



MyID PIV
Version 12.9

Mobile Identity Documents

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

Copyright

© 2001-2023 Intercede Limited. All rights reserved.

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

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

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

Licenses and Trademarks

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

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

Apache log4net

Copyright 2004-2021 The Apache Software Foundation

This product includes software developed at

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

Bouncy Castle

Copyright © 2000 – 2011 The Legion Of The Bouncy Castle (<http://www.bouncycastle.org>)

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN

ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

KSoap2

Copyright © 2003,2004 Stefan Haustein, Oberhausen, Rhld., Germany

Copyright © 2006, James Seigel, Calgary, AB., Canada

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

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

Mobile Identity Documents	1
Copyright	2
Conventions used in this document	4
Contents	5
1 Introduction	7
2 Overview	8
2.1 The mobile identity document enrollment process	9
2.2 The mobile identity document verification process	10
2.3 Supported devices	10
2.4 Prerequisites	11
2.4.1 SMS gateway	11
2.4.2 REST API for provisioning mobile identity documents	11
3 Configuring the system	12
3.1 Setting the signing certificate	13
3.1.1 Required certificate properties	13
3.1.2 Adding the certificate to the registry	14
3.2 Setting the configuration options	15
3.2.1 Web service location	15
3.2.2 Setting the authentication code complexity	16
3.2.3 Biometric authentication	16
3.2.4 Configuring the image location	17
3.2.5 Maximum session count	18
3.3 Granting access to the workflows	19
3.3.1 Roles	19
3.3.2 Scope	19
3.4 Configuring SMS and email notifications	20
3.4.1 Configuring SMS and email notifications for the MyID Operator Client	21
3.4.2 Configuring SMS and email notifications for MyID Desktop	22
3.4.3 Configuring the SMS gateway for MyID Desktop	23
3.5 Creating the mobile identity document credential profile	24
3.5.1 Controlling the provisioning of multiple mobile identity documents	27
4 Requesting mobile identity documents	28
4.1 Requesting a mobile identity document for another user	28
4.1.1 Requesting a mobile identity document in MyID Desktop	29
4.2 Requesting a mobile identity document for your own mobile device	30
5 Working with mobile identity documents	32
5.1 Enabling and disabling mobile identity documents	32
5.1.1 Disabling a mobile identity document	32
5.1.2 Enabling a mobile identity document	33
5.2 Updating mobile identity documents	34
5.2.1 Requesting an update for a single mobile identity document	34
5.2.2 Requesting an update for multiple mobile identity documents	35
5.3 Canceling mobile identity documents	38

- 5.3.1 Canceling a mobile identity document38
- 5.3.2 Requesting a cancellation for a mobile identity document 39
- 5.3.3 Canceling multiple mobile identity documents41
- 5.4 Reporting on mobile identity documents 44

1 Introduction

This document provides information on the support for MyID[®] Mobile Identity Documents and the MyID Wallet app, including details on the following:

- Configuring the system to support the provisioning of mobile identity documents to the wallet app on your mobile devices.
- Requesting mobile identity documents through MyID.
- Managing mobile identity documents through MyID.

This release provides support for a range of Android and iOS mobile devices.

For information on using the mobile identity documents on your mobile device, see the information accompanying the app.

Note: There is a significant overlap in the configuration and use of mobile identities and mobile identity documents. For information on mobile identities, see the [Mobile Identity Management](#) guide.

2 Overview

MyID's mobile identity documents feature allows you to request a mobile identity document and associated graphical badge layouts, and provision them to the wallet app on your mobile device.

You can include user photographs, organization logos, text information from the person's user account in MyID, and barcodes (both 1D and PDF417 2D) on these graphical badge layouts.

In contrast to a mobile identity, a mobile identity document provides information *about* a person, rather than a credential that proves *who* a person is.

You can use mobile identity documents for a variety of purposes. For example:

- Driver's license.
- Age verification.
- Proof of entitlement (for example, loyalty cards).
- Proof of qualification (for example, accreditations, education).
- Proof of access rights (military bases, sites and so on).
- Proof of authority (warrant cards and so on).

MyID provides a standards-based mobile identity document feature, complying with ISO/IEC 18013-5. Mobile identity documents issued by MyID are verifiable, cryptographically secure, and incorporate privacy by design.

Intercede provides a sample document format, which works with the MyID Wallet app, but your organization may want to create its own document formats, and its own wallet app using the MyID Identity Agent Framework API; this allows you to include custom attributes in your mobile identity documents. For more information on this process, contact Intercede customer support quoting reference SUP-381.

2.1 The mobile identity document enrollment process

The process for enrolling a person and issuing them a mobile identity document is:

1. Create the person's account in MyID.

This account represents the document holder.

2. Carry out your organization's enrollment process.

This process incorporates confirming the person's identity and capturing information, both to support enrollment and to include in the mobile identity document.

3. The person installs the wallet app on their mobile device.

Intercede provides the MyID Wallet app, but your organization may want to create its own wallet app using the MyID Identity Agent Framework API; this allows you to include custom attributes in your mobile identity documents.

4. Using MyID, a MyID operator requests (and optionally approves) a mobile identity document for the person.

The operator can use the MyID Operator Client or MyID Desktop. Alternatively, you can use the MyID Core API or the Credential Web Service API to make the request.

5. MyID uses email or an SMS gateway to send a message to the person's email address or phone number.

6. When the message is received on the person's mobile device, they click the link or notification.

The type of notification depends on their mobile device type and whether the message is sent through SMS or email. The person follows the instructions displayed on the mobile device.

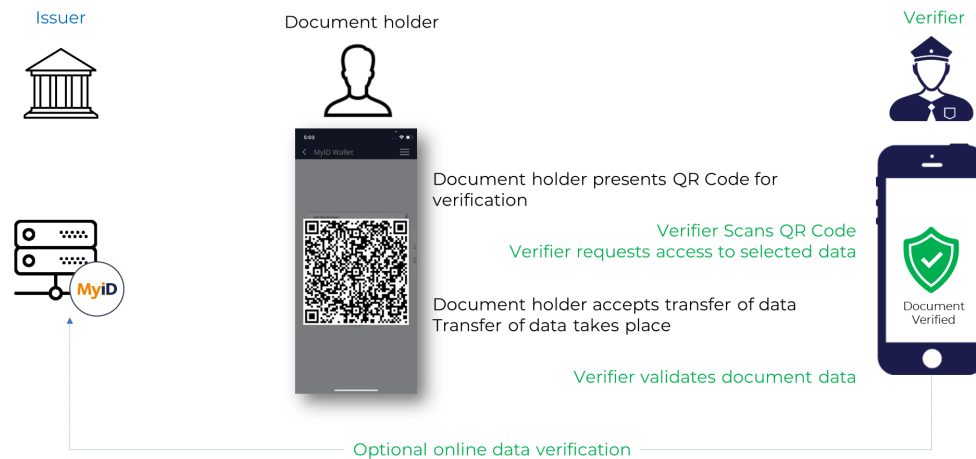
Alternatively, you can use the MyID Operator Client or MyID Desktop to request a mobile identity document for your own device. If you are using MyID Desktop to request your own mobile identity document, you can choose to display a QR code on screen that you can scan with the wallet app rather than use an email or SMS notification.

7. Use the wallet app to download the document and graphical badge layouts to the mobile device from the MyID server.

2.2 The mobile identity document verification process

Once a document holder has been issued a mobile identity document by the issuer (MyID), they can present the document to a verifier.

You can use any verifier app that supports ISO/IEC 18013-5 and Bluetooth Low Energy connections.



The process is:

1. The document holder opens their wallet app and selects the document they want to be verified.
The wallet app displays a QR code.
2. The verifier opens their verifier app and scans the QR code.
3. The verifier connects to the document holder's app using Bluetooth and requests access to specific data.
4. The document holder accepts the transfer of data.
5. The wallet app transfers the data to the verifier app using Bluetooth.
6. The verifier validates the document data.
The document data is cryptographically signed; the verifier can use this digital signature to validate the document.

Optionally, the verifier system can carry out an online data verification against the MyID system using the MyID Core API to ensure that the document is still considered valid and has not been disabled or canceled.

2.3 Supported devices

Devices running the following operating systems are supported:

- iOS.
- Android.

See the information provided with your wallet app for information on the specific versions supported. For more information about mobile operating system support, contact Intercede customer support quoting reference SUP-49.

2.4 Prerequisites

This section contains details of the prerequisites for provisioning mobile identity documents through MyID.

2.4.1 SMS gateway

You can configure the system to use any SMS gateway. To set up the system to communicate with your SMS gateway and allow MyID to send text messages to the users' mobile devices, you must have some knowledge of ASP and JavaScript.

Alternatively, you can use email for notifications.

See section [3.4, *Configuring SMS and email notifications*](#) for details.

2.4.2 REST API for provisioning mobile identity documents

MyID provides a REST API for provisioning mobile credentials and mobile identity documents (`rest.provision`). Make sure you select the **Provisioning API (rest.provision)** option on the Server Roles and Features screen in the MyID Installation Assistant when installing MyID.

3 Configuring the system

This chapter contains information on configuring your MyID system to allow you to request and provision mobile identity documents.

You must:

- Set up a certificate that is used to sign the mobile identity documents.
This verifies that the mobile identity document was issued by your MyID system.
See section [3.1, *Setting the signing certificate*](#).
- Set the MyID configuration options.
These ensure that your system is configured to issue mobile identity documents.
See section [3.2, *Setting the configuration options*](#).
- Set up the SMS and email notifications.
MyID sends notifications to the person that there is a new mobile identity document, or an update to a mobile identity document, available; they can then use the wallet app to download the required data. You can configure MyID to send these notifications through email, as SMS messages, or a combination of both.
See section [3.4, *Configuring SMS and email notifications*](#).
- Create at least one credential profile for the mobile identity documents you want to issue.
The credential profile defines the content of the mobile identity documents.
See section [3.5, *Creating the mobile identity document credential profile*](#).

3.1 Setting the signing certificate

To provision mobile identity documents, you must set up a signing certificate on the MyID application server.

3.1.1 Required certificate properties

On your certificate authority, you must set up a certificate template with the following properties:

- Algorithm Name: `EDCSA_P256`
- Minimum Key Size: `256`
- Request Hash: `SHA256`
- Subject Name: `Supply in the request`
- Application Policies:
 - Remove all policies
 - Add a new policy with the name:
`id-md1-kpmdlDS`
and the object identifier:
`1.0.18013.5.1.2`
Note: This extension must be marked as critical.
- Key Usage: Only select `Digital Signature`
Note: This extension must also be marked as critical.

3.1.2 Adding the certificate to the registry

To configure the signing certificate in the registry:

1. On the MyID application server, log in using the MyID COM+ account.
2. Request a certificate using the previously-created signing certificate template that will be placed in the CAPI store.

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

3. Once the certificate has been generated, install and save it as a `.cer` file in Base64/PEM format.

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

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

4. Enter the filename of the certificate in the system registry:

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

- a. Run the Windows `regedit` utility.
- b. Navigate to:

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

- c. If not already present, create the following key:

- ContentSigningCOSE

- d. Create or set the following string value to the full path of the related certificate:

- ISO18013MsoSignerCertificate

3.2 Setting the configuration options

This section contains information about setting the MyID configuration options to enable you to provision mobile identity documents.

3.2.1 Web service location

Within MyID, you must set the location of the MyID web service that allows a mobile device to collect a mobile identity document.

To set the location of the web service:

1. From the **Configuration** category, select the **Operation Settings** workflow.
2. Click the **Certificates** tab.
3. Set the **Mobile Certificate Recovery Service URL** option to the location of the MyID Process Driver web service host.

Note: This option is used for more operations than just certificate recovery, despite the name.

For example, set the option to:

```
https://myserver
```

Replace `myserver` with the name of the server on which the web service is installed.

You are recommended to use SSL on this connection. Make sure you specify the correct protocol: `http` or `https`.

Note: The users' mobile devices must be able to access this URL. To be able to access the other MyID web services, all MyID web services must be installed on the same server.

4. If you have installed MyID in a distributed network where the web server is in a separate domain, you may have to supply a separate URL for your MyID client workstations to retrieve a QR code for mobile provisioning. In this case, set the **Web Server External Address** option to the URL of the MyID web services server that hosts the ProcessDriver web service. Make sure this URL is accessible to your MyID clients.

In the majority of network configurations, you can leave this option blank.

5. Click **Save changes**.

3.2.2 Setting the authentication code complexity

To set up the single-use authentication code that is used to secure mobile identity documents sent to the mobile device, you must use the **Certificate Recovery Password Complexity** configuration option to require numeric characters only.

To set the password complexity:

1. From the **Configuration** category, select the **Operation Settings** workflow.
2. Click the **Certificates** tab.
3. Set the **Certificate Recovery Password Complexity** option.

The format is `xx-yyN`, which is made up of:

- `xx` = minimum length.
- `yy` = maximum length.

The default is `04-08N` which means a code of 4 to 8 numbers.

4. Click **Save changes**.

3.2.3 Biometric authentication

MyID PIV systems support biometric authentication when updating and unlocking credentials. These features are not supported for mobile devices, therefore, on PIV systems, you must disable them before you can issue mobile identities successfully.

To set the biometric authentication options:

1. From the **Configuration** category, select the **Operation Settings** workflow.
2. Click the **Biometrics** tab.
3. Set the following options:

- Set the **Verify fingerprints during card update** option in the **Operation Settings** workflow set to `No`.

If this option is set to `Yes`, provisioning a mobile identity will fail with an error similar to:

```
Your mobile device is not compatible with biometric authentication
```

- Set the **Verify fingerprints during card unlock** option in the **Operation Settings** workflow set to `No`.

If this option is set to `Yes`, unlocking a mobile identity will fail with an error similar to:

```
Your mobile device is not compatible with biometric authentication
```

4. Click **Save changes**.

Note: When you set these options to `No`, you are removing the requirement to use biometrics when unlocking or updating smart cards as well as mobile identities.

3.2.4 Configuring the image location

To allow MyID to send badge images to the mobile device, you must make sure that the **Image Upload Server** configuration option (on the **Video** page of the **Operation Settings** workflow) is set to a value that can be resolved (to the name or IP address of the MyID web server) from the MyID Web Services server. For more information, see the *Configuring the image location* section in the [Administration Guide](#).

3.2.5 Maximum session count

If too many clients (whether mobile clients, or other clients such as MyID Desktop, the Self-Service App, or the Self-Service Kiosk) access the server at the same time for issuance or update processes, you may experience performance issues, and end users may experience errors.

If too many clients overload the server infrastructure, the errors may be generated from various points in the system (for example, from the database or the web server) and there may be a wide variety in the messages displayed; some error messages may be generic errors, with the details visible only in the MyID server logs.

If a user sees an "unexpected" error on the mobile device:

1. Review the MyID server logs for the time period involved. Check for timeout issues.
2. Review your infrastructure for high resource usage; for example, CPU, RAM, and so on.
3. Consider restricting the number of mobile sessions using the **Maximum session count** configuration option.

To set the maximum number of mobile sessions allowed.

1. From the **Configuration** category, select the **Operation Settings** workflow.
2. Click the **Identity Agent Policy** tab.
3. Set the following option:

- **Maximum session count**

This determines the number of concurrent sessions (whether from mobile clients or other clients such as MyID Desktop, the Self-Service App, or the Self-Service Kiosk) that are allowed by the server while still allowing mobile issuance and update operations.

Values:

0 – Do not allow mobile issuances or updates.

-1 – No limits.

Any other number determines the number of client sessions allowed. If this number is exceeded, the server returns HTTP 503 – service unavailable – to all mobile clients. This will also be recorded in the local event log.

Only mobile clients are prevented from connecting.

You are recommended to tailor this value to your hardware: too high a value, and your server may experience performance issues; too low and your server will be under-used.

As server deployments differ in computing capability, functionality usage, and data load, it is impossible to recommend precise values. You are recommended to try various values on a test system that mirrors the resources and data load of your production system.

4. Click **Save changes**.

3.3 Granting access to the workflows

The system makes use of the following workflows:

- **Cancel Credential** – used within MyID to cancel a mobile identity document.
- **Enable / Disable ID** – used within MyID to enable or disable a mobile identity document.
- **Request ID** – used within MyID for operator-guided requests for mobile identity documents to be installed on a mobile device.
- **Request My ID** – used within MyID for self-service requests for mobile identity documents to be installed on a mobile device.
- **Collect My Updates** – used by the wallet app to obtain a mobile identity document.
- **Issue Device** – used by the wallet app to obtain a mobile identity document.

Note: The **Collect My Updates** and **Issue Device** workflows are not used within MyID; they are used to control access from a mobile device to the features of the web service.

Use the **Edit Roles** workflow to grant access for these workflows to the roles you want to be able to access them.

3.3.1 Roles

You must add the **Collect My Updates** workflow to the Server Credentials role if the user does not already have access to this workflow through one of their other roles.

Note: You can use the Server Credentials role to control access to the collection service; allocate this role to the users who you want to be able to collect mobile IDs.

Alternatively, you can add the **Collect My Updates** workflows to an existing role to allow users in that role to collect mobile IDs.

3.3.2 Scope

When a mobile device user, for example a guard, requests the details for another mobile device user, the guard must have the correct scope within MyID to view the details of the other user; for example, the user must be in the same group as the guard if the guard has Department scope.

3.4 Configuring SMS and email notifications

You can choose whether to allow SMS, email, or both types of notification when sending provisioning messages to mobile devices.

MyID sends two notifications:

- A link to the collection URL.
MyID sends this notification as an email.
- An authentication code.

MyID sends this one time password either as a separate email, or as an SMS.

Note: The complexity of the authentication codes is determined by the **Certificate Recovery Password Complexity** configuration option (on the **Certificates** page of the **Operation Settings** workflow). See section [3.2.2, *Setting the authentication code complexity*](#) for details.

The two components of the notification (the collection URL and the authentication code) are sent separately for security, and you are recommended to configure MyID to send the collection URL as an email and the authentication code as a SMS for additional security.

3.4.1 Configuring SMS and email notifications for the MyID Operator Client

You control the way MyID sends notifications for the issuance of mobile identities through the MyID Operator Client by setting the notification scheme in the credential profile; see section [3.5, *Creating the mobile identity document credential profile*](#).

You must enable the notification methods using configuration options.

To enable SMS and email notifications:

1. From the **Configuration** category, select the **Operation Settings** workflow.
2. On the **General** tab, set the following options:
 - **SMS email notifications** – set to `Yes` to allow authentication codes to be sent through SMS.

If you do *not* set this option to `Yes`, you must configure the credential profile to send the authentication code as an email, or display the authentication code on screen when you request the mobile device.
 - **SMS gateway URL for notifications** – set to the URL of your SMS gateway.

By default, SMS messages are sent to through an email to SMS gateway, in the format `<cellnumber>@<gateway>`, where:
 - `<cellnumber>` – the cell phone number from the person's record.
 - `<gateway>` – the URL from the **SMS gateway URL for notifications** option.

For example: `00447700900123@msggateway.com`
If this is not suitable, you can customize the `sp_CustomPrepareSMS` stored procedure in the MyID database.
3. On the **Notifications** tab, set the following option:
 - **Send Email Notifications** – set to `Yes` to allow notifications to be sent through email.

You must configure an SMTP server in the **External Systems** workflow; see the [Setting up email](#) section in the [Advanced Configuration Guide](#).
4. Click **Save changes**.

3.4.2 Configuring SMS and email notifications for MyID Desktop

You control the way MyID sends notifications for the issuance of mobile identity documents through MyID Desktop by setting configuration options.

To allow provisioning messages:

1. From the **Configuration** category, select the **Operation Settings** workflow.
2. On the **Devices** tab, set the following options:
 - **Mobile Provision Via Email** – set this option to allow the notifications of mobile identity documents to be sent to the user's email address.
 - **Mobile Provision Via SMS** – set this option to allow the notifications of mobile identity documents to be sent to the user's mobile phone number.

Note: You can select one or both of these options. If you select both options, you can select which method to use when you request the mobile identity document.
3. On the **Notifications** tab, set the following options:
 - **Send Mobile OTP via SMS** – set this option to allow the operator to send the OTP authentication code directly to the mobile device.
 - **Note:** If you set **Send Mobile OTP via SMS** to **Yes**, whilst the OTP is sent as an SMS, for security reasons the notification message must be sent using email and *not* SMS. If you have set this option, make sure you also set the **Mobile Provision Via Email** option on the **Devices** tab.
 - **Mail Format** – make sure this option is set to **HTML**.
4. Click **Save changes**.

3.4.3 Configuring the SMS gateway for MyID Desktop

You can configure the system to use any SMS gateway. You must customize the following file:

```
customSMS.asp
```

Versions of this file are installed to the MyID web server in the following locations:

- Web\`<edition>`\untranslated\res\custom\js\`</code>`
- Web\`<edition>`\en\res\custom\js\`</code>`
- Web\`<edition>`\us\res\custom\js\`</code>`

Where `<edition>` is `WebPIV` for PIV, and `WebENT` for non-PIV editions of MyID.

You must make the same changes in each version of the file. If you have created any custom translations of the MyID website, you must also make the same change in the custom versions.

The sample file installed with the system is set up to use the SMS gateway provided by `www.2sms.com` – if you are using this service, edit the `username` line to include your 2sms account, and the `password` line to include your 2sms password.

If you are using any other system, you must customize the ASP file to conform to the calling requirements of your own SMS gateway.

This ASP file implements the following function:

```
customSendSMS(message, mobileNumber, userRS)
```

where:

- `message` – the body of the SMS text message to be sent to the mobile device.
- `mobileNumber` – the cell/mobile phone number from the user's MyID record.
- `userRS` – reserved for future use.

The function returns the response from the SMS gateway.

You can implement your system in any way. You are required only to send the body contained in `message` to the phone number in `mobileNumber`, and `return` the response from the gateway.

Note: You must keep a backup of this file once you have customized it.

3.5 Creating the mobile identity document credential profile

You must create a credential profile that contains the details of the mobile identity documents you want to provision to the wallet app.

To set up a mobile identity document credential profile:

1. From the **Configuration** category, select **Credential Profiles**.
You can also launch this workflow from the **Credential Configuration** section of the **More** category in the MyID Operator Client. See the *Using Credential Configuration workflows* section in the *MyID Operator Client* guide for details.
2. Click **New**.
3. Type a **Name** and optional **Description** for the credential profile.
4. In **Card Encoding**, select **Mobile Identity Document**.

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

5. Click the **Issuance Settings** section.
The issuance settings you can use for mobile identity documents is restricted. You can use the following:
 - **Validate Issuance**
 - **Validate Cancellation**
 - **Lifetime**
 - **Credential Group**
 - **Exclusive Group**
 - **Block Multiple Requests for Credential Group**
 - **Cancel Previously Issued Device**
 - **Enforce Photo at Issuance**

- **Notification Scheme** – select one of the following:
 - **Default** – MyID sends the collection URL as an email, the authentication code as a separate email, and the authentication code as an SMS.
 - **None** – MyID does not send any notifications. You must use the **Request Mobile (View Auth Code)** option in the MyID Operator Client to display the collection URL and authentication code on screen.
 - **Mobile Only – Auth Code Via Email** – MyID sends the collection URL as an email, and the authentication code as a separate email.
 - **Mobile Only – Auth Code Via SMS** – MyID sends the collection URL as an email, and the authentication code as an SMS.

Note: Notification schemes are relevant only for mobile devices requested through the MyID Operator Client or the MyID Core API. They do not affect the notifications sent when you request mobile devices through MyID Desktop or the Credential Web Service API.

See section [3.4.1, Configuring SMS and email notifications for the MyID Operator Client](#).

The complexity of the authentication codes is determined by the **Certificate Recovery Password Complexity** configuration option (on the **Certificates** page of the **Operation Settings** workflow). See section [3.2.2, Setting the authentication code complexity](#) for details.

- **Require user data to be approved**
- **Generate Code on Request**

See the *Issuance Settings* section of the [Administration Guide](#) for details of these options.

Note: The **Mail Documents** section is available in the credential profile, but is not currently supported for mobile identity documents.

6. Click the **Device Profiles** section.

You must select a **Document Format** that defines the content of the mobile identity document.

Device Profiles

Document Format

Document Format:

Device Profile

eGate (Axalto):

Selected Data Profile:

This release provides the following document format file:

- `Partial-ISO-18013-5.xml` – a partial implementation of the ISO-18013-5 standard, and allows you to use a third-party verifier app to carry out verification on a mobile identity document provisioned to the MyID Wallet app.

For information on customizing the document format or adding your own document format, contact Intercede customer support quoting reference SUP-381.

7. Click the **Requisite User Data** section.

This section contains a list of user attributes that must be present for this credential profile to be issued.

See the *Requisite User Data* section of the [Administration Guide](#) for details.

8. Click **Next**.

9. On the Select Roles screen, select the roles you want to be able to issue and receive mobile identity documents using this credential profile.

- The **Can Receive** option determines which roles can receive mobile identity documents issued using this credential profile.
- The **Can Request** option determines which roles can request mobile identity documents using this credential profile; for example, using **Request ID** for operator requests or **Request My ID** for self-service requests.
- The **Can Validate** option determines which roles can validate requests for mobile identity documents using this credential profile using the **Validate Request** workflow.
- The **Can Collect** option determines which roles can collect mobile identity documents using this credential profile; any user who is to receive a mobile identity document must have both the **Can Receive** and the **Can Collect** options.

Note: Not all options may be available, depending on your system configuration. See the *Working with credential profiles* section in the [Administration Guide](#) for details.

Note: Any role you want to receive mobile identity documents must have the **Issue Device** option selected in the **Cards** category within the **Edit Roles** workflow.

10. Click **Next**.

11. Select the card layouts you want to make available to the mobile device.

Badges based on these layouts will be transferred to the mobile device as part of the mobile identity document. When you select a card layout, its associated reverse layout (the `_back` layout, if preset) will also be available on the mobile device.

Note: If you include card layouts, there must be a default layout; also, you must ensure that there is no more than one associated reverse layout. Otherwise, an error similar to the following occurs:

```
PS81: "Layout selection invalid. Either no default front layout, or multiple back layouts present"
```

You can include user photographs, organization logos, text information from the person's user account in MyID, and barcodes (both 1D and 2D) on these card layouts. For information on using the **Card Layout Editor** to design layouts to use in your mobile identity documents, see the *Designing card layouts* section in the [Administration Guide](#) for details.

12. Click **Next**.

13. Type your **Comments** and click **Next** to complete the workflow.

3.5.1 Controlling the provisioning of multiple mobile identity documents

You can issue a mobile identity document to the same person more than once using the same credential profile. This means that the same document may appear multiple times on the person's device, or on more than one device belonging to the person.

If necessary, you can control the provisioning of multiple mobile identity documents by disabling or canceling the previously-issued document using the **Credential Group** and **Cancel Previously Issued Device** options in the credential profile. See the *Credential group* section in the [Administration Guide](#) for details.

You can also use the **Issue Over Existing Credential** option; if the credential profile being issued is the same as previously-issued mobile identity document, the previous document is canceled, and a new document is issued. This does not affect the previous document on the mobile device. See the *Issue over Existing Credential* section in the [Administration Guide](#) for details.

4 Requesting mobile identity documents

You can request a mobile identity document for your own mobile device or for another person's mobile device.

The user for whom the mobile identity document is requested must have the following:

- A cell/mobile phone number in their MyID record.
- An email address in their MyID record.

You can:

- As an operator, request a mobile identity document for another person.
See section [4.1, Requesting a mobile identity document for another user](#).
- Request a mobile identity document for yourself.
See section [4.2, Requesting a mobile identity document for your own mobile device](#).

4.1 Requesting a mobile identity document for another user

You can request a mobile identity document for a person in the following ways:

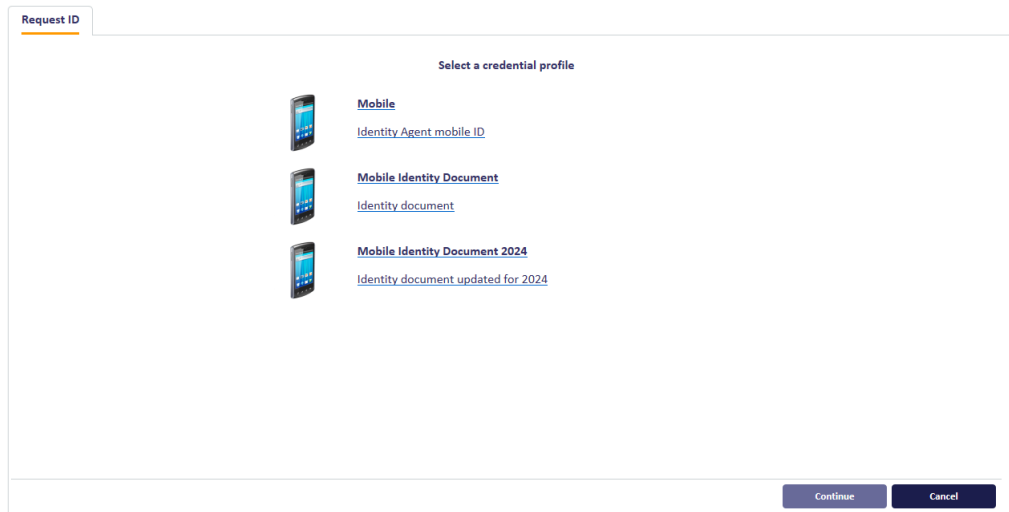
- Using the **Request Mobile** or **Request Mobile (View Auth Code)** options in the MyID Operator Client.
See the *Requesting a mobile device for a person* section in the [MyID Operator Client](#) guide.
- Using the MyID Core API.
This uses the same mechanism and requires the same configuration as the **Request Mobile** or **Request Mobile (View Auth Code)** options in the MyID Operator Client. See the *Accessing the API documentation* section in the [MyID Core API](#) guide for details of accessing the API documentation, which contains details of the relevant methods.
- Using the **Request ID** workflow in MyID Desktop.
See section [4.1.1, Requesting a mobile identity document in MyID Desktop](#).
- Using the Credential Web Service API.
This uses the same mechanism and requires the same configuration as the **Request ID** workflow in MyID Desktop. See the [Credential Web Service](#) guide.

4.1.1 Requesting a mobile identity document in MyID Desktop

Note: The **Request ID** workflow is not assigned to any roles by default. You must use the **Edit Roles** workflow to ensure that this workflow is assigned to the roles you want to be able to request mobile devices.

To request a mobile identity document for another user:

1. From the **Mobile Devices** category, select **Request ID**.
2. Use the Find Person screen to select the appropriate person.
3. Select the credential profile you want to use.



4. Click **Continue**.
5. Check that the phone number or email address is correct.

The phone number is taken from the **Cell** or **Mobile** (depending on the language setting) field in the user's MyID record.

6. If your system is not configured to send OTP authentication codes through SMS, take a note of the code on-screen.

If your system is configured to send OTP authentication codes through SMS, this code is sent directly to the mobile device.

This single-use code is required to install the mobile identity document on the mobile device. If you have set the credential profile to require validation, the password does not appear on this screen; instead, you must use the **Validate Request** workflow.

Note: The space in the password is optional when you enter the password on the mobile device.

7. Click **Send**.

If both SMS and Email options are available, choose one of the methods to send the notification.

MyID uses email or the SMS gateway to send a message. You can now collect the mobile identity document on your mobile device.

4.2 Requesting a mobile identity document for your own mobile device

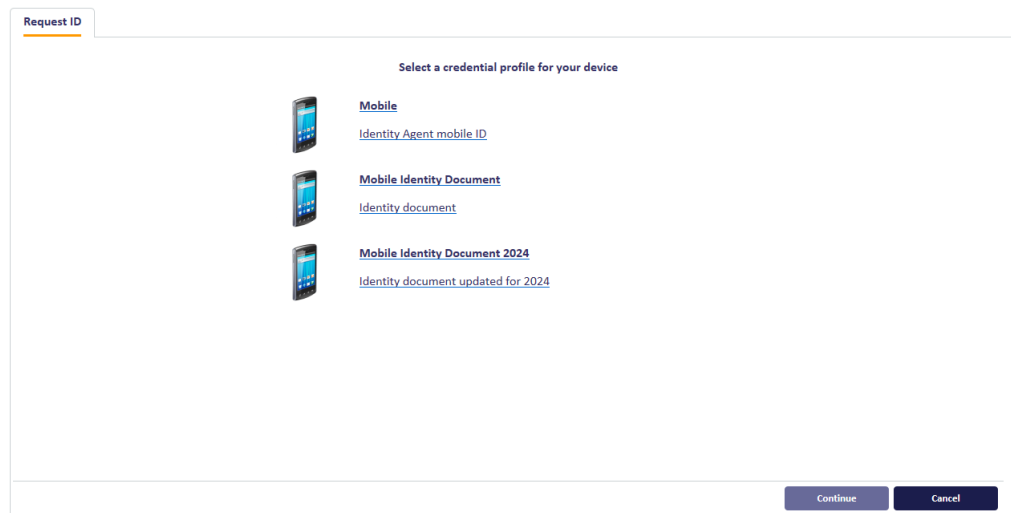
Note: The **Request My ID** workflow is not assigned to any roles by default. You must use the **Edit Roles** workflow to ensure that this workflow is assigned to the roles you want to be able to request mobile devices.

To request a mobile identity document for your own mobile device:

1. From the **Mobile Devices** category, select **Request My ID**.

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

2. Select the credential profile you want to use.



3. Click **Continue**.
4. Check that the phone number or email address is correct.

The phone number is taken from the **Cell** or **Mobile** (depending on the language setting) field in your MyID record.
5. If your system is not configured to send OTP authentication codes through SMS, take a note of the code on-screen.

If your system is configured to send OTP authentication codes through SMS, this code is sent directly to the mobile device.

This single-use code is required to install the mobile identity document on the mobile device. If you have set the credential profile to require validation, the password does not appear on this screen; instead, you must use the **Validate Request** workflow.

Note: The space in the password is optional when you enter the password on the mobile device.

6. Click **Send**.

If you do not have an email address or mobile number set up on your account, MyID displays a QR code. Open the wallet app on your phone and scan the QR code on screen, then click **Done**.

Note: If you have an email address or mobile number set up, but prefer to use a QR code, click the **QR Code** button at the bottom of the screen. This option is not available if the credential profile has the **Validate Issuance** option set.

5 Working with mobile identity documents

Once a person has been issued with a mobile identity document, you can use the MyID Operator Client to manage the mobile identity documents.

This chapter contains information on:

- Temporarily enabling and disabling mobile identity documents.
See section [5.1, *Enabling and disabling mobile identity documents*](#).
- Requesting updates for mobile identity documents.
See section [5.2, *Updating mobile identity documents*](#).
- Permanently canceling mobile identity documents.
See section [5.3, *Canceling mobile identity documents*](#).
- Viewing reports related to mobile identity documents.
See section [5.4, *Reporting on mobile identity documents*](#).

5.1 Enabling and disabling mobile identity documents

You can enable or disable a mobile identity document.

Note: This does not affect the mobile identity document on the wallet app itself, but it allows a third party to confirm the validity of a provisioned mobile identity document by checking it against the MyID database; for example, by producing a web service that checks the mobile identity document using the MyID Core API.

5.1.1 Disabling a mobile identity document

To disable a mobile identity document:

1. In the MyID Operator Client, search for the device you want to disable.

You can use the **Device** search report; you are recommended to add the **Device Category** from the **Additional search criteria** section, and select **Mobile Identity Document** from the drop-down list.

Alternatively, you can use the **Devices** tab on the View Person screen. On this screen, mobile identity documents appear with a **Device Type** of **Android Attribute Store** or **iOS Attribute Store**.

2. Select the mobile identity document you want to disable, and open it in the View Device screen.
3. Click **Disable Device**.

The Disable Device screen appears.

4. Select a **Reason** for disabling the mobile identity document.
5. Type any **Notes** you want to add.
6. Click **Save**.

The **Reason** and **Notes** are stored in the audit trail.

Note: Only the selected mobile identity document is affected. If the person has more than one mobile identity document stored in their wallet app, or has other mobile IDs stored on the same mobile device, these are not affected.

5.1.2 Enabling a mobile identity document

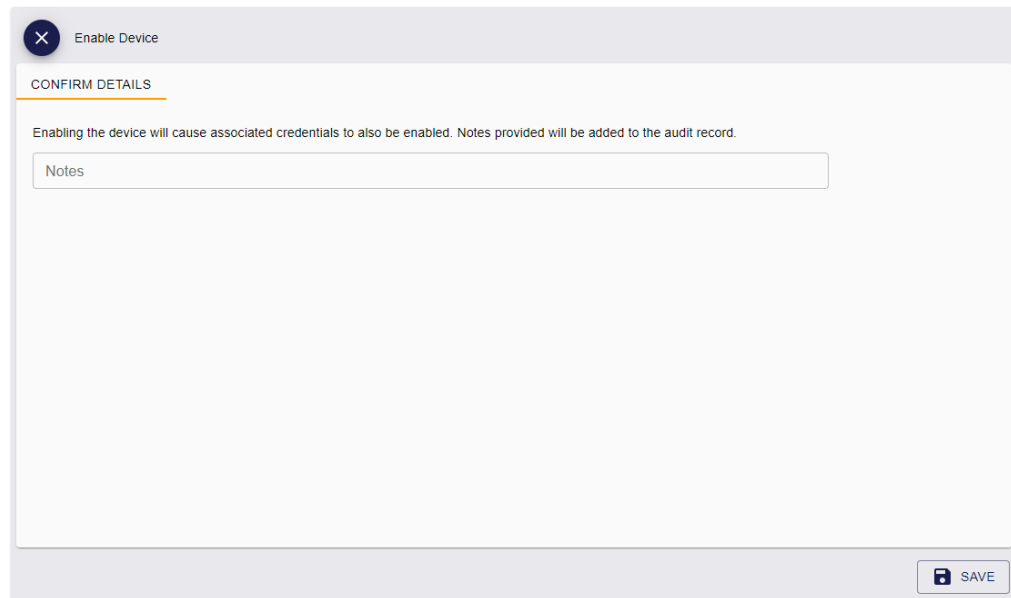
To enable a mobile identity document:

1. In the MyID Operator Client, search for the device you want to enable.

You can use the **Device** search report; you are recommended to add the **Device Category** from the **Additional search criteria** section, and select **Mobile Identity Document** from the drop-down list.

Alternatively, you can use the **Devices** tab on the View Person screen. On this screen, mobile identity documents appear with **Android Attribute Store** or **iOS Attribute Store** in the **Device Type** column. Disabled mobile identity documents appear with **No** in the **Enabled** column.

2. Select the mobile identity document you want to enable, and open it in the View Device screen.
 3. Click **Enable Device**.
- The Enable Device screen appears.



4. Type any **Notes** you want to add.

The **Notes** are stored in the audit trail.

5. Click **Save**.

MyID marks the mobile identity document as enabled in the database.

Note: Only the selected mobile identity document is affected. If the person has more than one mobile identity document stored in their wallet app, or has other mobile IDs stored on the same mobile device, these are not affected.

5.2 Updating mobile identity documents

You can request an update for an issued mobile identity document. Once you have requested an update, the person checks for updates on their wallet app, and an updated version of the mobile identity document is provisioned to their device; this uses the latest version of the credential profile, the latest version of the document format file, and pulls the latest information from the database to populate the document.

Note: You cannot update a mobile identity document that has been disabled or canceled.

5.2.1 Requesting an update for a single mobile identity document

To update a single mobile identity document:

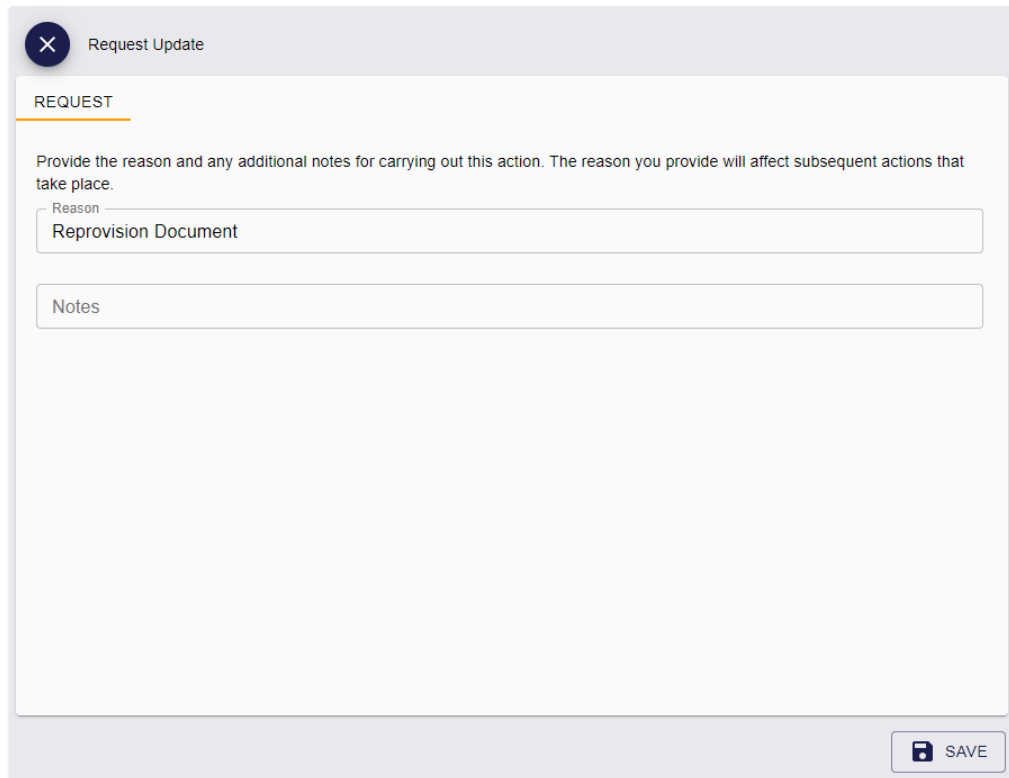
1. In the MyID Operator Client, search for the device you want to update.

You can use the **Device** search report; you are recommended to add the **Device Category** from the **Additional search criteria** section, and select **Mobile Identity Document** from the drop-down list.

Alternatively, you can use the **Devices** tab on the View Person screen. On this screen, mobile identity documents appear with a **Device Type** of **Android Attribute Store** or **iOS Attribute Store**.

2. Select the mobile identity document you want to update, and open it in the View Device screen.
3. Click **Request Update**.

The Request Update screen appears.



Note: You cannot change the credential profile when requesting an update.

4. Type any **Notes** you want to add.

The **Notes** are stored in the audit trail.

5. Click **Save**.

MyID requests an update for the mobile identity document, and sends an email notification to the person using the Reprovision Notification Document email template, telling them to open their Wallet app and check for updates.

5.2.2 Requesting an update for multiple mobile identity documents

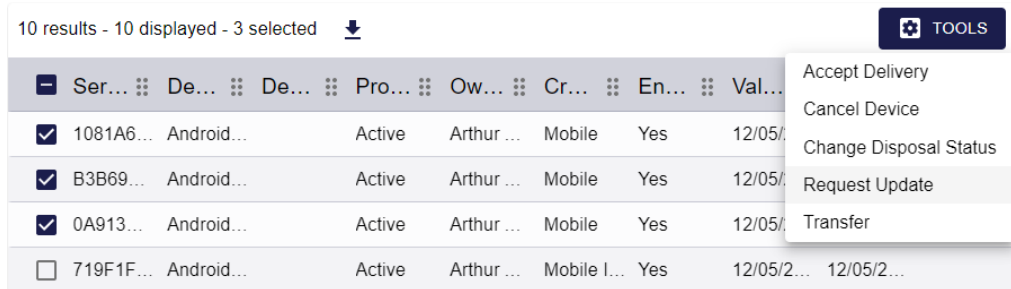
If you want to request updates for multiple mobile identity documents that were issued with the same credential profile, you can request the updates in a batch instead of requesting them one by one.

To request updates for multiple mobile identity documents:

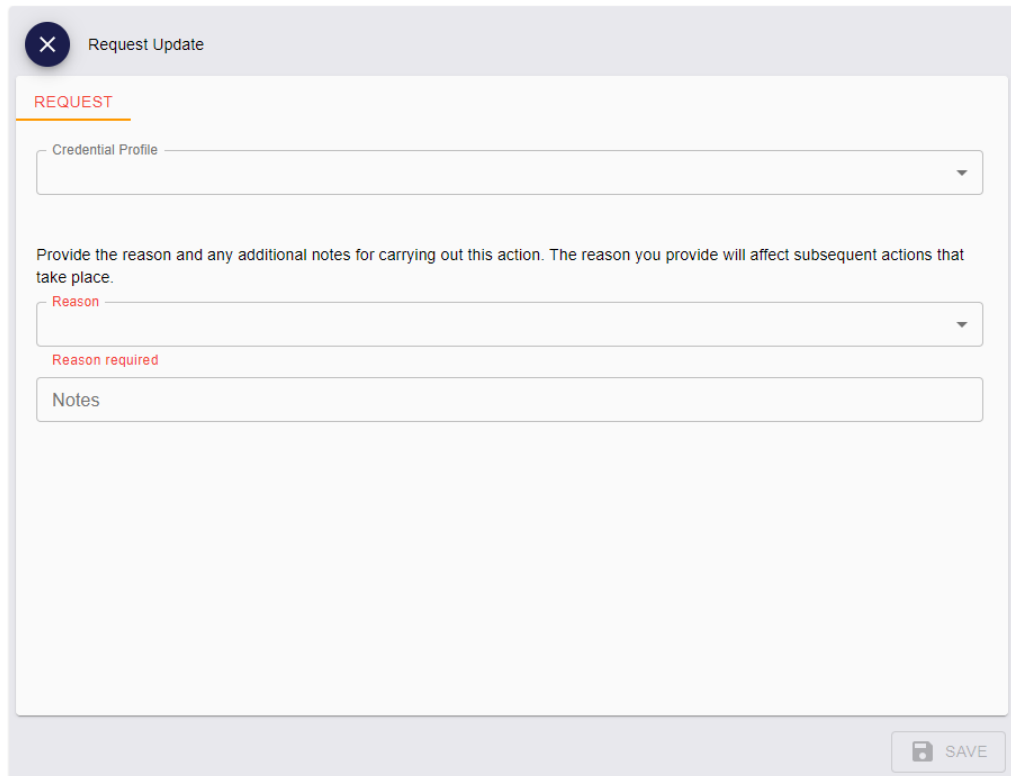
1. In the MyID Operator Client, search for the devices you want to update.
You can use the **Device** search report; you are recommended to add the **Device Category** from the **Additional search criteria** section, and select **Mobile Identity Document** from the drop-down list.
2. On the search results 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 5.2.1, *Requesting an update for a single mobile identity document* for details of requesting an update for a single device.

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



The Request Update screen appears.



Note: Because you can use the batch operation on multiple types of device at the same time, this screen does not restrict your options; you must set the required options manually:

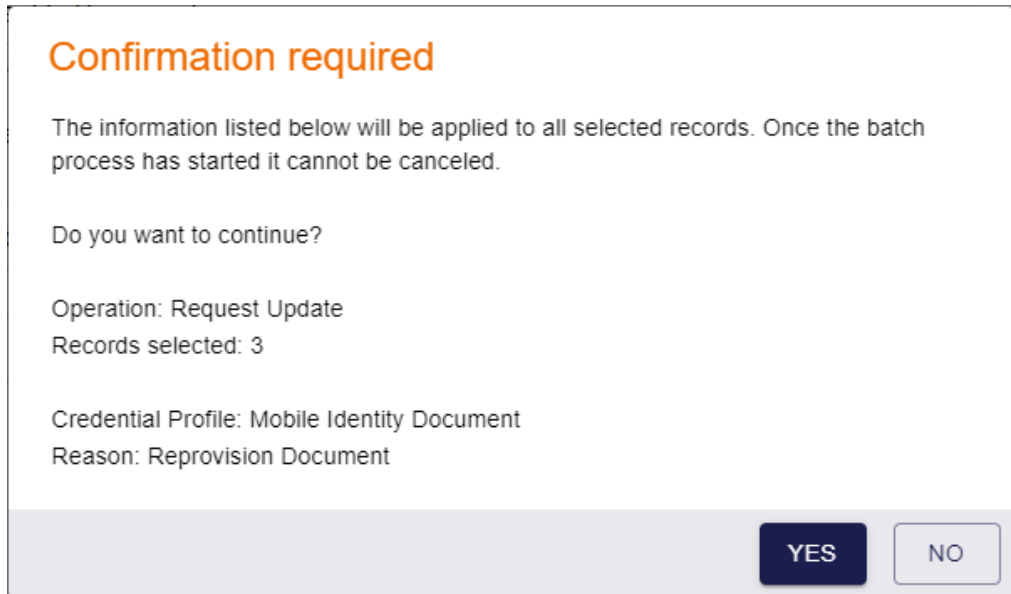
- **Credential Profile** – set to the same credential profile as you originally used to provision the mobile identity documents. You cannot request a batch update for mobile identity documents that were issued using different credential profiles.
- **Reason** – select **Reprovision Document**.

4. Type any **Notes** you want to add.

The **Notes** are stored in the audit trail.

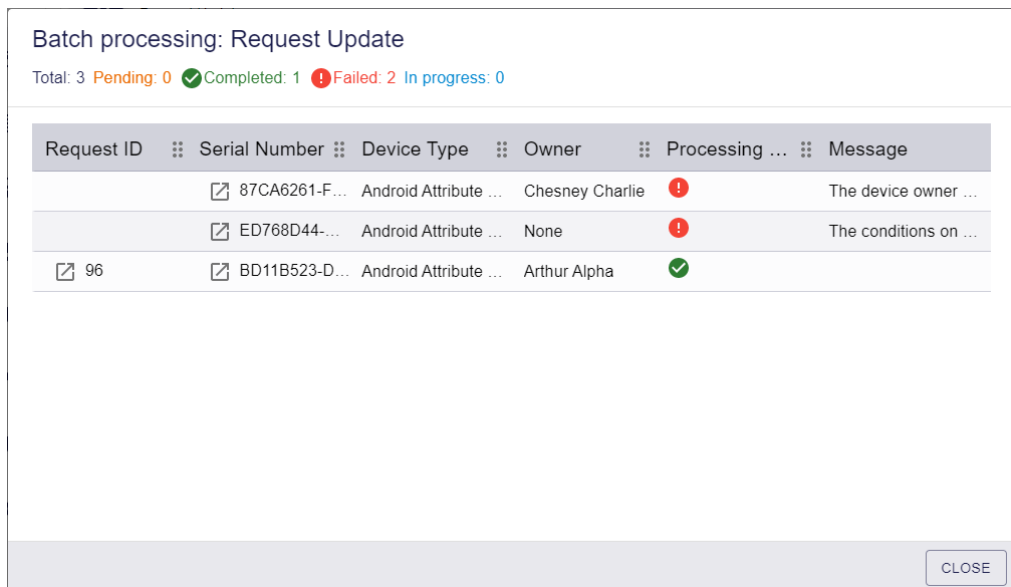
5. Click **Save**.

The confirmation screen appears.



6. 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.



7. 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; you may have selected a different credential profile than was originally used to provision

the mobile identity document; you may have selected a reason other than "Reprovision Document".

8. Click **Close**.

5.3 Canceling mobile identity documents

You can cancel a mobile identity document.

Note: This does not affect the mobile identity document on the wallet app itself, but it allows a third party to confirm the validity of a provisioned mobile identity document by checking it against the MyID database; for example, by producing a web service that checks the serial number of the mobile identity document using the MyID Core API.

Only the selected mobile identity document is affected when you cancel it. If the person has more than one mobile identity document stored in their wallet app, or has other mobile IDs stored on the same mobile device, these are not affected.

5.3.1 Canceling a mobile identity document

To cancel a mobile identity document:

1. In the MyID Operator Client, search for the device you want to cancel.

You can use the **Device** search report; you are recommended to add the **Device Category** from the **Additional search criteria** section, and select **Mobile Identity Document** from the drop-down list.

Alternatively, you can use the **Devices** tab on the View Person screen. On this screen, mobile identity documents appear with a **Device Type** of **Android Attribute Store** or **iOS Attribute Store**.

2. Select the mobile identity document you want to cancel, and open it in the View Device screen.
3. Click **Cancel Device**.

Cancel Device

CONFIRM DETAILS

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

Disposal Status

SAVE

Note: If the **Cancel Device** button is not available, but **Request Cancel** is available instead, the mobile identity document was issued with a credential profile that has the **Validate Cancellation** option set, and you must request the cancellation of the device, and then another operator must approve the cancellation. See section 5.3.2, [Requesting a cancellation for a mobile identity document](#).

4. Select a **Reason** from the drop-down list.

For most devices, the reason determines how the certificates are treated; as mobile identity documents do not have certificates, the reason you select is for informational purpose only for the audit; for example, **Lost**, **Damaged**, or **Stolen** may be appropriate values.

5. Type any **Notes** on the cancellation.

You can provide further information on your reasons for canceling the mobile identity document. This information is stored in the audit record.

Note: The **Disposal Status** is not relevant for mobile identity documents.

6. Click **Save**.

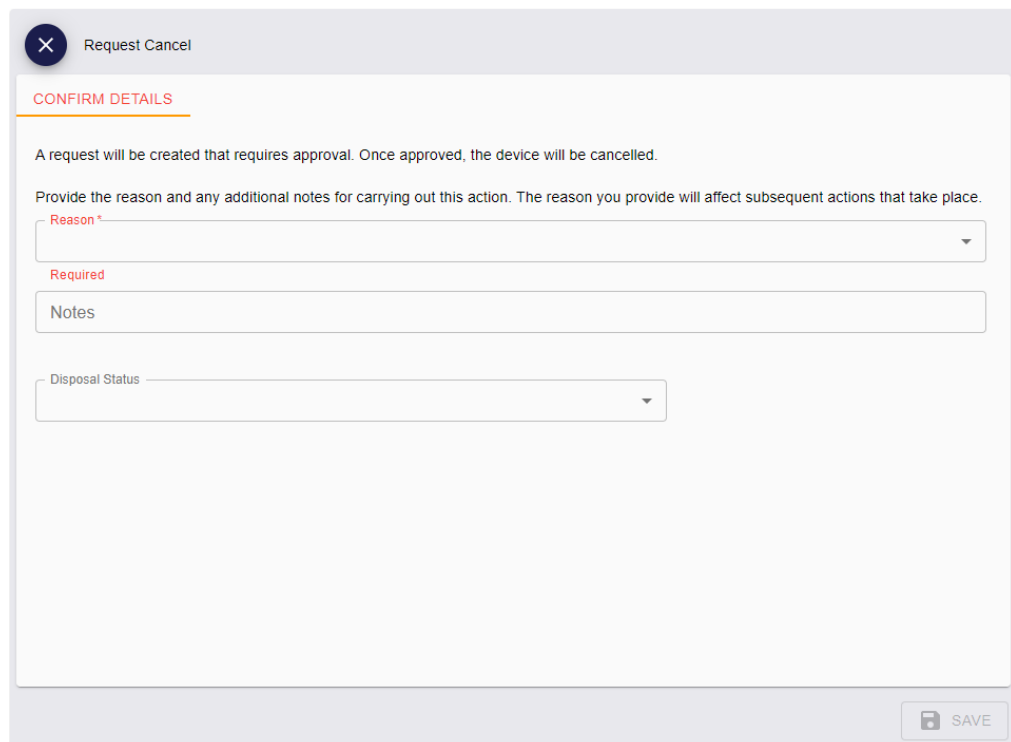
The mobile identity document is marked as canceled in the MyID database, and is disassociated from the person's user record. You can still view details of the mobile identity document from the **Previous Devices** tab on the View Person screen.

5.3.2 Requesting a cancellation for a mobile identity document

If the credential profile used to issue a mobile identity document had the **Validate Cancellation** option set, you cannot cancel the mobile identity document directly; you must request the cancellation of the mobile identity document, and have another operator approve the cancellation.

To request the cancellation of a mobile identity document:

1. In the MyID Operator Client, search for the device you want to cancel.
 You can use the **Device** search report; you are recommended to add the **Device Category** from the **Additional search criteria** section, and select **Mobile Identity Document** from the drop-down list.
 Alternatively, you can use the **Devices** tab on the View Person screen. On this screen, mobile identity documents appear with a **Device Type** of **Android Attribute Store** or **iOS Attribute Store**.
2. Select the mobile identity document you want to cancel, and open it in the View Device screen.
3. Click **Request Cancel**.



Note: If the **Request Cancel** button is not available, but **Cancel Device** is available instead, the mobile identity document was not issued with a credential profile that has the **Validate Cancellation** option set, and you can cancel the device without approval. See section [5.3.1, *Canceling a mobile identity document*](#).

4. Select a **Reason** from the drop-down list.
 For most devices, the reason determines how the certificates are treated; as mobile identity documents do not have certificates, the reason you select is for informational purpose only for the audit; for example, **Lost**, **Damaged**, or **Stolen** may be appropriate values.
5. Type any **Notes** on the cancellation.
 You can provide further information on your reasons for requesting the cancellation of the mobile identity document. This information is stored in the audit record.

Note: The **Disposal Status** is not relevant for mobile identity documents.

6. Click **Save**.

A request is created for the cancellation. Another operator must now approve or reject the cancellation; see the *Approving, rejecting, and canceling requests* section in the *MyID Operator Client* guide.

5.3.3 Canceling multiple mobile identity documents

If you want to cancel multiple mobile identity documents, you can cancel them in a batch instead of canceling them one by one.

Note: You cannot cancel multiple mobile identity documents if they were issued with the **Validate Cancellation** option set; you must request cancellation for each mobile identity document individually.

To cancel multiple mobile identity documents:

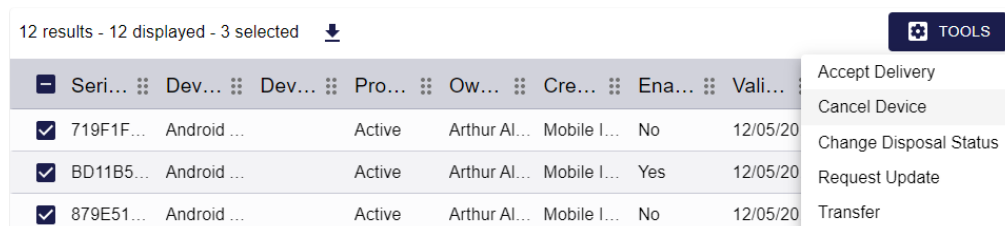
1. In the MyID Operator Client, search for the devices you want to cancel.

You can use the **Device** search report; you are recommended to add the **Device Category** from the **Additional search criteria** section, and select **Mobile Identity Document** from the drop-down list.

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 5.3.1, *Canceling a mobile identity document* for details of requesting an update for a single device.

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

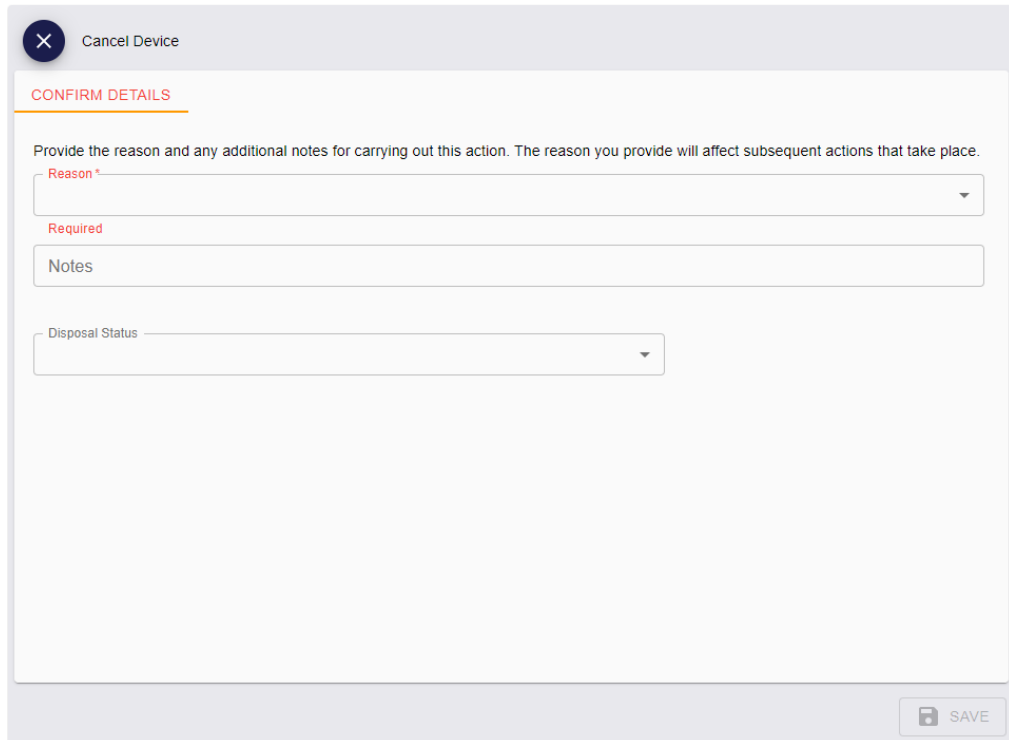


12 results - 12 displayed - 3 selected

<input type="checkbox"/>	Seri...	Dev...	Dev...	Pro...	Ow...	Cre...	Ena...	Vali...
<input checked="" type="checkbox"/>	719F1F...	Android ...		Active	Arthur Al...	Mobile I...	No	12/05/20
<input checked="" type="checkbox"/>	BD11B5...	Android ...		Active	Arthur Al...	Mobile I...	Yes	12/05/20
<input checked="" type="checkbox"/>	879E51...	Android ...		Active	Arthur Al...	Mobile I...	No	12/05/20

- Accept Delivery
- Cancel Device
- Change Disposal Status
- Request Update
- Transfer

The Cancel Device screen appears.



4. Select a **Reason** from the drop-down list.
For most devices, the reason determines how the certificates are treated; as mobile identity documents do not have certificates, the reason you select is for informational purpose only for the audit; for example, **Lost**, **Damaged**, or **Stolen** may be appropriate values.
5. Type any **Notes** you want to add.
The **Notes** are stored in the audit trail.
Note: The **Disposal Status** is not relevant for mobile identity documents.
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: Cancel Device
Records selected: 3

Reason: Lost
Notes: Mobile devices left on the train

YES
NO

- 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: 3 Pending: 0 ✔ Completed: 2 ❗ Failed: 1 In progress: 0

Owner	Processing sta...	Message
00001	❗	The conditions on the Operation with ID 100205 prohibit use of the operation for the t...
00001	✔	
00001	✔	

CLOSE

- 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 canceled, or the device may have been issued with the **Validate Cancellation** option set.
- Click **Close**.

5.4 Reporting on mobile identity documents

You can use device-related reports to provide information on the mobile identity documents that have been issued by your system.

For example:

- **Mobile Devices** – lists all mobile devices, including mobile identities and mobile identity documents.
- **Devices** – lists all devices.

When using these reports, you are recommended to add the **Device Category** from the **Additional search criteria** section, and select **Mobile Identity Document** from the drop-down list to restrict the results to mobile identity documents only.

Mobile identity documents are also summarized in the **Issued devices by category** report when you select **Mobile Identity Document** as the **Device Category**, and appear in the results list with **document** in the **Device Category** column.

Any actions carried out on mobile identity documents (issuing, enabling, disabling, updating, and canceling) are recorded in the audit trail. You can view the audit for a specific mobile identity document from the **Device History** tab of the View Device screen.