MyID PIV

Version 12.14

Error Code Reference

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

Document reference: IMP1952-12.14.0-PIV

March 2025

Copyright

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

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

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

Trademarks

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

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

Licenses

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

Conventions used in this document

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

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

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

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

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

  For example:

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

  For example:

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

Contents

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.

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

Error Code	10304
Text	Invalid Entry
Details	A certificate used during mobile provisioning contains invalid or corrupted data.
Solution	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.
Relates To	Identity Agent Provisioning

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

Error Code	21642
Text	Incompatible
Details	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.
Solution	Try selecting a different credential profile, or using a different device. See the **Audit Reporting** workflow for further details.
Relates To	Credential Issuance

Error Code	21643
Text	Insufficient Space
Details	Issuing the current device has been prevented because the device has insufficient space for the required number of certificates.
Solution	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 **Audit Reporting** workflow for further details.
Relates To	Credential Issuance

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

Error Code	21645
Text	Unsuitable Device
Details	Issuing the current device has been prevented because the device is unsuitable.
Solution	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 **Audit Reporting** workflow for further details.
Relates To	Credential Issuance

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

Error Code	21647
Text	Not Imported
Details	The issuance requires that the device being issued has already been imported into the system. The presented device is unknown to the system.
Solution	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 **Audit Reporting** workflow.
Relates To	Credential Issuance

Error Code	21648
Text	GUID is not valid.
Details	The GUID for the provisioning job has been corrupted.
Solution	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.
Relates To	Identity Agent Provisioning

Error Code	21776
Text	Authentication is required to continue. Your card's issuance profile is not configured to require one.
Details	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.
Solution	Authentication requirements can be configured in the **Credential Profiles** workflow.
Relates To	Credential Issuance

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

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

Error Code	50038
Text	The selected credential profile is not allowed because the person that requested the job was not allowed to request this credential profile.
Details	Validation failed because the operator does not have the correct permissions to make a request with the selected credential profile.
Solution	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 **Credential Profiles** workflow in MyID Desktop. See the *Working with credential profiles* section in the ***Administration Guide*** for further details.
Relates To	Adjudication

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

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

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

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

Error Code	82373
Text	You are unable to request a replacement card, please contact your administrator.
Details	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.
Solution	Check that the user meets all the requirements of the credential profile.
Relates To	Credential Issuance

Error Code	82450
Text	Invalid auth code for the specified job.
Details	The presented authentication code is incorrect.
Solution	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 **Request Auth Code** workflow.
Relates To	Authentication

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

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

Error Code	82502
Text	Only Identity Agent mobiles are supported.
Details	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.
Solution	Non-Identity Agent devices can be canceled using the **Request Replacement Card** workflow.
Relates To	Credential Issuance

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

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

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

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

Error Code	85121
Text	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
Details	The 9B key for this device has not been configured or has been configured incorrectly.
Solution	The 9B key can be configured using the **Key Management** workflow.
Relates To	Credential Issuance

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

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

Error Code	85124
Text	There is no CHUID signing certificate configured. Please consult the product documentation
Details	The CHUID signing certificate for this device has not been configured or has been configured incorrectly.
Solution	The certificate location is configured in the Registry of the Application server. See the *Configure server signing certificates* section of the ***PIV Integration Guide*** for more details.
Relates To	Credential Issuance

Error Code	85125
Text	The private key for a server signing certificate is not available. Please consult the product documentation
Details	The server signing certificate (CHUID signing certificate or OPACITY CVC signing certificate) for this device has been configured incorrectly.
Solution	The certificate location is configured in the registry of the MyID application server. See the *Configure server signing certificates* section of the ***PIV Integration Guide*** or the *Setting up OPACITY* section of the ***Smart Card Integration Guide*** for more details.
Relates To	Credential Issuance

Error Code	85126
Text	The FASCN is invalid. Card issuance can not continue
Details	The system has attempted to generate an identifier for the user and failed. This is usually a PIV compliant FASCN
Solution	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.
Relates To	Credential Issuance

Error Code	85127
Text	Some of the data provided is invalid. This could either be attributes of the Applicant or the Agency. Please review the details.
Details	The system has attempted to generate an identifier for the user and failed. This is usually a PIV compliant FASCN
Solution	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.
Relates To	Credential Issuance

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

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

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

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

Error Code	85184
Text	Could not determine Windows logon credentials.
Details	MyID is attempting to determine the Windows logon name for the connected user, but is failing to do so.

Solution	Ensure the client and the server are in the same Windows Domain
	Run the following script on the web server to enable IIS to determine the identity of the connecting client:
	`ConfigureWindowsAuthentication.ps1`
	This script is installed to the `Utilities` folder on the MyID web server; by default, this is:
	`C:\Program Files\Intercede\MyID\Utilities\`

Relates To	Update My Device

Error Code	85187
Text	There has been a problem updating your account.
Details	MyID has encountered an error performing the User Sync action during the Update My Device workflow.
Solution	Further details about the specific error are available in the Audit Reports workflow. 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.
Relates To	Update My Device

Error Code	85188
Text	Unable to connect to the authentication server
Details	An attempt by the Process Driver web service to connect to the authentication server web service failed
Solution	This error may occur if you are using a load balancer or have multiple web servers. In this case, carry out the following: 1. Set the `IssuerUri` option in the web.oauth2 application settings file. See the *Setting the issuer in web.oauth2* section in the ***MyID Operator Client*** guide. 2. Configure a shared JWT signing key so that all instances of web.oauth2 use the same signing key. See the *Load balancing* section in the ***MyID Operator Client*** guide. Instead of setting the shared JWT signing key, as an alternative you can set the `AuthServerUrl` option in the ProcessDriver `myid.config` file; see the *MyID Operator Client pass-through authentication with a load balancer* section in the ***MyID Operator Client*** guide.
Relates To	Authentication

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

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

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

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

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

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

Error Code	420000
Text	User cannot be issued with certificates.
Details	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.
Solution	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.
Relates To	Credential Issuance

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

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

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

Error Code	503000
Text	The system could not generate a unique FASCN for this device
Details	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.
Solution	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.
Relates To	Credential Issuance

Error Code	503001
Text	The system could not generate a credential number for this person.
Details	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.
Solution	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.
Relates To	Credential Issuance

Error Code	503002
Text	Failed to update FASCN or credential number
Details	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.
Solution	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.
Relates To	Credential Issuance

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

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

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

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

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

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

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

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

Error Code	800548
Text	Your card has not been issued and can't be used to logon.
Details	The device that is attempting to logon has not been issued.
Solution	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 **Request Card** workflow.
Relates To	Authentication

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

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

Error Code	800551
Text	Logon Denied.
Details	An attempt has been made to log in and that attempt has failed.
Solution	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. This situation may also occur on an upgraded MyID system where users have SHA1 passwords and the administrator has set the **Use Security Phrase algorithm version 2** configuration option. In this case, follow the instructions for *Upgrading security phrase security* in the ***Installation and Configuration Guide***. 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. This error may also occur if you are using Integrated Windows Logon and your system is not configured correctly; for example, if the `SystemAccounts.Domain` field has not been updated from LDAP. This error may also occur if you have a misconfigured UDL file for database connectivity. This error may also occur if you have attempted to use Integrated Windows Logon with a user in the Active Directory group Protected Users. As this error may have a variety of causes, you are recommended to try using the System Interrogation Utility to investigate further.
Relates To	Authentication

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

Error Code	800554
Text	Activation requires assistance.
Details	The credential profile is set up for assisted activation. You cannot use self-service activation for this device.
Solution	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. If the device is intended to be activated using assisted activation, use the **Assisted Activation** workflow to activate the device.
Relates To	Authentication

Error Code	800560
Text	Self-Service Unlock not allowed
Details	A self-service PIN reset has been initiated and the instance of the MWS server is not configured to allow self-service operations.
Solution	If self-service operations should be permitted, edit the file `myid.config`, and set the key `AllowSelfUnlockForPIV` to `true`. Additionally, verify that the configuration flag **Ask Security Questions for Self Service Card Unlock** is set to **Yes**. This flag is in the **Security Settings** workflow, on the **PINs** tab. See the *Configuring self-unlock* section in the ***Web Service Architecture*** guide for details of editing the `AllowSelfUnlockForPIV` setting.
Relates To	PIV Self Service

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

Error Code	800590
Text	The Certificate Policy is disabled and cannot be issued.
Details	An attempt has been made to issue a disabled certificate policy.
Solution	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 **Credential Profiles** workflow.
Relates To	Credential Issuance

Error Code	800591
Text	The Certificate Policy is Unmanaged and the user has not had a corresponding certificate imported.
Details	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. If the credential profile uses the **Use Existing** option, check that the unmanaged certificate has not expired; this configuration requires a valid certificate.
Solution	Either issue a different Credential Profile (one without an unmanaged certificate, or, in the case where the certificate has expired, with the **Historic Only** 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 **Upload PFX Certificates** workflow to upload a certificate.
Relates To	Identity Agent Provisioning

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

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

Error Code	800602
Text	iOS OTA Credential Profile not found
Details	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.
Solution	This can be set in the **Operation Settings** workflow, under the **Certificates** tab. The value is case sensitive. See the *Setting up iOS OTA provisioning* section in the ***Mobile Identity Management*** document for details.
Relates To	Identity Agent Provisioning

Error Code	800603
Text	iOS OTA Credential Profile has to be MachineIdentity
Details	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.
Solution	The credential profile can be modified in the **Credential Profiles** workflow. See the *Setting up iOS OTA provisioning* section in the ***Mobile Identity Management*** document for details.
Relates To	Identity Agent Provisioning

Error Code	800610
Text	The requested image was not found: {0}
Details	An image that is present in a card layout cannot be found.
Solution	Ensure the value in **Image Upload Server** on **Operation Settings** on the **Video** 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.
Relates To	Identity Agent Provisioning

Error Code	800630
Text	Biometrics are required
Details	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.
Solution	To collect the update, the user must enroll biometrics. Alternatively, configure the credential profile to have a biometric requirement of either **Never** or **Preferred**.
Relates To	Authentication

Error Code	800611
Text	The requested image timed out: {0}
Details	There has been a network issue retrieving an image used in a card layout.
Solution	Ensure the value in **Image Upload Server** on **Operation Setting**s on the **Video** 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.
Relates To	Identity Agent Provisioning

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

Error Code	881044
Text	The user account is locked.
Details	A user without security phrases set has attempted to perform a security phrase logon to the system. This attempt has been blocked. 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 `SAMAccountName` and `Domain` are not be stored in MyID) and MyID has attempted to fall back to logon with security phrases, which is not configured for use.
Solution	Security phrases can be set either using the **Change Security Phrases** or **Change My Security Phrases** workflows. See the *Logon using security phrases* and *Integrated Windows Logon* sections in the ***Administration Guide*** for details of configuring logon with security phrases and Integrated Windows Logon.
Relates To	Authentication

Error Code	881045
Text	User not found.
Details	The attempt to retrieve a users details, possibly from a connected LDAP system, has failed.
Solution	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 **Audit Reporting** workflow may be able to assist with diagnosing the problem.
Relates To	User Management

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

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

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

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

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

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

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

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

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

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

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

Error Code	881065
Text	You have insufficient security phrases configured.
Details	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.
Solution	If the intent is to allow the user to authenticate, and then set their own passphrases, ensure the user has permissions to **Change My Security Phrases** then change the **Set Security Phrase at Logon** option (on the **Logon** tab of the **Security Settings** workflow) to `1,110`.
Relates To	Authentication

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

Error Code	881100
Text	Virtual smart card issuance cannot continue
Details	An attempt has been made to issue a virtual smart card on a system but one of the following may apply: • Virtual smart card support is disabled on the system. • Attempt to generate the virtual smart card has failed. • The client operating system is not supported for VSCs.
Solution	To issue the device you must: • Enable virtual smart card support in the **Operation Settings** workflow. • Ensure that the TPM on the device is in a state to allow generation of a virtual smart card. • Make sure the client operating system meets the requirements in the Intercede VSC documentation. • The number of smart cards connected to the device does not exceed the maximum limit of 10.
Relates To	Credential Issuance

Error Code	881101
Text	Credential profile can only be issued to a virtual smart card. Issuance cannot continue.
Details	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.
Solution	Review your issuance process. Credential profile restrictions can be managed in the **Credential Profiles** workflow.
Relates To	Credential Issuance

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

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

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

Error Code	881116
Text	Failed to sign the terms and conditions.
Details	You have attempted to recover certificates to a device with terms and conditions that need to be signed, but the device does not already contain a signing certificate. You must have a signing certificate to allow you to sign the terms and conditions.
Solution	If you want to issue a new device with recovered certificates, *and* have Terms and Conditions cryptographically signed in the same process, you can use the following workaround: 1. Issue a new device for the purpose of key recovery, using a credential profile that contains a signing certificate first (with no key recovery specified). 2. Follow the process to request key recovery to an existing card. 3. Collect the key recovery to the device you have just issued. You can now sign the acceptance of the terms and conditions using the signing certificate already on the device.
Relates To	Credential Issuance

Error Code	881117
Text	Virtual smart card creation failed, please contact your administrator.
Details	An attempt has been made to issue a virtual smart card on a system but one of the following may apply: • Attempt to generate the virtual smart card has failed. • The client operating system is not supported for VSCs. See the **Audit Report** workflow for further details.
Solution	To issue the device you must: • Make sure that the TPM on the device is in a state to allow generation of a virtual smart card. • Make sure the client operating system meets the requirements in the VSC integration guide. • Make sure the number of smart cards connected to the device does not exceed the maximum limit of 10.
Relates To	Credential Issuance

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

Error Code	890020
Text	Insufficient permissions to access card profile.
Details	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.
Solution	Use the **Credential Profiles** workflow to configure the roles that are allowed to receive the temporary credential profile.
Relates To	Credential Issuance

Error Code	890042
Text	This action cannot be performed on your device.
Details	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.
Solution	Ensure a suitable credential profile has been requested for the user. Details about the credential presented can be found in the **Audit Reporting** workflow.
Relates To	Credential Issuance

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

Error Code	890054
Text	Action no longer available
Details	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.
Solution	The status of requests can be reviewed using the **Job Management** workflow.
Relates To	Credential Issuance

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

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

Error Code	890110
Text	No suitable credential profiles available.
Details	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.
Solution	Permissions can be edited in the **Edit Roles** workflow. Credential Profile permissions can be edited using the **Credential Profiles** workflow.
Relates To	Credential Issuance

Error Code	890467
Text	Unable to authenticate card. Unlocking your own card is not allowed.
Details	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
Solution	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 **Update Card** or **Request Card Update** workflows.
Relates To	PIV Self Service

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

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

Error Code	890478
Text	An unexpected problem has occurred, please wait a short while then try again.
Details	There has been an underlying error in COM+. It may be that the COM+ settings are invalid, or the service has become unavailable.
Solution	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.
Relates To	Authentication

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

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

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

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

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

Error Code	890490
Text	The card is not recognized or the user does not have permissions to use it.
Details	A device has been selected that the user does not have permissions to view or manipulate.
Solution	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 **Request Auth Code** workflow.
Relates To	Authentication

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

Error Code	890493
Text	An unknown error has occurred.
Details	An unexpected low level error has occurred.
Solution	The error is usually caused by low level exceptions being thrown by components. This can be caused by such things as: • The card layout assigned to the mobile credential profile having an image that was missing from the system. • A Content Signer Certificate not being correctly configured on the App Server. • Card access failure. • Other low level failure conditions. If you experience this error when attempting to issue a smart card set up for OPACITY, see the *Troubleshooting OPACITY smart cards* section in the ***Smart Card Integration Guide***. 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 *Certificate policies* section in the ***Windows Hello for Business*** guide. If you are trying to import a PIV card, this may be caused by another application accessing the smart card, including RDP sessions. Make sure no other applications that can access smart cards are running, and shut down any RDP sessions to the MyID server. Details of the issue will be available in the **Audit Reporting** and **System Events** workflows. If the problem persists, contact Intercede Support.
Relates To	All

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

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

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

Error Code	890499
Text	The card profile does not support encryption and therefore can not be used for key recovery
Details	The system was asked to recover a certificate to a device that cannot protect the private key for that certificate. This attempt was blocked.
Solution	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.
Relates To	Credential Issuance

Error Code	890500
Text	This card does not support biometric match from card.
Details	A request for a derived credential has been made from a card that does not support biometric matching.
Solution	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 **Require fingerprints for derived credentials** option to No.
Relates To	Credential Issuance

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

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

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

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

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

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

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

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

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

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

Error Code	890512
Text	numberOfAttempts
Details	Biometric validation has been attempted multiple times, and has failed each time. The retry limit has been reached and so the process is aborting.
Solution	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 **Operation Settings** workflow. If the problem is restricted to a subset of individuals, those individuals should re-enroll their biometric data.
Relates To	Authentication

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

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

Error Code	890517
Text	An error occurred when checking the machines DNS
Details	The Asset Name reported by the client software does not match an entry in the domain.
Solution	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.
Relates To	Virtual Smart Card Issuance

Error Code	890518
Text	An error occurred when checking the machines DNS
Details	The Asset Name reported by the client software does not match an entry in the domain.
Solution	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.
Relates To	Virtual Smart Card Issuance

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

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

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

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

Error Code	890527
Text	Device not assigned to a user
Details	The current device is expected to be issued, but it is not. The Audit will contain more details.
Solution	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 **Audit Reporting** workflow will contain more details about the inserted device.
Relates To	Credential Issuance

Error Code	890534
Text	The supplied card is not a temporary card
Details	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
Solution	Ensure the correct credential was presented. The **Audit Reporting** workflow will give details of the presented credential.
Relates To	Credential Lifecycle

Error Code	890535
Text	The supplied card is not assigned to the user
Details	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.
Solution	Ensure the correct credential was presented. The **Audit Reporting** workflow will give details of the presented credential.
Relates To	Credential Lifecycle

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

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

Error Code	890543
Text	User not logged in
Details	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.
Solution	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.
Relates To	Authentication

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

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

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

Error Code	890555
Text	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.
Details	The mobile provisioning has got into a state that cannot be recovered from automatically.
Solution	Cancel the device using the **Cancel Credential** workflow and repeat the issuance process.
Relates To	Identity Agent Provisioning

Error Code	890556
Text	Multiple matches
Details	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.
Solution	Cancel the device and repeat the issuance process. The status of jobs can be checked in the **Job Management** workflow.
Relates To	Identity Agent Provisioning

Error Code	890557
Text	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.
Details	An earlier issuance process for this device has previously failed. The system can automatically recover from most fail conditions but some are unrecoverable.
Solution	Cancel the device and repeat the issuance process. The status of jobs can be checked in the **Job Management** workflow.
Relates To	Identity Agent Provisioning

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

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

Error Code	890562
Text	This device cannot be provisioned at this time. The request on the server has expired. You will need to request the provisioning again.
Details	The provisioning job is no longer valid.
Solution	Cancel the device and repeat the issuance process. The status of jobs can be checked in the **Job Management** workflow. • **IKB-280 – Misleading error message text for error 890562** 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.
Relates To	Credential Issuance

Error Code	890564
Text	User is not suitable for certificate issuance
Details	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.
Solution	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.
Relates To	Credential Issuance

Error Code	890565
Text	There is no suitable card profile
Details	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
Solution	Create a suitable credential profile. See the *Setting up the Identity Agent credential profiles* section in the ***Mobile Identity Management*** document for details.
Relates To	Identity Agent Issuance

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

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

Error Code	890569
Text	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.
Details	The mobile provisioning has got into a state that cannot be recovered from automatically.
Solution	Cancel the device and repeat the issuance process.
Relates To	Identity Agent Provisioning

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

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

Error Code	890572
Text	There has been a configuration error. There is insufficient data available to provision this device.
Details	The system has attempted to generate an identifier for the user and failed. This is usually a PIV compliant FASCN.
Solution	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.
Relates To	Identity Agent Provisioning

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

Error Code	890574
Text	Your card was issued by an agency that does not allow derived credentials from this kiosk
Details	An attempt was made to request a derived credential from a card issued by an untrusted source. The issuance was blocked.
Solution	The **Cards Allowed For Derivation** flag in the **Operation Settings** workflow determines which devices are allowed to request derived credentials. See the *Determining which cards are available for derived credentials* section in the ***Derived Credentials Configuration Guide*** for further details. Details of the presented device can be found in the **Audit Reporting** workflow.
Relates To	Derived Credential Issuance

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

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

Error Code	890579
Text	The job specified is being used by another operator.
Details	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.
Solution	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.
Relates To	Credential Issuance

Error Code	890580
Text	There was a problem generating the Terms and Conditions. This process cannot continue.
Details	The required Terms and Conditions document for the credential issuance could not be created. As such, the issuance has been prevented.
Solution	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. Correct the terms and conditions document in the `ServerDocuments` table of the database and try again. If the problem persists, contact customer support.
Relates To	Credential Issuance

Error Code	890581
Text	User PIN not supported in Batch Process
Details	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.
Solution	Default filters usually prevent these credential profiles from being selectable. Do not remove these filters when selecting jobs. Use **Collect Card** for jobs that require the User PIN to be chosen.
Relates To	Credential Issuance

Error Code	890585
Text	Disabled devices cannot sign Terms and Conditions
Details	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.
Solution	Enable the device and repeat the workflow.
Relates To	Credential Issuance

Error Code	890586
Text	Disabled users cannot sign Terms and Conditions
Details	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.
Solution	Enable the user account and repeat the workflow.
Relates To	Credential Issuance

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

Error Code	890594
Text	You have no authentication mechanisms that are suitable for this operation.
Details	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.
Solution	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. If this error is encountered while attempting a self service unlock operation, it may be because the configuration option **Verify fingerprints during card unlock** is enabled and the user does not have fingerprints enrolled. 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 **Unlock My Card** workflow. If the user has no means to authenticate themselves then the process cannot continue.
Relates To	Authentication

Error Code	890596
Text	Your account is not eligible to receive this credential.
Details	An attempt has been made to collect a credential for a user whose account lacks the required attributes to receive that credential.
Solution	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. Check the audit, which may contain additional information about the missing attributes.
Relates To	Credential Issuance

Error Code	890597
Text	The specified user cannot be found.
Details	The user account identity is determined using either the UPN from the current Windows logon session or the value held in the `MYID_USERNAME` environment variable but cannot be found within MyID.
Solution	To correct this issue: • Check that the user account exists in MyID. • UPN matching is case-sensitive – check that the value used by Windows matches the case of the stored UPN in MyID. • Check that the value in `MYID_USERNAME` is set to the correct value for the MyID user account. For further details about how a user account is associated to MyID, see the *Specifying the target user* section in the ***Web Service Architecture*** guide.
Relates To	Authentication

Error Code	890598
Text	A problem has been reported by Windows (<error>). Check the Microsoft documentation for further details.
Details	The Windows Hello for Business enrollment failed due to a problem with your system, and Windows reported an error; for example, 0x80070015.
Solution	Check the Windows event log. If you have a persistent issue, see the *MyID Client Components* section in the ***Configuring Logging*** guide for information on how to enable MyID client logging for the `WHfB` component.
Relates To	Windows Hello

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

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

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

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

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

Error Code	890703
Text	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.
Details	The issuance of the device would place it in a group that has expired.
Solution	Update the group to expire in the future and repeat the collection. See the *Controlling license use for groups* section in the ***Administration Guide*** for details.
Relates To	Credential Issuance

Error Code	890704
Text	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.
Details	The issuance of the device would cause the device limit for the group to be exceeded and so has been prevented.
Solution	Increase the group device limit and repeat the collection. See the *Controlling license use for groups* section in the ***Administration Guide*** for details.
Relates To	Credential Issuance

Error Code	890705
Text	This request must be collected by the user account named in the request
Details	To collect a key recovery request, you must be the target of the request.
Solution	Ensure that you are the target of key recovery request that you want to collect.
Relates To	Credential Issuance

Error Code	890800
Text	Token validation failed.
Details	The OAuth2 authentication token passed through from Operator Client to ProcessDriver failed validation.
Solution	See the *MyID Operator Client advanced configuration* section in the ***MyID Operator Client*** guide. The Process Driver log may include additional information on the specific validation check that failed.
Relates To	Authentication

Error Code	890801
Text	Issuer validation failed.
Details	The OAuth2 authentication token passed through from the MyID Operator Client to ProcessDriver failed validation due to an Issuer mismatch.
Solution	See the *Setting the issuer for load-balanced systems* section in the ***MyID Operator Client*** guide.
Relates To	Authentication

Error Code	890811
Text	Unable to determine server address
Details	You have attempted to carry out authentication using an external identity provider but your system is misconfigured.
Solution	Check that the `AllowedHosts` setting is correct. The setting must match the URL used for the MyID web server. See the *Configuring the MyID web services for external identity providers* section in the ***MyID Authentication Guide*** guide.
Relates To	Authentication

Error Code	890812
Text	Unable to continue, invalid authenticated user
Details	You have attempted to carry out authentication using an external identity provider, but the user account with which you have authenticated is not the target user for the job.
Solution	Try the authentication again, and authenticate using the correct user account for the job. See the *Using an external identity provider* section in the ***Self-Service App*** guide.
Relates To	Authentication

Error Code	891014
Text	Your mobile device is not compatible with biometric authentication.
Details	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.
Solution	If biometric authentication is not required, review the configuration of the credential profile using the **Credential Profiles** workflow, under Issuance Settings. The global values are editable in the **Operation Settings** workflow.
Relates To	Credential Issuance

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

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

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

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

Error Code	892012
Text	This system is not configured to allow issuance of this type of credential. Please contact your administrator.
Details	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 **Enable Customer GlobalPlatform Keys** option (on the **Device Security** tab of the **Security Settings** workflow) is set to No.
Solution	Check that you have configured your system to issue this type of credential.
Relates To	Credential Issuance

Error Code	892015
Text	Card update failed due to non-compliance with T&C signing requirements.
Details	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.
Solution	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 **Credential Profiles** workflow.
Relates To	Credential Issuance

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

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

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

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

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

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

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

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

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

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

Error Code	892106
Text	System configuration error
Details	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.
Solution	Each COM+ application on the MyID application server needs to have the Web_Role enabled in the **Security** tab. Run the System Interrogation Utility to help you identify the issue; see the ***System Interrogation Utility*** guide for details.
Relates To	All

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

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

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

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

Error Code	9001005
Text	The terms and conditions certificate could not be validated. Note: This error is often only visible via the audit.
Details	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 **Audit Reporting** workflow may be able to assist with diagnosing the problem.
Solution	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 `certutil` utility on the application server: `certutil -f -urlfetch -verify <issuing CA certificate.cer>`
Relates To	Authentication

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

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

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

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

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

Error Code	9004028
Text	You do not have permission to access this workflow
Details	An attempt has been made to start a workflow the user does not have permissions to.
Solution	Check that the user has access to the required workflow. Permissions can be edited in the **Edit Roles** workflow. The user's role must have access to the required workflow, and must also have the appropriate logon method. 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 **Activate Card** workflow, or to import a PIV card, the Server Credentials role must be given access to the **Import from PIV Card** operation. **Note:** Any role that you want to receive mobile identities must have the **Issue Device** option selected in the **Cards** category in the **Edit Roles** workflow.
Relates To	Authentication

Error Code	9007084
Text	Operator may not issue this device
Details	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.
Solution	Check that the operator has access to the required credential collection workflow. You can edit permissions in the **Edit Roles** or the **Credential Profiles** workflows. The user's role must also have the appropriate logon method.
Relates To	Credential Issuance

Error Code	9007085
Text	This card cannot be used in its current state
Details	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.
Solution	The Card Applicant lacks the roles required to receive this credential.
Relates To	Credential Issuance

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

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

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

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

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

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

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

Error Code	9007093
Text	This card cannot be used in its current state
Details	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.
Solution	The job cannot be issued in its current state.
Relates To	Credential Issuance

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

Error Code	9007095
Text	This card cannot be used in its current state
Details	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.
Solution	The job cannot be issued. Request a new credential for the user.
Relates To	Credential Issuance

Error Code	9007096
Text	This card cannot be used in its current state
Details	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.
Solution	Collect the job using the self service application on an appropriate machine. If the problem persists, contact customer support.
Relates To	Credential Issuance

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

Error Code	9007098
Text	This card cannot be used in its current state
Details	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.
Solution	Repeat the process with a different device.
Relates To	Credential Issuance

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

Error Code	9007100
Text	This card cannot be used in its current state
Details	An attempt has been made to issue a credential. This issuance was prevented because it must be a known proximity card.
Solution	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.
Relates To	Credential Issuance

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

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

Error Code	9007103
Text	This card cannot be used in its current state
Details	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.
Solution	Enroll new facial biometrics for the applicant and then try again. Alternatively edit the credential profile to remove this requirement.
Relates To	Credential Issuance

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

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

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

Error Code	9007107
Text	This card cannot be used in its current state
Details	An attempt has been made to issue a credential. This issuance was prevented because the Data Model failed validation.
Solution	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.
Relates To	Credential Issuance

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

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

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

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

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

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

Error Code	9007138
Text	Device capacity exceed.
Details	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.
Solution	Reduce the number of certificates to be written or provide a different device.
Relates To	Credential Issuance

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

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

Error Code	9007150
Text	Credential profile requisite data is not set.
Details	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).
Solution	Ensure that the user has all the requisite data, or change the **Requisite User Data** criteria in the credential profile.
Relates To	Credential Issuance

Error Code	9007151
Text	An existing request or device exists with a different exclusive group
Details	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.
Solution	See the *Exclusive Group* section in the ***Administration Guide*** for details.
Relates To	Credential Issuance

Error Code	9007152
Text	The card suitability check has failed
Details	This error is displayed in the audit trail. 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. If the message is "Suitability check failure" then this means that MyID was unable to contact the card suitability check web service.
Solution	See the *Using the card suitability service* section in the ***Administration Guide*** for details.
Relates To	Credential Issuance

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

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

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

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

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

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

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

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

Error Code	9008112
Text	Reset PIN is not available for this device.
Details	You have attempted to reset the PIN for a device that does not support this operation.
Solution	Select a different device and try again.
Relates To	Credential Issuance

Error Code	9008113
Text	The device cannot be activated as the device is not pending activation
Details	An attempt has been made to activate a device but failed as the device is not pending activation.
Solution	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.
Relates To	Credential Issuance

Error Code	9008114
Text	Update job not available for the device
Details	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.
Solution	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.
Relates To	Credential Issuance

Error Code	9008115
Text	Card cannot be updated as content signer will expire during card lifetime
Details	The content signing certificate is nearing its expiry date, and the card lifetime is longer than the remaining lifetime of the certificate.
Solution	Renew the content signing certificate and try again.
Relates To	Credential Issuance

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

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

Error Code	9008118
Text	Enrollment data has not been validated within the last 24 hours
Details	Your system had been configured to require you to activate this device within 24 hours of validating the enrollment data.
Solution	Validate the enrollment data and make sure you attempt to activate the device within 24 hours.
Relates To	Credential Issuance

Error Code	9008120
Text	Cannot be a known Dual-Interface Card
Details	Your system has been configured to prevent the issuance of dual interface cards for this type of credential.
Solution	Select a different device and try again.
Relates To	Credential Issuance

Error Code	80072002
Text	User has no finger prints
Details	Biometric authentication is required to continue with the process, but the user has no biometrics captured.
Solution	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 **Credential Profiles** workflow to remove this restriction.
Relates To	Authentication

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

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

Error Code	80072104
Text	Invalid Authentication Code provided. No attempts remaining
Details	An authentication code has been entered incorrectly too many times and the process has been terminated.
Solution	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 **Request Auth Code** workflow.
Relates To	Authentication

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

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

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

Error Code	90200052
Text	Invalid OTP.
Details	An incorrect authentication code has been entered too many times while provisioning an Identity Agent, and so the process has been aborted.
Solution	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.
Relates To	Identity Agent Provisioning

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

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

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

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

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

Error Code	90200063
Text	MyID is not configured for this credential profile.
Details	An attempt has been made to request a derived credential for which MyID is not configured correctly.
Solution	Check that the credential profile has been set up correctly. 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 **Allow Logon Codes** configuration option is set to Yes. The audit will contain additional information regarding the underlying issue. See *The audit trail* section in the ***Administration Guide*** for further details.
Relates To	Derived Credentials

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

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

Error Code	90202843
Text	Certificate validation failed.
Details	An attempt was made to validate a credentials certificate during a derived credential request. The required certificate was either revoked or missing.
Solution	Full details of the invalid certificate can be found in the **Audit Reporting** workflow. The credential is not suitable for requesting Derived Credentials. Check the MyID server has been configured to trust the certificate authority that issued the certificate. See the ***Derived Credentials Configuration Guide*** for details.
Relates To	Derived Credential Issuance

Error Code	90202847
Text	User is not valid for issuing a derived credential.
Details	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.
Solution	Details of the missing data will be available in the **Audit Reporting** workflow. See the ***Derived Credentials Configuration Guide*** for details about how to configure Derived Credentials.
Relates To	Authentication

Error Code	90202848
Text	Configuration Error: Archive Certificate Policy does not match an allowed policy
Details	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.
Solution	Certificate policies are listed in the **Certificate Authorities** workflow. Contact Intercede Support if further assistance is required to configure this feature.
Relates To	Credential Issuance

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

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

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

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

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

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

Error Code	IA10001 IA10002 IA10003 IA10004 IA10005
Text	SOAP request failed
Details	See section *3.1*, *Troubleshooting network connectivity*.

Error Code	IA10006
Text	SOAP request failed
Details	This error has occurred during the first communication for the provisioning process to retrieve the PFX. This may be caused by exceeding the configured value for **Maximum Session Count** – this option determines the number of concurrent mobile issuance and update sessions are allowed by the server. See the *Maximum session count* section in the ***Mobile Identity Management*** document for details. 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 `ProcessDriver.asmx` service. For intermittent occurrence of this error, see section *3.1*, *Troubleshooting network connectivity*.

Error Code	IA10007 IA10008 IA10009 IA10010 IA10011 IA10012 IA10013 IA10014 IA10015
Text	SOAP request failed
Details	See section *3.1*, *Troubleshooting network connectivity*.

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

Error Code	IA10017 IA10018 IA10019 IA10020 IA10021 IA10022 IA10023 IA10024 IA10025 IA10026 IA10027 IA10028 IA10029 IA10030 IA10031 IA10032 IA10033 IA10034
Text	SOAP request failed
Details	See section *3.1*, *Troubleshooting network connectivity*.

Error Code	IA10035
Text	SOAP request failed
Details	This error has occurred when there has been a failure in the communications to report that a certificate has been collected. 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 `ProcessCard.asmx` service. See also section *3.1*, *Troubleshooting network connectivity*.

Error Code	IA10036 IA10037 IA10038 IA10039 IA10040 IA10041 IA10042 IA10043 IA10044
Text	SOAP request failed
Details	See section *3.1*, *Troubleshooting network connectivity*.

Error Code	IA10046
Text	The root certificate needs to be installed and trusted on the device
Details	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.

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

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

Error Code	IA12011
Text	Failed to install the certificate
Details	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.

Error Code	IA14001 IA14002 IA14003 IA14004 IA14005
Text	Failed to open a session to the smart card
Details	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.

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

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

Error Code	IA16002
Text	A signing operation has failed
Details	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. In this case, set the time to the correct value, and the issue disappears.

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

Error Code	IA17003
Text	One or more certificates not allowed to be stored on this type of storage device.
Details	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.

Error Code	IA17004
Text	Failed to write card layout data
Details	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.

Error Code	IA17009
Text	User aborted new pin entry
Details	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.

Error Code	IA17010
Text	Non-archived certificate request fail
Details	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.

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

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

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

Error Code	IA17015
Text	Archived certificate creation fail
Details	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.

Error Code	IA17016
Text	Failed to verify user pin
Details	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.

Error Code	IA17017
Text	Failed to verify user pin
Details	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.

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

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

Error Code	IA17021
Text	Invalid password algorithm specified.
Details	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.

Error Code	IA80003
Text	Problem starting provisioning
Details	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.

Error Code	IA80010
Text	Problem initializing the key store
Details	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 **Remove Identity** function from within Identity Agent on the device and then reissue the identity from MyID. This error may also occur if the **Envelope Transport Key Algorithm** configuration option (on the **Server** page of the **Security Settings** workflow) is not set to **3DES**.

Error Code	IA80020
Text	The correct OTP was not supplied by the user
Details	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.

Error Code	REST001
Text	The network has failed, please check connectivity
Details	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.

Error Code	REST002
Text	The user aborted the operation
Details	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.

Error Code	REST003
Text	Failed to get authorization
Details	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.

Error Code	REST004
Text	The MyID Server is busy. Please try again later
Details	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.

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

Error Code	REST006
Text	The URL is malformed
Details	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.

Error Code	REST007
Text	Unrecoverable error has occurred
Details	The framework/app is unable to continue with the provisioning process. Check the logs to see if troubleshooting information is available. 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 **Issue over Existing Credential** 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. This may also occur when issuing a mobile device with MDM restrictions and the MDM system does not recognize the mobile device as valid (for example, it is not registered, or does not have the required MDM attributes). This may also occur when issuing a mobile identity document where the document format has mandatory attributes (for example, a user photograph) that the recipient does not have. Check the audit to determine which attributes are missing.

Error Code	REST008
Text	Unrecoverable error has occurred
Details	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.

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

Error Code	-2147220723
Text	An error occurred logging into the card
Details	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. 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 ***Smart Card Integration Guide*** for details of which features your smart cards support.
Solution	Retry with a different PIN, *or*: Allow the workflow to complete.

Error Code	-2147220720
Text	An unexpected error has occurred.
Details	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. The error may also occur when using OPACITY SPE cards to indicate that the new user PIN was rejected. This error may also occur when attempting to collect an SPE card using a credential profile that has not been set up for OPACITY.
Solution	Retry with a different PIN, *or*: Allow the workflow to complete.

Error Code	-2147220711
Text	The operation is not supported by this type of smart card
Details	This error occurs when MyID has been unable to issue a certificate.
Solution	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.

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

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

Error Code	-2147023779
Text	The request could not be performed because of an I/O device error.
Details	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.
Solution	Check the card reader drivers and retry the operation. If the error continues, try a different card reader.

Error Code	-2146435068
Text	One or more of the supplied parameters could not be properly interpreted.
Details	The most likely reason for this error is: • 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.
Solution	There may be a variety of causes for this error. For example: • 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. • Use a PIN that matches the PIN policy of the card.

Error Code	-2146435038
Text	Smart card does not support the requested feature
Details	A feature was requested that is not supported by the smart card or the CSP.
Solution	This error may occur for a variety of reasons; for example: • The certificate template is not supported by the card. • The credential profile is misconfigured for the card. Check the MyID audit trail for more information.

Error Code	-2146435024
Text	There is no more storage space on the card to continue with this activity
Details	The following are the most likely reasons for this error: • Failure to locate a container during issuance due to failure to access the card, *or*: • Inability to create a container due to no storage space being available.
Solution	There may be a variety of causes for this error. For example: • For physical cards, check that the card is still inserted into the reader. • Check that the credential profile is not attempting to write too many certificates to the card. • Check that too many certificates are not being attempted to be retrieved onto the card.

Error Code	-2146434966
Text	Unexpected Error
Details	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.
Solution	Contact your administrator.

Error Code	-2146434965
Text	Device has an unknown Security Officer PIN
Details	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.
Solution	Contact your administrator.

Error Code	-2146434964
Text	Device has an unknown Security Officer PIN
Details	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.
Solution	Contact your administrator.

Error Code	-99900045
Text	An unknown error occurred while attempting to log in to the card.
Details	An attempt has been made to log in to the card which has failed. This can occur for physical or virtual cards.
Solution	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.

Error Code	-99900041
Text	Failed to communicate with MyID server. The application will now exit.
Details	The client application has been unable to communicate with the MyID server. 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. This problem may also be reported as error 9001005; see the entry for this error for further troubleshooting. The audit and system event messages may also indicate failure to validate certificates. If logging has been enabled, the information captured may include the text "The terms and conditions certificate could not be validated".
Solution	Check that your network connection is working between the client and the server. If you have configured logging for the client, the client log may contain more information on the problem; the log message will start with: `WorkflowRunner::Run - WebException thrown:` For information on setting up client logging, see the *Windows clients* section in the ***Configuring Logging*** guide.

Error Code	-99900037
Text	User communication is disabled. Unable to request missing card to be inserted into system. Please contact your system administrator.
Details	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.
Solution	Make sure the required smart card or VSC is present.

Error Code	-99900033
Text	An unknown error has occurred, contact customer support.
Details	An error has occurred at a low level that has not communicated any further details to the MyID software.
Solution	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.

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

Error Code	-99900028
Text	There has been an error accessing the Biometric device. Please contact your administrator.
Details	An unknown error has occurred with the biometric device.
Solution	Possible solutions: • 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. • Disconnect or disable other biometric or image capture devices that may be conflicting with the fingerprint reader to determine if that resolves the issue. • 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.

Error Code	-99900020
Text	No biometric device detected
Details	There has been a failure to detect a supported biometric verification device that is required for biometric verification. This can occur if: • The required driver or SDK is not installed for the biometric device. • The biometric device is not connected to the client machine. • Insufficient power is being provided to power the biometric device.
Solution	Ensure that the driver or SDK for the biometric device is installed. See the integration guide for the biometric device. Ensure that the biometric device is connected to the client machine and that sufficient power is being provided to the device.

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

Error Code	-9990003
Text	Certificate Issuance
Details	This error occurs when MyID has been unable to issue a certificate.
Solution	This error may occur for a wide variety of reasons. For example: • The certificate template is misconfigured. • The certificate service is not running. Check the MyID audit trail for more information about what has caused the certificates to fail to issue. 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 *Certificate policies* section in the ***Windows Hello for Business*** guide.

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

Error Code	128
Text	Failed to verify signature for running application.
Details	This error occurs when a MyID client has been unable to successfully validate component signatures.
Solution	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. If you cannot give the client access to the internet, add the following configuration to the client configuration file: `<add key="ComponentVerificationSkipRevocationChecks" value="TRUE"></add>` 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. 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 *Installing the MyID Installation Assistant* section in the ***Installation and Configuration Guide***.

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

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

Error Code	9007084
Text	Operator does not have the correct roles to collect this job
Details	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.
Solution	Change the operator's roles to an allowed role or reconfigure the credential profile to allow the operator's role.

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

Error Code	902014
Text	Intel Authenticate configuration check failed.
Details	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.
Solution	Check that the client is correctly configured.

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

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

Error Code	99900049
Text	Cannot perform an Intel Authenticate operation over a remote desktop connection.
Details	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.
Solution	Run the MyID client on a local machine.

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

Error Code	0x80094004
Text	The requested property value is empty.
Details	This error occurs when MyID has been unable to issue a certificate.
Solution	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.

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

Error Code	-99910011
Text	The printer failed to print the selected layout. Please contact your system administrator.
Details	There has been a problem with printing the card layout.
Solution	This might be caused by the following: • A configuration issue. Check that the **Image Upload Server** option (on the **Video** tab of the **Operation Settings** workflow) is pointing at the image upload server and that it is configured correctly. • Data error when sending the print data to the printer. Check for any errors being reported by the printer. Check the audit. • The printer not supporting a feature required by the print layout; for example, magstripe printing. Check for any errors reported by the printer.

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

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

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

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

Error Code	9009034
Text	The printer is in an unknown state.
Details	This may be as a result of: • The printer is unable to map its activity to one of the known set of activities. • The printer has reported an activity that is not known to MyID.
Solution	This may be a transient issue so wait for issue to clear. Contact the printer manufacturer if the issue persists. The printer has reported an activity that is not known to MyID. Wait for issue to clear. Contact customer support if issue persists.

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

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

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

Error Code	9009039
Text	The printer has reported a generic error state.
Details	When the printer is not reporting an error then this may indicate one of the following: • An error when attempting to send data to the printer. • Failure to retrieve the printer status information when the printer is connected. • An internal printer error resulting in the printer reporting an unknown error. • An exception within the printer adapter.
Solution	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. This may be caused by a transient communication issue so contact customer support if the issue persists.

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

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

Error Code	9009042
Text	There is a problem with the hopper in the printer.
Details	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.
Solution	If the hopper is empty, add cards and try again. 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. If the printer is showing any other fault, refer to the manufacturer's user guide.

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

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

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

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

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

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

Error Code	9009049
Text	The printer is not currently available.
Details	MyID is unable to communicate with the printer.
Solution	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.

Error Code	9009050
Text	The printer has been paused.
Details	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.
Solution	Resume the printer using the printer front panel.

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

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

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

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

Error Code	9009056
Text	The printer is currently initializing.
Details	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.
Solution	Wait for the printer to complete its initialization process

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

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

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

6 Image Capture component error codes

This section contains the list of errors that may occur when using the MyID Image Capture component.

Error Code	MIC0001
Text	An unexpected error occurred.
Details	This error is displayed for all unhandled issues.
Solution	Check the Image Capture log files for more information.

Error Code	MIC0002
Text	MyID Image Capture was provided with invalid data by the server
Details	Indicates a problem with the MyID installation.
Solution	Make sure that your MyID servers are installed and configured correctly, and have all the necessary prerequisite patches and modules installed.

Error Code	MIC0003
Text	MyID Image Capture was unable to load the UI libraries
Details	Usually caused by missing Image Capture files.
Solution	Ensure that the MyID Image Capture install directory contains both `IntercedeWpfControls.dll` and `IntercedeWpfTheme.dll`

Error Code	MIC0004
Text	Aware PreFace threw an exception during initialization
Details	Usually caused by missing Aware files.
Solution	Ensure that the MyID Image Capture install directory contains a `FaceModelStandard.dat` file.

Error Code	MIC0005
Text	MyID Image Capture was unable to load the .NET Aware PreFace libraries
Details	Usually caused by missing Aware files.
Solution	Ensure that the correct version of the Aware PreFace SDK has been installed, and that the MyID Image Capture install directory contains both `Aware.Preface.dll` and `Aware.Video.dll`. See the *Installing the Aware PreFace software for facial biometrics* section in the ***Installation and Configuration Guide*** for instructions on installing the Aware PreFace software.

Error Code	MIC0006
Text	MyID Image Capture was unable to load the native Aware PreFace libraries
Details	Usually indicates that the Aware PreFace SDK is not installed.
Solution	Make sure the Aware PreFace SDK is installed.

Error Code	MIC0007
Text	MyID Image Capture was unable to access the directory in which it stores its configuration
Details	Caused by directory access issues.
Solution	Ensure that the operator has read/write access to: `%UserProfile%\AppData\LocalLow\Intercede\ImageCapture`

Error Code	MIC0008
Text	MyID Image Capture was unable to load a required COM component
Details	This error indicates an issue with COM registration.
Solution	A reinstall of MyID Image Capture should resolve this issue.

7 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 *8*, *MyID Client Service error codes* for details.

Error Code	OA10000
Text	Server Error
Details	An internal server error has occurred.
Solution	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 **System Events** and **Audit Reporting** workflows within MyID, then the `web.oauth2` logs for more information. For information on configuring logging, see the *MyID REST and authentication web services* section in the ***Configuring Logging*** guide.

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

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

Error Code	OA10003
Text	You do not have sufficient security questions configured
Details	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 **Number of security questions for self-service authentication** configuration option.
Solution	Use the **Change Security Phrases** or **Change My Security Phrases** workflows to provide the required security phrases. See the *Setting security phrases* section in the ***Operator's Guide***. Alternatively, you can set a lower value for the **Number of security questions for self-service authentication** option. See the *Setting the number of security phrases required to authenticate* section in the ***Administration Guide***.

Error Code	OA10004
Text	Your username or security response is incorrect, or you may not have permission to access this client.
Details	The person attempting to log on has mistyped their username or security responses. Alternatively, your MyID license may have expired.
Solution	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 **Licensing** workflow. **Note:** 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 *Configuring the number of attempts to enter security phrases* section in the ***Administration Guide***.

Error Code	OA10005
Text	The registration link is invalid
Details	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.
Solution	Carry out the request again.

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

Error Code	OA10007
Text	Your OTP has been entered incorrectly, is locked, has expired, or you do not have permission to perform this operation. Please try again.
Details	The registration code was incorrect, has expired, or has been entered incorrectly too many times, or you do not have access to the **Register FIDO Security Key** operation.
Solution	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 *Automatic job cancellation* section in the ***Administration Guide***. Check that your have access to the **Register FIDO Security Key** operation; see the *Configuring roles for registering FIDO authenticators* section in the ***Passkey Integration Guide*** for details.

Error Code	OA10008
Text	Your session has timed out or is invalid, please try again
Details	You may have waited too long to complete the registration process.
Solution	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.

Error Code	OA10009
Text	Error registering FIDO in browser
Details	The `ServerDomain` app setting may configured incorrectly. Note that `ServerDomain` is case sensitive and must be consistent with the casing of the DNS Name in the web server's TLS certificate.
Solution	Set the `ServerDomain` in the app settings file. See the *Setting up the FIDO metadata* section in the ***Passkey Integration Guide*** for details.

Error Code	OA10010
Text	Error authenticating FIDO in browser.
Details	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. This may also occur if the web.oauth2 `Fido:Config:Origin` is configured incorrectly in the authentication service app settings file. Note that `Origin` is case sensitive and must be consistent with the casing of the DNS Name in the web server's TLS certificate
Solution	Set the `Origin` in the app settings file. See the *Setting up the FIDO metadata* section in the ***Passkey Integration Guide*** for details.

Error Code	OA10011
Text	FIDO authentication failed, please try again. You may not have permission to access this client.
Details	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. 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 **Require Client Side Discoverable Key** option, and consequently the FIDO authenticator does not have the key required for logon without a username.
Solution	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 *Setting up credential profiles for passkeys* section in the ***Passkey Integration Guide*** for details.

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

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

Error Code	OA10014
Text	FIDO registration failed, the credential profile is invalid
Details	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.
Solution	Request a FIDO authenticator using a different credential profile, and try again.

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

Error Code	OA10016
Text	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.
Details	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.
Solution	Either register a different token, register this token to a different credential profile using a credential profile that has **Require Attestation** set to **None**, 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 `MDSCacheDirPath` setting. See the *Setting up credential profiles for passkeys* or *Setting up a local metadata repository* section in the ***Passkey Integration Guide*** for details.

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

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

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

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

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

Error Code	OA10030
Text	MyID:Database:ConnectionStringCore is not configured
Details	A configuration file error has occurred. You must configure a database connection string.
Solution	Check the configuration file settings – `ConnectionStringCore` must be configured. See the *Configuring the standalone authentication service* section in the ***MyID Authentication Guide***.

Error Code	OA10031
Text	MyID:Database:ConnectionStringAuth is not configured
Details	A configuration file error has occurred. You must configure a database connection string.
Solution	Check the configuration file settings – `ConnectionStringAuth` must be configured. See the *Configuring the standalone authentication service* section in the ***MyID Authentication Guide***

Error Code	OA10032
Text	Unable to find configured JWT signing certificate
Details	No JWT signing certificate was found, but JWT signing is configured.
Solution	Check the JWT settings. See the *Load balancing* section in the ***MyID Operator Client*** guide.

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

Error Code	OA10034
Text	JWT signing key is configured, but has an incorrect algorithm or key size
Details	MyID has found an RSA key with an incorrect algorithm or key size.
Solution	Check the JWT settings. See the *Load balancing* section in the ***MyID Operator Client*** guide.

Error Code	OA10035
Text	Generated JWT signer certificate, but unable to load it
Details	A server error has occurred while attempting to validate the generated signer certificate.
Solution	Check the JWT settings. See the *Load balancing* section in the ***MyID Operator Client*** guide.

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

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

Error Code	OA10038
Text	You do not have permission to perform this operation
Details	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.
Solution	Check the roles that the person has and check the permissions these roles give in **Edit Roles**.

Error Code	OA10039
Text	You do not have permission to perform this operation on the identified object or the identified object does not exist
Details	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.
Solution	Check the roles that the person has and check the permissions these roles give in **Edit Roles**.

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

Error Code	OA10041
Text	Authorization failure, missing data
Details	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.
Solution	Check that your system is providing the data required to perform the extension grant.

Error Code	OA10042
Text	This item is not in the correct state to perform this operation
Details	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.
Solution	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 **Check For Updates** to refresh the list of available actions before attempting the operation again.

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

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

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

Error Code	OA10046
Text	The OTP has expired
Details	The authentication code has expired.
Solution	Request a new authentication code. The lifetime of authentication codes is controlled by the following configuration options on the **Auth Code** page of the **Security Settings** workflow: • **Auth Code Lifetime** • **Auth Code Lifetime for Immediate Use** (for short-use codes; for examples, authentication codes requested at the logon screen of the MyID Operator Client for immediate use).

Error Code	OA10047
Text	This item does not meet the requirements to perform this operation
Details	An operation for pass-through authentication has a condition that has not been met. Launching this operation is not allowed.
Solution	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.

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

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

Error Code	OA10050
Text	Number of fingerprint attempts has been exceeded
Details	The number of attempts to capture fingerprints has exceeded the configured maximum (the **Number of fingerprint validation attempts** configuration option on the **Biometrics** page of the **Operation Settings** workflow), either through failure to match or verify, or failure to capture.
Solution	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.

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

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

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

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

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

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

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

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

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

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

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

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

Error Code	OA10063
Text	You cannot retrieve security questions for this client
Details	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.
Solution	Check that the `appsettings.Production.jso`, `appsettings.json`, and custom client configuration files for the web.oauth2 web service are correctly configured.

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

Error Code	OA10065
Text	You cannot retrieve a challenge for this client
Details	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.
Solution	Check that the `appsettings.Production.jso`, `appsettings.json`, and custom client configuration files for the web.oauth2 web service are correctly configured.

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

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

Error Code	OA10068
Text	Windows logon failed, your windows account is unknown or untrusted
Details	You have attempted to sign in using Windows authentication, but your Windows account is not suitable.
Solution	See the *Signing in using Windows authentication* section in the ***MyID Operator Client*** guide.

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

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

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

Error Code	OA10072
Text	Authorization failure, missing data for Token Refresh
Details	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).
Solution	Check the token handle being sent, or log off and try again See the *Signing in using Windows authentication* section in the ***MyID Operator Client*** guide.

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

Error Code	OA10074
Text	External logon failed, no matching MyID user found
Details	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.
Solution	Use a different user, or configure your system to create users in MyID from the external identity provider. See the *Setting up an external identity provider* section in the ***MyID Authentication Guide*** for more information.

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

Error Code	OA10076
Text	External logon failed, external logon is not available in standalone mode
Details	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.
Solution	Use the web.oauth2 web service instead. See the *Setting up an external identity provider* section in the ***MyID Authentication Guide*** for more information.

Error Code	OA10077
Text	External logon failed, the attempted logon failed
Details	You have attempted to use an external identity provider, but the logon attempt failed.
Solution	Check your authentication with the external identity provider is valid, and try again. See the *Setting up an external identity provider* section in the ***MyID Authentication Guide*** for more information.

Error Code	OA10078
Text	External logon failed, no mappings found for claims
Details	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.
Solution	Check the mappings for your external identity provider. See the *Mapping attributes* section in the ***MyID Authentication Guide*** for more information.

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

Error Code	OA10080
Text	External logon failed, no claims supplied by external identity provider
Details	You have attempted to use an external identity provider, but the external identity provider did not provide any claims.
Solution	See the *Setting up an external identity provider* section in the ***MyID Authentication Guide*** for more information.

Error Code	OA10081
Text	The custom configuration file is not valid.
Details	The custom configuration appsettings file is not valid JSON or does not contain correctly formatted data.
Solution	Check your custom configuration `.json` files in the folders for custom clients, scopes, API resources or identity resources. See the *Custom configuration files* section in the ***MyID Core API*** guide.

Error Code	OA10082
Text	There was a problem processing the custom configuration files.
Details	The custom configuration appsettings file is not valid JSON, does not contain correctly formatted data, or you do not have permissions to the custom folder.
Solution	Check your custom configuration `.json` files in the folders for custom clients, scopes, API resources or identity resources. and check the Web Services user has permissions to the custom folders. See the *Custom configuration files* section in the ***MyID Core API*** guide.

Error Code	OA10084
Text	An error occurred while trying to retrieve an access token from an external source.
Details	MyID CMS was unable to obtain an OAuth access token to make API calls to the Entra authentication server.
Solution	Check the **External System** configuration associated with the credential profile; in particular, check the following fields: • **OAuth Token Endpoint** • **Client ID** • **Requested Scopes** • **Tenant ID** • **Client Secret** Check that these values are correct and match the access token configuration you set up on your Entra system.

Error Code	OA10085
Text	An error occurred while attempting to register your device with an external source
Details	MyID CMS tried to make an API call to the Entra authentication server to get the creation options for the new FIDO credential, but the API call returned an error.
Solution	Check the **External System** workflow; ensure that you have selected the **RESTFidoEntra** mapping file and that you have selected the correct field for **External Entra Reference**. See the *Setting up the external system* section in the ***Passkey Integration Guide*** for details. Check your permissions on Entra and make sure the application is set up with the correct permissions to make the required API calls; see the *Configuring Entra to allow MyID to access the passkey registration APIs* section for details.

Error Code	OA10086
Text	An error occurred while attempting to register your device with an external source
Details	After creating the FIDO credential, MyID CMS tried to register it with the Entra authentication server, but the API call returned an error.
Solution	Check the **External System** workflow; ensure that you have selected the **RESTFidoEntra** mapping file and that you have selected the correct field for **External Entra Reference**. See the *Setting up the external system* section in the ***Passkey Integration Guide*** for details. Check your permissions on Entra and make sure the application is set up with the correct permissions to make the required API calls; see the *Configuring Entra to allow MyID to access the passkey registration APIs* section for details.

Error Code	OA10087
Text	An error occurred while trying to retrieve data from the external system
Details	MyID CMS tried to get the external system details associated with the credential profile from the MyID application server, but an error was thrown by the application server components.
Solution	Check the MyID **System Events** log. This may occur if the Entra reference ID field configured in the external system is empty for the user collecting the credential.

Error Code	OA10088
Text	The MyID client service encountered an issue while attempting to register your device with an external source
Details	During FIDO issuance, MyID was either unable to communicate with the MyID Client Service, or an error was thrown by the MyID Client Service.
Solution	Make sure the MyID Client Service app is running when collecting the credential. Check the **Audit Reporting** workflow for further details about why the MyID Client Service threw an error. This error may occur if either the MyID Client Service cannot start or has not started within the timeout period allowed for the user to respond to a browser prompt to open the MyID Client Service automatically. Check that the MyID Client Service is running by looking for the MyID logo in the Windows system tray. Right click this icon to display a detailed log file. See the *Setting the MyID Client Service timeout* in the ***Passkey Integration Guide*** for details of configuring the MyID Client Service timeout. This error code has also been seen to occur if an error occurs within the Microsoft Windows process that interacts with the security key (for example, if there is a failure to register the passkey, or the security key rejects the user PIN). This error code has also been observed when using a Hyper-V client running Windows 11.

Error Code	OA10090
Text	The Passkey provided cannot be issued to because it has been marked as disposed
Details	At least one credential which was issued to the current device has its **Process Status** set to **Lost** or **Disposed**, therefore MyID CMS cannot issue any more credentials to that device. See the *Lost or disposed authenticators* section in the ***Passkey Integration Guide*** for details.
Solution	Change the disposal status or use a different device.

Error Code	OA10091
Text	FIDO registration failed, the credential profile is set to Enforce Restricted Direct Authenticator Attestation Check, but the token registered does not have metadata available on the server. Try registering a different token.
Details	The credential profile being collected is set up with the **Require Attestation** option set to **Basic (Restricted)**. During attestation checks, MyID CMS was able to find the metadata associated with the passkey used for collection, but it did not come from either the local basic metadata or enterprise metadata repositories.
Solution	If the user is trying to collect the passkey with the wrong authenticator device, try using the correct device. If the user is using the correct device, check the settings in the web.oauth2 application settings configuration file to ensure that either `Fido:Config:MDSCacheDirPath` or `Fido:Config:MDSCacheDirPathEnterprise` is configured for a local repository; see the *Setting up a local metadata repository* section in the ***Passkey Integration Guide*** for details.

Error Code	OA10092
Text	FIDO registration failed, the credential profile is set to Enforce Restricted Enterprise Authenticator Attestation Check, but the token registered does not have metadata available on the server. Try registering a different token
Details	The credential profile being collected is set up with the **Require Attestation** option set to **Enterprise (Restricted)**. During attestation checks, MyID CMS was able to find the metadata associated with the authenticator used for collection, but it did not come from the local enterprise metadata repository.
Solution	If the user is trying to collect the passkey with the wrong authenticator device, try using the correct device. If the user is using the correct device, check the settings in the web.oauth2 application settings configuration file to ensure that `Fido:Config:MDSCacheDirPathEnterprise` is configured for a local repository; see the *Setting up a local metadata repository* section in the ***Passkey Integration Guide*** for details. This error may also occur if you are using platform-managed enterprise attestation, and either the browser does not support this feature, or the browser has not been configured with a list of allowed domains; see the *Enabling platform-managed enterprise attestation in Google Chrome* section.

Error Code	OA10093
Text	FIDO registration failed, the credential profile is set to Enforce Enterprise Authenticator Attestation Check, but the attestation statement could not be verified as Enterprise. Try registering a different token
Details	The credential profile being collected is set up with the **Require Attestation** option set to **Enterprise**. During attestation checks, MyID CMS found the metadata associated with the authenticator used for collection, but it did not come from the enterprise metadata repository, and MyID CMS was unable to extract an enterprise attestation serial number from the attestation certificate.
Solution	If the user is trying to collect the passkey with the wrong authenticator device, try using the correct device. If the user is using the correct device, check the settings in the web.oauth2 application settings configuration file to ensure that `Fido:Config:MDSCacheDirPathEnterprise` is configured for a local repository; see the *Setting up a local metadata repository* section in the ***Passkey Integration Guide*** for details. This error may also occur if you are using platform-managed enterprise attestation, and either the browser does not support this feature, or the browser has not been configured with a list of allowed domains; see the *Enabling platform-managed enterprise attestation in Google Chrome* section.

Error Code	OC10001
Text	There are no actions available for your current logon method and the roles that you have been assigned.
Details	You have not been assigned any actions for use in the MyID Operator Client.
Solution	Ensure that the roles you have assigned provide MyID Operator Client actions. See the *Roles and groups* section in the ***MyID Operator Client*** guide.

Error Code	OC10002
Text	This web browser cannot be used. Please use an alternative web browser.
Details	An unsupported browser has been detected. Due to the browser technology used, you cannot use Internet Explorer to access the MyID Operator Client.
Solution	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 *Supported browsers* section in the ***MyID Operator Client*** guide.

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

Error Code	OC10004
Text	The server could not be contacted. Please try again.
Details	Connection to the server unavailable. Either the client is not connected to the Internet, or the server is offline.
Solution	Confirm that the API server is reachable, and try again. Confirm that you have the correct server address specified; see the *Specifying the server for the MyID Client Service* section in the ***MyID Operator Client*** guide. 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.

Error Code	OC10005
Text	The file you have uploaded is not an image. Please upload an image.
Details	You can choose from the following file types: • JPEG (`*.jpg`, `*.jpeg`) • Bitmap (`*.bmp`) • Graphics Interchange Format (`*.gif`) • Portable Network Graphics (`*.png`) If you select a file of the wrong type, MyID displays an error.
Solution	See the *Uploading an existing image file* section in the ***MyID Operator Client*** guide.

Error Code	OC10006
Text	MyID Client Service error
Details	You have attempted to use a feature provided by the MyID Client Service App, but the app is not running, or is configured incorrectly.
Solution	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. See the *Installing the MyID Client Service* section in the ***Installation and Configuration Guide*** for instructions on installing the MyID Client Service. This may also occur if MyID Desktop or the Self-Service App could not be found at the configured path. See the *Setting the location of MyID Desktop or the Self-Service App* section in the ***MyID Operator Client*** guide.

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

Error Code	OC10008
Text	Unable to launch the MyID Desktop or Self-Service App. Please check configuration and try again.
Details	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.
Solution	Confirm that the application is installed and available at the configured location. See the *Setting the location of MyID Desktop or the Self-Service App* section in the ***MyID Operator Client*** guide.

Error Code	OC10009
Text	Unable to connect to MyID Desktop or the Self-Service App. Please try again.
Details	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.
Solution	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. See the *Troubleshooting MyID Client Service connection issues* section in the ***MyID Operator Client*** guide.

Error Code	OC10010
Text	Unable to launch MyID Desktop or the Self-Service App. Please try again.
Details	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.
Solution	Try again when the current request has been completed.

Error Code	OC10011
Text	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.
Details	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.
Solution	Confirm that you have permissions to the link provided and try again.

Error Code	OC10012
Text	The item is not available. Check the link is valid and you have permission to access this information.
Details	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.
Solution	Confirm that you have permissions to the link provided and try again.

Error Code	OC10013
Text	Unable to launch MyID Desktop or the Self-Service App. Please check installed version and try again.
Details	An incorrect version of MyID Desktop or the Self-Service App has been detected.
Solution	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. 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 *Setting the location of MyID Desktop or the Self-Service App* section in the ***MyID Operator Client*** guide.

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

Error Code	OC10015
Text	At least one record must be selected in order to perform this operation.
Details	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.
Solution	Return to the main screen and try the operation again.

Error Code	OC10016
Text	Your login has expired. Please re-authenticate to the MyID Operator Client.
Details	Due to inactivity, you have been logged out of the MyID Operator Client.
Solution	Re-authenticate to the MyID Operator Client using the same user and logon mechanism. See the *Timeouts and re-authentication* section in the ***MyID Operator Client*** guide.

Error Code	OC10017
Text	You have re-authenticated to the MyID Operator Client with a different user. For security reasons, the operation has been canceled.
Details	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.
Solution	Use the same user and logon mechanism that was previously used to complete the intended operation. See the *Timeouts and re-authentication* section in the ***MyID Operator Client*** guide.

Error Code	OC10018
Text	You have re-authenticated to the MyID Operator Client with a different logon mechanism. For security reasons, the operation has been canceled.
Details	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.
Solution	Use the same logon mechanism that was previously used to complete the intended operation. See the *Timeouts and re-authentication* section in the ***MyID Operator Client*** guide.

Error Code	OC10019
Text	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.
Details	The request manifest was provided in an unexpected format and could not be parsed.
Solution	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.

Error Code	OC10020
Text	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.
Details	MyID Client Components (UMC) threw an exception in CreatePkcs10Ex.
Solution	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.

Error Code	OC10021
Text	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.
Details	MyID Client Components (UMC) threw an exception in AcceptPkcs7Ex2.
Solution	This error may be caused by the certificate policy for a soft certificate not having the **Private Key Exportable** option set; this also means that the policy must be configured on the CA to allow the private key to be exported. See the *Setting up a credential profile for soft certificates* section in the ***Administration Guide*** for details. This issue may also occur if the certificate file name generated from the certificate policy name contains invalid characters. As a workaround, you can customize the file names; see the *Customizing certificate file names* section in the ***MyID Operator Client*** guide. 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.

Error Code	OC10022
Text	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.
Details	Failed to load an archived certificate.
Solution	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.

Error Code	OC10023
Text	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.
Details	Failed to add an archived certificate to the user store.
Solution	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.

Error Code	OC10024
Text	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.
Details	Request included an extension that is not explicitly permitted. Default allowed extensions are .pfx and .cer.
Solution	This issue may occur if the certificate file name generated from the certificate policy name contains invalid characters. As a workaround, you can customize the file names; see the *Customizing certificate file names* section in the ***MyID Operator Client*** guide. 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.

Error Code	OC10025
Text	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.
Details	Auto-save has been disabled in the client configuration file.
Solution	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.

Error Code	OC10026
Text	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.
Details	An exception occurred during a file-write operation.
Solution	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.

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

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

Error Code	OC10030
Text	The MyID Client Service was unable to read the document.
Details	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.
Solution	Check that all pre-requisites are installed before attempting to print the document. See the *Client workstation* section in the ***Installation and Configuration Guide*** for details.

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

Error Code	OC10032
Text	A problem occurred when collecting the certificates. Please retry the operation.
Details	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.",
Solution	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."

Error Code	OC10033
Text	Error notifying the server of sign out. Your client has still been signed out.
Details	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.

Solution	Confirm that the `authServerRevocationLocation` is correctly set, the web.oauth2 web service has been configured correctly, and the database is reachable.
	The `authServerRevocationLocation` option is available in the `appSettings.js` file for the MyID Operator Client website, which is in the following folder on the web server by default:
	`C:\Program Files\Intercede\MyID\OperatorClient`
	The default value is:
	`authServerRevocationLocation: "/web.oauth2/connect/revocation",`

Error Code	WS10000
Text	Server error
Details	An internal server error has occurred.
Solution	Retry the operation; the cause could be a temporary issue such as a database timeout due to server load. 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 *Displaying images stored on the web server* section in the ***MyID Operator Client*** guide for details. If the problem persists, check the **System Events** and **Audit Reporting** workflows within MyID, then the `rest.core` logs for more information. For information on configuring logging, see the *MyID REST and authentication web services* section in the ***Configuring Logging*** guide.

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

Error Code	WS10002
Text	Unable to retrieve the values for the specified selection box.
Details	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.
Solution	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.

Error Code	WS10003
Text	Unable to retrieve the requested session information.
Details	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.
Solution	Re-authenticate and try again.

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

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

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

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

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

Error Code	WS20001
Text	Server configuration error - DataDictionary is inconsistent
Details	The MyID Project Designer configuration is incorrect, preventing the server from starting correctly.
Solution	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 *MyID REST and authentication web services* section in the ***Configuring Logging*** guide.

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

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

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

Error Code	WS30002
Text	Validation problem, the value for <field name>, <details>
Details	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.
Solution	Check the values you have entered for the specified field and try again.

Error Code	WS30003
Text	Invalid person id specified
Details	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.
Solution	Check the data you have entered and try again.

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

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

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

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

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

Error Code	WS30009
Text	Validation problem, the value for <field name>, <details>
Details	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".
Solution	Check the value you have entered for the specified field and try again.

Error Code	WS30010
Text	Validation problem, the value for <field name>, fails Validation rule <rule>
Details	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.
Solution	Check the values you have entered for the specified field and try again.

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

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

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

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

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

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

Error Code	WS30017
Text	Validation problem, the value for 'First Name', and 'Last Name' must be provided.
Details	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.
Solution	Ensure that you have specified one or both of the **First Name** and **Last Name** fields, then attempt to save the person's record again.

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

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

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

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

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

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

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

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

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

Error Code	WS30027
Text	Please select only certificates for a single owner
Details	All the certificates must have been issued to the target of the request (either the device owner for the device endpoint or the person specified in the people endpoint).
Solution	Check that the certificates you want to recover belong to the same person and try again.

Error Code	WS30028
Text	At least one certificate must be selected
Details	You must specify at least one certificate.
Solution	Specify a certificate and try again.

Error Code	WS30029
Text	Certificate to recover {Object ID} is not a valid certificate
Details	One of the object IDs in the certificates array passed in is not the object ID of a certificate.
Solution	Check the certificate IDs and try again.

Error Code	WS30030
Text	Certificate to recover {0} is not archived
Details	The certificate with the object ID in the error is not archived.
Solution	Select an archived certificate and try again.

Error Code	WS30032
Text	Certificates cannot be recovered for the selected card profile
Details	The credential profile selected is neither a contact or soft certificate card profile.
Solution	Select a different credential profile and try again.

Error Code	WS30033
Text	The certificates selected have conflicting recovery storage types. A request cannot include certificates that require both software only and hardware only policies
Details	One of the certificates passed in to recover has a recovery storage of Software Only and another has a recovery storage of Hardware Only.
Solution	Check the recovery storage settings for the certificates.

Error Code	WS30034
Text	At least one of the certificates selected has a storage policy that is not compatible with the selected device or credential profile. For example, a certificate with storage policy of Hardware cannot be recovered as a software certificate. If the storage policy is Software it cannot be recovered to a hardware device such as a smartcard or security key.
Details	This error can be caused if: • At least one of the certificates passed in to recover has a recovery storage of Software Only and the credential profile is a contact credential profile, or it is a recovery to an existing device. • At least one of the certificates passed in to recover has a recovery storage of Hardware Only and the credential profile is a soft certificate credential profile.
Solution	Check the recovery storage for the certificates and the details of the credential profile.

Error Code	WS30036
Text	Device is not at valid status for recovery
Details	When requesting a key recovery to an existing device, the device must be active.
Solution	Select an active device and try again.

Error Code	WS30037
Text	All selected certificates must be unique
Details	You have specified multiple of the same archived certificate ID for a key recovery request through the API. Note that this is not possible through the MyID Operator Client.
Solution	Check your list of certificate IDs and try again.

Error Code	WS30038
Text	The selected device does not support the recovery of this number of archived certificates
Details	You have selected more certificates than the maximum number of historic certificates supported by the device you have selected. **Note:** While this message prevents you from requesting too many certificates, you may still be able to request certificates that exceed the capacity of the card if the individual certificates are too large and take up more space than the card supports.
Solution	Remove some certificates from the request and try again.

Error Code	WS40000
Text	Validation problem, the value for 'Distinguished Name', already exists
Details	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.
Solution	Enter a unique DN for the person and try again. Alternatively, you can configure your system to allow duplicate DNs; the **Allow duplicate DN** configuration option determines whether unique DN values are required; see the *LDAP page (Operation Settings)* section in the ***Administration Guide*** for details.

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

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

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

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

Error Code	WS40005
Text	The item referenced was not found
Details	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.
Solution	Retry the operation. If the problem persists, check that you have sufficient privilege to access the item. 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. Check the MyID **System Events** workflow and the `rest.core` logs for more information. For information on configuring logging, see the *MyID REST and authentication web services* section in the ***Configuring Logging*** guide.

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

Error Code	WS40007
Text	The user location in the directory could not be matched to an existing group
Details	When importing a person to the MyID database from a directory, the person could not be matched to a group in MyID.
Solution	Try one of the following: • Manually pick a MyID group for the user to be imported into and save the record again. • Use the **Edit Groups** workflow in MyID Desktop and import the LDAP groups into MyID. See the *Importing an LDAP directory branch* section in the ***Operator's Guide*** for details. • If you want groups to be automatically imported from LDAP, set the **Automatically create MyID groups from the Organizational Unit of imported users** configuration option on the **LDAP** page of the **Operation Settings** workflow.

Error Code	WS40008
Text	Directory synchronization is not available with this API due to configuration or role limitations
Details	An attempt has been made to synchronize a person with the directory manually; however, this operation is disabled due to system configuration. Directory synchronization is controlled by the following configuration: • If the **Background Update** 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. • If the **Background Update** 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.
Solution	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.

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

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

Error Code	WS40011
Text	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.
Details	Either the selected maximum expiry date for the request, or the user maximum expiry date is in the past.
Solution	Specify a date for the request that is in the future and try again.

Error Code	WS40012
Text	The device cannot be replaced because it is not issued
Details	You have specified a device to be replaced, but MyID does not recognize it as an issued device.
Solution	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.

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

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

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

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

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

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

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

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

Error Code	WS40021
Text	The specified entity does not exist.
Details	A report is attempting to reference an unsupported entity.
Solution	The report is incorrectly defined. Redefine it to reference one of the following: • `adjudications` • `audits` • `authCodes` • `binaries` • `bioSamples` • `cardProfiles` • `controls` • `devices` • `directories` • `directoryGroups` • `directoryPeople` • `groups` • `installs` • `logEvents` • `notifications` • `people` • `reportDefinitions` • `reports` • `requests` • `sessions` • `settings`

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

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

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

Error Code	WS40025
Text	The user does not have the required contact details for this delivery mechanism.
Details	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.
Solution	Update the person to specify their email address or mobile number.

Error Code	WS40026
Text	The specified delivery mechanism is not enabled for this operation.
Details	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.
Solution	Use the **Email Templates** workflow to enable the required email template or select an alternative email template.

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

Error Code	WS40028
Text	The specified auth code action: {0}, is not supported.
Details	The specified action is not supported.
Solution	The action specified must be one of the following • `Activate` • `Collect` • `Logon` • `Unlock`

<table>
<tr><td><b>Error Code</b></td><td>WS40029</td></tr>
<tr><td><b>Text</b></td><td>The specified auth code action: {0}, is not supported for this item.</td></tr>
<tr><td><b>Details</b></td><td>Each action is linked to a specific entity.</td></tr>
<tr><td><b>Solution</b></td><td>Ensure you only select an action appropriate to the entity:
<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></td></tr>
</table>

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

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

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

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

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

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

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

Error Code	WS40037
Text	The request is for a person that is not within the authenticated operators scope
Details	The target user for the request is outside the scope of the authenticated operator.
Solution	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.

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

Error Code	WS40039
Text	This device does not meet the requirements of the credential profile.
Details	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.
Solution	Select a device that is compatible with the credential profile assigned to the request.

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

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

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

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

Error Code	WS40045
Text	The device cannot be updated because it has already expired.
Details	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.
Solution	Either renew the device, or issue a new device.

Error Code	WS40046
Text	The device cannot be updated because the issuance process has not been completed.
Details	The device must have a process status of Active and be assigned to a person.
Solution	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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Error Code	WS40063
Text	The device has not previously been assigned and cannot be reinstated
Details	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.
Solution	Choose a different device and try again.

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

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

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

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

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

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

Error Code	WS40074
Text	Must select a new owner to reassign
Details	You have specified the same person as the new owner as the current owner of the device.
Solution	Specify a different owner from the current owner and try to reassign the device again.

Error Code	WS40075
Text	Only one of x509 or pkcs12 must be set.
Details	You have attempted to request the import of a certificate and specified both an `x509` and a `pkcs12` parameter.
Solution	Specify only one of the certificate parameters (`x509` or `pksc12`) and try again. See the *Importing certificates* section in the ***MyID Core API*** guide.

Error Code	WS40076
Text	If using pkcs12 then password must be set
Details	You have attempted to request the import of a certificate using a Base 64-encode PFX file, but you have not specified the password for this file.
Solution	Specify the `password` parameter and try again. See the *Importing certificates* section in the ***MyID Core API*** guide.

Error Code	WS40077
Text	There was an error importing the certificate.
Details	There was an unknown issue importing the certificate.
Solution	Check the **System Events** workflow for more information on the error. See the *Importing certificates* section in the ***MyID Core API*** guide.

Error Code	WS40078
Text	User creation not allowed.
Details	You have attempted to request the import of a certificate that required MyID to create a new user, but creating a new user is not permitted.
Solution	Set the **Allow Certificate User Creation** option on the **Certificates** page of the **Operation Settings** workflow to `Yes` and try again. See the *Importing certificates* section in the ***MyID Core API*** guide.

Error Code	WS40079
Text	PKCS12 password is invalid.
Details	You have attempted to request the import of a PFX file, but the password is incorrect.
Solution	Check that you have specified the password correctly and try again. See the *Importing certificates* section in the ***MyID Core API*** guide.

Error Code	WS40080
Text	Provide a valid base64 pfx certificate.
Details	You have attempted to request the import of a PFX file, but the Base 64-encoded file you have provided is either invalid Base 64 or invalid data.
Solution	Check that you have encoded a valid PFX file correctly and try again. See the *Importing certificates* section in the ***MyID Core API*** guide.

Error Code	WS40081
Text	Provide a valid certificate.
Details	You have attempted to request the import of X.509 data, but the Base 64-encoded data you have provided is either invalid Base 64 or invalid data.
Solution	Check that you have provided the valid Base 64 data from the `.cer` file. Do not include the `-----BEGIN CERTIFICATE-----` or `-----END CERTIFICATE-----` lines. See the *Importing certificates* section in the ***MyID Core API*** guide.

Error Code	WS40082
Text	Select a valid certPolicyID.
Details	You have attempted to import a certificate, but MyID cannot find the certificate policy ID that you specified.
Solution	Check the value of the `certPolicyId` parameter. This must match an `ObjectID` in the `CetPolicies` table in the MyID database. See the *Importing certificates* section in the ***MyID Core API*** guide.

Error Code	WS40083
Text	User is not in the MyID Database.
Details	You have attempted to import a certificate, but MyID could not find the user in the database.
Solution	Either ensure that there is a user in the MyID database who matches the details in the certificate you are importing, or set the **Allow Certificate User Creation** option on the **Certificates** page of the **Operation Settings** workflow to `Yes` and try again. See the *Importing certificates* section in the ***MyID Core API*** guide.

Error Code	WS40084
Text	Cannot find unique user to assign.
Details	You have attempted to import a certificate, but there are multiple people in the MyID database who match the Distinguished Name or UPN of the certificate.
Solution	Either provide a different certificate, or call the `/api/People/{id}/certificateImport` endpoint to import the certificate for a specific user. See the *Importing certificates* section in the ***MyID Core API*** guide.

Error Code	WS40085
Text	Certificate already exists.
Details	You have attempted to import a certificate, but the certificate already exists in the MyID database.
Solution	Select a different certificate and try again. See the *Importing certificates* section in the ***MyID Core API*** guide.

Error Code	WS40086
Text	There is no valid group to assign to the imported user.
Details	You have attempted to import a person from a directory, but the person does not have an OU mapped from which to create a new group.
Solution	Make sure there is an existing group to which you can assign the person, then use the Edit Person (Directory) screen to import the person into MyID.

Error Code	WS50000
Text	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
Details	You do not have permission to perform the requested operation.
Solution	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. Check the MyID **System Events** and **Audit Reporting** workflows for more information about the operation being attempted.

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

Error Code	WS50002
Text	You do not have permission to update your own device
Details	The system is configured using the **Self-service** option (on the **Self-Service** page of the **Security Settings** 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.
Solution	Ask another operator to update the device for you.

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

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

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

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

Error Code	WS50007
Text	Invalid job status change
Details	You have attempted to update a request job to a status that is not permitted.
Solution	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. 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 **System Events** and **Audit Reporting** workflows.

Error Code	WS50008
Text	Your assigned roles do not have permission to request the credential profile specified
Details	You have specified a credential profile to which you do not have access.
Solution	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 **Can Request** option in the *Constrain credential profile issuer* section in the ***Administration Guide***.

Error Code	WS50009
Text	It is not possible to create requests for yourself or your devices.
Details	This message occurs when an attempt is made by an operator to request their own credentials. It could occur when: • Attempting to request a replacement for one of their devices. • Attempting to request a renewal for one of their devices. • Attempting to request a device for themselves (**Note:** The button for this is not available in MyID Operator Client). • Attempting to request an update for one of their devices.
Solution	Ask another operator to carry out the operation.

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

Error Code	WS50011
Text	The person selected does not have a role assigned that can hold the requested credential profile
Details	You have attempted to request a device using a credential profile to which the person does not have access.
Solution	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 **Can Receive** option in the *Linking credential profiles to roles* section in the ***Administration Guide***.

Error Code	WS50012
Text	The person selected does not have user data approved. The credential profile requires user data to be approved before it can be requested
Details	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.
Solution	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 **Require user data to be approved** option in the *Issuance Settings* section in the ***Administration Guide***.

Error Code	WS50013
Text	The account selected is not compatible with this request (kind is mismatched)
Details	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).
Solution	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. If you continue to have problems, check the configuration of the credential profile you are using. You can also check the MyID **System Events** and **Audit Reporting** workflows.

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

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

Error Code	WS50016
Text	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.
Details	You have specified a credential profile that has specific requisite user data requirements; the person you have specified does not meet those requirements.
Solution	Carry out one of the following: • Update the person's user account to meet the requisite data requirements. • Update the credential profile to allow the configured user data. • Select a different credential profile for which the user meets the requisite data requirements. See the *Requisite User Data* section in the ***Administration Guide*** for details.

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

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

Error Code	WS50019
Text	Requests created using this API must include an appropriate encoding type
Details	The MyID Operator Client supports credential profiles with a restricted list of **Card Encoding** options.
Solution	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. See the *Requesting a device for a person* section in the ***MyID Operator Client*** guide.

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

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

Error Code	WS50022
Text	A requested role is manager controlled and the operator does not hold the role that would permit them to assign it
Details	You have requested a role that is restricted by the **Managed By** option.
Solution	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. See the *Controlling the assigning of roles* section in the ***Administration Guide***.

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

Error Code	WS50024
Text	Enabling/Disabling a directory person is not allowed
Details	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.
Solution	Select a person in the MyID database and try again.

Error Code	WS50025
Text	You do not have permissions to edit PIV applicants
Details	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.
Solution	Check the role and permission assignments of the operator.

Error Code	WS50026
Text	You do not have permission to add or remove the specified administrator groups
Details	You have attempted to add or remove administration groups but you do not have permission to those groups.
Solution	Request permission from an administrator; see the *Administrative groups* section in the ***Administration Guide*** for details.

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

Error Code	WS50028
Text	You cannot validate or reject a request which does not have an Awaiting Validation status
Details	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.
Solution	Check the status of the request.

Error Code	WS50029
Text	You cannot cancel a request which has a Completed, Canceled or Failed status
Details	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.
Solution	Check the status of the request.

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

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

Error Code	WS50032
Text	The conditions on the Operation with ID <operation ID> prohibit use of the operation for the target entity
Details	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
Solution	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 **Validate Cancellation** option. 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 **Edit Person** operation to attempt to edit a person who holds the PIV Applicant role.

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

Error Code	WS50034
Text	The person selected does not have facial biometrics. The credential profile requires that the recipient has facial biometrics enrolled.
Details	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 **Require Facial Biometrics** option set, and the **Enforce biometrics at request** configuration option (on the **Biometrics** page of the **Operation Settings** workflow) is set.
Solution	Enroll facial biometrics for the person, select a different credential profile that does not have the **Require Facial Biometrics** option set, or set the **Enforce biometrics at request** configuration option to No.

Error Code	WS50035
Text	An existing request has been found that prevents this action. Check requests that are already created and if necessary cancel them.
Details	You have attempted to request a device for a person using a credential profile that has the **Block Multiple Requests for Credential Group** set, and the person already has an existing request for a device from the same credential group.
Solution	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 *Block Multiple Requests for Credential Group* section in the ***Administration Guide***.

Error Code	WS50036
Text	The person selected has a maximum credential expiry date that is before the date requested.
Details	You have requested an expiry date for a device that is after the person's maximum credential expiry date.
Solution	Choose an expiry date for the device that is before the person's maximum credential expiry date, and try again. See the *Editing a PIV applicant* and *Requesting a device for a person* sections in the ***MyID Operator Client*** guide for details.

Error Code	WS50037
Text	Creating a request is not allowed. <details>
Details	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.
Solution	Check the requirements of the customized system, adjust the request to meet those requirements, then try again.

Error Code	WS50038
Text	The selected credential profile is not allowed because the person that requested the job was not allowed to request this credential profile.
Details	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.
Solution	Select a different credential profile, or cancel the request and create a new device request.

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

Error Code	WS50040
Text	You do not have permission to perform this operation against the selected item.
Details	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.
Solution	Make sure that your scope permits you to carry out the appropriate actions for the target user, then try again.

Error Code	WS50041
Text	This action cannot be performed because the user has outstanding adjudications.
Details	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.
Solution	Complete or cancel the existing adjudication.

Error Code	WS50042
Text	The request task type is not supported by the credential profile.
Details	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.
Solution	Select the correct device type for the credential profile.

Error Code	WS50043
Text	This credential profile can only be requested from Request Device.
Details	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.
Solution	Use the correct process for requesting FIDO authenticators.

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

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

Error Code	WS50046
Text	The specified resource is not accessible, or does not exist.
Details	The resource requested needs to be one of the allowed resources.
Solution	The resource should be one of the following • `Base` • `CoreForms` • `CustomerTerms` • `ErrorCodes` • `MobileClient` • `OperatorClient` • `OtherClient` • `ProductTerms` • `ProjectDesigner`

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

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

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

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

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

Error Code	WS50052
Text	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.
Details	If the credential profile does not have the **Ignore User Expiry Date** option set, MyID checks the **Maximum credential expiry date** set for the device owner.. This value must not be before the expiry date of the device.
Solution	Increase the maximum credential expiry date for the device owner, change the credential profile of the device to set the **Ignore User Expiry Date** option, or issue a device to the user which does not exceed their maximum credential expiry date.

Error Code	WS50053
Text	The capabilities of the selected credential profile are not supported by this operation.
Details	Certain operations may allow only certain card capabilities for a device. For example, **Request Update** allows only Contact, Microsoft Virtual Smart Card, Identity Agent, or Windows Hello for Business devices. 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 *Requesting a Derived Credential* section in the ***Derived Credentials Self-Service Request Portal*** guide.
Solution	Select a credential profile that has one of the capabilities specified for the operation. You can check the JSON conditions in the `Operations` table of the MyID database for that operation ID.

Error Code	WS50054
Text	The selected credential profile has different capabilities to the current device credential profile.
Details	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.
Solution	Examine the previous profile in the **Credential Profiles** workflow, and create the new credential profile for the device to have the same card capabilities.

Error Code	WS50055
Text	The user has an existing request or device that exists with a different exclusive group, the request cannot be added.
Details	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.
Solution	See the *Exclusive Group* section in the ***Administration Guide*** for details.

Error Code	WS50056
Text	The user has an existing request or device that exists with a different exclusive group, the request cannot be validated.
Details	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.
Solution	See the *Exclusive Group* section in the ***Administration Guide*** for details.

Error Code	WS50057
Text	The user has an existing request or device that exists with a different exclusive group, the request cannot be collected.
Details	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.
Solution	See the *Exclusive Group* section in the ***Administration Guide*** for details.

Error Code	WS50058
Text	The selected user has no suitable biometric samples for EFT export.
Details	You have selected a person who does not have suitable biometric samples enrolled, and therefore cannot have their biometric samples exported as EFT. 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.
Solution	Ensure the selected person has the appropriate biometrics enrolled, or select a different person.

Error Code	WS50059
Text	The selected user has no fingerprint rolls available for EFT export.
Details	You have selected a person who does not have suitable fingerprint rolls captured, and therefore cannot have their biometric samples exported as EFT. 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.
Solution	Ensure the selected person has the appropriate biometrics enrolled, or select a different person.

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

Error Code	WS50061
Text	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.
Details	The issuance of the device would place it in a group that has expired.
Solution	Update the group to expire in the future and repeat the operation. See the *Controlling device assignments for groups* section in the ***Administration Guide*** for details.

Error Code	WS50062
Text	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.
Details	The issuance of the device would cause the device limit for the group to be exceeded and so has been prevented.
Solution	Increase the group device limit and repeat the operation. See the *Controlling device assignments for groups* section in the ***Administration Guide*** for details.

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

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

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

Error Code	WS50066
Text	This device already has an active request.
Details	You have attempted to request a cancellation for a device that already has an active cancellation request.
Solution	Approve, reject, or cancel the original cancellation request for the device.

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

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

Error Code	WS50069
Text	The operator does not have sufficient scope to view the requests of this account
Details	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.
Solution	Choose a different person, or amend your account to increase your scope.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Error Code	WS50088
Text	The device has to be actively issued to change owner.
Details	You have tried to reassign a device that is not active.
Solution	Make sure the device is active before you attempt to reassign it.

Error Code	WS50089
Text	Cannot reassign device with additional identity certificates on it.
Details	You have tried to reassign a device that contains additional identity certificates.
Solution	You cannot reassign a device that contains additional identity certificates. Select a different device.

Error Code	WS50090
Text	Cannot reassign device with a credential profile marked as key recovery.
Details	You have tried to reassign a device that is used for key recovery.
Solution	You cannot reassign a device that is used for key recovery, as it may contain certificates for another person. Select a different device.

Error Code	WS50091
Text	Cannot reassign device when the credential profile does not have an encoding capability of type contact.
Details	You have tried to reassign a device that is not a Contact smart card.
Solution	You can use the reassign option only for devices that have a credential profiles set up for Contact smart cards. Select a different device.

Error Code	WS50092
Text	Editing of additional identities is forbidden for imported additional identities.
Details	You have attempted to edit an additional identity that was imported; this is not permitted. You can edit only those additional identities that you created manually.
Solution	Select an additional identity that you have created manually instead. See the *Editing an additional identity* section in the ***MyID Operator Client*** guide.

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

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

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

8 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.

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

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

Error Code	3102131
Text	Failed to load image. This is usually because it is in an unsupported format.
Details	The MyID Image Editor was unable to process the provided data as a supported image type.
Solution	Ensure the provided image is in one of the supported formats: • JPEG (`*.jpg`, `*.jpeg`) • Bitmap (`*.bmp`) • Graphics Interchange Format (`*.gif`) • Portable Network Graphics (`*.png`)

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

Error Code	10000225
Text	Configuration File Error: Server setting not found. Make sure you have provided a valid server or SSA install path.
Details	No Server has been specified, and there is no path to a Self-Service App installation with a Server value in its configuration file.
Solution	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 `SsaPath` node contains the correct path to the Self-Service App program file.

Error Code	10000226
Text	Configuration File Error: DataSource setting not found. Make sure you have provided a valid DataSource or SSA install path.
Details	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.
Solution	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 `SsaPath` node contains the correct path to the Self-Service App program file.

Error Code	10000229
Text	A MyID Client Service window is already open. Please close any MyID Client Service windows and try again.
Details	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.
Solution	Close any open MyID Client Service windows and try again.

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

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

Error Code	10000235
Text	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.
Details	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.
Solution	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.

Error Code	10000228
Text	Failed to bind to local web-socket port. Make sure another application is not running and consuming your port.
Details	The MyID Client Service was unable to establish a binding to the port configured in the WebSocketPort configuration (default of 8081).
Solution	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. 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 *Enabling or disabling the MyID Client WebSocket Service* section in the ***Installation and Configuration Guide*** for details.

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

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

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

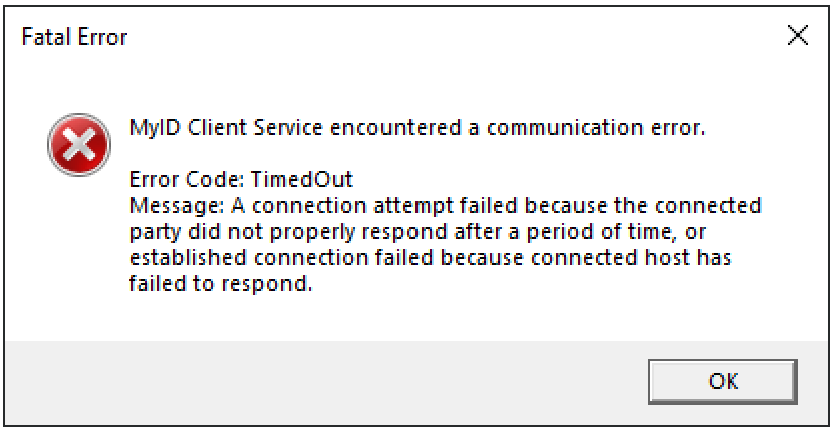
8.1 .NET Networking errors

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:



Fatal Error

MyID Client Service encountered a communication error.

Error Code: TimedOut
Message: A connection attempt failed because the connected party did not properly respond after a period of time, or established connection failed because connected host has failed to respond.

For more information, see the Microsoft documentation:

docs.microsoft.com/en-us/dotnet/api/system.net.sockets.socketerror