



MyID

Version 10.8 Update 2

Mobile Identity Management
Installation and Configuration Guide

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

Copyright

© 2001-2018 Intercede Limited. All rights reserved.

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

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

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

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

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.

Licenses and Trademarks

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

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

Conventions Used in this Document

- Lists:
 - ♦ Numbered lists are used to show the steps involved in completing a task when the order is important
 - ♦ Bulleted lists are used when the order is unimportant or to show alternatives
- **Bold** is used for menu items and for labels.
For example:
 - ♦ “Record a valid email address in **'From' email address**”
 - ♦ Select **Save** from the **File** menu
- *Italic* is used for emphasis and to indicate references to other sections within the current document:
For example:
 - ♦ “Copy the file *before* starting the installation”
 - ♦ “See *Issuing a Card* for further information”
- ***Bold and italic*** are used to identify the titles of other documents.
For example: “See the ***Release Notes*** for further information.”
Unless otherwise explicitly stated, all referenced documentation is available on the installation CD.
- A `fixed width` font is used where the identification of spaces is important, including filenames, example SQL queries and any entries made directly into configuration files or the database.
- **Notes** are used to provide further information, including any prerequisites or configuration additional to the standard specifications.
For example:
Note: This issue 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

1	Introduction.....	6
1.1	Supported devices	6
1.2	Supported key stores.....	6
1.3	Supported Mobile Device Management integration	6
1.4	Prerequisites and installation	7
1.4.1	SMS gateway.....	7
1.4.2	Communication with the MyID mobile web services	7
1.4.3	SSL certificate.....	7
1.4.4	IIS and web service users.....	7
1.4.5	Logon mechanisms for mobile identities	7
1.5	Overview.....	8
2	Configuring the System	9
2.1	Setting the content signing certificate	9
2.2	Setting the configuration options.....	10
2.2.1	Web service location.....	10
2.2.2	Setting the certificate recovery password complexity	10
2.2.3	Biometric authentication	11
2.2.4	Configuring the image location	11
2.2.5	Setting up support for historic certificates	11
2.3	Granting access to the workflows	12
2.3.1	Roles	12
2.3.2	Scope	12
2.4	Configuring SMS and email notifications	13
2.5	Configuring the SMS gateway	13
2.6	Configuring SMS and email certificate renewal notifications	14
2.7	Configuring the Certificate Authority	15
2.8	Registering mobile devices.....	15
2.9	Setting up iOS OTA provisioning	16
2.9.1	iOS OTA certificate requirements	17
2.10	Setting up the Identity Agent credential profiles.....	18
2.10.1	Creating the Identity Agent credential profile	18
3	Requesting and Approving Mobile IDs	21
3.1	Recovering archived certificates	21
3.2	Requesting a mobile ID for another user	22
3.3	Requesting a mobile ID for your own mobile device	23
4	Working with Mobile IDs	24
4.1	Cancelling a mobile ID	24
4.1.1	Important information about cancelling mobile IDs	24
4.2	Requesting replacement IDs.....	24
4.3	Enabling and disabling IDs	25
4.4	Unlocking IDs.....	25
5	Troubleshooting	26
5.1	Setting up logging	26
5.2	Retry attempts	26
5.3	Configuration issues	27

1 Introduction

This document provides information on the support for MyID® Mobile Identity Management (MIM), including details on the following:

- Configuring the system to support the installation of mobile identities on your mobile devices.
- Requesting mobile identities through MyID.
- Managing mobile identities through MyID.

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

In this document, the words *mobile device* may refer either to a smartphone or a tablet. Some devices are unable to receive SMS messages but can receive emails capable of starting the identity management process.

For information on using the mobile identities on your mobile device, see the information accompanying the individual client applications.

1.1 Supported devices

The following devices are supported:

- iOS 11.0, 10.0, 9.0
- Android 8.0, 7.0, 6.0, 5.0

If you would like to use a mobile operating system not listed here, contact Intercede customer support quoting reference SUP-49.

1.2 Supported key stores

MyID currently supports the following key stores:

- Intercede key store on iPhone and iPad.
- Intercede key store for Android devices running 4.3 (Jellybean) or above.
- Citrix SecureVault on iPhone and iPad.
- MobileIron AppConnect on iPhone and iPad.
- iOS first party accessible key store on iPhone and iPad.

1.3 Supported Mobile Device Management integration

MyID currently supports integration with the following Mobile Device Management (MDM) and associated systems:

- Citrix XenMobile 10.6.
- MobileIron Core 9.2 Derived Credentials.
- VMWare AirWatch 9.1.
- Centrify Identity Service.

Note: Contact Centrify for details of supported versions.

Contact the relevant vendor for full details of how to configure these MDM systems for integration with MyID.

1.4 Prerequisites and installation

1.4.1 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.

See section [2.5, Configuring the SMS gateway](#) for details.

Alternatively, you can use email for notifications.

1.4.2 Communication with the MyID mobile web services

To allow your mobile device to obtain and work with mobile IDs, your device must be able to communicate with the URLs of the MyID mobile web services; for example:

```
https://myserver/MyIDProcessDriver/
```

```
https://myserver/MyIDDDataSource/
```

```
https://myserver/CertificateCheck/
```

Where `myserver` is the name of the server on which the MyID web services are installed.

Note: If you attempt to browse to these URLs from the mobile device, you will see an error due to the security set up on the web service folders; this does not mean that the connection has failed.

Your PC-based MyID clients must also be able to communicate with these web services. For example, QR codes are generated on the web services server by the MyIDDDataSource web service, and embedded in the workflow.

1.4.3 SSL certificate

Before you start provisioning mobile devices, you must issue an SSL certificate from a trusted root CA.

Issuance will fail if the SSL certificate used on the MyID web server is untrusted by the mobile device. Intercede recommends that either an SSL certificate is issued by a trusted public root CA, or that devices have a trusted root CA for the issuing CA added to their Trusted Root stores.

1.4.4 IIS and web service users

The MyID IIS and MyID web service users must be members of the IIS_IUSRS Windows group; this is necessary for .NET 4 to operate correctly.

1.4.5 Logon mechanisms for mobile identities

The server update installation program turns on the **Password Logon** logon mechanism, which is essential for the correct operation of this mobile identities. You must review your settings for logon mechanisms for the end user roles – you can switch off password logon for individual roles by using the **Assign Logon Mechanisms** feature in the **Edit Roles** workflow.

1.5 Overview

This system allows you to request a mobile ID from your MyID system and store it on your mobile device; this allows you to use secure certificates with your email application for reading and writing encrypted and signed emails, display an identity badge, and so on.

The process is as follows:

1. You install the MyID Identity Agent app on your mobile device.
2. Using MyID, a MyID operator requests (and optionally approves) an ID for your mobile device.
3. MyID uses email or an SMS gateway to send a message to the user's email address or phone number that is stored as the **Cell** or **Mobile** (depending on the language setting) number in the MyID record.
4. When the message is received on your mobile device, you click the link or notification.

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

5. You use the Identity Agent app to download the certificates and badge layouts to your mobile device from the MyID web service.
6. You can now use your mobile device as a MyID device.

2 Configuring the System

You must configure your system to allow you to request mobile IDs and collect them on the mobile device.

2.1 Setting the content signing certificate

MyID must be able to sign the content for the mobile IDs before issuing them to mobile devices. Before MyID can use a certificate to sign the mobile IDs, the certificate must be available to the MyID COM user account.

1. On the MyID application server, log on using the account that you use to run the MyID components.
2. Request a certificate that will be placed in the CAPI store. You can issue a certificate from any certificate authority as long as it is available to CAPI.

Notes:

- ◆ Do not enable strong private key protection on the certificate, as this will prevent processing of the request by the MyID account.
 - ◆ CNG is currently not supported for this certificate.
 - ◆ By default, MyID uses SHA256 as the hashing algorithm when signing using this certificate. You must make sure that the CSP you use to issue the certificate supports SHA256.
3. Once the certificate has been generated, install and save it as a `.cer` file (in binary format). You must save it in a location accessible to the MyID application, so save it to the `Components` folder within the MyID installation folder.

Note: You may need administrative privileges to save files to this area.

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.

If the keys and values do not already exist, you must create them.

- a) From the **Start** menu, click **Run** and type `regedit` in the dialog displayed. Click **OK**.

- b) Navigate to:

```
HKEY_LOCAL_MACHINE\SOFTWARE\wow6432Node\Intercede\Edefice\ContentSigning
```

- c) Check that the value of the following string is set:

```
▫ Active – set to WebService
```

- d) Set the value of the following string to the full path of the certificate on the application server:

```
▫ WebService
```

For example:

```
C:\Program Files (x86)\Intercede\MyID\Components\mycert.cer
```

An example `.reg` file for setting the content signing certificate might be:

```
Windows Registry Editor Version 5.00
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Intercede\Edefice\ContentSigning]
"WebService"="C:\Program Files (x86)\Intercede\MyID\Components\mycert.cer"
"Active"="WebService"
```

2.2 Setting the configuration options

2.2.1 Web service location

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

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.

For example:

```
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 three 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 issuance. 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**.

2.2.2 Setting the certificate recovery password complexity

To set up the single-use authentication code that is used to secure mobile IDs 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**.

2.2.3 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.

2.2.4 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](#).

2.2.5 Setting up support for historic certificates

Note: Currently, you cannot provision historic certificates to MobileIron AppConnect or Citrix SecureVault keystores.

You can set up MyID to provide historic encryption certificates for mobile identities. This feature allows users to decrypt their old email messages on their mobile device. The historic encryption certificates are delivered to the mobile device when the mobile identity is issued.

To configure MyID to provide historic certificates, you must use the certificate options in the credential profile. See the [Administration Guide](#) for details of the **Issue new**, **Use existing**, and **Historic Only** options.

2.3 Granting access to the workflows

The system makes use of the following workflows:

- **Cancel Credential** – used within MyID to cancel a mobile ID and revoke its certificates.
- **Enable / Disable ID** – used within MyID to enable or disable a mobile ID, and suspend or enable its certificates.
- **Request ID** – used within MyID for operator-guided requests for mobile IDs to be installed on a mobile device.
- **Request My ID** – used within MyID for self-service requests for mobile IDs to be installed on a mobile device.
- **Request Replacement ID** – used within MyID to request a replacement for a missing or damaged mobile ID.
- **Unlock Credential** – used within MyID to retrieve an unlock code for an issued mobile ID.
- **Collect My Updates** – used by the Identity Agent app to obtain a mobile ID.
- **Issue Device** – used by the Identity Agent app to obtain a mobile ID.

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.

2.3.1 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.

2.3.2 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.

2.4 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.

You can also choose whether to display OTP codes on-screen or to send them to the mobile using SMS.

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 IDs to be sent to the user's email address.
 - ♦ **Mobile Provision Via SMS** – set this option to allow the notifications of mobile IDs 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.
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, as a security feature, the OTP is sent as an SMS while the notification message must be sent using email and *not* SMS; make sure you select the **Mobile Provision Via Email** option on the **Devices** tab.
 - ♦ **Mail Format** – make sure this option is set to **HTML**.
4. Click **Save changes**.

2.5 Configuring the SMS gateway

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\untranslated\res\custom\js\`
- `Web\en\res\custom\js\`
- `Web\us\res\custom\js\`

You must make the same changes in each version of the file. If you have created any custom translations of the MyID web site, 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.

2.6 Configuring SMS and email certificate renewal notifications

You can decide whether to send renewal messages through email, through SMS, or through both email and SMS.

To allow MyID to send SMS messages, set the **SMS email notifications** on the **General** tab of the **Operation Settings** workflow to *Yes*.

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

- `<cellnumber>` – the cell phone number from the user's record.
- `<gateway>` – the URL from the **SMS gateway URL for notifications** option on the **General** tab of the **Operation Settings** workflow.

For example: `00447700900123@smsgateway.com`

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

You can use different content for email and SMS certificate renewal messages, and different content for different kinds of device – mobile or card, for example. Six additional renewal messages are provided – three messages for SMS to mobile devices, and three messages for email to mobile devices. Use the **Email Templates** workflow to edit the content of these messages.

2.7 Configuring the Certificate Authority

You must configure the certificate template to set the options for storing the certificate on your mobile device.

For the **Certificate Storage** and **Recovery Storage** options, select the following:

- **Hardware** – the certificate is stored on the mobile device secure element. This provides high security, and requires a secure element to be present in the mobile device.
- **Both** – for the purposes of writing certificates to mobile devices, this works in the same way. You cannot select **Hardware** only.
- **Software** – the certificate is stored on the mobile device local key store.

2.8 Registering mobile devices

You can use the **Mobile Device Restrictions** option to set up your credential profiles to issue mobile identities only to those mobile devices that have been registered with MyID.

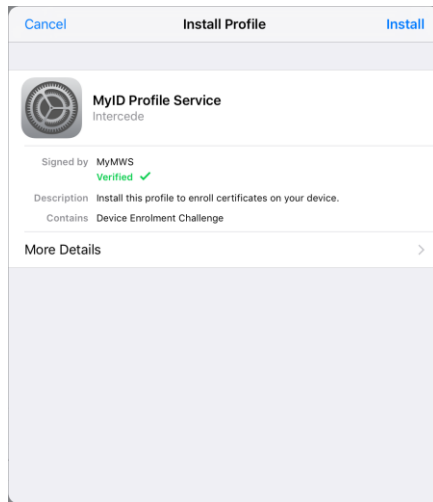
You can obtain the serial number from the Identity Agent app on the mobile device.

Once you have the serial number, you can use the `AddDevice` method of the Device Management API to register the device with MyID.

See the [Device Management API](#) document for details.

2.9 Setting up iOS OTA provisioning

You can configure MyID to enroll a certificate on your iOS device using Over the Air (OTA) provisioning. The update appears on the device as a profile to be installed when you are issuing a mobile identity.



This feature requires the following additional web service modules to be installed and configured on your MyID server:

- SCEP – Simple Certificate Enrollment Protocol (SCEP) device identities.
You must follow the instructions in the *Installation and Configuration* section of the [SCEP Device Identities Integration Guide](#) before setting up iOS OTA provisioning. You do not need to request or collect any SCEP device identities.
- IOSOTA – OTA (Over The Air) provisioning of certificates to iOS.

The SCEP module is available in the APIs folder on the product CD, and the IOSOTA module is available in the Mobile folder on the product CD.

To configure MyID for OTA provisioning:

1. Create an **Identity Agent (Only)** credential profile that uses the following:
 - ♦ A **Card Format** of **IOS**.
 - ♦ One or more certificates that uses the **iOS System Store** container.

See section 2.10, [Setting up the Identity Agent credential profiles](#) for details.
2. Create a **Device Identity (Only)** credential profile that uses the following:
 - ♦ **Require Challenge** option selected.

See the *Setting up a credential profile to use to issue device identities* section in the [Administration Guide](#) for details of completing the credential profile.

See also section 2.9.1, [iOS OTA certificate requirements](#) for details of the requirements for the device certificate.
3. From the **Configuration** category, select **Operation Settings**.
4. Click the **Certificates** tab.
5. Set the following options:
 - ♦ **iOS OTA Credential Profile** – set this option to the name of the Device Identity credential profile.
 - ♦ **iOS OTA Organization** – set this option to the name of your organization. This appears on the OTA provisioning message on the mobile device.

In the screenshot above, this option has been set to `Intercede`.

- ◆ **iOS OTA Display Name** – set this option to a name for the OTA update. This appears on the OTA provisioning message on the mobile device.

In the screenshot above, this option has been set to `MyID Profile Service`.

- ◆ **iOS OTA Description** – set this option to the a description for the OTA update. This appears on the OTA provisioning message on the mobile device.

In the screenshot above, this option has been set to `Install this profile to enroll certificates on your device`.

6. If required, you can customize the transform on the web services server that is used to display the intermediate web page that presents a link to the CA root certificate and the Enroll page used to provision the certificates.

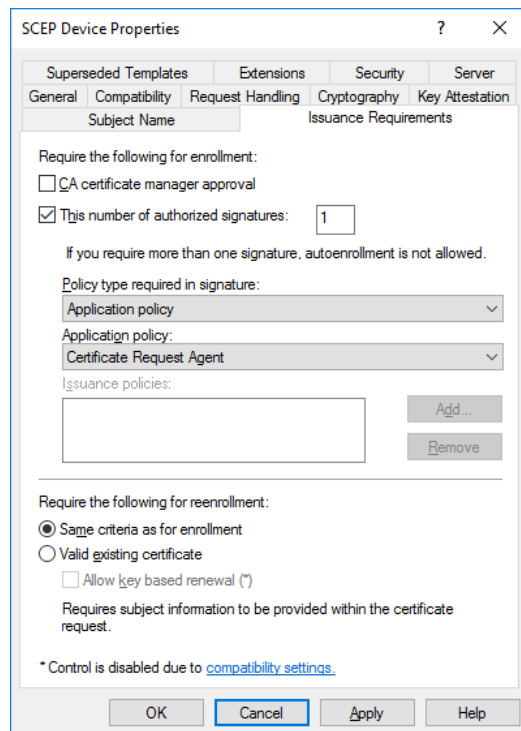
See the [Web Service Architecture Installation and Configuration](#) guide for details.

7. Click **Save changes**.

2.9.1 iOS OTA certificate requirements

This section contains some specific issuance requirements for the certificate template for a Microsoft Certificate Authority for iOS OTA issuance.

- The certificate you use for iOS OTA issuance must have the **CA certificate manager approval** option deselected.
- Set the **Policy type required in signature** drop-down list to **Application policy**.
- Set the **Application policy** drop-down list to **Certificate Request Agent**.



If you see a message in the "Failed requests" section of the CA similar to:

One or more signatures did not include the required application or issuance policies. The request is missing one or more required valid signatures.

this means that the **Application policy** option is set to **Any Purpose** instead of **Certificate Request Agent**.

2.10 Setting up the Identity Agent credential profiles

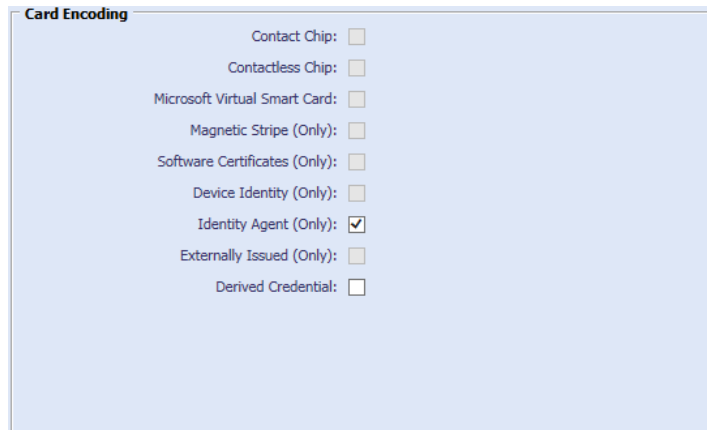
You must create at least one new credential profile for issuing mobile IDs to mobile devices.

The credential profile contains the certificates that you want to issue to mobile users. You may create as many of these credential profiles as you need.

2.10.1 Creating the Identity Agent credential profile

To create a credential profile for issuing mobile identities:

1. From the **Configuration** category, select **Credential profiles**.
2. Click **New**.
3. Type a **Name** for the credential profile.



Card Encoding

- Contact Chip:
- Contactless Chip:
- Microsoft Virtual Smart Card:
- Magnetic Stripe (Only):
- Software Certificates (Only):
- Device Identity (Only):
- Identity Agent (Only):
- Externally Issued (Only):
- Derived Credential:

4. In **Card Encoding**, select **Identity Agent (Only)**.
5. In **Issuance Settings**, in the **Mobile Device Restrictions** drop-down list, select one of the following:
 - ♦ **Any** – The mobile identity can be loaded onto any mobile.
 - ♦ **Known Mobiles** – The mobile identity can be loaded onto any mobile that has already been registered with MyID. See section 2.8, *Registering mobile devices* for details.
 - ♦ **My Mobiles Only** – The mobile identity can be loaded only onto mobiles associated with the user's account.
6. Make sure that you do not require any biometrics:
 - ♦ **Require Fingerprints at Issuance** – set to **Never required**.
 - ♦ **Require Facial Biometrics** – set to **Never required**.
7. In **Device Profiles**, set the following from the **Card Format** drop-down list:
 - ♦ For Citrix enabled mobile devices, select **Citrix SecureVault**.
Select a different option for Citrix devices *only* if you have a customized data model that you must use for your system.

If you have upgraded from MyID 10.8 or earlier, you may have the option to select **Legacy Citrix Vault**. This is for a legacy version of Citrix; do not select this option unless Intercede advises you otherwise.
 - ♦ To issue archived certificates to the iOS System Store, select **iOS**.
 - ♦ For MobileIron enabled mobile devices, select **MobileIron AppConnect**.
Select a different option for MobileIron devices *only* if you have a customized data model that you must use for your system.

- ◆ For VMware AirWatch and Centrify Identity Service enabled mobile devices, make sure that **None** is selected.
- ◆ For all other mobile devices, make sure that **None** is selected.

Note: If you attempt to issue a mobile device using a credential profile that includes support for certificates stored in the Citrix, MobileIron, or iOS System Store, but the mobile device does not support these certificate stores, the issuance will succeed; however, any certificates specified by the credential profile to be installed to containers that the mobile device does not support will be ignored.

For example, if your credential profile contains a Citrix Signing certificate, a Citrix Encryption certificate, and a certificate with no container specified, a Citrix-enabled mobile device will receive all three certificates, while a mobile device that is not Citrix-enabled will receive only the certificate with no container specified.

8. Click **Next**.
9. Select the certificates you want to make available.
 - ◆ For credential profiles that use a Citrix data model, select the Citrix containers for the certificates.
 You can also select the **iOS System Store** for one or more certificates. See section 2.9, [Setting up iOS OTA provisioning](#) for details of provisioning certificates to the iOS System Store.
 - ◆ For credential profiles that use an iOS data model, you can select the **iOS System Store** for one or more archive certificates.
 - ◆ For credential profiles that use a MobileIron data model, select the MobileIron containers for the certificates.
 - ◆ For VMware AirWatch and Centrify Identity Service enabled mobile devices, do not select any containers.
 - ◆ For all other types of credential profiles, do not select any containers.

All of the certificates you select here will be issued to your mobile device.

You can select the archived and historic certificate options on this screen. See the [Administration Guide](#) for details of the **Issue new**, **Use existing**, and **Historic Only** options.

If you want to distribute certificates that were not issued through MyID, you can import a PFX file then select the **Unmanaged** certificate option to specify it for distribution to the mobile device. See the [Import and distribute certificates to devices](#) section in the [Administration Guide](#) for details of setting up your credential profile and using the **Upload PFX Certificates** workflow.

10. Click **Next** and proceed to the Select Roles screen.
11. Select the roles you want to be able to issue and receive this credential profile.
 - ◆ The **Can Receive** option determines which roles can receive credentials issued using this credential profile.
 - ◆ The **Can Request** option determines which roles can request credentials 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 credentials using this credential profile using the **Validate Request** workflow.
 - ◆ The **Can Collect** option determines which roles can collect credentials using this credential profile; any user who is to receive a mobile identity must have both the **Can Receive** and the **Can Collect** options.
 - ◆ The **Can Unlock** option determines which roles can unlock mobile identities using the **Unlock Credential** workflow.

Note: Not all options may be available, depending on your system configuration. See the [Administration Guide](#) for details.

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

12. Click **Next**.

13. 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 ID. Note, however, that the reverse sides of the selected layouts (the `_back` layouts) will not be available on the mobile device.

Note: Card layouts are optional, and will be created only when using the Intercede key store and certificates are selected in the credential profile.

14. Select one of the layouts to be the default layout.

This layout will be displayed by default when using the Identity Agent app, and will be used for phone-to-phone identity verification.

15. Click **Next**.

16. Type your **Comments** and complete the workflow.

3 Requesting and Approving Mobile IDs

You can request a mobile ID for your own mobile device or for another user's mobile device.

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

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

Note: The **Request ID** and **Request My ID** workflows are not assigned to any roles by default. You must use the **Edit Roles** workflow to ensure that these workflows are assigned to the roles you want to be able to request certificates for their mobile device.

In addition to the **Request ID** and **Request My ID** workflows within MyID, you can also request a mobile ID from an external system using the Credential Web Service API. For more information, see the [Credential Web Service](#) document.

Collecting the mobile ID may take several minutes, depending on the complexity of the certificates and the speed of your network connection. If the collection fails due to network problems, you are recommended to use the **Cancel Credential** workflow to cancel the mobile ID, then request another mobile ID for the user.

3.1 Recovering archived certificates

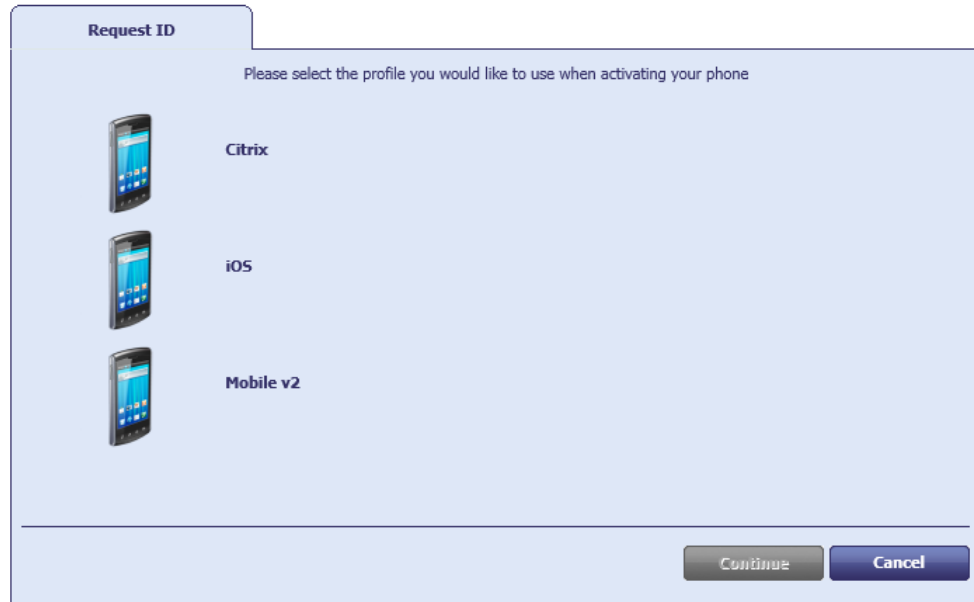
To recover a certificate from an existing card, the user must have a certificate that:

- is issued to a current device.
- has archived keys.
- is issuable and recoverable to software.
- has a policy that is available on at least one credential profile available to the user that has **Identity Agent (Only)** selected.

3.2 Requesting a mobile ID for another user

To request a mobile ID 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.

Note: The email address is case sensitive for the Citrix credential store. You must ensure that the email address in the user record is in lower case and that the address matches exactly in other areas of the system; for example, on Exchange Server and in the LDAP directory.

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 ID 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 ID on your mobile device.

3.3 Requesting a mobile ID for your own mobile device

To request a mobile ID for your own mobile device:

1. From the **Mobile Devices** category, select **Request My ID**.
2. Select the credential profile you want to use.



3. Click **Continue**.
4. Take a note of the password.
This single-use code is required to install the mobile ID 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.

5. Check that the phone number or email address is correct, then click **Send**.

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

Note: The email address is case sensitive for the Citrix credential store. You must ensure that the email address in your user record is in lower case and that the address matches exactly in other areas of the system; for example, on Exchange Server and in the LDAP directory.

If you do not have a username or password set up on your account, MyID displays a QR code. Open the Identity Agent 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.

4 Working with Mobile IDs

Once a user has been issued with a mobile ID, you can use MyID to manage the mobile IDs and their certificates.

4.1 Cancelling a mobile ID

The **Cancel Credential** workflow allows you to cancel an issued ID and revoke its certificates.

This does not affect the contents of the mobile device directly, but it revokes or suspends the certificates that were copied to the mobile device, and cancels the device in the MyID database. Any online check of the certificates or the mobile ID will fail, indicating that the mobile ID is no longer valid.

You can use this option if provisioning the mobile device fails, the mobile device is lost or stolen, or if the certificates expire and need to be replaced on the same device.

See the [Administration Guide](#) for details of using the **Cancel Credential** workflow.

4.1.1 Important information about cancelling mobile IDs

Cancelling a mobile ID from MyID does not affect the contents of the mobile device directly; as a result, customer 9B or GlobalPlatform keys and randomized SOPINs will not be reset to their factory defaults.

If any of the following situations occur, you will be unable to use the SIM card:

- A SIM card with customized 9B keys is moved to a different device type (for example, from an Android to a BlackBerry smartphone) or to a different MyID system.
- A SIM card with randomized SOPIN is moved to a different device type or to a different MyID system.
- A SIM card with customized GlobalPlatform keys is moved to a different MyID system.

Cancelling a mobile ID from the mobile device *does* affect the contents of the mobile device directly; as a result, customer 9B or GlobalPlatform keys and randomized SOPINs will be reset to their factory defaults. You are therefore recommended, if the option exists on the mobile device, to use the option to cancel a mobile identity when the device is to be used elsewhere; for example, a different device type or MyID system.

Note: Cancelling a mobile ID from the mobile device removes the identity from the mobile device, but does not revoke the certificates. The recommended method is to use **Cancel Credential** within MyID to cancel the mobile identity in the MyID database and revoke its certificates, then cancel the mobile identity on the mobile device itself to clean up the security objects on the device.

4.2 Requesting replacement IDs

The **Request Replacement ID** workflow allows you to replace a mobile ID that is missing or damaged.

1. From the **Mobile Devices** category, click **Request Replacement ID**.
2. Use the Find Person screen to select the person.
The devices assigned to the person are listed.
3. Select the device you want to replace.
4. Select a reason and provide **Details** for the card replacement, then click **Next**.

The old mobile ID is canceled, and a job for a replacement mobile ID is created.

Note: If you are requesting a replacement for a mobile identity based on an MIM credential profile, the replacement must use an Identity Agent-based credential profile.

4.3 Enabling and disabling IDs

The **Enable / Disable ID** workflow allows you to change the status of an issued ID and its certificates; you can disable an ID so that the certificates are suspended, or enable an ID so that the user can use its certificates again.

To enable or disable a mobile ID:

1. From the **Mobile Devices** category, click **Enable / Disable ID**.
2. Click **Search** then use the Find Person screen to find the cardholder, then select the device you want to enable or disable.
3. To disable a mobile ID, select the reason and type the details for disabling the mobile ID, then click **Disable**.

To re-enable a mobile ID, click **Enable**.

4.4 Unlocking IDs

Note: This feature is available on Android and iOS mobile devices only.

The **Unlock Credential** workflow allows you to retrieve an unlock code for an issued ID. The mobile device owner starts the unlock process on their mobile device, then contacts the helpdesk operator, who uses the **Unlock Credential** workflow to provide an unlocking code.

For information on using the **Unlock Credential** workflow, see the [Administration Guide](#).

5 Troubleshooting

5.1 Setting up logging

You can configure the Identity Agent app to create a log file for debugging purposes. Customer support may ask you to switch logging on and send the resulting log file to Intercede for analysis.

To enable logging, use the following configuration options on the **Identity Agent Policy** page of the **Operation Settings** workflow:

- **Administrator email address** – Set this to the email address to which Identity Agent will send logs for troubleshooting purposes.
- **Log level** – Set this to the level of debug logging you want Identity Agent to produce. Higher levels result in more detail, but larger files.

Set to one of the following:

- 0 – NONE
- 1 – FATAL
- 2 – ERROR
- 3 – WARNING
- 4 – INFO
- 5 – DEBUG
- 6 – VERBOSE

Note: This setting affects the level of *debug* logging only; the Identity Agent also logs all *messages* that occur between the client and the server. If you want to switch off logging altogether, set the **Maximum number of log files** to 0.

- **Maximum log storage space** – The maximum amount of space (in MB) that log files will take up on a device. Once this limit is reached, log files will be deleted automatically, oldest first, to clear room for new files.
- **Maximum number of log files** – The maximum number of log files to be stored on a device. Once this limit is reached, log files will be deleted automatically, oldest first, to clear room for new files.

To allow as many files as will fit in the maximum log storage space, set this value to -1.

5.2 Retry attempts

You can configure how Identity Agent handles attempts to reconnect to the server if the connection is lost during an operation.

Use the following configuration options on the **Identity Agent Policy** page of the **Operation Settings** workflow:

- **Maximum retry attempts**
The maximum number of times Identity Agent should attempt to reconnect to the server if connection is lost during an operation. The default is 5 times.
- **Minimum retry delay**
The minimum delay, in seconds, between each attempt to contact the server after connection has been lost. The default is 10 seconds.

5.3 Configuration issues

- None of the selected user's certificates are configured to be allowed to be put on a mobile phone.

Make sure that you have setup the credential profiles correctly according to the instructions in this document. Make sure that the user has permission to receive the credential profile, and that the issuer can issue the credential profile.

Make sure that the certificate policy is the correct one.

Make sure that the certificate policy can be issued in software.

- The selected user has no certificates suitable for mobile devices and there are no credential profiles available for issuance.

Make sure that the user has permission to receive the credential profile, and that the issuer can issue the credential profile.

Make sure that the certificate policy is the correct one.

- The selected user has neither phone number nor email address registered and so is not suitable for mobile device activation.

Make sure that the user has an entry in the MyID database for Mobile or Cell phone number or for email address. If you are using LDAP integration, and you do not have this field populated in the directory, synchronizing MyID with the directory may clear this field from the MyID database.