



# **MyID Enterprise**

**Version 12.10**

## **Error Code Reference**

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

## Copyright

© 2001-2024 Intercede Limited. All rights reserved.

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

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

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

### **Licenses and Trademarks**

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

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

### **Apache log4net**

Copyright 2004-2021 The Apache Software Foundation

This product includes software developed at

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

## Conventions used in this document

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

For example:

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

For example:

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

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

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

For example:

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

For example:

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

## Contents

<b>Error Code Reference</b>	<b>1</b>
<b>Copyright</b>	<b>2</b>
<b>Conventions used in this document</b>	<b>3</b>
<b>Contents</b>	<b>4</b>
<b>1 Introduction</b>	<b>5</b>
<b>2 Web Service error codes</b>	<b>6</b>
<b>3 MyID Identity Agent error codes</b>	<b>80</b>
3.1 Troubleshooting network connectivity	88
3.2 Configuring logging for Identity Agent	89
3.2.1 Sending logs to the system administrator	89
<b>4 MyID Windows client error codes</b>	<b>90</b>
4.1 Generic errors	98
<b>5 Printer error codes</b>	<b>100</b>
<b>6 MyID Operator Client error codes</b>	<b>106</b>
<b>7 MyID Client Service error codes</b>	<b>178</b>
7.1 .NET Networking errors	181

# 1 Introduction

This document provides a reference to the error codes that appear in MyID®, and possible actions that you can carry out if the errors occur.

**Important:** When searching for an error, use the error code, not the error text. In some cases, the error text may have been optimized for the client where it appears.

## 2 Web Service error codes

This section contains a list of the errors that can occur when using the MyID Web Services. Not all of these errors can appear if you are using exclusively Intercede software on the client. Often multiple error messages will share common text but have a different code. This is to assist in locating the cause of the issue. Further details about each error can often be found in the **Audit Reports** workflow.

To assist with the diagnosis of issues, Intercede support may guide you to enable logging on the `ProcessDriver` service; you can then provide these logs to customer support for analysis. See the *MyID Web Services* section in the [Configuring Logging](#) guide for details of enabling logging.

The specific text displayed on a client may have been optimized for that client, and not explicitly match the text below. When searching, search on the error number, not the error text.

<b>Error Code</b>	2978
<b>Text</b>	Please check your configuration. If the problem occurs again, contact your administrator.
<b>Details</b>	An attempt has been made to cancel a Device Identity and the user does not have permissions to create the Cancel Device Identity job.
<b>Solution</b>	Check that the user has the <b>(Devices)</b> group in their administrative groups.
<b>Relates To</b>	Device Identity Management

<b>Error Code</b>	10304
<b>Text</b>	Invalid Entry
<b>Details</b>	A certificate used during mobile provisioning contains invalid or corrupted data.
<b>Solution</b>	The certificate is unusable. The PFX file that the certificate was imported from is probably invalid. Source a valid PFX file and import it again.
<b>Relates To</b>	Identity Agent Provisioning

<b>Error Code</b>	21629
<b>Text</b>	Already Issued
<b>Details</b>	Issuing the current device has been prevented because the device is already issued.
<b>Solution</b>	If the device should not be issued to anyone, it can be canceled using the <b>Cancel Credential</b> workflow or <b>Remote Cancel Credential</b> . The <b>Audit Reporting</b> workflow will give details of the user that the device is already issued to.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	21642
<b>Text</b>	Incompatible
<b>Details</b>	Issuing the current device has been prevented because the device is incompatible. It may be that a virtual smart card was selected for a credential profile that is restricted to physical smart cards, or that the inserted smart card does not support a data model assigned to the credential profile.
<b>Solution</b>	Try selecting a different credential profile, or using a different device. See the <b>Audit Reporting</b> workflow for further details.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	21643
<b>Text</b>	Insufficient Space
<b>Details</b>	Issuing the current device has been prevented because the device has insufficient space for the required number of certificates.
<b>Solution</b>	Provide the user with a device that has capacity for the chosen credential profile. If the credential profile was chosen in error, request a different credential profile with fewer certificates on it. See the <b>Audit Reporting</b> workflow for further details.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	21644
<b>Text</b>	Incorrect Device
<b>Details</b>	Issuing to the current device has been prevented because the request is bound to a different device.
<b>Solution</b>	Provide the user with the correct device, and ensure that it is this device the user is attempting to issue. See the <b>Audit Reporting</b> workflow for further details about the device the user used.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	21645
<b>Text</b>	Unsuitable Device
<b>Details</b>	Issuing the current device has been prevented because the device is unsuitable.
<b>Solution</b>	It may be that a virtual smart card was selected for a credential profile that is restricted to physical smart cards, or that the inserted smart card does not support a data model assigned to the credential profile. Check that the selected credential profile is suitable for the device the user is trying to issue. See the <b>Audit Reporting</b> workflow for further details.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	21646
<b>Text</b>	Job Invalid
<b>Details</b>	Issuing the current device has been prevented because the request is in an invalid state. Repeating the issuance may help. See the <b>Audit Reporting</b> workflow for further details.
<b>Solution</b>	Canceling the job in the Job Management workflow and repeating the issuance process should resolve this. If it does not, see the <b>Audit Reporting</b> workflow for further details as to the cause.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	21647
<b>Text</b>	Not Imported
<b>Details</b>	The issuance requires that the device being issued has already been imported into the system. The presented device is unknown to the system.
<b>Solution</b>	The user may be attempting to issue the credentials to a foreign card. Check that device the user is attempting to issue to. Details of the device can be found in the <b>Audit Reporting</b> workflow.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	21648
<b>Text</b>	GUID is not valid.
<b>Details</b>	The GUID for the provisioning job has been corrupted.
<b>Solution</b>	Check the email template is sending it correctly. Details can be found in the mobile documentation. If the provisioning was using a Derived Credential kiosk, try scanning the code again. If this fails, contact Intercede Support.
<b>Relates To</b>	Identity Agent Provisioning

<b>Error Code</b>	21776
<b>Text</b>	Authentication is required to continue. Your card's issuance profile is not configured to require one.
<b>Details</b>	Self-service credential activation must be configured to require at least one form of authentication. If none are configured, any attempt to self activate the credential will be blocked.
<b>Solution</b>	Authentication requirements can be configured in the <b>Credential Profiles</b> workflow.
<b>Relates To</b>	Credential Issuance



<b>Error Code</b>	21777
<b>Text</b>	This job can not be collected as a self-service operation as it requires countersigning.
<b>Details</b>	You have attempted a self-service collection of a job that requires another operator to be present for countersigning.
<b>Solution</b>	Select a different job, or ask an operator to collect the job with the assistance of a another operator to countersign.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	30021
<b>Text</b>	Adjudication requires fingerprint samples captured using a 10-Slap enrollment device. Check that you have captured new fingerprints before submitting for adjudication
<b>Details</b>	<p>Pending biometric samples that were captured using a 10-Slap enrollment device could not be found for the person.</p> <p>This error may also occur if the <b>Fingerprints identification check enabled</b> configuration option (on the <b>Biometrics</b> page of the <b>Operation Settings</b> workflow) is not set.</p>
<b>Solution</b>	Ensure that the person has pending biometric samples that were captured using a 10-Slap enrollment device, then try the action again.
<b>Relates To</b>	Adjudication

<b>Error Code</b>	50038
<b>Text</b>	The selected credential profile is not allowed because the person that requested the job was not allowed to request this credential profile.
<b>Details</b>	Validation failed because the operator does not have the correct permissions to make a request with the selected credential profile.
<b>Solution</b>	<p>Try another credential profile for which the operator does have permission to create requests, or grant the operator permissions to use the credential profile. Permissions are set in the <b>Credential Profiles</b> workflow in MyID Desktop.</p> <p>See the <i>Working with credential profiles</i> section in the <a href="#">Administration Guide</a> for further details.</p>
<b>Relates To</b>	Adjudication

<b>Error Code</b>	50039
<b>Text</b>	You cannot action your own adjudications.
<b>Details</b>	MyID prevents an operator from carrying out actions on their own adjudications.
<b>Solution</b>	Ask another operator who has the correct permissions to carry out the required actions on the adjudication for your account.
<b>Relates To</b>	Adjudication

<b>Error Code</b>	50041
<b>Text</b>	This action cannot be performed because the user has outstanding adjudications.
<b>Details</b>	MyID prevents you from carrying out this action on people who have outstanding adjudications.
<b>Solution</b>	Ensure that the person has adjudication records that have decision statuses that are either "Approved" or "Not Required".
<b>Relates To</b>	Adjudication

<b>Error Code</b>	50042
<b>Text</b>	External adjudication server has not been configured
<b>Details</b>	You must configure the connection to the adjudication system before you can carry out adjudication actions.
<b>Solution</b>	Use the External Systems workflow to create an external system entry for the adjudication server. See the <i>Adjudication Integration Guide</i> for details.
<b>Relates To</b>	Adjudication

<b>Error Code</b>	82369
<b>Text</b>	The capacity limit has been reached for the system.
<b>Details</b>	The action would exceed the current license capacity.
<b>Solution</b>	Cancel existing users or devices or obtain additional licenses.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	82373
<b>Text</b>	You are unable to request a replacement card, please contact your administrator.
<b>Details</b>	An attempt to request a replacement card failed. This could be due to the credential profile having prerequisite data requirements that the user doesn't fulfill.
<b>Solution</b>	Check that the user meets all the requirements of the credential profile.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	82450
<b>Text</b>	Invalid auth code for the specified job.
<b>Details</b>	The presented authentication code is incorrect.
<b>Solution</b>	Check that the code was entered correctly. The input device may have caps lock enabled, or be set to an incorrect region. A new authentication code can be requested using the <b>Request Auth Code</b> workflow.
<b>Relates To</b>	Authentication

<b>Error Code</b>	82452
<b>Text</b>	SAM Account not found
<b>Details</b>	There has been a problem identifying the user's Windows credentials.
<b>Solution</b>	Retry the current process. If the problem persists, and there have been no changes to the network infrastructure, contact Intercede Support.
<b>Relates To</b>	Authentication

<b>Error Code</b>	82501
<b>Text</b>	The specified mobile does not have any issued devices.
<b>Details</b>	A request has been attempted to replace an Identity Agent device that contains no valid keystores. This attempt has been blocked.
<b>Solution</b>	The Identity agent device is in an errored state and should be re-issued. Use the <b>Cancel Credential</b> and <b>Request ID</b> workflows to achieve this. If the problem persists, contact Intercede Support.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	82502
<b>Text</b>	Only Identity Agent mobiles are supported.
<b>Details</b>	A request has been attempted to replace a non-Identity Agent in a workflow specifically intended for Identity Agent devices. This attempt has been blocked.
<b>Solution</b>	Non-Identity Agent devices can be canceled using the <b>Request Replacement Card</b> workflow.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	85080
<b>Text</b>	Open Platform Keys are not defined for this device
<b>Details</b>	This usually occurs when a configured GlobalPlatform keyset cannot be found in the database, or a keyset has not been configured.
<b>Solution</b>	Ensure GlobalPlatform keys are correctly configured for the device being issued.
<b>Relates To</b>	Global Platform Security

<b>Error Code</b>	85118
<b>Text</b>	The 9B key for this device has not been configured or has been configured incorrectly. This needs to be corrected before issuance can continue.
<b>Details</b>	The 9B key for this device has not been configured or has been configured incorrectly.
<b>Solution</b>	The 9B key can be configured using the <b>Key Management</b> workflow.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	85119
<b>Text</b>	The 9B key specified for this device are incorrect. This needs to be corrected before issuance can continue
<b>Details</b>	The 9B key for this device has not been configured or has been configured incorrectly.
<b>Solution</b>	The 9B key can be configured using the <b>Key Management</b> workflow.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	85120
<b>Text</b>	The 9B key specified for this device are incorrect. This needs to be corrected before issuance can continue
<b>Details</b>	The 9B key for this device has not been configured or has been configured incorrectly.
<b>Solution</b>	The 9B key can be configured using the <b>Key Management</b> workflow.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	85121
<b>Text</b>	The 9B key specified for this device are incorrect. Please ensure that the correct Encryption Type has been selected. This needs to be corrected before issuance can continue
<b>Details</b>	The 9B key for this device has not been configured or has been configured incorrectly.
<b>Solution</b>	The 9B key can be configured using the <b>Key Management</b> workflow.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	85122
<b>Text</b>	The GlobalPlatform keys for this card are missing or incorrect. These need to be corrected before issuance can continue
<b>Details</b>	The GlobalPlatform keys for this device have not been configured or have been configured incorrectly.
<b>Solution</b>	The GlobalPlatform keys can be configured using the <b>Manage Global Platform Keys</b> workflow.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	85123
<b>Text</b>	The GlobalPlatform keys for this card are missing or incorrect. Please verify the key version. These need to be corrected before issuance can continue
<b>Details</b>	The GlobalPlatform keys for this device have not been configured or have been configured incorrectly.
<b>Solution</b>	The GlobalPlatform keys can be configured using the <b>Manage Global Platform Keys</b> workflow.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	85124
<b>Text</b>	There is no CHUID signing certificate configured. Please consult the product documentation
<b>Details</b>	The CHUID signing certificate for this device has not been configured or has been configured incorrectly.
<b>Solution</b>	The certificate location is configured in the Registry of the Application server.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	85125
<b>Text</b>	The private key for the CHUID signing certificate is not available. Please consult the product documentation
<b>Details</b>	The CHUID signing certificate for this device has been configured incorrectly.
<b>Solution</b>	The certificate location is configured in the Registry of the Application server.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	85126
<b>Text</b>	The FASCN is invalid. Card issuance can not continue
<b>Details</b>	The system has attempted to generate an identifier for the user and failed. This is usually a PIV compliant FASCN
<b>Solution</b>	If a FASCN is expected, the user lacks mandatory data. Please enroll the user again. Details of the missing data will be highlighted in the Audit Report. If a FASCN is not required, change the node BuildFASCN from 1 to 0 in the relevant CardProperties file.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	85127
<b>Text</b>	Some of the data provided is invalid. This could either be attributes of the Applicant or the Agency. Please review the details.
<b>Details</b>	The system has attempted to generate an identifier for the user and failed. This is usually a PIV compliant FASCN
<b>Solution</b>	If a FASCN is expected, the user lacks mandatory data. Please enroll the user again. Details of the missing data will be highlighted in the Audit Report. If a FASCN is not required, change the node BuildFASCN from 1 to 0 in the relevant CardProperties file.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	85128
<b>Text</b>	The user's biometrics are not valid. Please check server version
<b>Details</b>	The system has attempted to write biometric data to a card, but the biometric data is invalid.
<b>Solution</b>	Please enroll the user again. Details for each supported biometric matching library are available with this release. If the problem persists, contact Intercede Support.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	85143
<b>Text</b>	The card is locked and requires activation.
<b>Details</b>	The system has attempted to write to a locked device
<b>Solution</b>	Activate the device using either the <b>Activate Card</b> process, or <b>Assisted Activation</b> workflow. Alternatively, if the card is no longer required, use the <b>Erase Card</b> workflow to unlock and erase the device.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	85167
<b>Text</b>	The key for this device has not been configured or has been configured incorrectly. This needs to be corrected before issuance can continue
<b>Details</b>	The 9B key for this device has not been configured or has been configured incorrectly.
<b>Solution</b>	The 9B key can be configured using the <b>Key Management</b> workflow.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	85182
<b>Text</b>	The Global Platform keys for this card are missing or incorrect. These need to be corrected before issuance can continue.
<b>Details</b>	The Global Platform keys for this device have not been configured or have been configured incorrectly.
<b>Solution</b>	The Global Platform keys can be configured using the <b>Manage Global Platform Keys</b> workflow.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	85184
<b>Text</b>	Could not determine Windows logon credentials.
<b>Details</b>	MyID is attempting to determine the Windows logon name for the connected user, but is failing to do so.
<b>Solution</b>	<p>Ensure the client and the server are in the same Windows Domain</p> <p>Run the following script on the web server to enable IIS to determine the identity of the connecting client:</p> <pre>ConfigureWindowsAuthentication.ps1</pre> <p>This script is installed to the <code>Utilities</code> folder on the MyID web server; by default, this is:</p> <pre>C:\Program Files\Intercede\MyID\Utilities\</pre>
<b>Relates To</b>	Update My Device

<b>Error Code</b>	85187
<b>Text</b>	There has been a problem updating your account.
<b>Details</b>	MyID has encountered an error performing the User Sync action during the Update My Device workflow.
<b>Solution</b>	<p>Further details about the specific error are available in the Audit Reports workflow.</p> <p>Common causes include requesting a credential profile that the user does not have permissions to receive, and requesting a credential profile that does not exist.</p>
<b>Relates To</b>	Update My Device

<b>Error Code</b>	85188
<b>Text</b>	Unable to connect to the authentication server
<b>Details</b>	An attempt by the Process Driver web service to connect to the authentication server web service failed
<b>Solution</b>	<p>This error may occur if you are using a load balancer or have multiple web servers.</p> <p>In this case, carry out the following:</p> <ol style="list-style-type: none"><li>1. Set the <code>IssuerUri</code> option in the <code>web.oauth2</code> application settings file. See the <i>Setting the issuer in web.oauth2</i> section in the <a href="#">MyID Operator Client</a> guide.</li><li>2. Configure a shared JWT signing key so that all instances of <code>web.oauth2</code> use the same signing key. See the <i>Load balancing</i> section in the <a href="#">MyID Operator Client</a> guide.  Instead of setting the shared JWT signing key, as an alternative you can set the <code>AuthServerUrl</code> option in the <code>ProcessDriver myid.config</code> file; see the <i>MyID Operator Client pass-through authentication with a load balancer</i> section in the <a href="#">MyID Operator Client</a> guide.</li></ol>
<b>Relates To</b>	Authentication

<b>Error Code</b>	410039
<b>Text</b>	Authentication Failed
<b>Details</b>	The data supplied to Logon either contained invalid data, or was missing essential data.
<b>Solution</b>	Further details will be available in the <b>Audit Reporting</b> workflow.
<b>Relates To</b>	Authentication



<b>Error Code</b>	410072
<b>Text</b>	You cannot collect this device because your original device has expired.
<b>Details</b>	A renewal cannot be collected because the device has expired.
<b>Solution</b>	Cancel the credential and issue a new one, or use the <b>Request Replacement Credential</b> workflow to request a replacement credential.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	410073
<b>Text</b>	Event not found
<b>Details</b>	An Identity Agent Provisioning job is missing or has an invalid status.
<b>Solution</b>	Retry the current process. If the problem persists, and there have been no changes to the network infrastructure, contact Intercede Support.
<b>Relates To</b>	Identity Agent Provisioning

<b>Error Code</b>	410074
<b>Text</b>	Job is invalid
<b>Details</b>	An Identity Agent Provisioning job has an invalid status.
<b>Solution</b>	Retry the current process. If the problem persists, and there have been no changes to the network infrastructure, contact Intercede Support.
<b>Relates To</b>	Identity Agent Provisioning

<b>Error Code</b>	410076
<b>Text</b>	The specified DN is not valid.
<b>Details</b>	The DN for the user is not in a valid format and cannot be processed.
<b>Solution</b>	If you believe the DN is valid, you can bypass validation by setting <code>ValidateDN</code> to a value of <code>false</code> in the <code>myid.config</code> file, or update the user's DN. See the <i>DN validation</i> section in the <a href="#">Web Service Architecture</a> guide.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	410077
<b>Text</b>	Unable to process the DN.
<b>Details</b>	The DN for the user cannot be processed into a format expected by the certificate authority.
<b>Solution</b>	Update the user's DN.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	420000
<b>Text</b>	User cannot be issued with certificates.
<b>Details</b>	The system is attempting to issue a credential with X509 certificates on it to a user with no Distinguished Name. A Distinguished Name is required for certificate issuance.
<b>Solution</b>	The Distinguished Name can be set using a number of processes. It is set when an account is imported from an LDAP. It is set when a user is assigned to a group or agency. It can be set using Lifecycle API. Ensure that the user has a Distinguished Name set and then retry the process.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	500041
<b>Text</b>	You cannot renew this device at this time.
<b>Details</b>	Cards can only be renewed when they are about to expire. The number of days before expiry is controlled by the configuration flag <code>CARD_RENEWAL_PERIOD</code> . The device has more days remaining than this value.
<b>Solution</b>	Wait until the device is within the renewal period and retry the operation. Alternatively, if the configured period is unsuitable, change the <b>Card Renewal Period</b> option (on the <b>Devices</b> page of the <b>Operation Settings</b> workflow) then retry the process.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	500042
<b>Text</b>	Existing Card found - You can not renew this device
<b>Details</b>	Cards can only be renewed if there are no outstanding credential requests for a user.
<b>Solution</b>	Collect all outstanding requests for the user, then repeat this process. If the requests are not required, they can be canceled using the <b>Job Management</b> workflow. A list of the IDs can be found in the <b>Audit Reporting</b> workflow.
<b>Relates To</b>	PIV Credential Issuance

<b>Error Code</b>	500048
<b>Text</b>	You cannot renew expired devices.
<b>Details</b>	Cards can only be renewed when they are valid. This device has expired.
<b>Solution</b>	Request a replacement credential specifying a reason that is not Renewal.
<b>Relates To</b>	PIV Credential Issuance

<b>Error Code</b>	503000
<b>Text</b>	The system could not generate a unique FASCN for this device
<b>Details</b>	An attempt has been made to issue a PIV-compatible device. There was an error encountered while trying to create the FASCN. The user account may not be in a suitable state to receive a PIV-compatible credential.
<b>Solution</b>	Ensure that the user account has all mandatory fields and that the user is approved for card issuance. If the problem persists, contact customer support.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	503001
<b>Text</b>	The system could not generate a credential number for this person.
<b>Details</b>	An attempt has been made to issue a PIV-compatible device. There was an error encountered while trying to create the Credential Number. The user account may not be in a suitable state to receive a PIV-compatible credential.
<b>Solution</b>	Ensure that the user account has all mandatory fields and that the user is approved for card issuance. If the problem persists, contact customer support.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	503002
<b>Text</b>	Failed to update FASCN or credential number
<b>Details</b>	An attempt has been made to update the FASCN or Credential Number on a user's record, but the logged on user lacks the relevant permissions.
<b>Solution</b>	This is usually caused when multiple PIV compatible cards are requested for a user, then that user collects them using a self service mechanism. If this is a use case that is required, contact Intercede Support for details on how to resolve this issue.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	800528
<b>Text</b>	Biometric logon is not allowed.
<b>Details</b>	An attempt has been made to authenticate with biometrics, and this logon mechanism is not enabled.
<b>Solution</b>	Biometric logon is currently used only for resetting PINs. See the <i>Self-service PIN reset authentication</i> section in the <a href="#">Operator's Guide</a> .
<b>Relates To</b>	Authentication

<b>Error Code</b>	800529
<b>Text</b>	Integrated windows logon is not allowed.
<b>Details</b>	An attempt has been made to authenticate with Windows Integrated authentication, and this logon mechanism is not enabled.
<b>Solution</b>	<p>Logon mechanisms are configured in the <b>Edit Roles</b> workflow. The logon mechanisms that you can use depend on which options you have selected on the <b>Logon Mechanisms</b> page of the <b>Security Settings</b> workflow.</p> <p>See the <i>Logon mechanisms</i> section in the <a href="#">Administration Guide</a> for details.</p>
<b>Relates To</b>	Authentication

<b>Error Code</b>	800530
<b>Text</b>	Token logon is not allowed.
<b>Details</b>	An attempt has been made to authenticate with an OTP token, and this logon mechanism is not enabled.
<b>Solution</b>	<p>Logon mechanisms are configured in the <b>Edit Roles</b> workflow. The logon mechanisms that you can use depend on which options you have selected on the <b>Logon Mechanisms</b> page of the <b>Security Settings</b> workflow.</p> <p>See the <i>Logon mechanisms</i> section in the <a href="#">Administration Guide</a> for details.</p>
<b>Relates To</b>	Authentication

<b>Error Code</b>	800531
<b>Text</b>	Device logon is not allowed.
<b>Details</b>	An attempt has been made to authenticate with credentials stored on a device, and this logon mechanism is not enabled.
<b>Solution</b>	<p>Logon mechanisms are configured in the <b>Edit Roles</b> workflow. The logon mechanisms that you can use depend on which options you have selected on the <b>Logon Mechanisms</b> page of the <b>Security Settings</b> workflow.</p> <p>See the <i>Logon mechanisms</i> section in the <a href="#">Administration Guide</a> for details.</p>
<b>Relates To</b>	Authentication

<b>Error Code</b>	800532
<b>Text</b>	Password logon is not allowed.
<b>Details</b>	An attempt has been made to authenticate with passphrases, and this logon mechanism is not enabled.
<b>Solution</b>	<p>Logon mechanisms are configured in the <b>Edit Roles</b> workflow. The logon mechanisms that you can use depend on which options you have selected on the <b>Logon Mechanisms</b> page of the <b>Security Settings</b> workflow.</p> <p>See the <i>Logon mechanisms</i> section in the <a href="#">Administration Guide</a> for details.</p>
<b>Relates To</b>	Authentication

<b>Error Code</b>	800533
<b>Text</b>	Unknown Device Inserted
<b>Details</b>	A user has attempted a self-service operation with a device that was not issued by the system.
<b>Solution</b>	Issue the user a new device and repeat the process.
<b>Relates To</b>	Biometric Logon

<b>Error Code</b>	800538
<b>Text</b>	Passphrase Logon is not allowed.
<b>Details</b>	An attempt to authenticate to MyID with passphrases whilst passphrase authentication is disabled. This attempt has been blocked.
<b>Solution</b>	Ask the user to authenticate with a device instead of passphrases.
<b>Relates To</b>	Authentication

<b>Error Code</b>	800540
<b>Text</b>	An error occurred attempting to retrieve data from the MyID Server
<b>Details</b>	The system has reported that there are no enabled authentication mechanisms available for self-service operations.
<b>Solution</b>	Contact Intercede Support.
<b>Relates To</b>	PIV Self Service

<b>Error Code</b>	800548
<b>Text</b>	Your card has not been issued and can't be used to logon.
<b>Details</b>	The device that is attempting to logon has not been issued.
<b>Solution</b>	The user may not have collected their issuance job yet. If no issuance job exists, or it has been canceled, a new request can be made using the <b>Request Card</b> workflow.
<b>Relates To</b>	Authentication

<b>Error Code</b>	800549
<b>Text</b>	Your card is disabled and can't be used to logon.
<b>Details</b>	The device that is attempting to logon has been disabled.
<b>Solution</b>	Use the <b>Enable / Disable Credential</b> workflow to enable it. If this is unexpected, see the <b>Audit Reporting</b> workflow for the initial issuance of the device, or the <b>Identify Credential</b> workflow for a history of actions against the device.
<b>Relates To</b>	Authentication

<b>Error Code</b>	800550
<b>Text</b>	You do not have sufficient privileges to perform this operation. Please contact your administrator.
<b>Details</b>	An attempt has been made to start an operation to which you have not been granted permissions.
<b>Solution</b>	Use the <b>Edit Roles</b> workflow to grant the appropriate permissions to the required workflow.
<b>Relates To</b>	All

<b>Error Code</b>	800551
<b>Text</b>	Logon Denied.
<b>Details</b>	An attempt has been made to log in and that attempt has failed.
<b>Solution</b>	<p>Ensure the correct passphrases have been entered. By default passphrases are case sensitive. If the authentication was with a device, ensure the device is enabled.</p> <p>This situation may also occur on an upgraded MyID system where users have SHA1 passwords and the administrator has set the <b>Use Security Phrase algorithm version 2</b> configuration option. In this case, follow the instructions for <i>Upgrading security phrase security</i> in the <a href="#">Installation and Configuration Guide</a>.</p> <p>This error may also occur if the user attempts to log on with an expired smart card or logon code, or attempts to log on with a disabled user account.</p> <p>This error may also occur if you are using Integrated Windows Logon and your system is not configured correctly; for example, if the <code>SystemAccounts.Domain</code> field has not been updated from LDAP.</p> <p>This error may also occur if you have a misconfigured UDL file for database connectivity.</p> <p>This error may also occur if you have attempted to use Integrated Windows Logon with a user in the Active Directory group Protected Users.</p> <p>As this error may have a variety of causes, you are recommended to try using the System Interrogation Utility to investigate further.</p>
<b>Relates To</b>	Authentication

<b>Error Code</b>	800552
<b>Text</b>	You cannot logon using this card.
<b>Details</b>	<p>An attempt has been made to log in with a disabled device. This attempt has been blocked.</p> <p>This may also occur if the card has been issued without MyID Logon capabilities.</p>
<b>Solution</b>	Details of the disabled device can be found in the <b>Audit Reporting</b> workflow. Devices can be enabled using the <b>Enable / Disable Credential</b> workflow.
<b>Relates To</b>	Authentication

<b>Error Code</b>	800554
<b>Text</b>	Activation requires assistance.
<b>Details</b>	The credential profile is set up for assisted activation. You cannot use self-service activation for this device.
<b>Solution</b>	<p>If the device is intended to be activated using a self-service method, you must edit the device's credential profile to allow self collection.</p> <p>If the device is intended to be activated using assisted activation, use the <b>Assisted Activation</b> workflow to activate the device.</p>
<b>Relates To</b>	Authentication

<b>Error Code</b>	800560
<b>Text</b>	Self-Service Unlock not allowed
<b>Details</b>	A self-service PIN reset has been initiated and the instance of the MWS server is not configured to allow self-service operations.
<b>Solution</b>	This applies only to PIV installations.
<b>Relates To</b>	PIV Self Service

<b>Error Code</b>	800564
<b>Text</b>	Self-Service Unlock not allowed
<b>Details</b>	<p>A self-service PIN reset has been initiated and MyID is not configured to allow self-service operations.</p> <p>This error may also occur if the card has been assigned, but not yet issued, and the cardholder attempts to reset the PIN.</p>
<b>Solution</b>	<p>See the <i>Allowing self-service unlocking</i> section in the <a href="#">Operator's Guide</a> for details of setting up your system for self-service unlocking.</p> <p>Make sure the card has been issued before attempting to reset the PIN.</p>
<b>Relates To</b>	Self Service

<b>Error Code</b>	800590
<b>Text</b>	The Certificate Policy is disabled and cannot be issued.
<b>Details</b>	An attempt has been made to issue a disabled certificate policy.
<b>Solution</b>	Select an alternate credential profile that does not contain a disabled certificate policy. This error may occur when attempting to issue a new instance of an unmanaged certificate. Unmanaged certificates should be set for historic recovery only in the <b>Credential Profiles</b> workflow.
<b>Relates To</b>	Credential Issuance



<b>Error Code</b>	800591
<b>Text</b>	The Certificate Policy is Unmanaged and the user has not had a corresponding certificate imported.
<b>Details</b>	<p>An attempt has been made to issue a Credential Profile to a user that contains an unmanaged certificate. The user has no valid imported unmanaged certificates.</p> <p>If the credential profile uses the <b>Use Existing</b> option, check that the unmanaged certificate has not expired; this configuration requires a valid certificate.</p>
<b>Solution</b>	Either issue a different Credential Profile (one without an unmanaged certificate, or, in the case where the certificate has expired, with the <b>Historic Only</b> option selected for the unmanaged certificate, which will not check the expiry date) or upload a valid certificate for the user; you can use the <b>Upload PFX Certificates</b> workflow to upload a certificate.
<b>Relates To</b>	Identity Agent Provisioning

<b>Error Code</b>	800600
<b>Text</b>	iOS OTA Organisation is mandatory
<b>Details</b>	An attempt has been made to issue an iOS device, but the Organisation field has not been configured.
<b>Solution</b>	This can be set in the <b>Operation Settings</b> workflow, under the <b>Certificates</b> tab. See the <i>Setting up iOS OTA provisioning</i> section in the <a href="#">Mobile Identity Management</a> document for details.
<b>Relates To</b>	Identity Agent Provisioning

<b>Error Code</b>	800601
<b>Text</b>	iOS OTA Credential Profile is mandatory
<b>Details</b>	An attempt has been made to issue an iOS device, but the OTA Credential Profile has not been configured.
<b>Solution</b>	This can be set in the <b>Operation Settings</b> workflow, under the <b>Certificates</b> tab. See the <i>Setting up iOS OTA provisioning</i> section in the <a href="#">Mobile Identity Management</a> document for details.
<b>Relates To</b>	Identity Agent Provisioning

<b>Error Code</b>	800602
<b>Text</b>	iOS OTA Credential Profile not found
<b>Details</b>	An attempt has been made to issue an iOS device, but the configured OTA credential profile is either incorrect, or the user lacks permissions to retrieve.
<b>Solution</b>	This can be set in the <b>Operation Settings</b> workflow, under the <b>Certificates</b> tab. The value is case sensitive. See the <i>Setting up iOS OTA provisioning</i> section in the <a href="#">Mobile Identity Management</a> document for details.
<b>Relates To</b>	Identity Agent Provisioning

<b>Error Code</b>	800603
<b>Text</b>	iOS OTA Credential Profile has to be MachineIdentity
<b>Details</b>	An attempt has been made to issue an iOS device using an OTA Credential Profile that is not configured to have the Device Identity capability.
<b>Solution</b>	The credential profile can be modified in the <b>Credential Profiles</b> workflow. See the <i>Setting up iOS OTA provisioning</i> section in the <a href="#">Mobile Identity Management</a> document for details.
<b>Relates To</b>	Identity Agent Provisioning

<b>Error Code</b>	800610
<b>Text</b>	The requested image was not found: {0}
<b>Details</b>	An image that is present in a card layout cannot be found.
<b>Solution</b>	Ensure the value in <b>Image Upload Server</b> on <b>Operation Settings</b> on the <b>Video</b> tab is resolvable by both the client and the server, and is correct. If it is, check to see if the image is actually in the location specified, and restore it if it is not.
<b>Relates To</b>	Identity Agent Provisioning

<b>Error Code</b>	800630
<b>Text</b>	Biometrics are required
<b>Details</b>	An attempt has been made to collect a device update for a credential profile that requires biometric authentication, but the device owner has no credentials enrolled.
<b>Solution</b>	To collect the update, the user must enroll biometrics. Alternatively, configure the credential profile to have a biometric requirement of either <b>Never</b> or <b>Preferred</b> .
<b>Relates To</b>	Authentication

<b>Error Code</b>	800611
<b>Text</b>	The requested image timed out: {0}
<b>Details</b>	There has been a network issue retrieving an image used in a card layout.
<b>Solution</b>	Ensure the value in <b>Image Upload Server</b> on <b>Operation Settings</b> on the <b>Video</b> tab is resolvable by both the client and the server, and is correct. If it is, check to see if the image is actually in the location specified, and restore it if it is not.
<b>Relates To</b>	Identity Agent Provisioning

<b>Error Code</b>	881043
<b>Text</b>	User account is disabled
<b>Details</b>	A user with a disabled account has attempted to perform a security phrase logon to the system. This attempt has been blocked.
<b>Solution</b>	User accounts can be enabled using the <b>Edit Person</b> workflow.
<b>Relates To</b>	Authentication

<b>Error Code</b>	881044
<b>Text</b>	The user account is locked.
<b>Details</b>	<p>A user without security phrases set has attempted to perform a security phrase logon to the system. This attempt has been blocked.</p> <p>This error may also occur if you have attempted to use Integrated Windows Logon, and this has failed (possibly because the user is in the Active Directory group Protected Users, or because the fields <code>SAMAccountName</code> and <code>Domain</code> are not be stored in MyID) and MyID has attempted to fall back to logon with security phrases, which is not configured for use.</p>
<b>Solution</b>	<p>Security phrases can be set either using the <b>Change Security Phrases</b> or <b>Change My Security Phrases</b> workflows.</p> <p>See the <i>Logon using security phrases</i> and <i>Integrated Windows Logon</i> sections in the <a href="#">Administration Guide</a> for details of configuring logon with security phrases and Integrated Windows Logon.</p>
<b>Relates To</b>	Authentication

<b>Error Code</b>	881045
<b>Text</b>	User not found.
<b>Details</b>	The attempt to retrieve a users details, possibly from a connected LDAP system, has failed.
<b>Solution</b>	Check that the user exists in the database. The account may have been removed during a process. If the account is linked to an LDAP, check the LDAP permissions for the MyID system accounts. The <b>Audit Reporting</b> workflow may be able to assist with diagnosing the problem.
<b>Relates To</b>	User Management

<b>Error Code</b>	881046
<b>Text</b>	Biometrics configuration problem
<b>Details</b>	The libraries for biometric matching on the server have failed to load.
<b>Solution</b>	Ensure the software is installed and the correct library selected in the <b>Operation Settings</b> workflow. Details for each supported biometric matching library are available in the integration guides provided with MyID.
<b>Relates To</b>	Authentication

<b>Error Code</b>	881048
<b>Text</b>	User has no devices.
<b>Details</b>	An operation has been initiated to perform an action on a user's credential. The selected user does not have any credentials.
<b>Solution</b>	The user's credentials may have been canceled prior to this operation. Check the <b>Audit Reporting</b> workflow for a history of the user's credentials.
<b>Relates To</b>	Credential Maintenance

<b>Error Code</b>	881055
<b>Text</b>	You have no devices. Please contact your administrator.
<b>Details</b>	The user has requested a self-service operation on a credential they own. They do not have any credentials.
<b>Solution</b>	The user's credentials may have been canceled prior to this operation. Check the <b>Audit Reporting</b> workflow for a history of the user's credentials.
<b>Relates To</b>	Self Service Operations

<b>Error Code</b>	881056
<b>Text</b>	You have no devices that are available for replacement. Please contact your administrator.
<b>Details</b>	The user has requested that a credential they own be replaced. They do not have any credentials.
<b>Solution</b>	The user's credentials may have been canceled prior to this operation. Check the <b>Audit Reporting</b> workflow for a history of the user's credentials.
<b>Relates To</b>	Self Service Operations

<b>Error Code</b>	881057
<b>Text</b>	The user account is locked.
<b>Details</b>	A user with a locked account has attempted to perform a password logon to the system. This attempt has been blocked.
<b>Solution</b>	User accounts can be unlocked using the <b>Unlock Security Phrases</b> workflow.
<b>Relates To</b>	Authentication

<b>Error Code</b>	881058
<b>Text</b>	Target is not approved to issue a Machine Identity.
<b>Details</b>	The credential profile is configured to require that the recipient is approved before issuance can occur.
<b>Solution</b>	For information on approving users, see the <i>Setting the User Data Approved flag</i> section in the <a href="#">Administration Guide</a> . Alternatively, this restriction can be removed using the <b>Credential Profiles</b> workflow.
<b>Relates To</b>	Device Identity Management

<b>Error Code</b>	881059
<b>Text</b>	The user account data must be approved before credentials can be issued or updated. Please contact an Administrator.
<b>Details</b>	The credential profile is configured to require that the recipient is approved before issuance can occur.
<b>Solution</b>	For information on approving users, see the <i>Setting the User Data Approved flag</i> section in the <a href="#">Administration Guide</a> . Alternatively, this restriction can be removed using the <b>Credential Profiles</b> workflow.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	881061
<b>Text</b>	The person has no activate authentication code configured.
<b>Details</b>	An Activation code is required, but there are no activation codes assigned to the user.
<b>Solution</b>	Activation codes can be requested using the <b>Request Auth Code</b> workflow.
<b>Relates To</b>	Authentication

<b>Error Code</b>	881062
<b>Text</b>	The person has no unlock authentication code configured.
<b>Details</b>	An unlock code is required, but there are no unlock codes assigned to the user.
<b>Solution</b>	Unlock codes can be requested using the <b>Request Auth Code</b> workflow.
<b>Relates To</b>	Authentication

<b>Error Code</b>	881063
<b>Text</b>	The person has no logon code configured.
<b>Details</b>	A logon code is required, but there are no logon codes assigned to the user.
<b>Solution</b>	Authentication and Unlock codes can be requested using the <b>Request Auth Code</b> workflow.
<b>Relates To</b>	Authentication

<b>Error Code</b>	881064
<b>Text</b>	User has no Logon Code.
<b>Details</b>	An attempt has been made by a user to perform a Logon Code authentication, but the account has no logon codes assigned to it.
<b>Solution</b>	Logon Codes can only be used once. If new codes are required, the workflow <b>Request Auth Code</b> can be used to handle this. Alternatively, repeat the process.
<b>Relates To</b>	Logon

<b>Error Code</b>	881065
<b>Text</b>	You have insufficient security phrases configured.
<b>Details</b>	An attempt has been made by a user to perform a Passphrase based authentication, but the account has insufficient passphrases to meet the current security setting. Additionally, the user does not have access to the configured workflow allowing them to set additional passphrases.
<b>Solution</b>	If the intent is to allow the user to authenticate, and then set their own passphrases, ensure the user has permissions to <b>Change My Security Phrases</b> then change the <b>Set Security Phrase at Logon</b> option (on the <b>Logon</b> tab of the <b>Security Settings</b> workflow) to 1, 110.
<b>Relates To</b>	Authentication

<b>Error Code</b>	881068
<b>Text</b>	Your authentication code has expired.
<b>Details</b>	The user's authentication code has expired and so they cannot authenticate.
<b>Solution</b>	The user will need to be issued a new authentication code.
<b>Relates To</b>	Authentication

<b>Error Code</b>	881100
<b>Text</b>	Virtual smart card issuance cannot continue
<b>Details</b>	<p>An attempt has been made to issue a virtual smart card on a system but one of the following may apply:</p> <ul style="list-style-type: none"> <li>• Virtual smart card support is disabled on the system.</li> <li>• Attempt to generate the virtual smart card has failed.</li> <li>• The client operating system is not supported for VSCs.</li> </ul>
<b>Solution</b>	<p>To issue the device you must:</p> <ul style="list-style-type: none"> <li>• Enable virtual smart card support in the <b>Operation Settings</b> workflow.</li> <li>• Ensure that the TPM on the device is in a state to allow generation of a virtual smart card.</li> <li>• Make sure the client operating system meets the requirements in the Intercede VSC documentation.</li> <li>• The number of smart cards connected to the device does not exceed the maximum limit of 10.</li> </ul>
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	881101
<b>Text</b>	Credential profile can only be issued to a virtual smart card. Issuance cannot continue.
<b>Details</b>	The selected credential profile can only be issued to a virtual smart card. The user has presented a device that is not a virtual smart card.
<b>Solution</b>	Review your issuance process. Credential profile restrictions can be managed in the <b>Credential Profiles</b> workflow.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	881102
<b>Text</b>	Credential profile cannot be issued to a virtual smart card. Issuance cannot continue.
<b>Details</b>	The selected credential profile cannot be issued to a virtual smart card. The user has presented a virtual smart card.
<b>Solution</b>	Review your issuance process. Credential profile restrictions can be managed in the <b>Credential Profiles</b> workflow.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	881104
<b>Text</b>	There has been an error deleting the virtual smart card.
<b>Details</b>	An attempt to delete a virtual smart card remotely has failed
<b>Solution</b>	Contact Intercede Support.
<b>Relates To</b>	Credential Termination

<b>Error Code</b>	881106
<b>Text</b>	Virtual smart card support is disabled, cancellation cannot continue.
<b>Details</b>	An attempt has been made to cancel a virtual smart card on a system that has virtual smart card support disabled
<b>Solution</b>	To cancel the device you must enable virtual smart card support in the <b>Operation Settings</b> workflow.
<b>Relates To</b>	Credential Termination



<b>Error Code</b>	881117
<b>Text</b>	Virtual smart card creation failed, please contact your administrator.
<b>Details</b>	<p>An attempt has been made to issue a virtual smart card on a system but one of the following may apply:</p> <ul style="list-style-type: none"><li>• Attempt to generate the virtual smart card has failed.</li><li>• The client operating system is not supported for VSCs.</li></ul> <p>See the <b>Audit Report</b> workflow for further details.</p>
<b>Solution</b>	<p>To issue the device you must:</p> <ul style="list-style-type: none"><li>• Make sure that the TPM on the device is in a state to allow generation of a virtual smart card.</li><li>• Make sure the client operating system meets the requirements in the VSC integration guide.</li><li>• Make sure the number of smart cards connected to the device does not exceed the maximum limit of 10.</li></ul>
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	890019
<b>Text</b>	Temporary card profile not found in configuration
<b>Details</b>	A fixed temporary credential profile has been configured, but the configuration references a credential profile that does not exist.
<b>Solution</b>	Use the <b>Operation Settings</b> workflow to ensure that the value specified in the <b>Temporary Credential Profile Name</b> matches the intended temporary credential profile exactly. The match is not case sensitive.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	890020
<b>Text</b>	Insufficient permissions to access card profile.
<b>Details</b>	The system has been configured to use a single, static credential profile for temporary replacement actions, but the user does not have permission to receive it.
<b>Solution</b>	Use the <b>Credential Profiles</b> workflow to configure the roles that are allowed to receive the temporary credential profile.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	890042
<b>Text</b>	This action cannot be performed on your device.
<b>Details</b>	The job about to be actioned is not suitable for the target device, for example, collecting an Identity Agent credential profile onto a smart card.
<b>Solution</b>	Ensure a suitable credential profile has been requested for the user. Details about the credential presented can be found in the <b>Audit Reporting</b> workflow.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	890053
<b>Text</b>	Approval is needed.
<b>Details</b>	An attempt has been made to issue a credential with a request that has not yet been validated.
<b>Solution</b>	Requests can be validated in the <b>Validate Request</b> workflow. Alternatively, if validation is not required, this requirement can be removed in the <b>Credential Profiles</b> workflow. Previous requests made when validation was required will still require validation. These requests can be canceled using the <b>Job Management</b> workflow.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	890054
<b>Text</b>	Action no longer available
<b>Details</b>	An attempt has been made to issue a credential with a request that is not in a valid state. It may be that the request has been suspended or canceled.
<b>Solution</b>	The status of requests can be reviewed using the <b>Job Management</b> workflow.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	890055
<b>Text</b>	You are not authorized to complete this action
<b>Details</b>	An attempt has been made to issue a credential by a user that lacks permission to that credential.
<b>Solution</b>	Credential profile permissions can be managed using the <b>Credential Profiles</b> workflow.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	890100
<b>Text</b>	You have no card profiles available.
<b>Details</b>	There are no suitable credential profiles available to the user.
<b>Solution</b>	Availability of credential profiles can be changed in the <b>Credential Profiles</b> workflow. See the <b>Audit Reporting</b> workflow for further details.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	890110
<b>Text</b>	No suitable credential profiles available.
<b>Details</b>	While attempting to replace the device, no suitable card profiles were found. This is probably due to user permission changes since the initial issuance of the device.
<b>Solution</b>	Permissions can be edited in the <b>Edit Roles</b> workflow. Credential Profile permissions can be edited using the <b>Credential Profiles</b> workflow.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	890467
<b>Text</b>	Unable to authenticate card. Unlocking your own card is not allowed.
<b>Details</b>	An attempt has been made to perform a self-service PIN unlock. The card in question does not have a card authentication certificate in container 5FC101, and so cannot be validated. The process has been blocked
<b>Solution</b>	If the card was issued by this system, then the credential profile needs to be updated to ensure a card authentication certificate is included in the correct container. Any previously issued devices will need to be updated before they can perform self service operations. This can be performed using the <b>Update Card</b> or <b>Request Card Update</b> workflows.
<b>Relates To</b>	PIV Self Service

<b>Error Code</b>	890468
<b>Text</b>	This version has been disabled.
<b>Details</b>	This is usually encountered when attempting to access ProcessDriver with an obsolete client.
<b>Solution</b>	Update the client software to be the latest version. If the problem persists, contact Intercede Support.
<b>Relates To</b>	Authentication

<b>Error Code</b>	890477
<b>Text</b>	Notification creation has failed.
<b>Details</b>	The system attempted to send a notification to another system, but this process has failed.
<b>Solution</b>	The <b>Audit Reporting</b> workflow may be able to assist with diagnosing the problem. If it does not, contact Intercede Support.
<b>Relates To</b>	Notifications

<b>Error Code</b>	890478
<b>Text</b>	An unexpected problem has occurred, please wait a short while then try again.
<b>Details</b>	There has been an underlying error in COM+. It may be that the COM+ settings are invalid, or the service has become unavailable.
<b>Solution</b>	If this is a consistent problem, permissions for the MyID system accounts may have changed. If it is an intermittent problem, the Windows Event Log may offer the cause of the authentication issues.
<b>Relates To</b>	Authentication

<b>Error Code</b>	890480
<b>Text</b>	Unable to register the device.
<b>Details</b>	An attempt to register a Trusted Platform Module with the system has failed.
<b>Solution</b>	The <b>Audit Reporting</b> workflow may be able to assist with diagnosing the problem.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	890482
<b>Text</b>	Invalid response to the Client Action.
<b>Details</b>	The client has responded to the MWS with either a blank or invalid response.
<b>Solution</b>	This is usually caused by an unexpected client side error. The <b>Audit Reporting</b> workflow may be able to assist with diagnosing the problem.
<b>Relates To</b>	All

<b>Error Code</b>	890483
<b>Text</b>	There are no jobs for this device.
<b>Details</b>	An attempt was made to activate a device which does not have a corresponding job.
<b>Solution</b>	The <b>Audit Reporting</b> workflow may be able to assist with diagnosing the problem.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	890488
<b>Text</b>	The card is not issued.
<b>Details</b>	An attempt was made to change the PIN for a credential that was not issued by the system.
<b>Solution</b>	Ensure that the user is using the correct device.
<b>Relates To</b>	Self Service Operations

<b>Error Code</b>	890489
<b>Text</b>	The card is disabled.
<b>Details</b>	An attempt has been made to reset the user PIN for a device that is currently disabled.
<b>Solution</b>	Details of the disabled device can be found in the <b>Audit Reporting</b> workflow. Devices can be enabled using the <b>Enable / Disable Credential</b> workflow.
<b>Relates To</b>	Self Service Operations

<b>Error Code</b>	890490
<b>Text</b>	The card is not recognized or the user does not have permissions to use it.
<b>Details</b>	A device has been selected that the user does not have permissions to view or manipulate.
<b>Solution</b>	Typically, this occurs during self service operations where a process is initiated with one card but, mid process, an alternative card is switched-in. It can also occur when an Auth Code that is tied to a device is used against another device. New authentication codes can be requested from the <b>Request Auth Code</b> workflow.
<b>Relates To</b>	Authentication

<b>Error Code</b>	890491
<b>Text</b>	An unknown error has occurred trying to capture biometrics.
<b>Details</b>	An unexpected error has occurred validating biometric data.
<b>Solution</b>	The <b>System Events</b> log may give further advice.
<b>Relates To</b>	Authentication

<b>Error Code</b>	890493
<b>Text</b>	An unknown error has occurred.
<b>Details</b>	An unexpected low level error has occurred.
<b>Solution</b>	<p>The error is usually caused by low level exceptions being thrown by components. This can be caused by such things as:</p> <ul style="list-style-type: none"><li>• The card layout assigned to the mobile credential profile having an image that was missing from the system.</li><li>• A Content Signer Certificate not being correctly configured on the App Server.</li><li>• Card access failure.</li><li>• Other low level failure conditions.</li></ul> <p>If you experience this error when attempting to issue a smart card set up for OPACITY, see the <i>Troubleshooting OPACITY smart cards</i> section in the <a href="#">Smart Card Integration Guide</a>.</p> <p>If you are attempting to issue a Windows Hello credential, this may be caused by selecting a certificate that is not suitable for Windows Hello. See the <i>Certificate policies</i> section in the <a href="#">Windows Hello for Business</a> guide.</p> <p>Details of the issue will be available in the <b>Audit Reporting</b> and <b>System Events</b> workflows. If the problem persists, contact Intercede Support.</p>
<b>Relates To</b>	All

<b>Error Code</b>	890495
<b>Text</b>	The job specified has not been found or is invalid.
<b>Details</b>	An attempt has been made to access a job, but the details for the job are incorrect.
<b>Solution</b>	Ensure that the job details are valid.
<b>Relates To</b>	All

<b>Error Code</b>	890496
<b>Text</b>	Attempted to execute un-approved command
<b>Details</b>	An unsolicited command has been attempted against a card.
<b>Solution</b>	Stop using the issuing workstation or device immediately and contact Intercede Support.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	890497
<b>Text</b>	Your session has expired, please try again.
<b>Details</b>	The action cannot be completed because the user did not complete the workflow in a reasonable time.
<b>Solution</b>	Ask the user to repeat the action. You can configure the duration using the <b>Task Number Timeout</b> setting on the <b>Process</b> tab of the <b>Security Settings</b> workflow. The default is 30 minutes.
<b>Relates To</b>	All

<b>Error Code</b>	890499
<b>Text</b>	The card profile does not support encryption and therefore can not be used for key recovery
<b>Details</b>	The system was asked to recover a certificate to a device that cannot protect the private key for that certificate. This attempt was blocked.
<b>Solution</b>	Ensure the credential profile is configured correctly. Any device that is to receive an archived certificate must be configured for MyID signing. This is usually a certificate policy of type Signature configured for signing within MyID. If you require further assistance, contact Intercede Support.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	890500
<b>Text</b>	This card does not support biometric match from card.
<b>Details</b>	A request for a derived credential has been made from a card that does not support biometric matching.
<b>Solution</b>	If it is not the intention to perform biometric matching during the request for derived credentials (for example, if you are using VSCs), set the <b>Require fingerprints for derived credentials</b> option to No.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	890501
<b>Text</b>	No Captured Sample
<b>Details</b>	The client has returned no biometric data.
<b>Solution</b>	Ensure that the correct client software is installed and that a suitable biometric capture device is connected to the client.
<b>Relates To</b>	Authentication

<b>Error Code</b>	890502
<b>Text</b>	No Sample From Card
<b>Details</b>	A card that we expected to have biometric data on it does not.
<b>Solution</b>	Canceling and re-issuing the device may help. The <b>Audit Reporting</b> workflow will show whether biometric data was written to the card during issuance.
<b>Relates To</b>	Authentication

<b>Error Code</b>	890503
<b>Text</b>	Security Phrases do not match
<b>Details</b>	The user has entered an incorrect security phrase during credential issuance, so the process has been aborted.
<b>Solution</b>	Repeat the process entering the correct security phrase. Security phrases can be reset either using the <b>Change Security Phrases</b> or <b>Change My Security Phrases</b> workflows.
<b>Relates To</b>	Authentication

<b>Error Code</b>	890504
<b>Text</b>	This device does not support the use of generic encryption keys
<b>Details</b>	This device does not support the use of generic keys for encryption. Issuance cannot continue.
<b>Solution</b>	The selected credential does not support the use of generic keys for encryption. You must select a certificate for encryption in the <b>Credential Profiles</b> workflow.
<b>Relates To</b>	Credential Issuance



<b>Error Code</b>	890505
<b>Text</b>	This device does not support the use of certificates for encryption.
<b>Details</b>	The selected credential does not support the use of certificates for encryption.
<b>Solution</b>	The <b>Credential Profiles</b> workflow can be used to control how a credential authenticates to MyID. Contact Intercede Support for further details.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	890506
<b>Text</b>	This device does not support the use of generic signing keys
<b>Details</b>	The selected credential does not support the use of generic keys for signing. Issuance cannot continue.
<b>Solution</b>	You must select a certificate for signing in the <b>Credential Profiles</b> workflow.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	890507
<b>Text</b>	This device does not support the use of certificates for signing
<b>Details</b>	The selected credential does not support the use of certificates for signing. Issuance cannot continue.
<b>Solution</b>	The <b>Credential Profiles</b> workflow can be used to control how a credential authenticates to MyID. Contact Intercede Support for further details.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	890509
<b>Text</b>	The card cannot hold recovered certificates.
<b>Details</b>	An attempt has been made to recover certificates to a credential that does not support certificate recovery.
<b>Solution</b>	Provide the user with a credential that is capable of recovering certificates. Details of the presented credential can be found in the <b>Audit Reporting</b> workflow.
<b>Relates To</b>	Certificate Recovery

<b>Error Code</b>	890510
<b>Text</b>	PIV: Card recipient not authorized
<b>Details</b>	The selected user is either disabled, or has not been approved for card issuance.
<b>Solution</b>	For information on approving users, see the <i>Setting the User Data Approved flag</i> section in the <a href="#">Administration Guide</a> . Alternatively, this restriction can be removed using the <b>Credential Profiles</b> workflow.
<b>Relates To</b>	Credential Request

<b>Error Code</b>	890511
<b>Text</b>	Insufficient data to issue card
<b>Details</b>	There is insufficient data to either build the FASCN or generate a UUID required for issuing this credential.
<b>Solution</b>	Details of the missing data will be available in the <b>Audit Reporting</b> and <b>System Events</b> workflows. If the problem persists, contact Intercede Support
<b>Relates To</b>	PIV Credential Issuance

<b>Error Code</b>	890512
<b>Text</b>	numberOfAttempts
<b>Details</b>	Biometric validation has been attempted multiple times, and has failed each time. The retry limit has been reached and so the process is aborting.
<b>Solution</b>	If biometric authentication is proving to have a high number of false negatives, the number of retries and the matching threshold can be configured in the <b>Operation Settings</b> workflow. If the problem is restricted to a subset of individuals, those individuals should re-enroll their biometric data.
<b>Relates To</b>	Authentication

<b>Error Code</b>	890513
<b>Text</b>	The captured fingerprints did not match those held on the card.
<b>Details</b>	Validation of a user's fingerprints against the biometric data stored on their card has failed.
<b>Solution</b>	The number of retries and the matching threshold can be configured in the <b>Operation Settings</b> workflow.
<b>Relates To</b>	Authentication

<b>Error Code</b>	890516
<b>Text</b>	Asset was not found in LDAP
<b>Details</b>	The Asset Name reported by the client software does not match an entry in the domain.
<b>Solution</b>	Ensure the workstation is joined to the domain and repeat the process. If the problem persists, contact Intercede Support.
<b>Relates To</b>	Virtual Smart Card Issuance

<b>Error Code</b>	890517
<b>Text</b>	An error occurred when checking the machines DNS
<b>Details</b>	The Asset Name reported by the client software does not match an entry in the domain.
<b>Solution</b>	Ensure the workstation is joined to the domain and repeat the process. Check the DNS entry for the workstation. If the problem persists, contact Intercede Support.
<b>Relates To</b>	Virtual Smart Card Issuance

<b>Error Code</b>	890518
<b>Text</b>	An error occurred when checking the machines DNS
<b>Details</b>	The Asset Name reported by the client software does not match an entry in the domain.
<b>Solution</b>	Ensure the workstation is joined to the domain and repeat the process. Check the DNS entry for the workstation. If the problem persists, contact Intercede Support.
<b>Relates To</b>	Virtual Smart Card Issuance

<b>Error Code</b>	890519
<b>Text</b>	This job is not being collected on the correct asset
<b>Details</b>	An attempt has been made to delete a virtual smart card from an incorrect machine.
<b>Solution</b>	Repeat the process from the correct machine. If the deletion request is no longer required, it can be canceled from the <b>Job Management</b> workflow.
<b>Relates To</b>	Credential Termination

<b>Error Code</b>	890520
<b>Text</b>	There has been an error generating the virtual smart card
<b>Details</b>	There has been an error creating a VSC remotely on the client workstation.
<b>Solution</b>	The <b>Audit Reporting</b> workflow will contain details of the error. Ensure your system is configured for virtual smart card issuance as detailed in the <a href="#">Microsoft VSC Integration Guide</a> , and that the client workstation is joined to the domain.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	890522
<b>Text</b>	There has been an error generating the virtual smart card
<b>Details</b>	There has been an error creating a VSC remotely on the client workstation.
<b>Solution</b>	The <b>Audit Reporting</b> workflow will contain details of the error. Ensure your system is configured for virtual smart card issuance as detailed in the <a href="#">Microsoft VSC Integration Guide</a> , and that the client workstation is joined to the domain.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	890524
<b>Text</b>	Maximum biographic retries exceeded
<b>Details</b>	The user has entered incorrect data too many times and the process has been aborted.
<b>Solution</b>	Retry the process with the correct biographic details. If the problem persists, contact Intercede Support
<b>Relates To</b>	Kiosk Biographic Logon

<b>Error Code</b>	890527
<b>Text</b>	Device not assigned to a user
<b>Details</b>	The current device is expected to be issued, but it is not. The Audit will contain more details.
<b>Solution</b>	The user is probably trying to use a device that has not been issued by MyID. It may be required to issue the user a credential. The <b>Audit Reporting</b> workflow will contain more details about the inserted device.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	890534
<b>Text</b>	The supplied card is not a temporary card
<b>Details</b>	A workflow that requires a temporary credential to be provided to it has had a permanent credential supplied. The workflow is not allowed to interact with this credential and so terminates
<b>Solution</b>	Ensure the correct credential was presented. The <b>Audit Reporting</b> workflow will give details of the presented credential.
<b>Relates To</b>	Credential Lifecycle

<b>Error Code</b>	890535
<b>Text</b>	The supplied card is not assigned to the user
<b>Details</b>	A self-service workflow that requires a temporary credential to be provided to it has had a different user's credential supplied. The workflow is not allowed to interact with this credential and so terminates.
<b>Solution</b>	Ensure the correct credential was presented. The <b>Audit Reporting</b> workflow will give details of the presented credential.
<b>Relates To</b>	Credential Lifecycle

<b>Error Code</b>	890537
<b>Text</b>	The device is unsuitable for the profile specified.
<b>Details</b>	The presented device is not suitable for the selected credential profile.
<b>Solution</b>	Details of why issuance was denied can be found in the <b>Audit Reporting</b> workflow. The usual cause is the device having insufficient space for the configured certificates.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	890540
<b>Text</b>	The content defined in the card profile is not currently supported by this issuance method. Please contact your system administrator
<b>Details</b>	The action being performed is not supported by the client being used. For example, SSA cannot issue credentials with generic signing keys.
<b>Solution</b>	Select an appropriate client to perform the intended action.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	890543
<b>Text</b>	User not logged in
<b>Details</b>	The current session is unauthenticated. This can happen if a client loses its cookie collection mid-process or a process has timed out. It can also happen if using a web farm that is not session aware. The error may also occur when entering an incorrect auth code.
<b>Solution</b>	Retry the current process. If entering an auth code, make sure you have entered the correct auth code (this error may be caused by a person having two auth codes for different purposes and using the wrong one for the current task). The timeout duration can be managed in IIS. If the problem persists, and there have been no changes to the network infrastructure, contact Intercede Support.
<b>Relates To</b>	Authentication

<b>Error Code</b>	890547
<b>Text</b>	No TPM Found
<b>Details</b>	The client workstation has reported that it has no Trusted Platform Module available. A TPM is required to perform Attested Device Identity issuance.
<b>Solution</b>	The client workstation is unsuitable to receive the credentials requested for it. Issuance cannot continue.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	890550
<b>Text</b>	Error with TPM
<b>Details</b>	The client workstation has reported that it has no Endorsement Key Hash available. An Endorsement Key is required to perform Attested Device Identity issuance.
<b>Solution</b>	The client workstation is unsuitable to receive the credentials requested for it. Issuance cannot continue.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	890551
<b>Text</b>	The machine specified has not been registered.
<b>Details</b>	A workstation can only receive an Attested Device Identity if it has been registered beforehand. This workstation has not been registered.
<b>Solution</b>	The workstation may have changed its DNS entry or ID since last being registered. Workstations can be registered using the <b>Register Credential</b> workflow.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	890555
<b>Text</b>	This mobile identity has previously been fully or partially provisioned. To provision it again, the mobile identity must be canceled on the server and a new request made.
<b>Details</b>	The mobile provisioning has got into a state that cannot be recovered from automatically.
<b>Solution</b>	Cancel the device using the <b>Cancel Credential</b> workflow and repeat the issuance process.
<b>Relates To</b>	Identity Agent Provisioning

<b>Error Code</b>	890556
<b>Text</b>	Multiple matches
<b>Details</b>	The mobile provisioning has got into a state that cannot be recovered from automatically. There are multiple outstanding requests and the correct one cannot be determined.
<b>Solution</b>	Cancel the device and repeat the issuance process. The status of jobs can be checked in the <b>Job Management</b> workflow.
<b>Relates To</b>	Identity Agent Provisioning

<b>Error Code</b>	890557
<b>Text</b>	This mobile identity has previously been fully or partially provisioned. To provision it again, the mobile identity must be canceled on the server and a new request made.
<b>Details</b>	An earlier issuance process for this device has previously failed. The system can automatically recover from most fail conditions but some are unrecoverable.
<b>Solution</b>	Cancel the device and repeat the issuance process. The status of jobs can be checked in the <b>Job Management</b> workflow.
<b>Relates To</b>	Identity Agent Provisioning

<b>Error Code</b>	890558
<b>Text</b>	The server has requested more security questions than we can provide.
<b>Details</b>	Server side authentication has failed.
<b>Solution</b>	If this occurs during Identity Agent provisioning, it means the Mobile user has been updated, and the account no longer works.
<b>Relates To</b>	Identity Agent Provisioning

<b>Error Code</b>	890561
<b>Text</b>	Your user account does not have permission to complete the request. Please contact your administrator
<b>Details</b>	The user does not have suitable permissions to complete the issuance process, or does not have access to the Credential Profile being requested.
<b>Solution</b>	If this occurs during the provisioning of a mobile device, the user must have access to <b>Collect My Updates</b> (workflow operation ID 242) for device logon. Permissions can be edited in the <b>Edit Roles</b> workflow. Credential profile permissions can be edited using the <b>Credential Profiles</b> workflow. See the <i>Granting access to the workflows</i> section in the <a href="#">Mobile Identity Management</a> document for details.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	890562
<b>Text</b>	This device cannot be provisioned at this time. The request on the server has expired. You will need to request the provisioning again.
<b>Details</b>	The provisioning job is no longer valid.
<b>Solution</b>	<p>Cancel the device and repeat the issuance process. The status of jobs can be checked in the <b>Job Management</b> workflow.</p> <ul style="list-style-type: none"> <li>• <b>IKB-280 – Misleading error message text for error 890562</b></li> </ul> <p>This error may also occur if you attempt to collect the job before it has been validated, in which case you do not need to cancel the job and repeat the issuance process, but must validate the job and then attempt to collect it again.</p>
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	890564
<b>Text</b>	User is not suitable for certificate issuance
<b>Details</b>	The system is attempting to issue a credential with X509 certificates on it to a user with no Distinguished Name. A Distinguished Name is required for certificate issuance.
<b>Solution</b>	The Distinguished Name can be set using a number of processes. It is set when an account is imported from an LDAP. It is set when a user is assigned to a group or agency. It can be set using Lifecycle API. Ensure that the user has a Distinguished Name set and then retry the process.
<b>Relates To</b>	Credential Issuance



<b>Error Code</b>	890565
<b>Text</b>	There is no suitable card profile
<b>Details</b>	An attempt has been made to issue a MIM-Badge style mobile device, but configuration is incomplete. There are no credential profiles with a suitable configuration
<b>Solution</b>	Create a suitable credential profile. See the <i>Setting up the Identity Agent credential profiles</i> section in the <a href="#">Mobile Identity Management</a> document for details.
<b>Relates To</b>	Identity Agent Issuance

<b>Error Code</b>	890566
<b>Text</b>	This device is not the one specified in the job.
<b>Details</b>	The request is for a different device to the one being presented.
<b>Solution</b>	Either use the correct device, or request a new provisioning for the presented device.
<b>Relates To</b>	Identity Agent Provisioning

<b>Error Code</b>	890568
<b>Text</b>	This device belongs to a different user than the one specified in the job.
<b>Details</b>	The device you are attempting to issue is already allocated to someone else.
<b>Solution</b>	Provide the user with a different device. If the device is a mobile device, you could use the <b>Cancel Credential</b> workflow to disassociate the device with the previous owner. If the device is a smart card, you could use the <b>Cancel Credential</b> or <b>Erase Card</b> workflow to cancel the device. After cancellation, the issuance can be re-attempted.
<b>Relates To</b>	Identity Agent Provisioning

<b>Error Code</b>	890569
<b>Text</b>	This mobile identity has previously been fully or partially provisioned. To provision it again, the mobile identity must be canceled on the server and a new request made.
<b>Details</b>	The mobile provisioning has got into a state that cannot be recovered from automatically.
<b>Solution</b>	Cancel the device and repeat the issuance process.
<b>Relates To</b>	Identity Agent Provisioning

<b>Error Code</b>	890570
<b>Text</b>	The device must be specified to provision this credential profile.
<b>Details</b>	The issuance is restricted to a sub-set of eligible devices. The device being issued is not part of that subset.
<b>Solution</b>	Restrictions are managed in the <b>Credential Profiles</b> workflow.
<b>Relates To</b>	Identity Agent Provisioning

<b>Error Code</b>	890571
<b>Text</b>	This device must be assigned to a user to provision this credential profile.
<b>Details</b>	The issuance is restricted to a sub-set of eligible devices. The device being issued is not part of that subset.
<b>Solution</b>	Restrictions are managed in the <b>Credential Profiles</b> workflow.
<b>Relates To</b>	Identity Agent Provisioning

<b>Error Code</b>	890572
<b>Text</b>	There has been a configuration error. There is insufficient data available to provision this device.
<b>Details</b>	The system has attempted to generate an identifier for the user and failed. This is usually a PIV compliant FASCN.
<b>Solution</b>	If a FASCN is expected, the user lacks mandatory data. Please enroll the user again. Details of the missing data will be highlighted in the Audit Report. If a FASCN is not required, change the node BuildFASCN from 1 to 0 in the relevant CardProperties file.
<b>Relates To</b>	Identity Agent Provisioning

<b>Error Code</b>	890573
<b>Text</b>	The system is at capacity. Issuance cannot continue.
<b>Details</b>	The action would exceed the current license capacity.
<b>Solution</b>	Cancel existing users or devices. Alternatively, obtain additional licenses.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	890574
<b>Text</b>	Your card was issued by an agency that does not allow derived credentials from this kiosk
<b>Details</b>	An attempt was made to request a derived credential from a card issued by an untrusted source. The issuance was blocked.
<b>Solution</b>	The <b>Cards Allowed For Derivation</b> flag in the <b>Operation Settings</b> workflow determines which devices are allowed to request derived credentials. Details of the presented device can be found in the <b>Audit Reporting</b> workflow.
<b>Relates To</b>	Derived Credential Issuance

<b>Error Code</b>	890575
<b>Text</b>	Invalid Credential Profile. Cannot issue new unmanaged certificates.
<b>Details</b>	The credential profile is set to issue a new instance of the "Unmanaged" certificate profile. This is invalid.
<b>Solution</b>	Edit the credential profile to issue "Historic Only" certificates of this policy. This can be performed in the <b>Credential Profiles</b> workflow.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	890578
<b>Text</b>	The mailer component was unable to send the mail to the specified SMTP server
<b>Details</b>	There has been a problem with the email server or settings.
<b>Solution</b>	Verify the SMTP server settings in the <b>External Systems</b> workflow. See the <i>Setting up email</i> section in the <a href="#">Advanced Configuration Guide</a> for details.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	890579
<b>Text</b>	The job specified is being used by another operator.
<b>Details</b>	An attempt has been made to action a job that is currently being actioned by another user of the system. This attempt has been blocked.
<b>Solution</b>	Sometimes this can occur if a session is forcibly closed mid-process and the job re-attempted. If this is the case, the lock should clear within 60 minutes.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	890580
<b>Text</b>	There was a problem generating the Terms and Conditions. This process cannot continue.
<b>Details</b>	The required Terms and Conditions document for the credential issuance could not be created. As such, the issuance has been prevented.
<b>Solution</b>	<p>The usual cause for this is a missing mapped field. This could be either a form element that has not been completed, or a user attribute that has no value.</p> <p>Correct the terms and conditions document in the <code>ServerDocuments</code> table of the database and try again. If the problem persists, contact customer support.</p>
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	890581
<b>Text</b>	User PIN not supported in Batch Process
<b>Details</b>	Credentials that require a manual PIN to be set are not appropriate for batch issuance, and so the issuance of the credential has been prevented.
<b>Solution</b>	Default filters usually prevent these credential profiles from being selectable. Do not remove these filters when selecting jobs. Use <b>Collect Card</b> for jobs that require the User PIN to be chosen.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	890585
<b>Text</b>	Disabled devices cannot sign Terms and Conditions
<b>Details</b>	The workflow requires that Terms and Conditions be signed in order to continue. It is not possible to sign with the presented credential as it is disabled. The workflow will not continue.
<b>Solution</b>	Enable the device and repeat the workflow.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	890586
<b>Text</b>	Disabled users cannot sign Terms and Conditions
<b>Details</b>	The workflow requires that Terms and Conditions be signed in order to continue. It is not possible to sign with the presented credential because the user account associated with it is disabled. The workflow will not continue.
<b>Solution</b>	Enable the user account and repeat the workflow.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	890588
<b>Text</b>	The request has not been approved yet. Try again later.
<b>Details</b>	An attempt has been made to action a job that is awaiting validation.
<b>Solution</b>	If you want to carry out this job, use the <b>Validate Request</b> workflow in MyID Desktop or the <b>Approve Request</b> option in MyID Operator Client to approve it. Otherwise, you can use the <b>Job Management</b> workflow to cancel the job.
<b>Relates To</b>	Identity Agent Provisioning

<b>Error Code</b>	890594
<b>Text</b>	You have no authentication mechanisms that are suitable for this operation.
<b>Details</b>	The user has either no self service authentication mechanisms available, or has failed to authenticate with all of their authentication mechanisms. They cannot perform the desired action.
<b>Solution</b>	<p>If the user has configured authentication mechanisms, repeat the process, passing the correct values. It may be necessary to unlock the user's security phrases.</p> <p>If this error is encountered while attempting a self service unlock operation, it may be because the configuration option <b>Verify fingerprints during card unlock</b> is enabled and the user does not have fingerprints enrolled.</p> <p>For self-service unlock operations using the Self-Service App or the Self-Service Kiosk, this error may also occur if the user does not have a role that has access to the <b>Unlock My Card</b> workflow.</p> <p>If the user has no means to authenticate themselves then the process cannot continue.</p>
<b>Relates To</b>	Authentication

<b>Error Code</b>	890596
<b>Text</b>	Your account is not eligible to receive this credential.
<b>Details</b>	An attempt has been made to collect a credential for a user whose account lacks the required attributes to receive that credential.
<b>Solution</b>	<p>The credential profile selected specifies requisite user data; the user does not have the required attributes populated. Either populate these attributes for the user, or select a credential profile that does not have these requirements.</p> <p>Check the audit, which may contain additional information about the missing attributes.</p>
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	890597
<b>Text</b>	The specified user cannot be found.
<b>Details</b>	The user account identity is determined using either the UPN from the current Windows logon session or the value held in the <code>MYID_USERNAME</code> environment variable but cannot be found within MyID.
<b>Solution</b>	<p>To correct this issue:</p> <ul style="list-style-type: none"><li>• Check that the user account exists in MyID.</li><li>• UPN matching is case-sensitive – check that the value used by Windows matches the case of the stored UPN in MyID.</li><li>• Check that the value in <code>MYID_USERNAME</code> is set to the correct value for the MyID user account.</li></ul> <p>For further details about how a user account is associated to MyID, see the <i>Specifying the target user</i> section in the <a href="#">Web Service Architecture</a> guide.</p>
<b>Relates To</b>	Authentication

<b>Error Code</b>	890599
<b>Text</b>	Failed to detect the Windows Hello reader
<b>Details</b>	Enrollment was reported as completing successfully, but MyID could not detect the Windows Hello device.
<b>Solution</b>	Check the Windows event log. If you have a persistent issue, see the <i>MyID Client Components</i> section in the <a href="#">Configuring Logging</a> guide for information on how to enable MyID client logging for the <code>WHfB</code> component.
<b>Relates To</b>	Windows Hello

<b>Error Code</b>	890600
<b>Text</b>	An unknown error occurred with Windows Hello for Business
<b>Details</b>	This error is unexpected.
<b>Solution</b>	Check the Windows event log. If you have a persistent issue, see the <i>MyID Client Components</i> section in the <a href="#">Configuring Logging</a> guide for information on how to enable MyID client logging for the <code>WHfB</code> component.
<b>Relates To</b>	Windows Hello

<b>Error Code</b>	890601
<b>Text</b>	Cannot perform this operation over a remote desktop connection
<b>Details</b>	Windows Hello for Business is not supported over RDP.
<b>Solution</b>	Make sure you are logged on directly to the PC you want to work with.
<b>Relates To</b>	Windows Hello

<b>Error Code</b>	890700
<b>Text</b>	You cannot reset your Windows Hello PIN using this application.
<b>Details</b>	Resetting a Windows Hello PIN is managed by Windows and may be dependent on Windows Hello group policy configuration.
<b>Solution</b>	Check the Microsoft documentation for details.
<b>Relates To</b>	Windows Hello

<b>Error Code</b>	890701
<b>Text</b>	You cannot change your Windows Hello PIN using this application.
<b>Details</b>	Changing a Windows Hello PIN is managed by Windows and may be dependent on Windows Hello group policy configuration.
<b>Solution</b>	Check the Microsoft documentation for details.
<b>Relates To</b>	Windows Hello

<b>Error Code</b>	890703
<b>Text</b>	The attempt to assign a device has been rejected. The device assignment end date for the group that this person is associated with has passed.
<b>Details</b>	The issuance of the device would place it in a group that has expired.
<b>Solution</b>	Update the group to expire in the future and repeat the collection. See the <i>Controlling license use for groups</i> section in the <a href="#">Administration Guide</a> for details.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	890704
<b>Text</b>	The attempt to assign a device has been rejected. The maximum number of assigned devices for the group that this person is associated with has been exceeded.
<b>Details</b>	The issuance of the device would cause the device limit for the group to be exceeded and so has been prevented.
<b>Solution</b>	Increase the group device limit and repeat the collection. See the <i>Controlling license use for groups</i> section in the <a href="#">Administration Guide</a> for details.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	890800
<b>Text</b>	Token validation failed.
<b>Details</b>	The OAuth2 authentication token passed through from Operator Client to ProcessDriver failed validation.
<b>Solution</b>	See the <i>MyID Operator Client advanced configuration</i> section in the <a href="#">MyID Operator Client</a> guide. The Process Driver log may include additional information on the specific validation check that failed.
<b>Relates To</b>	Authentication

<b>Error Code</b>	890801
<b>Text</b>	Issuer validation failed.
<b>Details</b>	The OAuth2 authentication token passed through from the MyID Operator Client to ProcessDriver failed validation due to an Issuer mismatch.
<b>Solution</b>	See the <i>Setting the issuer for load-balanced systems</i> section in the <a href="#">MyID Operator Client</a> guide.
<b>Relates To</b>	Authentication

<b>Error Code</b>	891014
<b>Text</b>	Your mobile device is not compatible with biometric authentication.
<b>Details</b>	The credential profile you are attempting to collect on a mobile device is configured to require biometric authentication, and the device is not capable of capturing that data.
<b>Solution</b>	If biometric authentication is not required, review the configuration of the credential profile using the <b>Credential Profiles</b> workflow, under Issuance Settings. The global values are editable in the <b>Operation Settings</b> workflow.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	891448
<b>Text</b>	The PIN on this device is not locked. You can only unlock this device when it is locked.
<b>Details</b>	An attempt has been made to unblock the PIN of a device that can only be unblocked when the user PIN is actually locked.
<b>Solution</b>	Enter the PIN incorrectly until the user PIN is blocked, then try again.
<b>Relates To</b>	Credential Issuance



<b>Error Code</b>	891449
<b>Text</b>	The PIN on this device is permanently locked. You will need to cancel and re-issue the device to be able to use it.
<b>Details</b>	An attempt has been made to unblock the PIN of a device that has had its PIN permanently blocked.
<b>Solution</b>	Unblocking the PIN on the device is not possible. To continue to use the device it will need to be canceled and re-issued.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	892001
<b>Text</b>	The MyID license has expired.
<b>Details</b>	The current MyID license has expired and needs to be renewed.
<b>Solution</b>	Run the <b>Licensing</b> workflow to request a new license.
<b>Relates To</b>	Licensing

<b>Error Code</b>	892002
<b>Text</b>	The MyID license is invalid.
<b>Details</b>	There is something wrong with the current MyID license.
<b>Solution</b>	Run the <b>Licensing</b> workflow to request a new license.
<b>Relates To</b>	Licensing

<b>Error Code</b>	892012
<b>Text</b>	This system is not configured to allow issuance of this type of credential. Please contact your administrator.
<b>Details</b>	You have attempted to collect a card, but the system configuration does not allow you to collect it. For example, you may be trying to collect a smart card that requires customer GlobalPlatform keys, but the <b>Enable Customer GlobalPlatform Keys</b> option (on the <b>Device Security</b> tab of the <b>Security Settings</b> workflow) is set to No.
<b>Solution</b>	Check that you have configured your system to issue this type of credential.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	892015
<b>Text</b>	Card update failed due to non-compliance with T&C signing requirements.
<b>Details</b>	The current workflow is incapable of performing the Terms and Conditions step, but system configuration dictates that this step is mandatory for the selected update.
<b>Solution</b>	If Terms and Conditions are required, use an alternative workflow to collect the update or contact Intercede Support. Terms and Conditions requirements can be configured in the <b>Credential Profiles</b> workflow.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	892016
<b>Text</b>	Server authentication not enabled, please contact your administrator.
<b>Details</b>	ProvisionDevice relies on a secure server side authentication process. This process has either not been configured or has been disabled.
<b>Solution</b>	Contact Intercede Support. MyID 9.0 systems may require a patch to enable this feature.
<b>Relates To</b>	Identity Agent Provisioning

<b>Error Code</b>	892021
<b>Text</b>	Finger print biometrics have expired.
<b>Details</b>	The biometrics captured for the user have expired.
<b>Solution</b>	Capture fresh biometrics and try again.
<b>Relates To</b>	Authentication

<b>Error Code</b>	892022
<b>Text</b>	Facial biometrics have expired.
<b>Details</b>	The biometrics captured for the user have expired.
<b>Solution</b>	Capture fresh biometrics and try again.
<b>Relates To</b>	Authentication

<b>Error Code</b>	892023
<b>Text</b>	Iris biometrics have expired.
<b>Details</b>	The biometrics captured for the user have expired.
<b>Solution</b>	Capture fresh biometrics and try again.
<b>Relates To</b>	Authentication

<b>Error Code</b>	892024
<b>Text</b>	Biometrics have expired.
<b>Details</b>	The biometrics captured for the user have expired.
<b>Solution</b>	Capture fresh biometrics and try again.
<b>Relates To</b>	Authentication

<b>Error Code</b>	892025
<b>Text</b>	Facial biometrics have not been found.
<b>Details</b>	There are no facial biometrics for the user.
<b>Solution</b>	Capture fresh biometrics and try again. If there is no requirement for facial biometrics, disable the need for facial biometrics in the credential profile.
<b>Relates To</b>	Authentication

<b>Error Code</b>	892026
<b>Text</b>	The server content signing certificate will expire before the device expires. Please contact your system administrator.
<b>Details</b>	The server content signing certificate will expire before the device expires.
<b>Solution</b>	Issue a new content signing certificate.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	892101
<b>Text</b>	You do not have access to any workflows.
<b>Details</b>	The account that has authenticated does not have access to any workflows available to the client.
<b>Solution</b>	Permissions can be configured in the <b>Edit Roles</b> workflow.
<b>Relates To</b>	Authentication

<b>Error Code</b>	892102
<b>Text</b>	Invalid session.
<b>Details</b>	The content of the data used to perform a logon has become corrupt.
<b>Solution</b>	Restart the client and try again.
<b>Relates To</b>	Authentication

<b>Error Code</b>	892103
<b>Text</b>	The system hasn't been configured to allow PFX files to be issued.
<b>Details</b>	An attempt to issue PFX certificates to an iOS based Identity Agent using Safari has failed
<b>Solution</b>	The account the web service is running as does not have write permissions to the <i>Generated</i> folder on the Web server.
<b>Relates To</b>	Identity Agent Issuance

<b>Error Code</b>	892106
<b>Text</b>	System configuration error
<b>Details</b>	This is usually encountered as soon as the client application loads, and means that the server has been incorrectly configured. For example, the Web Services user does not have permission to activate the COM components.
<b>Solution</b>	Each COM+ application on the MyID application server needs to have the Web_Role enabled in the <b>Security</b> tab. Run the System Interrogation Utility to help you identify the issue; see the <a href="#">System Interrogation Utility</a> guide for details.
<b>Relates To</b>	All

<b>Error Code</b>	892110
<b>Text</b>	Card label mapping is invalid
<b>Details</b>	The <b>Card label mapping</b> setting is not set to a valid attribute.
<b>Solution</b>	Make sure that the attribute is formatted correctly, and that it is valid. This can be checked and changed in the <b>Operation Settings</b> workflow, under the <b>Devices</b> tab. See the <i>Devices page (Operation Settings)</i> section in the <a href="#">Administration Guide</a> for details.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	9007124
<b>Text</b>	Card type must match the card stock
<b>Details</b>	The credential does not match the credential type of the credential stock for the credential profile selected.
<b>Solution</b>	Make sure the credential inserted or selected matches the credential type of the credential stock on the required credential profile.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	9000511
<b>Text</b>	Logon Failed: Incorrect credentials supplied.
<b>Details</b>	An attempt to authenticate to MyID with incorrect credentials was attempted. This attempt has been blocked.
<b>Solution</b>	This is usually due to a user entering incorrect Security Phrases. Security Phrases can be set either using the <b>Change Security Phrases</b> or <b>Change My Security Phrases</b> workflows.
<b>Relates To</b>	Authentication

<b>Error Code</b>	9001004
<b>Text</b>	The terms and conditions signed envelope could not be validated.
<b>Details</b>	The approval of the Terms and Conditions has failed to validate.
<b>Solution</b>	The credential being issued should be canceled. The <b>Audit Reporting</b> workflow may be able to assist with diagnosing the problem.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	9001005
<b>Text</b>	The terms and conditions certificate could not be validated. Note: This error is often only visible via the audit.
<b>Details</b>	Terms and Conditions have been signed with a certificate using MyID Desktop. The validity of that cannot be verified against the CA. This is usually due to a firewall blocking access to the Certificate Revocation List (CRL) from the MyID application server.  The <b>Audit Reporting</b> workflow may be able to assist with diagnosing the problem.
<b>Solution</b>	Configure the application server to allow it to validate certificates issued by the CA. Often this involves granting access to the CRL, or ensuring that the root CA is in the application server's trusted root store.  On a Microsoft CA, you can determine whether the application server can verify the certificate chain using the <code>certutil</code> utility on the application server:  <pre>certutil -f -urlfetch -verify &lt;issuing CA certificate.cer&gt;</pre>
<b>Relates To</b>	Authentication

<b>Error Code</b>	9001400
<b>Text</b>	Access Denied
<b>Details</b>	You have attempted to initiate a workflow you do not have permissions to.
<b>Solution</b>	Permissions can be edited in the <b>Edit Roles</b> workflow.
<b>Relates To</b>	Authentication

<b>Error Code</b>	9002020
<b>Text</b>	Invalid Asset Selected
<b>Details</b>	The identity the connecting client has reported is either blank, or does not match an existing entry in the database.
<b>Solution</b>	Device information can be entered either using the <b>Import Device</b> workflow or using the DWS web service.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	9002021
<b>Text</b>	Failed to add asset
<b>Details</b>	An attempt to add device identity information to the system has failed.
<b>Solution</b>	Check the data is valid and try again. If the problem persists, contact Intercede Support.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	9003348
<b>Text</b>	This card profile requires that the recipient has a photograph captured
<b>Details</b>	The credential profile being issued enforces the user to have a photograph captured.
<b>Solution</b>	Photographs can be captured either using the <b>Edit Person</b> workflow or using Lifecycle API. Alternatively, this requirement can be relaxed in the <b>Credential Profiles</b> workflow.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	9003400
<b>Text</b>	No biometric data captured
<b>Details</b>	The client has returned no biometric data.
<b>Solution</b>	Ensure that the correct client software is installed and that a suitable biometric capture device is connected to the client.
<b>Relates To</b>	Authentication

<b>Error Code</b>	9004028
<b>Text</b>	You do not have permission to access this workflow
<b>Details</b>	An attempt has been made to start a workflow the user does not have permissions to.
<b>Solution</b>	<p>Check that the user has access to the required workflow. Permissions can be edited in the <b>Edit Roles</b> workflow.</p> <p>The user's role must have access to the required workflow, and must also have the appropriate logon method.</p> <p>This error may also occur if a system role has been edited and an essential workflow removed; for example, if you want to carry out self activation processes, the system role "Activation User" must have access to the <b>Activate Card</b> workflow, or to import a PIV card, the Server Credentials role must be given access to the <b>Import from PIV Card</b> operation.</p> <p><b>Note:</b> Any role that you want to receive mobile identities must have the <b>Issue Device</b> option selected in the <b>Cards</b> category in the <b>Edit Roles</b> workflow.</p>
<b>Relates To</b>	Authentication

<b>Error Code</b>	9007084
<b>Text</b>	Operator may not issue this device
<b>Details</b>	An attempt has been made to collect a credential. This issuance was prevented because the operator does not have a suitable role to access this workflow.
<b>Solution</b>	Check that the operator has access to the required credential collection workflow. You can edit permissions in the <b>Edit Roles</b> or the <b>Credential Profiles</b> workflows. The user's role must also have the appropriate logon method.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	9007085
<b>Text</b>	This card cannot be used in its current state
<b>Details</b>	An attempt has been made to issue a credential. This issuance was prevented because the Card Applicant does not have a suitable role to collect this credential.
<b>Solution</b>	The Card Applicant lacks the roles required to receive this credential.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	9007086
<b>Text</b>	This card cannot be used in its current state
<b>Details</b>	An attempt has been made to issue a credential. This issuance was prevented because the Operator requested the job.
<b>Solution</b>	Have a different operator collect the credential
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	9007087
<b>Text</b>	This card cannot be used in its current state
<b>Details</b>	An attempt has been made to issue a credential. This issuance was prevented because you cannot collect your own card in this workflow.
<b>Solution</b>	Have a different operator collect the credential.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	9007088
<b>Text</b>	This card cannot be used in its current state
<b>Details</b>	An attempt has been made to issue a credential. This issuance was prevented because you cannot collect a job that you have validated.
<b>Solution</b>	Have a different operator collect the credential.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	9007089
<b>Text</b>	Card Applicant must have Facial Biometrics captured to continue.
<b>Details</b>	An attempt has been made to issue a credential. This issuance was prevented because the Card Applicant must have Facial Biometrics captured.
<b>Solution</b>	Enroll facial biometrics and try again.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	9007090
<b>Text</b>	This card cannot be used in its current state
<b>Details</b>	An attempt has been made to issue a credential. This issuance was prevented because the Card Applicant must have an image captured to continue.
<b>Solution</b>	Enroll a user photograph and try again.
<b>Relates To</b>	Credential Issuance



<b>Error Code</b>	9007091
<b>Text</b>	This card cannot be used in its current state
<b>Details</b>	An attempt has been made to issue a credential. This issuance was prevented because the Card Applicant must have their user data approved.
<b>Solution</b>	Approve the Card Applicant and try again.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	9007092
<b>Text</b>	This card cannot be used in its current state
<b>Details</b>	An attempt has been made to issue a credential. This issuance was prevented because the Job is configured for bureau issuance.
<b>Solution</b>	This job cannot be issued using MyID. If this is unexpected, contact customer support.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	9007093
<b>Text</b>	This card cannot be used in its current state
<b>Details</b>	An attempt has been made to issue a credential. This issuance was prevented because the card layout specified for this job is no longer valid.
<b>Solution</b>	The job cannot be issued in its current state.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	9007094
<b>Text</b>	This card cannot be used in its current state
<b>Details</b>	An attempt has been made to issue a credential. This issuance was prevented because the expiry date of this card has passed.
<b>Solution</b>	The job cannot be issued. Request a new credential for the user.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	9007095
<b>Text</b>	This card cannot be used in its current state
<b>Details</b>	An attempt has been made to issue a credential. This issuance was prevented because the lifetime of this card will be less than the minimum allowed.
<b>Solution</b>	The job cannot be issued. Request a new credential for the user.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	9007096
<b>Text</b>	This card cannot be used in its current state
<b>Details</b>	An attempt has been made to issue a credential. This issuance was prevented because it is a Virtual Smart Card request. The target device is not compatible with Virtual Smart Card Issuance.
<b>Solution</b>	Collect the job using the self service application on an appropriate machine. If the problem persists, contact customer support.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	9007097
<b>Text</b>	This card cannot be used in its current state
<b>Details</b>	An attempt has been made to issue a credential. This issuance was prevented because the card cannot be used with MyID.
<b>Solution</b>	The card is incompatible with MyID. If this is unexpected, contact customer support.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	9007098
<b>Text</b>	This card cannot be used in its current state
<b>Details</b>	An attempt has been made to issue a credential. This issuance was prevented because the card has been disposed or lost and unable to be reissued.
<b>Solution</b>	Repeat the process with a different device.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	9007099
<b>Text</b>	This card cannot be used in its current state
<b>Details</b>	An attempt has been made to issue a credential. This issuance was prevented because the credential must be issued to a known Serial Number.
<b>Solution</b>	Either use a device that was imported, or modify the credential profile to not require the target card to have been previously imported.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	9007100
<b>Text</b>	This card cannot be used in its current state
<b>Details</b>	An attempt has been made to issue a credential. This issuance was prevented because it must be a known proximity card.
<b>Solution</b>	Either use a device that was imported, or modify the credential profile to not require the target card to have a contactless component that has been previously imported.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	9007101
<b>Text</b>	This card cannot be used in its current state
<b>Details</b>	An attempt has been made to issue a credential. This issuance was prevented because the system is not set up to issue this card.
<b>Solution</b>	The card is incompatible with MyID. If this is unexpected, contact customer support.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	9007102
<b>Text</b>	This card cannot be used in its current state
<b>Details</b>	An attempt has been made to issue a credential. This issuance was prevented because the required biometrics have expired.
<b>Solution</b>	Enroll new biometrics for the applicant and then try again.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	9007103
<b>Text</b>	This card cannot be used in its current state
<b>Details</b>	An attempt has been made to issue a credential. This issuance was prevented because the Card Applicant must have Facial Biometrics captured to receive the credential profile.
<b>Solution</b>	Enroll new facial biometrics for the applicant and then try again. Alternatively edit the credential profile to remove this requirement.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	9007104
<b>Text</b>	This card cannot be used in its current state
<b>Details</b>	An attempt has been made to issue a credential. This issuance was prevented because the Iris biometrics will expire within card lifetime.
<b>Solution</b>	Enroll new iris biometrics for the applicant and then try again.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	9007105
<b>Text</b>	This card cannot be used in its current state
<b>Details</b>	An attempt has been made to issue a credential. This issuance was prevented because the required biometrics have expired.
<b>Solution</b>	Enroll new biometrics for the applicant and then try again.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	9007106
<b>Text</b>	This card cannot be used in its current state
<b>Details</b>	An attempt has been made to issue a credential. This issuance was prevented because the content signer will expire during card lifetime.
<b>Solution</b>	This will prevent all PIV compatible issuance. Issue a new content signing certificate to continue to be able to issue cards.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	9007107
<b>Text</b>	This card cannot be used in its current state
<b>Details</b>	An attempt has been made to issue a credential. This issuance was prevented because the Data Model failed validation.
<b>Solution</b>	If you are using custom data models, the data model you have chosen is invalid. If you are using MyID data models, contact customer support.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	9007108
<b>Text</b>	This card cannot be used in its current state
<b>Details</b>	An attempt has been made to issue a credential. This issuance was prevented because the card does not have GP key available.
<b>Solution</b>	Either configure the keys for this device in the <b>Key Management</b> workflow, or add an exclusion for this device in the <b>Security Settings</b> workflow.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	9007109
<b>Text</b>	This card cannot be used in its current state
<b>Details</b>	An attempt has been made to issue a credential. This issuance was prevented because the device must be a proximity card.
<b>Solution</b>	Present an appropriate device and try again. See the product documentation for supported proximity devices.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	9007110
<b>Text</b>	This card cannot be used in its current state
<b>Details</b>	An attempt has been made to issue a credential. This issuance was prevented because it must be a contact chip card.
<b>Solution</b>	Present an appropriate device and try again. See the product documentation for supported smart cards.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	9007111
<b>Text</b>	This card cannot be used in its current state
<b>Details</b>	An attempt has been made to issue a credential. This issuance was prevented because the job is expecting a different device.
<b>Solution</b>	Use the device specified at the time of the request and try again.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	9007112
<b>Text</b>	This card cannot be used in its current state
<b>Details</b>	An attempt has been made to issue a credential. This issuance was prevented because the device type is inappropriate for the workflow.
<b>Solution</b>	Use an appropriate device and try again. For advice with issuance processes, contact customer support.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	9007137
<b>Text</b>	The job is assigned to a card
<b>Details</b>	Credentials that are assigned to a specific card are not appropriate for batch issuance, and so the issuance of the credential has been prevented.
<b>Solution</b>	Use the <b>Collect Card</b> workflow for jobs that are assigned to a card.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	9007138
<b>Text</b>	Device capacity exceed.
<b>Details</b>	An attempt has been made to issue a credential. This issuance was prevented because the number of certificates that is required to be written the device would have exceeded its capacity.
<b>Solution</b>	Reduce the number of certificates to be written or provide a different device.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	9007146
<b>Text</b>	The content signing certificate has not been configured
<b>Details</b>	An attempt has been made to issue a credential. This issuance was failed because the required content signing certificate has not been configured.
<b>Solution</b>	Configure the content signing certificate.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	9007148
<b>Text</b>	The assisted activation card is assigned to the logged in operator
<b>Details</b>	Operator cannot activate cards that are assigned to themselves.
<b>Solution</b>	Ask another operator to carry out the assisted activation.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	9007150
<b>Text</b>	Credential profile requisite data is not set.
<b>Details</b>	You have attempted to issue a credential to a user who does not pass the requisite data checks set up on the credential profile (for example, if the credential profile is designed for Windows logon, and the user does not have a UPN).
<b>Solution</b>	Ensure that the user has all the requisite data, or change the <b>Requisite User Data</b> criteria in the credential profile.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	9007151
<b>Text</b>	An existing request or device exists with a different exclusive group
<b>Details</b>	You have attempted to collect a request for a device that has an exclusive group specified in its credential profile, but the target of the request already has a device, or a request for a device, that has a different exclusive group. You cannot have devices from different exclusive groups.
<b>Solution</b>	See the <i>Exclusive Group</i> section in the <a href="#">Administration Guide</a> for details.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	9007152
<b>Text</b>	The card suitability check has failed
<b>Details</b>	<p>This error is displayed in the audit trail.</p> <p>The message displayed for this error number depends on the response returned from the card suitability check web service; this may provide a reason why the card is not suitable for use.</p> <p>If the message is "Suitability check failure" then this means that MyID was unable to contact the card suitability check web service.</p>
<b>Solution</b>	See the <i>Using the card suitability service</i> section in the <a href="#">Administration Guide</a> for details.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	9008041
<b>Text</b>	Card was imported and cannot be used for this operation
<b>Details</b>	<p>An attempt is being made to manage a device that was imported into MyID.</p> <p>MyID can only manage devices issued by MyID</p>
<b>Solution</b>	<p>The operation cannot continue. Manage the device on the system that issued it.</p>
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	9008105
<b>Text</b>	The device is not ready for activation
<b>Details</b>	An attempt has been made to activate a device that does not have activation job.
<b>Solution</b>	Ensure that all the pre-activation stages has been completed before attempting to activate the device.
<b>Relates To</b>	Authentication

<b>Error Code</b>	9008106
<b>Text</b>	The device is already activated
<b>Details</b>	An attempt has been made to activate a device that has already been activated.
<b>Solution</b>	Ensure that the correct device has been presented for activation.
<b>Relates To</b>	Authentication

<b>Error Code</b>	9008107
<b>Text</b>	The device has not been configured for activation
<b>Details</b>	An attempt has been made to activate a device that was issued without the requirement for activation.
<b>Solution</b>	Ensure that the correct device has been presented for activation.
<b>Relates To</b>	Authentication

<b>Error Code</b>	9008108
<b>Text</b>	Cannot use device for signing
<b>Details</b>	The device has not been configured to allow the device to be used for signing.
<b>Solution</b>	Provide a suitable device for signing. Alternatively, update the credential profile to support signing and then update the device before trying again.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	9008109
<b>Text</b>	Cannot use device for signing
<b>Details</b>	The device cannot be used for signing as the device has been disabled.
<b>Solution</b>	Enable the device and then try again or present a suitable device for signing.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	9008110
<b>Text</b>	Cannot use device for signing
<b>Details</b>	The device cannot be used for signing as it has been issued to a different user or an activation job is not present.
<b>Solution</b>	Ensure that the correct device is presented for activation.
<b>Relates To</b>	Authentication

<b>Error Code</b>	9008111
<b>Text</b>	Cannot use device for signing
<b>Details</b>	The device cannot be used for signing as the user account has been disabled.
<b>Solution</b>	Re-enable the user account before trying again.
<b>Relates To</b>	Credential Issuance



<b>Error Code</b>	9008113
<b>Text</b>	The device cannot be activated as the device is not pending activation
<b>Details</b>	An attempt has been made to activate a device but failed as the device is not pending activation.
<b>Solution</b>	This may occur if the device is being issued with two stage activation but the first stage has not been completed. Ensure that all the pre-activation stages have been completed before trying again.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	9008114
<b>Text</b>	Update job not available for the device
<b>Details</b>	An attempt has been made to update a device but failed as the update job was not found. This may be due to the update job being deleted or suspended in-between the update job notification and the attempt to collect the updates.
<b>Solution</b>	If the update job has been suspended, unsuspend the job and then try again. Where the update job has been deleted, re-request the update job before trying again.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	9008116
<b>Text</b>	User's fingerprint enrollment data too old
<b>Details</b>	An attempt was made to issue a device but failed as the age of the fingerprint data exceeds the maximum biometric sample age.
<b>Solution</b>	Re-enroll the user's fingerprint before re-issuing the device.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	9008117
<b>Text</b>	User's biometric data too old
<b>Details</b>	An attempt was made to issue a device but failed as the age of the biometric data exceeds the maximum biometric sample age.
<b>Solution</b>	Re-enroll the user's biometrics before re-issuing the device.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	80072002
<b>Text</b>	User has no finger prints
<b>Details</b>	Biometric authentication is required to continue with the process, but the user has no biometrics captured.
<b>Solution</b>	Biometric data can either be captured using the Enroll Applicant workflow, or imported using the Lifecycle API. Alternatively, if biometrics are not required for credential issuance, you can use the <b>Credential Profiles</b> workflow to remove this restriction.
<b>Relates To</b>	Authentication

<b>Error Code</b>	80072003
<b>Text</b>	Unable to create an instance of bio authentication device
<b>Details</b>	The libraries for biometric matching on the server have failed to load.
<b>Solution</b>	Ensure the software is installed and the correct library selected in the <b>Operation Settings</b> workflow. Details for each supported biometric matching library are available in the Integration Guides provided with MyID.
<b>Relates To</b>	Authentication

<b>Error Code</b>	80072101
<b>Text</b>	Device has no Auth Code requested
<b>Details</b>	An authentication code is required, but there are no authentication codes assigned to the device.
<b>Solution</b>	Authentication codes are requested using the <b>Request Auth Code</b> workflow. Alternatively, if they are not required, the need for an authentication code can be controlled using the <b>Credential Profiles</b> workflow.
<b>Relates To</b>	Authentication

<b>Error Code</b>	80072104
<b>Text</b>	Invalid Authentication Code provided. No attempts remaining
<b>Details</b>	An authentication code has been entered incorrectly too many times and the process has been terminated.
<b>Solution</b>	Check that the code was entered correctly. The input device may have caps lock enabled, or be set to an incorrect region. A new authentication code can be requested using the <b>Request Auth Code</b> workflow.
<b>Relates To</b>	Authentication

<b>Error Code</b>	80072105
<b>Text</b>	No Authentication Code available
<b>Details</b>	An authentication code is required, but there are no authentication codes assigned to the device.
<b>Solution</b>	Authentication codes are requested using the <b>Request Auth Code</b> workflow. Alternatively, if they are not required, the need for an authentication code can be controlled using the <b>Credential Profiles</b> workflow.
<b>Relates To</b>	Authentication

<b>Error Code</b>	80072106
<b>Text</b>	Authentication Code error occurred
<b>Details</b>	An error has occurred validating the Authentication Code
<b>Solution</b>	Repeat the process with a new authentication code. If this problem persists, contact Intercede Support.
<b>Relates To</b>	Authentication

<b>Error Code</b>	90200006
<b>Text</b>	Session timed out
<b>Details</b>	The action cannot be completed because the user's session has timed out.
<b>Solution</b>	Ask the user to log into MyID again and repeat the action. The timeout duration can be managed using IIS.
<b>Relates To</b>	All

<b>Error Code</b>	90200052
<b>Text</b>	Invalid OTP.
<b>Details</b>	An incorrect authentication code has been entered too many times while provisioning an Identity Agent, and so the process has been aborted.
<b>Solution</b>	Check that the code was entered correctly. The input device may have caps lock enabled, or be set to an incorrect region. The request can be retried. The authentication code is only invalidated then the process completes.
<b>Relates To</b>	Identity Agent Provisioning

<b>Error Code</b>	90200053
<b>Text</b>	Unable to enroll identity agent.
<b>Details</b>	There has been an error starting the Identity Agent issuance process.
<b>Solution</b>	Check the <b>Audit Reporting</b> workflow for details of the error, and the <i>Troubleshooting</i> section in the <a href="#">Mobile Identity Management</a> document. If the problem persists, contact Intercede Support.
<b>Relates To</b>	Identity Agent Provisioning

<b>Error Code</b>	90200054
<b>Text</b>	The mobile is not the one specified in the job.
<b>Details</b>	A user is attempting to collect an Identity agent provisioning from an incorrect device.
<b>Solution</b>	Either use the correct device, or request an Identity Agent provisioning for the users current phone using the <b>Request ID</b> workflow.
<b>Relates To</b>	Identity Agent Provisioning

<b>Error Code</b>	90200055
<b>Text</b>	The job has already been collected.
<b>Details</b>	The mobile device job you are attempting to collect has already been collected.
<b>Solution</b>	If you are following the link from an email ensure you are not looking at an old email; otherwise, request a new credential.
<b>Relates To</b>	Identity Agent Provisioning

<b>Error Code</b>	90200056
<b>Text</b>	This mobile device has already been issued.
<b>Details</b>	The mobile device job you are attempting to collect is for a device which has already been issued.
<b>Solution</b>	If you want to issue the mobile device again, use <b>Cancel Credentials</b> to cancel the current issuance, then collect the new job.
<b>Relates To</b>	Identity Agent Provisioning

<b>Error Code</b>	90200062
<b>Text</b>	You are not able to collect this credential.
<b>Details</b>	An attempt has been made to request a derived credential for which the user is not permitted or configured correctly.
<b>Solution</b>	The audit will contain additional information regarding the underlying issue. See <i>The audit trail</i> section in the <a href="#">Administration Guide</a> for further details.
<b>Relates To</b>	Derived Credentials

<b>Error Code</b>	90200063
<b>Text</b>	MyID is not configured for this credential profile.
<b>Details</b>	An attempt has been made to request a derived credential for which MyID is not configured correctly.
<b>Solution</b>	<p>Check that the credential profile has been set up correctly.</p> <p>Also, if you are using logon codes (for example, when collecting derived credentials onto a VSC using the Self-Service App), make sure that the <b>Allow Logon Codes</b> configuration option is set to Yes.</p> <p>The audit will contain additional information regarding the underlying issue. See <i>The audit trail</i> section in the <a href="#">Administration Guide</a> for further details.</p>
<b>Relates To</b>	Derived Credentials

<b>Error Code</b>	90200593
<b>Text</b>	Configuration Error: Certificate storage incompatible with device
<b>Details</b>	An attempt has been made to issue a certificate to an unsuitable keystore.
<b>Solution</b>	Use the <b>Certificate Authorities</b> workflow to configure the storage mechanism for the policy that is being issued. Most mobile platforms implement a "software" keystore.
<b>Relates To</b>	Identity Agent Provisioning

<b>Error Code</b>	90200595
<b>Text</b>	An unexpected error has occurred
<b>Details</b>	The credential profile is set up for more historic certificates than the credential can hold.
<b>Solution</b>	Edit the credential profile to reduce the number of historic certificates.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	90202843
<b>Text</b>	Certificate validation failed.
<b>Details</b>	An attempt was made to validate a credentials certificate during a derived credential request. The required certificate was either revoked or missing.
<b>Solution</b>	Full details of the invalid certificate can be found in the <b>Audit Reporting</b> workflow. The credential is not suitable for requesting Derived Credentials.
<b>Relates To</b>	Derived Credential Issuance

<b>Error Code</b>	90202847
<b>Text</b>	User is not valid for issuing a derived credential.
<b>Details</b>	Something about the user makes the account unsuitable for use. It may be that they lack the required PIV extensions in their card, that the agency check has failed or that no suitable credential profiles have been configured.
<b>Solution</b>	Details of the missing data will be available in the <b>Audit Reporting</b> workflow.
<b>Relates To</b>	Authentication

<b>Error Code</b>	90202848
<b>Text</b>	Configuration Error: Archive Certificate Policy does not match an allowed policy
<b>Details</b>	There is a configuration error when attempting to import a certificate as part of a derived credential request. It does not match an available policy.
<b>Solution</b>	Certificate policies are listed in the <b>Certificate Authorities</b> workflow. Contact Intercede Support if further assistance is required to configure this feature.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	90202849
<b>Text</b>	Archived Certificate Import Configuration Error
<b>Details</b>	There is a configuration error when attempting to import a certificate as part of a derived credential request.
<b>Solution</b>	Certificate policies are listed in the <b>Certificate Authorities</b> workflow. Contact Intercede Support if further assistance is required to configure this feature.
<b>Relates To</b>	Credential Issuance

<b>Error Code</b>	90202907
<b>Text</b>	You do not have permissions to cancel this device.
<b>Details</b>	An attempt has been made to cancel a device that the authenticated user does not have control over.
<b>Solution</b>	If it is appropriate for the user to cancel the device, their scope can be changed in the <b>Edit Person</b> workflow.
<b>Relates To</b>	Credential Termination

<b>Error Code</b>	90202908
<b>Text</b>	An asset must be specified.
<b>Details</b>	The current stage requires that an asset was selected in a previous stage. It was not.
<b>Solution</b>	Correct the workflow to include an asset selection stage before the CancelDevice stage and retry the process. For further details, contact Intercede customer support.
<b>Relates To</b>	Credential Termination

<b>Error Code</b>	90300005
<b>Text</b>	You do not have sufficient privileges to perform this operation. Please contact your administrator
<b>Details</b>	The operator is attempting to use a workflow that requires the authentication of the target user. The operator lacks permissions to all authentication mechanisms.
<b>Solution</b>	Use the <b>Edit Roles</b> workflow to assign the operator at least one authentication mechanism for the workflow. If target user authentication is not required, assign the operator the <b>Bypass Authentication</b> item.
<b>Relates To</b>	Authentication

<b>Error Code</b>	99300010
<b>Text</b>	User not found.
<b>Details</b>	An error was encountered importing a user into MyID from an LDAP.
<b>Solution</b>	The <b>System Events</b> workflow may give further advice.
<b>Relates To</b>	Find Person

<b>Error Code</b>	99300102
<b>Text</b>	The type specified is not valid.
<b>Details</b>	A problem has been encountered identifying workflows that are suitable for a chosen object.
<b>Solution</b>	Details of the missing data will be available in the <b>Audit Reporting</b> and <b>System Events</b> workflows. If the problem persists, contact Intercede customer support.
<b>Relates To</b>	Launch Workflow

### 3 MyID Identity Agent error codes

This section contains the list of errors that may occur when using Identity Agent. If an error occurs that is not listed in this table, or a remedy for an error cannot be found, contact customer support, quoting the error number and reference SUP-207.

**Note:** Where the error code or details specify "Identity Agent", this is also applicable for the Identity Agent Framework.

<b>Error Code</b>	IA10001
	IA10002
	IA10003
	IA10004
	IA10005
<b>Text</b>	SOAP request failed
<b>Details</b>	See section <a href="#">3.1</a> , <i>Troubleshooting network connectivity</i> .

<b>Error Code</b>	IA10006
<b>Text</b>	SOAP request failed
<b>Details</b>	<p>This error has occurred during the first communication for the provisioning process to retrieve the PFX.</p> <p>This may be caused by exceeding the configured value for <b>Maximum Session Count</b> – this option determines the number of concurrent mobile issuance and update sessions are allowed by the server. See the <i>Maximum session count</i> section in the <a href="#">Mobile Identity Management</a> document for details.</p> <p>If this error consistently occurs when attempting to provision with Identity Agent, there is most likely a network misconfiguration; for example, with the firewall. In this case, the problem is with accessing the <code>ProcessDriver.asmx</code> service.</p> <p>For intermittent occurrence of this error, see section <a href="#">3.1</a>, <i>Troubleshooting network connectivity</i>.</p>



<b>Error Code</b>	IA10007
	IA10008
	IA10009
	IA10010
	IA10011
	IA10012
	IA10013
	IA10014
	IA10015
<b>Text</b>	SOAP request failed
<b>Details</b>	See section <a href="#">3.1, Troubleshooting network connectivity</a> .

<b>Error Code</b>	IA10016
<b>Text</b>	SOAP request failed
<b>Details</b>	<p>If this error consistently occurs, it may be due to a misconfigured <b>Image Upload Server</b> setting within MyID.</p> <p>Make sure that the value configured in MyID for the <b>Image Upload Server</b> configuration option is resolvable from the server hosting the MyID web services.</p> <p>For more information, see the <i>Configuring the image location</i> section in the <a href="#">Administration Guide</a>.</p> <p>For intermittent occurrence of this error, see section <a href="#">3.1, Troubleshooting network connectivity</a>.</p>

<b>Error Code</b>	IA10017
	IA10018
	IA10019
	IA10020
	IA10021
	IA10022
	IA10023
	IA10024
	IA10025
	IA10026
	IA10027
	IA10028
	IA10029
	IA10030
	IA10031
	IA10032
	IA10033
	IA10034
<b>Text</b>	SOAP request failed
<b>Details</b>	See section <a href="#">3.1, Troubleshooting network connectivity</a> .

<b>Error Code</b>	IA10035
<b>Text</b>	SOAP request failed
<b>Details</b>	<p>This error has occurred when there has been a failure in the communications to report that a certificate has been collected.</p> <p>If this error consistently occurs when attempting to provision with Identity Agent, there is most likely a network misconfiguration; for example, with the firewall. In this case, the problem is with accessing the <code>ProcessCard.asmx</code> service.</p> <p>See also section <a href="#">3.1, Troubleshooting network connectivity</a>.</p>

<b>Error Code</b>	IA10036
	IA10037
	IA10038
	IA10039
	IA10040
	IA10041
	IA10042
	IA10043
	IA10044
<b>Text</b>	SOAP request failed
<b>Details</b>	See section <a href="#">3.1, Troubleshooting network connectivity</a> .

<b>Error Code</b>	IA10046
<b>Text</b>	The root certificate needs to be installed and trusted on the device
<b>Details</b>	Your system is configured for HTTPS, but Identity Agent cannot find the root certificate. Make sure that the root certificate is installed and trusted on the device.

<b>Error Code</b>	IA12001
<b>Text</b>	Pin Blocked
<b>Details</b>	The user's PIN has become blocked. They should follow the unlock workflow for the key store in question.

<b>Error Code</b>	IA12002
<b>Text</b>	Decryption failure
<b>Details</b>	This error may occur during mobile credential issuance when using the MWS web service when you have the <b>Envelope Transport Key Algorithm</b> is set to AES. To resolve the issue, either configure the system for REST-based mobile provisioning (preferred), or change the <b>Envelope Transport Key Algorithm</b> setting to 3DES.

<b>Error Code</b>	IA12011
<b>Text</b>	Failed to install the certificate
<b>Details</b>	A likely cause of this error is when the time on the mobile device is set to before the 'enabled from' time of the certificate. Make sure the time on the mobile device is aligned with the time on the server.

<b>Error Code</b>	IA14001
	IA14002
	IA14003
	IA14004
	IA14005
<b>Text</b>	Failed to open a session to the smart card
<b>Details</b>	If the app is intended to be used with a physical smart card, ensure that a card reader is attached to the mobile device and a smart card correctly inserted.

<b>Error Code</b>	IA15004
<b>Text</b>	The OTP has been entered incorrectly too many times
<b>Details</b>	The user must close the Identity Agent, then click the link in the email to launch the process again.

<b>Error Code</b>	IA15005
<b>Text</b>	The provisioning attempt failed due to an incorrect OTP being provided
<b>Details</b>	The OTP has been entered incorrectly. The user must attempt to provide the OTP again.

<b>Error Code</b>	IA16002
<b>Text</b>	A signing operation has failed
<b>Details</b>	<p>The most likely cause of this error is that the time on the mobile device is set to before the time from which the certificate is enabled.</p> <p>In this case, set the time to the correct value, and the issue disappears.</p>

<b>Error Code</b>	IA17002
<b>Text</b>	Pin Blocked
<b>Details</b>	The user's PIN has become blocked. They should follow the unlock workflow for the key store in question.

<b>Error Code</b>	IA17003
<b>Text</b>	One or more certificates not allowed to be stored on this type of storage device.
<b>Details</b>	The certificate policy configuration on the MyID server does not have the correct hard or soft storage configuration for the device that is collecting the identity. Amend the certificate policy configuration, or collect the identity on a suitable device.

<b>Error Code</b>	IA17004
<b>Text</b>	Failed to write card layout data
<b>Details</b>	The MyID Identity Agent app had a problem when writing the card layout information. A reprovision may be attempted after ensuring that the device has permission and access and enough space on the device to store information.

<b>Error Code</b>	IA17009
<b>Text</b>	User aborted new pin entry
<b>Details</b>	The user canceled the PIN setting dialog during the workflow. The process must be restarted by the user on their mobile and the PIN setting completed without hitting cancel.

<b>Error Code</b>	IA17010
<b>Text</b>	Non-archived certificate request fail
<b>Details</b>	A certificate has failed to issue. Ensure that the Certificate Authority is running and has connectivity to the MyID system. Check the certificate policy configuration on the MyID server for the non-archived certificates in the provisioning profile. Look for problems such as invalid key size.  If the issue cannot be resolved, contact customer support.

<b>Error Code</b>	IA17011
<b>Text</b>	Failed to write certificate
<b>Details</b>	Ensure that at least the following versions of Identity Agent are being used:  iOS – 3.11 Android – 3.11 Windows – 2.10.1

<b>Error Code</b>	IA17012
<b>Text</b>	The user canceled the dialog
<b>Details</b>	The user canceled the dialog during a remote PIN unlock workflow. The user can try again, without canceling the process part way through.

<b>Error Code</b>	IA17014
<b>Text</b>	Pin Blocked
<b>Details</b>	The user's PIN has become blocked. They should follow the unlock workflow for the key store in question.

<b>Error Code</b>	IA17015
<b>Text</b>	Archived certificate creation fail
<b>Details</b>	A certificate has failed to issue. Ensure that the Certificate Authority is running and has connectivity to the MyID system. Check the certificate policy configuration on the MyID server for the archived certificates in the provisioning profile. Look for problems such as invalid key size.

<b>Error Code</b>	IA17016
<b>Text</b>	Failed to verify user pin
<b>Details</b>	The user's PIN could not be verified. The process must be restarted by the user on their mobile and the PIN setting completed without hitting cancel.

<b>Error Code</b>	IA17017
<b>Text</b>	Failed to verify user pin
<b>Details</b>	The user's PIN could not be verified. The process must be restarted by the user on their mobile and the PIN setting completed without hitting cancel.

<b>Error Code</b>	IA17018
<b>Text</b>	Please check the time on your device is correct and try again.
<b>Details</b>	Appears during a provision if there is more than a 10 minute time difference between the mobile device and the MyID web services server.

<b>Error Code</b>	IA17019
<b>Text</b>	Please check the time on your device is correct and try again.
<b>Details</b>	Appears during a renewal if there is more than a 10 minute time difference between the mobile device and the MyID web services server.

<b>Error Code</b>	IA17021
<b>Text</b>	Invalid password algorithm specified.
<b>Details</b>	During the online unlock, the replies to the security questions are encoded with a server-specified algorithm. This error occurs when the required algorithm is not supported by the Identity Agent. To address this issue, check whether a newer version of the Identity Agent is available with additional algorithm support.

<b>Error Code</b>	IA80003
<b>Text</b>	Problem starting provisioning
<b>Details</b>	This error may occur on iOS and Android phones when the job details supplied for a provisioning job are incorrect. Ensure that the supplied server URL matches that of the MyID server.

<b>Error Code</b>	IA80010
<b>Text</b>	Problem initializing the key store
<b>Details</b>	<p>This error may occur on iOS and Android phones when the SOPIN in MyID does not match the SOPIN on the device. If this is the case, use the <b>Remove Identity</b> function from within Identity Agent on the device and then reissue the identity from MyID.</p> <p>This error may also occur if the <b>Envelope Transport Key Algorithm</b> configuration option (on the <b>Server</b> page of the <b>Security Settings</b> workflow) is not set to <b>3DES</b>.</p>

<b>Error Code</b>	IA80020
<b>Text</b>	The correct OTP was not supplied by the user
<b>Details</b>	The user should check that the OTP being used is the one that was communicated to them. If provisioning still cannot be completed then the job should be canceled and a new one raised.

<b>Error Code</b>	REST001
<b>Text</b>	The network has failed, please check connectivity
<b>Details</b>	The mobile device is unable to connect reliably to the MyID Server. Check the device's Wi-Fi connection is operating normally; alternatively, if using cellular mobile data, check you are not in an area with poor signal reception.

<b>Error Code</b>	REST002
<b>Text</b>	The user aborted the operation
<b>Details</b>	At some point during provisioning the user selected abort/cancel. If they want to try again, they need to obtain a new provisioning link/QR code for the new attempt.

<b>Error Code</b>	REST003
<b>Text</b>	Failed to get authorization
<b>Details</b>	Trying to get authorization from the MyID Server to perform a provision has not been granted. Try with a different provisioning link/QR code to see if that fixes the issue.

<b>Error Code</b>	REST004
<b>Text</b>	The MyID Server is busy. Please try again later
<b>Details</b>	The provision attempt is valid but the MyID Server is too busy at this time to perform the provisioning. Try again later, at a time when there is less load on the server.

<b>Error Code</b>	REST005
<b>Text</b>	The information provided in the provisioning link is not valid
<b>Details</b>	Acquire a new provisioning link/QR code and attempt to provision with that instead.

<b>Error Code</b>	REST006
<b>Text</b>	The URL is malformed
<b>Details</b>	The server URL specified in the provisioning link/QR code is not valid. Try with a different provisioning link/QR code to see if that fixes the issue.

<b>Error Code</b>	REST007
<b>Text</b>	Unrecoverable error has occurred
<b>Details</b>	<p>The framework/app is unable to continue with the provisioning process. Check the logs to see if troubleshooting information is available.</p> <p>This may occur after failing to collect a REST provision using the authenticator app; subsequent attempts to collect the provision fail with this error. As a workaround, you are recommended to set the <b>Issue over Existing Credential</b> option in the credential profile; if the device is already issued to the target user, it is automatically canceled and then the new device issued.</p>

<b>Error Code</b>	REST008
<b>Text</b>	Unrecoverable error has occurred
<b>Details</b>	The framework/app is unable to continue with the provisioning process. Check the logs to see if troubleshooting information is available.

### 3.1 Troubleshooting network connectivity

To check network connectivity on the mobile device, check your device's Wi-Fi or network carrier settings to ensure that you have connectivity. Use your internet browser to ensure that you can connect to an intranet website. If you had connectivity but the connection was lost,



this was possibly environmental. Ensure you are in a place where the connection is reliable. Turning the device's Wi-Fi connectivity on or off during an operation will likely cause a connectivity issue.

To check that the server's network connectivity is working, try to connect from a different mobile device. If this fails and all clients are failing to connect, follow your process for checking system connectivity and integrity. For example, check that the MyID system is running, that the IIS server is running, the firewall is operating correctly, and any load balancers are correctly configured.

## 3.2 Configuring logging for Identity Agent

Logging is enabled by default. For information on configuring the logging, see the *Setting up logging* section in the [Mobile Identity Management](#) document.

### 3.2.1 Sending logs to the system administrator

The user must have an email account set up on the mobile device.

If an error occurs, you can tap **More Details**, then **Send diagnostic logs**. This allows you to select your email client and send the logs to your system administrator.

Alternatively, to send a log at a later date, you can select **Advanced Options > Logging and Diagnostics**. Select the entry you want to send, then tap **email logs**.

## 4 MyID Windows client error codes

This section contains the list of errors that may occur when using the MyID Windows clients – Desktop, Self-Service App, and Self-Service Kiosk.

<b>Error Code</b>	-2147220729
<b>Text</b>	Incorrect PIN
<b>Details</b>	The incorrect PIN has been entered for the card.
<b>Solution</b>	Retry with the correct PIN.

<b>Error Code</b>	-2147220723
<b>Text</b>	An error occurred logging into the card
<b>Details</b>	<p>The entered PIN is either longer or shorter than is accepted by the card. This error may also occur if you quit the workflow before the workflow has completed.</p> <p>This error may occur if you have attempted to issue an archive ECC certificate to a smart card that does not support that feature. See the <a href="#">Smart Card Integration Guide</a> for details of which features your smart cards support.</p>
<b>Solution</b>	Retry with a different PIN, or: Allow the workflow to complete.

<b>Error Code</b>	-2147220720
<b>Text</b>	An unexpected error has occurred.
<b>Details</b>	<p>This error may occur if the user is required to be logged in to the card, but the user is not logged in. This can occur if you quit the workflow before the workflow has completed.</p> <p>The error may also occur when using OPACITY SPE cards to indicate that the new user PIN was rejected.</p> <p>This error may also occur when attempting to collect an SPE card using a credential profile that has not been set up for OPACITY.</p>
<b>Solution</b>	Retry with a different PIN, or: Allow the workflow to complete.

<b>Error Code</b>	-2147220711
<b>Text</b>	The operation is not supported by this type of smart card
<b>Details</b>	This error occurs when MyID has been unable to issue a certificate.
<b>Solution</b>	This error may occur when attempting to write a certificate to a card that does not support the key length or type specified in the request. Check your credential profile and certificate templates to ensure that you are not attempting to issue, for example, 2048-bit keys to a card that supports on 1024-bit keys, or ECC keys to a card that supports only RSA keys.

<b>Error Code</b>	-2147220685
<b>Text</b>	Attempt to enter an invalid passphrase or PIN.
<b>Details</b>	This error can occur for some cards when attempting to change a PIN and the new PIN is the same as the previous PIN.
<b>Solution</b>	Retry with a different PIN.

<b>Error Code</b>	-2147024865
<b>Text</b>	A device attached to the system is not functioning.
<b>Details</b>	This error can occur for a card if a reader or printer has been removed from the system or has been powered off.
<b>Solution</b>	Do not disconnect the card reader in the middle of card issuance.

<b>Error Code</b>	-2147023779
<b>Text</b>	The request could not be performed because of an I/O device error.
<b>Details</b>	This error can occur if a call to a device has taken an excessively long time, causing the session to the card to time out.
<b>Solution</b>	Check the card reader drivers and retry the operation. If the error continues, try a different card reader.

<b>Error Code</b>	-2146435068
<b>Text</b>	One or more of the supplied parameters could not be properly interpreted.
<b>Details</b>	<p>The most likely reason for this error is:</p> <ul style="list-style-type: none"> <li>Some Smart Cards contain the PIN policy on the card, and if the PIN being supplied does not match this policy this error can occur.</li> </ul>
<b>Solution</b>	<p>There may be a variety of causes for this error. For example:</p> <ul style="list-style-type: none"> <li>Change the credential profile to match the PIN policy of the cards; MyID will then inform the user that it does not meet the PIN policy.</li> <li>Use a PIN that matches the PIN policy of the card.</li> </ul>

<b>Error Code</b>	-2146435038
<b>Text</b>	Smart card does not support the requested feature
<b>Details</b>	A feature was requested that is not supported by the smart card or the CSP.
<b>Solution</b>	<p>This error may occur for a variety of reasons; for example:</p> <ul style="list-style-type: none"> <li>• The certificate template is not supported by the card.</li> <li>• The credential profile is misconfigured for the card.</li> </ul> <p>Check the MyID audit trail for more information.</p>

<b>Error Code</b>	-2146435024
<b>Text</b>	There is no more storage space on the card to continue with this activity
<b>Details</b>	<p>The following are the most likely reasons for this error:</p> <ul style="list-style-type: none"> <li>• Failure to locate a container during issuance due to failure to access the card, <i>or</i>:</li> <li>• Inability to create a container due to no storage space being available.</li> </ul>
<b>Solution</b>	<p>There may be a variety of causes for this error. For example:</p> <ul style="list-style-type: none"> <li>• For physical cards, check that the card is still inserted into the reader.</li> <li>• Check that the credential profile is not attempting to write too many certificates to the card.</li> <li>• Check that too many certificates are not being attempted to be retrieved onto the card.</li> </ul>

<b>Error Code</b>	-2146434966
<b>Text</b>	Unexpected Error
<b>Details</b>	There has been a failure in attempting to change the SOPIN on the card. This may be because the maximum number of PIN attempts have been exceeded.
<b>Solution</b>	Contact your administrator.

<b>Error Code</b>	-2146434965
<b>Text</b>	Device has an unknown Security Officer PIN
<b>Details</b>	There has been a failure in attempting to change the SOPIN on the card. This may be because the maximum number of PIN attempts have been exceeded.
<b>Solution</b>	Contact your administrator.

<b>Error Code</b>	-2146434964
<b>Text</b>	Device has an unknown Security Officer PIN
<b>Details</b>	There has been a failure in attempting to change the SOPIN on the card. This may be because the maximum number of PIN attempts have been exceeded.
<b>Solution</b>	Contact your administrator.

<b>Error Code</b>	-99900045
<b>Text</b>	An unknown error occurred while attempting to log in to the card.
<b>Details</b>	An attempt has been made to log in to the card which has failed. This can occur for physical or virtual cards.
<b>Solution</b>	For physical cards, check that the card is correctly inserted into the reader. For virtual cards, check that the client can access the TPM. Check that the client has not gone into sleep mode.

<b>Error Code</b>	-99900041
<b>Text</b>	Failed to communicate with MyID server. The application will now exit.
<b>Details</b>	<p>The client application has been unable to communicate with the MyID server.</p> <p>This may be caused by failure to validate a signing certificate when accepting terms and conditions text in workflows, where the credential profile requires acceptance to be explicit, silent, or countersigned. This can occur when the CRL of the certificate authority that issued the signing certificate is not accessible.</p> <p>This problem may also be reported as error 9001005; see the entry for this error for further troubleshooting.</p> <p>The audit and system event messages may also indicate failure to validate certificates.</p> <p>If logging has been enabled, the information captured may include the text "The terms and conditions certificate could not be validated".</p>
<b>Solution</b>	<p>Check that your network connection is working between the client and the server.</p> <p>If you have configured logging for the client, the client log may contain more information on the problem; the log message will start with:</p> <pre>WorkflowRunner::Run - WebException thrown:</pre> <p>For information on setting up client logging, see the <i>Windows clients</i> section in the <a href="#">Configuring Logging</a> guide.</p>

<b>Error Code</b>	-99900037
<b>Text</b>	User communication is disabled. Unable to request missing card to be inserted into system. Please contact your system administrator.
<b>Details</b>	The smart card or VSC required cannot be found. This may occur in Self-Service App automation mode when a VSC for which the app is trying to process a lock PIN job has been removed from the PC.
<b>Solution</b>	Make sure the required smart card or VSC is present.

<b>Error Code</b>	-99900033
<b>Text</b>	An unknown error has occurred, contact customer support.
<b>Details</b>	An error has occurred at a low level that has not communicated any further details to the MyID software.
<b>Solution</b>	This error may be caused by a variety of low-level issues. For example, this error has been seen when a Kerberos token bloat issue has occurred, where the Kerberos ticket is too big for IIS to handle.

<b>Error Code</b>	-99900031
<b>Text</b>	Operation does not exist or you do not have access to operation
<b>Details</b>	The application has been launched specifying a workflow that either does not exist or to which the user does not have access.
<b>Solution</b>	Check that the operation ID is a valid number. Check that the user has access to the appropriate workflow.

<b>Error Code</b>	-99900028
<b>Text</b>	There has been an error accessing the Biometric device. Please contact your administrator.
<b>Details</b>	An unknown error has occurred with the biometric device.
<b>Solution</b>	Possible solutions: <ul style="list-style-type: none"><li>• Check the device is supported by your installation and all required software has been installed correctly as described in the MyID integration guide for the device, including required device drivers from the device vendor.</li><li>• Disconnect or disable other biometric or image capture devices that may be conflicting with the fingerprint reader to determine if that resolves the issue.</li><li>• Occasionally issues have been seen when multiple devices are connected to the computer resulting in variable power levels to the reader – check if connecting the device to a different USB port on the computer or disconnecting other devices resolves the issue, or consider using a powered USB hub.</li></ul>

<b>Error Code</b>	-99900020
<b>Text</b>	No biometric device detected
<b>Details</b>	<p>There has been a failure to detect a supported biometric verification device that is required for biometric verification. This can occur if:</p> <ul style="list-style-type: none"> <li>• The required driver or SDK is not installed for the biometric device.</li> <li>• The biometric device is not connected to the client machine.</li> <li>• Insufficient power is being provided to power the biometric device.</li> </ul>
<b>Solution</b>	<p>Ensure that the driver or SDK for the biometric device is installed. See the integration guide for the biometric device.</p> <p>Ensure that the biometric device is connected to the client machine and that sufficient power is being provided to the device.</p>

<b>Error Code</b>	-99900009
<b>Text</b>	An error occurred attempting to retrieve data from the MyID Server
<b>Details</b>	The client application has been unable to communicate with the MyID server.
<b>Solution</b>	<p>Check that your network connection is working between the client and the server.</p> <p>Check the <b>Audit Reporting</b> workflow to see if there is any additional information that may indicate a problem on the server.</p> <p>If you have configured logging for the client, the client log may contain more information on the problem.</p> <p>For information on setting up client logging, see the <i>Windows clients</i> section in the <a href="#">Configuring Logging</a> guide.</p> <p>See also the entry for error -99900041 which may occur in similar circumstances.</p>

<b>Error Code</b>	-99900003
<b>Text</b>	Certificate Issuance
<b>Details</b>	This error occurs when MyID has been unable to issue a certificate.
<b>Solution</b>	<p>This error may occur for a wide variety of reasons. For example:</p> <ul style="list-style-type: none"> <li>• The certificate template is misconfigured.</li> <li>• The certificate service is not running.</li> </ul> <p>Check the MyID audit trail for more information about what has caused the certificates to fail to issue.</p> <p>If you are attempting to issue a Windows Hello credential, this may be caused by selecting a certificate that is not suitable for Windows Hello. See the <i>Certificate policies</i> section in the <a href="#">Windows Hello for Business</a> guide.</p>

<b>Error Code</b>	-9990001
<b>Text</b>	Unable to access MyID
<b>Details</b>	This error occurs when an unexpected problem occurs when attempting to log on to MyID with security questions. May be caused by network problems.
<b>Solution</b>	Check that your network is working correctly and that your MyID servers are running. If problems persist, contact Intercede.

<b>Error Code</b>	128
<b>Text</b>	Failed to verify signature for running application.
<b>Details</b>	This error occurs when a MyID client has been unable to successfully validate component signatures.
<b>Solution</b>	<p>Allow the client access to the internet when it launches – this will give Windows access to the latest CRLs and CAs to perform signature verification.</p> <p>If you cannot give the client access to the internet, add the following configuration to the client configuration file:</p> <pre>&lt;add key="ComponentVerificationSkipRevocationChecks" value="TRUE"&gt;&lt;/add&gt;</pre> <p>to disable revocation checks, which should negate the need for an internet connection. See the installation guide for your client for details. Note that this reduces the integrity of the signature verification, as the client will be unable to determine if any of the certificates in the chain have been revoked since signing occurred – as such, you should ensure that the client's configuration file is modifiable only by users with administrative privileges.</p> <p>If you continue to see this error even with revocation checks disabled, it is likely that you do not have the relevant root certificates installed on your machine. In this instance, you should ensure that the DigiCert root certificates are correctly installed in the Trusted Roots store on your machine; see the <i>Installing the MyID Installation Assistant</i> section in the <a href="#">Installation and Configuration Guide</a>.</p>

<b>Error Code</b>	890583
<b>Text</b>	Failed to delete the credential.
<b>Details</b>	This error may occur when attempting to delete a VSC if the TPM has not recovered from being woken from a sleep state.
<b>Solution</b>	Check the state of the TPM by running <code>tpm.msc</code> (with elevated privilege) to verify that the TPM is available. Restart the device if the TPM is not in available.



<b>Error Code</b>	890606
<b>Text</b>	Microsoft WebView2 Runtime <VERSION> or higher is not installed. Please contact your administrator.
<b>Details</b>	The Microsoft WebView2 Runtime is required to render certain HTML elements, such as terms and conditions documents, but the required version is not installed.
<b>Solution</b>	Install the latest version of the Microsoft WebView2 Runtime. See the <i>Microsoft WebView2 Runtime</i> section in the <a href="#">Installation and Configuration Guide</a> .

<b>Error Code</b>	9007084
<b>Text</b>	Operator does not have the correct roles to collect this job
<b>Details</b>	The credential profile is configured to only allow a limited set of roles to collect the profile. The operator does not have one of these assigned roles.
<b>Solution</b>	Change the operator's roles to an allowed role or reconfigure the credential profile to allow the operator's role.

<b>Error Code</b>	9007137
<b>Text</b>	The job is assigned to a card
<b>Details</b>	This error is displayed in <b>Batch Collect Card</b> when attempting to collect a job that is assigned to a specific card.
<b>Solution</b>	This job should be collected using <b>Collect Card</b> using the card to which it has been assigned.

<b>Error Code</b>	902014
<b>Text</b>	Intel Authenticate configuration check failed.
<b>Details</b>	The client is not correctly configured for Intel Authenticate. MyID support for Intel Authenticate Virtual Smart Cards has now been deprecated. If you are currently using this solution or have further questions about it, contact Intercede for further details quoting SUP-349.
<b>Solution</b>	Check that the client is correctly configured.

<b>Error Code</b>	99900046
<b>Text</b>	Cannot perform this operation over a remote desktop connection.
<b>Details</b>	VSC operations cannot be performed over a remote desktop connection.
<b>Solution</b>	Run the MyID client on a local machine.

<b>Error Code</b>	99900048
<b>Text</b>	Cannot perform this operation over a remote desktop connection.
<b>Details</b>	Non-removable device operations (VSC and Device Identities) cannot be performed over a remote desktop connection.
<b>Solution</b>	Run the MyID client on a local machine.

<b>Error Code</b>	99900049
<b>Text</b>	Cannot perform an Intel Authenticate operation over a remote desktop connection.
<b>Details</b>	Intel Authenticate operations cannot be performed over a remote desktop connection.  MyID support for Intel Authenticate Virtual Smart Cards has now been deprecated. If you are currently using this solution or have further questions about it, contact Intercede for further details quoting SUP-349.
<b>Solution</b>	Run the MyID client on a local machine.

<b>Error Code</b>	99900050
<b>Text</b>	Cannot perform a TPM operation over a remote desktop connection.
<b>Details</b>	TPM operations cannot be performed over a remote desktop connection.
<b>Solution</b>	Run the MyID client on a local machine.

<b>Error Code</b>	0x80094004
<b>Text</b>	The requested property value is empty.
<b>Details</b>	This error occurs when MyID has been unable to issue a certificate.
<b>Solution</b>	This error may occur when attempting to write a certificate to a card that does not support the key length or type specified in the request. Check your credential profile and certificate templates to ensure that you are not attempting to issue, for example, 2048-bit keys to a card that supports on 1024-bit keys, or ECC keys to a card that supports only RSA keys.

## 4.1 Generic errors

You may see an error similar to the following before completing the logon process:

Unable to perform the requested action

If so, check the [Installation and Configuration Guide](#) and make sure that you have configured your system correctly.

In particular, check the following sections:

- *Launch and activation permissions*
- *Web server on a separate machine*
- *MSDTC security configuration*

If you need further diagnostic information, you can set up your MyID Desktop application to write debug information to a log file. For more information, see the *Windows clients* section in the [Configuring Logging](#) guide.

## 5 Printer error codes

This section contains the list of errors that may occur when using printers with MyID.

**Note:** Currently, the error codes are not displayed on-screen for printer error codes.

<b>Error Code</b>	-99910012
<b>Text</b>	The printer failed to read a card. Please contact your system administrator.
<b>Details</b>	MyID requested that the printer load a card, but the printer did not respond to say that the card was loaded within 40 seconds.
<b>Solution</b>	Check that your printer is working correctly.

<b>Error Code</b>	-99910011
<b>Text</b>	The printer failed to print the selected layout. Please contact your system administrator.
<b>Details</b>	There has been a problem with printing the card layout.
<b>Solution</b>	<p>This might be caused by the following:</p> <ul style="list-style-type: none"><li>• A configuration issue. Check that the <b>Image Upload Server</b> option (on the <b>Video</b> tab of the <b>Operation Settings</b> workflow) is pointing at the image upload server and that it is configured correctly.</li><li>• Data error when sending the print data to the printer. Check for any errors being reported by the printer. Check the audit.</li><li>• The printer not supporting a feature required by the print layout; for example, magstripe printing. Check for any errors reported by the printer.</li></ul>

<b>Error Code</b>	-99900044
<b>Text</b>	Moving a card has failed - Please contact your system administrator.
<b>Details</b>	The printer failed to load, move or eject a card.
<b>Solution</b>	Check the printer status panel for additional details. Check for card jams. Restart the printer.

<b>Error Code</b>	-99900043
<b>Text</b>	Unable to move card - Please contact your administrator.
<b>Details</b>	The printer cannot currently load, move or eject a card. If available, additional details from the printer will be shown describing the printer error.
<b>Solution</b>	Follow the instructions on the printer error dialog to resolve the problem. Check for card jams within the printer. Restart the printer.

<b>Error Code</b>	-99900042
<b>Text</b>	Attempting to move a card with no print job in progress. Please contact your administrator.
<b>Details</b>	The MyID client is in an inconsistent internal state.
<b>Solution</b>	Restart the workflow, or restart the client.

<b>Error Code</b>	9009033
<b>Text</b>	No printers have been found.
<b>Details</b>	No printer detected by Windows.
<b>Solution</b>	Connect the required printer and restart the workflow.

<b>Error Code</b>	9009034
<b>Text</b>	The printer is in an unknown state.
<b>Details</b>	<p>This may be as a result of:</p> <ul style="list-style-type: none"><li>• The printer is unable to map its activity to one of the known set of activities.</li><li>• The printer has reported an activity that is not known to MyID.</li></ul>
<b>Solution</b>	<p>This may be a transient issue so wait for issue to clear. Contact the printer manufacturer if the issue persists.</p> <p>The printer has reported an activity that is not known to MyID. Wait for issue to clear. Contact customer support if issue persists.</p>

<b>Error Code</b>	9009035
<b>Text</b>	There has been a connection failure with the printer.
<b>Details</b>	SDK has detected error with the data port or data transmission.
<b>Solution</b>	<p>This may be a transient error due to the printer failing to respond to data transmission.</p> <p>If problem persists check the printer connection.</p> <p>Check if there is an error being reported on the printer front panel and refer to the manufacturer's user guide.</p>

<b>Error Code</b>	9009036
<b>Text</b>	The cover on the printer is open.
<b>Details</b>	Printer cover is open.
<b>Solution</b>	Close the cover and try again.

<b>Error Code</b>	9009037
<b>Text</b>	The printer SDK has not been found.
<b>Details</b>	MyID failed to detect the SDK required for the printer operation.
<b>Solution</b>	Install the printer SDK and try again.

<b>Error Code</b>	9009039
<b>Text</b>	The printer has reported a generic error state.
<b>Details</b>	<p>When the printer is not reporting an error then this may indicate one of the following:</p> <ul style="list-style-type: none"><li>• An error when attempting to send data to the printer.</li><li>• Failure to retrieve the printer status information when the printer is connected.</li><li>• An internal printer error resulting in the printer reporting an unknown error.</li><li>• An exception within the printer adapter.</li></ul>
<b>Solution</b>	<p>Check the printer front panel to determine if the printer is reporting an error. If an error is being reported, refer to the manufacturer's user guide.</p> <p>This may be caused by a transient communication issue so contact customer support if the issue persists.</p>

<b>Error Code</b>	9009040
<b>Text</b>	There is a problem feeding the card into the printer.
<b>Details</b>	Unable to feed a card from the card feeder or move a card between printer internal stations.
<b>Solution</b>	<p>Check the printer and remove any obstructions.</p> <p>Check that the cards have been loaded correctly into the hopper.</p>

<b>Error Code</b>	9009041
<b>Text</b>	There is a problem with the film in the printer.
<b>Details</b>	The printer has detected a film error.
<b>Solution</b>	Check the error being reported on the printer front panel and refer to the manufacturer's user guide.

<b>Error Code</b>	9009042
<b>Text</b>	There is a problem with the hopper in the printer.
<b>Details</b>	The printer is reporting a hopper as empty or full. The printer may report a hopper as full after a preset number of cards have been ejected to the output bin even when the hopper is not actually full.
<b>Solution</b>	<p>If the hopper is empty, add cards and try again.</p> <p>If the printer indicates that an output hopper is full, remove any cards from the output hopper and clear the hopper count using the printer front panel.</p> <p>If the printer is showing any other fault, refer to the manufacturer's user guide.</p>

<b>Error Code</b>	9009043
<b>Text</b>	An unknown error has occurred with the printer that does not fit into any of the predetermined error categories.
<b>Details</b>	The printer is unable to categorize the reported error.
<b>Solution</b>	Check the error being reported on the printer front panel and refer to the manufacturer's user guide.

<b>Error Code</b>	9009044
<b>Text</b>	There is a problem with the laminator in the printer.
<b>Details</b>	The printer has detected a laminator error.
<b>Solution</b>	Check the error being reported on the printer front panel and refer to the manufacturer's user guide.

<b>Error Code</b>	9009045
<b>Text</b>	There has been a problem moving the card in the printer.
<b>Details</b>	There was a failure to move a card between printer internal stations.
<b>Solution</b>	Check the error being reported on the printer front panel and refer to the manufacturer's user guide.

<b>Error Code</b>	9009046
<b>Text</b>	There has been a problem with a Plug-In in the printer.
<b>Details</b>	One or more of the printer board plug-ins have failed.
<b>Solution</b>	Check the error being reported on the printer front panel and refer to the manufacturer's user guide.

<b>Error Code</b>	9009047
<b>Text</b>	The printer is busy.
<b>Details</b>	The printer is performing an operation that prevents it processing the existing job.
<b>Solution</b>	Wait for the printer to complete its internal action.

<b>Error Code</b>	9009048
<b>Text</b>	There has been a jam in the printer.
<b>Details</b>	A card jam has been detected.
<b>Solution</b>	Clear the card jam and try again.

<b>Error Code</b>	9009049
<b>Text</b>	The printer is not currently available.
<b>Details</b>	MyID is unable to communicate with the printer.
<b>Solution</b>	Check that the printer is powered on. Check the printer connection. Duplicate printer devices may be installed if a printer is connected to a different USB port. In this case, ensure that the currently active printer device is selected if there are multiple printer devices for the same printer.

<b>Error Code</b>	9009050
<b>Text</b>	The printer has been paused.
<b>Details</b>	The printer has been placed into paused state. This may be as a result of user action through the printer front panel or as a result of a printer error.
<b>Solution</b>	Resume the printer using the printer front panel.

<b>Error Code</b>	9009051
<b>Text</b>	There has been a state mismatch in the printer.
<b>Details</b>	The client has requested an action that is not supported in the current printer state.
<b>Solution</b>	Restart the workflow and report issue to customer support.

<b>Error Code</b>	9009052
<b>Text</b>	There has been a problem with the ribbon in the printer.
<b>Details</b>	The printer has detected an error with the printer ribbon.
<b>Solution</b>	Check the error being reported on the printer front panel and refer to the manufacturer's user guide.



<b>Error Code</b>	9009053
<b>Text</b>	There is not a session open with the printer.
<b>Details</b>	A session required to perform the required operation is not available.
<b>Solution</b>	This is an internal MyID client error. Restart the workflow and report issue to customer support.

<b>Error Code</b>	9009054
<b>Text</b>	There is a problem with a station in the printer.
<b>Details</b>	An internal printer station has reported an error.
<b>Solution</b>	Check the error being reported on the printer front panel and refer to the manufacturer's user guide.

<b>Error Code</b>	9009056
<b>Text</b>	The printer is currently initializing.
<b>Details</b>	The printer has been restarted, or is recovering from an error condition, and is in the process of re-initializing. Initialization is also reported while MyID creates a connection to the printer.
<b>Solution</b>	Wait for the printer to complete its initialization process

<b>Error Code</b>	9009057
<b>Text</b>	The printer is cooling down.
<b>Details</b>	The printer is cooling down before continuing with the operation.
<b>Solution</b>	Wait for the printer to complete its cooling down process.

<b>Error Code</b>	9009058
<b>Text</b>	The printer is currently heating up.
<b>Details</b>	The printer is heating up before continuing with its operation.
<b>Solution</b>	Wait for the printer to complete its heating up process.

<b>Error Code</b>	9009059
<b>Text</b>	The printer is currently in standby mode.
<b>Details</b>	The printer is currently in standby mode.
<b>Solution</b>	No action required. The printer will automatically resume from standby when a printer activity is started.

## 6 MyID Operator Client error codes

This section contains the list of server-generated errors that may occur when using the MyID Operator Client, the MyID Core API, or the web.oauth2 and web.oauth2.ext authentication services.

To assist with the diagnosis of issues, Intercede support may guide you to enable logging on the `rest.core` or `web.oauth2` web services; you can then provide these logs to customer support for analysis. See the *MyID REST and authentication web services* section in the [Configuring Logging](#) guide for details of enabling logging.

**Note:** You may also see errors produced by the MyID Client Service when using the MyID Operator Client. See section 7, *MyID Client Service error codes* for details.

<b>Error Code</b>	OA10000
<b>Text</b>	Server Error
<b>Details</b>	An internal server error has occurred.
<b>Solution</b>	Retry the operation; the cause could be a temporary issue such as a database timeout due to server load.  If the problem persists, check the <b>System Events</b> and <b>Audit Reporting</b> workflows within MyID, then the <code>web.oauth2</code> logs for more information. For information on configuring logging, see the <i>MyID REST and authentication web services</i> section in the <a href="#">Configuring Logging</a> guide.

<b>Error Code</b>	OA10001
<b>Text</b>	Unable to communicate with app - ensure that MyID UMC app (MyIdClientService) is running
<b>Details</b>	The web page has been unable to communicate with the MyID Client Service.
<b>Solution</b>	Make sure the MyID Client Service is installed and running. See the <i>Installing the MyID Client Service</i> section in the <a href="#">Installation and Configuration Guide</a> .  Make sure that the browser you are using supports websockets connections to <code>ws://localhost</code> . See the <i>Supported browsers</i> section in the <a href="#">MyID Operator Client</a> guide.

<b>Error Code</b>	OA10002
<b>Text</b>	Invalid credentials
<b>Details</b>	The credentials you have supplied for authentication are not valid.
<b>Solution</b>	Supply valid credentials for logon.

<b>Error Code</b>	OA10003
<b>Text</b>	You do not have sufficient security questions configured
<b>Details</b>	The person attempting to log on must have sufficient security questions set up on their account. The number of required security phrases is specified by the <b>Number of security questions for self-service authentication</b> configuration option.
<b>Solution</b>	Use the <b>Change Security Phrases</b> or <b>Change My Security Phrases</b> workflows to provide the required security phrases. See the <i>Setting security phrases</i> section in the <a href="#">Operator's Guide</a> .  Alternatively, you can set a lower value for the <b>Number of security questions for self-service authentication</b> option. See the <i>Setting the number of security phrases required to authenticate</i> section in the <a href="#">Administration Guide</a> .

<b>Error Code</b>	OA10004
<b>Text</b>	Your username or security response is incorrect, or you may not have permission to access this client.
<b>Details</b>	The person attempting to log on has mistyped their username or security responses. Alternatively, your MyID license may have expired.
<b>Solution</b>	Try again. If the problem does not appear to be related to your security response, log on to MyID using MyID Desktop and check the status of your license in the <b>Licensing</b> workflow.  <b>Note:</b> If the number of failed attempts exceeds the configuring maximum (by default, three) the person may be locked out and will have to have their security phrases unlocked. See the <i>Configuring the number of attempts to enter security phrases</i> section in the <a href="#">Administration Guide</a> .

<b>Error Code</b>	OA10005
<b>Text</b>	The registration link is invalid
<b>Details</b>	The registration job ID is not a valid job ID.  This can also occur if there is a problem with the request that is being collected, or the request is not at the 'Awaiting Issue' status; for example, if it has been canceled.
<b>Solution</b>	Carry out the request again.

<b>Error Code</b>	OA10006
<b>Text</b>	Logoncode OTPs are disabled on the server
<b>Details</b>	The <b>Allow Logon Codes</b> option is not set on the server, or the person's role does not have access to the Password logon mechanism.
<b>Solution</b>	Set the <b>Allow Logon Codes</b> option, make sure the person has access to the Password logon mechanism, then try again. See the <i>Setting the configuration options</i> and the <i>Configuring roles for registering FIDO authenticators</i> sections in the <a href="#">FIDO Authenticator Integration Guide</a> for details.

<b>Error Code</b>	OA10007
<b>Text</b>	Your OTP has been entered incorrectly, is locked, has expired, or you do not have permission to perform this operation. Please try again.
<b>Details</b>	The registration code was incorrect, has expired, or has been entered incorrectly too many times, or you do not have access to the <b>Register FIDO Security Key</b> operation.
<b>Solution</b>	Retry entering the registration code. If it continues to fail, it may be locked. Request another FIDO authenticator. You can use the automatic job cancellation feature in MyID to remove any old uncollected, locked, or expired jobs; see the <i>Automatic job cancellation</i> section in the <a href="#">Administration Guide</a> . Check that you have access to the <b>Register FIDO Security Key</b> operation; see the <i>Configuring roles for registering FIDO authenticators</i> section in the <a href="#">FIDO Authenticator Integration Guide</a> for details.

<b>Error Code</b>	OA10008
<b>Text</b>	Your session has timed out or is invalid, please try again
<b>Details</b>	You may have waited too long to complete the registration process.
<b>Solution</b>	Try again. If you have already used your registration code, you must request the FIDO authenticator again, which will send you a new registration code.

<b>Error Code</b>	OA10009
<b>Text</b>	Error registering FIDO in browser
<b>Details</b>	The <code>ServerDomain</code> app setting may be configured incorrectly. Note that <code>ServerDomain</code> is case sensitive and must be consistent with the casing of the DNS Name in the web server's TLS certificate.
<b>Solution</b>	Set the <code>ServerDomain</code> in the app settings file. See the <i>Adding the access token to the web service configuration file</i> section in the <a href="#">FIDO Authenticator Integration Guide</a> for details.

<b>Error Code</b>	OA10010
<b>Text</b>	Error authenticating FIDO in browser.
<b>Details</b>	<p>A cause of this is if the FIDO credential was registered on a website running a different origin to the website that is performing the authentication – at registration, FIDO credentials become locked to the origin on which they were registered.</p> <p>This may also occur if the <code>web.oauth2 Fido:Config:Origin</code> is configured incorrectly in the authentication service app settings file. Note that <code>Origin</code> is case sensitive and must be consistent with the casing of the DNS Name in the web server's TLS certificate</p>
<b>Solution</b>	<p>Set the <code>Origin</code> in the app settings file.</p> <p>See the <i>Adding the access token to the web service configuration file</i> section in the <a href="#">FIDO Authenticator Integration Guide</a> for details.</p>

<b>Error Code</b>	OA10011
<b>Text</b>	FIDO authentication failed, please try again. You may not have permission to access this client.
<b>Details</b>	<p>This may occur when the credential profile for a FIDO authenticator was set up to require user verification, but the FIDO authenticator does not support that feature.</p> <p>This may also occur when you are attempting to log on with a FIDO authenticator without providing a username, but the credential profile was not set up with the <b>Require Client Side Discoverable Key</b> option, and consequently the FIDO authenticator does not have the key required for logon without a username.</p>
<b>Solution</b>	<p>Try a different FIDO authenticator, try a credential profile that has been set up with less stringent requirements, or try a credential profile that sets up the client side discoverable key; see the <i>Setting up a credential profile for FIDO authenticators</i> section in the <a href="#">FIDO Authenticator Integration Guide</a> for details.</p>

<b>Error Code</b>	OA10012
<b>Text</b>	FIDO registration failed, the FIDO token used to register was not trusted. Try a different FIDO token if you have one. <details>
<b>Details</b>	The FIDO authenticator you have tried to register failed the attestation check.
<b>Solution</b>	Try a different FIDO authenticator.

<b>Error Code</b>	OA10013
<b>Text</b>	FIDO registration failed, user mismatch
<b>Details</b>	The FIDO authenticator cannot be registered as there is a problem matching the user.
<b>Solution</b>	Try registering the authenticator to a different user.

<b>Error Code</b>	OA10014
<b>Text</b>	FIDO registration failed, the credential profile is invalid
<b>Details</b>	The credential profile is not valid, or the person for whom the FIDO authenticator was requested has changed roles, and can no longer receive the originally-requested credential profile.
<b>Solution</b>	Request a FIDO authenticator using a different credential profile, and try again.

<b>Error Code</b>	OA10015
<b>Text</b>	FIDO registration failed, this token is already registered
<b>Details</b>	The FIDO authenticator is already registered.
<b>Solution</b>	Try a different FIDO authenticator.

<b>Error Code</b>	OA10016
<b>Text</b>	FIDO registration failed, the credential profile is set to Enforce Authenticator Attestation Check, but the token registered does not have metadata available on the server. Try registering a different token.
<b>Details</b>	The manufacturer did not register metadata with the FIDO metadata service, and the file-based metadata does not include information about this token. This token cannot be used with this credential profile.
<b>Solution</b>	<p>Either register a different token, register this token to a different credential profile using a credential profile that does not have <b>Enforce Authenticator Attestation Check</b> set, get the token manufacturer to publish the metadata for this token to the FIDO metadata service, or obtain the FIDO metadata and configure it manually on the server using the <code>MDSCacheDirPath</code> setting.</p> <p>See the <i>Setting up a credential profile for FIDO authenticators</i> or <i>Setting up a local metadata repository</i> section in the <a href="#">FIDO Authenticator Integration Guide</a> for details.</p>

<b>Error Code</b>	OA10017
<b>Text</b>	FIDO registration failed, there was a problem accessing the FIDO Metadata Server
<b>Details</b>	There was a problem trying to get a metadata TOC payload entry from the FIDO metadata service.
<b>Solution</b>	Check that the URLs <code>https://*.fidoalliance.org</code> are accessible from the web server and try again.

<b>Error Code</b>	OA10018
<b>Text</b>	You do not have any FIDO tokens registered
<b>Details</b>	The person has attempted to authenticate to the MyID authentication service using FIDO, but does not have any registered FIDO authenticators.
<b>Solution</b>	Request a FIDO authenticator for the person.

<b>Error Code</b>	OA10019
<b>Text</b>	Username should not be null or empty
<b>Details</b>	The MyID Username claim was missing in the cookie for the call to logon with FIDO.
<b>Solution</b>	Restart the browser and try again.

<b>Error Code</b>	OA10020
<b>Text</b>	FIDO basic and FIDO high logon mechanisms are disabled for this client
<b>Details</b>	No supported FIDO logon mechanisms were found.
<b>Solution</b>	This may be the result of an attempt to bypass FIDO logon mechanisms. Make sure you have gone through the correct procedure.

<b>Error Code</b>	OA10021
<b>Text</b>	Invalid return URL
<b>Details</b>	The return link from a logon authentication call was invalid.
<b>Solution</b>	This may be the result of a redirect attack or a malicious link. Make sure you have gone through the correct procedure.

<b>Error Code</b>	OA10030
<b>Text</b>	MyID:Database:ConnectionStringCore is not configured
<b>Details</b>	A configuration file error has occurred. You must configure a database connection string.
<b>Solution</b>	Check the configuration file settings – <code>ConnectionStringCore</code> must be configured. See the <i>Configuring the standalone authentication service</i> section in the <a href="#">MyID Authentication Guide</a> .

<b>Error Code</b>	OA10031
<b>Text</b>	MyID:Database:ConnectionStringAuth is not configured
<b>Details</b>	A configuration file error has occurred. You must configure a database connection string.
<b>Solution</b>	Check the configuration file settings – <code>ConnectionStringAuth</code> must be configured. See the <i>Configuring the standalone authentication service</i> section in the <a href="#">MyID Authentication Guide</a>

<b>Error Code</b>	OA10032
<b>Text</b>	Unable to find configured JWT signing certificate
<b>Details</b>	No JWT signing certificate was found, but JWT signing is configured.
<b>Solution</b>	Check the JWT settings. See the <i>Load balancing</i> section in the <a href="#">MyID Operator Client</a> guide.

<b>Error Code</b>	OA10033
<b>Text</b>	No JWT signing certificate configured and no RSA signing key containername configured
<b>Details</b>	MyID is configured to use a previously configured RSA keyname but no RSA container name was found.
<b>Solution</b>	Check the JWT settings. See the <i>Load balancing</i> section in the <a href="#">MyID Operator Client</a> guide.

<b>Error Code</b>	OA10034
<b>Text</b>	JWT signing key is configured, but has an incorrect algorithm or key size
<b>Details</b>	MyID has found an RSA key with an incorrect algorithm or key size.
<b>Solution</b>	Check the JWT settings. See the <i>Load balancing</i> section in the <a href="#">MyID Operator Client</a> guide.



<b>Error Code</b>	OA10035
<b>Text</b>	Generated JWT signer certificate, but unable to load it
<b>Details</b>	A server error has occurred while attempting to validate the generated signer certificate.
<b>Solution</b>	Check the JWT settings. See the <i>Load balancing</i> section in the <a href="#">MyID Operator Client</a> guide.

<b>Error Code</b>	OA10036
<b>Text</b>	No JWT signing certificate configured and no RSA signing key containername configured, and not configured to generate a JWT signing key
<b>Details</b>	A configuration error has occurred. No authentication method has been set.
<b>Solution</b>	Check the JWT settings. See the <i>Load balancing</i> section in the <a href="#">MyID Operator Client</a> guide.

<b>Error Code</b>	OA10037
<b>Text</b>	You do not have permission to perform this operation. Your permissions could not be verified
<b>Details</b>	A valid access token has not been supplied to authorize this extension grant. The token may be missing, may not contain the required claims.
<b>Solution</b>	Check that your system is providing the correct data for the extension grant.

<b>Error Code</b>	OA10038
<b>Text</b>	You do not have permission to perform this operation
<b>Details</b>	This can happen if the caller does not have scope over the object (request, device or person) in the context of the operation being performed.
<b>Solution</b>	Check the roles that the person has and check the permissions these roles give in <b>Edit Roles</b> .

<b>Error Code</b>	OA10039
<b>Text</b>	You do not have permission to perform this operation on the identified object or the identified object does not exist
<b>Details</b>	This can happen if the caller does not have scope over the object (request, device or person) in the context of the operation being performed.
<b>Solution</b>	Check the roles that the person has and check the permissions these roles give in <b>Edit Roles</b> .

<b>Error Code</b>	OA10040
<b>Text</b>	Your assigned roles do not have permission to collect this request's credential profile
<b>Details</b>	The credential profile does not include any of your roles in the <b>Can Collect</b> option.
<b>Solution</b>	Edit the credential profile to add one of your roles to the <b>Can Collect</b> options for the profile.

<b>Error Code</b>	OA10041
<b>Text</b>	Authorization failure, missing data
<b>Details</b>	Data required to perform the extension grant is missing. This should not be seen through the MyID Operator Client but may occur if integrating third party systems to perform token operation extension grants if they do not supply the required data.
<b>Solution</b>	Check that your system is providing the data required to perform the extension grant.

<b>Error Code</b>	OA10042
<b>Text</b>	This item is not in the correct state to perform this operation
<b>Details</b>	You have attempted to carry out an operation that requires a particular status; for example, collecting a card requires a job status of Awaiting Issue. If this error occurs, the status is no longer correct for the operation; this may occur when multiple operators attempt to carry out an operation on the same item.
<b>Solution</b>	Go back and attempt the operation again from the beginning; if the item is not in the correct status, you should not be offered the opportunity to carry out the operation.  If you are using the self-service menu in the MyID Operator Client, click <b>Check For Updates</b> to refresh the list of available actions before attempting the operation again.

<b>Error Code</b>	OA10043
<b>Text</b>	Your assigned roles do not have permission to unlock this device
<b>Details</b>	When the configuration flag <b>Constrain Credential Profile Unlock Operator</b> is set, when unlocking devices for other users you require the <b>Can Unlock</b> permission for the credential profile of that device.
<b>Solution</b>	Edit the credential profile to add one of your roles to the <b>Can Unlock</b> options for the profile.

<b>Error Code</b>	OA10044
<b>Text</b>	You cannot perform this operation on yourself
<b>Details</b>	You have attempted to perform an operation that is not allowed for self-service on your own account.
<b>Solution</b>	Either perform the operation on another person's account, or get another operator to perform the operation on your account.

<b>Error Code</b>	OA10045
<b>Text</b>	You cannot perform this operation on others
<b>Details</b>	You have attempted to perform an operation that is allowed for self-service only on another person.
<b>Solution</b>	Either perform the operation on your own account, or get the other person to perform the operation on their own account.

<b>Error Code</b>	OA10046
<b>Text</b>	The OTP has expired
<b>Details</b>	The authentication code has expired.
<b>Solution</b>	<p>Request a new authentication code.</p> <p>The lifetime of authentication codes is controlled by the following configuration options on the <b>Auth Code</b> page of the <b>Security Settings</b> workflow:</p> <ul style="list-style-type: none"><li>• <b>Auth Code Lifetime</b></li><li>• <b>Auth Code Lifetime for Immediate Use</b> (for short-use codes; for examples, authentication codes requested at the logon screen of the MyID Operator Client for immediate use).</li></ul>

<b>Error Code</b>	OA10047
<b>Text</b>	This item does not meet the requirements to perform this operation
<b>Details</b>	An operation for pass-through authentication has a condition that has not been met. Launching this operation is not allowed.
<b>Solution</b>	This operation can be performed only if the subject of the operation meets the criteria configured for the operation. Ensure that the subject of the operation meets the configured criteria, or if these have been customized in MyID Project Designer, ensure that this has been configured correctly.

<b>Error Code</b>	OA10048
<b>Text</b>	The user does not have the required contact details for this delivery mechanism
<b>Details</b>	A notification cannot be sent, the required contact details (email address or cell phone number) are not known for this user.
<b>Solution</b>	Contact an administrator to get the contact details updated.

<b>Error Code</b>	OA10049
<b>Text</b>	An error occurred capturing the fingerprint. Please try again
<b>Details</b>	MyID failed to capture the fingerprint due to an issue with the fingerprint reader.
<b>Solution</b>	Check that the fingerprint reader is connected, and that its drivers are installed correctly.

<b>Error Code</b>	OA10050
<b>Text</b>	Number of fingerprint attempts has been exceeded
<b>Details</b>	The number of attempts to capture fingerprints has exceeded the configured maximum (the <b>Number of fingerprint validation attempts</b> configuration option on the <b>Biometrics</b> page of the <b>Operation Settings</b> workflow), either through failure to match or verify, or failure to capture.
<b>Solution</b>	Close the authentication popup window and try again. If you continue to experience failures, check that your fingerprint reader is connected, and that its drivers are installed correctly.

<b>Error Code</b>	OA10051
<b>Text</b>	No match was found for the fingerprint
<b>Details</b>	A fingerprint was captured, but no match was found in MyID.
<b>Solution</b>	Check that you have fingerprints captured in your MyID user account.

<b>Error Code</b>	OA10052
<b>Text</b>	Authorization failure, missing data
<b>Details</b>	The request for the secondary authentication extension grant is missing some information.
<b>Solution</b>	Check the call to get the secondary authentication extension grant has the required parameters, such as the necessary tokens.

<b>Error Code</b>	OA10053
<b>Text</b>	You do not have permission to perform this operation
<b>Details</b>	The primary token (the MyID Logon token) is invalid.
<b>Solution</b>	Check that the MyID Logon token is valid, and has not expired.

<b>Error Code</b>	OA10054
<b>Text</b>	You do not have permission to perform this operation
<b>Details</b>	The secondary authentication token (biometric) failed validation against MyID.
<b>Solution</b>	Check the secondary authentication token has the required claims and validity.

<b>Error Code</b>	OA10055
<b>Text</b>	You do not have permission to perform this operation
<b>Details</b>	The tokens were valid, but the user's or token's permission has been denied for the attempted operation.
<b>Solution</b>	Check your MyID configuration for operation authentication.

<b>Error Code</b>	OA10056
<b>Text</b>	Invalid request for Secondary Authentication
<b>Details</b>	Invalid data was found when attempting to verify the Secondary Authentication token.
<b>Solution</b>	Check your MyID configuration for operation authentication.

<b>Error Code</b>	OA10057
<b>Text</b>	A required claim is missing for Secondary Authentication
<b>Details</b>	The secondary authentication token presented was missing required claims.
<b>Solution</b>	Check your MyID configuration for operation authentication.

<b>Error Code</b>	OA10058
<b>Text</b>	There are no fingerprints registered for this person
<b>Details</b>	The user has tried to authenticate with a fingerprint, but no fingers are registered or enrolled in MyID.
<b>Solution</b>	The user must enroll fingerprints.

<b>Error Code</b>	OA10059
<b>Text</b>	There are no update jobs to collect for this device
<b>Details</b>	There are no update jobs available to be collected for this device.
<b>Solution</b>	There may not be any jobs or there may be jobs awaiting validation. Check that there are appropriate update jobs available for the device.

<b>Error Code</b>	OA10060
<b>Text</b>	The credential profile to be collected requires user data approval, but the target user has no such approval
<b>Details</b>	The person for whom you are attempting to collect the card for is not approved, but has a credential profile requiring approval.
<b>Solution</b>	Use a different credential profile, or approve the person.

<b>Error Code</b>	OA10061
<b>Text</b>	The credential profile to be collected requires terms and conditions to be accepted, but assisted collection of updates does not support this
<b>Details</b>	The credential profile being collected requires terms and conditions to be accepted, but this is not supported by Assisted Collect.
<b>Solution</b>	Collect this profile using a self service operation, or use a different credential profile.

<b>Error Code</b>	OA10062
<b>Text</b>	MyID client service is not running
<b>Details</b>	You have attempted to use the <b>Manage My Credentials</b> option on the MyID Authentication screen, but the MyID Client Service application is not running.
<b>Solution</b>	Close the MyID Authentication screen, start the MyID Client Service, then click <b>Sign In</b> and <b>Manage My Credentials</b> again. See the <i>Managing your credentials from the MyID Authentication screen</i> section in the <a href="#">MyID Operator Client</a> guide.

<b>Error Code</b>	OA10063
<b>Text</b>	You cannot retrieve security questions for this client
<b>Details</b>	You have attempted to use headless passphrase authentication (for example, for PIN unlock for mobile identities) but the client ID specified in the API call is not listed in the application settings file.
<b>Solution</b>	Check that the <code>appsettings.Production.json</code> and <code>appsettings.json</code> files for the web.oauth2 web service are correctly configured.

<b>Error Code</b>	OA10064
<b>Text</b>	The security questions logonmechanism is disabled for this client
<b>Details</b>	You have attempted to use headless passphrase authentication (for example, for PIN unlock for mobile identities) but either the <b>Password Logon</b> mechanism (on the <b>Logon Mechanisms</b> page of the <b>Security Settings</b> workflow) or the <code>EnableHeadlessPassphraseLogin</code> option (in the application settings JSON file for the web.oauth2 web service) is not enabled. Both must be enabled to use this feature.
<b>Solution</b>	Check that the <b>Password Logon</b> option and the <code>appsettings.Production.json</code> and <code>appsettings.json</code> files for the web.oauth2 web service are correctly configured.

<b>Error Code</b>	OA10065
<b>Text</b>	You cannot retrieve a challenge for this client
<b>Details</b>	You have attempted to use headless card authentication (for example, for certificate renewal for mobile identities) but the client ID specified in the API call is not listed in the application settings file.
<b>Solution</b>	Check that the <code>appsettings.Production.json</code> and <code>appsettings.json</code> files for the web.oauth2 web service are correctly configured.

<b>Error Code</b>	OA10066
<b>Text</b>	The smartcard logon logonmechanism is disabled for this client
<b>Details</b>	You have attempted to use headless card authentication (for example, for certificate renewal for mobile identities) but either the <b>Smart Card Logon</b> mechanism (on the <b>Logon Mechanisms</b> page of the <b>Security Settings</b> workflow) or the <code>EnableHeadlessCardLogin</code> option (in the application settings JSON file for the web.oauth2 web service) is not enabled. Both must be enabled to use this feature.
<b>Solution</b>	Check that the <b>Smart Card Logon</b> option and the <code>appsettings.Production.json</code> and <code>appsettings.json</code> files for the web.oauth2 web service are correctly configured.

<b>Error Code</b>	OA10067
<b>Text</b>	Key-pair authentication failed, or you may not have permission to access this client
<b>Details</b>	You have attempted to use headless card authentication (for example, for certificate renewal for mobile identities) but the key pair used is invalid.
<b>Solution</b>	Try the operation again.

<b>Error Code</b>	OA10068
<b>Text</b>	Windows logon failed, your windows account is unknown or untrusted
<b>Details</b>	You have attempted to sign in using Windows authentication, but your Windows account is not suitable.
<b>Solution</b>	See the <i>Signing in using Windows authentication</i> section in the <a href="#">MyID Operator Client</a> guide.

<b>Error Code</b>	OA10069
<b>Text</b>	Windows logon failed, your user account is not permitted to logon
<b>Details</b>	You have attempted to log on to MyID using Windows authentication, but the specified user account does not have permission to do so.
<b>Solution</b>	Make sure the logon name provided exists, and has permission to log on with Windows authentication.  See the <i>Signing in using Windows authentication</i> section in the <a href="#">MyID Operator Client</a> guide.

<b>Error Code</b>	OA10070
<b>Text</b>	Windows Authentication is disabled on the server
<b>Details</b>	You have attempted to log on to MyID using Windows authentication, but your server is not configured to allow it.
<b>Solution</b>	Check that the <b>Integrated Windows Logon</b> mechanism is enabled on the <b>Logon Mechanisms</b> page of the <b>Security Settings</b> workflow.  On the MyID web server, in IIS, check the <b>Authentication</b> settings for web.oauth2, and make sure that both <b>Anonymous Authentication</b> and <b>Windows Authentication</b> are enabled.  See the <i>Signing in using Windows authentication</i> section in the <a href="#">MyID Operator Client</a> guide.

<b>Error Code</b>	OA10071
<b>Text</b>	Refresh Token failed to retrieve token
<b>Details</b>	The refresh token could not be found in the internal store, based on the handle provided.
<b>Solution</b>	Check the token handle being sent, or log off and try again.  See the <i>Signing in using Windows authentication</i> section in the <a href="#">MyID Operator Client</a> guide.



<b>Error Code</b>	OA10072
<b>Text</b>	Authorization failure, missing data for Token Refresh
<b>Details</b>	This error may be caused by the request for the Refresh token missing the token handle value (the value returned with the initial logon token).
<b>Solution</b>	Check the token handle being sent, or log off and try again See the <i>Signing in using Windows authentication</i> section in the <a href="#">MyID Operator Client</a> guide.

<b>Error Code</b>	OA10073
<b>Text</b>	Logon is not permitted - the system license has expired. Contact a system administrator.
<b>Details</b>	Your MyID system has a time-based license that has now expired. You can no longer log on to the MyID Operator Client.
<b>Solution</b>	Contact a system administrator who has access to MyID Desktop and the <b>Licensing</b> workflow. See the <i>License management</i> section in the <a href="#">Administration Guide</a> guide.

<b>Error Code</b>	OA10074
<b>Text</b>	External logon failed, no matching MyID user found
<b>Details</b>	You have attempted to use an external identity provider, but it is configured to require a matching existing MyID user, and no matching user was found.
<b>Solution</b>	Use a different user, or configure your system to create users in MyID from the external identity provider. See the <i>Setting up an external identity provider</i> section in the <a href="#">MyID Authentication Guide</a> for more information.

<b>Error Code</b>	OA10075
<b>Text</b>	External logon failed, external logon mechanism invalid
<b>Details</b>	You have attempted to use an external identity provider, but have not specified a valid logon mechanism.
<b>Solution</b>	Check your configuration to ensure that you have specified a valid external identity provider that is fully configured and is not disabled. See the <i>Setting up an external identity provider</i> section in the <a href="#">MyID Authentication Guide</a> for more information.

<b>Error Code</b>	OA10076
<b>Text</b>	External logon failed, external logon is not available in standalone mode
<b>Details</b>	You have attempted to use an external identity provider, but you are using the web.oauth2.ext web service, which does not support external identity providers.
<b>Solution</b>	Use the web.oauth2 web service instead. See the <i>Setting up an external identity provider</i> section in the <a href="#">MyID Authentication Guide</a> for more information.

<b>Error Code</b>	OA10077
<b>Text</b>	External logon failed, the attempted logon failed
<b>Details</b>	You have attempted to use an external identity provider, but the logon attempt failed.
<b>Solution</b>	Check your authentication with the external identity provider is valid, and try again. See the <i>Setting up an external identity provider</i> section in the <a href="#">MyID Authentication Guide</a> for more information.

<b>Error Code</b>	OA10078
<b>Text</b>	External logon failed, no mappings found for claims
<b>Details</b>	You have attempted to use an external identity provider, but the claims supplied by the provider do not have any matches in the configured mappings.
<b>Solution</b>	Check the mappings for your external identity provider. See the <i>Mapping attributes</i> section in the <a href="#">MyID Authentication Guide</a> for more information.

<b>Error Code</b>	OA10079
<b>Text</b>	External logon failed, a mandatory attribute is not present in either the claims or the user info
<b>Details</b>	You have attempted to use an external identity provider, but an attribute that you have configured to be mandatory has not been found.
<b>Solution</b>	Check the mappings for your external identity provider. See the <i>Mapping attributes</i> section in the <a href="#">MyID Authentication Guide</a> for more information.

<b>Error Code</b>	OA10080
<b>Text</b>	External logon failed, no claims supplied by external identity provider
<b>Details</b>	You have attempted to use an external identity provider, but the external identity provider did not provide any claims.
<b>Solution</b>	See the <i>Setting up an external identity provider</i> section in the <a href="#">MyID Authentication Guide</a> for more information.

<b>Error Code</b>	OC10001
<b>Text</b>	There are no actions available for your current logon method and the roles that you have been assigned.
<b>Details</b>	You have not been assigned any actions for use in the MyID Operator Client.
<b>Solution</b>	Ensure that the roles you have assigned provide MyID Operator Client actions. See the <i>Roles and groups</i> section in the <a href="#">MyID Operator Client</a> guide.

<b>Error Code</b>	OC10002
<b>Text</b>	This web browser cannot be used. Please use an alternative web browser.
<b>Details</b>	An unsupported browser has been detected. Due to the browser technology used, you cannot use Internet Explorer to access the MyID Operator Client.
<b>Solution</b>	The MyID Operator Client is designed to work on a range of browsers running on Windows 10 or Windows 11, excluding Internet Explorer. You are recommended to use Google Chrome, Microsoft Edge (Chromium version) or Mozilla Firefox. See the <i>Supported browsers</i> section in the <a href="#">MyID Operator Client</a> guide.

<b>Error Code</b>	OC10003
<b>Text</b>	There has been a problem on the server and it is not possible to continue.
<b>Details</b>	The API server is unreachable or has been configured incorrectly.
<b>Solution</b>	<p>Confirm that the API server is reachable, and has been configured correctly.</p> <p>Check the URLs in the web service configuration files; they must use https and be valid URLs. See <i>The rest.core web service configuration file</i> and <i>The web.oauth2 web service configuration file</i> sections in the <a href="#">MyID Operator Client</a> guide for details of the web service configuration files.</p> <p>The REST-based web services require HTTPS, and will not operate if this is not set up. For more information, see the <i>REST-based web services</i> section in the <a href="#">System Interrogation Utility</a> guide.</p>

<b>Error Code</b>	OC10004
<b>Text</b>	The server could not be contacted. Please try again.
<b>Details</b>	Connection to the server unavailable. Either the client is not connected to the Internet, or the server is offline.
<b>Solution</b>	<p>Confirm that the API server is reachable, and try again.</p> <p>Confirm that you have the correct server address specified; see the <i>Specifying the server for the MyID Client Service</i> section in the <a href="#">MyID Operator Client</a> guide.</p> <p>Confirm that your environment's security (for example, the load balancer or firewall) has been configured to allow full access to the REST web services; while some systems may be locked down to allow only GET and POST, the MyID web services require the full range of verbs, including (but not limited to) GET, POST, PATCH, OPTIONS, and DELETE.</p>

<b>Error Code</b>	OC10005
<b>Text</b>	The file you have uploaded is not an image. Please upload an image.
<b>Details</b>	<p>You can choose from the following file types:</p> <ul style="list-style-type: none"> <li>• JPEG (*.jpg, *.jpeg)</li> <li>• Bitmap (*.bmp)</li> <li>• Graphics Interchange Format (*.gif)</li> <li>• Portable Network Graphics (*.png)</li> </ul> <p>If you select a file of the wrong type, MyID displays an error.</p>
<b>Solution</b>	See the <i>Uploading an existing image file</i> section in the <a href="#">MyID Operator Client</a> guide.

<b>Error Code</b>	OC10006
<b>Text</b>	MyID Client Service error
<b>Details</b>	You have attempted to use a feature provided by the MyID Client Service App, but the app is not running, or is configured incorrectly.
<b>Solution</b>	<p>This may occur when accessing smart card, editing captured images, or other operations provided by the MyID Client Service App. Make sure the app is running.</p> <p>See the <i>Installing the MyID Client Service</i> section in the <a href="#">Installation and Configuration Guide</a> for instructions on installing the MyID Client Service.</p> <p>This may also occur if MyID Desktop or the Self-Service App could not be found at the configured path.</p> <p>See the <i>Setting the location of MyID Desktop or the Self-Service App</i> section in the <a href="#">MyID Operator Client</a> guide.</p>

<b>Error Code</b>	OC10007
<b>Text</b>	A problem has occurred when connecting to the camera.
<b>Details</b>	<p>The MyID Image Capture component cannot make a connection to the camera.</p> <p>The camera might be in use or has a low maximum supported camera resolution.</p>
<b>Solution</b>	<p>Confirm that the camera is operating correctly and can support a minimum resolution of 640x480.</p> <p>Confirm that the camera is not currently in use in another application, then start Image Capture again.</p>

<b>Error Code</b>	OC10008
<b>Text</b>	Unable to launch the MyID Desktop or Self-Service App. Please check configuration and try again.
<b>Details</b>	MyID Desktop or the Self-Service App could not be found at the configured path. Check the MyID Client Service log in the Windows system tray for further details.
<b>Solution</b>	<p>Confirm that the application is installed and available at the configured location.</p> <p>See the <i>Setting the location of MyID Desktop or the Self-Service App</i> section in the <a href="#">MyID Operator Client</a> guide.</p>

<b>Error Code</b>	OC10009
<b>Text</b>	Unable to connect to MyID Desktop or the Self-Service App. Please try again.
<b>Details</b>	The MyID Client Service failed to start a client application due to a timeout error. Check the MyID Client Service log in the Windows system tray for further details.
<b>Solution</b>	<p>Try again. If this issue persists, confirm that MyID Desktop and the Self-Service App are able to start within the configured timeout setting. This issue has been seen on environments where there is no Internet connection.</p> <p>See the <i>Troubleshooting MCS connection issues</i> section in the <a href="#">MyID Operator Client</a> guide.</p>

<b>Error Code</b>	OC10010
<b>Text</b>	Unable to launch MyID Desktop or the Self-Service App. Please try again.
<b>Details</b>	MyID Desktop or the Self-Service App is running but is already servicing a request. Try again when the current request has been completed. Check the MyID Client Service log in the Windows system tray for further details.
<b>Solution</b>	Try again when the current request has been completed.

<b>Error Code</b>	OC10011
<b>Text</b>	The item is not available. This may be due to the item changing status, the link no longer being valid or you do not have permission to access this information.
<b>Details</b>	The operation or entity provided in the URL link is not available. Confirm that the link provided is valid and you have permissions for the operation specified.
<b>Solution</b>	Confirm that you have permissions to the link provided and try again.

<b>Error Code</b>	OC10012
<b>Text</b>	The item is not available. Check the link is valid and you have permission to access this information.
<b>Details</b>	The search provided in the URL link is not available. Confirm that the link provided is valid and you have permissions for the search specified.
<b>Solution</b>	Confirm that you have permissions to the link provided and try again.

<b>Error Code</b>	OC10013
<b>Text</b>	Unable to launch MyID Desktop or the Self-Service App. Please check installed version and try again.
<b>Details</b>	An incorrect version of MyID Desktop or the Self-Service App has been detected.
<b>Solution</b>	<p>Confirm that the correct version of MyID Desktop or the Self-Service App is installed, and try again. You may have to upgrade your version of MyID Desktop or the Self-Service App to the latest version to support the feature you are trying to use.</p> <p>If you have more than one version of the client software installed, make sure that the MyID Client Service is configured with the location of the correct version. See the <i>Setting the location of MyID Desktop or the Self-Service App</i> section in the <a href="#">MyID Operator Client</a> guide.</p>

<b>Error Code</b>	OC10014
<b>Text</b>	This action cannot be performed. Please check the installed version of MyID Client Service, and try again.
<b>Details</b>	The version of MyID Client Service that is currently installed does not support performing this action.
<b>Solution</b>	Install a later version of MyID Client Service, and try again.

<b>Error Code</b>	OC10015
<b>Text</b>	At least one record must be selected in order to perform this operation.
<b>Details</b>	You have attempted to run a batch operation with no items selected. This may occur if you attempt to return to an intermediate URL in the batch process.
<b>Solution</b>	Return to the main screen and try the operation again.

<b>Error Code</b>	OC10016
<b>Text</b>	Your login has expired. Please re-authenticate to the MyID Operator Client.
<b>Details</b>	Due to inactivity, you have been logged out of the MyID Operator Client.
<b>Solution</b>	<p>Re-authenticate to the MyID Operator Client using the same user and logon mechanism.</p> <p>See the <i>Timeouts and re-authentication</i> section in the <a href="#">MyID Operator Client</a> guide.</p>

<b>Error Code</b>	OC10017
<b>Text</b>	You have re-authenticated to the MyID Operator Client with a different user. For security reasons, the operation has been canceled.
<b>Details</b>	A different user was used to re-authenticate to the MyID Operator Client. You have returned to the home page, and the previous operation has been canceled.
<b>Solution</b>	Use the same user and logon mechanism that was previously used to complete the intended operation. See the <i>Timeouts and re-authentication</i> section in the <a href="#">MyID Operator Client</a> guide.

<b>Error Code</b>	OC10018
<b>Text</b>	You have re-authenticated to the MyID Operator Client with a different logon mechanism. For security reasons, the operation has been canceled.
<b>Details</b>	A different logon mechanism was used to re-authenticate to the MyID Operator Client. You have returned to the home page, and the previous operation has been canceled.
<b>Solution</b>	Use the same logon mechanism that was previously used to complete the intended operation. See the <i>Timeouts and re-authentication</i> section in the <a href="#">MyID Operator Client</a> guide.

<b>Error Code</b>	OC10019
<b>Text</b>	A technical problem occurred when processing the certificate using MyID client services. This issue requires detailed troubleshooting by a system administrator. Please consult MyID documentation for more information.
<b>Details</b>	The request manifest was provided in an unexpected format and could not be parsed.
<b>Solution</b>	If this issue can be reproduced, examine logs from the MyID Client Service at the time the problem occurred. To access the MyID client service log information, right click on the MyID icon in the Windows system tray on the computer affected and select 'Show'. This information may need to be analyzed by Intercede support.



<b>Error Code</b>	OC10020
<b>Text</b>	A technical problem occurred when processing the certificate using MyID client services. This issue requires detailed troubleshooting by a system administrator. Please consult MyID documentation for more information.
<b>Details</b>	MyID Client Components (UMC) threw an exception in CreatePkcs10Ex.
<b>Solution</b>	If this issue can be reproduced, examine logs from the MyID client service at the time the problem occurred. To access the MyID client service log information, right click on the MyID icon in the Windows system tray on the computer affected and select 'Show'. This information may need to be analyzed by Intercede support.

<b>Error Code</b>	OC10021
<b>Text</b>	A technical problem occurred when processing the certificate using MyID client services. This issue requires detailed troubleshooting by a system administrator. Please consult MyID documentation for more information.
<b>Details</b>	MyID Client Components (UMC) threw an exception in AcceptPkcs7Ex2.
<b>Solution</b>	<p>This error may be caused by the certificate policy for a soft certificate not having the <b>Private Key Exportable</b> option set; this also means that the policy must be configured on the CA to allow the private key to be exported.</p> <p>See the <i>Setting up a credential profile for soft certificates</i> section in the <a href="#">Administration Guide</a> for details.</p> <p>This issue may also occur if the certificate file name generated from the certificate policy name contains invalid characters.</p> <p>As a workaround, you can customize the file names; see the <i>Customizing certificate file names</i> section in the <a href="#">MyID Operator Client</a> guide.</p> <p>After checking the above workarounds, if this issue continues, examine logs from the MyID client service at the time the problem occurred. To access the MyID client service log information, right click on the MyID icon in the Windows system tray on the computer affected and select 'Show'. This information may need to be analyzed by Intercede support.</p>

<b>Error Code</b>	OC10022
<b>Text</b>	A technical problem occurred when processing the certificate using MyID client services. This issue requires detailed troubleshooting by a system administrator. Please consult MyID documentation for more information.
<b>Details</b>	Failed to load an archived certificate.
<b>Solution</b>	If this issue can be reproduced, examine logs from the MyID client service at the time the problem occurred. To access the MyID client service log information, right click on the MyID icon in the Windows system tray on the computer affected and select 'Show'. This information may need to be analyzed by Intercede support.

<b>Error Code</b>	OC10023
<b>Text</b>	A technical problem occurred when processing the certificate using MyID client services. This issue requires detailed troubleshooting by a system administrator. Please consult MyID documentation for more information.
<b>Details</b>	Failed to add an archived certificate to the user store.
<b>Solution</b>	If this issue can be reproduced, examine logs from the MyID client service at the time the problem occurred. To access the MyID client service log information, right click on the MyID icon in the Windows system tray on the computer affected and select 'Show'. This information may need to be analyzed by Intercede support.

<b>Error Code</b>	OC10024
<b>Text</b>	A technical problem occurred when processing the certificate using MyID client services. This issue requires detailed troubleshooting by a system administrator. Please consult MyID documentation for more information.
<b>Details</b>	Request included an extension that is not explicitly permitted. Default allowed extensions are .pfx and .cer.
<b>Solution</b>	<p>This issue may occur if the certificate file name generated from the certificate policy name contains invalid characters.</p> <p>As a workaround, you can customize the file names; see the <i>Customizing certificate file names</i> section in the <a href="#">MyID Operator Client</a> guide.</p> <p>If this issue can be reproduced, examine logs from the MyID client service at the time the problem occurred. To access the MyID client service log information, right click on the MyID icon in the Windows system tray on the computer affected and select 'Show'. This information may need to be analyzed by Intercede support.</p>

<b>Error Code</b>	OC10025
<b>Text</b>	A technical problem occurred when processing the certificate using MyID client services. This issue requires detailed troubleshooting by a system administrator. Please consult MyID documentation for more information.
<b>Details</b>	Auto-save has been disabled in the client configuration file.
<b>Solution</b>	If this issue can be reproduced, examine logs from the MyID client service at the time the problem occurred. To access the MyID client service log information, right click on the MyID icon in the Windows system tray on the computer affected and select 'Show'. This information may need to be analyzed by Intercede support.

<b>Error Code</b>	OC10026
<b>Text</b>	A technical problem occurred when processing the certificate using MyID client services. This issue requires detailed troubleshooting by a system administrator. Please consult MyID documentation for more information.
<b>Details</b>	An exception occurred during a file-write operation.
<b>Solution</b>	If this issue can be reproduced, examine logs from the MyID client service at the time the problem occurred. To access the MyID client service log information, right click on the MyID icon in the Windows system tray on the computer affected and select 'Show'. This information may need to be analyzed by Intercede support.

<b>Error Code</b>	OC10028
<b>Text</b>	The printer is unavailable. Please check the printer is operational and not in use.
<b>Details</b>	There has been a problem with the printer.
<b>Solution</b>	Check the printer for any messages.

<b>Error Code</b>	OC10029
<b>Text</b>	The printer reported the print operation has failed. Please see the printer for further details.
<b>Details</b>	There has been a problem with the printer.
<b>Solution</b>	Check the printer for any messages.

<b>Error Code</b>	OC10030
<b>Text</b>	The MyID Client Service was unable to read the document.
<b>Details</b>	The MyID Client Service requires the WebView2 Runtime component to be installed on the client PC to allow it to read and print HTML document templates.
<b>Solution</b>	Check that all pre-requisites are installed before attempting to print the document. See the <i>Client workstation</i> section in the <a href="#">Installation and Configuration Guide</a> for details.

<b>Error Code</b>	OC10031
<b>Text</b>	The MyID Client Service was unable to read the document.
<b>Details</b>	The MyID Client Service could not read the mailing document due to a permissions error.
<b>Solution</b>	Check that the MyID Client Service is not running with elevated permissions.

<b>Error Code</b>	OC10032
<b>Text</b>	A problem occurred when collecting the certificates. Please retry the operation.
<b>Details</b>	A technical problem occurred when processing the certificate using MyID client services. This issue requires detailed troubleshooting by a system administrator. Please consult MyID documentation for more information.",
<b>Solution</b>	If this issue can be reproduced, examine logs from the MyID client service at the time the problem occurred. To access the MyID client service log information, right click on the MyID icon in the Windows system tray on the computer affected and select 'Show'. This information may need to be analyzed by Intercede support."

<b>Error Code</b>	OC10033
<b>Text</b>	Error notifying the server of sign out. Your client has still been signed out.
<b>Details</b>	A technical issued occurred when signing out. The session has been cleared on this computer but this issue should be reported to an administrator for further investigation if the problem persists.
<b>Solution</b>	<p>Confirm that the <code>authServerRevocationLocation</code> is correctly set, the <code>web.oauth2</code> web service has been configured correctly, and the database is reachable.</p> <p>The <code>authServerRevocationLocation</code> option is available in the <code>appSettings.js</code> file for the MyID Operator Client website, which is in the following folder on the web server by default:</p> <p><code>C:\Program Files\Intercede\MyID\OperatorClient</code></p> <p>The default value is:</p> <pre>authServerRevocationLocation: "/web.oauth2/connect/revocation",</pre>

<b>Error Code</b>	WS10000
<b>Text</b>	Server error
<b>Details</b>	An internal server error has occurred.
<b>Solution</b>	<p>Retry the operation; the cause could be a temporary issue such as a database timeout due to server load.</p> <p>This error may also occur if you have configured your system to use the web server to store images and have attempted to upload an image using the MyID Operator Client; this is not a supported configuration; see the <i>Displaying images stored on the web server</i> section in the <a href="#">MyID Operator Client</a> guide for details.</p> <p>If the problem persists, check the <b>System Events</b> and <b>Audit Reporting</b> workflows within MyID, then the <code>rest.core</code> logs for more information. For information on configuring logging, see the <i>MyID REST and authentication web services</i> section in the <a href="#">Configuring Logging</a> guide.</p>

<b>Error Code</b>	WS10001
<b>Text</b>	Unable to convert WSQ image to 378 biometric format
<b>Details</b>	The supplied WSQ image is either corrupt or invalid or the Aware components are not installed on the server.
<b>Solution</b>	<p>Check that the WSQ image is valid.</p> <p>Check that the Aware components are installed on the server.</p> <p>See the <i>Aware Fingerprint Capture</i> guide provided with the Aware Fingerprint Capture module.</p>

<b>Error Code</b>	WS10002
<b>Text</b>	Unable to retrieve the values for the specified selection box.
<b>Details</b>	A problem has occurred with a dynamic drop-down list, where the contents of one list depend on another; MyID was unable to call the stored procedure specified for the dependent list. This feature may have been implemented on a custom system using Project Designer.
<b>Solution</b>	Check that your linked picklists are configured correctly in Project Designer; if your custom system was provided by Intercede, contact customer support, quoting the error reference WS10002.

<b>Error Code</b>	WS10003
<b>Text</b>	Unable to retrieve the requested session information.
<b>Details</b>	There is an API method that allows you to retrieve information about the currently authenticated session. This error appears when there is a problem determining the session.
<b>Solution</b>	Re-authenticate and try again.

<b>Error Code</b>	WS10004
<b>Text</b>	Unable to generate the requested report file.
<b>Details</b>	There is no report matching the specified operation id in the database.
<b>Solution</b>	Check the ID of the report and try again.

<b>Error Code</b>	WS10005
<b>Text</b>	Unable to generate the requested EFT export file.
<b>Details</b>	When you export EFT files, MyID attempts to write them to the location specified in the <b>EFT export directory</b> configuration option (on the <b>Import &amp; Export</b> tab of the <b>Operation Settings</b> workflow), or to the <code>FileExport</code> folder under the MyID installation folder if this is not set. The MyID COM user must have write access to this folder.
<b>Solution</b>	Make sure the MyID COM user has write access to the export folder and try again.

<b>Error Code</b>	WS10006
<b>Text</b>	Unable to substitute values, entity name invalid.
<b>Details</b>	You have attempted to use a substitution code for the <b>Additional Identity LDAP Self-Service User Filter</b> configuration but have specified an entity other than <code>People</code> . You must use <code>People</code> in the substitution code; for example;  [[ <code>People.LogonName</code> ]]
<b>Solution</b>	See the <i>Setting up additional identities</i> section in the <a href="#">Administration Guide</a> for details of valid substitution codes.

<b>Error Code</b>	WS10007
<b>Text</b>	Unable to substitute values, field name invalid.
<b>Details</b>	You have attempted to use a substitution code for the <b>Additional Identity LDAP Self-Service User Filter</b> configuration but have specified a field that is not in the <code>vPeopleUserAccounts</code> view.
<b>Solution</b>	See the <i>Setting up additional identities</i> section in the <a href="#">Administration Guide</a> for details of valid substitution codes.

<b>Error Code</b>	WS20000
<b>Text</b>	Server configuration error
<b>Details</b>	There is a problem with the server configuration.
<b>Solution</b>	Check the <b>System Events, Audit Reporting</b> workflows within MyID, then the <code>rest.core</code> logs for more information. For information on configuring logging, see the <i>MyID REST and authentication web services</i> section in the <a href="#">Configuring Logging</a> guide.

<b>Error Code</b>	WS20001
<b>Text</b>	Server configuration error - DataDictionary is inconsistent
<b>Details</b>	The MyID Project Designer configuration is incorrect, preventing the server from starting correctly.
<b>Solution</b>	If you are using MyID Project Designer to develop your own custom configuration, use Project Designer to correct the configuration and reapply the project configuration.  Check the logs for information about the faulty data. For information on configuring logging, see the <i>MyID REST and authentication web services</i> section in the <a href="#">Configuring Logging</a> guide.

<b>Error Code</b>	WS20002
<b>Text</b>	Server configuration error - SearchCriteria is inconsistent
<b>Details</b>	The definition of the search criteria is incorrect.
<b>Solution</b>	<p>This requires a database fix.</p> <p>You must contact customer support quoting reference SUP-327 and provide details of which search operation is experiencing this error.</p> <p>You will also be asked to provide log files; for information on configuring logging, see the <i>MyID REST and authentication web services</i> section in the <a href="#">Configuring Logging</a> guide.</p>

<b>Error Code</b>	WS30000
<b>Text</b>	Minimum data not supplied
<b>Details</b>	There has been a problem with the processing of information entered on the form.
<b>Solution</b>	Check the data you have entered and try again.

<b>Error Code</b>	WS30001
<b>Text</b>	Invalid data supplied
<b>Details</b>	There has been a problem with the processing of information entered on the form.
<b>Solution</b>	Check the data you have entered and try again.

<b>Error Code</b>	WS30002
<b>Text</b>	Validation problem, the value for <field name>, <details>
<b>Details</b>	This error occurs when the <field name> field contains a value that is not allowed. This is a generic error; you are more likely to see a more specific error that gives a reason for the validation problem.
<b>Solution</b>	Check the values you have entered for the specified field and try again.

<b>Error Code</b>	WS30003
<b>Text</b>	Invalid person id specified
<b>Details</b>	The person you have specified does not exist; for example, the person may have been removed by another operator. Alternatively, you have specified a person over whom you do not have permission.
<b>Solution</b>	Check the data you have entered and try again.



<b>Error Code</b>	WS30004
<b>Text</b>	Validation problem, the value for <field name>, invalid role specified
<b>Details</b>	You have selected a role that is not allowed.
<b>Solution</b>	Check the roles you have selected and try again.

<b>Error Code</b>	WS30005
<b>Text</b>	Validation problem, the value for <field name>, must be no more than <number> characters
<b>Details</b>	The value you have entered for the specified field is too long.
<b>Solution</b>	Provide a shorter value for the field and try again.

<b>Error Code</b>	WS30006
<b>Text</b>	Validation problem, the value for <field name>, invalid value for search criteria
<b>Details</b>	The value you have entered for the specified field is not allowed as part of the search criteria.
<b>Solution</b>	Check the search criteria you have entered and try again.

<b>Error Code</b>	WS30007
<b>Text</b>	Validation problem, the value for <field name>, must contain a value
<b>Details</b>	You have not entered a value for the specified field.
<b>Solution</b>	Enter a value for the specified field and try again.

<b>Error Code</b>	WS30008
<b>Text</b>	Validation problem, the value for <field name>, is not a selectable value
<b>Details</b>	You have provided a value for the specified field that is not available in the drop-down list.
<b>Solution</b>	Check the value you have entered for the specified field and try again.

<b>Error Code</b>	WS30009
<b>Text</b>	Validation problem, the value for <field name>, <details>
<b>Details</b>	You have entered a value for the specified field that contains a value that is not allowed. The <details> provide more information about why this value was not allowed; for example, "must be a date in the past" or "must be alphanumeric".
<b>Solution</b>	Check the value you have entered for the specified field and try again.

<b>Error Code</b>	WS30010
<b>Text</b>	Validation problem, the value for <field name>, fails Validation rule <rule>
<b>Details</b>	You have entered a value for the specified field that contains a value that is not allowed. There is no description for this validation rule; it may be a custom validation rule.
<b>Solution</b>	Check the values you have entered for the specified field and try again.

<b>Error Code</b>	WS30011
<b>Text</b>	Validation problem, the value for <field name>, can only be 0 or 1
<b>Details</b>	You have entered a value for the specified field other than 0 or 1, and this field only allows those values.
<b>Solution</b>	Enter a value of 0 or 1 in the specified field and try again.

<b>Error Code</b>	WS30012
<b>Text</b>	Validation problem, the value for <field name>, must be a number
<b>Details</b>	You have entered a value for the specified field that is not a number.
<b>Solution</b>	Enter a number in the specified field and try again.

<b>Error Code</b>	WS30013
<b>Text</b>	Validation problem, the value for <field name>, must be a valid uuid
<b>Details</b>	A field has been supplied to the server that is not a valid UUID (universally unique identifier).
<b>Solution</b>	<p>If you are using the MyID Operator Client, retry the operation. If the problem persists, contact customer support, quoting reference SUP-328.</p> <p>You will be asked to provide log files; for information on configuring logging, see the <i>MyID REST and authentication web services</i> section in the <a href="#">Configuring Logging</a> guide.</p>

<b>Error Code</b>	WS30014
<b>Text</b>	Validation problem, the value for <field name>, must be a date or datetime
<b>Details</b>	You have entered a value for the specified field that is not a valid date or time and date value.
<b>Solution</b>	Check the value you have entered and try again.

<b>Error Code</b>	WS30015
<b>Text</b>	Validation problem, the value for <field name>, is mandatory
<b>Details</b>	You have not entered a value for the specified field; this field is mandatory.
<b>Solution</b>	Enter a value for the specified field and try again.

<b>Error Code</b>	WS30016
<b>Text</b>	Validation problem, the value for <field name>, is not a valid StatusMapping
<b>Details</b>	The value you have entered for the specified field is not a valid certificate reason (StatusMapping).
<b>Solution</b>	Check the value you have entered and try again.

<b>Error Code</b>	WS30017
<b>Text</b>	Validation problem, the value for 'First Name', and 'Last Name' must be provided.
<b>Details</b>	You have attempted to save a person's record with neither a first name nor a last name. You must include one or both of these values.
<b>Solution</b>	Ensure that you have specified one or both of the <b>First Name</b> and <b>Last Name</b> fields, then attempt to save the person's record again.

<b>Error Code</b>	WS30018
<b>Text</b>	Validation problem, the value for <field name>, is not an allowed value
<b>Details</b>	The value you have entered for the specified field is not permitted.
<b>Solution</b>	Check the value you have entered and try again.

<b>Error Code</b>	WS30019
<b>Text</b>	Validation problem, the value for <field name>, is not correctly encoded binary data
<b>Details</b>	You have attempted to submit a file (for example, an image file) but the binary data file is not encoded correctly.
<b>Solution</b>	Check the file you are submitting and try again.

<b>Error Code</b>	WS30020
<b>Text</b>	The value provided contains one or more characters which are disallowed.
<b>Details</b>	The provided password is not valid.
<b>Solution</b>	Provide a password that contains allowed characters and try again.

<b>Error Code</b>	WS30021
<b>Text</b>	Biometric samples of the required type cannot be found for the user.
<b>Details</b>	<p>Adjudication requires fingerprint samples captured using a 10-Slap enrollment device. Check that you have captured new fingerprints before submitting for adjudication.</p> <p>This error may also occur if the <b>Fingerprints identification check enabled</b> configuration option (on the <b>Biometrics</b> page of the <b>Operation Settings</b> workflow) is not set.</p>
<b>Solution</b>	See the <i>Adjudication Integration Guide</i> provided with the Adjudication module and the <i>Aware Fingerprint Capture</i> guide provided with the Aware Fingerprint Capture module for details.

<b>Error Code</b>	WS30022
<b>Text</b>	must be a date in the future
<b>Details</b>	The field failed validation as the provided value can only be a date in the future.
<b>Solution</b>	Provide a date in the future and try again.

<b>Error Code</b>	WS30023
<b>Text</b>	must be a date in the past
<b>Details</b>	The field failed validation as the provided value can only be a date in the past.
<b>Solution</b>	Provide a date in the past and try again.

<b>Error Code</b>	WS30024
<b>Text</b>	Serial number range information must be supplied.
<b>Details</b>	You have attempted to import devices without providing a serial number range.
<b>Solution</b>	Provide a range of serial numbers to import and try again.

<b>Error Code</b>	WS30025
<b>Text</b>	must be a date in the past within correct range
<b>Details</b>	The field failed validation as the provided value must be a date within correct range in the past.
<b>Solution</b>	Provide a date in the past in the correct range and try again.

<b>Error Code</b>	WS30026
<b>Text</b>	must be a date in the future within correct range
<b>Details</b>	The field failed validation as the provided value must be a date within correct range in the future.
<b>Solution</b>	Provide a date in the future in the correct range and try again.

<b>Error Code</b>	WS40000
<b>Text</b>	Validation problem, the value for 'Distinguished Name', already exists
<b>Details</b>	You have specified a Distinguished Name for the person that is already used for a different person, and your system is configured to require unique DNs.
<b>Solution</b>	Enter a unique DN for the person and try again. Alternatively, you can configure your system to allow duplicate DNs; the <b>Allow duplicate DN</b> configuration option determines whether unique DN values are required; see the <i>LDAP page (Operation Settings)</i> section in the <a href="#">Administration Guide</a> for details.

<b>Error Code</b>	WS40001
<b>Text</b>	Validation problem, the value for 'Logon', already exists
<b>Details</b>	You have specified a Logon name for the person that is already used for another person. Logon names must be unique.
<b>Solution</b>	Enter a unique logon name and try again.

<b>Error Code</b>	WS40002
<b>Text</b>	The specified Credential Profile could not be found
<b>Details</b>	The credential profile you selected is no longer available.
<b>Solution</b>	Select a different credential profile and try again.

<b>Error Code</b>	WS40003
<b>Text</b>	Duplicate group name is not allowed (a group with this name already exists for this parent)
<b>Details</b>	You have specified a group name that already exists. Groups that are located under the same parent group must have unique names.
<b>Solution</b>	Enter a new group name and try again.

<b>Error Code</b>	WS40004
<b>Text</b>	Unable to get default roles for group
<b>Details</b>	When adding a person, default roles are retrieved from that person's group – this operation has failed.
<b>Solution</b>	Retry the operation. Make sure that the group you have selected is valid.

<b>Error Code</b>	WS40005
<b>Text</b>	The item referenced was not found
<b>Details</b>	You have selected an item (for example, a person, device, or request) that does not exist, has been removed by another operator, or over which you do not have permission.
<b>Solution</b>	<p>Retry the operation. If the problem persists, check that you have sufficient privilege to access the item.</p> <p>You may have attempted to carry out an operation on a request that has been canceled. Make sure the item is in the correct status.</p> <p>Check the MyID <b>System Events</b> workflow and the <code>rest.core</code> logs for more information. For information on configuring logging, see the <i>MyID REST and authentication web services</i> section in the <a href="#">Configuring Logging</a> guide.</p>

<b>Error Code</b>	WS40006
<b>Text</b>	The required group, <group name>, is not available
<b>Details</b>	You have specified a group that is not available.
<b>Solution</b>	Check the group name and try again.

<b>Error Code</b>	WS40007
<b>Text</b>	The user location in the directory could not be matched to an existing group
<b>Details</b>	When importing a person to the MyID database from a directory, the person could not be matched to a group in MyID.
<b>Solution</b>	<p>Try one of the following:</p> <ul style="list-style-type: none"><li>• Manually pick a MyID group for the user to be imported into and save the record again.</li><li>• Use the <b>Edit Groups</b> workflow in MyID Desktop and import the LDAP groups into MyID.</li></ul> <p>See the <i>Importing an LDAP directory branch</i> section in the <a href="#">Operator's Guide</a> for details.</p> <ul style="list-style-type: none"><li>• If you want groups to be automatically imported from LDAP, set the <b>Automatically create MyID groups from the Organizational Unit of imported users</b> configuration option on the <b>LDAP</b> page of the <b>Operation Settings</b> workflow.</li></ul>

<b>Error Code</b>	WS40008
<b>Text</b>	Directory synchronization is not available with this API due to configuration or role limitations
<b>Details</b>	<p>An attempt has been made to synchronize a person with the directory manually; however, this operation is disabled due to system configuration.</p> <p>Directory synchronization is controlled by the following configuration:</p> <ul style="list-style-type: none"><li>• If the <b>Background Update</b> configuration option is turned on, people are automatically updated in the MyID database when they are retrieved. In this situation it does not make sense to synchronize the person from LDAP manually. An attempt to trigger a manual synchronization would produce this error; however, the button does not appear.</li><li>• If the <b>Background Update</b> configuration option is turned off, if the caller has roles to enable manual directory sync, the operator can request a directory synchronization by clicking the button. In this situation, this error code will not occur.</li></ul>
<b>Solution</b>	As the button appears only when it is allowed by system configuration, this error is unlikely to appear. However, if it does appear, it means that a client is out of step with the server configuration. Shut down the client, clear the browser cache, and try the operation again.

<b>Error Code</b>	WS40009
<b>Text</b>	You must provide a reason for rejecting the specified request.
<b>Details</b>	You have attempted to reject a request without specifying a reason. A reason is mandatory when rejecting a request.
<b>Solution</b>	Specify a reason for rejecting the request and try again.

<b>Error Code</b>	WS40010
<b>Text</b>	You must provide a reason for canceling the specified request.
<b>Details</b>	You have attempted to cancel a request without specifying a reason. A reason is mandatory when canceling a request.
<b>Solution</b>	Specify a reason for canceling the request and try again.

<b>Error Code</b>	WS40011
<b>Text</b>	When creating or approving a request, the job expiry date must be in the future. Either the newly selected request maximum expiry date, or the user maximum expiry date of the request target is in the past.
<b>Details</b>	Either the selected maximum expiry date for the request, or the user maximum expiry date is in the past.
<b>Solution</b>	Specify a date for the request that is in the future and try again.

<b>Error Code</b>	WS40012
<b>Text</b>	The device cannot be replaced because it is not issued
<b>Details</b>	You have specified a device to be replaced, but MyID does not recognize it as an issued device.
<b>Solution</b>	Specify a valid issued device and try again.  This error may occur if you attempt to update a key recovery card; key recovery cards are not fully-featured MyID cards and can only be used for key recovery.

<b>Error Code</b>	WS40013
<b>Text</b>	The device cannot be replaced because it is has already expired
<b>Details</b>	You have specified a device to be replaced, but it has already expired.
<b>Solution</b>	Specify a currently-issued device to be replaced, or request a new device to replace the original expired device.



<b>Error Code</b>	WS40014
<b>Text</b>	The device cannot be replaced because it is too close to its expiry date
<b>Details</b>	<p>You have attempted to replace a device, but it will expire soon. You must renew the device instead.</p> <p>By default, the renewal window is 42 days; this is configured by the <b>Card Renewal Period</b> option on the <b>Devices</b> page of the <b>Operation Settings</b> workflow. You can renew a card if its expiry date is within this window.</p>
<b>Solution</b>	Renew the device.

<b>Error Code</b>	WS40015
<b>Text</b>	The device cannot be replaced because it does not have a credential profile
<b>Details</b>	You have attempted to replace a device, but the credential profile used to issue the device has been removed.
<b>Solution</b>	Cancel the device and issue a new one.

<b>Error Code</b>	WS40016
<b>Text</b>	The device cannot be renewed because its remaining lifetime does not fall within the configured window for renewals
<b>Details</b>	<p>By default, the renewal window is 42 days; this is configured by the <b>Card Renewal Period</b> option on the <b>Devices</b> page of the <b>Operation Settings</b> workflow. You can renew a card if its expiry date is within this window.</p>
<b>Solution</b>	Wait for the device to fall within the window for renewals before trying again.

<b>Error Code</b>	WS40017
<b>Text</b>	You must provide at least one resource name.
<b>Details</b>	When requesting translations a resource name must be specified.
<b>Solution</b>	Ensure that the resource name is specified; see the Swagger documentation for the MyID Core API for more details.

<b>Error Code</b>	WS40018
<b>Text</b>	You must provide a language.
<b>Details</b>	The language value was not specified in the body in call to set the language.
<b>Solution</b>	Ensure that the language is specified; see the Swagger documentation for the MyID Core API for more details.

<b>Error Code</b>	WS40019
<b>Text</b>	The specified language has not been configured for use.
<b>Details</b>	There is no resource file on the server for the language specified.
<b>Solution</b>	Create a new resource file for the specified language. For information about translating the MyID interface, contact customer support quoting reference SUP-138.

<b>Error Code</b>	WS40020
<b>Text</b>	No languages have been configured for use.
<b>Details</b>	There are no resource files installed on the server.
<b>Solution</b>	Your installation appears to have become corrupt. Check your backups.

<b>Error Code</b>	WS40021
<b>Text</b>	The specified entity does not exist.
<b>Details</b>	A report is attempting to reference an unsupported entity.
<b>Solution</b>	<p>The report is incorrectly defined. Redefine it to reference one of the following:</p> <ul style="list-style-type: none"><li>• adjudications</li><li>• audits</li><li>• authCodes</li><li>• binaries</li><li>• bioSamples</li><li>• cardProfiles</li><li>• controls</li><li>• devices</li><li>• directories</li><li>• directoryGroups</li><li>• directoryPeople</li><li>• groups</li><li>• installs</li><li>• logEvents</li><li>• notifications</li><li>• people</li><li>• reportDefinitions</li><li>• reports</li><li>• requests</li><li>• sessions</li><li>• settings</li></ul>

<b>Error Code</b>	WS40022
<b>Text</b>	The specified operation id is not a valid search operation.
<b>Details</b>	There is no report matching the specified operation id in the database.
<b>Solution</b>	Check the ID of the report and try again.

<b>Error Code</b>	WS40023
<b>Text</b>	The specified search operation id cannot be used for this endpoint.
<b>Details</b>	Each operation id is linked to a specific entity; for example, device, people, request.
<b>Solution</b>	Check the operation ID and try again.

<b>Error Code</b>	WS40024
<b>Text</b>	The delivery mechanism specified does not exist or is not allowed for this operation.
<b>Details</b>	Only specific delivery mechanisms are allowed based on the specific operation.
<b>Solution</b>	Get a list of suitable delivery mechanisms by making a call to: <code>GET /api/Devices/{id}/codes/deliveryMechanisms</code> See the Swagger documentation for the MyID Core API for more details.

<b>Error Code</b>	WS40025
<b>Text</b>	The user does not have the required contact details for this delivery mechanism.
<b>Details</b>	A request to send the user an email notification when the user does not have an email address or an SMS notification when the user does not have a cell phone number was attempted. The audit of the attempt will detail which property is required.
<b>Solution</b>	Update the person to specify their email address or mobile number.

<b>Error Code</b>	WS40026
<b>Text</b>	The specified delivery mechanism is not enabled for this operation.
<b>Details</b>	A request to send the user a notification was attempted when the email template is not enabled. The audit of the attempt will detail which email template was selected.
<b>Solution</b>	Use the <b>Email Templates</b> workflow to enable the required email template or select an alternative email template.

<b>Error Code</b>	WS40027
<b>Text</b>	An auth code action must be supplied.
<b>Details</b>	When requesting a list of delivery mechanisms an action must be specified.
<b>Solution</b>	See the Swagger documentation for the MyID Core API for more details.

<b>Error Code</b>	WS40028
<b>Text</b>	The specified auth code action: {0}, is not supported.
<b>Details</b>	The specified action is not supported.
<b>Solution</b>	<p>The action specified must be one of the following</p> <ul style="list-style-type: none"><li>• Activate</li><li>• Collect</li><li>• Logon</li><li>• Unlock</li></ul>

<b>Error Code</b>	WS40029										
<b>Text</b>	The specified auth code action: {0}, is not supported for this item.										
<b>Details</b>	Each action is linked to a specific entity.										
<b>Solution</b>	<p>Ensure you only select an action appropriate to the entity:</p> <table><tr><th>Action</th><th>Entity</th></tr><tr><td>Activate</td><td>Devices</td></tr><tr><td>Collect</td><td>Requests</td></tr><tr><td>Logon</td><td>People</td></tr><tr><td>Unlock</td><td>Devices</td></tr></table>	Action	Entity	Activate	Devices	Collect	Requests	Logon	People	Unlock	Devices
Action	Entity										
Activate	Devices										
Collect	Requests										
Logon	People										
Unlock	Devices										

<b>Error Code</b>	WS40030
<b>Text</b>	Email notifications have not been configured. Please contact your administrator.
<b>Details</b>	An attempt to send a notification was made when notifications are not configured.
<b>Solution</b>	See the <i>Setting up email</i> section in the <b>Advanced Configuration Guide</b> for details.

<b>Error Code</b>	WS40031
<b>Text</b>	This device is already assigned, and must be canceled before it can be reassigned to a different person. The system is not configured to allow unrestricted cancellation.
<b>Details</b>	The <b>Unrestricted Cancellation</b> option in the credential profile is not set, and the operator has selected a device that is already issued or assigned to another request.
<b>Solution</b>	Cancel the device before attempting to assign it.  Alternatively, if you want to assign a device without first canceling it, you must set the <b>Unrestricted Cancellation</b> option in the credential profile. This option appears only if the <b>Enable unrestricted cancellation</b> option on the <b>Issuance Processes</b> tab of the <b>Operation Settings</b> workflow is set to <b>Yes</b>

<b>Error Code</b>	WS40032
<b>Text</b>	This device has a disposal status that prevents it being issued again.
<b>Details</b>	The selected device has a disposal status of 'Lost', 'Disposed' or 'Collected'.
<b>Solution</b>	Either select a different device, or change the disposal status of the selected device.

<b>Error Code</b>	WS40033
<b>Text</b>	This device cannot be issued or updated by MyID.
<b>Details</b>	The selected device is 'Unmanaged', does not have GlobalPlatform or 9B keys, or cannot be issued due to secure by default configuration.
<b>Solution</b>	Either select a different device, or ensure the correct keys have been entered into MyID to make the selected device issuable.

<b>Error Code</b>	WS40034
<b>Text</b>	The request already has an assigned device.
<b>Details</b>	The request already has a device assigned.
<b>Solution</b>	Either select a different device, or unassign the selected device from its current request.

<b>Error Code</b>	WS40035
<b>Text</b>	The request type does not permit device assignment.
<b>Details</b>	The selected request is not an issuance or replacement issuance request.
<b>Solution</b>	This request cannot be used to assign a device; select a different request.

<b>Error Code</b>	WS40036
<b>Text</b>	The request is not awaiting issuance or awaiting validation.
<b>Details</b>	The selected request is not at status 'Awaiting Issue' or 'Awaiting Validation'.
<b>Solution</b>	Adjust the selected request to be an appropriate status before assigning a device to it.

<b>Error Code</b>	WS40037
<b>Text</b>	The request is for a person that is not within the authenticated operators scope
<b>Details</b>	The target user for the request is outside the scope of the authenticated operator.
<b>Solution</b>	Either adjust your MyID group and role settings to ensure the target for the request is in scope of the authenticated operator, or assign the device to the request using a different operator who has scope over the target for the request.

<b>Error Code</b>	WS40038
<b>Text</b>	This device is not known to MyID and the credential profile can only be used with known serial numbers.
<b>Details</b>	The selected device is not known to the MyID database, and the credential profile for the request has <b>Only Issue to Known Serial Numbers</b> configured.
<b>Solution</b>	Use a different device that is known to the MyID database. Alternatively, import the device to the MyID database using the <b>Import Serial Numbers</b> workflow, or change the credential profile to deselect the <b>Only Issue to Known Serial Numbers</b> option.

<b>Error Code</b>	WS40039
<b>Text</b>	This device does not meet the requirements of the credential profile.
<b>Details</b>	The device selected is not a 'Contact' or 'Contactless' card or the credential profile is not of encoding type 'Contact' or 'Contactless'. 'Contact' cards can only be selected for 'Contact' encoding type credential profiles, and 'Contactless' cards can only be selected for 'Contactless' encoding type credential profiles.
<b>Solution</b>	Select a device that is compatible with the credential profile assigned to the request.

<b>Error Code</b>	WS40040
<b>Text</b>	The request does not have an assigned device.
<b>Details</b>	The selected request does not have a device assigned to it.
<b>Solution</b>	Ensure the request has a device assigned to it, or select a different request.

<b>Error Code</b>	WS40041
<b>Text</b>	This device is already assigned, and must be canceled before it can be reassigned to a different person.
<b>Details</b>	The <b>Unrestricted Cancellation</b> option in the credential profile is not set, and the operator has selected a device that is already issued or assigned to another request.
<b>Solution</b>	Cancel the device before attempting to assign it.  Alternatively, if you want to assign a device without first canceling it, you must set the <b>Unrestricted Cancellation</b> option in the credential profile. This option appears only if the <b>Enable unrestricted cancellation</b> option on the <b>Issuance Processes</b> tab of the <b>Operation Settings</b> workflow is set to <b>Yes</b> .

<b>Error Code</b>	WS40042
<b>Text</b>	This device is assigned to the current operator.
<b>Details</b>	The selected device is already assigned to the current operator.
<b>Solution</b>	Select a different device.

<b>Error Code</b>	WS40044
<b>Text</b>	There are no status mappings available for the selected operation.
<b>Details</b>	The attempted operation requires a status mapping to be selected, but there are no status mappings available for that operation ID.
<b>Solution</b>	You can check the <code>vAllowedStatuses</code> view in the database, which shows the operations that have corresponding status mappings.

<b>Error Code</b>	WS40045
<b>Text</b>	The device cannot be updated because it has already expired.
<b>Details</b>	To perform this operation, the selected device must not have expired.  This error may occur when attempting to reinstate a device, if the original device has expired.
<b>Solution</b>	Either renew the device, or issue a new device.



<b>Error Code</b>	WS40046
<b>Text</b>	The device cannot be updated because the issuance process has not been completed.
<b>Details</b>	The device must have a process status of Active and be assigned to a person.
<b>Solution</b>	Ensure that the device has an owner, and that it is issued. This error may occur if you attempt to update a key recovery card; key recovery cards are not fully-featured MyID cards and can only be used for key recovery.

<b>Error Code</b>	WS40047
<b>Text</b>	The device cannot be updated because it does not have a credential profile.
<b>Details</b>	The selected device must have a credential profile.
<b>Solution</b>	Ensure that the device has not been canceled or erased. Reissue the device if necessary.

<b>Error Code</b>	WS40048
<b>Text</b>	The location cannot be updated because an existing location has the requested name.
<b>Details</b>	You have attempted to create or edit a location but have specified the name of an existing location. Location names must be unique.
<b>Solution</b>	Type a different name and try again.

<b>Error Code</b>	WS40049
<b>Text</b>	The device cannot be transferred because it is in an invalid state.
<b>Details</b>	You have attempted to transfer a device, but it is currently assigned to a person or is already allocated to a stock transfer.
<b>Solution</b>	Select a different device and try again.

<b>Error Code</b>	WS40050
<b>Text</b>	The device cannot be canceled and have its disposal status set to <Status>.
<b>Details</b>	You have attempted to cancel a device and set its disposal status to an invalid value.
<b>Solution</b>	Select an appropriate disposal status for the device.

<b>Error Code</b>	WS40051
<b>Text</b>	The device is still active and has not expired, so cannot have its disposal status changed.
<b>Details</b>	You have attempted to set the disposal status for a device that is still active.
<b>Solution</b>	Cancel the device first then set the disposal status.

<b>Error Code</b>	WS40052
<b>Text</b>	The device has expired but the system is configured to not allow expired devices to have their disposal status changed.
<b>Details</b>	You have attempted to set the disposal status for a device that has expired, but the <b>Allow disposal of expired devices</b> configuration option is set to <b>No</b> .
<b>Solution</b>	Set the <b>Allow disposal of expired devices</b> configuration option to <b>Yes</b> and try again.

<b>Error Code</b>	WS40053
<b>Text</b>	The device selected cannot be disposed. Please refer to product documentation for further guidance.
<b>Details</b>	You have specified a device of type <code>ServerCredential</code> for disposal using the API; you cannot set the disposal status of these devices.
<b>Solution</b>	Select a different device and try again.

<b>Error Code</b>	WS40054
<b>Text</b>	The additional identity specified already exists.
<b>Details</b>	You have attempted to add an additional identity to a person who already has that user and certificate policy selected as an additional identity.
<b>Solution</b>	Select a different user or certificate policy and try again.

<b>Error Code</b>	WS40055
<b>Text</b>	The request doesn't have an assigned device
<b>Details</b>	A server document has been attempted to be generated for a request that does not have an assigned device.
<b>Solution</b>	Select a different request and try again.

<b>Error Code</b>	WS40056
<b>Text</b>	The credential profile does not have a document for the requested doctype
<b>Details</b>	You have attempted to print a document, but there is no document template selected in the credential profile.
<b>Solution</b>	Edit the credential profile to select a document template and try again.

<b>Error Code</b>	WS40057
<b>Text</b>	Unable to generate a server document, the request type is invalid.
<b>Details</b>	<p>You have attempted to print a document for a type of request that does not support printing documents.</p> <p>This may also occur if you have attempted to print a document for a request that has been canceled.</p>
<b>Solution</b>	Select a different request and try again.

<b>Error Code</b>	WS40058
<b>Text</b>	Unable to generate a server document, the status of the request is invalid.
<b>Details</b>	You have attempted to print a document for a request that has not been completed.
<b>Solution</b>	Complete the request and try to print the document again.

<b>Error Code</b>	WS40059
<b>Text</b>	Unable to generate a server document, the collection period is over.
<b>Details</b>	Your system has been customized with a time limit for printing mailing documents, and it has been too long since the job was completed.
<b>Solution</b>	You cannot print a document for this device. If you want to print a document, you must issue a new device.

<b>Error Code</b>	WS40060
<b>Text</b>	Unable to generate a server document, PIN Mailer request not found.
<b>Details</b>	You have attempted to print a PIN mailer, but there is no request for the PIN mailer.
<b>Solution</b>	Select a different request and try again. Alternatively, ensure that the original request has been collected, and a PIN mailer request has been generated.

<b>Error Code</b>	WS40061
<b>Text</b>	Unable to generate a server document, unknown document type.
<b>Details</b>	You have attempted to print a document, but the specified document type is not correct.
<b>Solution</b>	Check the document type and try again.

<b>Error Code</b>	WS40062
<b>Text</b>	The device is currently assigned and cannot be reinstated
<b>Details</b>	You have attempted to reinstate a device that is still assigned to a person.
<b>Solution</b>	Choose a different device and try again.

<b>Error Code</b>	WS40063
<b>Text</b>	The device has not previously been assigned and cannot be reinstated
<b>Details</b>	You have attempted to reinstate a device, but the device has not previously been assigned to a person on the current MyID system, so cannot be reinstated.
<b>Solution</b>	Choose a different device and try again.

<b>Error Code</b>	WS40064
<b>Text</b>	The device is in an invalid state and cannot be reinstated
<b>Details</b>	You have attempted to reinstate a device, but it is not in the correct state.
<b>Solution</b>	Choose a different device and try again.

<b>Error Code</b>	WS40065
<b>Text</b>	Device cannot be reinstated because it is not a card
<b>Details</b>	You have attempted to reinstate a device, but it is not a smart card. For example, you cannot reinstate VSCs or mobile identities.
<b>Solution</b>	Choose a different device and try again.

<b>Error Code</b>	WS40066
<b>Text</b>	The certificate cannot have its renewal status changed as it is not currently issued.
<b>Details</b>	Certificate has not yet been successfully collected, and needs to be fully issued before being able to change the renewal settings.
<b>Solution</b>	Collect the certificate and ensure that it is fully issued, then try again.

<b>Error Code</b>	WS40068
<b>Text</b>	The directory connection failed with the supplied credentials.
<b>Details</b>	You have attempted a test or verification on a directory connection, but the connection has failed.
<b>Solution</b>	Check that you have provided the correct details for your directory.

<b>Error Code</b>	WS40069
<b>Text</b>	Supplied credentials cannot build a valid server location.
<b>Details</b>	You have attempted to test or update the details for a directory connection, but MyID cannot construct a valid location for your directory.
<b>Solution</b>	Make sure that you have provided all of the required information, including the host and port.

<b>Error Code</b>	WS40072
<b>Text</b>	User Relationship already exists
<b>Details</b>	You have attempted to create a relationship between two people accounts, but the relationship already exists.
<b>Solution</b>	Make sure you have selected the correct people and relationship type.

<b>Error Code</b>	WS50000
<b>Text</b>	Your current authentication level cannot access this information. The logon credential used, roles that logon credential can access and scope available to those roles may limit your access
<b>Details</b>	You do not have permission to perform the requested operation.
<b>Solution</b>	<p>Check the roles and scope for the operator who is attempting to carry out this operation. It is possible to have different scopes for different operations; for example, you may be allowed to view all people in the system, but only be allowed to edit people from a particular group.</p> <p>Check the MyID <b>System Events</b> and <b>Audit Reporting</b> workflows for more information about the operation being attempted.</p>

<b>Error Code</b>	WS50001
<b>Text</b>	Licence Limit Reached
<b>Details</b>	You have attempted to add a person or request a device but have reached the maximum number of people or devices.
<b>Solution</b>	Either remove some people or devices that are no longer required, or request extra licenses from Intercede. See the <i>Requesting licenses</i> section in the <a href="#">Administration Guide</a> for details.

<b>Error Code</b>	WS50002
<b>Text</b>	You do not have permission to update your own device
<b>Details</b>	The system is configured using the <b>Self-service</b> option (on the <b>Self-Service</b> page of the <b>Security Settings</b> workflow) to prevent you from performing updates to devices that belong to you; for example, you are not allowed to enable a disabled device that belongs to you.
<b>Solution</b>	Ask another operator to update the device for you.

<b>Error Code</b>	WS50003
<b>Text</b>	You do not have permission to update the device you authenticated with
<b>Details</b>	You have attempted to perform an update on the device that you logged on with. This is not allowed.
<b>Solution</b>	Ask another operator to update the device for you.

<b>Error Code</b>	WS50004
<b>Text</b>	The system is not configured to allow you to edit your own information
<b>Details</b>	The system is configured to prevent you from updating your own details.
<b>Solution</b>	Ask another operator to edit your information.

<b>Error Code</b>	WS50005
<b>Text</b>	Searching for people in the database is disabled
<b>Details</b>	You have attempted to search for a person in the MyID database, but MyID is not configured to do so.
<b>Solution</b>	You can search the MyID database only if you have configured MyID to do so; you must set the <b>Search a directory</b> configuration option to <b>No</b> or <b>Ask</b> . See the <i>LDAP page (Operation Settings)</i> section in the <a href="#">Administration Guide</a> for details.

<b>Error Code</b>	WS50006
<b>Text</b>	Searching for people in the directory is disabled
<b>Details</b>	You have attempted to search for a person in an attached directory, but MyID is not configured to do so.
<b>Solution</b>	You can search a directory only if you have configured MyID to do so; you must set the <b>Search a directory</b> configuration option to <b>Yes</b> or <b>Ask</b> . See the <i>LDAP page (Operation Settings)</i> section in the <a href="#">Administration Guide</a> for details.

<b>Error Code</b>	WS50007
<b>Text</b>	Invalid job status change
<b>Details</b>	You have attempted to update a request job to a status that is not permitted.
<b>Solution</b>	<p>The MyID Operator Client prevents you from making changes that are not permitted; however, it is possible that another operator has made a change to the status of the request job at the same time.</p> <p>Retry the operation; if the problem persists, close the Operator Client, clear the browser cache, and try again. If the problem persists further, check the MyID <b>System Events</b> and <b>Audit Reporting</b> workflows.</p>

<b>Error Code</b>	WS50008
<b>Text</b>	Your assigned roles do not have permission to request the credential profile specified
<b>Details</b>	You have specified a credential profile to which you do not have access.
<b>Solution</b>	<p>The credential profiles available depend on the role of the operator and the role of the person for whom you are requesting the device; see the details of the <b>Can Request</b> option in the <i>Constrain credential profile issuer</i> section in the <a href="#">Administration Guide</a>.</p>

<b>Error Code</b>	WS50009
<b>Text</b>	It is not possible to create requests for yourself or your devices.
<b>Details</b>	<p>This message occurs when an attempt is made by an operator to request their own credentials. It could occur when:</p> <ul style="list-style-type: none"><li>• Attempting to request a replacement for one of their devices.</li><li>• Attempting to request a renewal for one of their devices.</li><li>• Attempting to request a device for themselves (<b>Note:</b> The button for this is not available in MyID Operator Client).</li><li>• Attempting to request an update for one of their devices.</li></ul>
<b>Solution</b>	Ask another operator to carry out the operation.

<b>Error Code</b>	WS50010
<b>Text</b>	Your assigned roles do not have permission to approve or reject requests for this credential profile
<b>Details</b>	You have attempted to approve or reject a request that uses a credential profile that you are not allowed to validate.
<b>Solution</b>	<p>The credential profiles you can validate depend on your role; see the details of the <b>Can Validate</b> option in the <i>Constrain credential profile validator</i> section in the <a href="#">Administration Guide</a>.</p>

<b>Error Code</b>	WS50011
<b>Text</b>	The person selected does not have a role assigned that can hold the requested credential profile
<b>Details</b>	You have attempted to request a device using a credential profile to which the person does not have access.
<b>Solution</b>	The credential profiles available depend on the role of the operator and the role of the person for whom you are requesting the device; see the details of the <b>Can Receive</b> option in the <i>Linking credential profiles to roles</i> section in the <a href="#">Administration Guide</a> .

<b>Error Code</b>	WS50012
<b>Text</b>	The person selected does not have user data approved. The credential profile requires user data to be approved before it can be requested
<b>Details</b>	You have attempted to request a device using a credential profile that requires the person to have the User Data Approved flag set on their account, but the person does not have this flag set.
<b>Solution</b>	Either set the User Data Approved flag, or edit the credential profile so that it does not require this flag; see the details of the <b>Require user data to be approved</b> option in the <i>Issuance Settings</i> section in the <a href="#">Administration Guide</a> .

<b>Error Code</b>	WS50013
<b>Text</b>	The account selected is not compatible with this request (kind is mismatched)
<b>Details</b>	Requests cannot be made for the selected person. This could be due to this account being a special kind of record that represents a non-person entity (for example, for device identities).
<b>Solution</b>	<p>If you are trying to request a credential for a non-person, such as a device identity, use MyID Desktop instead; the MyID Operator Client does not currently support requests of this kind.</p> <p>If you continue to have problems, check the configuration of the credential profile you are using. You can also check the MyID <b>System Events</b> and <b>Audit Reporting</b> workflows.</p>

<b>Error Code</b>	WS50014
<b>Text</b>	You are not permitted to approve or reject requests that you have made
<b>Details</b>	You have attempted to approve or reject a request that you initiated. You cannot validate these requests.
<b>Solution</b>	Ask another operator to validate the request.



<b>Error Code</b>	WS50015
<b>Text</b>	You are not permitted to approve or reject requests that you will receive
<b>Details</b>	You have attempted to approve or reject a request for your own device. You cannot validate these requests.
<b>Solution</b>	Ask another operator to validate the request.

<b>Error Code</b>	WS50016
<b>Text</b>	The person selected does not have all required information for this credential profile. Check the Person History audit details to identify the missing requisite user data.
<b>Details</b>	You have specified a credential profile that has specific requisite user data requirements; the person you have specified does not meet those requirements.
<b>Solution</b>	<p>Carry out one of the following:</p> <ul style="list-style-type: none"><li>• Update the person's user account to meet the requisite data requirements.</li><li>• Update the credential profile to allow the configured user data.</li><li>• Select a different credential profile for which the user meets the requisite data requirements.</li></ul> <p>See the <i>Requisite User Data</i> section in the <a href="#">Administration Guide</a> for details.</p>

<b>Error Code</b>	WS50017
<b>Text</b>	The person selected does not have a Distinguished Name. This profile requires a Distinguished Name for credential issuance.
<b>Details</b>	You have specified a credential profile that requires a Distinguished Name for issuing its certificates.
<b>Solution</b>	Update the person's user account to provide a Distinguished Name.

<b>Error Code</b>	WS50018
<b>Text</b>	This credential profile can only be requested using a Derived Credential process
<b>Details</b>	You have specified a credential profile that is used for Derived Credentials.
<b>Solution</b>	Specify a different credential profile, or request the device using the appropriate process for derived credentials; for example, see the <i>Requesting a Derived Credential</i> section in the <a href="#">Derived Credentials Self-Service Request Portal</a> guide.

<b>Error Code</b>	WS50019
<b>Text</b>	Requests created using this API must include an appropriate encoding type
<b>Details</b>	The MyID Operator Client supports credential profiles with a restricted list of <b>Card Encoding</b> options.
<b>Solution</b>	<p>Check the credential profile you are trying to use. Either select a credential profile that is supported by the MyID Operator Client, or, if you need to use a credential profile that is not supported, use MyID Desktop instead.</p> <p>See the <i>Requesting a device for a person</i> section in the <a href="#">MyID Operator Client</a> guide.</p>

<b>Error Code</b>	WS50020
<b>Text</b>	A requested role has been excluded through the application of group role restrictions
<b>Details</b>	You have requested a role for a person that is not available because the person's group does not allow this role.
<b>Solution</b>	Either select a different role or amend the group so that it has access to the required role. See the <i>Changing a group</i> section in the <a href="#">Operator's Guide</a> for details.

<b>Error Code</b>	WS50021
<b>Text</b>	The scope requested for a role is greater than the maximum scope assignable by the current operator
<b>Details</b>	You have requested a scope level that is higher than your own scope. An operator cannot assign a scope higher than their own level.
<b>Solution</b>	Request a lower scope level that is at your own level or lower.

<b>Error Code</b>	WS50022
<b>Text</b>	A requested role is manager controlled and the operator does not hold the role that would permit them to assign it
<b>Details</b>	You have requested a role that is restricted by the <b>Managed By</b> option.
<b>Solution</b>	<p>Either select a different role, or update the Managed By option for the required role to contain one of your own roles; this will allow you to assign the role.</p> <p>See the <i>Controlling the assigning of roles</i> section in the <a href="#">Administration Guide</a>.</p>

<b>Error Code</b>	WS50023
<b>Text</b>	This type of request is not allowed to be updated
<b>Details</b>	You have attempted to update a request that is not allowed to be updated.
<b>Solution</b>	Retry the operation. Further information is available in the MyID <b>System Events</b> and <b>Audit Reporting</b> workflows.

<b>Error Code</b>	WS50024
<b>Text</b>	Enabling/Disabling a directory person is not allowed
<b>Details</b>	You have attempted to enable or disable a person whose details are stored in a directory. You can enable or disable user accounts for people only if they are stored in the MyID database.
<b>Solution</b>	Select a person in the MyID database and try again.

<b>Error Code</b>	WS50025
<b>Text</b>	You do not have permissions to edit PIV applicants
<b>Details</b>	You have attempted to edit a PIV applicant; this is not possible as you do not have permission to use the Edit PIV Applicant feature.
<b>Solution</b>	Check the role and permission assignments of the operator.

<b>Error Code</b>	WS50026
<b>Text</b>	You do not have permission to add or remove the specified administrator groups
<b>Details</b>	You have attempted to add or remove administration groups but you do not have permission to those groups.
<b>Solution</b>	Request permission from an administrator; see the <i>Administrative groups</i> section in the <a href="#">Administration Guide</a> for details.

<b>Error Code</b>	WS50027
<b>Text</b>	The operator does not have sufficient scope to create a request for this account
<b>Details</b>	You have attempted to create a request for a person, but that person does not sit within your scope.
<b>Solution</b>	Check your scope; see the <i>Scope and security</i> section in the <a href="#">Administration Guide</a> for details.

<b>Error Code</b>	WS50028
<b>Text</b>	You cannot validate or reject a request which does not have an Awaiting Validation status
<b>Details</b>	You have attempted to validate or reject a request, but the request is not awaiting validation, so does not need to be validated or rejected.
<b>Solution</b>	Check the status of the request.

<b>Error Code</b>	WS50029
<b>Text</b>	You cannot cancel a request which has a Completed, Canceled or Failed status
<b>Details</b>	You have attempted to cancel a request, but the request's status is Completed, Canceled or Failed; requests at those statuses do not need to be canceled.
<b>Solution</b>	Check the status of the request.

<b>Error Code</b>	WS50030
<b>Text</b>	The person selected does not have a photo. The credential profile requires the user to have a photo before it can be requested
<b>Details</b>	The <b>Enforce Photo at Issuance</b> option in the credential profile is set to <b>Request and Issuance</b> , which means that you cannot request or issue a card if the cardholder does not have a photo.
<b>Solution</b>	Capture a photo for the person and try again. Alternatively, edit the credential profile to set the <b>Enforce Photo at Issuance</b> option to <b>No</b> .

<b>Error Code</b>	WS50031
<b>Text</b>	Operation ID <operation> is not a permitted clone of operation <operation>
<b>Details</b>	An API call has been made which violates the cloned operation configuration.
<b>Solution</b>	If this occurs when using the MyID Operator Client, contact customer support. If this occurs when calling the REST API directly, check the <code>op</code> parameter references an allowed cloned operation.

<b>Error Code</b>	WS50032
<b>Text</b>	The conditions on the Operation with ID <operation ID> prohibit use of the operation for the target entity
<b>Details</b>	An operation has been attempted that is not permitted for the entity that would be affected by the operation. For example, the device type may be incompatible with the requested operation, or the person may be not be at an appropriate status
<b>Solution</b>	<p>This may occur in batch operations in the MyID Operator Client when you select an item that is not suitable; for example, if you select a device for a batch cancellation operation, but the device was issued with the <b>Validate Cancellation</b> option.</p> <p>If calling the API directly, make sure the operation that is being used is permitted for the entity that would be affected by the operation. For example, this error will occur when using the <b>Edit Person</b> operation to attempt to edit a person who holds the PIV Applicant role.</p>

<b>Error Code</b>	WS50033
<b>Text</b>	The person selected does not have fingerprint biometrics. The credential profile requires that the recipient has fingerprint biometrics enrolled.
<b>Details</b>	You have attempted to request a device for a person who does not have fingerprints stored in the MyID database, the credential profile for the device has the <b>Require Fingerprints at Issuance</b> option set, and the <b>Enforce biometrics at request</b> configuration option (on the <b>Biometrics</b> page of the <b>Operation Settings</b> workflow) is set.
<b>Solution</b>	Enroll fingerprints for the person, select a different credential profile that does not have the <b>Require Fingerprints at Issuance</b> option set, or set the <b>Enforce biometrics at request</b> configuration option to No.

<b>Error Code</b>	WS50034
<b>Text</b>	The person selected does not have facial biometrics. The credential profile requires that the recipient has facial biometrics enrolled.
<b>Details</b>	You have attempted to request a device for a person who does not have fingerprints stored in the MyID database, the credential profile for the device has the <b>Require Facial Biometrics</b> option set, and the <b>Enforce biometrics at request</b> configuration option (on the <b>Biometrics</b> page of the <b>Operation Settings</b> workflow) is set.
<b>Solution</b>	Enroll facial biometrics for the person, select a different credential profile that does not have the <b>Require Facial Biometrics</b> option set, or set the <b>Enforce biometrics at request</b> configuration option to No.

<b>Error Code</b>	WS50035
<b>Text</b>	An existing request has been found that prevents this action. Check requests that are already created and if necessary cancel them.
<b>Details</b>	You have attempted to request a device for a person using a credential profile that has the <b>Block Multiple Requests for Credential Group</b> set, and the person already has an existing request for a device from the same credential group.
<b>Solution</b>	Request a device from a different credential profile that is not subject to the same credential group restrictions, or cancel the existing request, if necessary.  See the <i>Block Multiple Requests for Credential Group</i> section in the <a href="#">Administration Guide</a> .

<b>Error Code</b>	WS50036
<b>Text</b>	The person selected has a maximum credential expiry date that is before the date requested.
<b>Details</b>	You have requested an expiry date for a device that is after the person's maximum credential expiry date.
<b>Solution</b>	Choose an expiry date for the device that is before the person's maximum credential expiry date, and try again.  See the <i>Requesting a device for a person</i> section in the <a href="#">MyID Operator Client</a> guide for details.

<b>Error Code</b>	WS50037
<b>Text</b>	Creating a request is not allowed. <details>
<b>Details</b>	You have attempted to create a request, but it does not meet the criteria set by a customized system. The <details> may provide more information.
<b>Solution</b>	Check the requirements of the customized system, adjust the request to meet those requirements, then try again.

<b>Error Code</b>	WS50038
<b>Text</b>	The selected credential profile is not allowed because the person that requested the job was not allowed to request this credential profile.
<b>Details</b>	The system has checked the permissions on the job (for example, the device request) and the issuer does not have the required permissions to request the credential profile selected.
<b>Solution</b>	Select a different credential profile, or cancel the request and create a new device request.

<b>Error Code</b>	WS50039
<b>Text</b>	You cannot action your own adjudications.
<b>Details</b>	The operator has attempted to generate or update an adjudication request for themselves.
<b>Solution</b>	Ask another operator to carry out the adjudication.

<b>Error Code</b>	WS50040
<b>Text</b>	You do not have permission to perform this operation against the selected item.
<b>Details</b>	You have attempted to perform an action on an item, but your scope does not permit the action. For example, if you have scope that allows you to view a user, and permission to validate requests, but your validate request scope does not allow you to validate requests for that user, you can attempt to validate a request for the user, but the action will not succeed, and this error appears.
<b>Solution</b>	Make sure that your scope permits you to carry out the appropriate actions for the target user, then try again.

<b>Error Code</b>	WS50041
<b>Text</b>	This action cannot be performed because the user has outstanding adjudications.
<b>Details</b>	A person can only have one adjudication that is being processed at once. This error appears when an adjudication request is attempted for a person who has an outstanding unfinished request.
<b>Solution</b>	Complete or cancel the existing adjudication.

<b>Error Code</b>	WS50042
<b>Text</b>	The request task type is not supported by the credential profile.
<b>Details</b>	The system can restrict certain credential profiles being used for certain types of jobs. For example, you cannot issue a VSC to a FIDO authenticator.
<b>Solution</b>	Select the correct device type for the credential profile.

<b>Error Code</b>	WS50043
<b>Text</b>	This credential profile can only be requested from Request Device.
<b>Details</b>	Request Card has been used for to generate a request for a FIDO device. There is a different workflow used to request FIDO device jobs.
<b>Solution</b>	Use the correct process for requesting FIDO authenticators.

<b>Error Code</b>	WS50044
<b>Text</b>	This device requires secondary authorization to cancel it. Please use the MyID Desktop Cancel Credentials workflow.
<b>Details</b>	You have attempted to cancel a device that was issued with a credential profile that had the <b>Validate Cancellation</b> option selected. Validating cancellations is not supported in the MyID Operator Client.
<b>Solution</b>	Use the <b>Cancel Credential</b> workflow in MyID Desktop to cancel the device.

<b>Error Code</b>	WS50045
<b>Text</b>	The device selected cannot be canceled. Please refer to product documentation for further guidance.
<b>Details</b>	You have attempted to cancel a server credential. You cannot cancel server credentials.
<b>Solution</b>	Choose a different device and try again.

<b>Error Code</b>	WS50046
<b>Text</b>	The specified resource is not accessible, or does not exist.
<b>Details</b>	The resource requested needs to be one of the allowed resources.
<b>Solution</b>	<p>The resource should be one of the following</p> <ul style="list-style-type: none"><li>• Base</li><li>• CoreForms</li><li>• CustomerTerms</li><li>• ErrorCodes</li><li>• MobileClient</li><li>• OperatorClient</li><li>• OtherClient</li><li>• ProductTerms</li><li>• ProjectDesigner</li></ul>

<b>Error Code</b>	WS50047
<b>Text</b>	Requests for Software Certificate Packages are not permitted for this operation.
<b>Details</b>	The credential profile specified does not allow issuance of software certificates.
<b>Solution</b>	Select a different credential profile or update the current credential profile to allow for software certificates.



<b>Error Code</b>	WS50048
<b>Text</b>	You do not have permission to download reports.
<b>Details</b>	The user requires permission to each specific report.
<b>Solution</b>	Grant the user additional roles or use the Edit Roles workflow to ensure the user has the required permissions. See the <i>Granting access to reports</i> section in the <a href="#">MyID Operator Client</a> guide for details.

<b>Error Code</b>	WS50049
<b>Text</b>	Additional authorization is required to perform this operation.
<b>Details</b>	Some workflows require additional authorization, such as a biometric check to perform.
<b>Solution</b>	You need to perform the <code>secondaryAuth</code> as specified in the link returned.

<b>Error Code</b>	WS50050
<b>Text</b>	The request is not at a valid status for this operation.
<b>Details</b>	You have attempted to carry out an operation on a request, but the request is at the wrong status.
<b>Solution</b>	Select a different request and try again.

<b>Error Code</b>	WS50051
<b>Text</b>	There are no available reports to perform a secondary search.
<b>Details</b>	The operator does not have permission to any reports to perform a secondary search within the MyID Operator Client.
<b>Solution</b>	Check the MyID permissions are correct using the <b>Edit Roles</b> workflow.

<b>Error Code</b>	WS50052
<b>Text</b>	The device owner has a maximum expiry date that is earlier than the expiry date of the device. The update cannot be requested because the credential profile does not have Ignore User Expiry Date set.
<b>Details</b>	If the credential profile does not have the <b>Ignore User Expiry Date</b> option set, MyID checks the <code>MaxRequestExpiryDate</code> set for the device owner in the Lifecycle API.. This value must not be before the expiry date of the device.
<b>Solution</b>	Increase the maximum credential expiry date for the device owner, change the credential profile of the device to set the <b>Ignore User Expiry Date</b> option, or issue a device to the user which does not exceed their maximum credential expiry date.

<b>Error Code</b>	WS50053
<b>Text</b>	The capabilities of the selected credential profile are not supported by this operation.
<b>Details</b>	<p>Certain operations may allow only certain card capabilities for a device. For example, <b>Request Update</b> allows only Contact, Microsoft Virtual Smart Card, Identity Agent, or Windows Hello for Business devices.</p> <p>This error may occur if you attempt to select a credential profile configured for derived credentials. Derived credentials must follow a different request process; for example, see the <i>Requesting a Derived Credential</i> section in the <a href="#">Derived Credentials Self-Service Request Portal</a> guide.</p>
<b>Solution</b>	<p>Select a credential profile that has one of the capabilities specified for the operation.</p> <p>You can check the JSON conditions in the <code>Operations</code> table of the MyID database for that operation ID.</p>

<b>Error Code</b>	WS50054
<b>Text</b>	The selected credential profile has different capabilities to the current device credential profile.
<b>Details</b>	<p>Certain operations allow you to change the credential profile of a device. This error means that when changing the credential profile, you must select a profile which has exactly the same card capabilities as the previous credential profile.</p>
<b>Solution</b>	<p>Examine the previous profile in the <b>Credential Profiles</b> workflow, and create the new credential profile for the device to have the same card capabilities.</p>

<b>Error Code</b>	WS50055
<b>Text</b>	The user has an existing request or device that exists with a different exclusive group, the request cannot be added.
<b>Details</b>	<p>You have attempted to request a device that has an exclusive group specified in its credential profile, but the target of the request already has a device, or a request for a device, that has a different exclusive group. You cannot have devices from different exclusive groups.</p>
<b>Solution</b>	<p>See the <i>Exclusive Group</i> section in the <a href="#">Administration Guide</a> for details.</p>

<b>Error Code</b>	WS50056
<b>Text</b>	The user has an existing request or device that exists with a different exclusive group, the request cannot be validated.
<b>Details</b>	You have attempted to validate a request for a device that has an exclusive group specified in its credential profile, but the target of the request already has a device, or a request for a device, that has a different exclusive group. You cannot have devices from different exclusive groups.
<b>Solution</b>	See the <i>Exclusive Group</i> section in the <a href="#">Administration Guide</a> for details.

<b>Error Code</b>	WS50057
<b>Text</b>	The user has an existing request or device that exists with a different exclusive group, the request cannot be collected.
<b>Details</b>	You have attempted to collect a request for a device that has an exclusive group specified in its credential profile, but the target of the request already has a device, or a request for a device, that has a different exclusive group. You cannot have devices from different exclusive groups.
<b>Solution</b>	See the <i>Exclusive Group</i> section in the <a href="#">Administration Guide</a> for details.

<b>Error Code</b>	WS50058
<b>Text</b>	The selected user has no suitable biometric samples for EFT export.
<b>Details</b>	<p>You have selected a person who does not have suitable biometric samples enrolled, and therefore cannot have their biometric samples exported as EFT.</p> <p>The person must either have an existing EFT stored, or suitable WSQ or WSQ roll image stored, from which an EFT can be generated then exported.</p>
<b>Solution</b>	Ensure the selected person has the appropriate biometrics enrolled, or select a different person.

<b>Error Code</b>	WS50059
<b>Text</b>	The selected user has no fingerprint rolls available for EFT export.
<b>Details</b>	<p>You have selected a person who does not have suitable fingerprint rolls captured, and therefore cannot have their biometric samples exported as EFT.</p> <p>The person must either have an existing EFT stored, or suitable WSQ or WSQ roll image stored, from which an EFT can be generated then exported.</p>
<b>Solution</b>	Ensure the selected person has the appropriate biometrics enrolled, or select a different person.

<b>Error Code</b>	WS50060
<b>Text</b>	Maximum number of generated sequential serial numbers exceeded.
<b>Details</b>	You can import a maximum of 10,000 devices at one time.
<b>Solution</b>	Provide a different range of serial numbers that totals 10,000 devices or fewer.

<b>Error Code</b>	WS50061
<b>Text</b>	The attempt to assign a device has been rejected. The device assignment end date for the group that this person is associated with has passed.
<b>Details</b>	The issuance of the device would place it in a group that has expired.
<b>Solution</b>	<p>Update the group to expire in the future and repeat the operation.</p> <p>See the <i>Controlling device assignments for groups</i> section in the <a href="#">Administration Guide</a> for details.</p>

<b>Error Code</b>	WS50062
<b>Text</b>	The attempt to assign a device has been rejected. The maximum number of assigned devices for the group that this person is associated with has been exceeded.
<b>Details</b>	The issuance of the device would cause the device limit for the group to be exceeded and so has been prevented.
<b>Solution</b>	<p>Increase the group device limit and repeat the operation.</p> <p>See the <i>Controlling device assignments for groups</i> section in the <a href="#">Administration Guide</a> for details.</p>

<b>Error Code</b>	WS50063
<b>Text</b>	The selected directory person is already in the MyID database.
<b>Details</b>	You have attempted to import a person from a directory, but the person is already in the MyID database.
<b>Solution</b>	Select a different person to import, or edit the existing person record in the MyID database.

<b>Error Code</b>	WS50064
<b>Text</b>	You are not allowed to deliver this device
<b>Details</b>	You have attempted to set the delivery status on your own device.
<b>Solution</b>	Select a different device, or ask another operator to set the delivery status for your device. See the <i>Accepting delivery for a device</i> section in the <a href="#">MyID Operator Client</a> guide for details.

<b>Error Code</b>	WS50065
<b>Text</b>	The device already has an active request
<b>Details</b>	You have attempted to request a cancellation for a device that already has an active cancellation request.
<b>Solution</b>	Approve, reject, or cancel the original cancellation request for the device.

<b>Error Code</b>	WS50067
<b>Text</b>	The selected certificate policy does not allow identity mapping.
<b>Details</b>	You have selected a certificate policy for an additional identity that does not have the <b>Allow Identity Mapping</b> option selected.
<b>Solution</b>	Select a different certificate policy and try again, or edit the certificate policy to have the <b>Allow Identity Mapping</b> option.

<b>Error Code</b>	WS50068
<b>Text</b>	Replacement card has gone too far through issuance to reinstate previous device.
<b>Details</b>	You have attempted to reinstate a device, but a replacement was requested and the replacement process is too far advanced.
<b>Solution</b>	Use the replacement device instead of the device you want to reinstate.

<b>Error Code</b>	WS50069
<b>Text</b>	The operator does not have sufficient scope to view the requests of this account
<b>Details</b>	You have attempted to carry out an operation on a person, but your scope does not allow you to view the requests for this person.
<b>Solution</b>	Choose a different person, or amend your account to increase your scope.

<b>Error Code</b>	WS50070
<b>Text</b>	The provided certificate cannot be suspended or revoked as it is not currently issued.
<b>Details</b>	The certificate has not yet been successfully collected, and needs be fully issued before being able to suspend or revoke it.
<b>Solution</b>	Make sure the certificate has been issued and try again.

<b>Error Code</b>	WS50071
<b>Text</b>	The provided certificate cannot be suspended or revoked as it has been issued by the 'Unmanaged' certificate authority.
<b>Details</b>	Certificates in the Unmanaged certificate authority certificates have not been issued from a CA using MyID.
<b>Solution</b>	Select a different certificate.

<b>Error Code</b>	WS50072
<b>Text</b>	You do not have permission to suspend or revoke this certificate.
<b>Details</b>	The operator has attempted to suspend or revoke a certificate they do not have scope to using the Rest API.
<b>Solution</b>	Select a different certificate or amend the scope of the operator and try again.

<b>Error Code</b>	WS50073
<b>Text</b>	The provided certificate cannot be unsuspended as it is not suspended.
<b>Details</b>	The certificate is not at a status valid for unsuspension operation
<b>Solution</b>	Select a different certificate.

<b>Error Code</b>	WS50074
<b>Text</b>	You do not have permission to unsuspend this certificate.
<b>Details</b>	The operator has attempted to unsuspend a certificate they do not have scope to using the Rest API.
<b>Solution</b>	Select a different certificate or amend the scope of the operator and try again.

<b>Error Code</b>	WS50075
<b>Text</b>	The provided revocation reason cannot be used for this certificate.
<b>Details</b>	You have provided a revocation reason that you cannot use for the certificate.
<b>Solution</b>	Select a different revocation reason and try again.

<b>Error Code</b>	WS50076
<b>Text</b>	The provided certificate cannot be paused as it is not pending issuance or revocation.
<b>Details</b>	The certificate is not at a status valid for the pause operation.
<b>Solution</b>	Select a different certificate and try again.

<b>Error Code</b>	WS50077
<b>Text</b>	You do not have permission to pause this certificate.
<b>Details</b>	Operator has attempted to pause a certificate they do not have scope to using the Rest API.
<b>Solution</b>	Select a different certificate or amend the scope of the operator and try again.

<b>Error Code</b>	WS50078
<b>Text</b>	The provided certificate cannot be paused as no retries will be attempted.
<b>Details</b>	The Retries value for the certificate in the MyID database is at a value of -1 so there are no more retry attempts left
<b>Solution</b>	Select a different certificate.

<b>Error Code</b>	WS50079
<b>Text</b>	The provided certificate cannot be resumed as it is not pending issuance or revocation.
<b>Details</b>	The certificate is not at a status that is valid for the resume operation.
<b>Solution</b>	Select a different certificate.

<b>Error Code</b>	WS50080
<b>Text</b>	You do not have permission to resume this certificate.
<b>Details</b>	Operator has attempted to resume a certificate they do not have scope to using the Rest API.
<b>Solution</b>	Select a different certificate or amend the scope of the operator and try again.

<b>Error Code</b>	WS50081
<b>Text</b>	The provided certificate cannot be unsuspended as it has been issued by the 'Unmanaged' certificate authority.
<b>Details</b>	Certificates in the Unmanaged certificate authority certificates have not been issued from a CA using MyID.
<b>Solution</b>	Select a different certificate.

<b>Error Code</b>	WS50082
<b>Text</b>	The certificate cannot have its renewal status changed as it has been issued by the 'Unmanaged' certificate authority.
<b>Details</b>	Certificates in the Unmanaged certificate authority certificates have not been issued from a CA using MyID.
<b>Solution</b>	Select a different certificate

<b>Error Code</b>	WS50083
<b>Text</b>	You do not have permission to change the renewal status of this certificate.
<b>Details</b>	The operator has attempted to change renewal status of a certificate they do not have scope to using the Rest API.
<b>Solution</b>	Select a different certificate or amend the scope of the operator and try again.

<b>Error Code</b>	WS50084
<b>Text</b>	The maximum number of devices for a given licence has been exceeded
<b>Details</b>	You have requested a device that requires a license, but you do not have sufficient available suitable device licenses for that category of device.
<b>Solution</b>	Contact Intercede and request additional licenses, or cancel some devices you no longer require to free up some licenses.

<b>Error Code</b>	WS50086
<b>Text</b>	At least one of the order by fields selected is not an orderable field.
<b>Details</b>	You have attempted to specify a field for sorting that does not support sorting.
<b>Solution</b>	Try the search again, specifying only fields that support sorting.



<b>Error Code</b>	WS50087
<b>Text</b>	At least one of the order by fields selected is an invalid field name.
<b>Details</b>	You have attempted to specify an invalid field name for a sorting column.
<b>Solution</b>	Try the search again, specifying the correct field name.

<b>Error Code</b>	WS40067
<b>Text</b>	Directory searches do not allow multiple column sorting
<b>Details</b>	You have attempted to search a directory using sorting from more than one column.
<b>Solution</b>	Try the search again, selecting at most one column for sorting.

<b>Error Code</b>	WS60000
<b>Text</b>	Database timeout. Please contact your administrator for more information.
<b>Details</b>	There was a performance issue when requesting a large amount of search data.
<b>Solution</b>	You may be able to improve performance by disabling the report search count. See the <i>Performance considerations for searching large sets of data</i> section in the <a href="#">MyID Operator Client</a> guide for details.

<b>Error Code</b>	WS60001
<b>Text</b>	The search query timed out. Please contact your administrator for more information.
<b>Details</b>	There was a performance issue when requesting a large amount of search data.
<b>Solution</b>	You may be able to improve performance by disabling the report search count. See the <i>Performance considerations for searching large sets of data</i> section in the <a href="#">MyID Operator Client</a> guide for details.

## 7 MyID Client Service error codes

This section contains the list of errors produced by the MyID Client Service that may occur when using the MyID Operator Client.

To assist with the diagnosis of issues, Intercede support may guide you to enable logging for the client service; you can then provide these logs to customer support for analysis. For information on configuring logging, see the *Windows clients* section in the [Configuring Logging](#) guide.

<b>Error Code</b>	881030
<b>Text</b>	An unknown error has occurred
<b>Details</b>	The MyID Client Service encountered an unknown error from which it could not recover.
<b>Solution</b>	There may be more information about the error in the client log, if logging is enabled.

<b>Error Code</b>	3102130
<b>Text</b>	Provided image path does not exist or is inaccessible.
<b>Details</b>	The MyID Image Editor uses the current user's temporary folder as a cache, but it is unable to access it.
<b>Solution</b>	Ensure the user's temporary folder has appropriate permissions. By default, this can be found at %userprofile%\AppData\Local\Temp

<b>Error Code</b>	3102131
<b>Text</b>	Failed to load image. This is usually because it is in an unsupported format.
<b>Details</b>	The MyID Image Editor was unable to process the provided data as a supported image type.
<b>Solution</b>	Ensure the provided image is in one of the supported formats: <ul style="list-style-type: none"><li>• JPEG (*.jpg, *.jpeg)</li><li>• Bitmap (*.bmp)</li><li>• Graphics Interchange Format (*.gif)</li><li>• Portable Network Graphics (*.png)</li></ul>

<b>Error Code</b>	10000224
<b>Text</b>	Configuration File Error: Invalid configuration
<b>Details</b>	The MyIdClientService.dll.config file is invalid, but the MyID Client Service could not determine the problem.
<b>Solution</b>	Ensure the configuration file exists, is populated with valid XML, and does not contain any duplicate or invalid values.

<b>Error Code</b>	10000225
<b>Text</b>	Configuration File Error: Server setting not found. Make sure you have provided a valid server or SSA install path.
<b>Details</b>	No Server has been specified, and there is no path to a Self-Service App installation with a Server value in its configuration file.
<b>Solution</b>	Ensure the Server node in the configuration file has a valid value, or, if you are using the Self-Service App's configuration, ensure that Self-Service App's Server configuration contains a valid value and the MyID Client Service's <code>SsaPath</code> node contains the correct path to the Self-Service App program file.

<b>Error Code</b>	10000226
<b>Text</b>	Configuration File Error: DataSource setting not found. Make sure you have provided a valid DataSource or SSA install path.
<b>Details</b>	No DataSource URI has been specified, and there is no path to an Self-Service App installation with a DataSource value in its configuration file.
<b>Solution</b>	Ensure the DataSource node in the configuration file has a valid value, or, if you are using the Self-Service App's configuration, ensure that Self-Service App's DataSource configuration contains a valid value and the MyID Client Service's <code>SsaPath</code> node contains the correct path to the Self-Service App program file.

<b>Error Code</b>	10000229
<b>Text</b>	A MyID Client Service window is already open. Please close any MyID Client Service windows and try again.
<b>Details</b>	The MyID Client Service can display only a single applet window at a time, but an operation was attempted that requires a window to be displayed while one was already open.
<b>Solution</b>	Close any open MyID Client Service windows and try again.

<b>Error Code</b>	10000233
<b>Text</b>	Failed to initialise translations - see the log for more details.
<b>Details</b>	There was an error updating the local translation cache.
<b>Solution</b>	There may be more information about the error in the client log, if logging is enabled.

<b>Error Code</b>	10000234
<b>Text</b>	Configuration File Error: Invalid DisableAccessControl setting provided; value must be either 'true' or 'false'.
<b>Details</b>	An invalid value has been provided for the DisableAccessControl configuration.
<b>Solution</b>	Ensure the DisableAccessControl configuration has a value of either <code>true</code> or <code>false</code> . Removing the node from the configuration file is the equivalent of it having a value of <code>false</code> .

<b>Error Code</b>	10000235
<b>Text</b>	Configuration File Error: Invalid AccessControlAllowOrigin setting provided; value must contain at-least one fully-resolved URI, or, in the case of multiple allowed-origins, a comma-separated list of fully-resolved URIs.
<b>Details</b>	Either the AccessControlAllowOrigin configuration has not been specified (and DisableAccessControl is not set to true), an invalid value has been supplied, or the value is not in the expected format.
<b>Solution</b>	Ensure the AccessControlAllowOrigin configuration is valid; value must contain at-least one fully-resolved URI, or, in the case of multiple allowed-origins, a comma-separated list of fully-resolved URIs.

<b>Error Code</b>	10000228
<b>Text</b>	Failed to bind to local web-socket port. Make sure another application is not running and consuming your port.
<b>Details</b>	The MyID Client Service was unable to establish a binding to the port configured in the WebSocketPort configuration (default of 8081).
<b>Solution</b>	<p>Close any applications that are consuming the port that the MyID Client Service is trying to bind to. If this is not possible, you can change the port the MyID Client Service uses by updating its WebSocketPort configuration; note that you must make the equivalent configuration change on the Operator Client server or it will not know which port to use to connect to the MyID Client Service.</p> <p>This error may occur if you have installed the MyID Client WebSocket Service but have not configured the MyID Client Service to use it. See the <i>Enabling or disabling the MyID Client WebSocket Service</i> section in the <a href="#">Installation and Configuration Guide</a> for details.</p>

<b>Error Code</b>	10000230
<b>Text</b>	An error occurred when communicating with EdeficeSmartCard.
<b>Details</b>	An unknown error occurred communicating with an internal component (EdeficeSmartCard).
<b>Solution</b>	There may be more information about the error in the client log, if logging is enabled.

<b>Error Code</b>	10000231
<b>Text</b>	An error occurred when communicating with Enveloper.
<b>Details</b>	An unknown error occurred communicating with an internal component (Enveloper).
<b>Solution</b>	There may be more information about the error in the client log, if logging is enabled.

<b>Error Code</b>	10000232
<b>Text</b>	An error occurred when communicating with SoftwareCrypto.
<b>Details</b>	An unknown error occurred communicating with an internal component (SoftwareCrypto).
<b>Solution</b>	There may be more information about the error in the client log, if logging is enabled.

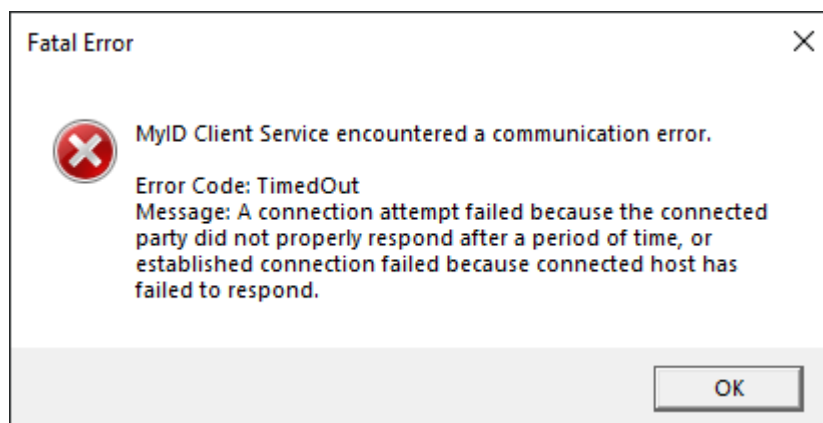
## 7.1 .NET Networking errors

Networking errors from .NET are presented directly; these are not produced by the MyID Client Service, and so do not have Intercede error codes.

These errors are presented with the following text:

MyID Client Service encountered a communication error.

For example:



For more information, see the Microsoft documentation:

[docs.microsoft.com/en-us/dotnet/api/system.net.sockets.socketerror](https://docs.microsoft.com/en-us/dotnet/api/system.net.sockets.socketerror)