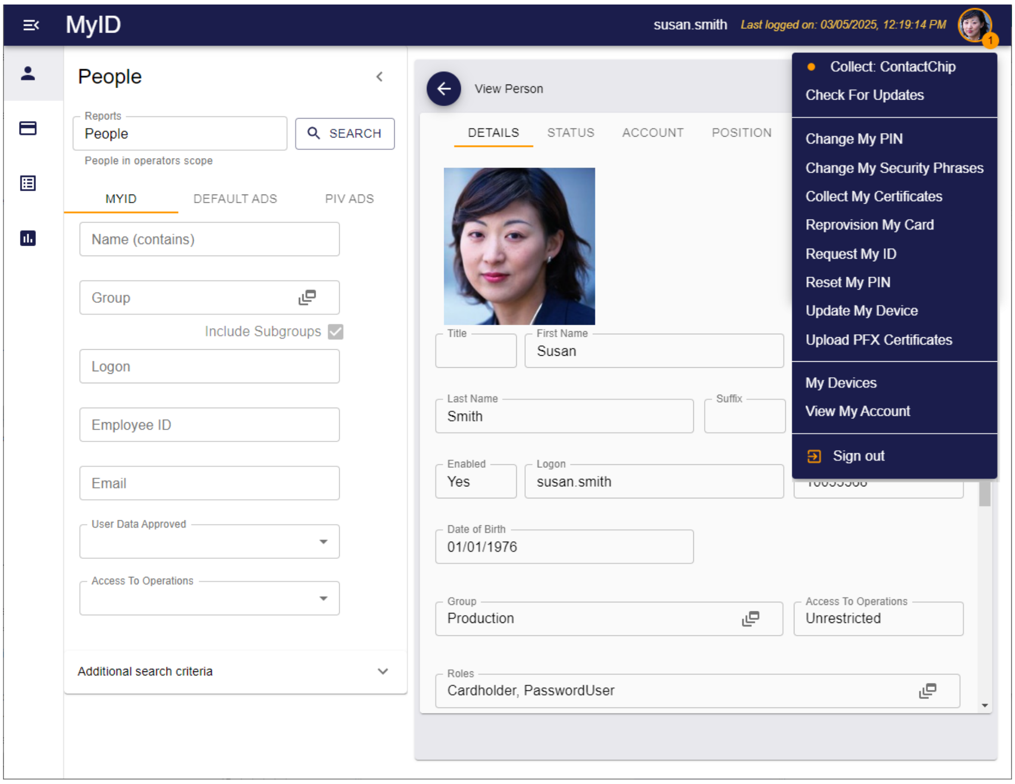
If you sign out, or close the browser window, you must re-authenticate when you want to continue using the MyID Operator Client.

There is a limit of 6 days (518400 seconds) beyond which you cannot continue to extend the authenticated session. If you reach this limit (for example, with an automated system), you must re-authenticate before you can continue working with the MyID Operator Client.

If you want to change the default access period, extension period, or limit, you can edit the application settings file for the web.oauth2 web service; see section *19.4.15*, *Configuring re-authentication timeout periods*.

If you want to disable this feature, you can edit the MyID Operator Client settings file; see section *19.4.16*, *Enabling or disabling re-authentication*.

3.3 MyID Operator Client user interface


MyID
People
SEARCH
MYID
DEFAULT ADS
PIV ADS
Name (contains)
Group
Include Subgroups ☑
Logon
Employee ID
Email
User Data Approved
Access To Operations
Additional search criteria
View Person
DETAILS
STATUS
ACCOUNT
POSITION
Collect: ContactChip
Check For Updates
Change My PIN
Change My Security Phrases
Collect My Certificates
Reprovision My Card
Request My ID
Reset My PIN
Update My Device
Upload PFX Certificates
My Devices
View My Account
Sign out

susan.smith *Last logged on: 03/05/2025, 12:19:14 PM*

Reports: People
People in operators scope

Title:
First Name: Susan
Last Name: Smith
Suffix:
Enabled: Yes
Logon: susan.smith
Date of Birth: 01/01/1976
Group: Production
Access To Operations: Unrestricted
Roles: Cardholder, PasswordUser

The MyID Operator Client comprises the following elements:

- Title bar
- Self-service menu
- Category list
- Search form
- Display form

In the title bar, you can:

- Toggle the display of the category list and the search form, click the tray button:

Button	Action
≡<	Hide the category list and search form.
≡	Display the category list and search form.

- Click **MyID** to return to the landing screen.

  Note: This label is translatable, so your system administrator may have changed the **MyID** label; for example, there may be different labels for your pre-production system and your production system. For information about translating the MyID interface, contact customer support quoting reference SUP-138.

- See the logon name of the currently logged-on operator.
- See the last logon time of the currently logged-on operator.

In the self-service menu, you can:

- Click the user icon to open or close the menu.
- Collect any self-service requests.
- Carry out other self-service tasks; for example, changing your device PIN.
- View a list of your own devices.
- View your own account.
- Sign out.

See section *18*, *Carrying out self-service operations* for details.

In the category list, you can:

- Click the category to display the appropriate search form; for example, click **People** to display the People search form. The **More** category contains links to administrative workflows in MyID Desktop, organized into several sub-categories; see section *17*, *Launching administrative workflows*.

In the search form, you can:

- Complete any search details and click **Search**.
- On the appropriate form, click **Add** to add a new person or **Read Card** to view details of a device.
- Click the **<** button at the top to hide the search form.

  The form hides automatically when you select a item in the search results. Click **>** to display the form again.
- Click the tabs to display different search options; for example, you can choose whether to search the MyID database or an attached directory, if your system is set up to do so. If there are more tabs than can be displayed on screen, click the **>** and **<** buttons to change the displayed tabs.
- Select **Additional search criteria** to display more search options. Select the additional criteria to add them to the search form. Click the close **x** buttons on the additional criteria to remove them from the search form.

In the display form, you can:

- Work with tables of search results.

  See section *3.4*, *Working with tables of records*.
- View details of the selected record.
- Click the tabs to display different categories of information about the selected record. If there are more tabs than can be displayed on screen, click the **>** and **<** buttons to change the displayed tabs.
- To cancel an action form (for example, Edit Person or Request Device Issuance) and return to the viewing form, click the close button:

✕

- To close a viewing form and return to the search results list, click the back button:

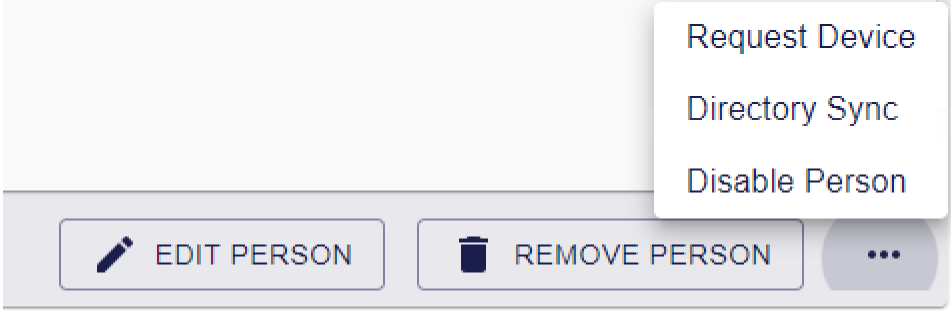
  ←

  You can use the back button to step back through several viewing forms. For example, if you view a person, click on a link to one of their devices, then click on a link for open requests for that device, you can click back to go back to the device, then back to go back to the person.

3.3.1 Using the button bar

Use the buttons at the bottom of the form to carry out actions on the selected item; for example, you can edit a person's user account, or request a device.

The options available depend on your system configuration, the status of the item you are viewing, and your role permissions. The button bar displays the four most relevant actions; click the **...** option to display more available actions.



Note: You can change the number of buttons displayed in the button bar. See section *19.4.14*, *Changing the number of buttons displayed in the button bar*

3.3.2 Launching MyID Desktop, Self-Service App, or MyID Client for Windows workflows

Some operations listed on the button bar (for example **Reset Card PIN**) and operations in the self-service menu are carried out by launching a MyID Desktop workflow, or a Self-Service App or MyID Client for Windows action; this allows you to perform activities in MyID Operator Client (such as interacting with smart cards) that are implemented in a native client rather than the browser. To use these features, you must have the MyID Client Service, MyID Desktop, and the Self-Service App or the MyID Client for Windows installed.

As the Self-Service App and the MyID Client for Windows carry out the same operations, by default the MyID Client Service determines which application to use by checking first if the Self-Service App is installed, and if not, checking whether the MyID Client for Windows is installed. If you want to change this priority, you can set a configuration option; see section *19.4.20*, *Configuring the priority for self-service applications*.

Note: If you have not installed MyID Desktop or the Self-Service App to their default locations, you must configure the MyID Client Service with its installed location; see section *19.4.10*, *Setting the location of MyID Desktop or the Self-Service App* for details. If you have used an MSIX installer, the MyID Client Service uses the registered locations for MyID Desktop, the Self-Service App, or the MyID Client for Windows, so you do not need to set the location of the applications.

When you launch MyID Desktop, the Self-Service App, or the MyID Client for Windows from the MyID Operator Client, the application is authorized to carry out a single task; for example, resetting a card's PIN. When you have completed the task and clicked **Finish**, the application window closes and control is returned to the MyID Operator Client window. If you close the MyID Operator Client browser window after launching the application, you can still complete the single task; it does not rely on the browser window remaining open.

Important: To use this feature, you must upgrade your MyID Client Service, MyID Desktop, Self-Service App, and MyID Client for Windows software to the latest versions.

3.3.3 Displaying dates and times

Dates and times are displayed in the MyID Operator Client based on the server settings rather than the browser or operating system settings.

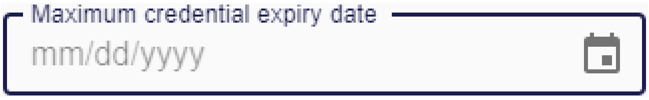
By default, the MyID Operator Client uses the following date and time format:

- `MM/dd/yyyy, hh:mm:ss a` – for example, `09/18/2021, 8:58:11 AM`.

If you want to use different time and date formats, for example for different locales, you can customize the server dictionaries; contact customer support quoting SUP-138 for details.

3.3.4 Entering dates and times

To edit a date on a form, you can type the date into the field. When you click within an empty field, the expected format is shown:

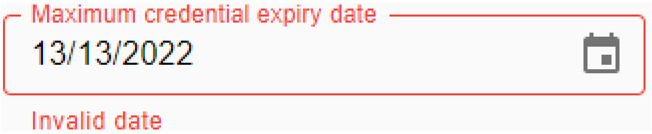


Maximum credential expiry date

mm/dd/yyyy

Important: If you have customized the date format on your server, the display format and the date entry format may be different. The date display format is determined by the server settings, while the date entry format is determined by your browser locale.

If you type an invalid date, the field displays a warning:



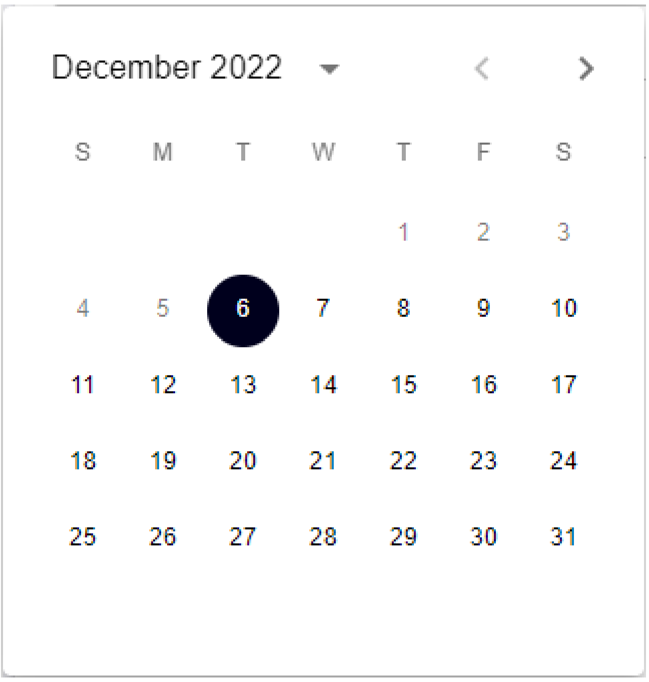
Maximum credential expiry date

13/13/2022

Invalid date

To select the date instead of typing it, you can click the calendar button:

This displays the calendar control:



December 2022

S	M	T	W	T	F	S
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Select the date you want to use, then click **OK**.

Note: The accepted range for all dates is January 1 1900 to January 1 2100.

3.3.5 Using the browser location bar

The location bar of your browser updates with the current location within the MyID Operator Client website. You can bookmark these links, or send them to other operators; when you click on these links, you authenticate to the MyID Operator Client website if necessary, then open the page at the correct location, if your role and scope permissions allow you to do so, and the specified item still exists.

For example, you can create links for the following:

- The front page.

  For example:

  `https://servername/MyID/OperatorClient/#/`

- A particular category.

  For example:

  `https://servername/MyID/OperatorClient/#/people`

  `https://servername/MyID/OperatorClient/#/devices`

  `https://servername/MyID/OperatorClient/#/requests`

- A set of search criteria.

  For example:

  `https://servername/MyID/OperatorClient/#/people?logonName=*don*`

  `https://servername/MyID/OperatorClient/#/people?groupId=6480C875-C564-4B8E-A761-E373181F13DA&includeSubgroups=1`

  `https://servername/MyID/OperatorClient/#/requests?status=Awaiting+Validation`

  This allows you to bookmark frequently-used search screens. For example, you may want to create a search for people in a particular group, users whose logon name contains a particular string, or a list of requests that are awaiting validation.

- A sorted search.

  For example:

  `https://servername/MyID/OperatorClient/#/people/reports/100102?order_by=-groupName%2C%2Bsurname`

  The `order_by` parameter takes a comma-delimited list of the field names by which you want to sort. Prefix the field name by `-` to sort descending, or `+` to sort ascending. You must URL-encode the delimiting commas as `%2C` and the `+` signs as `%2B`.

  You can specify the sort criteria using the MyID Core API using the `order_by` parameter.

- A particular person, device, or request.

  For example:

  `https://servername/MyID/OperatorClient/#/people/0F3E10FE-8B80-4FA4-BF21-556A4E370C6F`

  `https://servername/MyID/OperatorClient/#/requests/27A62218-A95B-45FF-A722-F70FB2273E70`

This allows you to send a link to another operator; for example, you may have raised a device request for a person that requires validation. You cannot validate the device request as you raised it, so you can ask another operator to validate the request, and provide a link to the request to make it easy for them to locate.

- An action on a particular person, device, or request.

  For example:

  `https://servername/MyID/OperatorClient/#/people/0F3E10FE-8B80-4FA4-BF21-556A4E370C6F/100107`

- An Add button action.

  For example:

  `https://servername/MyID/OperatorClient/#/people/add`

- If you want to open the screen with the category list and search form hidden, for example if you are embedding the MyID Operator Client screen in an iframe on your intranet page, you can add `/embedded` after the `#` in the URL; for example:

  `https://servername/MyID/OperatorClient/#/embedded/people/0F3E10FE-8B80-4FA4-BF21-556A4E370C6F`

  Note: Each embedded MyID Operator Client screen requires authentication. If you want to avoid having to authenticate each time, you can configure the MyID authentication server to allow you to request an access token, then pass that to the embedded Operator Client screen; see the *Authenticating for embedded Operator Client screens* section in the ***MyID Authentication Guide*** for details.

3.3.6 Opening a new tab or window

If you have a list of search results, you can right-click on an item in the list, then select either **Open in a new tab** or **Open in a new window** from the pop-up menu; the MyID Operator Client opens a new tab or window at the appropriate location.

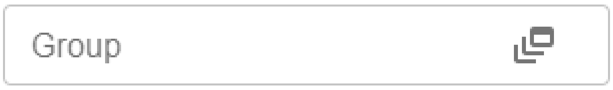
You can also right-click on buttons to open in a new tab or window if the action of the button would be to open a new screen; for example, you can right-click **Request Device**, which opens the Request Device Issuance screen, but you cannot open **Directory Sync** in a new tab or page, as this action does not open a new screen.

Note: When you open a screen in a new tab or new window, the category list and search form are automatically hidden. To toggle the display of the category list (and search form, if appropriate), click the tray button:

≡

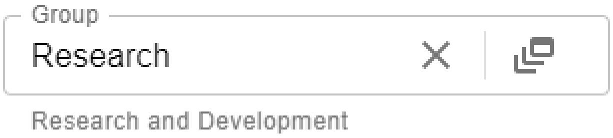
3.3.7 Selecting a group

The **Group** option appears on several forms:



Click the box to open the Group dialog, which allows you to select a group from the MyID database or from your directory.

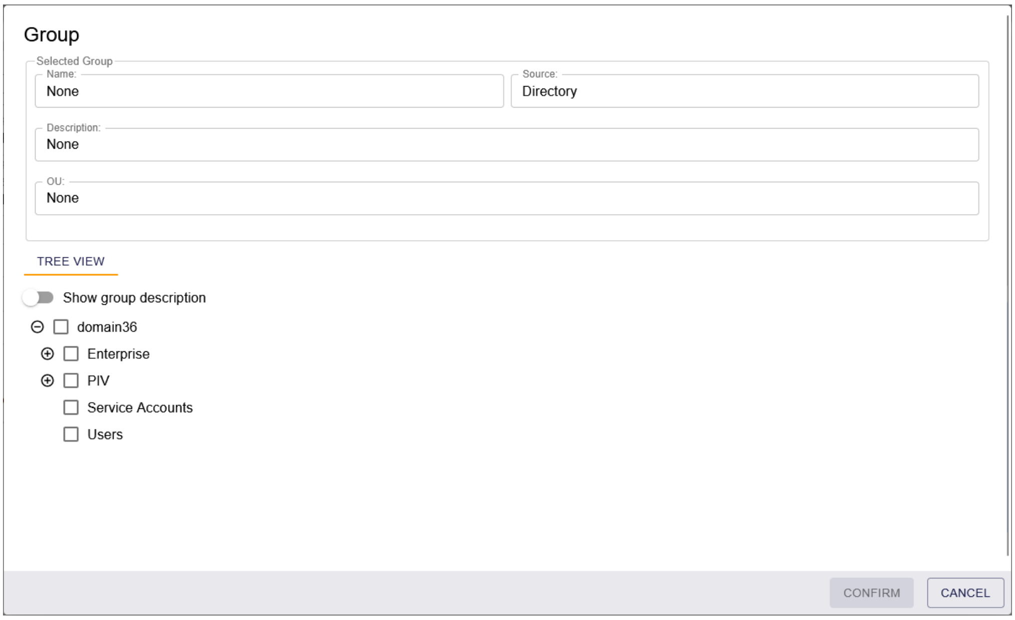
Once you have selected a group, its name appears in the box; if the group has a description, it is displayed beneath the box.



Group
Research
Research and Development

3.3.7.1 Selecting a group from a directory

When you are viewing the groups from a directory (for example, when searching for a person and you have selected a directory rather than the MyID database), MyID displays a hierarchical list of the groups in the directory, with the **Source** set as **Directory** in the **Selected Group** section of the dialog.



Group

Selected Group

Name: None

Source: Directory

Description: None

OU: None

TREE VIEW

Show group description

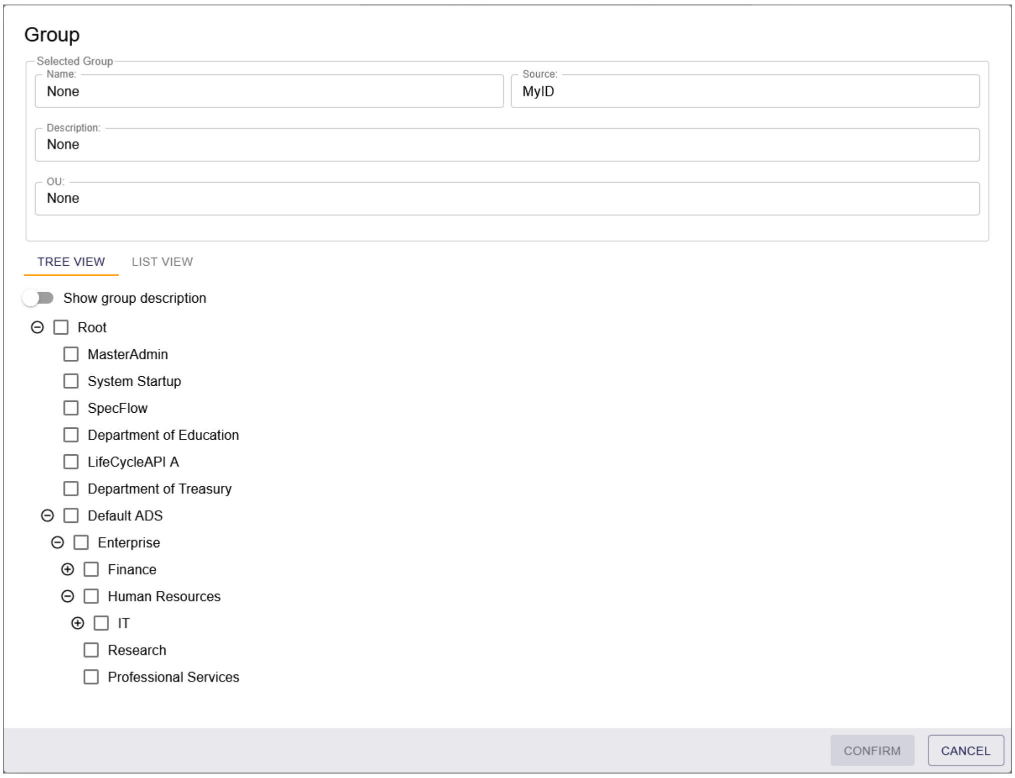
⊖ ☐ domain36
  ⊕ ☐ Enterprise
  ⊕ ☐ PIV
  ☐ Service Accounts
  ☐ Users

- Click the expand group icon ⊕ to expand a group
- Click the close group icon ⊖ to close a group.
- Click **Show group description** to display the descriptions for the groups instead of their names.

  Note: If a group does not have a description, its name is displayed instead.
- Select a group from the tree; the name, description, and OU of the group are displayed in the **Selected Group** section of the dialog.
- Click **Confirm** to confirm your selection and close the dialog.

3.3.7.2 Selecting a group from the MyID database

When you are viewing the groups from the MyID database (for example, when searching for a person in MyID, or selecting the group for a device or request), MyID displays a hierarchical list of the groups in the database, with the **Source** set as **MyID** in the **Selected Group** section of the dialog.



Group

Selected Group

Name: None

Source: MyID

Description: None

OU: None

Show group description

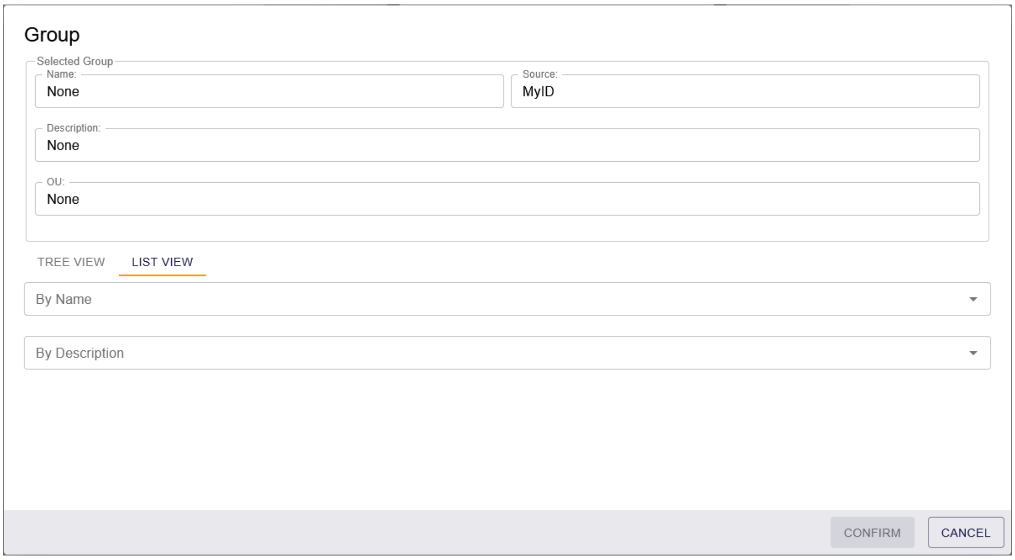
- ⊖ ☐ Root
  - ☐ MasterAdmin
  - ☐ System Startup
  - ☐ SpecFlow
  - ☐ Department of Education
  - ☐ LifeCycleAPI A
  - ☐ Department of Treasury
  - ⊖ ☐ Default ADS
    - ⊖ ☐ Enterprise
      - ⊕ ☐ Finance
      - ⊖ ☐ Human Resources
        - ⊕ ☐ IT
        - ☐ Research
        - ☐ Professional Services

- Click the expand group icon ⊕ to expand a group
- Click the close group icon ⊖ to close a group.
- Click **Show group description** to display the descriptions for the groups instead of their names.

  Note: If a group does not have a description, its name is displayed instead.
- Select a group from the tree; the name, description, and OU of the group are displayed in the **Selected Group** section of the dialog.
- Click **Confirm** to confirm your selection and close the dialog.

Note: If your system is configured for administrative groups, you can also select any of the groups for which you have administrative access, even if they are not within your own scope. Administrative groups are displayed at the bottom of the list in a separate node. For more information, see section *4.9*, *Working with administrative groups*.

As an alternative to the hierarchical tree view, you can display the available groups as a drop-down list; select the **List View** option.



Group

Selected Group

Name: None

Source: MyID

Description: None

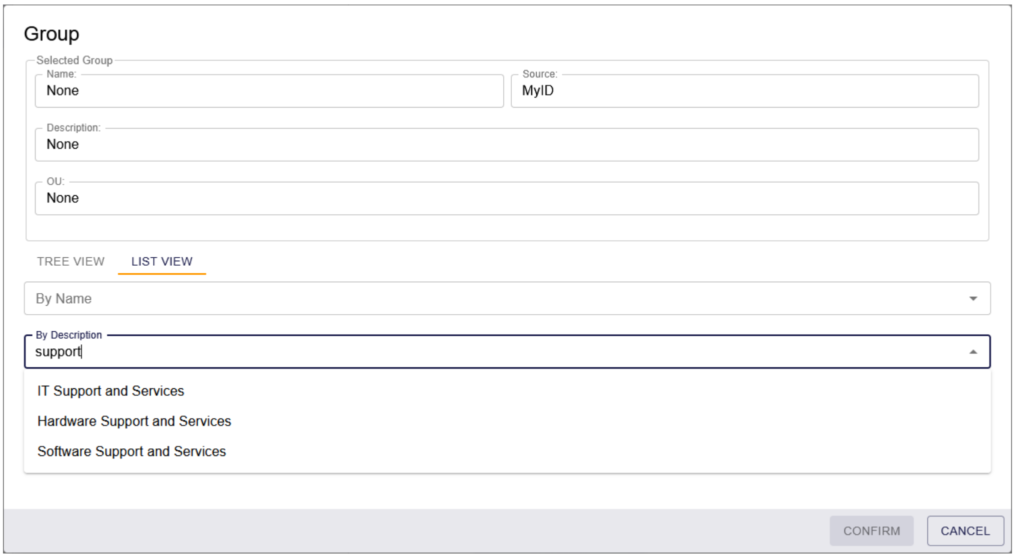
OU: None

TREE VIEW
LIST VIEW
By Name
By Description
CONFIRM
CANCEL

Select a group name from the **By Name** drop-down list, or select a group description from the **By Description** drop-down list.

You can type in the box to filter the available values; for example, typing `support` may return:

- IT Support and Services
- Hardware Support and Services
- Software Support and Services



Group

Selected Group

Name: None

Source: MyID

Description: None

OU: None

By Description: support

IT Support and Services

Hardware Support and Services

Software Support and Services

TREE VIEW
LIST VIEW
By Name
CONFIRM
CANCEL

Note: If a group does not have a description, it does not appear in the **By Description** drop-down list; you must select it from the **By Name** drop-down list instead.

3.4 Working with tables of records

The MyID Operator Client displays tables of records in the following places:

- In search results forms.

  For example, when you select the **People** search, or the **Issued Devices by Category** report.

  Search results are displayed in pages. Scroll to retrieve the next page of results automatically. The number of displayed results is shown at the top of the form.

  If more results are available, the text **(scroll for more)** appears; for example:

  `257 results - 50 displayed (scroll for more)`

  You can select a record from the search results to open the viewing form; for example, View Person or View Device.
- In secondary search forms.

  For example, when searching for a device to assign to a request.
- In data tables.

  For example, on the **Devices** tab of the View Person screen.
- In batch results.

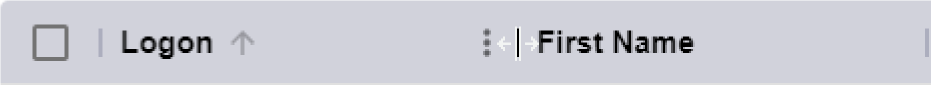
  For example, after requesting devices for multiple people.

3.4.1 Working with columns

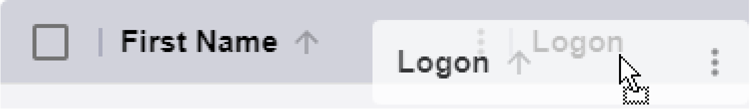
You can resize, move, or show and hide the columns in the display.

3.4.1.1 Resizing and moving columns

To resize a column, click the sizing bar between columns, and drag the column to the required size.



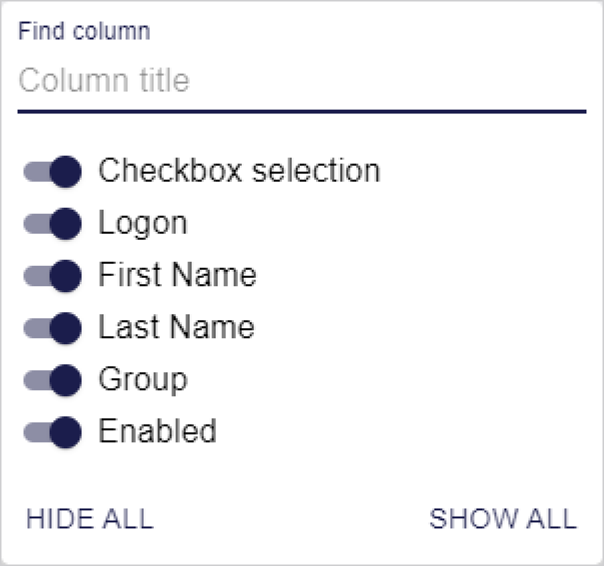
To move a column, click the column, and drag it to the required position.



3.4.1.2 Displaying and hiding columns

You can choose to display or hide each column on the display. This allows you to concentrate on the information that is important to you and to reduce on-screen clutter.

To display or hide multiple columns at the same time, use the column selector; click the **Columns** ▥ button. You can also open this selector by clicking the three dot menu option on any column and selecting **Manage columns**. The three dot menu option is visible when you hover your mouse over the column title.



Find column
Column title
Checkbox selection
Logon
First Name
Last Name
Group
Enabled
HIDE ALL
SHOW ALL

You can filter the list of columns by typing in the **Find column** field.

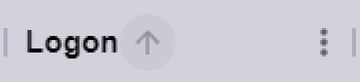
Select a column to display it, or deselect the column to hide it.

You can also click **Hide All** or **Show All** to hide or display all the columns.

To hide a single column, click the three dot menu option on the column you want to hide, then select **Hide column** from the pop-up menu.

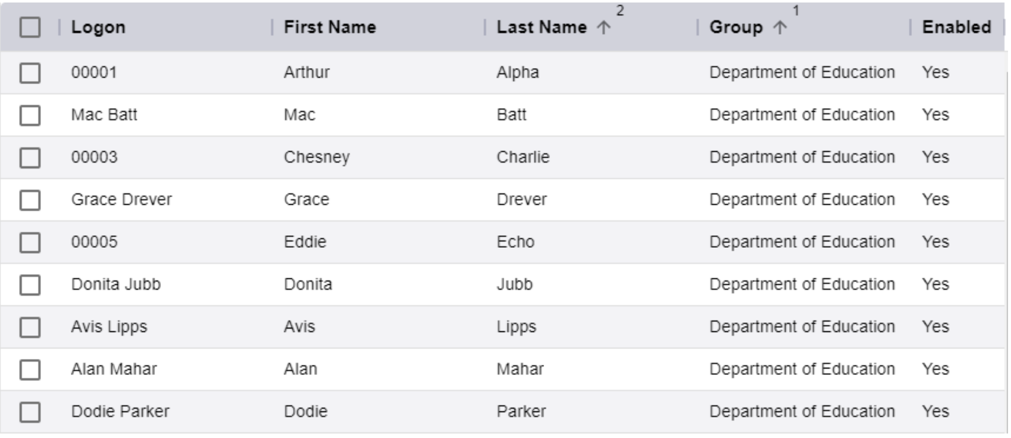
3.4.2 Sorting

Note: Not all columns are sortable. If a column is sortable, the sorting arrow appears when you hover your mouse pointer over the header tile.



To sort a column, click the header tile. Click once to sort ascending, again to sort descending, and again to stop sorting. Alternatively, you can sort ascending or descending by clicking the three dot menu option and selecting **Sort by ASC** or **Sort by DESC** from the pop-up menu.

You can sort by multiple columns. For example, in the People report, sort by **Last Name**, then sort by **Group**, and MyID sorts the records by last name within their groups. The sort indicators include numbers to show you the precedence of the sort; the most recent sorted column takes precedence.



☐	Logon	First Name	Last Name ↑ 2	Group ↑ 1	Enabled
☐	00001	Arthur	Alpha	Department of Education	Yes
☐	Mac Batt	Mac	Batt	Department of Education	Yes
☐	00003	Chesney	Charlie	Department of Education	Yes
☐	Grace Drever	Grace	Drever	Department of Education	Yes
☐	00005	Eddie	Echo	Department of Education	Yes
☐	Donita Jubb	Donita	Jubb	Department of Education	Yes
☐	Avis Lipps	Avis	Lipps	Department of Education	Yes
☐	Alan Mahar	Alan	Mahar	Department of Education	Yes
☐	Dodie Parker	Dodie	Parker	Department of Education	Yes

Note: Not all tables of records allow sorting on multiple columns. For example, if you are searching a directory, you can sort on only one column; this is for performance reasons.

If you download the results of a report to a file, the sort order is applied to the data in the downloaded file. See section *7.2*, *Running reports* for details of downloading reports.

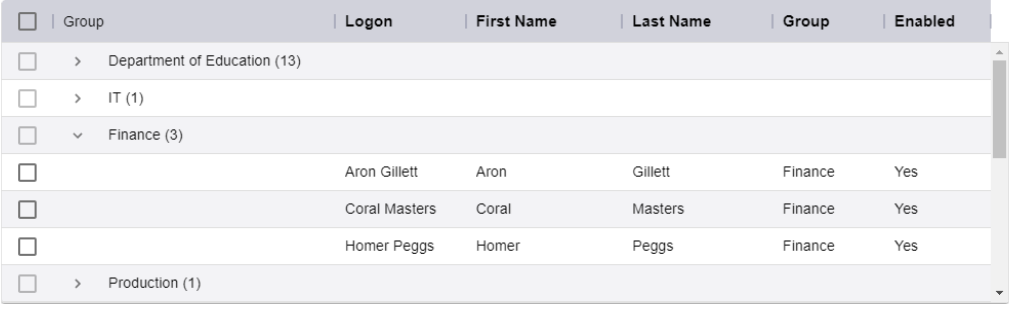
The sort criteria are included in the browser location bar; this also means you can specify the sort criteria using the MyID Core API. See section *3.3.5*, *Using the browser location bar*.

3.4.3 Grouping

You can group your records; this allows you to collapse a group and concentrate on one section at a time.

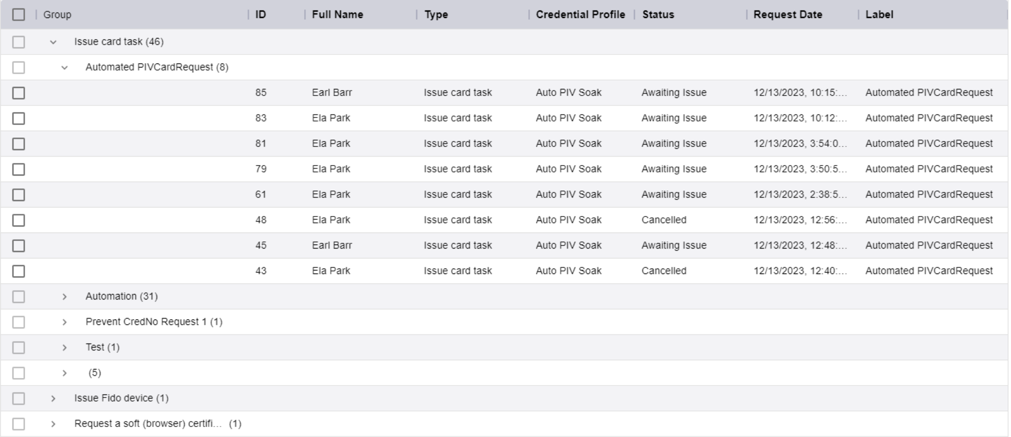
To group your records, click the three dot menu option on the column you want to group, then from the pop-up menu select **Group by <column name>**.

MyID collapses the search results into their groups. The number of records in the group is displayed in brackets. Click the **>** symbol to expand the group.



☐	Group	Logon	First Name	Last Name	Group	Enabled
☐	› Department of Education (13)					
☐	› IT (1)					
☐	⌄ Finance (3)					
☐		Aron Gillett	Aron	Gillett	Finance	Yes
☐		Coral Masters	Coral	Masters	Finance	Yes
☐		Homer Peggs	Homer	Peggs	Finance	Yes
☐	› Production (1)					

You can group by multiple columns. The first grouping that is set takes precedence.



☐	Group	ID	Full Name	Type	Credential Profile	Status	Request Date	Label
☐	⌄ Issue card task (46)							
☐	⌄ Automated PIVCardRequest (8)							
☐		85	Earl Barr	Issue card task	Auto PIV Soak	Awaiting Issue	12/13/2023, 10:15:...	Automated PIVCardRequest
☐		83	Ela Park	Issue card task	Auto PIV Soak	Awaiting Issue	12/13/2023, 10:12:...	Automated PIVCardRequest
☐		81	Ela Park	Issue card task	Auto PIV Soak	Awaiting Issue	12/13/2023, 3:54:0...	Automated PIVCardRequest
☐		79	Ela Park	Issue card task	Auto PIV Soak	Awaiting Issue	12/13/2023, 3:50:5...	Automated PIVCardRequest
☐		61	Ela Park	Issue card task	Auto PIV Soak	Awaiting Issue	12/13/2023, 2:38:5...	Automated PIVCardRequest
☐		48	Ela Park	Issue card task	Auto PIV Soak	Cancelled	12/13/2023, 12:56:...	Automated PIVCardRequest
☐		45	Earl Barr	Issue card task	Auto PIV Soak	Awaiting Issue	12/13/2023, 12:48:...	Automated PIVCardRequest
☐		43	Ela Park	Issue card task	Auto PIV Soak	Cancelled	12/13/2023, 12:40:...	Automated PIVCardRequest
☐	› Automation (31)							
☐	› Prevent CredNo Request 1 (1)							
☐	› Test (1)							
☐	› (5)							
☐	› Issue Fido device (1)							
☐	› Request a soft (browser) certifi... (1)							

You can have both sorting and grouping on the same table; first set up your sorting, then select your groupings. If you want to have your groupings sorted, set the sorting for those columns before selecting the groupings.

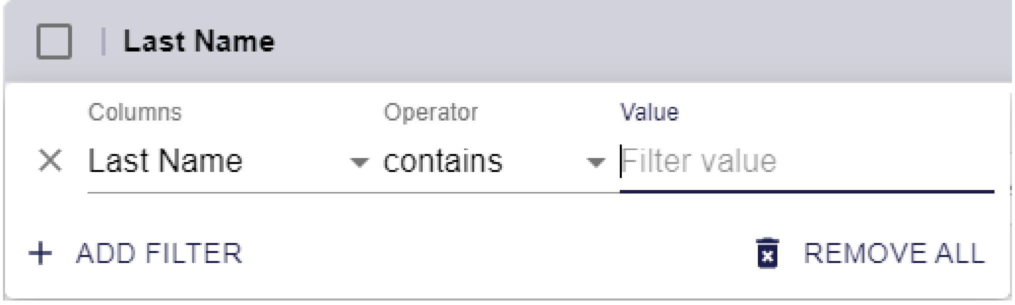
To stop grouping, click the three dot menu option on the column by which you are grouping, then from the pop-up menu select **Stop grouping by <column name>**.

3.4.4 Filtering

You can filter the displayed records.

To filter on a column, click the three dot menu option on the column you want to filter, then from the pop-up menu select **Filter**.

Alternatively, click the **Filters** button.



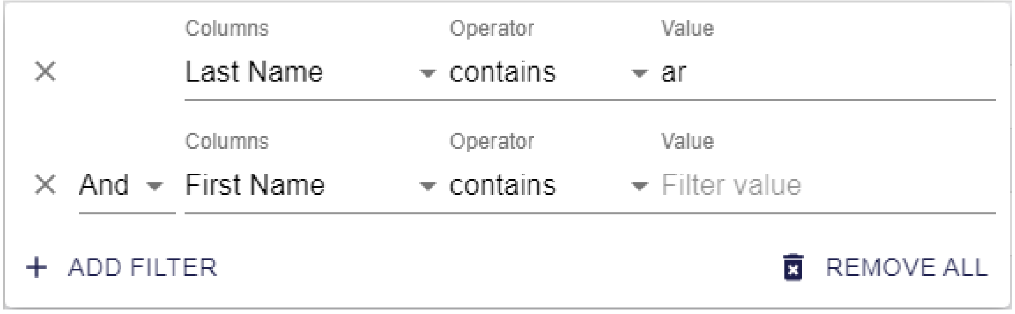
Columns: Last Name
Operator: contains
Value: Filter value

Enter the criteria for the filter:

- **Columns** – select the column on which you want to filter.
- **Operator** – select the operator.

  The operations available depend on the type of field; for example, dates have operators such as **is after** or **is on or before**, numeric values have operator such as **=** or **>=**, and text fields have operators such as **contains** or **starts with**.
- **Value** – type the value you want to filter on. For dates, you can use the date picker.

If you want to add another filter, click **Add Filter**.



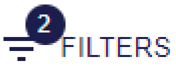
Columns: Last Name
Operator: contains
Value: ar

And
Columns: First Name
Operator: contains
Value: Filter value

Select the conjunction for the filters:

- **And** – both filters must be satisfied.
- **Or** – either filter can be satisfied.

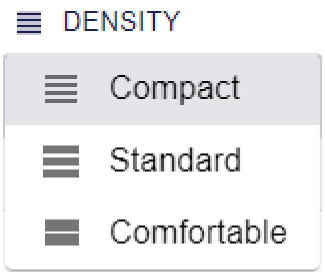
When one or more filter is active, the **Filters** button displays a number indicating the number of active filters.



Click the **Filters** button to display the active filters. From this dialog, you can amend the filters; click the **Delete** ✕ button to remove a filter, or click **Remove All** to remove all filters.

3.4.5 Changing the row spacing

You can change the spacing of the rows. Click the **Density** ≣ button.


DENSITY
Compact
Standard
Comfortable

From the pop-up menu, select one of the following to change the spacing of the rows:

- **Compact** – narrowest spacing.
- **Standard** – medium spacing.
- **Comfortable** – wide spacing.

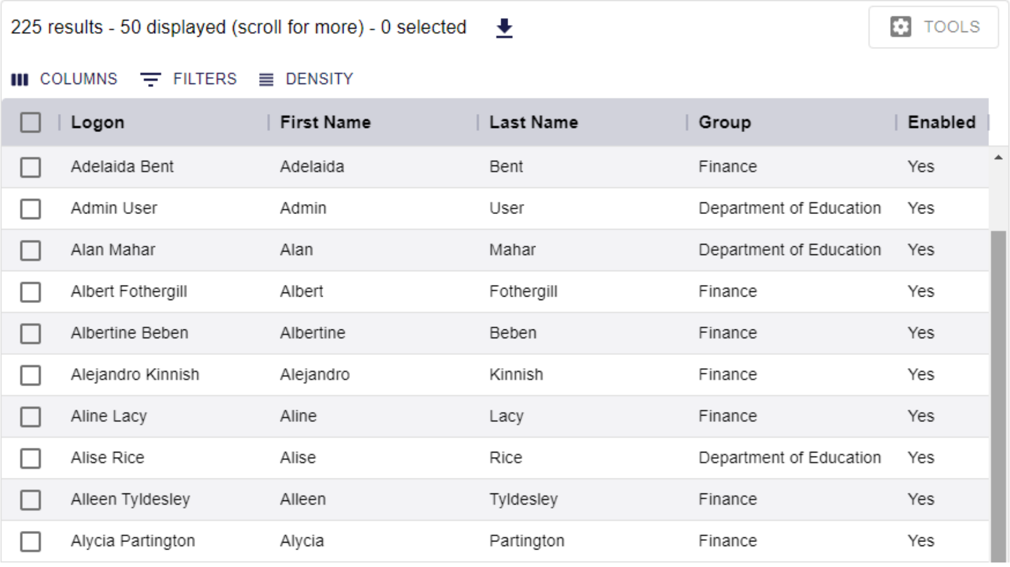
3.4.6 Working on multiple records

If you want to work on multiple records (for example, to edit multiple people, or cancel multiple requests) you can use the select option in the results screen

You can either work through the records one by one, or carry out the work as a batch operation using the Tools menu.

3.4.6.1 Working through multiple records individually

Search for the records you want to work with, and the results appear.

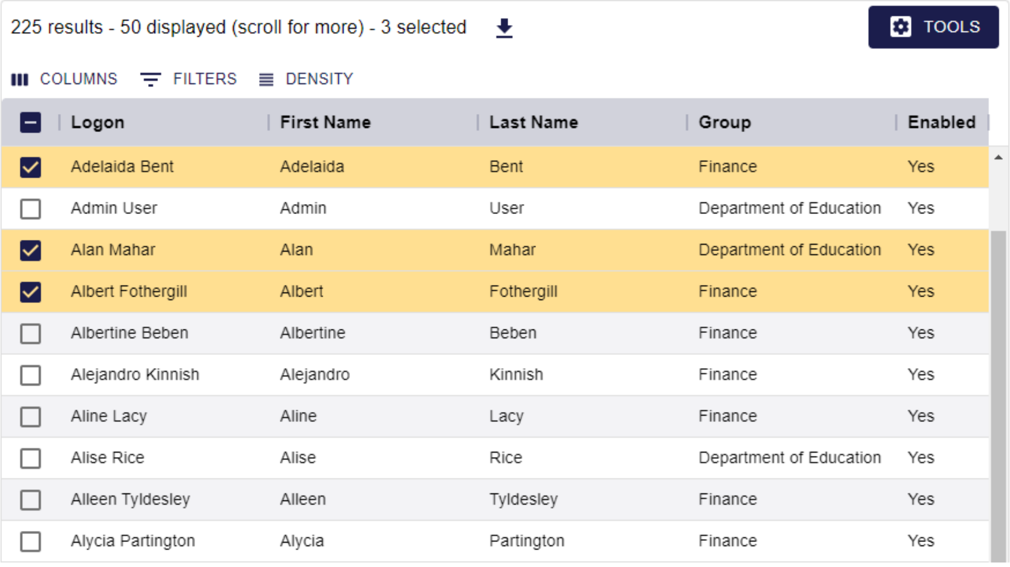


225 results - 50 displayed (scroll for more) - 0 selected

☐	Logon	First Name	Last Name	Group	Enabled
☐	Adelaida Bent	Adelaida	Bent	Finance	Yes
☐	Admin User	Admin	User	Department of Education	Yes
☐	Alan Mahar	Alan	Mahar	Department of Education	Yes
☐	Albert Fothergill	Albert	Fothergill	Finance	Yes
☐	Albertine Beben	Albertine	Beben	Finance	Yes
☐	Alejandro Kinnish	Alejandro	Kinnish	Finance	Yes
☐	Aline Lacy	Aline	Lacy	Finance	Yes
☐	Alise Rice	Alise	Rice	Department of Education	Yes
☐	Alleen Tyldesley	Alleen	Tyldesley	Finance	Yes
☐	Alycia Partington	Alycia	Partington	Finance	Yes

In the above example, you have searched for everyone in your organization; however, you only need to edit three of the people listed, not all of them.

Use the checkboxes at the left of each record to mark the records you are interested in.



225 results - 50 displayed (scroll for more) - 3 selected

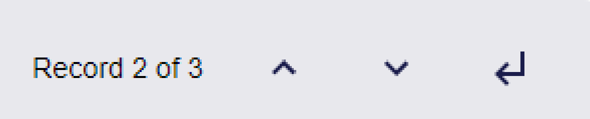
⊟	Logon	First Name	Last Name	Group	Enabled
☑	Adelaida Bent	Adelaida	Bent	Finance	Yes
☐	Admin User	Admin	User	Department of Education	Yes
☑	Alan Mahar	Alan	Mahar	Department of Education	Yes
☑	Albert Fothergill	Albert	Fothergill	Finance	Yes
☐	Albertine Beben	Albertine	Beben	Finance	Yes
☐	Alejandro Kinnish	Alejandro	Kinnish	Finance	Yes
☐	Aline Lacy	Aline	Lacy	Finance	Yes
☐	Alise Rice	Alise	Rice	Department of Education	Yes
☐	Alleen Tyldesley	Alleen	Tyldesley	Finance	Yes
☐	Alycia Partington	Alycia	Partington	Finance	Yes

Note: You can mark or deselect *all* records using the checkbox in the header.

Once you have marked the records you want to work with, click on any marked record to open the set.

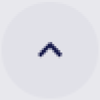
Note: If you click a record that is not marked, that record opens, and is not included in the set; however, if you return to the results list, you will not have lost your marked records.

The navigation toolbar at the top right of the record shows your position in the results set and allows you to move between records:



To navigate the records:

- To view the previous record, click the **Previous** button:



- To view the next record, click the **Next** button:

- To return to the search list, click the **Return to results** button:

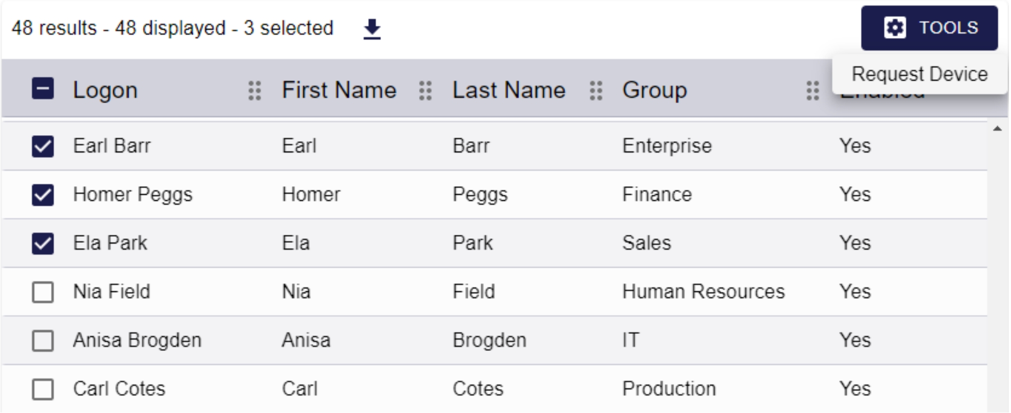
3.4.6.2 Working through multiple records as a batch operation

For some operations (for example, requesting devices for multiple people, or approving multiple requests, you can use the **Tools** menu to carry out the operation in a batch.

Note: You can access the **Tools** menu only if you have a role with the **Tools Menu** option from the **Configuration** section of the **Edit Roles** workflow.

Search for the records you want to work with, and the results appear.

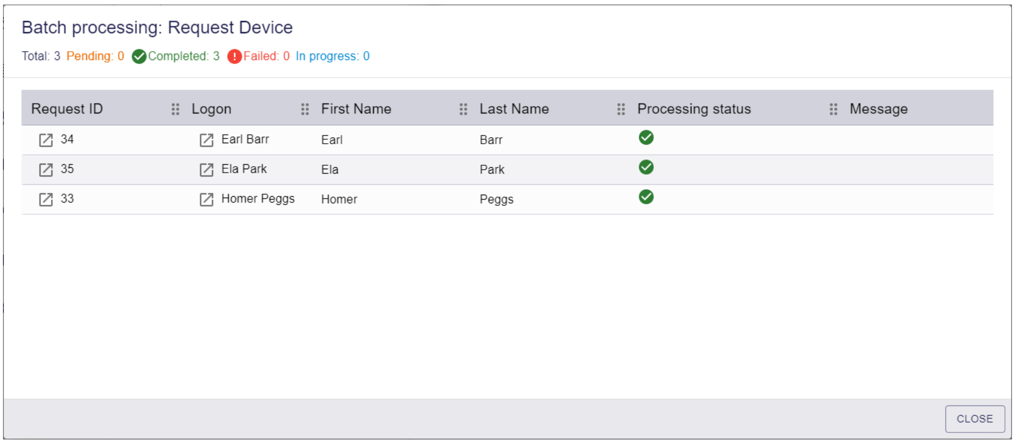
Use the checkboxes at the left of each record to mark the records you are interested in, then, from the **Tools** menu, select the operation you want to carry out.



48 results - 48 displayed - 3 selected

	Logon	First Name	Last Name	Group	
☑	Earl Barr	Earl	Barr	Enterprise	Yes
☑	Homer Peggs	Homer	Peggs	Finance	Yes
☑	Ela Park	Ela	Park	Sales	Yes
☐	Nia Field	Nia	Field	Human Resources	Yes
☐	Anisa Brogden	Anisa	Brogden	IT	Yes
☐	Carl Cotes	Carl	Cotes	Production	Yes

You can then confirm the details, and MyID processes the operation for each of your selected items as a batch.



Batch processing: Request Device

Total: 3 Pending: 0 ✓Completed: 3 !Failed: 0 In progress: 0

Request ID	Logon	First Name	Last Name	Processing status	Message
34	Earl Barr	Earl	Barr	✓	
35	Ela Park	Ela	Park	✓	
33	Homer Peggs	Homer	Peggs	✓	

3.4.7 Performance considerations for searching large sets of data

You may experience performance issues when searching large sets of data. In addition, when you sort on a column, MyID retrieves the records from the server, so the performance issue may occur several times when working with the records rather than once when initially retrieving the information from the database.

In some circumstances, you may see errors similar to the following:

```
WS60000 – Database timeout. Please contact your administrator for more information.
```

```
WS60001 – The search query timed out. Please contact your administrator for more information.
```

You are recommended to restrict your search query to identify the narrowest range of results.

Where it is not possible to narrow the range of results, to mitigate the performance issue, you can switch off the retrieval of the count of the number of records; this has been shown to improve the performance when working with large sets of data.

To disable the count of records on reports:

1. From the **Configuration** category, select **Operation Settings**.
2. On the **General** tab, set the following:
   - **Disable Report Count** – set to Yes.

     By default, this option is set to No, which means that MyID retrieves a count of the number of records whenever performing a search.
3. Click **Save changes**.

3.5 Roles and groups

The features you can access in the MyID Operator Client depend on your role as an operator, and the roles you can have depend on which group you belong to.

To specify which roles are available to each group, you must use the **Add Group** or **Amend Group** workflows; see the *Working with groups* section in the ***Operator's Guide*** for details.

To specify which features are available to each role, you must use the **Edit Roles** workflow; see the *Roles* section in the ***Administration Guide*** for details.

The options that appear in the **Edit Roles** workflow map to the features in the MyID Operator client in the following way:

Option in Edit Roles	Feature
Add Person	Browse Groups
	Browse
	Search Group
	View Person
	Add Person
	View Persons Images
All Requests	Search Reports
	All Requests

Option in Edit Roles	Feature
Archived Requests	Search Reports
	Archived Requests
Assign Card	Assign Device Search
	Assign Device
	Unassign Device
	Assign Device (Search)
Assigned Devices	Search Reports
	Assigned Devices
Cancel Credential	Browse
	View Device
	Browse Groups
	Search Group
	View Person
	Devices
	People
	Devices
	Cancel Device
Cancel Request	Browse Groups
	Browse
	View Request
	Requests
	Search Group
	Cancel Request
Devices	Search Reports
	Devices
Directory Sync	Directory Sync
Download Reports	Download Reports

Option in Edit Roles	Feature
Edit Person	Edit Person (Directory)
	Edit Person (Directory)
	Browse Directory Root
	Browse Directory Root
	Browse Directory Groups
	Browse Directory Groups
	Search Person (Directory)
	Browse
	Search Person (Directory)
	View Person (Directory)
	View Person (Directory)
	Search Group
	Search Group
	Browse Groups
	Browse
	Browse Groups
	Enable Person
	Edit Person
	Disable Person
	Enable Person
	View Persons Images
	View Persons Images
	Disable Person
	People
	View Person
	People
	View Person
Get Relationships	View Relationship
Identify Card	Devices
	View Device
	Device Certificates
	Device Requests
Manage Relationships	Add Relationship
	Delete Relationship
Mobile Devices	Search Reports
	Mobile Devices

Option in Edit Roles	Feature
People	Search Reports
	People
Authenticate	Authenticate
Provision Certificates	View Certificate
Remove Person	Search Group
	Browse Groups
	Browse
	View Person
	People
	Remove Person
Request Card	Request Device
	Devices
	People
	View Person
	View Persons Images
	Persons Available Credential Profiles
	Requests
	Browse
	Search Group
	Browse Groups
	View Request
	Requests
	Request Device
	Persons Credential Profiles (Directory)
	View Person (Directory)
	Search Person (Directory)
	Browse Directory Groups
	Browse Directory Root
Request Card Update	Request Update

Option in Edit Roles	Feature
Request Replacement Card	View Request
	Requests
	Requests
	Persons Available Credential Profiles
	View Persons Images
	Request Replacement Device
	Request Device Renewal
	Device Available Credential Profiles
	View Person
	People
	Devices
Requests	Search Reports
	Requests
Send Auth Code for Activation	Get Activation Code Expiry for Device
	Send Auth Code for Activation
Send Auth Code for Job Collection	Get Collection Code Expiry for Job
	Send Auth Code for Job Collection
Send Auth Code for Logon	Get Auth Code Expiry for Person Logon
	Send Auth Code for Logon
Send Auth Code for PIN Unlock	Get Unlock PIN Code Expiry for Device
	Send Auth Code for PIN Unlock
Unassigned Devices	Search Reports
	Unassigned Devices
Unrestricted Audit Report	Search Reports
	Unrestricted Audit Report
Validate Request	Requests
	Reject Request
	Jobs Available Credential Profiles
	View Request
	Approve Request
	Browse Groups
	Search Group
	Browse
View Auth Code for Activation	Get Activation Code for Device
	View Auth Code for Activation
View Auth Code for Job Collection	Get Collection Code for Job
	View Auth Code for Job Collection

Option in Edit Roles	Feature
View Auth Code for Logon	Get Auth Code for Person Logon
	View Auth Code for Logon
View Auth Code for PIN Unlock	Get Unlock PIN Code for Device
	View Auth Code for PIN Unlock
View Person	View Person (Directory)
	Search Person (Directory)
	Browse Directory Root
	Browse Directory Groups
	Browse
	Browse Groups
	Requests
	View Request
	Search Group
	Devices
	Requests
	View Person
	People
	View Persons Images
View User Audit	History
	View Person
	People
	Search Group
	Browse Groups
	Browse
	View Audit
	Audit Details

3.5.1 Roles example

For example:

- Operator Andrea is in the HR group. This group has access to the roles Standard Operator (which has access to the **View Person** feature) and Data Entry (which has access to the **Edit Person** and **Add Person** features). With these two roles, Andrea can search for people, view their details, edit their details, and add new people, but cannot request devices.
- Operator Boris is in the IT group. This group has the Standard Operator role, as above, and the Device Operator role, which has access to the **Request Card** feature (this provides access to the **Request Device** option in the MyID Operator Client; the corresponding workflow in MyID Desktop is called **Request Card**, hence the name).

Boris can search for people, view their details, and request devices for them, but cannot edit their details or add new people.

- Operator Charley is in the HR group like Andrea, but while the group has access to the Standard Operator and Data Entry roles, Charley has been assigned only the Standard Operator role. Charley can search for people and view their details, but cannot request devices, edit their details, or add new people.

3.5.2 Scope

The extent to which operators can carry out actions for people is determined by their *scope*. For example, if Andrea is in charge of data entry for the HR department, you may want to restrict her to viewing, editing, and adding people only in the HR group and its subgroups; in this case, you would give Andrea the Standard Operator and Data Entry roles with a scope of Division. Charley, on the other hand, has wider responsibilities, and can search for and view people throughout the system with the Standard Operator role and a scope of All.

For more information, see the *Scope and security* section in the ***Administration Guide***.

3.5.3 Administrative groups

You may not want the scope of an operator to be determined by their *own* group. For example, Andrea is in the HR department, but may be given extra responsibility for working with people to Finance department. To manage this, instead of simply giving Andrea a scope of All, you can give Andrea one or more *administrative groups*. For example, you can add the Finance group as one of Andrea's administrative groups, and Andrea can work with members of the Finance group as well as her own HR group.

For more information on working with administrative groups in the MyID Operator Client, see section *4.9*, *Working with administrative groups*.

4 Working with people

A *person* in MyID is someone with a record stored within MyID that allows them to be issued a smart card or other device. A person may also be a MyID operator or administrator who can log on to MyID to carry out an operator's or administrator's tasks.

The MyID Operator Client allows you to work with people in the following ways:

- You can search for a person in the database or in your attached directory.

  See section *4.1*, *Searching for a person*.
- You can add a person.

  See section *4.2*, *Adding a person*.
- You can edit a person's details.

  See section *4.3*, *Editing a person*.
- You can capture user images for a person's account using a webcam or by uploading an existing picture.

  See section *4.4*, *Capturing images*.
- You can request a device for a person.

  See section *4.5*, *Requesting a device for a person*.
- You can request a mobile device for a person.

  See section *4.6*, *Requesting a mobile device for a person*.
- You can synchronize a person with a directory.

  See section *4.7*, *Synchronizing a person*.
- You can enable or disable a person's account.

  See section *4.8*, *Enabling or disabling a person*
- You can select and assign administrative groups.

  See section *4.9*, *Working with administrative groups*.
- You can remove a person's account from MyID.

  See section *4.10*, *Removing a person*.
- You can authenticate a person's identity using fingerprints, identity documents, or security phrases.

  See section *4.11*, *Authenticating a person*.
- You can send an authentication code to a person to allow them to log on to MyID.

  See section *4.12*, *Sending an authentication code to a person*.
- You can view an authentication code for a person that allows them to log on to MyID.

  See section *4.13*, *Viewing an authentication code for a person*.
- You can change or unlock a person's security phrases using the **Change Security Phrases** and **Unlock Security Phrases** workflows in MyID Desktop.

  See section *4.14*, *Working with security phrases*.
- You can add, edit, or remove a person's additional identities.

  See section *12*, *Working with additional identities*.

- You can print a card layout for a person onto a card that does not have a chip using the **Print Badge** workflow in MyID Desktop.

  See section *4.15*, *Printing a badge*.
- You can manage a person's relationships.

  See section *4.16*, *Working with relationships*.

4.1 Searching for a person

To search for a person:

1. Click the **People** category.
2. Select the search to use from the **Reports** drop-down list.

   By default, only the **People** search is available; however, your system may have additional people searches that you use for reporting.
3. Select where to search.

   You can search the MyID database, or an attached directory; you may have more than one directory. If your system is set up with more than one source of people information, click the tabs to select where to search.

   If you are using the **Additional Identities (AID)** search report, you can search only the MyID database; you cannot search a directory.

   Your system may contain people from several sources: people who exist only in the MyID database, people who exist in both the MyID database and in a directory, where their accounts are linked, or people who exist only in a directory.

   Note: You can search a directory only if you have configured MyID to do so; you must set the **Search a directory** configuration option to **Yes** or **Ask**. See the *LDAP page (Operation Settings)* section in the ***Administration Guide*** for details.
4. Enter some or all of the search criteria.

   Note: Search criteria are not case sensitive.

   - **Name (contains)** – type some characters from the person's name.

     You cannot use wildcards in this field; it automatically uses fuzzy matching.

     For example, if you search for `Sam`, the search results contain records where the **Full Name** or **Logon Name** fields contain the following:

     - Sam Smith
     - Jane Samson
     - Samuel Johnson
     - Samantha Samuels

     However, as the fuzzy matching searches only the start of the word, the following would not appear:

     - Alice Balsam

If you specify more than one word in this field, the search results contain records that match *all* the words. For example, if you search for `Sam John`, the results include:

- Sam Johnson
- John Samson
- Samantha Johnson
- John Samuels

However, the following do not appear:

- Sam Smith (no match for "John")
- John Smith (no match for "Sam")
- Sam Littlejohn (no match for "John" – it does not occur at the start of a word)

This field is available only when searching the MyID database.

- **Group** – click the open icon ⧉ to select the group to which the person belongs.

  See section *3.3.7*, *Selecting a group*.

  If you want to view people from the groups below the selected group in the hierarchy, ensure that the **Include Subgroups** option is selected.
- **Logon** – type the person's logon name. You can use wildcards.
- **Employee ID** – type the person's employee ID. You can use wildcards.
- **Email** – type the person's email address. You can use wildcards.

Note: The available search criteria may depend on whether you are searching the MyID database or an attached directory.

You can also select **Additional search criteria**. See section *7.3.1*, *People report* for details of which fields are available for the People search.

Select the additional criteria to add them to the search form. Click the close **x** buttons on the additional criteria to remove them from the search form.

5. Click **Search**.

   The list of matching results appears.

   Records are sorted in the order they appear in the MyID database; currently, you cannot change the sort order.

   If more results are available, the text **(scroll for more)** appears; scroll to retrieve the next page of results automatically.

   A maximum of 200 results are returned. If the number of results exceeds the limit, a **+** sign is appended to the number of results; for example:

   ```
   200+ results - 50 displayed (scroll for more)
   ```

   In this case, you are recommended to change your search criteria to provide a more focused set of results.

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

6. Click a record to display the person's details.

   Note: If the person has been added to the MyID database, the form is titled View Person. If the person is only in a directory, and has not yet been added to the MyID database, the form is titled View Person (Directory).

   You can view information on the following tabs:

   - **Details** – view the person's details.
   - **Account** – view the person's directory account details.

     Note: In MyID Desktop, the **Account** tab appears only if the **Enable ADS Fields** configuration option is set. This option does not affect the MyID Operator Client – the **Account** tab is always available.
   - **Devices** – view the list of devices currently assigned to the person.

     Note: Mobile devices are not included in this list.
   - **Requests** – view the list of active requests for the person.

     See section *6*, *Working with requests*.
   - **History** – view the list of audit entries relating to the person.

     See section *4.1.1*, *Viewing a person's history*.
   - **Relationships** – view the list of relationships for the person.

     See section *4.16*, *Working with relationships*.
   - **Certificates** – view the list of certificates assigned to the person.

     See section *13.1.2*, *Viewing a person's certificates*.
   - **Attribute Changes** – view the list of the fields that have changed for the person, as well as the previous value and new value for each field.
   - **Previous Devices** – view the list of devices previously issued to the person.

     Note: Any previously-issued devices that have subsequently been assigned to other people are not listed.

     You can use this list to reinstate devices that have been mistakenly canceled or erased; see section *5.19*, *Reinstating a device*.
   - **Additional Identities** – add, remove, and edit additional identities for a person.

     See section *12*, *Working with additional identities*.

   From this screen, you can:

   - Edit the person's details. See section *4.3*, *Editing a person*.
   - Remove a person's record from the MyID database. See section *4.10*, *Removing a person*.
   - Request a device for the person. section *4.5*, *Requesting a device for a person*.
   - Request a mobile device for the person. section *4.6*, *Requesting a mobile device for a person*.
   - Synchronize the person's account with the directory. See section *4.7*, *Synchronizing a person*.

- Enable or disable a person's user account. See section *4.8*, *Enabling or disabling a person*.

Note: If you are viewing your own record, you cannot edit the account, request a device, or enable/disable the account. Another operator must carry out these operations on your behalf.

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

For example:

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

4.1.1 Viewing a person's history

The **History** tab displays the 1000 most recent entries relating to the person in the MyID database; it is not available for people who are only in the directory.

Note: You must have a role that has access to the View User Audit or View Full Audit feature to view this tab; see section *3.5*, *Roles and groups*. The View User Audit feature is in the People category of the **Edit Roles** workflow, while the View Full Audit feature is in the Reports category, under Audit Reporting.

If you have role permissions to the View Full Audit feature, you can click on an entry in the report to display the View Audit screen. See section *16.1*, *Viewing audit details* for more information. This also provides information, on the **Attribute Changes** tab, about the fields that have changed, as well as their previous and new values.

Audit entries relating to the following workflows are never displayed on the **History** tab, for reasons of security:

- **Mobile Certificate Recovery**
- **Request Key Recovery**
- **Approve Key Recovery**
- **Collect Key Recovery**
- **View Key Recovery**
- **Collect My Key Recovery**

Some other entries relating to MyID Desktop workflows may not be displayed, particularly in systems upgraded from older versions of MyID, due to inconsistencies in how user information is recorded in the audit data.

There is a difference between the contents of audit entries created from operations in the MyID Operator Client and MyID Desktop: operations carried out in the MyID Operator Client produce audit entries that detail only what has been changed, while operations carried out in MyID Desktop produce audit entries that also include data that has not been changed. Note also that the history displayed in MyID Desktop displays only changes made to the person's account, while the **History** tab in the MyID Operator Client displays all audit entries for which the person was the target.

Note: The **History** tab does not currently display any archived audit entries.

You can also view the history for a device; see section *5.1.1*, *Viewing a device's history*.

4.1.2 Wildcards

For fields where you can use wildcards, you can use the following:

- `*` for multiple characters.

  For example, `Sa*` matches Sam, Samuel, and Samantha.
- `?` for single characters.

  For example, `Sa?` matches Sam, but not Samuel or Samantha.

  Note: When searching for people, you cannot use `?` for a single-character wildcard if you are searching an LDAP directory. The `?` wildcard is supported only when searching in the MyID database.

4.2 Adding a person

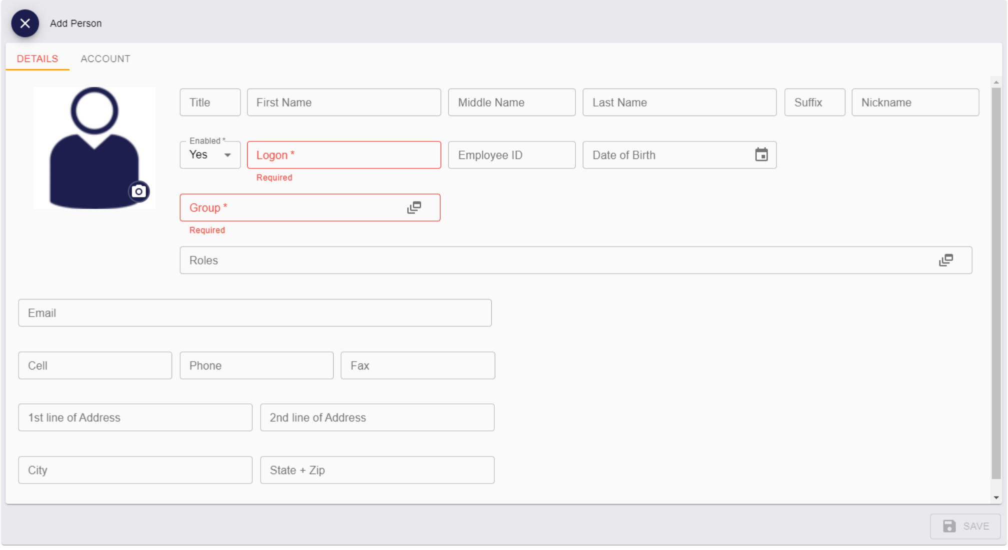
You can add a person to the MyID database manually, or you can import a person's details from a linked directory into the MyID database.

4.2.1 Adding a person manually

To add a person to the MyID database:

1. Select the **People** category.
2. Click **Add**.

   The Add Person form appears.


Add Person
DETAILS
ACCOUNT
Title
First Name
Middle Name
Last Name
Suffix
Nickname
Logon *
Required
Employee ID
Date of Birth
Group *
Required
Roles
Email
Cell
Phone
Fax
1st line of Address
2nd line of Address
City
State + Zip
SAVE

Enabled * Yes

3. Complete the person's details.

   Note: Required fields are marked with an asterisk `*` – the **Save** button is not available until you have completed all of these fields.

   Note: The fields may have different names depending on your language settings; for example, **Cell** and **Mobile**.

   The following fields are available:

   - The user image. See section *4.4*, *Capturing images*.
   - **Title** – type the person's title.

- **First Name** – type the person's first name.
- **Middle Name** – type the person's middle name or initials.
- **Last Name** – Type the user's last name.

  Note: You must include one or both of **First Name** and **Last Name**.
- **Enabled** – select **Yes** or **No** from the drop-down list.

  If you select **No**, you will not be able to issue any devices to the user. You can enable or disable a person's user account after you have added them; see section *4.8*, *Enabling or disabling a person*.
- **Logon** – type a **Logon** name for the person.

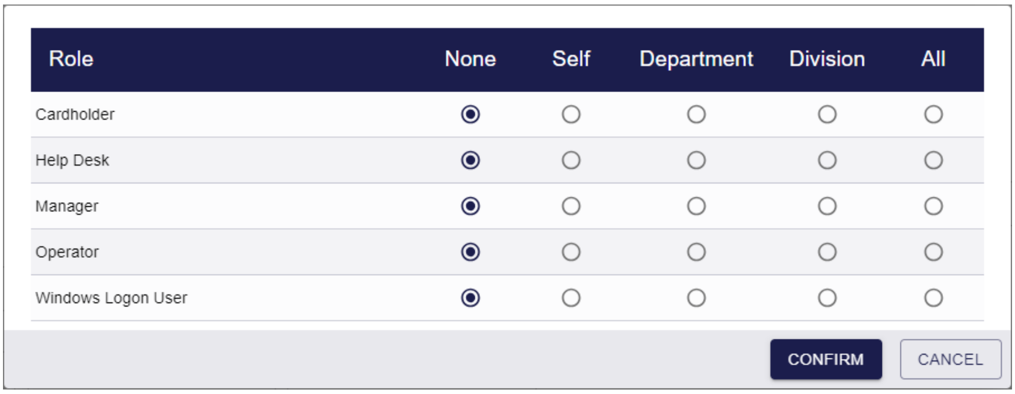
  Important: This field *must* be unique.

  The person can use this to log on to MyID without using a card if your system is set up to allow logon using security phrases only.
- **Email** – type the person's email address.

  An email address is required for notifications, including activation codes, if required.
- **Group** – click the open icon to select the group to which the person belongs.

  See section *3.3.7*, *Selecting a group*.
- **Access to Operations** – select one of the following:
  - **Restricted** – the person's account is restricted to the access provided by the Cardholder role only. This is set automatically if the user has been inactive and your system is configured to restrict inactive accounts.
  - **Unrestricted** – the person's account has normal access. However, if your system is configured to restrict inactive accounts, if the person does not log in for the configured amount of time, their account is set to **Restricted**.
  - **Not Monitored** – the person's account is never set to **Restricted**, no matter how long it has been since their last logon.

  See the *Restricting inactive users* section in the ***Administration Guide*** for more information.
- **Roles** – click the open icon to open the Role selector.



Role	None	Self	Department	Division	All
Cardholder	●	○	○	○	○
Help Desk	●	○	○	○	○
Manager	●	○	○	○	○
Operator	●	○	○	○	○
Windows Logon User	●	○	○	○	○

Select the roles and scope you want the person to have.

The *roles* for a user determine which MyID operations the person can perform; for example, to request a card.

The *scope* for each role determines the range of people the person can use the MyID operations on; for example, to be able to request a card only for themselves, or to be able to request a card for anyone in their group.

The available scope settings 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 person.
- **Division** – all people in the same group as the person or a sub-group of it.
- **All** – the role can be performed in relation to anyone.

For more information, see the *Roles, groups, and scope* section in the ***Administration Guide***.

Click **CONFIRM**.

- **Employee ID** – type a unique identifier for the person.
- **Cell** – type the person's cellphone number.
- **Phone** and **Fax** – type the person's land line phone number and fax number.
- **Address 1**, **Address 2**, **City** and **State + Zip** – type the person's address.

4. Click the **Account** tab to provide details of the person's LDAP account.

   For more information, see section *4.3.1*, *Editing directory information*.

   Note: Depending on your system configuration, you may have to specify a unique value for the **Distinguished Name**. The **Allow duplicate DN** configuration option determines whether unique DN values are required; see the *LDAP page (Operation Settings)* section in the ***Administration Guide*** for details.

5. Click **Save** to add the person to the MyID database.

4.2.2 Adding a person from a directory

To add a person to the MyID database from a directory:

1. Search for a person in a directory, and view their details.

   See section *4.1*, *Searching for a person* for details.
2. Click **Edit Person**.
3. Make any appropriate changes, then click **Save**.

   Alternatively, you can import a person from a directory without having to edit any of the person's details; select one of the following options:

   - **Request Mobile** or **Request Mobile (View Auth Code)** – attempts to import the person and request a mobile device. See section *4.6*, *Requesting a mobile device for a person*.
   - **Request Device** – attempts to import the person and request a device. See section *4.5*, *Requesting a device for a person*.
   - **Import** – attempts to import the person from the directory. Click **Confirm** to import the person, or **Cancel** to cancel the import.

   The person is added to the MyID database. The person is added to an existing group if a MyID group matches their directory group.

   Note: If a matching group does not already exist in MyID, you are unable to set any roles. When you save the person record, MyID creates a group if the **Automatically create MyID groups from the Organizational Unit of imported users** option is set, which assigns default roles to the person; you can then edit the person to amend their list of groups.

   You can also configure MyID to assign roles to a person based on their LDAP group membership; these roles are automatically assigned in addition to any group default roles when you add a person or change a person's group through directory synchronization. For information on setting this up, see the *Linking roles to LDAP* section in the ***Administration Guide***.

4.2.3 Adding multiple people from a directory

If you have several people to import from a directory at the same time, you can import them in a batch instead of importing them one by one.

Note: You can access the **Tools** menu only if you have a role with the **Tools Menu** option from the **Configuration** section of the **Edit Roles** workflow.

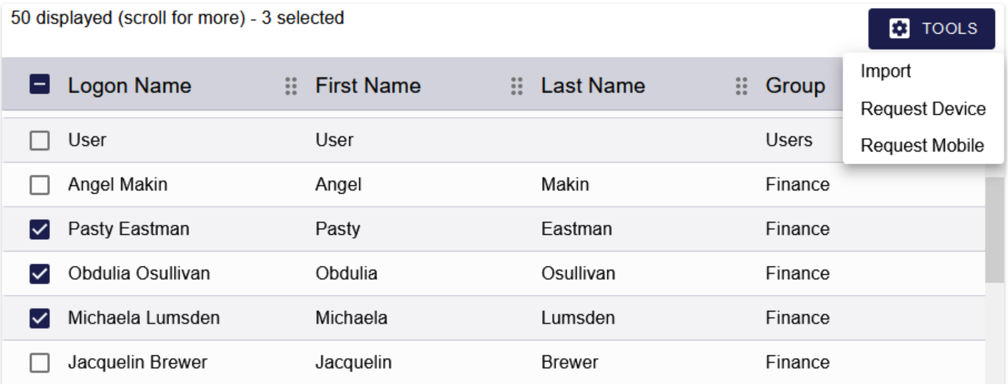
To import multiple people:

1. Search the directory for the people you want to import.

   See section *4.1*, *Searching for a person*.

2. On the search results page, use the checkboxes to the left of the records to select one or more people.

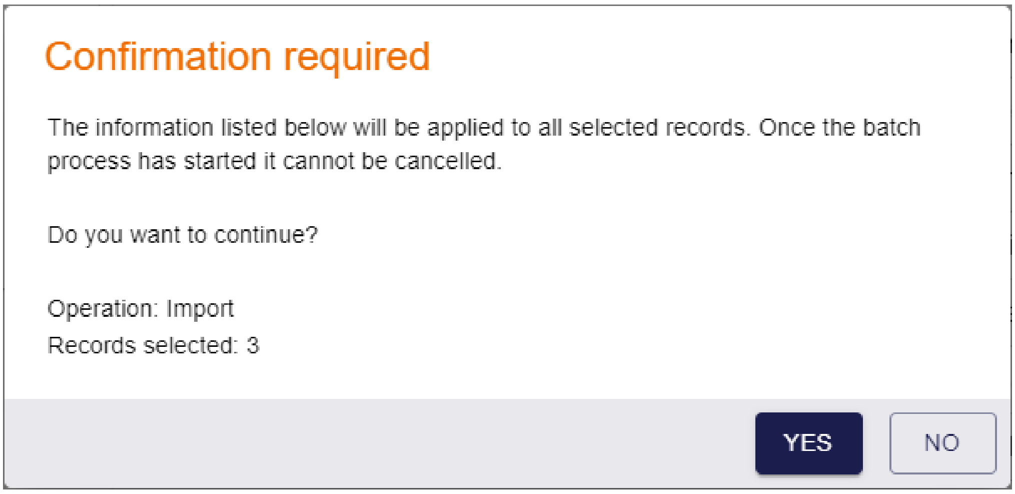
3. From the **Tools** menu, select **Import**.



50 displayed (scroll for more) - 3 selected

	Logon Name	First Name	Last Name	Group
☐	User	User		Users
☐	Angel Makin	Angel	Makin	Finance
☑	Pasty Eastman	Pasty	Eastman	Finance
☑	Obdulia Osullivan	Obdulia	Osullivan	Finance
☑	Michaela Lumsden	Michaela	Lumsden	Finance
☐	Jacquelin Brewer	Jacquelin	Brewer	Finance

   The confirmation screen appears.



Confirmation required

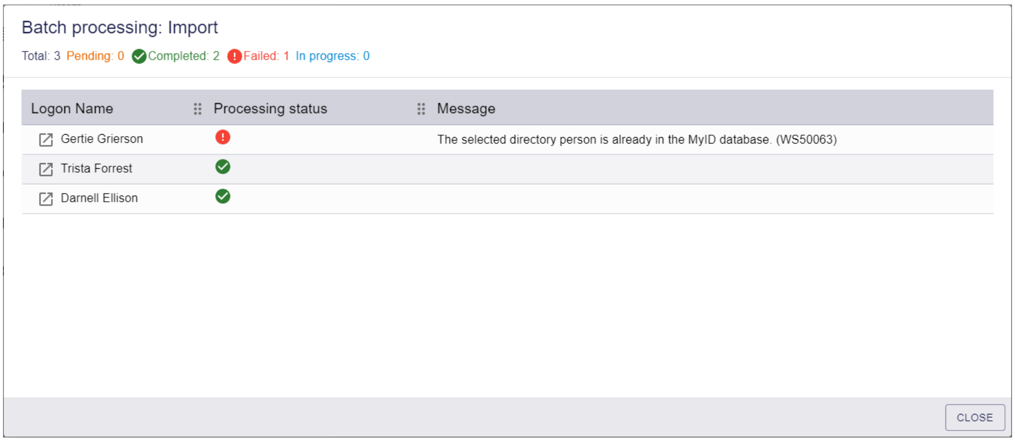
The information listed below will be applied to all selected records. Once the batch process has started it cannot be cancelled.

Do you want to continue?

Operation: Import
Records selected: 3

4. Click **Yes** to proceed with the import, or **No** to go back to the list of people.

   When you click **Yes**, the Batch Processing screen appears.



Batch processing: Import

Total: 3 Pending: 0 ✓Completed: 2 !Failed: 1 In progress: 0

Logon Name	Processing status	Message
Gertie Grierson	!	The selected directory person is already in the MyID database. (WS50063)
Trista Forrest	✓	
Darnell Ellison	✓	

5. The imports are processed. The table shows the status of each import:

✓	The import succeeded.
!	The import failed. The Message column displays the reason for the failure; for example, the person may already be in the MyID database.

6. Click **Close**.

4.3 Editing a person

You can edit the details in a person's record in the MyID database or in an attached directory.

To edit a person:

1. Search for a person, and view their details.

   See section *4.1*, *Searching for a person* for details.

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

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

2. Click the **Edit Person** option in the button bar at the bottom of the screen.

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

3. Update the person's details.

   For information on changing the user image, see section *4.4*, *Capturing images*.

   Note: If the person is already in the MyID database, the form is titled Edit Person. If the person is only in a directory, and has not yet been added to the MyID database, the form is titled Edit Person (Directory). Once you have made any changes to the person, the person is imported to MyID, and any edits you make will use the Edit Person form.

   You can edit the same details as are available when adding a person; see section *4.2*, *Adding a person* for details.

However, you cannot edit the **Enabled** field – to enable or disable a person's user account, see section *4.8*, *Enabling or disabling a person*.

If your system is set up for administrative groups, you can specify administrative groups for the person; see section *4.9.2*, *Assigning administrative groups*.

Note: Depending on how your system is set up, you may not be able to edit all of the fields that are visible.

4. Click **Save**.

4.3.1 Editing directory information

If the person is linked to a directory, and you want to edit the information on the **Account** tab, you must set the following configuration option:

- **Edit Directory Information** – on the **LDAP** tab of the **Operation Settings** workflow. Set this to Yes to allow operators to edit the information on the **Account** tab for people with accounts linked to a directory.

Whether or not the person is linked to a directory, you can edit the **Distinguished Name** field only if the **Edit DN** configuration option is set. This option requires an additional software update – contact customer support quoting reference SUP-322 for details.

Note: You are not recommended to set the **Edit Directory Information** option if you have the **Background update** option set; any changes you made to the directory information would be overwritten by changes from the directory every time you viewed or edited a person. If you want to be able to edit directory information, set the **Background update** option to No, then use manual directory synchronization if and when required; see section *4.7*, *Synchronizing a person* for details.

If you have the **Automatically create MyID groups from the Organizational Unit of imported users** option set to No, and **Edit Directory Information** set to No, MyID is unable to create a group to match the directory group, so you must set the group of the person manually.

For more information on directory integration, see the *Using an LDAP directory* section in the ***Administration Guide***.

For information on the **User SID** field, see the *Including user security identifiers in certificates* section in the ***Administration Guide***.

For information on the **External Reference ID 1**, **2**, and **3** fields, see the *Updating the Entra ID using the MyID Operator Client* section in the ***Passkey Integration Guide***.

4.4 Capturing images

You can capture user images for a person using an attached webcam, or by uploading an existing photograph. This feature is available in the Edit Person and Add Person screens.

4.4.1 Requirements for image capture

MyID requires a webcam with a resolution of at least 640x480. If the camera supports a higher resolution, MyID uses the full resolution available.

You can adjust the brightness and contrast of the image on the webcam feed only if the camera itself allows it.

MyID can access the camera only if it is not being used by another application; make sure the camera is not being used before attempting to capture an image.

If for any reason there are no compatible webcams available, the Image Capture screen will still allow you to upload an existing image file.

Image capture is supported on all browsers supported by the MyID Operator Client – see section *2.1.1*, *Supported browsers*.

Note, however, the following limitations when using Firefox:

- The image capture resolution is limited to 640x480.
- You cannot set the brightness or contrast.

4.4.2 Configuring image capture

To enable or disable image capture in the MyID Operator Client, set the **Image Capture** option on the **Video** tab of the **Operation Settings** workflow. If you set this option to `Yes`, you can capture images; if you set this option to `No`, the images already captured appear read-only, and you cannot capture new images or update existing images.

The image capture configuration options (on the **Video** tab of the **Operation Settings** workflow) control how you can crop images in the MyID Image Editor.

- To set a fixed size image, set the **Image Crop Height** and **Image Crop Width** options to the size (in pixels) of the image you want to upload. 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 fixed image size. 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**.

  Note: These settings take precedence over the other image crop settings.

- To limit the uploaded image to a maximum height and width, set the **Validate Image Size** option, then set the **Maximum Image Height** and **Maximum Image Width** settings (in pixels). You can move and resize the cropping rectangle on the image to any position or size. When the MyID Image Editor uploads the resulting image to the server, it is scaled down to within the **Maximum Image Height** and **Maximum Image Width**, maintaining its aspect ratio; if the image is the same size or smaller, it remains the same size.

  Note: If **Validate Image Size** is set to No, the **Maximum Image Height** and **Maximum Image Width** settings are ignored.

- To fix the aspect ratio of the image, set the **Image Crop Aspect Ratio** to the required image aspect ratio (`width:height`). For example, for a UK passport photo ratio, use `35:45`. 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 specified aspect ratio.

  You can combine this option with the **Validate Image Size** option to specify an image of a particular aspect ratio with a maximum size. If the **Image Crop Aspect Ratio** is, for example, `1:2`, and both the **Maximum Image Height** and **Maximum Image Width** settings are `1000`, the maximum image size that respects both the aspect ratio and the maximum dimensions is 500x1000.

You can also configure the compression on the resulting images uploaded to the server:

- **JPEG Compression Ratio** – set this to the compression value from `1` to `100`. The default is `90`. The lower the number, the greater the compression.

Examples:

- You want all uploaded user images to be exactly 600x800 pixels.

  To do this, set the **Image Crop Height** to `800` and the **Image Crop Width** to `600`.

  The operator can then capture images of any size, crop them to a fixed 3:4 aspect ratio (calculated from the fixed width and height), and when they are uploaded to the server, the images are rescaled to exactly 600x800. Low resolution images (for example, from a 640x480 webcam) are scaled up, and high resolution images (for example, from a 4K webcam) are scaled down.

- You want all uploaded images to be in a 3:4 aspect ratio. You are happy with low resolution images, but to save space, you want images to have a maximum size of 1200x1600.

  To do this, set the **Image Crop Aspect Ratio** to 3:4, the **Validate Image Size** option to Yes, the **Maximum Image Height** to 1600 and the **Maximum Image Width** to 1200.

  The operator can then capture images of any size, crop them to a fixed 3:4 aspect ratio, and when they are uploaded to the server, if the images are larger than 1200x1600, they are rescaled to exactly 1200x1600. Low resolution images (for example, 300x400 images from a 640x480 webcam) are uploaded without scaling.

- You want square images, but have no requirements for size.

  To do this, set the **Image Crop Aspect Ratio** to 1:1.

  The operator can then capture images of any size, crop them to a fixed 1:1 aspect ratio, and when they are uploaded to the server, the images are uploaded without scaling.

4.4.3 Capturing an image from a webcam

To capture an image from a webcam:

1. Click the camera icon on the user image:

   The Image Capture dialog appears.

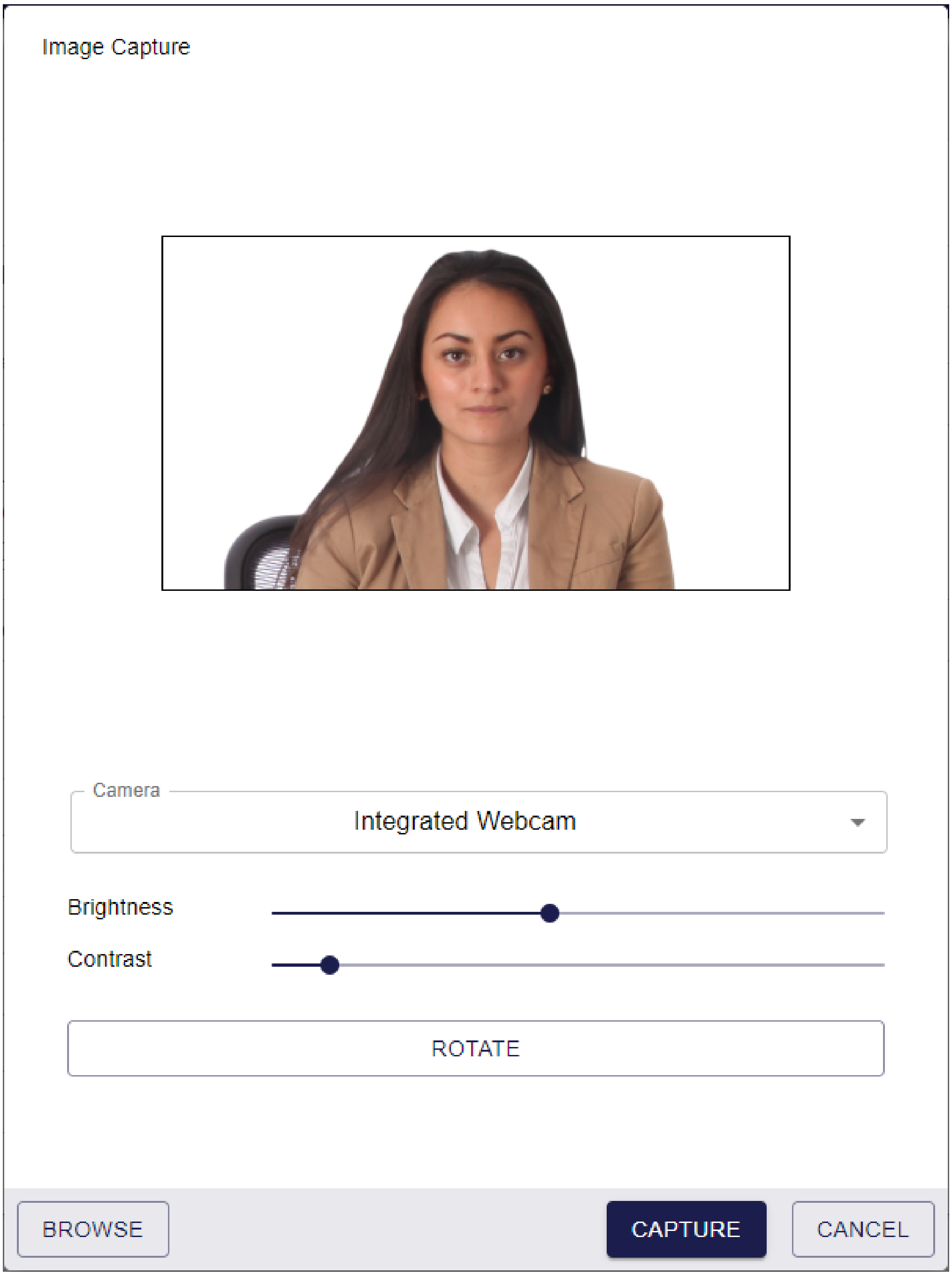


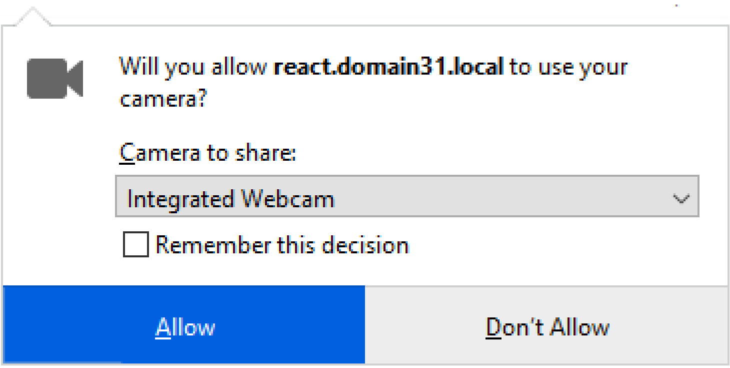
Image Capture

Camera: Integrated Webcam

Brightness
Contrast
ROTATE
BROWSE
CAPTURE
CANCEL

Your browser may prompt you to allow access to the camera. For example:

Firefox:



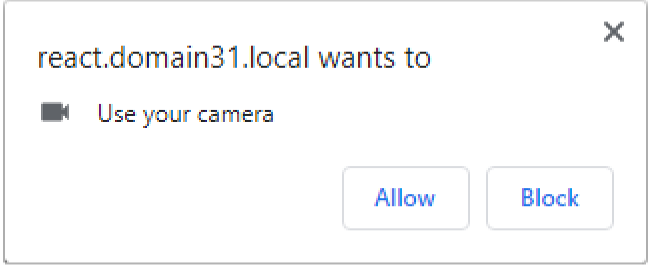
Will you allow **react.domain31.local** to use your camera?

Camera to share:

Integrated Webcam

☐ Remember this decision

Chrome:



react.domain31.local wants to

Use your camera

2. Select your webcam from the **Camera** drop-down list, if you have more than one.

   For example, you may have a laptop with an integrated camera, but also a high-quality external camera that you want to use to capture user images.

   MyID remembers your camera selection the next time you open the Image Capture dialog.

3. Set the following options:

   - **Brightness** – adjust the brightness of the image.
   - **Contrast** – adjust the contrast of the image.

   If you change these settings, MyID remembers the settings for the particular webcam the next time you open the Image Capture dialog.

   Note: These options are available only if your webcam supports them, and are not available if you are using the Firefox browser.

4. If necessary, you can click **Rotate** to rotate the image by 90°.

   MyID remembers your preferred rotation setting the next time you open the Image Capture dialog.

5. Click **Capture**.

   The MyID Image Editor opens.

   See section *4.4.5*, *Cropping and editing user images* for details of working with the image.

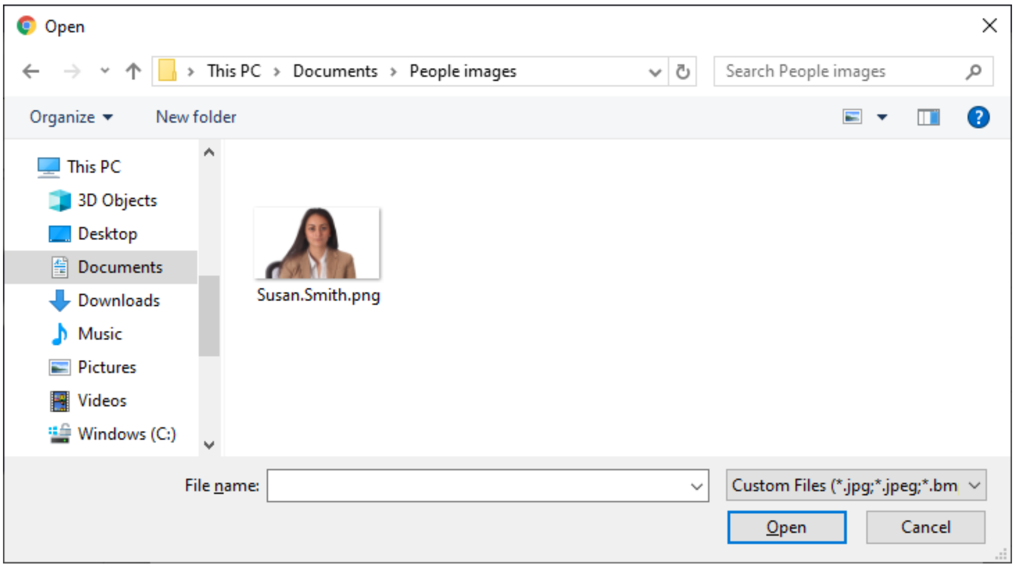
4.4.4 Uploading an existing image file

To upload an existing image:

1. Click the camera icon on the user image:

2. Click **Browse**.

   The file dialog opens.


Open
This PC › Documents › People images
Search People images
Organize ▾
New folder
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Windows (C:)
Susan.Smith.png
File name:
Custom Files (*.jpg;*.jpeg;*.bm
Open
Cancel

3. Select the image you want to upload.

   You can choose from the following file types:

   - JPEG (`*.jpg`, `*.jpeg`)
   - Bitmap (`*.bmp`)
   - Graphics Interchange Format (`*.gif`)
   - Portable Network Graphics (`*.png`)

   If you select a file of the wrong type, MyID displays an error.

4. Click **Open**.

   The MyID Image Editor opens.

   See section *4.4.5*, *Cropping and editing user images* for details of working with the image.

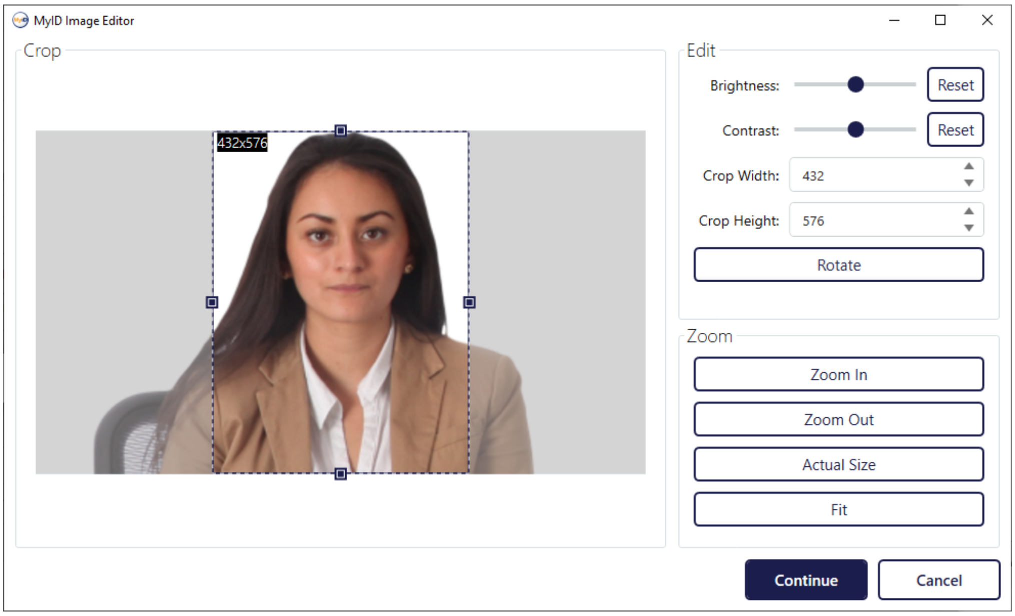
4.4.5 Cropping and editing user images

The MyID Image Editor appears when you have captured a webcam image or uploaded an existing image file.

To crop and edit the image:

1. Select the crop area.

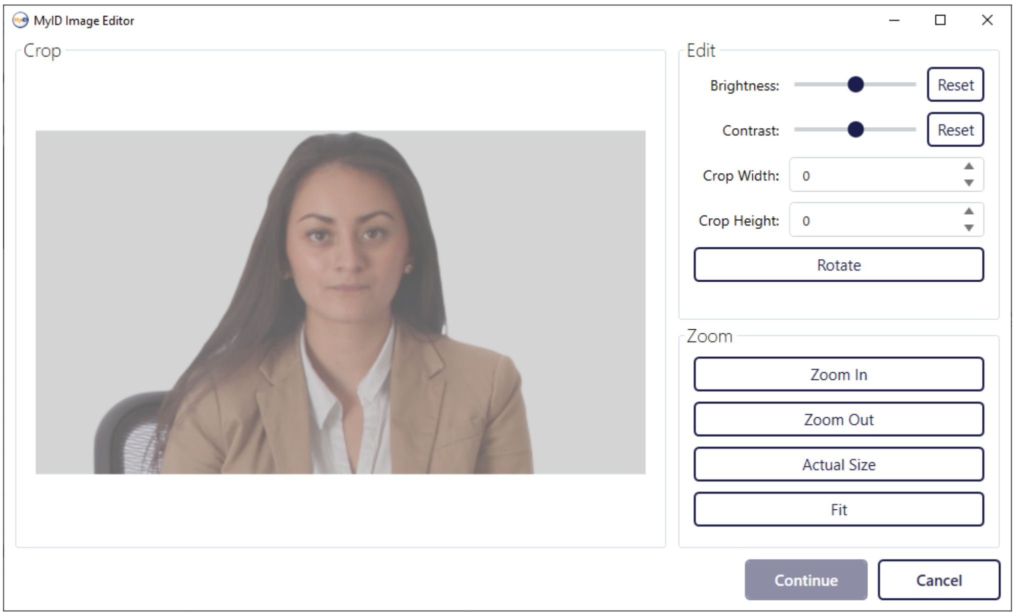
   If you have set the **Image Crop Height** and **Image Crop Width** options, or the **Image Crop Aspect Ratio** option, the editor displays an initial crop selection as large as possible while respecting the fixed aspect ratio.

   
   MyID Image Editor
   Crop
   432x576
   Edit
   Brightness:
   Reset
   Contrast:
   Reset
   Rotate
   Zoom
   Zoom In
   Zoom Out
   Actual Size
   Fit
   Continue
   Cancel

   Crop Width: 432
   Crop Height: 576

   You can resize the crop selection, but it automatically maintains its aspect ratio.

   If you do not have these options set, the editor does not display an initial crop selection.

   
   MyID Image Editor
   Crop
   Edit
   Brightness:
   Reset
   Contrast:
   Reset
   Rotate
   Zoom
   Zoom In
   Zoom Out
   Actual Size
   Fit
   Continue
   Cancel

   Crop Width: 0
   Crop Height: 0

   Click and drag on the image to select the part of the image you want to use.

Once you have a selection, you can modify it.

- To change the size of the selection:
  - Click and drag the sizing handles.
  - Hold down the CTRL key and roll the mouse wheel.
  - Use the **Crop Width** and **Crop Height** fields to specify the size of the selection.
- To move the selection, click within the selection and drag it.

2. Set the following options:
   - **Brightness** – adjust the brightness of the image.
   - **Contrast** – adjust the contrast of the image.
3. To rotate the image by 90°, click **Rotate**.

   Note: When you rotate the image, it resets the crop settings.
4. To allow you to make accurate selections, you can adjust the zoom level:
   - **Zoom In** – click to zoom in on the image. You can scroll around the image within the editor.
   - **Zoom Out** – click to zoom out of the image.
   - **Actual Size** – click to display the image at its actual pixel size.
   - **Fit** – fit the image within the editor. This is the default setting.
5. Once you are happy with the image, click **Continue**.

   The MyID Image Editor copies the resulting image to the form.

   Note: The image is not uploaded to the server until you click **Save**.

4.4.6 Troubleshooting image capture

- **Unable to click on the camera icon**

  If you cannot click the camera icon to launch the image capture control, check that the **Image Capture** configuration option is set.

  See section *4.4.2*, *Configuring image capture* for details.

- **Problem connecting to a camera**

  If you see a message similar to the following:

  ```
  A problem has occurred when connecting to the camera.
  Click Cancel, check the camera is operating correctly and not currently
  in use and then start Image Capture again.
  ```

  This may be caused by another application using the camera. Make sure there are no other applications or browsers currently using the camera. Alternatively, this may be caused by a problem within Windows. Check the Windows Device Manager to ensure that the camera is enabled.

- **Unable to find a camera**

  If you see a message similar to the following:

  ```
  A compatible camera has not been found
  ```

  This means that MyID has been unable to find an attached camera that supports the minimum requirements (640x480 resolution). You can attach an external camera that meets the requirements.

  Note: If for any reason MyID cannot connect to a compatible webcam, the Image Capture screen will still allow you to upload an existing image file.

- **Unable to connect to the MyID Client Service App**

  If you see a message similar to the following when opening the MyID Image Editor:

  ```
  OC10006 MyID Client Service error
  Unable to communicate with MyID Client Service. Ensure it is running
  ```

  This may be caused by the MyID Client Service App not running; this app provides the image editing capabilities. Make sure the MyID Client Service App is running and try again.

- **Out of memory**

  If you see a message similar to:

  ```
  OutOfMemoryException
  ```

  This may be caused by attempting to process very large images on a 32-bit operating system. Either use smaller images or carry out your image capture work on a 64-bit operating system.

- **Please wait... message displayed**

  If the MyID Image Editor does not open, and a `Please wait...` message is displayed instead, check that you have the latest version of the MyID Client Service installed.

4.4.7 Viewing images

To view an enlarged version of a captured image on the Edit Person screen or the View Person screen, click the image preview on the **Details** tab. To close the image preview, click elsewhere on the screen.

4.5 Requesting a device for a person

You can request a device for a person; for example, a smart card.

You can currently use the MyID Operator Client to request devices where the **Card Encoding** option in the credential profile is set to any of the following:

- **Contact Chip**
- **Contactless Chip**
- **Physical Printed Card**
- **Microsoft Virtual Smart Card**
- **Software Certificates**
- **Windows Hello**
- **FIDO Authenticator**

Note: To request a mobile device for a person, that is, a device using a credential profile where the **Card Encoding** is **Identity Agent**, you must use the **Request Mobile** or **Request Mobile (View Auth Code)** options instead. See section *4.6*, *Requesting a mobile device for a person*.

Depending on how your MyID system is set up, the person may be able to collect the device themselves (for example, using the Self-Service App), may require their request to be validated by an operator before collection, or may require the assistance of an operator to collect the device through MyID Desktop – MyID provides many issuance models to suit your organization's needs.

The issuance model depends on the configuration of the credential profile used to request the device. For more information, see the *Managing credential profiles* section in the ***Administration Guide***.

4.5.1 Requesting a device

To request a device for a person:

1. Search for a person, and view their details.

   See section *4.1*, *Searching for a person* for details.

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

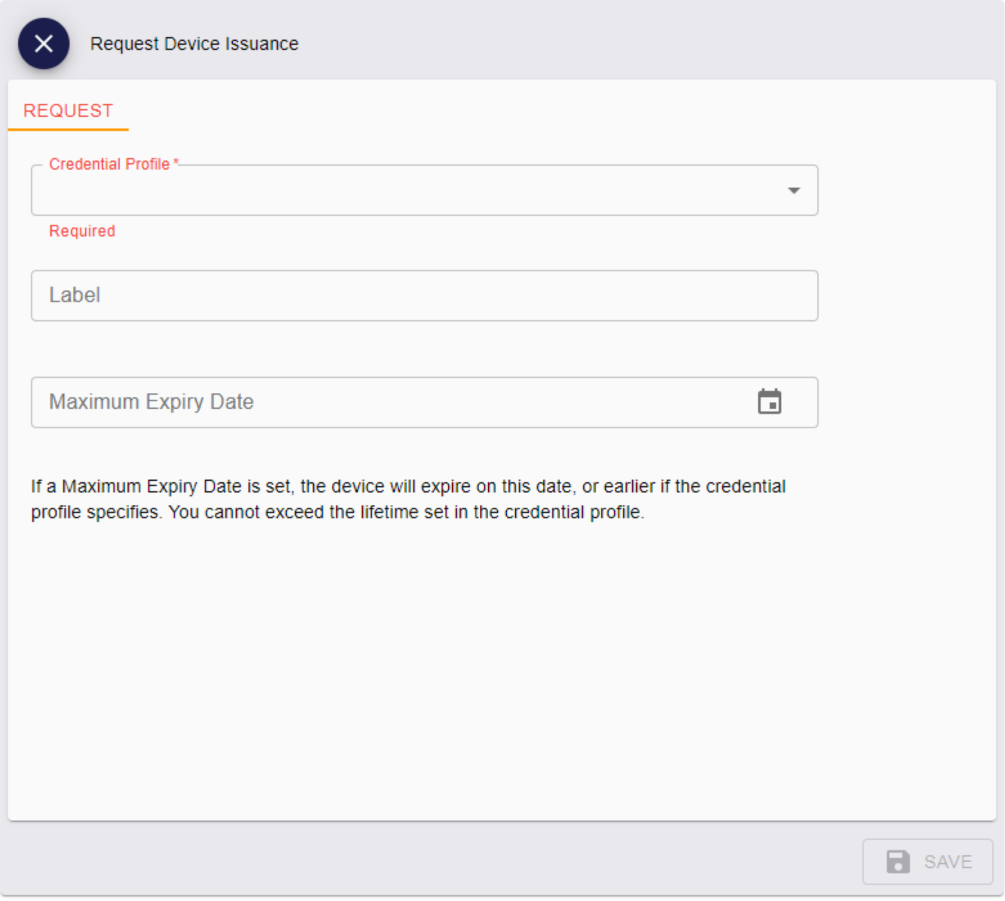
   For example:

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

You can request a device for a person directly from a directory; MyID automatically carries out the import of the person's details into the MyID database as if you had added the person from the directory manually (see section *4.2.2*, *Adding a person from a directory*). Any issues that occur when attempting to import the person's details are displayed on screen when you click **Save**.

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

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



If a Maximum Expiry Date is set, the device will expire on this date, or earlier if the credential profile specifies. You cannot exceed the lifetime set in the credential profile.

3. From the **Credential Profile** drop-down list, select the credential profile you want to use for the device.

   The credential profiles available depend on the role of the operator and the role of the person for whom you are requesting the device; see the *Linking credential profiles to roles* section in the ***Administration Guide***.

   It is possible that there may be no credential profiles available for the person; this is most likely to occur when you are requesting a device for a person directly from the directory, and LDAP linked roles and default group roles are not set up; in this case, you are recommended to edit the person's details and manually assign a role that has access to one or more credential profiles.

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

   You can use the label to search for the request:

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

  See section *6.1*, *Searching for a request*.
- In MyID Desktop, in the **Job Management** workflow, use the **Batch Label** box.

  See the *Searching for jobs* section in the ***Administration Guide***.

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

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

   The maximum expiry date is the requested date on which the device will expire. You can select any date up to the `MaxRequestExpiryDate` specified for the person in the Lifecycle API. Note, however, that you cannot exceed the **Lifetime** setting for the credential profile; if the request is made for a credential to expire on a date six months from now, but the credential profile has a lifetime of 30 days, the device will be issued with a lifetime of 30 days.

   The credential profile can override the `MaxRequestExpiryDate` set for the person if the **Ignore User Expiry Date** option on the credential profile is set.

   Note: If the **Expire cards at end of day** configuration option (on the **Issuance Processes** page of the **Operation Settings** workflow) is set to Yes, the requested date will be 23:59 UTC on the date selected. See the *Issuance Processes page (Operation Settings)* section in the ***Administration Guide***.
6. Click **Save** to make the request.

Once you have created the request, the View Request screen appears. From this screen, you can cancel or collect the device request. See section *6*, *Working with requests*.

Note, however, that if the credential profile requires validation, you cannot approve or reject the request from this screen; another operator must carry out the approval procedure.

4.5.2 Requesting devices for multiple people

If you want to request devices for multiple people, you can request the devices in a batch instead of requesting them one by one.

Note: You can access the **Tools** menu only if you have a role with the **Tools Menu** option from the **Configuration** section of the **Edit Roles** workflow.

To request devices for multiple people:

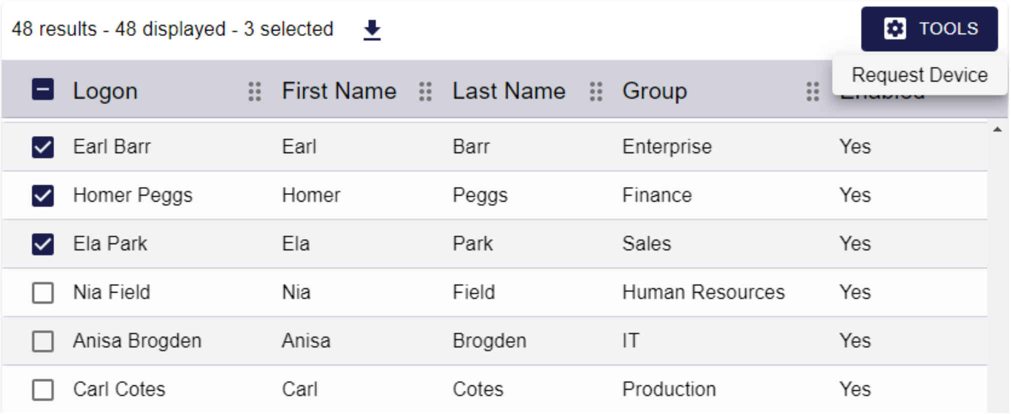
1. Search the directory for the people for whom you want to request devices.

   See section *4.1*, *Searching for a person*.

2. On the search results page, use the checkboxes to the left of the records to select one or more people.

   Note: If you select one person, the process is the same as clicking the **Request Device** option in the button bar at the bottom of the View Person screen; MyID uses the batch process only if you select more than one person. See section *4.5.1*, *Requesting a device* for details of requesting a single device.

3. From the **Tools** menu, select **Request Device**.



48 results - 48 displayed - 3 selected

⊟	Logon	First Name	Last Name	Group	
☑	Earl Barr	Earl	Barr	Enterprise	Yes
☑	Homer Peggs	Homer	Peggs	Finance	Yes
☑	Ela Park	Ela	Park	Sales	Yes
☐	Nia Field	Nia	Field	Human Resources	Yes
☐	Anisa Brogden	Anisa	Brogden	IT	Yes
☐	Carl Cotes	Carl	Cotes	Production	Yes

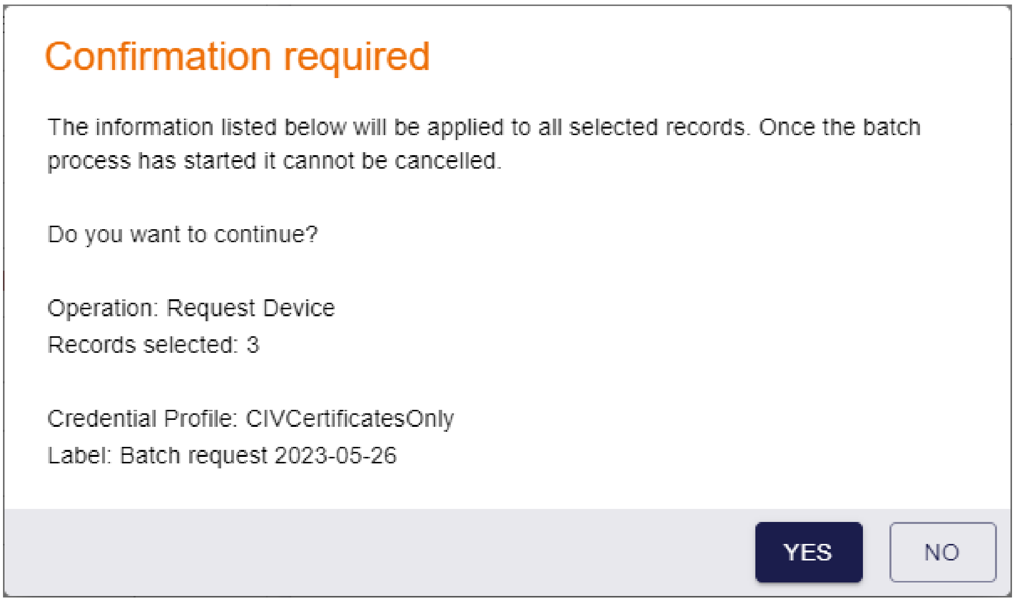
   The Request Device Issuance screen appears.

   Complete the details as for requesting a device for a single person, including the credential profile to be used for the requested devices; see section *4.5.1*, *Requesting a device*.

   Note: The list of credential profiles is constrained by the roles of the operator, not the potential recipients; this means that you can attempt to request devices using credential profiles that are not available to an individual recipient. If a credential profile is not available for a recipient, the request fails at the batch processing stage; however, the requests for other recipients who *do* have permission to receive the credential profile succeed.

4. Click **Save**.

   The confirmation screen appears.



Confirmation required

The information listed below will be applied to all selected records. Once the batch process has started it cannot be cancelled.

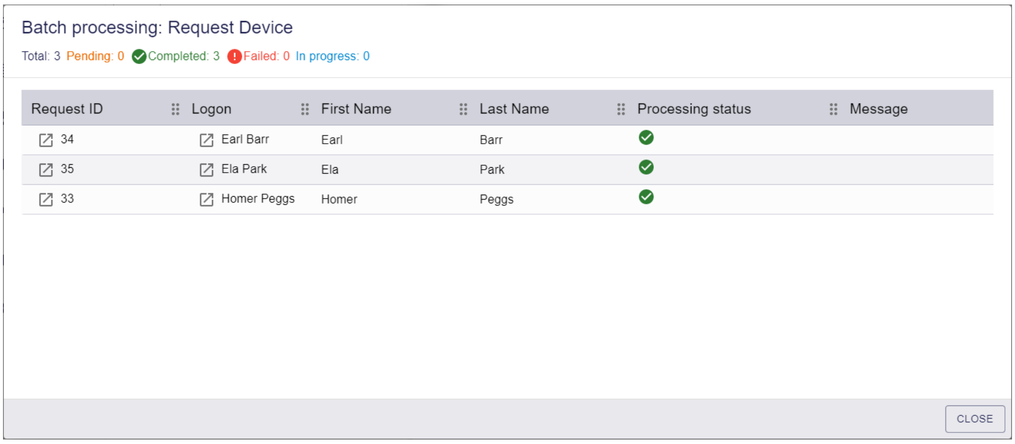
Do you want to continue?

Operation: Request Device
Records selected: 3

Credential Profile: CIVCertificatesOnly
Label: Batch request 2023-05-26

5. Click **Yes** to proceed with the request, or **No** to go back to the list of people.

   When you click **Yes**, the Batch Processing screen appears.



Batch processing: Request Device

Total: 3 Pending: 0 ✓Completed: 3 !Failed: 0 In progress: 0

Request ID	Logon	First Name	Last Name	Processing status	Message
34	Earl Barr	Earl	Barr	✓	
35	Ela Park	Ela	Park	✓	
33	Homer Peggs	Homer	Peggs	✓	

6. The requests are processed. The table shows the status of each request:

✓	The request succeeded.
!	The request failed. The Message column displays the reason for the failure; for example, the person may not have permissions for the credential profile selected.

7. Click **Close**.

4.5.3 Known issues

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

  A problem has been identified when the following scenario occurs:

  - A user account is added to MyID from Active Directory.
  - The user account is removed from Active Directory, but no removal of the account from MyID takes place.
  - A new user account is created in Active Directory with the same logon name.
  - An attempt is made to request credentials for that user account in MyID.

  When this occurs, errors similar to the following appear:

  - In the Request Card workflow in MyID Desktop:

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

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

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

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

4.6 Requesting a mobile device for a person

See the ***Mobile Identity Management*** guide for details of configuring your system to issue mobile IDs, and the ***Mobile Identity Documents*** guide for details of configuring your system to issue mobile identity documents..

4.6.1 Requesting a mobile device

To request a mobile device for a person:

1. Search for a person, and view their details.

   See section *4.1*, *Searching for a person* for details.

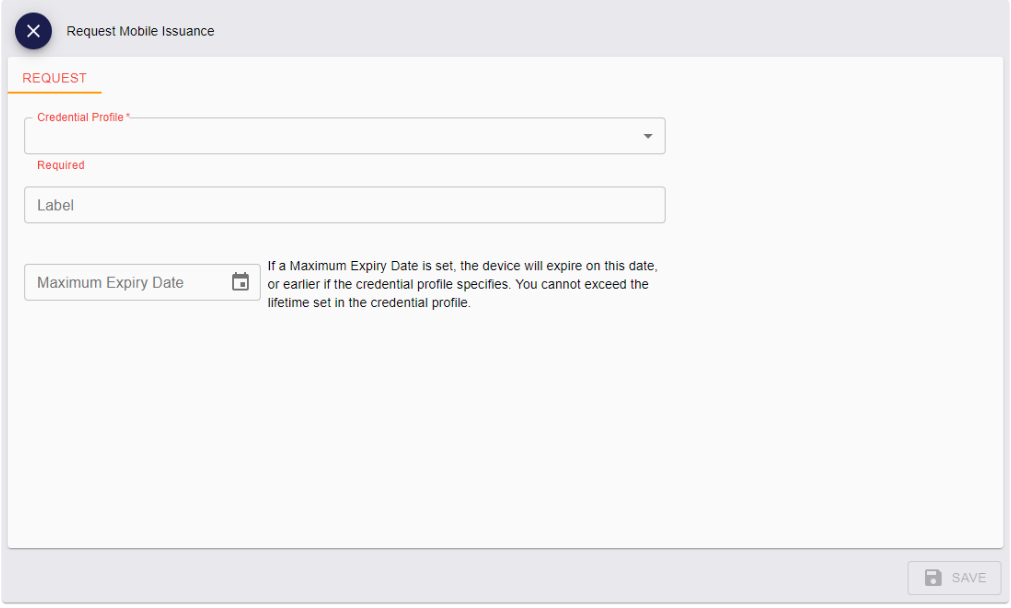
   You can also view a person's details from any form that contains a link to their account.

   For example:

   - Click the link icon ↗ on the **Full Name** field of the View Request form.
   - Click the link icon ↗ on the **Owner** field of the View Device form.
2. Click one of the following options in the button bar at the bottom of the screen:
   - **Request Mobile** – requests a mobile device for the person.
   - **Request Mobile (View Auth Code)** – requests a mobile device for the person, and displays the collection URL and authentication code for the device on the View Request screen at the end of the process.

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

   The Request Mobile Issuance screen appears.



If a Maximum Expiry Date is set, the device will expire on this date, or earlier if the credential profile specifies. You cannot exceed the lifetime set in the credential profile.

3. From the **Credential Profile** drop-down list, select the credential profile you want to use for the device.

   The credential profile must have a **Card Encoding** setting of **Identity Agent** for mobile identities, or **Mobile Identity Document** for mobile identity documents.

   See the *Creating the Identity Agent credential profile* section in the ***Mobile Identity Management*** guide for details of mobile identity credential profiles.

   See the *Creating the mobile identity document credential profile* section in the ***Mobile Identity Documents*** guide for details of mobile identity credential profiles.

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

   You can use the label to search for the request:

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

     See section *6.1*, *Searching for a request*.

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

     See the *Searching for jobs* section in the ***Administration Guide***.

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

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

   The maximum expiry date is the requested date on which the device will expire. You can select any date up to the `MaxRequestExpiryDate` specified for the person in the Lifecycle API. Note, however, that you cannot exceed the **Lifetime** setting for the credential profile; if the request is made for a credential to expire on a date six months from now, but the credential profile has a lifetime of 30 days, the device will be issued with a lifetime of 30 days.

   The credential profile can override the `MaxRequestExpiryDate` set for the person if the **Ignore User Expiry Date** option on the credential profile is set.

Note: If the **Expire cards at end of day** configuration option (on the **Issuance Processes** page of the **Operation Settings** workflow) is set to Yes, the requested date will be 23:59 UTC on the date selected. See the *Issuance Processes page (Operation Settings)* section in the ***Administration Guide***.

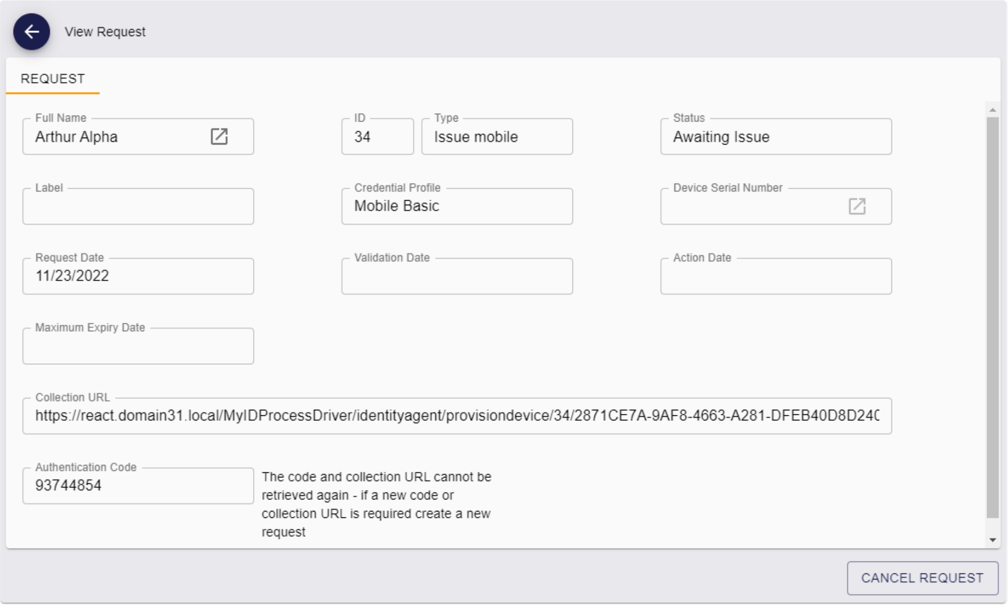
6. Click **Save** to make the request.

Once you have created the request, the View Request screen appears. From this screen, you can cancel the device request. If the request requires validation, another operator must approve the request; the operator who makes a request cannot validate it. See section *6.2*, *Approving, rejecting, and canceling requests*.

Once the request is ready for collection (after approval, if necessary), MyID sends the collection URL and an authentication code to the person for whom the device was requested; see the *Configuring SMS and email notifications for the MyID Operator Client* section in the ***Mobile Identity Management*** guide or the *Configuring SMS and email notifications for the MyID Operator Client* section in the ***Mobile Identity Documents*** guide for details.

As an alternative to sending the collection URL and authentication code as notifications, you can use the **Request Mobile (View Auth Code)** option instead; when you use this option, the following additional information is provided on the View Request screen:

- **Collection URL** – The URL that the person must access on their mobile device to collect the mobile device.
- **Authentication Code** – The authentication code that the person must provide to collect the mobile device.



Full Name: Arthur Alpha
ID: 34
Type: Issue mobile
Status: Awaiting Issue
Label:
Credential Profile: Mobile Basic
Device Serial Number:
Request Date: 11/23/2022
Validation Date:
Action Date:
Maximum Expiry Date:
Collection URL: https://react.domain31.local/MyIDProcessDriver/identityagent/provisiondevice/34/2871CE7A-9AF8-4663-A281-DFEB40D8D24
Authentication Code: 93744854

The code and collection URL cannot be retrieved again - if a new code or collection URL is required create a new request

You can provide these details to the person manually; this is an alternative to using email and SMS notifications to provide this information. If the credential profile requires validation, make sure that the request has been validated before you provide the information to the person; if you use email and SMS notifications, then these are not sent until the request has been validated.

Note: These fields are displayed only once, at the end of the **Request Mobile (View Auth Code)** operation; if you view the request again, you will not be able to view this information.

4.6.2 Requesting mobile devices for multiple people

If you want to request mobile devices for multiple people, you can request the mobile devices in a batch instead of requesting them one by one.

Note: You can access the **Tools** menu only if you have a role with the **Tools Menu** option from the **Configuration** section of the **Edit Roles** workflow.

To request mobile devices for multiple people:

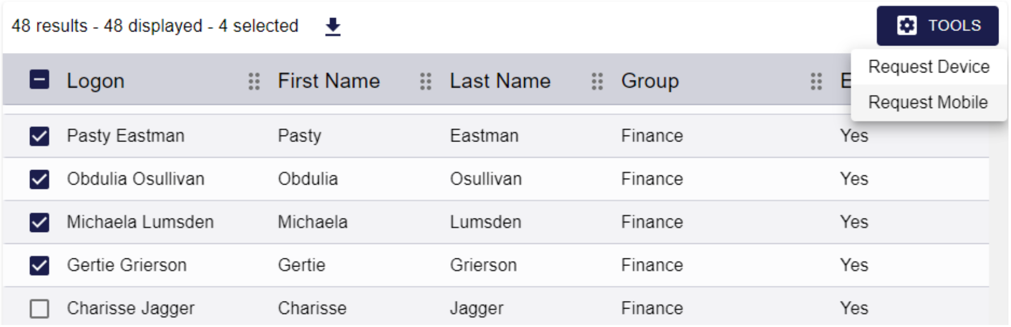
1. Search the directory for the people for whom you want to request mobile devices.

   See section *4.1*, *Searching for a person*.

2. On the search results page, use the checkboxes to the left of the records to select one or more people.

   Note: If you select one person, the process is the same as clicking the **Request Mobile** option in the button bar at the bottom of the View Person screen; MyID uses the batch process only if you select more than one person. See section *4.6.1*, *Requesting a mobile device* for details of requesting a single device.

3. From the **Tools** menu, select **Request Mobile**.

   48 results - 48 displayed - 4 selected

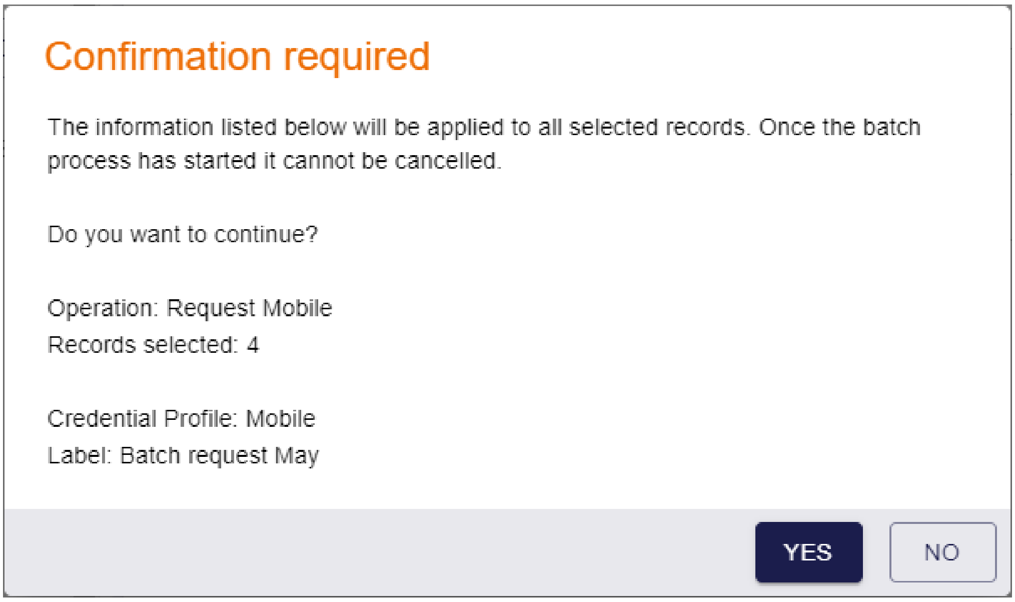
	Logon	First Name	Last Name	Group	E
☑	Pasty Eastman	Pasty	Eastman	Finance	Yes
☑	Obdulia Osullivan	Obdulia	Osullivan	Finance	Yes
☑	Michaela Lumsden	Michaela	Lumsden	Finance	Yes
☑	Gertie Grierson	Gertie	Grierson	Finance	Yes
☐	Charisse Jagger	Charisse	Jagger	Finance	Yes

   The Request Mobile Issuance screen appears.

   Complete the details as for requesting a device for a single person, including the credential profile to be used for the requested devices; see section *4.6.1*, *Requesting a mobile device*.

4. Click **Save**.

   The confirmation screen appears.



Confirmation required

The information listed below will be applied to all selected records. Once the batch process has started it cannot be cancelled.

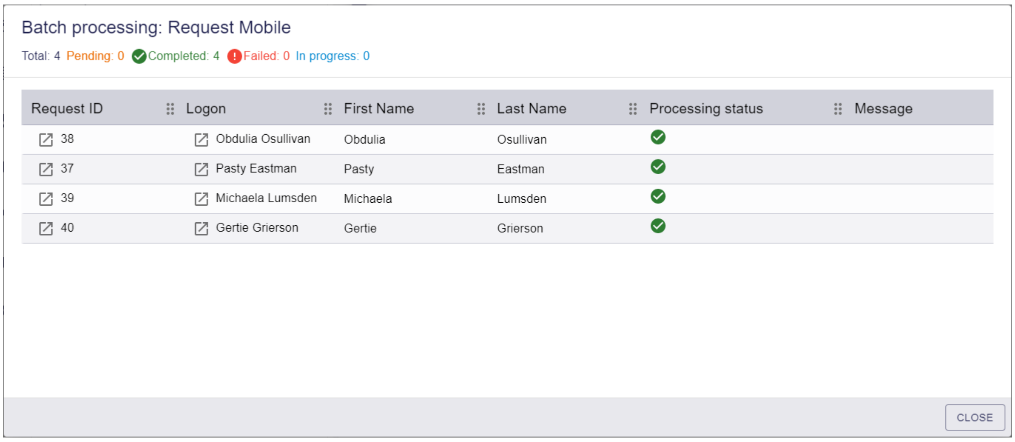
Do you want to continue?

Operation: Request Mobile
Records selected: 4

Credential Profile: Mobile
Label: Batch request May

5. Click **Yes** to proceed with the request, or **No** to go back to the list of people.

   When you click **Yes**, the Batch Processing screen appears.



Batch processing: Request Mobile

Total: 4 Pending: 0 ✓Completed: 4 !Failed: 0 In progress: 0

Request ID	Logon	First Name	Last Name	Processing status	Message
38	Obdulia Osullivan	Obdulia	Osullivan	✓	
37	Pasty Eastman	Pasty	Eastman	✓	
39	Michaela Lumsden	Michaela	Lumsden	✓	
40	Gertie Grierson	Gertie	Grierson	✓	

6. The requests are processed. The table shows the status of each request:

✓	The request succeeded.
!	The request failed. The Message column displays the reason for the failure; for example, the person may not have permissions for the credential profile selected.

7. Click **Close**.

4.7 Synchronizing a person

You can manually synchronize a person's details with your directory.

Manual synchronization is not required if you have the **Background update** option set; when this option is set, MyID synchronizes the directory information whenever you view or edit the person within MyID. See the *Using an LDAP directory* section in the ***Administration Guide***.

Note: Your role must have permission to use the **Directory Sync** option to use this feature. See section *3.5*, *Roles and groups* for details.

To synchronize a person:

1. Search for a person in the MyID database, and view their details.

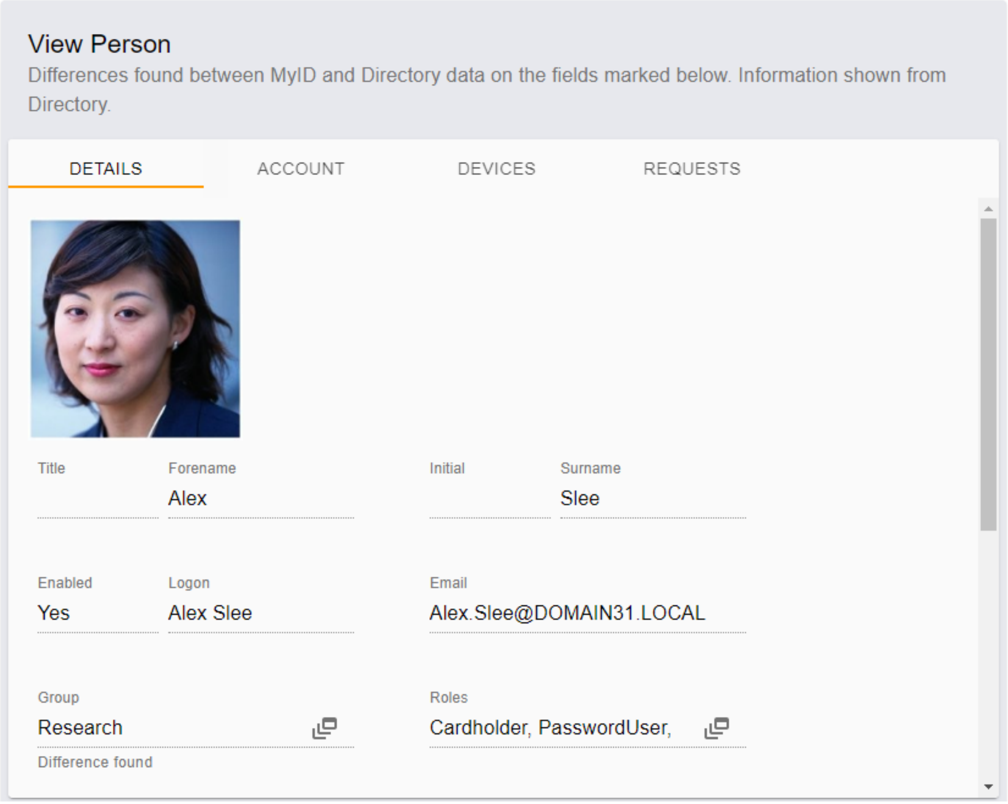
   See section *4.1*, *Searching for a person* for details.

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

   For example:

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

   If there are any differences between the details stored in the MyID database and the directory, these are highlighted on screen. The differences are shown for any directory-linked account, whether you searched the MyID database or searched a directory. In this case, the account details from the directory are displayed; in all other situations, the information displayed is taken from the MyID database.



View Person

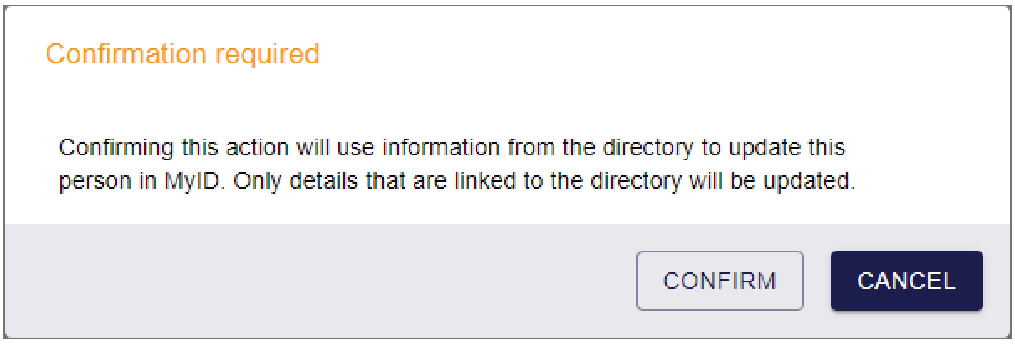
Differences found between MyID and Directory data on the fields marked below. Information shown from Directory.

Title	Forename Alex	Initial	Surname Slee
Enabled Yes	Logon Alex Slee	Email Alex.Slee@DOMAIN31.LOCAL	
Group Research Difference found		Roles Cardholder, PasswordUser,	

2. Click the **Directory Sync** option in the button bar at the bottom of the screen.

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

   A confirmation dialog appears.

   Confirmation required

   Confirming this action will use information from the directory to update this person in MyID. Only details that are linked to the directory will be updated.

3. Click **Confirm** to synchronize the person's details with the directory.

When a synchronization (whether a manual directory synchronization, caused by the **Background update** option, or triggered by the Batch LDAP Synchronization Tool) sets a person's **Enabled** flag to No, the person's user account in MyID is disabled, and all of their devices, certificates, and jobs are suspended. If a synchronization sets a person's **Enabled** flag to Yes, their account is enabled again; if the **Enable credentials when person is enabled** configuration option is set to Yes, all of their issued but disabled devices and suspended certificates and jobs are reactivated.

4.8 Enabling or disabling a person

You can enable or disable a person's user record in MyID. A person whose account is disabled cannot log on to MyID, and cannot be issued a card. You cannot disable a person's user record in a directory; this feature is for people stored in the MyID database only.

4.8.1 Disabling a person's user record

To disable a person's user record:

1. Search for a person in the MyID database, and view their details.

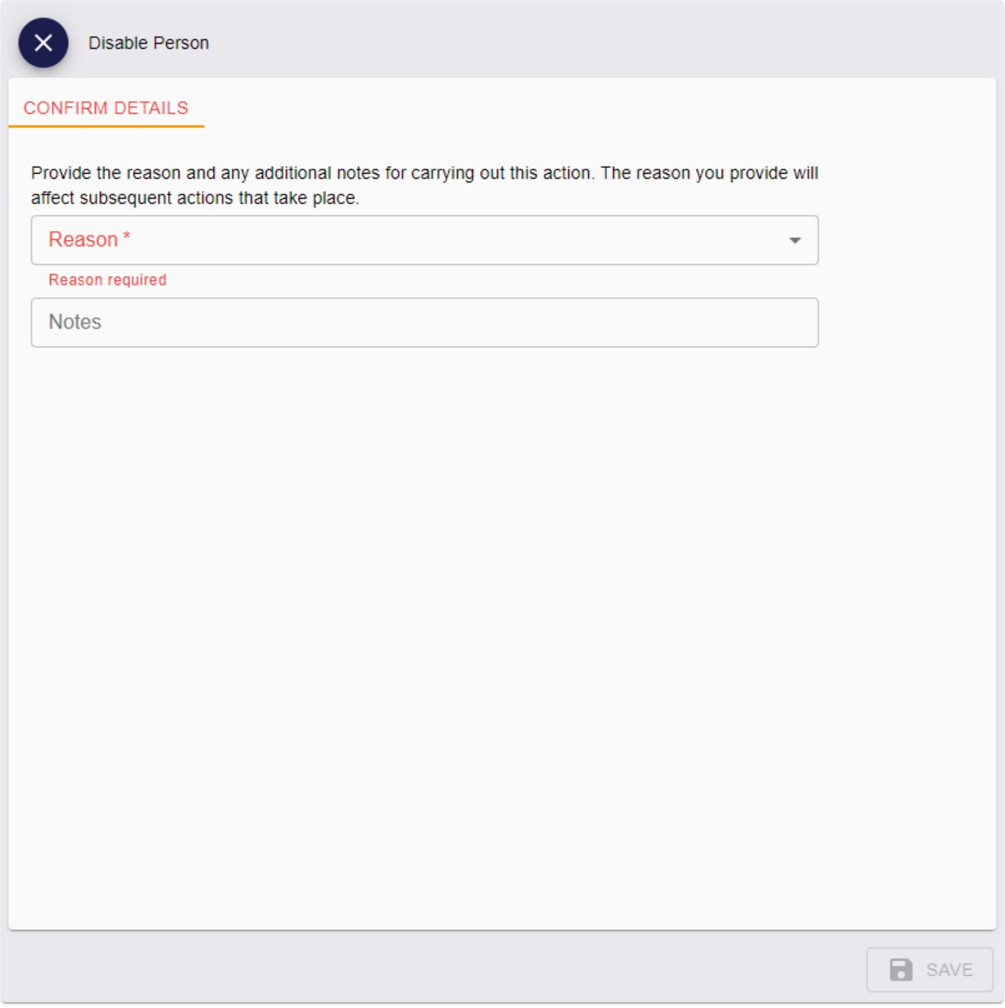
   See section *4.1*, *Searching for a person* for details.

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

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

2. Click the **Disable Person** option in the button bar at the bottom of the screen.

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



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

3. From the **Reason** drop-down list, select the reason that you are disabling the person's user record.

   The reason you select determines what happens to any devices already issued to the person. See the *Certificate reasons* section in the ***Operator's Guide*** for details.
4. Type any additional **Notes** in the provided box.
5. Click **Save**.

4.8.2 Enabling a person's user account

To re-enable a person's user record:

1. Search for a person in the MyID database, and view their details.

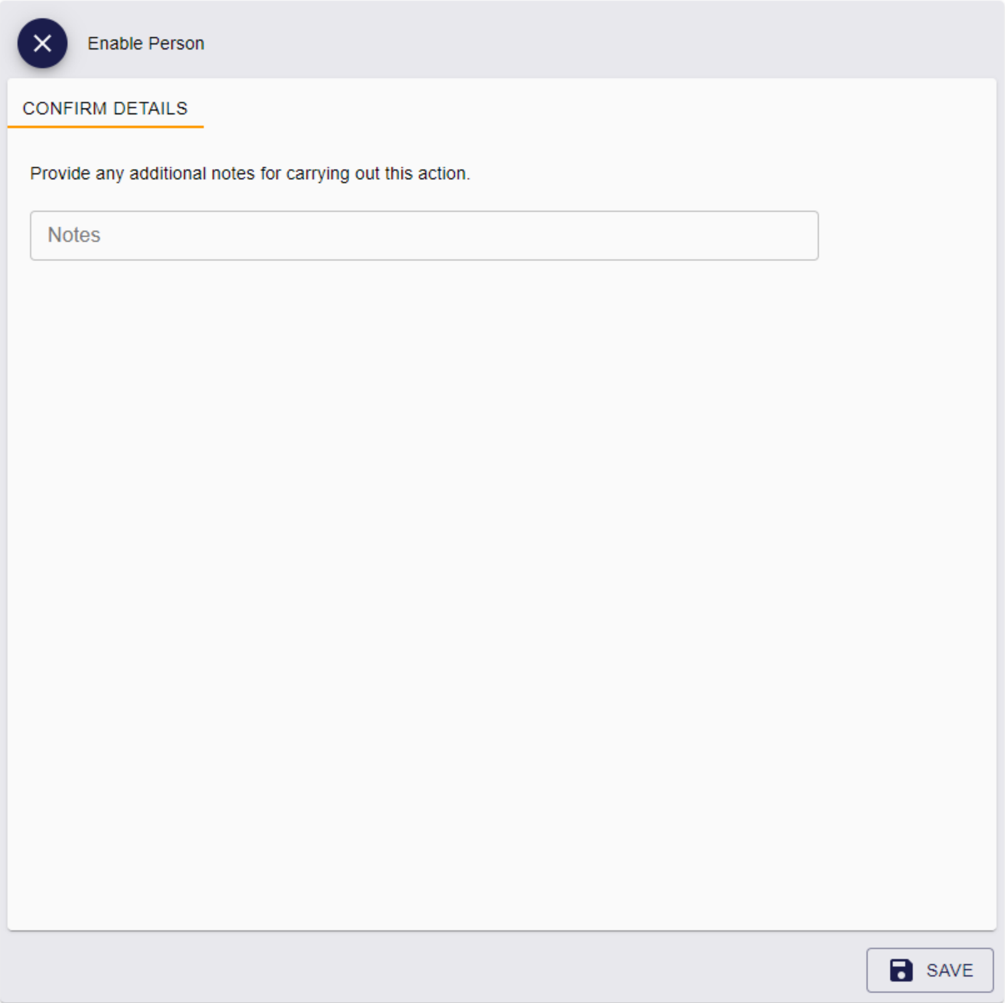
   See section *4.1*, *Searching for a person* for details.

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

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

2. Click the **Enable Person** option in the button bar at the bottom of the screen.

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



Provide any additional notes for carrying out this action.

3. Type any **Notes** in the provided box.
4. Click **Save**.

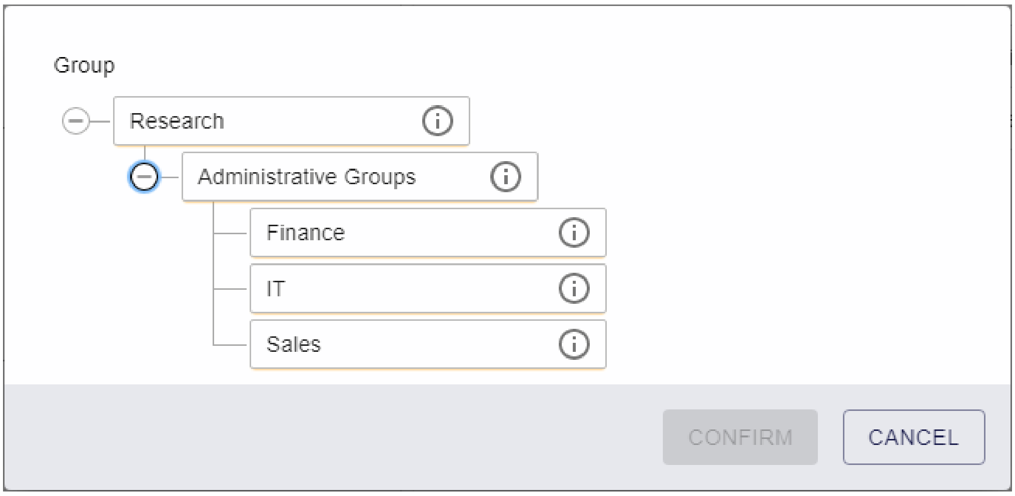
4.9 Working with administrative groups

You can set up your MyID system to allow administrative groups; these are extra groups for which an operator has administrative access.

You must set the **Allow Administrative Groups** option on the **Process** tab of the **Security Settings** workflow; see the *Administrative groups* section in the ***Administration Guide*** for details.

4.9.1 Selecting an administrative group

Any administrative groups you have available are displayed in the group selection dialog at the bottom of the list:


Group
Research
Administrative Groups
Finance
IT
Sales
CONFIRM
CANCEL

Expand the **Administrative Groups** option, select the administrative group you want to use, then click **Confirm**.

Note: If you are selecting a group as part of your search criteria, if the administrative group is linked to an OU in your directory, MyID searches that OU as well as any sub-OUs, even if those sub-OUs are not themselves mapped in MyID.

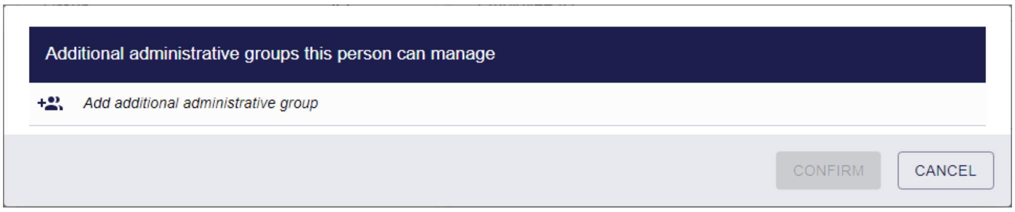
4.9.2 Assigning administrative groups

If your system is set up for administrative groups, you can assign administrative groups when you are editing a person.

To assign administrative groups:

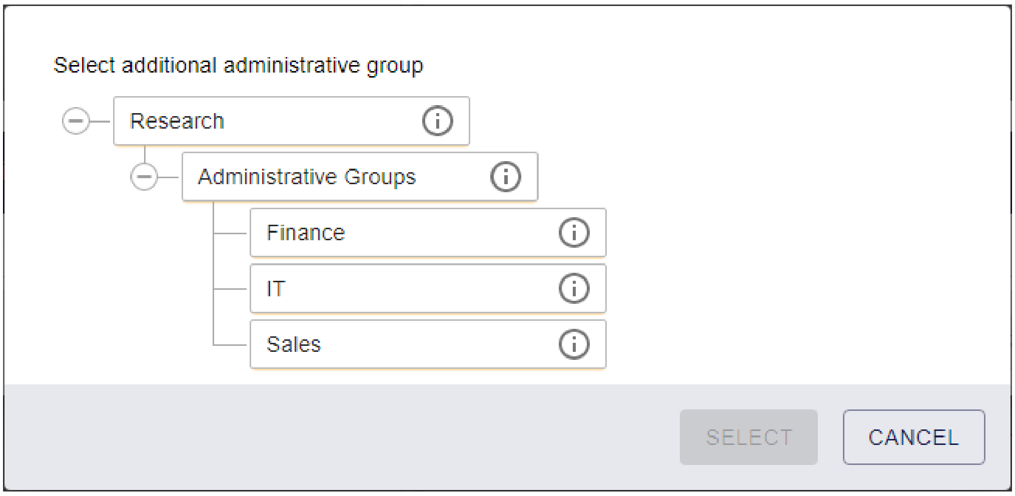
1. On the Edit Person screen, click the **Administrative Groups** field.

   A dialog appears listing any existing administrative groups, and allowing you to add new administrative groups.


Additional administrative groups this person can manage
Add additional administrative group
CONFIRM
CANCEL

2. To add a group:
   a. Click the add icon next to *Add additional administrative group*.

      A dialog appears that allows you to select a group.



Select additional administrative group

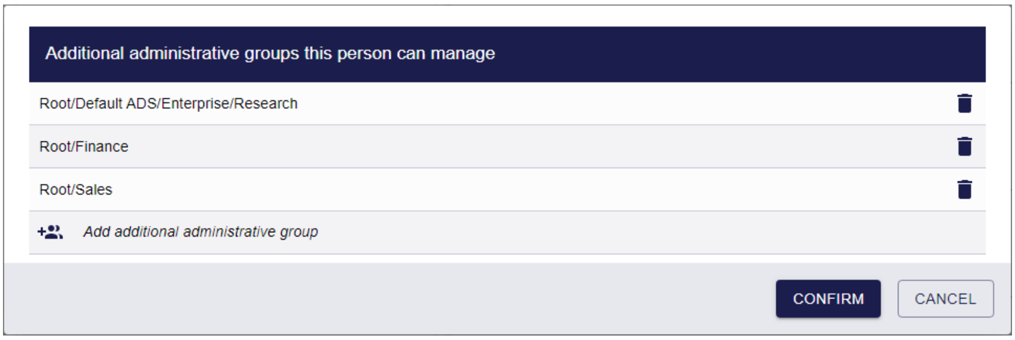
- Research
  - Administrative Groups
    - Finance
    - IT
    - Sales

   b. Select the group you want to add as an administrative group.

      You can select any group for which you have scope, or any group for which you have administrative access.

   c. Click **Select**.

      The group is added to the list.



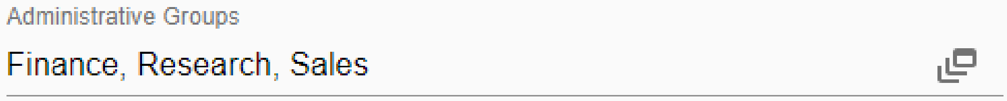
Additional administrative groups this person can manage

Root/Default ADS/Enterprise/Research
Root/Finance
Root/Sales

3. To add more groups, click the add icon again.
4. To remove an administrative group, click the delete icon for the group.

   Note: You can remove an administrative group only if you have permission to that group yourself; that is, it is within your scope, or in your own list of administrative groups.
5. When you have completed the list of administrative groups, click **Confirm**.

   The list of groups is displayed in the **Administrative Groups** field.



Administrative Groups: Finance, Research, Sales

4.10 Removing a person

You can remove a person from the system, revoking any certificates and canceling any devices that have been issued to them. All information about the person is removed from the system, with the exception of audit information.

You can configure MyID so that any people that are removed are archived in a separate table on the database, allowing you to keep track of all the users that have existed in the system; see the *Archiving deleted users* section in the ***Administration Guide*** for details.

To remove a person's user record:

1. Search for a person in the MyID database, and view their details.

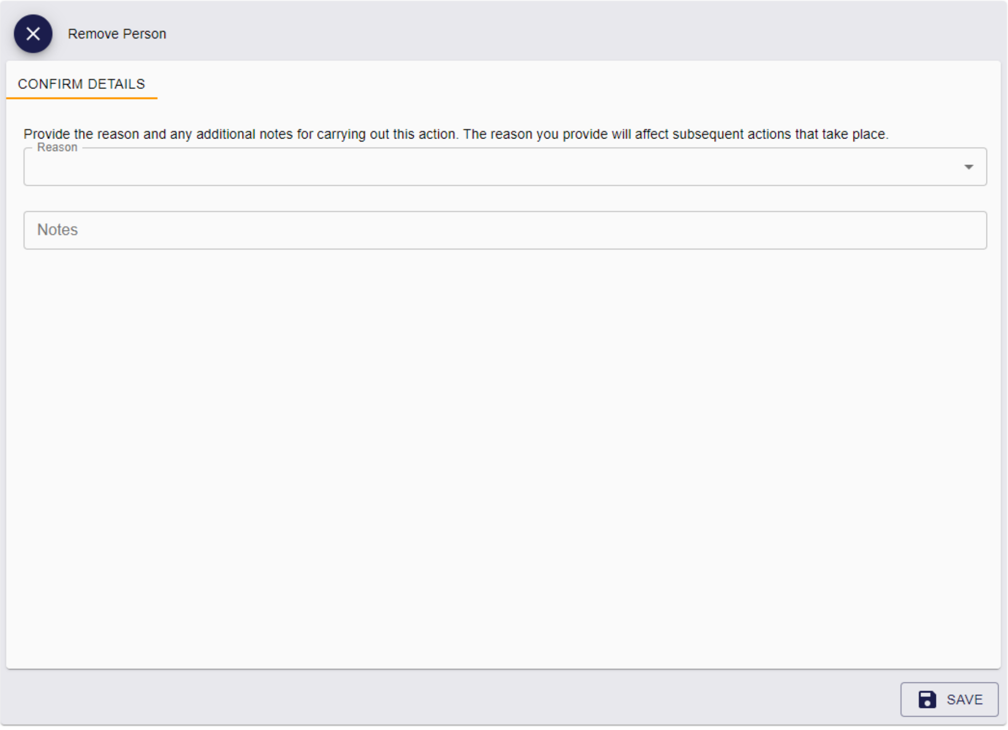
   See section *4.1*, *Searching for a person* for details.

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

   - Click the link icon ↗ on the **Full Name** field of the View Request form.
   - Click the link icon ↗ on the **Owner** field of the View Device form.
2. Click the **Remove Person** option in the button bar at the bottom of the screen.

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

   The Remove Person screen appears.



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

3. From the **Reason** drop-down list, select the reason that you are removing the person's user record.

The reason you select determines what happens to any devices and certificates already issued to the person. See the *Certificate reasons* section in the ***Operator's Guide*** for details.

4. Type any additional **Notes** in the provided box.
5. Click **Save**.

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

4.11 Authenticating a person

You can authenticate a person using their stored fingerprints, identity documents, security phrases, or by operator approval, using the **Authenticate Person** workflow in MyID Desktop.

For more information about using MyID Desktop and Self-Service App workflows from within the MyID Operator Client, see section *3.3.2*, *Launching MyID Desktop, Self-Service App, or MyID Client for Windows workflows*.

To authenticate a person:

1. Search for a person in the MyID database, and view their details.

   See section *4.1*, *Searching for a person* for details.

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

   - Click the link icon ↗ on the **Full Name** field of the View Request form.
   - Click the link icon ↗ on the **Owner** field of the View Device form.
2. Click the **Authenticate Person** option in the button bar at the bottom of the screen.

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

   The **Authenticate Person** workflow appears in a MyID Desktop window with the person already selected.

   See the *Authenticating users* section in the ***Operator's Guide***.

4.12 Sending an authentication code to a person

As an operator, you can send an authentication code to a person that allows them to authenticate to the MyID server and log on to the MyID Operator Client.

For more information on setting up MyID for authentication code logon, see the *Configuring authentication codes for the MyID authentication server* section in the ***Administration Guide***.

To send an authentication code to a person:

1. Search for a person in the MyID database, and view their details.

   See section *4.1*, *Searching for a person* for details.

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

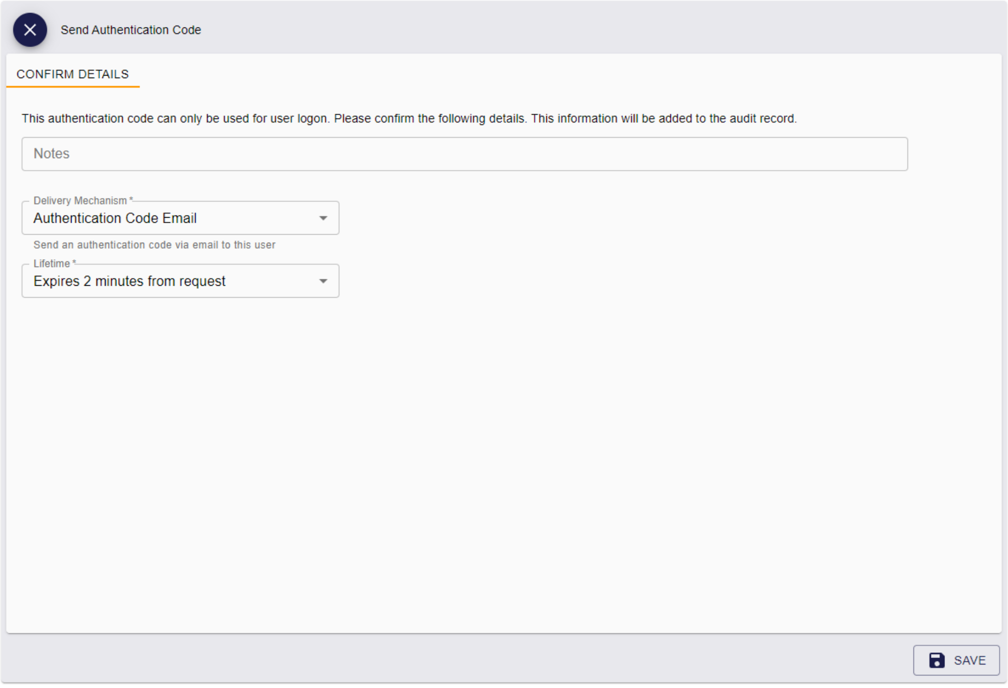
- Click the link icon ↗ on the **Full Name** field of the View Request form.
- Click the link icon ↗ on the **Owner** field of the View Device form.

2. Click the **Send Auth Code** option in the button bar at the bottom of the screen.

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

   You must make sure that you have the **Send Auth Code for Logon** option selected for your role in the **Edit Roles** workflow.

   The Send Authentication Code screen appears.



Send Authentication Code

CONFIRM DETAILS

This authentication code can only be used for user logon. Please confirm the following details. This information will be added to the audit record.

Notes

Delivery Mechanism *: Authentication Code Email

Send an authentication code via email to this user

Lifetime *: Expires 2 minutes from request

3. Type any **Notes** you want to store in the audit trail about the operation.
4. From the **Delivery Mechanism** drop-down list, select how you want to send the code.

   You can choose from:

   - **Authentication Code Email** – sends the code as an email to the person's configured email address. This option is available if the **Authentication Code Email** template is enabled in the **Email Templates** workflow.
   - **Authentication Code SMS** – sends the code as a text message to the person's configured cell phone number. This option is available if the **Authentication Code SMS** template is enabled in the **Email Templates** workflow.

   Note: The complexity of the code is determined by the **Complexity** option configured in the email template. See the *Changing email messages* section in the ***Administration Guide*** for details.

5. From the **Lifetime** drop-down list, select how long you want the code to be valid.

   The options here are determined by the values saved in the **Auth Code Lifetime for Immediate Use** and **Auth Code Lifetime** configuration options; by default, the options are:

   - **Expires 30 days from request** – based on the default **Auth Code Lifetime** setting of 720 hours.
   - **Expires 2 minutes from request** – based on the default **Auth Code Lifetime for Immediate Use** setting of 120 seconds.

6. Click **Save**.

   MyID sends the authentication code to the person, who can then use it to authenticate to MyID; see section *3.2.5*, *Signing in using single-use authentication codes*.

4.13 Viewing an authentication code for a person

As an operator, you can request an authentication code for a person that allows them to authenticate to the MyID server and log on to the MyID Operator Client. The code is displayed on your screen, and you can then provide it to the person who needs to log on; for example, by reading the code out over the phone.

For details of using an authentication code to log on to MyID, see section *3.2.5*, *Signing in using single-use authentication codes*.

For more information on setting up MyID for authentication code logon, see the *Configuring authentication codes for the MyID authentication server* section in the ***Administration Guide***.

To view an authentication code for a person:

1. Search for a person in the MyID database, and view their details.

   See section *4.1*, *Searching for a person* for details.

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

   For example:

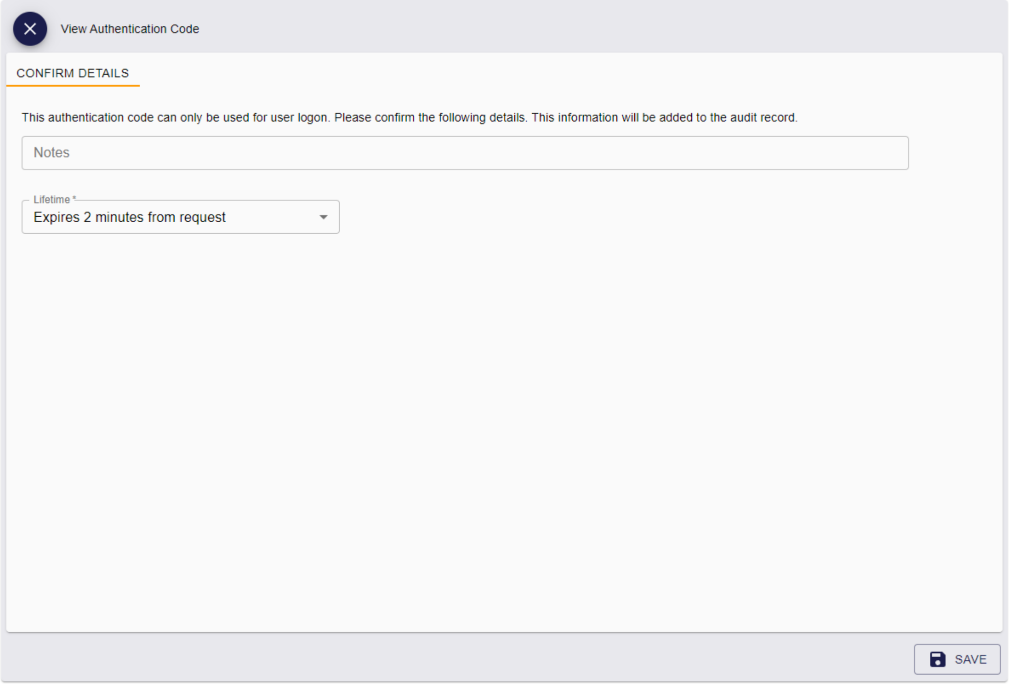
   - Click the link icon ↗ on the **Full Name** field of the View Request form.
   - Click the link icon ↗ on the **Owner** field of the View Device form.

2. Click the **View Auth Code** option in the button bar at the bottom of the screen.

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

   You must make sure that you have the **View Auth Code for Logon** option selected for your role in the **Edit Roles** workflow.

   The View Authentication Code screen appears.



This authentication code can only be used for user logon. Please confirm the following details. This information will be added to the audit record.

Notes

Lifetime *: Expires 2 minutes from request

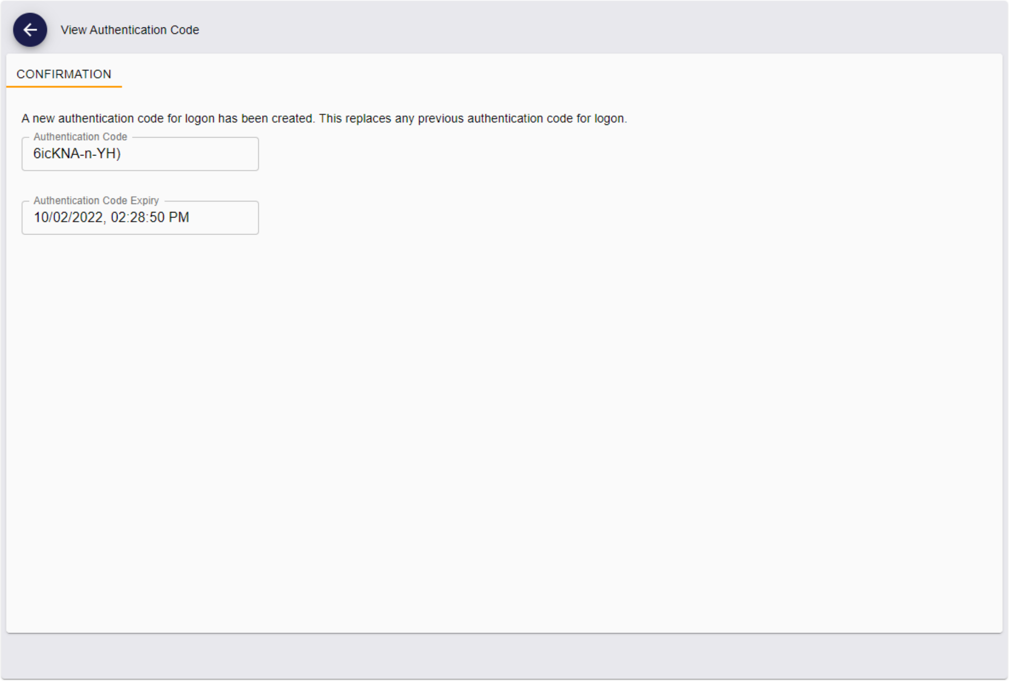
3. Type any **Notes** you want to store in the audit trail about the operation.
4. From the **Lifetime** drop-down list, select how long you want the code to be valid.

   The options here are determined by the values saved in the **Auth Code Lifetime for Immediate Use** and **Auth Code Lifetime** configuration options; by default, the options are:

   - **Expires 30 days from request** – based on the default **Auth Code Lifetime** setting of 720 hours.
   - **Expires 2 minutes from request** – based on the default **Auth Code Lifetime for Immediate Use** setting of 120 seconds.

   Note: The complexity of the code is determined by the **Auth Code Complexity** configuration option.
5. Click **Save**.

   MyID displays the authentication code on screen. You can now provide this to the person who needs to authenticate to MyID; for example, you can read the code out over the phone, or send it by a secure chat channel.



A new authentication code for logon has been created. This replaces any previous authentication code for logon.

Authentication Code: 6icKNA-n-YH)

Authentication Code Expiry: 10/02/2022, 02:28:50 PM

4.14 Working with security phrases

You can launch the **Change Security Phrases** and **Unlock Security Phrases** workflows in MyID Desktop from the View Person screen.

For more information about using MyID Desktop and Self-Service App workflows from within the MyID Operator Client, see section *3.3.2*, *Launching MyID Desktop, Self-Service App, or MyID Client for Windows workflows*.

4.14.1 Changing a person's security phrases

If a person needs to change their security phrases, you can do it for them using the **Change Security Phrases** workflow.

To change a person's security phrases:

1. Search for a person in the MyID database, and view their details.

   See section *4.1*, *Searching for a person* for details.

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

   For example:

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

2. Click the **Change Security Phrases** option in the button bar at the bottom of the screen.

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

   The **Change Security Phrases** workflow appears in a MyID Desktop window with the person already selected.

   See the *Changing security phrases for a user* section in the ***Operator's Guide***.

4.14.2 Unlocking a person's 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 person's security phrases:

1. Search for a person in the MyID database, and view their details.

   See section *4.1*, *Searching for a person* for details.

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

   - Click the link icon ↗ on the **Full Name** field of the View Request form.
   - Click the link icon ↗ on the **Owner** field of the View Device form.
2. Click the **Unlock Security Phrases** option in the button bar at the bottom of the screen.

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

   The **Unlock Security Phrases** workflow appears in a MyID Desktop window with the person already selected.

   See the *Unlocking security phrases* section in the ***Administration Guide***.

4.15 Printing a badge

You can use the **Print Badge** workflow to print a card layout for a specific person onto a card that does not have a chip.

For more information about using MyID Desktop and Self-Service App workflows from within the MyID Operator Client, see section *3.3.2*, *Launching MyID Desktop, Self-Service App, or MyID Client for Windows workflows*.

To print a badge for a person:

1. Search for a person in the MyID database, and view their details.

   See section *4.1*, *Searching for a person* for details.

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

   - Click the link icon ↗ on the **Full Name** field of the View Request form.
   - Click the link icon ↗ on the **Owner** field of the View Device form.
2. Click the **Print Badge** option in the button bar at the bottom of the screen.

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

   The **Print Badge** workflow appears in a MyID Desktop window with the person already selected.

   See the *Printing badges* section in the ***Operator's Guide***.

4.16 Working with relationships

This feature requires additional customization using MyID Project Designer. For information on using relationships and user categories, contact Intercede customer support to discuss the requirements of your project, quoting reference SUP-384.

You can create relationships between two person accounts, or between person accounts of different categories.

You can view the relationships for a person on the **Relationships** tab of the View Person screen. If the person has no relationships, no information is available on this tab.

You can add or remove relationships of existing relationship types using the MyID Core API; however, by default, there are no relationship types – you must add them using Project Designer.

Note: To view the **Relationships** tab, you must have the **Get Relationships** option in **Edit Roles**. To add or remove relationships using the MyID Core API, you must have the **Manage Relationships** option in **Edit Roles**.

5 Working with devices

A device is an item such as a smart card, USB token, virtual smart card, or mobile device (cellphone or tablet) that can hold information about the person who has been issued the device, such as certificates and applets.

The MyID Operator Client allows you to work with devices in the following ways:

- You can create a request for a new device.

  See section *4.5*, *Requesting a device for a person*.
- You can search for a device.

  See section *5.1*, *Searching for a device*.
- You can search, view, and report on categories of devices.

  See section *5.3*, *Working with device categories*.
- You can read a device attached to the PC.

  See section *5.2*, *Reading a device*.
- You can request a replacement device.

  See section *5.4*, *Requesting a replacement device*.
- You can request a replacement mobile device.

  See section *5.5*, *Requesting a replacement mobile device*.
- You can request a renewal for a device that is near expiry.

  See section *5.6*, *Renewing a device*.
- You can cancel a device.

  See section *5.7*, *Canceling a device*.
- Reset the PIN for the device using the **Reset Card PIN** workflow in MyID Desktop.

  See section *5.8*, *Resetting a device's PIN*.
- Change the PIN for the device using the **Change PIN** workflow in MyID Desktop.

  See section *5.9*, *Changing a device PIN*.
- Carry out an assisted activation using the **Assisted Activation** workflow in MyID Desktop.

  See section *5.10*, *Activating a device*.
- Erase a device using the **Erase Card** workflow in MyID Desktop.

  See section *5.11*, *Erasing a device*.
- Unlock the device using the **Unlock Credential** workflow in MyID Desktop.

  See section *5.12*, *Unlocking a device*.
- You can send an authentication code to a person so they can activate their device.

  See section *5.13*, *Sending an authentication code to activate a device*.
- You can send a code to a person so they can unlock their device.

  See section *5.14*, *Sending a code to unlock a device*.

- Update a device using the **Collect My Updates** feature in the Self-Service App or the **Collect Updates** workflow in MyID Desktop.

  See section *5.15*, *Updating a device*.

- Completely re-encode a card using the **Reprovision Card** workflow in MyID Desktop.

  See section *5.16*, *Reprovisioning a device*.

- Request an update or full reprovision for a device.

  See section *5.17*, *Requesting an update for a device*.

- Manage access for a VSC using the **Manage VSC Access** and **Unlock VSC Temporary Access** workflows in MyID Desktop.

  See section *5.18*, *Managing VSCs*.

- Reinstate a device that has been mistakenly canceled or erased.

  See section *5.19*, *Reinstating a device*.

- Disposing of a device using the **Card Disposal** workflow in MyID Desktop.

  See section *5.20*, *Disposing of a device*.

- Printing a mailing document using the **Print Mailing Document** workflow in MyID Desktop.

  See section *5.21*, *Printing a mailing document*.

- Enable or disable a device.

  See section *5.22*, *Enabling and disabling devices*.

- Viewing extended device information using the **Identify Device (Administrator)** workflow in MyID Desktop.

  See section *5.23*, *Viewing extended information about a device*.

- Import a range of devices by providing details of their serial numbers.

  See section *5.24*, *Importing a range of devices*.

- Import a range of devices by providing their serial numbers in a manifest file.

  See section *5.25*, *Importing devices from a manifest file*.

- Search for imported devices and view their details.

  See section *5.26*, *Viewing imported devices*.

- Accept delivery for a single device or a batch of devices.

  See section *5.27*, *Accepting delivery for a device*.

- Viewing the initial server-generated PIN for a device.

  See section *5.28*, *Viewing the initial PIN for a device*.

5.1 Searching for a device

To search for a device:

1. Click the **Devices** category.
2. Select the search to use from the drop-down list.

   The following searches are available:

- **Assigned Devices** – searches only devices that are currently assigned to a person. This is the default search.
- **Mobile Devices** – searches only mobile devices.

  See section *7.3.16*, *Mobile Devices report*.
- **Unassigned Devices** – searches only devices that are *not* currently assigned to a person.

  See section *7.3.18*, *Unassigned Devices report*.
- **Available Device Stock** – provides a list of each device in the system available for stock transfer.

  See section *7.3.19*, *Available Device Stock report*.
- **Assign Device Search** – a limited search that is designed primarily to search for devices that you can assign to a request.

  See section *6.5*, *Assigning a device to a request* and section *7.3.20*, *Assign Device Search report*.
- **Devices** – searches all devices.

  See section *7.3.14*, *Devices report*.
- **Awaiting Delivery** – returns only devices that are awaiting delivery.

  See section *7.3.21*, *Awaiting Delivery report*.
- **Device Disposal** – displays devices and their disposal status.

  See section *7.3.22*, *Device Disposal report*.

However, your system may have additional custom device searches that you use for reporting.

3. Enter some or all of the search criteria for the target of the request.

   If you are using the default **Assigned Devices** search, the following search criteria are available:

   - **Owner Name (contains)** – type part of the device owner's name. You do not have to use wildcards; the search will match any part of the text you enter with the device owner's name.
   - **Group** – click the open icon to select the group to which the device owner belongs.

     See section *3.3.7*, *Selecting a group*.

     If you want to view devices for people from the groups below the selected group in the hierarchy, select the **Include Subgroups** option.
   - **Credential Profile** – select the credential profile that was used to issue the device from the drop-down list.
   - **Device Type** – select the type of device from the drop-down list.
   - **Process Status** – select the status of the device from the drop-down list; for example, **Active** or **Erased**.
   - **Enabled** – select whether or not the device is enabled from the drop-down list.

- **Serial Number** – type the serial number for the device. You can use wildcards.
- **Expires After** – select the date after which the device will expire.
- **Expires Before** – select the date before which the device will expire.

You can also select the following **Additional search criteria**:

- **Valid After** – select the date after which the device became valid.
- **Valid Before** – select the date before which the device became valid.
- **Chip** – type the chip type for the device; for example, Oberthur ID-One PIV. You can use wildcards.
- **Device Category** – select the category of device.

  See section *5.3*, *Working with device categories*.

If you are using other searches, the criteria may be different.

4. Click **Search**.

   The list of matching results appears.

   Search results are displayed in pages. Scroll to retrieve the next page of results automatically.

   Note: The results are restricted to devices that have owners who fall within your scope, plus any unassigned devices.

5. Click a record to display the details of the device.

   You can view information on the following tabs:

   - **Details** – view the basic details of the device, including device type, serial number, and owner.
   - **Certificates** – view the list of certificates stored on the device.

     See section *13.1.3*, *Viewing a device's certificates*.
   - **Requests** – view any open requests for the device; for example, reprovision card tasks. You can click on the request in the list to view the full details of the request, and carry out actions such as approving, rejecting, or canceling the request.

     For more information, see section *6*, *Working with requests*.
   - **Device History** – view the audit history for the device.

     See section *5.1.1*, *Viewing a device's history*.
   - **Linked Credentials** – view all the credentials that are stored on the same physical device.

     For example, if you have issued multiple passkeys to the same token, or a PIV credential and a passkey to the same token, and your devices are configured for enterprise attestation so that MyID CMS can use the device serial number to correlate the devices, those related credentials are displayed on this tab.

     See the *Linked credentials* section in the ***Passkey Integration Guide*** for details.

   From this screen, you can:

- Request a replacement device. See section *5.4*, *Requesting a replacement device*.
- Request a replacement mobile device. See section *5.5*, *Requesting a replacement mobile device*.
- Renew a device. See section *5.6*, *Renewing a device*.
- Cancel a device. See section *5.7*, *Canceling a device*.
- Reset the PIN for the device. See section *5.8*, *Resetting a device's PIN*.
- Change the PIN for the device. See section *5.9*, *Changing a device PIN*.
- Carry out an assisted activation. See section *5.10*, *Activating a device*.
- Erase a device. See section *5.11*, *Erasing a device*.
- Unlock a device. See section *5.12*, *Unlocking a device*.
- Send or view an activation code for the device. See section *5.13*, *Sending an authentication code to activate a device*.
- Send or view and unlock code for a device. See section *5.14*, *Sending a code to unlock a device*.
- Collect any updates available for a device. See section *5.15*, *Updating a device*.
- Completely re-encode a card using the **Reprovision Card** workflow in MyID Desktop. See section *5.16*, *Reprovisioning a device*.
- Request an update or full reprovision for a device.

  See section *5.17*, *Requesting an update for a device*.
- Manage access for a VSC using the **Manage VSC Access** and **Unlock VSC Temporary Access** workflows in MyID Desktop. See section *5.18*, *Managing VSCs*.
- Reinstate a device that has been mistakenly canceled using the **Reinstate Card** workflow in MyID Desktop. See section *5.19*, *Reinstating a device*.
- Disposing of a device using the **Card Disposal** workflow in MyID Desktop. See section *5.20*, *Disposing of a device*.
- Printing a mailing document using the **Print Mailing Document** workflow in MyID Desktop. See section *5.21*, *Printing a mailing document*.
- Enable or disable a device. See section *5.22*, *Enabling and disabling devices*.
- View extended device information using the **Identify Device (Administrator)** workflow in MyID Desktop. See section *5.23*, *Viewing extended information about a device*.

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

For example:

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

5.1.1 Viewing a device's history

The **Device History** tab displays the audit for the device.

Note: You must have a role that has access to the View User Audit or View Full Audit feature to view this tab; see section *3.5*, *Roles and groups*. The View User Audit feature is in the People category of the **Edit Roles** workflow, while the View Full Audit feature is in the Reports category, under Audit Reporting.

If you have role permissions to the View Full Audit feature, you can click on an entry in the list to display the View Audit screen. See section *16.1*, *Viewing audit details* for more information. This also provides information, on the **Attribute Changes** tab, about the fields that have changed, as well as their previous and new values.

If the device has been canceled or erased, and you have role permissions to the View Full Audit feature, the MyID Operator Client displays the entire history of the device for all previous owners. However, if the device is currently issued to a person, it displays only the history of the device relating to that person.

For example, if you issue a device to Susan Smith, then erase it and issue it to Janet Jones, then erase it again and issue it to Susan Smith, the history of the device shows only the audit events that occurred during either of the times it was issued to Susan Smith, and does not include any events relating to Janet Jones. If you want to view the audit history for the time the device was issued to Janet Jones, you can use the **History** tab on the View Person screen for Janet Jones (see section *4.1.1*, *Viewing a person's history*) or the Unrestricted Audit Report (see section *7.3.7*, *Unrestricted Audit Report*).

5.1.2 Wildcards

For fields where you can use wildcards, you can use the following:

- `*` for multiple characters.

  For example, `Sa*` matches Sam, Samuel, and Samantha.

- `?` for single characters.

  For example, `Sa?` matches Sam, but not Samuel or Samantha.

  Note: When searching for people, you cannot use `?` for a single-character wildcard if you are searching an LDAP directory. The `?` wildcard is supported only when searching in the MyID database.

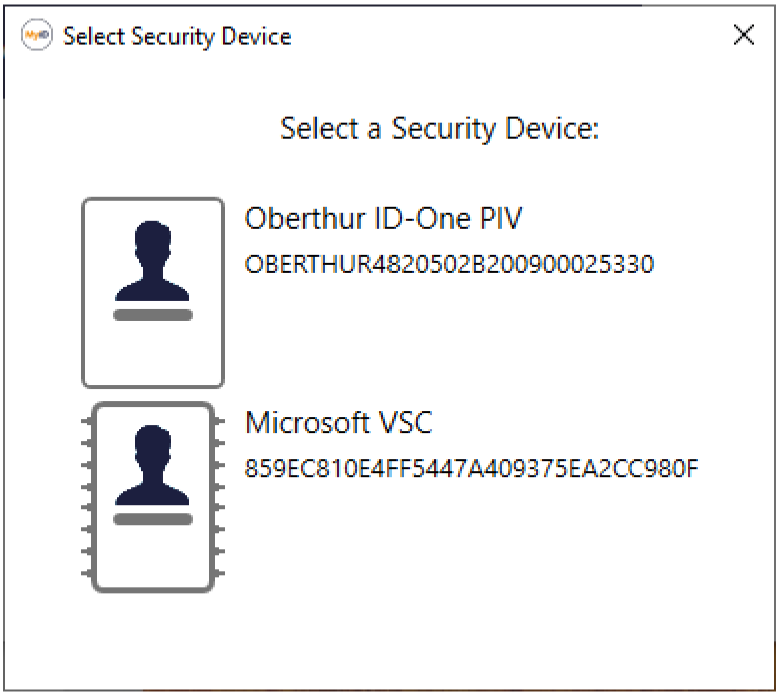
5.2 Reading a device

If you have a device present, you can read it directly instead of searching for it in the MyID database.

To read a device:

1. Click the **Devices** category.
2. Click **Read Card**.

   The Select Security Device dialog appears.



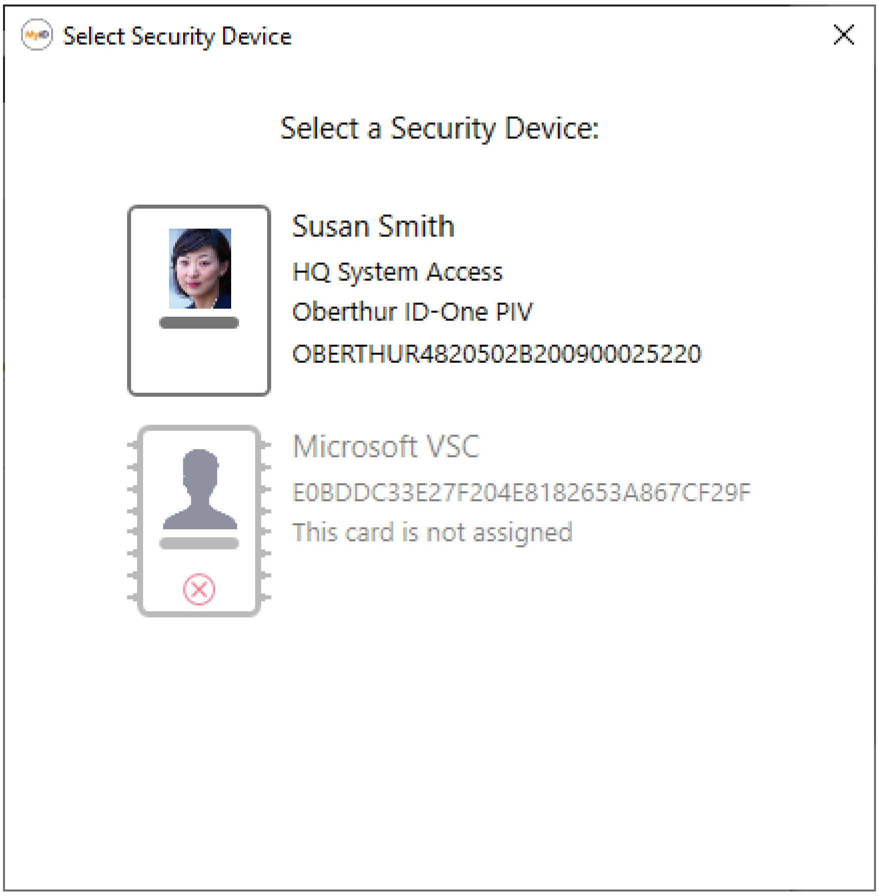
Select a Security Device:

Oberthur ID-One PIV
OBERTHUR4820502B200900025330

Microsoft VSC
859EC810E4FF5447A409375EA2CC980F

If there is a **Device Friendly Name** specified in the credential profile that was used to issue the device, this is displayed next to the smart card.

If you have scope or administrative group permissions that allow you to manage the owner of the device, you can also see the cardholder's user image and full name along with to the device serial number.


Select Security Device
Select a Security Device:
Susan Smith
HQ System Access
Oberthur ID-One PIV
OBERTHUR4820502B200900025220
Microsoft VSC
E0BDDC33E27F204E8182653A867CF29F
This card is not assigned

In addition, you can set the **Show Full Name at Logon** and **Show Photo at Logon** options (on the **Logon** page of the **Security Settings** workflow) to configure this screen to display the associated user image and full name of the cardholder, even if you do not have scope or administrative group permissions that allow you to manage the owner of the device.

Note: If you enable this feature, it is possible to obtain user photos and cardholder names without authentication; the default behavior is to display the user image and full name only for devices where the operator has the appropriate permissions to manage the cardholder's account.

3. Insert the smart card you want to read, or select a VSC that is stored on the PC.

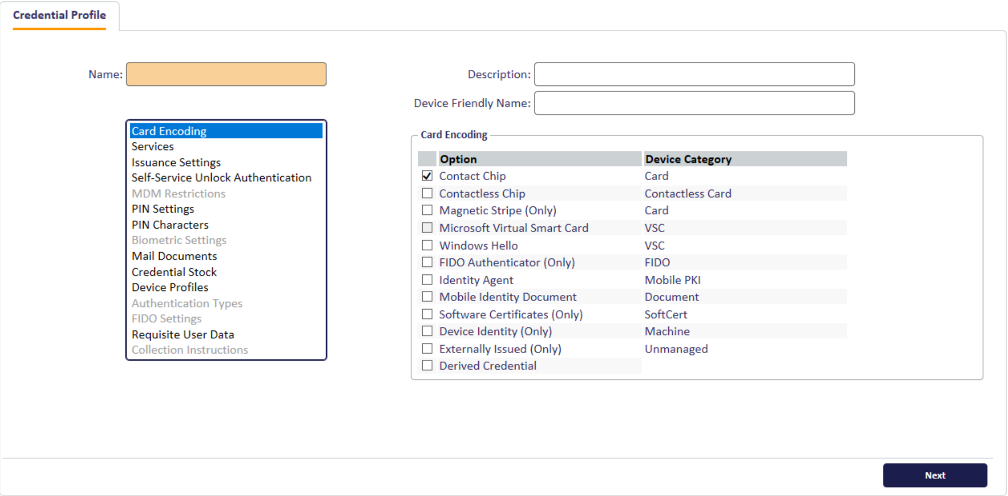
   Note: The device must have been issued by the current MyID system. You cannot read devices issued by other systems.

   The View Device screen appears. See section *5.1*, *Searching for a device* for details of the actions you can carry out on this screen.

5.3 Working with device categories

Each device that you work with in MyID belongs to a device category.

When you select the **Card Encoding** for a credential profile, you specify the category:



Credential Profile
Name:
Description:
Device Friendly Name:
Card Encoding
Services
Issuance Settings
Self-Service Unlock Authentication
MDM Restrictions
PIN Settings
PIN Characters
Biometric Settings
Mail Documents
Credential Stock
Device Profiles
Authentication Types
FIDO Settings
Requisite User Data
Collection Instructions
Next

Card Encoding

	Option	Device Category
☑	Contact Chip	Card
☐	Contactless Chip	Contactless Card
☐	Magnetic Stripe (Only)	Card
☐	Microsoft Virtual Smart Card	VSC
☐	Windows Hello	VSC
☐	FIDO Authenticator (Only)	FIDO
☐	Identity Agent	Mobile PKI
☐	Mobile Identity Document	Document
☐	Software Certificates (Only)	SoftCert
☐	Device Identity (Only)	Machine
☐	Externally Issued (Only)	Unmanaged
☐	Derived Credential	

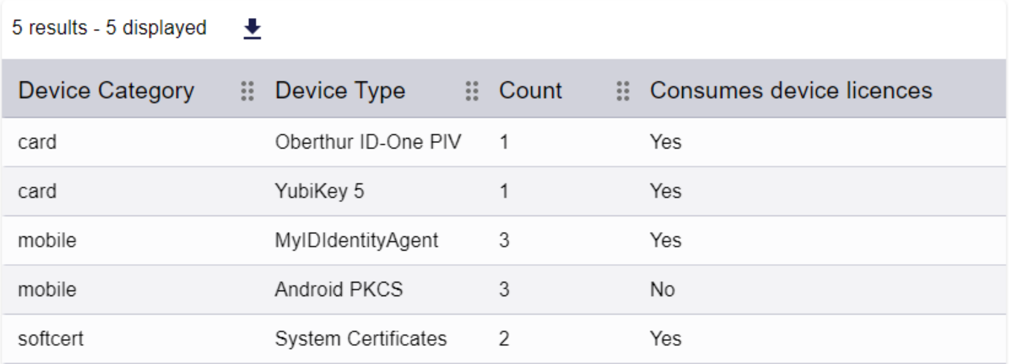
This **Device Category** groups the various card encoding options into logical categories. Note that Derived Credential does not have a category, as a derived credential always has another device type; for example, a VSC derived credential, or a contact card derived credential.

See the *Working with credential profiles* section in the ***Administration Guide*** for details.

The **Device Category** for an individual device is displayed on the View Device screen.

You can use the device category to search for individual devices; most device search reports contain **Device Category** in the **Additional Search Criteria** section.

You can also produce a report that displays the total number of issued devices by device type, including details of their category:



5 results - 5 displayed

Device Category	Device Type	Count	Consumes device licences
card	Oberthur ID-One PIV	1	Yes
card	YubiKey 5	1	Yes
mobile	MyIDIdentityAgent	3	Yes
mobile	Android PKCS	3	No
softcert	System Certificates	2	Yes

See section *7.3.27*, *Issued devices by category report* for details of running this report.

Note: A single mobile device may contain multiple logical devices (in the above example, the three `MyIDIdentityAgent` devices and three `Android PKCS` devices relate to three mobile devices) but only one logical device for each mobile device counts towards the license total; this is shown by the **Consumes device licenses** column.

5.4 Requesting a replacement device

You can request a replacement card for another person.

Note: To request a replacement mobile device for a person, that is, a device using a credential profile where the **Card Encoding** is **Identity Agent**, you must use the **Request Replacement Mobile** or **Request Replacement Mobile (View Auth Code)** options instead. See section *5.5*, *Requesting a replacement mobile device*.

To request a replacement card:

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

   See section *5.1*, *Searching for a device*.

   Alternatively, insert the device into a reader.

   See section *5.2*, *Reading a device*.

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

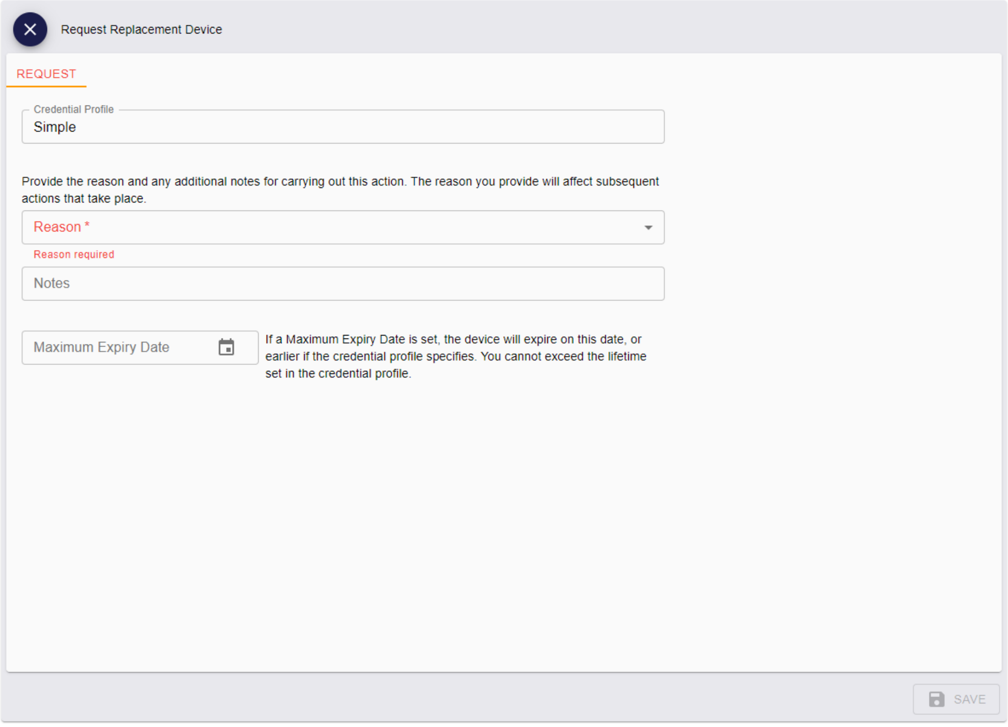
   For example:

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

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

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

   The Request Replacement Device screen appears.



Credential Profile: Simple

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

If a Maximum Expiry Date is set, the device will expire on this date, or earlier if the credential profile specifies. You cannot exceed the lifetime set in the credential profile.

3. The **Credential Profile** for the device being replaced is displayed.

   Note: If you are requesting a temporary replacement device, and there is a corresponding _temp credential profile, this is used automatically for the replacement device. The _temp credential profile is displayed in the resulting request. See the *Temporary replacement credential profiles* section in the ***Operator's Guide*** for details of _temp credential profiles.

4. Select the **Reason** for the replacement from the drop-down list.

   The reason you select determines what happens to your original device and its certificates. including what happens to the recovery of archived certificates. See the *Certificate reasons* section in the ***Operator's Guide*** for details.

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

5. Type any **Notes**.

6. If the **Set expiry date at request** option (on the **Issuance Processes** page of the **Operation Settings** workflow) is set, you can set or amend the **Maximum Expiry Date** for the request. The expiry date cannot exceed the expiry date of the device being replaced. Within this limit, you can select any date up to the `MaxRequestExpiryDate` specified for the person in the Lifecycle API. Note, however, that you cannot exceed the **Lifetime** setting for the credential profile; if the request is made for a credential to expire on a date six months from now, but the credential profile has a lifetime of 30 days, the device will be issued with a lifetime of 30 days.

   The credential profile can override the `MaxRequestExpiryDate` set for the person if the **Ignore User Expiry Date** option on the credential profile is set.

7. Click **Save**.

5.5 Requesting a replacement mobile device

When you request a replacement mobile device, the original device is canceled and its certificates revoked.

To request a replacement mobile device:

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

   See section *5.1*, *Searching for a device*.

   You can use the **Mobile Devices** search to restrict your search to mobile devices only; see section *7.3.16*, *Mobile Devices report*.

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

   For example:

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

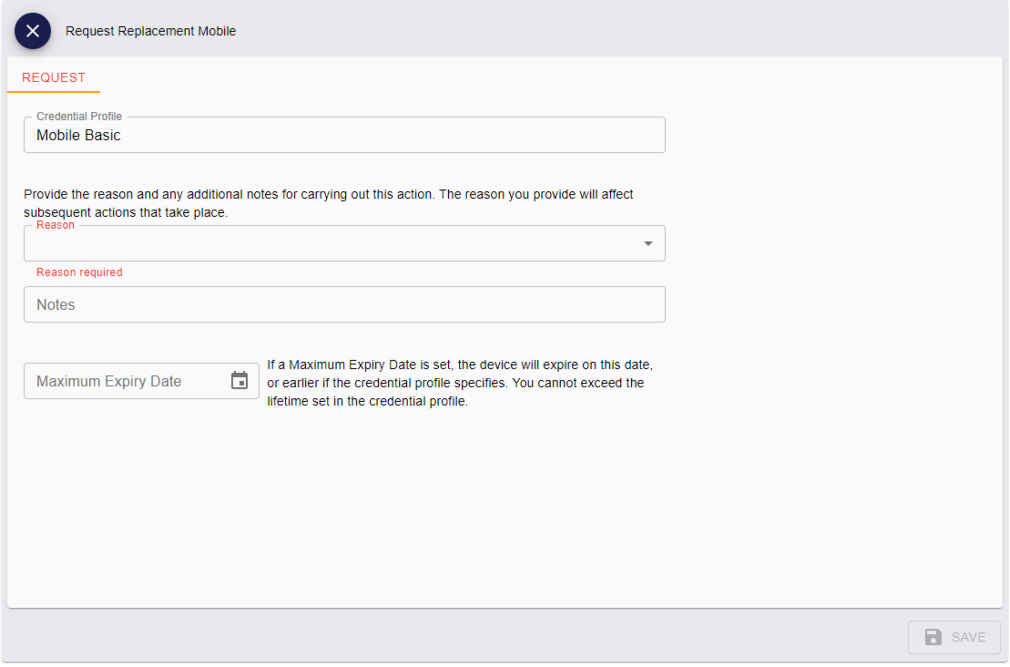
2. Click one of the following options in the button bar at the bottom of the screen:

   - **Request Replacement Mobile** – requests a replacement mobile device for the person.

- **Request Replacement Mobile (View Auth Code)** – requests a replacement mobile device for the person, and displays the collection URL and authentication code for the device on the View Request screen at the end of the process.

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

The Request Replacement Mobile screen appears.



Credential Profile: Mobile Basic

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

Reason

Reason required

Notes

Maximum Expiry Date

If a Maximum Expiry Date is set, the device will expire on this date, or earlier if the credential profile specifies. You cannot exceed the lifetime set in the credential profile.

3. The **Credential Profile** for the device being replaced is displayed.

   You cannot change the credential profile.

4. Select the **Reason** for the replacement from the drop-down list.

   The reason you select determines what happens to your original device and its certificates. including what happens to the recovery of archived certificates. See the *Certificate reasons* section in the ***Operator's Guide*** for details.

5. Type any **Notes**.
6. Optionally, set the **Maximum Expiry Date**.

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

   The maximum expiry date is the requested date on which the device will expire. You can select any date up to the `MaxRequestExpiryDate` specified for the person in the Lifecycle API. Note, however, that you cannot exceed the **Lifetime** setting for the credential profile; if the request is made for a credential to expire on a date six months from now, but the credential profile has a lifetime of 30 days, the device will be issued with a lifetime of 30 days.

   The credential profile can override the `MaxRequestExpiryDate` set for the person if the **Ignore User Expiry Date** option on the credential profile is set.

Note: If the **Expire cards at end of day** configuration option (on the **Issuance Processes** page of the **Operation Settings** workflow) is set to Yes, the requested date will be 23:59 UTC on the date selected. See the *Issuance Processes page (Operation Settings)* section in the ***Administration Guide***.

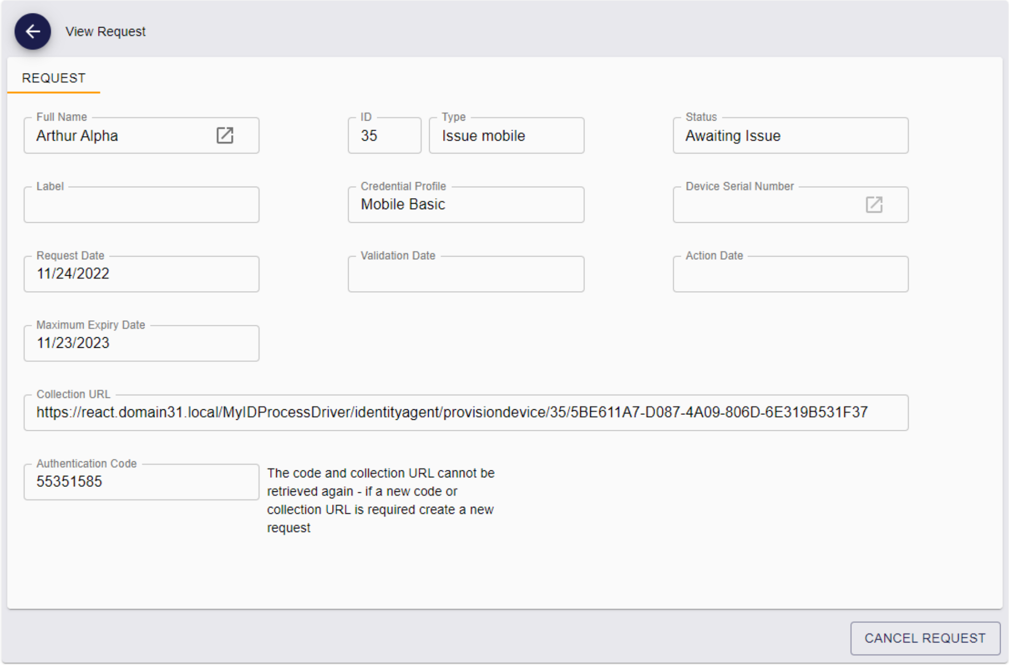
7. Click **Save**.

The old mobile device is canceled, and a request is created for the replacement; once the request is created, the View Request screen appears. From this screen, you can cancel the device request. If the credential profile requires validation, another operator must approve the request; the operator who makes a request cannot validate it. See section *6.2*, *Approving, rejecting, and canceling requests*.

Once the request is ready for collection (after approval, if necessary), MyID sends the collection URL and an authentication code to the person for whom the device was requested; see the *Configuring SMS and email notifications for the MyID Operator Client* section in the ***Mobile Identity Management*** guide for details.

As an alternative to sending the collection URL and authentication code as notifications, you can use the **Request Replacement Mobile (View Auth Code)** option instead; when you use this option, the following additional information is provided on the View Request screen:

- **Collection URL** – The URL that the person must access on their mobile device to collect the mobile device.
- **Authentication Code** – The authentication code that the person must provide to collect the mobile device.



Full Name: Arthur Alpha
ID: 35
Type: Issue mobile
Status: Awaiting Issue
Label:
Credential Profile: Mobile Basic
Device Serial Number:
Request Date: 11/24/2022
Validation Date:
Action Date:
Maximum Expiry Date: 11/23/2023
Collection URL: https://react.domain31.local/MyIDProcessDriver/identityagent/provisiondevice/35/5BE611A7-D087-4A09-806D-6E319B531F37
Authentication Code: 55351585

The code and collection URL cannot be retrieved again - if a new code or collection URL is required create a new request

You can provide these details to the person manually; this is an alternative to using email and SMS notifications to provide this information. If the request requires validation, make sure that the request has been validated before you provide the information to the person; if you use email and SMS notifications, then these are not sent until the request has been validated.

Note: These fields are displayed only once, at the end of the **Request Replacement Mobile (View Auth Code)** operation; if you view the request again, you will not be able to view this information.

5.6 Renewing a device

You can request a renewal for a device that is near its expiry. By default, the renewal window is 42 days; this is configured by the **Card Renewal Period** option on the **Devices** page of the **Operation Settings** workflow. You can renew a card if its expiry date is within this window.

To renew a device:

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

   See section *5.1*, *Searching for a device*.

   Alternatively, insert the device into a reader.

   See section *5.2*, *Reading a device*.

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

   For example:

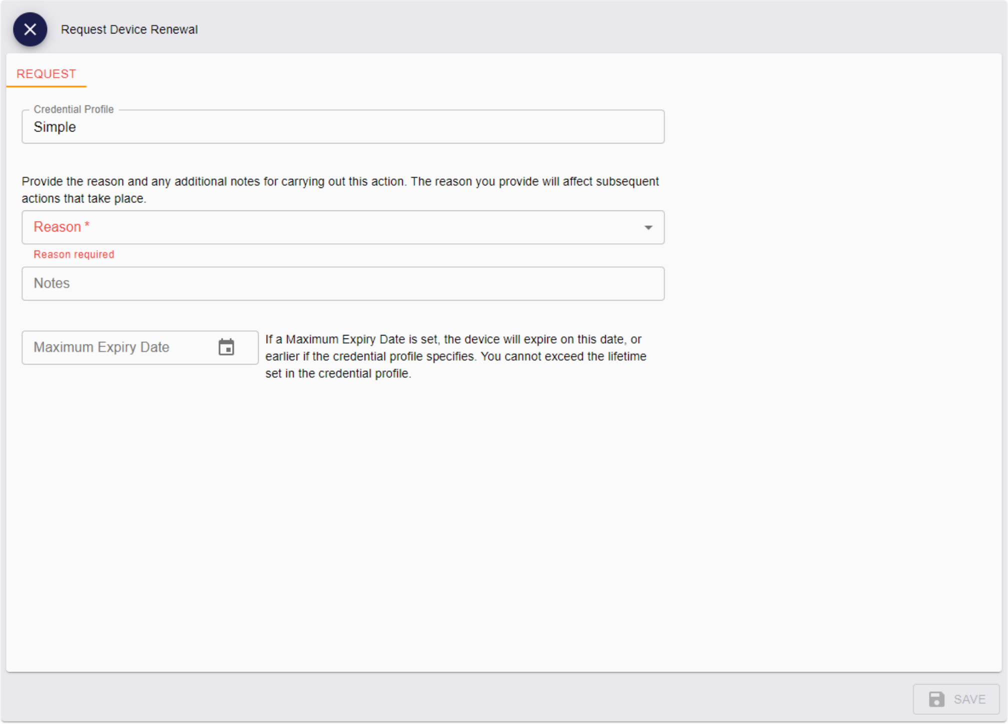
   - Click the item in the list on the **Devices** tab of the View Person form.
   - Click the link icon ↗ on the **Device Serial Number** field of the View Request form.

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

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

   If the device is not within the renewal window, or if you do not have permission to request a device for the selected person, the **Request Device Renewal** button is not available.

   The Request Device Renewal screen appears.



Credential Profile
Simple

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

Reason required

If a Maximum Expiry Date is set, the device will expire on this date, or earlier if the credential profile specifies. You cannot exceed the lifetime set in the credential profile.

3. If the **Set Credential Profile On Renewal** option (on the **Issuance Processes** page of the **Operation Settings** workflow) is set, you can select a different **Credential Profile** from the drop-down list.
4. Select the **Reason** for the replacement from the drop-down list.

   By default, the only option available is **Request device Renewal**.

   The reason determines what happens to your original device and its certificates. including what happens to the recovery of archived certificates. See the *Certificate reasons* section in the ***Operator's Guide*** for details.
5. Type any **Notes**.
6. If the **Set expiry date at request** option (on the **Issuance Processes** page of the **Operation Settings** workflow) is set, you can set or amend the **Maximum Expiry Date** for the request. You can select any date up to the `MaxRequestExpiryDate` specified for the person in the Lifecycle API. Note, however, that you cannot exceed the **Lifetime** setting for the credential profile; if the request is made for a credential to expire on a date six months from now, but the credential profile has a lifetime of 30 days, the device will be issued with a lifetime of 30 days.

   The credential profile can override the `MaxRequestExpiryDate` set for the person if the **Ignore User Expiry Date** option on the credential profile is set.
7. Click **Save**.

For mobile devices, MyID sends notifications to the device owner when the request is awaiting issue; see the *Configuring SMS and email notifications for the MyID Operator Client* section in the ***Mobile Identity Management*** guide for details.

5.7 Canceling a device

You can cancel a device, whether or not it is present. This process does not change the contents of the device itself, but cancels the holder's access to MyID and revokes any certificates, if it contains any.

If you want to remove all content from a device, use the **Erase Card** workflow; see section *5.11*, *Erasing a device*.

Note: You cannot cancel your own device if you used it to authenticate to MyID; either authenticate using a different method or ask another operator to cancel the device.

5.7.1 Canceling a device

To cancel a device:

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

   See section *5.1*, *Searching for a device*.

   Alternatively, insert the device into a reader.

   See section *5.2*, *Reading a device*.

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

   For example:

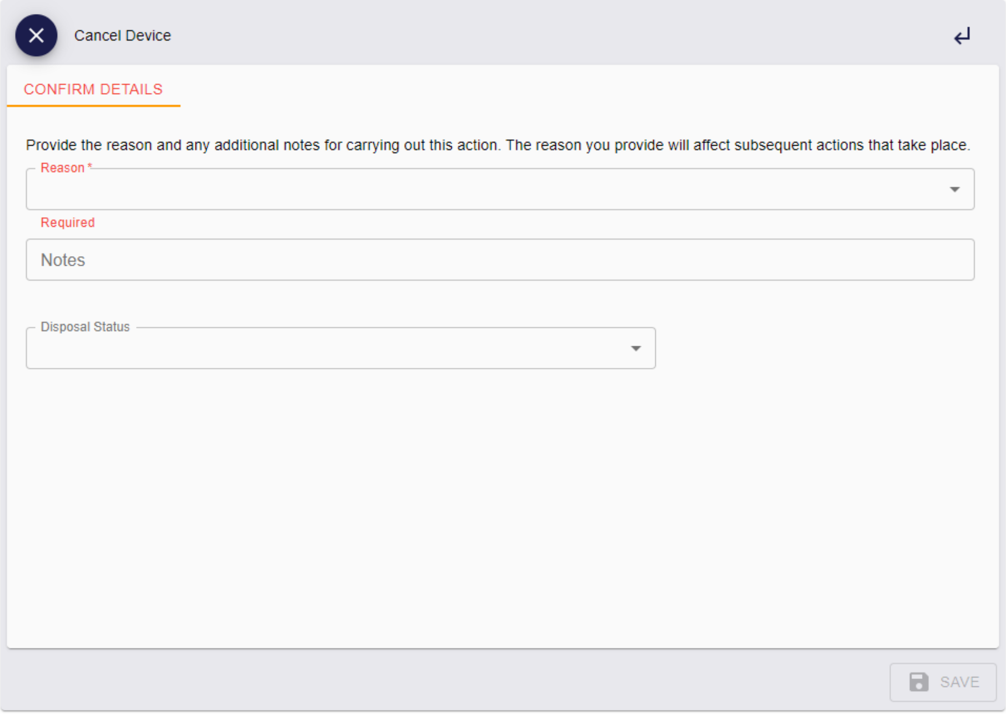
   - Click the item in the list on the **Devices** tab of the View Person form.
   - Click the link icon ↗ on the **Device Serial Number** field of the View Request form.

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

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

   Note: You cannot use this feature to cancel a device that was issued using a credential profile that had the **Validate Cancellation** option selected. Instead, you must use the **Request Cancel** option; see section *5.7.3*, *Requesting a cancellation for a device*.

   The Cancel Device screen appears.



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

3. Select the **Reason** for the cancellation from the drop-down list.

   This reason affects how MyID treats the certificates on the credential.

   See the *Certificate reasons* section in the ***Operator's Guide*** for details of how each reason affects the device's certificates.

4. Type any **Notes** on the cancellation.

   You can provide further information on your reasons for canceling the device. This information is stored in the audit record.

5. Select the **Disposal Status** for the device.

   This creates an audit trail of the date and time of the disposal along with the identity of the operator who disposed of the card.

   Select one of the following statuses:

   - **Collected**
   - **Disposed**
   - **Legacy**
   - **Lost**
   - **None**
   - **Not Collected**

   Note: When you mark a card with the status **Disposed** or **Lost**, MyID prevents it from ever being issued again. If you select any of the other disposal statuses, you *can* issue the card again.

   You can customize your system with additional disposal statuses; for information on the configuration required, contact customer support quoting reference SUP-387.

   See section *5.20*, *Disposing of a device* for more information.

6. Click **Save**.

Note: If you cancel a mobile device, all devices on the same mobile are canceled. For example, if the mobile device contains both a software store and a system store, and you cancel the software store, the system store is also canceled.

5.7.2 Canceling multiple devices

If you want to cancel multiple devices, you can cancel them in a batch instead of canceling them one by one.

Note: You can access the **Tools** menu only if you have a role with the **Tools Menu** option from the **Configuration** section of the **Edit Roles** workflow.

To cancel multiple devices:

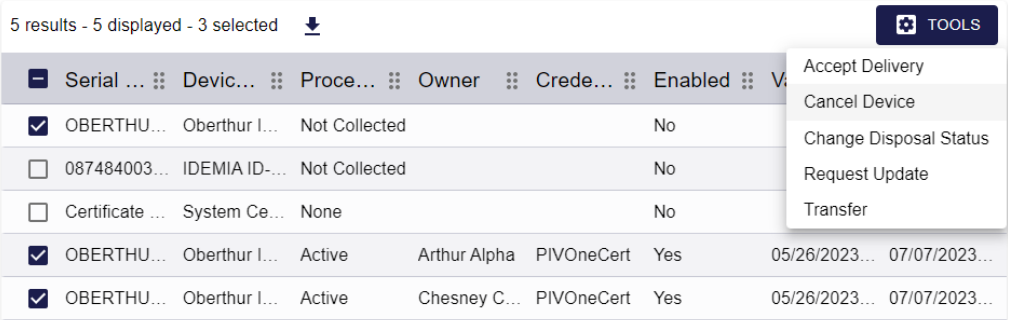
1. Search for the devices you want to cancel.

   See section *5.1*, *Searching for a device*.

2. On the search results page, use the checkboxes to the left of the records to select one or more devices.

   Note: If you select one device, the process is the same as clicking the **Cancel Device** option in the button bar at the bottom of the View Device screen; MyID uses the batch process only if you select more than one device. See section *5.7.1*, *Canceling a device* for details of canceling a single device.

3. From the **Tools** menu, select **Cancel Device**.



5 results - 5 displayed - 3 selected

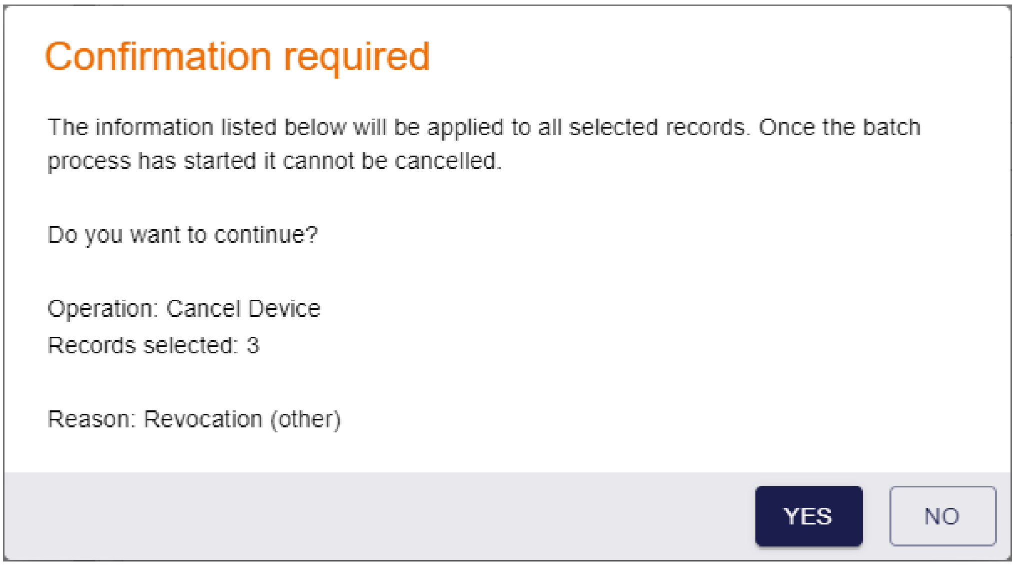
☐	Serial ...	Devic...	Proce...	Owner	Crede...	Enabled	V	
☑	OBERTHU...	Oberthur I...	Not Collected			No		
☐	087484003...	IDEMIA ID-...	Not Collected			No		
☐	Certificate ...	System Ce...	None			No		
☑	OBERTHU...	Oberthur I...	Active	Arthur Alpha	PIVOneCert	Yes	05/26/2023...	07/07/2023...
☑	OBERTHU...	Oberthur I...	Active	Chesney C...	PIVOneCert	Yes	05/26/2023...	07/07/2023...

The Cancel Device screen appears.

Complete the details as for canceling a single device; see section *5.7.1*, *Canceling a device*.

4. Click **Save**.

The confirmation screen appears.



Confirmation required

The information listed below will be applied to all selected records. Once the batch process has started it cannot be cancelled.

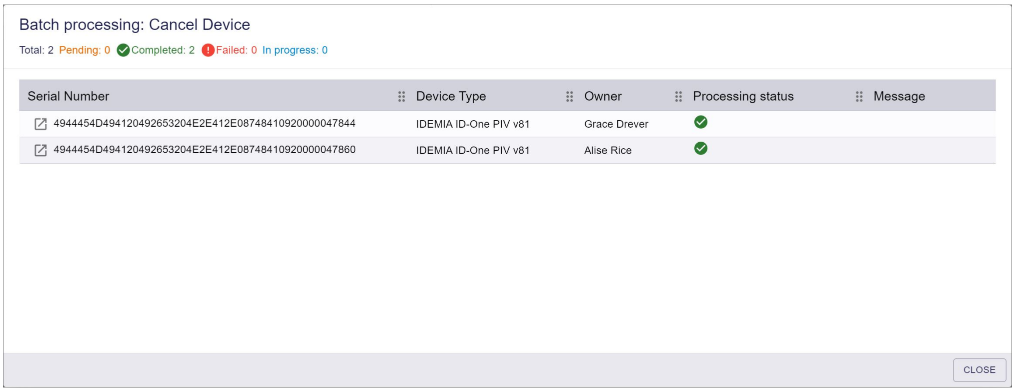
Do you want to continue?

Operation: Cancel Device
Records selected: 3

Reason: Revocation (other)

5. Click **Yes** to proceed with the cancellation, or **No** to go back to the list of devices.

When you click **Yes**, the Batch Processing screen appears.



Batch processing: Cancel Device

Total: 2 Pending: 0 ✓Completed: 2 !Failed: 0 In progress: 0

Serial Number	Device Type	Owner	Processing status	Message
4944454D494120492653204E2E412E08748410920000047844	IDEMIA ID-One PIV v81	Grace Drever	✓	
4944454D494120492653204E2E412E08748410920000047860	IDEMIA ID-One PIV v81	Alise Rice	✓	

6. The cancellations are processed. The table shows the status of each cancellation:

✓	The cancellation succeeded.
❗	The cancellation failed. The Message column displays the reason for the failure; for example, you may have selected a reason (status mapping) that is appropriate only for temporary devices (for example, Found Original) but the device is not a temporary device.

7. Click **Close**.

5.7.3 Requesting a cancellation for a device

If the credential profile used to issue a device had the **Validate Cancellation** option set, you cannot cancel a device directly; you must request the cancellation of the device, and have another operator approve the cancellation.

Note: The device remains active and available for use until the cancellation request is approved. If the request is rejected, no cancellation takes place.

To request the cancellation of a device:

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

   See section *5.1*, *Searching for a device*.

   Alternatively, insert the device into a reader.

   See section *5.2*, *Reading a device*.

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

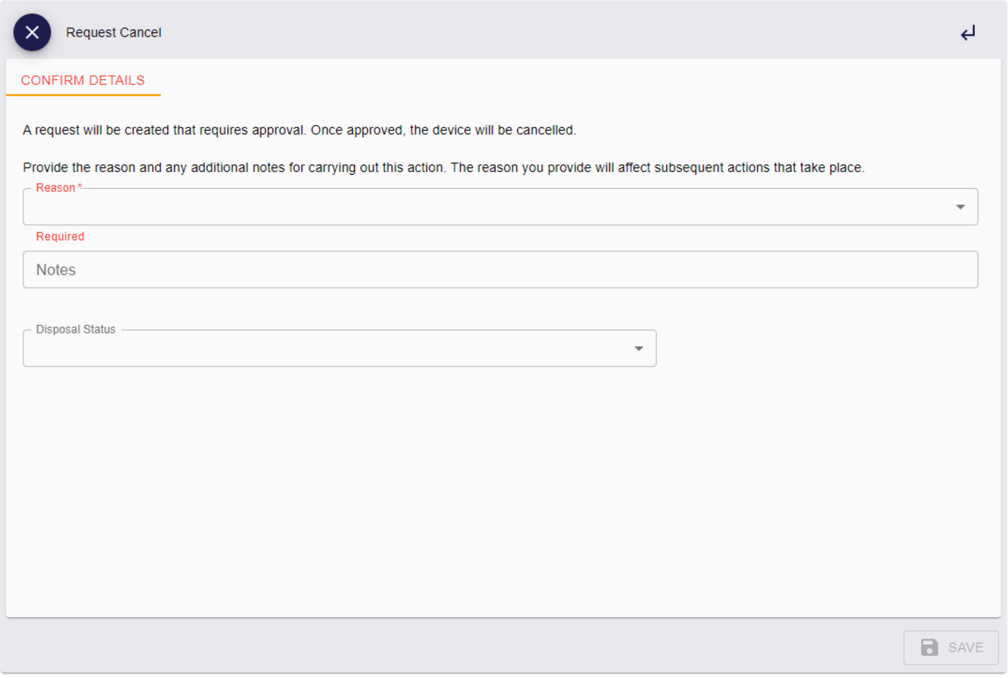
   For example:

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

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

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

   The Request Cancel screen appears.



A request will be created that requires approval. Once approved, the device will be cancelled.

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

3. Select the **Reason** for the cancellation from the drop-down list.

   This reason affects how MyID treats the certificates on the credential.

   See the *Certificate reasons* section in the ***Operator's Guide*** for details of how each reason affects the device's certificates.

4. Type any **Notes** on the cancellation.

   You can provide further information on your reasons for canceling the device. This information is stored in the audit record.

5. Select the **Disposal Status** for the device.

   This creates an audit trail of the date and time of the disposal along with the identity of the operator who disposed of the card.

   Select one of the following statuses:

   - **Collected**
   - **Disposed**
   - **Legacy**
   - **Lost**
   - **None**
   - **Not Collected**

   Note: When you mark a card with the status **Disposed** or **Lost**, MyID prevents it from ever being issued again. If you select any of the other disposal statuses, you *can* issue the card again.

   See section *5.20*, *Disposing of a device* for more information.

6. Click **Save**.

   MyID creates a request for the cancellation. You can view the details of the request, and cancel it if it was created in error, but you cannot approve or reject it yourself; you must ask another operator to approve the request. If necessary, you can send the URL of the View Request screen to the other operator; for example:

   ```
   https://myid.example.com/MyID/OperatorClient/#/requests/1F0859A9-0B33-
   4188-B423-5A5BB2088CFB
   ```

   The other operator can then approve, reject, or cancel the request.

   See section *6.2*, *Approving, rejecting, and canceling requests* for details.

5.8 Resetting a device's PIN

From the View Device screen, you can launch the **Reset Card PIN** workflow in MyID Desktop to reset the PIN of a device.

For more information about using MyID Desktop workflows from within the MyID Operator Client, see section *3.3.2*, *Launching MyID Desktop, Self-Service App, or MyID Client for Windows workflows*.

If the device is not present, you can use the **Unlock Credential** workflow in conjunction with the MyID Card Utility (if supported by the card). See section *5.12*, *Unlocking a device*.

If you know the current PIN, and want to change it, you can use the **Change PIN** workflow instead; see section *5.9*, *Changing a device PIN*.

To reset a device's PIN:

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

   See section *5.1*, *Searching for a device*.

Alternatively, insert the device into a reader.

See section *5.2*, *Reading a device*.

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

For example:

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

2. Click the **Reset PIN** option in the button bar at the bottom of the screen.

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

   The **Reset Card PIN** workflow appears in a MyID Desktop window with the device already selected.

   For information on using the **Reset Card PIN** workflow, see the *Resetting a card's PIN* section in the ***Operator's Guide***.

5.9 Changing a device PIN

From the View Device screen, you can launch the **Change PIN** workflow in MyID Desktop to change the PIN of a device. You must know the current PIN for the device.

If you need to reset the device PIN, see section *5.8*, *Resetting a device's PIN*.

For more information about using MyID Desktop workflows from within the MyID Operator Client, see section *3.3.2*, *Launching MyID Desktop, Self-Service App, or MyID Client for Windows workflows*.

To change a device's PIN:

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

   See section *5.1*, *Searching for a device*.

   Alternatively, insert the device into a reader.

   See section *5.2*, *Reading a device*.

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

   For example:

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

2. Click the **Change PIN** option in the button bar at the bottom of the screen.

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

   The **Change PIN** workflow appears in a MyID Desktop window with the device already selected.

   For information on using the **Change PIN** workflow, see the *Changing a card's PIN* section in the ***Operator's Guide***.

5.10 Activating a device

From the View Device screen, you can launch the **Assisted Activation** workflow in MyID Desktop to carry out an operator-assisted activation of a device.

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

For more information about using MyID Desktop workflows from within the MyID Operator Client, see section *3.3.2*, *Launching MyID Desktop, Self-Service App, or MyID Client for Windows workflows*.

To activate a device:

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

   See section *5.1*, *Searching for a device*.

   Alternatively, insert the device into a reader.

   See section *5.2*, *Reading a device*.

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

   For example:

   - Click the item in the list on the **Devices** tab of the View Person form.
   - Click the link icon ↗ on the **Device Serial Number** field of the View Request form.
2. Click the **Assisted Activation** option in the button bar at the bottom of the screen.

   The option appears only if the selected device requires activation.

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

   The **Assisted Activation** workflow appears in a MyID Desktop window with the device already selected.

   For information on using the **Assisted Activation** workflow, see the *Assisted activation* section in the ***Operator's Guide***.
3. Once you have completed the activation, remove the device from the reader.

   If you leave the device in the reader and try to perform other operations, the MyID Operator Client may report the device as locked.

5.11 Erasing a device

From the View Device screen, you can launch the **Erase Card** workflow in MyID Desktop to erase the content on the selected device.

For more information about using MyID Desktop workflows from within the MyID Operator Client, see section *3.3.2*, *Launching MyID Desktop, Self-Service App, or MyID Client for Windows workflows*.

To erase a device:

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

   See section *5.1*, *Searching for a device*.

   Alternatively, insert the device into a reader.

   See section *5.2*, *Reading a device*.

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

   For example:

   - Click the item in the list on the **Devices** tab of the View Person form.
   - Click the link icon ↗ on the **Device Serial Number** field of the View Request form.
2. Click the **Erase** option in the button bar at the bottom of the screen.

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

   The **Erase Card** workflow appears in a MyID Desktop window.

   See the *Erasing a card* section in the ***Operator's Guide***.

5.12 Unlocking a device

From the View Device screen, you can launch the **Unlock Credential** workflow in MyID Desktop to obtain a code that the cardholder can use to unlock a device PIN. This uses a challenge-response process available to many device types, such as smart cards, USB tokens, virtual smart cards and Mobile credentials issued by MyID

For example, you can use the MyID Card Utility; this is a utility that allows you to carry out a remote unlock or change the PIN on cards that support PIV applets.

For information on using the MyID Card Utility, see the *Remote PIN Management utility for PIV cards* section in the ***Operator's Guide***.

For more information about using MyID Desktop workflows from within the MyID Operator Client, see section *3.3.2*, *Launching MyID Desktop, Self-Service App, or MyID Client for Windows workflows*.

If the card is present, you can use the **Reset PIN** workflow instead; this does not require a challenge-response process. See section *5.8*, *Resetting a device's PIN*.

To obtain an unlock code:

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

   See section *5.1*, *Searching for a device*.

   Alternatively, insert the device into a reader.

   See section *5.2*, *Reading a device*.

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

For example:

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

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

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

   The **Unlock Credential** workflow appears in a MyID Desktop window with the device already selected.

   See the *Unlocking a credential remotely* section in the ***Operator's Guide***.

5.13 Sending an authentication code to activate a device

If the credential profile for a device has been configured for activation, and has the **Activation Authentication** option set to use an authentication code, once the device is ready for activation (that is, the **Status** is **PendingActivation**) you can send an authentication code to the person so they can activate their device.

For information on setting up a credential profile for activation, see the *Activating cards* section in the ***Administration Guide***.

You can send an authentication code to the person through email or as an SMS message to their cell phone.

Alternatively you can allow an operator to view an authentication code on their screen, which they can then read out over the phone or paste into a secure chat channel to allow the person to activate their device.

You can also choose whether to send a short use authentication code for immediate use (which is valid for two minutes by default) or a long use authentication code (which is valid for 30 days by default).

5.13.1 Configuring authentication codes for activation

1. Set the configuration options:
    a. From the **Configuration** category, select **Security Settings**.
    b. On the **Auth Code** tab, set the following:
        - **Auth Code Complexity** – set this to the complexity you want to use for requests where the complexity is not specified 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.
        - **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.
    c. Click **Save changes**.
2. In the **Edit Roles** workflow, make sure the operator has the **Send Auth Code for Activation** or **View Auth Code for Activation** option selected for their role.
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:

    - **Activation 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.
    - **Activation 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. If you disable both email templates, the operator cannot send an authentication code, but may still be able to view an authentication code on screen using the View Auth Code feature.

    Note: The complexity of the code is determined by the **Complexity** option configured in the email template. See the *Changing email messages* section in the ***Administration Guide*** for details. If you are displaying the code on screen instead, the complexity of the code is determined by the **Auth Code Complexity** configuration option.

    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 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:
   1. From the **Configuration** category, select **Operation Settings**.
   2. 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.
   3. Click **Save changes**.

5.13.2 Sending an authentication code for activation

To send an authentication code for activation:

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

   See section *5.1*, *Searching for a device*.

   Alternatively, insert the device into a reader.

   See section *5.2*, *Reading a device*.

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

   For example:

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

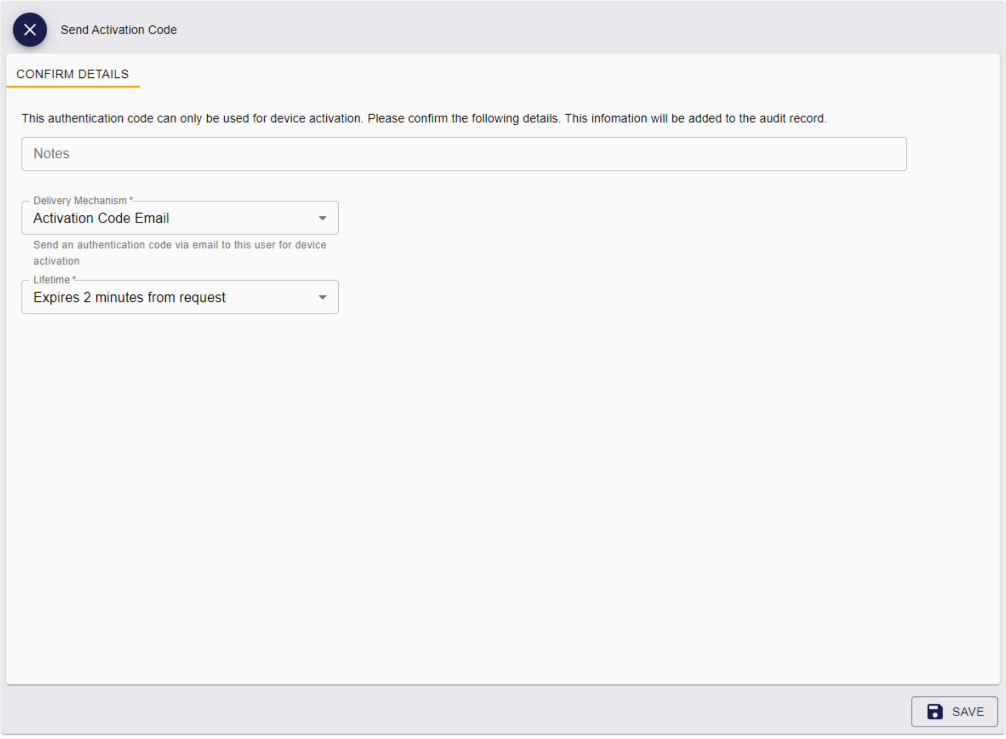
2. Click the **Send Auth Code** option in the button bar at the bottom of the screen.

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

   The **Send Auth Code** option appears only if the device is in a suitable state for activation; that is, it has been issued with a credential profile configured to use authentication codes for activation, and is at a **Status** of **PendingActivation**. You must also make sure that you have the **Send Auth Code for Activation** option selected for your role in the **Edit Roles** workflow.

   Note: The **Send Auth Code** option may also appear if the card has been fully issued; in this case, it sends an unlock code rather than an authentication code. See section *5.14*, *Sending a code to unlock a device* for details.

   The Send Activation Code screen appears.



This authentication code can only be used for device activation. Please confirm the following details. This infomation will be added to the audit record.

Delivery Mechanism *: Activation Code Email

Send an authentication code via email to this user for device activation

Lifetime *: Expires 2 minutes from request

3. Type any **Notes** you want to store in the audit trail about the operation.
4. From the **Delivery Mechanism** drop-down list, select how you want to send the code.

   You can choose from:

   - **Activation Code Email** – sends the code as an email to the person's configured email address. This option is available if the **Activation Code Email** template is enabled in the **Email Templates** workflow.
   - **Activation Code SMS** – sends the code as a text message to the person's configured cell phone number. This option is available if the **Activation Code SMS** template is enabled in the **Email Templates** workflow.

   Note: The complexity of the code is determined by the **Complexity** option configured in the email template. See the *Changing email messages* section in the ***Administration Guide*** for details.
5. From the **Lifetime** drop-down list, select how long you want the code to be valid.

   The options here are determined by the values saved in the **Auth Code Lifetime for Immediate Use** and **Auth Code Lifetime** configuration options; by default, the options are:

   - **Expires 30 days from request** – based on the default **Auth Code Lifetime** setting of 720 hours.
   - **Expires 2 minutes from request** – based on the default **Auth Code Lifetime for Immediate Use** setting of 120 seconds.
6. Click **Save**.

   MyID sends the authentication code to the person, who can then use it to activate their device.

5.13.3 Viewing an authentication code for activation

To view an authentication code for activation on screen:

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

   See section *5.1*, *Searching for a device*.

   Alternatively, insert the device into a reader.

   See section *5.2*, *Reading a device*.

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

   For example:

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

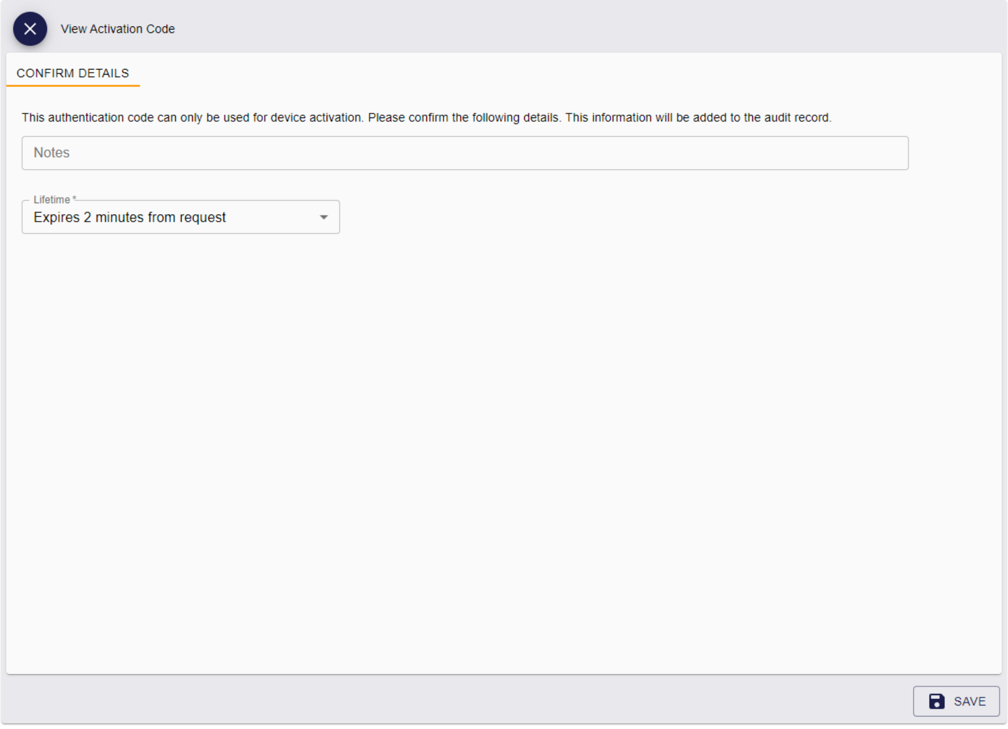
2. Click the **View Auth Code** option in the button bar at the bottom of the screen.

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

   The **View Auth Code** option appears only if the device is in a suitable state for activation; that is, it has been issued with a credential profile configured to use authentication codes for activation, and is at a **Status** of **PendingActivation**. You must also make sure that you have the **View Auth Code for Activation** option selected for your role in the **Edit Roles** workflow.

   Note: The **View Auth Code** option may also appear if the card has been fully issued; in this case, it generates an unlock code rather than an authentication code. See section *5.14*, *Sending a code to unlock a device* for details.

   The View Activation Code screen appears.



This authentication code can only be used for device activation. Please confirm the following details. This information will be added to the audit record.

Lifetime *: Expires 2 minutes from request

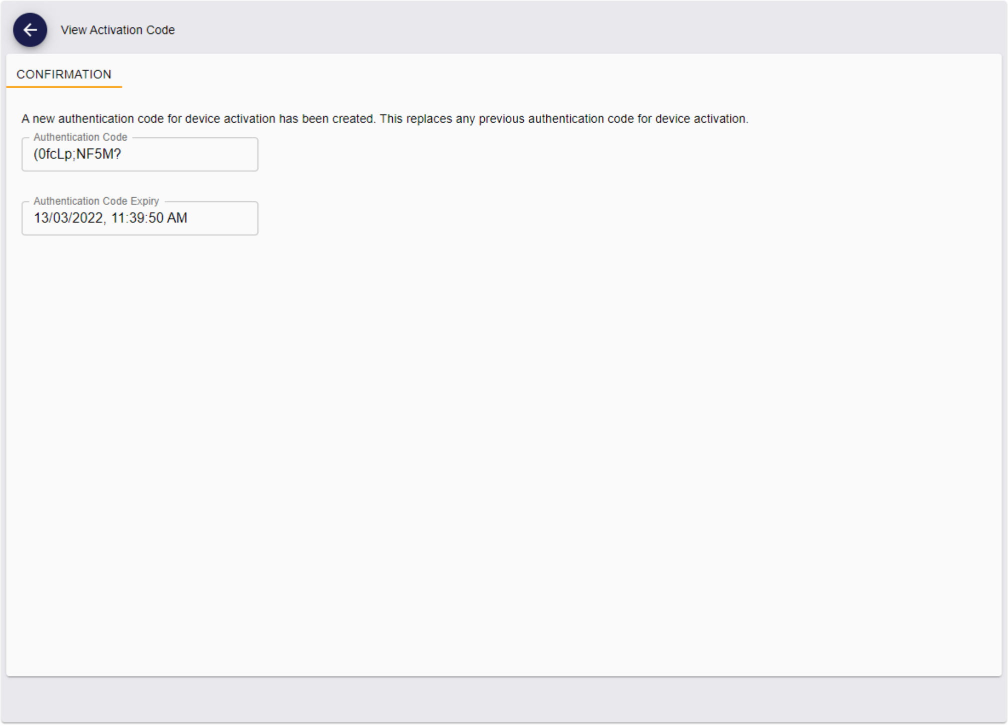
3. Type any **Notes** you want to store in the audit trail about the operation.
4. From the **Lifetime** drop-down list, select how long you want the code to be valid.

   The options here are determined by the values saved in the **Auth Code Lifetime for Immediate Use** and **Auth Code Lifetime** configuration options; by default, the options are:

   - **Expires 30 days from request** – based on the default **Auth Code Lifetime** setting of 720 hours.
   - **Expires 2 minutes from request** – based on the default **Auth Code Lifetime for Immediate Use** setting of 120 seconds.

   Note: The complexity of the code is determined by the **Auth Code Complexity** configuration option.
5. Click **Save**.

   MyID displays the authentication code on screen. You can now provide this to the person who needs to activate their device; for example, you can read the code out over the phone, or send it by a secure chat channel.



A new authentication code for device activation has been created. This replaces any previous authentication code for device activation.

Authentication Code: (0fcLp;NF5M?

Authentication Code Expiry: 13/03/2022, 11:39:50 AM

5.14 Sending a code to unlock a device

If a cardholder has locked their device, you can send an authentication code that can be used for unlocking the device and resetting the PIN.

You can send an unlock code to the person through email or as an SMS message to their cell phone.

Alternatively you can allow an operator to view an unlock code on their screen, which they can then read out over the phone or paste into a secure chat channel to allow the person to unlock their device.

You can also choose whether to send a short use unlock code for immediate use (which is valid for two minutes by default) or a long use unlock code (which is valid for 30 days by default).

The cardholder can provide the authentication code when using the **Reset PIN** option in the Self-Service App or the **I want to reset my PIN** option in the Self-Service Kiosk, or an operator can unlock the device using the **Authentication Code** tab of the **Reset Card PIN** or **Unlock Credential** workflows; see section *5.8*, *Resetting a device's PIN* and section *5.12*, *Unlocking a device*.

5.14.1 Configuring authentication codes for unlocking

1. Set the configuration options:
    a. From the **Configuration** category, select **Security Settings**.
    b. On the **Auth Code** tab, set the following:
        - **Auth Code Complexity** – set this to the complexity you want to use for requests where the complexity is not specified 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.
        - **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.
    c. Click **Save changes**.
2. In the **Edit Roles** workflow, make sure the operator has the **Send Auth Code for PIN Unlock** or **View Auth Code for PIN Unlock** option selected for their role.
3. From the **Configuration** category, select **Email Templates**.

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

    - **Unlock Credential 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.
    - **Unlock Credential 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. If you disable both email templates, the operator cannot send an unlock code, but may still be able to view an unlock code on screen using the View Auth Code feature.

    Note: The complexity of the code is determined by the **Complexity** option configured in the email template. See the *Changing email messages* section in the ***Administration Guide*** for details. If you are displaying the code on screen instead, the complexity of the code is determined by the **Auth Code Complexity** configuration option.

    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 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**.

5.14.2 Sending an unlock code

To send an unlock code for a device:

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

   See section *5.1*, *Searching for a device*.

   Alternatively, insert the device into a reader.

   See section *5.2*, *Reading a device*.

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

   For example:

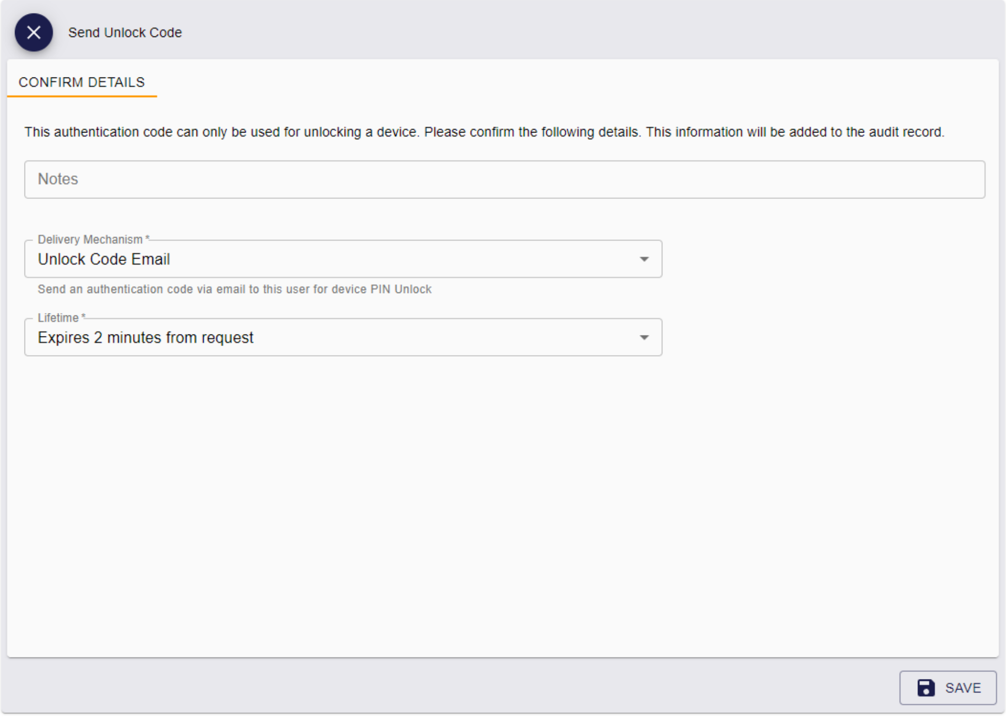
   - Click the item in the list on the **Devices** tab of the View Person form.
   - Click the link icon ↗ on the **Device Serial Number** field of the View Request form.

2. Click the **Send Auth Code** option in the button bar at the bottom of the screen.

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

   The **Send Auth Code** option appears only if the device is in a suitable state for unlocking; it must be active and issued, and a contact card, Identity Agent, or Microsoft VSC. If the device requires activation, this option sends an authentication code instead (see section *5.13*, *Sending an authentication code to activate a device*). You must also make sure that you have the **Send Auth Code for PIN Unlock** option selected for your role in the **Edit Roles** workflow.

   The Send Unlock Code screen appears.



This authentication code can only be used for unlocking a device. Please confirm the following details. This information will be added to the audit record.

Notes

Delivery Mechanism *: Unlock Code Email

Send an authentication code via email to this user for device PIN Unlock

Lifetime *: Expires 2 minutes from request

3. Type any **Notes** you want to store in the audit trail about the operation.

4. From the **Delivery Mechanism** drop-down list, select how you want to send the code.

   You can choose from:

   - **Unlock Code Email** – sends the code as an email to the person's configured email address. This option is available if the **Unlock Credential Code Email** template is enabled in the **Email Templates** workflow.
   - **Unlock Code SMS** – sends the code as a text message to the person's configured cell phone number. This option is available if the **Unlock Credential Code SMS** template is enabled in the **Email Templates** workflow.

   Note: The complexity of the code is determined by the **Complexity** option configured in the email template. See the *Changing email messages* section in the ***Administration Guide*** for details.

5. From the **Lifetime** drop-down list, select how long you want the code to be valid.

   The options here are determined by the values saved in the **Auth Code Lifetime for Immediate Use** and **Auth Code Lifetime** configuration options; by default, the options are:

   - **Expires 30 days from request** – based on the default **Auth Code Lifetime** setting of 720 hours.
   - **Expires 2 minutes from request** – based on the default **Auth Code Lifetime for Immediate Use** setting of 120 seconds.

6. Click **Save**.

   MyID sends the authentication code to the person, who can then use it to reset their device PIN, either using the **Reset PIN** option in the Self-Service App or the **I want to reset my PIN** option in the Self-Service Kiosk, or with the assistance of an operator using the **Reset Card PIN** or **Unlock Credential** workflow; see section *5.8*, *Resetting a device's PIN* and section *5.12*, *Unlocking a device*.

5.14.3 Viewing an unlock code

To view an unlock code for a device:

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

   See section *5.1*, *Searching for a device*.

   Alternatively, insert the device into a reader.

   See section *5.2*, *Reading a device*.

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

   For example:

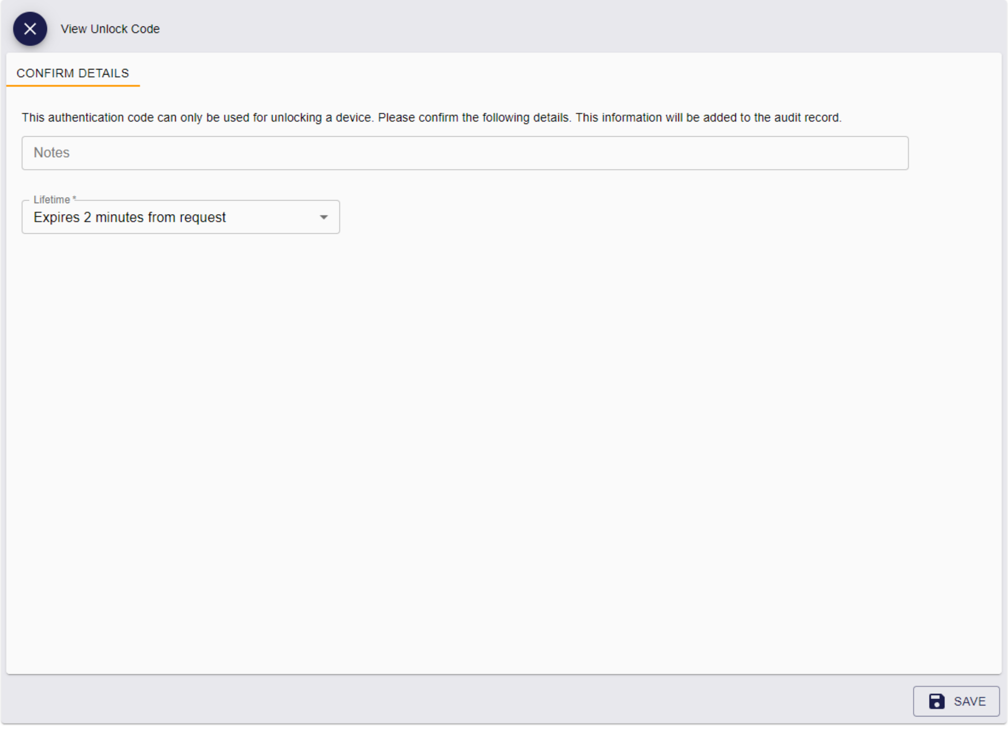
   - Click the item in the list on the **Devices** tab of the View Person form.
   - Click the link icon ↗ on the **Device Serial Number** field of the View Request form.

2. Click the **View Auth Code** option in the button bar at the bottom of the screen.

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

   The **View Auth Code** option appears only if the device is in a suitable state for unlocking; it must be active and issued, and a contact card, Identity Agent, or Microsoft VSC. If the device requires activation, this option sends an authentication code instead (see section *5.13*, *Sending an authentication code to activate a device*). You must also make sure that you have the **View Auth Code for PIN Unlock** option selected for your role in the **Edit Roles** workflow.

   The View Unlock Code screen appears.



This authentication code can only be used for unlocking a device. Please confirm the following details. This information will be added to the audit record.

Lifetime *: Expires 2 minutes from request

3. Type any **Notes** you want to store in the audit trail about the operation.

4. From the **Lifetime** drop-down list, select how long you want the code to be valid.

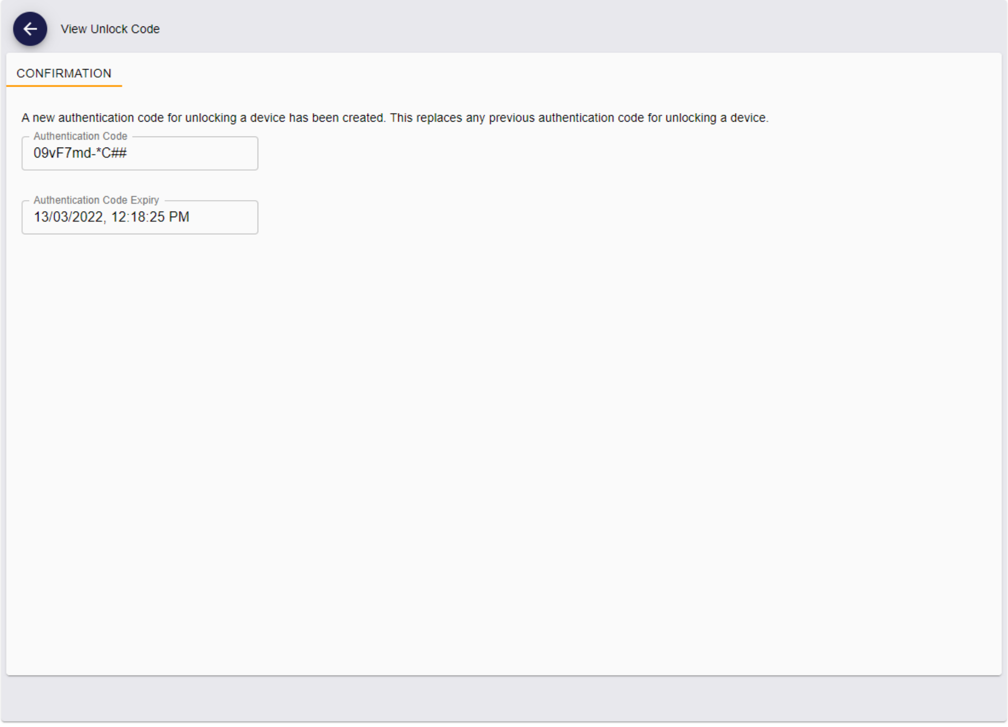
   The options here are determined by the values saved in the **Auth Code Lifetime for Immediate Use** and **Auth Code Lifetime** configuration options; by default, the options are:

   - **Expires 30 days from request** – based on the default **Auth Code Lifetime** setting of 720 hours.
   - **Expires 2 minutes from request** – based on the default **Auth Code Lifetime for Immediate Use** setting of 120 seconds.

   Note: The complexity of the code is determined by the **Auth Code Complexity** configuration option.

5. Click **Save**.

   MyID displays the unlock code on screen. You can now provide this to the person who needs to unlock their device; for example, you can read the code out over the phone, or send it by a secure chat channel.



A new authentication code for unlocking a device has been created. This replaces any previous authentication code for unlocking a device.

Authentication Code: 09vF7md-*C##

Authentication Code Expiry: 13/03/2022, 12:18:25 PM

   The person can then use it to reset their device PIN, either using the **Reset PIN** option in the Self-Service App or the **I want to reset my PIN** option in the Self-Service Kiosk, or with the assistance of an operator using the **Reset Card PIN** or **Unlock Credential** workflow; see section *5.8*, *Resetting a device's PIN* and section *5.12*, *Unlocking a device*.

5.15 Updating a device

From the View Device screen, you can:

- Check for updates for your own device, and launch the **Collect My Updates** feature in the Self-Service App to carry out the updates on your device.
- Check for updates for another person's device, and launch the **Collect Updates** workflow in MyID Desktop to carry out the updates for the device.

For more information about using MyID Desktop and Self-Service App workflows from within the MyID Operator Client, see section *3.3.2*, *Launching MyID Desktop, Self-Service App, or MyID Client for Windows workflows*.

You can request updates for a device using the **Request Update** option on the View Device screen. See section *5.17*, *Requesting an update for a device*.

5.15.1 Collecting updates for your own device

To check for updates to your own device:

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

   See section *5.1*, *Searching for a device*.

   Alternatively, insert your device into a reader.

   See section *5.2*, *Reading a device*.

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

   For example:

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

2. Click the **Collect Updates** option in the button bar at the bottom of the screen.

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

   The MyID Operator Client checks whether there are any update jobs available. If no jobs are available, it displays the message:

   ```
   OA10059: There are no update jobs to collect for this device
   ```

   If there is an update job available for the device, the **Collect My Updates** feature appears in a Self-Service App window with the device update task already selected.

   See the *Self-Service App features* section in the ***Self-Service App*** guide.

5.15.2 Collecting updates for another person's device

To check for updates to another person's device:

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

   See section *5.1*, *Searching for a device*.

   Alternatively, insert the device into a reader.

   See section *5.2*, *Reading a device*.

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

   For example:

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

2. Click the **Collect Updates** option in the button bar at the bottom of the screen.

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

   The MyID Operator Client checks whether there are any update jobs available. If no jobs are available, it displays the message:

   ```
   OA10059: There are no update jobs to collect for this device
   ```

   If there is an update job available for the device, the **Collect Updates** workflow appears in a MyID Desktop window with the device already selected.

   See the *Collect Updates workflow* section in the ***Operator's Guide***.

5.16 Reprovisioning a device

From the View Device screen, you can launch the **Reprovision Card** workflow in MyID Desktop to re-encode a another person's device completely, based on the data in the MyID database, using the latest version of the credential profile used during issuance.

For more information about using MyID Desktop workflows from within the MyID Operator Client, see section *3.3.2*, *Launching MyID Desktop, Self-Service App, or MyID Client for Windows workflows*.

To reprovision a device:

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

   See section *5.1*, *Searching for a device*.

   Alternatively, insert the device into a reader.

   See section *5.2*, *Reading a device*.

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

   For example:

   - Click the item in the list on the **Devices** tab of the View Person form.
   - Click the link icon ↗ on the **Device Serial Number** field of the View Request form.
2. Click the **Reprovision** option in the button bar at the bottom of the screen.

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

   If the **Reprovision** option does not appear, the device may not be suitable for reprovision; for example, you cannot carry out a reprovision on your own device.

   The **Reprovision Card** workflow appears in a MyID Desktop window with the card already selected. If you have not already done so, insert the device you want to reprovision; you cannot select a different device within the workflow. Further checks on the device are carried out in the workflow.

   See the *Reprovisioning cards* section in the ***Operator's Guide***.

5.17 Requesting an update for a device

You can request an update for a device, either to update the device to the latest version of the credential profile used to issue it, or to reprovision it completely, using either the same credential profile or a different credential profile.

You can requests updates for issued contact smart cards, VSCs, mobile devices, and Windows Hello devices. You cannot request updates for your own device.

Note: If you want to request an update for a mobile identity document, the options you can select on the Request Update screen are restricted. See the *Updating mobile identity documents* section in the ***Mobile Identity Documents*** guide for details.

5.17.1 Requesting an update

To request an update for a device:

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

   See section *5.1*, *Searching for a device*.

   Alternatively, insert the device into a reader.

See section *5.2*, *Reading a device*.

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

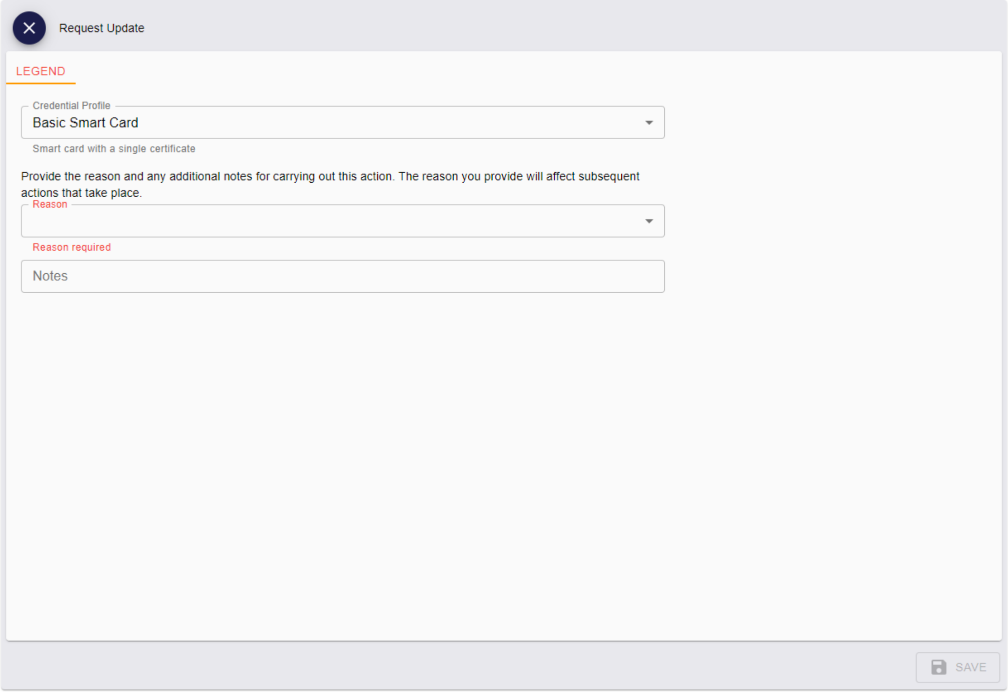
For example:

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

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

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

   The Request Update screen appears:



Credential Profile
Basic Smart Card
Smart card with a single certificate

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

3. From the **Credential Profile** drop-down list, select the credential profile you want to use.

   The list defaults to the credential profile used to issue the device. You can update the device to the latest version of the credential profile, or re-issue the device using a different credential profile.

   Note: If you are using the current credential profile, you must have the **Can Collect** permission set up in the credential profile. If you are using a different credential profile, you must have the **Can Request** permission set up in the credential profile.

   Make sure you select a credential profile that matches the capabilities of the device you want to update; for example, if your device is a contact smart card, you cannot update to a credential profile that is both contact and contactless.

4. From the **Reason** drop-down list, select one of the following options:

   - **Reprovision all content on the device** – this option erases and then writes the device content, re-encoding the device completely.

- **Apply latest updates** – this option updates the device to the latest version of the specified credential profile; for example, you can add new certificates to an existing device using this option.

5. Type any **Notes** on the request.

   You can provide further information on your reasons for requesting an update for the device. This information is stored in the audit record.

6. Click **Save**.

Note: Creating a request cancels any previous requests of the same type; that is, creating an update request cancels any previous update requests, and creating a reprovision request cancels any previous reprovision requests.

If you have selected the same credential profile for an update, you do not need to approve the request, even if the credential profile has the **Validate Issuance** option set. However, if you change the credential profile to one that has the **Validate Issuance** option set, you must approve the request before you can collect it. See section *6.2*, *Approving, rejecting, and canceling requests*.

You can collect the updates (both simple updates and reprovisions) using the **Collect Updates** option on the View Device screen. See section *5.15*, *Updating a device*.

For mobile devices, MyID sends notifications to the device owner when the request is awaiting issue; see the *Configuring SMS and email notifications for the MyID Operator Client* section in the ***Mobile Identity Management*** guide for details.

5.17.2 Requesting updates for multiple devices

If you want to request updates for multiple devices, you can request the updates in a batch instead of requesting them one by one.

Note: You can access the **Tools** menu only if you have a role with the **Tools Menu** option from the **Configuration** section of the **Edit Roles** workflow.

To request updates for multiple devices:

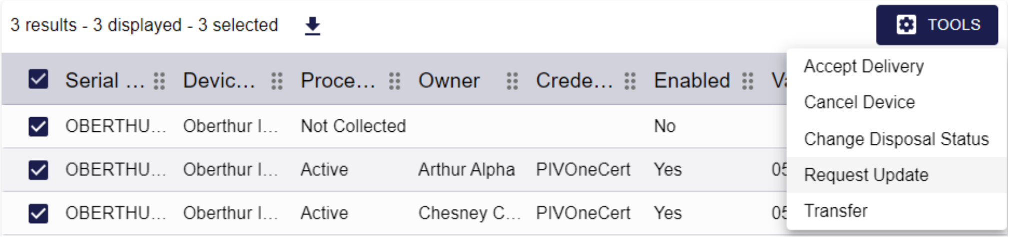
1. Search for the devices you want to update.

   See section *5.1*, *Searching for a device*.

2. On the search results page, use the checkboxes to the left of the records to select one or more devices.

   Note: If you select one device, the process is the same as clicking the **Request Update** option in the button bar at the bottom of the View Device screen; MyID uses the batch process only if you select more than one device. See section *5.17.1*, *Requesting an update* for details of requesting an update for a single device.

3. From the **Tools** menu, select **Request Update**.



3 results - 3 displayed - 3 selected

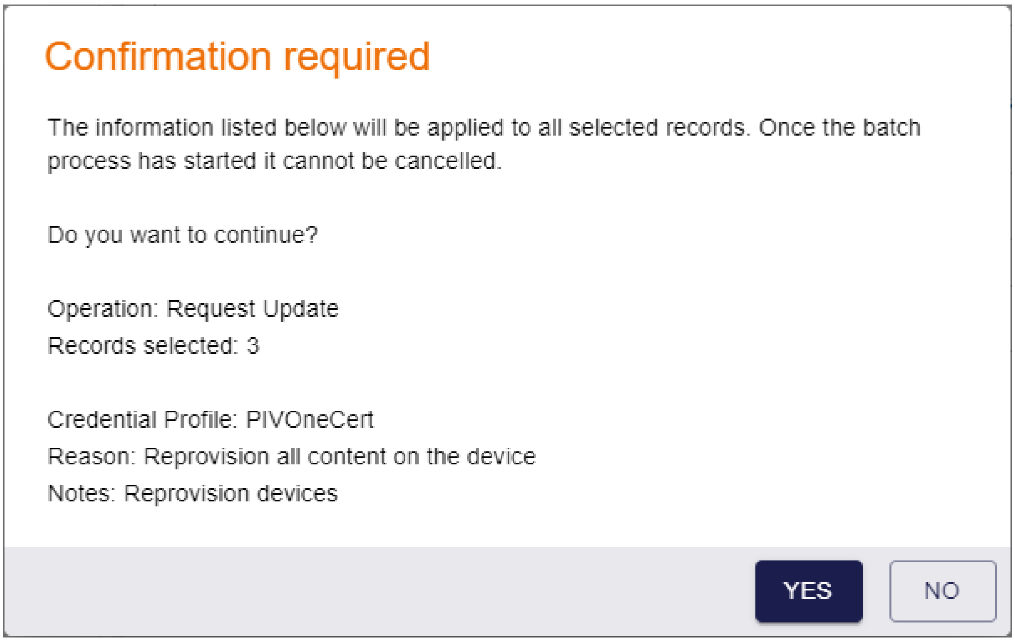
☑	Serial ...	Devic...	Proce...	Owner	Crede...	Enabled	V
☑	OBERTHU...	Oberthur I...	Not Collected			No	
☑	OBERTHU...	Oberthur I...	Active	Arthur Alpha	PIVOneCert	Yes	05
☑	OBERTHU...	Oberthur I...	Active	Chesney C...	PIVOneCert	Yes	05

The Request Update screen appears.

Complete the details as for requesting an update for a single device; see section *5.17.1*, *Requesting an update*.

4. Click **Save**.

   The confirmation screen appears.



Confirmation required

The information listed below will be applied to all selected records. Once the batch process has started it cannot be cancelled.

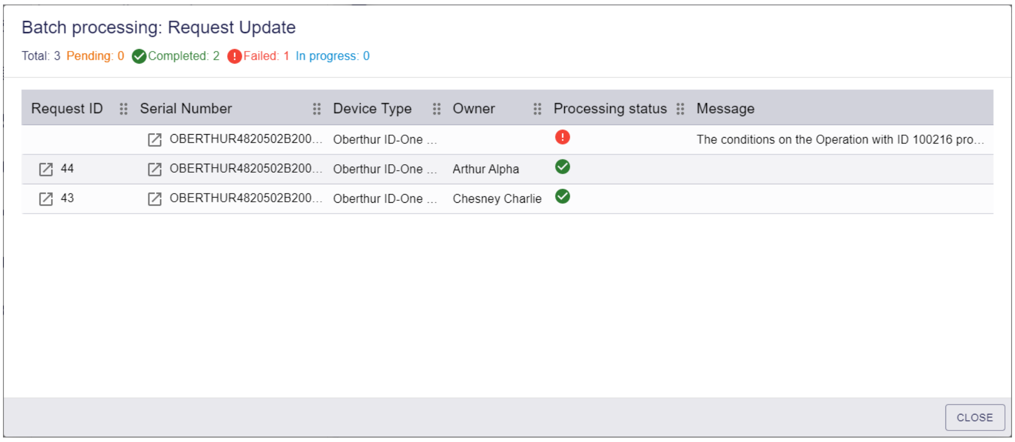
Do you want to continue?

Operation: Request Update
Records selected: 3

Credential Profile: PIVOneCert
Reason: Reprovision all content on the device
Notes: Reprovision devices

5. Click **Yes** to proceed with the request, or **No** to go back to the list of devices.

   When you click **Yes**, the Batch Processing screen appears.



Batch processing: Request Update

Total: 3 Pending: 0 ✓Completed: 2 !Failed: 1 In progress: 0

Request ID	Serial Number	Device Type	Owner	Processing status	Message
	OBERTHUR4820502B200...	Oberthur ID-One ...		!	The conditions on the Operation with ID 100216 pro...
44	OBERTHUR4820502B200...	Oberthur ID-One ...	Arthur Alpha	✓	
43	OBERTHUR4820502B200...	Oberthur ID-One ...	Chesney Charlie	✓	

6. The requests are processed. The table shows the status of each request:

✓	The request succeeded.
!	The request failed. The Message column displays the reason for the failure; for example, the device may not be in the correct state to be updated.

7. Click **Close**.

5.18 Managing VSCs

If you view a VSC on the View Device screen, you can launch the **Manage VSC Access** or **Unlock VSC Temporary Access** workflows to manage access to the VSCs. The **Manage VSC Access** workflow allows you to request, update, and cancel VSC locks; the **Unlock VSC Temporary Access** workflow allows you to provide time-limited VSC access.

For more information about using MyID Desktop and Self-Service App workflows from within the MyID Operator Client, see section *3.3.2*, *Launching MyID Desktop, Self-Service App, or MyID Client for Windows workflows*.

5.18.1 Requesting, updating, and canceling VSC locks

To request, update, or cancel a VSC lock:

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

   See section *5.1*, *Searching for a device*.

   From the **Device Type** drop-down list, select **Microsoft VSC**.

   Alternatively, read the VSC from the current PC.

   See section *5.2*, *Reading a device*.

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

   For example:

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

2. Click the **Manage VSC Access** option in the button bar at the bottom of the screen.

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

   If the **Manage VSC Access** option does not appear, the device may not be suitable for reprovision; for example, it may not be a VSC.

   The **Manage VSC Access** workflow appears in a MyID Desktop window with the VSC already selected.

   See the *Managing VSC access* section in the ***Microsoft VSC Integration Guide***.

5.18.2 Providing time-limited VSC access

To provide temporary access to a VSC:

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

   See section 5.1, *Searching for a device*.

   From the **Device Type** drop-down list, select **Microsoft VSC**.

   Alternatively, read the VSC from the current PC.

   See section 5.2, *Reading a device*.

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

   For example:

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

2. Click the **Unlock VSC Temporary Access** option in the button bar at the bottom of the screen.

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

   If the **Unlock VSC Temporary Access** option does not appear, the device may not be suitable for reprovision; for example, it may not be a VSC.

   The **Unlock VSC Temporary Access** workflow appears in a MyID Desktop window with the VSC already selected.

   See the *Providing time-limited VSC access* section in the ***Microsoft VSC Integration Guide***.

5.19 Reinstating a device

From the View Device screen, you can use the **Reinstate** option to reissue a canceled or erased smart card to its original user. This may be useful if you cancel a device that does not need to be canceled; for example, if a cardholder reports their device as missing, then subsequently finds it before the replacement device has been issued.

When you reinstate a device, MyID creates a request for a new device, linked to the original device's serial number; you must collect this request onto the original device. You must carry out the same issuance process as defined in the credential profile; for example, the credential profile may require activation, or require authentication codes.

If there is a request for a replacement device that has not yet been collected, this request is canceled automatically. If a replacement device has already been collected, you cannot reinstate the original.

You cannot reinstate a device if:

- The device is not a smart card.

  You cannot reinstate VSCs or mobile devices, for example.
- The device has been assigned to a different person.

  If Person A had a device, it was erased, then assigned to Person B, you can no longer reinstate the card for Person A, even if it is subsequently erased and no longer assigned to Person B.
- The device has been disposed of.

  See section *5.20*, *Disposing of a device* for details of setting the disposal status of a device.
- The original device expiry date has passed.
- A replacement for the original device has been collected.
- The cardholder or operator no longer has permissions to receive or request the credential profile.
- The cardholder no longer has any user data required by the credential profile.

Note: This feature is more flexible than the **Reinstate Card** workflow in MyID Desktop, as it does not require the credential profile to be configured for activation, and works with any smart card, not just PIV cards. For more information about the **Reinstate Card** workflow, see the *Reinstating cards* section in the ***Operator's Guide***.

To reinstate a device:

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

   See section *5.1*, *Searching for a device*.

   Use the **Devices** search report, rather than the default **Assigned Devices** search report, which does not return any canceled or erased devices.

   Alternatively, insert the device into a reader.

   See section *5.2*, *Reading a device*.

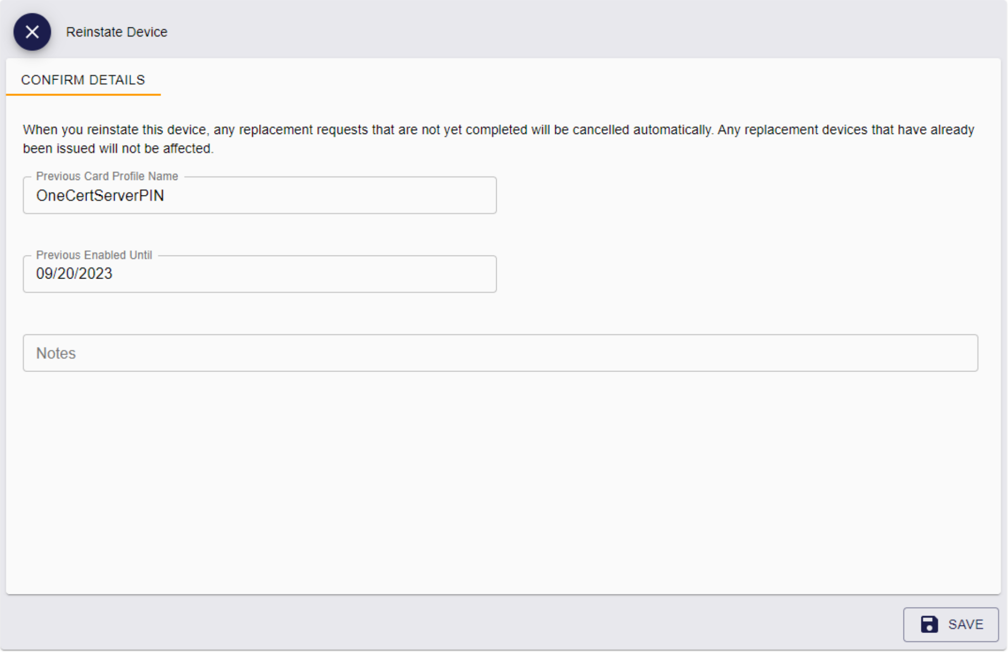
   You can also view the device by selecting an item from the list in the **Previous Devices** tab of the View Person screen. This lists each device that the person has previous been issued, unless the device has subsequently been assigned to a different person.

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

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

   If the **Reinstate** option does not appear, the device may not be suitable for being reinstated; for example, it may not be in a canceled state.

   The Reinstate Device screen appears.



When you reinstate this device, any replacement requests that are not yet completed will be cancelled automatically. Any replacement devices that have already been issued will not be affected.

Previous Card Profile Name: OneCertServerPIN

Previous Enabled Until: 09/20/2023

   This screen displays the **Previous Card Profile Name** and **Previous Enabled Until** values for the device; you cannot change these values, and they are used for the reinstated device.

3. Type any **Notes** on the operation.

   You can provide further information on your reasons for reinstating the device. This information is stored in the audit record.

4. Click **Save**.

   MyID creates a request for the device, assigned to the previous owner, with the same expiry date. You can now collect this request using the issuance process defined in the credential profile.

   Note: If the original issuance process required 2-step activation using an authentication code that was sent automatically, MyID does not send another authentication code automatically when you reinstate the device; instead, you must request an authentication code manually to complete the activation.

5.20 Disposing of a device

From the View Device screen, you can mark a card as disposed within MyID. This creates an audit trail of the date and time of the disposal along with the identity of the operator who disposed of the card. When you cancel a device and disassociate it from its user, you can set the disposal status; see section *5.7*, *Canceling a device*.

You can use the Change Disposal Status option to change the disposal status of a canceled device. In addition, if the card has expired, and the **Allow disposal of expired devices** configuration option is set to **Yes**, you can set the disposal status of the device without canceling it.

Note: You can also use the **Erase Card** workflow to set the disposal status of cards. See section *5.11*, *Erasing a device*.

5.20.1 Setting the disposal status of a device

To set the disposal status of a device:

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

   See section *5.1*, *Searching for a device*.

   Alternatively, insert the device into a reader.

   See section *5.2*, *Reading a device*.

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

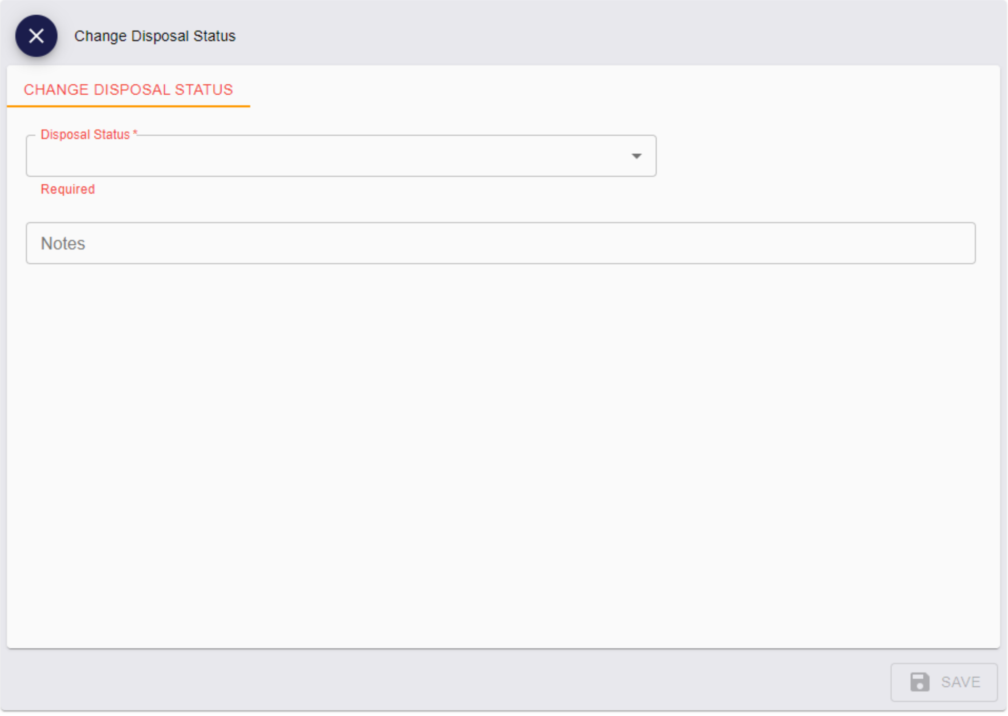
   For example:

   - Click the item in the list on the **Devices** tab of the View Person form.
   - Click the link icon ↗ on the **Device Serial Number** field of the View Request form.
2. Click the **Change Disposal Status** option in the button bar at the bottom of the screen.

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

   If the **Change Disposal Status** option does not appear, the device may not be suitable for being disposed; for example, it may not be in a canceled state.

   The Change Disposal Status screen appears.



3. Select the **Disposal Status** for the device.

   This creates an audit trail of the date and time of the disposal along with the identity of the operator who disposed of the card.

   Select one of the following statuses:

   - **Collected**
   - **Disposed**

- **Legacy**
- **Lost**
- **None**
- **Not Collected**

Note: When you mark a card with the status **Disposed** or **Lost**, MyID prevents it from ever being issued again. If you select any of the other disposal statuses, you *can* issue the card again.

You can customize your system with additional disposal statuses; for information on the configuration required, contact customer support quoting reference SUP-387.

4. Type any **Notes** about the reason you are disposing of the card.
5. Click **Save**.

5.20.2 Setting the disposal status of multiple devices

If you want to set the disposal status of multiple devices, you can set the disposal status in a batch instead of setting the status one by one.

Note: You can access the **Tools** menu only if you have a role with the **Tools Menu** option from the **Configuration** section of the **Edit Roles** workflow.

To set the disposal status of multiple devices:

1. Search for the devices for which you want to set the disposal status.

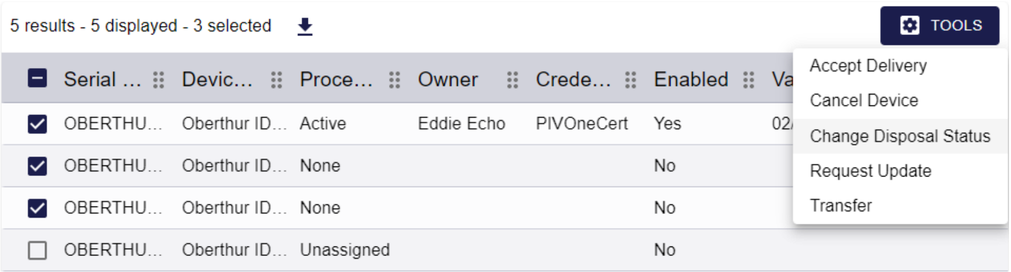
   See section *5.1*, *Searching for a device*.

   You can use the **Device Disposal** search to find devices with a particular disposal status or revocation reason.

2. On the search results page, use the checkboxes to the left of the records to select one or more devices.

   Note: If you select one device, the process is the same as clicking the **Change Disposal Status** option in the button bar at the bottom of the View Device screen; MyID uses the batch process only if you select more than one device. See section *5.20.1*, *Setting the disposal status of a device* for details of setting the disposal status of a single device.

3. From the **Tools** menu, select **Change Disposal Status**.



5 results - 5 displayed - 3 selected

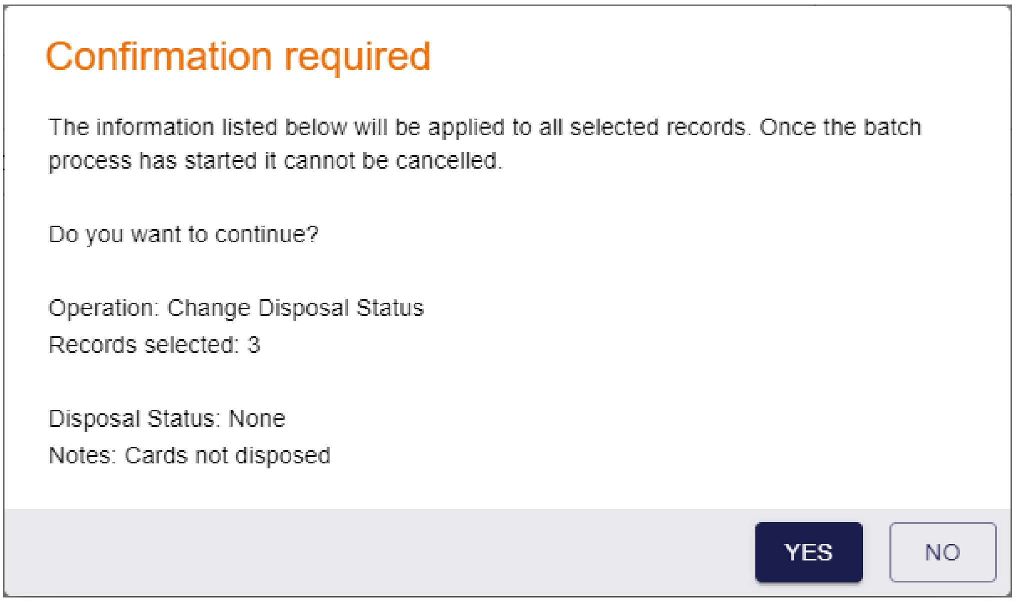
	Serial ...	Devic...	Proce...	Owner	Crede...	Enabled	Va
☑	OBERTHU...	Oberthur ID...	Active	Eddie Echo	PIVOneCert	Yes	02
☑	OBERTHU...	Oberthur ID...	None			No	
☑	OBERTHU...	Oberthur ID...	None			No	
☐	OBERTHU...	Oberthur ID...	Unassigned			No	

   The Change Disposal Status screen appears.

   Complete the details as for setting the disposal status of a single device; see section *5.20.1*, *Setting the disposal status of a device*.

4. Click **Save**.

   The confirmation screen appears.



Confirmation required

The information listed below will be applied to all selected records. Once the batch process has started it cannot be cancelled.

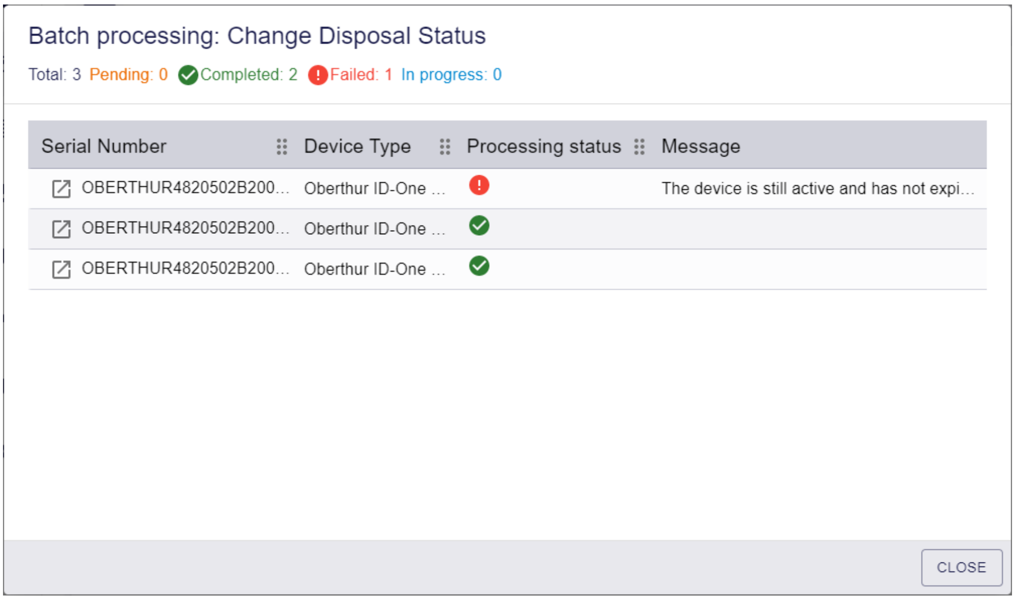
Do you want to continue?

Operation: Change Disposal Status
Records selected: 3

Disposal Status: None
Notes: Cards not disposed

5. Click **Yes** to proceed with the disposal, or **No** to go back to the list of devices.

   When you click **Yes**, the Batch Processing screen appears.



Batch processing: Change Disposal Status

Total: 3 Pending: 0 ✓Completed: 2 !Failed: 1 In progress: 0

Serial Number	Device Type	Processing status	Message
OBERTHUR4820502B200...	Oberthur ID-One ...	!	The device is still active and has not expi...
OBERTHUR4820502B200...	Oberthur ID-One ...	✓	
OBERTHUR4820502B200...	Oberthur ID-One ...	✓	

6. The disposals are processed. The table shows the status of each disposal:

✓	The disposal succeeded.
!	The disposal failed. The Message column displays the reason for the failure; for example, you may have selected a device that is still active and has not yet been canceled.

7. Click **Close**.

5.21 Printing a mailing document

From the View Device screen, you can launch the **Print Mailing Document** workflow in MyID Desktop to print the mail merge document associated with a card.

For more information about using MyID Desktop and Self-Service App workflows from within the MyID Operator Client, see section *3.3.2*, *Launching MyID Desktop, Self-Service App, or MyID Client for Windows workflows*.

To print a mailing document:

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

   See section *5.1*, *Searching for a device*.

   Alternatively, insert the device into a reader.

   See section *5.2*, *Reading a device*.

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

   For example:

   - Click the item in the list on the **Devices** tab of the View Person form.
   - Click the link icon ↗ on the **Device Serial Number** field of the View Request form.
2. Click the **Print Mailing Document** option in the button bar at the bottom of the screen.

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

   The **Print Mailing Document** workflow appears in a MyID Desktop window with the device already selected. If you have not already done so, insert the device you want to print; you cannot select a different device within the workflow.

   See the *Printing mailing documents* section in the ***Operator's Guide***.

5.22 Enabling and disabling devices

You can enable or disable an issued device. When you disable a device, the device is disabled in the MyID database so that it cannot be used to authenticate to MyID, and its certificates are suspended, if any are issued on the device.

Note: If you enable or disable a mobile device, all devices on the same mobile are affected. For example, if the mobile device contains both a software store and a system store, and you disable the software store, the system store is also disabled.

5.22.1 Disabling a device

To disable a device:

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

   See section *5.1*, *Searching for a device*.

   Alternatively, insert the device into a reader.

   See section *5.2*, *Reading a device*.

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

   For example:

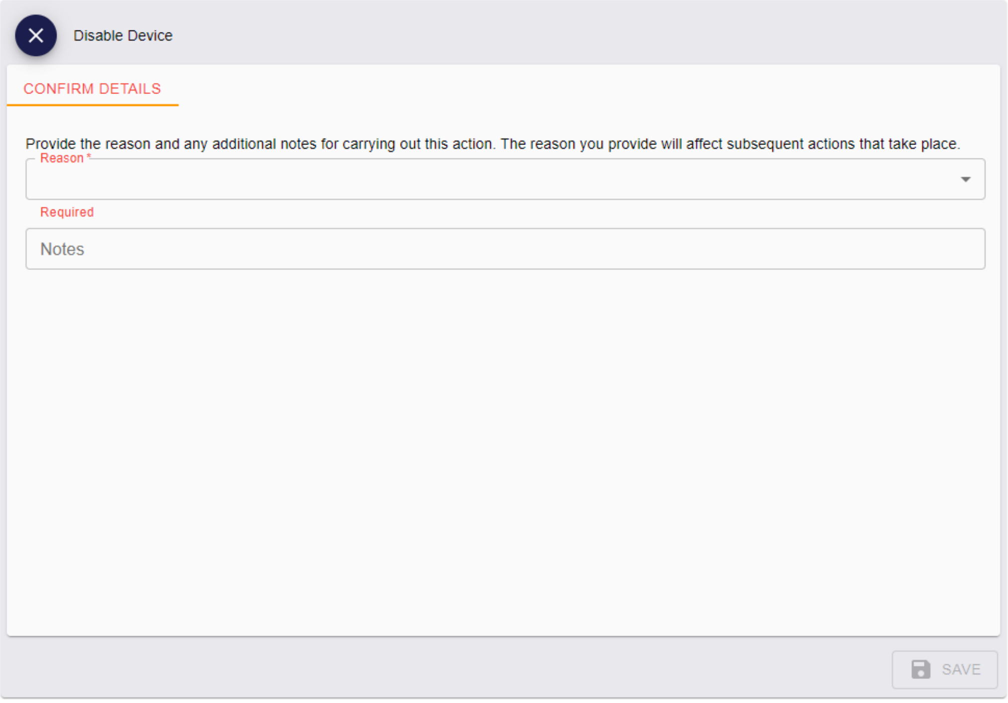
   - Click the item in the list on the **Devices** tab of the View Person form.
   - Click the link icon ↗ on the **Device Serial Number** field of the View Request form.

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

   The option appears only if the selected device is fully issued and currently enabled.

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

   The Disable Device screen appears.

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

3. Select the **Reason** for disabling the device from the drop-down list.

   This reason affects how MyID treats the certificates on the credential.

   See the *Certificate reasons* section in the ***Operator's Guide*** for details of how each reason affects the device's certificates.

4. Type any **Notes** on the operation.

   You can provide further information on your reasons for disabling the device. This information is stored in the audit record.

5. Click **Save**.

5.22.2 Enabling a device

If you have previously disabled a device, you can re-enable it. The device is re-enabled in the MyID database so that it can be used to sign on to MyID again, and any suspended certificated are re-enabled.

To enable a device:

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

   See section *5.1*, *Searching for a device*.

   Alternatively, insert the device into a reader.

   See section *5.2*, *Reading a device*.

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

   For example:

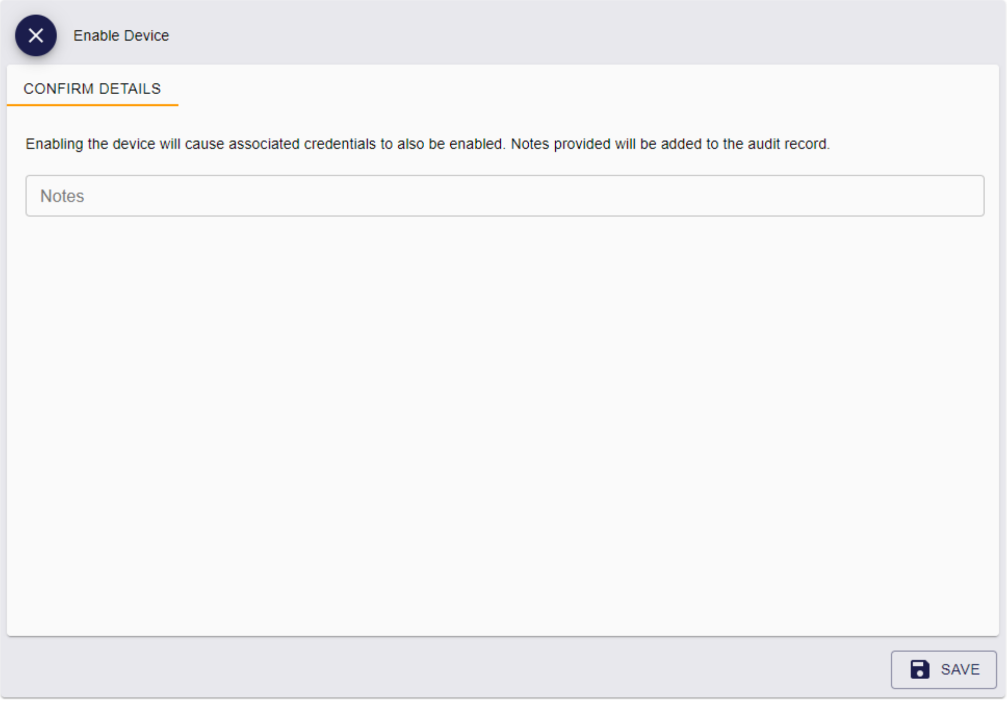
   - Click the item in the list on the **Devices** tab of the View Person form.
   - Click the link icon ↗ on the **Device Serial Number** field of the View Request form.

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

   The option appears only if the selected device is currently disabled.

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

   The Enable Device screen appears.



Enabling the device will cause associated credentials to also be enabled. Notes provided will be added to the audit record.

3. Type any **Notes** on the operation.

   You can provide further information on your reasons for enabling the device. This information is stored in the audit record.

4. Click **Save**.

5.23 Viewing extended information about a device

The View Device screen displays information about the selected device; the **Identify Device (Administrator)** workflow in MyID Desktop provides additional information about the device, including the initial server-generated PIN, if available.

You can also view the server-generated PIN on the View Device screen in the MyID Operator Client; see section *5.28*, *Viewing the initial PIN for a device*.

For more information about using MyID Desktop and Self-Service App workflows from within the MyID Operator Client, see section *3.3.2*, *Launching MyID Desktop, Self-Service App, or MyID Client for Windows workflows*.

To view extended device information:

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

   See section *5.1*, *Searching for a device*.

   Alternatively, insert the device into a reader.

   See section *5.2*, *Reading a device*.

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

   For example:

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

2. Click the **Identify Device (Administrator)** option in the button bar at the bottom of the screen.

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

   Note: The **Identify Device (Administrator)** option is available only if the device has been issued.

   The **Identify Device (Administrator)** workflow appears in a MyID Desktop window with the device already selected. If you have not already done so, insert the device you want to print; you cannot select a different device within the workflow.

   See the *Using the Identify Device (Administrator) workflow* section in the ***Operator's Guide***.

5.24 Importing a range of devices

You can import a range of devices by specifying the format of the serial numbers you want to import; for example, you may have taken receipt of a box of devices with sequential serial numbers.

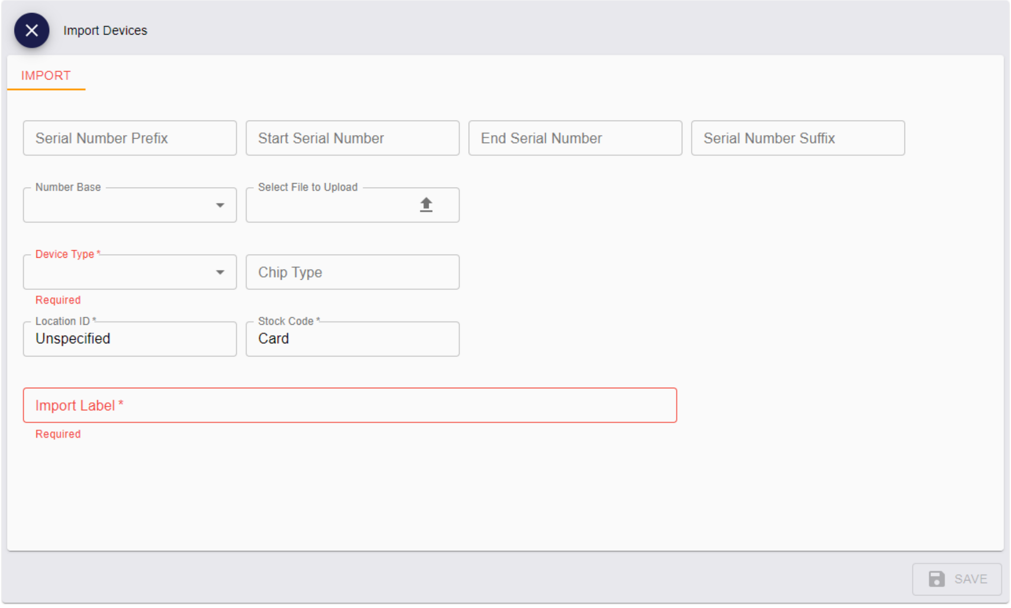
Note: By default, you can import a maximum of 10,000 devices at one time. To change this limit, in the **Operation Settings** workflow, on the **Import & Export** tab, set the **Import Devices Sequential Range Limit** option to the number of devices you want to be able to import at one time.

Alternatively, you can import a manifest file; see section *5.25*, *Importing devices from a manifest file*.

To import a range of devices:

1. Select the **Devices** category.
2. Click **Import**.

   The Import Devices screen appears.


Import Devices
IMPORT
Serial Number Prefix
Start Serial Number
End Serial Number
Serial Number Suffix
Number Base
Select File to Upload
Device Type *
Required
Chip Type
Import Label *
Required
SAVE

Location ID *: Unspecified

Stock Code *: Card

3. Complete the following fields:
    - **Serial Number Prefix** – provide the prefix for the serial number.
    - **Start Serial Number** – provide the first serial number to be imported. This is the numeric (either decimal or hexadecimal) part of the serial number that changes for each device.
    - **End Serial Number** – provide the last serial number to be imported.
    - **Serial Number Suffix** – provide the suffix for the serial number.
    - **Number Base** – select whether the serial numbers are in decimal or hexadecimal format.
    - **Device Type** – select the type of device from the drop-down list.
    - **Chip Type** – optionally, provide the chip type for the device; for example, `IDEMIA ID-One PIV v81`.
    - **Location ID** – select the initial location for the devices from the drop-down list.

      See section *9*, *Working with locations*.
    - **Stock Code** – select the stock code for the devices.

      See section *8.2*, *Editing inventory lists* for details of setting up the list of stock codes.
    - **Import Label** – type a label to be associated with the imported devices. You can use this in the Available Device Stock search criteria to find these devices; see section *5.26*, *Viewing imported devices*.
4. Click **Save**.

5.24.1 Example serial number import

If you provide the following:

- **Serial Number Prefix** – `ABC`
- **Start Serial Number** – `100100`
- **End Serial Number** – `100200`
- **Serial Number Suffix** – `XYZ`
- **Number Base** – **Dec (0-9)**

MyID imports the following range of serial numbers:

```
ABC100100XYZ

ABC100101XYZ

ABC100102XYZ

...

ABC100199XYZ

ABC100200XYZ
```

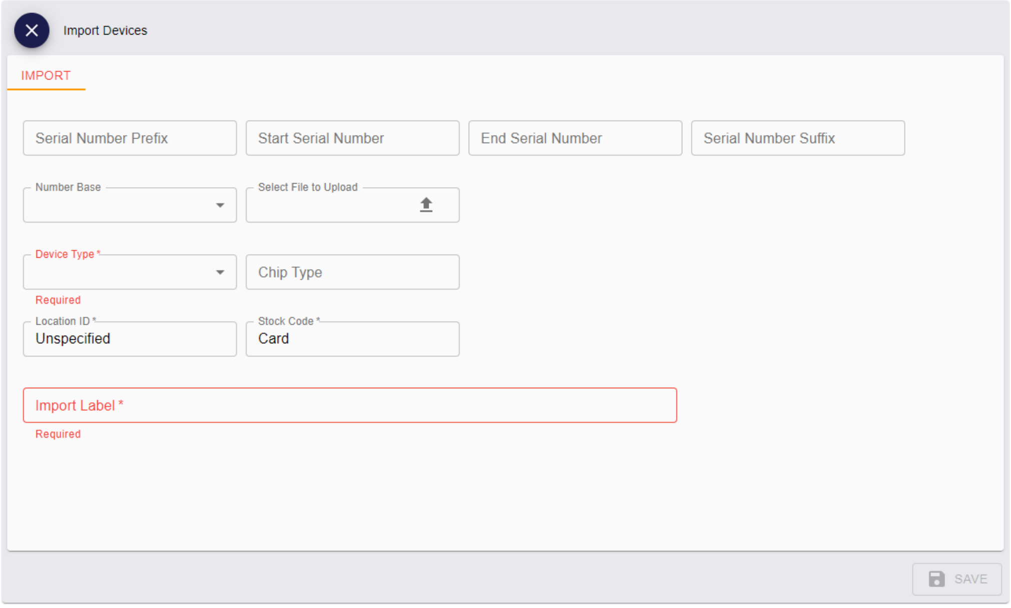
5.25 Importing devices from a manifest file

Important: Before you can import devices from a manifest file, you must customize your MyID installation with a hook that converts the import file into a format that MyID can use. For more information, contact Intercede quoting reference SUP-372.

If you are importing a batch of devices with sequential serial numbers, you can specify the range in the Import Devices screen; see section *5.24*, *Importing a range of devices*. However, if your devices do not fit into a neatly sequential range, you can import their serial numbers using a manifest file.

1. Select the **Devices** category.
2. Click **Import**.

   The Import Devices screen appears.


Import Devices
IMPORT
Serial Number Prefix
Start Serial Number
End Serial Number
Serial Number Suffix
Number Base
Select File to Upload
Device Type *
Required
Chip Type
Import Label *
Required
SAVE

Location ID *: Unspecified

Stock Code *: Card

3. Click **File** and select the manifest file containing the serial numbers you want to import.
4. Complete the following fields:
   - **Device Type** – select the type of device from the drop-down list.
   - **Chip Type** – optionally, provide the chip type for the device; for example, `IDEMIA ID-One PIV v81`.
   - **Location ID** – select the initial location for the devices from the drop-down list.

     See section *9*, *Working with locations*.
   - **Stock Code** – select the stock code for the devices.

     See section *8.2*, *Editing inventory lists* for details of setting up the list of stock codes.
   - **Import Label** – type a label to be associated with the imported devices. You can use this in the Available Device Stock search criteria to find these devices; see section *5.26*, *Viewing imported devices*.
5. Click **Save**.

5.26 Viewing imported devices

You can search for imported devices and view their details, including the location, stock code, import label, and any stock transfers to which they are currently assigned.

To view imported devices:

1. Select the **Devices** category.
2. From the **Reports** drop-down list, select the search report you want to use.
   - The **Devices** search provides extensive search options and can return all devices in your system.

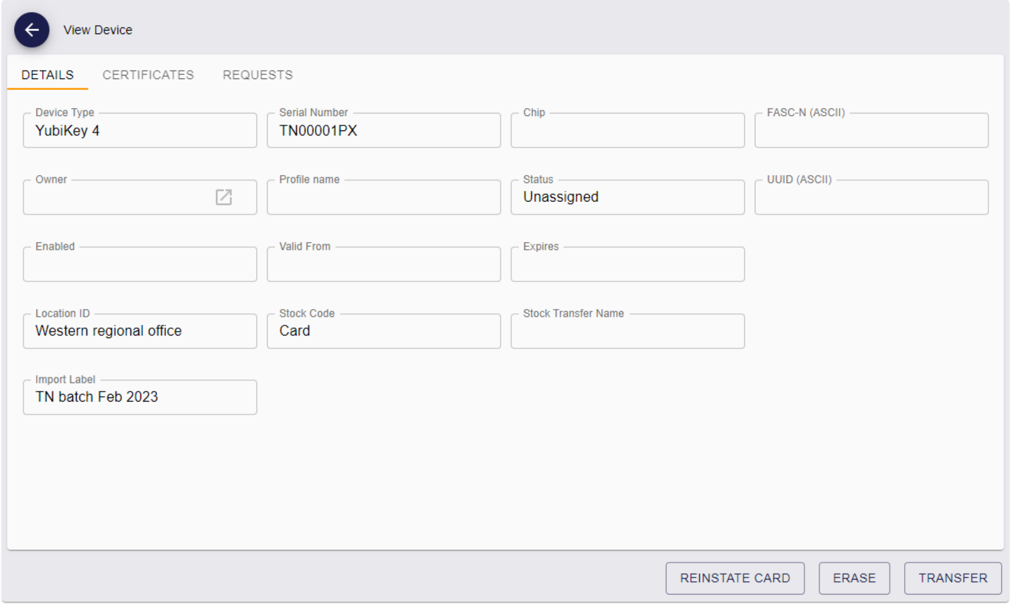
     See the *Searching for a device* section in the *MyID Operator Client* guide for details.
   - The **Available Device Stock** search provides a list of each device in the system available for stock transfer; that is, not currently issued and not currently assigned to a stock transfer. You can use the **Import Label**, **Location**, or **Stock Code** in the search criteria to search for particular imported devices.

     See section *7.3.19*, *Available Device Stock report*.
3. Click **Search**.

   MyID returns a list of devices.

   From this list, you can transfer devices; see section *11*, *Working with stock transfers*.
4. Click a record to display the details of the device.

   The View Device screen appears.


View Device
DETAILS
CERTIFICATES
REQUESTS
Chip
FASC-N (ASCII)
Owner
Profile name
UUID (ASCII)
Enabled
Valid From
Expires
Stock Transfer Name
REINSTATE CARD
ERASE
TRANSFER

Device Type: YubiKey 4
Serial Number: TN00001PX
Status: Unassigned
Location ID: Western regional office
Stock Code: Card
Import Label: TN batch Feb 2023

See the *Searching for a device* section in the *MyID Operator Client* guide for details of the standard information available on this screen.

The following additional fields are available on the **Details** tab when you have the inventory control module installed:

- **Location ID** – The name of the location where the device is kept.
- **Stock Code** – The stock code assigned to the device.
- **Stock Transfer Name** – If the device is currently assigned to a stock transfer, the name of the transfer appears here.
- **Import Label** – The label specified when you imported the device.

You can also click **Transfer** to allocate this single device to a stock transfer; see section *11.4.2*, *Adding a single device to a stock transfer*.

5.26.1 Viewing device import requests

You can also search for device import requests. These requests are excluded from the standard Requests search.

To view device import requests:

1. Select the **Requests** category.
2. From the **Reports** drop-down list, select **Device Import Requests**.
3. Provide any search criteria,.

   See section *7.3.6*, *Device Import Requests report* for details of the search criteria you can use.
4. Click **Search**.

   MyID returns a list of device import requests.
5. Click a record to display the details of the request.

5.27 Accepting delivery for a device

If your system is set up for a delivery stage within the device issuance process that allows you to confirm that the device has been delivered to the applicant, you must mark a device as delivered before it can be activated. The request job remains at the Awaiting Delivery status until you have confirmed that the device has been delivered.

5.27.1 Configuring the card delivery process for a delivery stage

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

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

To set the option:

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

5.27.2 Issuing a card that requires a delivery stage

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

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

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

5.27.3 Marking a device as delivered

To mark a device as delivered:

1. Search for a device.

   You can use the **Awaiting Delivery** search report.

   See section *5.1*, *Searching for a device*.

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

   For example:

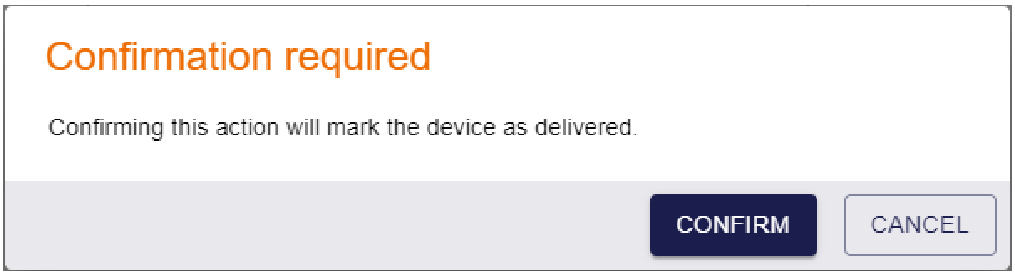
    - Click the item in the list on the **Devices** tab of the View Person form.
    - Click the link icon ↗ on the **Device Serial Number** field of the View Request form.

2. On the View Device screen, click the **Accept Delivery** option in the button bar at the bottom of the screen.

   Note: You cannot mark a card as delivered if you were the operator who requested the job, or if the card is intended for you.

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

   The confirmation dialog appears.



Confirmation required

Confirming this action will mark the device as delivered.

3. Click **Confirm** to mark the card as delivered.

Note: Unlike in the **Deliver Card** workflow in MyID Desktop, you work with the device, not the job. Also, you cannot reject a delivery; if you do not want to accept the delivery, click **Cancel Device** on the View Device screen, which cancels both the device and the job.

5.27.4 Marking multiple devices as delivered

If you have several devices to mark as delivered at the same time, you can accept delivery in a batch instead of accepting them one by one.

Note: You can access the **Tools** menu only if you have a role with the **Tools Menu** option from the **Configuration** section of the **Edit Roles** workflow.

To accept multiple device deliveries:

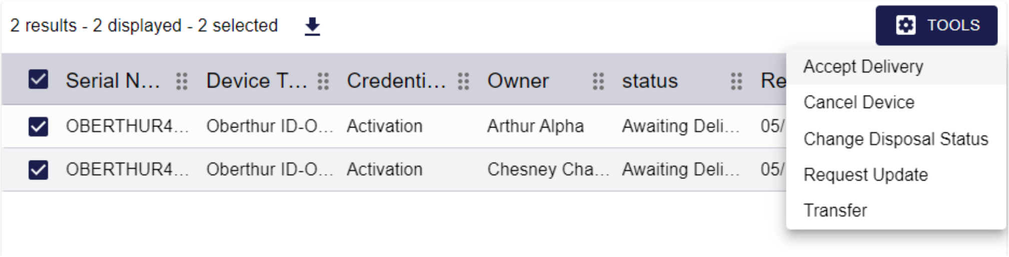
1. Search for the devices you want to accept.

   You can use the **Awaiting Delivery** search report.

   See section *5.1*, *Searching for a device*.

2. Use the checkboxes to the left of the devices to select one or more device.

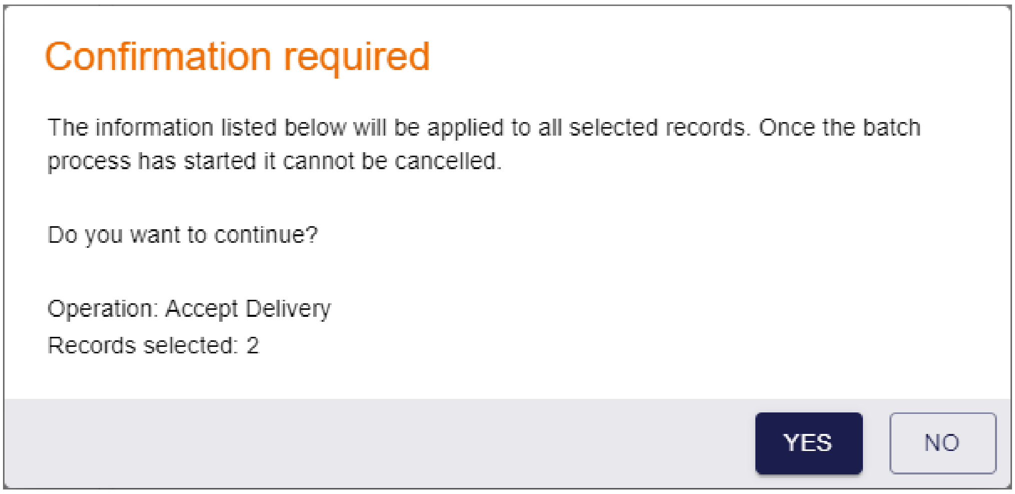
3. From the **Tools** menu, select **Accept Delivery**.



2 results - 2 displayed - 2 selected

☑	Serial N…	Device T…	Credenti…	Owner	status	Re
☑	OBERTHUR4…	Oberthur ID-O…	Activation	Arthur Alpha	Awaiting Deli…	05/
☑	OBERTHUR4…	Oberthur ID-O…	Activation	Chesney Cha…	Awaiting Deli…	05/

The confirmation screen appears.



Confirmation required

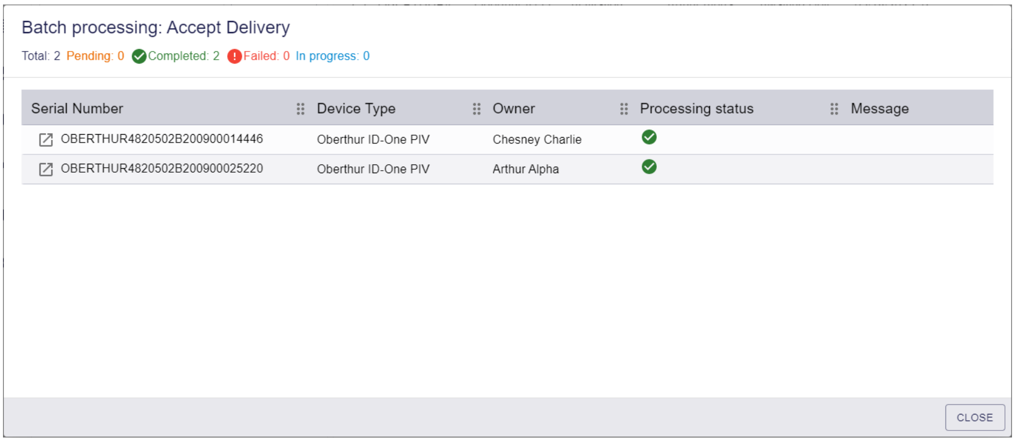
The information listed below will be applied to all selected records. Once the batch process has started it cannot be cancelled.

Do you want to continue?

Operation: Accept Delivery
Records selected: 2

4. Click **Yes** to proceed with the delivery, or **No** to go back to the list of devices.

   When you click **Yes**, the Batch Processing screen appears.



Batch processing: Accept Delivery

Total: 2 Pending: 0 ✓Completed: 2 ❗Failed: 0 In progress: 0

Serial Number	Device Type	Owner	Processing status	Message
OBERTHUR4820502B200900014446	Oberthur ID-One PIV	Chesney Charlie	✓	
OBERTHUR4820502B200900025220	Oberthur ID-One PIV	Arthur Alpha	✓	

The deliveries are processed. The table shows the status of each delivery:

✓	The delivery succeeded.
❗	The delivery failed. The Message column displays the reason for the failure; for example, you may not have permissions to accept delivery (you cannot accept delivery for a device if you requested it, or if the device is for you) or the device may not be in the correct state to be accepted for delivery.

5. Click **Close**.

5.28 Viewing the initial PIN for a device

If you have configured your credential profile to generate an initial PIN for the device using the **EdeficePinGenerator** or **EdeficePolicyPinGenerator** algorithm, MyID can regenerate the PIN that was used when the device was issued using the same secure method, and display it on the View Device screen.

As this is sensitive information, the field that displays the initial PIN on the View Device screen is protected by a special role named View Device Initial PIN. Only operators who have this role can see the field that contains the initial PIN.

See the *PIN generation* section of the ***Administration Guide*** for details of configuring your system to generate initial PINs on the MyID server.

5.28.1 Configuring the View Device Initial PIN role

When installing or upgrading MyID, the View Device Initial PIN role is added to your system, unless it exists already. The role is defined with no access to any operations; it acts as an *additional* permission that allows you to view the field that contains the initial PIN for a device only if you already have access to the View Device screen.

In addition, the role is configured with Smart Card as its only logon method; this means that if you log on to the MyID Operator Client using any other logon mechanism (for example, passwords) you cannot see the initial PIN field on the View Device screen. If you want to be able to view the initial PINs when logging in to MyID using any other method, you must configure the logon methods for the View Device Initial PIN role; see the *Assigning logon mechanisms* section of the ***Administration Guide*** for details.

If you delete the View Device Initial PIN role from your system, you can no longer view the initial PINs on the View Device screen. If you subsequently want to re-enable this feature, you can create a new role with the same name.

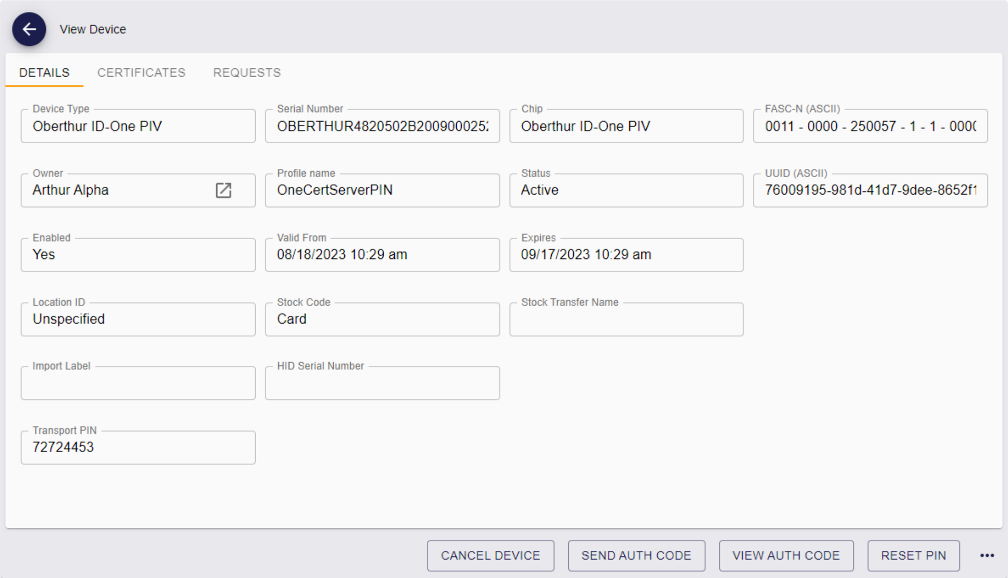
You are recommended to restrict access to this role by allowing only specified roles to assign it to other operators. To do this, you can set the **Managed By** option for the role; see the *Controlling the assigning of roles* section of the ***Administration Guide*** for details.

5.28.2 Viewing the initial PIN on the View Device screen

If the following conditions are met:

- Your user account has the View Device Initial PIN role assigned.
- You have the required permissions to access the View Device screen.
- You have logged on to the MyID Operator Client using a logon mechanism allowed by the View Device Initial PIN role.

then the **Transport PIN** field is displayed on the **Details** tab of the View Device screen.



Device Type: Oberthur ID-One PIV
Serial Number: OBERTHUR4820502B200900025
Chip: Oberthur ID-One PIV
FASC-N (ASCII): 0011 - 0000 - 250057 - 1 - 1 - 000
Owner: Arthur Alpha
Profile name: OneCertServerPIN
Status: Active
UUID (ASCII): 76009195-981d-41d7-9dee-8652f1
Enabled: Yes
Valid From: 08/18/2023 10:29 am
Expires: 09/17/2023 10:29 am
Location ID: Unspecified
Stock Code: Card
Stock Transfer Name:
Import Label:
HID Serial Number:
Transport PIN: 72724453

If the device was issued with a server-generated PIN using the **EdeficePinGenerator** or **EdeficePolicyPinGenerator** algorithm, the PIN is displayed in this field; otherwise, the field is left blank.

6 Working with requests

A request is a task in the MyID system that was created by an operator to carry out an action for a person; for example, to request a new device, or to update an existing device.

The MyID Operator Client allows you to work with requests in the following ways:

- You can create a request for a new device.

  See section *4.5*, *Requesting a device for a person*.
- You can create a request for a replacement device.

  See section *5.4*, *Requesting a replacement device*.
- You can view requests.

  See section *6.1*, *Searching for a request*.
- You can approve a request.

  See section *6.2.1*, *Approving requests*.
- You can reject a request.

  See section *6.2.2*, *Rejecting requests*.
- You can cancel a request.

  See section *6.2.3*, *Canceling requests*.
- You can cancel multiple requests at the same time.

  See section *6.2.6*, *Canceling multiple requests*.
- You can collect a request using the **Collect Card** workflow in MyID Desktop or **Collect My Card** in the Self-Service App.

  See section *6.3*, *Collecting a device request*.
- You can send a code to a person to allow them to collect a request.

  See section *6.4*, *Sending a collection code*.
- You can assign a specific device to a request.

  See section *6.5*, *Assigning a device to a request*.

6.1 Searching for a request

To search for a request:

1. Click the **Requests** category.
2. Select the search to use from the drop-down list.

   By default, only the **Requests** search is available; however, your system may have additional custom requests searches that you use for reporting.
3. Enter some or all of the search criteria for the target of the request:

- **Name (contains)** – type some characters from the person's name.

  You cannot use wildcards in this field; it automatically uses fuzzy matching.

  For example, if you search for `Sam`, the search results contain records where the **Full Name** or **Logon Name** fields contain the following:

  - Sam Smith
  - Jane Samson
  - Samuel Johnson
  - Samantha Samuels

  However, as the fuzzy matching searches only the start of the word, the following would not appear:

  - Alice Balsam

  If you specify more than one word in this field, the search results contain records that match *all* the words. For example, if you search for `Sam John`, the results include:

  - Sam Johnson
  - John Samson
  - Samantha Johnson
  - John Samuels

  However, the following do not appear:

  - Sam Smith (no match for "John")
  - John Smith (no match for "Sam")
  - Sam Littlejohn (no match for "John" – it does not occur at the start of a word)

- **Group** – click the open icon ⧉ to select the group to which the person belongs.

  See section *3.3.7*, *Selecting a group*.

  If you want to view requests for people from the groups below the selected group in the hierarchy, select the **Include Subgroups** option.

- **Credential Profile** – from the drop-down list, select the credential profile that was used in the request.
- **Status** – from the drop-down list, select the status of the request.

  For example, select **Awaiting Issue** to search for requests for devices that are available but have not yet been collected.

You can also select the following **Additional search criteria**:

- **Logon** – type the logon name of the person.
- **Type** – from the drop-down list, select the type of request; for example, **IssueCard** or **CancelCard**.
- **ID** – type the specific internal ID of the request, if you know it. The ID is displayed in the list of search results and on the View Request form.
- **Label** – type the label applied to the request.

- **Requested After** – select a date. Only requests made after this date are returned.
- **Requested Before** – select a date. Only requests made before this date are returned.
- **Validated After** – select a date. Only requests validated after this date are returned.
- **Validated Before** – select a date. Only requests validated before this date are returned.
- **Device Type** – from the drop-down list, select the manufacturer and model of device; for example, Oberthur ID-One PIV.
- **Device Serial Number** – type the serial number of the device.

Select the additional criteria to add them to the search form. Click the close **x** buttons on the additional criteria to remove them from the search form.

4. Click **Search**.

   The list of matching results appears.

   Records are sorted most recent first; currently, you cannot change the sort order.

5. To carry out actions on multiple requests, select the checkbox to the left of the requests, then from the **Tools** menu select the batch operation.

   Note: You can access the **Tools** menu only if you have a role with the **Tools Menu** option from the **Configuration** section of the **Edit Roles** workflow.

   From this menu, you can:

   - Cancel multiple requests. See section *6.2.6*, *Canceling multiple requests*.

6. To work on a single request, click a record to display the details of the request.

   You can view information about the request, including its status, and the dates it was requested, validated, or actioned.

   From this screen, you can:

   - Approve, reject, or cancel a request. See section *6.2*, *Approving, rejecting, and canceling requests*.
   - Collect a request. See section *6.3*, *Collecting a device request*.
   - Send a collection code for the request. See section *6.4*, *Sending a collection code*.
   - Assign a specific device to the request. See section *6.5*, *Assigning a device to a request*.
   - Click the link icon ↗ on the **Full Name** field to view the person's details.

You can also view a request from any form that displays a link to the request.

For example:

- Click the entry in the list of requests in the **Requests** tab of the View Person form.
- Click the entry in the list of requests in the **Device Requests** tab of the View Device form.
- View the screen that appears automatically after you have requested a device, assuming that the request does not need to be approved by another operator first.

6.2 Approving, rejecting, and canceling requests

You can approve, reject, or cancel an outstanding request for a person; for example a request to issue a device.

Whether or not a request requires approval depends on the **Validate Issuance** setting in the credential profile; see the *Working with credential profiles* section in the ***Administration Guide*** for details.

To approve or reject a request, you must have permission to validate the credential profile; see the *Constrain credential profile validator* section in the ***Administration Guide*** for details. You also cannot be the operator who made the request, or the person who will receive the requested device.

6.2.1 Approving requests

To approve a request:

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

   See section *6.1*, *Searching for a request*.

   You can use the alternative **Requests for review** report to display all requests that are awaiting validation.

   You can also view a request from any form that displays a link to the request.

   For example:

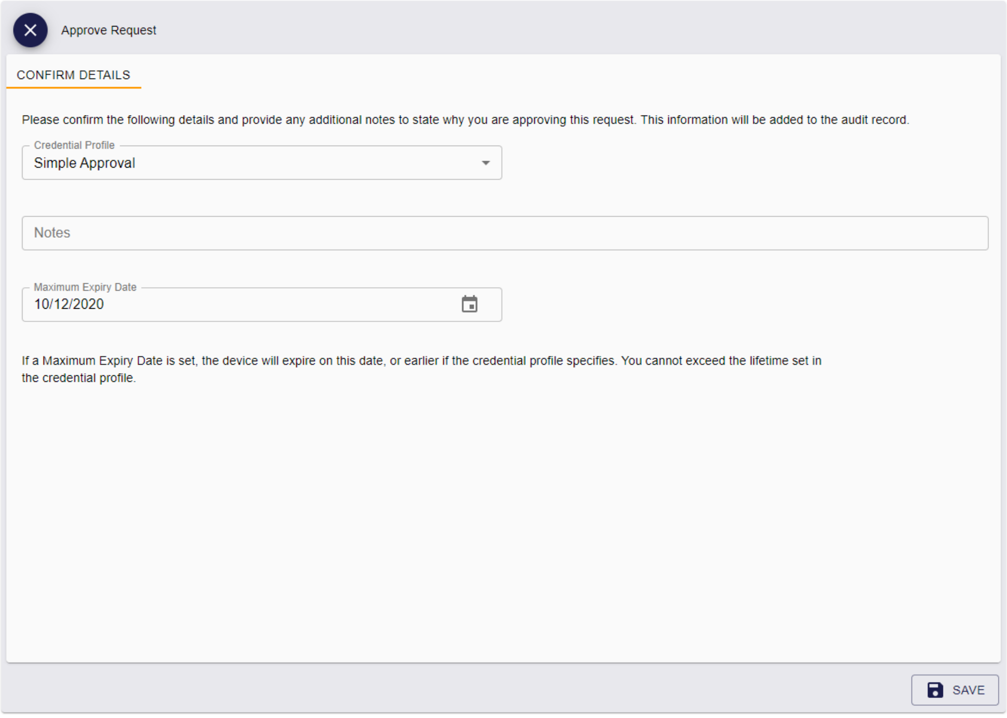
   - Click the entry in the list of requests in the **Requests** tab of the View Person form.
   - Click the entry in the list of requests in the **Device Requests** tab of the View Device form.
   - View the screen that appears automatically after you have requested a device, assuming that the request does not need to be approved by another operator first.

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

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

   If this option is not available, the request does not require validation.

   The Approve Request screen appears.



Please confirm the following details and provide any additional notes to state why you are approving this request. This information will be added to the audit record.

Credential Profile: Simple Approval

Notes

Maximum Expiry Date: 10/12/2020

If a Maximum Expiry Date is set, the device will expire on this date, or earlier if the credential profile specifies. You cannot exceed the lifetime set in the credential profile.

3. Review the details of the request.

   If the **Change Credential Profile At Approval** configuration option (on the **Issuance Processes** page of the **Operation Settings** workflow) is set, you can select a different credential profile from the drop-down list. You must have the appropriate permission to request the credential profile, and the target must have the appropriate permission to receive it.

   You can provide any additional **Notes** to state why you are approving the request.

   If the **Set expiry date at request** option (on the **Issuance Processes** page of the **Operation Settings** workflow) is set, you can set or amend the **Maximum Expiry Date** for the request. You can select any date up to the `MaxRequestExpiryDate` specified for the person in the Lifecycle API. Note, however, that you cannot exceed the **Lifetime** setting for the credential profile; if the request is made for a credential to expire on a date six months from now, but the credential profile has a lifetime of 30 days, the device will be issued with a lifetime of 30 days.

   The credential profile can override the `MaxRequestExpiryDate` set for the person if the **Ignore User Expiry Date** option on the credential profile is set.

   If maximum expiry date set in the request exceeds the `MaxRequestExpiryDate` set for the person, at approval, if the operator does not have permission to modify they date (that is, it is not shown on screen) the maximum expiry date for the request is reset to be the same as the date set for the person. This happens automatically; the updated date is also recorded in the audit, and the correct date is shown when subsequently viewing the request. In this scenario, if the operator *does* have permission to change the date in the request, the date validation highlights that it needs to be changed, and the operator cannot proceed until they have amended the date. The calendar control is constrained to the date set for the person.

If you do not want to approve the request, click the Close button:

⊗

4. To approve the request, click **Save**.

6.2.2 Rejecting requests

To reject a request:

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

   See section *6.1*, *Searching for a request*.

   You can use the alternative **Requests for review** report to display all requests that are awaiting validation.

   You can also view a request from any form that displays a link to the request.

   For example:

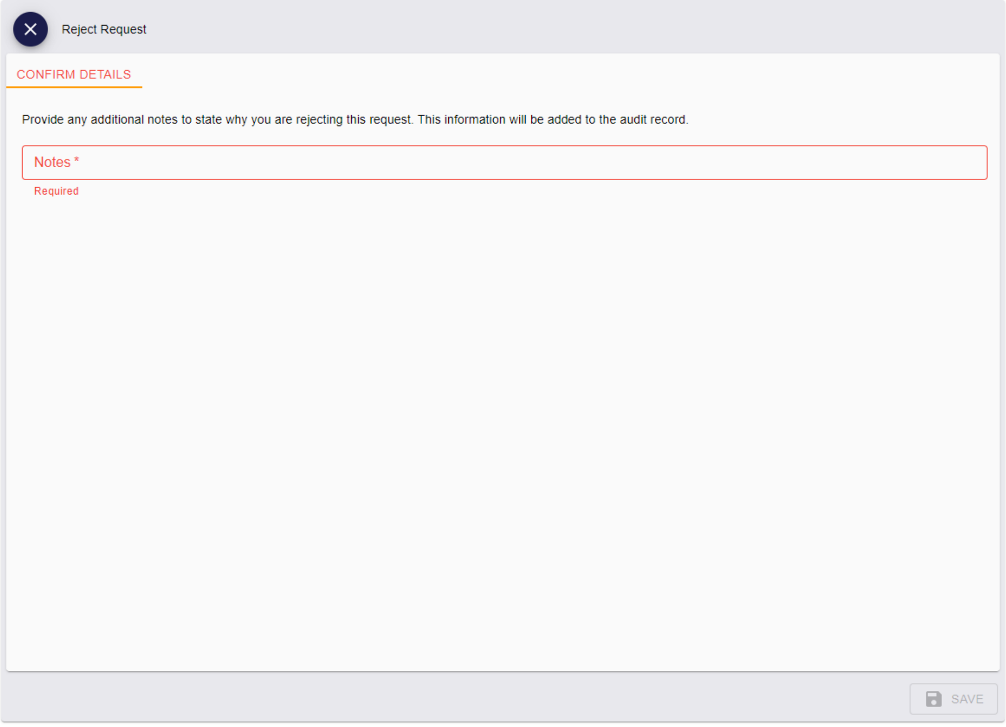
   - Click the entry in the list of requests in the **Requests** tab of the View Person form.
   - Click the entry in the list of requests in the **Device Requests** tab of the View Device form.
   - View the screen that appears automatically after you have requested a device, assuming that the request does not need to be approved by another operator first.

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

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

   If this option is not available, the request does not require validation. You can still cancel the request; see section *6.2.3*, *Canceling requests*.

   The Reject Request screen appears.



Provide any additional notes to state why you are rejecting this request. This information will be added to the audit record.

3. Review the details of the request, and provide any additional **Notes** to state why you are rejecting the request.

   The **Notes** are mandatory.

   If you do not want to reject the request, click the Close button:

   ✕

4. To reject the request, click **Save**.

6.2.3 Canceling requests

To cancel a request:

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

   See section *6.1*, *Searching for a request*.

   You can use the alternative **Requests for review** report to display all requests that are awaiting validation.

   You can also view a request from any form that displays a link to the request.

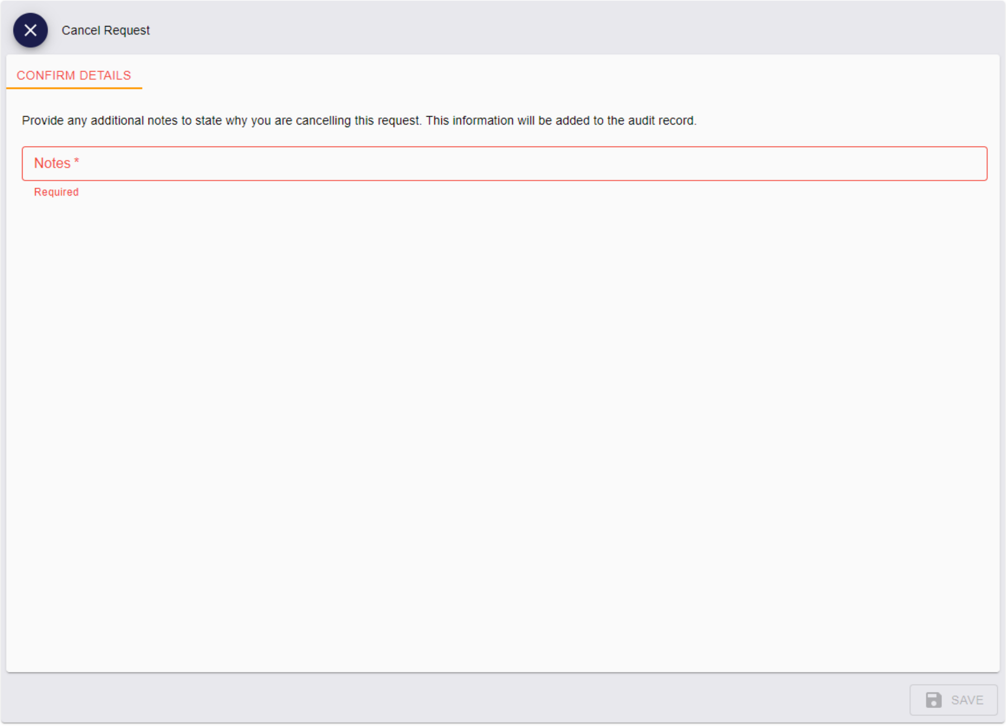
   For example:

   - Click the entry in the list of requests in the **Requests** tab of the View Person form.
   - Click the entry in the list of requests in the **Device Requests** tab of the View Device form.
   - View the screen that appears automatically after you have requested a device, assuming that the request does not need to be approved by another operator first.

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

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

   The Cancel Request screen appears.



Provide any additional notes to state why you are cancelling this request. This information will be added to the audit record.

3. Review the details of the request, and provide any additional **Notes** to state why you are canceling the request.

   The **Notes** are mandatory.

   If you do not want to cancel the request, click the Close button:

   ✕

4. To cancel the request, click **Save**.

6.2.4 Approving multiple requests

If you have several requests to approve at the same time, you can approve them in a batch instead of approving them one by one.

Note: You can access the **Tools** menu only if you have a role with the **Tools Menu** option from the **Configuration** section of the **Edit Roles** workflow.

To approve multiple requests:

1. Search for the requests you want to approve.

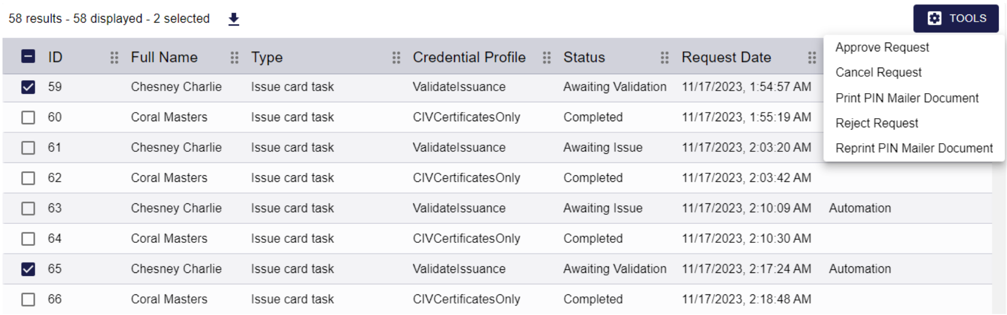
   See section *6.1*, *Searching for a request*.

   You can use the alternative **Requests for review** report to display all requests that are awaiting validation.

2. Use the checkboxes to the left of the requests to select one or more requests.

Note: If you select one request, the process is the same as clicking the **Approve Request** option in the button bar at the bottom of the View Request screen; MyID uses the batch process only if you select more than one request. See section *6.2.1*, *Approving requests* for details of approving a single request.

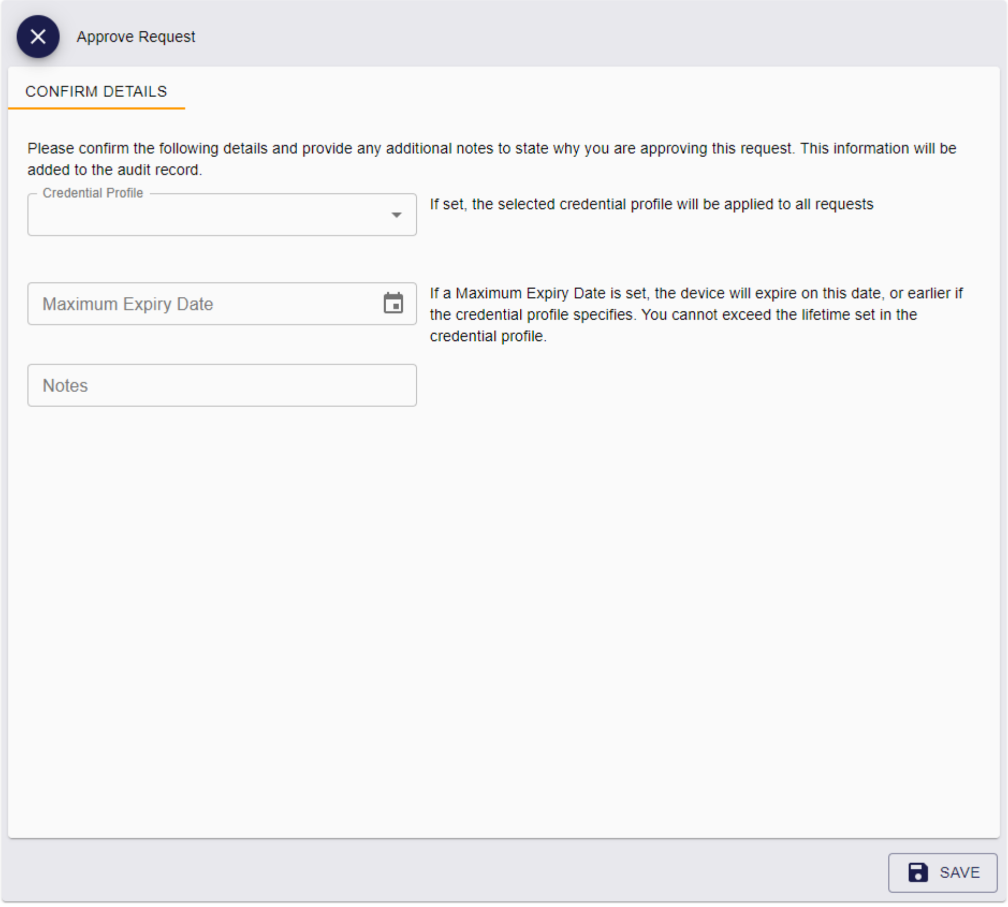
3. From the **Tools** menu, select **Approve Request**.



58 results - 58 displayed - 2 selected

	ID	Full Name	Type	Credential Profile	Status	Request Date	
☑	59	Chesney Charlie	Issue card task	ValidateIssuance	Awaiting Validation	11/17/2023, 1:54:57 AM	
☐	60	Coral Masters	Issue card task	CIVCertificatesOnly	Completed	11/17/2023, 1:55:19 AM	
☐	61	Chesney Charlie	Issue card task	ValidateIssuance	Awaiting Issue	11/17/2023, 2:03:20 AM	
☐	62	Coral Masters	Issue card task	CIVCertificatesOnly	Completed	11/17/2023, 2:03:42 AM	
☐	63	Chesney Charlie	Issue card task	ValidateIssuance	Awaiting Issue	11/17/2023, 2:10:09 AM	Automation
☐	64	Coral Masters	Issue card task	CIVCertificatesOnly	Completed	11/17/2023, 2:10:30 AM	
☑	65	Chesney Charlie	Issue card task	ValidateIssuance	Awaiting Validation	11/17/2023, 2:17:24 AM	Automation
☐	66	Coral Masters	Issue card task	CIVCertificatesOnly	Completed	11/17/2023, 2:18:48 AM	

The Approve Request screen appears.



Please confirm the following details and provide any additional notes to state why you are approving this request. This information will be added to the audit record.

If set, the selected credential profile will be applied to all requests

If a Maximum Expiry Date is set, the device will expire on this date, or earlier if the credential profile specifies. You cannot exceed the lifetime set in the credential profile.

If the **Change Credential Profile At Approval** configuration option (on the **Issuance Processes** page of the **Operation Settings** workflow) is set, you can select a different credential profile from the drop-down list.

Note: The list of credential profiles is constrained by the roles of the operator, not the potential recipients; this means that you can attempt to approve requests for devices using credential profiles that are not available to an individual recipient. If a credential profile is not available for a recipient, the request approval fails at the batch processing stage; however, the requests for other recipients who *do* have permission to receive the credential profile succeed.

If the **Set expiry date at request** option (on the **Issuance Processes** page of the **Operation Settings** workflow) is set, you can set or amend the **Maximum Expiry Date** for the request; see section *6.2.1*, *Approving requests*.

4. Provide any additional **Notes** to state why you are approving the requests.

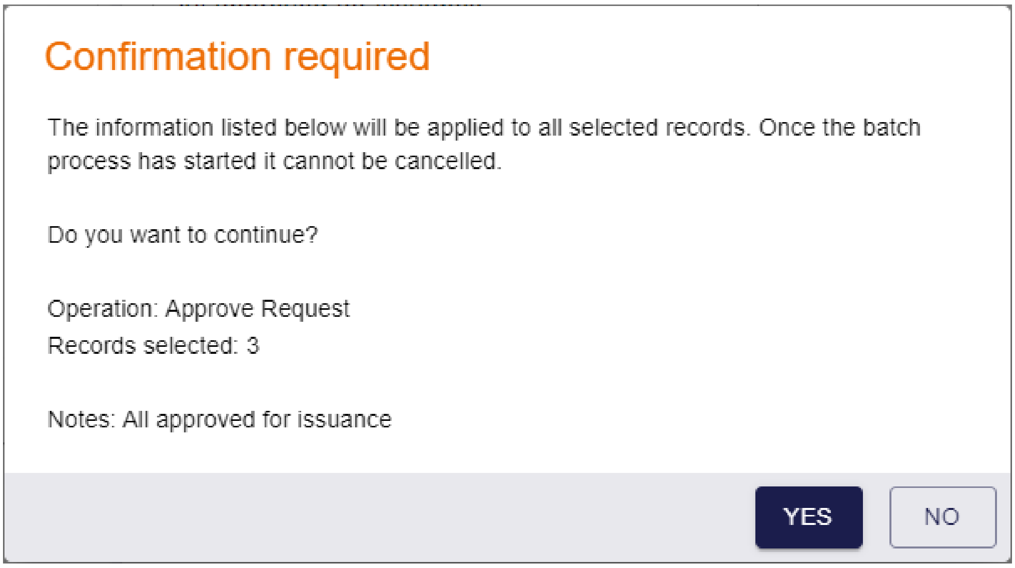
   The **Notes** are optional.

   If you do not want to approve the requests, click the Close button:

   ✕

5. Click **Save**.

   The confirmation screen appears.



Confirmation required

The information listed below will be applied to all selected records. Once the batch process has started it cannot be cancelled.

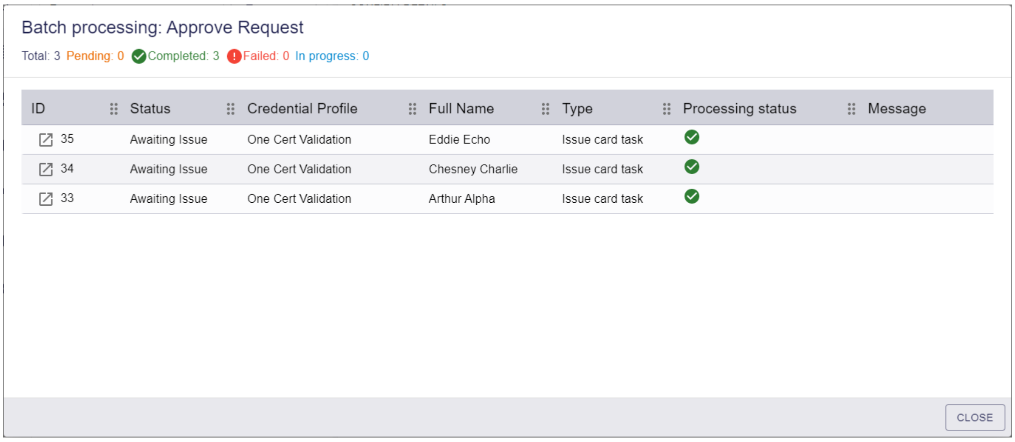
Do you want to continue?

Operation: Approve Request
Records selected: 3

Notes: All approved for issuance

6. Click **Yes** to proceed with the batch approval, or **No** to go back to the Approve Request screen.

   When you click Yes, the Batch Processing screen appears.



Batch processing: Approve Request

Total: 3 Pending: 0 ✓Completed: 3 !Failed: 0 In progress: 0

ID	Status	Credential Profile	Full Name	Type	Processing status	Message
35	Awaiting Issue	One Cert Validation	Eddie Echo	Issue card task	✓	
34	Awaiting Issue	One Cert Validation	Chesney Charlie	Issue card task	✓	
33	Awaiting Issue	One Cert Validation	Arthur Alpha	Issue card task	✓	

The request approvals are processed. The table shows the status of each request:

✓	The approval succeeded.
!	The approval failed. The Message column displays the reason for the failure; for example, you may have attempted to approve a request that was already in a Completed, Canceled, or Failed state.

7. Click **Close**.

6.2.5 Rejecting multiple requests

If you have several requests to reject at the same time, you can reject them in a batch instead of rejecting them one by one.

Note: You can access the **Tools** menu only if you have a role with the **Tools Menu** option from the **Configuration** section of the **Edit Roles** workflow.

To reject multiple requests:

1. Search for the requests you want to reject.

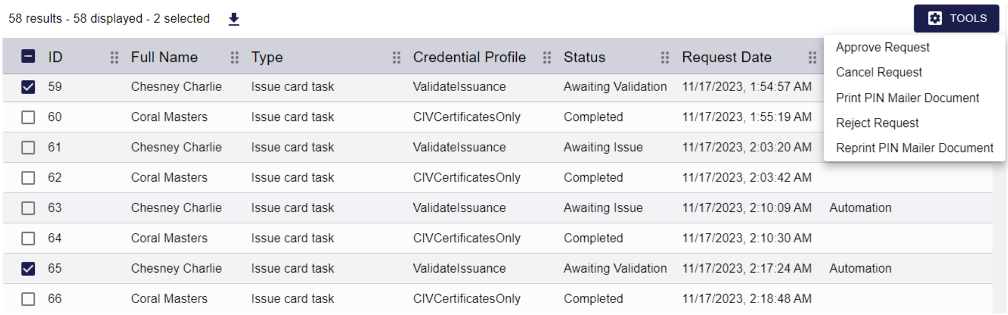
   See section *6.1*, *Searching for a request*.

   You can use the alternative **Requests for review** report to display all requests that are awaiting validation.

2. Use the checkboxes to the left of the requests to select one or more requests.

   Note: If you select one request, the process is the same as clicking the **Reject Request** option in the button bar at the bottom of the View Request screen; MyID uses the batch process only if you select more than one request. See section *6.2.2*, *Rejecting requests* for details of rejecting a single request.

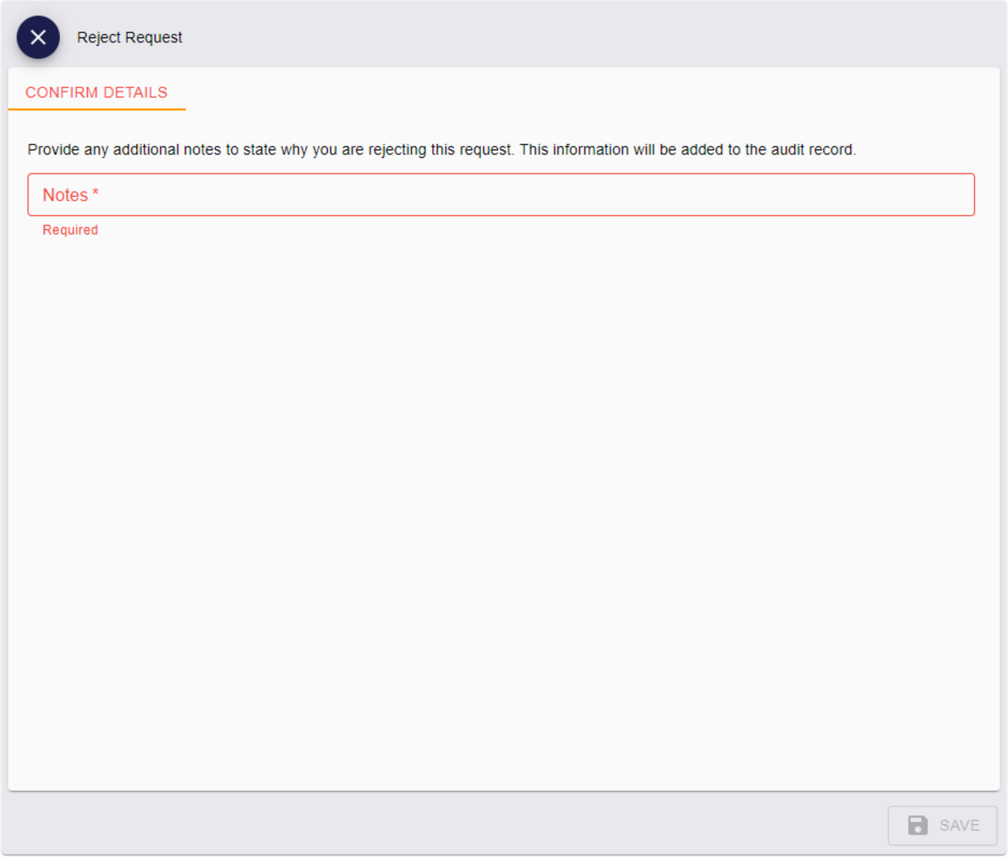
3. From the **Tools** menu, select **Reject Request**.


TOOLS
Approve Request
Cancel Request
Print PIN Mailer Document
Reject Request
Reprint PIN Mailer Document

58 results - 58 displayed - 2 selected

☐	ID	Full Name	Type	Credential Profile	Status	Request Date	
☑	59	Chesney Charlie	Issue card task	ValidateIssuance	Awaiting Validation	11/17/2023, 1:54:57 AM	
☐	60	Coral Masters	Issue card task	CIVCertificatesOnly	Completed	11/17/2023, 1:55:19 AM	
☐	61	Chesney Charlie	Issue card task	ValidateIssuance	Awaiting Issue	11/17/2023, 2:03:20 AM	
☐	62	Coral Masters	Issue card task	CIVCertificatesOnly	Completed	11/17/2023, 2:03:42 AM	
☐	63	Chesney Charlie	Issue card task	ValidateIssuance	Awaiting Issue	11/17/2023, 2:10:09 AM	Automation
☐	64	Coral Masters	Issue card task	CIVCertificatesOnly	Completed	11/17/2023, 2:10:30 AM	
☑	65	Chesney Charlie	Issue card task	ValidateIssuance	Awaiting Validation	11/17/2023, 2:17:24 AM	Automation
☐	66	Coral Masters	Issue card task	CIVCertificatesOnly	Completed	11/17/2023, 2:18:48 AM	

The Reject Request screen appears.


Reject Request
CONFIRM DETAILS
Notes *
Required
SAVE

Provide any additional notes to state why you are rejecting this request. This information will be added to the audit record.

4. Provide any additional **Notes** to state why you are rejecting the requests.

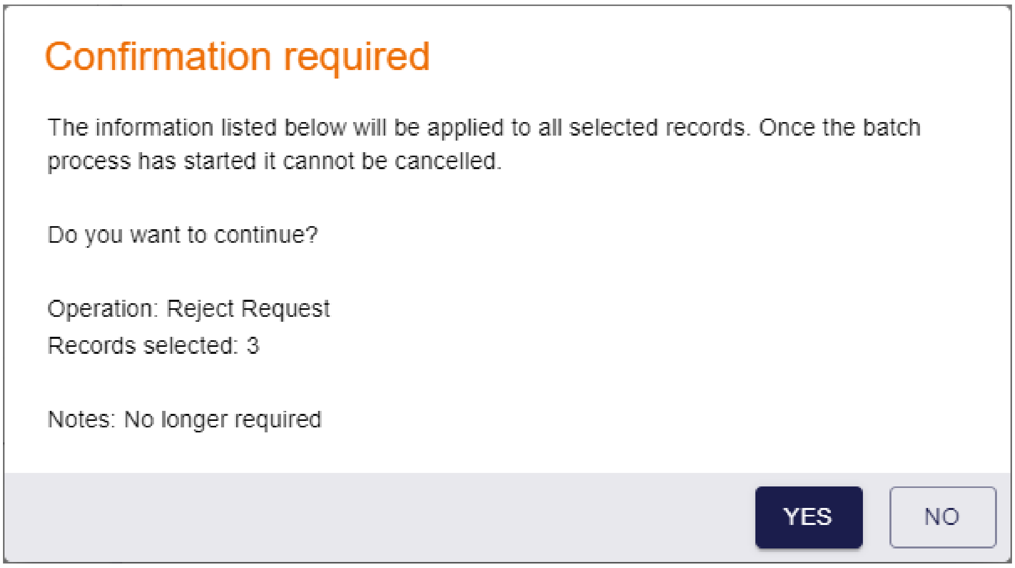
   The **Notes** are mandatory.

   If you do not want to reject the requests, click the Close button:

   ✕

5. Click **Save**.

   The confirmation screen appears.



Confirmation required

The information listed below will be applied to all selected records. Once the batch process has started it cannot be cancelled.

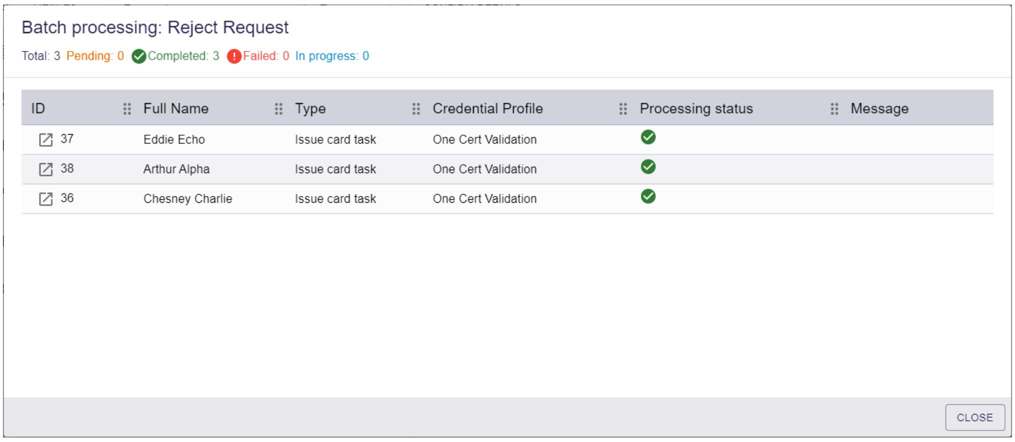
Do you want to continue?

Operation: Reject Request
Records selected: 3

Notes: No longer required

6. Click **Yes** to proceed with the batch rejection, or **No** to go back to the Reject Request screen.

   When you click Yes, the Batch Processing screen appears.



Batch processing: Reject Request

Total: 3 Pending: 0 ✓Completed: 3 !Failed: 0 In progress: 0

ID	Full Name	Type	Credential Profile	Processing status	Message
37	Eddie Echo	Issue card task	One Cert Validation	✓	
38	Arthur Alpha	Issue card task	One Cert Validation	✓	
36	Chesney Charlie	Issue card task	One Cert Validation	✓	

The request rejections are processed. The table shows the status of each request:

✓	The rejection succeeded.
!	The rejection failed. The Message column displays the reason for the failure; for example, you may have attempted to reject a request that was already in a Completed, Canceled, or Failed state.

7. Click **Close**.

6.2.6 Canceling multiple requests

If you have several requests to cancel at the same time, you can cancel them in a batch instead of canceling them one by one.

Note: You can access the **Tools** menu only if you have a role with the **Tools Menu** option from the **Configuration** section of the **Edit Roles** workflow.

To cancel multiple requests:

1. Search for the requests you want to cancel.

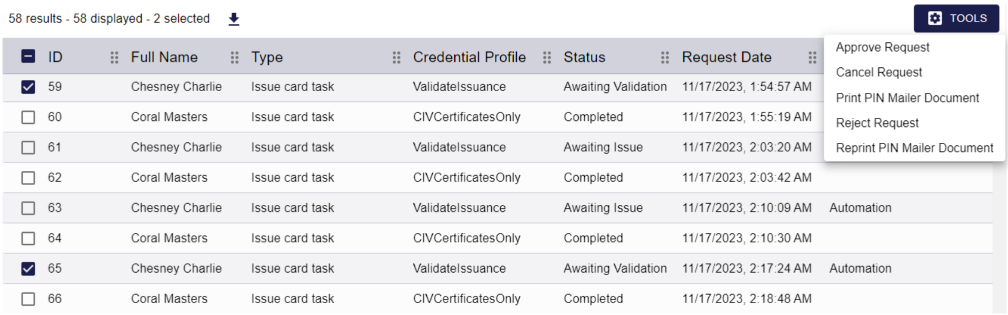
   See section *6.1*, *Searching for a request*.

   You can use the alternative **Requests for review** report to display all requests that are awaiting validation.

2. Use the checkboxes to the left of the requests to select one or more requests.

   Note: If you select one request, the process is the same as clicking the **Cancel Request** option in the button bar at the bottom of the View Request screen; MyID uses the batch process only if you select more than one request. See section *6.2.3*, *Canceling requests* for details of canceling a single request.

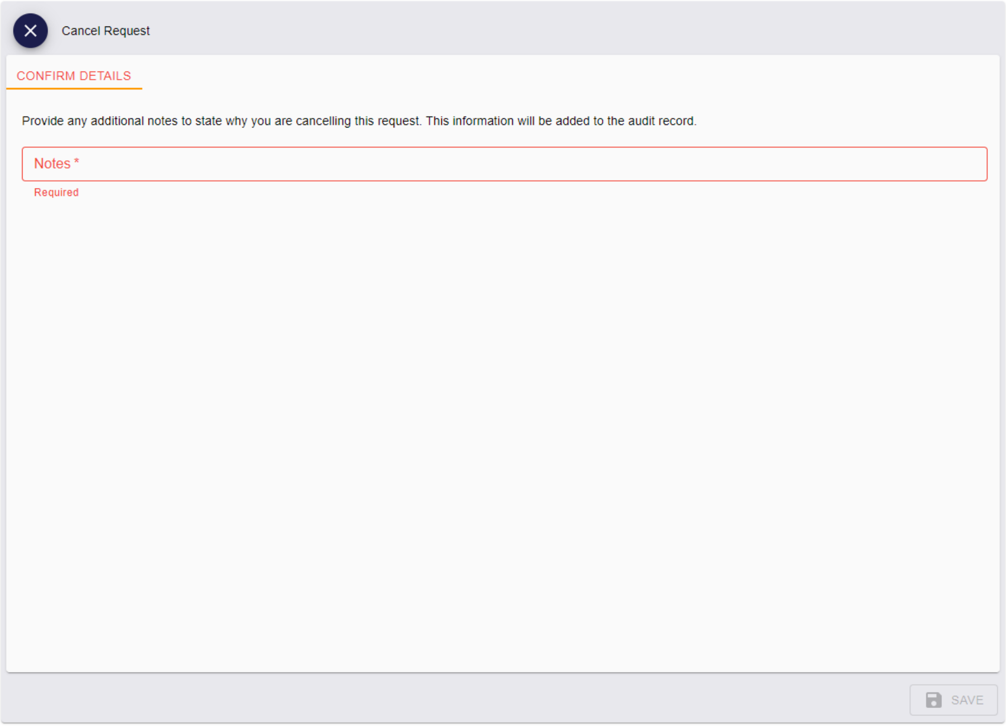
3. From the **Tools** menu, select **Cancel Request**.


TOOLS
Approve Request
Cancel Request
Print PIN Mailer Document
Reject Request
Reprint PIN Mailer Document

58 results - 58 displayed - 2 selected

⊟	ID	Full Name	Type	Credential Profile	Status	Request Date	
☑	59	Chesney Charlie	Issue card task	ValidateIssuance	Awaiting Validation	11/17/2023, 1:54:57 AM	
☐	60	Coral Masters	Issue card task	CIVCertificatesOnly	Completed	11/17/2023, 1:55:19 AM	
☐	61	Chesney Charlie	Issue card task	ValidateIssuance	Awaiting Issue	11/17/2023, 2:03:20 AM	
☐	62	Coral Masters	Issue card task	CIVCertificatesOnly	Completed	11/17/2023, 2:03:42 AM	
☐	63	Chesney Charlie	Issue card task	ValidateIssuance	Awaiting Issue	11/17/2023, 2:10:09 AM	Automation
☐	64	Coral Masters	Issue card task	CIVCertificatesOnly	Completed	11/17/2023, 2:10:30 AM	
☑	65	Chesney Charlie	Issue card task	ValidateIssuance	Awaiting Validation	11/17/2023, 2:17:24 AM	Automation
☐	66	Coral Masters	Issue card task	CIVCertificatesOnly	Completed	11/17/2023, 2:18:48 AM	

The Cancel Request screen appears.


Cancel Request
CONFIRM DETAILS
Notes *
Required
SAVE

Provide any additional notes to state why you are cancelling this request. This information will be added to the audit record.

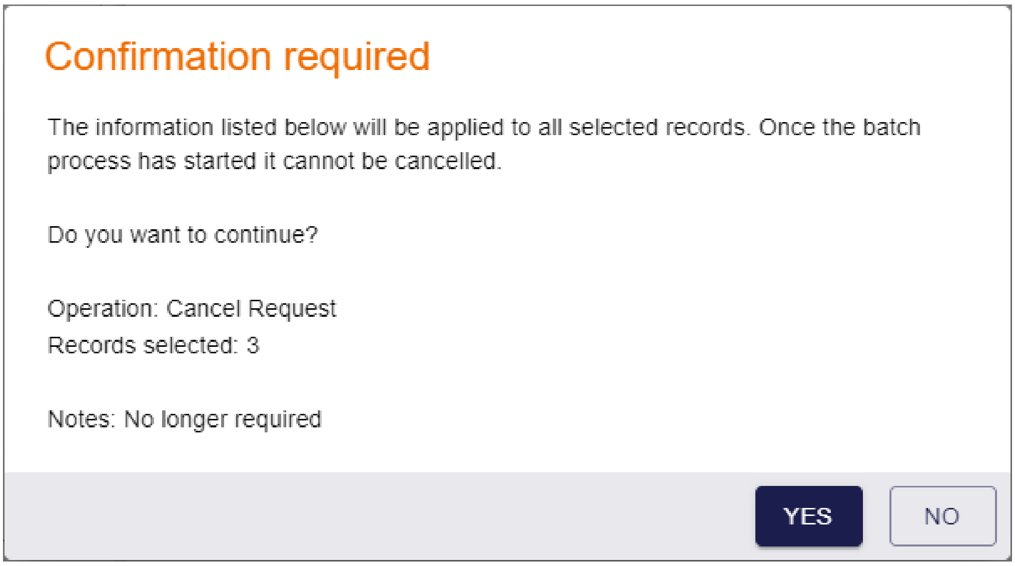
4. Provide any additional **Notes** to state why you are canceling the requests.

   The **Notes** are mandatory.

   If you do not want to cancel the requests, click the Close button:

5. Click **Save**.

   The confirmation screen appears.



Confirmation required

The information listed below will be applied to all selected records. Once the batch process has started it cannot be cancelled.

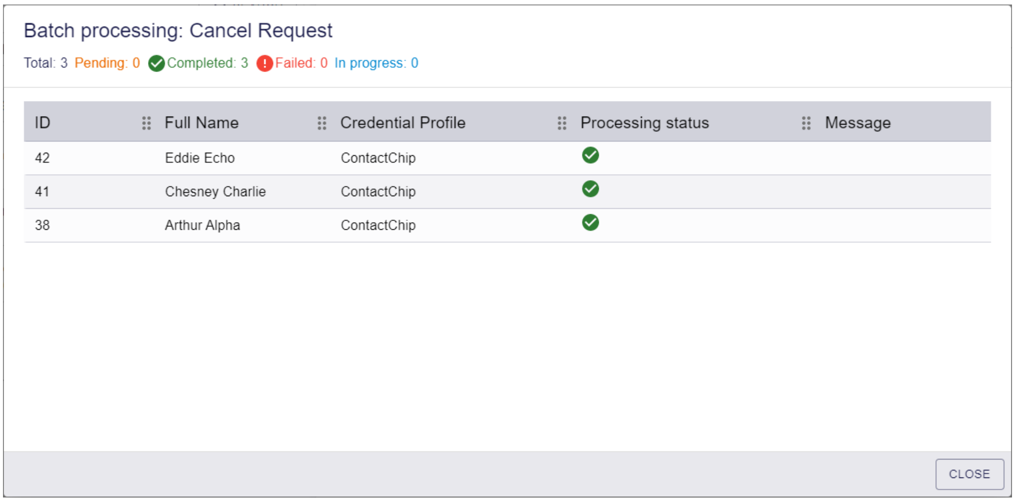
Do you want to continue?

Operation: Cancel Request
Records selected: 3

Notes: No longer required

6. Click **Yes** to proceed with the batch cancellation, or **No** to go back to the Cancel Request screen.

   When you click Yes, the Batch Processing screen appears.



Batch processing: Cancel Request

Total: 3 Pending: 0 ✓Completed: 3 ❗Failed: 0 In progress: 0

ID	Full Name	Credential Profile	Processing status	Message
42	Eddie Echo	ContactChip	✓	
41	Chesney Charlie	ContactChip	✓	
38	Arthur Alpha	ContactChip	✓	

The request cancellations are processed. The table shows the status of each request:

✓	The cancellation succeeded.
❗	The cancellation failed. The Message column displays the reason for the failure; for example, you may have attempted to cancel a request that was already in a Completed, Canceled, or Failed state.

7. Click **Close**.

6.3 Collecting a device request

From the View Request screen, you can launch the **Collect Card** workflow in MyID Desktop to collect a request for a device, or the **Collect My Card** feature in the MyID Self-Service App to collect a request for a device for yourself. You can also launch the MyID Client Service to collect a soft certificate request.

For more information about using MyID Desktop and Self-Service App workflows from within the MyID Operator Client, see section *3.3.2*, *Launching MyID Desktop, Self-Service App, or MyID Client for Windows workflows*.

To collect a device request:

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

   See section *6.1*, *Searching for a request*.

   You can also view a request from any form that displays a link to the request.

   For example:

   - Click the entry in the list of requests in the **Requests** tab of the View Person form.
   - Click the entry in the list of requests in the **Device Requests** tab of the View Device form.
   - View the screen that appears automatically after you have requested a device, assuming that the request does not need to be approved by another operator first.

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

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

   If this option is not available, the request cannot be collected; for example, it may require validation.

   - If the request is for another person:

     The **Collect Card** workflow appears in a MyID Desktop window with the request already selected.

     See the *Collecting a card* section in the ***Operator's Guide***.

   - If the request is for yourself:

     The **Collect My Card** feature appears in a Self-Service App window with the request already selected.

     See the *Self-Service App features* section in the ***Self-Service App*** guide.

   - If the request is for a soft certificate:

     The Collect Soft Certificates screen appears, which allows you to download the certificates and print a transport document.

     See section *14.1*, *Collecting a soft certificate*.

6.4 Sending a collection code

If the credential profile for a device has been set up with **Issuance Settings > Generate Code on Request** set to **Simple Logon Code** or **Complex Logon Code**, when the device is requested, MyID sends an email message with a single-use code that the person can use to log on to MyID for the single purpose of collecting their device.

If necessary (for example, if the original code has expired) you can use the **Send Auth Code** feature on the View Request screen of the MyID Operator Client to send another code to the person; you can choose to send the code in an email or in an SMS text message to their cell phone.

Alternatively you can allow an operator to view a job collection code on their screen, which they can then read out over the phone or paste into a secure chat channel to allow the person to collect their device.

When you send a code, it replaces any previously-issued code.

You can send a code even if the credential profile has not been set up to send a code automatically on issuance (**Issuance Settings > Generate Code on Request** set to **None**); for example, you can create a request for a device, then when the cardholder contacts the helpline to indicate they are ready to collect their device, you can issue a short lifetime code for immediate use.

For information about configuring MyID and using these codes, see the *Setting up logon codes* and *Using logon codes* sections of the ***Administration Guide***.

6.4.1 Sending a collection code by email or SMS

To request a collection code:

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

   See section *6.1*, *Searching for a request*.

   You can also view a request from any form that displays a link to the request.

   For example:

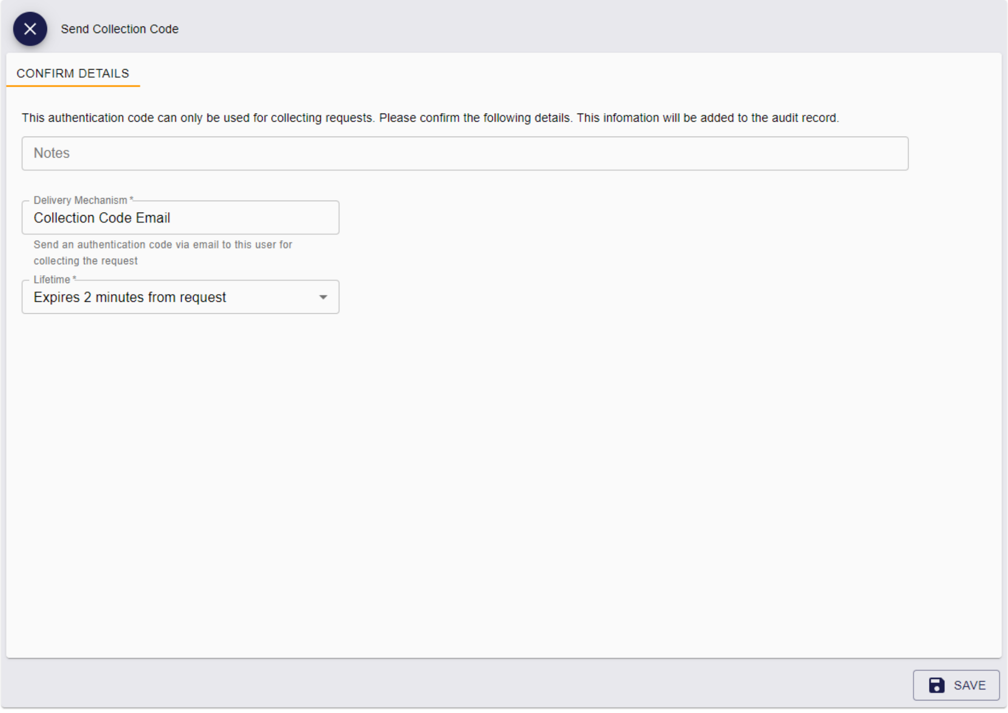
   - Click the entry in the list of requests in the **Requests** tab of the View Person form.
   - Click the entry in the list of requests in the **Device Requests** tab of the View Device form.
   - View the screen that appears automatically after you have requested a device, assuming that the request does not need to be approved by another operator first.

2. Click the **Send Auth Code** option in the button bar at the bottom of the screen.

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

   If this option is not available, the request is not suitable to be collected using a code; for example, it may be already collected, require activation, or be a bureau request. You can send codes for contact cards, soft certificate packages, Windows Hello, or Microsoft VSCs. You must also make sure that you have the **Send Auth Code for Job Collection** option selected for your role in the **Edit Roles** workflow.

   The Send Collection Code screen appears:



This authentication code can only be used for collecting requests. Please confirm the following details. This infomation will be added to the audit record.

Delivery Mechanism *: Collection Code Email

Send an authentication code via email to this user for collecting the request

Lifetime *: Expires 2 minutes from request

3. Type any **Notes** you want to store in the audit trail about the operation.

4. From the **Delivery Mechanism** drop-down list, select how you want to send the code.

   You can choose from:

   - **Collection Code Email** – sends the code as an email to the person's configured email address. This option is available if the **Job Collection Auth Code Email** template is enabled in the **Email Templates** workflow.
   - **Collection Code SMS** – sends the code as a text message to the person's configured cell phone number. This option is available if the **Job Collection Auth Code SMS** template is enabled in the **Email Templates** workflow.

   Note: The complexity of the code is determined by the **Generate Code on Request** setting in the credential profile, or if the credential profile does not contain a complexity setting, by the **Auth Code Complexity** configuration option.
5. From the **Lifetime** drop-down list, select how long you want the code to be valid.

   The options here are determined by the values saved in the **Auth Code Lifetime for Immediate Use** and **Logon Code Lifetime** configuration options; by default, the options are:

   - **Expires 30 days from request** – based on the default **Logon Code Lifetime** setting of 720 hours.
   - **Expires 2 minutes from request** – based on the default **Auth Code Lifetime for Immediate Use** setting of 120 seconds.
6. Click **Save**.

   MyID sends the code to the person, who can then use it to collect their device. See the *Using logon codes* section of the ***Administration Guide*** for details of collecting devices using codes In the Self-Service Kiosk, the Self-Service App, and MyID Desktop.

6.4.2 Viewing a collection code on screen

To view a collection code:

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

   See section *6.1*, *Searching for a request*.

   You can also view a request from any form that displays a link to the request.

   For example:

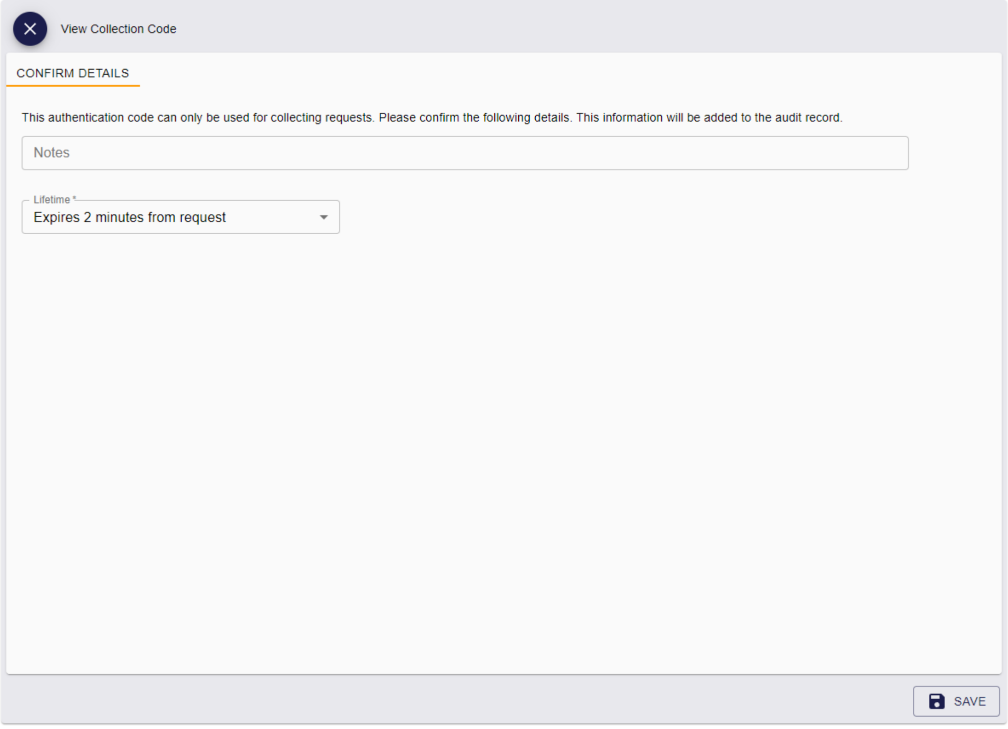
   - Click the entry in the list of requests in the **Requests** tab of the View Person form.
   - Click the entry in the list of requests in the **Device Requests** tab of the View Device form.
   - View the screen that appears automatically after you have requested a device, assuming that the request does not need to be approved by another operator first.

2. Click the **View Auth Code** option in the button bar at the bottom of the screen.

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

   If this option is not available, the request is not suitable to be collected using a code; for example, it may be already collected, require activation, or be a bureau request. You can send codes for contact cards, soft certificate packages, Windows Hello, or Microsoft VSCs. You must also make sure that you have the **View Auth Code for Job Collection** option selected for your role in the **Edit Roles** workflow.

   The View Collection Code screen appears:



This authentication code can only be used for collecting requests. Please confirm the following details. This information will be added to the audit record.

Notes

Lifetime *: Expires 2 minutes from request

3. Type any **Notes** you want to store in the audit trail about the operation.

4. From the **Lifetime** drop-down list, select how long you want the code to be valid.

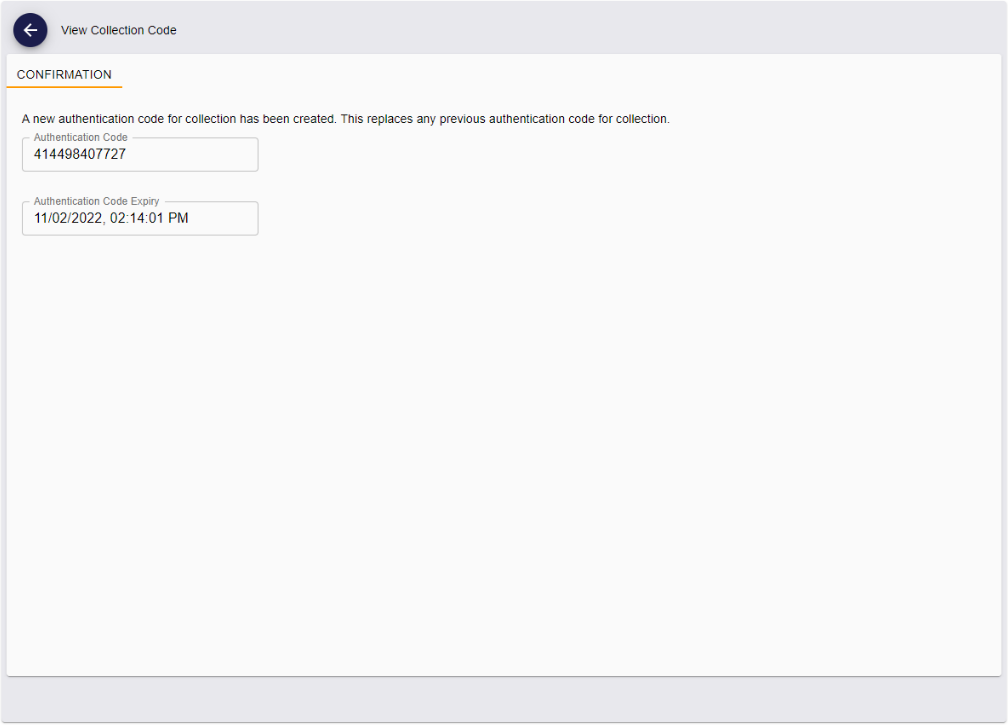
   The options here are determined by the values saved in the **Auth Code Lifetime for Immediate Use** and **Logon Code Lifetime** configuration options; by default, the options are:

   - **Expires 30 days from request** – based on the default **Logon Code Lifetime** setting of 720 hours.
   - **Expires 2 minutes from request** – based on the default **Auth Code Lifetime for Immediate Use** setting of 120 seconds.

   Note: The complexity of the code is determined by the **Generate Code on Request** setting in the credential profile, or if the credential profile does not contain a complexity setting, by the **Auth Code Complexity** configuration option.

5. Click **Save**.

   MyID displays the collection code on screen. You can now provide this to the person who needs to collect their device; for example, you can read the code out over the phone, or send it by a secure chat channel.



A new authentication code for collection has been created. This replaces any previous authentication code for collection.

Authentication Code: 414498407727

Authentication Code Expiry: 11/02/2022, 02:14:01 PM

The person can then use it to collect their device. See the *Using logon codes* section of the ***Administration Guide*** for details of collecting devices using codes In the Self-Service Kiosk, the Self-Service App, and MyID Desktop.

6.5 Assigning a device to a request

You can assign a specific device to an issuance or replacement issuance request. This ensures that the request can be collected using the specified device only.

You can insert the device to assign it to the request, or you can search for the device from the list of devices already known to MyID.

If you no longer want to associate a specific device with a request, you can unassign it.

The device you select must be suitable for collection; it cannot be at a status of Lost or Disposed, and it must be of the correct type (for example, Contact Chip or Contactless) for the credential profile. You cannot assign a device for a printed physical card.

You can assign devices that have already been assigned only if the **Unrestricted Cancellation** option is set in the credential profile; in this case, when you assign the device to the current request, any previous request that had the same device assigned is canceled. Similarly, if the device has already been issued, when you assign the device to the current request, the previously-issued device is canceled.

You can restrict MyID to assign only devices that are known to MyID; that is, they have previously been issued in MyID or had their serial numbers imported. In the credential profile, set the **Only Issue to Known Serial Numbers** option. This affects only assigning devices directly; when you search for a device to assign, MyID returns only those devices already in its database anyway. See the *Importing serial numbers* section in the ***Administration Guide*** for more information.

6.5.1 Assigning a device directly

You can assign a device to a request by inserting the device.

To assign a device directly:

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

   See section *6.1*, *Searching for a request*.

   You can also view a request from any form that displays a link to the request.

   For example:

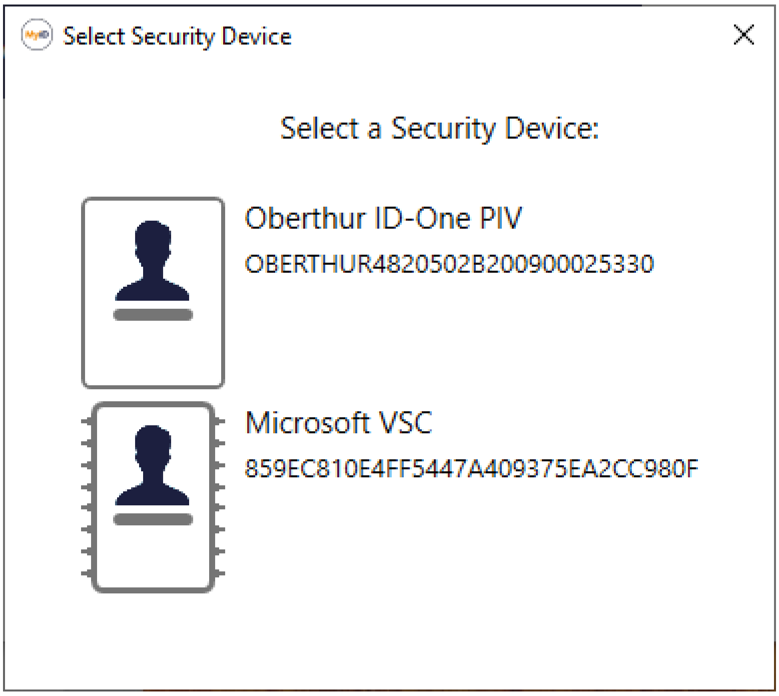
   - Click the entry in the list of requests in the **Requests** tab of the View Person form.
   - Click the entry in the list of requests in the **Device Requests** tab of the View Device form.
   - View the screen that appears automatically after you have requested a device, assuming that the request does not need to be approved by another operator first.

2. Click the **Assign Device (Connect)** option in the button bar at the bottom of the screen.

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

   If this option is not available, the request cannot have a device assigned; for example, it may already have a device assigned.

   The Select Security Device dialog appears.



Select Security Device

Select a Security Device:

Oberthur ID-One PIV
OBERTHUR4820502B200900025330

Microsoft VSC
859EC810E4FF5447A409375EA2CC980F

3. Select the device you want to assign.

   The device is assigned to the request, and its serial number appears in the **Device Serial Number** field on the View Request screen. You can now collect the request only using the specified device.

6.5.2 Searching for a device to assign

Instead of inserting a device to be assigned to a request, you can search for a device that is already known to MyID. To enable this option, you must set the following configuration option:

- **Allow card serial number to be entered during Request Card workflow** – on the **Devices** page of the **Operation Settings** workflow.

To search for a device to assign:

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

   See section *6.1*, *Searching for a request*.

   You can also view a request from any form that displays a link to the request.

   For example:

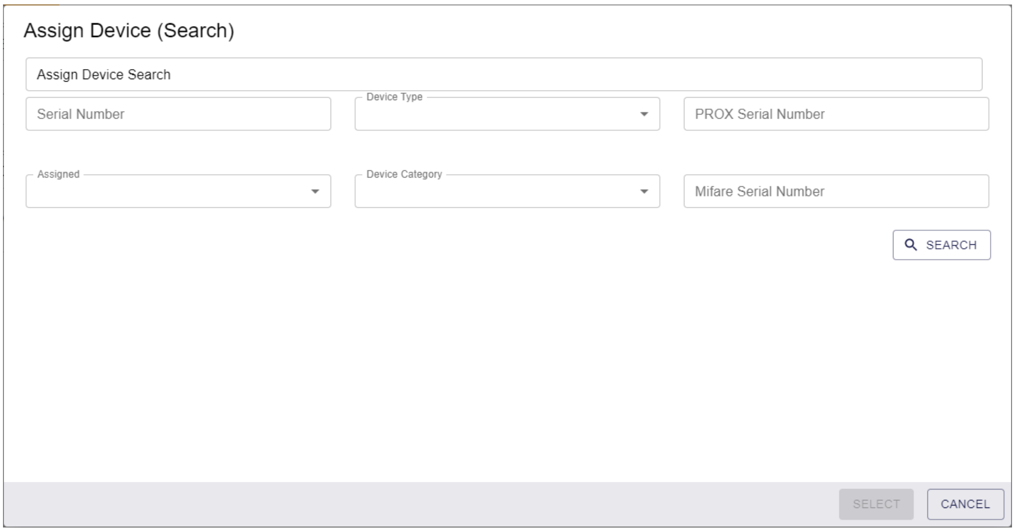
   - Click the entry in the list of requests in the **Requests** tab of the View Person form.
   - Click the entry in the list of requests in the **Device Requests** tab of the View Device form.
   - View the screen that appears automatically after you have requested a device, assuming that the request does not need to be approved by another operator first.

2. Click the **Assign Device (Search)** option in the button bar at the bottom of the screen.

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

   If this option is not available, the request cannot have a device assigned; for example, it may already have a device assigned.

   The device search form appears:



3. Provide your search criteria:

   - **Serial Number** – Type the serial number for the device you want to assign.

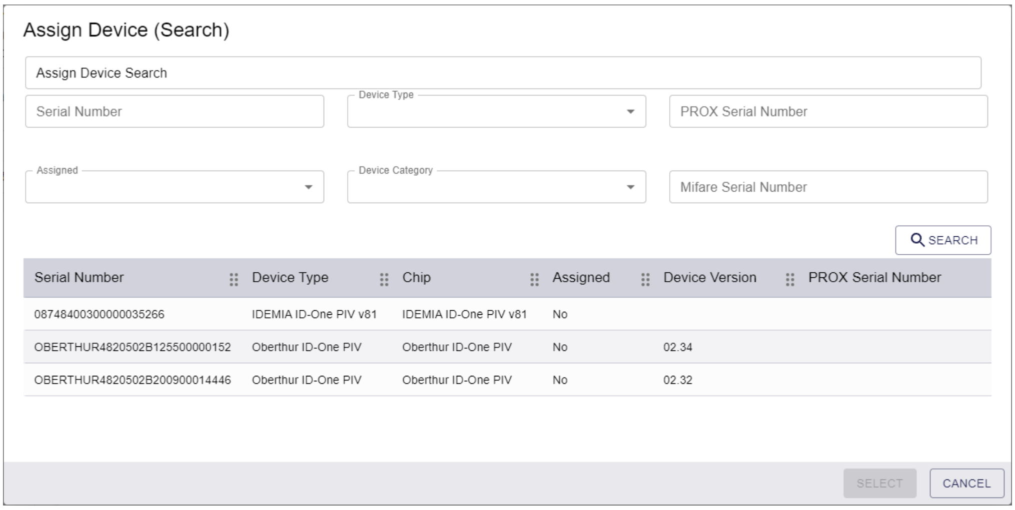
     You can use wildcards in this field; use `*` to indicate multiple characters or `?` to indicate a single character.
   - **Device Type** – Select the type of device from the drop-down list.
   - **PROX Serial Number** – Type the PROX serial number for the device.

- **Assigned** – Select **No** from the drop-down list to restrict the results to devices that are not already assigned.
- **Device Category** – From the drop-down list, select the category of device; for example, **Card**.

  See section *5.3*, *Working with device categories* for more information.
- **Mifare Serial Number** – If your MyID system is configured to recognize MIFARE cards, type the MIFARE serial number of the MIFARE card.

4. Click **Search**.

   The list of available devices appears.



Assign Device (Search)
Assign Device Search
Serial Number
Device Type
PROX Serial Number
Assigned
Device Category
Mifare Serial Number
SEARCH
SELECT
CANCEL

Serial Number	Device Type	Chip	Assigned	Device Version	PROX Serial Number
08748400300000035266	IDEMIA ID-One PIV v81	IDEMIA ID-One PIV v81	No		
OBERTHUR4820502B125500000152	Oberthur ID-One PIV	Oberthur ID-One PIV	No	02.34	
OBERTHUR4820502B200900014446	Oberthur ID-One PIV	Oberthur ID-One PIV	No	02.32	

5. Select the device from the list, then click **Select**.

   The device is assigned to the request, and its serial number appears in the **Device Serial Number** field on the View Request screen. You can now collect the request only using the specified device.

6.5.3 Unassigning a device

If you no longer want to associate a device with a request, you can unassign the device.

To unassign a device:

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

   See section *6.1*, *Searching for a request*.

   You can also view a request from any form that displays a link to the request.

   For example:

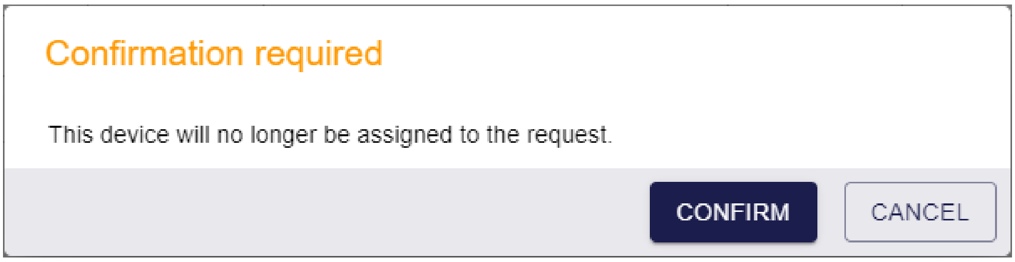
   - Click the entry in the list of requests in the **Requests** tab of the View Person form.
   - Click the entry in the list of requests in the **Device Requests** tab of the View Device form.
   - View the screen that appears automatically after you have requested a device, assuming that the request does not need to be approved by another operator first.

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

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

   If this option is not available, the request cannot have a device assigned; for example, it may already have a device assigned.

   The confirmation dialog appears.

   Confirmation required

   This device will no longer be assigned to the request.

3. Click **Confirm**.

   The device is no longer associated with the request. You can now assign a different device, or collect the request without restrictions on the particular device to use.

6.5.4 Auditing for device assignment

The underlying mechanism for assigning a device to a request is the same whether you search for a device or insert a device. Accordingly, all audit entries for assigning a device (whether through search or directly) use the same operation name "Assign Device (Connect)" in the **Audit Reporting** workflow.

7 Working with reports

The MyID Operator Client provides a series of reports that you can use to interrogate the data held in your MyID system. Some reports act as search options for the main categories; for example, the Devices, Assigned Devices, and Unassigned Devices reports each provide a different way of searching for a device in the Devices category; you can click on the report to open the View Device screen for that device. Other reports are simple lists of information from the MyID database; for example, the Unrestricted Audit Report provides a list of audit entries.

You can download the results of a report as a CSV (comma separated value) file that you can import into a spreadsheet for further sorting and analysis.

Note: It is possible to create customized reports for use in the MyID Operator Client or through the MyID Core API; contact customer support quoting reference SUP-329 for details.

The MyID Operator Client allows you to work with reports in the following ways:

- You can control who has access to individual reports.

  See section *7.1*, *Granting access to reports*.
- You can run reports and download results.

  See section *7.2*, *Running reports*.
- You can view the details of each report.

  See section *7.3*, *Available reports*.

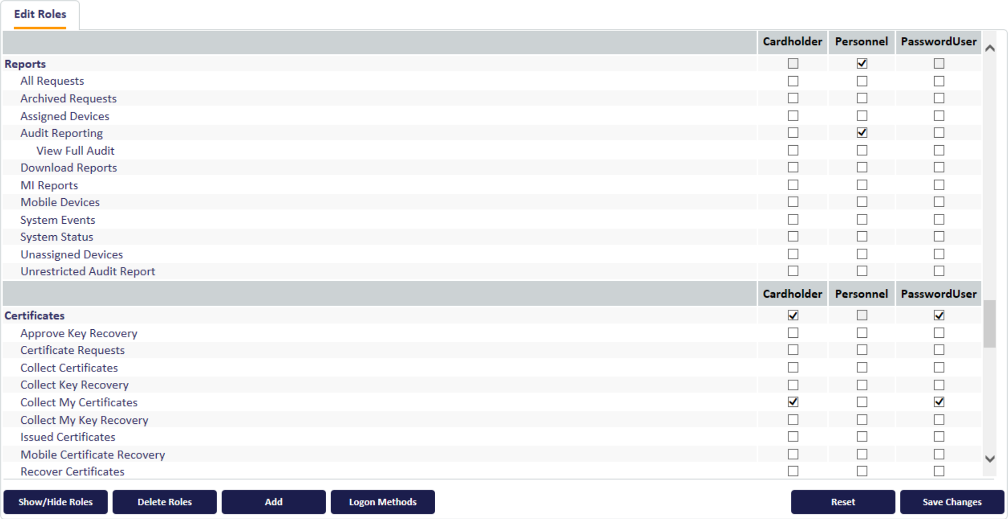
7.1 Granting access to reports

The main category reports are used as the default search options for each category; if you have access to that category, you have access to the report:

- People
- Devices
- Requests

The Assign Device Search report is available if you have access to the Assign Device feature, which is controlled by the **Assign Card** option in the **Edit Roles** workflow.

All other reports are controlled through the **Reports** category within the **Edit Roles** workflow.



	Cardholder	Personnel	PasswordUser
Reports	☐	☑	☐
All Requests	☐	☐	☐
Archived Requests	☐	☐	☐
Assigned Devices	☐	☐	☐
Audit Reporting	☐	☑	☐
View Full Audit	☐	☐	☐
Download Reports	☐	☐	☐
MI Reports	☐	☐	☐
Mobile Devices	☐	☐	☐
System Events	☐	☐	☐
System Status	☐	☐	☐
Unassigned Devices	☐	☐	☐
Unrestricted Audit Report	☐	☐	☐
	Cardholder	**Personnel**	**PasswordUser**
Certificates	☑	☐	☑
Approve Key Recovery	☐	☐	☐
Certificate Requests	☐	☐	☐
Collect Certificates	☐	☐	☐
Collect Key Recovery	☐	☐	☐
Collect My Certificates	☑	☐	☑
Collect My Key Recovery	☐	☐	☐
Issued Certificates	☐	☐	☐
Mobile Certificate Recovery	☐	☐	☐
Recover Certificates	☐	☐	☐

In addition, access to the **Download results** feature is controlled by the **Download Reports** option.

See the *Roles* section in the ***Administration Guide*** for details of using the **Edit Roles** workflow.

7.2 Running reports

To run a report:

1. Click the **Reports** category.
2. From the drop-down list, select the report you want to run.

   See section *7.3*, *Available reports* for information on each report, including details of what search criteria are available, what results are returned, the limit on the number of records returned.
3. Complete the search criteria.
4. Click **Search**.

   The results are displayed. If the report allows it, you can click on a row to display the details of that item; for example, you can click on a record in the Unassigned Devices report to open the View Device screen for that device.

   Click the **Download results** button to download all results (up to the data limit, not restricted by what is currently on screen) to a CSV file in your browser's configured download folder:

   Note: If you have specified any columns on which you want to sort the records, this sort order is applied when downloading the results to a file. See section *3.4.2*, *Sorting* for details of sorting report results. Note, however, that grouping, filtering, and changing the visible columns or their order are not reflected in the downloaded report.

   Access to the **Download results** feature is controlled by the **Download Reports** option in the **Reports** section of the **Edit Roles** workflow.

   There is a default limit of 20,000 results for downloaded reports. Systems that have been customized with Project Designer may have different limits.

   Note: You cannot download the results of an LDAP directory search.

7.2.1 Paging of results

Search results are displayed in pages. Scroll to retrieve the next page of results automatically. The number of displayed results is shown at the top of the form.

If more results are available, the text **(scroll for more)** appears; for example:

```
2008 results - 50 displayed (scroll for more) - 0 selected
```

```
2008 results - 2008 displayed - 0 selected
```

Note: LDAP searches have a default limit of 1000 items; for example:

```
250 displayed (scroll for more) - 0 selected
```

```
1000 displayed - 0 selected
```

7.2.2 Running reports through the MyID Core API

Instead of running reports through the MyID Operator Client, you can run the reports through the `reports` method of the MyID Core API.

To run the report through the API, you need:

- The ID of the report.

  The report ID is listed along with the details of each report in this guide.
- The parameters used for the search criteria.

  For details of the parameters, see the Swagger documentation for the MyID Core API. See the *Accessing the API documentation* section in the ***MyID Core API*** guide for details of viewing the API documentation.

For example, if you want to call the **Available Device Stock** report for a particular stock code and location, you need the ID of the report and the parameters used for stock code and location. In this case, the ID is `290009`, and the parameters are `stockCode` and `location.name`.

For example:

```
https://myserver/rest.core/api/reports/290009?stockCode=Card&location.name
=Headquarters
```

To run the report with no search parameters, use the `q=*` parameter; for example:

```
https://myserver/rest.core/api/reports/290009?q=*
```

Note: Date and time formats are as follows:

`YYYY-MM-DD`

`YYYY-MM-DDTHH:MM:SS`

When URL encoding a request, replace the `:` symbols in the time component with `%3A`.

Examples:

`2023-12-21`

`2023-12-21T21:30:00`

`2023-12-21T21%3A30%3A00`

Results are returned in JSON format, and are paged as they are when running reports within the MyID Operator Client. The JSON output provides a link you can use to obtain the next page of results, if necessary; for example:

```
{
  "op":"nextPage",
  "cat":"page",
  "desc":"Next Page of Results",
  "verb":"GET",
  "href":"reports/290009?stockCode=Card&location.name=Headquarters&page=2"
},
```

To obtain a count of the total number of records, use the `count` endpoint for the report; for example:

```
https://myserver/rest.core/api/reports/290009/count?q=*
```

This returns a count of the total number of records, and indicates whether this total has reached the report data limit (by default, 20,000 records). For example:

```
{
  "recordCount":9520,
  "maxReached":false
}
```

See the *Server-to-server authentication* and *End-user authentication* sections in the ***MyID Core API*** guide for details of authenticating to the API and calling its methods.

7.3 Available reports

This section lists the available reports. Some reports are associated with particular categories, and are available in both their own category and the Reports category, while other reports are available only in the Reports category.

See:

- section *7.3.1*, *People report*.
- section *7.3.2*, *Requests report*.
- section *7.3.3*, *Locations report*.
- section *7.3.4*, *Stock Limits report*.
- section *7.3.5*, *Assigned Devices report*.
- section *7.3.6*, *Device Import Requests report*.
- section *7.3.7*, *Unrestricted Audit Report*.
- section *7.3.8*, *Requests for review report*.
- section *7.3.9*, *Print PIN Mailer report*.
- section *7.3.10*, *Reprint PIN Mailer report*.
- section *7.3.11*, *Person Status Summary report*.
- section *7.3.12*, *Request Fulfillment report*.
- section *7.3.14*, *Devices report*.
- section *7.3.15*, *Archived Requests report*.
- section *7.3.16*, *Mobile Devices report*.
- section *7.3.17*, *All Requests report*.
- section *7.3.18*, *Unassigned Devices report*.
- section *7.3.19*, *Available Device Stock report*.
- section *7.3.20*, *Assign Device Search report*.
- section *7.3.21*, *Awaiting Delivery report*.
- section *7.3.22*, *Device Disposal report*.
- section *7.3.23*, *Certificates report*.
- section *7.3.24*, *Stock Transfers report*.
- section *7.3.25*, *Stock Per Location report*.
- section *7.3.26*, *Additional Identities (AID) report*.
- section *7.3.27*, *Issued devices by category report*.
- section *7.3.28*, *Assigned Devices by Group report*.
- section *7.3.29*, *My Devices report*.
- section *7.3.30*, *SecureVault Usage report*.
- section *7.3.31*, *Passkeys report*.

7.3.1 People report

This is the default search for the People category. It returns all people that match the search criteria.

This report is available automatically if you have access to the People category.

7.3.1.1 Search criteria

You can use the following search criteria:

Field	Description
Name (contains)	Type some characters from the person's name. You cannot use wildcards in this field; it automatically uses fuzzy matching.
Group	Select the group to which the person belongs.
Logon	Type the person's logon name. You can use wildcards.
Employee ID	Type the person's employee ID. You can use wildcards.
Email	Type the person's email address. You can use wildcards.
Access to Operations	Select whether the person has the **Access to Operations** option set to **Restricted**, **Unrestricted**, or **Not Monitored**. For more information, see the *Restricting inactive users* section in the ***Administration Guide***.

Note: When searching a directory, you can use only the **Logon** and **Group** fields.

You can also select the following **Additional search criteria**:

Field	Description
First Name	Type the person's first name. You can use wildcards.
Last Name	Type the person's last name. You can use wildcards. When searching a directory, this field is labeled **Surname**.
Role	Select the person's role from the drop-down list.
SAM Account Name	Type the person's SAM Account Name, which appears on the **Account** tab of the View Person screen. You can use wildcards.
User Principal Name	Type the person's User Principal Name, which appears on the **Account** tab of the View Person screen. You can use wildcards.
User SID Present	Select whether the person has a User Security Identifier. See the *Including user security identifiers in certificates* section in the ***Administration Guide*** for details.
Enabled	Select whether the person's account is enabled.
Group Name	Type the group to which the person belongs. You can use wildcards.

Field	Description
External Reference ID 1	Maps to the `XuSYSExternalReferenceId1` field in the MyID database, which you can use to store a reference to the person's account in an external system. This is the default field to store the Entra ID; see the *Issuing passkeys with Microsoft Entra* section in the ***Passkey Integration Guide***. **Note:** If you search for * the report returns all people who have a value set for **External Reference ID 1**.
External Reference ID 2	Maps to the `XuSYSExternalReferenceId2` field in the MyID database.
External Reference ID 3	Maps to the `XuSYSExternalReferenceId3` field in the MyID database.

Note: When searching a directory, you can use only the **First Name** and **Surname** fields.

7.3.1.2 Report fields

The report contains the following fields:

Field	Description
Logon	The person's logon name.
First Name	The person's first name.
Last Name	The person's last name. When searching a directory, this field is labeled **Surname**.
Group	The group to which the person belongs.
Enabled	Whether the person's account is enabled.

You can click on an item in the list of results to open the View Person screen.

7.3.1.3 Data limit

When searching an LDAP, the report has a default limit of 1000 items; see section *7.2.1*, *Paging of results*.

7.3.1.4 Running the report through the API

The People report has the report ID `100102`.

See section *7.2.2*, *Running reports through the MyID Core API* for more details of running reports through the MyID Core API.

7.3.1.5 Further information

See section *4.1*, *Searching for a person* for more information.

7.3.2 Requests report

This is the default search for the Requests category. It returns all live requests, and excludes any archived requests.

This report is available automatically if you have access to the Requests category.

7.3.2.1 Search criteria

You can use the following search criteria:

Field	Description
Name (contains)	Type some characters from the person's name.
Group	Select the group to which the person belongs.
Credential Profile	From the drop-down list, select the credential profile that was used in the request.
Status	From the drop-down list, select the status of the request. For example, select **Awaiting Issue** to search for requests for devices that are available but have not yet been collected.

You can also select the following **Additional search criteria**:

Field	Description
Logon	Type the logon name of the person.
Type	From the drop-down list, select the type of request; for example, **Issue card task** or **Cancel card task**.
Device Category	From the drop-down list, select the category of device; for example, **Card**. See section *5.3*, *Working with device categories* for more information.
ID	Type the specific internal ID of the request, if you know it. The ID is displayed in the list of search results and on the View Request form.
Label	Type the label applied to the request.
Requested After	Select a date. Only requests made after this date are returned.
Requested Before	Select a date. Only requests made before this date are returned.
Validated After	Select a date. Only requests validated after this date are returned.
Validated Before	Select a date. Only requests validated before this date are returned.
Device Type	From the drop-down list, select the manufacturer and model of device; for example, Oberthur ID-One PIV.

Field	Description
Device Serial Number	Type the serial number for the associated device. You can use wildcards.
Full Name	Type the full name of the person for whom the request was made. You can use wildcards. This differs from **Name (contains)** in that this field is for matching the whole of the name, not only a part of it.
Task Type	Type the type of the request; for example, **Issue card task** or **Cancel card task**. You can use wildcards.

7.3.2.2 Report fields

The report contains the following fields:

Field	Description
ID	The internal ID of the job.
Full Name	The full name of the person for whom the request was made.
Type	The type of request; for example, `Issue card task` or `Apply update`.
Credential Profile	The credential profile associated with the request.
Status	The status of the request; for example, `Awaiting Validation` or `Completed`.
Request Date	The date the request was made.
Label	The label applied to the request, if any.

You can click on an item in the list of results to open the View Request screen.

7.3.2.3 Running the report through the API

The Requests report has the report ID `100406`.

See section *7.2.2*, *Running reports through the MyID Core API* for more details of running reports through the MyID Core API.

7.3.2.4 Further information

See section *6.1*, *Searching for a request* for more information.

7.3.3 Locations report

The Locations report provides a list of each location in the system.

This report is available in the **Reports** category, and is the primary search in the **Locations** category.

7.3.3.1 Search criteria

You can use the following search criteria:

Field	Description
Name	Type the name of the location. You can use wildcards.
Enabled	Select the enabled status of the location from the drop-down list.
Kind	Select the kind of location from the drop-down list.

7.3.3.2 Report fields

The report contains the following fields:

Field	Description
Name	The name of the location.
Enabled	Whether the location is enabled.
Kind	The kind of location.

You can click on an item in the list of results to open the View Location screen.

7.3.3.3 Running the report through the API

The Locations report has the report ID `100702`.

See section *7.2.2*, *Running reports through the MyID Core API* for more details of running reports through the MyID Core API.

7.3.3.4 Further information

See section *9*, *Working with locations* for more information.

7.3.4 Stock Limits report

The Stock Limits report provides a list of the limits set up for stock for each location and stock type.

This report is available in the **Reports** category, and is the primary search in the **Stock Limits** category.

7.3.4.1 Search criteria

You can use the following search criteria:

Field	Description
Location Name	Type the location for the stock limit. You can use wildcards.
Stock Code	Type the stock code for the devices. You can use wildcards.

7.3.4.2 Report fields

The report contains the following fields:

Field	Description
Location Name	The location specified for the stock limit.
Stock Code	The stock code specified for the stock limit.
Minimum Quantity	The minimum number of devices with the specified stock code at the specified location.
Reorder Quantity	The number of devices to reorder when the available stock drops below the minimum quantity.

You can click on an item in the list of results to open the View Stock Limit screen.

7.3.4.3 Running the report through the API

The Stock Limits report has the report ID `100802`.

See section *7.2.2*, *Running reports through the MyID Core API* for more details of running reports through the MyID Core API.

7.3.4.4 Further information

See section *10*, *Working with stock limits* for more information.

7.3.5 Assigned Devices report

This search is an alternative search for the Devices category that returns only assigned devices in the MyID database. Unassigned devices are excluded.

This report is available only if you have been granted access. See section *7.1*, *Granting access to reports* for details.

7.3.5.1 Search criteria

You can use the following search criteria:

Field	Description
Owner Name (contains)	Type part of the device owner's name. You do not have to use wildcards; the search will match any part of the text you enter with the device owner's name.
Group	Select the group to which the device owner belongs.
Credential Profile	Select the credential profile that was used to issue the device from the drop-down list.
Device Type	Select the type of device from the drop-down list.
Device Version	Type the firmware version of the device; this is used to distinguish YubiKey devices.
Process Status	Select the status of the device from the drop-down list; for example, **Active** or **Erased**.
Enabled	Select whether or not the device is enabled from the drop-down list.
Serial Number	Type the serial number for the device. You can use wildcards.
Expires After	Select the date after which the device will expire.
Expires Before	Select the date before which the device will expire.

You can also select the following **Additional search criteria**:

Field	Description
Valid After	Select the date after which the device became valid.
Valid Before	Select the date before which the device became valid.
Chip	Type the chip type for the device; for example, Oberthur ID-One PIV. You can use wildcards.
Device Category	From the drop-down list, select the category of device; for example, **Card**. See section *5.3*, *Working with device categories* for more information.
Enabled (text)	Type whether or not the device is enabled.
Owner	Type the name of the person who is the device owner. This is an alternative to **Owner Name (contains)** that allows you to use wildcards.

7.3.5.2 Report fields

The report contains the following fields:

Field	Description
Owner	The person who owns the device.
Credential Profile	The credential profile used to issue the device.
Device Type	The type of the device.
Device Version	The device firmware version used to distinguish YubiKey devices.
Process Status	The status of the device; for example, `Active` or `PendingActivation`.
Valid From	The validity start date.
Expires	The date the device expires.
Enabled	Whether or not the device is currently enabled.
Serial Number	The serial number of the device.

You can click on an item in the list of results to open the View Device screen.

7.3.5.3 Running the report through the API

The Assigned Devices report has the report ID `290001`.

See section *7.2.2*, *Running reports through the MyID Core API* for more details of running reports through the MyID Core API.

7.3.5.4 Further information

See section *5.1*, *Searching for a device* for more information.

7.3.6 Device Import Requests report

The Device Import Requests report provides a list of device import requests.

This report is available in the **Reports** category, and as an alternative search in the **Requests** category.

7.3.6.1 Search criteria

You can use the following search criteria:

Field	Description
Status	Select the status of the request from the drop-down list.
Label	Type the label you specified when importing the devices. You can use wildcards.
Requested After	Select a start date for the range of dates you want to view.
Requested Before	Select an end date for the range of dates you want to view.
Initiator	Type the logon name for the operator who initiated the import. You can use wildcards.

You can also select the following **Additional search criteria**:

Field	Description
ID	The unique numeric ID of the request.

7.3.6.2 Report fields

The report contains the following fields:

Field	Description
ID	The unique numeric ID of the request.
Initiator	The logon name for the operator who initiated the import.
Status	The status of the request.
Request Date	The date the import was requested.
Label	The label provided when importing the devices.

You can click on an item in the list of results to open the View Request screen.

7.3.6.3 Running the report through the API

The Devices Import Requests report has the report ID `290014`.

See section *7.2.2*, *Running reports through the MyID Core API* for more details of running reports through the MyID Core API.

7.3.6.4 Further information

See section *5.26.1*, *Viewing device import requests* for more information.

7.3.7 Unrestricted Audit Report

This report is available in the Reports category, and provides a list of all audit actions stored in the MyID audit trail. No scope is enforced; you can view a list of the actions carried out by all operators for all target people.

This report is available only if you have been granted access. See section *7.1*, *Granting access to reports* for details.

7.3.7.1 Search criteria

You can use the following search criteria:

Field	Description
After	Select a date. Only audited actions after this date are returned.
Before	Select a date. Only audited actions before this date are returned.
Operation	Select the MyID operation from the drop-down list.
Operator (contains)	Type some characters of the logon name of the operator who carried out the action. You cannot use wildcards in this field; it automatically uses fuzzy matching.
Person (contains)	Type some characters of the logon name of the person who was the target of the action. You cannot use wildcards in this field; it automatically uses fuzzy matching.
Audit Status	Select the status of the audit; for example, you can search for only failures.
Audit Type	Select the type of audit; for example, Audit, Error, or Trace. By default, the report displays all types of audit. As Trace entries are listed on the **Audit Trace** tab of the **View Audit** screen for their parent Audit entry, you are recommended to select **Audit** in the **Audit Type** search criterion, and drill down into the detailed traces from the View Audit screen as required.
Audit ID	Type the ID of the audit entry. You can use wildcards.

You can also select the following **Additional search criteria**:

Field	Description
Operator (Logon Name) (historic)	Type the logon name of the operator who carried out the action. You can use this if the operator's logon name has changed to search for actions carried out under the previous logon name. You can use wildcards. **Note:** Using the **Operator (contains)** field instead searches for the current logon name, but returns all audited actions carried out under all of the operator's logon names.
Person (Logon Name) (historic)	Type the logon name of the person who was the target of the action. You can use this if the person's logon name has changed to search for actions carried out for the previous logon name. You can use wildcards. **Note:** Using the **Person (contains)** field instead searches for the current logon name, but returns all audited actions carried out for all of the person's logon names.
Client Identifier	The client identifier may have been captured for the operator, depending on your system configuration. You can use wildcards. See the *Logging the client IP address and identifier* section in the ***Administration Guide*** for details.
IP Address	The IP address (like the client identifier) may have been captured for the operator, depending on your system configuration. You can use wildcards.

7.3.7.2 Report fields

The report contains the following fields:

Field	Description
Timestamp	The date and time of the action.
End Timestamp	The date and time when the action ends.
Operation	The MyID operation that was carried out.
Operator	The logon name of the operator who carried out the action.
Person	The logon name of the person who was the target of the action.
Message	The message stored in the audit trail for the action.
Audit Status	The status of the action; for example, Success or Failure.
Audit Type	The type of audit; for example, Audit, Error, or Trace.

If you have role permissions to the View Full Audit feature, you can click on an entry in the report to display the View Audit screen. See section *16.1*, *Viewing audit details* for more information. This also provides information, on the **Attribute Changes** tab, about the fields that have changed, as well as their previous and new values.

7.3.7.3 Running the report through the API

The Unrestricted Audit Report has the report ID `290015`.

See section *7.2.2*, *Running reports through the MyID Core API* for more details of running reports through the MyID Core API.

7.3.7.4 Further information

See section *16*, *Working with the audit trail* and the *The audit trail* section in the ***Administration Guide***.

7.3.8 Requests for review report

The Requests for review report provides a list of requests that are awaiting validation.

This report is available in the **Reports** category, and as an alternative search in the **Requests** category.

7.3.8.1 Search criteria

You can use the following search criteria:

Field	Description
Name (contains)	Type some characters from the person's name.
Group	Select the group to which the person belongs.
Credential Profile	From the drop-down list, select the credential profile that was used in the request.

You can also select the following **Additional search criteria**:

Field	Description
Logon	Type the logon name of the person.
Type	From the drop-down list, select the type of request; for example, **IssueCard** or **CancelCard**.
ID	Type the specific internal ID of the request, if you know it. The ID is displayed in the list of search results and on the View Request form.
Label	Type the label applied to the request.
Requested After	Select a date. Only requests made after this date are returned.
Requested Before	Select a date. Only requests made before this date are returned.
Device Type	From the drop-down list, select the manufacturer and model of device; for example, Oberthur ID-One PIV.
Device Serial Number	Type the serial number of the device.
Full Name	Type the full name of the person for whom the request was made. You can use wildcards. This differs from **Name (contains)** in that this field is for matching the whole of the name, not only a part of it.
Task Type	Type the type of the request; for example, **Issue card task** or **Cancel card task**. You can use wildcards.

7.3.8.2 Report fields

The report contains the following fields:

Field	Description
ID	The internal ID of the job.
Full Name	The full name of the person for whom the request was made.
Type	The type of request; for example, `Issue card task` or `Apply update`.
Credential Profile	The credential profile associated with the request.
Status	The status of the request; for example, `Awaiting Validation` or `Completed`.
Request Date	The date the request was made.
Label	The label applied to the request, if any.

You can click on an item in the list of results to open the View Request screen.

7.3.8.3 Running the report through the API

The Requests for review report has the report ID `290025`.

See section *7.2.2*, *Running reports through the MyID Core API* for more details of running reports through the MyID Core API.

7.3.8.4 Further information

See section *6.2*, *Approving, rejecting, and canceling requests* for more information.

7.3.9 Print PIN Mailer report

The Print PIN Mailer report provides a list of all requests for PIN mailer documents that have not yet been printed. These requests are created when you collect a request for a soft certificate package. You can use this report to print PIN mailer documents individually or as a batch.

Once a PIN mailer document has been printed for a soft certificate package, you cannot use the **Print PIN Mailer Document** option again; reprinting PIN mailers is restricted to operators who have permissions to the **Reprint PIN Mailer Document** option.

This report is available in the **Reports** category, and as an alternative search in the **Requests** category.

7.3.9.1 Search criteria

You can use the following search criteria:

Field	Description
Name (contains)	Type some characters from the person's name.
Group	Select the group to which the person belongs.
Credential Profile	From the drop-down list, select the credential profile that was used in the request.

Field	Description
Requested After	Select a date. Only requests made after this date are returned.
Requested Before	Select a date. Only requests made before this date are returned.
Device Serial Number	Type the serial number of the device.

7.3.9.2 Report fields

The report contains the following fields:

Field	Description
ID	The internal ID of the job.
Full Name	The full name of the person for whom the request was made.
Credential Profile	The credential profile associated with the request.
Status	The status of the request; for example, `Created`.
Request Date	The date the request was made.
Serial Number	The serial number of the device.

You can click on an item in the list of results to open the View Request screen, from which you can select the **Print Mailer Document** option; alternatively, you can select multiple items from the list, then from the **Tools** menu select **Print Mailer Document** to print a batch of PIN documents.

Note: You can access the **Tools** menu only if you have a role with the **Tools Menu** option from the **Configuration** section of the **Edit Roles** workflow.

7.3.9.3 Running the report through the API

The Print PIN Mailer report has the report ID `290026`.

See section *7.2.2*, *Running reports through the MyID Core API* for more details of running reports through the MyID Core API.

7.3.9.4 Further information

See section *14.2*, *Printing mailing documents for a soft certificate package* for more information.

7.3.10 Reprint PIN Mailer report

The Reprint PIN Mailer report provides a list of all requests for PIN mailer documents, whether or not they have already been printed. These requests are created when you collect a request for a soft certificate package. You can use this report to reprint PIN mailer documents individually or as a batch.

Once a PIN mailer document has been printed for a soft certificate package, you cannot use the **Print PIN Mailer Document** option again; reprinting PIN mailers is restricted to operators who have permissions to the **Reprint PIN Mailer Document** option.

This report is available in the **Reports** category, and as an alternative search in the **Requests** category.

7.3.10.1 Search criteria

You can use the following search criteria:

Field	Description
Name (contains)	Type some characters from the person's name.
Group	Select the group to which the person belongs.
Credential Profile	From the drop-down list, select the credential profile that was used in the request.
Requested After	Select a date. Only requests made after this date are returned.
Requested Before	Select a date. Only requests made before this date are returned.
Status	The status of the request; for example, `Created` (for new PIN mailer request) or `Completed` (for PIN mailer requests that have already been printed, and can be reprinted only using the Reprint PIN Mailer Document option).
Device Serial Number	Type the serial number of the device.

7.3.10.2 Report fields

The report contains the following fields:

Field	Description
ID	The internal ID of the job.
Full Name	The full name of the person for whom the request was made.
Credential Profile	The credential profile associated with the request.
Status	The status of the request; for example, `Created` or `Completed`.
Request Date	The date the request was made.
Serial Number	The serial number of the device.

You can click on an item in the list of results to open the View Request screen, from which you can select the **Reprint Mailer Document** option; alternatively, you can select multiple items from the list, then from the **Tools** menu select **Reprint Mailer Document** to reprint a batch of PIN documents.

Note: You can access the **Tools** menu only if you have a role with the **Tools Menu** option from the **Configuration** section of the **Edit Roles** workflow.

7.3.10.3 Running the report through the API

The Reprint PIN Mailer report has the report ID `290027`.

See section *7.2.2*, *Running reports through the MyID Core API* for more details of running reports through the MyID Core API.

7.3.10.4 Further information

See section *14.2*, *Printing mailing documents for a soft certificate package* for more information.

7.3.11 Person Status Summary report

This report displays a list of people with summary information about their devices and requests.

This report is available only if you have been granted access. See section *7.1*, *Granting access to reports* for details.

7.3.11.1 Search criteria

You can use the following search criteria:

Field	Description
Name (contains)	Type some characters from the person's name. You cannot use wildcards in this field; it automatically uses fuzzy matching.
Group	Select the group to which the person belongs.
Logon	Type the person's logon name. You can use wildcards.
Employee ID	Type the person's employee ID. You can use wildcards.
Email	Type the person's email address. You can use wildcards.
Enabled	Whether the person's account is enabled.

You can also select the following **Additional search criteria**:

Field	Description
First Name	Type the person's first name. You can use wildcards.
Last Name	Type the person's last name. You can use wildcards. When searching a directory, this field is labeled **Surname**.
Role	Select the person's role from the drop-down list.
SAM Account Name	Type the person's SAM Account Name, which appears on the **Account** tab of the View Person screen. You can use wildcards.
User Principal Name	Type the person's User Principal Name, which appears on the **Account** tab of the View Person screen. You can use wildcards.
User SID Present	Whether the person has a User Security Identifier. See the *Including user security identifiers in certificates* section in the ***Administration Guide*** for details.
Group Name	Type the group to which the person belongs. You can use wildcards.

Note: When searching a directory, you can use only the **First Name** and **Surname** fields.

7.3.11.2 Report fields

The report contains the following fields:

Field	Description
Logon	The person's logon name.
Full Name	The person's full name.
Enabled	Whether the person's account is enabled.
Group	The group to which the person belongs.
Devices	The number of devices the person has owned.
Open Requests	The number of open requests for the person.
Completed Requests	The number of completed requests for the person.
Failed Requests	The number of failed requests for the person.

You can click on an item in the list of results to open the View Person screen.

7.3.11.3 Running the report through the API

The People report has the report ID `290028`.

See section *7.2.2*, *Running reports through the MyID Core API* for more details of running reports through the MyID Core API.

7.3.11.4 Further information

See section *4.1*, *Searching for a person* for more information.

7.3.12 Request Fulfillment report

This report contains device lifecycle requests with device and group information.

This report is available only if you have been granted access. See section *7.1*, *Granting access to reports* for details.

7.3.12.1 Search criteria

You can use the following search criteria:

Field	Description
Name (contains)	Type some characters from the person's name.
Group	Select the group to which the person belongs.
Credential Profile	From the drop-down list, select the credential profile that was used in the request.
Status	From the drop-down list, select the status of the request. For example, select **Awaiting Issue** to search for requests for devices that are available but have not yet been collected.

You can also select the following **Additional search criteria**:

Field	Description
Logon	Type the logon name of the person.
Type	From the drop-down list, select the type of request; for example, **Issue card task** or **Cancel card task**.
Device Category	From the drop-down list, select the category of device; for example, **Card**. See section *5.3*, *Working with device categories* for more information.
ID	Type the specific internal ID of the request, if you know it. The ID is displayed in the list of search results and on the View Request form.
Label	Type the label applied to the request.
Requested After	Select a date. Only requests made after this date are returned.
Requested Before	Select a date. Only requests made before this date are returned.
Validated After	Select a date. Only requests validated after this date are returned.
Validated Before	Select a date. Only requests validated before this date are returned.
Device Type	From the drop-down list, select the manufacturer and model of device; for example, Oberthur ID-One PIV.

Field	Description
Device Serial Number	Type the serial number for the associated device. You can use wildcards.
Full Name	Type the full name of the person for whom the request was made. You can use wildcards. This differs from **Name (contains)** in that this field is for matching the whole of the name, not only a part of it.
Task Type	Type the type of the request; for example, **Issue card task** or **Cancel card task**. You can use wildcards.

7.3.12.2 Report fields

The report contains the following fields:

Field	Description
ID	The internal ID of the job.
Full Name	The full name of the person for whom the request was made.
Group	The group of the person for whom the request was made.
Type	The type of request; for example, `Issue card task` or `Apply update`.
Credential Profile	The credential profile associated with the request.
Status	The status of the request; for example, `Awaiting Validation` or `Completed`.
Request Date	The date the request was made.
Action Date	The date the request was completed.
Device Type	The type of device.
Serial Number	The serial number of the device.

You can click on an item in the list of results to open the View Request screen.

7.3.12.3 Running the report through the API

The Requests report has the report ID `290029`.

See section *7.2.2*, *Running reports through the MyID Core API* for more details of running reports through the MyID Core API.

7.3.12.4 Further information

See section *6.1*, *Searching for a request* for more information.

7.3.13 People with Restricted Access to Operations report

This search is an alternative search for the People category that returns only people who have the **Access to Operations** option set to **Restricted**. It returns all people that match the search criteria.

7.3.13.1 Search criteria

You can use the following search criteria:

Field	Description
Name (contains)	Type some characters from the person's name. You cannot use wildcards in this field; it automatically uses fuzzy matching.
Group	Select the group to which the person belongs.
Logon	Type the person's logon name. You can use wildcards.
Employee ID	Type the person's employee ID. You can use wildcards.
Email	Type the person's email address. You can use wildcards.

You can also select the following **Additional search criteria**:

Field	Description
First Name	Type the person's first name. You can use wildcards.
Last Name	Type the person's last name. You can use wildcards.
Role	Select the person's role from the drop-down list.
SAM Account Name	Type the person's SAM Account Name, which appears on the **Account** tab of the View Person screen. You can use wildcards.
User Principal Name	Type the person's User Principal Name, which appears on the **Account** tab of the View Person screen. You can use wildcards.
User SID Present	Whether the person has a User Security Identifier. See the *Including user security identifiers in certificates* section in the ***Administration Guide*** for details.
Enabled	Whether the person's account is enabled.
Group Name	Type the group to which the person belongs. You can use wildcards.

7.3.13.2 Report fields

The report contains the following fields:

Field	Description
Logon	The person's logon name.
First Name	The person's first name.
Last Name	The person's last name.
Group	The group to which the person belongs.
Enabled	Whether the person's account is enabled.

You can click on an item in the list of results to open the View Person screen.

7.3.13.3 Running the report through the API

The People with Restricted Access to Operations report has the report ID `290030`.

See section *7.2.2*, *Running reports through the MyID Core API* for more details of running reports through the MyID Core API.

7.3.13.4 Further information

See the *Restricting inactive users* section in the ***Administration Guide*** for more information.

7.3.14 Devices report

This report returns all devices in the MyID database, both assigned and unassigned.

This report is available automatically if you have access to the Devices category.

7.3.14.1 Search criteria

You can use the following search criteria:

Field	Description
Owner Name (contains)	Type part of the device owner's name. You do not have to use wildcards; the search will match any part of the text you enter with the device owner's name.
Group	Select the group to which the device owner belongs.
Credential Profile	Select the credential profile that was used to issue the device from the drop-down list.
Device Type	Select the type of device from the drop-down list.
Device Version	Type the firmware version of the device; this is used to distinguish YubiKey devices.
Process Status	Select the status of the device from the drop-down list; for example, **Active** or **Erased**.
Enabled	Select whether or not the device is enabled from the drop-down list.
Serial Number	Type the serial number for the device. You can use wildcards.

You can also select the following **Additional search criteria**:

Field	Description
Chip	Type the chip type for the device; for example, Oberthur ID-One PIV. You can use wildcards.
Valid After	Select the date after which the device became valid.
Valid Before	Select the date before which the device became valid.
Expires After	Select the date after which the device will expire.
Expires Before	Select the date before which the device will expire.
Device Category	From the drop-down list, select the category of device; for example, **Card**. See section *5.3*, *Working with device categories* for more information.
HID Serial Number	Type the HID serial number for the device.
Enabled (text)	Select whether or not the device is enabled.
Owner	Type the name of the person who is the device owner. This is an alternative to **Owner Name (contains)** that allows you to use wildcards.
MIfare serial number	Type the MIFARE serial number for the device.

7.3.14.2 Report fields

The report contains the following fields:

Field	Description
Serial Number	The serial number of the device.
Device Type	The type of the device.
Device Version	Type the firmware version of the device; this is used to distinguish YubiKey devices.
Process Status	The status of the device; for example, `Active` or `PendingActivation`.
Owner	The person who owns the device.
Credential Profile	The credential profile used to issue the device.
Enabled	Whether or not the device is currently enabled.
Valid From	The validity start date.
Expires	The date the device expires.
HID Serial Number	The HID serial number for the device.

You can click on an item in the list of results to open the View Device screen.

7.3.14.3 Running the report through the API

The Devices report has the report ID `100202`.

See section *7.2.2*, *Running reports through the MyID Core API* for more details of running reports through the MyID Core API.

7.3.14.4 Further information

See section *5.1*, *Searching for a device* for more information.

7.3.15 Archived Requests report

This report is available in the Reports category, and returns only requests that have been archived. No scope is enforced; you can view a list of the requests made by all operators for all target people.

Note: This report provides only a list of the requests. You cannot click on a record to view more details of the request.

This report is available only if you have been granted access. See section *7.1*, *Granting access to reports* for details.

7.3.15.1 Search criteria

You can use the following search criteria:

Field	Description
Group	Select the group to which the person belongs.
Logon	Type the logon name of the person.
Credential Profile	From the drop-down list, select the credential profile that was used in the request.
Status	From the drop-down list, select the status of the request. For example, select **Awaiting Issue** to search for requests for devices that are available but have not yet been collected.

You can also select the following **Additional search criteria**:

Field	Description
Type	From the drop-down list, select the type of request; for example, **IssueCard** or **CancelCard**.
ID	Type the specific internal ID of the request, if you know it. The ID is displayed in the list of search results and on the View Request form.
Label	Type the label applied to the request.
Requested After	Select a date. Only requests made after this date are returned.
Requested Before	Select a date. Only requests made before this date are returned.
Validated After	Select a date. Only requests validated after this date are returned.
Validated Before	Select a date. Only requests validated before this date are returned.
Device Type	From the drop-down list, select the manufacturer and model of device; for example, Oberthur ID-One PIV.
Device Serial Number	Type the serial number of the device.

7.3.15.2 Report fields

The report contains the following fields:

Field	Description
ID	The internal ID of the job.
Full Name	The full name of the person for whom the request was made.
Type	The type of request; for example, `Issue card task` or `Apply update`.
Credential Profile	The credential profile associated with the request.
Status	The status of the request; for example, `Completed`.
Request Date	The date the request was made.
Label	The label applied to the request, if any.

7.3.15.3 Running the report through the API

The Archived Requests report has the report ID `290016`.

See section *7.2.2*, *Running reports through the MyID Core API* for more details of running reports through the MyID Core API.

7.3.15.4 Further information

See the *Archiving jobs* section in the ***Advanced Configuration Guide***.

If you are using a separate archive database, and you do not see archived information in this report, make sure you have updated the `ArchiveDatabaseLocation` function and the `mis_PIVArchivedRequests` and `mis_PIVAllRequests` views; see the *Setting up a separate database for the jobs archive* section in the ***Advanced Configuration Guide***for details.

7.3.16 Mobile Devices report

This search is an alternative search for the Devices category that returns details of issued mobile devices.

This report is available only if you have been granted access. See section *7.1*, *Granting access to reports* for details.

7.3.16.1 Search criteria

You can use the following search criteria:

Field	Description
Owner Name (contains)	Type part of the device owner's name. You do not have to use wildcards; the search will match any part of the text you enter with the device owner's name.
Group	Select the group to which the device owner belongs.
Credential Profile	Select the credential profile that was used to issue the device from the drop-down list.
Process Status	Select the status of the mobile device element that holds the certificates. from the drop-down list; for example, **Active** or **Erased**.
Enabled	Select whether or not the mobile device element is enabled from the drop-down list.

You can also select the following **Additional search criteria**:

Field	Description
Valid After	Select the date after which the device became valid.
Valid Before	Select the date before which the device became valid.
Expires After	Select the date after which the device will expire.
Expires Before	Select the date before which the device will expire.
Device Category	From the drop-down list, select the category of device; for example, **Mobile** or **Mobile Identity Document**. See section *5.3*, *Working with device categories* for more information.
Mobile ID	The External MDM identifier for the mobile device. You can use wildcards.
Model	The reported mobile device model. You can use wildcards.
OS	The reported mobile OS and version. You can use wildcards.
App Name	The reported app name. You can use wildcards.
Enabled (text)	Select whether or not the device is enabled.
Owner	Type the name of the person who is the device owner. This is an alternative to **Owner Name (contains)** that allows you to use wildcards.

7.3.16.2 Report fields

The report contains the following fields:

Field	Description
Process Status	The device status for the mobile device element that holds the certificates.
Owner	The full name of the device owner.
Credential Profile	The credential profile used to issue the mobile device.
Enabled	Whether the mobile device element is enabled.
Valid From	The validity start date.
Expires	The date the device expires.
Device Category	The category of the device; for example, **Mobile**.
Mobile ID	The External MDM identifier for the mobile device.
Model	The reported mobile device model.
OS	The reported mobile OS and version.

You can click on an item in the list of results to open the View Device screen for the mobile device element that holds the issued certificates.

7.3.16.3 Running the report through the API

The Mobile Devices report has the report ID `290008`.

See section *7.2.2*, *Running reports through the MyID Core API* for more details of running reports through the MyID Core API.

7.3.16.4 Further information

See section *5.1*, *Searching for a device* for more information.

7.3.17 All Requests report

This report is available in the Reports category, and returns all live and archived requests. No scope is enforced; you can view a list of the requests made by all operators for all target people.

Note: This report provides only a list of the requests. You cannot click on a record to view more details of the request.

This report is available only if you have been granted access. See section *7.1*, *Granting access to reports* for details.

7.3.17.1 Search criteria

You can use the following search criteria:

Field	Description
Group	Select the group to which the person belongs.
Logon	Type the logon name of the person.
Credential Profile	From the drop-down list, select the credential profile that was used in the request.
Status	From the drop-down list, select the status of the request. For example, select **Awaiting Issue** to search for requests for devices that are available but have not yet been collected.

You can also select the following **Additional search criteria**:

Field	Description
Type	From the drop-down list, select the type of request; for example, **IssueCard** or **CancelCard**.
ID	Type the specific internal ID of the request, if you know it. The ID is displayed in the list of search results and on the View Request form.
Label	Type the label applied to the request.
Requested After	Select a date. Only requests made after this date are returned.
Requested Before	Select a date. Only requests made before this date are returned.
Validated After	Select a date. Only requests validated after this date are returned.
Validated Before	Select a date. Only requests validated before this date are returned.
Device Type	From the drop-down list, select the manufacturer and model of device; for example, Oberthur ID-One PIV.
Device Serial Number	Type the serial number of the device.

7.3.17.2 Report fields

The report contains the following fields:

Field	Description
ID	The internal ID of the job.
Full Name	The full name of the person for whom the request was made.
Type	The type of request; for example, `Issue card task` or `Apply update`.
Credential Profile	The credential profile associated with the request.
Status	The status of the request; for example, `Awaiting Validation` or `Completed`.
Request Date	The date the request was made.
Label	The label applied to the request, if any.

7.3.17.3 Running the report through the API

The All Requests report has the report ID `290017`.

See section *7.2.2*, *Running reports through the MyID Core API* for more details of running reports through the MyID Core API.

7.3.17.4 Further information

See the *Archiving jobs* section in the ***Advanced Configuration Guide*** for information on archiving request jobs, and section *6.1*, *Searching for a request* for more information about requests.

If you are using a separate archive database, and you do not see archived information in this report, make sure you have updated the `ArchiveDatabaseLocation` function and the `mis_PIVArchivedRequests` and `mis_PIVAllRequests` views; see the *Setting up a separate database for the jobs archive* section in the ***Advanced Configuration Guide***for details.

7.3.18 Unassigned Devices report

This search is an alternative search for the Devices category that returns only unassigned devices in the MyID database. Assigned devices are excluded.

This report is available only if you have been granted access. See section *7.1*, *Granting access to reports* for details.

7.3.18.1 Search criteria

You can use the following search criteria:

Field	Description
Serial Number	Type the serial number for the device. You can use wildcards.
Device Type	Select the type of device from the drop-down list.
Revocation Reason	Select the reason the device is no longer assigned to a person from the drop-down list; for example, **Lost** or **Damaged**.
Import Label	The label assigned to the device at import. See section *5.24*, *Importing a range of devices*.

You can also select the following **Additional search criteria**:

Field	Description
Device Category	From the drop-down list, select the category of device; for example, **Card**. See section *5.3*, *Working with device categories* for more information.
Is Assigned to Transfer	Select whether the device has been assigned to a transfer. See section *11.4*, *Adding devices to a stock transfer*.

7.3.18.2 Report fields

The report contains the following fields:

Field	Description
Serial Number	The serial number of the device.
Device Type	The type of the device.
Previously Assigned	Whether the device was previously assigned to a person.
Revocation Reason	The reason the device is no longer assigned to a person.
Import Label	The label assigned to the device at import.

You can click on an item in the list of results to open the View Device screen.

7.3.18.3 Running the report through the API

The Unassigned Devices report has the report ID `290005`.

See section *7.2.2*, *Running reports through the MyID Core API* for more details of running reports through the MyID Core API.

7.3.18.4 Further information

See section *5.1*, *Searching for a device* for more information.

7.3.19 Available Device Stock report

The Available Device Stock report provides a list of each device in the system available for stock transfer; that is, not currently issued and not currently assigned to a stock transfer. This report is available only if you have been granted access. See section *7.1*, *Granting access to reports* for details.

This report is available in the **Reports** category, and as an alternative search in the **Devices** category.

7.3.19.1 Search criteria

You can use the following search criteria:

Field	Description
Import Label	Type the label assigned when the devices were imported. You can use wildcards.
Stock Code	Type the stock code for the devices. You can use wildcards.
Location	Type the location where the device is located. You can use wildcards.

You can also select the following **Additional search criteria**:

Field	Description
Device Type	Select the type of device from the drop-down list.
From Serial Number	Type the first serial number you want to return.
To Serial Number	Type the last serial number you want to return.

7.3.19.2 Report fields

The report contains the following fields:

Field	Description
Serial Number	The serial number of the device.
Device Type	The type of the device; for example, **Contactless Card**.
Device Category	The category of the device; for example, **Card**. See section *5.3*, *Working with device categories* for more information.
Import Label	The import label added when the device was imported.
Stock Code	The stock code assigned to the device.
Location	The location where the device is located.

You can click on an item in the list of results to open the View Device screen.

Select one or more items in the list, then select **Transfer** from the **Tools** menu to allocate the selected devices to a stock transfer.

Note: You can access the **Tools** menu only if you have a role with the **Tools Menu** option from the **Configuration** section of the **Edit Roles** workflow.

7.3.19.3 Running the report through the API

The Available Device Stock report has the report ID `290009`.

See section *7.2.2*, *Running reports through the MyID Core API* for more details of running reports through the MyID Core API.

7.3.19.4 Further information

See section *11.4*, *Adding devices to a stock transfer* for more information.

7.3.20 Assign Device Search report

This search is an alternative search for the Devices category that is designed primarily to search for devices that you can assign to a request.

This report is available if you have access to the Assign Device feature.

7.3.20.1 Search criteria

You can use the following search criteria:

Field	Description
Serial Number	Type the serial number for the device. You can use wildcards.
Device Type	Select the type of device from the drop-down list.
PROX Serial Number	Type the PROX serial number for the device.
Assigned	Select whether the devices are already assigned.

You can also select the following **Additional search criteria**:

Field	Description
Device Category	From the drop-down list, select the category of device; for example, **Card**. See section *5.3*, *Working with device categories* for more information.
MiFare Serial Number	If your MyID system is configured to recognize MIFARE cards, type the MIFARE serial number of the MIFARE card.

7.3.20.2 Report fields

The report contains the following fields:

Field	Description
Serial Number	The serial number of the device.
Device Type	The type of the device.
Chip	The device chip type.
Assigned	Whether the device is already assigned.
Device Version	The device firmware version used to distinguish YubiKey devices.
PROX Serial Number	The PROX serial number of the device, if any.
MiFare Serial Number	The MIFARE serial number of the device, if any.

You can click on an item in the list of results to open the View Device screen.

7.3.20.3 Running the report through the API

The Assign Device Search report has the report ID `290006`.

See section *7.2.2*, *Running reports through the MyID Core API* for more details of running reports through the MyID Core API.

7.3.20.4 Further information

See section *5.1*, *Searching for a device* and section *6.5*, *Assigning a device to a request* for more information.

7.3.21 Awaiting Delivery report

This search is an alternative search for the Devices category that returns only devices that are awaiting delivery.

This report is available only if you have been granted access. See section *7.1*, *Granting access to reports* for details.

7.3.21.1 Search criteria

You can use the following search criteria:

Field	Description
Owner Name (contains)	Type part of the device owner's name. You do not have to use wildcards; the search will match any part of the text you enter with the device owner's name.
Group	Select the group to which the device owner belongs.
Credential Profile	Select the credential profile that was used to issue the device from the drop-down list.
Device Type	Select the type of device from the drop-down list.
Process Status	Select the status of the device from the drop-down list; for example, **Active** or **Erased**.
Enabled	Select whether or not the device is enabled from the drop-down list.
Serial Number	Type the serial number for the device. You can use wildcards.

You can also select the following **Additional search criteria**:

Field	Description
Chip	Type the chip type for the device; for example, Oberthur ID-One PIV. You can use wildcards.
Valid After	Select the date after which the device became valid.
Valid Before	Select the date before which the device became valid.
Expires After	Select the date after which the device will expire.
Expires Before	Select the date before which the device will expire.
Device Category	From the drop-down list, select the category of device; for example, **Card**. See section *5.3*, *Working with device categories* for more information.

7.3.21.2 Report fields

The report contains the following fields:

Field	Description
Serial Number	The serial number of the device.
Device Type	The type of the device.
Credential Profile	The credential profile used to issue the device.

Field	Description
Owner	The person who owns the device.
Job Status	The status of the device; for example, `Awaiting Delivery`.
Request Date	The date the device was requested.
Label	The label applied to the activation job for the device.

You can click on an item in the list of results to open the View Device screen.

7.3.21.3 Running the report through the API

The Awaiting Delivery report has the report ID `290023`.

See section *7.2.2*, *Running reports through the MyID Core API* for more details of running reports through the MyID Core API.

7.3.21.4 Further information

See section *5.27*, *Accepting delivery for a device* for more information.

7.3.22 Device Disposal report

This search is an alternative search for the Devices category that displays devices and their disposal status.

This report is available only if you have been granted access. See section *7.1*, *Granting access to reports* for details.

7.3.22.1 Search criteria

You can use the following search criteria:

Field	Description
Device Disposal	Select the status of the device disposal.
Revocation Reason	Select the revocation reason that was selected when the device was canceled or erased.

You can also select the following **Additional search criteria**:

Field	Description
Group Name	Select the group to which the device owner belongs.
Owner Logon Name	Type the logon name of the device owner. You can use wildcards.
Serial Number	Type the serial number for the device. You can use wildcards.
Device Type	Select the device type.
Expires After	Select a date to filter the expiry dates for the devices.
Expires Before	Select a date to filter the expiry dates for the devices.

7.3.22.2 Report fields

The report contains the following fields:

Field	Description
Owner	The person who owns the device.
Serial Number	The serial number of the device.
Device Type	The type of the device.
Expires	The date the device expires.
Disposal Status	The disposal status of the device.
Revocation Reason	The reason provided when canceling or erasing the device.

You can click on an item in the list of results to open the View Device screen.

7.3.22.3 Running the report through the API

The Device Disposal report has the report ID `290020`.

See section *7.2.2*, *Running reports through the MyID Core API* for more details of running reports through the MyID Core API.

7.3.22.4 Further information

See section *5.20*, *Disposing of a device* for more information about device disposal.

7.3.23 Certificates report

This is the default search for the Certificates category. It returns all certificates in the MyID database.

This report is available automatically if you have access to the Certificates category.

7.3.23.1 Search criteria

You can use the following search criteria:

Field	Description
Issued To	Type the logon name of the person to whom the certificate was issued.
Certificate Authority	Select the certificate authority that was used to issue the certificate.
Certificate Status	Select the status of the certificate.
Certificate Serial Number	Type the serial number of the certificate. You can use wildcards.
Issued After	Select the date after which the certificate was issued.
Issued Before	Select the date before which the certificate was issued.
Expiry Date After	Select the date after which the certificate expires.
Expiry Date Before	Select the date before which the certificate expires.
Maximum Days to Expiry	Type the maximum number of days before the certificate expires; for example, type `30` to search for certificates that expire in the next 30 days.
User DN	Type the user DN associated with the certificate. You can use wildcards.
User SID Present	Select whether the certificate has a User Security Identifier associated with it. See the *Including user security identifiers in certificates* section in the ***Administration Guide*** for details.
User SID	Type the User Security Identifier associated with the certificate. You can use wildcards.

You can also select the following **Additional search criteria**:

Field	Description
ID	The MyID internal unique ID of the certificate.

7.3.23.2 Report fields

The report contains the following fields:

Field	Description
ID	The MyID internal unique ID of the certificate.
Issued To	The logon name of the person to whom the certificate was issued.
Certificate Policy	The certificate policy that was used to issue the certificate.

Field	Description
Serial Number	The certificate's serial number.
Date Issued	The date the certificate was issued.
Expiry Date	The certificate expiry date.
Status	The status of the certificate; for example, `Issued` or `Revoked`.
User DN	The user DN associated with the certificate.
Certificate Authority	The certificate authority that was used to issue the certificate.

You can click on an item in the list of results to open the View Certificate screen.

7.3.23.3 Running the report through the API

The Certificates report has the report ID `101110`.

See section *7.2.2*, *Running reports through the MyID Core API* for more details of running reports through the MyID Core API.

7.3.23.4 Further information

See section *13.1*, *Viewing a certificate* for more information.

7.3.24 Stock Transfers report

The Stock Transfers report provides a list of the stock transfers in the system.

This report is available in the **Reports** category, and is the primary search in the **Stock Transfers** category.

7.3.24.1 Search criteria

You can use the following search criteria:

Field	Description
From Location	Type the location from which stock is being transferred. You can use wildcards.
To Location	Type the location to which stock is being transferred. You can use wildcards.
Stock Code	Type the stock code for the devices being transferred. You can use wildcards.

You can also select the following **Additional search criteria**:

Field	Description
Quantity	Type the quantity of the stock transfer.
Date Created After	Select a creation date to filter the list of stock transfers.
Date Created Before	Select a creation date to filter the list of stock transfers.
Date Updated After	Select an update date to filter the list of stock transfers.
Date Updated Before	Select an update date to filter the list of stock transfers.

7.3.24.2 Report fields

The report contains the following fields:

Field	Description
From Location	The location from which stock is being transferred.
To Location	The location to which stock is being transferred.
Stock Code	The stock code for the devices being transferred.
Quantity	The quantity of stock being transferred.
Status	The status of the stock transfer.
Date Created	The date the stock transfer was created.
Date Updated	The date the stock transfer was updated.

You can click on an item in the list of results to open the View Transfer screen.

7.3.24.3 Running the report through the API

The Stock Transfers report has the report ID `101202`.

See section *7.2.2*, *Running reports through the MyID Core API* for more details of running reports through the MyID Core API.

7.3.24.4 Further information

See section *11*, *Working with stock transfers* for more information.

7.3.25 Stock Per Location report

The Stock Per Location report provides a list of the available stock for each location and stock type (that is, devices not currently issued and not currently assigned to a stock transfer), along with the stock limits set up.

This report is available in the **Reports** category.

7.3.25.1 Search criteria

You can use the following search criteria:

Field	Description
Location Name	Type the location for the available stock. You can use wildcards.
Stock Code	Type the stock code for the devices. You can use wildcards.

7.3.25.2 Report fields

The report contains the following fields:

Field	Description
Location Name	The location specified for the stock limit.
Stock Code	The stock code specified for the stock limit.
Unallocated Devices	The number of unallocated devices; that is, devices not currently issued and not currently assigned to a stock transfer.
Minimum Quantity	The minimum number of devices with the specified stock code at the specified location.
Reorder Quantity	The number of devices to reorder when the available stock drops below the minimum quantity.

7.3.25.3 Running the report through the API

The Stock Per Location report has the report ID `290010`.

See section *7.2.2*, *Running reports through the MyID Core API* for more details of running reports through the MyID Core API.

7.3.25.4 Further information

See section *10.5*, *Checking stock limits* for more information.

7.3.26 Additional Identities (AID) report

This search is an alternative search for the People category that returns a list of additional identities.

This report is available only if you have been granted access. See section *7.1*, *Granting access to reports* for details.

7.3.26.1 Search criteria

You can use the following search criteria:

Field	Description
Group	Select the group to which the person belongs.
Logon	Type the person's logon name. You can use wildcards.
AID UPN	Type the additional identity User Principal Name. You can use wildcards.
AID Email	Type the additional identity email. You can use wildcards.
Certificate Policy	Select the certificate policy from the drop-down list. Only certificate policies that support additional identity mapping are available for selection. Leave blank for any certificate policy.

Note: You can search only the MyID database using this report; you cannot search a directory.

You can also select the following **Additional search criteria**:

Field	Description
First Name	Type the person's first name. You can use wildcards. This field (along with **Last Name** and **Full Name**) is the name of the person who has the additional identity, not the name of the additional identity.
Last Name	Type the person's last name. You can use wildcards.
Full Name	Type the person's full name. You can use wildcards.
AID SID Present	Controls whether additional identities with or without a user security identifier are displayed. • Yes – display only additional identities with a user security identifier. • No – display only additional identities that do not have a user security identifier.
AID DN	Type the additional identity distinguished name. You can use wildcards.
AID User SID	Type the additional identity user security identifier (user SID). You can use wildcards.

7.3.26.2 Report fields

The report contains the following fields:

Field	Description
Logon	The person's logon name.
AID UPN	The additional identity User Principal Name.
AID Email	The additional identity email.

Field	Description
Certificate Policy	The certificate policy used to issue the additional identity certificate.
AID DN	The additional identity distinguished name.
AID User SID	The additional identity user security identifier (user SID).

You can click on an item in the list of results to open the View Person screen for the owner of the additional identity. From there, you can use the **Additional Identities** tab to work with that person's additional identities.

7.3.26.3 Running the report through the API

The Additional Identities (AID) report has the report ID `290013`.

See section *7.2.2*, *Running reports through the MyID Core API* for more details of running reports through the MyID Core API.

7.3.26.4 Further information

See section *4.1*, *Searching for a person* for more information.

For information about additional identities, see section *12*, *Working with additional identities*.

7.3.27 Issued devices by category report

The Issued devices by category report allows you to display totals of issued types of devices, detailing their categories.

This report is available only if you have been granted access. See section *7.1*, *Granting access to reports* for details.

7.3.27.1 Search criteria

You can use the following search criteria:

Field	Description
Device Category	Select the category you want to view from the drop-down list, or select All to view all categories.

7.3.27.2 Report fields

The report contains the following fields:

Field	Description
Device Category	The category of device.
Device Type	The type of device.
Count	The number of issued devices for the device type.
Consumes device licenses	Whether the type of device consumes licenses. A single mobile device may contain multiple logical devices (for example, a `MyIDIdentityAgent` device type and a `Android PKCS` device type) but only one logical device for each mobile device counts towards the license total; in this case, the `MyIDIdentityAgent` device type consumes a license, but the `Android PKCS` device type does not.

7.3.27.3 Running the report through the API

The Issued devices by category report has the report ID `290022`.

See section *7.2.2*, *Running reports through the MyID Core API* for more details of running reports through the MyID Core API.

7.3.27.4 Further information

See section *5.3*, *Working with device categories* for more information about device categories.

7.3.28 Assigned Devices by Group report

The Assigned Devices by Group report allows you to manage groups that have limited license settings.

This report is available only if you have been granted access. See section *7.1*, *Granting access to reports* for details.

7.3.28.1 Search criteria

You can use the following search criteria:

Field	Description
Group	Select the group to which the device owner belongs.
Credential Profile	Select the credential profile that was used to issue the device from the drop-down list.

7.3.28.2 Report fields

The report contains the following fields:

Field	Description
Group	The name of the group.
Parent Group	The name of the group's parent.
Group Device Assignment End Date	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.
Group Max No. of Assigned Devices	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.
Credential Profile	The credential profile used to assign devices.
Assigned Devices	The number of assigned devices.

7.3.28.3 Running the report through the API

The Assigned Devices by Group report has the report ID `290024`.

See section *7.2.2*, *Running reports through the MyID Core API* for more details of running reports through the MyID Core API.

7.3.28.4 Further information

See the *Controlling device assignments for groups* section in the ***Administration Guide*** for details.

7.3.29 My Devices report

This report returns all devices in the MyID database that currently belong to the logged-in user.

This report is available only if you have been granted access. See section *7.1*, *Granting access to reports* for details.

7.3.29.1 Search criteria

You can use the following search criteria:

Field	Description
Owner Name (contains)	No applicable. The owner is always your own account.
Group	Select the group to which the device owner belongs.
Credential Profile	Select the credential profile that was used to issue the device from the drop-down list.
Device Type	Select the type of device from the drop-down list.
Device Version	Type the firmware version of the device; this is used to distinguish YubiKey devices.
Process Status	Select the status of the device from the drop-down list; for example, **Active** or **Erased**.
Enabled	Select whether or not the device is enabled from the drop-down list.
Serial Number	Type the serial number for the device. You can use wildcards.

You can also select the following **Additional search criteria**:

Field	Description
Chip	Type the chip type for the device; for example, Oberthur ID-One PIV. You can use wildcards.
Valid After	Select the date after which the device became valid.
Valid Before	Select the date before which the device became valid.
Expires After	Select the date after which the device will expire.
Expires Before	Select the date before which the device will expire.
Device Category	From the drop-down list, select the category of device; for example, **Card**. See section *5.3*, *Working with device categories* for more information.
HID Serial Number	Type the HID serial number for the device.
Owner	Type the name of the person who is the device owner. This is an alternative to **Owner Name (contains)** that allows you to use wildcards.
MIfare serial number	Type the MIFARE serial number for the device.

7.3.29.2 Report fields

The report contains the following fields:

Field	Description
Serial Number	The serial number of the device.
Device Type	The type of the device.
Device Version	Type the firmware version of the device; this is used to distinguish YubiKey devices.
Process Status	The status of the device; for example, `Active` or `PendingActivation`.
Owner	The person who owns the device.
Credential Profile	The credential profile used to issue the device.
Enabled	Whether or not the device is currently enabled.
Valid From	The validity start date.
Expires	The date the device expires.
HID Serial Number	The HID serial number for the device.

You can click on an item in the list of results to open the View Device screen.

7.3.29.3 Running the report through the API

The Devices report has the report ID `290031`.

See section *7.2.2*, *Running reports through the MyID Core API* for more details of running reports through the MyID Core API.

7.3.29.4 Further information

See section *5.1*, *Searching for a device* for more information.

7.3.30 SecureVault Usage report

This report is available in the Reports category, and returns a count of the number of keys archived in MyID SecureVault.

This report is available only if you have been granted access. See section *7.1*, *Granting access to reports* for details.

7.3.30.1 Search criteria

There are no search criteria for this report.

7.3.30.2 Report fields

The report contains the following fields:

Field	Description
Vault Name	The name of the MyID SecureVault instance. Currently, you can use only a single instance of MyID SecureVault with MyID CMS.
Keys	The number of keys archived in MyID SecureVault.

7.3.30.3 Running the report through the API

The All Requests report has the report ID `290037`.

See section *7.2.2*, *Running reports through the MyID Core API* for more details of running reports through the MyID Core API.

7.3.30.4 Further information

See the *MyID SecureVault* section in the ***Administration Guide***.

7.3.31 Passkeys report

The Passkeys report provides a list of passkeys in your system, including details of the authentication server (for example, Microsoft Entra) used to issue the devices.

This report is available in the **Reports** category, and as an alternative search in the **Devices** category.

You must use the **Edit Roles** workflow to provide access to this report.

7.3.31.1 Search criteria

You can use the following search criteria:

Field	Description
Owner Name (contains)	Type part of the device owner's name. You do not have to use wildcards; the search will match any part of the text you enter with the device owner's name.
Group	Select the group to which the device owner belongs.
Credential Profile	Select the credential profile that was used to issue the device from the drop-down list.
Authentication Server	Select the authentication server for your FIDO devices. Select **MyID CMS** if you are using MyID as the authentication server for your passkeys. If you are using an external authentication server for your passkeys (for example, Microsoft Entra), select the name of the external system you created from the drop-down list.
Device Type	Select the type of device from the drop-down list.
Process Status	Select the status of the device from the drop-down list; for example, **Active** or **Erased**.
Enabled	Select whether or not the device is enabled from the drop-down list.

You can also select the following **Additional search criteria**:

Field	Description
Valid After	Select the date after which the device became valid.
Valid Before	Select the date before which the device became valid.
Expires After	Select the date after which the device will expire.
Expires Before	Select the date before which the device will expire.
Enabled (text)	Select whether or not the device is enabled.
Owner	Type the name of the person who is the device owner. This is an alternative to **Owner Name (contains)** that allows you to use wildcards.

7.3.31.2 Report fields

The report contains the following fields:

Field	Description
Owner	The person who owns the device.
Credential Profile	The credential profile used to issue the device.
Device Type	The type of the device.
Process Status	The status of the device; for example, `Active` or `PendingActivation`.
Authentication Server	The name of the authentication server used to issue the device.
Enabled	Whether or not the device is currently enabled.
Valid From	The validity start date.
Expires	The date the device expires.

7.3.31.3 Running the report through the API

The Passkeys report has the report ID `290036`.

See section *7.2.2*, *Running reports through the MyID Core API* for more details of running reports through the MyID Core API.

7.3.31.4 Further information

See the ***Passkey Integration Guide*** for details.

8 Working with inventory management

The inventory process is as follows:

1. Determine the types of stock you want to manage.

   For example, you may want to manage facility access cards separately from USB tokens, so you create the following card stocks:

   - Facility Access Cards
   - USB Tokens

   These card stocks can have more than one type of device; for example, your facility access cards may come from more than one manufacturer, or your USB tokens may have different form factors.

   Use the **List Editor** to add values to the **Stock Code** list for each type of stock. See section *8.2*, *Editing inventory lists*.

2. Determine the types of location you want to manage.

   For example, you may have offices and warehouses, so you create the following kinds of location:

   - Office
   - Warehouse

   Use the **List Editor** to add values to the **Kind** list for each type of location. See section *8.2*, *Editing inventory lists*.

3. If required, determine the names of the couriers you want to use for transferring devices from one location to another.

   For example, you may want to be able to use internal mail or a commercial courier service.

   Use the **List Editor** to add values to the **Courier** list for each type of courier. See section *8.2*, *Editing inventory lists*.

4. Set up the locations in your organization.

   For example, you may have a headquarters, two regional offices, and a warehouse.

   Use the **Locations** category to add your locations. See section *9*, *Working with locations*.

5. For each location, set up stock limits.

   For each stock code, you can set a minimum quantity for that location, and a quantity of devices to reorder when the stock drops below that level.

   Use the **Stock Limits** category to add your stock limits. See section *10*, *Working with stock limits*.

6. Import batches of devices.

   When you receive a box of devices, you can import the serial numbers from the devices, either as a sequential range or from a manifest file, specify them as a particular stock code, and assign the devices to a particular location.

   Use the **Import** facility in the **Devices** category to import your devices. See section *5.24*, *Importing a range of devices*.

7. Monitor the stock levels in each of your locations.

   Use the **Stock Per Location** report to view how many unallocated devices are in each location, along with details of their stock limits. When a device is imported and assigned to a location, it appears as an unallocated device. When it is issued to a person, the number of unallocated devices in that location for that stock code is reduced by one.

   You can run the **Stock Per Location** report within the MyID Operator Client or through the MyID Core API. See section *10.5*, *Checking stock limits*.

8. If a location requires more devices, you can either order more, and import them once they have arrived, or transfer devices from a different location.

   To transfer devices from one location to another:

   a. Create a stock transfer.

      You can specify the source and destination locations, the stock code for the devices to be transferred, the number of devices to be transferred, and the courier and tracking code. You can edit the stock transfer to add the tracking code later, once you have dispatched the stock transfer, if required.

      Use the **Stock Transfers** category to create or edit a stock transfer. See section *11*, *Working with stock transfers*.

   b. Allocate the required number of devices to the stock transfer.

      You are recommended to use the **Available Device Stock** report, specifying the source **Location** and the **Stock Code** for the devices you want to transfer, then from the results select the appropriate number of devices, and use the batch **Transfer** option from the **Tools** menu to assign these devices to the stock transfer. See section *11.4.1*, *Adding a batch of devices to a stock transfer*.

      Alternatively, you can use the **Transfer** option on the View Device screen to allocate a single device to the transfer. See section *11.4.2*, *Adding a single device to a stock transfer*.

   c. Dispatch the stock transfer.

      Use the **Dispatch Stock Transfer** option on the View Transfer screen. See section *11.7*, *Dispatching a stock transfer*.

      The devices are removed from the source location. At this point you may want to add a tracking code for the courier you are using to transfer the devices to their new location.

   d. Once the stock transfer has arrived at its destination, receive the stock transfer.

      Use the **Receive Stock Transfer** option on the View Transfer screen. See section *11.9*, *Receiving a stock transfer*.

      The devices are added to the destination location.

   Important: MyID ensures that you do not select devices that have been issued, or that have already been assigned to a stock transfer. However, the transfer process does *not* validate that you have selected devices from the correct location or of the correct stock code, or that you have selected the correct number of devices. You can dispatch an empty stock transfer, a stock transfer filled with devices from the wrong location, or a stock transfer that has the wrong types of devices. Make sure that you allocate the devices to the stock transfer carefully.

8.1 Setting up inventory roles

You must use the **Edit Roles** workflow to assign the inventory features to the roles you want to be able to access these features. You can assign the features to different roles; for example, you may have administrators who are responsible for managing the list of locations and their limits, operators who carry out day-to-day stock transfers, and analysts who run inventory reports.

To assign inventory features to roles:

1. In the MyID Operator Client, from the **More** category, select **Configuration Settings** then **Edit Roles**.

   Alternatively, in MyID Desktop, from the **Configuration** category, select **Edit Roles**.
2. Use the **Show/Hide Roles** option to display the role you want to work with.
3. Select the following features:
   - **Cards** section:
     - **Import** – allows you to import a range of serial numbers for a device and allocate them to a location.
     - **Transfer Device** – allows you to transfer one or more imported devices from one location to another.
   - **Reports** section:
     - **Available Device Stock** – allows you to run the **Available Device Stock** report, which provides a list of unallocated devices that are available to transfer from one location to another.
     - **Device Import Requests** – allows you to run the **Device Import Requests** report, which provides a list of device import requests you have created.
     - **Locations** – allows you to run the **Locations** report, which provides a list of the locations in the system.
     - **Stock Limits** – allows you to run the **Stock Limits** report, which provides a list of each location in the system along with the configured minimum quantities and re-order quantities.
     - **Stock Per Location** – allows you to run the **Stock Per Location** report, which provides a list of each location in the system along with the unallocated stock at each location.
     - **Stock Transfers** – allows you to run the Stock Transfers report, which provides a list of all current and previous stock transfers, along with their status.

     Note: Some reports are made available when you select their related feature; for example, the **Locations** report is available if you provide access to any features in the **Locations** section in **Edit Roles**. However, if you subsequently remove access from the report, you will also lose access to the related features.
   - **Configuration** section:
     - **List Editor** – this is a standard MyID workflow, and is not specific to inventory management. However, you must have access to this workflow to update the lists of stock code, kinds of location, and couriers. See section *8.2*, *Editing inventory lists*.

- **Locations** section:
    - **Add Location** – allows you to add a new location.
    - **Edit Location** – allows you to edit the details of an existing location.
    - **View Location** – allows you to view the details of a location.

  Adding a feature in this section also provides access to the **Locations** report.
- **Stock Limits** section:
    - **Add Stock Limit** – allows you to add a stock limit.
    - **Delete Stock Limit** – allows you to delete a stock limit.
    - **Edit Stock Limit** – allows you to edit an existing stock limit.
    - **View Stock Limit** – allows you to view the details of a stock limit.

  Adding a feature in this section also provides access to the **Stock Limits** report.
- **Stock Transfers** section:
    - **Add Stock Transfer** – allows you to add a stock transfer.
    - **Cancel Stock Transfer** – allows you to cancel a stock transfer,
    - **Dispatch Stock Transfer** – allows you to mark a stock transfer as dispatched.
    - **Edit Stock Transfer** – allows you to edit an existing stock transfer.
    - **Fail Stock Transfer** – allows you to fail a stock transfer that has been dispatched but not yet received, either marking the devices as lost or returned.
    - **Receive Stock Transfer** – allows you to mark a dispatched stock transfer as received at its destination.
    - **View Stock Transfer** – allows you to view a stock transfer.

  Adding a feature in this section also provides access to the **Stock Transfers** report.

4. Click **Save Changes**.

For more information about editing roles, see the *Roles, groups, and scope* section in the ***Administration Guide***.

8.2 Editing inventory lists

The inventory control system uses MyID lists for the following:

- Courier – a list of couriers that you can use in stock transfers to record how you are transporting the devices from one location to another.
- Kind – a list of the kinds of location; for example, office or warehouse.
- Stock Code – a list of the identifiers for types of device. Used in locations and in stock limits.

Note: You must have access to the **List Editor** option in Edit Roles; see section *8.1*, *Setting up inventory roles*.

To edit the possible values for an inventory list:

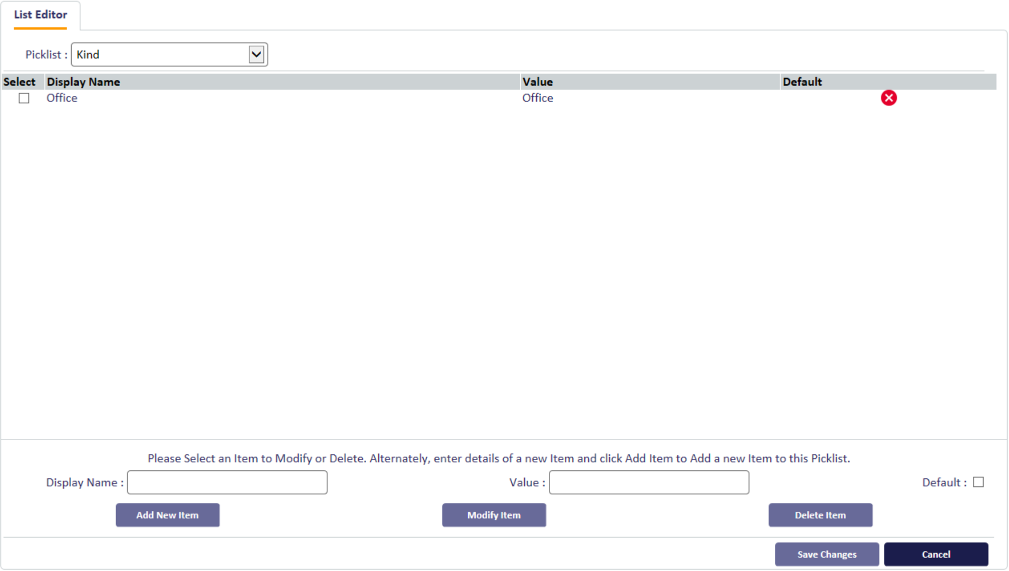
1. In the MyID Operator Client, from the **More** category, select **Configuration Settings** then **List Editor**.

   Alternatively, in MyID Desktop, from the **Configuration** category, select the **List Editor** workflow.

2. Select which list you want to edit in the **Picklist** field.

   For inventory lists, select one of the following:

   - **Courier**
   - **Kind**
   - **Stock Code**



Picklist : Kind

Select	Display Name	Value	Default
☐	Office	Office	⊗

Please Select an Item to Modify or Delete. Alternately, enter details of a new Item and click Add Item to Add a new Item to this Picklist.

Display Name :

Value :

Default : ☐

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, database 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.

Avoid removing or changing stock codes that are in use. If you remove or change a stock code, you may experience inconsistency when viewing previously-created records that used that stock code; the old stock code does not appear in the View Stock Limit screen, but does appear in the list of results for the Stock Limits reports.

9 Working with locations

You can configure locations within MyID to represent the places in your organization where device stock is stored and used. For example, you may have the following locations:

- Headquarters
- Northern regional office
- Western regional office
- Central warehouse

You want to be able to track how much device stock you have available in each location. There is no benefit in knowing that you have 1000 available devices, if they are all in the headquarters, and you have 50 new employees in the Northern regional office who need devices this week. Once you have set up your locations, you can set stock limits for these locations; see section *10*, *Working with stock limits*.

You may want to differentiate the kinds of location; for example, you may want to keep your offices separate from your warehouse. MyID allows you to create a list of these kinds of location; you can use the **List Editor** to edit the **Kind** list. See section *8.2*, *Editing inventory lists* for details.

The MyID Operator Client allows you to work with locations in the following ways:

- You can add a new location.

  See section *9.1*, *Adding a location*.
- You can search for a location.

  See section *9.2*, *Searching for a location*.
- You can edit an existing location, including enabling or disabling the location.

  See section *9.3*, *Editing a location*.

Note: You cannot delete a location once it has been added; however, you can edit its details.

9.1 Adding a location

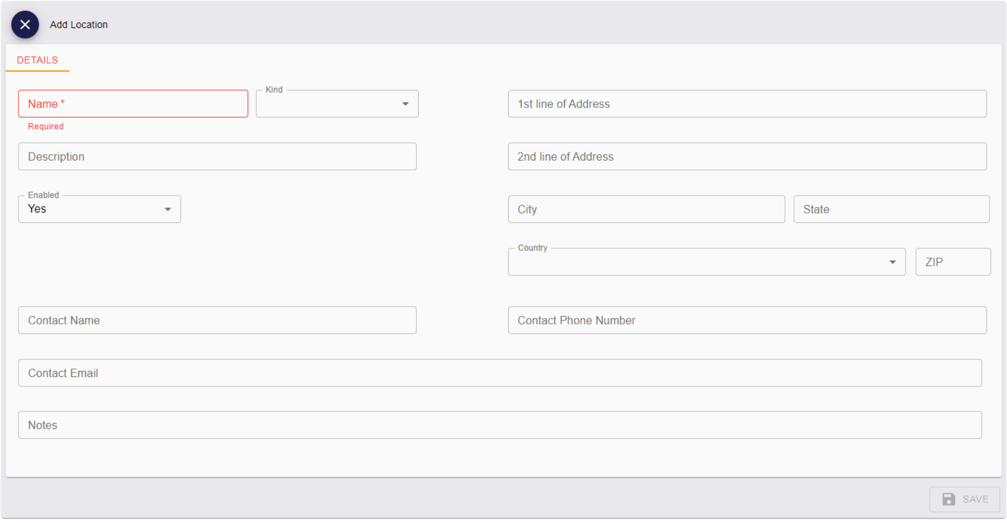
To add a location to the MyID system:

1. Select the **Locations** category.

   You must have the appropriate permissions to access this category. See section *8.1*, *Setting up inventory roles*.

2. Click **Add**.

   The Add Location screen appears.


Add Location
DETAILS
Name *
Required
Kind
Description
Contact Name
Contact Email
Notes
1st line of Address
2nd line of Address
City
State
Country
ZIP
Contact Phone Number
SAVE

Enabled: Yes

3. Complete the following details:
   - **Name** – type the name of the location. This is the only mandatory field.
   - **Kind** – select the kind of location from the drop-down list. You can control the available options in the **Kind** drop-down list using the **List Editor**; see section *8.2*, *Editing inventory lists*.
   - **Description** – type the description for the location.
   - **Enabled** – select Yes to enable the location, or No to disable the location.

     Note: This option is used for reporting purposes only. It does not affect whether you can use the location for stock transfers.
   - Address details – provide the address of the location.
   - Contact details – provide the name, phone number, and email address of the contact point for the location.

   You can also add any **Notes** in the box.

4. Click **Save**.

9.2 Searching for a location

To search for a location:

1. Select the **Locations** category.

   You must have the appropriate permissions to access this category. See section *8.1*, *Setting up inventory roles*.

2. Enter some or all of the search criteria.

   Note: Search criteria are not case sensitive.

   - **Name** – Type the name of the location. You can use wildcards.
   - **Enabled** – Select the enabled status of the location from the drop-down list.
   - **Kind** – Select the kind of location from the drop-down list.

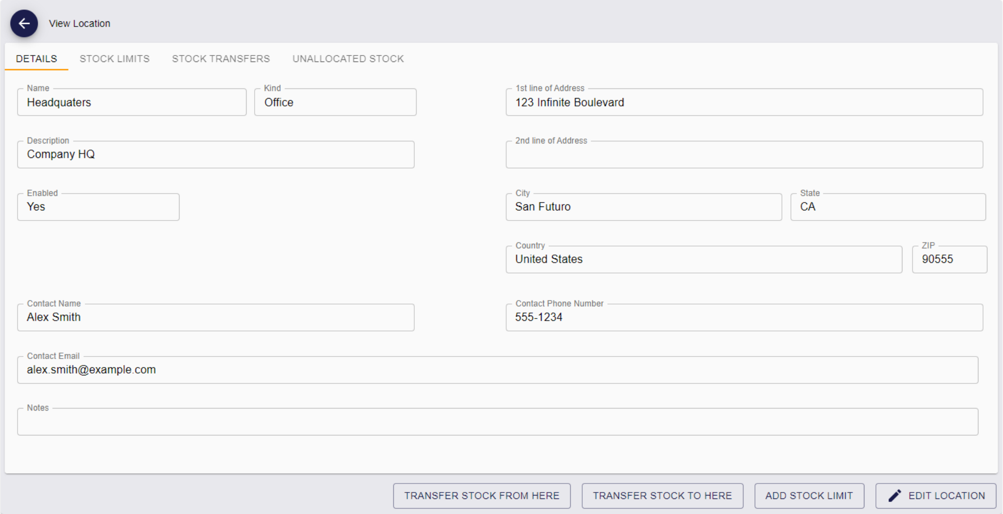
   You can also select **Additional search criteria**. See section *7.3.3*, *Locations report* for details of which fields are available for the Locations search.

3. Click **Search**.

   The list of matching results appears.

   Records are sorted oldest first; currently, you cannot change the sort order.

4. Click a record to view the location's details.



Name: Headquaters
Kind: Office
1st line of Address: 123 Infinite Boulevard
Description: Company HQ
2nd line of Address:
Enabled: Yes
City: San Futuro
State: CA
Country: United States
ZIP: 90555
Contact Name: Alex Smith
Contact Phone Number: 555-1234
Contact Email: alex.smith@example.com
Notes:

The View Location screen displays the following:

- **Details** – displays the name, kind of location, and address and contact details for the location.
- **Stock Limits** – displays a list of the stock limits set up for the location. You can click on an item in the list to open the View Stock Limit screen, which allows you to view, edit, or delete the stock limit.

  See section *10*, *Working with stock limits*.
- **Stock Transfers** – displays a list of the stock transfers related to the location, whether as a source or a destination. You can click on an item in the list to open the View Transfer screen, which allows you to view the details of the transfer.

See section *11*, *Working with stock transfers*.

- **Unallocated Stock** – displays a list of the unallocated devices associated with the location. Unallocated devices are devices that have not been issued to a person and have not already been assigned to a stock transfer. You can click on an item in the list to open the View Device screen, which allows you to transfer a single device. Note, however, that you cannot carry out batch transfer operations from this screen; you must run the Available Device Stock report instead.

  See section *11.4*, *Adding devices to a stock transfer*.

From the View Location screen, you can carry out the following actions:

- Edit the location.

  See section *9.3*, *Editing a location*.
- Add a stock limit for the location.

  See section *10.1.1*, *Adding a stock limit from the View Location screen*.
- Create a stock transfer to or from the location.

  See section *11.1.1*, *Adding a stock transfer from the View Location screen*.

9.3 Editing a location

You can edit the details for location, including enabling or disabling the location.

To edit a location:

1. Select the **Locations** category.

   You must have the appropriate permissions to access this category. See section *8.1*, *Setting up inventory roles*.

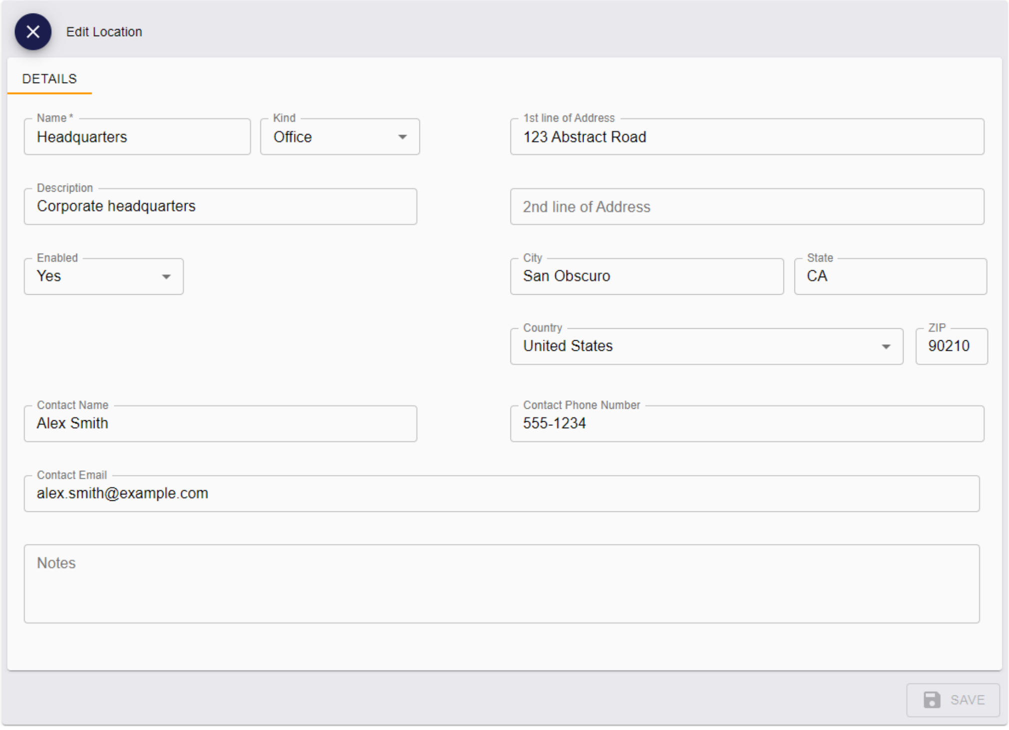
2. Search for a location and open it in the View Location screen.

   For details of searching for a location, see section *9.2*, *Searching for a location*.

3. Click **Edit Location** in the button bar at the bottom of the screen.

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

   The Edit Location screen appears.



Name *: Headquarters
Kind: Office
1st line of Address: 123 Abstract Road
Description: Corporate headquarters
2nd line of Address
Enabled: Yes
City: San Obscuro
State: CA
Country: United States
ZIP: 90210
Contact Name: Alex Smith
Contact Phone Number: 555-1234
Contact Email: alex.smith@example.com
Notes

4. Make any changes to the details of the location.
5. Click **Save**.

10 Working with stock limits

MyID allows you to set stock limits for your locations. For each type of device stock, you can set a minimum number of devices to keep on hand, and specify the number of devices to reorder.

You can use a report to track how many devices each location has available, and compare this to the limits you have set up.

The MyID Operator Client allows you to work with stock limits in the following ways:

- You can add a stock limit.

  See section *10.1*, *Adding a stock limit*.
- You can search for a stock limit.

  See section *10.2*, *Searching for a stock limit*.
- You can edit a stock limit.

  See section *10.3*, *Editing a stock limit*.
- You can delete a stock limit.

  See section *10.4*, *Deleting a stock limit*.
- You can check stock limits.

  See section *10.5*, *Checking stock limits*.

10.1 Adding a stock limit

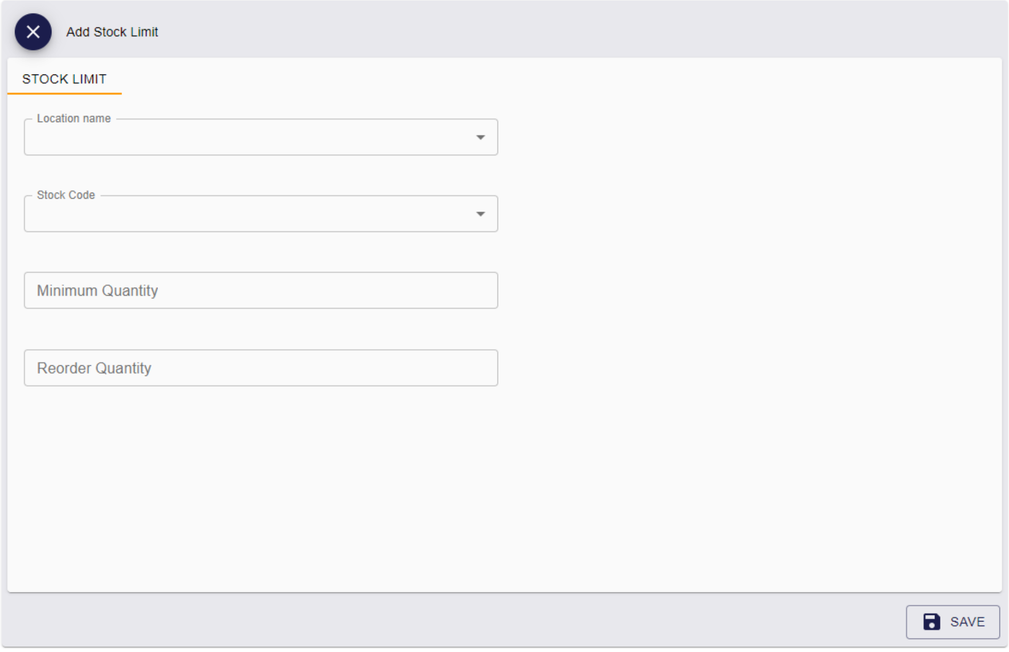
You can add a new stock limit for a location.

To add a stock limit:

1. Select the **Stock Limits** category.

   You must have the appropriate permissions to access this category. See section *8.1*, *Setting up inventory roles*.
2. Click **Add**.

   The Add Stock Limit screen appears.


Add Stock Limit
STOCK LIMIT
Location name
Stock Code
Minimum Quantity
Reorder Quantity
SAVE

3. Complete the following details:
   - **Location Name** – type the name of the location.
   - **Stock Code** – select the code for the device stock.

     You can control the available options in the **Stock Code** drop-down list using the **List Editor**; see section *8.2*, *Editing inventory lists*.
   - **Minimum Quantity** – type the minimum number of available devices you want to keep at this location.
   - **Reorder Quantity** – type the number of devices to order when the number of available devices drops below the minimum quantity.
4. Click **Save**.

10.1.1 Adding a stock limit from the View Location screen

As an alternative method, you can create a stock limit from the View Location screen.

1. Search for a location and view its details.

   See section *9.2*, *Searching for a location*.

2. On the View Location screen, select **Add Stock Limit** in the button bar.

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

   The Add Stock Limit screen appears with the **Location name** field filled in with the current location.

10.2 Searching for a stock limit

To search for a stock limit:

1. Select the **Stock Limits** category.

   You must have the appropriate permissions to access this category. See section *8.1*, *Setting up inventory roles*.
2. Enter some or all of the search criteria.

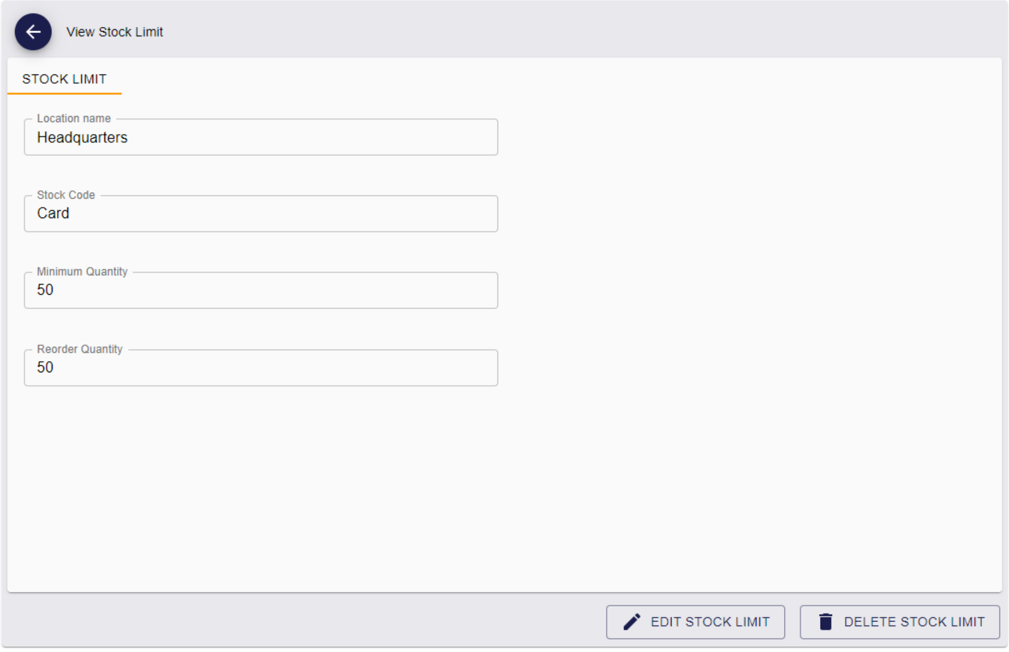
   Note: Search criteria are not case sensitive.

   - **Location Name** – Type the name of the location. You can use wildcards.
   - **Stock Code** – Type the stock code used for the devices.

   See section *7.3.4*, *Stock Limits report* for details of the report used to search stock limits.
3. Click **Search**.

   The list of matching results appears. Stock limits are listed in the order they were created, oldest first; you cannot change this order.
4. Click a record to view the details of the stock limit.

   The View Stock Limit screen appears.



Location name: Headquarters

Stock Code: Card

Minimum Quantity: 50

Reorder Quantity: 50

The View Stock Limit screen displays the following:

- **Location Name** – the name of the location.
- **Stock Code** – the code for the device stock.
- **Minimum Quantity** – the minimum number of available devices you want to keep at this location.
- **Reorder Quantity** – the number of devices to order when the number of available devices drops below the minimum quantity.

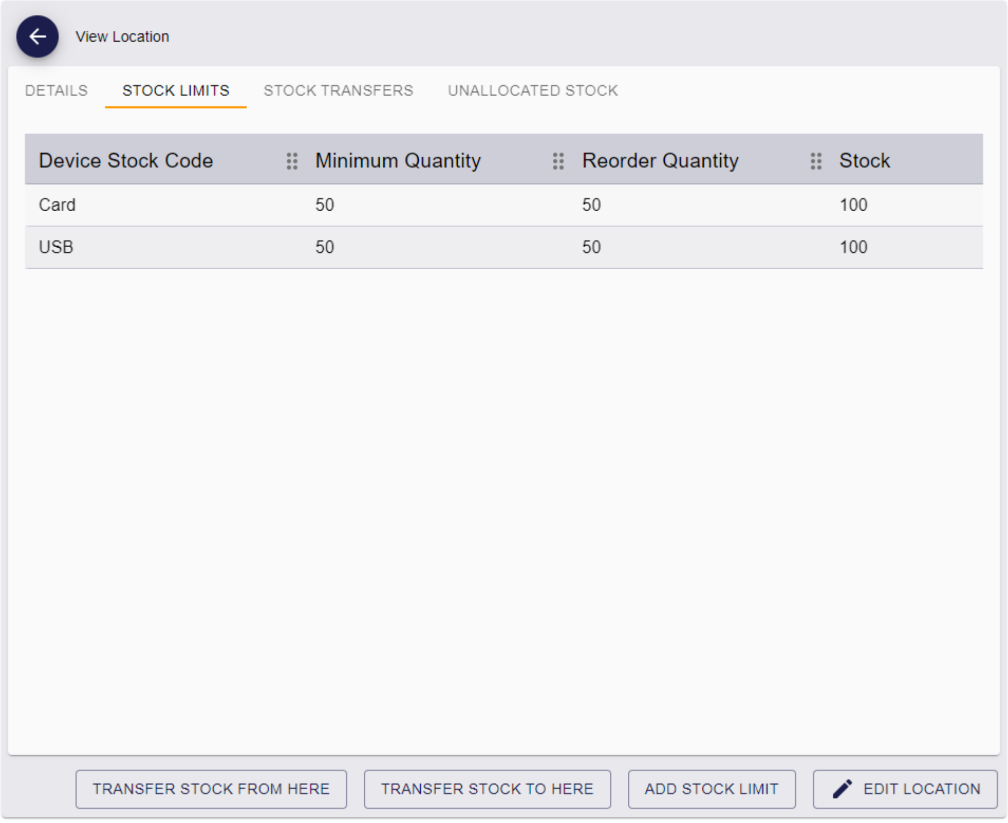
From this screen, you can:

- Edit the stock limit.

  See section *10.3*, *Editing a stock limit*.
- Delete the stock limit.

  See section *10.4*, *Deleting a stock limit*.

You can also display a stock limit from the **Stock Limits** tab of the View Location screen.



View Location
DETAILS
STOCK LIMITS
STOCK TRANSFERS
UNALLOCATED STOCK
TRANSFER STOCK FROM HERE
TRANSFER STOCK TO HERE
ADD STOCK LIMIT
EDIT LOCATION

Device Stock Code	Minimum Quantity	Reorder Quantity	Stock
Card	50	50	100
USB	50	50	100

This screen displays all stock limits set up for the current location, along with the current unallocated stock for that location.

Click an entry in this list to open the View Stock Limit screen.

10.3 Editing a stock limit

You can edit the details of an existing stock limit.

To edit a stock limit:

1. Select the **Stock Limits** category.

   You must have the appropriate permissions to access this category. See section *8.1*, *Setting up inventory roles*.

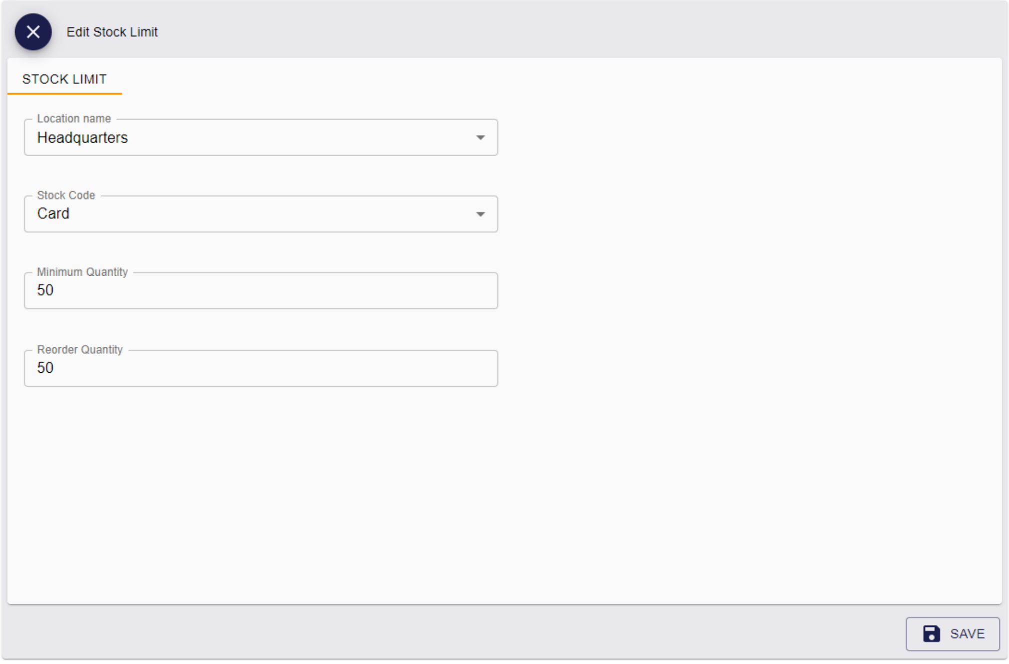
2. Search for a stock limit and open it in the View Stock Limit screen.

   For details of searching for a stock limit, see section *10.2*, *Searching for a stock limit*.

3. Click **Edit Stock Limit** in the button bar at the bottom of the screen.

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

   The Edit Stock Limit screen appears.

   Location name: Headquarters

   Stock Code: Card

   Minimum Quantity: 50

   Reorder Quantity: 50

4. Make any changes to the details of the stock limit.
5. Click **Save**.

10.4 Deleting a stock limit

You can delete a stock limit if it is not longer required.

To delete a stock limit:

1. Select the **Stock Limits** category.

   You must have the appropriate permissions to access this category. See section *8.1*, *Setting up inventory roles*.

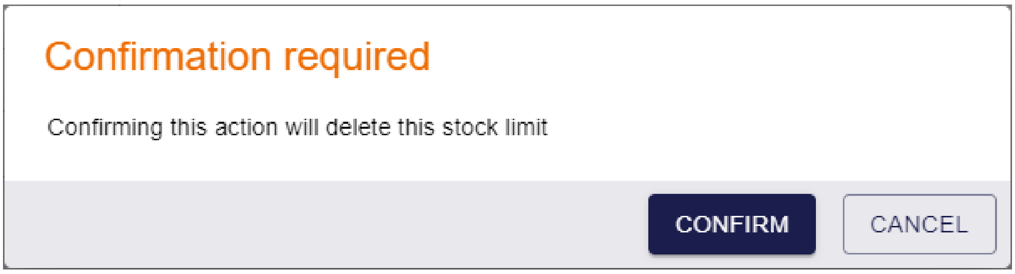
2. Search for a stock limit and open it in the View Stock Limit screen.

   For details of searching for a stock limit, see section *10.2*, *Searching for a stock limit*.

3. Click **Delete Stock Limit** in the button bar at the bottom of the screen.

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

   A confirmation dialog appears.

   Confirmation required

   Confirming this action will delete this stock limit

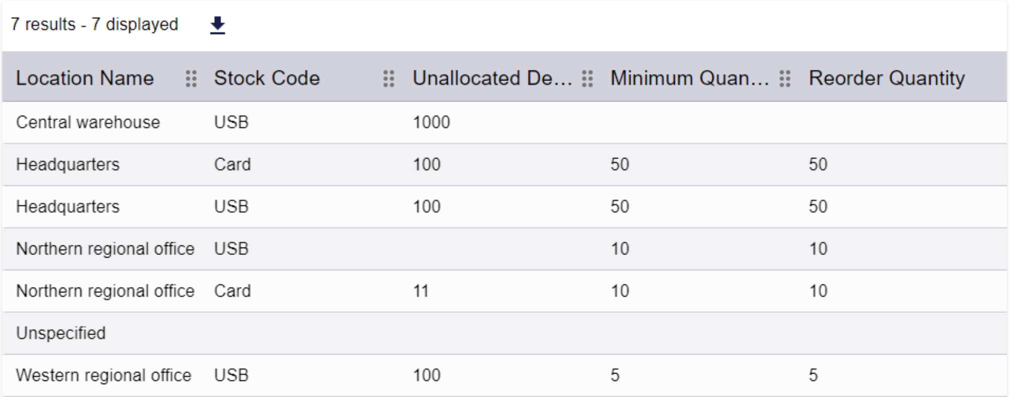
4. Click **Confirm**.

10.5 Checking stock limits

You must monitor your stock levels to ensure that your locations have not fallen below their stock limits. You can do this using the Stock Per Location report or the **Stock Limits** tab of the View Location screen.

10.5.1 Checking stock limits using the Stock Per Location report

You can use the Stock Per Location report to check whether any of your locations have fallen below their stock limits. This provides a list of the available stock for each location and stock type (that is, devices not currently issued and not currently assigned to a stock transfer), along with the stock limits set up. You can use this to identify which locations have stock that has fallen below the required minimum, and use this information to order new batches of devices, or transfer devices from one location to another.



7 results - 7 displayed

Location Name	Stock Code	Unallocated De…	Minimum Quan…	Reorder Quantity
Central warehouse	USB	1000		
Headquarters	Card	100	50	50
Headquarters	USB	100	50	50
Northern regional office	USB		10	10
Northern regional office	Card	11	10	10
Unspecified				
Western regional office	USB	100	5	5

See section *7.3.25*, *Stock Per Location report*.

If you call the report through the MyID Core API, the results are returned in JSON format.

The `fields` section provides the headers for the report.

The `results` section provides an entry for each row in the report.

```
{
  "fields":[
    {
      "name":"Name",
      "description":"Location Name",
      "type":"text"
    },
    {
      "name":"StockCode",
      "description":"Stock Code",
      "type":"text"
    },
    {
      "name":"UnallocatedDevices",
      "description":"Unallocated Devices",
      "type":"number"
    },
    {
      "name":"MinimumQuantity",
      "description":"Minimum Quantity",
      "type":"number"
    },
    {
      "name":"ReorderQuantity",
      "description":"Reorder Quantity",
      "type":"number"
    }
  ],
  "results":[
    {
      "Name":"Central warehouse",
      "StockCode":"USB",
      "UnallocatedDevices":1000,
      "MinimumQuantity":0,
      "ReorderQuantity":0,
      "id":"1"
    },
    {
      "Name":"Headquarters",
      "StockCode":"Card",
      "UnallocatedDevices":100,
      "MinimumQuantity":50,
      "ReorderQuantity":50,
      "id":"2"
    }
  ],
  "links":[
    {
      "cat":"self",
      "srv":"https://react.domain25.local/rest.core/api/"
    }
  ]
}
```

See section *7.3.25.3*, *Running the report through the API*.

10.5.2 Checking stock limits on the View Location screen

The Stock Limits tab of the View Location screen displays the stock limits set up for that location, along with the stock levels.

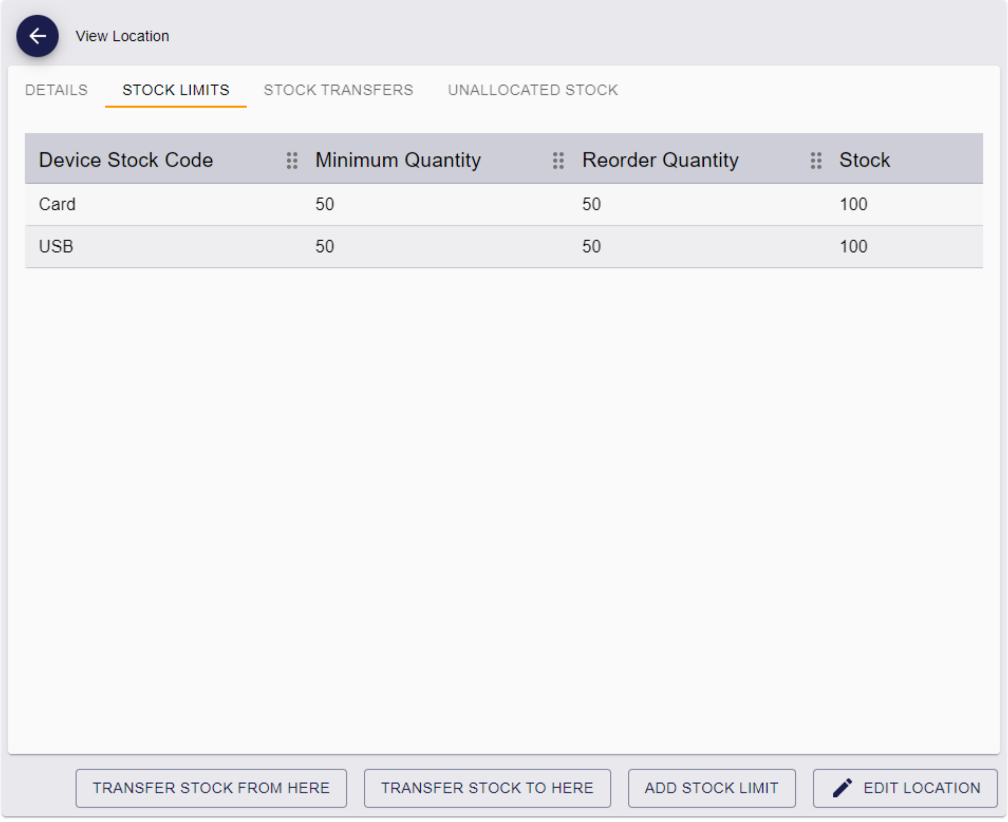
To check the stock limits:

1. Search for a location and display its details.

   See section *9.2*, *Searching for a location*.

2. Click the **Stock Limits** tab.

   A report of each stock limit for that location along with the available stock appears.


View Location
DETAILS
STOCK LIMITS
STOCK TRANSFERS
UNALLOCATED STOCK
TRANSFER STOCK FROM HERE
TRANSFER STOCK TO HERE
ADD STOCK LIMIT
EDIT LOCATION

Device Stock Code	Minimum Quantity	Reorder Quantity	Stock
Card	50	50	100
USB	50	50	100

11 Working with stock transfers

When you monitor the stock levels at your locations, and notice that the stock levels have dropped below your configured stock limits, you can either order new devices to be sent straight to that location, or, if you have stock elsewhere (for example, in a warehouse) you can transfer devices from one location to another.

MyID allows you to manage the transfer of stock from one location to another using stock transfers. You can think of a stock transfer as a box, into which you can put your devices, then send the box from the source location to their destination.

The basic process is as follows:

1. Create a stock transfer "box" to contain the devices.
2. Add devices to the box.
3. Dispatch the box to its destination.
4. Once the box has arrived, mark it as received.

The MyID Operator Client allows you to work with stock transfers in the following ways:

- You can add a stock transfer.

  See section *11.1*, *Adding a stock transfer*.
- You can search for a stock transfer and view its details.

  See section *11.2*, *Searching for a stock transfer*.
- You can edit the details of a stock transfer.

  See section *11.3*, *Editing a stock transfer*.
- You can add devices to a stock transfer, either as a batch or one at a time.

  See section *11.4*, *Adding devices to a stock transfer*.
- You can cancel a stock transfer and release any devices allocated to it.

  See section *11.5*, *Canceling a stock transfer*.
- You can check the contents of a stock transfer before dispatching it.

  See section *11.6*, *Checking the contents of a stock transfer*.
- You can dispatch a stock transfer.

  See section *11.7*, *Dispatching a stock transfer*.
- You can fail a stock transfer if it fails to arrive at its destination.

  See section *11.8*, *Failing a stock transfer*.
- You can receive a stock transfer at its destination.

  See section *11.9*, *Receiving a stock transfer*.

11.1 Adding a stock transfer

Before you can transfer devices from one location to another, you must create a stock transfer.

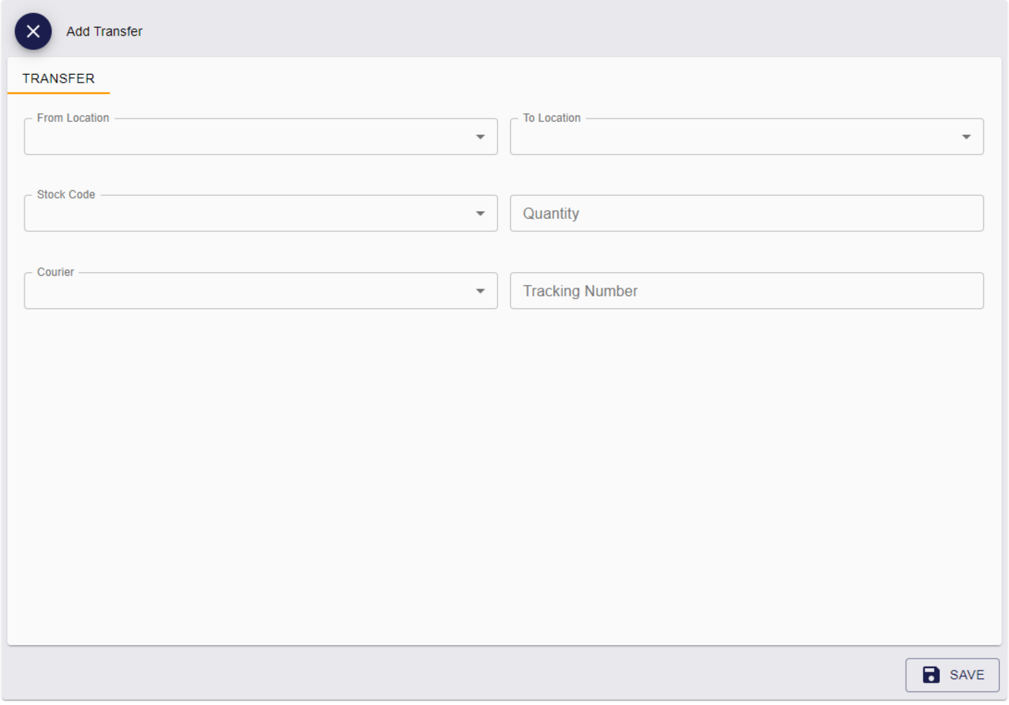
To add a stock transfer:

1. Select the **Stock Transfers** category.

   You must have the appropriate permissions to access this category. See section *8.1*, *Setting up inventory roles*.

2. Click **Add**.

   The Add Stock Transfer screen appears.



3. Complete the following details:
   - **From Location** – select the location where the devices are currently held.
   - **To Location** – select the location to which you want to transfer the devices.
   - **Stock Code** – select the stock code for the devices you want to transfer.
   - **Quantity** – type the quantity of devices you want to transfer.
   - **Courier** – select the method you want to use to transfer devices between locations.
   - **Tracking Number** – type the tracking number for the courier.

     You may want to leave this blank, and come back to edit the stock transfer to add the tracking number once you have dispatched the stock transfer.

   Note: You can control the available options in the **Stock Code** and **Courier** drop-down list using the **List Editor**; see section *8.2*, *Editing inventory lists*.

4. Click **Save**.

11.1.1 Adding a stock transfer from the View Location screen

As an alternative method, you can create a stock transfer from the View Location screen.

1. Search for a location and view its details.

   See section *9.2*, *Searching for a location*.
2. On the View Location screen, select one of the following options in the button bar:
   - **Transfer Stock from Here** – opens the Add Stock Transfer screen with the **From Location** field filled in with the current location.
   - **Transfer Stock to Here** – opens the **Add Stock Transfer** screen with the **To Location** field filled in with the current location.

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

11.2 Searching for a stock transfer

To search for a stock transfer:

1. Select the **Stock Transfers** category.

   You must have the appropriate permissions to access this category. See section *8.1*, *Setting up inventory roles*.

2. Enter some or all of the search criteria.

   Note: Search criteria are not case sensitive.

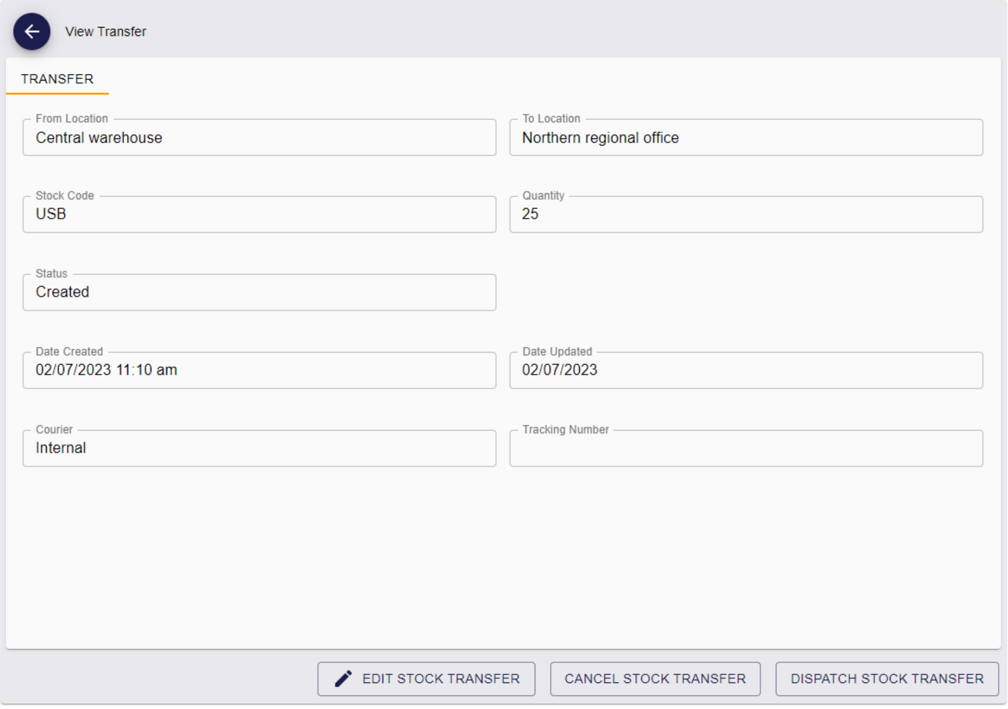
   - **From Location** – Type the name of the location from which you want to transfer devices. You can use wildcards.
   - **To Location** – Type the name of the location to which you want to transfer devices. You can use wildcards.
   - **Stock Code** – Type the stock code used for the devices. You can use wildcards.
   - **Status** – Select the status of the stock transfer.

   You can also select **Additional search criteria**. See section *7.3.24*, *Stock Transfers report* for details of which fields are available for the Stock Transfers search.

3. Click **Search**.

   The list of matching results appears. Stock transfers are listed in the order they were created, oldest first; you cannot change this order.

4. Click a record to view the details of the stock transfer.



View Transfer

TRANSFER

From Location: Central warehouse
To Location: Northern regional office
Stock Code: USB
Quantity: 25
Status: Created
Date Created: 02/07/2023 11:10 am
Date Updated: 02/07/2023
Courier: Internal
Tracking Number:

The View Stock Transfer screen displays the following:

- **From Location** – the location where the devices are currently held from the drop-down list.
- **To Location** – the location to which you want to transfer the devices from the drop-down list.
- **Stock Code** – the stock code for the devices you want to transfer.
- **Quantity** – the quantity of devices you want to transfer.
- **Status** – the status of the transfer. The possible statuses are:
  - **Created** – the stock transfer has been created but not yet dispatched.
  - **InTransit** – the stock transfer has been dispatched.
  - **Received** – the stock transfer has been received at its destination.
  - **Cancelled** – the stock transfer has been canceled.
  - **Failed** – the stock transfer has been marked as failed; for example, lost in transit or returned to sender.
- **Date Created** – the date the stock transfer was added.
- **Date Updated** – the date the stock transfer was last updated.
- **Courier** – the method you want to use to transfer the devices between your locations.
- **Tracking Number** – the tracking number for the courier.

From the View Stock Transfer screen, you can carry out the following actions:

- Edit the details of the stock transfer.

  See section *11.3*, *Editing a stock transfer*.
- Cancel the stock transfer.

  See section *11.5*, *Canceling a stock transfer*.
- Dispatch the stock transfer to its destination.

  See section *11.7*, *Dispatching a stock transfer*.
- Fail a stock transfer that was lost in transit or returned to sender.

  See section *11.8*, *Failing a stock transfer*.
- Receive a stock transfer that has arrived at its destination.

  See section *11.9*, *Receiving a stock transfer*.

11.3 Editing a stock transfer

You can edit the details of a stock transfer; for example, you can add a tracking number to the courier details once you have dispatched the stock transfer to its destination.

To edit a stock transfer:

1. Select the **Stock Transfers** category.

   You must have the appropriate permissions to access this category. See section *8.1*, *Setting up inventory roles*.

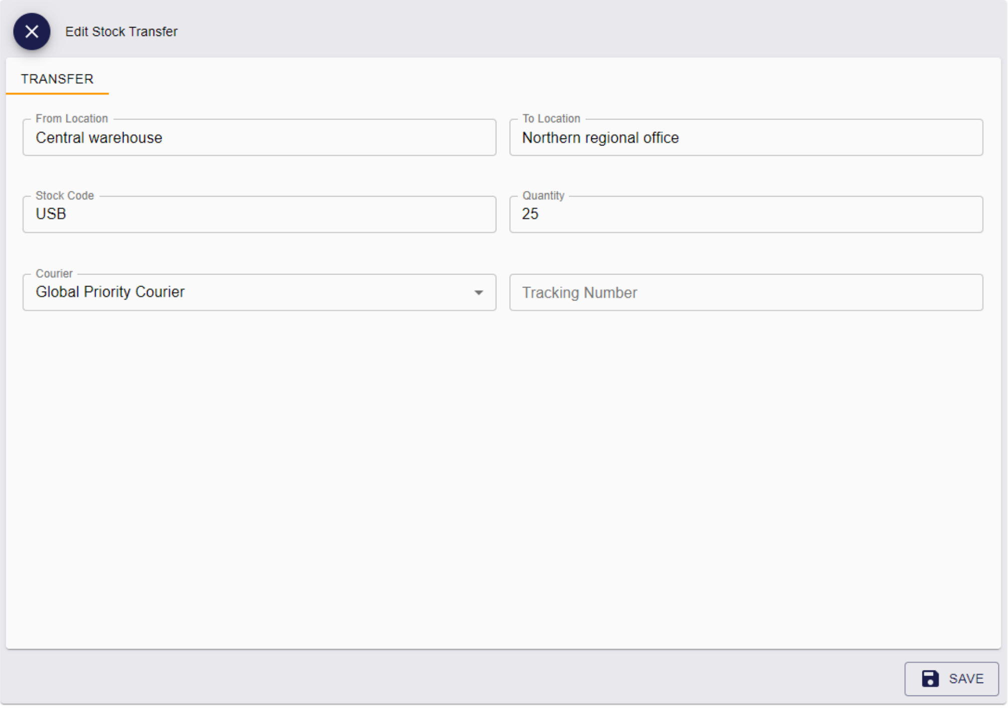
2. Search for a stock transfer and open it in the View Stock Transfer screen.

   For details of searching for a stock transfer, see section *11.2*, *Searching for a stock transfer*.

3. Click **Edit Stock Transfer** in the button bar at the bottom of the screen.

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

   The Edit Stock Transfer screen appears.



From Location: Central warehouse
To Location: Northern regional office
Stock Code: USB
Quantity: 25
Courier: Global Priority Courier
Tracking Number

4. Make any changes to the details of the stock transfer.
5. Click **Save**.

11.4 Adding devices to a stock transfer

Once you have created a stock transfer, you can add devices to transfer.

You must select available devices; that is, devices that have been added to the system, but are not currently issued or already assigned to another stock transfer. To help you identify these devices, you can use the Available Device Stock report; see section *7.3.19*, *Available Device Stock report*

Important: When you create a stock transfer, you specify the source location of the devices, the stock code for the devices, and the quantity of the devices. MyID does *not* verify the source, type, or quantity of devices; you must take care when adding devices. In addition, you cannot see a list of the devices currently allocated to a stock transfer; for help in identifying the contents of a stock transfer, see section *11.6*, *Checking the contents of a stock transfer*.

11.4.1 Adding a batch of devices to a stock transfer

You can add a batch of devices to a stock transfer in a single operation.

Note: You can access the **Tools** menu only if you have a role with the **Tools Menu** option from the **Configuration** section of the **Edit Roles** workflow.

To add a batch of devices to a stock transfer:

1. Search for the devices you want to transfer.

   You are recommended to use the Available Device Stock report:

   a. Select the **Reports** category.

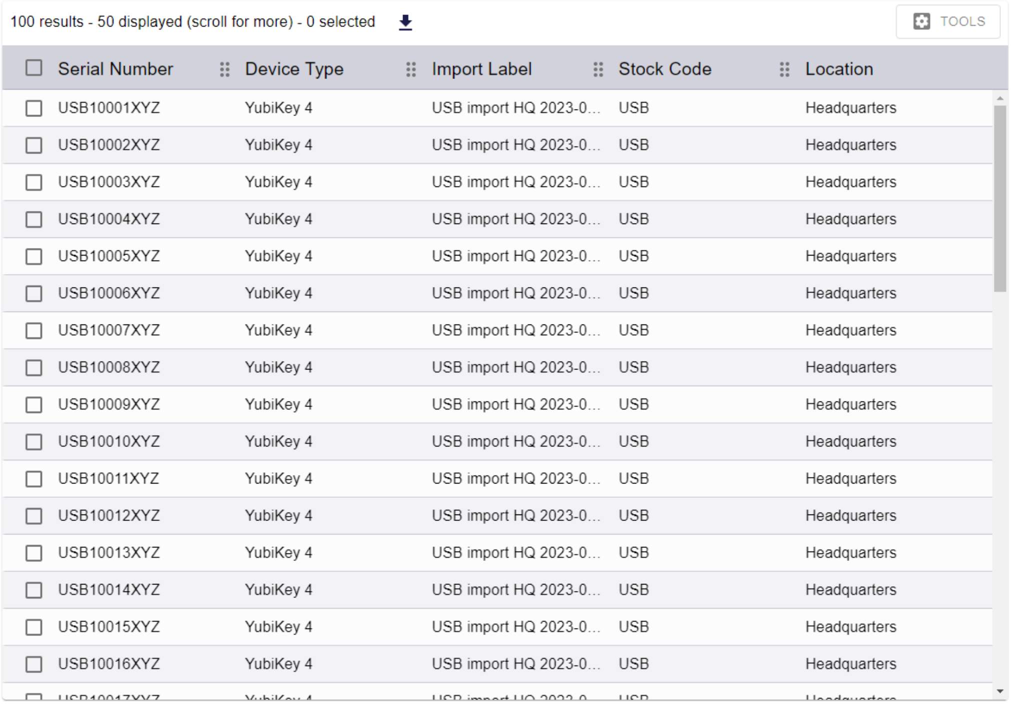
   b. From the **Reports** drop-down list, select **Available Device Stock**.

   c. Complete the search criteria.

      For example, if you have created a stock transfer for 10 devices from your Warehouse to your Headquarters location, with a stock code of USB, specify a **Location** of `Headquarters` and a **Stock Code** of `USB`.

   d. Click **Search**.

   The devices are listed.



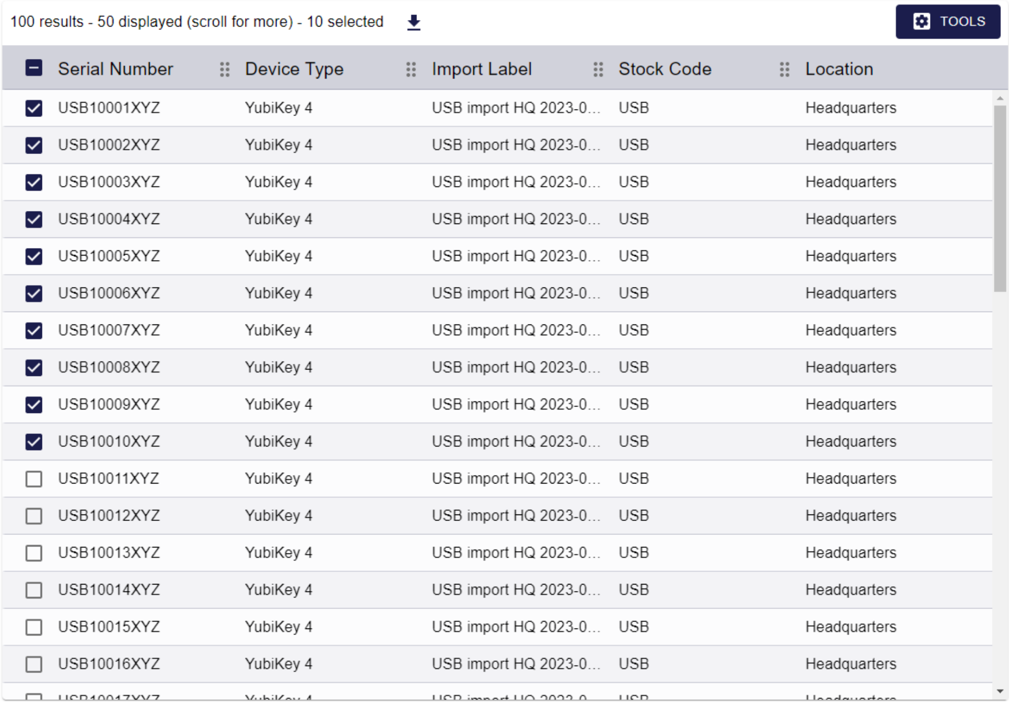
100 results - 50 displayed (scroll for more) - 0 selected

☐	Serial Number	Device Type	Import Label	Stock Code	Location
☐	USB10001XYZ	YubiKey 4	USB import HQ 2023-0...	USB	Headquarters
☐	USB10002XYZ	YubiKey 4	USB import HQ 2023-0...	USB	Headquarters
☐	USB10003XYZ	YubiKey 4	USB import HQ 2023-0...	USB	Headquarters
☐	USB10004XYZ	YubiKey 4	USB import HQ 2023-0...	USB	Headquarters
☐	USB10005XYZ	YubiKey 4	USB import HQ 2023-0...	USB	Headquarters
☐	USB10006XYZ	YubiKey 4	USB import HQ 2023-0...	USB	Headquarters
☐	USB10007XYZ	YubiKey 4	USB import HQ 2023-0...	USB	Headquarters
☐	USB10008XYZ	YubiKey 4	USB import HQ 2023-0...	USB	Headquarters
☐	USB10009XYZ	YubiKey 4	USB import HQ 2023-0...	USB	Headquarters
☐	USB10010XYZ	YubiKey 4	USB import HQ 2023-0...	USB	Headquarters
☐	USB10011XYZ	YubiKey 4	USB import HQ 2023-0...	USB	Headquarters
☐	USB10012XYZ	YubiKey 4	USB import HQ 2023-0...	USB	Headquarters
☐	USB10013XYZ	YubiKey 4	USB import HQ 2023-0...	USB	Headquarters
☐	USB10014XYZ	YubiKey 4	USB import HQ 2023-0...	USB	Headquarters
☐	USB10015XYZ	YubiKey 4	USB import HQ 2023-0...	USB	Headquarters
☐	USB10016XYZ	YubiKey 4	USB import HQ 2023-0...	USB	Headquarters

2. Select the devices you want to transfer.

   Use the check boxes to the left of the records to select the devices.

   For example, you may want to select 10 devices for the stock transfer.

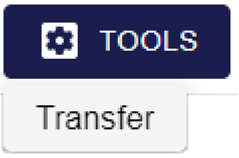


100 results - 50 displayed (scroll for more) - 10 selected

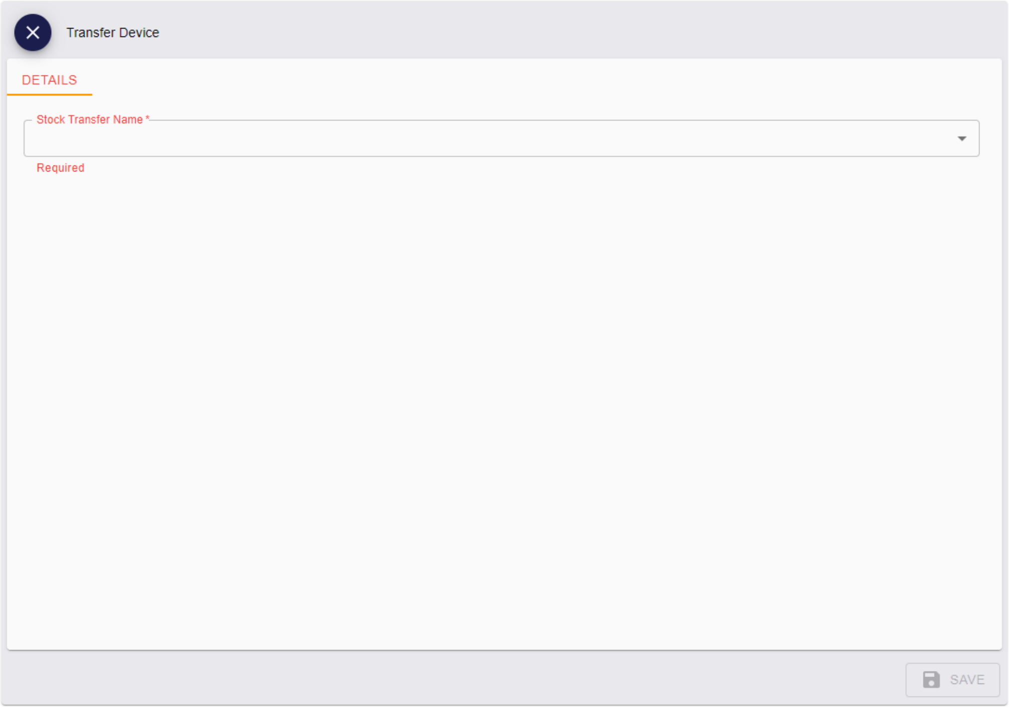
☐	Serial Number	Device Type	Import Label	Stock Code	Location
☑	USB10001XYZ	YubiKey 4	USB import HQ 2023-0...	USB	Headquarters
☑	USB10002XYZ	YubiKey 4	USB import HQ 2023-0...	USB	Headquarters
☑	USB10003XYZ	YubiKey 4	USB import HQ 2023-0...	USB	Headquarters
☑	USB10004XYZ	YubiKey 4	USB import HQ 2023-0...	USB	Headquarters
☑	USB10005XYZ	YubiKey 4	USB import HQ 2023-0...	USB	Headquarters
☑	USB10006XYZ	YubiKey 4	USB import HQ 2023-0...	USB	Headquarters
☑	USB10007XYZ	YubiKey 4	USB import HQ 2023-0...	USB	Headquarters
☑	USB10008XYZ	YubiKey 4	USB import HQ 2023-0...	USB	Headquarters
☑	USB10009XYZ	YubiKey 4	USB import HQ 2023-0...	USB	Headquarters
☑	USB10010XYZ	YubiKey 4	USB import HQ 2023-0...	USB	Headquarters
☐	USB10011XYZ	YubiKey 4	USB import HQ 2023-0...	USB	Headquarters
☐	USB10012XYZ	YubiKey 4	USB import HQ 2023-0...	USB	Headquarters
☐	USB10013XYZ	YubiKey 4	USB import HQ 2023-0...	USB	Headquarters
☐	USB10014XYZ	YubiKey 4	USB import HQ 2023-0...	USB	Headquarters
☐	USB10015XYZ	YubiKey 4	USB import HQ 2023-0...	USB	Headquarters
☐	USB10016XYZ	YubiKey 4	USB import HQ 2023-0...	USB	Headquarters

   The text at the top of the list tells you how many devices you have selected.

3. From the **Tools** menu, select **Transfer**.



The Transfer Device screen appears.



Stock Transfer Name *

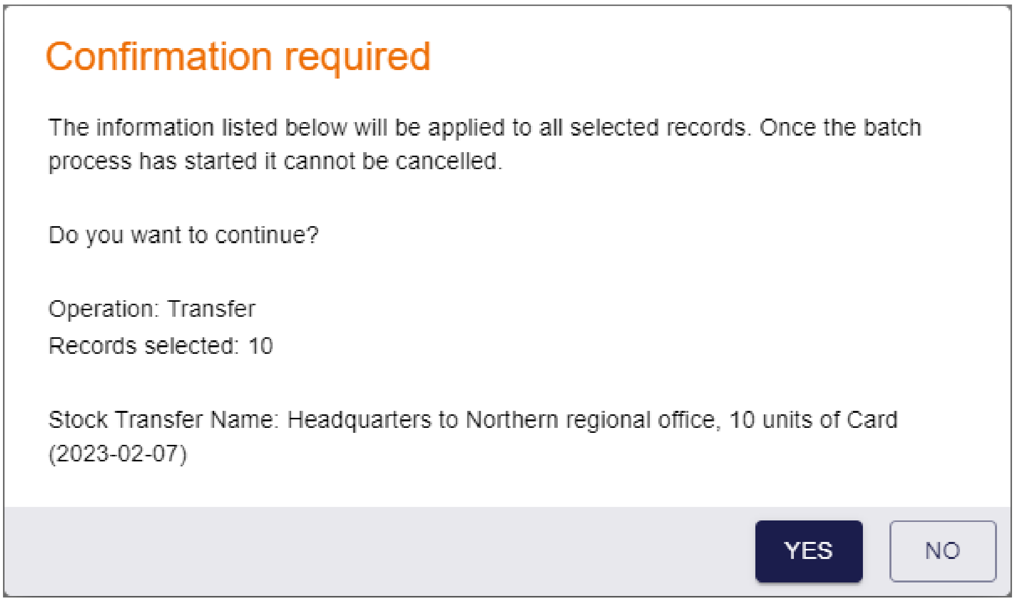
Required

4. From the **Stock Transfer Name** drop-down list, select the stock transfer to which you want to allocate these devices.

   Important: Check that you have selected the correct stock transfer. The name of the stock transfer tells you the source and destination locations, the quantity required, and the stock code of the devices to be transferred.

5. Click **Save**.

   A confirmation screen appears.



Confirmation required

The information listed below will be applied to all selected records. Once the batch process has started it cannot be cancelled.

Do you want to continue?

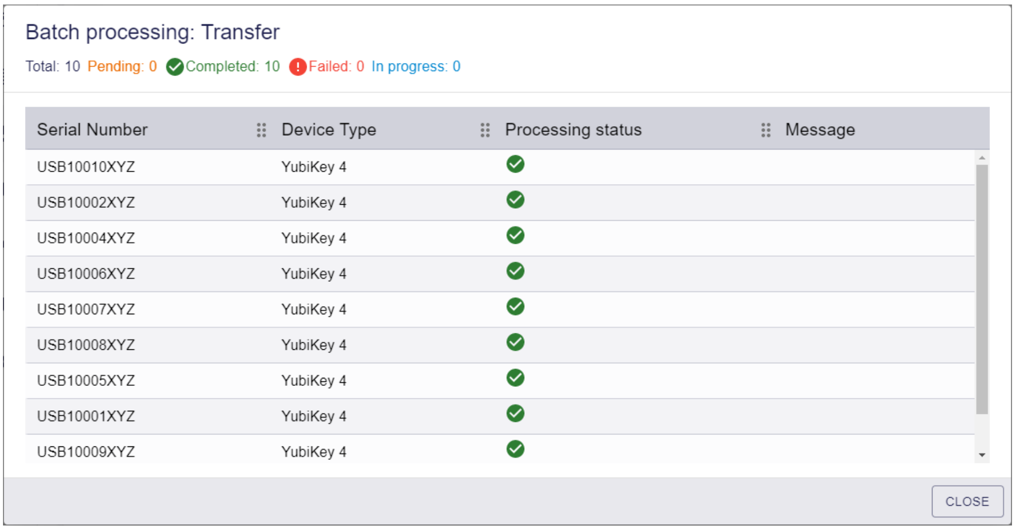
Operation: Transfer
Records selected: 10

Stock Transfer Name: Headquarters to Northern regional office, 10 units of Card (2023-02-07)

6. Click **Yes**.

   The Batch processing screen appears, showing the progress as the devices are allocated to the stock transfer.

   Do not close the MyID Operator Client window while the batch processing is in progress.



Batch processing: Transfer

Total: 10 Pending: 0 ✓Completed: 10 !Failed: 0 In progress: 0

Serial Number	Device Type	Processing status	Message
USB10010XYZ	YubiKey 4	✓	
USB10002XYZ	YubiKey 4	✓	
USB10004XYZ	YubiKey 4	✓	
USB10006XYZ	YubiKey 4	✓	
USB10007XYZ	YubiKey 4	✓	
USB10008XYZ	YubiKey 4	✓	
USB10005XYZ	YubiKey 4	✓	
USB10001XYZ	YubiKey 4	✓	
USB10009XYZ	YubiKey 4	✓	

The table shows the status of each device:

✓	The device was allocated to the stock transfer successfully.
!	The device could not be allocated to the stock transfer. The Message column displays the reason for the failure; for example, you may have attempted to transfer a device that was issued, or was allocated to a different stock transfer.

7. Click **Close**.

11.4.2 Adding a single device to a stock transfer

You can add a single device to a stock transfer from the View Device screen; for example, you may have erased a card that was previously issued to a person, and now want to send it back to a central location to be reused.

To add a single device to a stock transfer:

1. Search for the device you want to add.

   See section *5.26*, *Viewing imported devices*.
2. Click a record to display the details of the device.

   The View Device screen appears.
3. Click **Transfer** in the button bar at the bottom of the screen.

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

   Note: If the device is already allocated to a stock transfer, or is currently issued, the **Transfer** option does not appear.
4. The Transfer Device screen appears.
5. From the **Stock Transfer Name** drop-down list, select the stock transfer to which you want to allocate this device.

   Important: Check that you have selected the correct stock transfer. The name of the stock transfer tells you the source and destination locations, the quantity required, and the stock code of the devices to be transferred.
6. Click **Save**.

11.5 Canceling a stock transfer

You can cancel a stock transfer that has been created but not yet dispatched.

If a stock transfer has already been dispatched, you must fail the stock transfer before you can cancel it; see section *11.8*, *Failing a stock transfer*.

Depending on the reason you provide when canceling the stock transfer, any devices allocated to the stock transfer are either released or marked as disposed.

To cancel a stock transfer:

1. Select the **Stock Transfers** category.

   You must have the appropriate permissions to access this category. See section *8.1*, *Setting up inventory roles*.

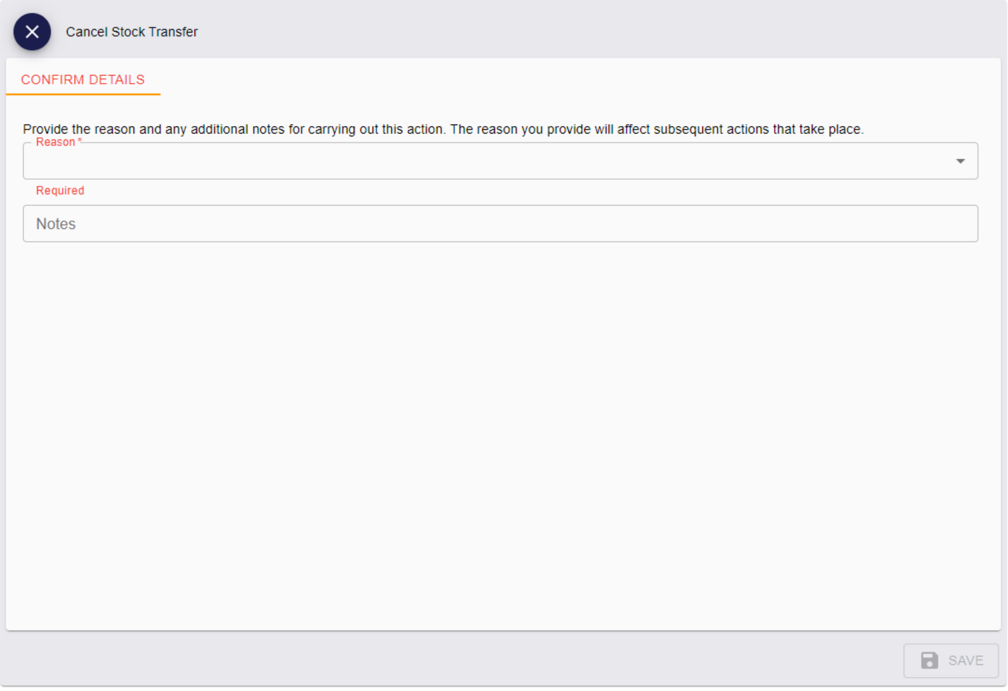
2. Search for a stock transfer and open it in the View Stock Transfer screen.

   For details of searching for a stock transfer, see section *11.2*, *Searching for a stock transfer*.

3. Click **Edit Stock Transfer** in the button bar at the bottom of the screen.

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

   The Cancel Stock Transfer screen appears.



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

Reason *

Required

Notes

4. Select a **Reason** for the cancellation from the drop-down list.

   Select one of the following options:

   - **Lost in Transit (Dispose)** – the devices allocated to the stock transfer are lost, and must be marked as disposed.
   - **Stock Returned / Not Dispatched** – the devices allocated to the stock transfer were returned from their destination or never dispatched, and are returned to their source location.

     Use this option if you added the incorrect devices to a stock transfer and want to correct the mistake.
5. Type any **Notes** in the box provided.
6. Click **Save**.

The stock transfer is canceled, and any devices that were allocated to it are removed from the stock transfer. The status of the devices is updated based on the **Reason** you provided; the devices are either marked as disposed, and cannot be used again, or are released and become available for use again.

11.6 Checking the contents of a stock transfer

MyID does not confirm that the devices you have selected as part of a stock transfer are the correct type, or are from the correct location. You can see if an individual device is assigned to a stock transfer from the View Device screen; however, there is no way to view a list of all devices assigned to a stock transfer within MyID.

If you want to confirm which devices are assigned to a stock transfer, you can run the following SQL against the MyID database:

```
select StockTransfers.ReadableName As StockTransfer, Devices.SerialNumber,
Devices.StockCode, Locations.Name As Location
from Devices
inner join StockTransfers on Devices.StockTransferID = Stocktransfers.ID
inner join Locations on Devices.LocationID = Locations.ID
order by Devices.StockTransferID
```

This returns a list of each active stock transfer, with the devices that are assigned to them, along with the devices' stock code and location. For example:

StockTransfer	SerialNumber	StockCode	Location
Headquarters to Western regional office, 10 units of Card (2023-02-03)	TN00013PX	Card	Headquarters
Headquarters to Western regional office, 10 units of Card (2023-02-03)	TN00014PX	Card	Headquarters
Headquarters to Western regional office, 10 units of Card (2023-02-03)	TN00015PX	Card	Headquarters

You can see from this report that only three devices have been assigned to the stock transfer, when the transfer calls for 10 (the `ReadableName` field in the `StockTransfers` table provides a good summary of what is expected for the transfer). You can now use the **Available Device Stock** report to locate seven additional devices with the Card stock code that are currently located at Headquarters, then use the **Transfer** option to assign them to the stock transfer.

If you discover that the transfer contains devices with the wrong stock code, or are in the wrong location, or the transfer contains too many devices, you can use the **Cancel Stock Transfer** option on the **View Transfer** screen, and select the **Stock Returned / Not Dispatched** option to release the devices and start again with a new stock transfer.

11.7 Dispatching a stock transfer

Once you have created a stock transfer and allocated devices to it, you can mark the transfer as dispatched.

To dispatch a stock transfer:

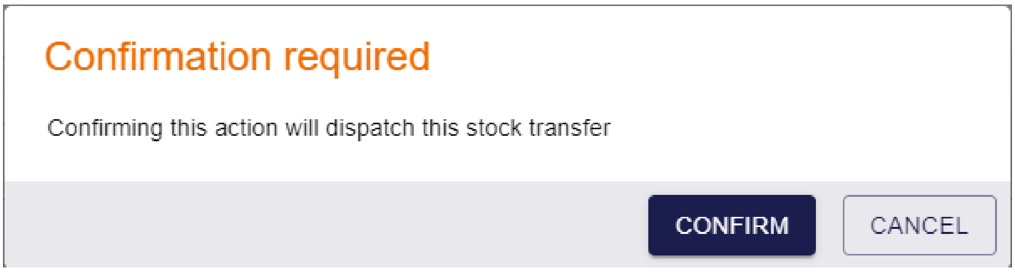
1. Select the **Stock Transfers** category.

   You must have the appropriate permissions to access this category. See section *8.1*, *Setting up inventory roles*.
2. Search for a stock transfer and open it in the View Stock Transfer screen.

   For details of searching for a stock transfer, see section *11.2*, *Searching for a stock transfer*.
3. Click **Dispatch Stock Transfer** in the button bar at the bottom of the screen.

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

   A confirmation dialog appears.

   Confirmation required

   Confirming this action will dispatch this stock transfer

4. Click **Confirm**.

The stock transfer is marked as dispatched, and the status is set to `InTransit`.

When a stock transfer is in transit, you can carry out the following actions:

- Edit the stock transfer.

  For example, you may want to edit the stock transfer to add a tracking number for the courier.

  See section *11.3*, *Editing a stock transfer*.
- Fail the stock transfer.

  If the stock transfer does not arrive at its destination, you must fail the stock transfer so that you can then cancel the stock transfer and update the allocated devices appropriately.

  See section *11.8*, *Failing a stock transfer*.
- Receive the stock transfer.

  When the stock transfer has arrived at its destination, you must mark it as received so that the allocated devices are added to their destination location.

  See section *11.9*, *Receiving a stock transfer*.

11.8 Failing a stock transfer

If you have dispatched a stock transfer, but it has failed to arrive at its destination, you can fail the transfer, indicating that it has been lost in transit, returned to sender, or is under investigation.

To fail a stock transfer:

1. Select the **Stock Transfers** category.

   You must have the appropriate permissions to access this category. See section *8.1*, *Setting up inventory roles*.

2. Search for a stock transfer and open it in the View Stock Transfer screen.

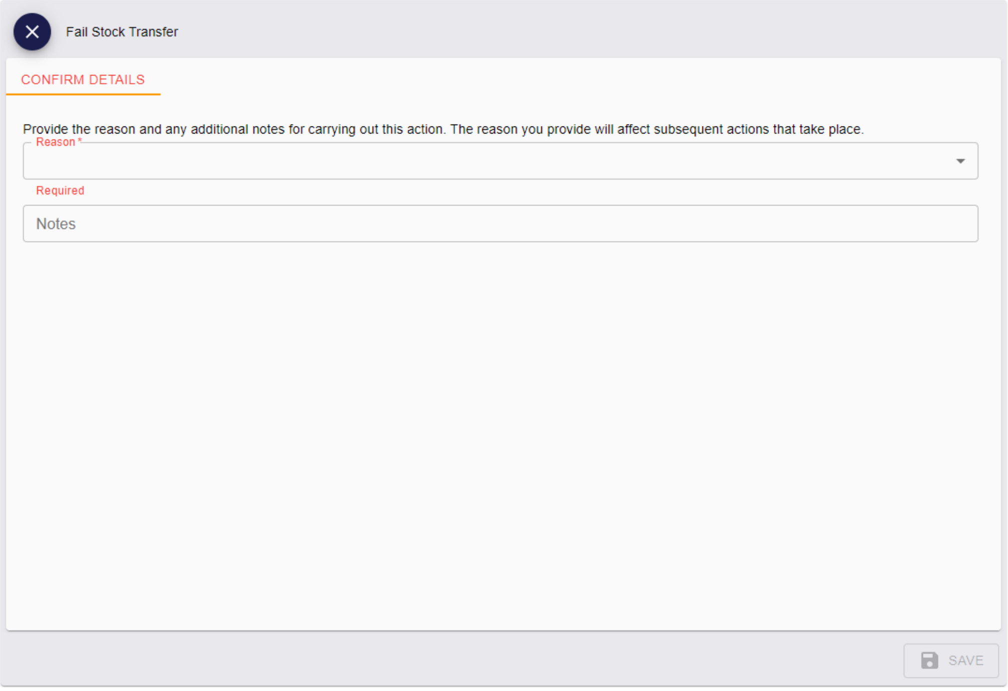
   For details of searching for a stock transfer, see section *11.2*, *Searching for a stock transfer*.

3. Click **Fail Stock Transfer** in the button bar at the bottom of the screen.

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

   Note: You can fail a stock transfer only if it has a status of `InTransit`.

   The Fail Stock Transfer screen appears.



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

4. Select a **Reason** for the failure from the drop-down list.

   Select one of the following options:

   - **Lost in Transit (Dispose)** – the devices allocated to the stock transfer are lost.
   - **Stock Returned / Not Dispatched** – the devices allocated to the stock transfer were returned from their destination or never dispatched.
   - **Not Received / Pending Investigation** – the status of the stock transfer is unclear and requires investigation.

   Important: Setting a reason for the failure does *not* change the status of the devices allocated to the stock transfer. Once you have failed the stock transfer, you must use the **Cancel Stock Transfer** option to update the status of the devices. Note also that you cannot change a stock transfer from failed to received even if the package eventually arrives at its destination, so do not use the **Not Received / Pending Investigation** option for deliveries that may just be delayed in transit.

5. Type any **Notes** in the box provided.
6. Click **Save**.

The status of the stock transfer is changed to `Failed`. To dispose of or release the devices allocated to the stock transfer, use the **Cancel Stock Transfer** option; see section *11.5*, *Canceling a stock transfer*.

11.9 Receiving a stock transfer

Once a stock transfer has been received at its destination, you can mark the transfer as received. When you do this, the devices in the stock transfer are updated to have the destination as their specified location, and the unallocated stock at the destination is updated.

To receive a stock transfer:

1. Select the **Stock Transfers** category.

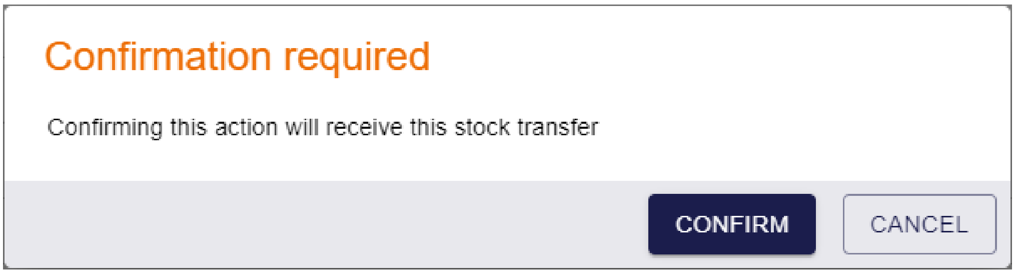
   You must have the appropriate permissions to access this category. See section *8.1*, *Setting up inventory roles*.
2. Search for a stock transfer and open it in the View Stock Transfer screen.

   For details of searching for a stock transfer, see section *11.2*, *Searching for a stock transfer*.
3. Click **Receive Stock Transfer** in the button bar at the bottom of the screen.

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

   Note: You can receive a stock transfer only if it has a status of `InTransit`.

   A confirmation dialog appears.

   Confirmation required

   Confirming this action will receive this stock transfer

4. Click **Confirm**.

The stock transfer is now marked as received, and all devices allocated to the stock transfer are added to the available stock of the destination location.

12 Working with 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.

The MyID Operator Client allows you to work with additional identities in the following ways:

- You can create an additional identity manually, providing all the details without importing the record from a directory.

  See section *12.1*, *Creating an additional identity*.
- You can edit an additional identity that you have created manually.

  See section *12.2*, *Editing an additional identity*.
- You can import an additional identity from a directory.

  See section *12.3*, *Importing an additional identity*.
- You can remove an additional identity.

  See section *12.4*, *Removing an additional identity*.
- You can view the certificates associated with an additional identity.

  See section *13.1.4*, *View an additional identity's certificates*.

For information about configuring your system for additional identities, see the *Additional identities* section in the ***Administration Guide***.

12.1 Creating an additional identity

Instead of importing an additional identity from a directory, you can add the details manually. The User Principal Name, Distinguished Name, and User SID must match an entry in a directory for the additional identity certificate to be used for Windows authentication. You must ensure that the details you enter are correct for the systems that will use the certificates.

You can create an additional identity manually only for another person; you cannot create an additional identity manually for your own account. For your own account, you must import an additional identity instead to ensure that it comes from a trusted source.

Note: If you have a credential issued to a person that supports additional identities (that is, it has the **Issue Additional Identities** option selected in the credential profile), and you create an additional identity, if the **Automatically create card update jobs when additional identities are modified** configuration option (on the **Issuance Processes** page of the **Operation Settings** workflow) is set to Yes, a job is created automatically to update the credential.

To create an additional identity manually:

1. Search for a person, and view their details.

   See section *4.1*, *Searching for a person* for details.

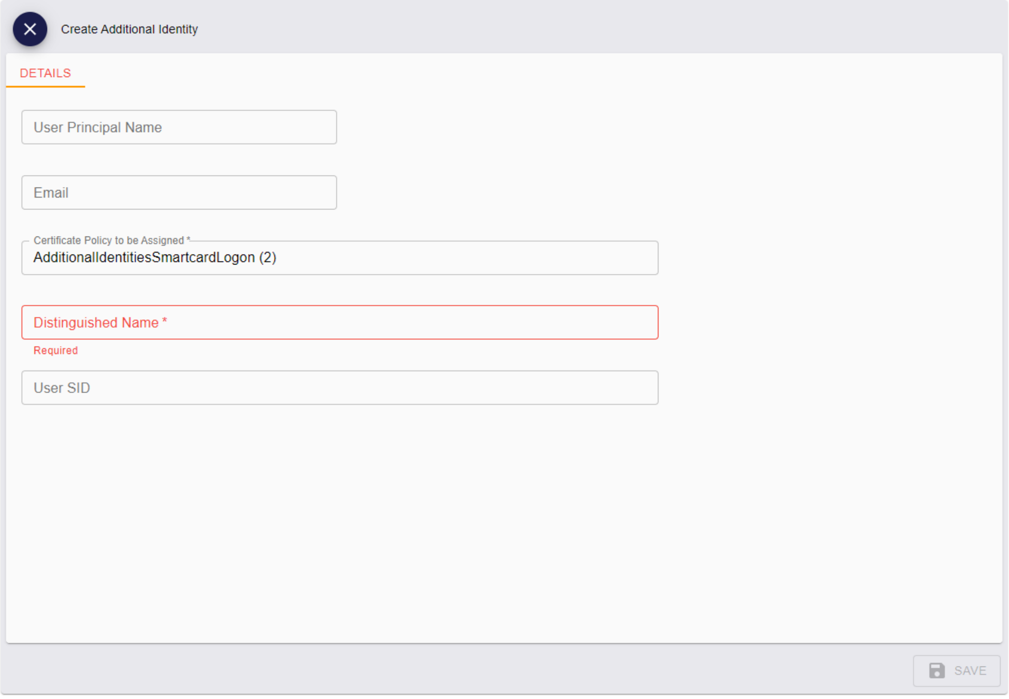
You can also view a person's details from any form that contains a link to their account. For example:

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

2. Click the **Create Additional Identity** option in the button bar at the bottom of the screen.

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

   Note: You cannot create an additional identity manually for your own account.


Create Additional Identity
DETAILS
User Principal Name
Email

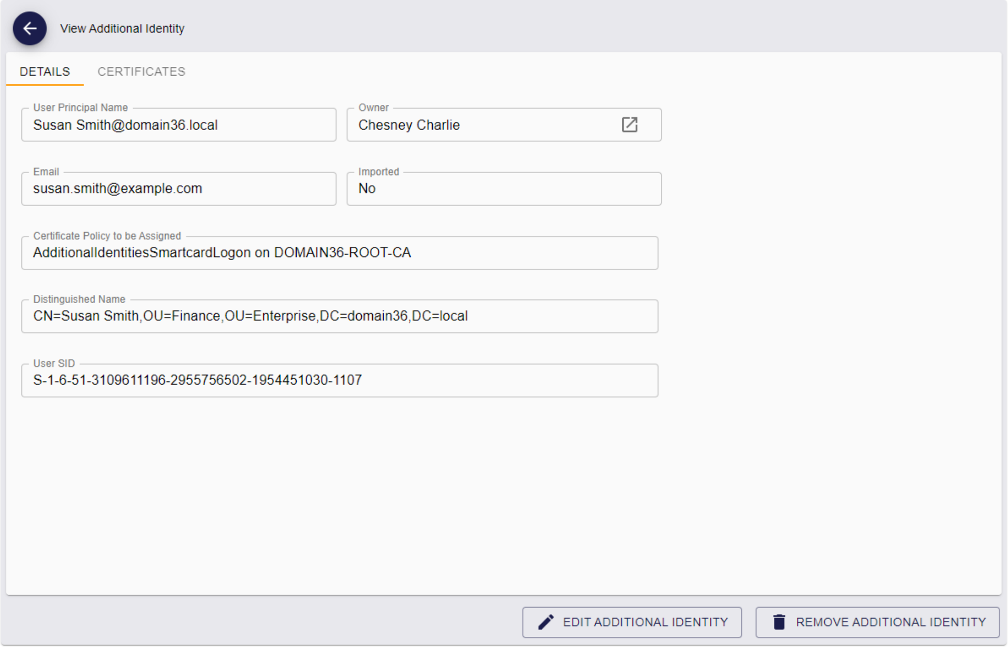
Certificate Policy to be Assigned *: AdditionalIdentitiesSmartcardLogon (2)

Distinguished Name *
Required
User SID
SAVE

3. Complete the following details:
   - **User Principal Name**
   - **Email**
   - **Certificate Policy to be Assigned**

     Note: If you have only one certificate policy configured for additional identities, it is selected automatically.
   - **Distinguished Name**
   - **User SID**
4. Click **Save**.

The View Additional Identity screen appears.



User Principal Name: Susan Smith@domain36.local
Owner: Chesney Charlie
Email: susan.smith@example.com
Imported: No
Certificate Policy to be Assigned: AdditionalIdentitiesSmartcardLogon on DOMAIN36-ROOT-CA
Distinguished Name: CN=Susan Smith,OU=Finance,OU=Enterprise,DC=domain36,DC=local
User SID: S-1-6-51-3109611196-2955756502-1954451030-1107

You can access this screen at any time from the **Additional Identities** tab on the View Person screen.

From this screen, you can:

- View the details of the additional identity.
- Use the **Certificates** tab to view the certificates associated with the additional identity.

  See section *13.1.4*, *View an additional identity's certificates*.
- Edit the details of the additional identity.

  See section *12.2*, *Editing an additional identity*.
- Remove the additional identity.

  See section *12.4*, *Removing an additional identity*.

12.2 Editing an additional identity

If you have created an additional identity manually, you can edit its details. You cannot edit imported additional identities.

Note: If you have a credential issued to a person that supports additional identities (that is, it has the **Issue Additional Identities** option selected in the credential profile), and you edit an additional identity, if the **Automatically create card update jobs when additional identities are modified** configuration option (on the **Issuance Processes** page of the **Operation Settings** workflow) is set to Yes, a job is created automatically to update the credential.

To edit an additional identity:

1. Search for a person, and view their details.

   See section *4.1*, *Searching for a person* for details.

   You can use the **Additional Identities (AID)** alternative report to search. This report returns a list of additional identities; when you select an additional identity, it opens the View Person screen for the owner of the additional identity. See section *7.3.26*, *Additional Identities (AID) report* for details.

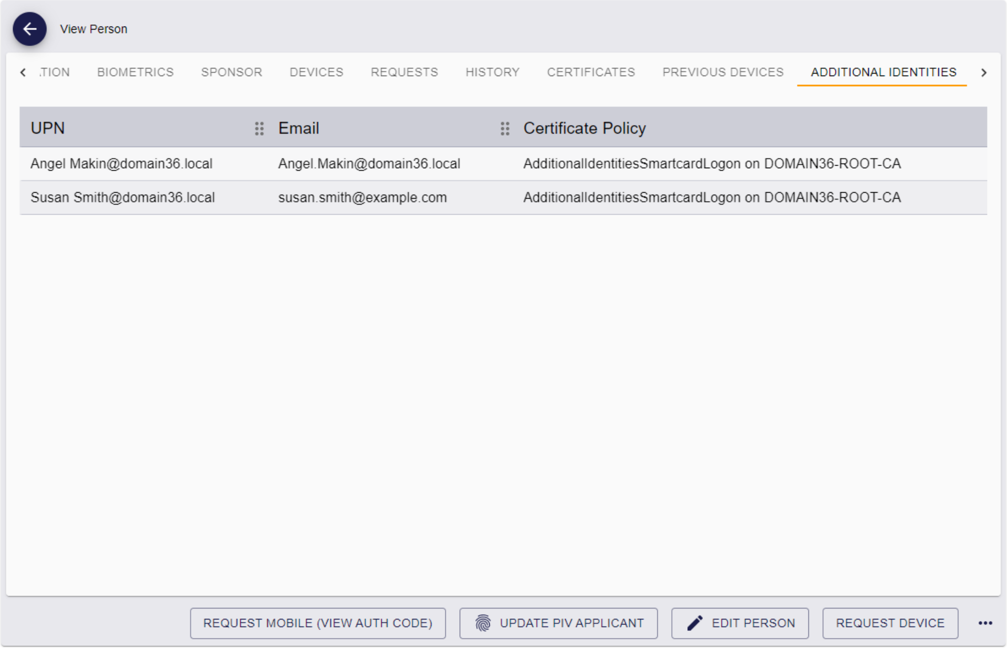
   You can also view a person's details from any form that contains a link to their account.

   For example:

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

2. Select the **Additional Identities** tab.

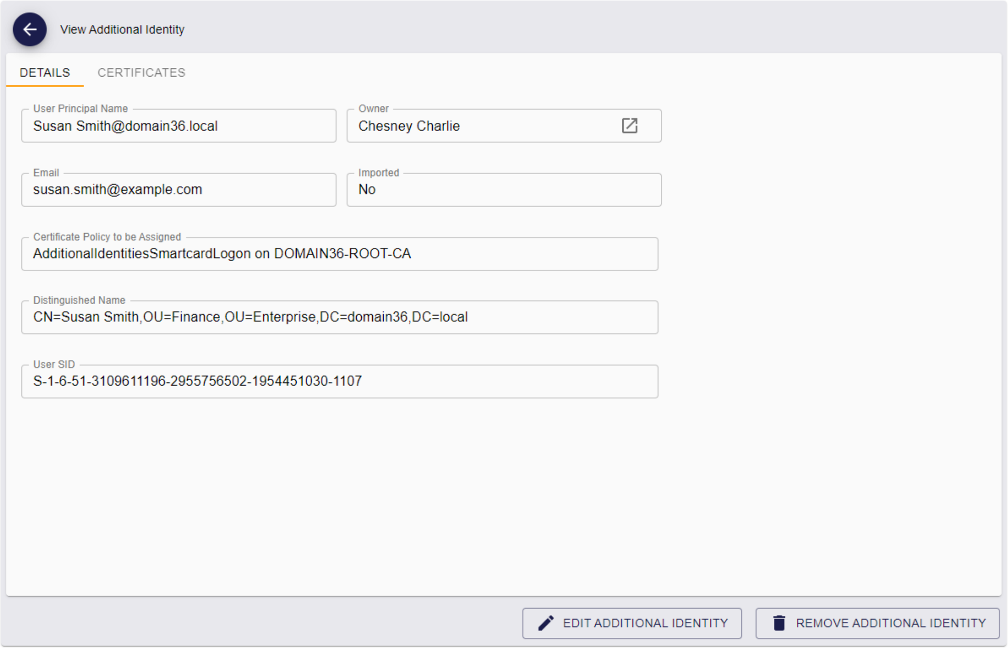
   The list of additional identities owned by the person appears.


View Person
TION
BIOMETRICS
SPONSOR
DEVICES
REQUESTS
HISTORY
CERTIFICATES
PREVIOUS DEVICES
ADDITIONAL IDENTITIES
REQUEST MOBILE (VIEW AUTH CODE)
UPDATE PIV APPLICANT
EDIT PERSON
REQUEST DEVICE

UPN	Email	Certificate Policy
Angel Makin@domain36.local	Angel.Makin@domain36.local	AdditionalIdentitiesSmartcardLogon on DOMAIN36-ROOT-CA
Susan Smith@domain36.local	susan.smith@example.com	AdditionalIdentitiesSmartcardLogon on DOMAIN36-ROOT-CA

3. Select an additional identity from the list.

   The View Additional Identity screen appears.


View Additional Identity
DETAILS
CERTIFICATES
EDIT ADDITIONAL IDENTITY
REMOVE ADDITIONAL IDENTITY

User Principal Name: Susan Smith@domain36.local

Owner: Chesney Charlie

Email: susan.smith@example.com

Imported: No

Certificate Policy to be Assigned: AdditionalIdentitiesSmartcardLogon on DOMAIN36-ROOT-CA

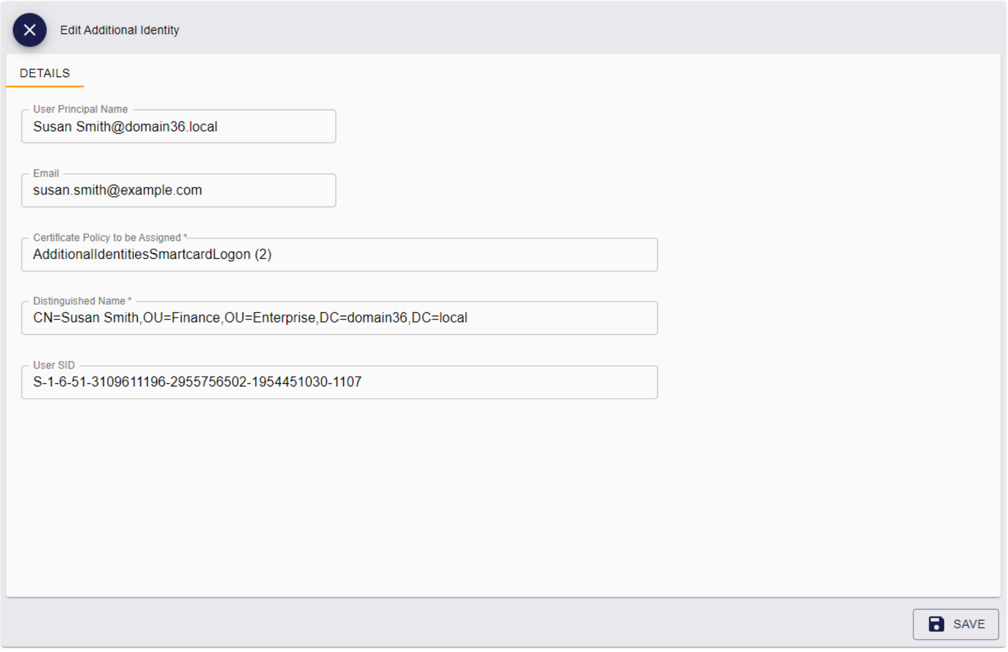
Distinguished Name: CN=Susan Smith,OU=Finance,OU=Enterprise,DC=domain36,DC=local

User SID: S-1-6-51-3109611196-2955756502-1954451030-1107

4. Click **Edit Additional Identity**.

   Note: You cannot edit an additional identity if it was imported.

   The Edit Additional Identity screen appears.


Edit Additional Identity
DETAILS
SAVE

User Principal Name: Susan Smith@domain36.local

Email: susan.smith@example.com

Certificate Policy to be Assigned *: AdditionalIdentitiesSmartcardLogon (2)

Distinguished Name *: CN=Susan Smith,OU=Finance,OU=Enterprise,DC=domain36,DC=local

User SID: S-1-6-51-3109611196-2955756502-1954451030-1107

5. Edit the details of the additional identity, then click **Save**.

12.3 Importing an additional identity

You can import an additional identity from your directory. You can allow an operator to import an additional identity for another person, or allow a person to import an additional identity for their own account. In both cases, you can set a filter on the LDAP query to restrict the directory entries available to be added as additional identities.

Note: If you have a credential issued to a person that supports additional identities (that is, it has the **Issue Additional Identities** option selected in the credential profile), and you import an additional identity, if the **Automatically create card update jobs when additional identities are modified** configuration option (on the **Issuance Processes** page of the **Operation Settings** workflow) is set to Yes, a job is created automatically to update the credential.

To import an additional identity:

1. Search for a person, and view their details.

   See section *4.1*, *Searching for a person* for details.

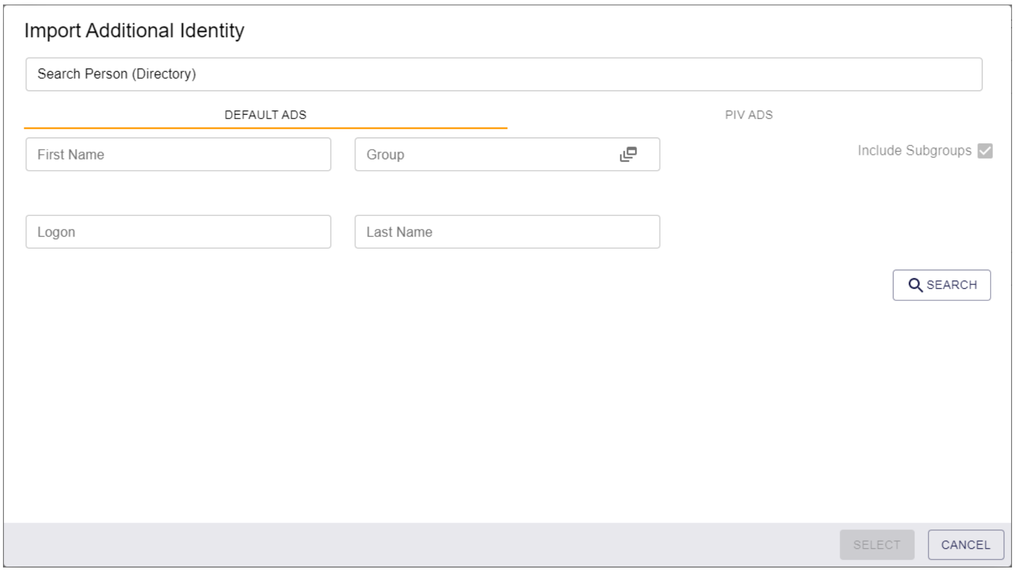
   You can also view a person's details from any form that contains a link to their account. For example:

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

2. Click the **Import Additional Identity** option in the button bar at the bottom of the screen.

   Note: If you are viewing your own record, the button is labeled **Import My Additional Identity**.

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



3. If you have more than one directory, select the directory you want to search using the tabs.

4. Type your search criteria.

   You can search using the following criteria:

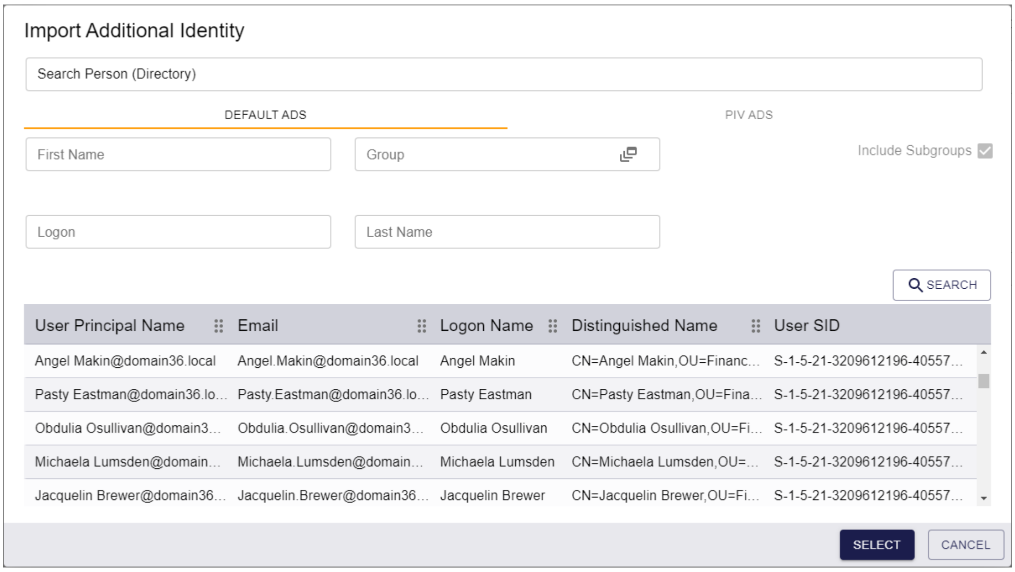
   - **First Name**
   - **Last Name**
   - **Logon**
   - **Group**

5. Click **Search**.

   Note: To set up a filter for the results returned from the directory, in the **Operation Settings** workflow, on the **LDAP** tab, you can set the following options:

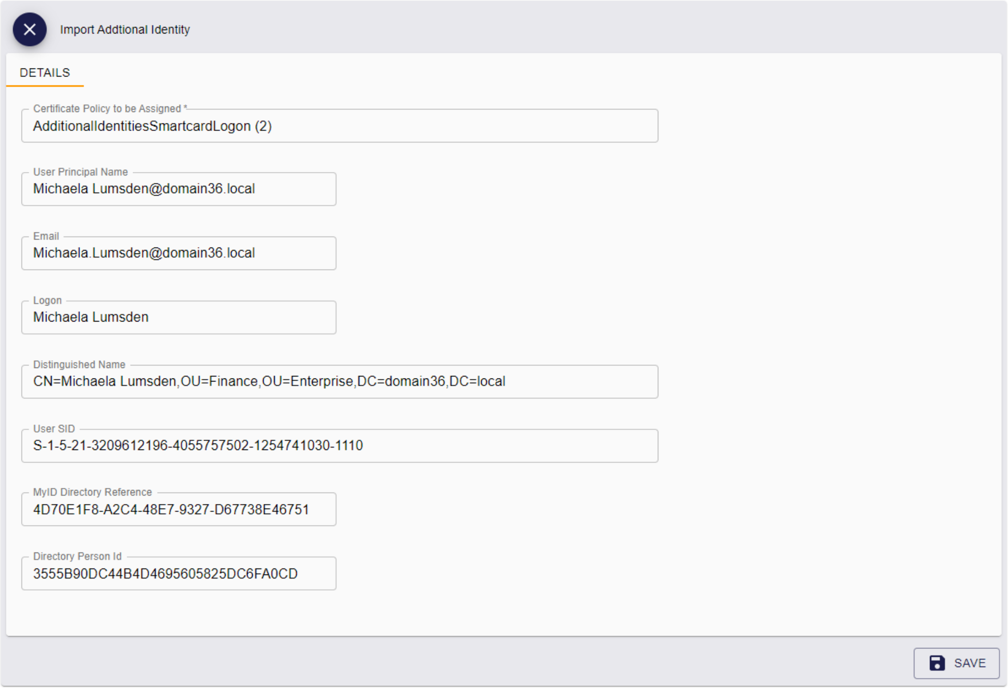
   - **Additional Identity LDAP Operator User Filter** – set a query filter when importing an additional identity for another person.
   - **Additional Identity LDAP Self-Service User Filter** – set a query filter when importing an additional identity for your own account.

   For further information, see the *Setting up additional identities* section in the ***Administration Guide***.



User Principal Name	Email	Logon Name	Distinguished Name	User SID
Angel Makin@domain36.local	Angel.Makin@domain36.local	Angel Makin	CN=Angel Makin,OU=Financ...	S-1-5-21-3209612196-40557...
Pasty Eastman@domain36.lo...	Pasty.Eastman@domain36.lo...	Pasty Eastman	CN=Pasty Eastman,OU=Fina...	S-1-5-21-3209612196-40557...
Obdulia Osullivan@domain3...	Obdulia.Osullivan@domain3...	Obdulia Osullivan	CN=Obdulia Osullivan,OU=Fi...	S-1-5-21-3209612196-40557...
Michaela Lumsden@domain...	Michaela.Lumsden@domain...	Michaela Lumsden	CN=Michaela Lumsden,OU=...	S-1-5-21-3209612196-40557...
Jacquelin Brewer@domain36...	Jacquelin.Brewer@domain36...	Jacquelin Brewer	CN=Jacquelin Brewer,OU=Fi...	S-1-5-21-3209612196-40557...

6. Select the LDAP record you want to import, then click **Select**.



Certificate Policy to be Assigned *: AdditionalIdentitiesSmartcardLogon (2)

User Principal Name: Michaela Lumsden@domain36.local

Email: Michaela.Lumsden@domain36.local

Logon: Michaela Lumsden

Distinguished Name: CN=Michaela Lumsden,OU=Finance,OU=Enterprise,DC=domain36,DC=local

User SID: S-1-5-21-3209612196-4055757502-1254741030-1110

MyID Directory Reference: 4D70E1F8-A2C4-48E7-9327-D67738E46751

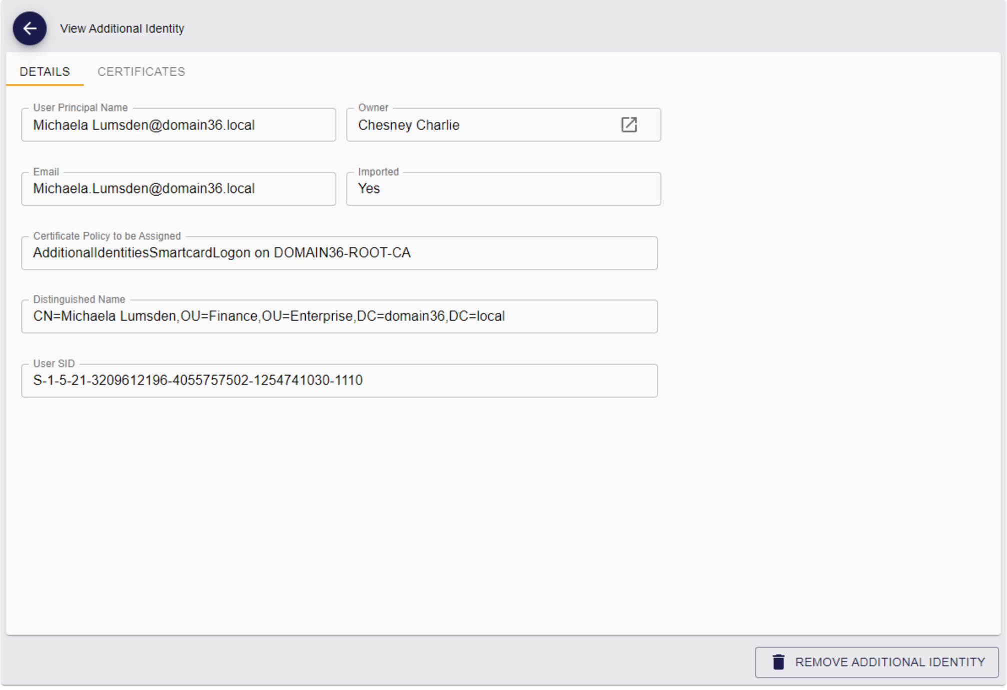
Directory Person Id: 3555B90DC44B4D4695605825DC6FA0CD

7. Select the certificate policy you want to use from the **Certificate Policy to be Assigned** drop-down list.

   Note: If you have only one certificate policy configured for additional identities, it is selected automatically.

8. Review the details of the additional identity, then click **Save**.

   The View Additional Identity screen appears.



User Principal Name: Michaela.Lumsden@domain36.local
Owner: Chesney Charlie
Email: Michaela.Lumsden@domain36.local
Imported: Yes
Certificate Policy to be Assigned: AdditionalIdentitiesSmartcardLogon on DOMAIN36-ROOT-CA
Distinguished Name: CN=Michaela Lumsden,OU=Finance,OU=Enterprise,DC=domain36,DC=local
User SID: S-1-5-21-3209612196-4055757502-1254741030-1110

You can access this screen at any time from the **Additional Identities** tab on the View Person screen.

From this screen, you can:

- View the details of the additional identity.
- Use the **Certificates** tab to view the certificates associated with the additional identity.

  See section *13.1.4*, *View an additional identity's certificates*.
- Remove the additional identity.

  See section *12.4*, *Removing an additional identity*.

Note: You cannot edit an imported additional identity. You can edit additional identities only if you create them manually rather than importing them from a directory.

12.4 Removing an additional identity

If you no longer need an additional identity, you can remove it. Any certificates that were issued as part of the additional identity are revoked.

To remove an additional identity:

1. Search for a person, and view their details.

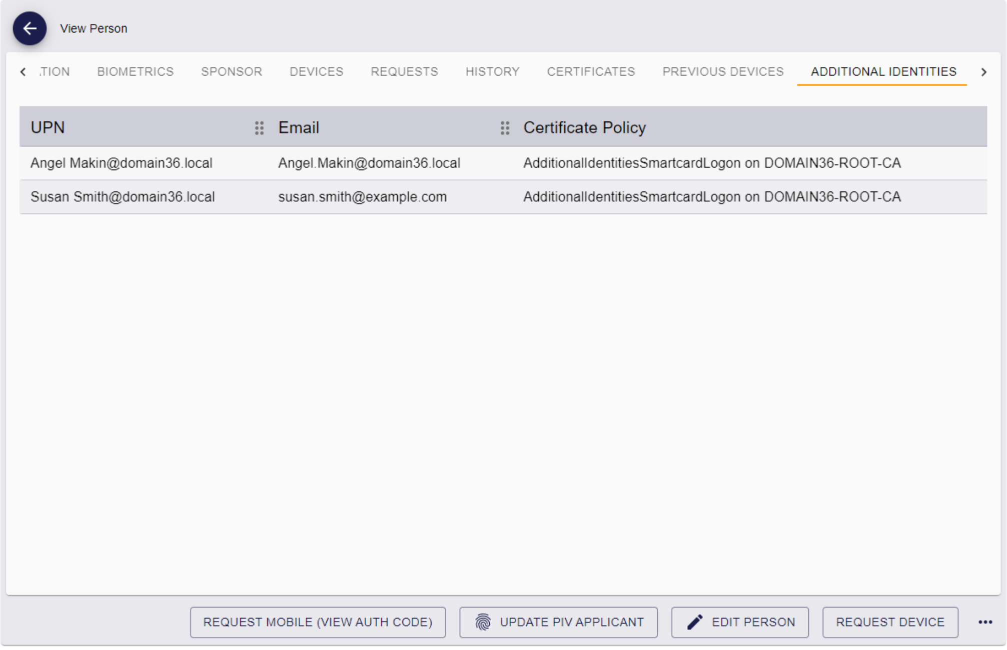
   See section *4.1*, *Searching for a person* for details.

   You can use the **Additional Identities (AID)** alternative report to search. This report returns a list of additional identities; when you select an additional identity, it opens the View Person screen for the owner of the additional identity. See section *7.3.26*, *Additional Identities (AID) report* for details.

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

   - Click the link icon ↗ on the **Full Name** field of the View Request form.
   - Click the link icon ↗ on the **Owner** field of the View Device form.
2. Select the **Additional Identities** tab.

   The list of additional identities owned by the person appears.

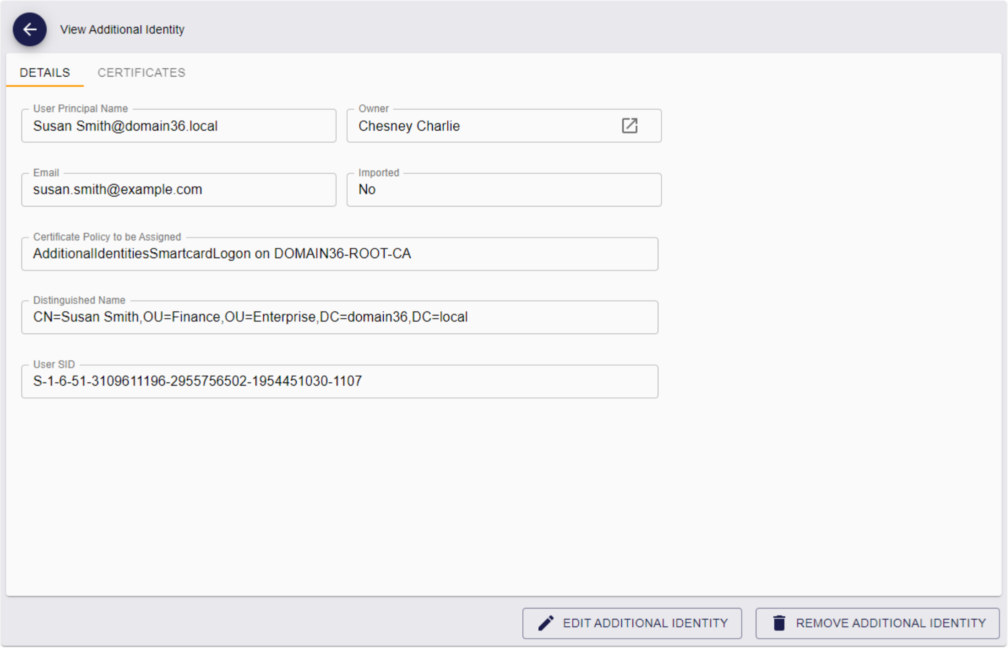

View Person
.TION
BIOMETRICS
SPONSOR
DEVICES
REQUESTS
HISTORY
CERTIFICATES
PREVIOUS DEVICES
ADDITIONAL IDENTITIES

UPN	Email	Certificate Policy
Angel Makin@domain36.local	Angel.Makin@domain36.local	AdditionalIdentitiesSmartcardLogon on DOMAIN36-ROOT-CA
Susan Smith@domain36.local	susan.smith@example.com	AdditionalIdentitiesSmartcardLogon on DOMAIN36-ROOT-CA

REQUEST MOBILE (VIEW AUTH CODE)
UPDATE PIV APPLICANT
EDIT PERSON
REQUEST DEVICE
...

3. Select an additional identity from the list.

   The View Additional Identity screen appears.


View Additional Identity
DETAILS
CERTIFICATES
EDIT ADDITIONAL IDENTITY
REMOVE ADDITIONAL IDENTITY

User Principal Name: Susan Smith@domain36.local

Owner: Chesney Charlie

Email: susan.smith@example.com

Imported: No

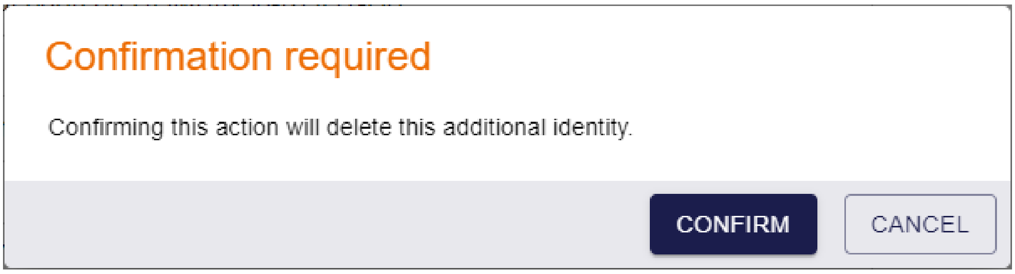
Certificate Policy to be Assigned: AdditionalIdentitiesSmartcardLogon on DOMAIN36-ROOT-CA

Distinguished Name: CN=Susan Smith,OU=Finance,OU=Enterprise,DC=domain36,DC=local

User SID: S-1-6-51-3109611196-2955756502-1954451030-1107

4. Click **Remove Additional Identity**.

   The confirmation screen appears.


CONFIRM
CANCEL

Confirmation required

Confirming this action will delete this additional identity.

5. Click **Confirm** to delete the additional identity, or **Cancel** to cancel the operation.

13 Working with certificates

MyID allows you to manage your certificates either through the device that contains them or as individual certificates. For information on managing your devices, see section *5*, *Working with devices*.

The MyID Operator Client allows you to work with certificates in the following ways:

- You can view the details of a certificate.

  See section *13.1*, *Viewing a certificate*.
- You can revoke, suspend, or unsuspend a certificate.

  See section *13.2*, *Revoking, suspending, and unsuspending certificates*.
- You can pause and resume processing of a certificate.

  See section *13.3*, *Pausing and resuming certificate processing*.
- You can change the renewal settings for a certificate.

  See section *13.4*, *Changing renewal settings for a certificate*.

13.1 Viewing a certificate

You can view a certificate in the following ways:

- Searching for a certificate.

  See section *13.1.1*, *Searching for a certificate*.
- Viewing the list of certificates assigned to a person.

  See section *13.1.2*, *Viewing a person's certificates*.
- Viewing the list of certificates assigned to a device.

  See section *13.1.3*, *Viewing a device's certificates*.
- Viewing the list of certificates assigned to an additional identity.

  See section *13.1.4*, *View an additional identity's certificates*.

Once you have displayed the list of certificates, you can click on a certificate in the list to display the View Certificate screen, which allows you to manage the certificate. See section *13.1.5*, *Viewing a certificate's details*.

13.1.1 Searching for a certificate

To search for a certificate:

1. Click the **Certificates** category.
2. Enter some or all of the search criteria for the certificate.

   The following search criteria are available:

   - **Certificate Policy** – select the certificate policy that was used to issue the certificate.
   - **Certificate Authority** – select the certificate authority that was used to issue the certificate.
   - **Certificate Status** – select the status of the certificate.
   - **Certificate Serial Number** – type the serial number of the certificate. You can use wildcards.
   - **Issued After** – select the date after which the certificate was issued.
   - **Issued Before** – select the date before which the certificate was issued.
   - **Expiry Date After** – select the date after which the certificate expires.
   - **Expiry Date Before** – select the date before which the certificate expires.
   - **Maximum Days to Expiry** – type the maximum number of days before the certificate expires; for example, type `30` to search for certificates that expire in the next 30 days.
   - **User DN** – type the user DN associated with the certificate. You can use wildcards.
   - **User SID Present** – select whether the certificate has a User Security Identifier associated with it.

     See the *Including user security identifiers in certificates* section in the ***Administration Guide*** for details.
   - **User SID** – type the User Security Identifier associated with the certificate. You can use wildcards.
3. Click **Search**.

   The list of matching results appears.
4. To carry out actions on multiple requests, select the checkbox to the left of the certificates, then from the **Tools** menu select the batch operation.

   From this menu, you can:

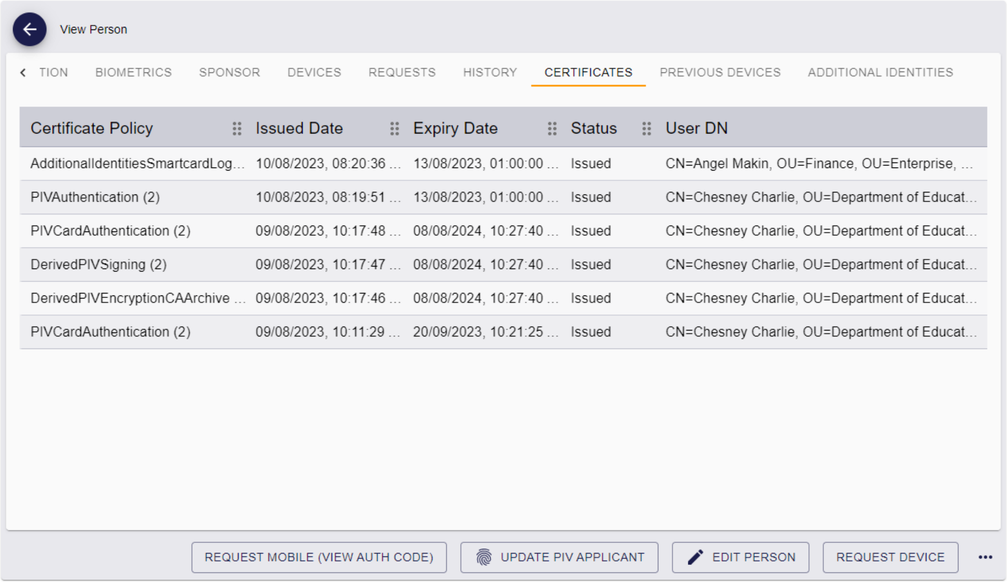
   - Edit the certificate renewal details.
   - Pause or resume certificate processing.
   - Revoke certificates.
   - Unsuspend certificates.

   Note: You can access the **Tools** menu only if you have a role with the **Tools Menu** option from the **Configuration** section of the **Edit Roles** workflow.
5. To work on a single certificate, click a record to display the View Certificate screen.

   See section *13.1.5*, *Viewing a certificate's details*.

13.1.2 Viewing a person's certificates

To view the list of all certificates issued to a person, on the View Person screen, click the **Certificates** tab.



View Person
TION
BIOMETRICS
SPONSOR
DEVICES
REQUESTS
HISTORY
CERTIFICATES
PREVIOUS DEVICES
ADDITIONAL IDENTITIES

Certificate Policy	Issued Date	Expiry Date	Status	User DN
AdditionalIdentitiesSmartcardLog...	10/08/2023, 08:20:36 ...	13/08/2023, 01:00:00 ...	Issued	CN=Angel Makin, OU=Finance, OU=Enterprise, ...
PIVAuthentication (2)	10/08/2023, 08:19:51 ...	13/08/2023, 01:00:00 ...	Issued	CN=Chesney Charlie, OU=Department of Educat...
PIVCardAuthentication (2)	09/08/2023, 10:17:48 ...	08/08/2024, 10:27:40 ...	Issued	CN=Chesney Charlie, OU=Department of Educat...
DerivedPIVSigning (2)	09/08/2023, 10:17:47 ...	08/08/2024, 10:27:40 ...	Issued	CN=Chesney Charlie, OU=Department of Educat...
DerivedPIVEncryptionCAArchive ...	09/08/2023, 10:17:46 ...	08/08/2024, 10:27:40 ...	Issued	CN=Chesney Charlie, OU=Department of Educat...
PIVCardAuthentication (2)	09/08/2023, 10:11:29 ...	20/09/2023, 10:21:25 ...	Issued	CN=Chesney Charlie, OU=Department of Educat...

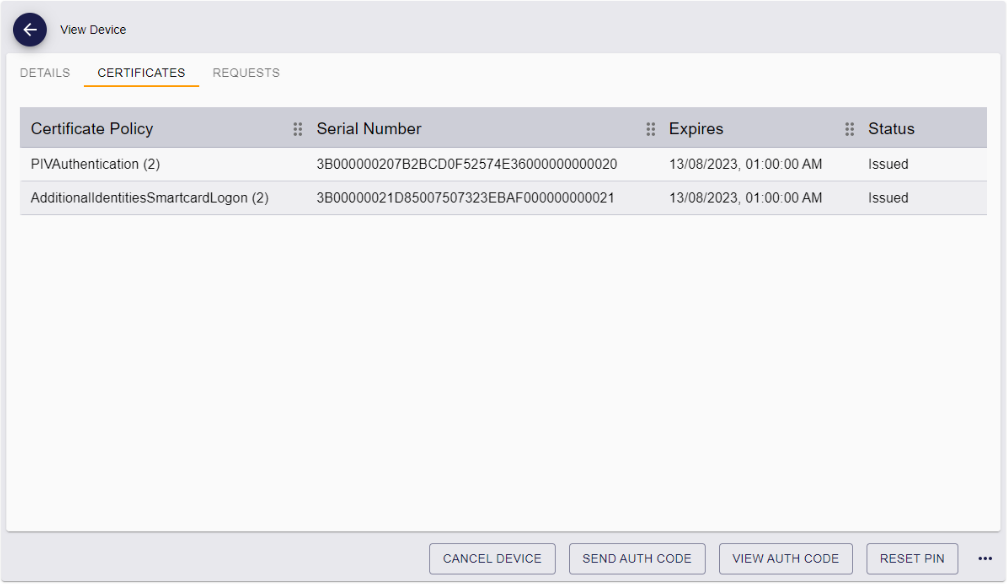
REQUEST MOBILE (VIEW AUTH CODE)
UPDATE PIV APPLICANT
EDIT PERSON
REQUEST DEVICE
...

See section *4.1*, *Searching for a person* for details of accessing the View Person screen.

Click a certificate to display the View Certificate screen for that certificate. See section *13.1.5*, *Viewing a certificate's details*.

13.1.3 Viewing a device's certificates

To view the list of all certificates on a device, on the View Device screen, click the **Certificates** tab.



View Device
DETAILS
CERTIFICATES
REQUESTS

Certificate Policy	Serial Number	Expires	Status
PIVAuthentication (2)	3B000000207B2BCD0F52574E36000000000020	13/08/2023, 01:00:00 AM	Issued
AdditionalIdentitiesSmartcardLogon (2)	3B00000021D85007507323EBAF000000000021	13/08/2023, 01:00:00 AM	Issued

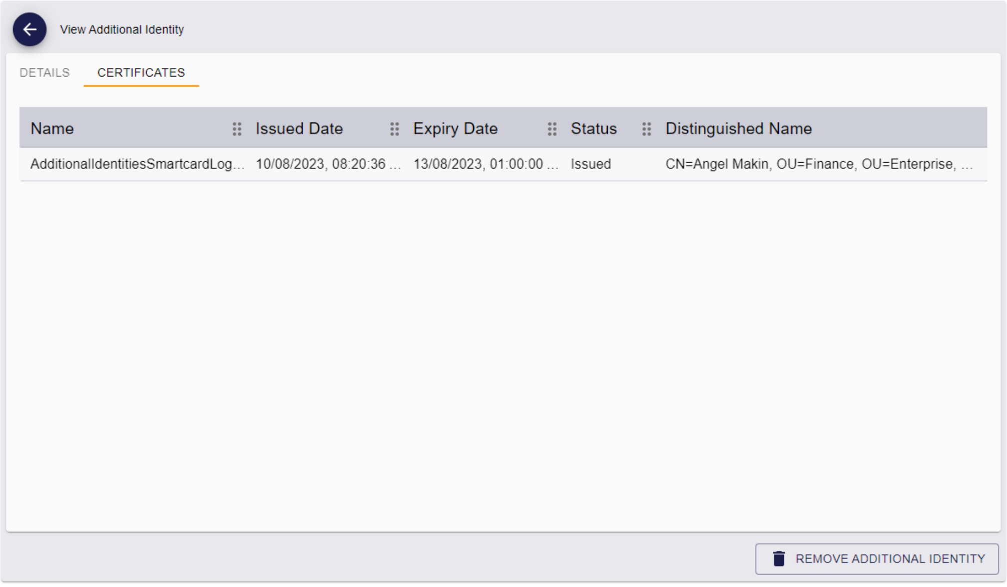
CANCEL DEVICE
SEND AUTH CODE
VIEW AUTH CODE
RESET PIN
•••

See section *5.1*, *Searching for a device* for details of accessing the View Device screen.

Click a certificate to display the View Certificate screen for that certificate. See section *13.1.5*, *Viewing a certificate's details*.

13.1.4 View an additional identity's certificates

To view a list of the certificates assigned to an additional identity, on the View Additional Identity screen, click the **Certificates** tab.



Name	Issued Date	Expiry Date	Status	Distinguished Name
AdditionalIdentitiesSmartcardLog…	10/08/2023, 08:20:36 …	13/08/2023, 01:00:00 …	Issued	CN=Angel Makin, OU=Finance, OU=Enterprise, …

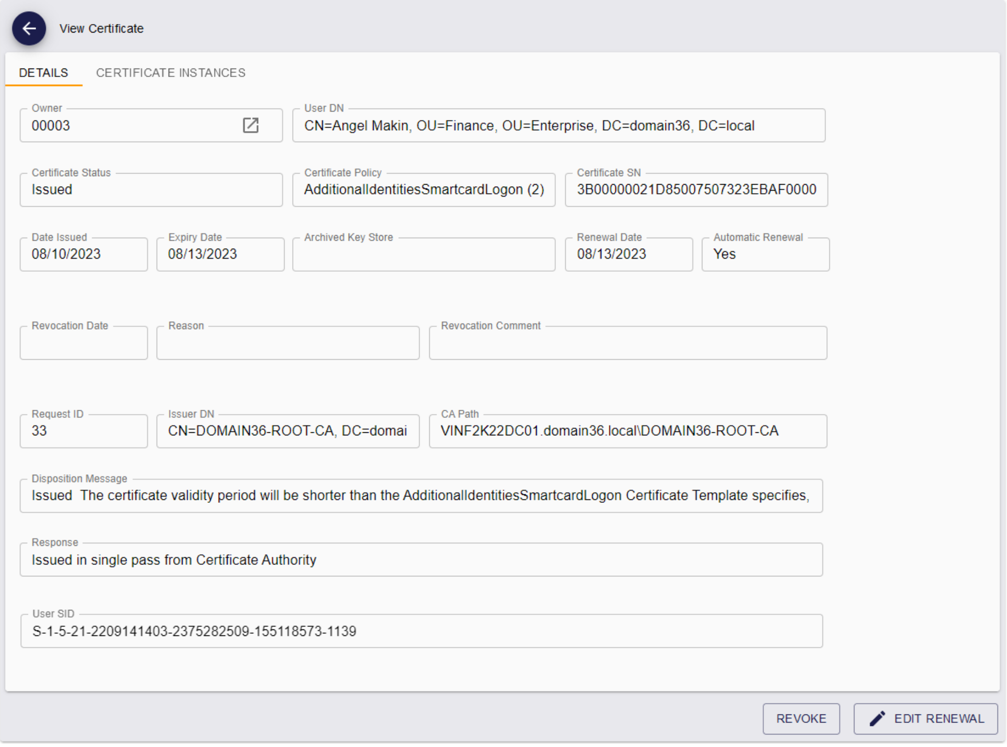
You can access the View Additional Identity screen from the **Additional Identities** tab of the View Person screen.

See section *12*, *Working with additional identities* for details of working with additional identities.

Click a certificate to display the View Certificate screen for that certificate. See section *13.1.5*, *Viewing a certificate's details*.

13.1.5 Viewing a certificate's details

The View Certificate screen allows you to view a certificate's details.


View Certificate
DETAILS
CERTIFICATE INSTANCES
REVOKE
EDIT RENEWAL

Owner: 00003

User DN: CN=Angel Makin, OU=Finance, OU=Enterprise, DC=domain36, DC=local

Certificate Status: Issued

Certificate Policy: AdditionalIdentitiesSmartcardLogon (2)

Certificate SN: 3B00000021D85007507323EBAF0000

Date Issued: 08/10/2023

Expiry Date: 08/13/2023

Archived Key Store:

Renewal Date: 08/13/2023

Automatic Renewal: Yes

Revocation Date:

Reason:

Revocation Comment:

Request ID: 33

Issuer DN: CN=DOMAIN36-ROOT-CA, DC=domai

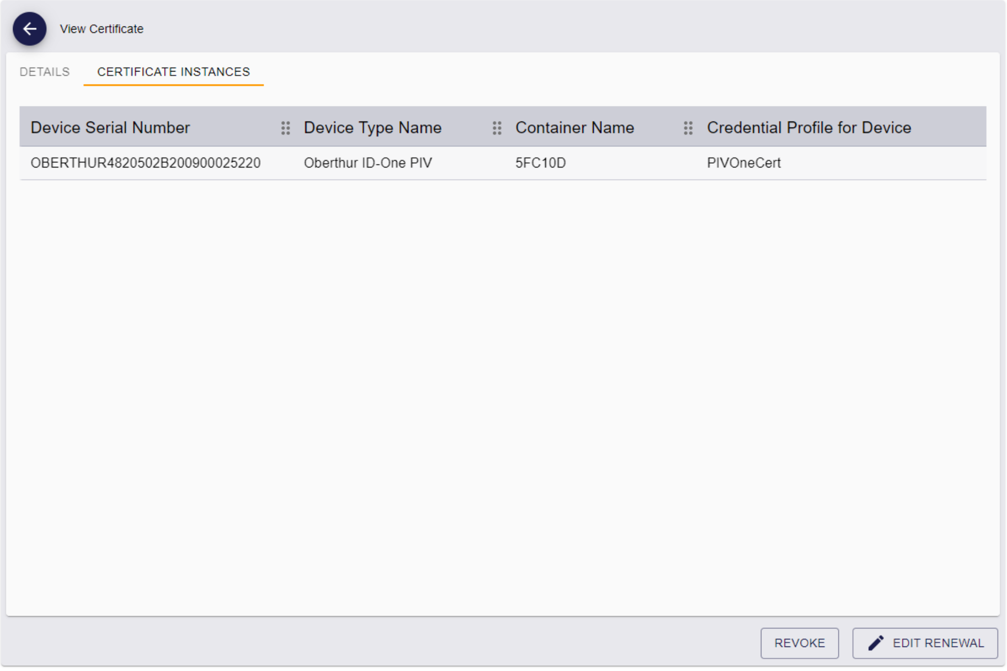
CA Path: VINF2K22DC01.domain36.local\DOMAIN36-ROOT-CA

Disposition Message: Issued The certificate validity period will be shorter than the AdditionalIdentitiesSmartcardLogon Certificate Template specifies,

Response: Issued in single pass from Certificate Authority

User SID: S-1-5-21-2209141403-2375282509-155118573-1139

To view the devices where the certificate resides, click the **Certificate Instances** tab.


View Certificate
DETAILS
CERTIFICATE INSTANCES
REVOKE
EDIT RENEWAL

Device Serial Number	Device Type Name	Container Name	Credential Profile for Device
OBERTHUR4820502B200900025220	Oberthur ID-One PIV	5FC10D	PIVOneCert

You can click on a device in the list to display the View Device screen for that device.

From the View Certificate screen, you can also:

- Revoke, suspend, or unsuspend a certificate.

  See section *13.2*, *Revoking, suspending, and unsuspending certificates*.
- Pause and resume processing of a certificate.

  See section *13.3*, *Pausing and resuming certificate processing*.
- Change the renewal settings for a certificate.

  See section *13.4*, *Changing renewal settings for a certificate*.

13.2 Revoking, suspending, and unsuspending certificates

You can revoke or suspend certificates by canceling, erasing, or disabling the device on which they live; however, you may want to revoke or suspend a certificate independently of its device. The View Certificate screen allows you to do this.

If you have suspended a certificate, you can also unsuspend the certificate to make it active again.

Important: Whenever you make a change to a certificate status, the certificate is immediately placed into a pending state. Certificate changes are carried out by the MyID certificate service on the application server. You can attempt pause the processing of a certificate change to resume later; however, the MyID certificate service may already have processed the certificate change. See section *13.3*, *Pausing and resuming certificate processing*.

Note: You cannot change revoke, suspend, or unsuspend certificates from the Unmanaged CA; these certificates have not been issued from a CA using MyID.

13.2.1 Revoking or suspending a certificate

You use the same process to revoke or suspend a certificate. The effect on the certificate (revocation or suspension) depends on the reason you choose.

To revoke or suspend a certificate:

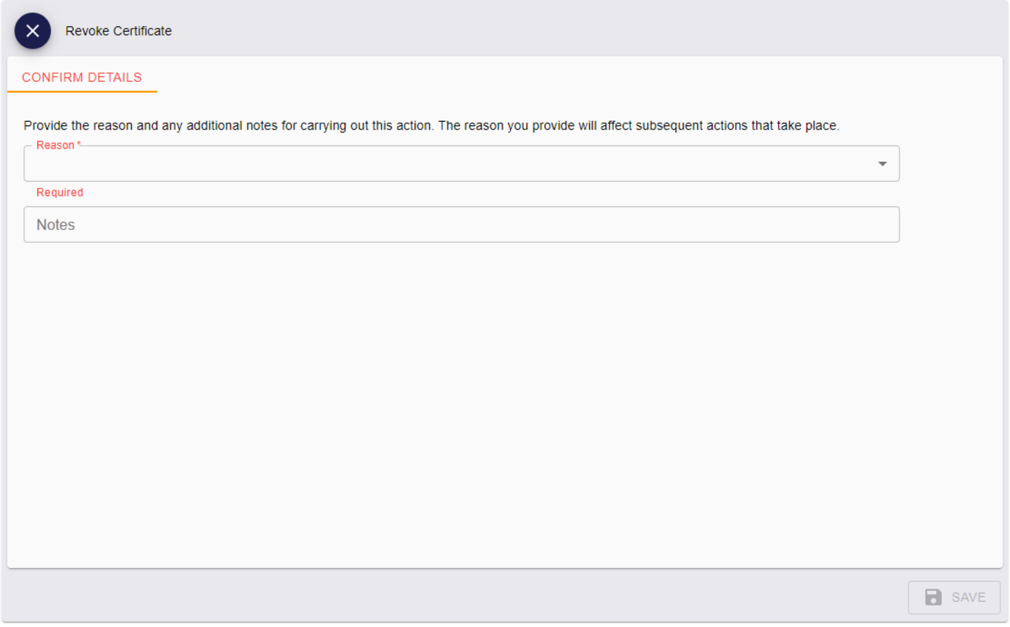
1. Search for a certificate, and view its details.

   See section *13.1*, *Viewing a certificate*.

2. On the View Certificate screen, click **Revoke**.

   If the **Revoke** option is not available, you may not have permissions to revoke certificates, or the certificate may not be in the correct state; a certificate must be in the Issued state if you want to revoke or suspend it.

   The Revoke Certificate screen appears.



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

3. Select the **Reason** for the revocation or suspension from the drop-down list.

   This reason affects how MyID treats the certificate.

   See the *Certificate reasons* section in the ***Operator's Guide*** for details of how each reason affects the certificate.

   Note: You can suspend an archived certificate by selecting the **Suspension (other)** or **Pending Investigation** reason on the Revoke Certificate screen in the MyID Operator Client, or through the MyID Core API using the reason status mapping ID `92` – for **Suspension(other)** – or ID `93` – for **Pending Investigation**. You cannot suspend an archived certificate using any other method; for example, by canceling a device, or by suspending an individual certificate in MyID Desktop.

4. Type any **Notes** on the revocation or suspension.

   You can provide further information on your reasons for revoking or suspending the certificate. This information is stored in the audit record.

5. Click **Save**.

13.2.2 Revoking or suspending multiple certificates

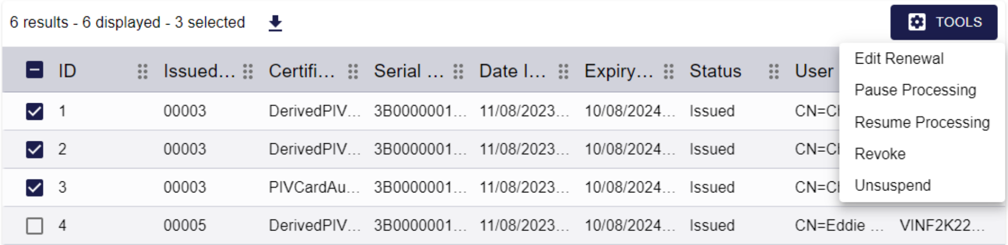
If you want to revoke or suspend multiple certificates, you can process them in a batch instead of selecting them one by one.

Note: You can access the **Tools** menu only if you have a role with the **Tools Menu** option from the **Configuration** section of the **Edit Roles** workflow.

To revoke or suspend multiple certificates:

1. Click the **Certificates** category.
2. Enter some or all of the search criteria for the certificate.

   See section *13.1.1*, *Searching for a certificate*.
3. Click **Search**.
4. On the search results page, use the checkboxes to the left of the records to select one or more certificates.
5. From the **Tools** menu, select **Revoke**.

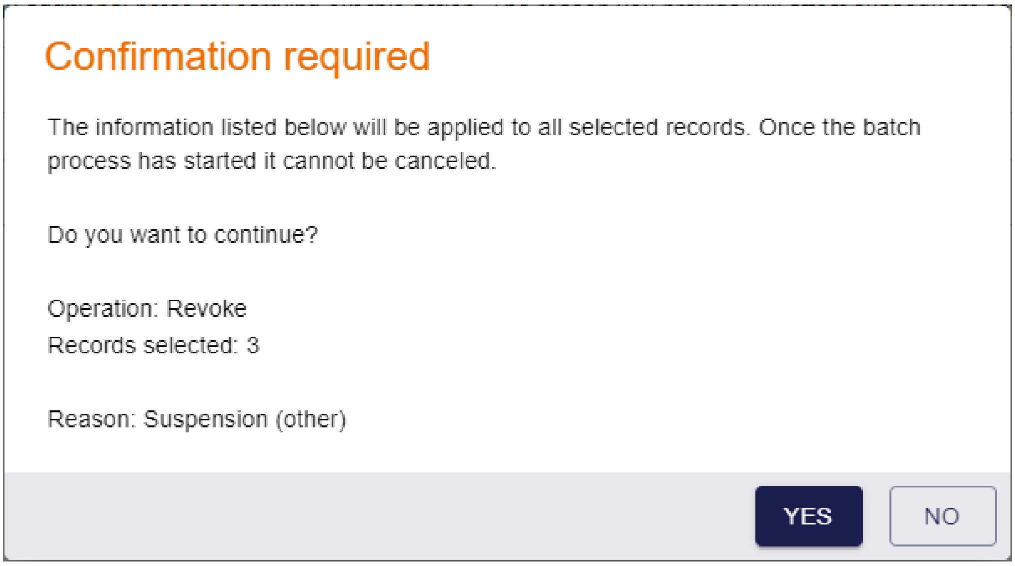
   6 results - 6 displayed - 3 selected

⊟	ID	Issued...	Certifi...	Serial ...	Date I...	Expiry...	Status	User	
☑	1	00003	DerivedPIV...	3B0000001...	11/08/2023...	10/08/2024...	Issued	CN=Cl	
☑	2	00003	DerivedPIV...	3B0000001...	11/08/2023...	10/08/2024...	Issued	CN=Cl	
☑	3	00003	PIVCardAu...	3B0000001...	11/08/2023...	10/08/2024...	Issued	CN=Cl	
☐	4	00005	DerivedPIV...	3B0000001...	11/08/2023...	10/08/2024...	Issued	CN=Eddie ...	VINF2K22...

   The Revoke Certificate screen appears.

   Complete the details as for revoking or suspending a single device; see section *13.2.1*, *Revoking or suspending a certificate*.
6. Click **Save**.

   The confirmation screen appears.

   Confirmation required

   The information listed below will be applied to all selected records. Once the batch process has started it cannot be canceled.

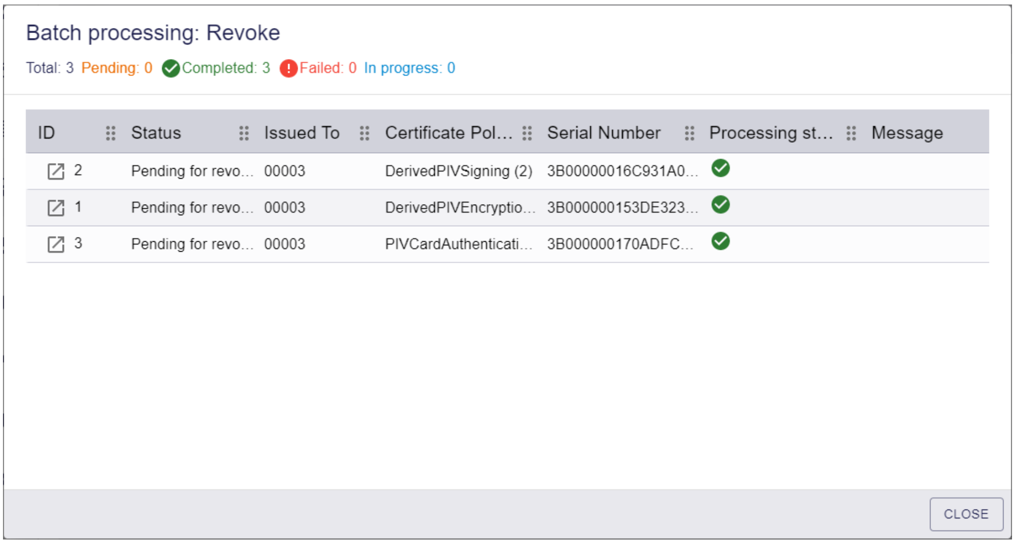
   Do you want to continue?

   Operation: Revoke
   Records selected: 3

   Reason: Suspension (other)

7. Click **Yes** to proceed with the revocation, or **No** to go back to the list of certificates.

   When you click **Yes**, the Batch Processing screen appears.



Batch processing: Revoke

Total: 3 Pending: 0 ✓Completed: 3 !Failed: 0 In progress: 0

ID	Status	Issued To	Certificate Pol…	Serial Number	Processing st…	Message
2	Pending for revo…	00003	DerivedPIVSigning (2)	3B00000016C931A0…	✓	
1	Pending for revo…	00003	DerivedPIVEncryptio…	3B000000153DE323…	✓	
3	Pending for revo…	00003	PIVCardAuthenticati…	3B000000170ADFC…	✓	

8. The revocations or suspensions are processed. The table shows the status of each certificate change:

✓	The revocation or suspension succeeded.
!	The revocation or suspension failed. The Message column displays the reason for the failure; for example, the certificate may be in the wrong status for the action; you can revoke or suspend a certificate only if it is in the Issued state.

9. Click **Close**.

13.2.3 Unsuspending a certificate

If you have temporarily suspended a certificate, you can unsuspend it to make it active again.

To unsuspend a certificate:

1. Search for certificates.

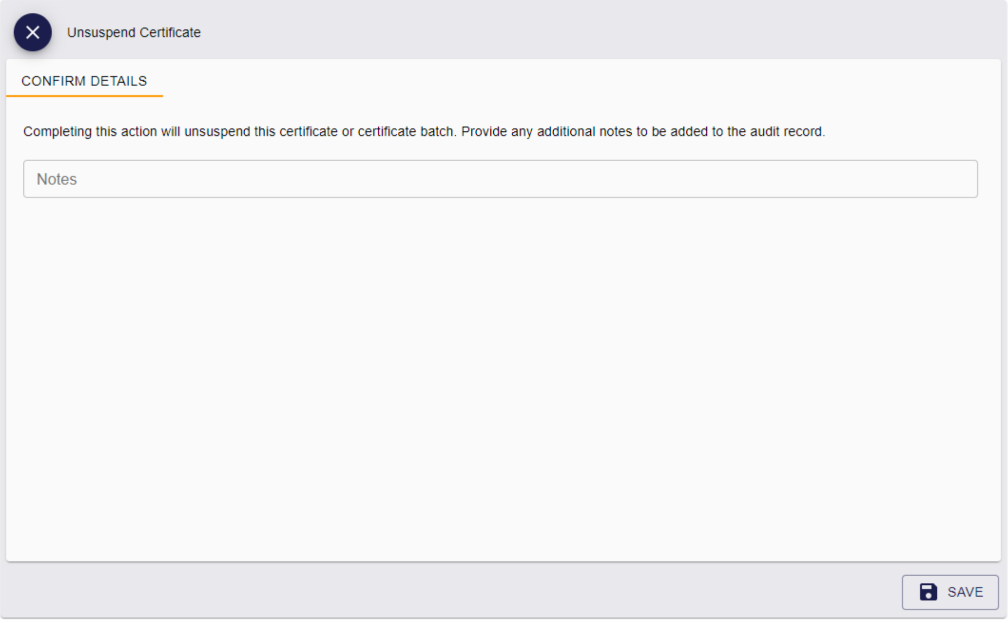
   See section *13.1*, *Viewing a certificate*.

   You can select **Suspended** from the **Certificate Status** drop-down list to return a list of all suspended certificates.

2. On the View Certificate screen, click **Unsuspend**.

   If the **Unsuspend** option is not available, you may not have permissions to unsuspend certificates, or the certificate may not be in the correct state; a certificate must be in the Suspended state if you want to unsuspend it.

   The Unsuspend Certificate screen appears.



Completing this action will unsuspend this certificate or certificate batch. Provide any additional notes to be added to the audit record.

3. Type any **Notes** on the unsuspension.

   You can provide further information on your reasons for unsuspending the certificate. This information is stored in the audit record.

4. Click **Save**.

13.2.4 Unsuspending multiple certificates

If you want to unsuspend multiple certificates, you can process them in a batch instead of selecting them one by one.

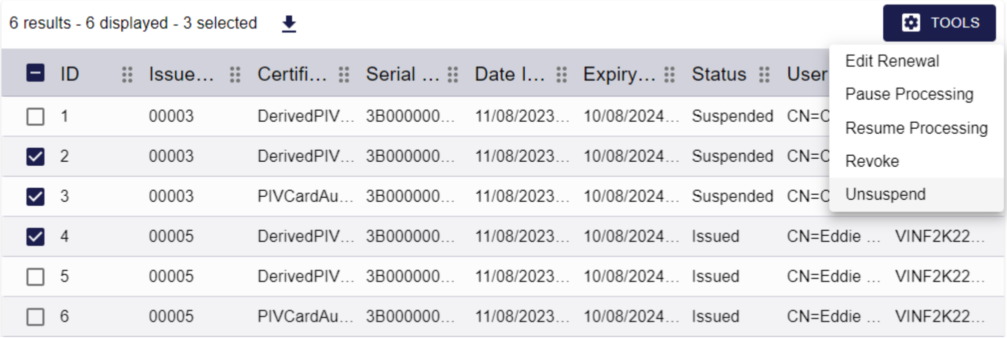
Note: You can access the **Tools** menu only if you have a role with the **Tools Menu** option from the **Configuration** section of the **Edit Roles** workflow.

To unsuspend multiple certificates:

1. Click the **Certificates** category.
2. Enter some or all of the search criteria for the certificate.

   You can select **Suspended** from the **Certificate Status** drop-down list to return a list of all suspended certificates.

   See section *13.1.1*, *Searching for a certificate*.
3. Click **Search**.
4. On the search results page, use the checkboxes to the left of the records to select one or more certificates.
5. From the **Tools** menu, select **Unsuspend**.



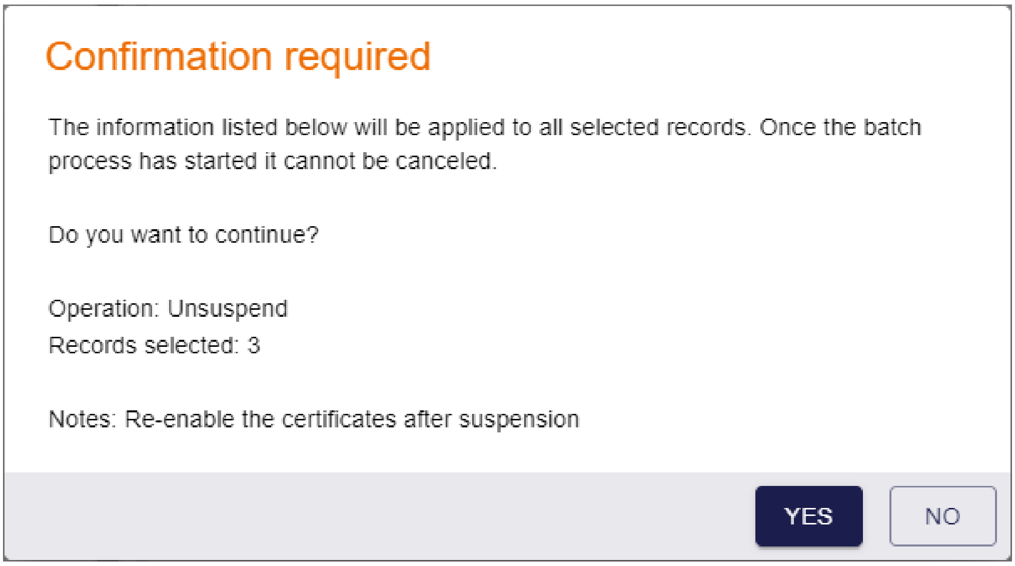
6 results - 6 displayed - 3 selected

▣	ID	Issue…	Certifi…	Serial …	Date I…	Expiry…	Status	User	
☐	1	00003	DerivedPIV…	3B000000…	11/08/2023…	10/08/2024…	Suspended	CN=C	
☑	2	00003	DerivedPIV…	3B000000…	11/08/2023…	10/08/2024…	Suspended	CN=C	
☑	3	00003	PIVCardAu…	3B000000…	11/08/2023…	10/08/2024…	Suspended	CN=C	
☑	4	00005	DerivedPIV…	3B000000…	11/08/2023…	10/08/2024…	Issued	CN=Eddie …	VINF2K22…
☐	5	00005	DerivedPIV…	3B000000…	11/08/2023…	10/08/2024…	Issued	CN=Eddie …	VINF2K22…
☐	6	00005	PIVCardAu…	3B000000…	11/08/2023…	10/08/2024…	Issued	CN=Eddie …	VINF2K22…

   The Unsuspend Certificate screen appears.

   Complete the details as for unsuspending a single device; see section *13.2.3*, *Unsuspending a certificate*.
6. Click **Save**.

The confirmation screen appears.



Confirmation required

The information listed below will be applied to all selected records. Once the batch process has started it cannot be canceled.

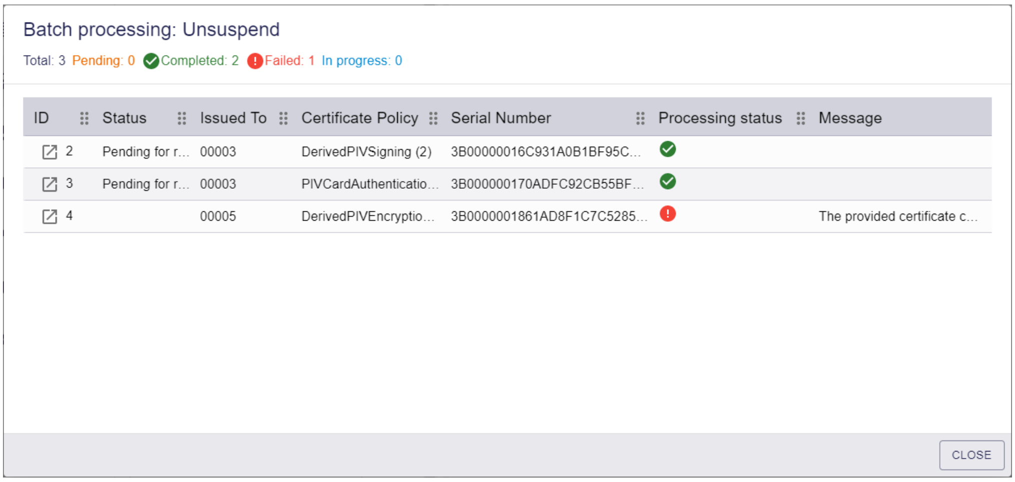
Do you want to continue?

Operation: Unsuspend
Records selected: 3

Notes: Re-enable the certificates after suspension

7. Click **Yes** to proceed with the unsuspension, or **No** to go back to the list of certificates.

   When you click **Yes**, the Batch Processing screen appears.



Batch processing: Unsuspend

Total: 3 Pending: 0 ✓Completed: 2 !Failed: 1 In progress: 0

ID	Status	Issued To	Certificate Policy	Serial Number	Processing status	Message
2	Pending for r…	00003	DerivedPIVSigning (2)	3B00000016C931A0B1BF95C…	✓	
3	Pending for r…	00003	PIVCardAuthenticatio…	3B000000170ADFC92CB55BF…	✓	
4		00005	DerivedPIVEncryptio…	3B0000001861AD8F1C7C5285…	!	The provided certificate c…

8. The unsuspension changes are processed. The table shows the status of each certificate change:

✓	The unsuspension succeeded.
!	The unsuspension failed. The Message column displays the reason for the failure; for example, the certificate may be in the wrong status for the action; you can unsuspend a certificate only if it is in the Suspended state.

9. Click **Close**.

13.3 Pausing and resuming certificate processing

Whenever you make a change to a certificate status (for example, revoking or unsuspending a certificate), the certificate is immediately placed into a pending state. Certificate changes are carried out by the MyID certificate service on the application server (eCertificate Services Server), and the time it takes to make the changes depends on a variety of factors, including the number of certificate status changes requested and the load on the server. You can attempt to pause the processing of a certificate change to resume later; however, the MyID certificate service may already have processed the certificate change. See section *13.3*, *Pausing and resuming certificate processing*.

13.3.1 Pausing certificate processing

To pause the processing of a certificate:

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

   See section *13.1*, *Viewing a certificate*.

   You can select one of the following options from the **Certificate Status** drop-down list:

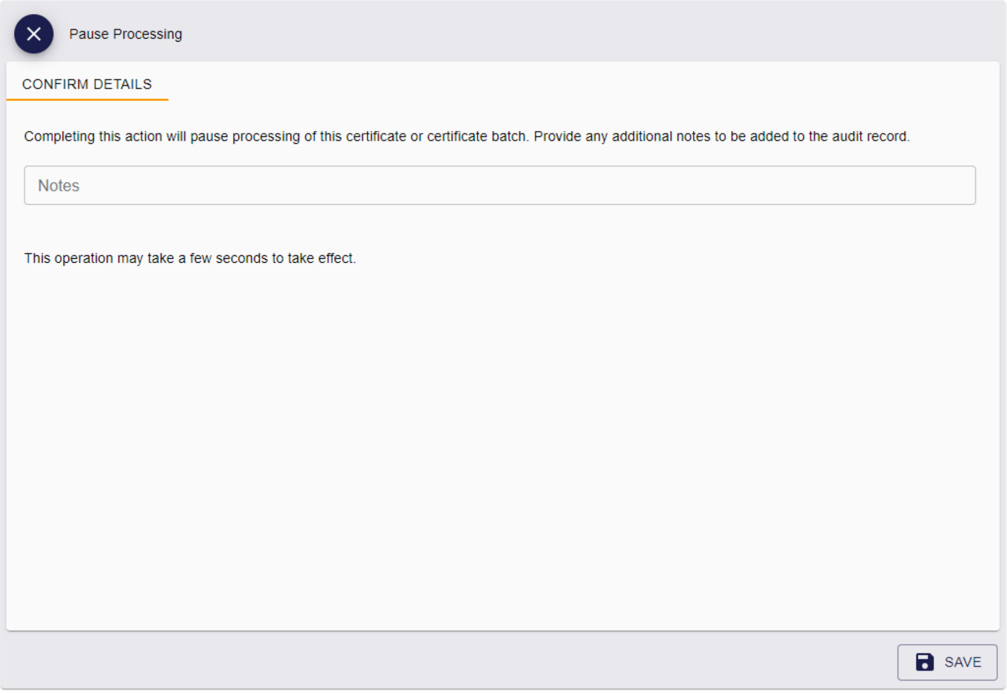
   - **Pending for issue**
   - **Pending for revoke**
   - **Submitted for issue**
   - **Submitted for revoke**

   You cannot pause the processing of a certificate if it has any other status.
2. Click **Pause Processing**.

   If the **Pause Processing** option is not available, you may not have permissions to pause the processing of certificates, or the certificate may not be in the correct state.

   Note: The options displayed were correct at the point the MyID Operator Client loaded the form. The MyID certificate service may process the certificate change before you click the option.

   The Pause Processing screen appears.

   Completing this action will pause processing of this certificate or certificate batch. Provide any additional notes to be added to the audit record.

   This operation may take a few seconds to take effect.
3. Type any **Notes** on the pause.

   You can provide further information on your reasons for pausing processing of the certificate. This information is stored in the audit record.
4. Click **Save**.

If the pause succeeds, the certificate will not change status until you resume processing.

13.3.2 Pausing processing for multiple certificates

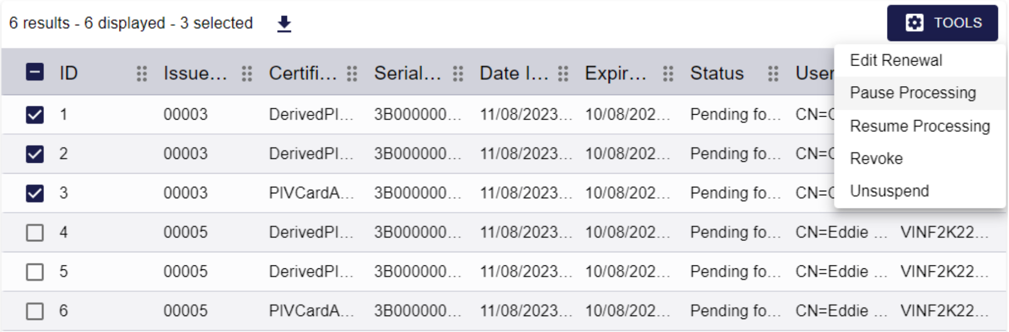
If you want to pause processing for multiple certificates, you can process them in a batch instead of selecting them one by one.

Note: You can access the **Tools** menu only if you have a role with the **Tools Menu** option from the **Configuration** section of the **Edit Roles** workflow.

To pause processing for multiple certificates:

1. Click the **Certificates** category.
2. Enter some or all of the search criteria for the certificate.

   See section *13.1.1*, *Searching for a certificate*.
3. Click **Search**.
4. On the search results page, use the checkboxes to the left of the records to select one or more certificates.
5. From the **Tools** menu, select **Pause Processing**.

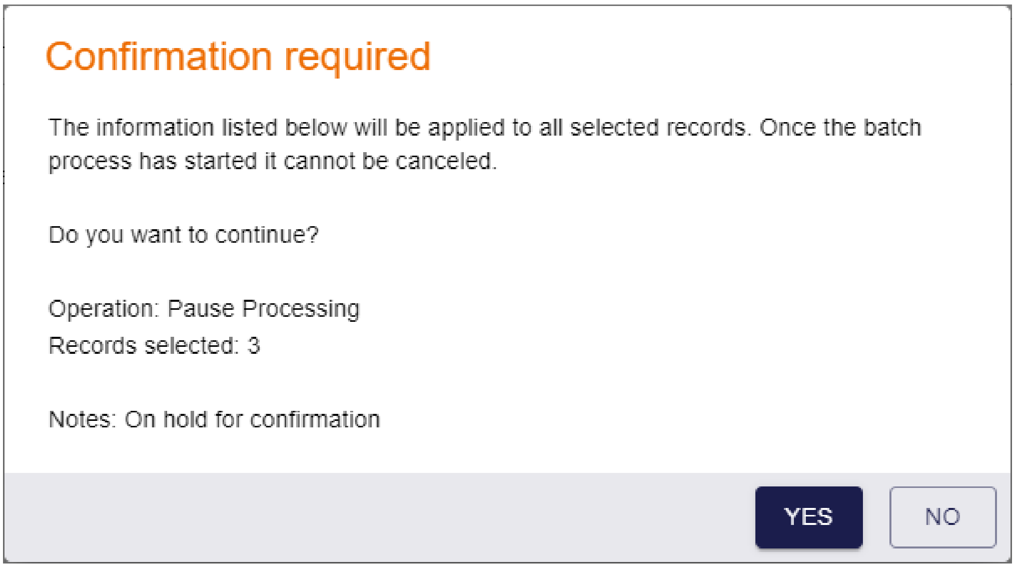
   6 results - 6 displayed - 3 selected

▬	ID	Issue...	Certifi...	Serial...	Date I...	Expir...	Status	User	
☑	1	00003	DerivedPI...	3B000000...	11/08/2023...	10/08/202...	Pending fo...	CN=(	
☑	2	00003	DerivedPI...	3B000000...	11/08/2023...	10/08/202...	Pending fo...	CN=(	
☑	3	00003	PIVCardA...	3B000000...	11/08/2023...	10/08/202...	Pending fo...	CN=(	
☐	4	00005	DerivedPI...	3B000000...	11/08/2023...	10/08/202...	Pending fo...	CN=Eddie ...	VINF2K22...
☐	5	00005	DerivedPI...	3B000000...	11/08/2023...	10/08/202...	Pending fo...	CN=Eddie ...	VINF2K22...
☐	6	00005	PIVCardA...	3B000000...	11/08/2023...	10/08/202...	Pending fo...	CN=Eddie ...	VINF2K22...

   The Pause Processing screen appears.

   Complete the details as for pausing a single certificate; see section *13.3.1*, *Pausing certificate processing*.
6. Click **Save**.

   The confirmation screen appears.



Confirmation required

The information listed below will be applied to all selected records. Once the batch process has started it cannot be canceled.

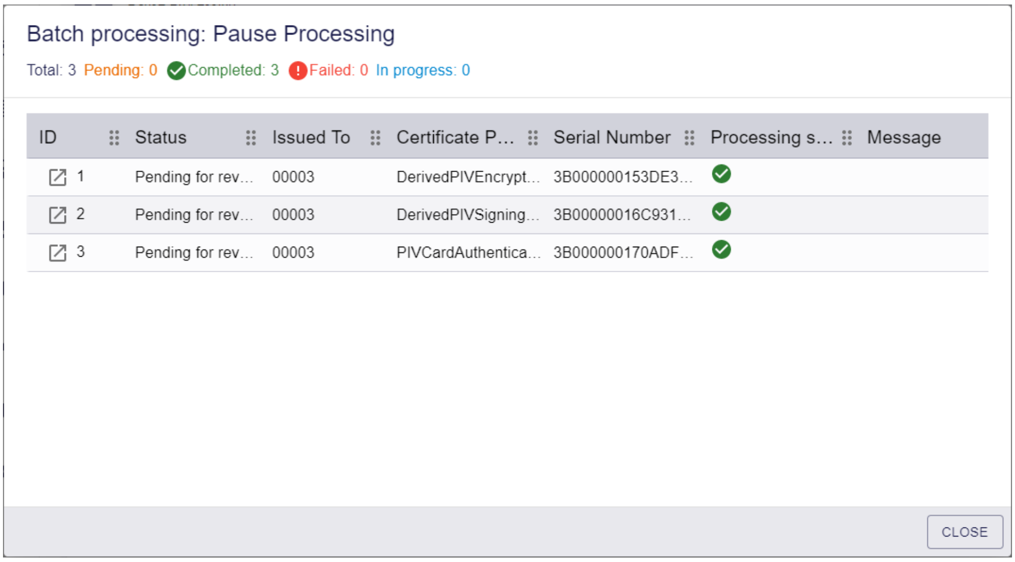
Do you want to continue?

Operation: Pause Processing
Records selected: 3

Notes: On hold for confirmation

7. Click **Yes** to proceed with the action, or **No** to go back to the list of certificates.

   When you click **Yes**, the Batch Processing screen appears.



Batch processing: Pause Processing

Total: 3 Pending: 0 ✓Completed: 3 !Failed: 0 In progress: 0

ID	Status	Issued To	Certificate P…	Serial Number	Processing s…	Message
1	Pending for rev…	00003	DerivedPIVEncrypt…	3B000000153DE3…	✓	
2	Pending for rev…	00003	DerivedPIVSigning…	3B00000016C931…	✓	
3	Pending for rev…	00003	PIVCardAuthentica…	3B000000170ADF…	✓	

8. The actions are processed. The table shows the status of each certificate change:

✓	The change succeeded.
!	The change failed. The Message column displays the reason for the failure; for example, the certificate may be in the wrong status for the action; the MyID certificate server may have processed the certificate change already, or the certificate may already be paused.

9. Click **Close**.

13.3.3 Resuming processing

If you have paused processing of a certificate, you can resume processing to allow the MyID certificate service to process the changes to the certificate status.

To resume processing for a certificate:

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

   See section *13.1*, *Viewing a certificate*.

   You can select one of the following options from the **Certificate Status** drop-down list:

   - **Pending for issue**
   - **Pending for revoke**
   - **Submitted for issue**
   - **Submitted for revoke**

   You cannot resume the processing of a certificate if it has any other status.

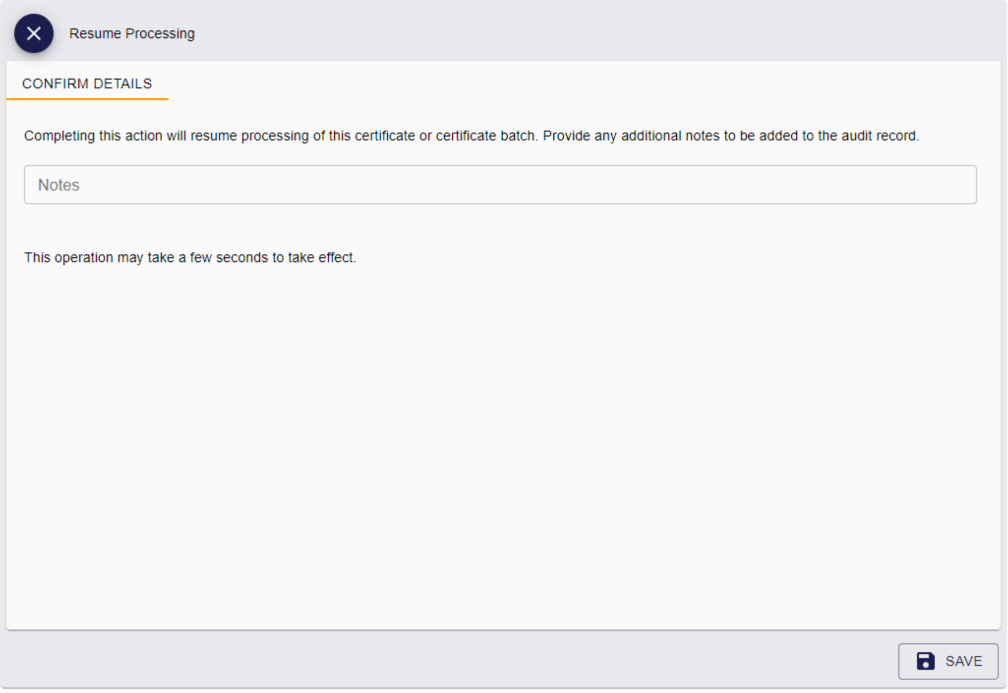
   Note: If you attempt to resume the processing of a certificate that has not been paused, the MyID Operator Client does not display an error or warning, and allows you to proceed.

2. Click **Resume Processing**.

   If the **Resume Processing** option is not available, you may not have permissions to resume the processing of certificates, or the certificate may not be in the correct state.

   Note: The options displayed were correct at the point the MyID Operator Client loaded the form. The MyID certificate service may process the certificate change before you click the option.

   The Resume Processing screen appears.



Completing this action will resume processing of this certificate or certificate batch. Provide any additional notes to be added to the audit record.

This operation may take a few seconds to take effect.

3. Type any **Notes** on the resumption.

   You can provide further information on your reasons for resuming processing of the certificate. This information is stored in the audit record.

4. Click **Save**.

If the resumption succeeds, the MyID certificate service carries on processing the certificate.

13.3.4 Resuming processing for multiple certificates

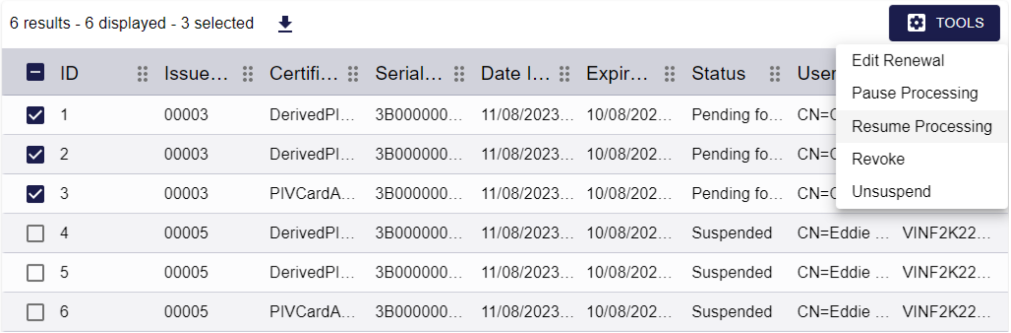
If you want to resume processing for multiple certificates, you can process them in a batch instead of selecting them one by one.

Note: You can access the **Tools** menu only if you have a role with the **Tools Menu** option from the **Configuration** section of the **Edit Roles** workflow.

To resume processing for multiple certificates:

1. Click the **Certificates** category.
2. Enter some or all of the search criteria for the certificate.

   See section *13.1.1*, *Searching for a certificate*.
3. Click **Search**.
4. On the search results page, use the checkboxes to the left of the records to select one or more certificates.
5. From the **Tools** menu, select **Resume Processing**.



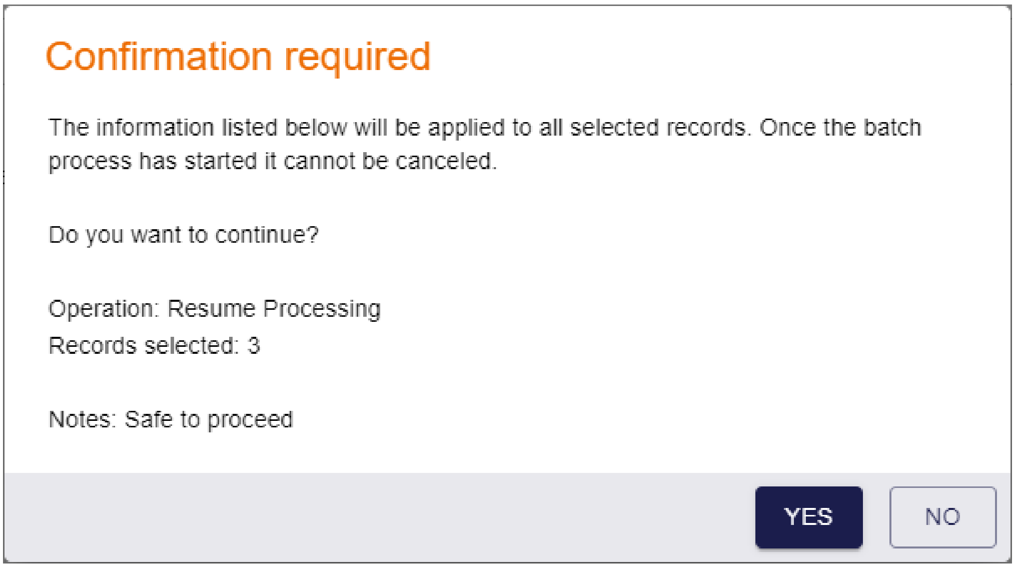
6 results - 6 displayed - 3 selected

⊟	ID	Issue…	Certifi…	Serial…	Date I…	Expir…	Status	User	
☑	1	00003	DerivedPI…	3B000000…	11/08/2023…	10/08/202…	Pending fo…	CN=	
☑	2	00003	DerivedPI…	3B000000…	11/08/2023…	10/08/202…	Pending fo…	CN=	
☑	3	00003	PIVCardA…	3B000000…	11/08/2023…	10/08/202…	Pending fo…	CN=	
☐	4	00005	DerivedPI…	3B000000…	11/08/2023…	10/08/202…	Suspended	CN=Eddie …	VINF2K22…
☐	5	00005	DerivedPI…	3B000000…	11/08/2023…	10/08/202…	Suspended	CN=Eddie …	VINF2K22…
☐	6	00005	PIVCardA…	3B000000…	11/08/2023…	10/08/202…	Suspended	CN=Eddie …	VINF2K22…

   The Resume Processing screen appears.

   Complete the details as for resuming a single certificate; see section *13.3.3*, *Resuming processing*.
6. Click **Save**.

   The confirmation screen appears.



Confirmation required

The information listed below will be applied to all selected records. Once the batch process has started it cannot be canceled.

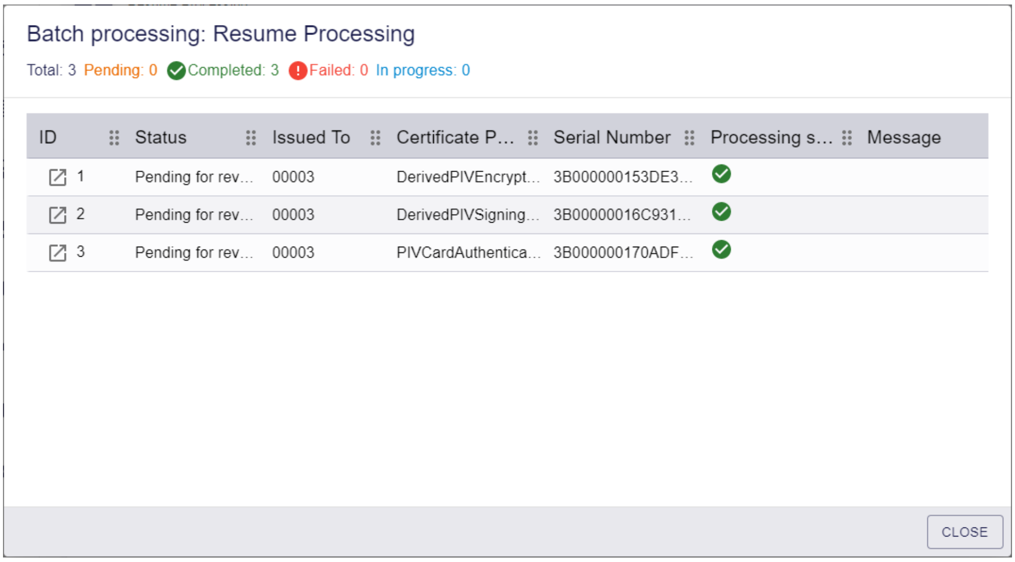
Do you want to continue?

Operation: Resume Processing
Records selected: 3

Notes: Safe to proceed

7. Click **Yes** to proceed with the action, or **No** to go back to the list of certificates.

   When you click **Yes**, the Batch Processing screen appears.



Batch processing: Resume Processing

Total: 3 Pending: 0 ✓Completed: 3 !Failed: 0 In progress: 0

ID	Status	Issued To	Certificate P…	Serial Number	Processing s…	Message
1	Pending for rev…	00003	DerivedPIVEncrypt…	3B000000153DE3…	✓	
2	Pending for rev…	00003	DerivedPIVSigning…	3B00000016C931…	✓	
3	Pending for rev…	00003	PIVCardAuthentica…	3B000000170ADF…	✓	

8. The actions are processed. The table shows the status of each certificate change:

✓	The change succeeded, and the MyID certificate service will process the certificate.
!	The change failed. The Message column displays the reason for the failure; for example, the certificate may be in the wrong status for the action; the MyID certificate server may have processed the certificate change already.

9. Click **Close**.

13.4 Changing renewal settings for a certificate

You can change the following renewal settings for a certificate:

- The renewal date.
- Whether the certificate renews automatically.

Note: You can change the renewal settings for a certificate only if it is currently issued and active. You cannot change the renewal settings for a certificate if it has been revoked or suspended, or is pending a change. You can also not change the renewal settings for certificates from the Unmanaged CA; these certificates have not been issued from a CA using MyID.

13.4.1 Changing a certificate's renewal settings

To change a certificate's renewal settings:

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

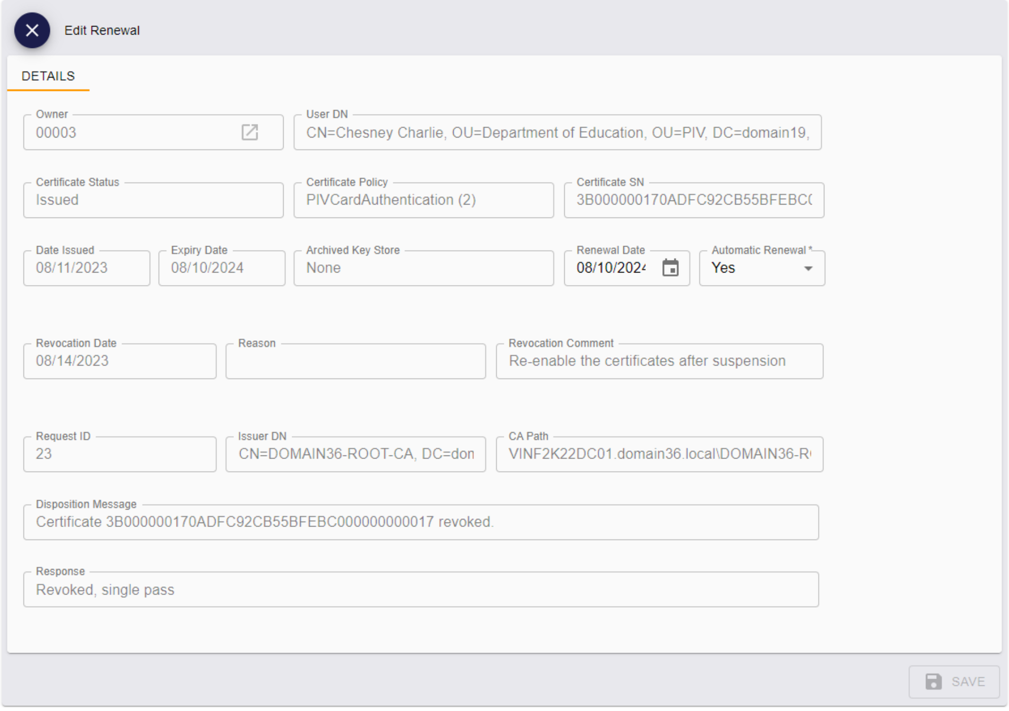
   See section *13.1*, *Viewing a certificate*.

   You can select **Issued** from the **Certificate Status** drop-down list to return all active certificates.

   You cannot change the renewal settings of a certificate if it has any other status.

2. Click **Edit Renewal**.

   The Edit Renewal screen appears.



Owner: 00003
User DN: CN=Chesney Charlie, OU=Department of Education, OU=PIV, DC=domain19,
Certificate Status: Issued
Certificate Policy: PIVCardAuthentication (2)
Certificate SN: 3B000000170ADFC92CB55BFEBC
Date Issued: 08/11/2023
Expiry Date: 08/10/2024
Archived Key Store: None
Renewal Date: 08/10/202
Automatic Renewal *: Yes
Revocation Date: 08/14/2023
Reason:
Revocation Comment: Re-enable the certificates after suspension
Request ID: 23
Issuer DN: CN=DOMAIN36-ROOT-CA, DC=don
CA Path: VINF2K22DC01.domain36.local\DOMAIN36-R
Disposition Message: Certificate 3B000000170ADFC92CB55BFEBC000000000017 revoked.
Response: Revoked, single pass

3. Edit one or both of the following fields:
   - **Renewal Date** – select or type a date for the certificate to be renewed.
   - **Automatic Renewal** – select **Yes** to renew the certificate automatically, or **No** to prevent the certificate from being renewed automatically.

4. Click **Save**.

   The certificate's renewal settings are updated. The renewal settings are updated immediately in the MyID database; you do not have to wait for the MyID certificate service to process the change, and you cannot use the **Pause Processing** option to pause the change.

13.4.2 Changing the renewal settings for multiple certificates

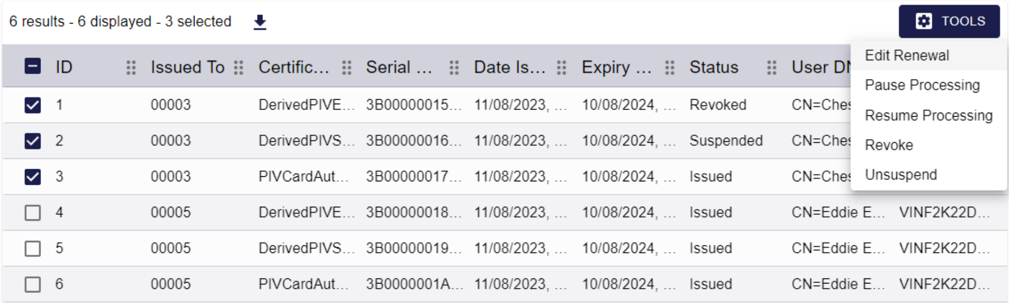
If you want to change the renewal settings for multiple certificates, you can process them in a batch instead of selecting them one by one.

Note: You can access the **Tools** menu only if you have a role with the **Tools Menu** option from the **Configuration** section of the **Edit Roles** workflow.

To change the renewal settings for multiple certificates:

1. Click the **Certificates** category.
2. Enter some or all of the search criteria for the certificate.

   See section *13.1.1*, *Searching for a certificate*.
3. Click **Search**.
4. On the search results page, use the checkboxes to the left of the records to select one or more certificates.
5. From the **Tools** menu, select **Pause Processing**.

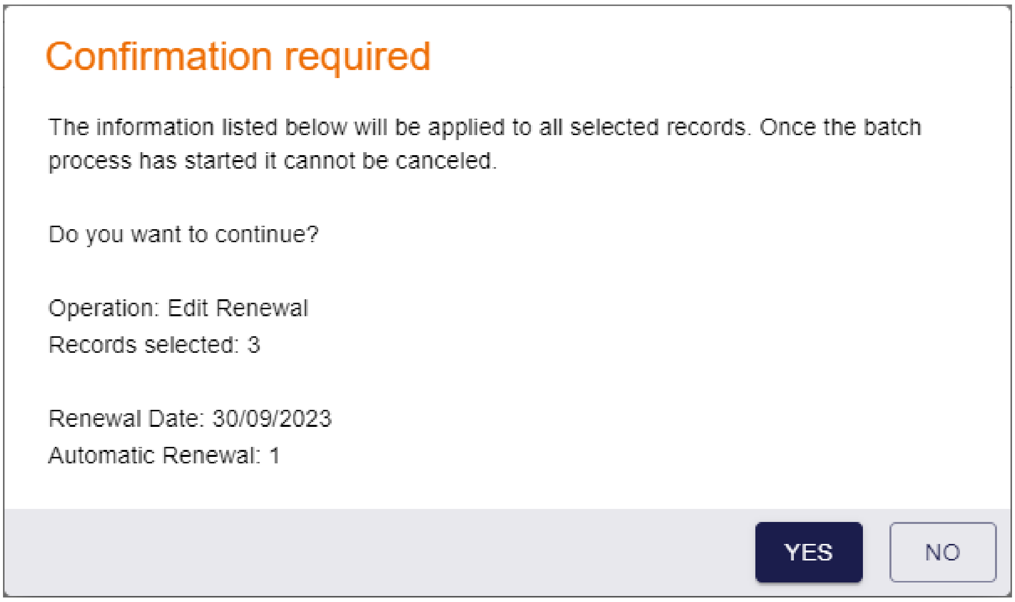
   6 results - 6 displayed - 3 selected

☐	ID	Issued To	Certific...	Serial ...	Date Is...	Expiry ...	Status	User DI	
☑	1	00003	DerivedPIVE...	3B00000015...	11/08/2023, ...	10/08/2024, ...	Revoked	CN=Ches	
☑	2	00003	DerivedPIVS...	3B00000016...	11/08/2023, ...	10/08/2024, ...	Suspended	CN=Ches	
☑	3	00003	PIVCardAut...	3B00000017...	11/08/2023, ...	10/08/2024, ...	Issued	CN=Ches	
☐	4	00005	DerivedPIVE...	3B00000018...	11/08/2023, ...	10/08/2024, ...	Issued	CN=Eddie E...	VINF2K22D...
☐	5	00005	DerivedPIVS...	3B00000019...	11/08/2023, ...	10/08/2024, ...	Issued	CN=Eddie E...	VINF2K22D...
☐	6	00005	PIVCardAut...	3B0000001A...	11/08/2023, ...	10/08/2024, ...	Issued	CN=Eddie E...	VINF2K22D...

   The Edit Renewal screen appears.

   Complete the details as for editing the renewal settings for a single certificate; see section *13.4.1*, *Changing a certificate's renewal settings*.
6. Click **Save**.

   The confirmation screen appears.



Confirmation required

The information listed below will be applied to all selected records. Once the batch process has started it cannot be canceled.

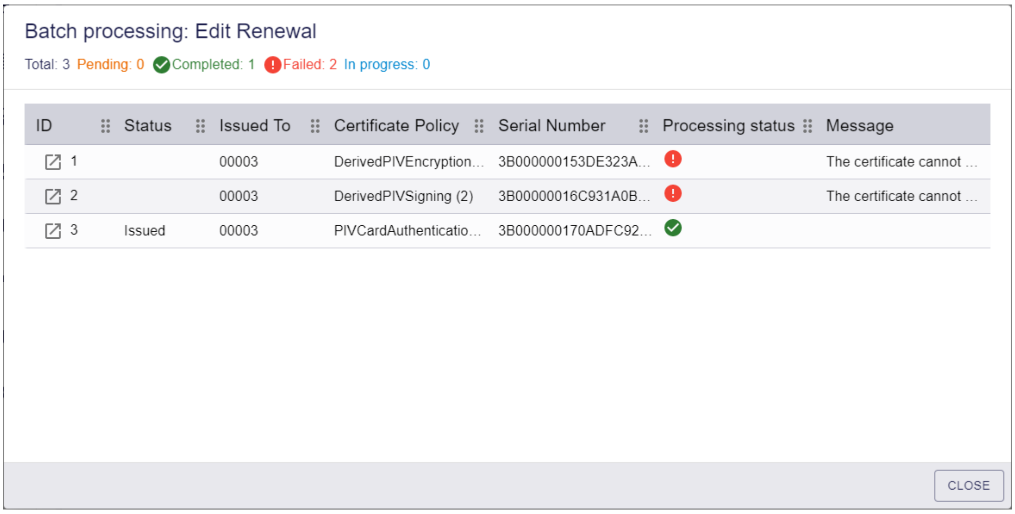
Do you want to continue?

Operation: Edit Renewal
Records selected: 3

Renewal Date: 30/09/2023
Automatic Renewal: 1

7. Click **Yes** to proceed with the action, or **No** to go back to the list of certificates.

   When you click **Yes**, the Batch Processing screen appears.



Batch processing: Edit Renewal

Total: 3 Pending: 0 ✓Completed: 1 !Failed: 2 In progress: 0

ID	Status	Issued To	Certificate Policy	Serial Number	Processing status	Message
1		00003	DerivedPIVEncryption…	3B000000153DE323A…	!	The certificate cannot …
2		00003	DerivedPIVSigning (2)	3B00000016C931A0B…	!	The certificate cannot …
3	Issued	00003	PIVCardAuthenticatio…	3B000000170ADFC92…	✓	

8. The actions are processed. The table shows the status of each certificate change:

✓	The change succeeded.
!	The change failed. The Message column displays the reason for the failure; for example, the certificate may be in the wrong status for the action; you can edit the renewal settings only for certificates that have the status **Issued**.

9. Click **Close**.

14 Working with soft certificates

Soft certificates are stored on your PC, or on removable storage such as a USB stick, rather than issued to a smart card. You can either request a certificate and allow the user to collect it to their PC's certificate store using MyID, or you can create a certificate in a password-protected file that you can send to the user. MyID allows you to print a transport document to accompany the soft certificate package, and a separate PIN mailer document that you can send under different cover to the user.

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

Important: Collecting soft certificates in the MyID Operator Client requires the MyID Client Service to be running on the client, and the rest.provision web service to be running on the web server. In addition, you must have the WebView2 component installed on the client PC to be able to print transport or mailing documents; see the *Microsoft WebView2 Runtime* section in the ***Installation and Configuration Guide***.

Note: By default, when MyID issues software certificates, it encrypts the passwords protecting the PFX files using AES256/SHA2. However, some Operating Systems do not support this modern security standard, which creates a problem when importing the certificates onto these; for example, any Apple OS (macOS or iOS), any Windows Server OS lower than Windows 2019, and any Windows client OS lower than Windows 10 build 1709. If you want to import software certificates onto an OS that does support not the encryption of PFX files using AES256/SHA2, you must set the **Use SHA1 encryption for certificates issued as PFX files** option in the **Server** tab of the **Security Settings** workflow to `Yes`.

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

MyID allows you to work with soft certificates in the following ways:

- Create a credential profile for soft certificates.

  See the *Setting up a credential profile for soft certificates* section in the ***Administration Guide*** for details of setting up a credential profile that allows you to issue software certificate packages.

- Request a soft certificate for a person.

  To request a soft certificate for a person, request a device using the soft certificate credential profile you created.

  See section *4.5*, *Requesting a device for a person*.

- Approve the request for a soft certificate

  If you set the **Validate Issuance** option on the soft certificate credential profile, an operator must approve the request before you can collect the soft certificate package.

  See section *6.2.1*, *Approving requests*.

- Collect a soft certificate.

  You can collect a soft certificate to the local PC's system certificate store, to a .pfx file located anywhere on your file system, or automatically saved to a USB device attached to your PC, depending on how the credential profile is configured.

  See section *14.1*, *Collecting a soft certificate*.
- Print transport and PIN mailer documents for a soft certificate

  See section *14.2*, *Printing mailing documents for a soft certificate package*.
- Cancel a soft certificate package, revoking its certificates.

  See section *5.7*, *Canceling a device*.
- Disable a soft certificate package, suspending its certificates.

  See section *5.22*, *Enabling and disabling devices*.
- Request a replacement for a soft certificate package.

  See section *5.4*, *Requesting a replacement device*.
- Customize the automatically-created certificate file names.

  See section *14.3*, *Customizing certificate file names*.

14.1 Collecting a soft certificate

You can collect a soft certificate request for yourself or for another person. You can save the certificates to your Personal certificate store, to a selected file location, or automatically to an attached USB device, depending on how the soft certificate credential profile is configured. The soft certificates are saved as PFX files.

Note: By default, when MyID issues software certificates, it encrypts the passwords protecting the PFX files using AES256/SHA2. However, some Operating Systems do not support this modern security standard, which creates a problem when importing the certificates onto these; for example, any Apple OS (macOS or iOS), any Windows Server OS lower than Windows 2019, and any Windows client OS lower than Windows 10 build 1709. If you want to import software certificates onto an OS that does support not the encryption of PFX files using AES256/SHA2, you must set the **Use SHA1 encryption for certificates issued as PFX files** option in the **Server** tab of the **Security Settings** workflow to `Yes`.

You can also print a transport document for the soft certificate request.

Important: Saving soft certificate packages and printing transport documents requires the MyID Client Service to be running.

To collect a soft certificate request:

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

   See section *6.1*, *Searching for a request*.

   You can display the **Type** field from the **Additional search criteria** and select the **Request a soft (browser) certificate for a user** option from the drop-down list.

   You can also view a request from any form that displays a link to the request.

   For example:

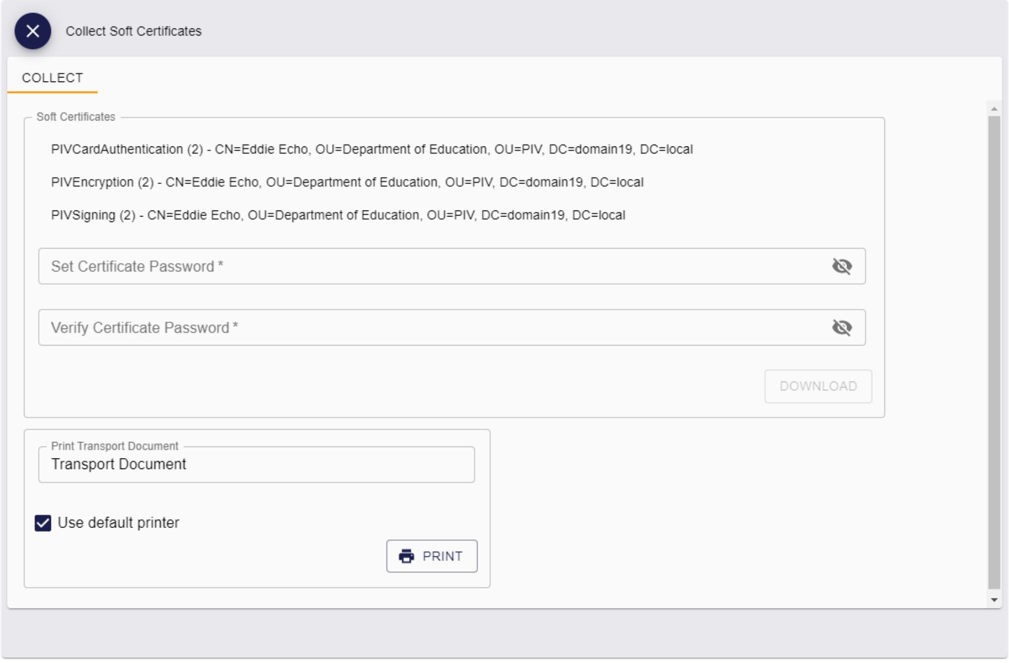
   - Click the entry in the list of requests in the **Requests** tab of the View Person form.
   - Click the entry in the list of requests in the **Device Requests** tab of the View Device form.
   - View the screen that appears automatically after you have requested a device, assuming that the request does not need to be approved by another operator first.

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

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

   If this option is not available, the request cannot be collected; for example, it may require validation.

   The Collect Soft Certificates screen appears.


Collect Soft Certificates
COLLECT
Soft Certificates
Set Certificate Password *
Verify Certificate Password *
DOWNLOAD
Print Transport Document
PRINT

PIVCardAuthentication (2) - CN=Eddie Echo, OU=Department of Education, OU=PIV, DC=domain19, DC=local

PIVEncryption (2) - CN=Eddie Echo, OU=Department of Education, OU=PIV, DC=domain19, DC=local

PIVSigning (2) - CN=Eddie Echo, OU=Department of Education, OU=PIV, DC=domain19, DC=local

Transport Document

☑ Use default printer

3. If the credential profile requires a user-specified PIN, type the password in the **Set Certificate Password** and **Verify Certificate Password** fields.

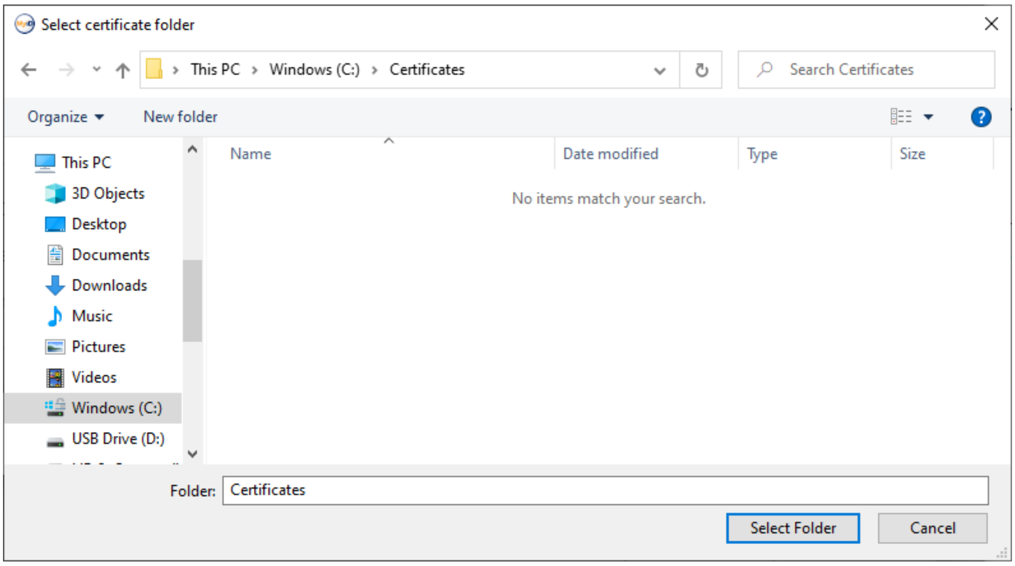
   Otherwise, MyID generates a password on the server for .pfx files. This password is not displayed on screen; you must set up a PIN mailing document to provide this password to the user.

   Note: If there are multiple certificate files in the soft certificate package, they all use the same password.

4. Click **Download**.

   The MyID Client Service must be running on your PC.

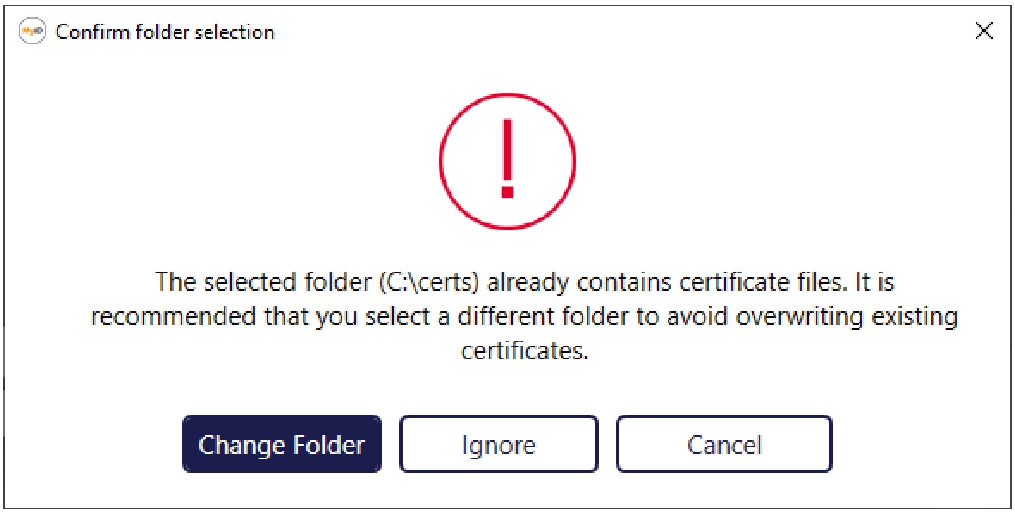
   - If a certificate policy is configured for **FileStore**, select the folder on your PC where you want to save the .pfx file.


Select certificate folder
This PC > Windows (C:) > Certificates
Search Certificates
Organize
New folder
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Windows (C:)
USB Drive (D:)
Name
Date modified
Type
Size
Select Folder
Cancel

No items match your search.

Folder: Certificates

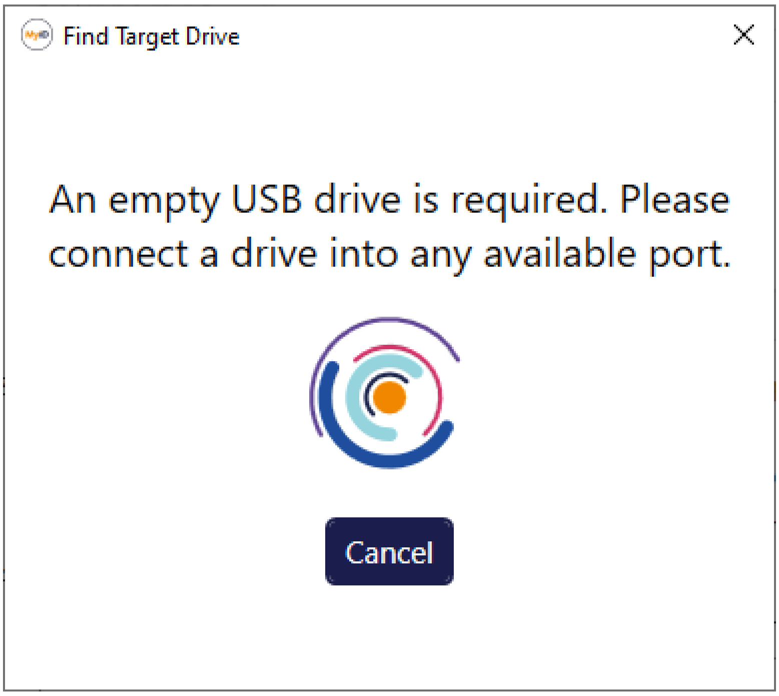
Note: If the folder already contains certificate files, a warning is displayed:


Confirm folder selection
Change Folder
Ignore
Cancel

The selected folder (C:\certs) already contains certificate files. It is recommended that you select a different folder to avoid overwriting existing certificates.

If you ignore this warning and continue, if the folder contains a .pfx file with the same automatically-generated name, MyID overwrites the older file without further warning. Alternatively, you can change the folder, or cancel the operation.

- If a certificate policy is configured for **AutoSave**, MyID scans your PC for an empty USB drive.

  Find Target Drive

  An empty USB drive is required. Please connect a drive into any available port.

  Insert an empty USB drive into your PC. As soon as MyID detects an empty USB drive, it saves the .pfx file to that drive. If you have a USB drive attached that has files on it, and delete the files, MyID detects the newly-empty drive and saves the .pfx file.

- If a certificate policy is configured for **SystemStore**, MyID saves it to the Personal store of the logged-on Windows user automatically.

Note: If you cancel the folder selection or the USB find dialog, MyID deletes any .pfx files it has already created, but any certificates written to the Personal certificate store are not removed. You can attempt to download the certificates again; MyID obtains new certificates. Any certificates that were not fully collected are revoked automatically a short time later.

The file names used for the certificate .pfx files are generated automatically. You can customize the format; see section *14.3*, *Customizing certificate file names*.

5. If you have a transport document configured for the soft certificate package, click **Print**.

   You can use transport documents to provide covering letters for the certificate package; for example, if you are distributing the certificate package on USB drives. Do not include the password in the transport document; you are recommended to provide the password in a PIN mailing document sent separately for security reasons.

   Note: You cannot print a transport document until you have successfully downloaded the certificates.

   For more information on transport documents and PIN mailing documents, see section *14.2*, *Printing mailing documents for a soft certificate package*.

6. Once you have downloaded the certificates, and printed the transport document if required, click **Close**.

   ✕

14.2 Printing mailing documents for a soft certificate package

When working with soft certificates, MyID allows you to print the following types of document:

- Transport Document

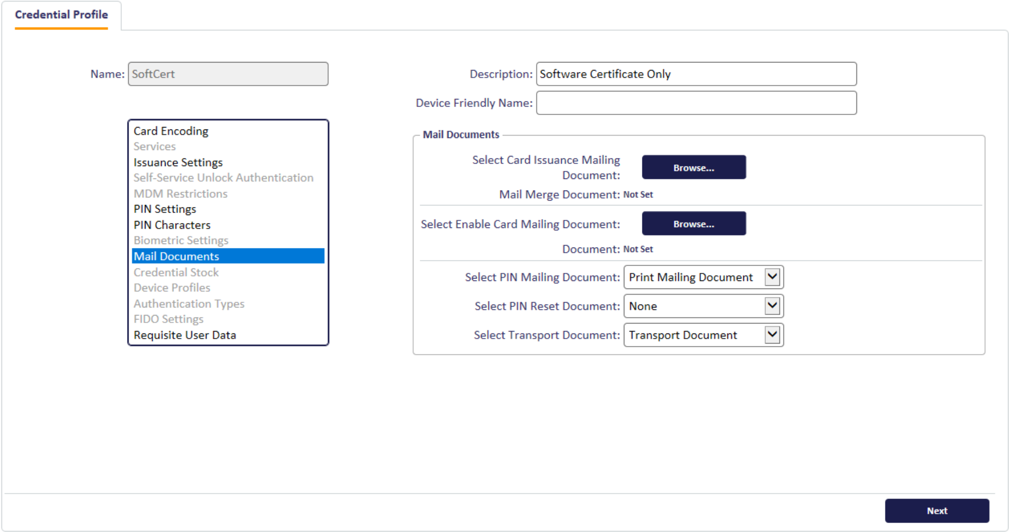
  You can print this document when collecting a soft certificate package. This document can contain a cover letter that you can send with the soft certificate package (for example, if you are distributing the soft certificate packages on USB drives). You must not include a PIN in this document, for reasons of security. You can print this document when collecting a soft certificate package, or at a later date once the soft certificate package has been collected.
- PIN Mailing Document

  You can print this document after you have collected a soft certificate package. This document can contain a PIN (assuming you have configured the credential profile to use a suitable server generated PIN) that you can provide to the user under separate cover, for reasons of security.

  You can print a mailing document only once, unless you have the elevated privilege of being able to reprint mailing documents; this is treated as a separate operation that you can control using the **Edit Roles** workflow.

You must have the WebView2 component installed to be able to print transport or mailing documents. See the *Microsoft WebView2 Runtime* section in the ***Installation and Configuration Guide***.

You can specify which templates are used in the **Mail Documents** section of the credential profile.



Credential Profile
Card Encoding
Services
Issuance Settings
Self-Service Unlock Authentication
MDM Restrictions
PIN Settings
PIN Characters
Biometric Settings
Mail Documents
Credential Stock
Device Profiles
Authentication Types
FIDO Settings
Requisite User Data
Browse...
Browse...
Next

Name: SoftCert

Description: Software Certificate Only

Device Friendly Name:

Mail Documents

Select Card Issuance Mailing Document:

Mail Merge Document: Not Set

Select Enable Card Mailing Document:

Document: Not Set

Select PIN Mailing Document: Print Mailing Document

Select PIN Reset Document: None

Select Transport Document: Transport Document

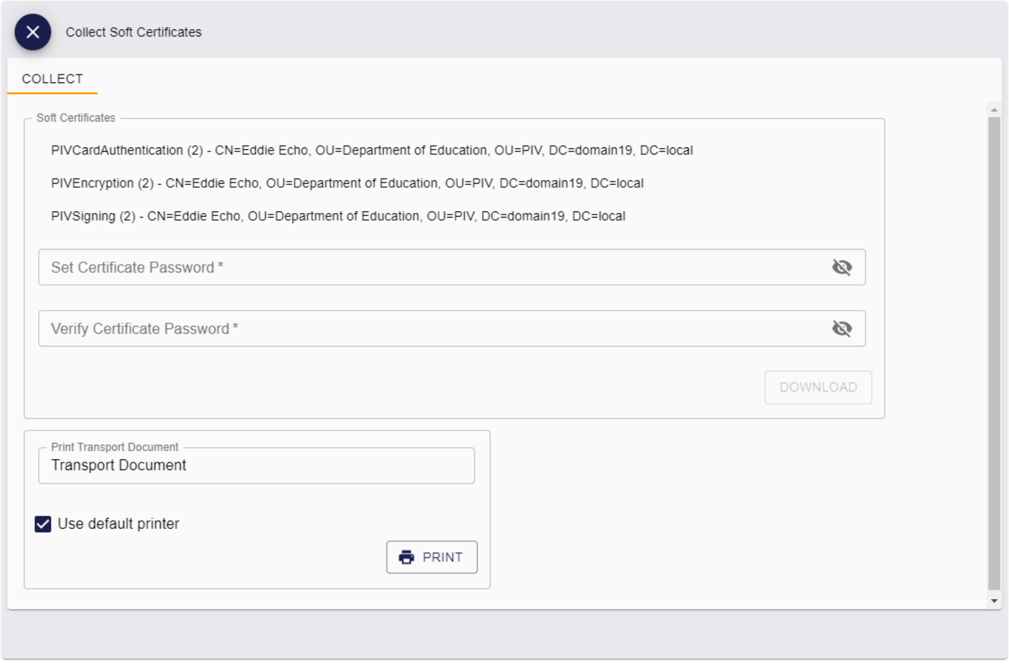
See the *Setting up a credential profile for soft certificates* section in the ***Administration Guide*** for details.

The HTML templates are stored in the database. There is currently no user interface that allows you to upload new mailing document templates to the database; for information on creating templates, contact customer support to obtain the *Mailing Documents* guide, quoting reference SUP-255.

Note: MyID uses the MyID Client Service to print mailing documents. If the MyID Client Service is not running, MyID attempts to print the document using your browser's built-in printing facility instead. Note that you cannot automatically select the default printer and print seamlessly without further interaction if you are using the browser's printing facility.

14.2.1 Printing a transport document

On the Collect Soft Certificates screen, once you have downloaded the soft certificate package, you can print the transport document.


Collect Soft Certificates
COLLECT
Soft Certificates
Set Certificate Password *
Verify Certificate Password *
DOWNLOAD
Print Transport Document
PRINT

PIVCardAuthentication (2) - CN=Eddie Echo, OU=Department of Education, OU=PIV, DC=domain19, DC=local

PIVEncryption (2) - CN=Eddie Echo, OU=Department of Education, OU=PIV, DC=domain19, DC=local

PIVSigning (2) - CN=Eddie Echo, OU=Department of Education, OU=PIV, DC=domain19, DC=local

Print Transport Document: Transport Document

☑ Use default printer

See section *14.1*, *Collecting a soft certificate* for details.

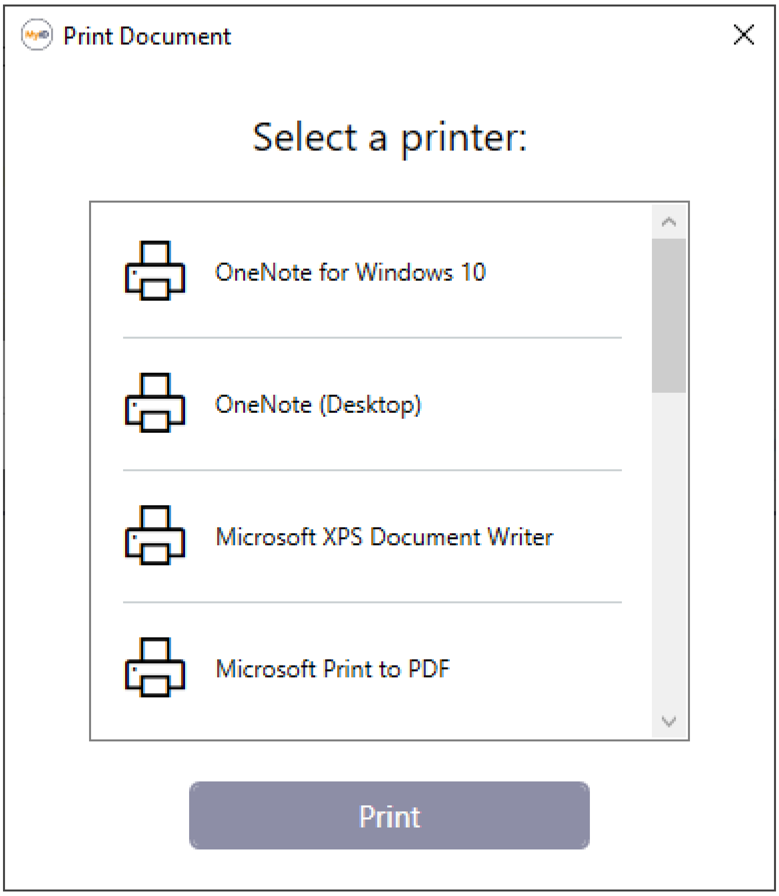
Note: If you attempt to print the transport document before successfully downloading the soft certificate package, an error similar to the following appears:

- WS40058 – Unable to generate a server document, the status of the request is invalid.

Make sure you have downloaded the certificate package before you click **Print**.

To print the transport document:

1. If you want to use the Windows default printer, make sure **Use default printer** is selected.
2. Click **Print**.
3. If you are selecting the printer manually, choose the printer from the list and click **Print**.


Print Document
Select a printer:
OneNote for Windows 10
OneNote (Desktop)
Microsoft XPS Document Writer
Microsoft Print to PDF
Print

14.2.2 Reprinting a transport document

If you need to reprint a transport document for a soft certificate request, you can do so from the View Request screen for the soft certificate, as long as the request is at status "Completed".

14.2.3 Printing a mailing document

When you collect a soft certificate package, a new request is created in MyID of type "Print PIN Mailer Document". These requests do not appear in the standard Requests report, but appear in the Print PIN Mailer report instead.

To print a mailing document:

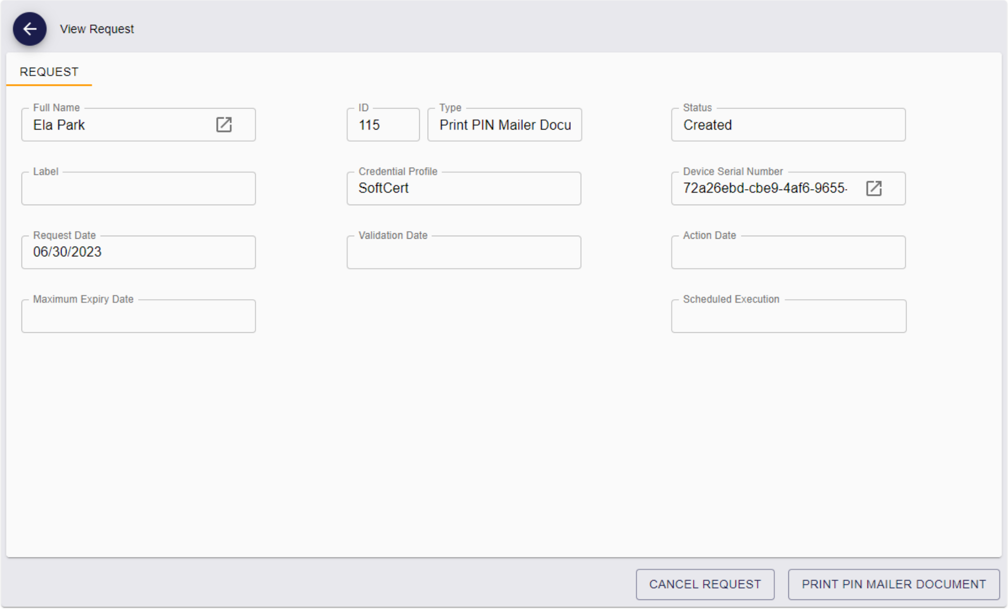
1. Click the **Requests** category.
2. From the **Reports** drop-down list, select **Print PIN Mailer**.

   See section *7.3.9*, *Print PIN Mailer report* for details of the search criteria you can use.

   Note: For convenience, you can also print a print mailer document from the View Request screen of the original soft certificate request; that is, from a request of type "Request a soft (browser) certificate for a user" at status "Completed" *if* there is an associated request of type "Print PIN Mailer Document" at status "Created".
3. Click **Search**.

   The list of matching results appears.
4. Select the request you want to print.

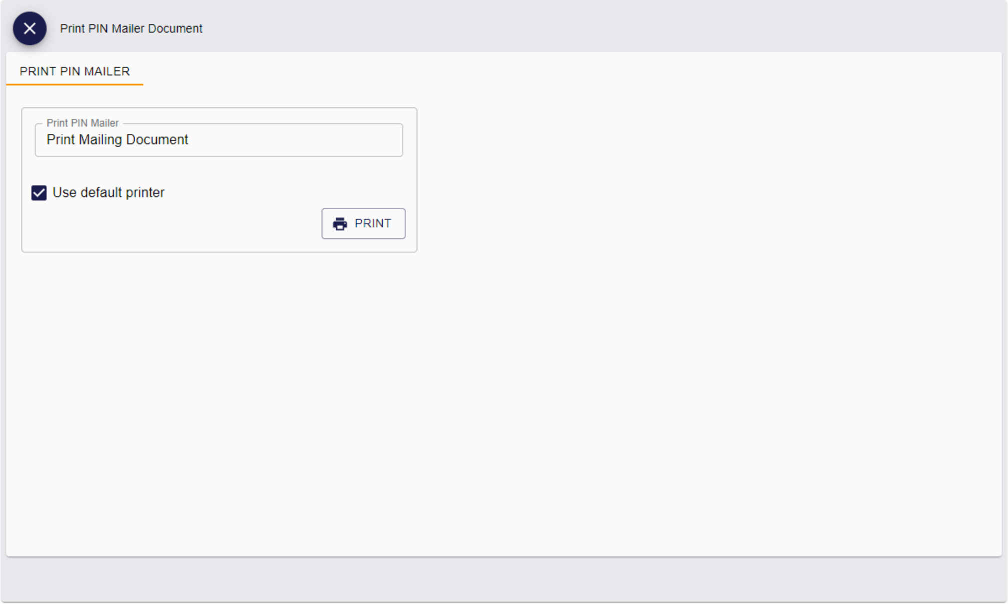
   The View Request screen appears.



Full Name Ela Park	ID 115	Type Print PIN Mailer Docu	Status Created
Label	Credential Profile SoftCert		Device Serial Number 72a26ebd-cbe9-4af6-9655-
Request Date 06/30/2023	Validation Date		Action Date
Maximum Expiry Date			Scheduled Execution

5. Click **Print PIN Mailer Document**.

The Print PIN Mailer Document screen appears.



Print PIN Mailer: Print Mailing Document

☑ Use default printer

6. If you want to use the Windows default printer, make sure **Use default printer** is selected.
7. Click **Print**.

   If you are selecting the printer manually, choose the printer from the list and click **Print**.

   MyID prints the document, and sets the "Print PIN Mailer Document" request to "Completed". You can attempt to print the document multiple times, as long as you do not close the Print PIN Mailer Document screen; once you leave this screen, you can reprint a document only if you have permissions to the **Reprint PIN Mailer Document** operation.
8. Once you have printed the document successfully, click **Close**.

   ✕

14.2.4 Reprinting a mailing document

For reasons of security, once a PIN mailing document has been printed, you cannot reprint it using the **Print PIN Mailer Document** operation. You can reprint a PIN mailer only if you have access to the **Reprint PIN Mailer Document** operation; you are recommended to make this operation available as an elevated privilege for selected operators.

To reprint a mailing document:

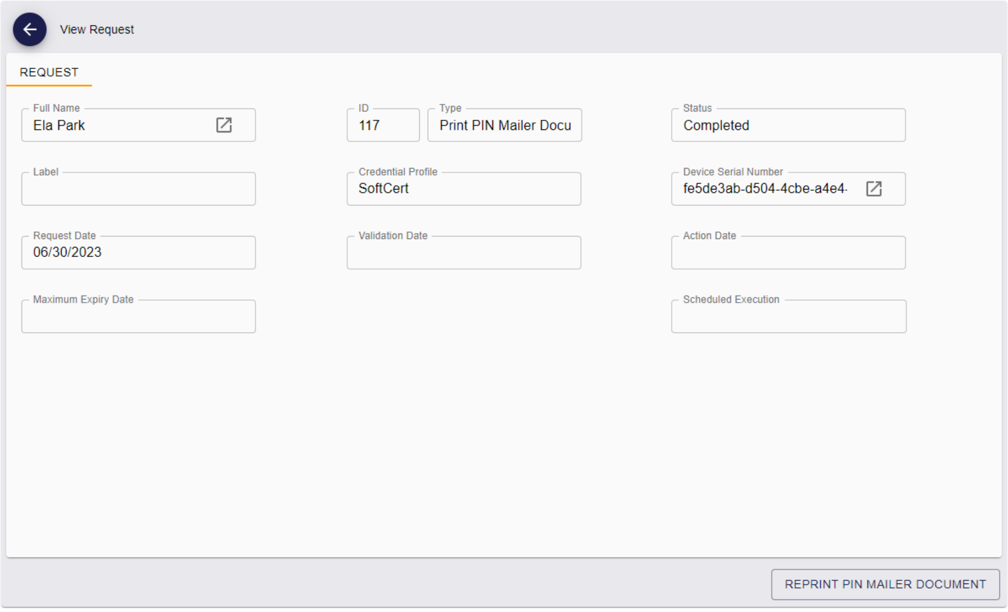
1. Click the **Requests** category.
2. From the **Reports** drop-down list, select **Reprint PIN Mailer**.

   See section *7.3.10*, *Reprint PIN Mailer report* for details of the search criteria you can use.

   Note: For convenience, you can also reprint a print mailer document from the View Request screen of the original soft certificate request; that is, from a request of type "Request a soft (browser) certificate for a user" at status "Completed" *if* there is an associated request of type "Print PIN Mailer Document" at status "Completed".
3. Click **Search**.

   The list of matching results appears.
4. Select the request you want to print.

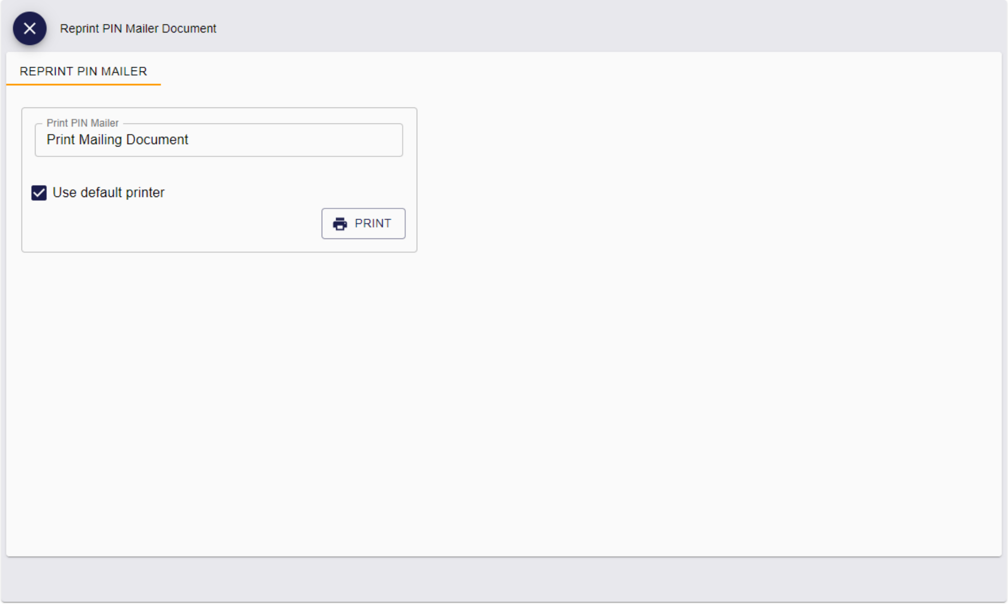
   The View Request screen appears.



Full Name: Ela Park
ID: 117
Type: Print PIN Mailer Docu
Status: Completed
Label:
Credential Profile: SoftCert
Device Serial Number: fe5de3ab-d504-4cbe-a4e4-
Request Date: 06/30/2023
Validation Date:
Action Date:
Maximum Expiry Date:
Scheduled Execution:

5. Click **Reprint PIN Mailer Document**.

The Reprint PIN Mailer Document screen appears.


Reprint PIN Mailer Document
REPRINT PIN MAILER
PRINT

Print PIN Mailer: Print Mailing Document

☑ Use default printer

6. If you want to use the Windows default printer, make sure **Use default printer** is selected.
7. Click **Print**.

   If you are selecting the printer manually, choose the printer from the list and click **Print**.
8. Once you have printed the document successfully, click **Close**.

14.2.5 Printing multiple mailing documents

If you need to print or reprint multiple mailing documents, you can do so as a batch operation.

Note: You can access the **Tools** menu only if you have a role with the **Tools Menu** option from the **Configuration** section of the **Edit Roles** workflow.

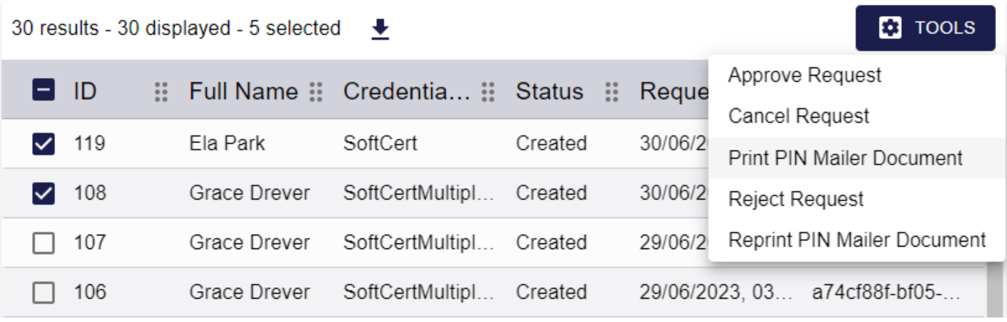
To print multiple mailing documents:

1. Click the **Requests** category.
2. From the **Reports** drop-down list, select one of the following:
   - **Print PIN Mailer**

     Provides a list of all printing requests that have not yet been printed. See section *7.3.9*, *Print PIN Mailer report* for details of the search criteria you can use.
   - **Reprint PIN Mailer**

     Provides a list of all printing requests, whether or not they have already been printed. See section *7.3.10*, *Reprint PIN Mailer report* for details of the search criteria you can use.
3. Click **Search**.

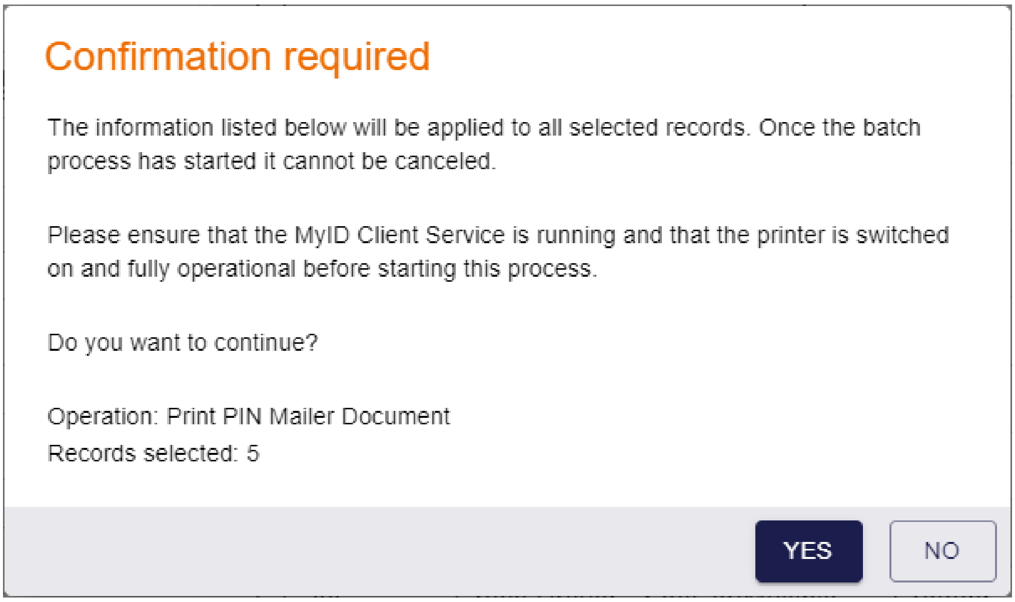
   The list of matching results appears.
4. Use the checkboxes to the left of the requests to select one or more requests.
5. From the **Tools** menu, select **Print PIN Mailer Document** or **Reprint PIN Mailer Document**.



30 results - 30 displayed - 5 selected

⊟	ID	Full Name	Credentia…	Status	Reque	
☑	119	Ela Park	SoftCert	Created	30/06/2	
☑	108	Grace Drever	SoftCertMultipl…	Created	30/06/2	
☐	107	Grace Drever	SoftCertMultipl…	Created	29/06/2	
☐	106	Grace Drever	SoftCertMultipl…	Created	29/06/2023, 03…	a74cf88f-bf05-…

6. The confirmation screen appears.



Confirmation required

The information listed below will be applied to all selected records. Once the batch process has started it cannot be canceled.

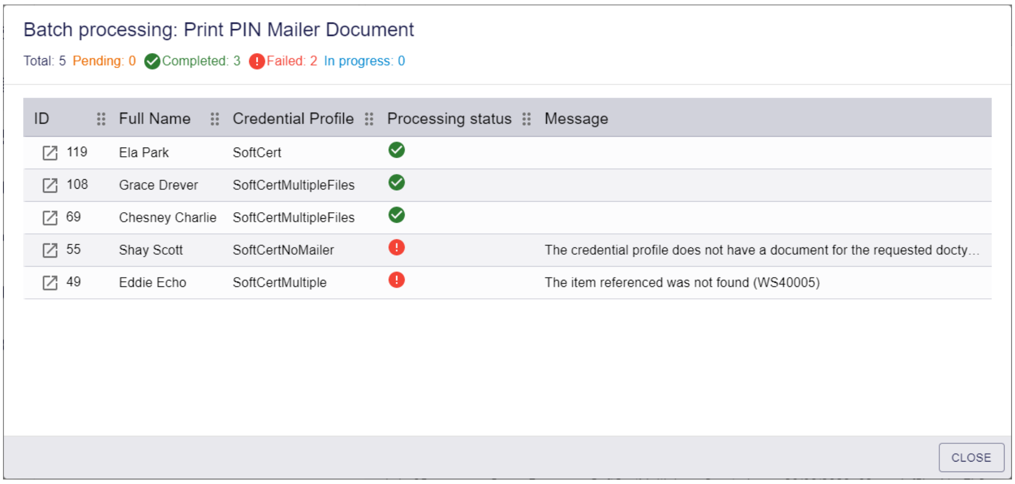
Please ensure that the MyID Client Service is running and that the printer is switched on and fully operational before starting this process.

Do you want to continue?

Operation: Print PIN Mailer Document
Records selected: 5

7. Click **Yes** to proceed with the batch approval, or **No** to go back to the list of requests.

When you click Yes, the Batch Processing screen appears.



Batch processing: Print PIN Mailer Document

Total: 5 Pending: 0 ✓Completed: 3 !Failed: 2 In progress: 0

ID	Full Name	Credential Profile	Processing status	Message
119	Ela Park	SoftCert	✓	
108	Grace Drever	SoftCertMultipleFiles	✓	
69	Chesney Charlie	SoftCertMultipleFiles	✓	
55	Shay Scott	SoftCertNoMailer	!	The credential profile does not have a document for the requested docty...
49	Eddie Echo	SoftCertMultiple	!	The item referenced was not found (WS40005)

The print requests are processed. The table shows the status of each request:

✓	The print succeeded.
!	The print failed. The Message column displays the reason for the failure; for example, there may not be a document template selected for the credential profile.

8. Click **Close**.

14.3 Customizing certificate file names

When you save a soft certificate .pfx file to your PC or to a USB drive, MyID automatically creates a file name in the following format:

`<LogonName>_<PolicyName>.pfx`

where:

- `<LogonName>` is the person's logon name.
- `<PolicyName>` is the name of the certificate policy used to issue the certificate.

Any spaces in the file name, or characters that are not valid for file names (that is, `~` or `$` as the first character, or any of the following characters `" < > | : * ? \ /`) are replaced by underscores.

For example:

`Susan.Smith_PIVSigning_(2).pfx`

To customize the format of these automatically-generated certificate file names, you must edit the `appsettings.Production.json` file of the rest.provision web service:

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 `CertificateFileName` section.

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

   The format is:

```
{
  "MyID": {
    ...
    "CertificateFileName": {
      "default": "[[People.LogonName]] [[PolicyName]]"
    },
    ...
  }
}
```

   You can use the following substitutions:

   - `[[People.FieldName]]` – where `FieldName` is the name of a field in the `vPeopleUserAccounts` view in the MyID database.

     For example:

     `[[People.LogonName]]`

     `[[People.GroupName]]`

- `[[PolicyName]]` – the "friendly" name for the policy. This depends on the certificate authority, and may not be suitable for display; you can substitute unsuitable policy names for more readable text on a policy-by-policy basis; see section *14.3.1*, *File name formats for individual certificate policies*.
- `[[DateTime.Format]]` – where `Format` is the date and time format you want to use.

  Sample codes:

  - `yyyy` – year; for example, `2021`.
  - `MM` – two-digit month; for example, `09`.
  - `MMM` – short month; for example, `Sep`.
  - `MMMM` – full month; for example, `September`.
  - `dd` – two-digit day; for example, `02`.
  - `HH` – hour in 24-hour clock; for example, `23`.
  - `hh` – hour in 12-hour clock; for example, `11`.
  - `mm` – minutes; for example, `29`.
  - `ss` – seconds; for example, `45`.

  You can use `-` to separate the components of the date and time. Do not use `:` or `/` as this causes errors when creating the filename. Any characters you use must be valid for filenames.

  Examples:

  - `[[DateTime.yyyy-MM-dd]]`
  - `[[DateTime.yyyy-MM-dd HHmm]]`

  Note: Times are in UTC.
- `[[RandomNumber.####]]` – adds a random number to the file name. The number of digits in the random number is determined by the number of # signs you include.

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.

14.3.1 File name formats for individual certificate policies

You can also specify custom formats for individual certificate policies.

In the `CertificateFileName` section, add a section for each certificate policy. Any policy not listed uses the `default` format.

```
{
  "MyID": {
    ...
    "CertificateFileName": {
      "default": "[[People.LogonName]] [[PolicyName]]",
      "policy": [
        {
          "name": "PolicyFriendlyName",
          "fileName": "FilenameFormat"
        }
      ]
    },
    ...
  }
}
```

where:

- `name` – the friendly name for the certificate policy.
- `filename` – the format to use for .pfx files for certificates created from that policy.

You can create multiple `name`/`fileName` pairs within the policy node; for example:

```
"policy": [
  {
    "name": "PolicyFriendlyName",
    "fileName": "FilenameFormat"
  },
  {
    "name": "PolicyFriendlyName 2",
    "fileName": "FilenameFormat 2"
  }
]
```

14.3.2 Example custom file name format

For example:

```
"CertificateFileName": {
  "default": "[[People.LogonName]] [[PolicyName]] [[DateTime.yyyy-MM-dd HHmm]]",
  "policy": [
    {
      "name": "PIVSigning (2)",
      "fileName": "[[People.LogonName]] Signing Certificate [[DateTime.yyyy-MM-dd HHmm]]
[[RandomNumber.########]]"
    },
    {
      "name": "PIVEncryption (2)",
      "fileName": "[[People.LogonName]] Encryption Certificate [[DateTime.yyyy-MM-dd
HHmm]]"
    },
  ]
},
```

This example uses a default format that includes the person's logon name, the policy friendly name, and the date and time the certificate was issued.

It also specifies a custom format for the `PivSigning (2)` certificate policy, that replaces the friendly name with the words "Signing Certificate" and an eight-digit random number, and a custom format for `PIVEncryption (2)` that replaces the friendly name with the words "Encryption Certificate".

Example filenames produced by this format are:

- `Susan.Smith PIVCardAuthentication (2) 2023-06-30 1341.pfx`
- `Susan.Smith Encryption Certificate 2023-06-30 1341.pfx`
- `Susan.Smith Signing Certificate 2023-06-30 1341 37593128.pfx`

15 Recovering keys

You can use the MyID Operator Client to request a smart card, VSC, Windows Hello credential, or soft certificate package containing recovered certificates and keys.

You can recover these keys to a new, dedicated device that is used only to store recovered keys, or you can add the recovered keys to an existing issued device. In either case, you must issue the recovered keys to the original owner of the certificate.

See the *Key recovery* section in the ***Administration Guide*** for more information about key recovery; in particular, see the *Setting up the credential profile for key recovery* section for details of setting up a credential profile for a key recovery device. Note, however, that the collection procedure for key recovery requests made through the MyID Core API or the MyID Operator Client is different from the collection procedure for requests made through MyID Desktop.

If the certificate policy is configured to use MyID SecureVault to archive its keys, you can recover the keys from the MyID SecureVault key store; see the *MyID SecureVault* section in the ***Administration Guide*** for details.

See the *Requesting key recovery* section in the ***MyID Core API*** guide for details of using the MyID Core API to request key recovery operations.

This chapter contains information on the following:

- An overview of the key recovery process.

  See section *15.1*, *What is key recovery?*
- Setting up permissions for key recovery, including permissions to the embedded reports used within the key recovery screens.

  See section *15.2*, *Setting up permissions for key recovery*.
- Requesting key recovery, either to a dedicated key recovery device or to an existing issued device.

  See section *15.3*, *Requesting a key recovery*.
- Collecting a key recovery, either to a dedicated key recovery device or as an update to an existing device.

  See section *15.4*, *Collecting recovered keys*.

15.1 What is key recovery?

A certificate and private key is used to encrypt and decrypt information; for example, emails and documents.

If you lose the private key, you cannot access the encrypted information, unless you can recover the private key; to do this, the key must have been securely stored. Secure storage of the private key is called *key escrow*.

Key recovery is the process of retrieving the private key from escrow, along with the certificate, and providing it to the person that needs to access the encrypted information.

In most cases, the private key should only ever be accessible to the certificate owner.

15.1.1 Use cases

The following use cases apply when dealing with key recovery:

- Automated key recovery.

  You can configure your credential profiles to recover archived certificates using the **Action** option on the **Select Certificates** page of the **Credential Profiles** workflow; for example, if a certificate based on this policy has been issued to the user before, and the certificate is live and unexpired, it can be recovered onto the credential. If there are no available archived certificates, a new certificate is issued.

  See the *Selecting certificates* section in the ***Administration Guide*** for more information.

- Self-service key recovery.

  A certificate owner can log onto the MyID Operator Client and choose the certificates they want to recover, either to an existing device that they own, to a new physical device, or as soft certificates.

  They can then collect the new device or device updates through the MyID Operator Client or a self-service application.

- Administrator-initiated key recovery for self-service collection.

  An administrator can log onto the MyID Operator Client, select the person for whom they want to recover certificates, then choose the certificates to recover, either to an existing device belonging to the certificate owner, to a new physical device, or as soft certificates.

  The certificate owner can then collect the new device or device updates through the MyID Operator Client or a self-service application.

- Administrator-initiated key recovery for administrator collection.

  An administrator can log onto the MyID Operator Client, select the person for whom they want to recover certificates, then choose the certificates to recover, either to an existing device belonging to the certificate owner, to a new physical device, or as soft certificates.

  The administrator can then collect the new device or device updates through the MyID Operator Client.

  Note: If the administrator is collecting updates to an existing device belonging to the certificate owner, the certificate owner must be present with their device to enter their PIN.

15.2 Setting up permissions for key recovery

You can control access to the key recovery features using the **Edit Roles** workflow.

Note: In addition to the permissions granting access to the key recovery operations, you must grant additional permissions to use the embedded reports for device and certificate selection.

To set permissions for key recovery operations:

1. In the MyID Operator Client, from the **More** category, select **Configuration Settings > Edit Roles**.

   Alternatively, in MyID Desktop, from the **Configuration** category, select the **Edit Roles** workflow.

   The **Edit Roles** workflow appears in MyID Desktop. See the *Roles* section in the ***Administration Guide*** for details of using this workflow.
2. To request key recovery to an issued device, set the following permissions:
   - **Reports > Certificates To Recover To Device**
   - **Reports > Devices To Recover**
   - **Certificates > Recover Certificates**

   Note: The cardholder or operator who collects the updates to the issued device must also have the appropriate permissions in the **Cards** category; for example:
   - **Collect Updates**
   - **Collect My Updates**
3. To request key recovery to a new device, set the following permissions:
   - **Cards > Recover Certificates To New Device**
   - **Reports > Certificates To Recover**
   - **Certificates > View Certificate**

   Note: The cardholder or operator who validates or collects the new key recovery card must also have the appropriate permissions in the **Cards** category; for example:
   - **Collect Card**
   - **Collect Soft Certificate**
   - **Validate Request**
4. To request a self-service key recovery to an existing device using the **My Devices** option on the MyID Operator Client self-service menu, set the following permission:
   - **Reports > My Devices**
5. Click **Save Changes**.

If you want users to be able to request key recovery to a new device, you must also set the **Allow self requests** configuration option on the **Self-Service** page of the **Security Settings** workflow. Setting this option enables the **Recover Certificates To New Device** and **Recover Certificates To Issued Device** options on the View Person screen for your own user account. Note, however, that the **Recover Certificates To This Device** option on the View Device screen for your own devices is unaffected by this configuration option, so you can still recover certificates to an existing device.

15.3 Requesting a key recovery

Before you can recover keys from archived certificates, you must request a key recovery. This can be one of the following:

- A request to update an existing smart card with the certificates required.

  If you want to recover certificates to an existing device, you must specify the device onto which you want to issue the recovered certificates. This device must be issued to the owner of the certificates you want to recover.

  You can do this either through the View Person screen or the View Device screen.
- A request to issue a new smart card to hold the certificates – this is controlled by credential profile configuration.
- A request to recover the certificates as soft certificates (for example, PFX files, or directly to the system store) – this is controlled by credential profile configuration.

15.3.1 Recovering certificates to an existing device through the View Person screen.

To recover certificates to an existing device through the View Person screen:

1. Search for a person, and view their details.

   See section *4.1*, *Searching for a person* for details.

   If you want to recover certificates for yourself, you can open the View Person screen for your own account using the **View My Account** option on the MyID Operator Client self-service menu.

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

   For example:

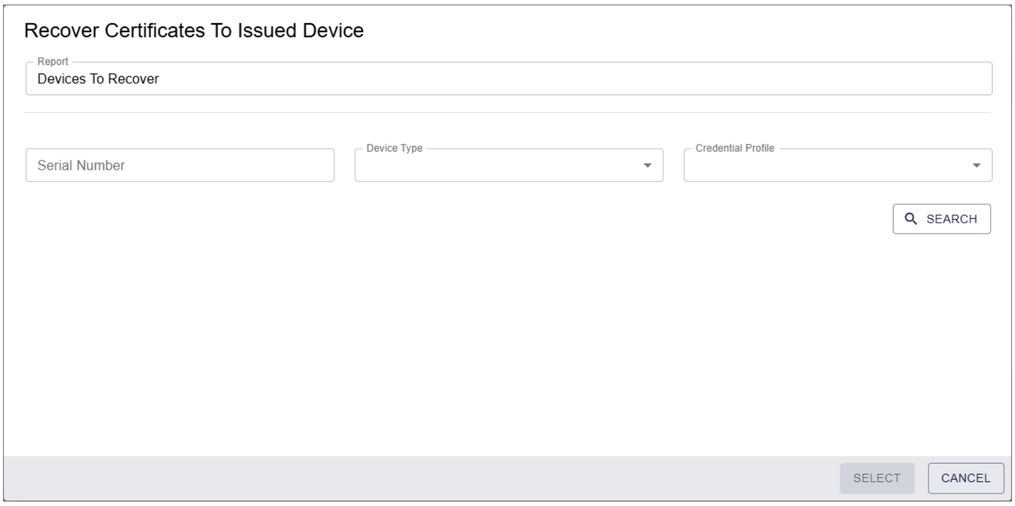
   - Click the link icon ↗ on the **Full Name** field of the View Request form.
   - Click the link icon ↗ on the **Owner** field of the View Device form.

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

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

   Note: The **Recover Certificates To Issued Device** option appears on the View Person screen for your own account only if the **Allow self requests** configuration option on the **Self-Service** page of the **Security Settings** workflow is set. See section *15.2*, *Setting up permissions for key recovery*.

   The device search screen appears.



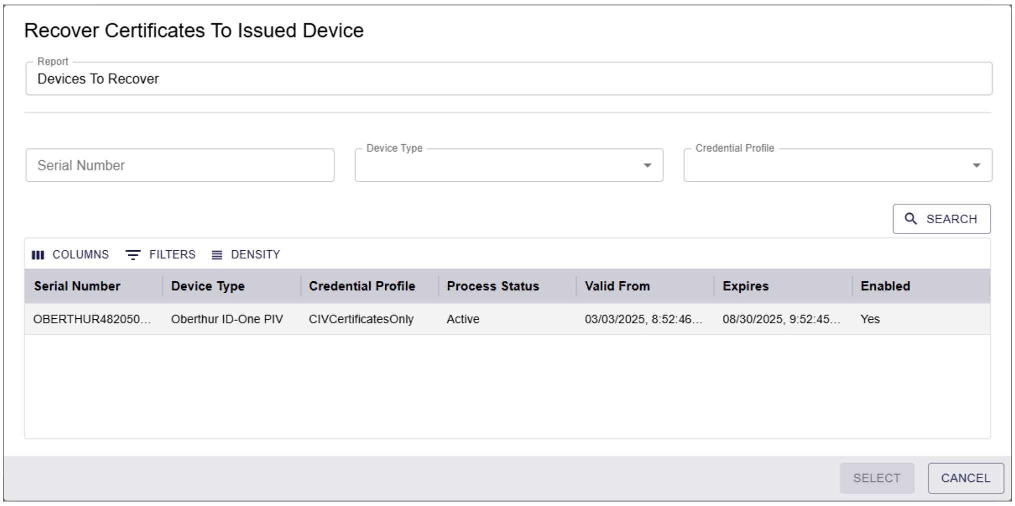
Recover Certificates To Issued Device

Report: Devices To Recover

Serial Number
Device Type
Credential Profile
SEARCH
SELECT
CANCEL

3. Enter any search criteria you want to apply, then click **Search**.

   The list of matching devices belonging to the person appears.



Recover Certificates To Issued Device

Report: Devices To Recover

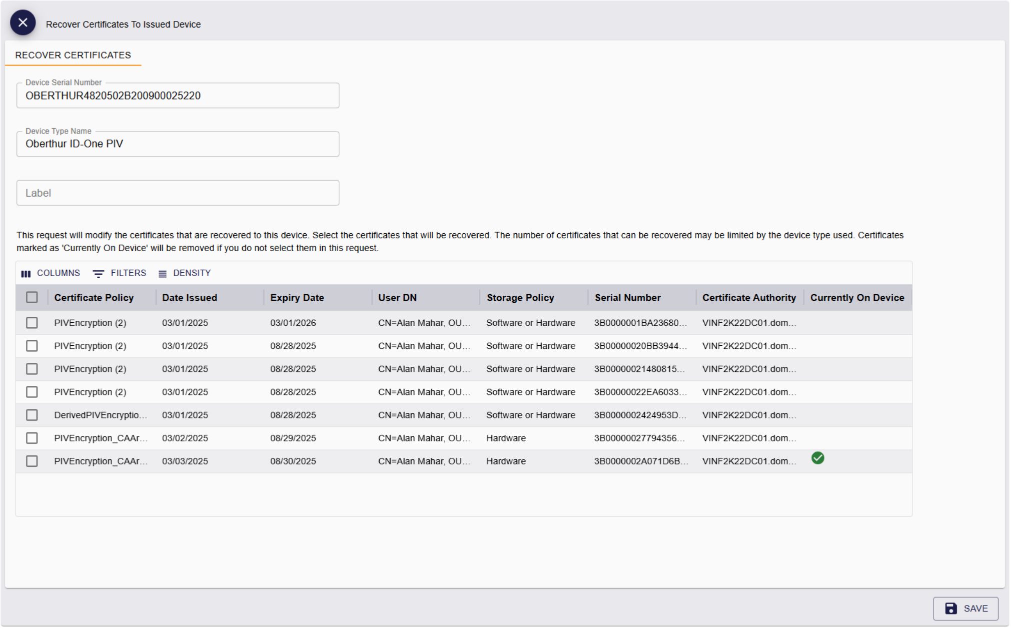
Serial Number
Device Type
Credential Profile
SEARCH
COLUMNS
FILTERS
DENSITY
SELECT
CANCEL

Serial Number	Device Type	Credential Profile	Process Status	Valid From	Expires	Enabled
OBERTHUR482050...	Oberthur ID-One PIV	CIVCertificatesOnly	Active	03/03/2025, 8:52:46...	08/30/2025, 9:52:45...	Yes

Note: You must have permissions to the **Devices To Recover** report that is embedded in this screen; see section *15.2*, *Setting up permissions for key recovery*.

4. Select a device from the list, then click **Select**.

   The list of available certificates to recover appears.



Recover Certificates To Issued Device

RECOVER CERTIFICATES

Device Serial Number: OBERTHUR4820502B200900025220

Device Type Name: Oberthur ID-One PIV

Label

This request will modify the certificates that are recovered to this device. Select the certificates that will be recovered. The number of certificates that can be recovered may be limited by the device type used. Certificates marked as 'Currently On Device' will be removed if you do not select them in this request.

☐	Certificate Policy	Date Issued	Expiry Date	User DN	Storage Policy	Serial Number	Certificate Authority	Currently On Device
☐	PIVEncryption (2)	03/01/2025	03/01/2026	CN=Alan Mahar, OU...	Software or Hardware	3B0000001BA23680...	VINF2K22DC01.dom...	
☐	PIVEncryption (2)	03/01/2025	08/28/2025	CN=Alan Mahar, OU...	Software or Hardware	3B00000020BB3944...	VINF2K22DC01.dom...	
☐	PIVEncryption (2)	03/01/2025	08/28/2025	CN=Alan Mahar, OU...	Software or Hardware	3B00000021480815...	VINF2K22DC01.dom...	
☐	PIVEncryption (2)	03/01/2025	08/28/2025	CN=Alan Mahar, OU...	Software or Hardware	3B00000022EA6033...	VINF2K22DC01.dom...	
☐	DerivedPIVEncryptio...	03/01/2025	08/28/2025	CN=Alan Mahar, OU...	Software or Hardware	3B0000002424953D...	VINF2K22DC01.dom...	
☐	PIVEncryption_CAAr...	03/02/2025	08/29/2025	CN=Alan Mahar, OU...	Hardware	3B00000027794356...	VINF2K22DC01.dom...	
☐	PIVEncryption_CAAr...	03/03/2025	08/30/2025	CN=Alan Mahar, OU...	Hardware	3B0000002A071D6B...	VINF2K22DC01.dom...	✓

   Note: You must have permissions to the **Certificates To Recover To Device** report that is embedded in this screen; see section *15.2*, *Setting up permissions for key recovery*.

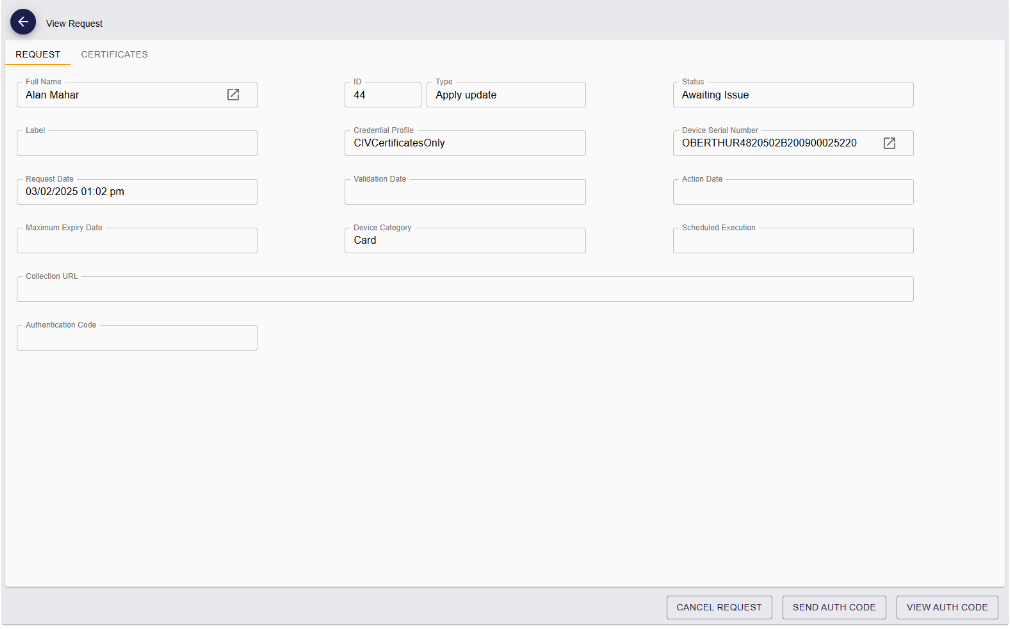
   This screen displays the certificates belonging to the device owner that you can recover to the device.

5. Select the certificates you want to recover to the device.

   Important: The **Currently On Device** column displays whether the certificate is already on the selected device. If you do not select a certificate that is already on the device, the device update process *removes* the certificate. Make sure the list of certificates includes all of the certificates you want to include on the device.

6. Click **Save**.

   MyID creates an update request for the device.


View Request
REQUEST
CERTIFICATES
Label
Validation Date
Action Date
Maximum Expiry Date
Scheduled Execution
Collection URL
Authentication Code
CANCEL REQUEST
SEND AUTH CODE
VIEW AUTH CODE

Full Name: Alan Mahar
ID: 44
Type: Apply update
Status: Awaiting Issue
Credential Profile: CIVCertificatesOnly
Device Serial Number: OBERTHUR4820502B200900025220
Request Date: 03/02/2025 01:02 pm
Device Category: Card

You can now collect this update; for example, click on the link in the **Device Serial Number** box to display the View Device screen, then select the **Collect Updates** option in the button bar at the bottom of the screen. Alternatively, the device owner can collect the updates as a self-service operation. See section *15.4.3*, *Collecting recovered keys to an existing device*.

15.3.2 Recovering certificates to an existing device through the View Device screen

To recover certificates to an existing device through the View Device screen:

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

   See section *5.1*, *Searching for a device*.

   Alternatively, insert the device into a reader.

   See section *5.2*, *Reading a device*.

   If you want to recover your own certificates to your own existing device, you can find your devices using the **My Devices** option on the MyID Operator Client self-service menu.

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

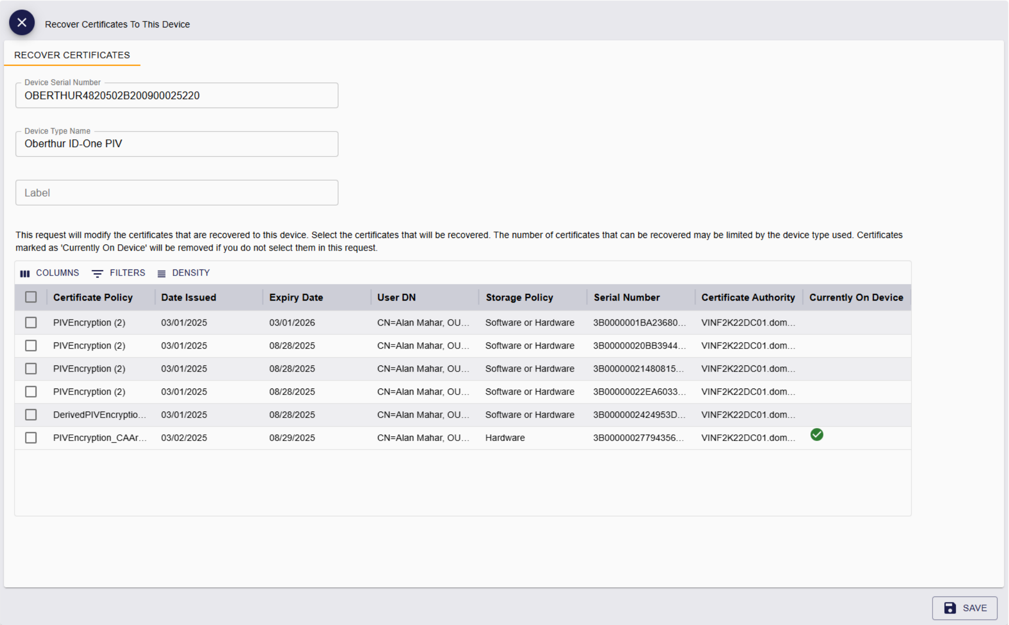
   For example:

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

2. Click the **Recover Certificates To This Device** option in the button bar at the bottom of the screen.

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

   The Recover Certificates To This Device screen appears.



Device Serial Number: OBERTHUR4820502B200900025220

Device Type Name: Oberthur ID-One PIV

Label

This request will modify the certificates that are recovered to this device. Select the certificates that will be recovered. The number of certificates that can be recovered may be limited by the device type used. Certificates marked as 'Currently On Device' will be removed if you do not select them in this request.

☐	Certificate Policy	Date Issued	Expiry Date	User DN	Storage Policy	Serial Number	Certificate Authority	Currently On Device
☐	PIVEncryption (2)	03/01/2025	03/01/2026	CN=Alan Mahar, OU...	Software or Hardware	3B0000001BA23680...	VINF2K22DC01.dom...	
☐	PIVEncryption (2)	03/01/2025	08/28/2025	CN=Alan Mahar, OU...	Software or Hardware	3B00000020BB3944...	VINF2K22DC01.dom...	
☐	PIVEncryption (2)	03/01/2025	08/28/2025	CN=Alan Mahar, OU...	Software or Hardware	3B00000021480815...	VINF2K22DC01.dom...	
☐	PIVEncryption (2)	03/01/2025	08/28/2025	CN=Alan Mahar, OU...	Software or Hardware	3B00000022EA6033...	VINF2K22DC01.dom...	
☐	DerivedPIVEncryptio...	03/01/2025	08/28/2025	CN=Alan Mahar, OU...	Software or Hardware	3B0000002424953D...	VINF2K22DC01.dom...	
☐	PIVEncryption_CAAr...	03/02/2025	08/29/2025	CN=Alan Mahar, OU...	Hardware	3B00000027794356...	VINF2K22DC01.dom...	✓

   Note: You must have permissions to the **Certificates To Recover To Device** report that is embedded in this screen; see section *15.2*, *Setting up permissions for key recovery*.

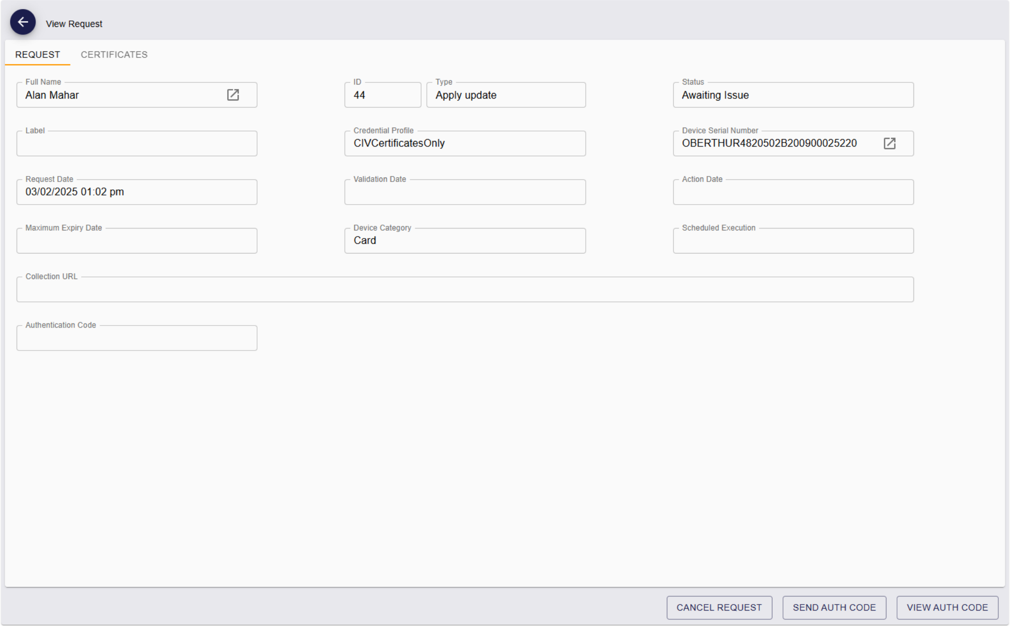
   This screen displays the certificates belonging to the device owner that you can recover to the device.

3. Select the certificates you want to recover to the device.

   Important: The **Currently On Device** column displays whether the certificate is already on the selected device. If you do not select a certificate that is already on the device, the device update process *removes* the certificate. Make sure the list of certificates includes all of the certificates you want to include on the device.

4. Click **Save**.

   MyID creates an update request for the device.

   Full Name: Alan Mahar
   ID: 44
   Type: Apply update
   Status: Awaiting Issue
   Label:
   Credential Profile: CIVCertificatesOnly
   Device Serial Number: OBERTHUR4820502B200900025220
   Request Date: 03/02/2025 01:02 pm
   Validation Date:
   Action Date:
   Maximum Expiry Date:
   Device Category: Card
   Scheduled Execution:
   Collection URL:
   Authentication Code:

   You can now collect this update; for example, click on the link in the **Device Serial Number** box to display the View Device screen, then select the **Collect Updates** option in the button bar at the bottom of the screen. Alternatively, the device owner can collect the updates as a self-service operation. See section *15.4.3*, *Collecting recovered keys to an existing device*.

15.3.3 Recovering certificates to a new device or soft certificate package

Instead of recovering certificates to the certificate owner's existing device, you can issue the recovered certificates to a dedicated key recovery device. These devices are limited in their use, and are intended only to store the recovered certificates.

You can use either a smart card or a soft certificate package to contain the recovered certificates; this is determined by the credential profile. See the *Setting up the credential profile for key recovery* section in the ***Administration Guide***.

To request a key recovery device:

1. Search for a person, and view their details.

   See section *4.1*, *Searching for a person* for details.

   If you want to recover certificates for yourself, you can open the View Person screen for your own account using the **View My Account** option on the MyID Operator Client self-service menu.

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

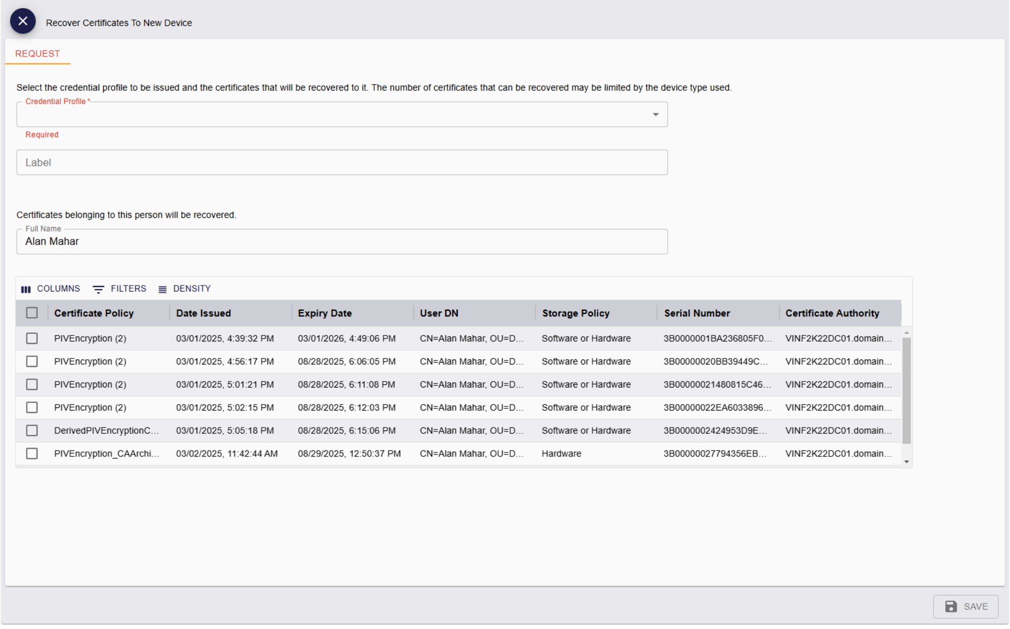
- Click the link icon ☐ on the **Full Name** field of the View Request form.
- Click the link icon ☐ on the **Owner** field of the View Device form.

2. Click the **Recover Certificates To New Device** option in the button bar at the bottom of the screen.

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

   Note: The **Recover Certificates To New Device** option appears on the View Person screen for your own account only if the **Allow self requests** configuration option on the **Self-Service** page of the **Security Settings** workflow is set. See section *15.2*, *Setting up permissions for key recovery*.

   The Recover Certificates To New Device screen appears.



Select the credential profile to be issued and the certificates that will be recovered to it. The number of certificates that can be recovered may be limited by the device type used.

Credential Profile *
Required

Label

Certificates belonging to this person will be recovered.

Full Name: Alan Mahar

☐	Certificate Policy	Date Issued	Expiry Date	User DN	Storage Policy	Serial Number	Certificate Authority
☐	PIVEncryption (2)	03/01/2025, 4:39:32 PM	03/01/2026, 4:49:06 PM	CN=Alan Mahar, OU=D...	Software or Hardware	3B0000001BA236805F0...	VINF2K22DC01.domain...
☐	PIVEncryption (2)	03/01/2025, 4:56:17 PM	08/28/2025, 6:06:05 PM	CN=Alan Mahar, OU=D...	Software or Hardware	3B00000020BB39449C...	VINF2K22DC01.domain...
☐	PIVEncryption (2)	03/01/2025, 5:01:21 PM	08/28/2025, 6:11:08 PM	CN=Alan Mahar, OU=D...	Software or Hardware	3B00000021480815C46...	VINF2K22DC01.domain...
☐	PIVEncryption (2)	03/01/2025, 5:02:15 PM	08/28/2025, 6:12:03 PM	CN=Alan Mahar, OU=D...	Software or Hardware	3B00000022EA6033896...	VINF2K22DC01.domain...
☐	DerivedPIVEncryptionC...	03/01/2025, 5:05:18 PM	08/28/2025, 6:15:06 PM	CN=Alan Mahar, OU=D...	Software or Hardware	3B0000002424953D9E...	VINF2K22DC01.domain...
☐	PIVEncryption_CAArchi...	03/02/2025, 11:42:44 AM	08/29/2025, 12:50:37 PM	CN=Alan Mahar, OU=D...	Hardware	3B00000027794356EB...	VINF2K22DC01.domain...

3. Select a **Credential Profile** from the drop-down list.

   If only one key recovery credential profile is available, it is selected automatically. You may have multiple credential profiles available; for example, one credential profile for recovering certificates to a physical smart card, and another for recovering certificates to a PFX.

4. Optionally, type a **Label** to the request.

   You can use this label to search for the request.

5. Select the certificates you want to recover.

   Note: Check the **Storage Policy** column to ensure that the certificates can be recovered to your chosen device; for example, you cannot recover a certificate with a storage policy of Hardware to a soft certificate.

6. Click **Save**.

MyID creates a request for the device or soft certificates.

You can now collect this device or soft certificates; for example, click the **Collect** option in the button bar at the bottom of the screen. Alternatively, the device owner can collect the device as a self-service operation. See section *15.4.1*, *Collecting recovered keys to a new smart card* and section *15.4.2*, *Collecting recovered keys as soft certificates* for details.

15.4 Collecting recovered keys

Once you have created a request for recovered keys, you can collect the device or the device update. An operator can collect a key recovery device for any user within their scope, or the certificate owner can collect their own device through a self-service operation.

Similarly, an operator can collect a key recovery device update for any user within their scope, as long as they have the device present, or the device owner can update their own device through a self-service operation.

These key recovery requests are treated the same as other device requests and device update requests, subject to the same scope checking and role restrictions based on the associated credential profile.

15.4.1 Collecting recovered keys to a new smart card

When you request key recovery to a new smart card, MyID creates a device request. You can then use the collect operation to collect the key recovery device or PFX containing the recovered archived certificates.

Note: If the credential profile has the **Validate Issuance** option set, an operator must approve the request using the **Approve Request** option on the View Request screen before you can collect the smart card. You cannot use the **Approve Key Recovery** workflow in MyID Desktop; this workflow is for key recovery requests initiated through MyID Desktop only, not for key recovery requests initiated through the MyID Operator Client or the MyID Core API.

The device owner can collect their key recovery smart card in the following ways:

- Through the self-service menu in the MyID Operator Client.

  Open the self-service menu in the MyID Operator Client, then select the collect job from the list.

  Note: You may have to click **Check for Updates** first.
- Through one of the self-service applications (the Self-Service App, the MyID Client for Windows, or the MyID Client for Mac).

  Open the self-service application, then select the **Collect Security Device** task from the list.

An operator can collect a device request in the following ways:

- In the MyID Operator Client, on the View Request screen for the key recovery request, click **Collect** from the options at the bottom of the screen.
- In MyID Desktop, from the **Cards** category, select **Collect Card**.

15.4.2 Collecting recovered keys as soft certificates

When you request key recovery to a soft certificate package, MyID creates a device request that you can collect as a downloaded PFX file or add automatically to your system store (depending on the **Software certificate recovery location** option in the **Key Recovery** section of the credential profile; see the *Setting up the credential profile for key recovery* section in the ***Administration Guide***).

Note: If the credential profile has the **Validate Issuance** option set, an operator must approve the request using the **Approve Request** option on the View Request screen before you can collect the soft certificates. You cannot use the Approve Key Recovery workflow in MyID Desktop; this workflow is for key recovery requests initiated through MyID Desktop only, not for key recovery requests initiated through the MyID Operator Client or the MyID Core API.

An operator can collect the soft certificate request for any user within their scope, and the certificate owner can collect their own soft certificate.

In either case, to collect the soft certificate, in the MyID Operator Client, from the View Request screen for the key recovery request, click **Collect** from the options at the bottom of the screen.

For more information about collecting soft certificates, see section *14.1*, *Collecting a soft certificate*.

15.4.3 Collecting recovered keys to an existing device

When you request key recovery to an existing device, MyID creates a device update request for the specified device. You can then use a device update operation to collect the certificates onto the device.

Important: When you select the certificates to be recovered to the device to create the request, if you deselect a certificate that is already on the device, the device update process *removes* the certificate. Make sure the list of certificates you include in the recovery request includes all of the certificates you want to include on the device.

The device owner can update their device in the following ways:

- Through the self-service menu in the MyID Operator Client.

  Open the self-service menu in the MyID Operator Client, then select the update job from the list.

  Note: You may have to click **Check for Updates** first.
- Through one of the self-service applications (the Self-Service App, the MyID Client for Windows, or the MyID Client for Mac).

  Open the self-service application, then select the **Update Security Device** task from the list.

An operator can assist with updating a device with recovered certificates in the following ways:

- In the MyID Operator Client, from the View Device screen for the device you want to update, click **Collect Updates** from the options at the bottom of the screen.
- In MyID Desktop, from the Cards category, select **Collect Updates**, then insert the device you want to update.

Note: The device owner must be present to insert their PIN for the update to proceed.

15.4.4 Known issues

- **IKB-435 – Device updates after key recovery has been collected may remove the selected certificates**

  When a key recovery request has been processed that recovers a selection of certificates to a device, a subsequent update to that device may remove the certificates depending on the credential profile configuration. As update and reprovision requests for a device synchronize the device’s assigned credential profile, the selected key history may be removed.

  To address this, you are recommended to repeat the key recovery request for the device.

16 Working with the audit trail

MyID retains an audit trail of operations carried out within the system. You can view the audit trail in the following places:

- From the **History** tab of the View Person screen.

  See section *4.1.1*, *Viewing a person's history*.
- From the **Device History** tab of the View Device screen.

  See section *5.1.1*, *Viewing a device's history*.
- From the **Unrestricted Audit Report**.

  See section *7.3.7*, *Unrestricted Audit Report*.

If you have role permissions to the View Full Audit feature, you can click on an entry on the **History** tab of the View Person screen, the **Device History** tab of the View Device screen, or in the **Unrestricted Audit Report** to display the audit information in the View Audit screen. See section *16.1*, *Viewing audit details*.

You can also view the audit trail in the following place:

- **MyID Desktop**

  You can launch the **Audit Reporting** MyID Desktop workflow from the **Additional Reporting** section of the **More** category in the MyID Operator Client. This workflow allows you to list audit events for either a single workflow or task within MyID or for all operations.

  See the *Running the audit report* section in the ***Administration Guide*** for details.

For more information about the audit trail, including how to configure which items are audited and how scope is respected, see the *The audit trail* section in the ***Administration Guide***.

Important: If you are upgrading a customized system that has changed which items are audited, these changes must be applied to the upgraded system; contact customer support quoting reference SUP-334 for more information.

16.1 Viewing audit details

If you have role permissions to the View Full Audit feature, you can click on an entry on the **History** tab of the View Person screen, the **Device History** tab of the View Device screen, or in the **Unrestricted Audit Report** to display the audit information in the View Audit screen.

The View Audit screen contains the following tabs:

- **Audit** – contains basic information about the audit entry, including the operation name and the time the operation started.

  This tab may contain information about the client IP address and identifier, if your system is configured to capture this information. See the *Logging the client IP address and identifier* section in the ***Administration Guide*** for details.

- **Audit Details** – contains details of the information captured about the operation; for example, for a card request, this would contain the name of the credential profile specified.

  If the audit contains a binary object (for example, a user image or signed Terms and Conditions document) you can click on the link to view the stored image or document in a new window.

  CLICK TO VIEW

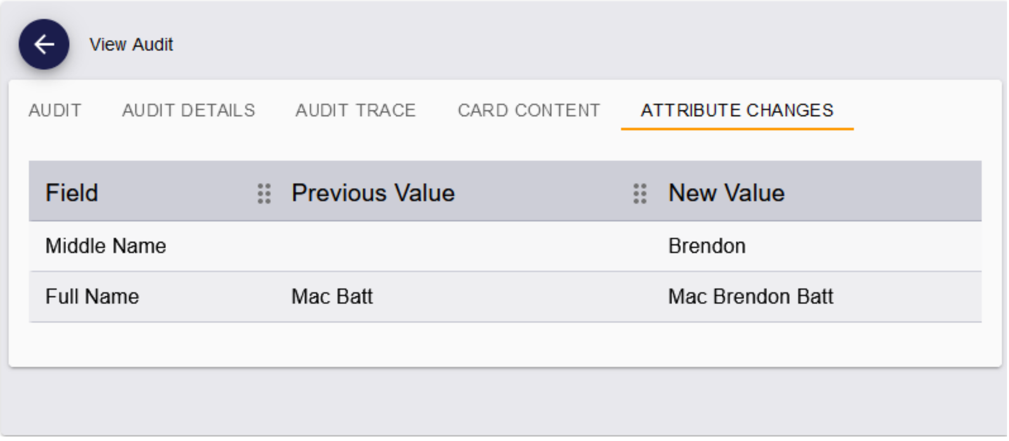
  Note: Signed terms and conditions documents are stored in the audit only when the **Persist terms and conditions** configuration option (on the **Devices** page of the **Operation Settings** workflow) is set, the credential profile was configured for activation, and the cardholder accepted the terms and conditions during the device activation. See the *Storing signed terms and conditions* section in the ***Administration Guide*** for details.

- **Audit Trace** – Displayed for Audit entries only. Contains a list of the individual Trace entries relating to the current Audit entry, if any. You can click on an item in the list to display the View Audit screen for that Trace entry.

  There may be multiple Trace entries nested beneath each Audit entry. These provide lower-level detail about the different stages of the operation being carried out.

- **Card Content** – Displayed for Audit entries only. Contains a list of changes to the device that occurred as part of the audited operation.

- **Attribute Changes** – Displayed for Audit entries only. Contains a list of the fields that were changed as part of the audited operation, as well as the previous value and new value for the field.


View Audit
AUDIT
AUDIT DETAILS
AUDIT TRACE
CARD CONTENT
ATTRIBUTE CHANGES

Field	Previous Value	New Value
Middle Name		Brendon
Full Name	Mac Batt	Mac Brendon Batt

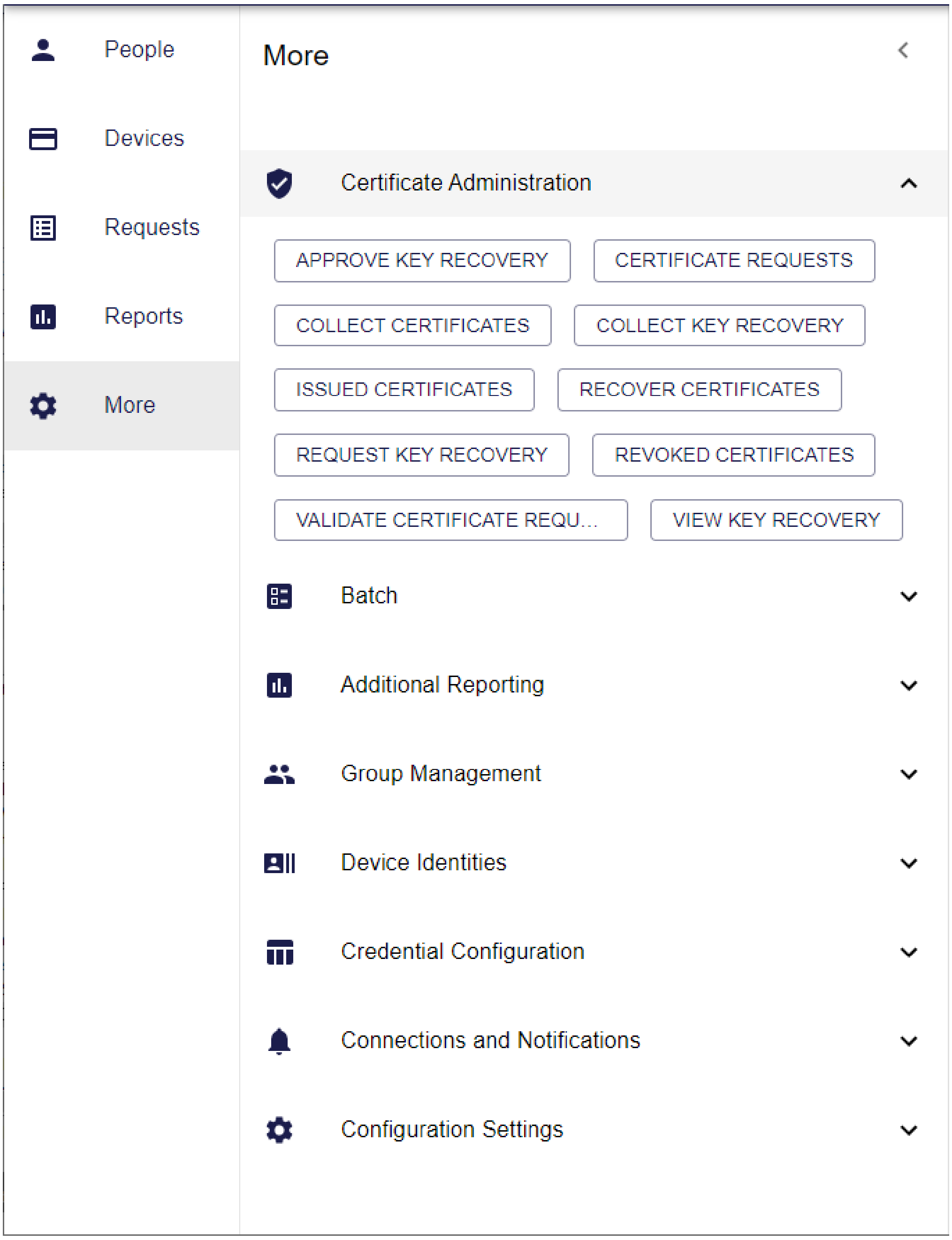
Note: You can also view the attribute changes for a person using the **Attribute Changes** tab on the View Person screen.

- **Signing Details** – Displayed for Trace entries only. Displays any information about the signing that was used for the operation, if any.
- **Signed Data** – Displayed for Trace entries only. Displays the signed content for operation, if any. For example, there may be signed data if the cardholder signed terms and conditions as part of an assisted activation process.

17 Launching administrative workflows

You can launch individual administrative workflows from the **More** category in the MyID Operator Client. The **More** category appears if you have access to one or more workflows in the category.

Access to these workflows is controlled through the **Edit Roles** workflow in MyID Desktop, which is also available as an option in the **Configuration Settings** section of the **More** menu.


People
Devices
Requests
Reports
More
More
Certificate Administration
APPROVE KEY RECOVERY
CERTIFICATE REQUESTS
COLLECT CERTIFICATES
COLLECT KEY RECOVERY
ISSUED CERTIFICATES
RECOVER CERTIFICATES
REQUEST KEY RECOVERY
REVOKED CERTIFICATES
VALIDATE CERTIFICATE REQU...
VIEW KEY RECOVERY
Batch
Additional Reporting
Group Management
Device Identities
Credential Configuration
Connections and Notifications
Configuration Settings

You must have MyID Desktop installed, and the MyID Client Service app installed and running, to use these features. For more information about using MyID Desktop workflows from within the MyID Operator Client, see section *3.3.2*, *Launching MyID Desktop, Self-Service App, or MyID Client for Windows workflows*.

The options in the **More** category are organized into the following sections:

- **Certificate Administration**

  This section contains links that allow you to launch MyID Desktop workflows to work with certificates.

  See section *17.1*, *Using Certificate Administration workflows*.
- **Batch**

  This section contains links that allow you to launch MyID Desktop workflows to carry out batch operations.

  See section *17.2*, *Using Batch workflows*.
- **Bureau**

  This section contains links that allow you to launch MyID Desktop workflows to carry out bureau operations.

  See section *17.3*, *Using Bureau workflows*.
- **Additional Reporting**

  This section contains links that allow you to launch MyID Desktop workflows displaying a variety of reports, including auditing, MI Reports, system events, and system status.

  See section *17.4*, *Using Additional Reporting workflows*.
- **Group Management**

  This section contains links that allow you to launch MyID Desktop workflows to work with groups.

  See section *17.5*, *Using Group Management workflows*.
- **Device Identities**

  This section contains links that allow you to launch MyID Desktop workflows to work with device identities.

  See section *17.6*, *Using Device Identities workflows*.
- **Credential Configuration**

  This section contains links that allow you to launch MyID Desktop workflows to work with credential profiles, card layouts, credential stock and credential serial numbers.

  See section *17.7*, *Using Credential Configuration workflows*.
- **Connections and Notifications**

  This section contains links that allow you to launch MyID Desktop workflows to work with external systems (including directories and certificate authorities) and notifications.

  See section *17.8*, *Using Connections and Notifications workflows*.

- **Configuration Settings**

  This section contains links that allow you to launch MyID Desktop workflows to configure your system settings.

  See section *17.9*, *Using Configuration Settings workflows*.

17.1 Using Certificate Administration workflows

The **Certificate Administration** section of the **More** category allows you to launch MyID Desktop workflows to work with certificates.

Certificate Administration

You can carry out the following:

- **Approve Key Recovery**

  Launches the **Approve Key Recovery** workflow in MyID Desktop to allow you to approve a request for a key recover where the credential profile used to request the key recovery has the **Validate Issuance** option set.

  See the *Validating a key recovery request* section in the ***Administration Guide*** for details.

- **Collect Certificates**

  Launches the **Collect Certificates** workflow in MyID Desktop to allow you to collect any pending certificates onto a smart card.

  See the *Collecting certificates* section in the ***Operator's Guide*** for details.

- **Collect Key Recovery**

  Launches the **Collect Key Recovery** workflow in MyID Desktop to allow you to collect a key recovery job and write the certificates containing the recovered keys to a smart card.

  See the *Collecting a key recovery job for another user* section in the ***Administration Guide*** for details.

- **Recover Certificates**

  Launches the **Recover Certificates** workflow in MyID Desktop to allow you to recover certificates to another user's card. You can also recover soft certificates to a PFX file.

  See the *Recovering someone else's certificates* section in the ***Operator's Guide*** for details.

- **Request Key Recovery**

  Launches the **Request Key Recovery** workflow in MyID Desktop to allow you to request a key recovery job.

  See the *Requesting a key recovery* section in the ***Administration Guide*** for details.

- **Validate Certificate Request**

  Launches the Validate Certificate Request workflow in MyID Desktop to allow you to validate a request for a soft certificate package.

  See the *Validating soft certificate requests* section in the ***Operator's Guide*** for details.

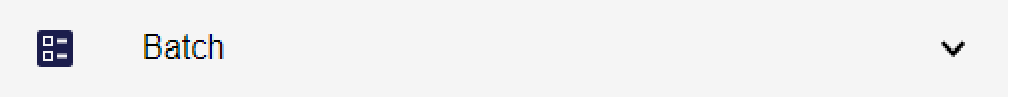
- **View Key Recovery**

  Launches the **View Key Recovery** workflow in MyID Desktop to allow you to view the details of all completed, canceled, or in progress key recovery operations.

  See the *Viewing key recovery operations* section in the ***Administration Guide*** for details.

17.2 Using Batch workflows

The **Batch** section of the **More** category allows you to launch MyID Desktop workflows to carry out batch operations.



You can carry out the following:

- **Batch Collect Card**

  Launches the **Batch Collect Card** workflow in MyID Desktop to allow you to collect a batch of cards in one operation. You can collect cards that have been requested as a batch, or cards that have been requested individually.

  See the *Collecting a batch of cards* section in the ***Operator's Guide*** for details.

- **Batch Encode Card**

  Launches the **Batch Encode Card** workflow in MyID Desktop to allow you to pre-encode cards with their personalization details. When you distribute the cards to the applicants, the applicants can then activate their cards quickly without having to encode them.

  See the *Batch encoding cards* section in the ***Operator's Guide*** for details.

- **Batch Request Card**

  Launches the **Batch Request Card** workflow in MyID Desktop to allow you to request a batch of cards in one operation.

  See the *Requesting a batch of cards* section in the ***Operator's Guide*** for details.

- **Job Management**

  Launches the **Job Management** workflow in MyID Desktop to allow you to view, suspend, unsuspend, or cancel jobs.

  See the *Job management* section in the ***Administration Guide*** for details.

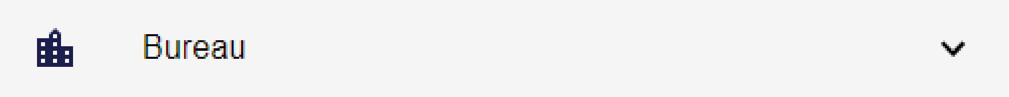
- **Print Card**

  Launches the Print Card workflow in MyID Desktop to allow you to print a card that has already been issued.

  See the *Printing cards* section in the ***Operator's Guide***.

17.3 Using Bureau workflows

The **Bureau** section of the **More** category allows you to launch MyID Desktop workflows that allow you to work with bureau requests.



You can carry out the following:

- **Bureau Requests**

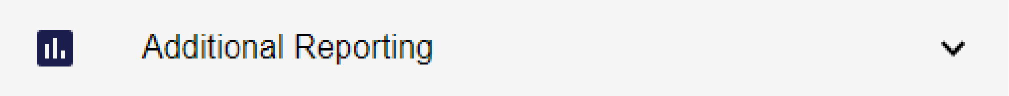
  Launches the **Bureau Requests** workflow in MyID Desktop to allow you to view the progress of your bureau requests.

  This option is available only when your system has been configured to work with a bureau to produce smart cards and has the MyID bureau module installed.

  See your *Bureau Integration Guide* for details.

17.4 Using Additional Reporting workflows

The **Additional Reporting** section of the **More** category allows you to launch MyID Desktop workflows displaying a variety of reports, including auditing, MI Reports, system events, and system status.



You can carry out the following:

- **Audit Reporting**

  Launches the **Audit Reporting** workflow in MyID Desktop to allow you to list audit events for either a single workflow or task within MyID or for all operations.

  See the *Running the audit report* section in the ***Administration Guide*** for details.

- **MI Reports**

  Launches the **MI Reports** workflow in MyID Desktop to allow you to run Management Information Reports against your system.

  See the *Running MI reports* section in the ***Operator's Guide*** for details.

- **System Events**

  Launches the **System Events** workflow in MyID Desktop to allow you to view the events that have occurred on your system.

  See the *System events report* section in the ***Administration Guide*** for details.

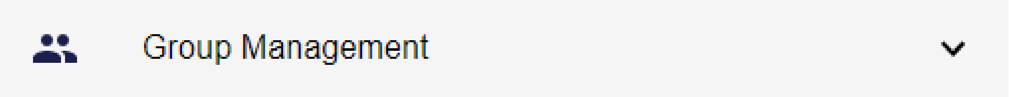
- **System Status**

  Launches the **System Status** workflow in MyID Desktop to allow you to view the status of your system.

  See the *System status report* section in the ***Administration Guide*** for details.

17.5 Using Group Management workflows

The **Group Management** section of the **More** category allows you to launch MyID Desktop workflows that allow you to add, edit, or remove groups.



You can carry out the following:

- **Add Group**

  Launches the **Add Group** workflow in MyID Desktop to allow you to add a new group to your system.

  See the *Adding a group* section in the ***Operator's Guide*** for details.

- **Amend Group**

  Launches the **Amend Group** workflow in MyID Desktop to allow you to change the details of a single group.

  See the *Changing a group* section in the ***Operator's Guide*** for details.

- **Edit Groups**

  Launches the **Edit Groups** workflow in MyID Desktop to allow you to add, rename, edit, and remove groups; you can also import an LDAP directory branch into your group structure.

  See the *Editing groups* section in the ***Operator's Guide*** for details.

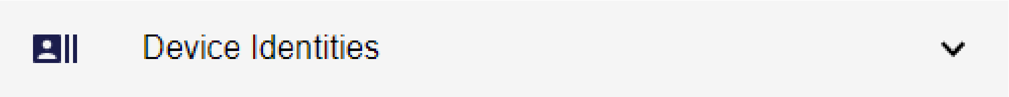
- **Remove Group**

  Launches the **Remove Group** workflow in MyID Desktop to allow you to remove a single group.

  See the *Deleting a group* section in the ***Operator's Guide*** for details.

17.6 Using Device Identities workflows

The **Device Identities** section of the **More** category allows you to launch MyID Desktop workflows that allow you to work with device identities, including adding and editing devices, and requesting, validating, and canceling device identity requests.



For more information on device identities, see the *Managing devices* section in the ***Administration Guide***

You can carry out the following:

- **Add Devices**

  Launches the **Add Devices** workflow in MyID Desktop to allow you to add devices, to which you can then issue device identities.

  See the *Adding devices* section in the ***Administration Guide*** for details.

- **Cancel Device Identity**

Launches the **Cancel Device Identity** workflow in MyID Desktop to allow you to cancel a device identity.

See the *Canceling device identities* section in the ***Administration Guide*** for details.

- **Confirm Cancel Device Request**

  Launches the **Confirm Cancel Device Request** workflow in MyID Desktop to allow you validate a request to cancel a device identity where the credential profile used to request the device identity has the **Validate Cancellation** option set.

  See the *Approving device identity cancellations* section in the ***Administration Guide*** for details.
- **Edit Devices**

  Launches the **Edit Devices** workflow in MyID Desktop to allow you to edit the details for a device.

  See the *Editing a device* section in the ***Administration Guide*** for details.
- **Request Device Identity**

  Launches the **Request Device Identity** workflow in MyID Desktop to allow you to request a device identity for a device.

  See the *Requesting a device identity* section in the ***Administration Guide*** for details.
- **Validate Device Request**

  Launches the **Validate Device Request** workflow in MyID Desktop to allow you to validate a request for a device identity where the credential profile used to request the device identity has the **Validate Issuance** option set.

  See the *Validating a device identity request* section in the ***Administration Guide*** for details.

17.7 Using Credential Configuration workflows

The **Credential Configuration** section of the **More** category allows you to launch MyID Desktop workflows that allow you to work with credential profiles, card layouts, credential stock and credential serial numbers.

Credential Configuration

You can carry out the following:

- **Card Layout Editor**

  Launches the **Card Layout Editor** workflow in MyID Desktop to allow you to specify the content and layout of the information to be printed on a smart card when it is issued.

  See the *Designing card layouts* section in the ***Administration Guide*** for details.
- **Credential Profiles**

  Launches the **Credential Profiles** workflow in MyID Desktop to allow you to specify the content and issuance processes for smart cards, VSCs, mobile identities, and so on.

  See the *Working with credential profiles* section in the ***Administration Guide*** for details.

- **Credential Stock**

  Launches the **Credential Stock** workflow in MyID Desktop to allow you to work with credential stock definitions. Credential stock is relevant only when working with a bureau to produce your smart cards.

  See your *Bureau Integration Guide* for details.

- **Import Serial Numbers**

  Launches the **Import Serial Numbers** workflow in MyID Desktop to allow you to import a range of serial numbers for cards; you can then create a credential profile that will only issue cards that have been previously imported.

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

17.8 Using Connections and Notifications workflows

The **Connections and Notifications** section of the **More** category allows you to launch MyID Desktop workflows that allow you to work with external systems (including directories and certificate authorities) and notifications.

Connections and Notifications

You can carry out the following:

- **Certificate Authorities**

  Launches the **Certificate Authorities** workflow in MyID Desktop to allow you to work with certificate authorities, including connecting to CAs and enabling and configuring certificate templates.

  See the *Connecting to a CA* and *Enabling certificates on a CA* sections in the ***Administration Guide*** for details.

- **Directory Management**

  Launches the **Directory Management** workflow in MyID Desktop to allow you to work with LDAP directories.

  See the *Creating the connections* section in the ***Administration Guide*** for details.

- **Email Templates**

  Launches the **Email Templates** workflow in MyID Desktop to allow you to edit or add email templates to be used for notifications.

  See the *Changing email messages* and *Adding a new email template* sections in the ***Administration Guide*** for details.

- **External Systems**

  Launches the **External Systems** workflow in MyID Desktop to allow you to set up an SMTP server for email notifications and other external systems.

  See the *External systems* section in the ***Administration Guide*** and the *Setting up email* section in the ***Advanced Configuration Guide*** for details.

- **Notifications Management**

  Launches the **Notifications Management** workflow in MyID Desktop to allow you to view, resend, or cancel notifications.

  See the *Using the Notifications Management workflow* section in the ***Administration Guide*** for details.

17.9 Using Configuration Settings workflows

The **Configuration Settings** section of the **More** category allows you to launch MyID Desktop workflows that allow you to configure your system settings.

Configuration Settings

You can carry out the following:

- **Audited Items**

  Launches the **Audited Items** workflow in MyID Desktop to allow you to specify which items are included in the audit trail.

  See the *Specifying the items to audit* section in the ***Administration Guide*** for details.

- **Edit Roles**

  Launches the **Edit Roles** workflow in MyID Desktop to allow you to configure access to workflows and features for each role.

  See the *Roles* section in the ***Administration Guide*** for details.

- **Key Manager**

  Launches the **Key Manager** workflow in MyID Desktop to allow you to manage keys (for example, transport keys and 9B keys).

  See the *The Key Manager workflow* section in the ***Administration Guide*** for details.

- **Licensing**

  Launches the **Licensing** workflow in MyID Desktop to allow you to work with your MyID licenses, including viewing the status of your license, requesting new licenses, and adding new licenses.

  See the *License management* section in the ***Administration Guide*** for details.

- **List Editor**

  Launches the **List Editor** workflow in MyID Desktop to allow you to amend the lists used in various workflows within MyID.

  See the *Changing list entries* section in the ***Administration Guide*** for details.

- **Manage Applet**

  Launches the **Manage Applet** workflow in MyID Desktop to allow you to add, edit, and upgrade applets for loading onto smart cards.

  See the *Managing applets* section in the ***Administration Guide*** for details.

- **Manage GlobalPlatform Keys**

  Launches the **Manage GlobalPlatform Keys** workflow in MyID Desktop to allow you to configure the GlobalPlatform keys for your smart cards.

  See the *Managing GlobalPlatform keys* section in the ***Administration Guide*** for details.
- **Operation Settings**

  Launches the **Operation Settings** workflow in MyID Desktop to allow you to set the configuration options for your MyID system.

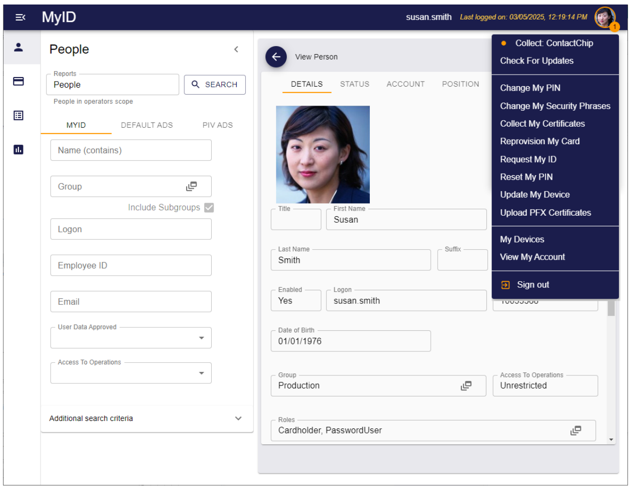
  See the *Operation Settings* section in the ***Administration Guide*** for details.
- **Security Settings**

  Launches the **Security Settings** workflow in MyID Desktop to allow you to set the configuration options related to security for your MyID system.

  See the *Security Settings* section in the ***Administration Guide*** for details.

18 Carrying out self-service operations

The user icon at the top right of the screen allows you to open and close the self-service menu.


MyID
susan.smith
Last logged on: 03/05/2025, 12:19:14 PM
People
SEARCH
People in operators scope
MYID
DEFAULT ADS
PIV ADS
Name (contains)
Group
Include Subgroups
Logon
Employee ID
Email
User Data Approved
Access To Operations
Additional search criteria
View Person
DETAILS
STATUS
ACCOUNT
POSITION
Collect: ContactChip
Check For Updates
Change My PIN
Change My Security Phrases
Collect My Certificates
Reprovision My Card
Request My ID
Reset My PIN
Update My Device
Upload PFX Certificates
My Devices
View My Account
Sign out

Reports: People
Title:
First Name: Susan
Last Name: Smith
Suffix:
Enabled: Yes
Logon: susan.smith
Date of Birth: 01/01/1976
Group: Production
Access To Operations: Unrestricted
Roles: Cardholder, PasswordUser

Using this menu, you can:

- Collect self-service requests.

  See section *18.1*, *Collecting self-service requests*.
- Launch self-service workflows.

  See section *18.2*, *Launching self-service workflows*.
- View a list of your own devices by clicking **My Devices**.

  This launches the My Devices report, which lists all the devices that belong to you.

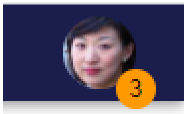
  Note: You must have access to the **My Devices** option in the **Reports** section of the **Edit Roles** workflow to use this option; see section *7.1*, *Granting access to reports*.
- View your own account by clicking **View My Account**.

  This opens the View Person screen with your own account loaded.

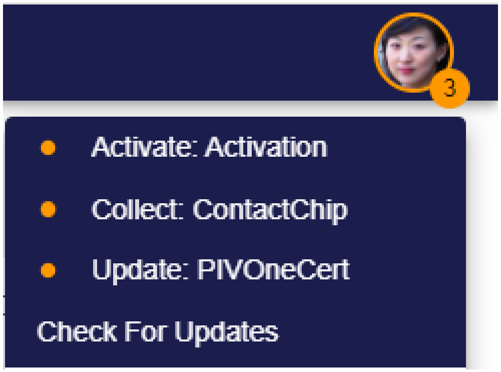
  Note: You are prevented from carrying out most operations on your own account from this screen. Use the self-service menu to carry out operations on your own account.
- Sign out of MyID by clicking **Sign out**.

18.1 Collecting self-service requests

If you have any self-service requests that are available to collect (for example, device updates, activations, or collections), the number of requests appears on a badge on the user icon in the self-service menu.



Open the menu and the self-service requests appear at the top of the menu.



Before you click the option, you are recommended to click **Check For Updates** to ensure that the list of requests is up-to-date, and has not been altered by another operator; for example, another operator may have canceled a device request, or added a device update request.

Click the self-service option, and the Self-Service App or the MyID Client for Windows launches to take you through the collection process.

You must have either the Self-Service App or the MyID Client for Windows installed, and the MyID Client Service app installed and running, to use these features. For more information about using Self-Service workflows from within the MyID Operator Client, see section *3.3.2*, *Launching MyID Desktop, Self-Service App, or MyID Client for Windows workflows*.

18.2 Launching self-service workflows

You can carry out the following self-service operations from the menu:

- **Change My PIN** – Launches the Self-Service App or the MyID Client for Windows with the **Change My PIN** operation, allowing you to change the PIN of your issued device.

  See the *Self-Service App features* section in the ***Self-Service App*** guide or the *Changing your PIN* section in the ***MyID Client for Windows*** guide.
- **Change My Security Phrases** – Launches the Self-Service App or the MyID Client for Windows with the **Change My Security Phrases** operation, allowing you to change the security phrases you use for authentication.

  See the *Self-Service App features* section in the ***Self-Service App*** guide or the *Changing your security phrases* section in the ***MyID Client for Windows*** guide.

- **Collect My Certificates** – Launches MyID Desktop with the **Collect My Certificates** workflow, allowing you to collect packages of soft certificates that have been requested for you by an operator.

  See the *Issuing soft certificates using a credential profile* section in the ***Operator's Guide***.
- **Collect My Key Recovery** – Launches MyID Desktop with the **Collect My Key Recovery** workflow, allowing you to collect a key recovery job and write the certificates containing the recovered keys to a smart card.

  See the *Collecting a key recovery job for yourself* section in the ***Administration Guide***.
- **Recover My Certificates** – Launches MyID Desktop with the **Recover My Certificates** workflow, allowing you to recover your own certificates.

  Note: You must be logged in to the MyID Operator Client with a smart card to use this workflow from the MyID Operator Client. If you need to recover certificates while logged on with a different method (for example, security phrases) you must use MyID Desktop instead.

  See the *Recovering your own certificates* section in the ***Operator's Guide***.
- **Reprovision My Card** – Launches MyID Desktop with the **Reprovision My Card** workflow, allowing you to reprovision your own card.

  See the *Reprovisioning cards* section in the ***Operator's Guide***.
- **Request My ID** – Launches MyID Desktop with the **Request My ID** workflow, allowing you to request a mobile ID or mobile identity document for your own mobile device.

  See the *Requesting a mobile ID for your own mobile device* section in the ***Mobile Identity Management*** guide and the *Requesting a mobile identity document for your own mobile device* section in the ***Mobile Identity Documents*** guide.
- **Reset My PIN** – Launches the Self-Service App or the MyID Client for Windows with the **Reset My PIN** operation, allowing you to reset the PIN of your issued device.

  See the *Self-Service App features* section in the ***Self-Service App*** guide or the *Resetting your PIN* section in the ***MyID Client for Windows*** guide.
- **Update My Device** – Launches the Self-Service App or the MyID App for Windows with the **Update My Device** operation, allowing you to update your issued device.

  See the *Self-Service App features* section in the ***Self-Service App*** guide or the *Updating your device* section in the ***MyID Client for Windows*** guide.
- **Upload PFX Certificates** – Launches MyID Desktop with the **Upload PFX Certificates** workflow, allowing you to upload certificates that have not been issued from a CA using MyID.

  See the *Uploading multiple PFX certificates* section in the ***Administration Guide***.

For more information about using MyID Desktop and Self-Service App workflows from within the MyID Operator Client, see section *3.3.2*, *Launching MyID Desktop, Self-Service App, or MyID Client for Windows workflows*.

19 Troubleshooting and advanced configuration

This section contains information on troubleshooting any problems you may have with the MyID Operator Client, including:

- Using the audit report to troubleshoot issues.

  See section *19.1*, *Viewing the Audit Report*.
- Known issues.

  See section *19.2*, *Known issues*.
- Error messages.

  See section *19.3*, *MyID Operator Client error messages*.
- Advanced configuration.

  See section *19.4*, *MyID Operator Client advanced configuration*.
- Troubleshooting issues with launching MyID Desktop or the Self-Service App.

  See section *19.6*, *Troubleshooting MyID Client Service connection issues*.

19.1 Viewing the Audit Report

The **Audit Reporting** workflow in MyID Desktop contains information about the actions carried out in the MyID system. This can help you troubleshoot any issues that may occur.

When viewing the report, you can select specific MyID Operator Client operations; for example:

- From the **Operation** drop-down list, select **Add Person** to view details of when people were added to the system using MyID Desktop.
- From the **Operation** drop-down list, select **Add Person (MyID Operator Client)** to view details of when people were added to the system using the MyID Operator Client.

For more information on using the **Audit Reporting** workflow, see the *Running the audit report* section in the ***Administration Guide***.

19.2 Known issues

This section contains information about issues you may encounter when working with the MyID Operator Client.

- **IKB-390 – Timezone not reflected when viewing dates in a results list**

  A late breaking issue has been identified that causes search results in the MyID Operator Client to display the time components of date/time fields in Coordinated Universal Time (UTC) instead of the local timezone of the client computer.

  To correct this issue, you can apply an additional update: HOTFIX-12.9.0.1. For further information, contact Intercede customer support quoting reference IKB-390.

19.2.1 .NET Core Desktop Runtime versions

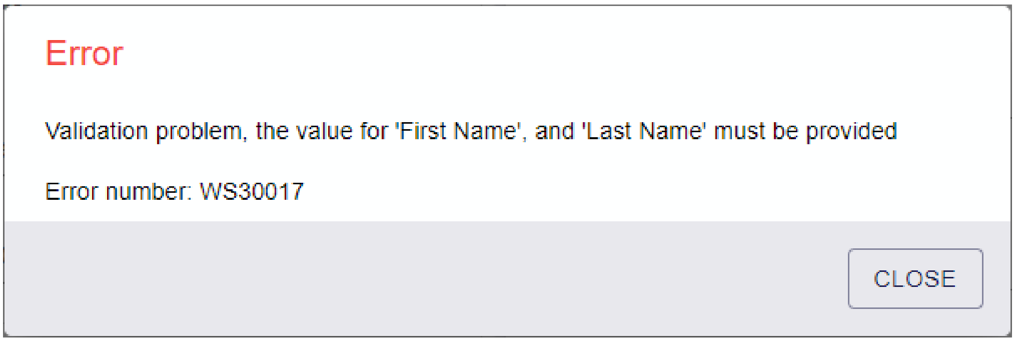
You must have the .NET Core Desktop Runtime installed to use the MyID Client Service. Make sure you are running the correct version; see the *.NET Core Hosting* section in the ***Installation and Configuration Guide*** for details.

19.2.2 Full size images with Narrator on Microsoft Edge

You cannot view an enlarged image preview when using the Narrator screen-reader with Microsoft Edge.

19.3 MyID Operator Client error messages

When an error occurs, the MyID Operator Client displays a message similar to the following:


Error

Validation problem, the value for 'First Name', and 'Last Name' must be provided

Error number: WS30017

The error number is a unique reference to the issue that you can use to look up the causes and potential solutions for the problem; see the *MyID Operator Client error codes* section in the ***Error Code Reference*** guide.

The MyID Client Service may also produce errors; see the *MyID Client Service error codes* section in the ***Error Code Reference*** guide.

You may also encounter errors that are caused by fundamental infrastructure errors; for example, if the server cannot start. In this case, the errors produced by IIS are available in the **Applications and Services Logs** section of the Windows Event Viewer.

19.3.1 MyID Client Service versions

If you attempt to use an older MyID Client Service version that does not support a particular feature, the MyID Operator Client stays in a "please wait" state for approximately five minutes before timing out and displaying a message similar to the following:

```
Unexpected error when communicating with MyID Client Service. Confirm
correct version is installed, and it supports the <feature> method
```

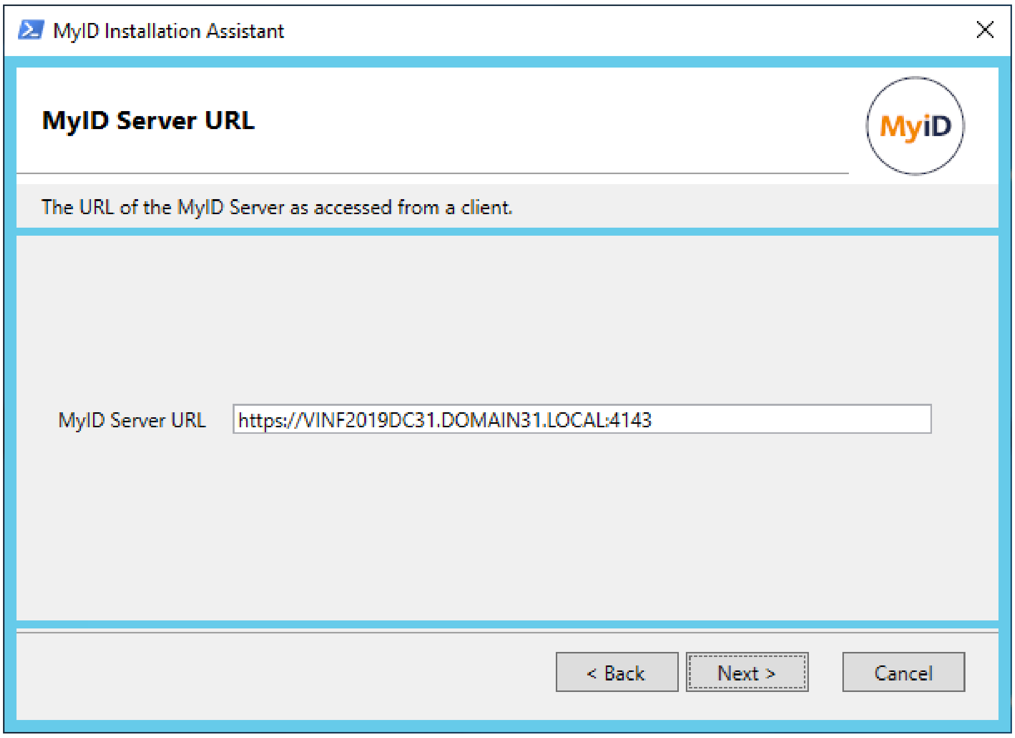
where `<feature>` is one of the following:

Feature	**Description**	**MyID Client Service version**	**Released with MyID version**
`SelectCard`	Reading a card	1.0	11.6
`CaptureFingerprints`	Fingerprint capture	1.1	11.7
`CaptureFacialBioWithMic`	Biometric facial capture	1.1	11.7
`ScanDocument`	Document scanning	1.2	11.8
`ModifyImage`	Image Editor	1.3	12.0
`StartWithToken`	Launch MyID Desktop workflows	1.4	12.1
`GetClientId`	Client identifiers	1.7	12.4
`SetTheme`	Setting the client theme	1.7	12.4
`SelectCard`	Reading a card (with authentication)	1.9	12.6
`PrintHtmlDocument`	Print an HTML mailing document	1.10	12.7
`ProcessCertIssuanceManifest`	Soft certificate issuance	1.10	12.7
`ProcessCertRequestManifest`	Soft certificate request	1.10	12.7

Note: The `StartWithToken` error appears immediately, rather than after the five minute timeout period.

19.4 MyID Operator Client advanced configuration

On the MyID web server, the OAuth2 authentication mechanism relies on the configuration of the URL that the end user will use to access the web server. The MyID Installation Assistant sets this up when you install MyID:



The URL of the MyID Server as accessed from a client.

MyID Server URL: https://VINF2019DC31.DOMAIN31.LOCAL:4143

However, there may be some circumstances under which you need to amend this setting after installation. In this case, you can edit the configuration files for both web services.

19.4.1 The rest.core web service configuration file

The `appsettings.json` file contains the settings for the rest.core web service, and is located in the following folder by default:

```
C:\Program Files\Intercede\MyID\rest.core\
```

The `MyID:Auth:AuthServerUrl` setting provides the URL of web.oauth2 web service. At runtime, the rest.core web service carries out a request to this URL to interact with the web.oauth2 service. If it cannot perform this request, there will be a 500 server error.

The URL must be resolvable on the web server, and https (TLS) must be used.

Note: Confirm that your environment's security (for example, your load balancer or firewall) has been configured to allow full access to the REST web services; while some systems may be locked down to allow only GET and POST, the MyID web services require the full range of verbs, including (but not limited to) GET, POST, PATCH, OPTIONS, and DELETE.

For information on why the URL may not be resolvable, and help in making it resolvable, see section *19.6.3*, *Server name does not resolve*.

Important: The URL settings are updated when you run the installation program. If you have made any manual changes to the `appsettings.json` file, these are overwritten by the values you provide in the installer.

19.4.2 The web.oauth2 web service configuration file

The `appsettings.json` file contains the settings for the web.oauth2 web service, and is located in the following folder by default:

```
C:\Program Files\Intercede\MyID\web.oauth2
```

In the `Clients` section, for the `"ClientId": "myid.operatorclient"`, the `RedirectUris` setting contains a list of URLs. These are the URLs to which the `oauth2` protocol is allowed to redirect back.

The list must contain an entry that represents the URL that the end user will use in the browser to reach the MyID Operator Client. If the URL does not match, when you attempt to sign in, you will see an error similar to:

```
Sorry, there was an error : unauthorized_client
```

Important: The URL settings are updated when you run the installation program. If you have made any manual changes to the `appsettings.json` file, these are overwritten by the values you provide in the installer.

19.4.3 2-way SSL/TLS

While you can use 2-way SSL/TLS for other methods of accessing MyID (the Self-Service App, the Self-Service Kiosk, and MyID Desktop), this is *not* supported for the MyID Operator Client or the MyID Client Service.

19.4.4 Displaying images stored on the web server

By default, MyID stores images in the database. If your system has any images on the web server (for example, if you have an upgraded system, where previously-captured images are on the web server while new images are stored in the database), you must configure the rest.core web service with the image location to allow the MyID Operator Client to display the images that are stored on the web server.

Important: Do not switch your system to storing images on the web server if you are using the MyID Operator Client to capture images. The MyID Operator Client will experience errors if you attempt to capture images when your system is configured to store images on the web server.

Edit the `appsettings.Production.json` file, which is the override file for the `appsettings.json` file, and is located in the following folder by default:

```
C:\Program Files\Intercede\MyID\rest.core\
```

If you do not have an `appsettings.Production.json` file already, you must create one, containing the following:

```
{
  "MyID": {
    "UpimagesFolder": "",
  }
}
```

If you do have an existing `appsettings.Production.json` file, you must add the `UpimagesFolder` entry to the `MyID` section.

In the `MyID` section, change the `UpimagesFolder` entry to point to the directory that contains the images; for example:

```
"UpimagesFolder": "C:\\Program
Files\\Intercede\\MyID\\Web\\WebENT\\upimages",
```

Note: This is the default location; your system may have the images stored in a different location.

Make sure you escape all backslashes with backslashes, as in the example above.

Once you have saved the file, recycle the application pool to refresh the settings:

1. On the MyID web server, in Internet Information Services (IIS) Manager, select **Application Pools**.
2. Right-click the **myid.rest.core.pool** application pool, then from the pop-up menu click **Recycle**.

19.4.5 Changing the port

By default, the MyID Operator Client and its web service use port 8081. If you want to use a different port, after installing MyID and the MyID Client Service, you must edit configuration files on the client and on the web server.

Important: Back up your files before making any changes.

1. On each client PC using the MyID Operator Client:
   a. Open the `MyIDClientService.dll.config` file in a text editor.

      This file is located in the MyID Client Service program folder. By default, this is:

      `C:\Program Files (x86)\Intercede\MyIDClientService`

   b. Locate the following line:

      `<add key="WebSocketPort" value="8081"/>`

   c. Change the `value` to the port you want to use.

      For example:

      `<add key="WebSocketPort" value="6066"/>`

   d. Save the configuration file.
2. On the web server:
   a. Open the `appSettings.js` file in a text editor.

      This file is located in the Operator Client web folder; by default, this is:

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

   b. Locate the following line:

      `wsLocation: "ws://127.0.0.1:8081/"`

   c. Change the port number in the `wsLocation` parameter to the port you want to use.

      For example:

      `wsLocation: "ws://127.0.0.1:6066/"`

   d. Open the `appsettings.json` file for the web.oauth2 web service in a text editor.

      This file is located in the web.oauth2 folder; by default, this is:

      `C:\Program Files\Intercede\MyID\web.oauth2`

   e. Locate the following line in the `"ApiResources": "ssaclient"` section:

      `"port": 8081`

   f. Change the port number to the port you want to use.

      For example:

      `"port": 6066`
3. Reset the web server.
   a. On the MyID web server, in Internet Information Services (IIS) Manager, select **Application Pools**.

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

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

4. On each client PC using the MyID Operator Client, restart the MyID Client Service app:
   a. Right-click the MyID Client Service icon in the task bar.
   b. From the pop-up menu, click Exit.
   c. Clear the browser cache.
   d. Run the **MyID Client Service App** from the Windows Start menu.

Important: If you upgrade your MyID system, you must make these changes again.

Note: If you are using the MyID Client WebSocket Service to allow multiple instances of the MyID Client Service to work through a single WebSocket port, you must also set the WebSocket port in the MyID Client WebSocket Service configuration file to the same value; see the *Updating the port and server details* section in the ***Installation and Configuration Guide*** for details.

19.4.6 Load balancing

The MyID Operator Client and the rest.core web service are stateless, and do not have any session affinity; however, the web.oauth2 web service *does* have state:

- It uses authentication cookies that cannot be shared between multiple server tiers; however, the lifetime of the authentication cookie is just the duration of the authentication, which typically takes a few seconds to complete.
- It uses an RSA key (that by default it automatically generates the first time it runs) that is used to sign the JWT tokens. If there are multiple web.oauth2 instances on different servers, without additional configuration they will each use a different signing key, and therefore each instance will be its own authentication service that is independent from the other instances. This would mean that each client of the web.oauth2 server must target that individual instance, not the load balanced front-end. However; it is possible to configure multiple web.oauth2 instances to share the same key.

There are the following options for managing load balancing:

- The load balancer ties each client to a specific server.

  If a specific client computer is always redirected to the same server, and that server is used to return all websites and web services (operator client, rest.core, web.oauth2) then each web server can work independently.

  Note: In this configuration, any third-party systems that are using the web.oauth2 service themselves for authentication would need to target a specific instance rather than the load-balanced front end.

- The load balancer provides browser session affinity for web.oauth2 (but each web.oauth2 shares the same signing key).

  This is the preferred configuration for multiple servers hosting web.oauth2. In this configuration, you generate a JWT signing key and share it with all instances of web.oauth2 on all servers. All web.oauth2 servers are therefore signing with the same signing key.

In the `appsettings.Production.json` configuration file, there are settings under `MyID:JwtSigner` that you can change to configure the web.oauth2 server to use a specified key or certificate (which you can generate separately).

To configure session affinity and a shared signing key for your web.oauth2 servers:

1. Run the following PowerShell script:

   ```
   $subject = "JWS Signer Certificate"
   $expiry = (Get-Date).AddYears(20)
   New-SelfSignedCertificate -Type Custom -subject $subject -notafter
   $expiry -KeyUsage DigitalSignature -KeyAlgorithm RSA -KeyLength 2048 -
   CertStoreLocation cert:\CurrentUser\My
   ```

   Note: This example uses a certificate with a lifetime of 20 years. The certificate must be replaced before it expires. You can set this to a length that suits your organization's needs by editing the `$expiry` line in the PowerShell script.

2. Take a note of the certificate thumbprint that is produced by the script.

3. Export the certificate as a PFX file:

   a. Prepare the following PowerShell script, making the appropriate substitutions:

      ```
      $CertPassword = ConvertTo-SecureString -String "pfxpassword" -Force
      -AsPlainText
      Export-PfxCertificate -Cert cert:\CurrentUser\My\CertThumbprint -
      FilePath jwtsigningkey.pfx -Password $CertPassword
      ```

      Set the following substitutions:

      - `pfxpassword` – Choose a strong PFX password. Make sure you take a note of this password.
      - `CertThumbprint` – Provide the certificate thumbprint generated above.

        Alternatively, you can retrieve the thumbprint by viewing the certificate.
      - `jwtsigningkey.pfx` – Specify where you want the file to be created.

        You must specify a path to which the user has write access.

   b. Run the PowerShell script.

      The script creates the PFX file.

      Important: You must keep the PFX file and its password safe and secure.

4. On each web server:

   a. Log on as the MyID web services user.

      This is the user under which the web.oauth2 service runs.

   b. Copy the PFX file onto the server.

   c. At the Windows command prompt, run the following, providing the appropriate path and name for the PFX file:

      ```
      certutil -csp "Microsoft Software Key Storage Provider" -user -
      importpfx jwtsigningkey.pfx
      ```

   d. Add the thumbprint to the `appsettings.Production.json` file.

This is the override file for the `appsettings.json` file, and is located in the following folder by default:

`C:\Program Files\Intercede\MyID\web.oauth2\`

If you do not have an `appsettings.Production.json` file already, you must create one, containing the following:

```
{
  "MyID": {
    "JwtSigner": {
        "ContainerName": "MyIDAuth JWT Signer",
        "GenerateKey": true,
        "Thumbprint": "<certificate thumbprint>"
          }
        }
}
```

If the `appsettings.Production.json` file already exists, add the `MyID:JwtSigner` information to the existing file.

Replace `<certificate thumbprint>` with the thumbprint of the certificate you generated above.

e. Reset the web server:
   i. On the MyID web server, in Internet Information Services (IIS) Manager, select **Application Pools**.
   ii. Right-click the **myid.rest.core.pool** application pool, then from the pop-up menu click **Recycle**.
   iii. Right-click the **myid.web.oauth2.pool** application pool, then from the pop-up menu click **Recycle**.

Now all instances of the web.oauth2 service on different servers are using the same JWT signing key. This means that the MyID Operator Client (or any other client) can authenticate to the web.oauth2 service on any web server (that is, determined by load balancing) and can then call the rest.core web service on any web server (determined by load balancing).

Note: In this configuration, a client must still use the same web.oauth2 instance for the duration of the authentication process, as the cookies used by web.oauth2 by default are tied to an instance.

19.4.7 Setting the issuer for load-balanced systems

In the JWT tokens that web.oauth2 creates and that services such as rest.core and ProcessDriver verify, by default the `Issuer` claim is determined according to the web origin that the computer used to access web.oauth2; for example:

```
https://myidserver/web.oauth2
```

In cases where there are multiple MyID servers involved, or a server is accessible using multiple web origins (for example, through a load balancer, or directly accessing the server) then a mismatch of different issuer values can happen, leading to tokens not being trusted.

When this happens, the error in the relying party (for example, rest.core or MyIDProcessDriver) log contains a message similar to:

```
Issuer validation failed
```

You can address this either by setting web.oauth2 to use a fixed `Issuer` value, or by setting rest.core to expect an alternative Issuer value. It is recommended to control this at the web.oauth2 level rather than working around it at rest.core.

19.4.7.1 Setting the issuer in web.oauth2

To set the issuer in web.oauth2:

1. Add the issuer URL to the `appsettings.Production.json` file for the web.oauth2 web service.

   This is the override file for the `appsettings.json` file, and is located in the following folder by default:

   ```
   C:\Program Files\Intercede\MyID\web.oauth2\
   ```

   If you do not have an `appsettings.Production.json` file already, you must create one, containing the following:

   ```
   {
     "MyID": {
       "IssuerUri": "<load balancer>",
       }
   }
   ```

   where:

   - `<load balancer>` – the URL of the web.oauth2 service through the load balancer you are using. For example:

     ```
     "IssuerUri": "https://loadbalancer/web.oauth2"
     ```

     Important: This URL is case sensitive.

   If the `appsettings.Production.json` file already exists, add the `MyID:IssuerUri` information to the existing file.

2. Reset the web server:

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

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

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

You can check that the intended `Issuer` value is set by obtaining the metadata in a browser; for example:

```
https://myserver/web.oauth2/.well-known/openid-configuration
```

19.4.7.2 Setting the issuer in rest.core

As an alternative to setting the issuer in the web.oauth2 service, you can set the issuer in the rest.core service. Note, however, that you are recommended to set the issuer in web.oauth2.

To set the issuer in rest.core:

1. Add the issuer URL to the `appsettings.Production.json` file for the rest.core web service.

   This is the override file for the `appsettings.json` file, and is located in the following folder by default:

   ```
   C:\Program Files\Intercede\MyID\rest.core\
   ```

   If you do not have an `appsettings.Production.json` file already, you must create one, containing the following:

   ```
   {
     "MyID": {
       "Auth": {
         "Issuer": "<load balancer>"
         }
       }
   }
   ```

   where:

   - `<load balancer>` – the URL of the web.oauth2 service through the load balancer you are using. For example:

     ```
     "Issuer": "https://loadbalancer/web.oauth2"
     ```

     Important: This URL is case sensitive.

   If the `appsettings.Production.json` file already exists, add the `MyID:Auth:Issuer` information to the existing file.

2. Reset the web server:

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

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

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

19.4.8 MyID Operator Client pass-through authentication with a load balancer

When you launch a MyID Desktop or Self-Service App operation from the MyID Operator Client, it obtains an extension grant JWT from web.oauth2 which is then passed to the ProcessDriver web service.

By default, ProcessDriver uses the web.oauth2 service at the same web origin that the MyID Operator Client used to reach ProcessDriver. When a load balancer is used, ProcessDriver calls web.oauth2 through the load balancer and may end up reaching another server in the cluster.

If you set up a shared JWT signing key (see section *19.4.6*, *Load balancing*) and set the `IssuerUri` (see section *19.4.7.1*, *Setting the issuer in web.oauth2*) this will work.

However, if you do not have a shared JWT signing key configured, or the ProcessDriver web service cannot reach the load balancer's web origin, this may fail with error similar to:

```
85188 - Unable to connect to the authentication server
```

If this happens, you can configure ProcessDriver to reach web.oauth2 by specifying the following key in the ProcessDriver `myid.config` file:

```
<add key="AuthServerUrl" value="{authentication server URL}" />;
```

By default, this file is in the following folder:

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

Note: You must include `/web.oauth2` at the end of the URL; for example:

```
<add key="AuthServerUrl" value="https://auth.example.com/web.oauth2" />;
```

19.4.9 Translating the MyID Operator Client

For information about translating the MyID interface, contact customer support quoting reference SUP-138.

19.4.10 Setting the location of MyID Desktop or the Self-Service App

The MyID Operator Client can launch workflows in MyID Desktop, the Self-Service App, or the MyID Client for Windows to carry out operations that are not provided by the MyID Operator Client itself; for example, resetting PINs. By default, the MyID Client Service assumes that MyID Desktop has been installed to the default location:

```
C:\Program Files (x86)\Intercede\MyIDDesktop\
```

and the Self-Service App has been installed to the default location:

```
C:\Program Files (x86)\Intercede\MyIDApp\Self Service Application\
```

If you attempt to use a MyID Desktop or Self-Service App workflow and the MyID Client service cannot find the application, an error similar to the following appears:

```
OC10008 - Unable to launch the Desktop Application. Please check
configuration and try again.
```

or:

```
OC10008 - MyID Client Service error
```

If this occurs, you can edit the MyID Client Service configuration file and provide the location of MyID Desktop and the Self-Service App.

1. Open the `MyIDClientService.dll.config` file in a text editor.

   This file is located in the MyID Client Service program folder. By default, this is:

   ```
   C:\Program Files (x86)\Intercede\MyIDClientService
   ```

2. Add the following lines to the `appSettings` section:

   ```
   <add key="DskPath" value="C:\<Desktop install
   folder>\MyIDDesktop.exe"/>
   ```

   ```
   <add key="SsaPath" value="C:\<SSA install folder>\Self Service
   Application\MyIDApp.exe"/>
   ```

   where:

   - `<Desktop install folder>` is the folder where you have installed MyID Desktop.
   - `<SSA install folder>` is the folder where you have installed the Self-Service App.

   For example:

   ```
   <add key="DskPath" value="C:\Intercede\MyIDDesktop\MyIDDesktop.exe"/>
   ```

   ```
   <add key="SsaPath" value="C:\Intercede\MyIDApp\Self Service
   Application\MyIDApp.exe"/>
   ```

3. Save the configuration file.
4. Shut down and restart the MyID Client Service.

Note: If you have used an MSIX installer, the MyID Client Service uses the registered locations for the MyID Desktop, Self-Service App, or MyID Client for Windows, so you do not need to set the location of the applications.

19.4.11 Signature validation

The MyID Client Service performs signature validation of MyID Desktop before it launches the application to ensure that all components are properly signed by Intercede and have not been tampered with. These checks are performed using the native Windows APIs, and may require the client to connect to the Internet to retrieve the latest Certificate Revocation Lists (CRLs) for revocation checks of the Intercede signing certificate. If the client is permanently running in an isolated environment without access to the Internet, the CRLs cannot be retrieved, which can cause signature verification to fail.

You can disable these checks by editing the MyID Client Service configuration file.

1. Open the `MyIDClientService.dll.config` file in a text editor.

   This file is located in the MyID Client Service program folder. By default, this is:

   ```
   C:\Program Files (x86)\Intercede\MyIDClientService
   ```
2. Add the following line to the `appSettings` section:

   ```
   <add key="ComponentVerificationSkipRevocationChecks" value="true"/>
   ```
3. Save the configuration file.

19.4.12 Fast user switching

The MyID Client Service must bind to a WebSocket port that the MyID Operator Client is aware of, but only one instance can be bound to a port at a time. By default, if the MyID Client Service detects that the current user's session is being locked, it shuts down any running MyID Client Service applets (for example, the Select Security Device pop-up window, or the MyID Document Scanner) and unbinds from the WebSocket port to allow it to be consumed in another session.

When the MyID Client Service detects the session being unlocked, it rebinds to the WebSocket port.

This allows you to use the fast user switching feature of Windows.

Note. however, that if a MyID Desktop workflow has been launched by the MyID Operator Client, the Desktop instance remains open so the workflow can be completed, although the Operator Client will not receive feedback as it becomes disconnected when the MyID Client Service unbinds from the WebSocket port.

If you do not want your MyID Client Service pop-up windows to close when you lock your workstation, you can edit the MyID Client Service configuration file.

1. Open the `MyIDClientService.dll.config` file in a text editor.

   This file is located in the MyID Client Service program folder. By default, this is:

   `C:\Program Files (x86)\Intercede\MyIDClientService`
2. Set the `SupportFastUserSwitching` line in the `appSettings` section to `false`:

   ```
   <add key="SupportFastUserSwitching" value="false"/>
   ```

   If this line does not exist in the configuration file, you can add it to the `appSettings` section.
3. Save the configuration file.

Important: When this option is set to `false`, if you use the Fast User Switching feature in Windows to switch to another user account while the MyID Client Service is already running means the second login cannot launch the MyID Client Service because the port has already been consumed.

19.4.13 Configuring the timeout for launching external applications

The MyID Client Service can launch other applications (for example, MyID Desktop or the Self-Service App). You can configure the length of time the MyID Client Service waits before returning an error. By default, this is 60 seconds.

You can change the timeout by editing the MyID Client Service configuration file.

1. Open the `MyIDClientService.dll.config` file in a text editor.

   This file is located in the MyID Client Service program folder. By default, this is:

   `C:\Program Files (x86)\Intercede\MyIDClientService`

2. Edit the following line in the `appSettings` section:

   ```
   <add key="ExternalClientConnectionTimeoutSeconds" value="60"/>
   ```

   If this line does not exist in the configuration file, you can add it to the `appSettings` section.

3. Save the configuration file.

19.4.14 Changing the number of buttons displayed in the button bar

By default, the MyID Operator Client displays four buttons in the button bar. You can increase or decrease the number of buttons displayed. The minimum number of buttons displayed is one; if you set the limit high enough, you can display a button for each action to which you have access.

1. On the web server:

   a. Open the `appSettings.js` file in a text editor.

      This file is located in the Operator Client web folder; by default, this is:

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

   b. Locate the following line:

      ```
      numberOfFormActionsShown: 4,
      ```

   c. Change the value to the number of buttons you want to display.

      For example:

      ```
      numberOfFormActionsShown: 3,
      ```

   d. Save the file.

2. On each client, close the MyID Operator Client browser window.

   This ensures that the browser picks up the latest settings from the server.

3. Open the MyID Operator Client page and sign in.

19.4.15 Configuring re-authentication timeout periods

By default, MyID provides and authentication session for one hour, which can be extended at any point up to two hours after last using the MyID Operator Client, up to a limit of six days after the original authentication; see section *3.2.10*, *Timeouts and re-authentication*.

If you want to change these defaults, you can edit the application settings file for the web.oauth2 web service.

1. On the web server, in a text editor, open the `appsettings.Production.json` file for the web service.

   By default, this is:

   `C:\Program Files\Intercede\MyID\web.oauth2\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 `Clients` section, edit the section with a `ClientID` of `myid.operatorclient`.

   If the file does not contain this client, you can copy the details from the `appsettings.json` file. You do not need to copy the whole section, just the options you want to change.

   Important: Copy the `myid.operatorclient` settings to the same place (the first entry in the `Clients` section) in the `appsettings.Production.json` file as in the `appsettings.json` file; entries in arrays in this file are determined by their index.

   For example:

```
"Clients": [
  {
    "SlidingRefreshTokenLifetime":  7200,
    "AbsoluteRefreshTokenLifetime":  518400,
    "AccessTokenLifetime":  3600,
  },
  {},
  ...
```

3. Set the following values:
   - `SlidingRefreshTokenLifetime` – the number of seconds within which you can extend the authentication. The default is `7200` (two hours).
   - `AbsoluteRefreshTokenLifetime` – the number of seconds after which you must re-authenticate, even if you have been continually extending the authentication. The default is `518400` (six days).
   - `AccessTokenLifetime` – the number of seconds for which an access token is valid after authentication. The default is `3600` (one hour).
4. Save the file.
5. Recycle the application pool to refresh the settings:

   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**.

19.4.16 Enabling or disabling re-authentication

By default, you can extend your authentication session with the MyID Operator Client by continuing to use it; see section *3.2.10*, *Timeouts and re-authentication*.

If you want to disable this feature, and require re-authentication whenever the session expires (by default, after one hour) you can edit the MyID Operator Client settings file.

1. On the web server:
   a. Open the `appSettings.js` file in a text editor.

      This file is located in the Operator Client web folder; by default, this is:

      `C:\Program Files\Intercede\MyID\OperatorClient`
   b. Locate the following line:

      `authServerScopes: "myid.rest.basic offline_access",`
   c. Remove the `offline_access` scope to disable the extension of authentication sessions.

      For example:

      `authServerScopes: "myid.rest.basic",`
   d. Save the file.
2. On each client, close the MyID Operator Client browser window.

   This ensures that the browser picks up the latest settings from the server.
3. Open the MyID Operator Client page and sign in.

19.4.17 Changing the number of Add buttons

By default, the MyID Operator Client displays up to two **Add** buttons; for example, you may have a customized system with different types of People you can add. If there are additional options, these are available using the **...** option. You can adjust the number of displayed **Add** buttons; for example, you may have three different types of people, and want all three **Add** buttons to be visible.

1. On the web server:
   a. Open the `appSettings.js` file in a text editor.

      This file is located in the Operator Client web folder; by default, this is:

      `C:\Program Files\Intercede\MyID\OperatorClient`
   b. Locate the following line:

      ```
      numberOfAddActionsShown: 2,
      ```
   c. Change the value to the number of Add buttons you want to display.

      For example:

      ```
      numberOfAddActionsShown: 3,
      ```
   d. Save the file.
2. On each client, close the MyID Operator Client browser window.

   This ensures that the browser picks up the latest settings from the server.
3. Open the MyID Operator Client page and sign in.

19.4.18 Changing the size of the authentication pop-up window

The size of the authentication pop-up of the MyID Operator Client is appropriate if MyID is configured only for internal authentication, but you may want to change the size of the pop-up if you are using external IDPs that require extra space.

You can configure the height and width of the pop-up in the MyID Operator Client settings file.

1. On the web server:
   a. Open the `appSettings.js` file in a text editor.

      This file is located in the Operator Client web folder; by default, this is:

      `C:\Program Files\Intercede\MyID\OperatorClient`
   b. Locate the following line:

      `authWindowWidth: 550,`
   c. Change the value to the width that you want the authentication pop-up to be, in pixels.

      For example:

      `authWindowWidth: 600,`
   d. Locate the following line:

      `authWindowHeight: 550,`
   e. Change the value to the height that you want the authentication pop-up to be, in pixels.

      Note: This height does not include the height of the browser's title bar or address bar.

      For example:

      `authWindowHeight: 700,`
   f. Save the file.
2. On each client, close the MyID Operator Client browser window.

   This ensures that the browser picks up the latest settings from the server.
3. Open the MyID Operator Client page and sign in.

19.4.19 Configuring certificate saving and printing

You can configure the behavior of MyID when using the MyID Client Service to save soft certificates or print documents.

1. Open the `MyIDClientService.dll.config` file in a text editor.

   This file is located in the MyID Client Service program folder. By default, this is:

   ```
   C:\Program Files (x86)\Intercede\MyIDClientService
   ```

2. Edit the following settings in the `appSettings` section:
   - `AllowAutoSave` – by default, `true`. Set to `true` to allow MyID to select an external drive to which it can write soft certificates, or `false` to prevent this.
   - `AllowedSaveFileExtensions` – by default, `cer;pfx`. Set this to a semicolon-delimited list of allowed file extensions that you can use to write soft certificates to a file.
   - `AllowPrintWithoutConfirm` – by default, `true`. Set to `true` to allow MyID to print a mailing document silently without confirmation, or `false` to prevent this.
   - `EmptyDriveIgnoreRecycleBin` – by default, `false`. Set to `true` to ignore the Recycle Bin when checking if an external drive is empty, or `false` to check the Recycle Bin. By default, Windows does not add a Recycle Bin to USB drives.
   - `EmptyDriveIgnoreVolumeInformation` – by default, `true`. Set to true to ignore the special `VolumeInformation` directory that Windows adds to all drives by default when checking if an external drive is empty, or false to include this drive.

   If the lines do not exist in the configuration file, you can add them to the `appSettings` section; the format is:

   ```
   <add key="optionname" value="value"/>
   ```

   For example:

   ```
   <add key="AllowedSaveFileExtensions" value="cer;pfx"/>
   ```

3. Save the configuration file.

19.4.20 Configuring the priority for self-service applications

When you launch a self-service operation from the user menu (for example, collecting a device, or changing your security phrases), by default the MyID Client Service determines which application to use by checking first if the Self-Service App is installed, and if not, checking whether the MyID Client for Windows is installed.

If you want to change this priority so that the MyID Client Service checks for the MyID Client for Windows first, and only if that app is not installed, checks for the Self-Service App, you can set a configuration option.

To change the self-service application priority:

1. Open the `MyIDClientService.dll.config` file in a text editor.

   This file is located in the MyID Client Service program folder. By default, this is:

   ```
   C:\Program Files (x86)\Intercede\MyIDClientService
   ```
2. Edit the following setting in the `appSettings` section:

   - `PreferXplatSsa` – set this option to `true` to prefer the MyID Client for Windows, or `false` to prefer the Self-Service App. The default is `false`.

   If the line does not exist in the configuration file, you can add it to the `appSettings` section; for example:

   ```
   <add key="PreferXplatSsa" value="true"/>
   ```
3. Save the configuration file.

19.5 Refreshing the cache

When using the MyID Operator Client or other systems that use the rest.core, rest.provision, or web.oauth2 web services, the web services will check whether they need to refresh any cached information if it has been more than five seconds (by default) since they last checked.

19.5.1 Cached information

The following information in the MyID system is cached by the web services, and is refreshed frequently:

- Changes to configuration options made in the **Operation Settings** and **Security Settings** workflows.
- Changes to logon mechanisms made in the **Security Settings** workflow.
- Changes made in the **List Editor**.
- Changes made in the **Email Templates** workflow.
- Changes made by server configuration (CONFIG) package (for example, status mappings and binary object types).
- Changes applied from a Project Designer script (for example, MI reports and form layouts).

If you make a change to any of the above, after a maximum of five seconds (by default), the change is reflected in the behavior of the MyID Operator Client.

19.5.2 Excluded data

The following information is not affected by the cache refresh:

- Card properties files – as these files are not stored in the database, and instead stored as separate files, if you make any changes to card properties files you must you must recycle the application pools used for MyID in IIS, and restart the MyID `Edefice_BOL` component.
- Client applications – any caching that is carried out on the client applications (MyID Desktop, the Self-Service App, or the Self-Service Kiosk) is unaffected by the web service cache refresh.
- Dynamic data – the refresh mechanism applies only to static data that is not dependent on a user's permissions; some data is always retrieved fresh and does not use the cache. For example:
  - Roles
  - Credential profiles
  - Groups (including admin groups)

19.5.3 Configuring the cache refresh time

By default the cache refresh time is set to five seconds. This has been designed to have a minimal impact on performance; if the web service is not making any requests, it does not check whether it needs to refresh its cache. When the web service needs to obtain some information (for example, a configuration setting) it checks whether its cache is more than five seconds old, and if so, it checks the timestamp in the database for configuration changes and refreshes its cache if necessary.

However, you may want to adjust the cache refresh time for your system. To do so, edit the `appsettings.Production.json` files for the web services, which are the override files for the `appsettings.json` files, and are located in the following folders on the MyID web server by default:

`C:\Program Files\Intercede\MyID\rest.core\`

`C:\Program Files\Intercede\MyID\rest.provision\`

`C:\Program Files\Intercede\MyID\web.oauth2\`

If you do not have an `appsettings.Production.json` file already in each folder, you must create one, containing the following:

```
{
  "MyID":{
    "Caching":{
      "Interval":5
    }
  }
}
```

If you do have an existing `appsettings.Production.json` file, you must add the `Caching:Interval` entry to the `MyID` section.

Set the `Interval` value to the number of seconds for the cache refresh time.

Important: Do not set the `Interval` value to `0` – this causes the web services to check the database every time they use cached data, and this traffic can cause your system to slow down appreciably.

Once you have saved the files, recycle the application pools to refresh the settings:

1. On the MyID web server, in Internet Information Services (IIS) Manager, select **Application Pools**.
2. Right-click the **myid.rest.core.pool** application pool, then from the pop-up menu click **Recycle**.
3. Right-click the **myid.rest.provision.pool** application pool, then from the pop-up menu click **Recycle**.
4. Right-click the **myid.web.oauth2.pool** application pool, then from the pop-up menu click **Recycle**.

The MyID Edefice_BOL component also implements a cache refresh. To configure the cache refresh time for the Edefice_BOL component, you can edit the MyID application server registry. In the following key:

```
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Intercede\Edefice\Server
```

Create a DWORD value named:

```
CacheRefreshInterval
```

and set the value to the number of milliseconds for the cache refresh time; if this value does not exist, by default the Edefice_BOL component uses 5000 milliseconds (five seconds) for the cache refresh time.

19.5.4 Refreshing the cache through the MyID Core API

For your own applications, you may want to have control over refreshing the cache. You can force a refresh of the cache through the MyID Core API using the following endpoint:

```
POST /api/Service/RepopulateCache
```

See the Swagger API documentation for more information.

19.6 Troubleshooting MyID Client Service connection issues

This section contains information about problems you may experience when using the MyID Client Service to connect to MyID Desktop or the Self-Service App.

19.6.1 Connection issues

If you attempt to use a feature of the MyID Operator Client and get an error similar to:

```
OC10009 – Unable to connect to MyID Desktop or the Self-Service App. Please
try again.
```

This means there has been a problem with the connection between the MyID Client Service and MyID Desktop or the Self-Service App that caused the operation to exceed the timeout period. By default, this is 60 seconds; for information on configuring the timeout, see section *19.4.13*, *Configuring the timeout for launching external applications*.

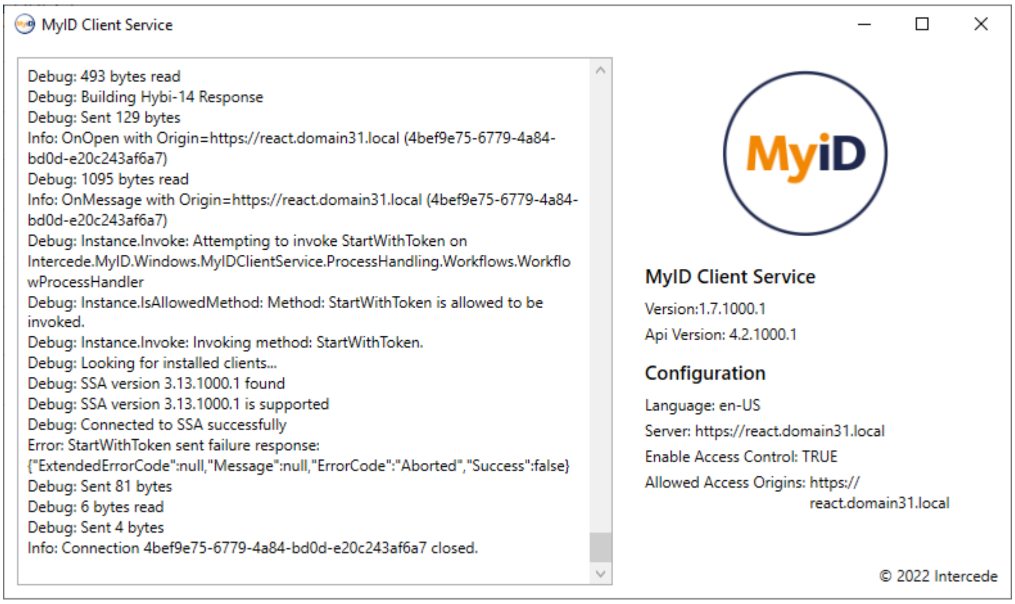
The possible causes are:

- The application could not start.
- The application took a long time to start.
- The application is already running, but not responding.

The troubleshooting procedure for this issue is:

1. Check the MyID Client Service log:
    a. Right-click the MyID Client Service icon in the Windows system tray.
    b. From the pop-up menu, click **Show**.

       The MyID Client Service window appears.



```
Debug: 493 bytes read
Debug: Building Hybi-14 Response
Debug: Sent 129 bytes
Info: OnOpen with Origin=https://react.domain31.local (4bef9e75-6779-4a84-
bd0d-e20c243af6a7)
Debug: 1095 bytes read
Info: OnMessage with Origin=https://react.domain31.local (4bef9e75-6779-4a84-
bd0d-e20c243af6a7)
Debug: Instance.Invoke: Attempting to invoke StartWithToken on
Intercede.MyID.Windows.MyIDClientService.ProcessHandling.Workflows.Workflo
wProcessHandler
Debug: Instance.IsAllowedMethod: Method: StartWithToken is allowed to be
invoked.
Debug: Instance.Invoke: Invoking method: StartWithToken.
Debug: Looking for installed clients...
Debug: SSA version 3.13.1000.1 found
Debug: SSA version 3.13.1000.1 is supported
Debug: Connected to SSA successfully
Error: StartWithToken sent failure response:
{"ExtendedErrorCode":null,"Message":null,"ErrorCode":"Aborted","Success":false}
Debug: Sent 81 bytes
Debug: 6 bytes read
Debug: Sent 4 bytes
Info: Connection 4bef9e75-6779-4a84-bd0d-e20c243af6a7 closed.
```

MyID Client Service

Version:1.7.1000.1

Api Version: 4.2.1000.1

Configuration

Language: en-US

Server: https://react.domain31.local

Enable Access Control: TRUE

Allowed Access Origins: https://react.domain31.local

© 2022 Intercede

    c. Check the log output for any messages relating to starting MyID Desktop (`DSK`) or the Self-Service App (`SSA`).

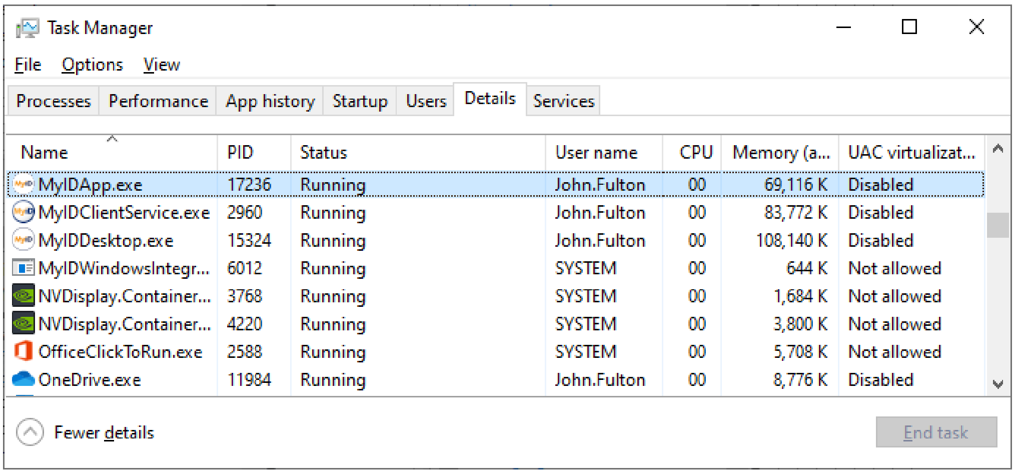
       If the problem is not apparent, continue with the troubleshooting.

2. Check whether the problem is a slow startup:
    a. Wait a few seconds before trying the operation again.
    b. If the operation succeeds after giving it sufficient time, check the following:
        - Network conditions
        - Client hardware requirements
        - Internet access

       If there is no Internet access, you may experience slow startup due to signature checks and CRL verification; in this case you can try one of the following:
        - Disable the signature checks. See section *19.4.11*, *Signature validation*.
        - Increase the timeout. See section *19.4.13*, *Configuring the timeout for launching external applications*.

   If this does not resolve the problem, continue with the troubleshooting.

3. Check if MyID Desktop or the Self-Service App are already running, and can be started:
   a. Close all open MyID Desktop or Self-Service App windows.
   b. Open the Windows Task Manager, then on the **Details** tab verify that no `MyIDDesktop` or `MyIDApp` processes are running.



Name	PID	Status	User name	CPU	Memory (a...	UAC virtualizat...
MyIDApp.exe	17236	Running	John.Fulton	00	69,116 K	Disabled
MyIDClientService.exe	2960	Running	John.Fulton	00	83,772 K	Disabled
MyIDDesktop.exe	15324	Running	John.Fulton	00	108,140 K	Disabled
MyIDWindowsIntegr...	6012	Running	SYSTEM	00	644 K	Not allowed
NVDisplay.Container...	3768	Running	SYSTEM	00	1,684 K	Not allowed
NVDisplay.Container...	4220	Running	SYSTEM	00	3,800 K	Not allowed
OfficeClickToRun.exe	2588	Running	SYSTEM	00	5,708 K	Not allowed
OneDrive.exe	11984	Running	John.Fulton	00	8,776 K	Disabled

   If there are processes running, use the Task Manager to close them; select the process and click **End Task**.
   c. Keeping the Task Manager open, try the operation again in the MyID Operator Client.
   d. If you do not see the `MyIDDesktop` or `MyIDApp` process appear in the Task Manager before the OC10009 error, this means that the application cannot start.

   Try launching MyID Desktop or the Self-Service App from the Windows Start menu; if this does not work, there is a problem with your installation of the application. Uninstall and then re-install your clients, then try again.

   If the issue persists after a reinstall, check any .NET errors relating to `MyIDDesktop` or `MyIDApp` in the Windows Event Viewer under **Windows Logs > Application**.

   Make sure you have the correct version of the .NET Core Desktop Runtime; see the *Prerequisites* section in the ***Installation and Configuration Guide***.
   e. If you do see the `MyIDDesktop` or `MyIDApp` process appear in the Task Manager before the OC10009 error, try the operation again.
4. If you are still unable to launch MyID Desktop or the Self-Service App from the MyID Operator Client:
   a. Set up logging for the appropriate applications.

   See the *Windows clients* section in the ***Configuring Logging*** guide.
   b. Try the operation again to ensure that the relevant information is included in these logs.
   c. Send the logs to Intercede Customer Support quoting reference SUP-364.

19.6.2 Mismatched client software versions

From time to time, MyID uses a new code signing certificate. The MyID Client Service validates the signatures of external applications (for example, MyID Desktop and the Self-Service App) and as a result will refuse to load the applications in the event of a mismatch of versions; you are recommended to upgrade all of your client software to the versions provided in the same release.

You can identify this issue in the MyID Client Service logs; an error similar to the following:

```
Client signature is not trusted
```

indicates that the MyID Client Service did not recognize the certificate used by the client software.

This situation also occurs when managing VSCs. If you are using the client applications provided with this release of MyID, you must also upgrade your Windows Integration Service (WSVC) software to the matching version provided.

19.6.3 Server name does not resolve

If, when you log on to the MyID Operator Client, the logon pop-up completes in a manner normal to a successful logon, but the MyID Operator Client does not log in, the rest.core web service is not working successfully.

The possible causes are:

- Issues with load balancing.
- The rest.core web service cannot resolve the server name URL.

To troubleshoot this issue, first ensure that you are load balancing correctly. For more information on load balancing, see section *19.4.6*, *Load balancing*.

If you are correctly load balancing, it is likely that the rest.core web service cannot connect to the following URL:

```
https://<servername>/web.oauth2/.well-known/openid-configuration
```

Where `<servername>` is the name of your server.

To check, set the logging for rest.core to `ALL`. Fore more information on logging for rest.core, see the *MyID REST and authentication web services* section of the ***Configuring Logging*** guide.

If the issue is that rest.core cannot resolve the URL, you will likely see the following error message.

```
Bearer was not authenticated. Failure message: IDX10204: Unable to validate
issuer. validationParameters.ValidIssuer is null or whitespace AND
validationParameters.ValidIssuers is null or empty.
```

You can narrow down the causes of the issue by carrying out the following procedure:

1. Log in to the web server with the MyID web service user account.

   This is the user account under which the rest.core service runs.
2. Run *one* of the following commands:

  - In PowerShell, run:

    ```
    Invoke-WebRequest https://<servername>/web.oauth2/.well-
    known/openid-configuration
    ```

  - At the Windows command prompt, run:

    ```
    curl https://<servername>/web.oauth2/.well-known/openid-
    configuration
    ```

  Where `<servername>` is the name of your server.

If you do not receive valid JSON as a response to your command, the issue is that the web service user on the web server cannot resolve the server URL. Possible causes include:

- A firewall is preventing the https call from being made.

  Check both the Windows Firewall and any external firewalls. If they are preventing the https call from being made, adjust the firewall rules.

- The server host name is not resolvable.

  You can check this by pinging the web server from the web service user account.

  At the Windows command prompt, run:

  ```
  ping <servername>
  ```

  Where `<servername>` is the name of your server.

  If this does not resolve to the expected IP address, the DNS lookup is not working. If necessary, you can use the `hosts` file on the web server to ensure that the web server's address resolves to its own IP address.

- The web server is not available on the server. To check if this is the issue, and why this is the issue, run *one* of the following commands:

  - In PowerShell, run:

    ```
    Invoke-WebRequest https://<servername>
    ```

  - At the Windows command prompt, run:

    ```
    curl https://<servername>
    ```

  Where `<servername>` is the name of your server.

  If the https URL cannot be reached, there is no connectivity to IIS over https.

  Then, run one of the following commands:

  - In PowerShell, run:

    ```
    Invoke-WebRequest http://<servername>
    ```

  - At the Windows command prompt, run:

    ```
    curl http://<servername>
    ```

  Where `<servername>` is the name of your server.

  If you can reach the http URL, but cannot reach the https URL cannot, there is probably an issue with TLS.

- The web server TLS certificate is invalid or not trusted.

  You can check if this is the issue by opening an Edge browser and entering the following URL:

`https://<servername>/web.oauth2/.well-known/openid-configuration`

Where `<servername>` is the name of your server.

If there are TLS issues, the Edge browser can help you identify the issue. Some possible issues are:

  - The root CA is not trusted.

    The root CA must be in the Trusted Root Certificate Authority certificate store when viewed on the web server by the web service user account.

  - Intermediate CAs are not known.

    If the intermediate CAs are not known, the **Certificate Hierarchy** may look incomplete. The **Certificate Hierarchy** is available on the **Details** page of the Certificate Viewer in the Edge browser.

    The intermediate CAs either must be resolvable from the URLs in the AIA extension, or must already be in the Intermediate Certificate Authority certificate store when viewed on the web server by the web service user account.

  - The origin in the TLS certificate does not match the origin in the URL of the https request.

    The origin in the TLS certificate is stored as the DNSName.

  - Your https inspection proxy is switching the TLS certificates in a way that means that the TLS certificates received when resolving the URL might not be the TLS certificates that you configured.

    If you have an https inspection proxy and it is causing this issue, you must take additional action to ensure these https proxy certificates are trusted and correct.

  - The configuration of your TLS protocols and ciphers do not allow the https requests from your web server to negotiate an allowed TLS protocol and cipher with the IIS web server.

- The IIS bindings for the website are preventing some network adapters from reaching IIS.

  To check if this is the issue, attempt to resolve the server name URL with user accounts on the same machine, and other machines. If some accounts and machines are able to resolve the URL but others cannot, this the cause of the issue is likely to be the IIS site bindings of the website.

  To see the site bindings:

  1. In IIS, click the **Default Web Site**.
  2. Under **Actions**, click **Bindings**.
  3. Review the **IP Address** settings of the `https` bindings.

  In mixed IPv4 and IPv6 environments, if an IPv4 address is selected, but IPv6 is used for the connection, or if an IPv6 address is selected, but IPv4 is used for the connection, this can prevent https calls from succeeding.

  Issues with IIS bindings may prevent users from reaching rest.core. If this occurs, the MyID Operator Client displays the error OC10003.

  To prevent IP address issues with IIS bindings, edit the binding of type `https` to set the **IP Address** to `All Unassigned`.

If you do get valid JSON as a response, the web service user on the web server can resolve the server URL. Your issue is therefore probably within your rest.core configuration. A possible cause is:

- The rest.core call is using http.

  OAuth2 requires https, so the rest.core and web.oauth2 web services are configured at installation to require https. In your rest.core configuration file, ensure that `MyID:Auth:AuthServerUrl` is set to an https address, not an http address. For information on the rest.core configuration file, see section *19.4.1*, *The rest.core web service configuration file*.