MyID

Self-Service App

Installation and Configuration Guide

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

Document reference: IMP1852-07 June 2017

Copyright

Conventions Used in this Document

- Lists:
  - Numbered lists are used to show the steps involved in completing a task when the order is important
  - Bulleted lists are used when the order is unimportant or to show alternatives

- **Bold** is used for menu items and for labels.

  For example:
  - "Record a valid email address in **'From' email address**"
  - Select **Save** from the **File** menu

- *Italic* is used for emphasis and to indicate references to other sections within the current document:

  For example:
  - "Copy the file *before* starting the installation"
  - "See *Issuing a Card* for further information"

- ***Bold and italic*** are used to identify the titles of other documents.

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

  Unless otherwise explicitly stated, all referenced documentation is available on the installation CD.

- A `fixed width` font is used where the identification of spaces is important, including filenames, example SQL queries and any entries made directly into configuration files or the database.

- **Notes** are used to provide further information, including any prerequisites or configuration additional to the standard specifications.

  For example:

  Note: This issue only occurs if updating from a previous version.

- Warnings are used to indicate where failure to follow a particular instruction may result in either loss of data or the need to manually configure elements of the system.

  For example:

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

Contents

1 Introduction

This document describes the installation and configuration of the MyID® Self-Service App.

This application allow cardholders to collect, activate and update the devices that have been issued to them by the MyID system without requiring operator access to MyID itself.

- The Self-Service App is designed to run on an individual user's PC and prompt the cardholder when their device needs to be collected, activated or updated.
- The Self-Service App Automation Mode is designed to collect device identities or carry out VSC lock operations without user interaction. When the app runs, if an appropriate job is available, it processes it from the MyID server.

The user interface is designed to guide users through the process without requiring extensive training or documentation.

1.1 Prerequisites and installation

For prerequisites and installation instructions, see the readme document provided with this release, which provides details of the MyID versions, software updates and other software you need to have installed on your server and clients.

- Self-Service App client

  Provided in this software update. Includes the Self-Service App Automation Mode.

- Web Service Architecture

  You must have the following MyID web services installed on your web server:

  - MyID Process Driver
  - MyID Data Source

  See the ***Web Service Architecture Installation and Configuration Guide*** for details. This document is provided with MyID.

  You are recommended to set up SSL on the connection between the Self-Service application clients and the MyID web services. See section *2.3*, *Setting up SSL* for details.

- MyID BioPack

  Provided as a separate MyID software update.

  If you intend to use biometric readers on the client PCs, you must install BioPack package of biometric components both on the MyID application server and on each client PC on which you want to use biometrics.

1.1.1 Communication between the Self-Service App and MyID

To allow your clients to communicate with the MyID server, your PC must be able to communicate with the URLs of the MyID mobile web services; for example:

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

```
https://myserver/MyIDDataSource/
```

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

1.1.2 Minimum client PC specifications

Your client PC must meet the following minimum specifications:

- 1 GHz 32-bit (x86) or 64-bit (x64) processor
- 1 GB RAM (32-bit) or 2 GB RAM (64-bit)
- 2 GB hard disk free space
- Screen resolution of 1024x768
- Network access

1.1.3 Supported operating systems

The Self-Service App is supported on the following client operating systems:

- Windows 7 (32-bit)
- Windows 7 (64-bit)
- Windows 8.1 (32-bit)
- Windows 8.1 (64-bit)
- Windows 10 (32-bit)
- Windows 10 (64-bit)

Note: The Self-Service App Automation Mode requires a 64-bit version of Windows 7.

1.1.4 Supported biometrics

The Self-Service App supports the following devices for biometric verification:

- Cross Match Verifier 300 (Windows 7 32-bit only)
- Cross Match Verifier 310 (Windows 7 32-bit and 64-bit only)
- Precise MC-250
- SecuGen Hamster IV
- SecuGen iD-USB-SC/PIV

Note: Do not attach Precise and CrossMatch devices to the same client PC, or you may experience problems that prevent you from scanning fingerprints.

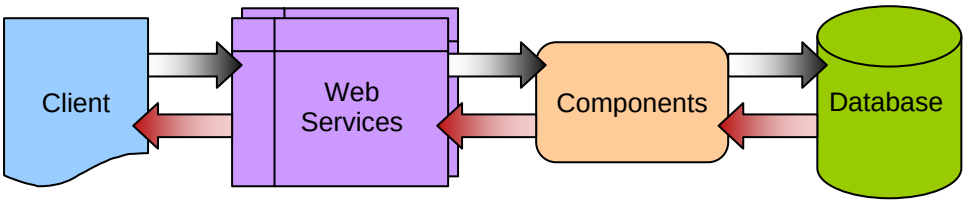
Note: The Cross Match matching library is not currently supported on MyID servers running Windows Server 2012. However, you can use the Cross Match Verifier reader on clients connected to a Windows Server 2012 client if the fingerprints were enrolled using Precise and the matching library is set to Precise. See the ***Cross Match Integration Guide*** for details.

Biometric verification is supported only on MyID PIV systems. It is not supported on MyID Enterprise systems.

Biometric verification is not supported on Windows 10.

1.2 Overview

1.2.1 Architecture



The Self-Service App passes requests through HTTP or HTTPS to the MyID Data Source and MyID Process Driver web services; both services are required for full operation. The web services communicate using DCOM with the MyID components on the application server; these components provide the business logic and communicate with the MyID database. Responses are returned to the client through the MyID web services.

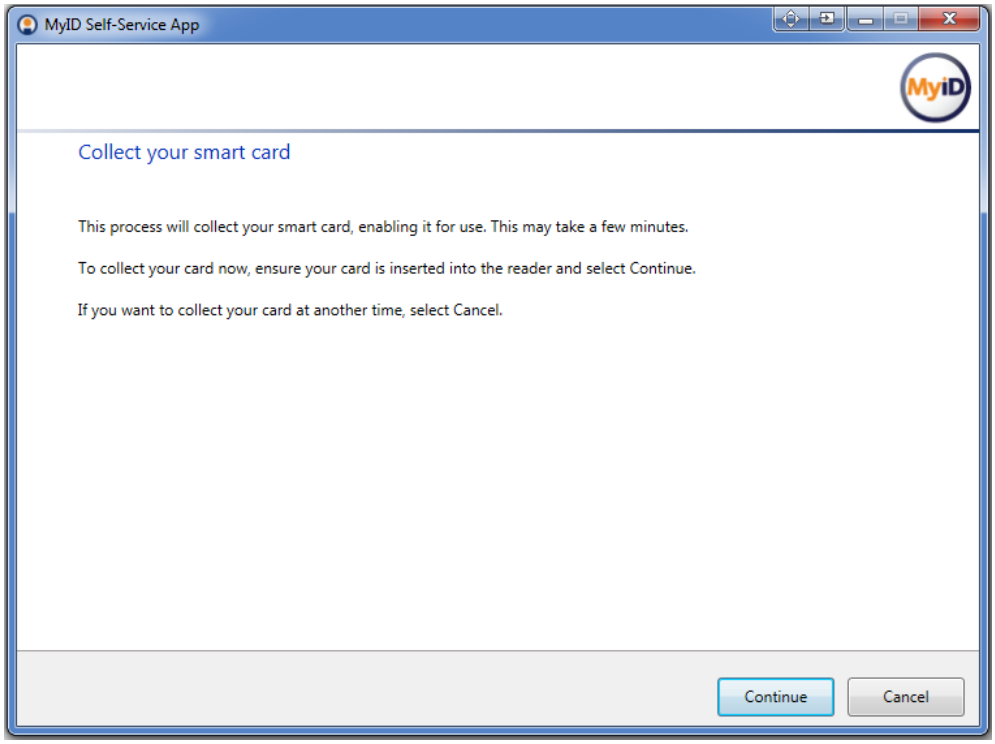
The web services, components and database may be on separate servers, or on the same server. The two web services must be installed on the same server.

The range of operations you can perform with the Self-Service App depends on the edition of MyID you are using – you can perform different operations with the PIV and Enterprise editions.

1.2.2 Self-Service App

The Self-Service App is designed to run on the cardholder's own PC and to provide notifications whenever the cardholder needs to update their device.

You can set up the Self-Service App to be run manually by the cardholder to check for updates, to run automatically at Windows logon, to run periodically as a scheduled task, and so on.



A simple scenario would be:

1. The cardholder logs on to their own PC.
2. The Self-Service App starts automatically.
3. The Self-Service App checks the MyID server for pending jobs for the cardholder.
4. If there are any jobs outstanding – for example, the collection of a new smart card – the Self-Service App pops up a notification in the Windows system tray.

   Note: If the user is collecting a job that supports both contact and virtual smart cards (VSCs), the Self-Service App gives preference to the collection of a VSC over a contact card.
5. The cardholder clicks the notification bubble and the Self-Service App window appears.
6. The Self-Service App guides the cardholder through updating their device.

   If there are no jobs available, the Self-Service App shuts down without alerting the cardholder. This ensures that the cardholder is only presented with information when they need to make a decision.

1.2.3 Self-Service App Automation Mode

The Self-Service App Automation Mode is designed to run on the cardholder's own PC and to collect device identities or carry out VSC lock operations without user interaction.

You can set up the Self-Service App Automation Mode to run automatically at Windows logon, to run periodically as a scheduled task, and so on.

Note: You must run the Self-Service App Automation Mode as an administrator, as the application requires access to the TPM to collect device identities.

A simple scenario for device identities would be:

1. The cardholder logs on to their own PC.
2. The Self-Service App Automation Mode starts automatically.
3. The Self-Service App Automation Mode checks the MyID server for requests for device identities.
4. If there is a pending request for a device identity for the current PC, the Self-Service App Automation Mode collects the device identity and installs it on the TPM on the PC.

   Note: If the PC previously had a device identity installed, any old certificates are removed from the TPM on the PC. Only the new certificate is retained.

   No user interaction is required.

1.2.4 Authentication

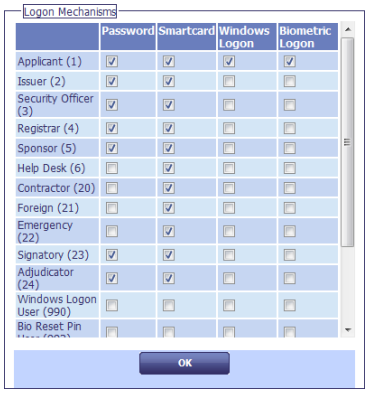
The cardholder can authenticate to the MyID server using the following methods:

Method	Self-Service App	Self-Service App Automation Mode
Smart card logon	Y	N
Security phrase logon	Y	Y
Windows authentication	Y	Y
Authentication codes	Y	N

The cardholder can also use various combinations; for example, smart card logon backed up by authentication codes.

See the MyID documentation for details of setting up the various types of authentication. The Self-Service App uses the same configuration for authentication as MyID Desktop.

When you set up the roles for access to particular workflows, you must make sure that the role has the correct logon methods; for example, if you add all the workflows to the Applicant role, and are using security phrase logon, you must set the Applicant role to have access to the Password logon mechanism.



1.3 Self-Service App features

Control over which features are available to Self-Service App users is maintained within MyID by using the standard roles mechanism. The cardholder must be granted a role that has access to the correct workflows.

Use the **Edit Roles** workflow to specify which workflows are available.

The Self-Service App can carry out the following operations:

- Check for outstanding jobs for the current user.
- Collect a card.

  Requires access to the **Collect My Card** workflow.
- Activate a card.

  Requires access to the **Activate Card** workflow.

  Note: For card activation, you must use Javacards that can have their keys locked; for example, Oberthur ID-One PIV cards. See the ***Administration Guide*** for more details of card activation.
- Update a card.

  Requires access to the **Collect My Updates** workflow.
- Collect a replacement card.

  Requires access to the **Collect My Card** workflow.
- Collect a certificate renewal.

  Requires access to the **Collect My Certificates** workflow.

1.4 Self-Service App Automation Mode features

The Self-Service App Automation Mode supports features that require no user interaction. The MyID user used to launch the app must be granted roles that have access to the correct workflows.

Use the **Edit Roles** workflow to specify which workflows are available.

- Collect a device identity.

  Requires access to the **Collect Device Identity** workflow.

  This feature collects the first, and only the first, device identity that has been requested for the machine. If it attempts to collect another, an error appears saying that a device identity has already been issued.

  This feature also requires a turned-on, initialized TPM, with ownership taken by the current operating system. Use the Trusted Platform Module (TPM) Management MMC snap-in to set this up.

  You must have the TPM Plug-in Module installed on your PC. Contact customer support for more information on obtaining this module, quoting reference SUP-102.

Warning:	Initializing a TPM, or taking ownership when you did not already have ownership, will clear any existing keys stored on the TPM.

- Lock or unlock a VSC.

  Requires access to the **Update VSC** workflow.

  This feature carries out the actions requested by the **Manage VSC Access** and **Unlock VSC Temporary Access** workflows in MyID.

  When you launch the Self-Service App Automation Mode using a MyID username and password, you are strongly recommended to use a specially-created MyID user that has access only to the required workflow. Create a new role, grant it access only to the **Update VSC** workflow, create a new user with access only to that role, and set the user's security phrases. The MyID user must also have sufficient scope to carry out operations on behalf of the end user.

2 Configuring the Self-Service App

2.1 Server location

The Self-Service App is configured to communicate with the MyID Web Services server when you install the application. If you want to change the server, you can edit the configuration file.

To edit the configuration file:

1. On the client PC, back up the `MyIDApp.exe.config` file in the following folder:

   ```
   C:\Program Files (x86)\Intercede\MyIDApp\Self Service Application\
   ```

   For the Self-Service App Automation Mode, this is the `MyIDApp64.exe.config` file in the following folder:

   ```
   C:\Program Files (x86)\Intercede\MyIDApp\Self Service Application Automation Mode\
   ```

2. Using a text editor, open the config file.

   Note: Make the changes to the config file exactly as shown. The case is important.

3. Edit the `value` parameter in the following line:

   ```
   <add key="Server" value="http://myserver.example.com/"></add>
   ```

   For example:

   ```
   <add key="Server" value="http://myserver2.example.com/"></add>
   ```

4. Save the configuration file.

2.2 Timeout

The Self-Service Application is configured to time out after 30 seconds on some workflow stages. This ends the current workflow after that period of inactivity. If you want to change the timeout, you can edit the configuration file.

To edit the configuration file:

1. On the client PC, back up the `MyIDApp.exe.config` file in the following folder:

   ```
   C:\Program Files (x86)\Intercede\MyIDApp\Self Service Application\
   ```

2. Using a text editor, open the `MyIDApp.exe.config` file.

   Note: Make the changes to the config file exactly as shown. The case is important.

3. Edit the `value` parameter in the following line:

   ```
   <add key="PageTimeoutSeconds" value="30"></add>
   ```

   If this line does not exist, you can add it to the `<appSettings>` section.

   For example:

   ```
   <add key="PageTimeoutSeconds" value="60"></add>
   ```

   This increases the timeout to 60 seconds.

4. Save the configuration file.

5. Restart the Self Service App.

2.3 Setting up SSL

2.3.1 One-way SSL

If you want to configure the Self-Service App to use one-way SSL for its communications with the MyID Web Services server, you must install the server's certificate under the Trusted Root Certification Authorities in the user's certificate store.

2.3.2 Two-way SSL

Note: If your server is set up to use two-way SSL, you must set up your client to use two-way SSL. If you do not use the `/ssl` command-line option, an error is displayed.

Note: The Self-Service App does not support two-way SSL using a certificate stored on a smart card.

To use two-way SSL using a specific certificate:

1. Install the client certificate in the user's personal store.

   The client certificate must have the Client Authentication application policy – this has the following OID:

   `1.3.6.1.5.5.7.3.2`

2. Find the client certificate's serial number:

   a) Run the `CertMgr.msc` snap-in.

   b) Expand **Personal > Certificates**.

   c) Double-click the client certificate.

   d) Click the **Details** tab.

3. Run the application using the following command line:

   `myidapp.exe /ssl /sslsn:<serial number>`

   where:

   `<serialnumber>` – the serial number of the client certificate. Enter the serial number without spaces. For example, if the serial number is:

   `62 00 00 00 34 fe 3c a9 a8 1c 98 6a f1 00 00 00 00 00 34`

   use the following command line

   `myidapp.exe /ssl /sslsn:6200000034fe3ca9a81c986af1000000000034`

If you run the application with the `/ssl` command line option but omit the `/sslsn` option, the application carries out the following:

1. The application checks the application settings file for the details of the last certificate that was successfully used to log on.
2. If no details are found, if the certificate is no longer in the personal store, or the server rejects the certificate, the application searches the personal store for certificates that match the issuer DN (optionally set up when you install the application) and have the Client Authentication policy.
3. If more than one certificate is found, the application displays a list of certificates for the user to select.

When the application has successfully logged on to the server using a certificate, the certificate's details are stored in the user's application settings file.

2.4 Integrated Windows Logon

If you set up the MyID server to use Integrated Windows Logon, the Self-Service App can use the cardholder's currently logged-on Windows identity to authenticate to MyID without having to enter passphrases or use a smart card.

Note: For Self-Service App Automation Mode, the logged-on Windows user must have administrative privileges.

To set up integrated Windows logon:

1. In MyID Desktop, from the **Configuration** category, select **Security Settings**.
   a) On the **Logon Mechanisms** tab, make sure that **Integrated Windows Logon** is set to Yes.
   b) Click **Save changes**, then click **Save** to confirm your changes..
2. From the **Configuration** category, select the **Directory Management** workflow and set up a configuration-only directory for MyID.
   a) Click **New** and enter a new name – this can be any value.
   b) Select the **Retrieve Base DN** option..

      MyID attempts to connect to the directory and, if successful, displays a list of possible DNs. Select one of the DNs from the list.

      In most cases, you must select the DN that begins `CN=Configuration`.
   c) Click **Save**.
3. Edit the roles within MyID.
   a) From the **Configuration** category, select **Edit Roles**.
   b) Click the **Logon Methods** option, and select **Windows Logon** for each role you want to be able to log on with Integrated Windows Logon.
   c) Click **OK**.
   d) Click **Save Changes**.

Note: The fields `SAMAccountName` and `Domain` must be stored in MyID when using Integrated Windows Logon.

You must also carry out additional configuration on the web services for Integrated Windows Logon; see the ***Web Service Architecture Installation and Configuration Guide*** for details.

2.5 Running the Self-Service App

The installation program creates a shortcut for the Self-Service App, but you are recommended to run the app in one of the following ways:

- Run the Self-Service App using a Windows Logon script.
- Run the Self-Service App using third-party software.
- Run the Self-Service App by putting a shortcut in the Startup program group.
- Run the Self-Service App using the Windows Scheduler.
- Run the Self-Service App from a hyperlink

To run the Self-Service App from the command line:

1. Open a command prompt and change to the MyIDApp folder:

   ```
   C:\Program Files\Intercede\MyIDApp\Self Service Application\
   ```

   On a 64-bit system, this is:

   ```
   C:\Program Files (x86)\Intercede\MyIDApp\Self Service Application\
   ```

2. Type the following, and press Enter:

```
MyIDApp.exe
```

For information about the additional command-line parameters, see section *3*, *Command Line Arguments*.

2.5.1 Launching the Self-Service App from a hyperlink

When you install the Self-Service App, it registers the `myidssa:` protocol – this means that you can click on hyperlinks on web pages and email messages to launch the Self-Service App.

Using the hyperlink mechanism, you can specify the following:

- Start the Self-Service App in standard mode.

  For example:

  ```
  myidssa://
  ```

- Start the Self-Service App with no popups.

  For example:

  ```
  myidssa:///nopopup
  ```

  Using the bare `myidssa://` link provides no feedback to the end user if there are no jobs to collect – you are recommended to use the `myidssa:///nopopup` link so that the user can see that the Self-Service App has started and checked for outstanding jobs.

- Start the Self-Service App to collect a specific job.

  You can use the `%jobid` placeholder in a MyID email template; this will be substituted with the appropriate job ID when the email message is created.

  For example, if your email template includes the following:

  ```
  Click <a href="myidssa:///jobid:%jobid">Self-Service App</a>
  ```

  when the email message is created, it would become something similar to:

  ```
  Click <a href="myidssa:///jobid:256">Self-Service App</a>
  ```

- Start the Self-Service App to collect a specific job for a specific user.

  To make sure that usernames with spaces are dealt with correctly, you must replace the spaces with + signs. For URLs created from email templates, MyID can do this automatically if you use the correct syntax. For example, if your email template includes the following:

  ```
  Click <a href="myidssa:///jobid:%jobid+/un:{%logonName:URI}">Self-Service App</a>
  ```

  when the email message is created, it would become something similar to:

  ```
  Click <a href="myidssa:///jobid:256+/un:Jane+Smith">Self-Service App</a>
  ```

When you click a link in another application (for example, in a browser, in an email, or within a document) a warning message is displayed. Click **Allow** or **Yes** (depending on the application) to open the link. You may also be able to deselect the **Always ask before opening this type of address** to prevent the warning message from appearing again.

Note: The installation program adds protocol registry entries for the current user only when installed by a non-administrator (`HKEY_CURRENT_USER`), or for all users when installed as an administrator (`HKEY_LOCAL_MACHINE`). The current user entry takes precedence if both are available. This may cause an issue if different users update the software to different versions in different locations. The registry locations are:

- `HKEY_CURRENT_USER\Software\Classes\myidssa`
- `HKEY_LOCAL_MACHINE\Software\Classes\myidssa`

2.6 Running the Self-Service App Automation Mode

Note: You must run the Self-Service App Automation Mode as an administrator, as the application requires access to the TPM to collect device identities.

The Self-Service App Automation Mode uses a 64-bit version of the executable, and therefore requires a 64-bit version of Windows to run.

To run the Self-Service App Automation Mode from the command line:

1. Open a command prompt and change to the MyIDApp folder:

   ```
   C:\Program Files (x86)\Intercede\MyIDApp\Self Service Application Automation Mode\
   ```

2. Type the following, and press Enter:

   ```
   MyIDApp64.exe /a <logon mechanism>
   ```

You must include a logon mechanism on the command line.

To run the Self-Service App Automation Mode using Windows integrated logon:

```
MyIDApp64.exe /a /lw
```

Note: If you are using Windows integrated logon, the logged-in user must be an administrator.

To run the Self-Service App Automation Mode using passwords:

```
MyIDApp64.exe /a /lp /un:username /pw:password1 /pw:password2
```

where:

- `username` – the MyID username.
- `password1` – the answer to the first security question.
- `password2` – the answer to the second security question.

The order of the security questions is the same as the order that appears in MyID Desktop if you are using security phrase logon.

2.7 Translating the user interface

The Self-Service App supports translation of the on-screen text to change the terminology used or to change the language completely.

Contact Intercede customer support for details, quoting reference SUP-71.

2.8 Logging

You can set up your Self-Service App to write debug information to a log file. You may need to provide this information to Intercede customer support.

Contact customer support quoting reference SUP-236.

2.9 Job filtering

You may not want every client application to handle every job that is available for the cardholder. For example, you may want your Self-Service Kiosks to handle only activation jobs, and require your cardholders to use their Self-Service Apps to handle all other jobs on their own workstations. You can set up the web service to provide a customized list of jobs.

See the ***Web Service Architecture Installation and Configuration Guide*** for details of setting up job filtering; this document is provided with the software update that installs the web services.

2.10 Specifying the target user

The user identifier for the Self-Service App that is passed to the MyID server is based on the Windows logon name of the user. This is then matched against the SAM Account Name stored for the user in the MyID database.

You can change this user identifier in two ways:

- Set the Windows environment variable `MYID_USERNAME` to the identifier you want to use. This value is used instead of the Windows logon name for all users on the PC.
- Alter the `ws_LogonJobs` view in the MyID database to change the definition of the `UserIdentifier` field to point to a different field. This allows you to compare the user identifier to a field other than the SAM Account Name for the user.

3 Command Line Arguments

The Self-Service App depends on command-line arguments for the `MyIDApp.exe` program. These command-line arguments determine the mode of the app, the authentication used, and so on.

For basic information about starting the app in its various modes, see the following sections:

- *2.5*, *Running the Self-Service App*
- *2.6*, *Running the Self-Service App Automation Mode*

This section contains a reference for the command line arguments.

You can specify the arguments at the Windows command prompt or as part of a Windows shortcut.

3.1 Command line reference

Syntax:

```
MyIDApp.exe <display-mode> <authentication-mode> <credentials>
<additional>
```

where:

- `<display-mode>` is one of the following:
  - `/h` – Displays the on-screen help text.
  - `/?` – Displays the on-screen help text.
  - `/err` – Displays the list of exit codes.
- `<authentication-mode>` is one of the following:
  - `/lp` – Security phrase logon provider.
  - `/lw` – Integrated Windows logon provider.

  Note: The authentication mode is used for the Self-Service App Automation Mode only.
- `<credentials>` includes the following when you have specified `/lp` as the authentication mode:
  - `/un:<username>` – The MyID username.

    Note: SSA treats usernames as URI-encoded; for example:

    `Jane+Smith`

    is treated as `Jane Smith`, with a space.
  - `/pw:<security phrase>` – The answers to a security phrase. You must include as many `/pw` arguments as there are security phrases set up for the user. The order of the security questions is the same as the order that appears on the MyID website if you are using security phrase logon.

  Note: The credentials are used for the Self-Service App Automation Mode only.

- `<additional>` may include the following:
  - `/a` – Starts the Self-Service App Automation Mode for collecting device identities.
  - `/nopopup` – The Self-Service App runs with no pop-up notification balloon messages. All messages appear within the main window.

    Note: You cannot use the `/nopopup` option with the Self-Service App Automation Mode.
  - `/hidecancel` – Removes the Cancel button from any page that displays it, and removes the minimize, maximize, and close buttons. This allows you to prevent users from cancelling operations.

    When you use `/hidecancel`, you must also use `/nopopup`.

    Note: The one exception where a cancel option still appears is if your system is not completely configured for secure issuance (see the **Device Security** page on the **Security Settings** workflow); for example, if **Require Random Security Officer PIN** is set to `No`. Under these circumstances, the Self-Service App displays a warning that the system is not fully configured for this type of device; at this stage, it is possible to continue or cancel.
  - `/hidenojobs` – Prevents the No Jobs Found page from being displayed.
  - `/vsconly` – Only Virtual Smart Card jobs will be detected. All other jobs will be ignored.

    Note: You cannot use the `/vsconly` option with the Self-Service App Automation Mode.
  - `/iptonly` – Only Intel Virtual Smart Card jobs will be detected. All other jobs will be ignored.

    Note: You cannot use the `/iptonly` option with the Self-Service App Automation Mode.
  - `/hidewindow` – Hides the Self-Service App window so that no user interface is displayed. Available only with the Self-Service App Automation Mode.
  - `/processalljobs` – Process all of the available jobs. Available only with the Self-Service App Automation Mode. Outputs a list of all jobs processed to the console. See section *4.4*, *Console output*.
  - `/ssl` and `/sslsn` – For two-way SSL. See section *2.3.2*, *Two-way SSL*.

3.2 Examples

Showing the on-screen help text:

```
MyIDApp.exe /?
```

or:

```
MyIDApp.exe /h
```

Showing the exit codes:

```
MyIDApp.exe /err
```

Starting the Self-Service App Automation Mode using security phrase authentication:

```
MyIDApp.exe /lp /un:user1 /pw:password1 /pw:password2 /a
```

If usernames or security phrases contain spaces, surround them in double quotes:

```
MyIDApp.exe /lp /un:"user 1" /pw:"pass word1" /pw:password2 /a
```

Alternatively, for user names, you can replace spaces with + signs:

```
MyIDApp.exe /lp /un:user+1 /pw:"pass word1" /pw:password2 /a
```

To start the Self-Service App Automation Mode using integrated windows authentication:

```
MyIDapp.exe /lw /a
```

4 Application Exit Codes

When the Self-Service App stops running, it sets an exit code that you can use to determine what happened in the last run of the application; for example, if the task succeeded or failed.

This section provides a reference for the possible exit codes.

4.1 Success exit codes

Success exit codes represent states where the application did not encounter any unforeseen problems.

Code	Description	Explanation
`0`	OK	Task completed, no errors reported.
`1`	No jobs available	No jobs were found for the current user when their details were submitted to the web service.

4.2 Failure exit codes

Failure exit codes represent states where the application encountered problems or needs to provide details to the user for alterations to the startup requirements of the application.

Code	Description	Explanation
`100`	Abort	Either the server issued an abort command, in which case the client terminated its operation, or the client encountered an error which caused it to terminate its operation early. If logging is enabled, evidence of the operation should be discoverable near the end of the log file.
`101`	Error	Either the server raised an error command, in which case the client terminated its operation, or the client encountered an error which caused it to terminate its operation early. If logging is enabled, evidence of the operation should be discoverable near the end of the log file.
`102`	Device already issued	When details of the current device (either TPM or smartcard) were submitted to the web service the determination was that the device was already issued. Therefore it is not possible to issue again to that device until it is cancelled.
`103`	Automation mode argument error	If the app is started with the `/a` command line argument but no additional authentication details are presented, the app will report an automation mode argument error.

Code	Description	Explanation
104	User name not provided	The username command line argument was empty or was not specified.
105	Password not provided	The password command line argument was empty or was not specified
106	Logon provider not provided	The logon provider command line argument was empty or was not specified.
107	Connectivity error	There was an error attempting to connect to the MyID Web Service. This could be due to network connectivity issues or server errors.
108	Unknown error	An unknown error was encountered. If logging is enabled, evidence of the issue should be discoverable in the log.
109	Unknown command switch	A command line argument was provided which is not part of the set of recognized command line arguments.
110	Authentication failed	Using the authentication details provided, the application could not authenticate the user against the MyID Web Service.
111	Unauthorized workflow access	When starting a workflow, the current user does not have the correct role permissions in order to access the workflow.
112	User terminated process	The user elected to terminate the MyID Self-Service app.
113	Client components not installed	Detection of the required MyID client components failed. Reinstall the Self-Service App.
114	Invalid CPU architecture	The current configuration conflicted with the CPU architecture.
115	Invalid command switch	A command line argument was provided but was either incomplete or a duplicate of an existing command line argument.
116	Component Verification Check Failed	The Self-Service App's components are not registered correctly or are not present.
117	Out Of Date Application	The version of the Self-Service App you are using is out of date.
118	Application is already running	You have attempted to run the Self-Service App when it is already running.
119	Logon provider parameters (`/lp`, `lw`) are only valid in conjunction with the automation mode (`/a`) switch	You have specified logon provider parameters, but have not specified the Automation Mode parameter.

Code	Description	Explanation
120	Mutual SSL has been requested but the server URL is unsecured.	You have specified `/ssl` on the command line, but the server does not use HTTPS.
121	Process all jobs (/processalljobs) is only valid in conjunction with the automation mode (/a) switch	The `/processalljobs` option is available only in Automation Mode.
122	Hide window (/hidewindow) is only valid in conjunction with the automation mode (/a) switch	The `/hidewindow` option is available only in Automation Mode.
123	Reserved for future use	
124	When using automation mode, the card that is needed to perform the action is unavailable.	Make sure the card is available.
125	When collecting multiple jobs using /processalljobs an error has occurred.	Check the console for errors.

4.3 Retrieving application exit codes

4.3.1 Displaying exit codes

You can display the list of exit codes by running the following at the command line:

```
MyIDApp.exe /err
```

To view the exit code from the last run of the application, at the Windows command prompt, type:

```
echo %errorlevel%
```

In Powershell, you can use `$LASTEXITCODE`.

4.3.2 Batch files

If you execute the app from a Windows batch file, you can capture the application exit codes and display them to the user.

Note: If you use a batch file to run the Self-Service App Automation Mode to collect device identities, you must run the batch file as an administrator.

For example, copy the following text into a `.bat` file:

```
@echo off
start /wait MyIDApp.exe /lp /un:"Simple User" /pw:"pass1" /pw:"pass2" /a
echo "Exit Code: " %errorlevel%
```

You can use the tables in sections 4.1 and 4.2 to determine the meaning of the code and display this to the end user; for example:

```
@echo off
start /wait MyIDApp.exe /lp /un:"Simple User" /pw:"pass1" /pw:"pass2" /a
IF %errorlevel% EQU 114 (echo "Invalid CPU Architecture")
IF %errorlevel% EQU 0 (echo "Complete")
```

4.4 Console output

When passing the `/processAllJobs` command line, the Self-Service App outputs the status of the processed jobs to the console. For example, if there were three jobs processed it would appear as:

```
Self Service Application Automation Mode
Job <ID> - <Application Return Code>
Job <ID> - <Application Return Code>
Job <ID> - <Application Return Code>
```

In this example:

- `<ID>` would be the ID of the job.
- `<Application Return Code>` would represent the status of this job..

  The application exit code would be either:

  - `0` if all jobs have been collected successfully.
  - `125` if one of the jobs have failed..

Example:

```
Self Service Application Automation Mode
Job 256 - 0
Job 267 - 101
Job 278 - 0
```

If there was a terminal error that stopped processing of the jobs it would appear as:

```
Self Service Application Automation Mode
Application terminated with <Application Return Code>
```

- `<Application Return Code>` would be the numeric value of the exit code. The application exit code would be the same value.

The following would be output if no jobs are found:

```
Self Service Application Automation Mode
0 Jobs found
```

- The application exit code would be `1` to state that no jobs have been found.

5 Troubleshooting

Code	Possible causes	Notes
103	For automation mode, the password logon provider is specified, but the user name is empty, or security phrases are not provided.	
104	User name is empty.	
105	Security phrases are not provided.	
106	No logon provider specified; that is, `/lp` or `/lw`.	
107	Attempting to connect to a non-existent server using the IP address or fully qualified domain name specified in the `MyIDApp.exe.config` file. Server is unavailable. SSL is incorrectly configured. No network connectivity.	
109	Unknown command line arguments specified. See section *3.1*, *Command line reference* for a list of accepted commands. Display mode not provided.	
110	Incorrect username. Incorrect security phrases.	If the username or security phrase words contain spaces, you must enclose the words in double quotes.
113	Incorrect or incompatible client components installed.	Reinstall the Self-Service App.
114	You attempted to run the Self-Service App on a 32-bit machine referencing 64-bit components.	This generally occurs if you attempt to collect a device identity on a machine that is incapable of supporting the 64-bit client components.
115	More than one display mode is encountered – `/d`, `/k`. More than one authentication mode is encountered – `/lp`, `/lw`. More than one username argument is encountered – `/un`. More than one automation mode is encountered – `/a`.	
119	One of the logon parameters – (`/lw`, `/lp`, `/pw`, or `/un` is encountered on the command line, but the automation mode parameter `/a` is missing.	

You may also experience the following error, which does not present an error code:

- **Problems collecting or updating cards**

  If you experience problems when collecting or updating cards, try increasing the **Certificate Refresh Threshold** option on the **Certificates** tab of the **Operation Settings** workflow to a higher value; for example, `45`.

  This problem may manifest with an error similar to:

  ```
  One of the certificates that have been requested for you has failed
  to issue. Please contact your administrator.
  ```

  Note that the certificate may have issued correctly even though the card update has failed.

6 Known Issues

- **CrossMatch Verifier outer edges issue**

  A problem currently exists where the outer edges of the finger print reader do not detect the finger when placed on the scanner plate of a CrossMatch Verifier. A finger placed in the centre of the scanner plate is detected correctly.

- **CrossMatch Verifier first time operations**

  When you scan a fingerprint for the first time using a CrossMatch Verifier, the scan does not work: the capture area lights up but no fingerprint is received by the Self-Service App. However. if you restart the Self-Service App and rescan it operates correctly.

- **Cannot run the Self-Service App if MyID is open in a browser**

  You cannot run the Self-Service App if you have an Internet Explorer window open at the MyID webpage. This is because both the Self-Service App and the MyID web application conflict with each other over card transaction locking.

- **Cannot choose a card in the Self-Service App**

  If you have more than one card reader, the Self-Service App does not allow you to select which reader to use. If you have unissued smart cards in more than one reader, and are collecting a card issuance job, the Self-Service App will select one of the cards without any user intervention.

- **Compatibility with previous versions of the biometric components**

  There is no backwards compatibility with older version of the MyID biometric components (BioPack). A future release will provide backwards compatibility.

- **Capturing command-line output**

  Running the Self-Service application with a parameter such as `/h` `/?` or `/err` runs on a new line in the command window. If you are trying to capture the output, this may cause problems. As a workaround, you can use the start command. For example, to capture the help text to a text file called `output.txt`:

  ```
  start /wait myidapp.exe /h > output.txt
  ```

- **MyID icon still visible in system tray when application is closed**

  When the Self-Service application has finished running, the application icon may still be visible in the Windows system tray. This is due to a known issue in Windows. Moving the mouse pointer over the icon causes the icon to disappear.

- **Cannot collect certificate recovery jobs**

  You cannot use the Self-Service App to collect certificate recovery jobs.

- **Enter PIN twice for card update and certificate renewal jobs**

  If you have terms and conditions enabled for the credential profile, and the **Terms and Conditions During Device Update** configuration option is set to `Yes`, you are required to enter the PIN both before the terms and conditions are displayed and after accepting the terms and conditions.

- **Error when multiple device identity jobs exist for the same device**

  When collecting a device identity using automation mode, if multiple device identity jobs are available for the device, the Self-Service App returns error code 101.

  As a workaround, make sure that only one device identity job exists in MyID for each device.